Cheng Li
Shiwen Mao (Eds.)

230

LNICST

Wireless Internet

10th International Conference, WiCON 2017
Tianjin, China, December 16–17, 2017
Proceedings

Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 230

More information about this series at http://www.springer.com/series/8197

Cheng Li · Shiwen Mao (Eds.)

Wireless Internet

10th International Conference, WiCON 2017
Tianjin, China, December 16–17, 2017
Proceedings

Springer

Editors
Cheng Li
Electrical and Computer Engineering
Memorial University
St. John's, NL
Canada

Shiwen Mao
Electrical and Computer Engineering
Auburn University
Auburn, AL
USA

ISSN 1867-8211 ISSN 1867-822X (electronic)
Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering
ISBN 978-3-319-90801-4 ISBN 978-3-319-90802-1 (eBook)
https://doi.org/10.1007/978-3-319-90802-1

Library of Congress Control Number: 2018943617

Printed on acid-free paper

This Springer imprint is published by the registered company Springer International Publishing AG part of Springer Nature
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

We are delighted to introduce the proceedings of the 10th edition of the 2017 European Alliance for Innovation (EAI) International Wireless Internet Conference (WiCON 2017). Over the years, WiCON has established itself as a research venue where key results in the areas of wireless Internet have appeared. WiCON 2017 continued to serve as a premier international conference to discuss novel research results related to the emerging wireless Internet, wireless communications, and networks.

The technical program of WiCON 2017 consisted of 42 full papers in six tracks to reflect the recent development and advancement in the area. The conference tracks were: Track 1 – Physical Layer (PHY) Track; Track 2 – Medium Access Control (MAC) Track; Track 3 – Network Track; Track 4 – Security Track; Track 5 – Cloud and Big Data Track; and Track 6 – Emerging Internet-of-Things (IoT) Track. We are delighted that this year's event maintained the tradition of high-quality contributions. Aside from the high-quality technical paper presentations, the technical program also featured two keynote speeches, which were given by Dr. Nei Kato from Tohoku University, Japan, and Dr. Ying-Chang Liang from University of Electronic Science and Technology of China. We were delighted to have these two internationally well-known researchers join us to share their vision on future research and development of wireless Internet technologies.

Coordination with the steering chairs, Imrich Chlamtac, Hsiao-Hwa Chen, and Jun Zheng was essential for the success of the conference. We sincerely appreciate their constant support and guidance. It was also a great pleasure to work with such an excellent Organizing Committee team who worked hard in organizing and supporting the conference. In particular, we thank the Technical Program Committee, led by our TPC co-chairs, Dr. Cheng Li and Dr. Shiwen Mao, who completed the peer-review process of technical papers and compiled a high-quality technical program. We are also grateful to the conference sponsor, Tianjin Chengjian University, the local arrangement chairs, Dr. Kun Hao and Dr. Yan Zhang, and the EAI conference managers, Lenka Bilska, for their support and all the authors who submitted their papers to the WiCON 2017 conference.

We strongly believe that WiCON provides a good forum for all researchers, developers, and practitioners to discuss all scientific and technological aspects that are relevant to wireless Internet. We also expect that future WiCON conferences will continue to be as successful and stimulating, as indicated by the contributions presented in this volume.

April 2018

Zhongxian Li
Nirwan Ansari
Cheng Li
Shiwen Mao

Organization

Steering Committee

Imrich Chlamtac	CREATE-NET/EAI, Italy
Athanasios Vasilakos	Kuwait University, Kuwait
Xudong Wang	Shanghai Jiao Tong University, China
Hsiao-Hwa Chen	National Cheng Kung University, Taiwan

Organizing Committee

General Chairs

Zhongxian Li	Tianjin Chengjian University, China
Nirwan Ansari	New Jersey Institute of Technology, USA

Executive Chair

Shudong Liu	Tianjin Chengjian University, P.R. China

Technical Program Committee Chairs

Cheng Li	Memorial University, Canada
Shiwen Mao	Auburn University, USA

Web Chairs

Wei Kong	Tianjin Chengjian University, P.R. China
Zijun Gong	Memorial University, Canada

Publicity and Social Media Chairs

Yi Liu	Tianjin Chengjian University, P.R. China
Lin Ma	Harbin Institute of Technology, China

Workshop Chair

Min Jia	Harbin Institute of Technology, China

Sponsorship and Exhibits Chair

Kun Hao	Tianjin Chengjian University, P.R. China

Publications Chair

Yan Zhang	Tianjin Chengjian University, P.R. China

Keynote Speakers Chair

Weixiao Meng	Communication Research Center, Harbin Institute of Technology, P.R. China

Network Track Chairs

Baoxian Zhang	University of China Academy of Sciences, China
Jalel Ben-Othman	University of Paris 13, France

PhD Track Chairs

Shuai Han	Harbin Institute of Technology, China
Yan Zhang	Tianjin Chengjian University, China

Security Track Chairs

Xiaodong Lin	University of Ontario Institute of Technology, Canada
Aiqing Zhang	Anhui Normal University, China

Local Chair

Kun Hao	Tianjin Chengjian University, P.R. China

Conference Manager

Lenka Bilska	EAI (European Alliance for Innovation), Italy

Technical Program Committee

Network Track

Hao Zhou	University of Science and Technology of China
Yassine Hadjadj-Aoul	IRISA, France
Razvan Stanica	INSA Lyon, France
Imane Horiya Brahmi	University College Dublin, Ireland
Pingguo Huang	Tokyo University of Science, Japan
Rukhsana Ruby	Shenzhen University, China
Yongxiang Zhao	Beijing Jiaotong University, China
Jie Hao	Nanjing University of Aeronautics and Astronautics, China
Zhenzhen Jiao	Institute of Computing Technology
Rui Tian	Beijing University of Technology, China
Baoxian Zhang	Graduate University of Chinese Academy of Sciences, China
Huifang Chen	Zhejiang University, China
Yongrui Chen	University of Chinese Academy of Sciences, China
Shuai Chen	Beijing Jiaotong University, China

Guodong Wang	South Dakota School of Mines and Technology, USA
Jing-Hong Lin	The University of Electro-Communications, China
Zenghua Zhao	Tianjin University, China
Guangsheng Feng	Harbin Engineering University, China

Phy Track

Jie Zeng	Tsinghua University, China
Xuewei Zhang	BUPT
Rukhsana Ruby	Shenzhen University, China
Jingning Wang	The 54th Research Institute of CETC
Tiankui Zhang	Beijing University of Posts and Telecommunications, China
Mu Zhou	CQUPT
Zijun Gong	Memorial University of Newfoundland, Canada
Weidang Lu	Zhejiang University of Technology, China
Xi Peng	HKUST
Xiuhua Li	University of British Columbia, Canada

Security Track

Bogdan Crainicu	Petru Maior University of Tirgu Mures, Romania
Al-Sakib Khan Pathan	Southeast University, Bangladesh
Urko Zurutuza	Mondragon Unibersitatea, Spain
Georgios Karopoulos	University of Athens, Greece
Aiqing Zhang	Anhui Normal University, China
Jianbing Nu	University of Waterloo, Canada
Qi Jiang	Xidian University, China
Bong Jun David Choi	The State University of New York Korea, South Korea
Debiao He	Wuhan University, China
Jun Shao	Zhejiang Gongshang University, China
Qi Li	Tsinghua University, China
Mi We	Shanghai University of Electric Power, China
Dongxiao Liu	University Waterloo, Canada
Meng Li	Beijing Institute of Technology, China
Mohamed Mahmoud	Tennessee Technological University, USA
Yong Deng	University of Ontario Institute of Technology, Canada
Dajiang Chen	University of Electronic Science and Technology of China
Kai Fan	Xidian University, China
Wenjuan Tang	Central South University, China
Sultan Basudan	University of Ontario Institute of Technology, Canada
Mianxiong Dong	Muroran Institute of Technology, Japan
Abdulrahman Alamer	University of Ontario Institute of Technology, Canada
Manaf Bin-Yahya	University of Waterloo, Canada
Mohammed Alhasani	University of Waterloo, Canada

MAC Track

Hakima Chaouchi	Telecom Sud Paris, Institut Mines Telecom, France
Abdelmalik Bachir	Biskra University, Algeria
Yuanzhu Chen	Memorial University, Canada
Yawgeng Chau	Yuan Ze University, Taiwan
Iwan Adhicandra	University of Sydney, Australia
Chao-Lieh Chen	National Kaohsiung First University of Science and Technology, Taiwan
Moussa Ayyash	Chicago State University, USA
Chung Shue Chen	Nokia Bell Labs
Kwang-Cheng Chen	National Taiwan University, Taiwan
Xiaodong Lin	Wilfrid Laurier University, Canada
Shih-Chang Huang	National Formosa University, Taiwan
Ke Zeng	Microsoft
Tai-Lin Chin	National Taiwan University of Science and Technology, Taiwan
Ganguk Hwang	KAIST, South Korea
Yu Gu	Hefei University of Technology, China
Ling-Jyh Chen	Academia Sinica, Taiwan
Emmanouil Kafetzakis	National Centre for Scientific Research Demokritos, Greece
Matthieu Gautier	Université de Rennes 1, IRISA, Inria, France
Shiwen Mao	Auburn University, USA
Mort Naraghi-Pour	Louisiana State University, USA
Ruidong Li	NICT
Ko-Chi Kuo	National Sun Yat-sen University, China
Lu Lu	Technology and Engineering Center for Space Utilization (CSU), Chinese Academy of Science, China
Peng-Yong Kong	Khalifa University, UAE
Abraham O. Fapojuwo	University of Calgary, Calgary, Canada
Peter Han Joo Chong	Auckland University of Technology, New Zealand
Tat Lok	The Chinese University of Hong Kong, SAR China
Parab Kulkarni	Toshiba
Wessam Ajib	University of Quebec at Montreal, Canada

Contents

WSNs and VANETs

Security and IoT

Wireless Networking (II)

Wireless Networking (I)

A Clustering-Based Spectrum Resource Allocation Algorithm for Dense Small Cell Networks

Donghong Jia, Jun Zheng(✉), and Jie Xiao

National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, Jiangsu, People's Republic of China
{donghongjia,junzheng,jiexiao}@seu.edu.cn

Abstract. This paper considers the spectrum resource allocation problem for dense small cell networks, and focuses on a system scenario where small cells are non-uniformly distributed in a macro cell. A clustering-based spectrum resource allocation (CSRA) algorithm is proposed to perform resource allocation for both macro-cell user equipments and small cell user equipments with the objective to maximize the system capacity. To minimize both intra-tier and inter-tier interferences in the system, the concept of clusters is introduced into spectrum resource allocation, and a few principles are correspondingly set for clustering. Moreover, an upper limit for the cluster size is set in for clustering to avoid the formation of a too large cluster, which otherwise would consume a large number of physical resource blocks (PRBs) and thus affect the system capacity. To increase spectrum utilization, all PRBs are allowed to be used by all users in the system. Simulation results show that the proposed CSRA algorithm can significantly increase the system capacity as compared with an existing CDRA algorithm.

Keywords: Clustering · Resource allocation · Small cell

1 Introduction

Dense small cell networks have been widely considered as a key technology for future cellular networks [1–3]. However, the extensive deployment of small cells would cause a sharp increase in interference between small cells and macro cells (inter-tier interference) and between neighboring small cells (intra-tier interference). Resource allocation is an efficient way to manage the inter-cell interference in a dense small cell network. Considerable studies have been conducted to find efficient solutions to resource allocation for mitigating the inter-cell interference [4–9]. In our previous work [9], we presented a clustering-based downlink resource allocation (CDRA) algorithm for a system scenario where small cells are uniformly distributed in a macro cell. For a non-distributed system scenario, however, the CDRA algorithm cannot well address the spectrum resource allocation, which motivated us to conduct this work.

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 3–13, 2018.
https://doi.org/10.1007/978-3-319-90802-1_1

In this paper, we study the spectrum resource allocation problem in dense small cell networks. In particular, we consider a system scenario where small cells are non-uniformly distributed in a macro cell. To minimize both intra-tier and inter-tier interferences, we introduce the concept of clusters into spectrum resource allocation, and correspondingly set a few principles for clustering. Unlike [9], an upper limit for the cluster size is set to avoid the formation of a too large cluster, which otherwise would cause the consumption of a large number of physical resource blocks (PRBs) and thus affect the system capacity. Moreover, all PRBs are allowed to be used by all users in the system, both MUEs and SUEs. Based on these strategies, a clustering-based spectrum resource allocation (CSRA) algorithm is proposed to perform PRB allocation for MUEs and SUEs with the objective to maximize the system capacity. Simulation results are shown to evaluate the performance of the proposed CSRA algorithm.

The rest of the paper is organized as follows. Section 2 formulates the resource allocation problem considered in this paper. Section 3 presents the proposed CSRA algorithm for dense small networks. Section 4 evaluates the performance of the CSRA algorithm based on simulation results. The paper is concluded in Sect. 5.

2 System Model and Problem Formulation

This section describes the system model and formulates the resource allocation problem considered in this paper.

2.1 System Model

Figure 1 illustrates a small cell network system considered in this paper, which consists of one macro cell and multiple small cells. A macro cell base station (MBS) is located in the center of the system, and multiple small cell base stations (SBS) are non-uniformly distributed within the macro cell. Each SBS is connected to the MBS through a backhaul network. Thus, the MBS can share common channel state and resource allocation status information (CSI) with all SBS. The macro cell contains multiple macro-cell user equipments (MUEs) and each small cell contains multiple small-cell user equipments (SUEs), which are randomly distributed in the coverage area of the macro cell and each small cell, respectively. Moreover, orthogonal frequency division multiplexing (OFDM) is employed for data transmission in the system. In spectrum resource allocation, the basic unit is one physical resource block (PRB). All PRBs in the system can be used by all SUEs and MUEs.

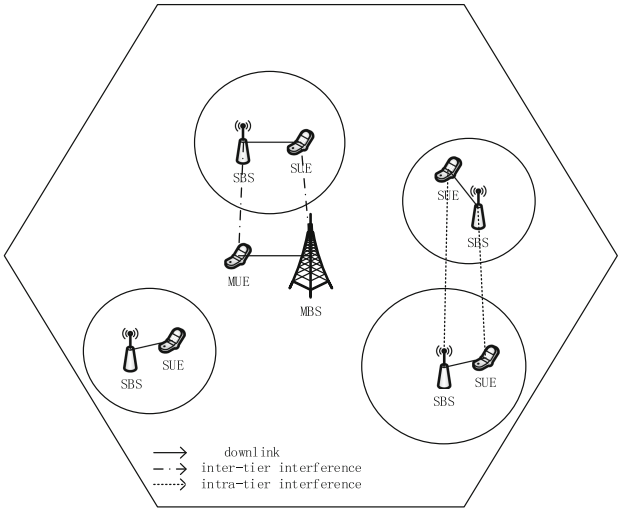


Fig. 1. System model

2.2 Problem Formulation

In this paper, we consider downlink spectrum resource allocation in the dense small cell network system shown in Fig. 1. In resource allocation, we focus on minimizing the inter-tier interference between MUEs and an SUEs sharing the same PRBs, and the intra-tier interference between SUEs in different small cells sharing the same PRBs. Thus, we assume that different MUEs in the macro cell are allocated different PRBs and different SUEs in the same small cell are allocated different PRBs. Meanwhile, different SUEs in different small cells are allowed to share the same PRBs. In this way, there is no interference between different MUEs in the macro cell and between different SUEs in the same small cell. The interference only exists between an MUE in the macro cell and an SUE in a small cell or between different SUEs in different small cells if they share the same PRBs.

Further, we assume that there are N small cells in the macro cell, which are denoted by i ($i = 1, 2, \ldots, N$). There are U_0 MUEs in the macro cell and there are U_i SUEs in small cell i. Thus, the total number of users in the system is

$$U_{Total} = \sum_{i=0}^{L} U_i \tag{1}$$

where $i = 0$ stands for the macro cell. Also, we assume that there are M PRBs available in the system, which are denoted by $k(k = 1, 2, \ldots, M)$. In addition, we assume that each user only needs one PRB for communication in resource allocation.

For resource allocation, we define a resource sharing distribution matrix for each cell, i.e.,

$$\prod_i = [\pi_{jk}]_{\mathrm{K}_i \times \mathrm{M}}, i = 0, 1, 2, \ldots, N; k = 1, 2, \ldots, M; j = 1, 2, \ldots U_i \tag{2}$$

where row j represents the jth user (MUE j or SUE j) in cell i and column k represents the kth PRB, $\pi_{jk} = 1$ indicates that user j is allocated PRB k while $\pi_{jk} = 0$ indicates user j is not allocated PRB k.

For *user j* in cell i, its data rate, denoted by R_{ij}, is given by

$$R_{ij} = \log_2\left(1 + SINR_{ij}\right) \tag{3}$$

where $SINR_{ij}$ represents the signal to interference plus noise ratio (SINR) of user j in cell i, and is given by

$$SINR_{ij} = \frac{P_{ij}G_{ij}}{I_{ij} + N_0} \tag{4}$$

where P_{ij} represents the transmission power from BS i to user j in cell i, G_{ij} represents the channel gain from BS i to user j in cell i, I_{ij} represents the interference at user j in cell i, and N_0 represents the additive white Gaussian noise power.

For SUE j in cell i ($i = 1,\ldots N$), I_{ij} is caused by the transmissions from the MBS and the SBSs of other small cells, who share the same PRB. Thus, I_{ij} is given by

$$I_{ij} = \pi_{0j}P_{0j}h_{0j} + \sum_{i'=1,i'\neq i}^{N} \pi_{i'j}P_{i'j}G_{i'j},\ \forall i, 1 \le i \le N \tag{5}$$

where the first item represents the interference from the MBS while the second represents the interference from other small cells.

For MUE j in cell 0, I_{0j} is given by

$$I_{0j} = \sum_{i=1}^{N} \pi_{ij}P_{ij}h_{ij}. \tag{6}$$

Obviously, I_{0j} is only caused by the SBSs of the small cells.

With the above assumptions and analyses, the downlink resource allocation problem considered in this paper is to find a set of resource allocation matrices $\prod_i (i = 0, 1, 2, \ldots, N)$ so that the sum-rate of all users in the system is maximized, i.e.,

$$\max \sum_{j=1}^{U_0} R_{0j} + \sum_{i=1}^{N}\sum_{j=1}^{U_i} R_{ij} \tag{7}$$

subject to

$$Z_0 \cup Z_1 \cup \ldots \cup Z_i \cup \ldots \cup Z_N \subseteq Z \tag{8}$$

$$\sum_{j=0}^{U_i} P_{ij} \le P_{\max,i}, \forall i \tag{9}$$

$$P_{ij} \geq 0, \forall i, j \tag{10}$$

where Z represents a set of PRBs available in the system, Z_i represents a set of PRBs allocated to the MUEs or SUEs in small cell i; constraint (8) specifies that the number of PRBs allocated to MUEs and SUEs should not be larger than that of the PRBs available in the system; constraint (9) specifies that the maximum sum power of the base station transmitting to all users in cell I is $P_{\max,i}$; constraint (10) enforces that the power used is always non-negative.

3 Clustering-Based Spectrum Resource Allocation Algorithm

This section presents the proposed CSRA algorithm to address the resource allocation problem described in the previous section.

3.1 Overview

The CSRA algorithm is a heuristic algorithm for allocating PRBs for the MUEs and SUEs in the small cell system shown in Fig. 1. It aims to minimize the intra-interference and inter-interference so that the total system capacity is maximized. In a small cell system, if two small cells are close to each other and two SUEs respectively belonging to the two small cells share the same PRB, it would cause a big interference between the two SUEs. The smaller the distance between the two small cells, the bigger the interference. To avoid severe interference between two SUEs in different two small cells, it is expected to allocate different PRBs to such two SUEs in resource allocation. To implement this, we introduce the concept of clusters in PRB allocation. Here, a cluster is defined as a group of small cells, which are close to each other in distance. To avoid intra-tier interferences between SUEs, the SUEs in different small cells within the same cluster should not be allocated the same PRBs in resource allocation.

The CSRA algorithm consists of three components: small cell clustering, small cell priority determination, and spectrum resource allocation. Next we describe the three components in more details.

3.2 Small Cell Clustering

With the introduction of clusters, clustering must be performed before spectrum resource allocation is performed. For this purpose, it is necessary to have reasonable clustering principles first.

As mentioned, if two small cells are close to each other, the intra-tier interference would be severe if the SUEs in the two small cells share the same PRBs. To avoid the potential intra-tier interference, if the distance between two SBSs is smaller than a given threshold, the two small cells should be included in the same cluster, as shown in Fig. 1. Thus, we obtain the first principle for clustering, i.e., the distance between any two small cells in a cluster must be smaller than a given threshold. The threshold value depends

on several system parameters, including the transmission power of an SBS, the macro cell radius, and the channel state.

Based on the first principle, a number of clusters could be formed in the system, and different combinations of clusters could be obtained, which means that the clustering result is not unique. In clustering, it is usually expected to include multiple small cells in one cluster in order to mitigate intra-tier interferences between SUEs; on the other hand, in a non-uniformly distributed dense small cell network system, a cluster could include many small cells, which would cause the consumption of a large number of PRBs. Thus, to avoid the formation of such clusters, the size of a cluster or the number of small cells included in a cluster should be limited by a given value. Based on this analysis, we obtain the second principle for clustering, i.e., a cluster can include multiple small cells, but has an upper limit.

Based on the first two principles, it is found that a small cell could belong to several different clusters. Thus, we obtain the third principle for clustering, i.e., a small cell is allowed to belong to different clusters.

Given the three clustering principles, the MBS can perform clustering to form all small cells in the system into a set of clusters. The main clustering procedures include the following steps:

(1) For each small cell, find out all other small cells with a distance to the small cell smaller than a given threshold.
(2) Find out a set of clusters which may include the current small cell based on the clustering principles.
(3) Repeat steps (1) and (2) until all small cells in the system are considered.
(4) Determine a set of clusters for resource allocation by finding the union of all sets of clusters obtained in steps (1)–(3).

3.3 Small Cell Priority Determination

After clustering, the MBS is supposed to determine the priority of each small cell for resource allocation before resource allocation is performed. In determining the priority of a small cell, two factors are taken into account: one is the size of the largest cluster the small cell belongs to and the other is the number of clusters the small cell belongs to. In general, a small cell in a cluster with a larger size should be assigned a higher priority than a small cell in a cluster with a smaller size. This is because in a larger cluster there are more small cells, which would cause more serious interferences between SUEs if they share the same PRBs. On the other hand, in each cluster, a small cell belonging to more clusters should be assigned a higher priority than other small cells in the cluster. This is because a small cell belonging to more clusters may affect the resource allocation for more small cells. If two small cells belong to the same number of clusters, one of them is randomly selected and is assigned a higher priority than the other. Once the priority of each small cell is determined, the MBS will broadcast the clustering information and small cell priority information to the system. In addition, the MBS itself is assigned a higher priority than all small cells.

3.4 Spectrum Resource Allocation

After the priority of each small cell is determined, the MBS and each SBS will perform PRB allocation for each MUE and SUE, respectively, based on their priorities. To minimize inter-tier and intra-tier interferences between different MUEs and/or SUEs, PRB allocation should adhere to the following allocation principles:

(1) Use orthogonal resources or different PRBs as many as possible;
(2) Allocating different PRBs to MUEs in the macro cell.
(3) Allocating different PRBs to SUEs in the same cluster.
(4) Allowing SUEs in a cluster share PRBs with SUEs not in the same cluster or with MUEs not in the coverage of the cluster if there are no more orthogonal PRBs remaining.

Based on the above allocation principles, the main resource allocation procedures include the following steps:

(1) The MBS performs PRB allocation for MUEs in the macro cell as follow:
    (a) Allocate orthogonal PRBs to all MUEs in the system;
    (b) Once the allocation is completed, the MBS broadcasts a signaling message to inform the system of its completion and the PRB allocation information;
(2) Once receiving the signaling message, the SBS of the small cell with the highest priority among all small cells not allocated will perform PRB allocation for its SUEs:
    (a) Allocate those orthogonal PRBs that have not been allocated first;
    (b) If no orthogonal PRB is available, share PRBs that have been allocated to those SUEs not in the same cluster the SBS belongs to, or share PRBs that have been allocated to those MUEs who are not in the coverage of the same cluster the SBS belongs to;
    (c) Once the SBS of the current small cell completes its resource allocation, it broadcasts a signaling message to inform the system of its completion;
(3) Repeat (2) until resource allocation for all small cells is performed.

4 Simulation Results

This section evaluates the performance of the proposed CSRA algorithm based on simulation results. The simulation experiments were conducted on a simulator that we developed using C++. For evaluation, we compare the CSRA algorithm with the CDRA algorithm proposed in [9] in terms of the total system capacity, i.e., the sum-rate of all users in the system. In the simulation experiments, we used the channel gain path loss model given in [10], i.e.,

$$\mathrm{PL} = 20\lg(\mathrm{d[m]}) + 20\lg(\mathrm{f[MHz]}) - 27.56 \tag{11}$$

The upper limit of the cluster size is set to one third of the number of small cells in the system. For simplicity, we assume that the number of SUEs in each small cell is equal. The parameters used in the simulation experiments are summarized in Table 1.

Table 1. Simulation Parameters

Parameter	Value
MBS transmission power	43 dBm
SBS transmission power	24 dBm
Number of PRBs	100
Macro cell radius	500 m
Small cell radius	50 m
Distance threshold	200 m
Spectrum frequency	2 GHz
PRB bandwidth	180 kHz
White noise power	−174 dB/Hz

Figure 2 shows the total system capacity with CSRA and CDRA, respectively, under different number of SUEs in each small cell. It is seen that CSRA can basically achieve a larger system capacity than CDRA. On the other hand, when the number of SUEs in each small cell is smaller, the total system capacities with both CSRA and CDRA increase as well. This is because in this case there are sufficient PRBs available for the SUEs. When the number of SUEs in each small cell increases beyond a certain number, the system capacities start to decline after reaching a peak. This is because in this case the number of PRBs in the system cannot accommodate the larger number of SUEs. More PRBs are shared and more interference is caused, resulting in the decrease of the total system capacity.

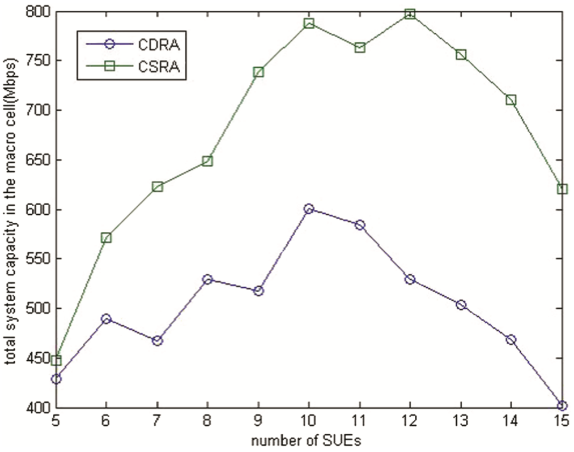


Fig. 2. Total system capacity vs number of SUEs in each small cell ($U_0 = 80$)

Figure 3 shows the total system capacity with CSRA and CDRA, respectively, under different numbers of MUEs in the macro cell. It is seen that CSRA can basically achieve a larger system capacity than CDRA. On the other hand, when the number of MUEs is smaller, the total system capacities with both CSRA and CDRA increase as well. This

is because in this case there are sufficient PRBs available for the MUEs. When the number of MUEs increases beyond a certain number, the system capacities start to decline after reaching a peak. This is because in this case the number of PRBs in the system cannot accommodate the larger number of MUEs. More PRBs are shared and more interference is caused, resulting in the decrease of the total system capacity.

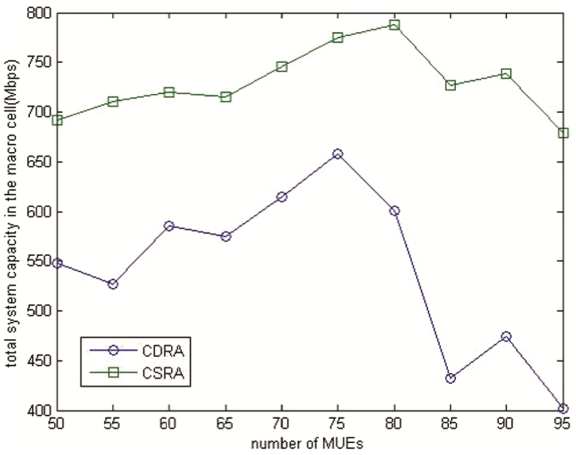


Fig. 3. Total system capacity vs number of MUEs ($U_i = 10$)

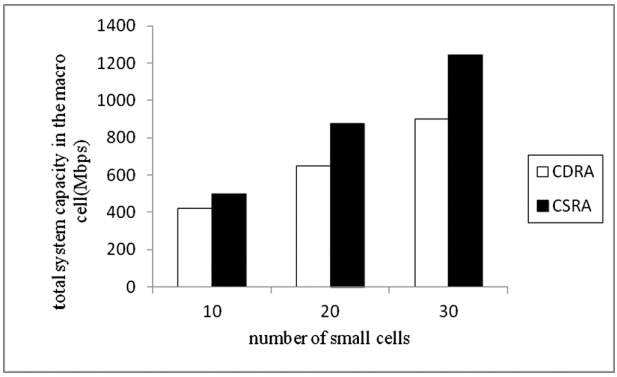


Fig. 4. Total system capacity vs number of small cells ($U_0 = 80$, $U_i = 12$)

Figure 4 shows the total system capacity with CSRA and CDRA, respectively, under different numbers of small cells in the system. It is seen that as the number of small cells in the system increases, the total system capacities with both ACDRA and CDRA increase as well. Meanwhile, the total system capacity with CSRA is larger than that with CDRA. The difference of the total system capacities with the two algorithms becomes larger as the number of small cells in the system increases.

Figure 5 shows the cumulative distribution function (CDF) of the system capacity with CSRA and CDRA, respectively. It is seen that CSRA outperforms CDRA in terms

of the system capacity. With CDRA, the data rates of about 40% users in the system are lower than 0.5 bps. In contrast, with CSRA, almost no user has a data rate lower than 0.5 bps.

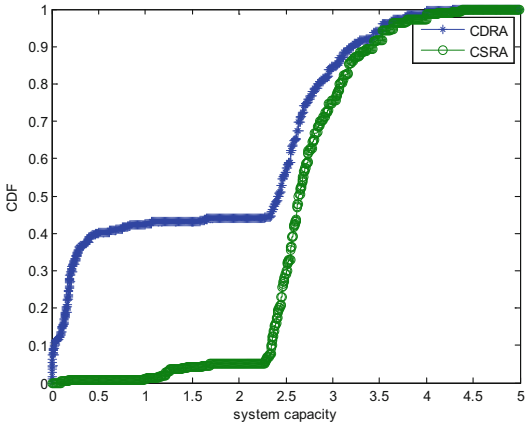


Fig. 5. CDF of system capacity ($U_0 = 90$, $U_i = 7$)

5 Conclusions

In this paper, we studied the spectrum resource allocation problem in dense small cell networks, and focused on a system scenario where small cells are non-uniformly distributed in a macro cell. The CSRA algorithm is proposed to perform PRB allocation for MUEs and SUEs with the objective to maximize the system capacity. To minimize both intra-tier and inter-tier interferences, we introduced the concept of clusters into spectrum resource allocation, and correspondingly set a few principles for clustering. Unlike [9], an upper limit for the cluster size is set to avoid the formation of a too large cluster, which otherwise would consume a large number of physical resource blocks (PRBs) and thus affect the system capacity. Moreover, all PRBs are allowed to be used by all users in the system, both MUEs and SUEs. Simulation results show that the proposed CSRA algorithm out performs the CDRA algorithm in terms of the system capacity.

References

1. Zhang, X., Zhang, J., Wang, W., et al.: Macro-assisted data-only carrier for 5G green cellular system. Commun. Mag. IEEE **53**(5), 223–231 (2015)
2. Hwang, I., Song, B., Soliman, S.S.: A holistic view on hyper-dense heterogeneous and small cell network. Commun. Mag. IEEE **51**(6), 20–27 (2013)
3. Lopez-Perez, D., et al.: Enhanced inter-cell interference coordination challenges in heterogeneous networks. Wirel. Commun. IEEE **18**(3), 22–30 (2011)

4. Xiao, Z., Yu, J., Li, T., et al.: Resource allocation via hierarchical clustering in dense small cell networks: a correlated equilibrium approach. In: Proceedings of 2016 IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC 2016), Valencia, Spain, pp. 1–5, September 2009
5. Xu, L., Mao, Y., Leng, S., et al.: A clustering-based resource allocation strategy with energy harvesting in dense small cell networks. In: Proceedings of 2016 IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC 2016), Chengdu, China, pp. 303–310, October 2016
6. Zhao, Y., Xia, H., Zeng, Z., et al.: Joint clustering-based resource allocation and power control in dense small cell networks. In: Proceedings of 2015 IEEE International Conference on Communications in China (ICCC 2016), Brest, France, July 2016
7. Luo, Y., Hua, C.: Resource allocation and user-centric clustering in ultra-dense networks with wireless backhaul. In: Proceedings of IEEE 8th International Conference on Wireless Communications and Signal Processing (WCSP 2016), Yangzhou, China, October 2016
8. Hatoum, A., Aitsaadi, N., Langar, R., Boutaba, R., Pujolle, G.: FCRA: femtocell cluster-based resource allocation scheme for OFDMA networks. In: Proceedings of 2011 IEEE International Conference on Communications (ICC 2011), Kyoto, Japan, pp. 1–6, June 2011
9. Fan, S., Zheng, J., Xiao, J.: A clustering-based downlink resource allocation algorithm for small cell networks. In: Proceedings of IEEE 7th International Conference on Wireless Communications and Signal Processing (WCSP 2015), Nanjing, China, October 2015
10. David, T., Pramod, V.: Fundamentals of Wireless Communication. Cambridge University Press, Cambridge (2005)

Energy-Efficient Partitioning Clustering Algorithm for Wireless Sensor Network

Koffi V. C. Kevin de Souza[1], Catherine Almhana[1], Philippe Fournier-Viger[2], and Jalal Almhana[1(✉)]

[1] Université de Moncton, Moncton, NB, Canada
jalal.almhana@umoncton.ca
[2] Harbin Institute of Technology (Shenzhen), Shenzhen, GD, China
philfv8@yahoo.com

Abstract. Wireless Sensor Networks (WSNs) have recently achieved tremendous success at both research and industry levels. WSNs are currently implemented in many areas, such as the military, environmental monitoring, and medicine. WSN nodes are battery-operated, and energy saving is critical for their survival. Several research papers have been published on how to optimize power usage. In this paper, we focus on improving power consumption by optimizing data transfer. We propose an Energy-Efficient Partitioning Algorithm to reduce data transfer and consequently improve power consumption. Using data collected from a real WSN in the City of Moncton, we implemented and compared the performance of the proposed algorithm with another data reduction algorithm. Experimental results show that our algorithm outperforms a recent data reduction technique in terms of power saving.

Keywords: Energy saving · Clustering times series · Smart meters
Wireless Sensor Networks · Data transfer

1 Introduction

In recent years, WSNs have achieved tremendous success with several research projects have been carried out by the academic community and findings disseminated through various channels, namely conferences and journal [1, 2, 4]. Also, industry has been very active in making WSN reliable components available at a reasonable cost. Many applications are using WSNs as they are easy to deploy compared to wired systems and offer a reliable, flexible, and efficient means to gather information from variety of sensor nodes to monitor variables such as heat, light, and water levels. These sensing components are generating great interest and demand from the Internet of Things (IoT) industry, which can be viewed as an extension of the traditional WSN. Sensor nodes are generally low-power battery-operated with limited lifetime, and energy saving is critical for long-time autonomous WSN operation. Several research papers were published on energy savings. They cover a variety of WSN layers, including application, transport, network, data link, and physical layers [6]. In this paper, we are interested in power saving techniques at the application level which are more suitable for the system studied here, water meter data extraction. The main

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 14–23, 2018.
https://doi.org/10.1007/978-3-319-90802-1_2

purpose of this system is to acquire enough data, through frequent readings, in order to detect major water leaks or Abnormal Water Consumption (AWC) and avoid water waste. Frequent Water Meter Readings (WMRs) are essential for timely AWC detection as remedy action can be taken at a very early stage of possible water leaks. However, frequent WMRs imply frequent Radio Data Transmissions (RDTs), and consequently more power draining from the sensor batteries.

Experimental results [1] showed that RDT takes a significant amount of energy when it is compared to processing, insofar as the power needed to transmit one bit is equivalent to that needed to process one thousand bits. Trading RDTs for processing seems to be profitable in terms of power saving, and this aspect is of particular interest in our study. Designing an efficient system which at the same time allows AWC detection and optimizes sensor battery usage is crucial for a reliable WSN application implementation.

A variety of techniques can be used for reducing the number of radio transmissions [7]. The most relevant ones fall into two categories: data driven approaches and data acquisition techniques. Data driven approaches include reduction schemes, data compression, and data prediction. Reduction schemes minimize the number of data transmissions by eliminating redundant or unnecessary data. Compression techniques send data, at the source node, in condensed format, which can be decompressed at the sink node. Prediction supposes that the sensed process can be modeled using time series or stochastic and algorithmic solutions. Data acquisition [7] can be achieved by several approaches: time driven, event driven, query based, and hybrid. The effectiveness of these approaches depends on the type and requirements of the application.

In this paper, we propose a new approach that combines a time driven technique and a data partitioning clustering method to reduce RDTs. To the best of our knowledge, it is the first time that data partitioning clustering is used for data transmission reduction. We implemented our approach on data collected over several months from the City of Moncton's WSN water meters which contains more than 20,000 Water Meter Nodes (WMNs). Experimental results showed that our approach offers better power consumption economy when compared to the data reduction algorithm proposed in [7].

In Sect. 2 related works are presented, in Sect. 3 we describe the case study, followed by our approach in Sect. 4. Sections 5 and 6 present experimental results and concluding remarks respectively.

2 Related Work

As previously mentioned, various power management techniques can be used in WSNs. Research and development in this area is substantial and broad, it is therefore neither possible nor appropriate to review all available power management techniques. Several approaches were proposed to be implemented at different layers, including application, transport, network, data link, mac, and physical layers [2, 3]. Taking into account the WMR application, and the architecture of the network we are studying specifically here, we are interested in those techniques implementable at the application level. In our case, we do not have access to other layers. We are mainly interested in strategies that allow to minimize the number of RDTs and preserve the main purpose of

the application in terms of proper water consumption monitoring, which requires frequent WMRs. RDTs have an important impact on power saving; experimental results showed that they require much more power compared to instructions processing at the node's microcontroller. Therefore, trading RDT for data processing appears to be a very good strategy.

At the application layer, several techniques are described in the literature [9, 10]. We can classify them into three categories: data reduction, data compression, and data prediction. In data reduction [11, 12], redundant or unneeded data can be removed without any loss of information. In data compression [4], data is encoded using a variety of algorithms and transferred in condensed form and they are decompressed at the receiving node (sink node). Data prediction [7], is a more elaborate technique than the previous ones, and involves that a model is built based on the sensed data over a relatively long period of time. One copy of the model is stored at the sink node or on a server in certain cases, and another copy is stored at the sensor node. Data can be retrieved at the sink node from the model instead of from the measurement at the sensor node. In our previous work, we implemented both data reduction and prediction techniques on similar data we collected from the City of Moncton, and it proved to be effective.

Beyond the above techniques used to reduce power consumption, it is key to mention here the importance of data acquisition and how it is implemented in the whole network. The way data is extracted can define the amount of the data collected, and consequently impact the power consumption. Four procedures [6] are commonly used for data extraction: time-driven, event-driven, query-based, and hybrid.

In this paper, we will propose a new algorithm to reduce RDTs. It uses data partitioning and clustering and is a completely different approach from all of the above-mentioned techniques. To the extent of our knowledge, it is the first time that a clustering approach is used for data transmissions reduction. There are two methods for building clusters [13]; hierarchical and partitioning. The hierarchical method starts by grouping the most similar profiles at the lower level and the less similar ones at the higher level. Meanwhile, the partitioning method attempts to divide a large cluster into smaller ones. We will use the K-means algorithm [3] for data partitioning clustering.

K-means is a popular method for clusters analysis and data mining. A partition is made on a set of data (n observations) into K clusters. It assigns an observation to the cluster with the closest mean.

Given that WMRs can be seen as time series, we will use the Euclidean Distance to measure the similarity between two different WMRs. Let x and y be n-dimensional vectors [14, 15]. The Euclidean distance of similarity is given by the following formula: $dist(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$. As the number of possible clusters is unknown in our case, we need validity measures such as Sum of Squared Error (SSE) and Calinski-Harabasz (CH). All cluster validation measures are based on compactness and separation. In Euclidean spaces, compactness means the set of data is closed and bound. Separation determines how distinct or well separated clusters are. The SSE is computed as: $SSE = \sum_{i=1}^{n} x_i^2 - \frac{1}{n}\left(\sum_{i=1}^{n} x_i\right)^2$. SSE is the total sum of all sums of Euclidean distance between the center and every profile in every cluster. The optimal value is in an elbow,

(see following section). The Calinski-Harabasz index evaluates the cluster validity based on the average between and within-cluster sum of squares [8].

3 A Case Study: WMRs in the City of Moncton

In this section, we will provide information about the application we are studying here, WSN WMRs in the City of Moncton.

3.1 Network Architecture [7]

Figure (1) shows the architecture of the sensor network in the City of Moncton, which includes approximately 20,000 geographically distributed nodes. The sink nodes are located in four towers, each with one square mile coverage, and data with timestamps is collected from each cluster node with some nodes reachable by more than one tower. Each meter node is equipped with a powerful narrow band UHF frequency (450–470 MHz) transmitter (FCC Part 90) with approximately more than one mile range. The sink node sends its collected data to a central server repository where data is processed using a wireless telephone line. Data extraction is based on periodic queries: every six hours for certain old meter node models and every hour for newer meter node models. In our study, we will use the data collected from the newer meter node models with hourly queries.

3.2 Data Extraction and Cleaning [7]

In collaboration with the City of Moncton, we were able to collect one year of data for more than 20,000 clients, the majority of whom have 4 readings/day, and some 24 readings/day. The results presented here are for the 1129 m, with 24 readings/day, as they offer better sampling of the water consumption process. Before implementing our approach described in the previous section, it was necessary to do some verification and cleaning of the raw data to remove any reading errors and make sure all meters have

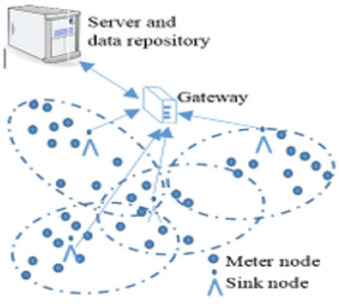


Fig. 1. The WSN architecture of the City of Moncton [7]

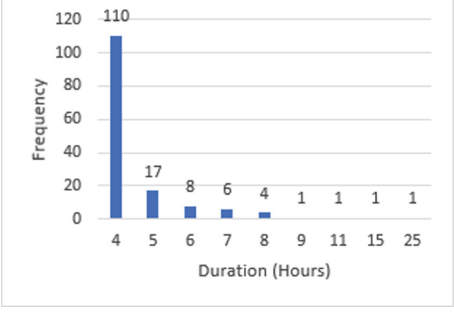


Fig. 2. Frequency of AWC readings vs. their durations for ε = 100%

exactly 24 readings/day, taken every hour. Some meters have more or less than 24 readings/day for certain days of the year. As shown in Fig. 1, certain nodes (meters) can reply to the queries coming from 2 sink nodes, as they are located within the communication range of both sink nodes, and the server will receive 2 readings for the same meter with a slight difference in time stamps. For example, we can have a reading at 4:00:00 PM and another at 4:00:10 PM, with a time difference of 10 s. In this case, we removed one of the readings. In other situations, where data is simply missing for unknown reasons, bad transmission for example, we were able to extrapolate the missing data as long as they are limited in number, i.e., less than 0.01%. Beyond this threshold, the meter data was removed from our study. It should be noted that the following results related to data transmission saving are compared to the current system used by the City of Moncton where no data transmission saving strategy is applied.

3.3 Abnormal Water Consumption

The main purpose of WMRs is to ensure proper water consumption monitoring and avoid waste of a natural resource fresh water. Consequently, it is important to detect any abnormal water consumption resulting from major leaks or from consumer abuse. There are a variety of reasons for water consumption increase/decrease, depending on the type of consumer, residential or industrial, as well as changes in users' habits. Not all sudden major water consumption increases are a result of water leaks, this why it is difficult to identify the source of increases. However, we can observe and quantify these increases through frequent WMRs. Major increases in water consumption will be described by the term 'Abnormal Water Consumption (AWC)'. An AWC event is observed when water consumption goes beyond a certain percentage ε of water consumption's moving average measured over n periods of time preceding this event. The AWC, or increase may last over extended periods during WMRs. Its importance depends on the value of ε and the duration of water consumption increase. An important AWC requires a careful monitoring, i.e. frequent WMRs.

4 Proposed Approach

Before describing our formal approach, we briefly explain the rationale behind it.

(a) As previously mentioned, the main purpose of WMR monitoring is to prevent major water waste and take the required action in the event of water leaks. Frequent WMRs, hourly in our case, should allow the detection of AWC. However, based on the data analysis, provided by the City of Moncton, the number of AWC increases is very limited and the events are of short duration. Figure 2 shows a histogram of AWC for 1129 water meters during the period from July 1st to December 31st (24 readings/day). An AWC event is detected when the water consumption exceeds a certain threshold we can define, (a formal definition will be provided later). It is obvious that the number of AWC events, 149, is very small relative to the total number of readings (4,877,280), i.e. less than 0.01%. Furthermore, the number of events where water consumption lasted

more than 8 h is in fact more limited, with only 4 events. We believe that frequent WMRs are not necessary for all water meters.

(b) Knowing the history of water consumption for each subscriber (private house, rental, industry, etc.) should give us some insight to build user profiles. An AWC is difficult to define. For example, a vacant rental property may see its water consumption suddenly increase when it is rented, yet this increase cannot be considered as an AWC event. Similar events may occur when home owners decide to fill up their swimming pools during the summer. This is why it is important to categorize subscribers based on their profile to avoid false AWC events [5].

(c) It is essential to isolate certain profiles (WMNs) that show AWC and put them into a specific group to be monitored frequently. This monitoring is done hourly in our study. The remaining profiles can be classified in groups or clusters, based on their water consumption variation. In our case, we chose the standard deviation as clustering criterion. Experimental results presented in Fig. 4 show that the best sampling or observation period is 36 h (36 readings), as it provides the best saving in terms of data transmissions.

(d) As the water consumption profile may change over time, it is important that we re-analyze the WMRs and adjust our partitioning clustering. In our application, we considered two time intervals; weekly and monthly.

Fig. 3. Elbow method; SSE vs number of clusters

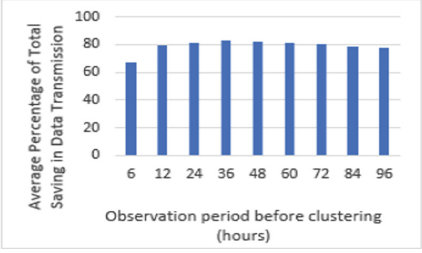


Fig. 4. Average percentage of total saving in data transmission vs observation (sampling) period

Below, we give a formal description of our approach. It includes the following steps:

Step 1. Isolate the set β of WMNs where AWC is detected. Let ε be the percentage of water consumption increase compared to the water consumption moving average $\gamma_{i,n}$ for a water meter i, computed over n previous periods of time. Let $a_i(t_j)$ be the water consumption for WMN i in the laps of time $t_j - t_{j-1}$.

i = 1, 2…. M, M is the number of water meters
j = 1, 2…. L, L is the number of readings,

$$\forall i \in \beta, \left(a_i\left(t_j\right)\right) > \left(\gamma_{i,n} + \varepsilon^* \gamma_{i,n}\right)$$

$\forall i \in \alpha, \left(a_i\left(t_j\right)\right) \leq \left(\gamma_{i,n} + \varepsilon^* \gamma_{i,n}\right)$, α represents the set of WMN where water consumption doesn't exceed the threshold $(\gamma_{i,n} + \varepsilon^* \gamma_{i,n})$.

Step 2. For each WMN $i \in \alpha$, compute the standard deviation θ_i from the set of data $\{a_i(t_j), j = 1\ldots L\}$, $i = 1\ldots m$. $\Theta = \{\theta_1, \theta_2, \ldots. \theta_m\}$, m is the number of elements in α.

Step 3. Partition Θ into g sub clusters $C_1, C_2, \ldots. C_k$, using the K-means method [3] as follows:

Let c_i be the center of sub-cluster C_i.

```
For k=2…m
       Procedure: Kmeans (k, Θ)
      Compute CHk and SSEk; validation parameters
End for

Procedure: Kmeans (k, Θ)

begin

      INPUT: Θ = {θ1, θ2, …. θm} (set of data)
                              k (number of clusters)
      OUTPUT: C = {c1, c2, …. ck} (set of cluster centers)
            Note that at the beginning k=m

         1  initialization:
            MAX=MaximumDistanceValue
            Assign ci a random value taken from Θ, ∀i, j,
            i≠j  ⇒ ci ≠ cj

         2  repeat
         3  for each θi ϵ Θ
         4      MinDistance = MAX
         5      ClusterGroup =  -1
         6      for each ci ϵ C
         7          dist = EuclideanDistance(θi,ci)
         8          if MinDistance > dist then
         9                MinDistance = dist
         10       Cluster Ci ← θ
         11         end if
         12     end for
         13 end for
         14 until no θi changes cluster
         15 return C = {c1, c2, …. ck}
end
```

Step 4. Validation: Knowing CH_k and SSE_k, see Table 1, determine the number of clusters g and validate this number using the elbow method for SSE, see Fig. 3 and the highest value given by the CH method [8].

Step 5. Compute the laps of time between two readings for each sub-cluster θ_i as follows: Upper Limit, UL = Max (c_i) Lower Limit, LL = Min (c_i)

– Assign the maximum sampling period to the sub-cluster with a center value c_i = LL and a minimum sampling period for the cluster with a center value c_i = UL. We can use a linear scale to assign a sampling period for each sub-cluster with LL < c_i < UL, a smaller sampling value for those near the UL and a bigger sampling value for those near LL. We believe that a sub cluster with small standard deviation should be monitored less frequently than the one with bigger value as they show little variation in their water consumption.

As water consumptions changes over time, it is important to retune the clustering. After a defined period T, we restart the procedure starting from step 1.

5 Experimental Results

Our experimental results are based on the data collected from 1,129 water meters from July 1st to December 31st, 24 readings/day. Figure 2 shows the frequency of AWC readings vs. their durations for ε = 100%. There are 149 AWC when we sample data hourly. When we implement our approach, which applies different data sampling periods, larger and cluster dependent, we were able to detect 122 AWC events, including all major event i.e. with more 4 h duration. This result is satisfactory in terms of the reliability of water meter monitoring. Figure 4 shows the Average Percentage of Total Saving in data transmission vs observation (sampling) period. From this figure, we can see that the best observation period is 36 h as it offers the maximum saving. Table 1. shows the values of SSE and CH as function of the number of clusters. The optimal number of cluster g is equal to 5. Figure 3 shows another representation for SSE where the elbow location indicates the optimal number of clusters.

In order to evaluate the performance of our approach we will compare our results to the data reduction techniques [7] where redundant readings are removed. Figure 5 and 6 show respectively the distribution (histogram) of data transmissions saving over 6 months when the data reduction technique and the data partitioning clustering approach are applied. From these figures, we observe that the most important saving occurs

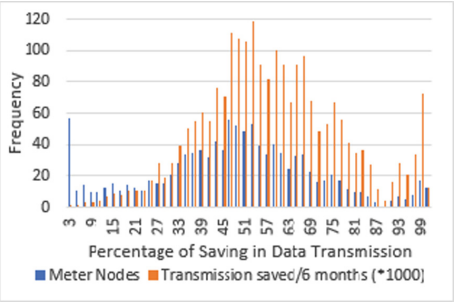


Fig. 5. Data transmission saving when data reduction technique is applied.

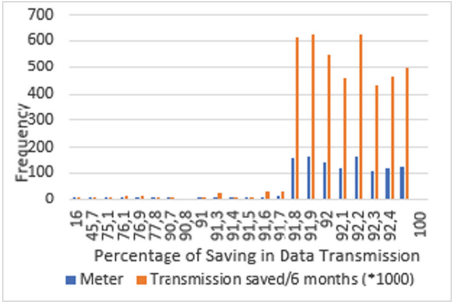


Fig. 6. Data transmission saving when the proposed partitioning clustering approach is used

between 45% and 75% for the data reduction technique and between 91% and 92% for the data partitioning clustering approach. Note that there is '0' saving for the WMNs in the set β as we monitor water consumption every hour.

Figure 7 shows the average percentage saving in data transmission for our approach as compared to the reduction technique. In our approach, the clustering is repeated weekly and monthly, and in both cases our solution offers better performance than the reduction technique. The improvement of saving is approximately 10% and 40% for weekly and monthly monitoring respectively.

Fig. 7. Comparison between cluster and redundancy approach

Table 1. SSE and CH values according the number of clusters

Number of clusters	SSE	CH
2	11,4915	0,01083
3	10,78	0,00735
4	10,0916	0,00637
5	**9,0819**	**0,01888**
6	9,0606	0,00570
7	9,0025	0,01047
8	8,7651	0,00380
9	8,6731	0,00843
10	8,456	0,00783
11	8,3308	0,00694

6 Conclusion

In this paper, we proposed a novel approach for RDT in WSNs that is based on partitioning clustering technique. To the best of our knowledge, it is the first time this approach is applied in this area. We compared the performance of our approach to another reduction technique based on redundant readings. Experimental results showed that our algorithm performs better in terms of transmission saving. In future work, we plan to compare our approach with modeling and prediction techniques.

Acknowledgement. This work is supported in part by an NSERC Discovery Grant awarded to Prof. Jalal Almhana and the Youth 1000 Funding of Prof. Philippe Fournier-Viger from the NSFC. We are grateful to the City of Moncton who provided us with the data.

References

1. Anastasi, G., Conti, M., Di Francesco, M., Passarella, A.: Energy conservation in wireless sensor networks using data reduction approaches: a survey. Int. J. Comput. Eng. Res. **7**(3), 537–568 (2013)
2. Karim, L., Anpalagan, A., Nasser, N., Almhana, J.: Sensor-based M2M agriculture monitoring systems for developing countries: state and challenges. Netw. Protoc. Algorithm J. **5**(3), 68–86 (2013)
3. MacQueen, J.B.: Some methods for classification and analysis of multivariate observations. In: 5th Berkeley Symposium on Mathematical Statistics and Probability, pp. 281–297. University of California Press (1967)
4. Tsai, K., Ye, M., Leu, F.: Secure power management scheme for WSN. In: 7th ACM CCS International Workshop on Managing Insider Security Threat, MIST 2015, pp. 63–66 (2015)
5. de Souza, K., Fournier-Vigier, P., Almhana, J.: Early detection of abnormal residential water consumption. Technical report (2017)
6. Said, J.E., Karim, L., Almhana, J., Anpalagan, A.: Heterogeneous mobility and connectivity-based clustering protocol for wireless sensor networks. In: ICC 2014, pp. 257–262 (2014)
7. Almhana, C., Choulakian, V., Almhana, J.: An efficient approach for data transmission in power-constrained wireless sensor network. In: ICC 2017, pp. 4058–4064 (2017)
8. Liu, Y., Li, Z., Xiong, H., Gao, X., Wu, J., Wu, S.: Understanding and enhancement of internal clustering validation measures. IEEE Trans. Cybern. **43**(3), 982–994 (2013)
9. Pantazis, N.A., Nikolidakis, S.A., Vergados, D.D.: Energy-efficient routing protocols in wireless sensor networks: a survey. Commun. Surv. Tutorials **15**(2), 551–591 (2013)
10. Ye, W., Heidemann, J.: An energy-efficient MAC protocol for wireless sensor networks. In: IEEE Computer and Communications Societies, pp. 1567–1576 (2002)
11. Younis, O., Fahmy, S.: HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Trans. Mob. Comput. **3**(4), 366–379 (2004)
12. Patil, S.A., Mishra, P.: Improved mobicast routing protocol to minimize energy consumption for underwater sensor networks. Int. J. Res. Sci. Eng. **3**(2), 197–204 (2017)
13. Liao, T.W.: Clustering of time series data – a survey. Pattern Recogn. **38**(11), 1857–1874 (2005)
14. Smith, B.A., Wong, A., Rajagopal, R.: A simple way to use interval data to segment residential customers for energy efficiency and demand response program targeting. In: ACEEE Summer Study on Energy Efficiency in Buildings (2012)
15. Lavin, A., Klabjan, D.: Clustering time-series energy data from smart meters. Energy Effi. **8**, 681–689 (2015)

Performance Evaluation of Multi-channel CSMA for Machine-to-Machine Communication

Changwei Zhang[1], Xinghua Sun[1], Jun Zhang[1,2(✉)], and Hongbo Zhu[1]

[1] Jiangsu Key Laboratory of Wireless Communications, Nanjing University of Posts and Telecommunications, Nanjing 210003, People's Republic of China
{1215012230,xinghua.sun,zhangjun,zhuhb}@njupt.edu.cn
[2] National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, People's Republic of China

Abstract. Machine-to-machine (M2M) communication aims to exchange information among a large number of devices without human interference. When more and more devices are connected, nevertheless, serious delay and energy efficiency problems may emerge due to massive access. In this paper, we apply a multi-channel Carrier Sense Multiple Access (CSMA) protocol for M2M communications where the frequency band is divided into several sub-bands. It is found that whether the band partitioning offers performance gains in terms of the delay and energy efficiency performance is critically determined by the traffic load. When the traffic load exceeds certain thresholds, a larger number of sub-channels is preferable. Moreover, it is found that the packet size and the signal-to-noise ratio (SNR) have a crucial effect on the thresholds. Based on this, the number of sub-channels can be optimally chosen accordingly to make sure that the system operates in the optimum working zone.

Keywords: M2M · Multi-channel CSMA · Delay · Energy efficiency

1 Introduction

Machine-to-machine (M2M) communication is a basic form of communications in the Internet of Things (IoT), mainly involving seamless exchange of information among a large number of devices without human interference [1]. M2M applications include all aspects of life, such as smart home, smart health, smart grid and industrial automation [2]. In these applications, the number of nodes is very large, for example, in the field of smart meters, the number of smart meters is expected to be 35,670/cell with a radius of 2 km in urban London [3]. In such an environment, it is crucial to ensure such a large number of nodes can successfully access the channel. In addition, the energy efficiency is also a key metric for devices powered by battery, e.g. in IoT. 3GPP organization has specified that the battery life should reach to more than 10 years in Massive IoT [4]. To achieve this goal, the access mechanism should have high energy efficiency.

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 24–33, 2018.
https://doi.org/10.1007/978-3-319-90802-1_3

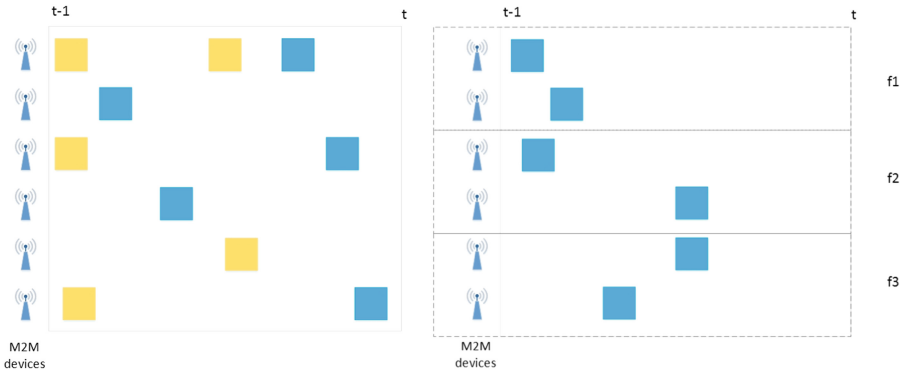
There have been many solutions aiming to alleviate channel contention for M2M communications. In [5], authors introduced a protocol that each node takes turns to access the channel. Although the wireless source can be allocated flexibly in a time division protocol, the strict time synchronization is difficult to implement. Authors in [6] divided the space into several parts, and used different timing alignment (TA) values for each location to distinguish between different nodes. Besides the time and space division, nodes can be grouped by using different frequency bands. In [7,8], authors proposed multi-channel Carrier Sense Multiple Access (CSMA) protocols. In particular, spectrum sensing was adopted in [7], with which, the coordinator will help each node to choose one less crowded channel to improve the spectral efficiency if the load in one channel is too heavy. [8] adopted an adaptive backoff algorithm, enabling each station to attempt data transmissions on the high signal-to-noise ratio (SNR) sub-channel. These schemes aimed to improve the throughput, yet did not characterize the delay and energy efficiency performance.

In this paper, we apply a multi-channel non-persistent CSMA protocol for M2M communications. By dividing the whole frequency band into n sub-bands, the number of competing nodes in each sub-band is reduced, leading to a lower collision probability. With a narrower bandwidth of each sub-band, nevertheless, the transmission time of each packet becomes longer. To see whether the band partitioning is beneficial, we characterize the delay and energy efficiency performance of multi-channel non-persistent CSMA. It is found that the delay and energy efficiency performance of multi-channel CSMA is critically determined by the traffic load. When the traffic load exceeds certain thresholds, a larger number of sub-channels is preferable. Moreover, the packet size and the SNR has a crucial effect on the thresholds. Based on this, the number of sub-channels can be optimally chosen accordingly to the traffic load to make sure that the system operates in the optimum working zone.

The rest of the paper is structured as follows: Sect. 2 describes the system model and multi-channel CSMA protocol. We then analyse the performance of multi-channel CSMA protocol in Sect. 3. In Sect. 4, we present the performance of multi-channel CSMA with different number of sub-channels. Finally, Sect. 5 concludes the paper.

2 System Model

Considering a cell with a large number of IoT nodes scattered in the cell. Each node adopts CSMA to access the channel, as this protocol does not require additional control overhead and can adapt well to changes in the number of nodes accessing the Base Station (BS) [9]. Generally, CSMA protocol has three mechanisms, namely 1-persistent CSMA, p-persistent CSMA and non-persistent CSMA. Among them, non-persistent CSMA does not continue to listen on the channel. If the channel is busy, it will wait for a while and listen again. If the channel is idle, the data will be sent immediately. Due to its simplicity, we focus on non-persistent CSMA in this paper.



(a) n=1 (b) n=3

Fig. 1. n-channel non-persistent CSMA.

When the traffic load is heavy, nevertheless, the CSMA protocol will lead to a serious conflict among nodes. To alleviate the channel contention, we consider a multi-channel CSMA protocol, where the entire frequency band is divided into several sub-bands, and nodes that use the same sub-band belongs to one group. As an example, it is shown in Fig. 1b that the entire frequency band is divided into three sub-bands and 6 nodes are divided into 3 groups. Nodes from different groups can transmit data at the same time without causing collisions. As each node only competes with other nodes in the same sub-channel, the channel contention can be alleviated.

3 Performance Analysis

To analyze the performance of the networks, we can focus on one of these n channels. Figure 2 demonstrates that the channel has two states, including the busy state and the idle state. The transition probability between the two states is 1, and the probability of being idle and being busy is same, so we have $\pi_{idle} = \pi_{busy} = 0.5$. Let g (packets per second) denote aggregated packets arrival rate from all nodes to BS, which consists the arrival rates of new packets and retransmitted packets, respectively. The mean channel idle period between two

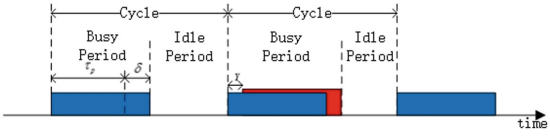


Fig. 2. Cycle structure of non-persistent CSMA.

consecutive packets is given by $T_i = \frac{1}{g}$. All packets' length are fixed to be D, and the transmission time is given by

$$\tau_p = \frac{n \cdot D}{W \log(1 + n\rho)}, \tag{1}$$

where W and ρ denote system bandwidth and received SNR respectively. δ and δ_d denote propagation delay and sensing delay respectively. It means that if a node sends a packet, it takes δ seconds before the BS receive the packet, and takes δ_d seconds before other nodes can sense the channel is busy. Therefore, in the first transmission cycle showed in Fig. 2, channel's busy state will last $\tau_p + \delta$ seconds. Otherwise, if a collision happens, which is showed in the second cycle in Fig. 2, the busy period should be $\tau_p + \delta + Y$, where Y denotes the time between the cycle beginning and the last interfering packet was scheduled [10]. As a result, the average busy period can be expressed as $T_b = \tau_p + \delta_d + \hat{Y}$, where the average value of Y is given by

$$\hat{Y} = \delta - \frac{1 - e^{-g\delta_d}}{g}. \tag{2}$$

In multi-channel CSMA, the entire frequency band is divided into n sub-bands. So the packets arrival rate in each sub-band is $g_n = \frac{g}{n}$. From analysis above, it can be seen the condition that the packet is successfully transmitted is that the channel is idle at the time of transmission and no other nodes send data after a certain period of time after transmission. The probability of successful packet transmission can be expressed as $p_{succ} = p_i \cdot p_s$, where p_i represents the probability of channel idle and p_s represents the probability that no other nodes send packets after the packet is sent for a period of time. It can be obtained that

$$\begin{aligned} p_i &= \frac{\pi_{idle} T_i}{\pi_{idle} T_i + \pi_{busy} T_b} \\ &= \frac{\frac{1}{g_n}}{\frac{1}{g_n} + \tau_p + \delta_d + \delta - \frac{1 - e^{-g_n \delta_d}}{g_n}} \\ &= \frac{1}{g_n T + e^{-g_n \delta_d}}, \end{aligned} \tag{3}$$

where $T = \tau_p + \delta_d + \delta$. From analysis in [10], we know that the probability that a node does not send a packet for a period of time x is e^{-gx}, then $p_s = e^{-g_n \delta_d}$. Accordingly, we have

$$\begin{aligned} p_{succ} &= p_i \cdot p_s \\ &= \frac{1}{g_n T e^{g_n \delta_d} + 1}. \end{aligned} \tag{4}$$

3.1 Delay Analysis

We define delay as the time from the generation of the packet to successful transmission of the packet [11]. The average packet delay is then given by

$$D(g_n) = \sum_{k=0}^{k_m} (1-p_{succ})^k p_{succ} \cdot [\tau_p + k(\frac{1-p_i}{1-p_{succ}}\theta_b + p_i\frac{1-p_s}{1-p_{succ}}(\theta_f+\tau_p))]$$
$$\approx \tau_p + (\frac{1}{p_{succ}} - 1)[\frac{1-p_i}{1-p_{succ}}\theta_b + p_i\frac{1-p_s}{1-p_{succ}}(\theta_f+\tau_p)], \quad (5)$$

where k_m indicates the maximum number of retransmission attempts for the node. θ_b and θ_f indicates the average backoff time due to a busy channel and packet conflict respectively, $\frac{1-p_i}{1-p_{succ}}$ and $\frac{1-p_s}{1-p_{succ}}$ are the corresponding probabilities.

By dividing one channel into n sub-channels, multi-channel CSMA protocol can alleviate contention in every sub-channel. But a narrower bandwidth may prolong the packet transmission time. When the traffic load is small, the collision probability in single channel CSMA is not high, so dividing the whole bandwidth into n sub-channels may increase delay and reduce the energy efficiency. To see whether n-channel offers any performance gain, we define $D(\frac{g}{n_1})$ and $D(\frac{g}{n_2})$ denote the delay performance of n_1-channel CSMA and n_2-channel CSMA, respectively. Here it is clear that n_1-channel CSMA is better than n_2-channel CSMA in terms of the delay performance if $D(\frac{g}{n_1}) < D(\frac{g}{n_2})$. The following lemma shows that whether $D(\frac{g}{n_1})$ is larger than $D(\frac{g}{n_2})$ depends on the traffic load g.

Lemma 1. *There exists a delay threshold $g^D_{n_1,n_2}$, such that if $g > g^D_{n_1,n_2}$, $D(\frac{g}{n_1}) > D(\frac{g}{n_2})$; otherwise, if $g < g^D_{n_1,n_2}$, $D(\frac{g}{n_1}) < D(\frac{g}{n_2})$.*

Proof. See Appendix.

From Lemma 1 we can see with the increment of the traffic load g, multi-channel CSMA outperforms than single-channel CSMA in terms of delay. When the traffic load g is heavy, having more sub-bands is preferable.

To find the optimal $n^{*.D}$, we have:

(1) If $g < g^D_{1,2}$, then $n^{*.D} = 1$;
(2) When $n \geq 2$, if $g^D_{n-1,n} \leq g < g^D_{n,n+1}$, then $n^{*.D} = n$.

3.2 Energy Efficiency Analysis

Energy efficiency can be calculated by dividing the average amount of data that can be transferred per packet successfully by the total energy required to send a packet, i.e., we have

$$E(g_n) = \frac{Dp_{succ}}{E_{packet}}$$
$$= \frac{D}{E_s + \frac{g_nTe^{2g_n\delta_d}}{1+g_nTe^{g_n\delta_d}}E_f + (1+(g_nT-1)e^{g_n\delta_d})E_b}, \quad (6)$$

where E_{packet} denotes the average energy required for each packet to be sent, E_b, E_f and E_s denote required energy when the channel is busy, the conflict occurred in the transmission and transmit data successfully. They can be calculated as follows:

$$E_b = P_l \theta_b, \tag{7}$$

$$E_f = E_s + P_l \theta_f, \tag{8}$$

$$E_s = (P_c + \xi P_t)\tau_p + P_l \tau_r, \tag{9}$$

where P_l, P_c and P_t denote the power consumption of channel detecting, power consumption of the circuit in the transmission packet mode and the transmission power of the transmission data. ξ is the reciprocal of the magnification of the power amplifier, before nodes receive acknowledgment packet information transmitted from BS, the node needs to keep listening to the channel, this takes τ_r seconds.

Similarly, we define $E(\frac{g}{n_1})$ and $E(\frac{g}{n_2})$ denote the energy efficiency performance of n_1-channel CSMA and n_2-channel CSMA, respectively. The following lemma shows that whether $E(\frac{g}{n_1})$ is larger than $E(\frac{g}{n_2})$ depends on the traffic load g.

Lemma 2. *There exist a energy efficiency threshold $g^E_{n_1,n_2}$, such that if $g > g^E_{n_1,n_2}$, $E(\frac{g}{n_1}) < E(\frac{g}{n_2})$; otherwise, if $g < g^E_{n_1,n_2}$, $E(\frac{g}{n_1}) > E(\frac{g}{n_2})$.*

Proof. See Appendix.

From Lemma 2 we can see with the increment of traffic load g, multi-channel CSMA outperforms than single-channel CSMA in terms of energy efficiency. When the traffic load g is heavy, having more sub-bands is preferable.

To find the optimal $n^{*.E}$, we have:

(1) If $g < g^E_{1,2}$, then $n^{*.E} = 1$;
(2) When $n \geq 2$, if $g^E_{n-1,n} \leq g < g^E_{n,n+1}$, then $n^{*.E} = n$.

4 Performance Comparison

In this section, we illustrate numerical results of delay and energy efficiency performance of multi-channel CSMA. To see whether grouping nodes by frequency is beneficial or not, we use the basic single channel CSMA as a benchmark. In addition, we will explore how the packet size D and the SNR ρ influence the delay threshold and the energy efficiency threshold. Table 1 lists the parameters used in the numerical analysis.

Table 1. Numerical analysis parameters

Parameters	Value
P_c, P_t	20 mW, 50 mW
θ_b, θ_f	40 ms
δ_d, δ	1 ms
E_s, E_f, E_b	$0.002 \times \tau_p + 0.001, E_s + 0.001, 0.002$
T	$0.002 + \tau_p$
W	900 kHz

4.1 Numerical Results of Delay and Energy Efficiency

It can be seen from Fig. 3 that when the traffic load g is small, single channel CSMA protocol has the shortest delay, but in the high load region, its delay performance deteriorates. This is because the collision probability increases dramatically, leading to a huge waste of time. When the traffic load g exceeds certain thresholds, a larger number of sub-channels is preferable. It is because in the high load region, the collision probability is reduced with multi-channel CSMA due to the load in each sub-channel is lower, thereby the delay is reduced.

Figure 4 shows the $n^{*,D}$ based on the delay performance. We can find that with the increment of traffic load g, the $n^{*,D}$ increases. This is because when the traffic load g becomes heavy, the number of nodes in every sub-channels increase, which will cause serious collision problem again, so it is better to use more sub-channels.

Figure 5 shows how the energy efficiency varies with traffic load g. It can be seen that when the traffic load is small, single channel CSMA has the highest energy efficiency. When traffic load g exceeds certain thresholds, the energy efficiency of the multi-channel CSMA protocol is higher than that of single channel CSMA. It is because with multi-channel CSMA, the load in each sub-channel is lower, so the retransmission caused by collision can be reduced, thereby can reduce energy waste.

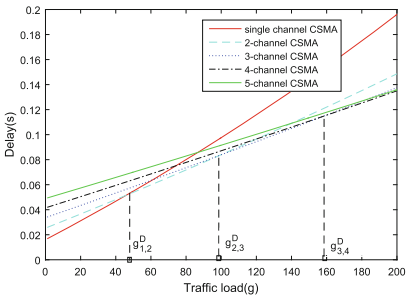


Fig. 3. Delay performance of n-channel CSMA. D = 50 Kbits, $\rho = 10$.

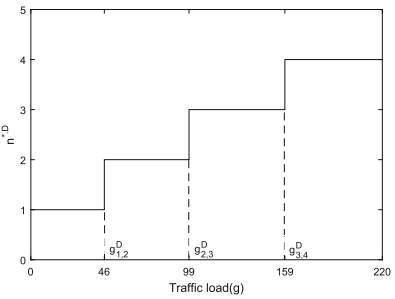


Fig. 4. $n^{*,D}$ versus traffic load g. D = 50 Kbits, $\rho = 10$.

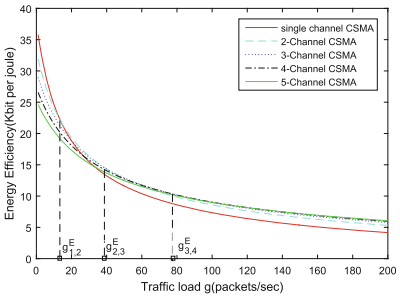


Fig. 5. Energy efficiency of n-channel CSMA. D = 50 Kbits, $\rho = 10$.

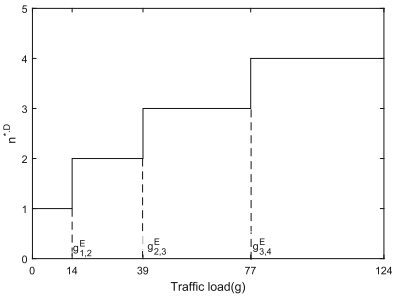


Fig. 6. $n^{*,E}$ versus traffic load g. D = 50 Kbits, $\rho = 10$.

Figure 6 shows the $n^{*,E}$ based on the energy efficiency performance. It can be seen that the $n^{*,E}$ also increases with the traffic load g. With the increment of the traffic load g, the deterioration of the energy efficiency is faster than delay, so the $n^{*,E}$ based on the energy efficiency increases faster than $n^{*,D}$. From Figs. 4 and 6, we can conclude that the n^* increases with the increment of traffic load.

4.2 Delay and Energy Efficiency Threshold

Next, we will demonstrate the delay and the energy efficiency thresholds with $n_1 = 1$ and $n_2 = 2$. Figure 7 illustrates that delay threshold increases as the SNR and the packet size increase. It is because when SNR and packet size increase, the gap of packet transmission time between the 2-channel CSMA and the single-channel CSMA becomes larger. In order to compensate for this gap, only when the probability of collision is high in the single-channel CSMA protocol, the delay of 2-channel CSMA can be better than that of single-channel CSMA, so the thresholds increases as packet size and SNR increase.

Figure 8 illustrates that energy efficiency threshold increases as the packet size D and SNR ρ increase, which is similar to the result obtained in the delay

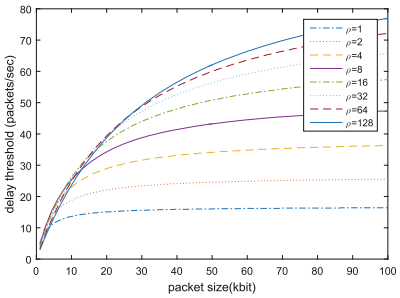


Fig. 7. Effect of packet size and SNR on the delay threshold.

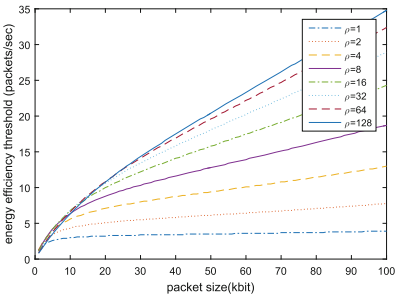


Fig. 8. Effect of packet size and SNR on the energy efficiency threshold.

thresholds. The reason is that to improve energy efficiency, it is necessary to reduce the waste of energy by having a shorter packet delay. Therefore the delay and energy efficiency thresholds in these two figures are similar.

5 Conclusion

In this paper, the performance of multi-channel CSMA protocol is analyzed. It is found that the number of channels n should be adaptively tuned according to traffic load g. When g exceeds certain thresholds, a larger number of sub-channels is preferable. Moreover the influence of the packet size and SNR on the thresholds is explored, which provides guidance for the optimal tuning of the number of channels towards better delay and energy efficiency performance.

Acknowledgements. This work was supported by the National Natural Science Foundation of China (NSFC) under Grants 61427801, 61401224, and 61671251, the Natural Science Foundation Program through Jiangsu Province of China under Grant BK20140882 and BK20150852, and the open research fund of National Mobile Communications Research Laboratory, Southeast University under Grant 2017D05.

Appendix: Proof of Lemmas 1 and 2

Let $f^D_{n_1,n_2}(g) = D(\frac{g}{n_1}) - D(\frac{g}{n_2}), n_1 < n_2$, we have

$$f^D_{n_1,n_2}(g) = [\frac{g}{n_1}(\frac{Dn_1}{W\log(1+n_1\rho)} + \delta + \delta_d)e^{\frac{g}{n_1}\delta_d} - \frac{g}{n_2}(\frac{Dn_2}{W\log(1+n_2\rho)} + \delta + \delta_d)e^{\frac{g}{n_2}\delta_d}]\theta_b + (e^{\frac{g}{n_1}\delta_d}\frac{Dn_1}{W\log(1+n_1\rho)} - e^{\frac{g}{n_2}\delta_d}\frac{Dn_2}{W\log(1+n_2\rho)}). \quad (10)$$

It can be seen when $g = 0$, $f^D_{n_1,n_2}(g) < 0$, and when g goes to infinite, $f^D_{n_1,n_2}(g) > 0$, so there exist at least a value of g makes $f^D_{n_1,n_2}(g) = 0$. Moreover, we have

$$\frac{d}{dg}f^D_{n_1,n_2}(g) = T_{n_1}\theta_b\frac{1}{n_1}e^{\frac{g}{n_1}\delta_d}(1+\frac{g}{n_1}\delta_d) - T_{n_2}\theta_b\frac{1}{n_2}e^{\frac{g}{n_2}\delta_d}(1+\frac{g}{n_2}\delta_d) + e^{\frac{g}{n_1}\delta_d}\frac{D\delta_d}{W\log(1+n_1\rho)} - e^{\frac{g}{n_2}\delta_d}\frac{D\delta_d}{W\log(1+n_2\rho)}, \quad (11)$$

where $T_{n_1} = \frac{Dn_1}{W\log(1+n_1\rho)} + \delta + \delta_d$ and $T_{n_2} = \frac{Dn_2}{W\log(1+n_2\rho)} + \delta + \delta_d$, which can be treated as two constants in this expression. When δ_d and δ in T_{n_1} and T_{n_2} is negligible, this equation can be rewritten as

$$\frac{d}{dg}f^D_{n_1,n_2}(g) \approx \frac{D\theta_b}{W\log(1+n_1\rho)} - \frac{D\theta_b}{W\log(1+n_2\rho)}. \quad (12)$$

When $g > 0$ and $n_1 < n_2$, we have $\frac{d}{dg}f^D_{n_1,n_2}(g) > 0$, so $f^D_{n_1,n_2}(g)$ monotonically increases with g. Therefore, there exists a threshold of $g^D_{n_1,n_2}$, such that

if $g > g^D_{n_1,n_2}$, $f^D_{n_1,n_2}(g) > 0$, i.e., $D(\frac{g}{n_1}) > D(\frac{g}{n_2})$, otherwise, $f^D_{n_1,n_2}(g) < 0$, i.e., $D(\frac{g}{n_1}) < D(\frac{g}{n_2})$.

Similarly, we can obtain $f^E_{n_1,n_2}(g)$ as

$$f^E_{n_1,n_2}(g) = E(\frac{g}{n_1}) - E(\frac{g}{n_2}) = \frac{D}{E_s + \frac{gT_{n_1}e^{2\frac{g}{n_1}\delta_d}}{n_1+gT_{n_1}e^{\frac{g}{n_1}\delta_d}}E_f + (1+(\frac{g}{n_1}T_{n_1}-1)e^{\frac{g}{n_1}\delta_d})E_b} - \frac{D}{E_s + \frac{gT_{n_2}e^{2\frac{g}{n_2}\delta_d}}{n_2+gT_{n_2}e^{\frac{g}{n_2}\delta_d}}E_f + (1+(\frac{g}{n_2}T_{n_2}-1)e^{\frac{g}{n_2}\delta_d})E_b}. \quad (13)$$

When $g = 0$, $f^E_{n_1,n_2}(g) > 0$, and when g goes to infinite, $f^E_{n_1,n_2}(g) < 0$. Moreover, it can be proved that when $g > 0$ and $n_1 < n_2$, $\frac{d}{dg}f^E_{n_1,n_2}(g) < 0$, so $f^E_{n_1,n_2}(g)$ monotonically decreases with g. Therefore, there exist a threshold $g^E_{n_1,n_2}$, such that if $g > g^E_{n_1,n_2}$, $f^E_{n_1,n_2}(g) < 0$, i.e., $E(\frac{g}{n_1}) < E(\frac{g}{n_2})$, otherwise, $f^E_{n_1,n_2}(g) > 0$, i.e., $E(\frac{g}{n_1}) > E(\frac{g}{n_2})$.

References

1. Rajandekar, A., Sikdar, B.: A survey of MAC layer issues and protocols for machine-to-machine communications. IEEE Internet Things J. **2**, 175–186 (2015)
2. Park, I.S., Shitiri, E., Cho, H.S.: An orthogonal coded hybrid MAC protocol with received power based prioritization for M2M networks. In: IEEE International Conference on Ubiquitous Future Network, pp. 733–735. IEEE Press (2016)
3. Jang, H.S., Kim, S.M., Ko, K.S., Cha, J., Sung, D.K.: Spatial group based random access for M2M communications. IEEE Commun. Lett. **18**, 961–964 (2014)
4. Ericsson: Cellular networks for massive IoT, Janurary 2016. https://www.ericsson.com
5. Ergen, S.C., Varaiya, P.: TDMA scheduling algorithms for wireless sensor networks. Wirel. Netw. **16**, 985–997 (2010)
6. Ko, K.S., Min, J.K., Bae, K.Y., Dan, K.S.: A novel random access for fixed-location machine-to-machine communications in OFDMA based systems. IEEE Commun. Lett. **16**, 1428–1431 (2012)
7. Karaoglu, B., Heinzelman, W.: Cooperative load balancing and dynamic channel allocation for cluster-based mobile ad hoc networks. IEEE Trans. Mobile Comput. **14**, 951–963 (2015)
8. Kwon, H., Seo, H., Kim, S., Lee, B.G.: Generalized CSMA/CA for OFDMA systems: protocol design, throughput analysis, and implementation issues. IEEE Trans. Wirel. Commun. **8**, 4176–4187 (2009)
9. Wang, G., Zhong, X.F., Mei, S.L., Wang, J.: An adaptive medium access control mechanism for cellular based machine to machine (M2M) communication. In: 2010 IEEE International Conference on Wireless Information Technology and Systems, pp. 1–4. IEEE Press (2010)
10. Rom, R., Sidi, M.: Multiple Access Protocols: Performance and Analysis. Springer Science & Business Media, Heidelberg (2012). https://doi.org/10.1007/978-1-4612-3402-9
11. Miao, G.W., Azari, A., Hwang, T.: E^2-MAC: energy efficient medium access for massive M2M communications. IEEE Trans. Commun. **64**, 4720–4735 (2016)

Optimal Smart Prepayment for Mobile Access Service via Stackelberg Game

Yuan Wu(✉), Haowei Mao, Xiaowei Yang, Liping Qian, Weidang Lu, and Liang Huang

College of Information Engineering, Zhejiang University of Technology, Hangzhou, China
{iewuy,lpqian,luweid,lianghuang}@zjut.edu.cn,
hwmao_zjut@163.com, xwyang_zjut@163.com

Abstract. In this paper we propose a smart prepayment for mobile access network Service Provider (SP) to charge End-Users (EUs). Prepayment is a desirable charging approach, since it helps the SP to reduce its loss in bad-debt and capital devaluation. Meanwhile, Quality of Service (QoS) is a major concern from the EUs' perspective, especially when they have heavy traffic demands and suffer from network congestion due to limited access bandwidths. Our proposed prepayment thus aims at improving both the SP's economic reward and the EUs' QoS. To analyze the benefit from the proposed prepayment scheme, we model the interaction between the SP and the EUs as a Stackelberg game, which is based on the rationale that improved QoS will be an incentive for the EUs to prepay. In this game model, the SP plays as a leader and determines its prepayment policy to optimize its reward, and the EU plays as a game follower and determines its prepaid amount as a response to the SP's policy. The equilibrium of this game model strongly depends on the EUs' traffic load level, which we quantify and analyze in depth. Our results show that both of the SP and the EUs can benefit from the equilibrium of the game model, implying that the proposed prepayment scheme will yield a desirable win-win outcome.

Keywords: Smart pricing · Mobile network service · Optimization Stackelberg game

1 Introduction

Facing a rapid growth in wired/wireless access networks, many mobile access Service Providers (SPs) are expected to provide access to a large number of End-Users (EUs) with heterogeneous traffic demands. The SPs, however, usually have limited bandwidths in access links (e.g., cellular networks), which results in a dilemma between obtaining higher profits through providing services to more EUs and suffering from the consequent network congestions due to excessive EUs' traffic demands. One of the most effective approaches to tackle this dilemma is

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 34–50, 2018.
https://doi.org/10.1007/978-3-319-90802-1_4

to increase the bandwidths of access links, e.g., through updating their network infrastructures. However, the SPs usually hesitate to do so because of huge capital investments and more importantly, their uncertainties in cost-recovery, e.g., due to failure to collect the entire service fees from EUs (i.e., the so-called "bad-debts"). A mechanism to motivate the SPs to increase the access bandwidths is prepayment, i.e., the SPs are allowed to collect (or partially collect) the service fee at the beginning of a service cycle. Then the SPs can increase the EUs' access bandwidths based on the received prepayment. For example, this can be logically implemented through the SPs' traffic-shaping, i.e., the SPs increase the bandwidth-limit on the EU's traffic according to the EU's prepaid amount. Hence, the EU is motivated to choose the option of prepayment for a better QoS-performance. Prepayment will generally benefit the SPs economically from the following two aspects: (i) the prepayment can save the SPs' loss due to capital devaluation. Specifically, the capital usually devalues over time (for example, a current value v is only worth of $v\alpha$ at the end of a service cycle, where α denotes the discount factor), and hence obtaining the service fee at the beginning of a service cycle means a greater profit compared to obtaining it at the end of the cycle; (ii) the prepaying can reduce the SPs' loss due to the bad-debt, i.e. the SP fails to collect the entire service fee from the EU at the end of the service cycle. Therefore, prepayments have been widely accepted and used by SPs [8–10]. Different from the SP's interest, Quality of Service (QoS) is a key concern of EUs, especially when they have heavy traffic loads and hence suffer from network congestions due to limited access bandwidths. For instance, most of the popular applications on mobile terminals, such as multimedia streaming, online gaming and group communications are usually QoS-sensitive and suffer from insufficient access bandwidths (in particular, as reported in [11], prepayment will be well suitable to charge realtime applications like multimedia streaming, online gaming and etc). As described earlier, choosing the option of prepayment can motivate the SPs to increase its access bandwidth, and thus can effectively alleviate the network congestions and improve the EUs' QoS-experience.

Considering different interests of SP and EUs, a smart prepayment scheme can be envisioned to encourage the collaborations between the SP and the EUs. Put it simply, the SP commits to using a portion of the EUs' prepayment to increase its access bandwidth (or equivalently to increase the EUs' bandwidth-limit in traffic shaping), and as a response the EUs are encouraged to choose the option of prepayment for better QoS. However, the questions about this prepayment scheme are (i) how much of the EUs' prepayment the SP will spend in upgrading its access bandwidth, (ii) as a response, how much the EUs will choose to prepay. More importantly, (iii) how much will the SP and EUs benefit from this scheme, and do they have a joint incentive to adopt this scheme? These questions motivate our work. To analyze the prepayment scheme and answer the above questions, we model the strategic interaction between the SP and the EUs as a noncooperative game. Intuitively, the interests of the SP and the EUs are conflicting with each other, i.e., the SP expects to obtain a greater prepayment from the EU but spending less in increasing its bandwidth. In comparison, the EU expects to receive a better QoS but spending less prepayment. Hence, the game naturally fits our need for

modeling. In particular, based on the rationale that *the improved QoS from this prepayment scheme will be an incentive for EUs to prepay*, we adopt the Stackelberg game, a leader-follower dynamic game, to model the specific SP-EUs interaction [19] (another reason for us to choose the Stackelberg game is that the access service providers usually possess dominant positions in practical markets compared to individual EU). The equilibrium of this Stackelberg game, i.e., the ultimate state that either SP or EUs will not change their decision unilaterally, represents the optimal prepayment scheme and hence facilitates our quantitative analysis on the benefits from this scheme. We analyze the equilibrium of the proposed Stackelberg game via backward induction. We find that the equilibrium strongly depends on the EUs' traffic load, and hence we differentiate three traffic load regions to quantify the equilibrium (we also show the uniqueness of the equilibrium for each region). Based on the obtained equilibrium, we quantify the SP and EUs' rewards from the prepayment scheme. Our results show that both the SP and the EUs will benefit significantly from the game equilibrium, which implies a win-win outcome from the prepayment. The proposed prepayment scheme can effectively motivate the cooperation among different users and operators in different paradigms in future 5G cellular networks [14–16].

Related Work: Models of charging have been longstanding concerns for network operators and service providers [1]. Related work can be roughly categorized according to the subjects investigated, which include *whom to charge* [2,3], *what to charge* [4,5], and *how to charge* [6,7]. However, an issue less explored before is *when to charge*. Regarding this issue, prepaying and post-paying are two important candidates in practice. Compared to the prepayment, the post-payment means that the SP is only allowed to collect the service fee at the end of the service cycle. While the post-paying has been widely adopted at present, the prepaying has its own advantages and hence attracts lots of interests (please refer to [8] for a survey of different models of prepaid mobile services and [9] for general customers and markets). In fact, with a rapid growth in 3G commercial communication networks, the prepaid access service has been widely adopted by many access SPs [10] and has been considered to be well suitable for realtime multimedia applications like video streaming, online-gaming and etc. From customers' point of view, it is reported that the prepayment is especially preferred by customers with tight budgets and eager to control their expenses closely, e.g., the reported demand for prepaid billing is 90–95% at initial sign-up in fast growing regions such as South America, Asia and Africa [11]. While, in developed regions, prepayment is also attractive to customers without good credit history, teenagers, and early-adopters of new services. Recent work [12,13] investigated the implementation issue of the prepayment for mobile network operators. Specifically, [12] focused on the prepaid voice-service and analyzed the optimal frequency for credit checking and updating with the objective to achieve a good balance between minimizing the checking cost and the bad-debt. [13] investigated how each user allocated its prepaid credit to executed sessions.

2 Design of Smart Prepayment Scheme

2.1 Proposed Prepayment Scheme and Its Game Model

We specify the proposed prepayment scheme as follows. Suppose that the SP adopts traffic-shaping mechanism to manage the EUs' traffic in access network. The SP is allowed to collect the service fee (in partial) from EUs at the beginning of the service cycle. The SP designs its prepayment policy to encourage the EUs' prepayment. Specifically, the SP's policy is characterized by a parameter β, which specifies the portion of the EU's prepaid amount used to increase the EU's bandwidth-limit in traffic-shaping. Given the SP's policy β, the EU determines how much to prepay, i.e., its prepaid amount p out of the original service-fee T. With the prepayment scheme, the SP controls β to trade off between its benefit from obtaining the EUs' prepayment and its expense on increasing the bandwidth of access link, and the EUs controls p to trade off between its improved QoS-performance from increased link bandwidth and its economic loss due to prepaying.

The objectives of the SP and EUs are conflicting with each other, i.e., the SP expects to obtain a greater prepayment from the EU but spending less in increasing its bandwidth-limit. In comparison, the EU expects to receive a better QoS but prepay less. Hence, it is important to investigate what will be the equilibrium for the prepayment scheme where both the SP will not change its policy β and the EU will not change its prepaid amount p unilaterally. To investigate this equilibrium, we consider a simple yet illustrative model as follows. The strategic interaction between the SP and EUs is modeled as a Stackelberg game, where the SP plays as the game leader and determines its policy β in advance. The EUs play as the game followers and determine their prepaid amount p as a response to the SP's prepayment policy β. The Stackelberg game captures the practical market where the SP usually possesses a dominant position in comparison with individual EU. Notice that as an initial step to analyze the prepayment scheme in this work, we first choose to model a representative EU, which represents a class of EUs with homogeneous traffic characteristic (thus, it suffices for all EU to use the same prepayment p and for the SP to use the same policy β). This choice helps us focus on analyzing the strategic interaction between the SP and the EU and quantifying their benefits from the prepayment scheme. Nevertheless, in practice multiple classes of EUs with heterogeneous characteristic (e.g., traffic demands) need to be investigated, which is an important extension for our future work. We illustrate the decision-making of the SP and the EUs in the next two subsections.

2.2 Modeling of the Decision-Making of the SP

The SP controls its prepayment policy β to optimize its own reward by solving the following problem

$$\texttt{(SP-P)}: \max_{0\le\beta\le 1} V(\beta, p) = p(1-\beta)(1-\alpha) + \theta p\alpha, \tag{1}$$

where the discount factor α (ranging from 0 to 1) measures the rate at which the capital devalues over time. $\alpha = 1$ means no devaluation, and $\alpha = 0$ means a complete devaluation. The risk factor θ measures the probability that the SP fails to get the service fee from the EU, which results in a bad-debt. The EUs' prepaid amount is denoted by p. We explain the two parts of the SP's reward function $V(\beta, p)$ in details as follows.

Part (i): the first part $p(1-\beta)(1-\alpha)$ in (1) denotes the *additional* reward the SP can obtain compared to the post-payment. It can be explained as follows. Recall that T denotes the original service fee the EU has to pay. With the prepayment, the SP obtains $p(1-\beta) + (T-p)\alpha$, which includes $p(1-\beta)$ at the beginning of the service and $(T-p)\alpha$ at the end. Notice that the SP spends $p\beta$ in increasing the EU's bandwidth limit according to its prepayment policy, hence $p\beta$ is deduced from the SP's reward. By contrast, with the post-payment, at the end of the service cycle, the SP can obtain $p(1-\beta)\alpha + (T-p)\alpha = (T-p\beta)\alpha$. Notice that, to make a fair comparison, we also assume that the SP spends $p\beta\alpha$ in increasing its bandwidth with the post-payment, which however happens at the end of the service cycle. Table 1 lists the difference between the post-payment and the prepayment. The difference between the sum of the first row for post-payment and the sum of the second row for prepayment gives the first part in (1), i.e., $p(1-\beta)(1-\alpha)$.

Part (ii): the second part $\theta p\alpha$ in (1) denotes the SP's gain from reducing the loss due to bad-debt. Specifically, with prepayment, the SP has a risk of losing $\theta(T-p)\alpha$ due to the bad-debt at the end of the service cycle. In comparison, with postpayment, the SP faces a risk of losing $\theta T\alpha$ at the end. The difference between them yields $\theta p\alpha$.

Table 1. Difference between the post-payment and prepayment

	Beginning of the service cycle	End of the service cycle
Post-payment	0	$(T-p\beta)\alpha$
Prepayment	$p(1-\beta)$	$(T-p)\alpha$

In summary, the SP's reward function (1) trades off between the economic gain the SP obtains from prepayment and its additional cost in increasing the bandwidth-limit for EUs. The SP's reward function (1) measures the *additional* gain from the prepayment compared to that from the conventional postpayment, i.e., a positive reward means that the SP gains more from the prepayment and will choose the option of prepaying self-incentively. This corresponds to a key motivation for our work, i.e., investigating whether both the SP and EU can benefit from the proposed prepayment (compared to the postpayment).

2.3 Modeling of Decision-Making of the Presentative EU

The presentative EU plays as a follower and determines its prepaid amount p (as a response to the SP's policy β) by solving the following problem.

$$\texttt{(EU-P)}: \max_{0\le p\le T} U(\beta,p)=\omega\frac{p\beta}{\mu}\frac{1}{(C-x)(\frac{p\beta}{\mu}+C-x)}-p(1-\alpha), \tag{2}$$

where C denotes the bandwidth-limit without prepaying, and x denotes the EU's traffic load. μ denotes the marginal cost for the SP to increase bandwidth-limit.

As shown in the EU's reward function $U(\beta,p)$, we measure the EU's reward as the difference between its improved delay performance and its economic loss. Specifically, with prepayment, the EU's bandwidth-limit is increased and hence its average traffic delay is improved by $\frac{p\beta}{\mu}\frac{1}{(C-x)(\frac{p\beta}{\mu}+C-x)}$. For simplicity, we use the M/M/1 queue model to quantify the EU's average delay under a given traffic load. Similar models quantifying user's dissatisfaction due to average traffic delay also appeared in [17,18] regarding to the optimization of network operators. Here, ω denotes the weighting factor that maps the EU's improved delay-performance into its perceptive reward (which is comparable with its economic loss). Without loss of generality, we set $\omega=1$ in the rest of this paper. Meanwhile, $p(1-\alpha)$ denotes the EU's economic loss due to prepaying, which is the difference between the EU's payment $T\alpha$ with post-payment and its payment $p+(T-p)\alpha$ with prepayment. In summary, $U(\beta,p)$ represents that the EU aims to achieve a good balance between receiving an improved QoS-performance and reducing its economic loss.

Functions (1) and (2) show the conflicting objectives of SP and EUs. The equilibrium of the above interaction between the SP and EU represents the stable state the SP and EUs will reach, and no one will deviate from this equilibrium unilaterally. We derive this equilibrium in the next section.

3 Analysis of Equilibrium

3.1 Backward Induction and Equivalent Formulation

In the above formulated Stackelberg game, the SP possesses the dominant position and hence has the so-called first-move advantage [19], i.e., the SP can optimize its policy β by expecting the EU's response (i.e., the prepaid amount p). Thus, we adopt the backward induction to derive this equilibrium.

We first derive the EU's best choice of prepaid amount given the SP's prepayment policy β. Since in problem (EU-P), the EU's reward function is strictly concave with respect to p, the first order condition for optimality is applicable. By setting $\frac{\partial U(\beta,p)}{\partial p}=0$, we obtain the EU's optimal prepaid amount p as a response to the SP's policy β as follows

$$p(\beta)=\min\Big\{\sqrt{\frac{\mu}{\beta}}\sqrt{\frac{1}{1-\alpha}}-\frac{\mu}{\beta}(C-x),T\Big\}. \tag{3}$$

The above result shows that to guarantee $p(\beta) \geq 0$, it is required that $0 \leq \sqrt{\frac{\mu}{\beta}} \leq \sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$. It means that to encourage a positive prepayment from the EU, the SP has to commit a minimum investment, i.e., β should be above a certain threshold which depends on the EU's traffic load. By substituting (3) into the EU's objective function, we obtain the EU's reward as a function of the SP's policy β as follows

$$U^*(\beta) = U(\beta, p(\beta)) = \max\Big\{\frac{1}{C-x}\big(1 - \sqrt{\frac{\mu}{\beta}}\sqrt{1-\alpha}(C-x)\big)^2, U(\beta, T)\Big\}. \quad (4)$$

Remark 1: Equation (4) shows that, with a favorable SP's prepayment policy (i.e., condition $\sqrt{\frac{\mu}{\beta}}\sqrt{1-\alpha}(C-x) \leq 1$ is met to prevent a negative EU's prepaid amount), the EU always receives a nonnegative reward by choosing its prepaid amount according to (3), and hence the EU is encouraged to choose the option of prepaying.

Next, knowing the EU's best response, we analyze the SP's best prepayment policy. Suppose that the EU's original service fee T is relatively large. Then, using (3), the SP's optimization problem `(SP-P)` becomes

$$\max_{0\leq\beta\leq 1} \Big(\sqrt{\frac{\mu}{\beta}}\sqrt{\frac{1}{1-\alpha}} - \frac{\mu}{\beta}(C-x)\Big)\big((1-\beta)(1-\alpha) + \theta\alpha\big). \quad (5)$$

Let β^* denote the SP's optimal prepayment policy for the above problem. Then, the EU's optimal prepaid amount can be given by $p^* = p(\beta^*)$ according to (3). Hence, the profile (β^*, p^*) serves as the equilibrium for our formulated Stackelberg game. However, despite its simple form, the above problem (5) is nonconvex in general with respect to β. To tackle this difficulty and explore the hidden structural property, we first make a change of variables as follows: $z = \sqrt{\frac{\mu}{\beta}}$, or equivalently $\beta = \frac{\mu}{z^2}$. Notice that $z \geq \sqrt{\mu}$ since $0 \leq \beta \leq 1$.

Based on this change of variables, the EU's best choice (3) can be re-expressed as

$$p(z) = z\Big(\sqrt{\frac{1}{1-\alpha}} - z(C-x)\Big). \quad (6)$$

Meanwhile, the SP's optimization problem `(SP-P)` can be equivalently transformed into the following problem (here the symbol prime denotes the "Equivalence")

$$\texttt{(SP-P')}: \quad \max_{z\geq 0} \widetilde{V}(z) = F(z)G(z)$$
$$\text{subject to: } \sqrt{\mu} \leq z \leq \sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}, \quad (7)$$

where

$$F(z) = z\Big(\sqrt{\frac{1}{1-\alpha}} - (C-x)z\Big), \quad (8)$$
$$G(z) = \Big(1 - \alpha + \theta\alpha - (1-\alpha)\frac{\mu}{z^2}\Big). \quad (9)$$

However, directly solving the above problem (SP-P′) is yet straightforward because it is still nonconvex with respect to z. Fortunately, we can exploit the hidden structural property in problem (SP-P′), which facilitates our following solution procedures. As we will illustrate soon, the hidden property strongly depends on the EU's traffic load, which implies that *the EU's traffic load significantly influences the interaction between SP and EU as well as the resulting equilibrium-prepaying.* This influence can be intuitively interpreted as follows. With a heavy traffic load, the EU has a strong desire to improve its delay performance (according to the formula measuring the average traffic delay, a slight increase of the bandwidth limit will reduce the delay significantly under a heavy traffic load). Thus, the EU is willing to prepay more. In consequence, the SP sets a small β to maximize its reward. In contrast, with a light traffic load, the EU already has a good delay performance and hence has a weak desire to improve its delay performance. Thus, the EU will prepay less and the SP has to set a greater β (even close to 1).

In the next three subsections, we will illustrate the above intuition by quantifying three different traffic load regions (namely, the heavy, medium and light regions) and investigating the equilibrium for each region, respectively.

3.2 Equilibrium Under the Heavy Traffic Load Region

We first consider the heavy traffic load region. Suppose that $\sqrt{\mu} \leq \frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$ holds, which is equivalent to that the traffic load x meets $C \geq x \geq C - \frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{\sqrt{\mu}}$. We thus call it the heavy traffic load region. Our key findings in this region are as follows.

Key Findings in the Heavy Region: Each traffic load x in the heavy load region corresponds to a unique equilibrium, where the SP's policy $1 > \beta^* > 0$, and the SU's prepaid amount $p^* > 0$. Correspondingly, both SP and EU receive positive rewards at the equilibrium, i.e., they benefit from the this prepayment simultaneously.

As will be explained in Sect. 4, Fig. 1 shows the profile of equilibrium under different traffic loads via a numerical example. Figure 2 further shows the corresponding rewards at the equilibrium. Specifically, the above findings along with the numerical results match our intuition that the EU is strongly motivated to prepay under a heavy traffic load to improve its delay-performance and both the SP and EU will benefit from the prepayment significantly.

We explain these findings as follows. To solve problem (SP-P′) in the heavy traffic region, we first divide the feasible range of the decision variable z into two subranges, namely *Subrange 1:* $\sqrt{\mu} \leq z \leq \frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$ and *Subrange 2:* $\frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x} \leq z \leq \sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$. Next, we quantify the value of z which can maximize $\widetilde{V}(z)$ for each subrange as follows.

(1) Subrange 1: $\sqrt{\mu} \leq z \leq \frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$

It can be checked that both $F(z)$ and $G(z)$ are increasing in z. Hence, $\widetilde{V}(z)$ is increasing. As a result, in *Subrange 1*, the value of z that maximizes the objective function $\widetilde{V}(z)$ of problem (SP-P′) can be directly given as $z^* = \frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$.

(2) Subrange 2: $\frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x} \leq z \leq \sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$

$F(z)$ is decreasing in z while $G(z)$ is increasing in z. By checking $\frac{d\widetilde{V}(z)}{dz}$, we obtain

$$H(z) = \frac{d\widetilde{V}(z)}{dz} = \sqrt{\frac{1}{1-\alpha}}(1-\alpha+\theta\alpha)+\sqrt{1-\alpha}\frac{\mu}{z^2}-2z(C-x)(1-\alpha+\theta\alpha). \quad (10)$$

Notice that $H(z)$ is strictly decreasing in z, which implies that $\widetilde{V}(z)$ is strictly concave with respect to z. Therefore, in *Subrange 2*, there will be a unique value of z that maximizes $\widetilde{V}(z)$. Nevertheless, quantifying this unique z in a closed-form expression is challenging. Fortunately, we can identify the following result regarding to $H(z)$.

Proposition 1: In *Subrange 2* (i.e., $\frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x} \leq z \leq \sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$), there exists a unique value of z, which meets the condition that $H(z) = 0$.

Proof: We first show the following two important properties.
Property (i): by substituting $z = \sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$ into $H(z)$ (10), we obtain the following result

$$H(\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}) = \sqrt{\frac{1}{1-\alpha}}\big((1-\alpha)\mu(1-\alpha)(C-x)^2 - ((1-\alpha)+\theta\alpha)\big).$$

Since $\sqrt{\mu} \leq \sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$, i.e. $\mu(1-\alpha)(C-x)^2 \leq 1$, there exists $H(\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}) \leq 0$.
Property (ii): by substituting $z = \frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$ into $H(z)$ (10), we obtain the following result

$$H(\frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}) = 4\mu(1-\alpha)^{\frac{3}{2}}(C-x)^2 \geq 0.$$

The above *property (i)* and *property (ii)*, along with the property that $H(z)$ is strictly decreasing, indicate that within *Subrange 2*, i.e. $\frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x} \leq z \leq \sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$, there exists a unique value of z satisfying the condition $H(z) = 0$. Hence, we finish the proof. ■

(3) Summary of the Results in Subrange 1 and Subrange 2

Notice that the condition $H(z) = 0$ suffices to be the optimality condition for problem (SP-P′) under the heavy load region. Our analysis of *Subrange 1* and *Subrange 2* shows that, in the heavy load region, there exists a unique optimal solution for (SP-P′), and moreover this optimal solution resides within the range of $\frac{1}{2}\sqrt{\frac{1}{1-\alpha}\frac{1}{C-x}} \le z \le \sqrt{\frac{1}{1-\alpha}\frac{1}{C-x}}$. Let z^* denote this optimal solution. By exploiting the property that $H(z)$ is strictly decreasing, we can use the bisection algorithm to find z^* within the range of $\frac{1}{2}\sqrt{\frac{1}{1-\alpha}\frac{1}{C-x}} \le z \le \sqrt{\frac{1}{1-\alpha}\frac{1}{C-x}}$, thus solving problem (SP-P′). In particular, by using the bisection algorithm, we can determine this z^* within $\log_2 \frac{\frac{1}{2}\sqrt{\frac{1}{1-\alpha}\frac{1}{C-x}}}{\epsilon}$ rounds of iteration, where ϵ denotes the tolerance level of numerical error. After that, at the equilibrium, the SP's prepayment policy is given by

$$\beta^* = \frac{\mu}{(z^*)^2}, \tag{11}$$

and according to (6) the EU's prepaid amount is given by

$$p^* = z^*\Big(\sqrt{\frac{1}{1-\alpha}} - z^*(C-x)\Big). \tag{12}$$

3.3 Equilibrium Under the Medium Traffic Load Region

Next, we consider the medium traffic load region. Specifically, suppose that $\frac{1}{2}\sqrt{\frac{1}{1-\alpha}\frac{1}{C-x}} \le \sqrt{\mu} \le \sqrt{\frac{1}{1-\alpha}\frac{1}{C-x}}$, which is equivalent to that the traffic load x meets the condition $C - \frac{1}{2}\sqrt{\frac{1}{1-\alpha}\frac{1}{\sqrt{\mu}}} \ge x \ge C - \sqrt{\frac{1}{1-\alpha}\frac{1}{\sqrt{\mu}}}$. We thus call it the medium traffic load region. Our findings in this region are as follows.

Key Findings in the Medium Region: Each load x the medium region corresponds to a unique equilibrium. In particular, there exists a special traffic threshold Γ in the medium region. When the EU traffic load x is below Γ, then the SP's policy $\beta^* = 1$ (i.e., the SP has to spend entire the EU's prepayment in increasing the bandwidth-limit to attract the EU), and the EU's prepaid amount $p^* > 0$. Correspondingly, both the SP and EU obtain positive rewards, i.e., they benefit from the prepayment scheme (notice that even with $\beta^* = 1$, the SP still obtains a positive reward from saving its loss due to bad-debt). However, these rewards decrease as the EU traffic load x decreases.

As to be explained in Sect. 4, Fig. 1 shows the profile of equilibrium via a numerical example, and Fig. 2 shows the corresponding rewards, which verify the above findings. Compared to the heavy region, the EU becomes less motivated to prepay as its traffic load decreases in the medium region. As a result, the SP has to spend more in increasing its bandwidth to encourage the EU to prepay. Moreover, when the EU's traffic load is below the threshold Γ, the SP has to spend the entire prepayment in increasing its bandwidth. All these match our intuitions well.

We further explain these findings as follows. Notice that for the same reason as we describe in the previous subsection, there exists $H(\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}) \leq 0$. By substituting $\sqrt{\mu}$ into $H(z)$, we obtain that

$$H(\sqrt{\mu}) = 2(C-x)((1-\alpha)+\theta\alpha)(S-\sqrt{\mu}),$$

where

$$S = \frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x} + \frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}\frac{1-\alpha}{(1-\alpha)+\theta\alpha}.$$

Notice that $\frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x} \leq S \leq \sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$ always holds. In particular, the value of $H(\sqrt{\mu})$ is of interest since it helps to divide the medium traffic load region into two subregions with different characteristics, i.e., (i) the subregion that yields the SP's prepayment policy $\beta = 1$, and (ii) the subregion that yields the SP's prepayment policy $\beta < 1$. The details are illustrated as follows. By setting $H(\sqrt{\mu}) = 0$, we determine a threshold Γ with respect to the traffic load as

$$\Gamma = C - \frac{1}{\sqrt{\mu}}\left(\frac{1}{2}\sqrt{\frac{1}{1-\alpha}} + \frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1-\alpha}{1-\alpha+\theta\alpha}\right). \tag{13}$$

Using the threshold Γ, we thus consider two different subregions for the traffic load, namely, *Subregion (i):* $C - \sqrt{\frac{1}{1-\alpha}}\frac{1}{\sqrt{\mu}} \leq x \leq \Gamma$ and *Subregion (ii):* $\Gamma \leq x \leq C - \frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{\sqrt{\mu}}$. The details are as follows.

Subregion (i): the traffic load subregion of $C - \sqrt{\frac{1}{1-\alpha}}\frac{1}{\sqrt{\mu}} \leq x \leq \Gamma$.

When $C - \sqrt{\frac{1}{1-\alpha}}\frac{1}{\sqrt{\mu}} \leq x \leq \Gamma$, then $H(\sqrt{\mu}) \leq 0$. Since $H(\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}) \leq 0$ and $H(z)$ is strictly decreasing in z, there always exists $H(z) \leq 0$ within the range of $\sqrt{\mu} \leq z \leq \sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$. Therefore, the optimal solution for problem (SP-P′) can be directly given by $z^* = \sqrt{\mu}$ and $\beta^* = 1$. This result means that at the equilibrium, the SP has to use the entire EU's prepayment to increase its bandwidth. Correspondingly, the EU's prepaid amount can be determined as $p^* = \sqrt{\mu}\big(\sqrt{\frac{1}{1-\alpha}} - \sqrt{\mu}(C-x)\big)$ according to (3). Notice that even using $\beta^* = 1$, the SP still gets a nonnegative reward equal to $\theta\alpha\sqrt{\mu}\big(\sqrt{\frac{1}{1-\alpha}} - \sqrt{\mu}(C-x)\big)$, which stems from saving its loss in bad-debt.

Subregion (ii): the traffic load subregion of $\Gamma \leq x \leq C - \frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{\sqrt{\mu}}$.

When $\Gamma \leq x \leq C - \frac{1}{2}\sqrt{\frac{1}{1-\alpha}}\frac{1}{\sqrt{\mu}}$, then $H(\sqrt{\mu}) \geq 0$. Since $H(\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}) \leq 0$ and $H(\sqrt{\mu}) \geq 0$, further along with the property that $H(z)$ is strictly decreasing in z, there exists a unique value of z within the range of $\sqrt{\mu} \leq z \leq \sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}$ such that $H(z) = 0$, which corresponds to the optimality condition for problem (SP-P′). Again, let z^* denote the optimal value of z for problem (SP-P′). We can use the bisection algorithm to determine z^* such that $H(z^*) = 0$ is reached

(within $\log_2 \frac{\sqrt{\frac{1}{1-\alpha}}\frac{1}{C-x}-\sqrt{\mu}}{\epsilon}$ rounds of iteration). Therefore, the equilibrium can be given by $\beta^* = \frac{\mu}{(z^*)^2}$ and $p^* = z^*\big(\sqrt{\frac{1}{1-\alpha}} - z^*(c-x)\big)$.

In summary, in the region of the medium traffic load, by further differentiating two subregions (which are separated by the threshold Γ), we successfully quantify the equilibrium (β^*, p^*) for the proposed game.

Remark 2: The traffic threshold Γ, which separates the medium traffic load region, is an important indicator that determines *whether the SP will spend the entire EU's prepaid amount in increasing its bandwidth-limit or not.* Intuitively, with a traffic load below Γ, the EU is less motivated to prepay for an improved QoS performance. As a result, the SP has to spend more to attract the EU and thus gain less.

Remark 3: The traffic load threshold Γ given in (13) has the following three properties. Property (i): Γ is increasing in the risk factor θ; Property (ii): Γ is increasing in the marginal bandwidth-cost μ; Property (iii): Γ is decreasing in the discount factor α.

Property (i) is a direct result from (13). Intuitively, when the risk factor θ is larger, the SP can save more from reducing the bad-debt according to (1). Thus, the SP tends to increase its β, i.e. using a large portion of EU's prepaid amount to increase its access bandwidth.

Property (ii) is also a direct result from (13). It can be interpreted as follows. When the marginal cost μ is larger, the EU's improved delay performance tends to decrease according to (2) and (4). As a result, the SP has to increase its β to compensate for the EU's loss more significantly such that the EU is still motivated to prepay.

Property (iii) can be proved by showing that $\frac{\partial \Gamma}{\partial \alpha} \leq 0$. First, let $\Omega = \sqrt{\frac{1}{1-\alpha}}(1 + \frac{1-\alpha}{1-\alpha+\theta\alpha})$. We thus have $\Gamma = C - \frac{1}{\sqrt{\mu}}\frac{1}{2}\Omega$. Specifically, there exists

$$\frac{\partial \Omega}{\partial \alpha} = \sqrt{\frac{1}{1-\alpha}}\{\frac{(1-\alpha)(1-\theta)}{(1-\alpha+\theta\alpha)^2} + \frac{1}{2}\frac{1}{1-\alpha+\theta\alpha}\frac{\theta\alpha}{1-\alpha}\} \geq 0.$$

Since Ω is increasing in the discount factor α, Γ is decreasing in α. Intuitively, when the discount factor α is greater, the EU's economic loss decreases, and thus EU will receive a greater reward according to (2) and (4). As a result, the SP can reduce its β accordingly, meaning that the SP spends less in increasing its access bandwidth.

Due to the limited space, we will skip the details about the analysis for the light traffic load region in which the traffic load x satisfies $0 \leq x \leq C - \sqrt{\frac{1}{1-\alpha}}\frac{1}{\sqrt{\mu}}$. Notice that the methodology to analyze the light traffic load region is similar to that for the heave and medium load regions.

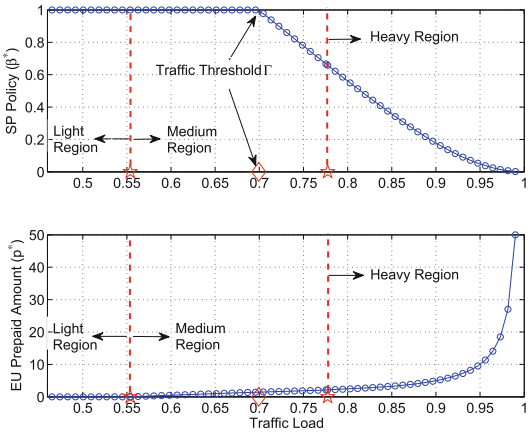


Fig. 1. Examples of equilibrium profile (β^*, p^*) under different traffic loads. Top subfigure: SP's prepayment policy β^* at the equilibrium. Bottom subfigure: EU's prepaid amount p^* at the equilibrium. We set $C = 10, \mu = 1, \alpha = 0.95, \theta = 0.1$.

4 Numerical Results

4.1 Equilibrium and the Corresponding Rewards

Figure 1 shows the equilibrium (β^*, p^*) under different traffic loads. We normalize both the traffic load x and the load threshold Γ by the link bandwidth C (i.e., the horizontal axis denotes the value of $\frac{x}{C}$). In Fig. 1, different traffic load regions are separated by the dash lines. Notice that in the light region we always have the SP's prepayment policy $\beta^* = 1$ and the EU's prepaid amount $p^* = 0$ at the equilibrium.

The results shown in Fig. 1 verify the equilibrium analyzed in Sect. 3. Specifically, when the EU's traffic load is in the medium region and below the traffic threshold Γ (which is denoted by the diamond), the EU has a relatively weak desire to improve its delay performance, and hence its prepaid amount p^* is relatively small. Correspondingly, the SP sets its prepayment policy $\beta^* = 1$ to encourage the EU's prepaying. In comparison, when the EU's traffic load is above the traffic threshold Γ, the EU's desire to improve its delay performance increases, and its prepaid amount p^* increases. Correspondingly, the SP can adopt a smaller β^*. Furthermore, when the EU's traffic load falls into in the heavy traffic-load region, the EU has a strong desire to improve its delay performance, and hence its prepaid amount p^* increases dramatically. Correspondingly, the SP further reduces its β^*.

Figure 2 further shows the rewards obtained by the SP and the EU at the equilibrium. Specifically, in the medium traffic load region, both the rewards of the SP and the EU are relatively low due to the EU's weak desire to improve its delay. In comparison, when the EU's traffic load is heavy, both the SP and the EU obtain significant rewards from the prepayments since the EU has a strong desire

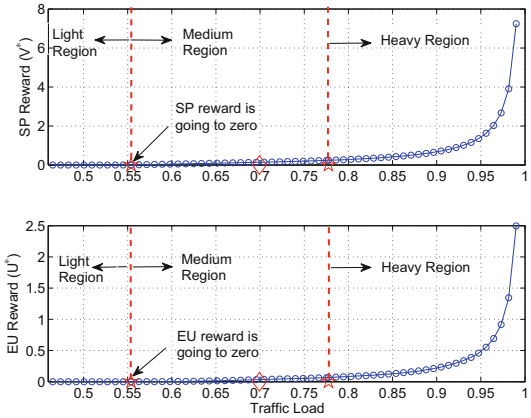


Fig. 2. Examples of equilibrium rewards under different traffic loads. Top subfigure: SP's reward at the equilibrium. Bottom subfigure: the EU's reward at the equilibrium. We set $C = 10, \mu = 1, \alpha = 0.95, \theta = 0.1$.

to improve its delay and hence a greater motivation for prepaying. In particular, the positive EU's reward and the positive SP's reward at the equilibrium (in the medium and heavy traffic regions) shown in Fig. 2 indicate that both the EU and SP can positively gain from prepaying in comparison with conventional post-payment scheme, i.e., thus achieving a desirable win-win result. Notice that as stated in Sect. 2, our definitions for the SP's reward and the EU's reward can be considered as measures of relative gains achieved by the prepayment schemes in comparison with the post-payment scheme. Therefore, the positive EU's reward and SP's reward at the equilibrium indicate the superior performance of the prepayment scheme.

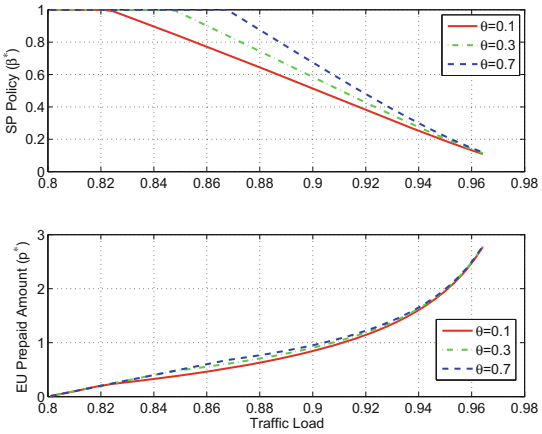


Fig. 3. Impact of the risk factor θ on the equilibrium profile. We set $\alpha = 0.75, \mu = 1$. Top subfigure: SP's prepayment policy β^*; Bottom subfigure: EU's prepaid amount p^*.

Figures 3 and 4 show the impact of the risk factor θ on the SP's prepayment policy and EU's prepaid amount at the equilibrium as well as their rewards.

The top subfigure in Fig. 3 shows that when the risk factor θ increases, the SP also increases its β^*. This result is consistent with the intuition well. Since as θ increases, the SP tries to save more by reducing its bad-debt according to its reward (5). Thus, the SP is willing to spend a greater part of the EU's prepaid amount in increasing the link capacity. Analytically, this result can also be illustrated as follows. To guarantee $H(z) = 0$, it requires (after some manipulations):

$$\sqrt{\frac{1}{1-\alpha}} = 2z(C-x) - \frac{\sqrt{1-\alpha}}{1-\alpha+\theta\alpha}\frac{\mu}{z^2}. \tag{14}$$

The right hand side (RHS) of (14) is increasing in both θ and z. Therefore, to meet condition (14), the optimal value of z decreases as θ increases. Thus, the SP's $\beta = \frac{\mu}{z^2}$ increases accordingly. Notice that the top subfigure in Fig. 3 also verifies that the traffic threshold Γ (i.e., the threshold beyond which the SP's policy $\beta^* < 1$) is increasing in θ, as stated in Property (i) Remark 3.

The bottom subfigure in Fig. 3 shows that as the risk factor θ increases, the EU also increases its prepaid amount p^*. This result matches the intuition that as the risk factor θ increases, the SP is willing to spend a greater portion of the EU's prepayment in increasing its link capacity, and the EU thus finds it is profitable to prepay more. Also analytically, this result can be illustrated as follows. Based on our analysis in Sect. 3, the optimal value of z can only reside in the interval of $[\max(\sqrt{\mu}, \frac{1}{2}\sqrt{\frac{1}{1-\alpha}\frac{1}{C-x}}), \sqrt{\frac{1}{1-\alpha}\frac{1}{C-x}})]$. Thus, according to the EU's best choice function (6), the EU's prepaid amount $p(z)$ is decreasing in z. Since z decreases as θ increases, the EU's prepaid amount p increases accordingly.

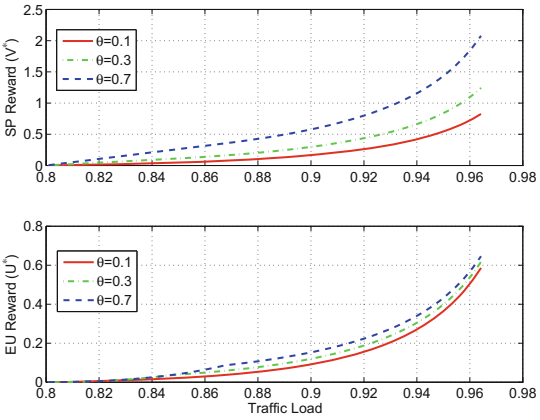


Fig. 4. Impact of the risk factor θ on the equilibrium rewards. We set $\alpha = 0.75, \mu = 1$. Top subfigure: SP's reward at the equilibrium; Bottom subfigure: EU's reward at the equilibrium.

Meanwhile, the results of Fig. 4 show that both the SP and the EU can benefit more from the prepayment scheme when the risk factor θ increases. Intuitively, as the risk factor increases, the prepayment scheme can save the SP's loss more due to bad-debt. Thus, both the SP and EUs benefit more. Specifically, the bottom subfigure in Fig. 4 shows as the risk factor θ increases, the EU's reward at the equilibrium increases. This result can be illustrated analytically as follows. According to (4), the EU's reward at equilibrium can be given by $U^*(z) = \frac{1}{C-x}(1 - z\sqrt{1-\alpha}(C-x))^2$ (for an easy presentation we stick with the use of $U(.)$ as the EU's reward function, which is a function of z instead of β). Since the SP's optimal decision z decreases as θ increases, the EU's utility increases consequently. Meanwhile, the top subfigure in Fig. 4 shows that the SP's reward at the equilibrium also increases as the risk factor θ increases.

5 Conclusion and Future Work

In this paper, we propose a smart prepayment scheme for the SP of access networks to improve its economic reward and better EUs' QoS-performance. Our analysis based on the model of Stackelberg game shows that both the SP and EUs can benefit from the optimal prepayment scheme (i.e., the equilibrium of the proposed game), thus yielding a win-win outcome. We also find that the EU's traffic load influences the optimal prepayment scheme, which we quantify and analyze by considering three different traffic load regions.

Acknowledgement. This work was supported in part by the National Natural Science Foundation of China under Grant 61572440 and Grant 61379122, in part by the Zhejiang Provincial Natural Science Foundation of China under Grant LR17F010002 and Grant LR16F010003, and in part by the Young Talent Cultivation Project of Zhejiang Association for Science and Technology (2016YCGC011).

References

1. Sen, S., Wong, C.J., Ha, S., Chiang, M.: Pricing Data: A Look at Past Proposals, Current Plans, and Future Trends. http://arxiv.org/abs/1201.4197
2. Hande, P., Chiang, M., Calderbank, A.R.: Network rate allocation with content provider participation. In: Proceedings of the 28th IEEE International Conference on Computer Communications (INFOCOM 2009) (2009)
3. Wu, Y., Kim, H., Hande, P., Chiang, M., Tsang, D.H.K.: Revenue sharing among ISPs in two-sided markets. In: Proceedings of the 30th IEEE International Conference on Computer Communications (INFOCOM 2011) (2011)
4. Ma, R., Chiu, D.M., Lui, J.C.S., Misra, V., Rubenstein, D.: Interconnecting eyeballs to content: a shapley value perspective on ISP peering and settlement. In: Proceedings of the 3rd International Workshop on Economics of Networked Systems (NetEcon 2008) (2008)
5. Bader, A.M., Nidal, N., Hossam, H.: Congestion pricing in wireless cellular networks. IEEE Commun. Surv. Tutor. **13**(3), 358–371 (2011)
6. Kesidis, G., Das, A., de Veciana, G.: On flat-rate and usage-based pricing for tiered commodity internet services. In: Proceedings of the CISS 2008 (2008)

7. Jiang, L., Parekh, S., Walrand, J.: Time-dependent network pricing and bandwidth trading. In: Proceedings of IEEE NOMS Workshop 2008 (2008)
8. Lin, Y.B., Lao, C.H.R., Chang, M.F.: Mobile prepaid phone services. IEEE Pers. Commun. **7**(3), 6–14 (2000)
9. Anning, P.: Prepaid: Issues, Economics and Growth. Prepaid International Forum, October 2012. http://prepaidforum.org/live/wp-content/uploads/2012/11/PIF-White-Paper_Prepaid_-Issues-Economics-Growth.pdf
10. Sprint Nextel Reports First Quarter 2011 Results. http://newsroom.sprint.com/article_display.cfm?article_id=1879
11. HP Intel Solution Center Blueprint: Prepaid Services for New Generation Mobile Network. http://www.hp.com/products1/solutioncenters/pdfs/prepaid_blueprint.pdf
12. Chang, M.F., Yang, W.Z., Lin, Y.B.: Performance of service-node-based mobile prepaid service. IEEE Trans. Veh. Technol. **51**(3), 597–612 (2002)
13. Lin, P., Lin, Y.B., Gan, C.H., Jeng, J.Y.: Credit allocation for UMTS prepaid service. IEEE Trans. Veh. Technol. **55**(1), 306–316 (2006)
14. Wu, Y., Chen, J., Qian, L., Huang, J., Shen, X.: Energy-aware cooperative traffic offloading via Device-to-Device cooperations: an analytical approach. IEEE Trans. Mob. Comput. **16**(1), 97–114 (2017)
15. Chen, X., Jiao, L., Li, W., Fu, X.: Efficient multi-user computation offloading for mobile-edge cloud computing. IEEE/ACM Trans. Netw. **24**(5), 2795–2808 (2016)
16. Wu, Y., Guo, K., Huang, J., Shen, X.: Secrecy-based energy-efficient data offloading via dual-connectivity over unlicensed spectrums. IEEE J. Sel. Areas Commun. **34**(12), 3252–3270 (2016)
17. Shen, H., Basar, T.: Optimal nonlinear pricing for a monopolistic network service provider with complete and incomplete information. IEEE JSAC **25**(6), 1216–1223 (2007)
18. Le Cadre, H., Bouhtou, M., Tuffin, B.: A pricing model for a mobile network operator sharing limited resource with a mobile virtual network operator. In: Reichl, P., Stiller, B., Tuffin, B. (eds.) ICQT 2009. LNCS, vol. 5539, pp. 24–35. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-01796-4_4
19. Basar, T., Olsder, G.T.: Dynamic Noncooperative Game Theory, 2nd edn. SIAM Series Classics in Applied Mathematics. SIAM, Philadephia

Massive MIMO and mmWave

Massive MIMO for Future Vehicular Networks: Compressed-Sensing and Low-Complexity Detection Schemes (Invited Paper)

Fan Jiang[1], Cheng Li[1,2(✉)], Zijun Gong[1], and Yan Zhang[2]

[1] Department of Electrical and Computer Engineering, Memorial University of Newfoundland, St. John's, NL A1B 3X5, Canada
{fjiang,licheng,zg7454}@mun.ca
[2] Tianjin Chengjian University, Tianjin, China
zhangyan@tcu.edu.cn

Abstract. The fast development of the fifth generation (5G) mobile communications system has brought a bright prospect of the next generation vehicular networks. Especially, a typical application in future vehicular networks is to deploy intelligent transportation systems (ITS), aiming to providing high level user experience on the move. To support the deployment of ITS, high rate communications and energy efficiency, low-latency transmission and low-complexity detection schemes are highly demanded. Massive multiple-input multiple-output (MIMO) has been seen as a promising candidate for the demand. The architecture that many vehicles access the roadside infrastructure is quite suitable for the employment of massive MIMO as large-scale antennas can be deployed at the roadside unit. However, the challenges along with massive MIMO is low complexity and efficient data detection schemes. In this paper, we provide an overview of low-complexity detection schemes in massive MIMO, and summarize the challenges and possible solutions.

Keywords: Vehicular networks · Massive MIMO · Low-complexity

1 Introduction

1.1 Intelligent Transportation Systems

With increasing number of vehicles on road nowadays, driving safety, traffic efficiency, and high quality in-vehicle entertainment service, have drawn much attention in both academia and industry [1–4]. The emerging intelligent transportation systems (ITS) have been widely studied aiming to meeting these requirements. Generally, both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications are required in ITS [1,2]. Specially, all vehicles on the road collect sensor data, including traffic information and road

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 53–63, 2018.
https://doi.org/10.1007/978-3-319-90802-1_5

conditions, and share with neighboring vehicles through V2V communications or report to roadside infrastructure through V2I communications. To fulfill these tasks, each vehicle is equipped with on-board unit (OBU), while the roadside unit (RSU) is deployed along the roadside infrastructure. OBU and RSU are acting as the radio interface to establish the dependable connection [1]. It is reported that 90% of vehicles will be connected via wireless links by 2020 [3]. Therefore, the deployment and investigation of ITS becomes significant.

Fig. 1. A typical vehicular network to support ITS service

A typical application scenario for ITS service is shown in Fig. 1, where multiple RSUs are deployed along the traffic road, serving numbers of vehicles on the street. Vehicles are connected through V2V communication links, so that information about traffic status and road conditions can be shared among vehicles. Besides, the vehicles can also access the RSU through V2I communication links, which supports various in-vehicle entertainment service such as video streaming and social interactions. Suppose an ambulance vehicle is committing an emergence and a huge number of cars are crowded in a busy street. On the one hand, the emergence information can be reported to all vehicles through V2V communications, and then all vehicles make proper action to cooperate. On the other hand, an alternative solution might be that the RSU collects this information and broadcasts in the vehicular network. By doing that, all vehicles in its communication range will be aware of this information. Actually, the important role of the RSU playing in ITS service has been demonstrated in [3–5]. Therefore, we mainly focus on V2I communication in this paper.

1.2 Massive MIMO in Vehicular-to-Infrastructure Communications

Using massive multiple-input multiple-output (MIMO) in next generation vehicular networks, has been investigated recently [5,6]. It is known that in current traditional small-scale MIMO system, the antenna size is limited since the wave length of the microwave signal is relatively large. However, millimeter wave frequency band has been proposed in vehicular communication, which enables the antenna elements at RSU reach up to 256 [6]. Besides, the massive MIMO architecture is suitable for multiple vehicles accessing RSU since hundreds of antennas can be deployed at roadside infrastructure. Massive MIMO has shown significant potential in improving system spectrum efficiency and energy efficiency [7,8]. These improvements, are beneficial to future vehicular networks.

Along with the benefits of massive MIMO, some practical issues need be addressed. Typically, in massive MIMO, the large array signal processing at RSU is a high computational load. The processing delay associated with the detection has great impact on the system latency requirement. To deal with these practical issues, we need low-complexity and efficient detection schemes. Besides, compressed-sensing based techniques have been widely applied to communication systems. For example, it is employed in [9] for channel estimation. In massive MIMO, it also has many possible roles to play, and one of them is data detection, as will be discussed in this paper.

1.3 Main Contributions

In [10], MIMO Detection schemes in fifty years have been summarized by the year of 2014. However, at that time, few works have been done on massive MIMO detection. As we know, the turbo receivers show great performance in the traditional small scale MIMO-OFDM systems for data detection [11,12]. For massive MIMO, many new works on data detection have been proposed recently, including using compressed sensing technique [13–15], and iterative methods [16–18]. In this paper, we will extensively overview these new detection schemes and summarize the challenges and possible solutions in the applications to vehicular communications.

1.4 Organization

The rest of the paper is organized as follows. In Sect. 2, we briefly introduce the massive MIMO system model. Compressed-sensing based data detection schemes are illustrated in Sect. 3. We present a class of low-complexity near linear minimum mean-square error (MMSE) detection schemes in Sect. 4. Finally, the conclusions are drawn in Sect. 5.

2 System Model

Consider a massive MIMO system with N_B antennas equipped at RSU, and N_U vehicular users are under service ($N_B \geq N_U$). The relationship between the received vector and the transmitted symbols can be expressed as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{z}, \tag{1}$$

where $\mathbf{y} \in \mathbb{C}^{N_B \times 1}$ denotes the received vector at base station. $\mathbf{H} \in \mathbb{C}^{N_B \times N_U}$ denotes the channel matrix, with the u-th column vector $\mathbf{h}_u = \mathbf{H}\mathbf{e}_u$ representing the channel impulse response from the u-th user to the base station. $\mathbf{x} \in \mathbb{C}^{N_U \times 1}$ is the transmitted symbol vector. $\mathbf{z} \in \mathbb{C}^{N_B \times 1}$ is the additive white Gaussian noise vector, satisfying $\mathrm{E}\left\{\mathbf{z}\mathbf{z}^{\mathrm{H}}\right\} = \sigma_z^2 \mathbf{I}_{N_B}$.

In [10], massive MIMO systems are divided into two groups, according to $\lim_{N_B, N_U \to \infty} \frac{N_U}{N_B} = c$ or $\lim_{N_B \to \infty} \frac{N_U}{N_B} = 0$. However, we can see this classification is not practical. This is because in real system configuration, the number of antennas and users will not be infinite. In this paper, we define $r = \frac{N_B}{N_U}$, $r \geq 1$. When r is sufficiently large, it corresponds the case that $\lim_{N_B \to \infty} \frac{N_U}{N_B} = 0$; and $r \to 1$, it corresponds to the case that the number of users is comparable to the number of antennas at base station. For different range, different detection schemes can be applied.

In the case r is close to 1, compressed-sensing based data detection schemes can be applied. In the case r is sufficiently large, low-complexity near Linear MMSE detection schemes can be adopted.

3 Compressed-Sensing Based Data Detection

When $r \to 1$, the performance of the linear MMSE detection scheme is far away from the optimal system performance [13]. By noting that the detected symbol vector after conventional detectors is generally acceptable in the operating regime, the error vector $\mathbf{e} = \mathbf{x} - \widehat{\mathbf{x}}$ is sparse. Therefore, we can use compressed-sensing techniques to recover the sparse error vector, hence the transmitted symbols. The block diagram of the compressed-sensing based detection schemes are shown in Fig. 2.

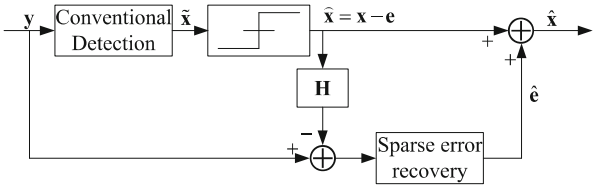


Fig. 2. Block diagram of the compressed-sensing based detection schemes

3.1 Transform to Sparse Vector Estimation Model

As the original transmitted symbols in (1) is non-sparse, the compressed-sensing techniques cannot directly applied to (1). Therefore, we need to transform the detection model to a sparse vector estimation one.

To begin with, with conventional detectors, the output estimation can be quantized to the closest constellation symbol. In adequate operating regime, the quantization error is small, for example, less than 10^{-1}. That is to say, the error vector after quantization is sparse, hence we can establish a new detection model, given by

$$\widehat{\mathbf{y}} = \mathbf{y} - \mathbf{H}\widehat{\mathbf{x}} = \mathbf{H}\mathbf{e} + \mathbf{z}. \tag{2}$$

As $\mathbf{e}$ is sparse, we can adopt the compressed-sensing techniques to recover $\mathbf{e}$.

3.2 Prevailing Compressed-Sensing Methods

Since $\mathbf{e}$ in Eq. (2) is sparse, the intuitive solutions to Eq. (2) is to find a sparse vector under the system constrain. Hence, we can use convex optimization approaches such as basis pursuit de-nosing method [19]. However, the computational complexity of such algorithms (or its variations) are, generally, is the order of $\mathcal{O}\left(N_B^2 N_U^3\right)$. Low-complexity compressed-sensing techniques normally are generalized as greedy algorithms or iterative methods.

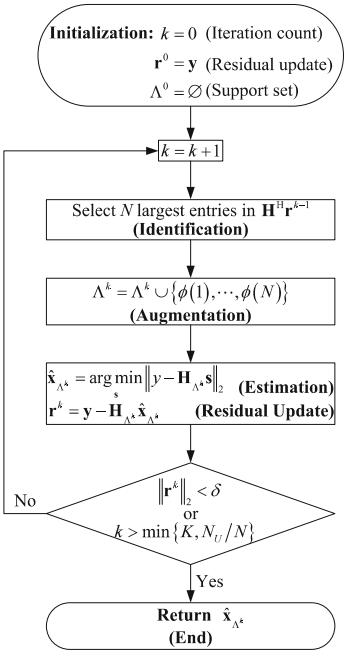


Fig. 3. The flow chart of the generalized OMP algorithm

The main process of the greedy algorithm consists of the following steps [13]: (1) identification; (2) augmentation; and (3) residual update. Specifically, the identification progress is to find the expected subset of the support sets. This

is usually to use the correlation between the selected columns from $\mathbf{H}$ and the residual. The augmentation progress is to generate the new sparse vector. The residual update is to generate the new residual by removing the identified sparse vector from received signal for next iteration. The well-known orthogonal matching pursuit (OMP) method is to find one optimal candidate using the greedy strategy [20]. Therefore, the overall computational complexity is in the order of $\mathcal{O}(KN_BN_U)$, where K is the sparsity of the signal vector. Some other variations of OMP have been investigated, such as compressive sampling matching pursuit (CoSaMP) [21], generalized OMP [22], and the most recent multipath matching pursuit [23]. Generally, the main difference between those variations is the identification and the correspondent augmentation progress. For example, generalized OMP is to select N indices instead of one in identification progress, and it degrades to OMP when $N = 1$. However, by selecting N indices, the iterations required for the recovery can be speeded up. The flow chart of the gOMP is presented in Fig. 3. Note in Fig. 3, when $N = 1$, the gOMP becomes OMP as for each iteration, only one candidate is selected.

Another low complexity compressed-sensing technique is to use iterative methods for sparse signal recovery [24]. The iterative update step is given by

$$\hat{\mathbf{s}}^{(i+1)} = T\left(\hat{\mathbf{s}}^{(i)} + \mathbf{H}^{\mathrm{H}}\left(\mathbf{y} - \mathbf{H}\hat{\mathbf{s}}^{(i)}\right)\right), \tag{3}$$

where $T(\cdot)$ is the thresholding operator to generate the next estimation from the previous estimation. More references in this algorithm can be found in [25,26].

3.3 Challenges and Possible Solutions

Compressed-sensing based detection schemes have shown enhanced performance compared to the conventional linear MMSE detection schemes. However, most of the work requires hard decision on symbol detection. That is to say, in each iteration, when the estimation is given, it is always quantized to the closed constellation symbol. However, in real applications, the soft-input channel coding schemes are always adopted, which requires soft output from the symbol detector. Therefore, we need to derive the soft output compressed sensing based detection schemes.

In order to address these issue, we need to investigate the expected signal component from the estimation, and derive the *a posteriori* signal-to-interference-plus-noise ratio (SINR). Different from hard decision strategy, the afterward processing may put extra computational load. However, soft output compressed-sensing based schemes, which are designed to maintain low complexity but achieve near optimal performance, will be an interesting topic.

4 Low-Complexity Near Linear MMSE Detection

As demonstrated in [7,8,16], when r is sufficiently large, by employing linear detection schemes, such as MMSE, zero-forcing, or even matched filter, we can

achieve near optimal system performance. Therefore, a class of these detection schemes have been widely studied recently [16–18,27–29]. Generally, these schemes can be categorized into two groups: to approach the matrix inversion [16,27] and to solve linear equations with iterative methods [17,18,28,29].

4.1 Methods to Approach Matrix Inversion

To begin with, the linear MMSE estimation in Eq. (1) is given by

$$\hat{\mathbf{x}} = \left(\mathbf{H}^{\mathrm{H}}\mathbf{H} + \sigma_z^2\mathbf{I}_{N_U}\right)^{-1}\mathbf{H}^{\mathrm{H}}\mathbf{y} = \mathbf{W}^{-1}\mathbf{y}^{\mathrm{MF}}, \tag{4}$$

where $\mathbf{W} = \mathbf{H}^{\mathrm{H}}\mathbf{H} + \sigma_z^2\mathbf{I}_{N_U}$, and $\mathbf{y}^{\mathrm{MF}} = \mathbf{H}^{\mathrm{H}}\mathbf{y}$ is the matched-filter output. With Neumann series expansion, the matrix inversion $\mathbf{W}^{-1}$ can be expanded as $\mathbf{W}^{-1} = \sum_{l=0}^{\infty}\left(\mathbf{X}^{-1}\left(\mathbf{X}-\mathbf{W}\right)\right)^l\mathbf{X}^{-1}$, where the convergence conditions are given by $\lim_{l\to\infty}\left(\mathbf{X}^{-1}\left(\mathbf{X}-\mathbf{W}\right)\right)^l = \mathbf{0}$. From the satisfied conditions, we can see that the higher order expansions can be omitted, leading to truncated approximation to matrix inversion, given by

$$\mathbf{W}^{-1} = \sum_{l=0}^{L-1}\left(\mathbf{X}^{-1}\left(\mathbf{X}-\mathbf{W}\right)\right)^l\mathbf{X}^{-1}. \tag{5}$$

When we select a matrix $\mathbf{X}$ that is very close to $\mathbf{W}$, the expansion order in Eq. (5) can be less than three, which is of low-complexity since the direct matrix inversion is in the order of $\mathcal{O}\left(N_U^3\right)$. Based on this idea, the authors in [16] select the diagonal matrix extracted from $\mathbf{W}$, and demonstrate that when $r \geq 16$, the expansion order $L \leq 3$.

However, using the diagonal matrix in the development may require large truncated orders when r is less than 16. To speed-up the convergence rate, Newton iteration has been introduced in [27]. However, Newton iteration involves matrix multiplications, and the computational complexity may be high even with only two iterations. Therefore, the authors in [27] propose to used the diagonal banded matrix in the development, and the iterations are limited to two. They also demonstrated that the performance with two iterations is better than that of the Neumann-series expansion based detection scheme when $r = 8$.

Generally, the methods to approach the matrix inversion suffers from matrix multiplications. Therefore, the applications of the methods in this category are limited to the scenario where r is sufficiently high (for example, $r \geq 8$).

4.2 Solving Linear Equations with Iterative Methods

By transforming the matrix inversion problem into linear equations, a class of iterative methods can be applied. To be specific, Eq. (4) is rewritten to

$$\mathbf{W}\hat{\mathbf{x}} = \mathbf{y}^{\mathrm{MF}}. \tag{6}$$

For Jacobi method [29], the iterative estimation is given by

$$\hat{\mathbf{x}}^{(i+1)} = \mathbf{D}^{-1}\left(\left(\mathbf{D}-\mathbf{W}\right)\hat{\mathbf{x}}^{(i)} + \mathbf{y}^{\mathrm{MF}}\right), \tag{7}$$

where $\mathbf{D} = \mathrm{diag}\left(\mathbf{W}\right)$. It has been shown in [17,30] that when the initial estimation for Jacobi method is given by $\hat{\mathbf{x}}^{(0)} = \mathbf{D}^{-1}\mathbf{y}^{\mathrm{MF}}$, the estimation after L iterations is equivalent to results in Neumann series expansion based method with L orders. However, instead of approaching the matrix inversion, the Jacobi method is to approach the estimation vector and only matrix-vector product is involved in iterative process. Therefore, the computational complexity is much reduced, allowing large number of iterations.

Similarly, the Gauss-Seidel method proposed in [28] using the triangular matrix in the development. Since an successive detection manner is introduced in Gauss-Seidel method, the convergence performance (rate and probability that convergence conditions are satisfied) is greatly improved [28]. Using this idea, the development of using the stair matrix in massive MIMO uplink signal detection is presented in [17]. It has been demonstrated that by using the stair matrix, the probability that the convergence conditions are satisfied is improved compared to the use of the diagonal matrix, which indicates that the system requirement for large r can be released. Meanwhile, the convergence rate is also improved, which means less iterations are required for convergence.

4.3 Challenges and Possible Solutions

Iterative methods have the advantages of low complexity; however, the processing time introduced in iterative processing is significant. Therefore, to achieve fast processing time but maintain near optimal system performance is a critical challenge for implementation.

One possible solution to the challengeable issue mentioned above is to use parallel processing structure. For example, in [18], the authors propose a block Gauss-Seidel method based signal detection scheme for massive MIMO in V2I communications. The main idea behind that proposal is to implement the iterative estimation in several independent blocks. This is realized by using the block diagonal matrix in the development of the iterative method. Specifically, $\mathbf{W}$ is divided into $\mathbf{W} = \mathbf{P} + \mathbf{Q}$, with the block diagonal matrix $\mathbf{P}$ given by

$$\mathbf{P} = \begin{bmatrix} \mathbf{P}\left(1\right) & & & \\ & \mathbf{P}\left(2\right) & & \\ & & \ddots & \\ & & & \mathbf{P}\left(B\right) \end{bmatrix}.$$

In addition, the iterative estimation can be given as

$$\mathbf{P}\hat{\mathbf{x}}^{(i+1)} = \mathbf{y}^{\mathrm{MF}} - \mathbf{Q}\hat{\mathbf{x}}^{(i)}, \tag{8}$$

Since $\mathbf{P}$ is a block diagonal matrix, the iterative estimation in Eq. (8) can be updated on each individual block independently, each with a much degraded

matrix size. The independent block update procedure can be implemented with parallel processing structure, and the processing time in each iteration can be greatly reduced. The parallel processing structure for the proposed detection scheme in [18] is shown in Fig. 4.

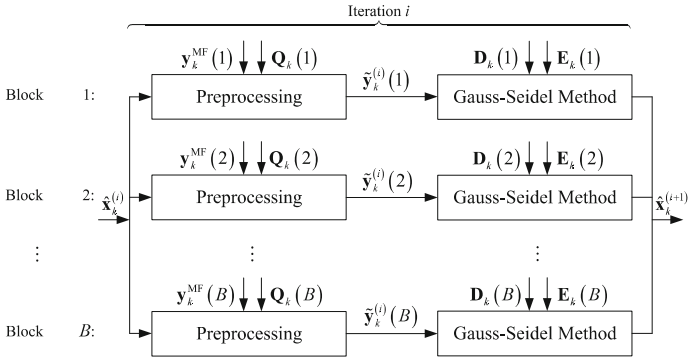


Fig. 4. The parallel processing structure of the block Gauss-Seidel method [18].

However, as the block diagonal matrix is adopted, the convergence performance (in terms of convergence rate and the probability that the convergence conditions are satisfied) will be another issue to be addressed.

5 Conclusions

In this paper, we start from the requirements of the ITS, and introduce a promising candidate technique, massive MIMO, for future vehicular networks. Especially, we specify that massive MIMO is quite suitable for multiple vehicles to access the roadside infrastructure where large scale antennas can be deployed. In addition, we overview the newly proposed compressed-sensing technique and a class of low-complexity near linear MMSE detection schemes in massive MIMO uplink data detection. We present the general procedure in implementation, and summarize future challenges and possible solutions along with these new techniques. Those challengeable issues brought in this paper can be valuable references for future research topics.

References

1. Mecklenbrauker, C., Molisch, A., Karedal, J., Tufvesson, F., Paier, A., Bernado, L., Zemen, T., Klemp, O., Czink, N.: Vehicular channel characterization and its implications for wireless system design and performance. IEEE Proc. **99**(7), 1189–1212 (2011)
2. Viriyasitavat, W., Boban, M., Tsai, H., Vasilakos, A.: Vehicular communications: survey and challenges of channel and propagation models. IEEE Veh. Technol. Mag. **10**(2), 55–66 (2015)

3. Su, Z., Hui, Y., Yang, Q.: The next generation vehicular networks: a content-centric framework. IEEE Wirel. Commun. Mag. **24**(1), 60–66 (2017)
4. Li, P., Zhang, T., Huang, C., Chen, X., Fu, B.: RSU-assisted geocast in vehicular ad hoc networks. IEEE Wirel. Commun. Mag. **24**(1), 53–59 (2017)
5. Zhang, R., Zhong, Z., Zhao, J., Li, B., Wang, K.: Channel measurement and packet-level modeling for V2I spatial multiplexing uplinks using massive MIMO. IEEE Trans. Veh. Technol. **65**(10), 7831–7843 (2016)
6. Choi, J., Va, V., Gonzalez-Prelcic, N., Daniels, R., Bhat, C., Heath, R.: Millimeter wave vehicular communication to support massive automotive sensing. IEEE Commun. Mag. **54**(12), 160–167 (2016)
7. Marzetta, T.: Noncooperative cellular wireless with unlimited numbers of base station antennas. IEEE Trans. Wirel. Commun. **9**(11), 3590–3600 (2010)
8. Ngo, H., Larsson, E., Marzetta, T.: Energy and spectral efficiency of very large multiuser MIMO systems. IEEE Trans. Commun. **61**(4), 1436–1449 (2013)
9. Zhang, Y., Venkatesan, R., Dobre, O.A., Li, C.: Novel compressed sensing-based channel estimation algorithm and near-optimal pilot placement scheme. IEEE Trans. Wirel. Commun. **15**(4), 2590–2603 (2016)
10. Yang, S., Hanzo, L.: Fifty years of MIMO detection: the road to large-scale MIMOs. IEEE Commun. Surv. Tutor. **17**(4), 1941–1988 (2015)
11. Jiang, F., Zhang, Y., Li, C.: A new SQRD-based soft interference cancelation scheme in multi-user MIMO SC-FDMA system. IEEE Commun. Lett. **21**(4), 821–824 (2017)
12. Li, C., Jiang, F., Meng, C., Gong, Z.: A new turbo equalizer conditioned on estimated channel for MIMO MMSE receiver. IEEE Commun. Lett. **21**(4), 957–960 (2017)
13. Choi, J., Shim, B.: New approach for massive MIMO detection using sparse error recovery. In: IEEE Proceedings of the GLOBECOM, Austin, TX, USA, pp. 3754–3759 (2014)
14. Peng, X., Wu, W., Sun, J., Liu, Y.: Sparsity-boosted detection for large MIMO systems. IEEE Commun. Lett. **19**(2), 191–194 (2015)
15. Choi, J., Shim, B., Ding, Y., Rao, B., Kim, D.: Compressed sensing for wireless communications: useful tips and tricks. IEEE Commun. Surv. Tutor. **19**(3), 1527–1550 (2017)
16. Wu, M., Yin, B., Wang, G., Dick, C., Cavallaro, J., Studer, C.: Large-scale MIMO detection for 3GPP LTE: algorithms and FPGA implementations. IEEE J. Sel. Top. Signal Process. **8**(5), 916–929 (2014)
17. Jiang, F., Li, C., Gong, Z., Su, R.: Stair matrix and its applications to massive MIMO uplink detection. Submitted to IEEE Trans. Commun. (2017, under review)
18. Jiang, F., Li, C., Gong, Z.: Block Gauss-Seidel method based detection in vehicle-to-infrastructure massive MIMO uplink. In: IEEE Proceedings of the GLOBECOM (2017)
19. Chen, S., Donoho, D., Saunders, M.: Atomic decomposition by basis pursuit. SIAM J. Sci. Comput. **20**(1), 33–61 (1998)
20. Tropp, J., Gilbert, A.: Signal recovery from random measurements via orthogonal matching pursuit. IEEE Trans. Inf. Theory **53**(12), 4655–4666 (2007)
21. Needell, D., Tropp, J.: CoSaMP: iterative signal recovery from incomplete and inaccurate samples. Appl. Comput. Harmon. Anal. **26**, 301–321 (2009)
22. Wang, J., Kwon, S., Shim, B.: Generalized orthogonal matching pursuit. IEEE Trans. Signal Process. **60**(12), 6202–6216 (2012)
23. Kwon, S., Wang, J., Shim, B.: Multipath matching pursuit. IEEE Trans. Inf. Theory **60**(5), 2986–3001 (2014)

24. Maleki, A., Donoho, D.: Optimally tuned iterative reconstruction algorithms for compressed sensing. IEEE J. Sel. Top. Signal Process. **4**(2), 330–341 (2010)
25. Blumensath, T., Davies, M.: Iterative hard thresholding for compressed sensing. Appl. Comput. Harmon. Anal. **27**(3), 265–274 (2009)
26. Bayati, M., Montanari, A.: The dynamics of message passing on dense graphs, with applications to compressed sensing. IEEE Trans. Inf. Theory **57**, 764–785 (2011)
27. Tang, C., Liu, C., Yuan, L., Xing, Z.: High precision low complexity matrix inversion based on Newton iteration for data detection in the massive MIMO. IEEE Commun. Lett. **20**(3), 490–493 (2016)
28. Dai, L., Gao, X., Su, X., Han, S., Wang, Z.: Low-complexity soft-output signal detection based on Gauss-Seidel method for uplink multiuser large-scale MIMO systems. IEEE Trans. Veh. Technol. **64**(10), 4839–4845 (2015)
29. Qin, X., Yan, Z., He, G.: A near-optimal detection scheme based on joint steepest descent and Jacobi method for uplink massive MIMO systems. IEEE Commun. Lett. **20**(2), 276–279 (2016)
30. Jiang, F., Li, C., Gong, Z.: A low complexity soft-output data detection scheme based on Jacobi method for massive MIMO uplink transmission. In: 2017 IEEE International Conference on Communication, pp. 1–5. IEEE Press, Paris (2017)

An Efficient Joint Tx-Rx Beam Search Scheme in mmWave Massive MIMO Systems (Invited Paper)

Liru Geng[1], Tiankui Zhang[1(✉)], Zhimin Zeng[1], and Xiao Han[2]

[1] Beijing Laboratory of Advanced Information Networks,
Beijing Key Laboratory of Network System Architecture and Convergence,
Beijing University of Posts and Telecommunications, Beijing, China
{genglr,zhangtiankui,zengzm}@bupt.edu.cn
[2] Network Technology Research Institution,
China United Network Communication Corporation Ltd., Beijing, China
hanxiao91@chinaunicom.cn

Abstract. This paper addresses the beam search complexity for massive multiple-input multiple-output (MIMO) in millimeter Wave (mmWave) band. In the mmWave massive MIMO systems, high-directional beams are used to against the severe path loss. However, it is faced with many challenges. One of them is that the beam search complexity and management overhead problems hinder the practical implement with a large number of antennas. To cope with the problem, an efficient joint transmit and receive (Tx-Rx) beam search scheme is proposed in this paper. In the initialization phase, the initial Tx-Rx beam pair is calculated by the coarse beam sweeping. Then, Rosenbrock algorithm is used to search the optimal beam pair in a two dimensional discrete space formed by the indexes of transmit beam and receive beam. In addition, double beam link is used to solve the link failure caused by channel block. Numerical simulation results are given to verify the effectiveness of the proposed scheme. Compared with the traditional beam search schemes, the proposed scheme can greatly reduce the search complexity and management overhead.

Keywords: Beam search · Rosenbrock algorithm · mmWave Massive MIMO · Beamforming · 5G

1 Introduction

To meet the high user data rate and high spectrum efficiency in the future wireless mobile communication, mmWave (millimeter-wave) band attracts attention

This paper is supported by the National Science and Technology Major Project (No. 2016ZX03001009-003). This paper is supported by the 111 project (No. B17007), and Director Funds of Beijing Key Laboratory of Network System Architecture and Convergence (2017BKL-NSAC-ZJ-07).

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 64–74, 2018.
https://doi.org/10.1007/978-3-319-90802-1_6

of the academia. However it suffers a serious attenuation caused by atmosphere. In order to against the path loss and improve the quality of link transmission, beamforming technology is used to provide high antenna gain and reduce inter-user interference by conducting directional transmission in the massive MIMO (multiple-input multiple-output) systems [1,2]. MIMO systems equipped with a large number of antennas and working at the mmWave band are called mmWave massive MIMO systems.

In the mmWave massive MIMO systems, beamforming enhances transmission signal to noise ratio (SNR) by making BS and UE aligned. However, when the number of antennas at the BS is large and beam width is very narrow, it faces many new challenges [2]. The first one is the coverage of the broadcast channel, which needs to make trade-offs of beam width, transmitting power and coverage range [3]. Secondly, beam management consisting beam searching, beam reporting, beam switching is necessarily to be studied. For beam searching, it requires a fast and accurate search scheme to find out the transmit and receive (Tx-Rx) beam pair which meets the transmission requirements in numerous beams with affordable signaling overhead [2]. Then the beam reporting stage is start, the optimal beam or beam group indexes and other related information are feedback from UE to BS [2]. Besides that, since the width of high directional beam is very narrow, a slight movement of UE will make the transmission beam pair mismatches, especially in a high mobility environment, the beam switching should be considered [4].

In the codebook based MIMO systems, codebooks are pre-defined. Beam search aims to select the optimal transmit and receive codebooks, corresponding to the optimal beam pair. A simple idea is the exhaustive search mechanism, but the significant protocol overhead and the computational complexity make it unfeasible. To deal with the problem, a classic scheme named two-stage search was proposed in IEEE 802 series standard draft [5]. The basic idea is firstly conducting the sector-level search, consisting of sweeping low-resolution codebooks (corresponding to coarse beams) and choosing the optimal one. The second stage is beam refinement determining the optimal high resolution codebook (corresponding to the fine beam) in the selected sector. It reduces the search overhead to a certain extent. But in case of a large codebook, the overhead is costly and its impracticable for massive MIMO systems.

Meanwhile, some researchers had proposed some beam search schemes to reduce the management overhead [6–8]. In [6], an unconstrained direct search method namely Rosenbrock algorithm was used to select the optimal beam pair at 60 GHz band, but it needs a pre-search process to iteratively discover the initial value. In [7], two factors making link failure, UE mobility and human block, were simply modeled. The former needs to search beams around the current beam pair to find another suitable one. The latter needs to switch an alternative link. However, the model is linear and independent of the moving speed, which may result in inaccurate application. A multi-device multi-path beamforming training method was proposed in [8]. It reduces the overall overhead of the system, but status of multi-device is the same and the optimization goal is not global.

To address the excessive searching overhead and computational complexity, an efficient joint Tx-Rx beam search scheme is proposed in this paper. In the initial phase, the initial search value is simply calculated by the optimal coarse beam pair obtained by the sweeping process to against the multipath effect and to avoid search failure due to the local optimum. Rosenbrock algorithm is used to search the optimal beam pair in a two dimensional discrete space formed by the indexes of Tx-Rx beams. The search process can be conducted at one side, so the search process can be performed at BS side. This can reduce the information exchanged between UE and BS, thus reducing management overhead and the implementation complexity at UE side. At the same time, double beam link can be performed to select several suitable beam pairs to against channel blockage and user interference. The simulation results show that, compared with the exhaustive search and two-stage search scheme, the proposed scheme can significantly reduce the beam search times.

The rest of this paper is organized as follows. The system model is presented in Sect. 2. The Joint Tx-Rx beam search scheme is proposed and described in Sect. 3. Simulation evaluations are shown in Sect. 4. Conclusions are drawn in Sect. 5.

2 System Model

In the mmWave massive MIMO systems, to reduce transmitting power and hardware complexity, the hybrid transceiver structure is adopted, as shown in Fig. 1. In the case of DL (downlink), the data stream is firstly digitally precoded, then processed by IFFT (Inverse Fast Fourier Transform), PSC (Parallel Serial Converter), ADC (Analog-to-Digital Conversion), etc. And then the PS (Phase Shifter) adjusts weights to generate a Tx beam at BS side. UE receives the signal with an Rx beam and processes it reversely.

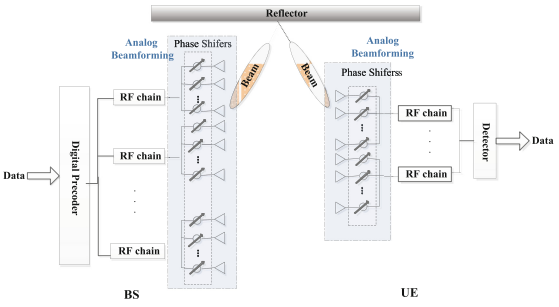


Fig. 1. System model

2.1 Antenna Model

Assume the antenna model is isotropic radiate and it has spherical radiation pattern and equal antenna gain for all spatial directions [9]. In order to simplify the channel model and consider the basic characteristics of the real antennas, assume that all beams are arranged in order and cover the entire communication space. And the optimal beam pair in this paper maximizes the received SNR.

With a large number of antennas, the beam can be equivalent to the basic directional beam. Assuming a 2D antenna model (which can be scalable to 3D), the main lobe gain can be expressed by the Gaussian attenuation function, and side lobe gain is a constant, which can be expressed,

$$G(\theta) = \begin{cases} G_0 \exp(-\alpha\theta^2), \theta < \frac{\theta_{ML}}{2} \\ G_C, else \end{cases} \tag{1}$$

where θ is the azimuth angle in the range $[-\pi, \pi]$, G_0 is the maximum antenna gain, G_C is the side lobe gain, θ_{ML} is the width of main lobe $\theta_{ML} \approx 2.6\theta_{-3\text{dB}}$ which is only depended to the half power beam width $\theta_{-3\text{dB}}$. The parameter α is a constant and can be calculated by $\theta_{-3\text{dB}}$, because $\frac{G}{G_0} = \exp(-\alpha(\frac{\theta_{-3\text{dB}}}{2})^2) = \frac{1}{2}$. Hence $\alpha = \frac{4\ln(2)}{\theta^2_{-3\text{dB}}}$. In decibel scale, the beam gain can be rewritten as follows,

$$G_{dB}(\theta) = \begin{cases} G_{0,dB} - 12(\frac{\theta}{\theta_{-3\text{dB}}})^2, \theta < \frac{\theta_{ML}}{2} \\ G_{C,dB}, else \end{cases}. \tag{2}$$

2.2 Path Loss

Unlike the widely used cellular low frequency band, mmWave band is greatly influenced by the atmosphere. There are little scatters in the environment, the penetration loss is high and the reflection effect is obvious. These features directly influence the channel characteristics. The path loss is the ratio of the receive signal power to the transmit signal power. It not only depends on the distance from UE to BS but also on the frequency. Thus the path loss is especially serious in the millimeter band. The mean of path loss can be expressed as follows [9],

$$PL(d) = PL_0 + n \cdot 10log(\frac{d}{d_0}) \tag{3}$$

where d is the distance from UE to BS, d_0 is the reference distance, PL_0 is the path loss at the reference distance, n is the path loss exponent.

2.3 Received SNR

Codebooks, corresponding to the beams, are pre-defined in the codebook based MIMO systems. In the two dimensional discrete space formed by the indexes of Tx and Rx beam, the received SNR, represented by γ, can be simplified so that it is dependent on the transmit and receive codebooks (p, q),

$$\gamma(p, q) = P_t + G_t(p) + G_r(q) - PL - N \tag{4}$$

where P_t, G_t, G_r are the transmitting power, the Tx beam gain and Rx beam gain. N is the mean noise power.

3 Scheme Design

In order to reduce the computational complexity and management overhead caused by beam search, we propose an efficient joint Tx-Rx beam search scheme. The beam search scheme aims to find out the optimal beam pair resulting in the largest received SNR. The maximum optimal objective function is written as follows,

$$\begin{aligned} &\max_{(p,q)} \gamma(p,q) \\ &s.t.(p,q) \in R^2 \end{aligned} \tag{5}$$

where R^2 is the two dimensional discrete integer space formed by the Tx and Rx beam indexes.

Owing to the antenna array placement, complex wireless transmission environment, beam sidelobes and other reasons, the analytic formula of the objective function does not exist. Even if it is an unconstrained numeric optimization problem [6], the gradient of the analytical formula cannot be calculated. This means the efficient gradient descent algorithm cannot be used. Therefore, we propose an efficient direct search method - Rosenbrock algorithm. It can control the search direction by calculating the value of the objective function, find the peak direction and find out the optimal beam pair efficiently. As shown in Fig. 2, the global optimum value is at the peak.

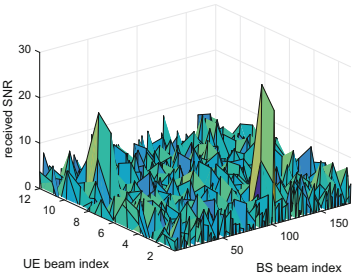


Fig. 2. Optimization objective function

Since Rosenbrock algorithm is essentially greedy, it is easy to fall into the local optimum, may resulting in an inaccuracy search. Therefore, it is necessary to set a suitable initial value. Once UE firstly discovers a cell or the communication link fails completely, it is necessary to conduct the synchronization and random access procedures. For the control signal transmission such as the synchronization signal and the broadcast channel, the coarse beams are swept to obtain the optimal beam pair. Thus, it is feasible to calculate the initial search value by the optimal coarse beam.

In fact, there are many reasons for beam failure, such as UE movement, UE rotation and obstacle block [10]. The best way to deal with the above cases is different. Due to the beam pair is misaligned, the first two cases need to search the re-aligned beam pair. In the last case, beams are aligned still but the link is blocked. The solution is switching the alternate communication link. Therefore, it is essential to find the optimal and suboptimal transmission beam pair in the initial access stage. As a result, it is necessary to search for an alternate beam pair and double beam link method can reduce the probability of transmission link failure. In this paper, the optimal beam pair is used to transmission and the sub-optimal beam pair is considered as an alternative one.

3.1 Scheme Procedure

Beam search process is shown in Fig. 3. Firstly, coarse beams are scanned. BS broadcasts the reference signal to UE using different transmit beams and UE receives the pilot separately using different receiving beams. Then the best two beam pairs are detected among the candidate ones and reported to BS. Then the center fine beams are positioned from the selected coarse beams and set as the initial values to the Rosenbrock algorithm respectively. Define all fine beams converging coarse beam are candidate beams and start search process. Finally select and switch the beam pair with the largest received SNR, store the suboptimal one as alternative link.

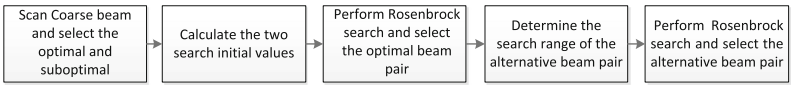


Fig. 3. Procedure of the joint Tx-Rx beam search scheme

The details of the Rosenbrock algorithm, the initial value setting and the double beam link are described below.

3.2 Rosenbrock Algorithm

The Rosenbrock algorithm consists of two procedures: pattern probing and pattern moving. The former aims to find the direction in which objective function increases. The latter construct new orthogonal directions.

At the pattern probing stage, set the center high resolution beam pair corresponding to the low resolution optimal one to the initial point $x(0) = (p^{(1)}, q^{(1)})$, the magnification factor $\mu > 1$, the shrink factor $0 < \nu < 1$, the initial search direction $d^{(1)} = (1, 0)^T$, $d^{(2)} = (0, 1)^T$, the initial steps (ξ_1, ξ_2). Assuming the first probing direction is $d^{(1)}$, make $y^{(1)} = x(0)$, and calculate $f(y^{(1)} + \xi_1 d^{(1)})$. If it is more than $f(y^{(1)})$, make $y^{(2)} = y^{(1)} + \xi_1 d^{(1)}$, $\xi_1 = \mu \cdot \xi_1$. If it is less than $f(y^{(1)})$, make $y^{(2)} = y^{(1)}$, $\xi_1 = \nu \cdot \xi_1$. Next, let $y^{(2)}$ an origin point and probing along $d^{(2)}$. Process it the same as above, then we get $y^{(3)}$. Two orthogonal

directions are completed and let $y^{(n)} = y^{(3)}$. A probing round is finished and the next round starts from the initial point $y^{(1)} = y^{(n)}$. After several rounds of probing, pattern probing finished until both directions fail. Then the last point is $x(k) = y^{(n+1)}$.

Then start pattern moving stage and construct new search directions. The increase direction of objective function can be expressed,

$$x(k) - x(k-1) = \sum_{i=1}^{n} \lambda_i d_i \tag{6}$$

where d_i is the ith orthogonal direction, λ_i is the distance moving along ith direction. Note $P = x(k) - x(k-1)$ and the next pattern probing should refer to the increase direction. Define $P^{(1)}, P^{(2)}, \cdots, P^{(n)}$ which satisfy,

$$P^{(j)} = \begin{cases} d_j, if \lambda_j \\ \sum\limits_{i=j}^{n} \lambda_j d_j, if \lambda_j \neq 0 \end{cases} \tag{7}$$

Since the search directions are orthogonal, Schmidt orthogonalization is introduced. Thus we can get,

$$Q^{(j)} = \begin{cases} P^{(j)}, if\ j = 1 \\ P^{(j)} - \sum\limits_{i=1}^{j-1} \frac{Q^{(i)T} P^{(j)}}{Q^{(i)T} Q^{(i)}}, if\ j > 1 \end{cases} \tag{8}$$

Normalize it.

$$\overline{d}^{(j)} = \frac{Q^{(j)}}{\left\| Q^{(j)} \right\|}. \tag{9}$$

Therefore the new probing directions are constructed.

Two stages above process alternately till finding out the maximum point of optimization function.

3.3 Initial Value Setting

Assume the arrangement and numbering order of the two-level beams are the same, all the fine beams covering each coarse beam can be determined. The total numbers of coarse beams and fine beams are respectively M, $N (M < N)$. If the target coarse beam index is p_c, the indexes of in its coverage ranges $\left[(p_w - 1) \cdot \frac{N}{M} + 1, p_w \cdot \frac{N}{M}\right]$, and the index of the center fine beam is as follows,

$$p_f = floor[(p_w - \frac{1}{2}) \cdot \frac{N}{M} + \frac{1}{2}] \tag{10}$$

where, $floor(\bullet)$ is the ceiling function. The index of the center fine beam corresponding to optimal coarse beam is set to the initial value of the Rosenbrock algorithm. Then it is easy to find the peak of the objective function.

3.4 Double Beam Link

Actually, it is unreliable to identify the reasons for the decline of link quality only by the reduction of SNR. When the link quality is degraded, the performance of the alternative beam pair is estimated. If the communication requirement can be met, directly switch the alternative beam pair and beam search process is not required immediately. If the link quality is still poor, start to search beams.

The alternative beam pair search is described below. Firstly, sweep the coarse beam and select the optimal as well as suboptimal coarse beam pair. Then find indexes of the corresponding center fine beams. The indexes of the optimal ones are set as the initial value of Rosenbrock algorithm and find out the optimal fine beam. Next conduct the alternate beam pair search. Set the fine beam indexes corresponding to the sub-optimal coarse beam pair as the initial value and remove the beams covered by the optimal coarse beam pair from search range. Then find out the suboptimal beam pair and store it as an alternative one.

One round of Rosenbrock search process can find out the best two beam pairs in fact, but in this paper we conduct two search processes to find the transmission and the alternative beam link. Because it is extremely possible that the suboptimal beam pair is the nearby beam of the optimal beam pair, not the reflection beam pair. Therefore delimiting the search again at the second search phase is necessary.

4 Performance Evaluation

Numerical simulations and analysis are conducted to verify the effectiveness of the joint Tx-Rx beam search scheme (abbreviated by JS). The comparison schemes are the exhaustive search mechanism (abbreviated by ES) and the two-stage search mechanism (abbreviated by TS). Simulation parameters are shown as Tables 1 and 2.

Table 1. System simulation parameters

Parameters	Value	Parameters	Value
Simulation area	80 m * 60 m	d_0	10 m
BS location	(40 m, 30 m)	PL_0	82.02 dB
Carrier frequency	28 GHz	n	2.36
Low beam resolution at UE	90°	P_t	30 dBm
Low beam resolution at BS	30°	N	−35 dBm

Firstly, the accuracy of the joint Tx-Rx beam search scheme is evaluated. In the simulation, assume the high beam resolution of UE is a constant 30° and the high beam resolution of BS is set as the variable. Only finding out one pair of

Table 2. Rosenbrock algorithm simulation parameters

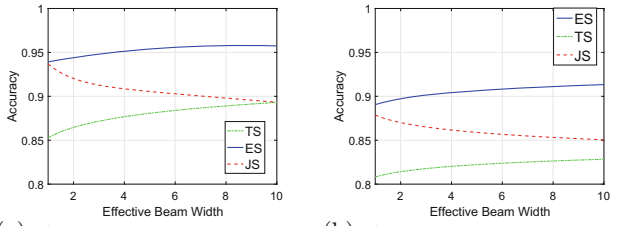
Parameters	Value
Magnification factor μ	2
Shrink factor ν	-0.5
Initial search direction	$d^{(1)}$, $d^{(2)}$
Initial search step	$\xi_1 = \xi_2 = 1$

beams i.e., the optimal beam pair, consider it successful when the search result is the same as the optimal beam pair. Searching for two pairs of beams i.e., the optimal and suboptimal beam pair, regard it as a success once the selected indexes of the two beam pairs are matched. Simulation drop of independent beam search is 10000. Calculate the success frequency to approximately estimate the accuracy, i.e., $accuracy = \frac{drops_{successful}}{drops_{total}}$, where $drops_{total}$ is the total simulation drop, $drops_{successful}$ is the successful simulation drop.

Simulation result of the proposed scheme and the comparison schemes is shown as Fig. 4 where the scale of the x-axis is the effective beam width. (a) is the accuracy result of searching one beam pair and (b) is that of two beam pairs. It can be seen that among the three schemes from figure (a), the accuracy of ES is the highest and more than 0.9, JS is the second and TS is the worst. The ES scheme traverses all beam pairs thus can easily find out the optimal beam pair. The JS scheme is a two dimensional joint search method, while the TS scheme separately considers BS and UE side. Obviously the former is more efficient and accurate. In addition, when the beam resolution is higher (the effective beam width is smaller), the performance of JS scheme improves more than that of the TS method. When the resolution gets lower, its advantage reduces. This proves that in the high beam resolution and quantities beam cases, the JS scheme is more efficient and accurate. Seen from figure (b), in case of searching the optimal and alternate beam pairs, the accuracy difference between the JS scheme and the ES scheme is much smaller than that in the case of searching for one beam pair, and difference between the TS scheme is slightly increased. That proves the JS scheme has advantages when double beam link mechanism is used.

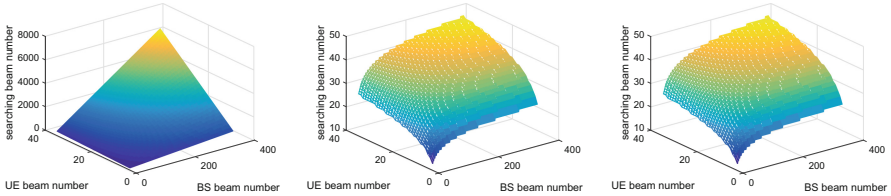
Next the complexity of the three search schemes is evaluated. The variables are the numbers of Tx and Rx beams. In the successful case, the mean number of the searched beams is simulated. Evaluation of the JS scheme complexity is still compared with the ES and the TS scheme.

Figure 5(a)–(c) are the searched beam numbers of the ES, the TS and proposed scheme respectively. It can be seen that the search number of the ES scheme is the largest, the TS scheme is the second and the proposed scheme is the least. Since the ES scheme needs to traverse all beam pairs to select the best beam pair, it maximizes the search number. The TS scheme is the deformation of the first one. Compared with ES scheme, the search time will reduce an order of magnitude. But when the beam number is massive, search overhead will still be considerable. In comparison with the TS scheme, the search number



(a) Accuracy of searching one beam pair. (b) Accuracy of searching two beam pairs.

Fig. 4. Accuracy of the joint Tx-Rx search scheme in comparison of the exhaustive search and two-stage search.



(a) ES scheme. (b) TS scheme. (c) JTRBS scheme.

Fig. 5. Search times of the joint Tx-Rx search scheme in comparison of the exhaustive search and two-stage search

of the proposed scheme can be reduced an order of magnitude. In addition, the search number of the first two schemes increases rapidly when the number of beams becomes very large. While that of the proposed scheme increase still, the growth rate is significantly slower. The results prove that the proposed scheme has a great advantage of reducing the computational complexity and management overhead of beam search in the mmWave massive MIMO systems.

5 Conclusion

An efficient joint Tx-Rx beam search scheme was proposed in the mmWave massive MIMO systems. An unconstrained optimization method, Rosenbrock algorithm is used to conduct joint Tx-Rx beam search in a two dimensional space. The optimal coarse beam pair obtained in the initial access is calculated as the initial value to approach the peak of objective function. So it can reduce the search time while ensuring the accuracy which is advantageous in reducing the management overhead. The conduct of the beam search process at the BS side can reduce the computational complexity of the UE. To against channel blockage the double beam link search process was used in the proposed scheme, enhancing the robustness of the system.

References

1. Gupta, A., Jha, R.K.: A survey of 5G network: architecture and emerging technologies. IEEE Access **3**, 1206–1232 (2015)
2. Guo, R., Lin, E., Zen, R., Kuo, R.: On beam-based access technology for 5G. IEEE Wirel. Commun. **23**(5), 2–3 (2016)
3. Jeong, C., Park, J., Yu, H.: Random access in millimeter-wave beamforming cellular networks: issues and approaches. IEEE Commun. Mag. **53**(1), 180–185 (2015)
4. Sung, N.W., Choi, Y.S.: Fast intra-beam switching scheme using common contention channels in millimeter-wave based cellular systems. In: 2016 18th International Conference on Advanced Communication Technology (ICACT), Pyeongchang, pp. 760–765 (2016)
5. IEEE Standard for Information Technology – Local and metropolitan area networks – Specific requirements – Part 15.3: Amendment 2: Millimeter-Wave-Based Alternative Physical Layer Extension. In: IEEE Std 802.15.3c-2009 (Amendment to IEEE Std 802.15.3-2003), pp. 1–200, 12 October 2009
6. Li, B., Zhou, Z., Zou, W., Sun, X., Du, G.: On the efficient beam-forming training for 60 GHz wireless personal area networks. IEEE Trans. Wirel. Commun. **12**(2), 504–515 (2013)
7. Gao, B., Xiao, Z., Zhang, C., Su, L., Jin, D., Zeng, L.: Double-link beam tracking against human blockage and device mobility for 60-GHz WLAN. In: IEEE Wireless Communications and Networking Conference (WCNC), Istanbul, pp. 323–328 (2014)
8. Gao, B., Xiao, Z., Su, L., Chen, Z., Jin, D., Zeng, L.: Multi-device multi-path beamforming training for 60-GHz millimeter-wave communications. In: 2015 IEEE International Conference on Communications (ICC), London, pp. 1328–1333 (2015)
9. Maltsev, A., Pudeyev, A., Bolotin, I., et al.: MiWEBA D5.1: channel modeling and characterization. Technical report (2014)
10. Shim, D.S., Yang, C.K., Kim, J.H., Han, J.P., Cho, Y.S.: Application of motion sensors for beam-tracking of mobile stations in mmWave communication systems. Sensors **14**(10), 19622–19638 (2014)

A Low-Complexity Discrete Gbest-guided Artificial Bee Colony Algorithm for Massive MIMO Detection

Boyang Zou(✉), Weixiao Meng, Lin Li, and Shuai Han

Communications Research Center, Harbin Institute of Technology, Harbin, China
16S005051@stu.hit.edu.cn, wxmeng@hit.edu.cn

Abstract. Massive multi-input multi-output (MIMO) technology is one of the most promising concepts in 5G wireless system. Grounded on the fact that the channel matrix in massive MIMO system is large dimensional, classical MIMO detection algorithms are not appropriate for large scaled antennas. In this paper, a low-complexity discrete gbest-guided artificial bee colony (DGABC) detection algorithm is proposed for massive MIMO uplink, chaotic maps for parameter adaptation is also proposed in order to improve the convergence characteristic of the DGABC algorithm and to prevent the algorithm from getting stuck in local solutions. Experiments show that the proposed DGABC detection algorithm outperforms both the original ABC algorithm and MMSE detection with a relatively low complexity.

Keywords: Massive multiple input multiple output (MIMO) system
Discrete gbest-guided artificial bee colony (DGABC)
Computational complexity · Detection algorithm · Chaotic maps

1 Introduction

Massive MIMO has been a key technology in wireless communication systems with much more antennas at both sides. While many traditional problems have been solved by massive MIMO benefitting from its advantageous properties of increased diversity, there are still some technical problems existing to be explored, one of which is the computational complexity of uplink symbol detection at the base station with large scaled antennas [1].

As antennas increase to a large amount, traditional detection algorithms for MIMO have poor bit error rate (BER) performance and high computational complexity. It is not appropriate for traditional algorithms to be applied directly in the massive MIMO system. Therefore, it is necessary to improve the massive

This work is supported by National Natural Science Foundation of China (61471143) and the Provincial Natural Science Foundation of Heilongjiang, China (No. ZD2-017013).

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 75–84, 2018.
https://doi.org/10.1007/978-3-319-90802-1_7

MIMO detection algorithm for optimum BER performance and low computational complexity. Karaboga proposed the artificial bee colony (ABC) algorithm firstly for numerical optimization problem [2], and it was applied for massive MIMO detection by Li [3]. In this paper, to reduce the computational complexity, we propose a novel initialization approach for DGABC algorithm by virtue of the prior information of matched filter in MMSE. Chaotic maps for parameter adaptation is also employed to improve the convergence characteristic of the algorithm. The proposed algorithm reduces the computational complexity apparently while achieving a near-optimal BER performance compared to the original ABC detection algorithm in [3].

The remainder of this paper is organized as follows. Section 2 describes system model of the massive MIMO uplink as well as some classical massive MIMO detection algorithms. The proposed low-complexity DGABC algorithm is presented in Sect. 3. We present the simulation of the low-complexity DGABC detection algorithm and analysis its computational complexity and BER performance in Sect. 4. Finally, the conclusion is given in Sect. 5.

Notation: Lowercase boldface letter is used to indicate a vector and uppercase boldface letter to indicate a matrix; superscript $(\cdot)^{-1}$ denotes matrix inversion, $(\cdot)^T$ and $(\cdot)^H$ denote transpose and complex conjugate transpose, $\|\cdot\|$ denotes two-norm, statistical expectation is denoted as $E\{\cdot\}$, $\Re(\cdot)$ indicates the real part of a complex number, $\Im(\cdot)$ indicates the imaginary part, $\mathbb{C}$ and $\mathbb{R}$, respectively, denotes the field of complex numbers and field of real numbers.

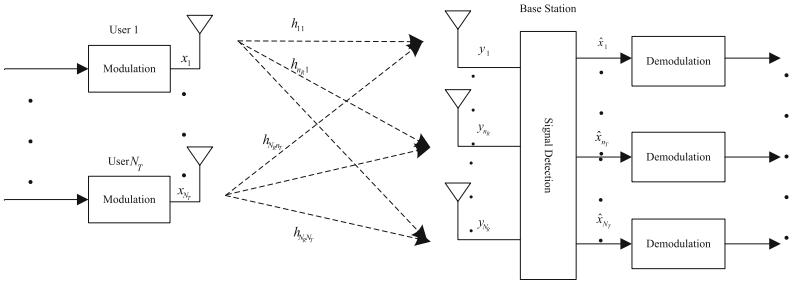


Fig. 1. System model of massive MIMO uplink

2 System Model of Massive MIMO Uplink

2.1 System Model

We consider a massive MIMO uplink consisted of N_T cells with single transmitting antenna and one BS with N_R receiving antennas ($N_R \geq N_T$). At the transmitter, the bit stream generated by users are modulated to transmitted symbols [4]. Modulation alphabet is donated as $\mathbb{S}$, and $\mathbb{R}$ denotes the real part

of Modulation alphabet $\mathbb{S}$ as in (1), and M-QAM is adopted. The perfect channel state information is known by the receiver throughput the paper.

$$\mathbb{S} = \mathbb{R} + j\mathbb{R}, \mathbb{R} \in [\pm 1, \pm 3, \cdots, \pm\sqrt{M} - 1]. \tag{1}$$

According to [5], the signal propagation process can be expressed as in (2)

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}. \tag{2}$$

For a clarity illustration, real-valued system model is adopted in this paper. Vector $\mathbf{y}$ is an $2N_R \times 1$ dimensional real received signal vector, $\mathbf{H}$ is an $2N_R \times 2N_T$ dimensional real Rayleigh fading channel matrix, $\mathbf{x}$ is an $2N_T \times 1$ dimensional transmitted real vector, and $\mathbf{n}$ is an $2N_R \times 1$ dimensional, independent zero-mean additive white Gaussian noise vector and $E\{\mathbf{n}\mathbf{n}^H\} = \sigma^2\mathbf{I}_{2N_R}$, where $\sigma^2 \in \mathbb{R}$ denotes the average noise variance per receiving antenna. The system model is as shown in Fig. 1.

2.2 Classical Detection Algorithms

Maximum Likelihood (ML) detection algorithm can obtain the optimum BER performance for MIMO [6].

$$\hat{\mathbf{x}}_{\mathrm{ML}} = \arg \min_{\mathrm{x} \in \mathbb{S}} \|\mathbf{y} - \mathbf{H}\mathbf{x}\|^2. \tag{3}$$

The complexity of ML detection algorithm is exponential in an order of magnitude of $\mathrm{O}(M^{N_T})$, which is extremely high in the case of scaled number of antennas [6]. The hardware implementation of ML is a most critical issue in the BS side.

Minimum mean square error (MMSE) decoder is a widely used linear detection algorithm. The matched-filter output is computed firstly as $\mathbf{y}^{\mathrm{MF}} = \mathbf{H}^H\mathbf{y}$, and the estimated transmitted symbol $\hat{\mathbf{x}}_{\mathrm{MMSE}}$ is achieved as in (4).

$$\hat{\mathbf{x}}_{\mathrm{MMSE}} = \mathbf{A}^{-1}\mathbf{y}^{MF}. \tag{4}$$

The detection results are obtained with hard decision. The computational complexity of MMSE is in an order of magnitude of $\mathrm{O}(N_T^3)$, which is much lower than that of the ML algorithm. However, the BER performance of MMSE is rather poorer compared with ML algorithm. Research on improvement of BER performance of MMSE detection has been extremely attractive.

3 Low-Complexity DGABC Detection Algorithm for Massive MIMO System

The process of searching the optimum solution vector in ML algorithm can be formalized as a nonlinear integer programming problem [7]. The ABC detection algorithm is applied in the process of bees foraging for food and obtains an

approximately optimum BER performance [3]. However, per-symbol complexity of the ABC algorithm is still as an order of $O(N_T^2)$. In this paper, a proposed low-complexity DGABC algorithm with a novel initialization and chaotic maps is proposed to reduce the computational complexity with a near-optimum performance.

3.1 ABC Optimization

The ABC algorithm is a heuristic random search algorithm deriving from the Swarm intelligence Optimization. In the ABC algorithm, each feasible solution to the problem is represented by a food source, and the nectar quality of the food source corresponds to the fitness of this feasible solution, which reflects the quality of this solution. The detailed process is introduced in [2].

In [7], discrete gbest-guided ABC (DGABC) detection algorithm was presented to solve the global service composition problem. In this paper, a proposed low-complexity DGABC detection algorithm is applied for massive MIMO detection, which can be recognized as an interger programming problem.

3.2 Proposed Low-Complexity DGABC Algorithm for Massive MIMO System

The solution vector $\hat{\mathrm{x}}$ is calculated as (5) from (2).

$$\hat{\mathbf{x}} = \arg \max_{\mathbf{x} \in \mathbb{S}} (2\mathbf{y}^H \mathbf{H} \hat{\mathbf{x}} - \hat{\mathbf{x}}^H \mathbf{H}^H \mathbf{H} \hat{\mathbf{x}}). \tag{5}$$

The cost function $f(\hat{\mathrm{x}})$ as in (6) is corresponding to the nectar amount in the ABC algorithm [3].

$$f(\hat{\mathbf{x}}) = \mathbf{2y^H H} \hat{\mathbf{x}} - \hat{\mathbf{x}}^{\mathbf{H}} \mathbf{H^H H} \hat{\mathbf{x}}. \tag{6}$$

The global optimum solution vector $\hat{\mathrm{x}}_{\mathrm{best}}$ is obtained until maximizing the cost function $f(\hat{x})$ as in (7).

$$\hat{\mathbf{x}}_{\mathrm{best}} = \arg \max_{\mathbf{x} \in \mathbb{S}} f(\mathbf{x}). \tag{7}$$

To speed up the convergence and obtain a better BER, hard decision result of MMSE is employed as the initial solution vector $\hat{\mathrm{x}}^{(0)} = \mathrm{x}_{\mathrm{MMSE}}$ in ABC detection algorithm [3]. However, the complexity of algorithm increases to $O({N_T}^3)$ resulting from the computation of MMSE. Instead, the algorithm proposed in this paper takes advantage of the properties of A^{-1} introduced in Sect. 2 that are applicable in massive MIMO [8]:

(i) A^{-1} is a diagonally dominant matrix.
(ii) All diagonal elements of A^{-1} are positive.

Deriving from the properties above, the sign of the ith element in $\hat{\mathbf{x}}$ is almost the same as that of the ith element in $\mathbf{y}^{MF}$. More precisely:

$$\begin{aligned} sign(\hat{\mathbf{x}}_{\mathrm{i}}^{(0)}) &= sign(\sum_{j=1}^{N} \mathrm{a'_{ij}} \mathbf{y}_{\mathrm{i}}{}^{MF}) \simeq sign(\mathrm{a'_{ij}} \mathbf{y}_{\mathrm{i}}{}^{MF}) \\ &= sign(\mathbf{y}_{\mathrm{i}}{}^{MF}). \end{aligned} \tag{8}$$

where $\hat{\mathbf{x}}_{\mathrm{i}}$ and $\mathbf{y}_{\mathrm{i}}{}^{MF}$ are the ith elements of $\hat{\mathbf{x}}$ and $\mathbf{y}^{MF}$ respectively, and a'_{ij} denotes the element of $\mathbf{A}^{-1}$ at the ith row and jth column, $j \in \{1, 2, \cdots 2N\}$. For example, if $sign(\hat{\mathbf{x}}_{\mathrm{i}}) = sign(\mathbf{y}_{\mathrm{i}}{}^{MF}) > 0$, the jth dimension of feasible initial solutions $\hat{x}_j^{(0)}$ is a positive value and generated from the positive part of real modulation alphabet as $[1, 3, \cdots \sqrt{M} - 1]$.

After initialization, the exploitation of all the SN feasible solutions will start. Let the maximum cycle number be $Maxiter$. The behaviors of employed bees, onlooker bees and scout bees are repeated in each cycle.

Algorithm 1. Low-complexity ABC detection algorithm

Require: $\mathbf{y}$,$\mathbf{H}$, σ^2, SN, $limit$,$Maxiter$
1: intialization of $\hat{\mathbf{x}}_{\mathrm{i}}^{(0)} (i = 1, 2, \cdots, SN)$.
2: **for** $i = 0$ to $Maxiter$ **do**
3: **for** $d = 0$ to SN **do**
4: $v_d^i \leftarrow \hat{x}_d^i + \lfloor \phi_d^i \times (\hat{x}_d^i - \hat{x}_e^i) \rfloor + \lfloor \varphi_d^i \times ({x_{best}}^i - \hat{x}_d^i) \rfloor$
5: **if** $f(\mathbf{v}_d) > f(\hat{\mathbf{x}}_d)$ **then**
6: $\hat{\mathbf{x}}_d \leftarrow \mathbf{v}_d, f(\hat{x}_d) \leftarrow f(v_d)$
7: **end if**
8: **end for**
9: **for** $f = 0$ to SN **do**
10: The fth onlooker bee selects jth food source through the wheel selection method.
11: $v_f^i \leftarrow \hat{x}_j^i + \lfloor \phi_f^i \times (\hat{x}_j^i - \hat{x}_e^i) \rfloor + \lfloor \varphi_f^i \times ({x_{best}}^i - \hat{x}_f^i) \rfloor$
12: **if** $f(\mathbf{v}_f) > f(\hat{\mathbf{x}}_j)$ **then**
13: $\hat{\mathbf{x}}_j \leftarrow \mathbf{v}_f, f(\hat{x}_j) \leftarrow f(v_f)$
14: **end if**
15: **end for**
16: **if** the kth solution ($k = 1, 2, \cdots, SN$) is not updated after $limit$ iterations **then**
17: $x_k^i \leftarrow lb + \lfloor rand(0, 1) \times (ub - lb) \rfloor$
18: **end if**
19: **end for**
20: update $Fitness\_best$ and x_{best} so far
Ensure: $\hat{\mathbf{x}}_{\mathrm{best}}$

Employed Bees Phase. There is one employed bee assigned to each food source. At the beginning of each cycle, the dth food source, of which the corresponding employed bee exploits the neighborhood, is denoted as X_d, where $X_d \in \mathbb{R}^{2N_T \times 1}$, $d \in \{1, 2, \cdots, SN\}$. The local search method is described as in (9)

$$v_d^i = \hat{x}_d^i + \left\lfloor \phi_d^i \times (\hat{x}_d^i - \hat{x}_e^i) \right\rfloor + \left\lfloor \varphi_d^i \times ({x_{best}}^i - \hat{x}_d^i) \right\rfloor . \tag{9}$$

The parameters i and e in (9) are generated randomly as in (10) and (11)

$$i = 1 + \lfloor rand(0,1) \times 2N_T \rfloor , \tag{10}$$

$$e = 1 + \lfloor rand(0,1) \times SN \rfloor . \tag{11}$$

The current global optimal composition solution is denoted as x_{best}, where $x_{best} \in \mathbb{R}^{N\times 1}$, and ${x_{best}}^i$ represents the ith element of x_{best}. To escape the local optimum, chaotic map is employed in the proposed algorithm to generate the factor ϕ_d^i and φ_d^i instead of stochastic sequence, while the initial value of the sequence c_0 is generated randomly in $(0, 1)$. The ϕ_d^i and φ_d^i are generated as in (12) and (13), and the c_k is updated as in (15) after each generation of ϕ and φ. Tent map is selected from the chaotic maps for its superior characteristics of convergence

$$\phi_n = 2c_k - 1, \tag{12}$$

$$\varphi_n = 2c_k, \tag{13}$$

$$c_{k+1} = \begin{cases} c_k/0.7 & c_k < 0.7, \\ 10(1-c_k)/3c_k & otherwise. \end{cases} \tag{14}$$

The rounding down operation $\lfloor \rfloor$ is introduced considering that each element of the v_d^i is an integer. The bound value will be assigned to v_d^i in case it is out of the bound $\lfloor lb, ub \rfloor$, where v_d denotes the location of the new food source attached to dth employed bee. The fitness value $f(v_d^i)$ of the new food source v_d^i will be calculated by cost function as in (6) after it is generated. If the fitness value of the new solution is higher, the original one will be replaced. After the search of the employed bees is finished, new population is updated.

Onlooker Bees Phase. The heuristic factor matrix is denoted as η in (15), which is an $2N_T \times 1$ real vector, each entry η_n of it is a real number reflecting the quality of the nth solution. The calculation of η_n is given in (15).

$$\eta_n = 1/f(\hat{x}_n). \tag{15}$$

The employed bees return to the hive and deliver the pheromone to the onlooker bees. The onlooker bee select the nth solution vector based on the selecting probability denoted as $p(n)$ in (16).

$$p(n) = \frac{\eta_n}{\sum\limits_{j=1}^{SN} \eta_j}. \tag{16}$$

The fth onlooker bee attaches itself to one nectar by Debs method based on selecting probability and exploit its neighborhood. Apparently, the food source with higher fitness value will attract more onlooker bees. The procedure of the exploitation is identical to (9), and the food source position is updated as the process of updating in the scout bees phase.

Scout Bees Phase. If the kth solution ($k = 1, 2, \cdots, SN$) is not updated after *limit* iterations, the attached employed bee will abandon the solution and become a scout bee to sought new nectar randomly through (17).

$$x_k^i = lb + \lfloor rand(0,1) \times (ub - lb) \rfloor . \tag{17}$$

The bound value will be assigned to x_k^i if it is out of the $\lfloor lb, ub \rfloor$. When the whole exploration is finished, the largest fitness value achieved so far is denoted as $Fitness\_best$ and its corresponding nectar position is denoted as x_{best}. Both $Fitness\_best$ and x_{best} will be updated.

The whole iteration will be repeated until the end condition is fulfilled. The global optimum solution vector $\hat{\mathbf{x}}_{\text{best}}$ is obtained and is remapped to the complex domain as the final detection result. The pseudo code of the proposed low-complexity DGABC detection algorithm is as shown in Algorithm 1.

4 Simulation and Numerical Result

In this section, the simulation of computational complexity and BER are stated to illustrate the performance of the low-complexity DGABC algorithm. For comparsions, ML detection, MMSE detection and original ABC detection in [3] are in consideration. The proposed algorithm is simulation in both 64×64 and 128×128 massive MIMO system. The transmitted signals are modulated by 16-QAM. Each antenna transmit 200000 symbols simultaneously.

We denote the average received SNR (dB) per received antenna as $\text{SNR(dB)} = 10\log_{10}((N_R E_a vg)/\sigma^2)$, where $E_a vg = 10$ is the mean symbol energy of the 16-QAM complex alphabet $\mathbb{S}$. The SNR ranges from 0 to 18 dB. Parameters of the algorithm are detailed in Table 1.

Table 1. Algorithm parameters setting

Amount of bee colony	$N = 40$
Number of employed bees	$SN = 20$
Heuristic factor β	0.8
Maximum number of iteration	20

4.1 Computational Complexity Analysis

The evaluation criterion of computational complexity is the order of magnitude of $\text{O}(\cdot)$ with the number of floating point operations. As shown in Table 2, there are three main parts constituting the computational complexity of the low-complexity DGABC detection algorithm. Since a large number of symbols are transmitted during one symbol time, average calculation per symbol is applied to measure the computational complexity. The per-symbol computation complexity of the DGABC algorithm is $\text{O}(N_T)$.

Table 2. Computational complexity of DGABC algorithm

Calculation of initial solution $\hat{\mathbf{x}}^{(0)}$t	$O(N_T^2)$
Calculation of cost function $F(\hat{\mathbf{x}})$	$O(N_T^2)$
Calculation of the solution vector searching	$O(N_T)$
The per-symbol computation complexity	$O(N_T)$

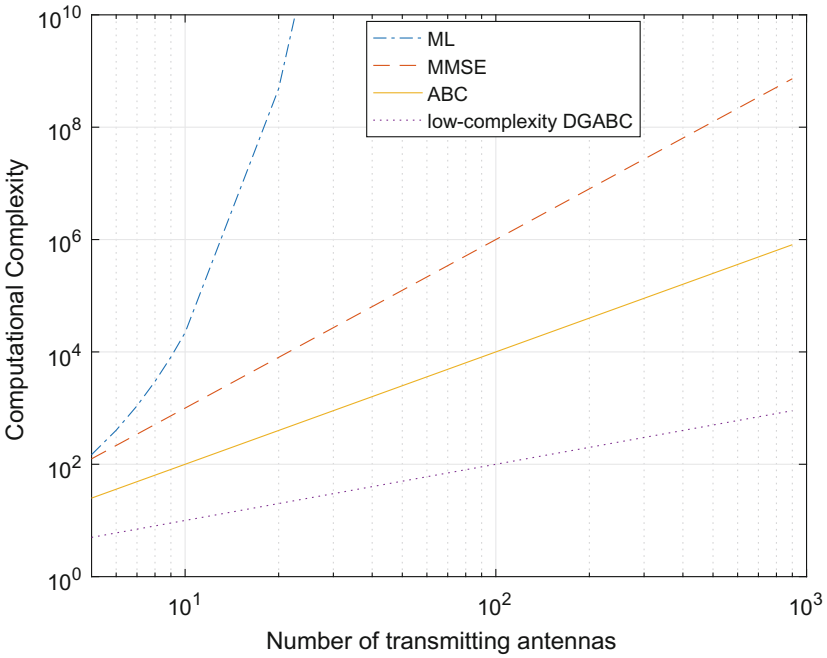


Fig. 2. The bit error (BER) performance of the low-complexity artificial bee colony (DGABC) detection algorithm for massive MIMO system at 16QAM; ABC, original artificial bee colony detection algorithm in [3], AWGN, addictive White Gaussian noise; MMSE, minimum mean square error; SISO, single-in-single-out.

The computational complexity of the proposed low-complexity DGABC detection algorithm is shown as in Fig. 2. With the number of transmitting antennas increasing, the computational complexity of ABC algorithm in [3] increases in two orders polynomial rate, the computational complexity of MMSE increases in three orders polynomial rate and the computational complexity of the proposed low-complexity DGABC algorithm increases in one order polynomial which is much lower than that of the original ABC algorithm. Obviously, the proposed DGABC algorithm lowers the computational complexity effectively.

4.2 BER Performance Simulation

As is introduced in Sect. 3, the optimum BER performance of ML is unable to be simulated in consideration of its exponential computational complexity. Therefore, we use lower bound of ML performance for massive MIMO obtained by the BER performance of the single-in-single-out (SISO) AWGN. The theoretical BER for M-QAM of SISO AWGN is given in [9] as (18).

$$P_{theory} = a \cdot Q(\sqrt{b \cdot (SNR/\log_2(M))}). \tag{18}$$

where $a = 2(1-1/\sqrt{M}/\log_2(\sqrt{M}))$, $b = (6\log 2(\sqrt{M})/(M-1))$, $Q(x)$ signifies a function of x, where $Q(x) = \frac{1}{2}erfc(\frac{x}{\sqrt{2}})$ and $erfc(\cdot)$ denotes the complementary error function.

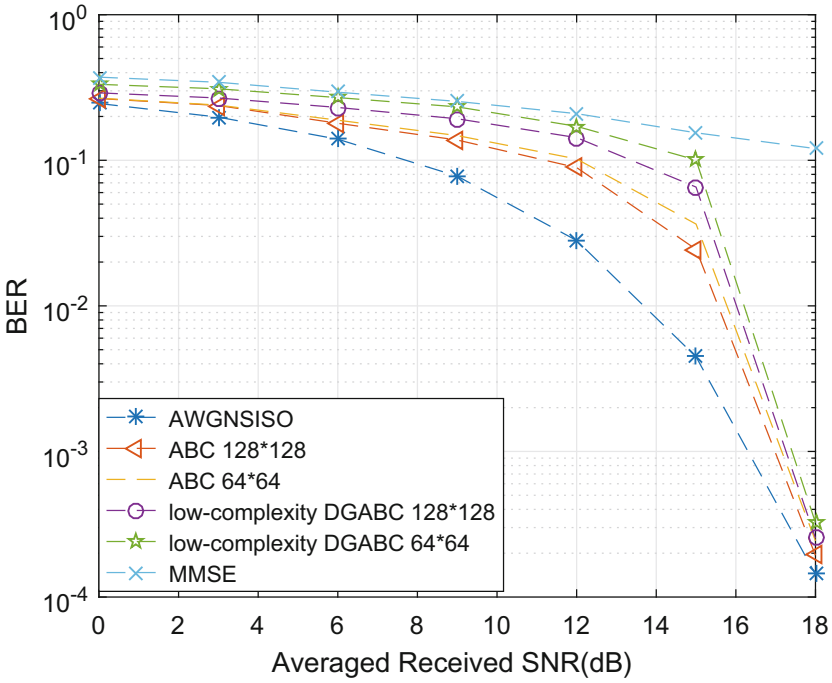


Fig. 3. The bit error (BER) performance of the proposed discrete gbest-guided artificial bee colony (DGABC) detection algorithm for massive MIMO system at 16QAM; AWGN, addictive White Gaussian noise; MMSE, minimum mean square error; SISO, single-in-single-out.

The BER performance of the proposed DGABC algorithm is shown as in Fig. 3. The original ABC algorithm achieves the optimum BER performance, while low-complexity DGABC algorithm obtains a sub-optimum BER performance with little gap. For example, low-complexity DGABC algorithm needs

13 dB to achieve the BER at a magnitude of 10^{-1}, which is less than 1 dB higher than that of the ABC algorithm. When the SNR approaches 18 dB, BER performance of low-complexity DGABC detection algorithm converges to the BER performance of both ML and ABC algorithm.

5 Conclusion

In this paper, we present a low-complexity DGABC algorithm for massive MIMO detection. With the prior information of the matched filter in MMSE detection, the initialization of solution vector is simplified. From the simulation and data analysis in both 64×64 and 128×128 massive MIMO system with 16QAM signals, the computation complexity of the proposed low-complexity DGABC algorithm is decreased with one order lower than the ABC algorithm in [3]. The SNR of the low-complexity DGABC that required to obtain the same BER is less than 1 dB higher than that of ABC algorithm, which can be regarded as near-optimum. Therefore, the proposed DGABC detection is efficient in computational complexity for massive MIMO system uplink detection.

References

1. Rusek, F., Persson, D., Lau, B.K., Larsson, E.G., Marzetta, T.L., Edfors, O., Tufvesson, F.: Scaling up MIMO: opportunities and challenges with very large arrays. IEEE Sign. Process. Mag. **30**(1), 4060 (2013)
2. Bonabeau, E., Dorigo, M., Theraulaz, G.: Swarm Intelligence: From Natural to Artificial Systems. Oxford University Press, New York (1999)
3. Li, L., Meng, W., Ju, S.: A novel artificial bee colony detection algorithm for massive MIMO system. Wirel. Commun. Mob. Comput. **16**(17), 3139–3152 (2016)
4. Khachan, A.M., Tenenbaum, A.J., Adve, R.S.: Linear processing for the downlink in multiuser MIMO systems with multiple data streams. In: Proceedings of IEEE International Conference on Communications (ICC), Istanbul, Turkey, pp. 4113–4118, June 2006
5. Yang, Y., Li, C.Q., Guo, Z.H.: Low-complexity soft-input soft-output detection based on EVD for MIMO systems. In: International Conference on Signal Processing (ICSP), pp. 1546–1550 (2014)
6. Larsson, E.G.: MIMO detection methods: how they work. IEEE Sign. Process. Mag. **26**, 9195 (2009)
7. Huo, Y., Zhuang, Y., Gu, J., Ni, S., Xue, Y.: Discrete gbest-guided artificial bee colony algorithm for cloud service composition. Appl. Intell. **42**, 661–678 (2015)
8. Kong, B.Y., Park, I.-C.: Low-complexity symbol detection for massive MIMO uplink based on Jacobi method. In: 2016 IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), pp. 1–5 (2016)
9. Cho, K., Yoon, D.: On the general BER expression of one- and two-dimensional amplitude modulations. IEEE Trans. Commun. **50**, 10741080 (2002)

Reconsider the Sparsity-Induced Least Mean Square Algorithms on Channel Estimation

Jie Wang(✉), Shangang Fan, Jie Yang, Jian Xiong, and Guan Gui

College of Telecommunication and Information Engineering,
Nanjing University of Posts and Telecommunications, Nanjing 210003, China
13675171572@163.com, sponder@126.com,
{jyang,jxiong,guiguan}@niupt.edu.cn

Abstract. This paper surveys recent advances related to sparse least mean square (LMS) algorithms. Since standard LMS algorithm does not take advantage of the sparsity information about the channel being estimated, various sparse LMS algorithms that are aim at outperforming standard LMS in sparse channel estimation are discussed. Sparse LMS algorithms force the solution to be sparse by introducing a sparse penalty to the standard LMS cost function. Under the reasonable conditions on the training datas and parameters, sparse LMS algorithms are shown to be mean square stable, and their mean square error performance and convergence rate are better than standard LMS algorithm. We introduce the sparse algorithms under Gaussian noises model. The simulation results presented in this work are useful in comparing sparse LMS algorithms against each other, and in comparing sparse LMS algorithms against standard LMS algorithm.

Keywords: Gradient decent · Least mean square (LMS) algorithm
Sparse penalty · Sparse channel estimation · Gaussian noises model

1 Introduction

We all know that least mean square (LMS) algorithm has been applied to solve various technical problems in signal processing fields and broadband wireless communication areas including adaptive communication line enhancement [1], system identification [2], channel estimation [3], echo cancelation [4], etc. The main reasons are that LMS algorithm has low computational complexity as well as does not need extensive stochastic knowledges of the channel models and the training data sequences compared to some other parameter estimation methods, for example, the recursive least squares (RLS) algorithm [5]. But the standard LMS algorithm don't consider the inherent sparse structure information of the system model which must weaken the performance of the estimation. The sparse channel means that there are a few domain taps, in another words, more than half of the channel coefficients are zero or near to zero [6–10]. The sparse channel structure is shown as in Fig. 1 in which the length of the channel is 16 but only four taps are nonzero. To utilize the strengths of LMS algorithm and take full advantage of the sparsity of the channel, many sparse LMS algorithms have been proposed in recent years. This paper main analyses the performance of spare channel estimation based on the sparse LMS algorithms under additive white Gaussian noises model.

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 85–102, 2018.
https://doi.org/10.1007/978-3-319-90802-1_8

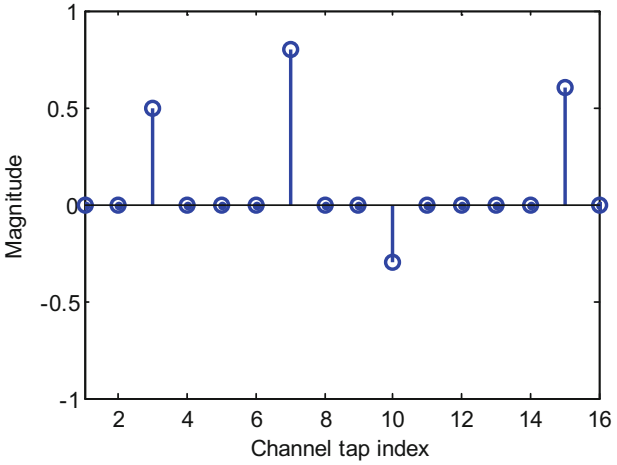


Fig. 1. Example of typical sparse channel model.

The proposed sparse LMS algorithms force the estimation to be sparse by introducing a sparse penalty to the classical LMS cost function. The sparse constraint forces the small channel coefficients to zero, which speed up convergence rate and lower the steady state error of the estimation when most taps of the channel are zero. This paper surveys the field of sparse channel estimation based on sparse LMS algorithms and how to design the sparse penalty to achieve the better performance including faster convergence rate, smaller mean square error, lower computation complexity etc.

Zero attracting least mean square (ZA-LMS) algorithm and Reweighted zero attracting least mean square (RZA-LMS) algorithm have been proposed in [11]. Reweighted ℓ_1-norm penalized least mean square (RL1-LMS) algorithm and ℓ_p-norm penalized least mean square (ℓ_p-norm LMS) algorithm in [12] are the improvements of ZA-LMS. To make much better use of the sparse structure, ℓ_0-norm penalized least mean square (ℓ_0-norm LMS) algorithm has been proposed in [13].

In order to compare these sparse LMS algorithms against each other better, we organize the presentation of the article into four main components. Section 2 reviews the system model being estimated and the standard LMS algorithm. Performance analysis of different sparsity-aware LMS algorithms under Gaussian noises model are presented in Sect. 3. Computer simulation results are shown in Sect. 4. Section 5 concludes the paper.

2 System Model and Problem Formulation

2.1 System Model

The system model of the sparse channel being estimated is as shown in Fig. 2. $\mathbf{x}_n$ is the input signal sequence which is defined as $\mathbf{x}_n = [x(n), x(n-1), \ldots, x(n-N-1)]^T$. N denotes the length of the channel. $\mathbf{w}$ is the actual unknown channel vector which is

defined as $\mathbf{w} = [w_0, w_1, \ldots, w_{N-1}]^{\mathrm{T}}$. $y(n)$ is the output signal of the actual channel, which is defined as $y(n) = \mathbf{w}^T\mathbf{x}_n$. $v(n)$ is the additive noise in the sparse channel being estimated. So $d(n)$ is the desired signal at the receiver side which is defined as

$$d(n) = \mathbf{w}^T\mathbf{x}_n + v(n) \tag{1}$$

And $\widehat{\mathbf{w}}_n$ presents the estimated channel vector at iteration n, which is defined as $\widehat{\mathbf{w}}_n = \left[w_{0,n}, w_{1,n}, \ldots, w_{N-1,n}\right]$. $\widehat{y}(n)$ is the output signal under the estimated channel vector $\widehat{\mathbf{w}}_n$, which is defined as $\widehat{y}(n) = \widehat{\mathbf{w}}_n^T\mathbf{x}_n$. $e(n)$ is the error between the desired output signal $d(n)$ and the output signal $\widehat{y}(n)$ based on the estimated channel coefficients, which is given by

$$e(n) = d(n) - \widehat{y}(n) = \mathbf{w}^T\mathbf{x}_n - \widehat{\mathbf{w}}_n^T\mathbf{x}_n + v(n) \tag{2}$$

What we should do is to find a vector, which is given by $\widehat{\mathbf{w}}_n$ to make $e(n)$ minimum.

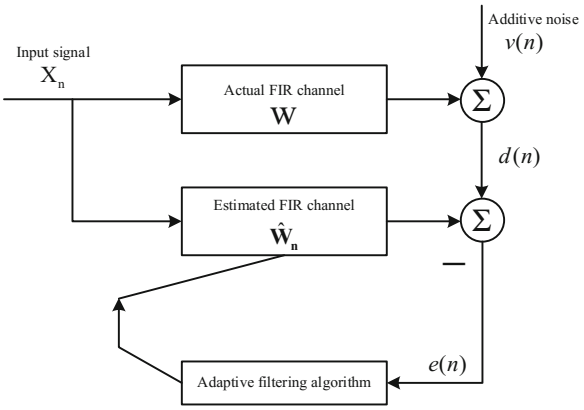


Fig. 2. LMS based system model.

2.2 Standard Least Mean Square Algorithm

Different adaptive filter algorithms utilize various cost functions to solve the problems of signal processing. We all seek the better cost functions either to adapt the channel better or to achieve the faster convergence speed. The cost function of standard least mean square algorithm is

$$G(n) = \frac{1}{2}e(n)^2 \tag{3}$$

And it use the gradient descent algorithm to minimize the Eq. (3) to get the solution of the actual channel vector [5]. So the iterative equation of the standard least mean square algorithm is given by

$$\mathbf{w}_{n+1} = \mathbf{w}_n - \mu \nabla_{\mathbf{w}_n} G(n) = \mathbf{w}_n + \mu e(n)\mathbf{x}_n \tag{4}$$

where μ is the step size of the adaptive filter algorithm. The parameter μ is critical to guarantee the convergence and stable state of the adaptive algorithm. The lager μ, the faster convergence speed of the algorithm but the larger mean square divation (MSD), i.e. $\mathrm{MSD(n)} = \mathrm{E}\left\{\|\mathbf{w} - \widehat{\mathbf{w}}_n\|_2^2\right\}$. And vice versa. To make sure that the least mean square algorithm convergences, μ is chosen within the scope of $0 < \mu < \lambda_{\max}^{-1}$ with $\lambda_{\max}$ being the maximum eigenvalue of the covariance matrix of $\mathbf{x_n}$, i.e. $\mathbf{R} \triangleq \mathrm{E}\left[\mathbf{x}_n\mathbf{x}_n^{\mathbf{T}}\right]$ [5]. To see the influence of parameter μ directly, the simulation results with different μ is shown in Fig. 3. In the numerical simulation, we set the length of the channel being estimated N = 128, the input signal power to additive noise power ratio $SNR = 20\,\mathrm{dB}$. The weights vector of the system is random sequence. The input signal sequences are pseudo random binary sequences and $v(n)$ is additive white Gaussian noises. Three different μ values of 0.01, 0.008 and 0.005 are considered. Simulation results are obtained by taking the average of the network mean square error (MSE) over 2000 independent Monte Carlo runs to smooth the out curves. From Fig. 3 we can see that when μ is smaller the convergence rate is slower but the MSE is smaller and vice versa.

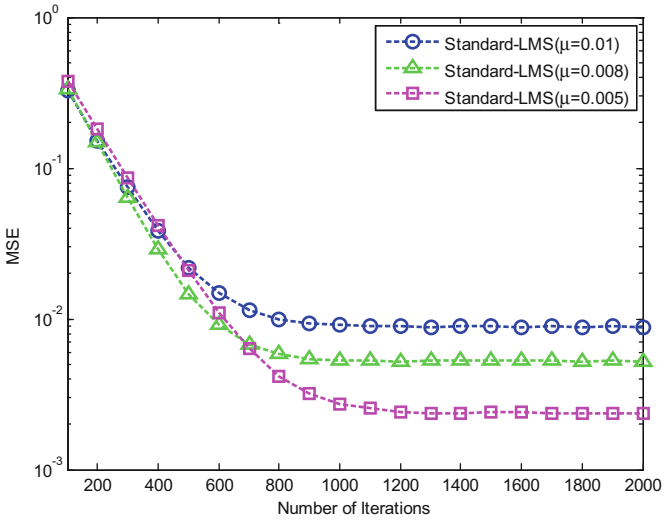


Fig. 3. MSE of standard LMS algorithm with different $\boldsymbol{\mu}$ values (SNR = 20 dB).

3 Reconsider of Sparse LMS Algorithm

In this section, all analysis are under the assumption that the additive noise $v(n)$ is additive white Gaussian noises model which is independent with input signal $\mathbf{x}_n$ [14].

3.1 The Presentation of Different Sparse Mean Square Algorithms

We present the system model and standard mean square algorithm in Section 2. In this Section, we analysis and compare the performance of different sparse adaptive filter algorithms under Gaussian noise environments. The basic idea of all the sparse mean square algorithms is to introduce a sparse penalty to the cost function of the standard LMS algorithm. The sparse constraint attracts the entries of the weights vector of the channel to zero in varying degrees. Accordingly, the estimation of the channel will have faster convergence rate and lower steady state error because most taps of the sparse channel are zero. The essential difference between various sparse algorithms is that the sparse penalties being proposed are diverse which will be analyzed in detail in the part B.

Zero attracting least mean square (ZA-LMS) algorithm: The cost function of ZA-LMS algorithm is $\mathrm{G}_{ZA}(\mathrm{n}) = \frac{1}{2}e^2(n) + \gamma_{ZA}\|\mathbf{w}_n\|_1$. Where $\gamma_{ZA}\|\mathbf{w}_n\|_1$ is sparse penalty, in which γ_{ZA} is regular parameter that balance the mean square error of the algorithm and the sparse degree of the system model. $\|.\|_1$ stands for the ℓ_1-norm of the vector. Based on the gradient decent algorithm, the update equation of the ZA-LMS algorithm is

$$\mathbf{w}_{n+1} = \mathbf{w}_n + \mu e(n)\mathbf{x}_n - \rho_{ZA} sgn(\mathbf{w}_n) \tag{5}$$

where $\rho_{\mathrm{ZA}} = \mu\gamma_{ZA}$.

Reweighted zero attracting least mean square (RZA-LMS) algorithm: The cost function of RZA-LMS is $\mathrm{G}_{\mathrm{RZA}}(n) = \frac{1}{2}e^2(n) + \gamma_{RZA}\sum_{i=1}^{N}\log\left(1 + [\mathbf{w}_n]_i/\epsilon'_{RZA}\right)$. Where $\gamma_{RZA}\sum_{i=1}^{N}\log\left(1 + [\mathbf{w}_n]_i/\epsilon'_{RZA}\right)$ is the sparse constraint, in which γ_{RZA} is regularization parameter that weights the mean square error of the algorithm and the sparse level of the system model and ϵ'_{RZA} is a positive number. Based on the gradient decent algorithm, the update equation of the RZA-LMS algorithm is

$$\mathbf{w}_{n+1} = \mathbf{w}_n + \mu e(n)\mathbf{x}_n - \rho_{RZA}\frac{sgn(\mathbf{w}_n)}{1 + \epsilon_{RZA}|\mathbf{w}_n|} \tag{6}$$

where $\rho_{RZA} = \mu\gamma_{RZA}\epsilon_{RZA}$ and $\epsilon_{\mathrm{RZA}} = 1/\epsilon'_{RZA}$.

Reweighted ℓ_1-norm penalized least mean square (RL1-LMS) algorithm: The cost function of RL1-LMS is $\mathrm{G}_{r\ell_1}(n) = \frac{1}{2}e^2(n) + \gamma_r\|\mathbf{s}_k\mathbf{w}_n\|_1$. Where $\gamma_r\|\mathbf{s}_k\mathbf{w}_n\|_1$ is the sparse constraint, in which γ_r is regular parameter that balance the mean square error of the algorithm and the sparse degree of the system model and $\mathbf{s}_k$ is a row vector with its elements are $[\mathbf{s}_k]_{\mathrm{i}} = \frac{1}{\epsilon_r + \left|[\mathbf{w}_{k-1}]_i\right|}$, i = 1, …, N. And ϵ_r is a positive number and $[.]_{\mathrm{i}}$ denotes

the i-th entry of the vector. $\|.\|_1$ stands for the ℓ_1-norm of the vector. Based on the gradient decent algorithm, the update equation of the RL1-LMS is

$$\mathbf{w}_{n+1} = \mathbf{w}_n + \mu e(n)\mathbf{x}_n - \rho_r \frac{sgn(\mathbf{w}_n)}{\epsilon_r + |\mathbf{w}_{n-1}|} \tag{7}$$

where $\rho_r = \mu\gamma_r$ and sgn(.) is the sign function which can be presented by $\mathrm{sgn(x)} = \begin{cases} 1, x > 0 \\ 0, x = 0 \\ -1, x < 0 \end{cases}$. The operation of sgn(.) is on every entry of the vector. The absolute value operator and the division operator in the last term of Eq. (7) are all component-wise.

ℓ_p-norm penalized least mean square (ℓ_p-norm LMS) algorithm: The cost function of ℓ_p-norm LMS is $\mathrm{G}_{\ell_\mathrm{p}}(n) = \frac{1}{2}e^2(n) + \gamma_p\|\mathbf{w}_n\|_\mathrm{p}$. Where $\gamma_\mathrm{p}\|\mathbf{w}_n\|_\mathrm{p}$ is sparse penalty, in which γ_p is regular parameter that weights the mean square error of the algorithm and the sparse degree of the system model. $\|.\|_\mathrm{p}$ stands for the ℓ_p-norm of the vector. The parameter p is a positive number with $0 < p < 1$. Based on the gradient decent algorithm, the update equation of the ℓ_p-norm LMS algorithm is

$$\mathbf{w}_{n+1} = \mathbf{w}_n + \mu e(n)\mathbf{x}_n - \rho_p \frac{\left(\|\mathbf{w}_n\|_\mathrm{p}\right)^{1-\mathrm{p}} sgn(\mathbf{w}_n)}{|\mathbf{w}_n|^{(1-\mathrm{p})}} \tag{8}$$

But to prevent the algorithm from being unstable when $\mathbf{w}_n$ is a zero vector, we usually add a regularization parameter ϵ_p to the last term of Eq. (8). Then the update equation of the ℓ_p-norm LMS is

$$\mathbf{w}_{n+1} = \mathbf{w}_n + \mu e(n)\mathbf{x}_n - \rho_p \frac{\left(\|\mathbf{w}_n\|_p\right)^{1-p} sgn(\mathbf{w}_n)}{\epsilon_p + |\mathbf{w}_n|^{(1-p)}} \tag{9}$$

where $\rho_p = \mu\gamma_p$.

ℓ_0-norm penalized least mean square (ℓ_0-norm LMS) algorithm: The risk function of ℓ_0-norm LMS is $\mathrm{G}_{\ell_0}(n) = \frac{1}{2}e^2(n) + \gamma_{\ell_0}\|\mathbf{w}_n\|_0$. Where $\gamma_{\ell_0}\|\mathbf{w}_n\|_0$ is sparse penalty, in which γ_{ℓ_0} is regular parameter that balance the mean square error of the algorithm and the sparse degree of the system model. $\|.\|_0$ stands for the ℓ_0-norm of the vector. As we all know, find the minimum solution of the ℓ_0-norm is a Non-Polynomial (NP) hard problem. So a approximate continuous function has been proposed in [15] which is $\|\mathbf{w}\|_0 \approx \sum_{i=1}^{N}\left(1 - e^{-\beta|[\mathbf{w}_n]_\mathrm{i}|}\right)$. Where |.| stands for the absolute operator and $[\mathbf{w}_n]_\mathrm{i}$ is the i-th element of the vector $\mathbf{w}$. β is a positive number. Then the cost function of ℓ_0-norm LMS can be rewritten as $\mathrm{G}_{\ell_0}(n) = \frac{1}{2}e^2(n) + \gamma_{\ell_0}\sum_{i=1}^{N}\left(1 - e^{-\beta|[\mathbf{w}_n]_\mathrm{i}|}\right)$. Based on the gradient decent algorithm, the update equation of the ℓ_0-norm LMS algorithm is

$$\mathbf{w}_{n+1} = \mathbf{w}_n + \mu e(n)\mathbf{x}_n - \rho_{l_0}\beta \operatorname{sgn}(\mathbf{w}_n)\mathrm{e}^{-\beta|\mathbf{w}_n|} \tag{10}$$

where $\rho_{l_0} = \mu\gamma_{\ell_0}$. But the term $\mathrm{e}^{-\beta|\mathbf{w}_n|}$ has very high computational complexity which isn't what we want. Then the first-order Taylor series expansion of exponential functions has been introduced in [15] which is shown as $e^{-\beta|[\mathbf{w}_n]_i|} \approx f(x) = \begin{cases} 1-\beta\left|[\mathbf{w}_n]_i\right|, & when\left|[\mathbf{w}_n]_i\right| \le 1/\beta \\ 0, & others \end{cases}$. Then the update equation of the ℓ_0-norm LMS is derived as

$$\mathbf{w}_{n+1} = \mathbf{w}_n + \mu e(n)\mathbf{x}_n - \rho_{l_0}\mathbf{J}(\mathbf{w}_n) \tag{11}$$

where $J\left([\mathbf{w}_n]_i\right) \approx \begin{cases} \beta sgn\left([\mathbf{w}_n]_i\right) - \beta^2\left([\mathbf{w}_n]_i\right), & when\left|[\mathbf{w}_n]_i\right| \le 1/\beta \\ 0, & others \end{cases}$, in which $[\mathbf{w}_n]_i$ is the i-th entry of the vector $\mathbf{w}_n$.

3.2 Analysis of the Difference Between the Five Sparse Algorithms

We present five sparse least mean square algorithms in part A. They have different sparse penalties which stand for the different sparse constraints to the channel vector being estimated. The regularization parameters in every algorithm also play a big role in the sparse constraint to the resolution of the channel.

The sparse penalty term of ZA-LMS algorithm is $\mathrm{h(t)}^{\mathrm{ZA}} = |\rho_{ZA} sgn(t)|$, where ρ_{ZA} decides the strength of the penalty term. From Fig. 4, we can know that ZA-LMS has the same sparse effects on all weights of the channel. It will cause the high steady state error of the algorithm against the dominant taps of the channel. As the improvement of ZA-LMS algorithm, RZA-LMS algorithm has a different sparse constraint which is $\mathrm{h(t)} = \left|\rho_{RZA}\frac{sgn(t)}{1+\epsilon_{RZA}|t|}\right|$, where ρ_{RZA} has the same role as the ρ_{ZA} plays. From Fig. 5, we can see that RZA-LMS algorithm attracts the entries of the channel vector to zero with different extent. The smaller the entry, the stronger strength. And vice versa. Accordingly, RZA-LMS algorithm normally have the better performance than ZA-LMS algorithm. The sparse penalty terms of the RL1-LMS algorithm and ℓ_p-norm LMS algorithm run similar as RZA-LMS algorithm. The main difference between the three algorithms is the distribution of the strength of sparse constraint to various taps of the channel. From Figs. 6 and 7, we can find that RL1-LMS algorithm and ℓ_p-norm LMS have a significantly stronger effects on small weights of the channel than RZA-LMS that will yield lower steady state error for sparse channel estimation.

The sparse penalty term of ℓ_0-norm LMS is $\mathrm{h(t)}^{\ell^0} = \left|\rho_{\ell_0} J(t)\right|$, where $J(t) \approx \begin{cases} \beta sgn(t) - \beta^2(t), & when|\mathrm{t}| \le 1/\beta \\ 0, & others \end{cases}$. From Fig. 8, we can get that the sparse attraction of ℓ_0-norm LMS algorithm only effects on the taps of the channel in a definite interval. This property of ℓ_0-norm LMS algorithm which reduce the mean square error of the weights out of the interval usually make it gain a more accurate estimation than another four sparse algorithms.

To compare the performance of the five sparse algorithms, we do the numerical simulation. The simulation results are shown in Fig. 9. The parameter values of every algorithm in the numeric simulation are shown in the Table 1.

From Fig. 9, we can see that the ZA-LMS have the faster convergence rate and larger MSE compared with the other four algorithm. And ℓ_0-norm LMS achieve the best performance in the simulation.

Table 1. Parameter values setting in Fig. 9.

Parameters	Values
Input signal	Pseudo-random binary sequences
The length of channel	N = 128
Number of dominant taps of channel vector	S = 16
Distribution of nonzero coefficients	Random Gaussian CN(0,1)
Signal to noise ratio for channel model	SNR = 20 dB
Gaussian noise distribution	Gaussian $\mathrm{CN}\left(0, \delta_n^2\right)$
Step size	$\mu = 0.005$
Parameters of algorithms	ρ_{ZA} = 1e−3, ρ_{RZA} = 1e−5, E_{RZA} = 25, ρ_r = 5e−6, p = 0.5, ρ_p = 5e−6, E_p = 0.05, β_0 = 10, ρ_0 = 1e−4

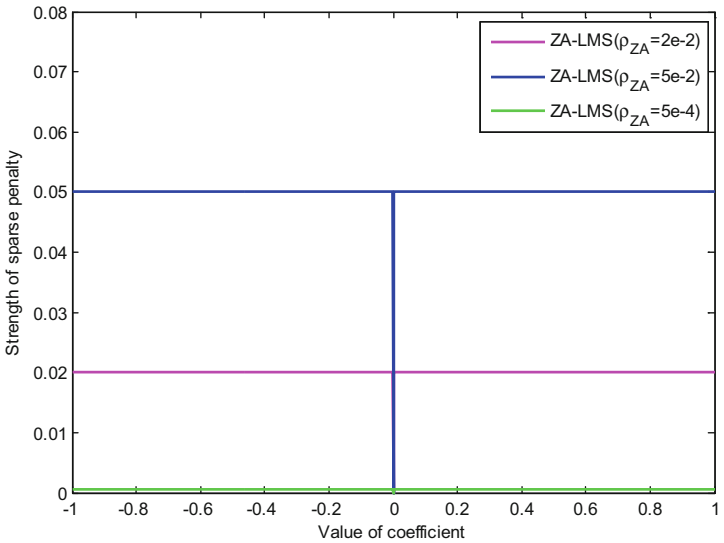


Fig. 4. Sparse constraints to channel vector **w** of ZA-LMS algorithm with different $\boldsymbol{\rho_{ZA}}$ values.

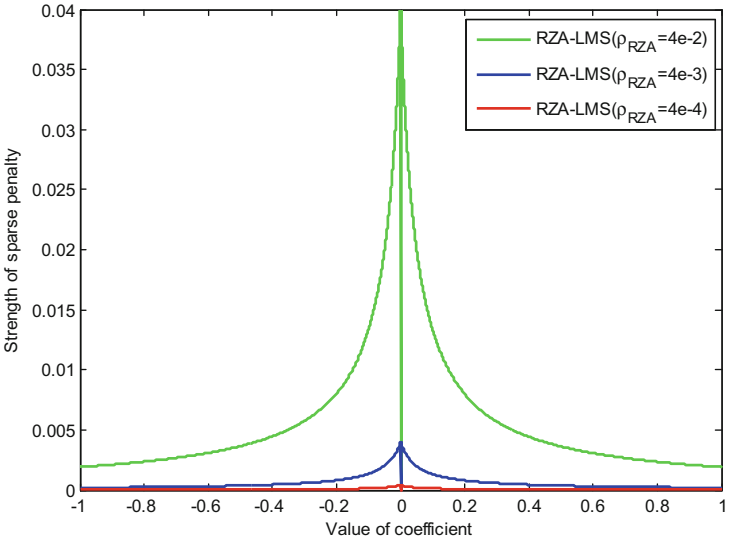


Fig. 5. Sparse constraints to channel vector **w** of RZA-LMS algorithm with different $\boldsymbol{\rho_{RZA}}$ values ($\boldsymbol{\epsilon_{RZA} = 20}$).

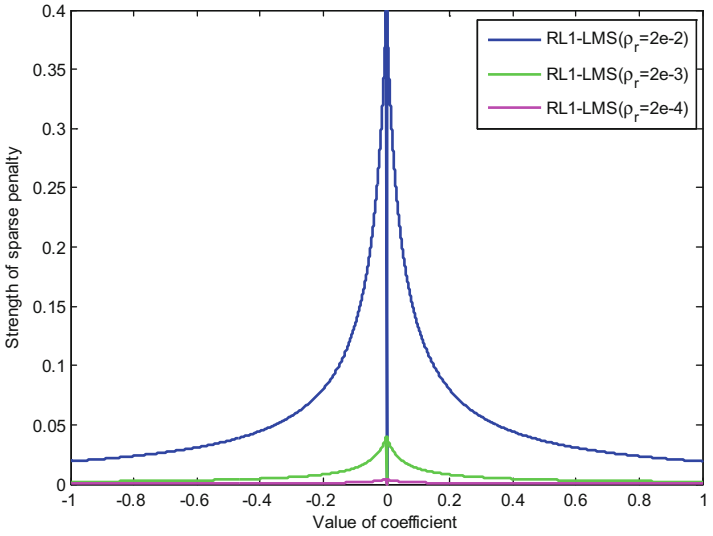


Fig. 6. Sparse constraints to channel vector **w** of RL1-LMS algorithm with different $\boldsymbol{\rho_r}$ values ($\boldsymbol{\epsilon_r = 5 \times 10^{-2}}$).

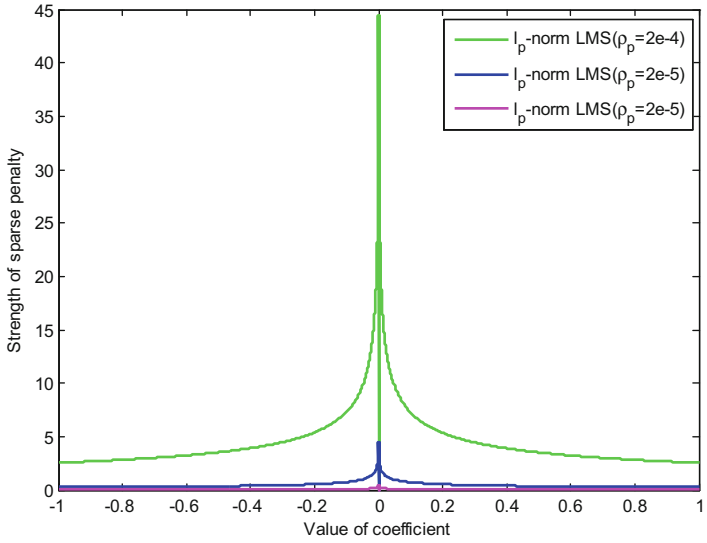


Fig. 7. Sparse constraints to channel vector $\mathbf{w}$ of ℓ_p-norm LMS algorithm with different $\boldsymbol{\rho_p}$ values ($\boldsymbol{\epsilon_p} = \mathbf{5} \times \mathbf{10}^{-\mathbf{2}}$,$\mathbf{p} = \mathbf{0.5}$).

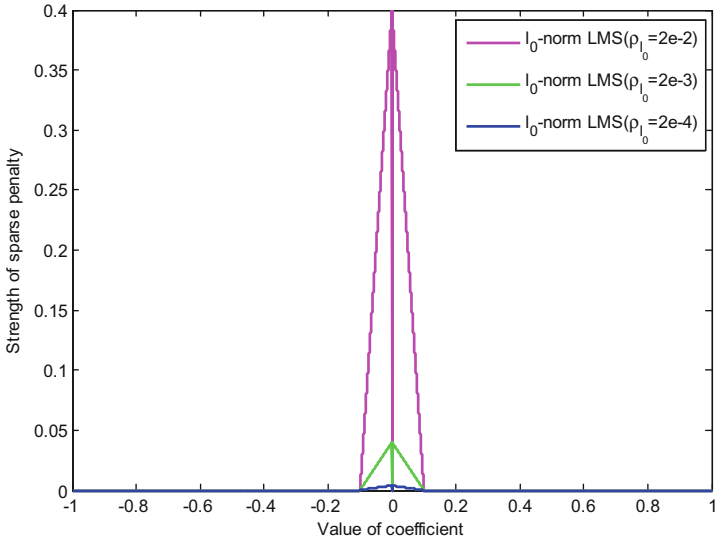


Fig. 8. Sparse constraints to channel vector $\mathbf{w}$ of ℓ_0-norm LMS algorithm with different $\boldsymbol{\rho_r}$ values ($\boldsymbol{\beta} = \mathbf{10}$).

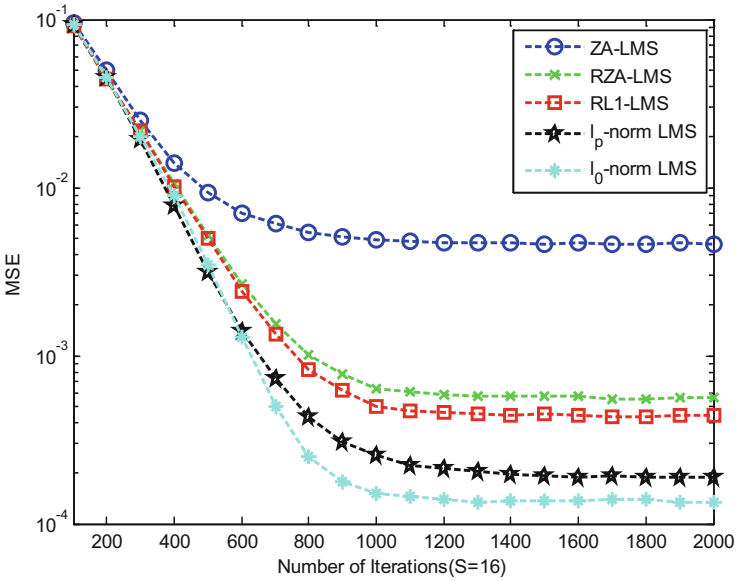


Fig. 9. Comparisons between different sparse LMS algorithms.

4 Simulation Results

Regular parameters of sparse LMS algorithms and the sparse degree of the channel have big implications for the gains of the algorithms. The steady state MSD equation $J_{ZA}(\infty)$ of ZA-LMS which has been derived in [16] is that

$$J_{ZA}(\infty) = \left[t^2 - \frac{(\pi-1)\mu\sigma_x^2+1}{2\pi\mu^2\sigma_x^4}\rho_{ZA}^2\right]\frac{2}{\mu\sigma_x^2} - \frac{\sigma_v^2}{\sigma_x^2} \tag{12}$$

where σ_v^2 denotes the variance of the additive noise $v(n)$ and σ_x^2 is the variance of the input sequence $\mathbf{x}(n)$. The parameter t is the positive solution of $c_1 t^2 + c_2 t + c_3 = 0$ in which $c_1 = L - \frac{2}{\mu\sigma_x^2}\left(1-\mu\sigma_x^2\right)$ and $c_2 = -2(L-S)\rho_{ZA}\frac{\sqrt{1-\mu\sigma_x^2}}{\sqrt{2\pi}\mu\sigma_x^2}$ and $c_3 = \left(\frac{L-2S}{2\pi}+M+1\right)\frac{1-\mu\sigma_x^2}{\mu^2\sigma_x^4}\rho_{ZA}^2 + \frac{\left(1-\mu\sigma_x^2\right)^2}{\pi\mu^3\sigma_x^6}\rho_{ZA}^2 + \frac{\sigma_v^2}{\sigma_x^2}\left(1-\mu\sigma_x^2\right)$. From Eq. (12) we can see that the steady state MSD depends on the sparse degree of the channel S, the regular parameter of the algorithm ρ_{ZA}, the step size μ and the channel length L [16]. When the sparsity of the channel is determined, the larger value of ρ_{ZA} will increase the gap between the large tap-weights and it's true value and the smaller value of ρ_{ZA} will decrease the effects of sparse constraint on sparse channels. Both of them destroy the performance of ZA-LMS algorithm. To see the influence of ρ_{ZA} directly we simulate the algorithm with different ρ_{ZA} values. The simulation based on the channel model with the length of the channel is $N = 128$, the sparse level of the channel is $S = 16$, the signal to noise ratio of the channel is $SNR = 20\,dB$. Simulation results are obtained by

taking the average of the network mean square error (MSE) over 2000 independent Monte Carlo runs. The simulation results are shown in Fig. 10. From the simulation result, we can see that when $\rho_{ZA} = 1 \times 10^{-4}$ that is smaller than 1×10^{-3} and is larger than 1×10^{-5} has the lowest steady state MSD.

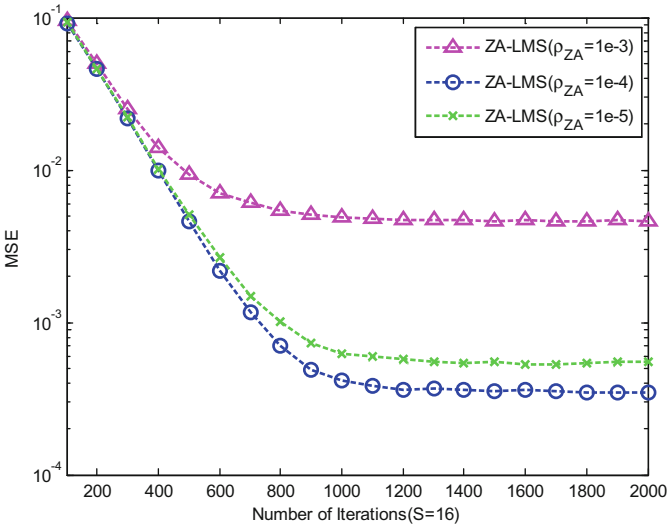


Fig. 10. ZA-LMS simulation with different $\boldsymbol{\rho_{ZA}}$ values.

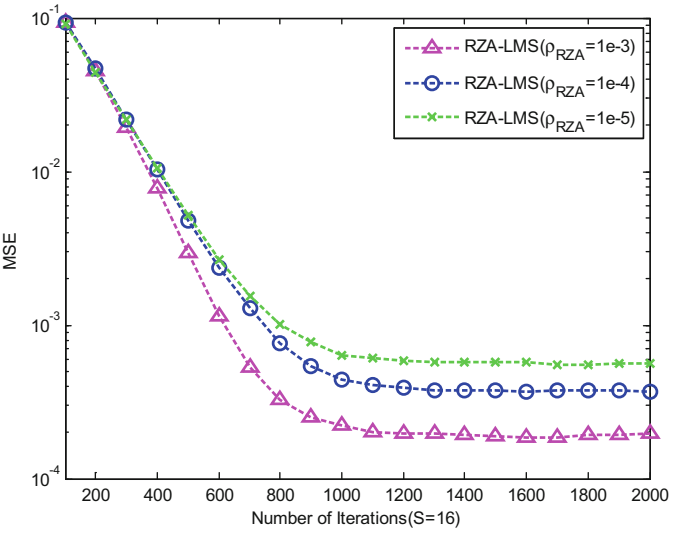


Fig. 11. RZA-LMS simulation with different $\boldsymbol{\rho_{RZA}}$ values.

The regularization parameters of another four sparse algorithm are similar as ZA-LMS. We simulate another four sparse algorithms with different regular parameters and fixed sparsity. All the simulations based on the same channel model with the length of the channel is N = 128, the sparse level of the channel is S = 16, the signal to noise ratio of the channel is SNR = 20 dB. Simulation results are obtained by taking the average of the network mean square divation (MSD) over 2000 independent Monte Carlo runs. The simulation results are shown in Figs. 11, 12, 13 and 14. The simulation results demonstrate the theoretical analysis that the smaller or larger values of ρ will degrade the performance of the algorithm.

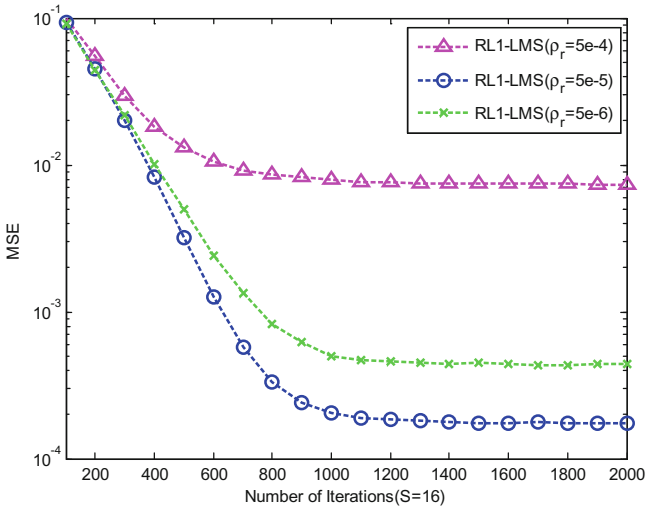


Fig. 12. RL1-LMS simulation with different ρ_r values.

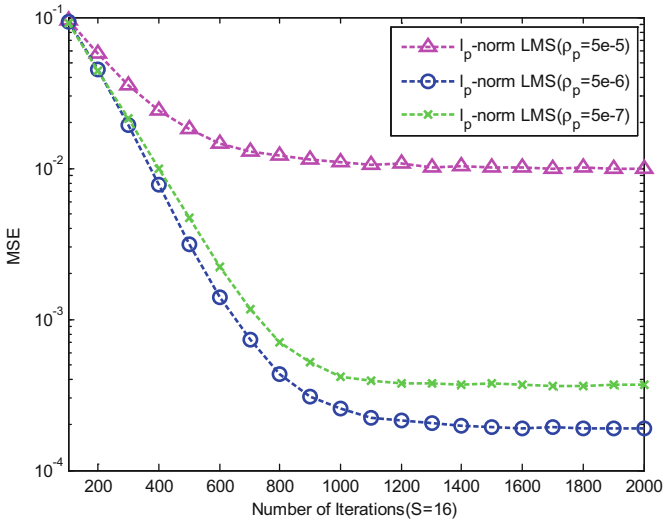


Fig. 13. ℓ_p-norm LMS simulation with different ρ_p values.

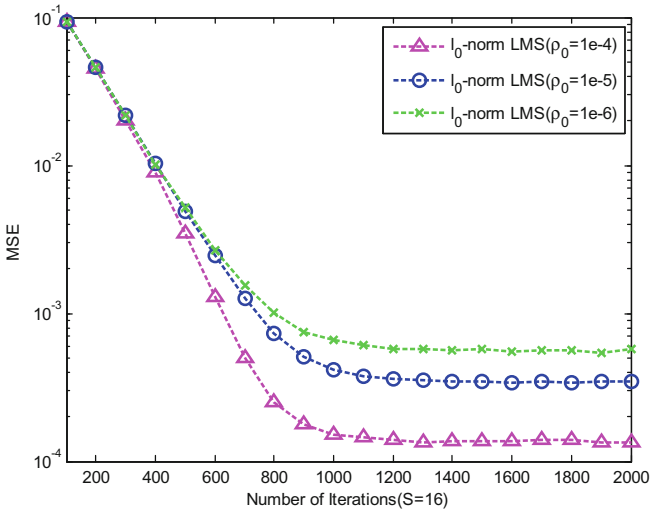


Fig. 14. ℓ_0-norm LMS simulation with different $\boldsymbol{\rho_0}$ values.

When the regularization parameter ρ_{ZA} is certain, namely, the sparse constraint is decided, the estimated solutions of the channel model with different number of zero coefficients will have various accuracy. The more the number of zero weights are, the more effectively the ZA-LMS algorithm attracts the tap-weights to zero and the vice versa. Accordingly, the performance of ZA-LMS algorithm increases with the strong sparse degree of the channel. Another four sparse algorithms have the same property. To see the influence of the spare level of channel model intuitively we simulate every algorithm with fixed regularization parameter ρ (ρ_{ZA}, ρ_{RZA}, ρ_r, ρ_p, ρ_0) and various channel model with different sparse structure. The simulation results are shown in Figs. 15, 16, 17, 18 and 19. The parameter values of the simulations are as shown in

Table 2. Parameter values of numeric simulation in Figs. 15, 16, 17, 18 and 19

Parameters	Values
Input signal	Pseudo-random binary sequences
The length of channel	N = 128
Number of dominant taps of channel vector	S ϵ {16, 32, 64}
Distribution of nonzero coefficients	Random Gaussian CN(0,1)
Signal to noise ratio for channel model	SNR = 20 dB
Gaussian noise distribution	Gaussian CN$\left(0, \delta_n^2\right)$
Step size	$\mu = 0.005$
Parameters of algorithms	ρ_{ZA} = 1e−4, ρ_{RZA} = 1e−3, E_{RZA} = 25, ρ_r = 5e−5, p = 0.5, ρ_p = 5e−6, E_p = 0.05, β_0 = 10, ρ_0 = 1e−4

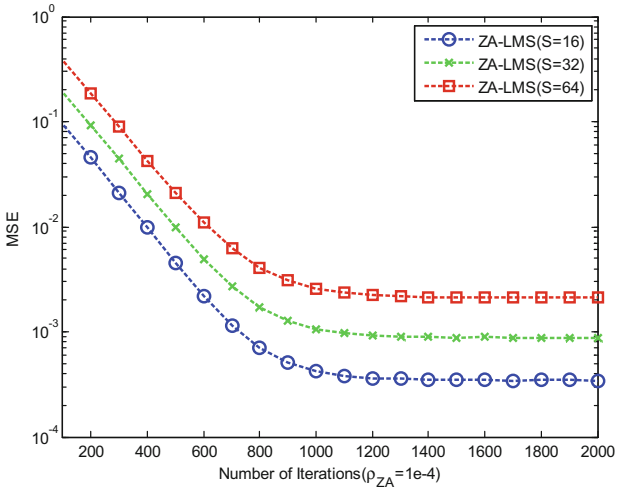


Fig. 15. Simulation of ZA-LMS algorithm with different S.

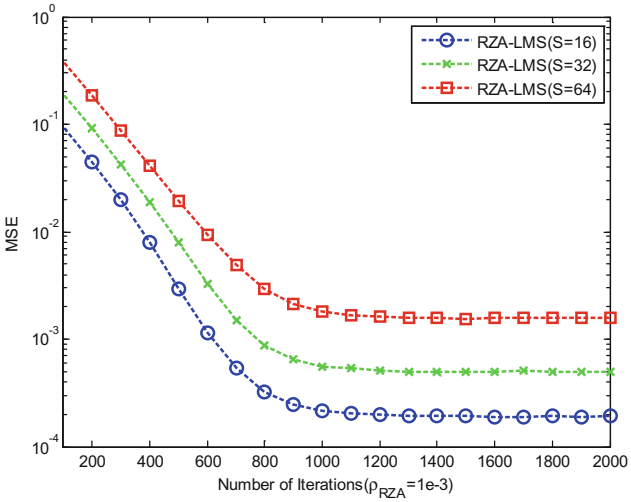


Fig. 16. Simulation of RZA-LMS algorithm with different S.

Table 2. From the simulation results we can get that the more sparse of the channel model structure, the better performance of the sparse algorithms will obtain. The conclusion is easy for us to understand because that the more numbers of the zero taps of the channel, there will be smaller bias between the estimated weights and their actual values.

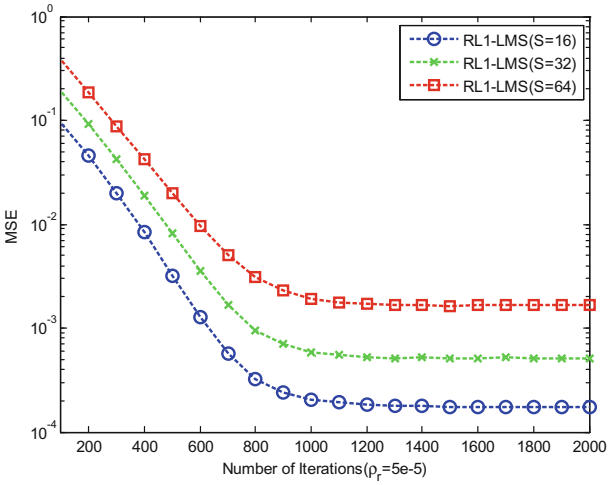


Fig. 17. Simulation of RL1-LMS algorithm with different S.

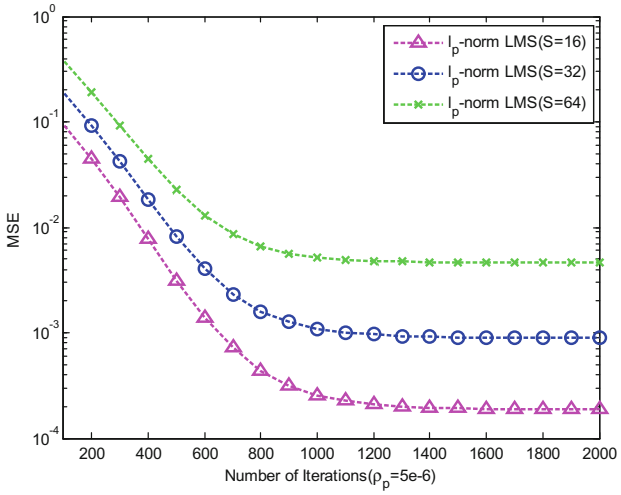


Fig. 18. Simulation of ℓ_p-norm LMS with different S.

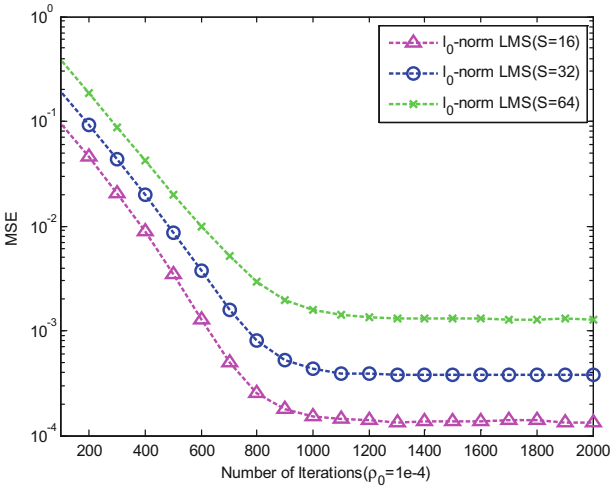


Fig. 19. Simulation of ℓ_0-norm LMS with different S.

5 Conclusions

We analyze and compare the sparse LMS algorithms performance from various aspects in this paper. The simulation results have demonstrated that the sparse LMS algorithm outperformance the traditional LMS algorithm. We know that there are many factors influence the performance of the algorithm, such as the cost function of the algorithm, the sparse constraint of the algorithm, the structure of the system model etc. To achieve the better estimation of the system, we should set proper parameter values. The more information of the system model we know, the more accurate algorithm we can design. The next work will explore more information of the system model and design more effective algorithms.

Acknowledgement. National Natural Science Foundation of China Grants (No. 61401069, No. 61701258), Jiangsu Specially Appointed Professor Grant (RK002STP16001), Innovation and Entrepreneurship of Jiangsu High-level Talent Grant (CZ0010617002), Natural Science Foundation of Jiangsu Province Grant (No. BK20170906), Natural Science Foundation of Jiangsu Higher Education Institutions Grant (No. 17KJB510044), High-Level Talent Startup Grant of Nanjing University of Posts and Telecommunications (XK0010915026) and "1311 Talent Plan" of Nanjing University of Posts and Telecommunications.

References

1. Mboup, M., Macchi, O., Bershad, N.: Steady-state superiority of LMS over LS for time-varying line enhancer in noisy environment. IEE Proc. F - Radar Sig. Process. **138**(4), 354–360 (1991)
2. Bershad, N.J., Bermudez, J.C.M., Member, S.: Stochastic analysis of the LMS algorithm for system identification with subspace inputs. IEEE Trans. Signal Process. **56**(3), 1018–1027 (2008)

3. Coleri, S., Ergen, M., Puri, A., Bahai, A.: Channel estimation techniques based on pilot arrangement in OFDM systems. IEEE Trans. Broadcast. **48**(3), 223–229 (2002)
4. Rao, H.I.K., Member, S., Farhang-boroujeny, B., Member, S.: Fast LMS/Newton algorithms for stereophonic acoustic echo cancellation. IEEE Trans. Signal Process. **57**(8), 2919–2930 (2009)
5. Taheri, O., Vorobyov, S.A.: Reweighted l_1-norm penalized LMS for sparse channel estimation and its analysis. Sign. Process. **104**, 70–79 (2014)
6. Vuokko, L., Kolmonen, V.M., Salo, J., Vainikainen, P.: Measurement of large-scale cluster power characteristics for geometric channel models. IEEE Trans. Antennas Propag. **55**(11), 3361–3365 (2007)
7. Czink, N., Yin, X., Özcelik, H., Herdin, M., Bonek, E., Fleury, B.H.: Cluster characteristics in a MIMO indoor propagation environment. IEEE Trans. Wirel. Commun. **6**(4), 1465–1474 (2007)
8. Adachi, F., Kudoh, E.: New direction of broadband wireless technology. Wirel. Commun. Mob. Comput. **7**(8), 969–983 (2007)
9. Molisch, A.F.: Ultrawideband propagation channels-theory, measurement, and modeling. IEEE Trans. Veh. Technol. **54**(5), 1528–1545 (2005)
10. Schreiber, W.F.: Advanced television systems for terrestrial broadcasting: some problems and some proposed solutions. Proc. IEEE **83**(6), 958–981 (1995)
11. Chen, Y., Gu, Y., Hero, A.O.: Sparse LMS for system identification. In: IEEE International Conference on Acoustics, Speech and Signal Processing, Taipei, Taiwan, 19–24 April 2009, pp. 3125–3128 (2009)
12. Taheri, O., Vorobyov, S.A.: Sparse channel estimation with l_p-norm and reweighted l_1-norm penalized least mean squares. In: IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Prague, Czech Republic, 22–27 May 2011, pp. 2864–2867 (2011)
13. Gu, Y., Jin, J., Mei, S.: l_0-norm constraint LMS algorithm for sparse system identification. IEEE Sign. Process. Lett. **16**(9), 774–777 (2009)
14. Li, Y., Wang, Y., Jiang, T.: Low complexity norm-adaption least mean square/fourth algorithm and its applications for sparse channel estimation. In: 2016 IEEE Wireless Communications and Networking Conference Doha, Qatar, 3–6 April 2016, pp. 1–6 (2016). Electronic ISSN 1558-2612
15. Gui, G., Peng, W., Adachi, F.: Improved adaptive sparse channel estimation based on the least mean square algorithm. In: IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, 7–10 April, pp. 3105–3109 (2013)
16. Shi, K., Shi, P.: Convergence analysis of sparse LMS algorithms with l_1-norm penalty based on white input signal. Sign. Proces. **90**(12), 3289–3293 (2010)

A Method for Analysing and Improving the Multi-user Detection Algorithm of SCMA

Shuai Han(✉), Yiteng Huang, and Bin Wang

Communications Research Center, Harbin Institute of Technology, Harbin, China
hanshuai@hit.edu.cn

Abstract. Sparse code multiple access (SCMA) is a novel kind of non-orthogonal multiple access technology which combines the ideas of CDMA and OFDMA. The modulation scheme based on the mapping of the codebook can be regarded as a kind of spread spectrum coding technology and the encoding gain helps to improve spectrum utilization, system capacity and transfer rate. At the receiver, the message passing algorithm (MPA) which is employed to detect multi-user signals can reduce the computational complexity because of the sparse structure. In this paper, we use the extrinsic information transfer chart (EXIT chart) to analyze MPA detection performance under different SNR conditions and propose serial MPA algorithm based on fairness which can improve the convergence performance of the algorithm and reduce the computational complexity. The theoretical derivation and simulation results demonstrate that serial MPA can improve the algorithm convergence performance and MPA detection are not apply to low SNR scenario.

Keywords: SCMA · EXIT chart
Serial MPA algorithm based on fairness · Multi-user detection
MPA convergence

1 Introduction

In the future 5G networks, the data flow rate of the system is greatly improved and occupies a wider range of bandwidth compared with 4G [1]. However, the reality is that a variety of standard communication systems mix together and the continuous spectrum resources are scant, so only limited discrete spectrum resources are available. Obviously, OFDM technology can not meet the needs of 5G mass connectivity. Therefore, 5G network sets higher demands upon the air interface techniques, in which sparse code multiple access (SCMA) is one of the standard candidates of air interface technology for 5G mobile communications [2].

B. Wang—This paper is sponsored by the funds of Science and Technology on Communication Networks Laboratory (No. KX162600029), the Huawei Innovation Research Program and the National Natural Science Foundation of China (No. 91438205).

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 103–115, 2018.
https://doi.org/10.1007/978-3-319-90802-1_9

SCMA combines the idea of CDMA and OFDMA [3] to achieve non-orthogonal multiple access in the frequency domain. It modulates the signal onto the multi-dimensional OFDMA subcarrier. The codebook mapping can be considered as a spread-spectrum coding technique, which can improve the spectrum utilization and improve the system performance. SCMA uses multi-dimensional codebook instead of QAM modulation and LDS spread [4] to provide the shaping gain and spread gain. In the SCMA system, the user's information is modulated on multiple carriers for diversity transmission, and its codebook mapping is various, so that the receiver can demodulate user information based on different carriers and different codebook to reduce the information collision. Message passing algorithm (MPA) with affordable complexity can be adopted to achieve near ML performance [5] in SCMA detection module. Weighted Message Passing Algorithm for SCMA is proposed in reference [6]. Bayesteh studied the blind detection algorithm for SCMA uplink [7].

However, there are few works have been done to study the MPA algorithm performance in SCMA detection system under different conditions. What's more, the convergence performance of the original MPA algorithm need to be improved in engineering implementation.

In this paper, we use the extrinsic information transfer chart (EXIT chart) to analyze MPA detection performance under different channel conditions [8]. It's convenient to find out whether the MPA algorithm can converge to exact solutions and the approximate number of iteration required for convergence through the simulation diagram. Besides, we propose serial MPA based on fairness to improve the convergence performance of original multi-user detection algorithm. Simulation result shows that the algorithm that we propose reduces the number of iterations significantly, improves the convergence performance of the algorithm, and reduces the computational complexity of the system. It will be introduced in Sect. 4 separately.

The remainder of this paper is organized as follows. In Sect. 2 we introduce the basic principle and system model of SCMA. Section 3 introduces extrinsic information transfer (EXIT) chart to analyse the MPA algorithm performance. the improvement detection algorithm is presented in Sect. 3B. Then, the original MPA algorithm performance is analysed through simulations in Sect. 4. Moreover, we propose serial detection algorithm based on fairness to improve the convergence performance of the algorithm and reduce the computational complexity of the system in this section. Finally, the conclusion is given in Sect. 5.

2 System Model

2.1 System Model

The structure of SCMA transmitter is shown in Fig. 1. The data streams from multiusers is processed by FEC encoder module first and then interleaving the encoded data to prevent burst errors. The processed data streams are sent to SCMA encoder and directly mapped to several orthogonal subcarriers according to the pre-designed codebooks. Finally, the whole data streams output from the

SCMA encoder are transmitted through the channel. The transmission signal is superimposed on the data of other users carried by the same subcarrier and introduces noise in the transmission process. Then the transmission signal is sent to receiver. The SCMA receiver structure is shown in Fig. 2. The SCMA decoder detects the user data streams which are interferenced by channel noise and other user data streams according to codebook and carrier allocation information we have known. After that, decode convolution code and restore data bits with hard decisions.

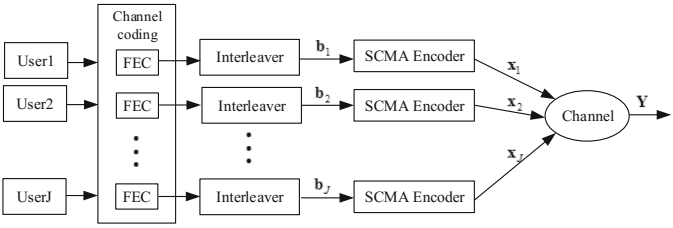


Fig. 1. SCMA transmitter structure

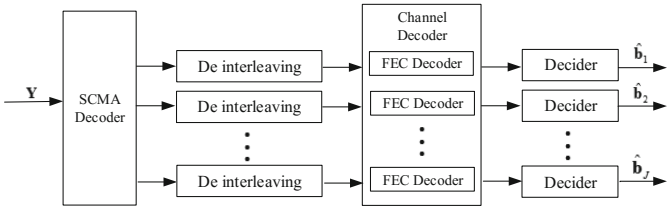


Fig. 2. SCMA receiver structure

SCMA Encoder. The SCMA encoder maps the interleaved binary bits to a multi-layer constellation symbol and then scatters the constellation point symbols on different subcarriers. In this paper, $\mathbf{B}$ and $\mathbf{C}$ denote sets of binary and complex numbers respectively. The map from binary bits to K-dimensional complex codebook can be expressed as $f : \mathbf{B}^{\log_2 M} \rightarrow \mathbf{C}^K$, where M is the number of constellation points, and K is the number of orthogonal subcarriers. The SCMA system allocates subcarriers for the user according to the allocation matrix $\mathbf{F}$ The row index k and the colomn index i of the matrix represent subcarrier k and user i respectively. If the element $(\mathbf{F})_{kj}$ in the matrix is 1, that means the subcarrier k is assigned to the user j. The matrix $\mathbf{F}$ below express a system which allocates 4 subcarriers to 6 users and each user occupies 2 subcarriers.

$$\mathbf{F} = \begin{bmatrix} 1\,1\,1\,0\,0\,0 \\ 1\,0\,0\,1\,1\,0 \\ 0\,1\,0\,1\,0\,1 \\ 0\,0\,1\,0\,1\,1 \end{bmatrix} \tag{1}$$

Signal Transmission Model. The signals of the J users are multiplexed to K orthogonal subcarriers. At the receiver, the attenuation signal of different users after channel transmission are superimposed on the subcarriers Therefore, the received symbol can be expressed as

$$\mathbf{y} = \sum\nolimits_{j=1}^{J} \mathrm{diag}(\mathbf{h}_j)\mathbf{x}_j + \mathbf{n}, \tag{2}$$

where $\mathbf{h}_j = (h_{1j}, h_{2j}, \ldots, h_{Kj})^T$ is the channel parameters vector of user j, indicating signal attenuation during transmission, $\mathbf{x}_j = (x_{1j}, x_{2j}, \ldots, x_{Kj})^T$ is SCMA codebook of the user j, and $\mathbf{n}$ is white noise, complying with Gaussian distribution in the complex domain.

SCMA Multiuser Detection. The optimal detection can be achieved by the maximum a posteriori probability (MAP) algorithm. The codeword matrix of each user is expressed as $\mathbf{X}_j = (x_1, x_2, \ldots, x_J)^T$ The estimated value of $\mathbf{X}$ is expressed as

$$\hat{\mathbf{X}} = \arg\max_{\mathbf{X} \in M^J} p(\mathbf{X}|\mathbf{y}) \tag{3}$$

Considering the complexity of detection, we transform the equation above into a marginal probability distribution problem and get the following equation

$$\hat{\mathbf{x}}_j = \arg\max_{a \in M} \sum_{\substack{\mathbf{X} \in M^J \\ \mathbf{X}_j = a}} P(\mathbf{X}|\mathbf{y}) \tag{4}$$

In the downlink, the number of system users is huge, and the amount of computation is so large that it is impossible to implement for a receiver. Therefore, multi-user detection based on factor graph is used to reduce the receiver computation complexity.

2.2 Classical Detection Algorithm

In the factor graph every circle represents a user (variable node) and every block represents a tone (function nodes), the factor graph represents system includes 6 users and 4 carriers is shown in Fig. 4. There are loops in the factor graph, which causing none of the line can be calculated first. The message passing algorithm (MPA) is applied for multi-user detection. The MPA algorithm decomposes the complex multi-user signal detection process into a number of relatively simple iterative steps, which are iteratively updated on the basis of probability information.

Each user and each subcarrier can be represented as a variable node (VN) and a function node (FN) respectively. Message transfer using a parallel mechanism, in each iteration process, all the function nodes and variable nodes are all parallel processing and delivery the messages (Fig. 3).

MPA iteratively updates the probability associated with the edges in the factor graph by passing the extrinsic information between VNs and FNs.

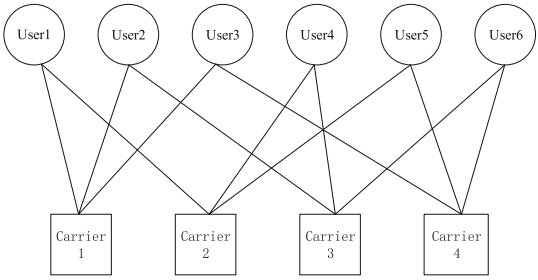


Fig. 3. SCMA system factor graph

First, initialize all variable nodes. Then, update the function node and variable node. The received signal for every VN is combined with the extrinsic information passed by the FN through the remainder of the edges connected to the FN. The passed message from FN to VN can be expressed as

$$\mu_{f_k \to V_m}(x_m) = \sum_{\sim\{x_m\}} \left\{ f_k(\{V_n = x_n\}_{V_n \in N(f_k)}) \prod_{V_n \in N(f_k)\backslash\{V_m\}} \mu_{V_n \to f_k}(x_n) \right\} \tag{5}$$

The prior information for every VN is combined with the extrinsic information passed by FN through the remainder of the edges connected to the VN. The passed message from VN to FN can be expressed as

$$\mu_{V_n \to f_l}(x_n) = \prod_{f_k \in N(V_n)\backslash\{f_l\}} \{\mu_{f_k \to V_n}(x_n)\} \tag{6}$$

Finally, after a few iterations, the probability message converges to the reliable value and the marginal probability of the variable can be expressed as

$$g_{V_n}(x_n) = \mu_{f_k \to V_n}(x_n) \times \mu_{V_n \to f_k}(x_n) \tag{7}$$

3 MPA Algorithm Performance Analysis and Enhance

3.1 Analyze the Performance of MPA Algorithm with Extrinsic Information Transfer (EXIT) Chart

The message passed between the VNs and FNs increases under the iterative process, and its own information is fed back as a priori information of the next iteration, so the independence of the message and the improvement in decoding performance is affected. Therefore, it is important to research the convergence of MPA algorithm.

From the system point of view, the iterative decoder can be regarded as a dynamic system. As an efficient tool for analyzing the convergence of iterative

decoding system, EXIT chart analysing the convergence based on mutual information. The SCMA receiver consists of the function node decoder (FND) and the variable node decoder (VND) [9], and the EXIT chart technology can be used to analyze the convergence of detection algorithm [10].

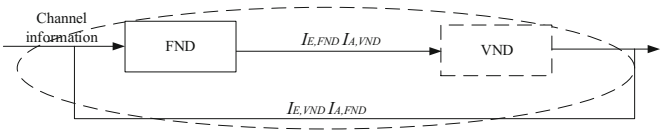


Fig. 4. SCMA detector structure

SCMA detector structure is shown in Fig. 4. In the multi-user detection process of the SCMA system, the prior information of a component detector is obtained from the extrinsic information of the other component detector, and the extrinsic information of the detector is independent of each other.

The relationship between the discrete input and output signals in the Gaussian white noise channel is shown in the following equation,

$$a = b + n \tag{8}$$

where b is the input signal, n is a Gauss noise with a mean value of 0 and an variance of δ^2. z is the output signal of the channel (only consider additive noise). The conditional probability function under the Gaussian noise channel can be expressed as

$$p(z|\mathbf{b} = b) = \frac{e^{-\frac{(z-b)^2}{2\delta^2}}}{\sqrt{2\pi}\delta_n} \tag{9}$$

The symbol b represents the random data information with a discrete value of 1 or 0. Thus, the log likelihood ratio of the transmitted data can be expressed as

$$Z = \ln \frac{p(z|b = 0)}{p(z|b = 1)} \tag{10}$$

We represent the prior information and the output information as mutual information. $I(X, Y)$ represents the mutual information between the variables X and Y. Variable X represents the signal sent by the SCMA system, and Y is the logarithmic likelihood of variable X. $I(X, Y)$ can be expressed as

$$I(X, Y) = H(X) - H(X|Y) \tag{11}$$

where the source entropy $H(X)$ represents the uncertainty of X, and $H(X|Y)$ represents the uncertainty of X under the condition that variable Y have been known. According to the derivation of probability relation, $I(X, Y)$ can be expressed as

$$I(X; Y) = \sum_{x,y} p(x, y) \log(\frac{p(y|x)}{p(y)}) \tag{12}$$

The value of variable X is 0 or 1, and Y is a continuous random variable, so $p(y)$ can be expressed as

$$p(y) = 1/2[p(y|x=0) + p(y|x=1)] \tag{13}$$

The mutual information between the transmitted data and the priori information of the component detector can be expressed as

$$\begin{aligned} I_A(X;Y) =& \frac{1}{2} \sum_{x=0,1} \int_{-\infty}^{+\infty} p_A(y|X=x) \\ & \log_2\left(\frac{2 \times p_A(y|X=x)}{p_A(y|X=0) + p_A(y|X=1)}\right) dy \end{aligned} \tag{14}$$

where factor p represents probability distribution.

Under the condition of BPSK modulation, p follows the Gaussian distribution, however, for the case of multi-modulation, there is no general conclusion. In the SCMA system, the constellation mapping based on the codebook design is various because of the change of the codebook, so it is complicated to obtain the probability distribution by the formula expression. In this case, the probability distribution is obtained by the way of Monte Carlo simulation and histogram statistics approximately.

Similar to the expression of $I_A(X;Y)$, $I_E(X;Y)$ can be expressed as

$$\begin{aligned} I_E(X;Y) =& \frac{1}{2} \sum_{x=0,1} \int_{-\infty}^{+\infty} p_E(y|X=x) \\ & \log_2\left(\frac{2 \times p_E(y|X=x)}{p_E(y|X=0) + p_E(y|X=1)}\right) dy \end{aligned} \tag{15}$$

Then the EXIT chart of the SCMA detector can be simulated.

3.2 Serial Message Pass Algorithm Based on Fairness

Message Update Based on Codeword Probability. Each iteration of the parallel MPA algorithm, all FNs update the message in parallel at the same time first, and then all VNs update the message simultaneously. The multi-user detection algorithm based on a parallel strategy whose updated message is passed to the corresponding variable node or function node at the beginning of the next iteration can't deliver the updated message immediately.

In addition, the algorithm requires large-capacity registers to store intermediate variables for parallel processing. Serial MPA algorithm based on fairness improves the convergence performance and save hardware resources.

According to the previous introduction to the MPA algorithm, the probability of outputting the codeword after t iterations can be expressed as

$$g^t(v_i) = \mu^t_{V_i \to f_j}(x_i) \times \mu^t_{f_j \to V_i}(x_i) \tag{16}$$

We can use $Q^t_{V_i}(x_i)$ and $\mu^t_{f_j \to V_i}(x_i)$ to calculate $\mu^t_{V_i \to f_j}(x_i)$ based on the above formula.

$$\mu^t_{V_i \to f_j}(x_i) = \frac{g^t(x_i)}{\mu^t_{f_j \to V_i}(x_i)} \tag{17}$$

The variable node update can be integrated into the function node update to calculate the marginal probability of the variable and save part of the intermediate variable storage space.

In serial MPA message delivery, as long as the function node information $\mu^t_{f_j \to V_i}(x_i)$ is updated, the probability information $g^{t-1}(x_i)$ of the corresponding user output codeword is updated immediately. $g^{t-1}(x_i)^{old}$ and $g^{t-1}(x_i)^{new}$ represent the probability information that before and after message update respectively. In addition, $g^{t-1}(x_i)^{new}$ is more accurate obviously. Then variable node update can be expressed as

$$\mu^t_{V_i \to f_j}(x_i) = \frac{g^{t-1}(x_i)^{new}}{\mu^{t-1}_{f_j \to V_i}(x_i)} \tag{18}$$

Based on the above discussion and the Eq. 15, the function node update of the serial MPA multiuser detection algorithm can be expressed as

$$\begin{aligned} \mu^t_{f_i \to V_i}(x_i) = \sum_{\sim v_i} \Bigg\{ & \frac{1}{\sqrt{2\pi}\delta} \exp\left(\frac{-1}{N_{0,n}} \| y_j - \sum_{x \in \xi_j} h_{j,x} v_{j,x} \|^2\right) \\ & \frac{Q^{t-1}(x_k)^{new}}{\mu^{t-1}_{f_j \to V_k}(x_i)} \prod_{l \in \xi_j / \{i,k\}} \frac{Q^{t-1}(x_k)^{old}}{\mu^{t-1}_{f_j \to V_l}(x_l)} \Bigg\} \end{aligned} \tag{19}$$

where ξ_j represents the set of users associated with the kth resource block, i and j represent the user in the set.

Serial Message Update Based on Fairness. The reliability of the function node update $\mu^t_{f_j \to V_i}(x_i)$ determines the accuracy of the codeword probability $g^t(x_i)$ that the detector calculates.

If the message $\mu_{V_i \to f_l}(v_i)$ passed from the VN to the FN is calculated based on the message $\mu_{f_k \to V_i}(v_i)$ that has been updated in this iteration we consider the message $\mu_{V_i \to f_l}(v_i)$ on the branch of the factor graph is credible and define it as credible branch. The function node update message $\mu^t_{f_j \to V_i}(v_i)$ is more accurate if the FN connects with more numbers of credible branches.

Because the serial MPA algorithm updates the message asynchronously, the further back function node update message is the more reliable. Serial message update based on fairness ensures uniform distribution of credible branches associated with each function node so that users' message in the system can be decoded fairly. The algorithm is expressed as Algorithm 1.

Algorithm 1. Serial message pass algorithm based on fairness

Require: y, H, δ^2, t_{max}

intialization:

for i=1,2,$\cdots$,J and i=1,2,$\cdots$,I **do**

  $g(x_i) = 1/M, \mu^0_{f_j \to V_i}(x_i) = 1/M$

end for

message update:

while $t \le t_{max}$ **do**

  for $j = 1, 2, \cdots, J$ **do**

    $M^j_{all}(x_i) = \prod_{i \in \xi_j} \frac{g^{t-1}(x_i)}{\mu^{t-1}_{f_j \to V_i}(x_i)}$

    for $i = 1, 2, \cdots, I$ **do**

      if $i \in \xi_j$ **then**

        $M^j_{temp}(x_i) = \frac{g^{t-1}(x_i)}{\mu^{t-1}_{f_j \to V_i}(x_i)}$

        $\mu^t_{f_j \to V_i}(x_i) = \sum_{\sim v_i} \left\{ \frac{1}{\sqrt{2\pi}\delta} \exp(-\frac{1}{2\delta^2} \left\| y_j - \sum_{v \in \xi_j} h_{j,v} x_{j,v} \right\|^2) \frac{M^j_{all}(x_i)}{M^j_{temp}(x_i)} \right\}$

        $g^{t-1}(x_i) = M^j_{temp}(v_i) \mu^t_{f_j \to V_i}(x_i)$

        $M^j_{all}(v_i) = \prod_{i \in \xi_j} \frac{g^{t-1}(x_i)}{\mu^{t-1}_{f_j \to V_i}(x_i)}$

      end if

    end for

  end for

  t=t+1

end while

for i= 1, 2, $\cdots$,I **do**

  $g(x_i) = \prod_{j \in \xi_i} \mu^{t_{max}}_{f_j \to V_i}(x_i)$

end for

Ensure: $g(x_i)$

4 Simulation Results and Analysis

4.1 Extrinsic Information Transfer (EXIT) Chart Simulation

We simulate the two component detector EXIT curve, and choose one to reversal the vertical and horizontal axis. Then, put the two simulation curve into a chart to analyse.

An EXIT chart example is shown in Fig. 5. The amount of mutual information transferred between the two component detectors varies with the direction of the arrow poles when the component detector iterative detection and decoding.

The space between the two curves is called the decoding space. The larger the space between the two curves, the less the number of iterations required for the algorithm convergence. The closer the intersection of the two curves get to one, the more accurate the iterative algorithm is.

The degrees of variable nodes in SCMA system factor graph represents the number of carriers that users multiplex. The three curves in Fig. 6 represent the

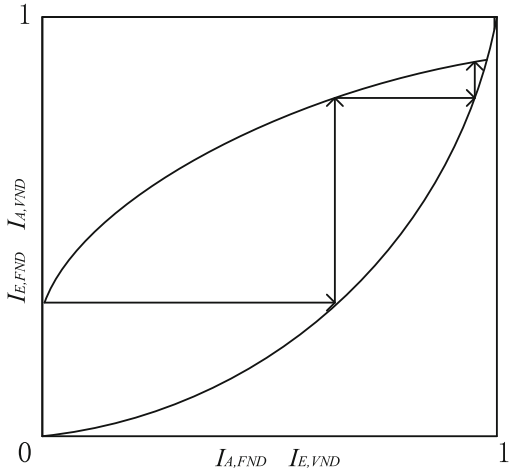


Fig. 5. EXIT chart example

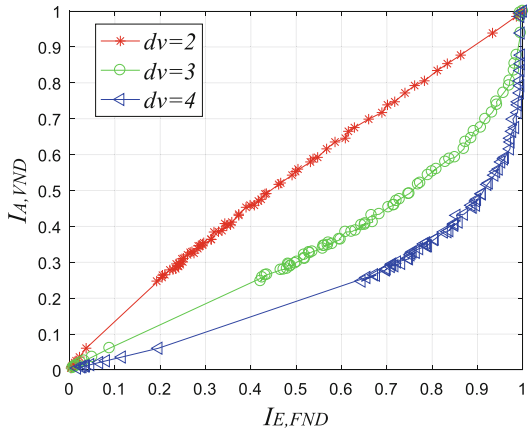


Fig. 6. The EXIT curve of the variable node

variable node EXIT curves when variable node degree is 2, 3 or 4 respectively. As the degree of variable node increases, the EXIT curve is closer to the horizontal axis and the decoding space is larger. Therefore, as the number of user multiplex resources increases, the iterative detection algorithm converges faster and gets better bit error rate performance. However, the system overload rate and the system capacity is reduce as user multiplex resources increases.

The EXIT chart of SCMA system under different SNR is shown as Fig. 7. It can be seen from the figure that the two component decoders can obtain new message through the iterations between the two component decoders, and the output information of the component decoders is more accurate. The iterations are stopped when the two component detector EXIT curves intersect.

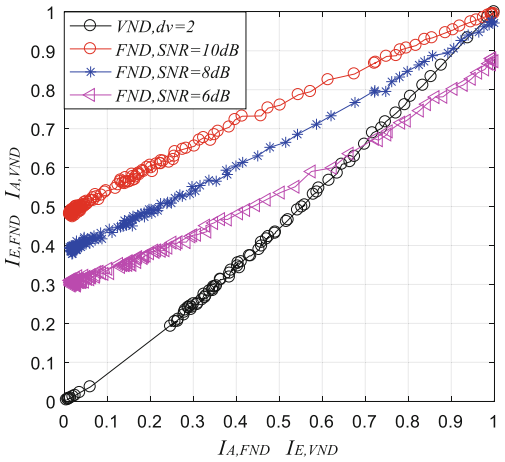


Fig. 7. The EXIT chart of SCMA system

Through the simulation results, we can find that the EXIT curves of the two component detectors have an intersection when using the MPA algorithm for multiuser detection in the SCMA system under different SNR. Therefore, we can use the EXIT chart to prove that MPA algorithm is convergent in the SCMA multi-user detection. The mutual information at the intersection of two EXIT curves in the simulation diagram increases as the SNR becomers higher, and the performance of the MPA algorithm is better correspondingly. The mutual information value is small at the intersection of two EXIT curves in the low SNR condition and therefore MPA algorithm can not converge to the exact value. The intersection coordinate of the EXIT curves in the chart is almost equal to one, the space between the two curves is wide and the decoding space is large in the condition that SNR is over 10 dB.

Therefore, MPA algorithm performances well in the high SNR condition and it isn't suitable for low SNR SCMA system.

4.2 Serial Message Pass Algorithm Based on Fairness

The SCMA system uses 16-point codebook mapping and then modulated signals are transmitted over Gaussian channels. Finally, BCJR algorithm is applied for decoding [11].

The convergence performance of the two algorithm that serial MPA based on fairness and original MPA algorithm are shown in Fig. 8. The serial MPA based on fainess converges only after 4 iterations, while the parallel MPA must iterate more than 10 times before it completely convergent.

Therefore, the algorithm that we propose reduces the number of iterations significantly, improves the convergence performance of the algorithm, and reduces the computational complexity of the system.

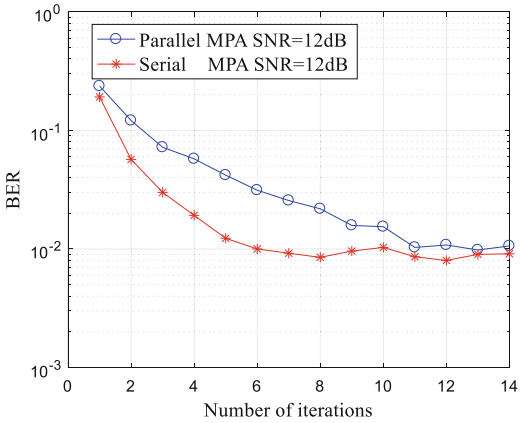


Fig. 8. The algorithm convergence performance comparison

5 Conclusion

In the paper, we use the extrinsic information transfer chart (EXIT chart) to analyze MPA detection performance. In the SCMA system, the constellation mapping based on the codebook design is various, so it is too complicated to obtain the probability distribution by mathematical formula derivation. Through the EXIT chart that we simulate, it is easy to analysis the MPA algorithm performance in SCMA detection system and come to the conclusion that MPA algorithm is not apply to the low SNR condition. Furthermore, we present serial MPA algorithm based on fairness to improve the convergence performance of original MPA algorithm and reduces the computational complexity of the detection system.

References

1. Agyapong, P.K., Iwamura, M., Staehle, D., Kiess, W., Benjebbour, A.: Design considerations for a 5G network architecture. IEEE Commun. Mag. **52**(11), 65–75 (2014)
2. Nikopour, H., Baligh, H.: Sparse code multiple access. In: IEEE 24th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), pp. 332–336. IEEE, London, UK (2013)
3. Ren, B., Han, S., Meng, W., Li, C., Wu, X.: Enhanced turbo detection for SCMA based on information reliability. In: 2015 IEEE/CIC International Conference on Communications in China, Shenzhen, China, November 2015
4. Prasad, R., Ruggieri, M.: Technology Trends in Wireless Communications. Artech House, Norwood (2003)
5. Weingarten, H., Steinberg, Y., Shamai, S.: The capacity region of the Gaussian multiple-input multiple-output broadcast channel. IEEE Trans. Inf. Theory **52**(9), 3936–3964 (2006)

6. Wei, D., Han, Y., Zhang, S., Liu, L.: Weighted message passing algorithm for SCMA. In: 2015 International Conference on Wireless Communications and Signal Processing (WCSP), Nanjing, pp. 1–5 (2015)
7. Bayesteh, A., Yi, E., Nikopour, H., Baligh, H.: Blind detection of SCMA for uplink grant-free multiple-access. In: 11th International Symposium on Wireless Communications Systems (ISWCS), Barcelona, pp. 853–857 (2014)
8. Ashikhmin, A., Kramer, G., ten Brink, S.: Extrinsic information transfer functions: model and erasure channel properties. IEEE Trans. Inf. Theory **50**(11), 2657–2673 (2004)
9. Du, Y., Dong, B., Wang, X., Dang, G., Gao, P.: Multiuser detection scheme for SCMA systems based on serial strategy. J. Electron. Inf. Technol. **38**(8), 1–6 (2016)
10. Wang, X., Du, Y., Cheng, C., Gao, P., Dong, B.: Convergence property analysis for multiuser detection schemes in SCMA systems based on EXIT chart. J. Sig. Process. **32**(12), 1440–1445 (2016)
11. Tuchler, M., Singer, A.C.: Turbo equalization, an overview. IEEE Trans. Inf. Theory **57**(2), 920–952 (2011)

WSNs and VANETs

Cluster-Based Cooperative Data Service for VANETs

Yongyue Shi[1,2], Xiao-hong Peng[2], Hang Shen[1], and Guangwei Bai[1(✉)]

[1] Department of Computer Science and Technology, Nanjing Tech University, Nanjing, China
{hshen,bai}@njtech.edu.cn

[2] School of Engineering and Applied Science, Aston University, Birmingham, UK
{shiy9,x-h.peng}@aston.ac.uk

Abstract. Vehicular Ad-hoc Network (VANET) plays an important role in improving traffic safety and efficiency. Vehicles with sensors on board can collect traffic and environmental information of their driving areas and, meanwhile, they also want to achieve a similar type of information for their interested regions. This paper establishes a data service model to facilitate information exchanges within a vehicular network, where both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications are involved. A new clustering algorithm which considers the mobility and the driving behavior is proposed in this model to enhance service efficiency and success rate. The performance of this model is evaluated through simulation.

Keywords: Cluster · V2X communications · Vehicular network

1 Introduction

In recent years, with the rapid development of Smart Cities and Intelligent Transportation Systems (ITS) [1], a new and modern transportation paradigm is formed aiming to make traveling on the road safer, more efficient and comfortable. The Vehicular Ad-hoc Network (VANET), extended from the Mobile Ad-hoc Network (MANET), is designed to improve the quality of experience for both drivers and passengers. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications (together abbreviated as V2X) are two main communications modes in VANETs. The roadside unit (RSU) is a stationary server installed along the road to provide information services via V2I communications.

The traffic and environmental information differs in different areas but remains largely unchanged within a shorter range of traveling distance. Therefore, collecting the local data and exchanging with RSUs to learn other traffic areas across vehicular networks help drivers learn about the real-time traffic/environmental information ahead, and is an effective solution for reducing road congestion and improving the driving experience. The Dedicated Short Range Communications (DSRC) scheme has been developed to support both V2V and V2I communications (together as V2X).

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 119–129, 2018.
https://doi.org/10.1007/978-3-319-90802-1_10

In general, the 5.9 GHz DSRC refers to a suite of standards for Wireless Access in Vehicular Environments (WAVE) [2], which include IEEE 802.11p, IEEE 1609.1/.2/.3/.4 protocols and the SAE J2735 message set dictionary. The high mobility of vehicles in addition to a large number of transmission terminals in an ad-hoc network presents a great challenge in V2X communications, in terms of high likelihood of congestion in data delivery and exchange in this environment.

This challenge can be addressed by the clustering method in V2X approaches. A VANET model with clusters (circled) is illustrated in Fig. 1, showing information exchanges between cluster heads and RSUs. The clustering method simplifies the data transmission structure in a complex network and increases the capacity of a system as it can better utilize the resources available. A cluster-based data service model via cooperative transmission in V2X is proposed in this paper, which includes both local information collection/submission and data downloading from RSU. We will show that the combined clustering and V2X methods can outperform the conventional schemes without using clusters, in terms of the service delivery efficiency.

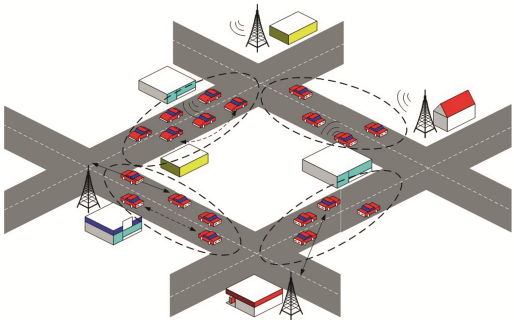


Fig. 1. A VANET model with clusters.

The rest of the paper is organized as follows. Section 2 introduces the related work in V2X communications and cluster-based dissemination methods. Section 3 presents the new clustering algorithm and Sect. 4 describes the proposed data service model. Section 5 provides simulation results and performance analysis. Finally, the paper is concluded in Sect. 6.

2 Related Work

There have been many research works dedicated to the performance improvement of vehicular communications. In V2V communications, adaptive data dissemination methods are used in vehicular networks with different densities [3], to reduce the retransmission times efficiently, with the help of a store and forward function. The idea of cooperation is to combine V2V with V2I, such as in a typical scenario [4] where the RSU provides services to passing vehicles via V2I communications and any vehicle is able to share its cached data with neighboring vehicles via V2V communications.

Network coding is also applied in this work to increase transmission efficiency, but its evaluation ignores the latency caused by the failed services.

In [5], more RSUs are considered to broadcast messages timely. Vehicles within the coverage of RSUs will receive the information seamlessly via the V2I mode and those which outside this transmission distance forward the information via V2V. The key point here is to decide the handover mechanism for ensuring stable connections.

The Lowest-ID clustering algorithm is used to select the cluster head (CH) based on the fixed ID number of each vehicle within the communication range [6]. This algorithm is not suitable in VANET due to high mobility and restricted routes for vehicles. A three-layer CH selection algorithm is proposed for multimedia services in a VANET [7], where clusters are formed based on the interest preferences of vehicle passengers. This scheme, however, cannot achieve a high efficiency when the requirements in the operation differ too much.

3 Clustering Algorithm

In a MANET, CHs can be selected by considering the position, neighbors, mobility, and battery power of the nodes in the network, and applying an algorithm called "combined weight" [8]. But in VANETs, the factors to consider are different due to the high mobility and the road structures, so we propose a new clustering algorithm which applies a new weighting method, which is more dedicated to VANETs.

There are three types of the nodes (vehicles) in a VANET: free node (FN), cluster head (CH), and cluster member (CM). The clustering algorithm considers only the one-hop neighbors of each node, the cluster size is decided by the number of CH's neighbors. The factors that could affect the selection of CH include position, velocity, connectivity and driving behavior.

The position of each node is obtained from GPS devices. The average distance between CH and CM should be short to keep CH close to the center of a cluster. The average relative distance between a node n_i and its neighbors, P_i, is given by:

$$P_i = \frac{1}{n} \sum_{j=1}^{n} \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2} \tag{1}$$

where n is the number of neighbors of node n_i, and x and y are coordinate values of two involved nodes.

The velocity of CH should be close to the average velocity of the cluster, so it can represent the cluster's mobility for building stable connections with its members. The stability, V_i, is represented by the difference between the velocity of a candidate node v_j and the average velocity of the traffic flow, i.e.:

$$V_i = \left| v_i - \frac{1}{n} \sum_{j=1}^{n} v_j \right| \tag{2}$$

where v_j is the velocity of the j-th neighbour of n_i.

Each node can have a different number of neighbors, denoted by N_i, reflecting the connectivity of n_i. The ideal connectivity is defined as λ, which represents the maximum number of neighboring nodes within one hop without causing traffic congestion, and is given by:

$$\lambda = 2R_t \times 133 \times n_l / 1000 \tag{3}$$

where R_t is the transmission range, n_l is the number of lanes. The value 133 represents the highest possible density (vehicles/(lane·km) [9]. The actual connectivity denoted as C_i, is then given by:

$$C_i = \left| N_i - \lambda \right| \tag{4}$$

The last factor involved is driving behavior, which shows how stable a vehicle is when running along the road in terms of the average acceleration of the vehicle a_i. The driving behavior denoted as D_i is then defined as:

$$D_i = \left| a_i \right| \tag{5}$$

These four factors are considered to have the same influence on the CH selection, so the final weighting metric W_i should be the sum of all normalized P_i, V_i, C_i and D_i:

$$W_i = P_i' + V_i' + C_i' + D_i' \tag{6}$$

$$P_i' = \frac{P_i}{P_{\max i}},\ V_i' = \frac{V_i}{V_{\max}},\ C_i' = \frac{C_i}{\sigma},\ D_i' = \frac{D_i}{D_{\max i}} \tag{7}$$

where P_{max} is the distance between the i-th vehicle and the farthest vehicle from it, V_{max} is the speed limitation by traffic rules that a vehicle can reach in the flow, D_{max} is the maximum absolute value of acceleration the vehicle can reach when it is running. A smaller W_i indicates higher suitability for the CH.

4 Cluster-Based Service Model

The proposed system model is a combination of both V2V and V2I. RSUs are located in different sections of a road and share a database server in the back-end as shown in Fig. 2. Vehicles act as nodes in the VANET concerned.

The database server stores the traffic and environmental information of different regions and is updated by each RSU periodically for the traffic situations, weather conditions and road status, etc. Vehicles are grouped into clusters to collect information and request for services. CH is selected to collect and aggregate information from cluster members (CMs) and disseminate service packets to CMs after receiving data from RSUs. Only CH can directly communicate with RSUs.

To reduce the transmission overhead, CH does not keep the list of its members, every CM stores the CH's ID to identify its cluster. When CH broadcasts the service packets,

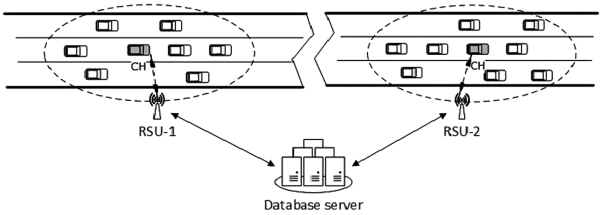


Fig. 2. Cluster-based service model.

the CMs who have the same CH ID and the targeted service ID will receive the service packets.

The system follows the standards of IEEE 802.11p, which specify 7 channels with 10 MHz bandwidth, including one control channel for exchanging control messages and safety information, and 6 service channels for delivering service data.

This system model enables real-time information sharing and reduces energy consumption because it shifts a significant amount of transmissions from V2I to V2V thanks to the cluster approach adopted. Only RSUs need to communicate with CHs, resulting in reduced transmission collision and energy consumption as well.

The whole cluster-based service model includes three main subsystems for data management, cluster operation, and service delivery, as described below.

4.1 Data Management Subsystem

4.1.1 Packets Classification

- Vehicle information packet (VIP): It carries the basic vehicle information: vehicle ID, velocity, position, etc.
- Cluster Head Announcement (CHA): CHA is broadcast by a node with a weight low enough to be a CH.
- Cluster Head Maintain (CHM): A node with the smallest W_i is selected as CH, and it then sends CHM to all its neighbours to declare its identity (CH ID).
- Service Data Packet (SDP): It consists the head (CH ID, packet ID, sender ID and time stamp.) and context (actual data to transmit).

4.1.2 Data Integration

The traffic/environmental information includes the average speed of the current flow, position, weather and traffic conditions, which is obtained by collecting relevant data from onboard sensors. The collected information is aggregated by CH as it has both universality and particularity. Each RSU maintains a database to store the service information collected from CHs and will also periodically update information from other servers. This information service helps drivers to choose better routes and avoid congestions and accidents. They can also be aware of the travel time they will spend.

4.2 Cluster Operation Subsystem

4.2.1 Cluster Forming

Any node whose status is free node (FN) can start the cluster forming process by sending out VIP, based on which each node can calculate its weight W_i. If a node achieves a smaller W_i than the weight threshold, $W_{Threshold}$ (i.e. $W_i < W_{Threshold}$), it will send CHA to neighbors to announce that. Any node that receives the CHA will compare the weight (W_i) with its own and send another CHA to argue if it has a smaller W_i. Otherwise, the node will keep waiting for CHM from others to confirm the CH ID. After sending a CHA, if a node has not received any argument after a threshold window T_w, it sends CHM to declare its identity as CH of its neighbors. Every node which receives this CHM will mark the CH ID as its head ID. If a node receives another CHM shortly after the one from the first CH, it would decide the new CH by comparing their weights.

4.2.2 Cluster Maintaining

As CH does not keep the list of its members, it detects the W_i periodically to maintain the CH status: if there are no obvious changes of its acceleration and $W_i < W_{Threhold}$ still stands, it resends its CHM to confirm its CH ID; otherwise, it sends VIP to start a new cluster forming process and changes its status as FN.

When a node becomes a CM, it stores the ID of the current CH. If it keeps overhearing CHM from the same CH, no changes will be made. If CM continuously overhears two CHMs from another CH, it changes its CH ID and becomes a member of a new cluster. If CM overhears no CHM after a threshold, it would switch to FN and sends out VIP.

4.3 Service Delivery Subsystem

Vehicles on the road may have different regions of interest and tend to learn the environmental and traffic conditions in those regions in advance. They also collect current traffic information from their onboard sensors and are responsible for reporting the information with a high priority (e.g. an accident) to its CH.

Each vehicle generates request packets containing the vehicle ID, request ID and region ID. Every CM sets the receiver ID as the CH ID and submits the requests along with the emergent information (if it has) to CH and then waits for service delivery. On receiving the packets, CH integrates the collected information and forward it all together with the requests of CMs to RSU.

When receiving the SDP packet from CH, RSU updates the database with the collected information and sends the service packets requested to CH. CH will continuously broadcast each service packet to its members. Upon overhearing the relative ID for its request, CM will save the packet and the request is satisfied. If CM still cannot obtain the service data after a waiting time period, this request is failed and after checking its cluster status this CM will send a request to CH again.

In this paper, the following three metrics are applied to evaluate the performance of the proposed system.

- Service ratio (γ). It is the ratio of the number of successful delivered requests n_s to the total number of requested services n, to evaluate the effectiveness of the V2X system, which is given by:

$$\gamma = \frac{n_s}{n} \tag{8}$$

- Average service delay (τ). It is defined as the average duration from a vehicle submitting a service request to it finally receiving the service packets, i.e.:

$$\tau = \frac{\sum_{i=1}^{n_s} t_{si} + n_{us} \cdot t_p}{n_s} \tag{9}$$

where t_{si} is the time duration of the i-th successful service transmission, n_{us} is the number of unsuccessful service requests, and t_p is the waiting time a vehicle spends for the service which is not delivered.

- Throughput (η). It is a widely applied metric to evaluate the transmission efficiency of a system, defined as the average size of data successfully delivered over a unit time.

$$\eta = \frac{p_s}{T} \tag{10}$$

where p_s is the total size of delivered service packets, T is the total service time.

5 Simulation and Results Analysis

5.1 Simulation Setup

The traffic scenario in this paper is set to be a single direction road with three lanes as is shown in Fig. 2. The average velocity of each lane is set as 60 km/h, 80 km/h and 100 km/h, respectively. Based on the Greenshield's Model in traffic flow theory [10], the velocity and the density of vehicles are linearly related to the condition of uninterrupted traffic flow, i.e.:

$$v = v_f - \frac{v_f}{d_c} \cdot d \tag{11}$$

where v and d are the velocity and density of vehicles, respectively. v_f is the maximum velocity a vehicle can reach in a lane, d_c is the traffic density under congested, which is 133 vehicles/(lane·km) as mentioned in Sect. 3. For different flow velocities, the distribution of vehicle density of each lane is shown in Fig. 3, from which six driving scenarios are designed with data entered in Table 1.

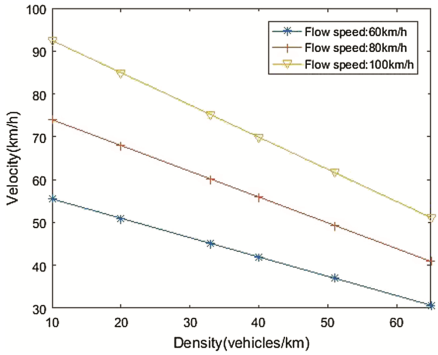


Fig. 3. Relation between velocity and density with different flow speeds.

Table 1. Density and velocity for each lane

Scenario		Average velocity (km/h)	Average density (vehicles/km)
1	Lane1	55.49	11.08
	Lane2	73.98	11.63
	Lane3	92.48	10.64
2	Lane1	50.98	22.17
	Lane2	67.97	21.61
	Lane3	84.96	21.28
3	Lane1	45.11	33.25
	Lane2	60.15	32.23
	Lane3	75.18	33.30
4	Lane1	41.95	42.12
	Lane2	55.93	41.56
	Lane3	69.92	41.23
5	Lane1	36.99	53.20
	Lane2	49.32	51.53
	Lane3	61.65	51.87
6	Lane1	30.67	66.50
	Lane2	40.90	65.03
	Lane3	51.12	48.21

The communication model is based on DSRC and the parameters of PHY layer and MAC layer are configured according to IEEE 802.11p. It operates in the 5.9 GHz band, there are one 10 MHz control channel and four 10 MHz service channels involved in this model. The transmission range is 300 m for vehicles and 600 m for RSU. Each message is 500 bits. Every vehicle randomly generates up to 7 to 12 requests and submits to the CH when entering the transmission range of the RSU.

The control group model which has no clusters is set in the simulation for the purpose of comparison with the proposed model, as shown in Fig. 4. The vehicles in the communication range of an RSU directly sends requests and information collected to RSU and wait for service packets. The RSU updates the traffic information to the database servers.

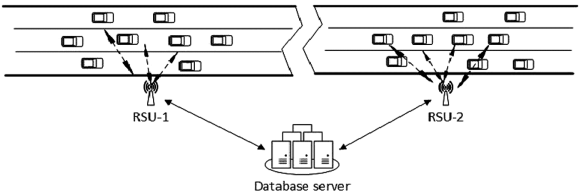


Fig. 4. Control group model.

5.2 Results Analysis

Figure 5 shows the service ratio of two different models (with and without clusters), for 6 different scenarios listed in Table 1. As we can see, the clustered system has achieved much higher and more stable service ratio than the control group in all scenarios. With clusters, the number of transmission links between vehicles and the RSU (V2I) is much reduced, resulting in much less collision than the control group. In the scenarios with higher vehicle densities, more requests are generated, and more communications process lead to the decrease of the service ratio in the control groups. However, the proposed model decreases the collision in V2I, while the cost in V2V among vehicles is much less than it in V2I as well, so the service ratio remains relatively stable. In addition, CH stores the service data, so it can serve the CMs even after they have left the coverage of the RSU as long as they are in the same cluster.

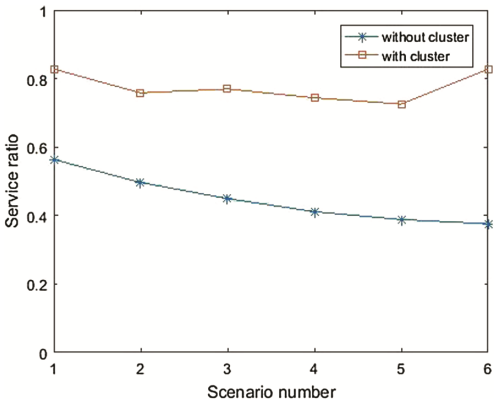


Fig. 5. Service ratio under different scenarios.

The average service delay of the two models under different scenarios is shown in Fig. 6. The delay consists of two parts: one is the time spent on delivering service data,

and the other is the time spent on waiting for retransmitting the requested service due to the failed previous transmission. The RSU in the control group serves requests from all vehicles, so there is a higher probability of collision than the clustered model, hence the higher number of unsuccessful services n_{us}. In the cluster-based approach, only CH involves direct communication with RSU, which is the main reason for low latency in its V2I communications. In addition, vehicles in the same cluster requesting the same service can be served concurrently through broadcasting by CH.

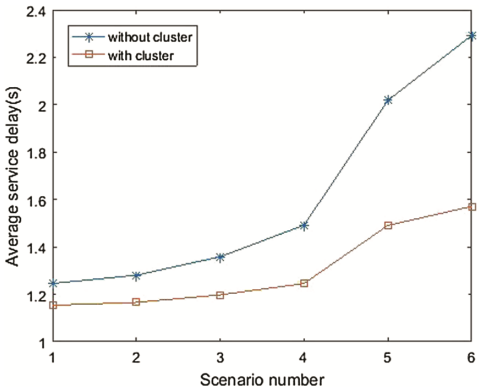


Fig. 6. Average service delay under different scenarios.

Figure 7 shows that the clustered system clearly outperforms the system without clusters in throughput for all scenarios. With the increase of vehicle densities, the transmission efficiency is affected in both groups, but the clustered model exhibits better performance than the non-clustered model in general. This is because the former can handle more requests in the same transmission duration and has fewer collisions in each cluster.

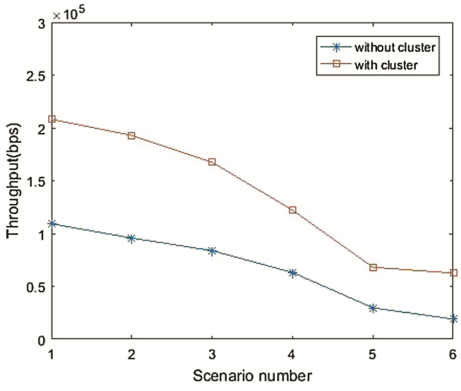


Fig. 7. Throughput under different scenarios.

6 Conclusion

In this paper, a cluster-based traffic/environmental information service model in VANETs has been proposed. The model covers the forming and maintaining of clusters and the service delivery through cluster-based V2X. The clustering and CH selection processes are based on the mobility of vehicles to ensure the stability and efficiency of data exchange and service delivery. As only CHs are responsible for direct communication with the RSU and disseminating service data to other vehicles in the network, the cluster-based V2X model presented in this work can significantly enhance service delivery efficiency through reducing transmission congestion and the average service delay. Simulation results have demonstrated a substantial performance improvement of this approach, compared to the conventional schemes without using clusters. The new evaluation metrics used in this work have also produced more realistic and accurate results for performance assessment.

Acknowledgement. The authors gratefully acknowledge the support and financial assistance provided by the National Natural Science Foundation of China under Grant Nos. 61502230 and 61073197, the Natural Science Foundation of Jiangsu Province under Grant No. BK20150960, the Natural Science Foundation of the Jiangsu Higher Education Institutions of China under Grant No. 15KJB520015.

References

1. Kumar, V., Mishra, S., Chand, N.: Applications of VANETs: present & future. Commun. Netw. **5**, 12 (2013)
2. Consortium, D.I.: DSRC technology and the DSRC industry consortium (DIC) prototype team. White Paper. Technical report (2005)
3. Leal, M.A., Röckl, M., Kloiber, B., de Ponte Müller, F., Strang, T.: Information-centric opportunistic data dissemination in vehicular Ad Hoc networks. In: Proceedings of 13th International IEEE Conference on Intelligent Transportation Systems, pp. 1072–1078 (2010)
4. Liu, K., Ng, J.K.-Y., Wang, J., Lee, V.C., Wu, W., Son, S.H.: Network-coding-assisted data dissemination via cooperative vehicle-to-vehicle/-infrastructure communications. IEEE Trans. Intell. Transp. Syst. **17**, 1509–1520 (2016)
5. Wang, Q., Fan, P., Letaief, K.B.: On the joint V2I and V2 V scheduling for cooperative VANETs with network coding. IEEE Trans. Veh. Technol. **61**, 62–73 (2012)
6. Jiang, M., Li, J., Tay, Y.: Cluster based routing protocol (CBRP). Draft-ietf-manet-cbrp-spec-01, txt, Internet Draft, IETF (1999)
7. Tal, I., Muntean, G.-M.: User-oriented cluster-based solution for multimedia content delivery over VANETs. In: Proceedings of IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), pp. 1–5 (2012)
8. Chatterjee, M., Das, S.K., Turgut, D.: WCA: a weighted clustering algorithm for mobile ad hoc networks. Cluster Comput. **5**, 193–204 (2002)
9. Artimy, M.M., Robertson, W., Phillips, W.J.: Connectivity in inter-vehicle ad hoc networks. In: Proceedings of Canadian Conference on Electrical and Computer Engineering, pp. 293–298 (2004)
10. Kuhne, R.D.: Foundations of Traffic Flow Theory I: Greenshields' Legacy-highway traffic. In: Symposium on the Fundamental Diagram: 75 Years (Greenshields 75 Symposium) (2008)

An Energy-Aware On-Demand Multicast Routing Protocol for Wireless Ad Hoc and Sensor Networks

Xiaoyao Huang and Baoxian Zhang(✉)

Research Center of Ubiquitous Sensor Networks,
University of Chinese Academy of Sciences, Beijing 100049, China
huangxiaoyao15@mails.ucas.edu.cn, bxzhang@ucas.ac.cn

Abstract. Energy efficient multicast is a crucial issue in wireless ad hoc and sensor networks. In this paper, we propose an energy-aware on-demand multicast routing protocol EAP, which is aimed to achieve reduced energy consumption and thus prolonged network lifetime. In EAP, adaptive power control and residual energy balancing are applied in an on-demand way for supporting energy efficient multicast routing. Accordingly, multicast trees are built with appropriate power threshold adjustment according to most recent route discovery history and further energy critical nodes are discouraged from serving as relay nodes in the multicast trees. Simulation results show that our protocol can obtain high performance with little overhead as compared with existing work.

Keywords: Energy-efficient multicast · On-demand routing · Network lifetime maximization

1 Introduction

Multicast is an important communication paradigm in wireless multihop network such as wireless ad hoc and sensor networks and it works to disseminate data from one source node to multiple multicast destinations simultaneously. Owning to its wide applications, multicast routing has become a hot research topic in wireless multi-hop networks. However, how to optimize the energy usage and accordingly maximally prolong the lifetime of wireless multi-hop networks is still a challenging issue [1, 2].

One major design objective of multicast routing is to maximize the network lifetime by constructing efficient multicast forwarding structures while minimizing the total power for delivering multicast packets on such structures. However, it has been proved that optimal multicast routing in a wireless multihop network is in general an NP-hard problem [3]. Accordingly, much work had been carried out to design efficient multicast routing heuristics. In addition, scalability is also a big concern to be considered when

This work was supported partially by the National Natural Science Foundation of China under grants 61471339, 61531006, 61173158.

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 130–139, 2018.
https://doi.org/10.1007/978-3-319-90802-1_11

providing multicasting services in wireless ad hoc network due to the highly dynamic nature of such networks.

In this paper, we propose an energy-aware on-demand multicast routing protocol, referred to as EAP. The design objective is to achieve improved energy use efficiency and thus prolonged network lifetime in wireless multihop networks. For this purpose, EAP mainly combines two routing strategies, namely, adaptive power threshold adjustment and residual energy balancing with energy-critical node avoidance. Adaptive power threshold adjustment is to restrict the longest link (i.e., the link with maximum power as determined by a given power threshold) during the construction of a multicast tree so as to greatly reduce the total power of such a tree. Nodes in the network also adaptively adjust their power threshold values based on most recent witnessed route discovery success/failure history in order to improve the quality of constructed multicast trees. Regarding residual energy balancing, energy critical nodes are discouraged from serving as relay nodes in a multicast tree by introducing different deferring times at different nodes in an on-demand tree construction process. For this purpose, we introduce simple but efficient strategy for nodes in the network to easily determine whether they are energy critical nodes or not based on the current energy distribution status at nodes in the network. EAP works in an on-demand manner for multicast tree construction and it does not require any geographical information in such process. We present detailed protocol design description of EAP. Simulation results show that EAP can achieve significantly prolonged network lifetime as compared with existing work.

The rest of this paper is organized as follows. In Sect. 2, we briefly review related work. Section 3 proposes our energy efficient multicast routing protocol. In Sect. 4, we conduct extensive simulations to evaluate performance of the proposed protocol by comparing it with existing work. In Sect. 5, we conclude this paper.

2 Related Work

Energy-aware multicasting in wireless ad hoc and sensor networks has been a hot topic in recent years and much work has been carried out in this area. Typically, there are mainly two classes of energy-aware multicast routing protocols: minimum power routing and maximum lifetime routing.

Finding a multicast tree with minimal power while covering all group members in a wireless multihop network had been proved to be NP-hard. Heuristic solutions for this purpose work to build a near-minimum power multicast tree. In [4], near-minimum power multicast trees are established by using global network state and multicast group-specific information. Different from the strategy in previous work like [4], different strategies were considered to minimize the energy for the tree constructions in different scenarios. In [5], the authors considered selection of appropriate forwarding nodes and also intelligent schedule of the transmission of the forwarding nodes to cover the receiving nodes with a minimum number of transmissions in duty-cycled wireless sensor networks. In [6], the authors granted the cognitive ability to each node so that each of them can obtain the minimum transmission power by sensing, acting, and deciding. Das et al. exploited fuzzy logic to choose the path with minimum energy consumption of

nodes [7]. The above protocols focuses on minimizing the total power for each multicast packet delivery while lack of consideration on energy balancing which can hurt the network lifetime.

The main idea of maximum lifetime routing is to balance the residual energy of the nodes in the network when conducting multicasting in such networks. BMT [8] modifies the relaxation operation and takes lifetime as the weight to build a multicast tree. Damdinsuren et al. [9] proposed the sharing-residual-energy-information method to extend the network lifetime. Paper [10] used network coding to improve the maximum lifetime in lossy wireless networks with AWGN channel and Rayleigh fading channel. Zhu and Shen used the particle swarm optimization to establish a delay constrained maximum lifetime multicast tree in the wireless ad hoc networks with directional antennas [11]. The algorithms mentioned above need global network state information which makes them have the scalability issue. In addition, overly pursuing of energy consumption balancing may cause excessive energy consumption at some nodes in the network, which in return hurts network lifetime.

3 Proposed Protocol

In this section, we propose our protocol EAP in detail. EAP is designed to achieve energy-efficient multicast routing for long network lifetime and low energy draining while incurring little overhead for multicast tree constructions. For this purpose, EAP incorporates two strategies: adaptive power threshold adjustment and residual energy balancing. Adaptive power threshold adjustment works to restrict the longest link (i.e., the link with the maximum link power as determined by pre-determined power threshold) in a multicast tree in order to support low-power multicast in networks wherein nodes can adaptively adjust their transmission powers depending on the transmission ranges. The purpose of introducing residual energy balancing is to discourage energy-critical nodes from serving as relay nodes on a multicast tree, whenever possible. The nodes falling into the energy critical range (or called energy protection range) are those nodes whose residual energy are lower than the current residual energy threshold. These two strategies will be described in details in the following subsections.

3.1 Adaptive Power Control

In this paper, we adopt the following power model for determining the transmission power for successful transmission between neighbor nodes. Specifically, the transmission power with distance d from a sender to destination receiver can be modeled as follows:

$$P(d) = kd^{\alpha} + c. \tag{1}$$

where k and c are constants and the value of α is typically between 2 and 4 based on radio propagation environment. Obviously, according to this power model, low-power routing prefers those paths consisting of more short links other than those paths

consisting of less long-haul links. The property also holds in power-efficient multicast as we study in this paper when building power-efficient multicast trees.

The procedure of the adaptive power threshold adjustment is partially borrowed from [12] and it was originally designed for power efficient unicast routing. Here, we modify it to support power-efficient multicast, which works as follows. The source node initiates the routing discovery by flooding a route request (RREQ) packet across the network, which carries a common transmission power value P_1 ($0 < P_1 < P_{max}$). P_1 is the initial power threshold as decided by the source for the route discovery and it can be updated when appropriate. Upon receiving a non-duplicate RREQ, an intermediate node u forwards it further by using the pre-determined common power level P_1 that the RREQ carries and records the node from which receiving the RREQ as the last hop. If a multicast destination receives such a RREQ, it sends a route reply (RREP) back to the source. When the number of replies collected equals the multicast group size G, a multicast tree is established successfully and the source can send multicast traffic downstream along the tree. However, if timed out and the number of replies is still smaller than G, the source will increase the power threshold by a certain amount and start another route discovery process. This process continues until the multicast tree is established successfully or reply number is still smaller than G even after increasing the common transmission power to P_{max}.

3.2 Residual Energy Balancing

Residual energy balancing works in the following way. Based on the membership status, nodes in the network can be divided into two types: group member and non-group member. Based on their residual energy amount, they can also be divided into two types: Energy-critical nodes (i.e., their residual energy are below the current energy protection threshold E_k) and energy-abundant nodes (i.e., their residual energy is above E_k). The energy protection threshold E_k is determined by using a given protection range β ($0 < \beta < 1$). For example, suppose $\beta = 20\%$ and the residual energy of nodes in the network ranges from E_{min} to E_{max}, the protocol is expected to protect 20% of nodes with the lowest residual energy and we have:

$$E_k = E_{min} + \beta \times \left(E_{max} - E_{min}\right).$$

In this paper, node energy is divided into L discrete levels to reduce the communication overhead. Let E_i denote the residual energy of node i and let L_i denote the residual energy level of node i. Then we have $L_i = L \times E_i / E_{max}$. Initially, all nodes in the network broadcast their energy levels across the network and E_k can be computed after receiving all nodes' energy levels. As the network keeps running and nodes in the network keep burning their energy, nodes' residual energy levels drop with time. In this case, as long as a node detects its current residual energy level is below the "known lowest residual energy level" in the network, it will broadcast its current residual energy level across the network to let other nodes in the network to learn the decrease of the "known lowest residual energy level." In this case, each node in the network can easily determine whether the node itself is in the energy protection range or not. During an on demand

routing process, different nodes shall be assigned different deferring times for further retransmitting a received RREQ packet according to their membership types and also their residual energy statuses. The purpose of this operation is to enable RREQs taking good routes to travel fast.

During the routing discovery process, when an intermediate node i receives a RREQ for the first time, it records the node from which it receives the RREQ as its last hop, sets its local deferring time according to its role in the network and forwards it when its deferring timer expires. The deferring time length at a node i is set as follows:

$$\text{RREQDelay}(i) = \begin{cases} random(0, T) + LPT_i & (i \text{ is a group member node}) \\ \min(Extrahop \times T, MAXT) + random(0, T) + LPT_i & (\text{otherwise}) \end{cases}. \quad (2)$$

In (2), T is the time unit. In addition, $random(0, T)$ returns a random value in the range of $(0, T)$ and it is introduced to avoid collision caused by the simultaneous transmission attempts of neighbor nodes. *ExtraHop* refers to the hop that the RREQ is away from the source or last group member encountered and it is introduced to recruit as few non-group members into the multicast tree as possible. *MAXT* is to control the maximum extra deferring time at non-group member nodes so as to control the worst-case path acquisition latency. *LPT* is a variable introduced to discourage energy critical node to join the tree as relay node. *LPT* is computed as follows, where E_i is the residual energy of node i:

$$LPT_i = \begin{cases} \max(2^{\frac{E_{max}}{E_i}} \times T, 8T) & if\ E_i < E_k \\ 0 & (otherwise) \end{cases}. \quad (3)$$

In this way, the possibility that energy critical nodes and non-member nodes join the multicast tree as relay nodes is greatly reduced, which is expected to be helpful for prolonging the network lifetime and also reducing total power consumption.

3.3 Detailed Protocol Design

EAP combines the above two strategies into the on-demand multicast tree constructions and the protocol design details are as follows.

All nodes in the network have two thresholds: power threshold and energy protection threshold. The initial power threshold at each node can be set to the maximum power (i.e., P_{max}) and can be adjusted based on the most recent success/failure of route discovery using different power thresholds as the node witnessed. Energy protection threshold E_k is determined as mentioned in the preceding subsection and will be updated as each node's residual energy keeps dropping. Moreover, the RREQ-deferring times at different nodes in the network are calculated by using Eq. (2).

When a source node s wants to initiate a multicast transmission, it first conducts a route discovery process by broadcasting a RREQ with the common transmission power P_s (the power threshold of source s) in the network. For an intermediate node receiving the RREQ for the first time, it will forward the RREQ with the common transmission power when its local deferring timer as calculated by using (2) expires. Duplicate RREQs

will be directly dropped without further processing. When the RREQ reaches a multicast destination, a route reply (RREP) will be sent back to the source along the reverse path. If the number of RREPs that the source collects in certain time equals the multicast group size G, the multicast tree is built successfully. Otherwise, the source s will increase its power threshold by a certain amount ΔP and initiates another route discovery process by carrying this updated power threshold value. The above process will be repeated until all multicast destinations are reached so that the tree construction is successful or no sufficient number of RREPs collected even after increasing P_s to P_{max}, which means failure of the route discovery process.

It is worth noting that the nodes overhearing the routing process will adjust their power threshold adaptively. For an arbitrary node u in the network, if it overhears a RREQ from source s in the kth route searching round, this process denoted as EAP(s, k), without hearing any RREQ $\in$ EAP(s, $k + 1$) which means success of EAP(s, k) for route discovery. In this case, u can adjust its power based on the overheard knowledge: If $P_u < P_s$, u will increase P_u by an amount of ΔP; Else, we have $P_u > P_s$, in this case, u will decrease P_u by an amount of $\Delta P'$ to approach P_s. This adaptive power threshold adjustment is to achieve a good tradeoff between route acquisition latency and path quality in terms of power consumption.

4 Simulation Results

In this section, we conduct simulations to evaluate the performance of the designed protocols by using a discrete-event simulator developed using C++. In the simulations, hundreds of connected topologies are generated randomly. Each result reported in the simulation figures is the average of different tests. Nodes are uniformly distributed in a 1000 m × 1000 m square area. For each multicast request, its source and multicast destinations are chosen randomly. The packet generating rate from the multicast source is 8 packets/s and the source continues sending 100 data packets for each request. Once a multicast session is over, a new multicast session will be generated randomly. The battery capacity E_{max} is set to 200 J and the residual energy range [0, E_{max}] is equally divided into 20 levels. The MAC layer is assumed ideal which can guarantee packet delivery without loss. The transmission power of each node is normalized over the max transmission power. The simulation parameters used are listed in Table 1.

Table 1. Simulation parameters.

Parameters	Values
Network deployment area	1000 m × 1000 m
Network size	100
Nodes' initial residual energy range	100–200 J
Maximum transmission distance	250 m
Transmission power adjust range	0–1 w
Data packet size	512 byte
Data rate	2 Mbps

In the simulations, we realized the following four protocols: EAP, EAP-E, EAP-P, and SRT. EAP-E implements the residual energy balancing part in EAP without considering the power control part (i.e., maximum transmit power is always used in both route discovery and data packet transmission), EAP-P implements the adaptive power control part in EAP without considering residual energy at nodes, and SRT works to build a multicast tree, which minimizes the sum of reciprocal of nodal residual energy from the multicast source to each group member during the multicast tree establishing process. All these protocols work in an on-demand manner for tree construction. In EAMRP and APCRP, the power increment Δp is set to $\frac{1}{8}$ and the power decrement $\Delta p'$ is set to $\frac{1}{16}$. These settings for adjusting power threshold values are to accelerate routing convergence with certain penalty in path quality. We mainly focus on two metrics: network lifetime and the energy consumed per multicast session. The lifetime of a network is measured as the duration until a first node run out of its energy.

4.1 Energy Protection Range Determining

The energy protection proportion β has a big impact on the performance of EAP and EAP-E. Figure 1 plots the network lifetime of EAP with different β values. In this test, the network size was fixed to 100 and the multicast group size was fixed to 15. In Fig. 1, it is seen that when the energy protection ratio is too low or too high, the network lifetime will both be short. That is because both cases cause too few nodes being protected (for the former case) or too few nodes serving as protectors for relaying (for the latter case), which hurt the performance of energy protection routing. In Fig. 1, the network lifetime reaches its peak when $\beta = 0.2$.

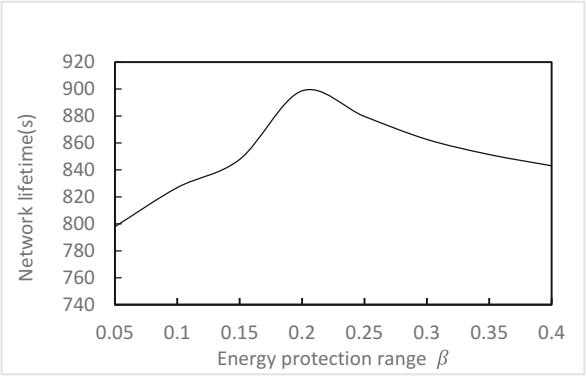


Fig. 1. Network lifetime with varying energy protection range β.

4.2 Searching Rounds in EAP

The average number of searching rounds required for a routing acquisition is illustrated in Fig. 2. In this test, the network size and energy protection proportion ratio are 100 and 0.15, respectively. We can see that with the increasing of multicast group size,

average number of searching rounds per route acquisition increases and the result lies between 1 and 2. That is because as multicast group size increases, the possibility at which a source reaches all the multicast destinations with the adjust power decreases so more searching rounds may be triggered.

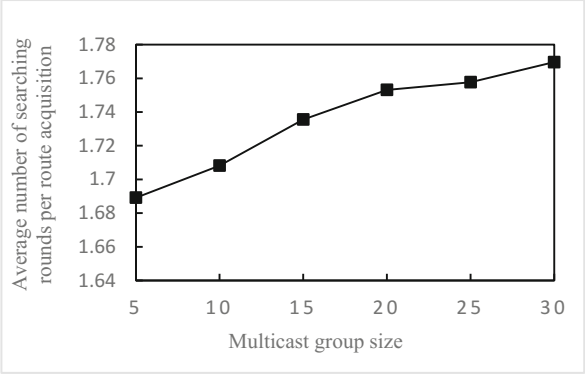


Fig. 2. Average number of searching rounds per route acquisition versus multicast group size.

4.3 Performance Comparison

In this experiment, we conduct simulations to observe the routing performance with varying multicast group size. Energy protection range and network size were fixed to 0.15 and 100, respectively. The multicast group size varies from 5 to 30 with step size 5. The simulation results are shown in Figs. 3 and 4. In Fig. 3, it is seen that network lifetime decreases as multicast group size increasing because larger group size leads to larger multicast tree, which will consume more energy per multicast packet delivery thus resulting in a shorter lifetime. The same reason applies to Fig. 4, where energy consumption increases with the increase of multicast group size. By comparison, we find that EAP performs the best in terms of network lifetime and it outperforms EAP-E

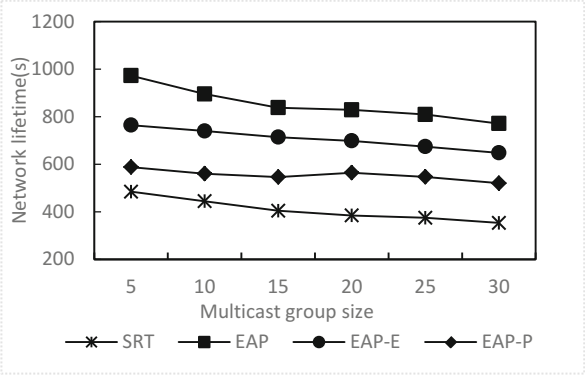


Fig. 3. Network lifetime by different algorithms/protocols versus multicast group size.

by 13–17% in terms of network lifetime while consuming almost the same amount of energy as compared with EAP-P.

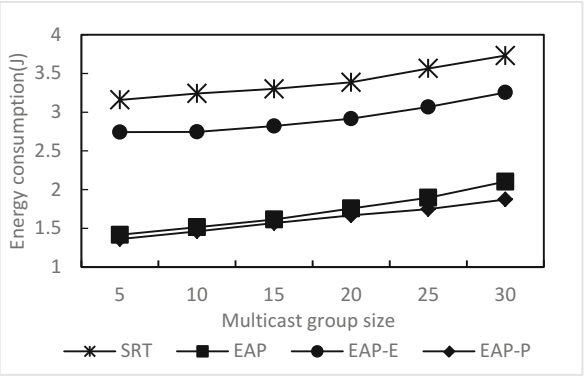


Fig. 4. Average energy consumption by different protocols per multicast packet versus multicast group size.

5 Conclusion

In this paper, we proposed an energy-aware on-demand multicast routing protocol EAP for wireless ad hoc and sensor networks wherein nodes are able to adjust their transmission powers according to communication ranges. EAP jointly considers minimized energy consumption and maximized network lifetime in its implementation. In EAP, nodes adaptively adjust their powers to achieve low power trees and discourage energy critical nodes from serving as relay nodes in a multicast tree. EAP is simple and requires neither local nor global status information. It incurs little overhead for multicast tree construction. Simulation results show that EAP can greatly prolong the network lifetime and reduce the energy consumption to a large extent as compared with existing work.

References

1. Floreen, P., Kaski, P., Kohonen, J., Orponen, P.: Lifetime maximization for multicasting in energy-constrained wireless networks. IEEE J. Sel. Areas Commun. **23**, 117–126 (2005)
2. Guo, S., Guo, M., Leung, V.: Exploring the multicast lifetime capacity of WANETs with directional multibeam antennas. In: IEEE INFOCOM 2009, pp. 2686–2690. IEEE Press, Rio de Janeiro (2009)
3. Ruiz, P.M., Gomez-Skarmeta, A.F.: Approximating optimal multicast trees in wireless multihop networks. In: 10th IEEE Symposium on Computers and Communications, ISCC 2005, pp. 686–691. IEEE Press, Murcia (2005)
4. Wieselthier, J.E., Nguyen, G.D., Ephremides, A.: Energy-efficient broadcast and multicast trees in wireless networks. Mob. Netw. Appl. **7**, 481–492 (2002)
5. Han, K., Liu, Y., Luo, J.: Duty-cycle-aware minimum-energy multicasting in wireless sensor networks. IEEE/ACM Trans. Netw. **21**, 910–923 (2013)

6. Jiang, D., Xu, Z., Lv, Z.: A multicast delivery approach with minimum energy consumption for wireless multi-hop networks. Telecommun. Syst. **62**, 771–782 (2016)
7. Das, S.K., Tripathi, S., Burnwal, A.P.: Fuzzy based energy efficient multicast routing for ad-hoc network. In: Third International Conference on Computer, Communication, Control and Information Technology, pp. 1–5. IEEE Press, Hooghly (2015)
8. Georgiadis, L.: Bottleneck multicast trees in linear time. IEEE Commun. Lett. **7**, 564–566 (2003)
9. Damdinsuren, C., Kominami, D., Sugano, M., Murata, M., Hatauchi, T.: Lifetime extension based on residual energy for receiver-driven multi-hop wireless network. Clust. Comput. **16**, 469–480 (2013)
10. Li, P., Guo, S., Leung, V.C.M.: Maximum-lifetime coding tree for multicast in lossy wireless networks. IEEE Wirel. Commun. Lett. **2**, 295–298 (2013)
11. Zhu, X., Shen, J.: Delay constrained maximum lifetime multicast based on particle swarm optimization in wireless ad hoc networks with directional antennas. In: 11th IEEE International Conference on Networking, Sensing and Control, pp. 255–260. IEEE Press, Miami (2014)
12. Zhang, B., Mouftah, H.T.: Energy-aware on-demand routing protocols for wireless ad hoc networks. Wirel. Netw. **12**, 481–494 (2016)

Energy Consumption of Polar Codes for Wireless Sensor Networks

Liping Li[1(✉)], Quanyv Wang[1], Yanjun Hu[1], and Chuan Zhang[2]

[1] Key Laboratory of Intelligent Computing and Signal Processing of the Ministry of Education of China, Anhui University, Hefei, China
liping_li@ahu.edu.cn

[2] National Mobile Communications Research Laboratory, Southeast University, Nanjing, China
chzhang@seu.edu.cn

Abstract. Internet of Things (IoT) is becoming a strong force driving the evolution of mobile communications. Wireless sensor networks (WSN) are important parts of IoT. Link reliability and power consumption are two critical design constraints in WSN designs. Error control coding (ECC) is a classic approach to increase link reliability and thus to lower the required transmitting power, however typically at the cost of an increased decoding complexity and power. The idea of this paper is to assess the potentials of applying polar codes to WSNs. For comparison, the well developed Turbo and LDPC codes are studied in terms of the error performance and the power consumption. The results in this paper show that when the ratio of the transmitting power over the decoding power is smaller than 2.5, applying polar codes is favorable in terms of the power consumption compared with Turbo and LDPC codes at the same BER performance. When this ratio is larger than 2.5, polar codes are almost the same as Turbo and LDPC codes in terms of the energy consumption.

Keywords: Internet of Things (IoT) · Error control codes
Polar codes · LDPC codes · Turbo codes · Energy consumption

1 Introduction

Four typical technical scenarios of 5G are derived from the main application scenarios, service requirements, and key challenges of mobile internet and Internet of Things (IoT) [1]. Wireless sensor networks (WSNs) are important parts of IoT. The most significant challenge in sensor networks is to overcome the energy constraints since sensor nodes typically have limited power.

In WSNs, to increase the link reliability, Automatic Repeat reQuest (ARQ) can be deployed when errors occur. However, energy is wasted due to the retransmission in the network. A particularly undesirable situation occurs when the channel condition is bad, causing successive retransmissions. Forward error correction (FEC) [2] is an effective way to reduce the frame error rate and consequently reduce the number of retransmissions.

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 140–149, 2018.
https://doi.org/10.1007/978-3-319-90802-1_12

Block codes and convolutional codes with Viterbi decoding are applied to WSNs in [3–8]. Iterative decoding algorithm justifies the ability of Turbo codes in solving the hot-spot problem and prolong the network lifetime [6]. Previous work using error control coding (ECC) in wireless sensor networks focused primarily on codes such as Reed-Solomon and convolutional codes. A hybrid scheme choosing the energy-efficient combination of ECC and ARQ is considered in [7]. Convolutional codes with different rates and constraint lengths are studied in [8] for wireless microsensor networks. Other system-level techniques such as modulation and MAC protocols are also considered to reduce the energy consumption in [8].

The aforementioned coding scheme indeed can increase link reliability and lower the required transmitting power. However, extra power consumption of decoders can not be neglected especially with sparse capacity-approaching codes [6,9]. It's shown in [9] that the transmitted power for short distances is only a few tens of the decoding power. Therefore, a coding scheme which can increase the link reliability but also consumes an acceptable level of decoding power is desired.

The discovery of channel polarization and polar codes by Arıkan [10] is universally recognized as a major breakthrough in coding theory. Polar codes provably achieve the capacity of binary-input discrete memoryless symmetric (B-DMS) channels, with a low encoding and decoding complexity. Moreover, polar codes have an explicit construction (there is no random ensemble to choose from) and a beautiful recursive structure that makes them inherently suitable for efficient implementation in hardware [11]. Therefore, in this paper, polar codes are studied when applied in WSNs. The focus of this paper is to qualify the ability of polar codes in increasing the link reliability while maintaining a low decoding power consumption. In this respect, two other codes are studied along with polar codes for comparison: Turbo codes [12] and LDPC codes [13,14]. As mentioned in [9], the decoding power is dominating the processing power at the chip. A fair comparison is carried out in this paper by forcing the three coding schemes having the same bit-error-rate (BER) performance, which results in different transmitting power requirements for Tubo, LDPC, and polar codes. The decoding power of these codes are multiples of the transmitting power [9] depending on the distance of communications and the specific system parameters: center frequency, bandwidth, and throughput. From simulations of a simple WSN network with 100 nodes, the life time of the WSN network is found to be the longest when applying polar codes and the ratio of the transmitting power over the decoding power is smaller than 2.5.

The rest of the paper is organized as follows. Section 2 introduces the basics of polar codes. Section 3 discusses the energy model used in this paper. Section 4 provides the BER performance and power consumption of several error correction codes. Finally the conclusion remarks are provided at the end.

2 Polar Codes Basics

In this section, the relevant theories of non-systematic polar codes and systematic polar codes are presented based on [10,15].

2.1 Non-systematic Polar Codes

Polar codes presented in [10] are in the non-systematic form. The generator matrix is $G_N = BF^{\otimes n}$ where B is a bit-reversal matrix, $F = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, $n = \log_2 N$, and $F^{\otimes n}$ is the nth Kronecker power of the matrix F over the binary field $\mathbb{F}_2$.

Throughout the paper, we use u_1^N to refer to a row vector with N elements: $v_1^N = (v_1, v_2, \ldots, v_N)$. Let $\mathcal{A}$ denote a set. Then $u_{\mathcal{A}}$ is a subvector of u_1^N with elements specified by $\mathcal{A}$. With these notations, the encoding of polar codes is: $x_1^N = u_1^N G_N$. Here the source vector is u_1^N which consists of the information bits and the frozen bits, denoted by $u_{\mathcal{A}}$ and $u_{\bar{\mathcal{A}}}$, respectively. The frozen bits are known to the receiver. The encoded bits in x_1^N are transmitted in N independent underlying channels. Let the underlying channel be W with a transition probability $W(x|y)$ where $x \in \mathcal{X} = \{0, 1\}$ and $y \in \mathcal{Y}$. The set $\mathcal{X}$ and $\mathcal{Y}$ contains the input and output alphabets, respectively. Note that W is a binary-input memoryless symmetric channel (B-MSC).

Transmitting the codeword x_1^N from N independent copies of W produces a vector channel:

$$W_N(y_1^N|u_1^N) = W^N(y_1^N|x_1^N) = W^N(y_1^N|u_1^N G_N) \tag{1}$$

This vector channel is split into N bit channels given by:

$$W_N^{(i)}(y_1^N, u_1^{i-1}|u_i) = \sum_{u_{i+1}^N \in \mathcal{X}^{N-i}} \frac{1}{2^{N-1}} W_N(y_1^N|u_1^N) \tag{2}$$

Polarization happens that when N is large enough, these bit channels either are noiseless, or completely noisy [10]. And the portion of the perfect bit channels is equal to the symmetric capacity of the underlying channel W.

To conclude this subsection, a note is necessary on the selection of the good bit channels in the set $\mathcal{A}$. Algorithms such as [16] can be used to sort the bit channels and the best of K bit channels can be selected when $K = NR$ (R being the code rate). Both set $\mathcal{A}$ and its complementary set $\bar{\mathcal{A}}$ are in $\{1, 2, \ldots, N\}$ for polar codes with a block length $N = 2^n$.

2.2 Construction of Systematic Polar Codes

For systematic polar codes, we also focus on a generator matrix without the permutation matrix B, namely $G = F^{\otimes n}$.

The source bits $\mathbf{u}$ can be split as $\mathbf{u} = (u_{\mathcal{A}}, u_{\bar{\mathcal{A}}})$. The first part $u_{\mathcal{A}}$ consists of user data that are free to change in each round of transmission, while the second part $u_{\bar{\mathcal{A}}}$ consists of data that are frozen at the beginning of each session and made known to the decoder. The codeword can then be expressed as

$$\mathbf{x} = u_{\mathcal{A}} G_{\mathcal{A}} + u_{\bar{\mathcal{A}}} G_{\bar{\mathcal{A}}} \tag{3}$$

where $G_{\mathcal{A}}$ is the sub-matrix of G with rows specified by the set $\mathcal{A}$. The systematic polar code is constructed by specifying a set of indices of the codeword $\mathbf{x}$ as the indices to convey the information bits. Denote this set as $\mathcal{B}$ and the complementary set as $\bar{\mathcal{B}}$. The codeword $\mathbf{x}$ is thus split as $(x_{\mathcal{B}}, x_{\bar{\mathcal{B}}})$. With some manipulations, we have

$$\begin{cases} x_{\mathcal{B}} = u_{\mathcal{A}} G_{\mathcal{A}\mathcal{B}} + u_{\bar{\mathcal{A}}} G_{\bar{\mathcal{A}}\mathcal{B}} \\ x_{\bar{\mathcal{B}}} = u_{\mathcal{A}} G_{\mathcal{A}\bar{\mathcal{B}}} + u_{\bar{\mathcal{A}}} G_{\bar{\mathcal{A}}\bar{\mathcal{B}}} \end{cases} \tag{4}$$

The matrix $G_{\mathcal{A}\mathcal{B}}$ is a sub-matrix of the generator matrix with elements $\{G_{i,j}\}_{i\in\mathcal{A}, j\in\mathcal{B}}$. Given a non-systematic encoder $(\mathcal{A}, u_{\bar{\mathcal{A}}})$, there is a systematic encoder $(\mathcal{B}, u_{\bar{\mathcal{A}}})$ which performs the mapping $x_{\mathcal{B}} \mapsto \mathbf{x} = (x_{\mathcal{B}}, x_{\bar{\mathcal{B}}})$. To realize this systematic mapping, $x_{\bar{\mathcal{B}}}$ needs to be computed for any given information bits $x_{\mathcal{B}}$. To this end, we see from (4) that $x_{\bar{\mathcal{B}}}$ can be computed if $u_{\mathcal{A}}$ is known. The vector $u_{\mathcal{A}}$ can be obtained as the following

$$u_{\mathcal{A}} = (x_{\mathcal{B}} - u_{\bar{\mathcal{A}}} G_{\bar{\mathcal{A}}\mathcal{B}})(G_{\mathcal{A}\mathcal{B}})^{-1} \tag{5}$$

From (5), it's seen that $x_{\mathcal{B}} \mapsto u_{\mathcal{A}}$ is one-to-one if $x_{\mathcal{B}}$ has the same elements as $u_{\mathcal{A}}$ and if $G_{\mathcal{A}\mathcal{B}}$ is invertible. In [15], it's shown that $\mathcal{B} = \mathcal{A}$ satisfies all these conditions in order to establish the one-to-one mapping $x_{\mathcal{B}} \mapsto u_{\mathcal{A}}$. In the rest of the paper, the systematic encoding of polar codes adopts this selection of $\mathcal{B}$ to be $\mathcal{B} = \mathcal{A}$. Therefore we can rewrite (4) as

$$\begin{cases} x_{\mathcal{A}} = u_{\mathcal{A}} G_{\mathcal{A}\mathcal{A}} + u_{\bar{\mathcal{A}}} G_{\bar{\mathcal{A}}\mathcal{A}} \\ x_{\bar{\mathcal{A}}} = u_{\mathcal{A}} G_{\mathcal{A}\bar{\mathcal{A}}} + u_{\bar{\mathcal{A}}} G_{\bar{\mathcal{A}}\bar{\mathcal{A}}} \end{cases} \tag{6}$$

3 Energy Model

In this section, the average energy consumption of Turbo codes, LDPC codes, and polar codes are analyzed. As in [9], the energy is largely divided as the transmitting power and the decoding power. Traditionally, the transmitting power dominates the link budget as communications normally travel a long distance. As the distance of communications became short and the capacity-approaching error correction codes developed, the decoding power started to dominate the processing power.

Figure 1 is a reproduction of the two cases considered in [9] where the dashed line is the decoding power of a real implementation of a LDPC decoder [17]: 144 mW. From Fig. 1 it can be seen that the transmitting power is small than the decoding power for distances within 10 m. This motivates us to investigate a general energy consumption model which is not related to any specific implementation. Instead, the ratio of the transmitting and decoding power is $\alpha = E_{tx}/E_{dec}$. We study the effect of the ratio α to the overall energy consumption in a WSN setting.

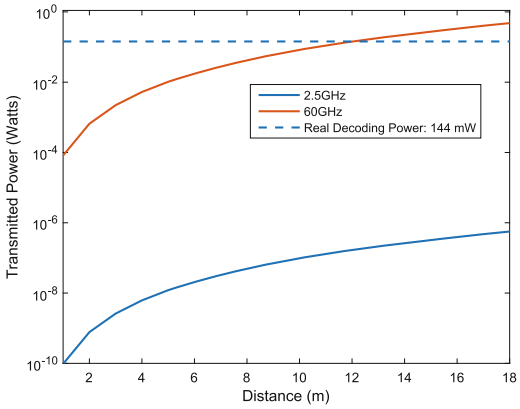


Fig. 1. Required power from Shannon prediction of two cases. Case 1 at 2.5 GHz: bandwidth is 80 MHz and the throughput is 26 MHz. Case 2 at 60 GHz: bandwidth is 3 GHz and the throughput is 1.5 GHz. The real decoding power is from [17].

3.1 General Energy Model

Suppose there are N_{total} total of nodes in a WSN, labeled from 1 to N_{total}. Since this work does not deal with routing or any other optimization related to WSNs, we assume a simple protocol: nodes 1 to N_{total} transmitting and receiving (decoding) one by one in the natural order. Each complete transmission from node 1 to node N_{total} is called one round of transmission. With such a simplification, we can evaluate how many times of runs such a network can perform and how many nodes are still alive in each run. Here we assume a complete non-heterogenous network, meaning that the nodes can have different energy levels.

Denote E^i_{total} as the total energy of node i. Suppose each time a node transmits, it transmits one second. In other words, the energy consumed by transmitting is E_{tx}. We also assume that the decoder continuously works for one second when a node performs decoding. Therefore, the total energy E^i_{total} in a node will be completely consumed after N_i times of transmitting and decoding with

$$E^i_{total} = N_i(E_{tx} + E_{dec}) \tag{7}$$

With $\alpha = E_{tx}/E_{dec}$, E^i_{total} can be written as

$$E^i_{total} = N_i(1 + \alpha)E_{dec} \tag{8}$$

3.2 Transmitting and Decoding Energy of Three Codes

In this section, based on (7) and (8), the energy consumption of three codes are analyzed and compared: LDPC codes [13,14], Turbo codes [12], and polar codes [10]. For a fair comparison, both E_{tx} and E_{dec} need to be adjusted in (7) and (8).

To achieve the same bit error rate P_b, the required signal-to-noise ratio (SNR) per bit (E_b/N_0) for different codes are different. For comparison, let $(E_b/N_0)_{ldpc}$ be the required SNR per bit for LDPC codes. Then, the required SNR per bit for polar codes and Turbo codes can be expressed as:

$$(E_b/N_0)_{turbo} = \alpha_t (E_b/N_0)_{ldpc} \tag{9}$$

$$(E_b/N_0)_{polar} = \alpha_p (E_b/N_0)_{ldpc} \tag{10}$$

Since there is no closed form expression for all three codes, the ratio α_t and α_p can only be obtained from numerical simulations for any given P_b. Once the ratio α_t and α_p are obtained, the transmitting power of polar and Turbo codes can be obtained relative to the LDPC code.

With the same block length and code rate, the decoding power of the three codes are analyzed based on the number of iterations in the decoding process. Other factors such as the decoder structure, the parallelism, and the log likelihood ratio (LLR) calculations are not considered. Suppose the number of iterations of the LDPC code is I_l. In the same way, the number of iterations of polar and Turbo codes is I_p and I_t, respectively. Let $\beta_p = I_p/I_l$ and $\beta_t = I_t/I_l$. Then the decoding power of the three codes can be expressed as:

$$(E_{dec})_{turbo} = \beta_t (E_{dec})_{ldpc} \tag{11}$$

$$(E_{dec})_{polar} = \beta_p (E_{dec})_{ldpc} \tag{12}$$

With (9)–(12), the total energy in (7) for node i can be expressed as:

$$(E^i_{total})_{turbo} = N_i(\alpha\alpha_t + \beta_t)(E_{dec})_{ldpc} \tag{13}$$

$$(E^i_{total})_{polar} = N_i(\alpha\alpha_p + \beta_p)(E_{dec})_{ldpc} \tag{14}$$

where the subscript 'turbo' means node i employing Turbo encoding and decoding and 'polar' means polar codes are employed for node i. Note that the WSN considered only employs one code type: either a Turbo code is employed for all nodes, or a LDPC code, or a polar code. Therefore, the energy consumption in (13) and (14) is the energy model for all nodes in a WSN.

4 Simulation Results

In this section, simulation results are provided to verify the performance of different ECC in WSNs. The LDPC code used in this section is constructed by the Construction 1A in [14]. The LDPC code has a block length 512 and code rate 1/2. The two generators for the rate 1/2 recursive systematic convolutional (RSC) code is: $G_1 = 13$ and $G_2 = 15$. The number of iterations in the decoding of this Turbo code is set to be $I_t = 10$. The average number of iterations in the decoding of the LDPC code is recorded in the simulation as $I_l = 5$. As for the polar code (block length 512 and code rate 1/2), since successive cancellation

(SC) [10] decoding is applied, the number of iterations in the decoding is $I_p = 1$. Therefore, the decoding power ratio is:

$$\beta_p = I_p/I_l = 1/5 \tag{15}$$

$$\beta_t = I_t/I_l = 10/5 = 2 \tag{16}$$

Note that with the previous settings of the three codes, LDPC, Turbo, and polar codes have the same code rate. This is the basis for a fair comparison among these codes in terms of the error performance and the energy consumption.

To obtain the relative transmitting power in achieving a given BER P_b, the BER performance of these codes is simulated. Figure 2 displays the BER performance in an additive white Gaussian noise (AWGN) channel. Note that in Fig. 2, the BER performance of the schemes in three short distance communication protocols are also provided. The (15, 10) shortened Hamming code is used in the BlueTooth protocol. The coding scheme of 802.11g is the convolutional code with a code rate 1/2 and a constraint length 7. Uncoded BPSK is used in the ZigBee protocol.

It can be seen from Fig. 2 that the BER performance of the coding schemes in BlueTooth and the 802.11g is worse than the coding schemes of (512, 256) polar and LDPC codes. The rate 1/2 Turbo codes has the best BER performance among the codes considered. Now let us set a target $P_b = 10^{-3}$. Then compared with the LDPC code, Turbo code needs around 0.9 dB less and polar code needs around 0.5 dB more E_b/N_0 to achieve this P_b. Therefore, the transmitting power adjustments are the following:

$$\alpha_p = (E_b/N_0)_{polar}/(E_b/N_0)_{ldpc} = 1.122 \tag{17}$$

$$\alpha_t = (E_b/N_0)_{turbo}/(E_b/N_0)_{ldpc} = 0.813 \tag{18}$$

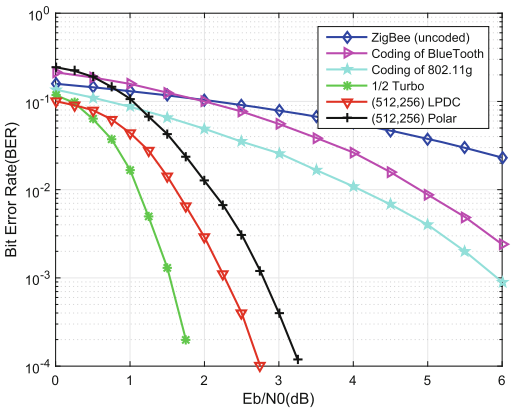


Fig. 2. The comparison of the BER performance of various codes in the AWGN channel. There is no coding in ZigBee. The code in BlueTooth is the shortened (15, 10) Hamming code. In 802.11g, the rate 1/2 convolutional code with a constraint length 7 is used. The rate 1/2 RSC Turbo code has two generators: $G_1 = 13$ and $G_2 = 15$.

With the transmitting power and the decoding power adjustments in (15)–(18), the only parameter in (13) and (14) is α, which is the ratio of the transmitting power relative to the decoding power. In the following simulations, this parameter α is set to different values to compare the energy consumption of the three coding schemes: polar code, LDPC code, and Turbo code described at the beginning of this section.

First of all, assume there are $N_{total} = 100$ nodes in the network. As discussed in Sect. 3.1, the nodes can have different energy levels. The total energy in node i is modelled as

$$E^i_{total} = 1 + e_i \quad \text{(Joules)} \tag{19}$$

where e_i is a random variable with uniform distribution. The random variables $\{e_i\}_{i=1}^{N_{total}}$ are independent. The transmission strategy described in Sect. 3.1 is used in the simulation: each node transmitting and receiving (decoding) one by one and each transmitting and decoding operation takes one second. Assume the decoding power for the LDPC code is $(E_{dec})_{ldpc} = 10^{-3}$ Watts. With the initial total energy distribution in this network, in the following operations in each second, all nodes in the network perform transmitting and decoding. As in Sect. 3.1, a complete transmission from node 1 to node $N_{total} = 100$ is one round of transmission. When the total energy E^i_{total} of node i is completely consumed from these transmitting and decoding operations, then this node dies. In each round, the total number of alive nodes are recorded for each decoding scheme.

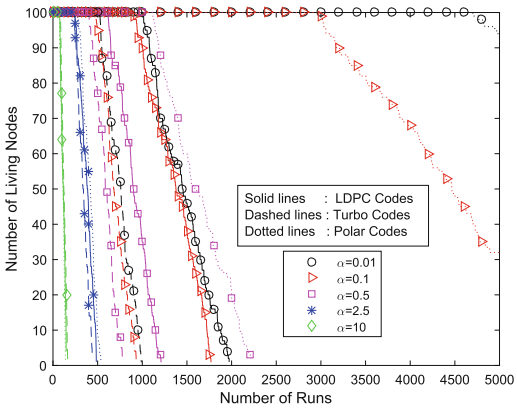


Fig. 3. Energy consumption comparison of three codes: polar code (512, 256), Turbo code, and LDPC code (512, 256). The Turbo code is rate 1/2 RSC code with $G_1 = 13$ and $G_2 = 15$. The LDPC code is constructed from Construction 1A from [14].

Figure 3 shows the energy consumption comparison of the three codes. The x-axis is the indices of the number of runs. The y-axis is the number of alive nodes in each run. For each code type, there are five curves: the solid lines are the alive nodes for the LDPC code, the dashed lines for the Turbo code,

and the dotted lines for the polar code. For each code type, the line with circles corresponds to $\alpha = 0.01$, meaning the transmitted power is only one hundredth of the decoding power. The other markers corresponds to the following: the line with triangles is for $\alpha = 0.1$, the line with squares is for $\alpha = 0.5$, the line with asterisks is for $\alpha = 2.5$, and the line with diamonds is for $\alpha = 10$.

For ease of description, a network is said to have a better energy efficiency if it has the most number of living nodes when operating with the same conditions compared with another network. From Fig. 3, it can be seen that the network employing polar code with $\alpha = 0.01$ and $\alpha = 0.1$ is very energy efficient: At runs 3000, all 100 nodes are still alive. However, all nodes are dead before run 2000 in this network employing LDPC (the solid line with circles) and Turbo codes (the dashed line with circles). At $\alpha = 0.5$, the network employing polar code displays a slightly better energy efficiency as that employing LDPC codes with $\alpha = 0.01$ $\alpha = 0.1$, which indicates that the network employing polar code can support a larger communication distance compared with that employing the LDPC code when the other parameters of the network are the same. This energy efficiency of polar code is even more pronounced when compared with the Turbo code: at $\alpha = 0.5$, the network life time with polar code is 1500 runs longer than the network employing Turbo codes.

However, when the transmitting power starts to dominate the energy consumption, all three codes converge in terms of the network lifetime. This can be seen from the three lines with asterisks (corresponding to the case of $\alpha = 2.5$) in Fig. 3. In this case, the transmitting power is 2.5 times larger than the decoding power. The networks employing polar, LDPC, and Turbo codes have almost the same energy efficiency at $\alpha = 2.5$. The same is true when $\alpha = 10$.

5 Conclusion

The use of forward error correcting codes can allow a system to operate at significantly lower SNR than an uncoded system for a given BER. But the choice of ECC is very important for a wireless sensor network. In this paper, we investigate the usage of polar codes applied in a WSN in a noisy environment. The main metric is the energy consumption when comparing polar codes with the existing capacity-achieving Turbo and LDPC codes. When the ratio of the transmitting power over the decoding power is below a threshold (in this paper, smaller than 2.5), polar codes are shown to be much energy efficient in prolonging the network lifetime compared with Turbo and LDPC codes. This shows that at low communication distances, polar codes are a very energy-efficient error correction code to be applied in WSNs.

Acknowledgement. This work was supported in part by National Natural Science Foundation of China through grant 61501002, in part by Natural Science Project of Ministry of Education of Anhui through grant KJ2015A102, in part by the Key Laboratory Project of the Key Laboratory of Intelligent Computing and Signal Processing of the Ministry of Education of China, Anhui University, in part by Talents Recruitment Program of Anhui University.

References

1. White paper on 5G concept: IMT-2020(5G) Promotion Group, February 2015
2. Lin, S., Costello, D.J.: Error Control Coding. Pearson Prentice Hall, Upper Saddle River (2004)
3. Kashani, Z.H., Shiva, M.: BCH coding and muti-hop communication in wireless sensor networks. In: IFIP International Conference on Wireless and Optical Communications Networks, pp. 1–5, April 2006
4. Kashani, Z.H., Shiva, M.: Channel coding in multi-hop wireless sensor networks. In: 2006 6th International Conference on ITS Telecommunications Proceedings, June 2006
5. Sankarasubramaniam, Y., Akyildiz, I.F., McLaughlin, S.W.: Energy efficiency-based packet size optimization in wireless sensor networks. In: IEEE International Workshop on Sensor Networks Protocols and Applications, May 2003
6. Vasudevan, S., Goeckel, D., Towsley, D.: Optimal power allocation in channel-coded wireless networks. In: Allerton Conference on Communication, Control and Computing, September 2004
7. Lettieri, P., Fragouli, C., Srivastava, M.B.: Low power error control for wireless links. In: 3rd Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM 1997), pp. 139–150, September 1997
8. Shih, E., Cho, S., Lee, F.S., Calhoun, B.H., Chandrakasan, A.: Design considerations for energy-efficient radios in wireless microsesor networks. J. VLSI Sig. Process. Syst. Sig. Image Video Technol. **37**(1), 77–94 (2004)
9. Grover, P., Woyach, K., Sahai, A.: Towards a communication-theoretic understanding of system-level power consumption. IEEE J. Sel. Areas Commun. **29**(8), 1744–1755 (2011)
10. Arikan, E.: Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. IEEE Trans. Inf. Theory **55**(7), 3051–3073 (2009)
11. Sarkis, G., Giard, P., Vardy, A., Thibeault, C., Gross, W.J.: Hardware implementation of successive-cancellation decoders for polar codes. IEEE J. Sel. Areas Commun. **32**(5), 946–957 (2014)
12. Berrou, C., Glavieux, A.: Near optimum error correcting coding and decoding turbocodes. IEEE Trans. Commun. **44**(10), 1261–1271 (1996)
13. Gallager, R.G.: Low Density Parity Check Codes. MIT Press, Cambridge (1963). Monograph. Accessed Aug 2013
14. MacKay, D.J.C., Neal, R.M.: Near Shannon limit performance of low density parity check codes. Electron. Lett. **33**(6), 457–458 (1997)
15. Arikan, E.: Systematic polar coding. IEEE Commun. Lett. **15**(8), 860–862 (2011)
16. Tal, I., Vardy, A.: How to construct polar codes. IEEE Trans. Inf. Theory **59**(10), 6562–6582 (2013)
17. Zhang, Z., Anantharam, V., Wainwright, M.J., Nikolic, B.: An efficient 10GBASE-T ethernet LDPC decoder design with low error floors. IEEE J. Solid-State Circ. **45**(4), 843–855 (2010)

A New Distributed Routing Protocol for Wireless Sensor Networks with Mobile Sinks

Hengyi Wen[1], Zheng Yao[1], Huiqiang Lian[2,3], and Baoxian Zhang[1(✉)]

[1] Research Center of Ubiquitous Sensor Networks,
University of Chinese Academy of Sciences, 19A Yuquan Road, Beijing 100049, China
wenhengyi15@mails.ucas.ac.cn, {yaozheng,bxzhang}@ucas.ac.cn
[2] University of Chinese Academy of Sciences, 19A Yuquan Road, Beijing 100049, China
lianhuiqiang15@mails.ucas.ac.cn
[3] Information Center, PetroChina Hebei Company, Shijiazhuang 050000, Hebei, China

Abstract. Mobile sinks have been widely used for data gathering in mobile-enabled wireless sensor networks (mWSNs). However, the frequent network topology dynamics caused by sink mobility in mWSNs may cause excessive protocol overhead for route discovery and maintenance and therefore routing performance degradation. In this paper, we design a new distributed routing protocol for achieving high routing performance in such networks. The designed routing protocol works in a reactive way for route learning/updating and it combines trail based forwarding and data-driven route learning/updating for improved performance as sink(s) move in the network. We present detailed design description of the new protocol. Simulation results show that our protocol can achieve high packet delivery ratio performance with low protocol overhead.

Keywords: Routing protocol · Wireless sensor networks · Mobile sinks

1 Introduction

Recently, wireless sensor networks with mobile sinks have been an attracting paradigm for data gathering in target environment. A wireless sensor network with one or multiple mobile sinks (MS) is typically referred to as mWSN. Much existing work has shown that use of mobile sinks can largely improve the performance of a WSN as compared with use of static sinks. However, sink mobility can cause unpredictable changes in network topology, which brings great challenges to the design of efficient routing protocols for such networks wherein sensor nodes only have limited resources and capabilities. Therefore, how to design efficient routing protocols for mWSNs to handle such sink mobility while achieving high routing performance with low protocol overhead has been a key issue in the research and design of mWSNs.

This work was supported partially by the National Natural Science Foundation of China under grants 61471339, 61531006, 61173158.

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 150–159, 2018.
https://doi.org/10.1007/978-3-319-90802-1_13

Much work has been carried out in the area of routing in mWSNs and existing protocols in this area can be divided into the following three types [1–3]: Location based routing protocols, topology based routing protocols, and reactive routing protocols. Location based protocols (e.g., LURP [4], TTDD [5], and ER [6]) require nodes in the network to have their own locations, their neighbors' locations, and packet destinations' locations. In these protocols, the location information will be used for guiding geographical packet forwarding in a hop-by-hop manner. However, in many cases, obtaining accurate location information of nodes is not always practical, in particular for mWSNs wherein mobile sinks can move rapidly and unpredictably. Topology based protocols (e.g., AVRP [7] and MDRP [8]) typically requires nodes in the network to form an efficient routing structure for packet delivery from sensor nodes to nearby mobile sinks. Topology based protocols can typically acquire short paths for packet delivery at the excessive cost of protocol overhead for path maintenance, which is often not attractive in WSNs with sporadic traffic. Reactive routing protocols (e.g., TRAIL [7] and DDRP [9]) works reactively for path delivery and maintenance, which has demonstrated good routing performance while having very low protocol overhead. In this paper, we shall focus on design of reactive routing protocol for mWSNs.

In this paper, we design an efficient distributed (reactive) routing protocol for mWSNs. The design objective is to achieve high routing performance with low protocol overhead. To achieve this goal, our protocol integrates trail based forwarding, data-driven packet forwarding, and random walk routing. In this way, our protocol combines sink-mobility-driven route learning and neighbor-forwarding-driven route learning with small protocol overhead. In the use of these forwarding strategies, routing distance and route freshness as characterized by time stamp freshness are used in the next hop selection. When a sensor node has no valid route for reaching a mobile sink, however, random walk routing is enforced until the data packets reach a sensor node on a fresh trail or with a valid route to reach a mobile sink. We present detailed protocol design of the protocol. Simulation results show that our protocol can achieve high packet delivery ratio performance with low protocol overhead.

The rest of this paper is scheduled as follows. In Sect. 2, we briefly review some existing routing protocols for mWSNs. In Sect. 3, we present the design of the new routing protocol. In Sect. 4, we conduct simulations to evaluate the performance of the designed protocol by comparing it with existing work. In Sect. 5, we conclude this paper.

2 Related Work

Much work has been carried out to support efficient routing in mWSNs and existing protocols in this aspect can be divided into the following three types: Location based routing protocols, topology based routing protocols, and reactive routing protocols. All these routing protocols can enable sensor nodes in the network to report their sensed data to a nearby mobile sink via multi-hop routing in a real-time fashion. Next, we shall respectively introduce typical protocols belonging to each of these types.

2.1 Location Based Routing Protocols

Location based routing protocols utilize node location information for assisting geographical packet forwarding in an mWSN. The major advantages of location based routing include simplicity, good routing performance, and high scalability. Typical location based routing protocols for mWSNs include Local Update-Based Routing Protocol (LURP) [4], Two-Tier Data Dissemination (TTDD) [5], and Elastic Routing (ER) [6].

LURP [4] works to restrict the location updating scope of mobile sink to a small circle other than the entire network, whenever possible. According to LURP, mobile sink chooses a small circular area and issues its up-to-date location inside the circle (at a high frequency) as long as it is still inside the circle. However, when it moves outside the circle, network-wide location updating will be triggered and a new circle will be chosen for local location updating but with higher frequency. Data packets outside the circle are forwarded toward the circle via geographical forwarding while topology-based routing is used inside the circle.

TTDD [5] provides scalable and efficient data delivery from a data source to multiple mobile sinks. Each data source proactively builds a grid structure in the network by dividing the sensing field into cells with dissemination nodes located at the crossing points of the grid. The delivery structure by TTDD is easy to maintain. However, with the increase of data source number and sink number, TTDD can produce excessive protocol overhead.

In ER [6], source sensors node can keep obtaining the newest location information of a mobile sink by its continuous data reporting to the sink. More concisely, when a sink node moves, its new location information is propagated backward along the data path to the source sensor via piggybacking the freshest sink location information into each data packet for forwarding downstream. Such piggybacking can allow the upstream node on a path to learn the freshest sink location in a hop-by-hop manner. Continuous data packet delivery in the forward direction enables the source node to learn the up-to-date location of its communicating mobile sink.

2.2 Topology Based Routing Protocols

Topology based protocols in general work proactively for route discovery and maintenance and they typically build efficient routing structure in the network, which provides short routes from each sensor node in the network to a nearby mobile sink at the cost of protocol overhead. Example protocols in this type include AVRP [7] and MDRP [8].

AVRP [7] has good performance in mWSNs with heavy traffic and infrequent movement of mobile sinks. It can reduce the protocol overhead by use of Voronoi scoping and dynamic selection of anchor node for each mobile sink in order to hide the short movement of the sinks. AVRP assumes that there are multiple mobile sinks moving in the sensing field uncontrollably and each of them selects a neighbor sensor as its anchor node. Voronoi scoping is used for restricting each mobile sink's interest dissemination scope for route updating.

MDRP [8] is designed to improve the performance of AVRP. It divides the Voronoi scope associated with each mobile sink into multiple disjoint layers according to the distance of sensor nodes away from the anchor node associated with the mobile sink. When a mobile sink moves inside the first layer, route updating will be only made inside the first layer. When it leaves the first layer and enters the kth level, route updating will be made in layers $\leq k$. In this way, MDRP is expected to largely reduce the protocol overhead as compared with AVRP with little sacrifice in routing performance.

2.3 Reactive Routing Protocols

Reactive routing protocols work in a reactive way for route discovery and updating. Typical protocols in this category include TRAIL and DDRP. The route discovery and maintenance in TRAIL is triggered by sink mobility while that in DDRP is triggered by neighbors' packet forwarding. Next, we shall respectively introduce how either protocol works.

TRAIL [7] is a combination of random walk and trail-based packet forwarding. TRAIL takes advantage of the trail left by mobile sink as it moves in the network. When a sensor has data packet(s) to report, if it has (fresh) trail to reach any mobile sink, trail based forwarding will be used. This process continues until the packet reaches a mobile sink along the trail. However, when no such trail is known, random walk will be used until reaching a mobile sink directly, a fresh sink, or timed out and thus dropped without further processing.

DDRP [9] takes advantage of the broadcast feature of wireless medium for gratuitous route learning/updating and thus reduce the protocol overhead for data reporting. In DDRP, each data packet carries an additional option recording the known distance from the sender of the packet to a target mobile sink. Overhearing of such a packet transmission will gratuitously provide those listening neighbors a route to reach mobile sink. Continuous such route-learning among neighbor nodes will provide fresh routes to more and more sensor nodes in the network.

Our protocol in this paper shall integrate the trail based forwarding strategy in TRAIL and the data-driven route learning/updating strategy in DDRP for further improved routing performance.

3 Protocol Design

In this section, we shall present the detailed design process of our protocol, which combines "trail based forwarding and data-driven routing and is referred to as TBD. We will first give an overview regarding how TBD works, then give necessary routing information to be kept at sensor nodes for TBD to work correctly. Finally, we present the detailed design description of TBD.

3.1 Protocol Overview

To achieve improved routing performance in mWSNs, TBD inherits the data-driven route learning capability in DDRP and also the sink-mobility-driven route learning capability in TRAIL. It accordingly utilizes the following strategies for packet forwarding: trail based forwarding, data-driven routing, and random walk routing. Trail based forwarding is to take advantage of the trail information left by sink mobility as sinks move in the network. Moreover, to efficiently handle trail broken issue, TBD adopts two-hop local broadcast for trail repair with limited protocol overhead. Data-driven routing is to take advantage of the routing information learnt via overhearing of data packet transmissions at neighbor nodes. Random walk routing is triggered when a packet holder has no any routing information to reach a sink node. In TBD, when a sensor node has a data packet to forward to a sink node, trail-based forwarding has the highest priority, data-driven routing is the second, and random walk has the lowest priority.

Compared with DDRP and TRAIL, TBD enables more nodes in the network to learn fresh routing information by inheriting the data-driven route learning capability in DDRP and the sink-mobility-driven route learning capability in TRAIL. In this way, it can largely reduce the probability at which random walk has to be triggered and also shorten the routing distance and therefore improve the routing performance.

3.2 Routing Information

For TBD to work properly, we make the following assumption: All nodes in the network (including both sensors and sinks) are equipped with omnidirectional antennas and have the same communication range. Furthermore, no location information of nodes is known. Next, we will introduce necessary routing information to be kept at sensor nodes for TBD to work correctly.

Table 1. Routing information kept at sensor nodes.

Items	Description
TRAIL_flag	A bool flag variable, which indicates whether a sensor node is on a trail or not. If it is true, it means the sensor is on a fresh trail; otherwise, it is false
DDRP_flag	A bool flag variable indicating whether a sensor node has a valid route to reach a mobile sink as learnt via neighbor-forwarding operations
Time_stamp	It records the time when a route to mobile sink was generated and it was copied from the time stamp carried in a data packet containing fresh route to a mobile sink or a beacon message
HopDist	*HopDist* records the distance from the current node to a sink
NextHopID	*NextHopID* is the ID of next-hop to reach a sink
ExpireTime	*ExpireTime* is the time when the current entry will expire if no further update received

According to TBD, there are at most two entries to be kept at each sensor node in the network, one is for data forwarding and the other is for backup. The information in

either entry is listed in Table 1. In Table 1, the first two items indicate in which way the routing information was learnt, time_stamp tells when the routing information was generated as stamped by the corresponding mobile sink. Initially, all nodes have no information about route to a sink and all the information in Table 1 will be Null.

Next, we introduce how the routing tables at sensor nodes are created and updated.

To enable trail based forwarding, the following procedure is taken for trail learning and updating. When a mobile sink moves in the network, it keeps broadcasting beacon messages periodically to its one-hop neighboring sensor nodes so as to leave a trail at sensors in the network. Accordingly, each neighboring sensor node of mobile sink knows that it can directly report data packets to a mobile sink. A beacon message carries the following information: The identifier of the mobile sink and a time stamp indicating when the message was generated. The sensor nodes which receive such beacon messages will locally create and update the corresponding routing tables as follows. It sets the flag TRAIL_flag = true, records the time stamp in its routing entry as that carried in the last received beacon message, and updates the ExpireTime field to Time_stamp + $\alpha \times T$ where α is a network parameter and T is the beacon interval.

To enable data-driven route learning/updating like in DDRP, each data packet contains an extra IP option Dist2mSink, which records the best known distance from the transmitter of the data packet to a nearby mobile sink. For example, if Dist2mSink equals to 3, then the transmitter of the packet is now three hops away from its target sink node. In actual protocol implementation, we assume Dist2mSink has a max value K. That is, a routing table only records routing information with distance $<K$ to reach a sink. There is a tradeoff between route learning scope and route freshness by adjusting the value of K. In the protocol operations, overhearing of such a packet transmission will gratuitously tell those listening neighbors fresh routes to reach a mobile sink. Continuous such route-learning among neighbor nodes will provide fresh routes for more and more sensor nodes in the network.

3.3 Data Packet Forwarding

In TBD, the priority of packet forwarding from the highest to lowest is as follows: trail based forwarding, data-driven routing/forwarding, and random walk routing. Accordingly, when fresh trail is available, trail based forwarding will be taken; else if data-driven learnt routing information is applicable, data-driven routing is performed; otherwise, random walk routing is taken. Figure 1 gives an example illustrating how a packet forwarding process works in the network when different routing information is available at different nodes. In this example, packet generated by a source sensor node is first forwarded via random walk, and then travel along route prepared by DDRP, and finally travel along a fresh trail before being reported to a mobile sink.

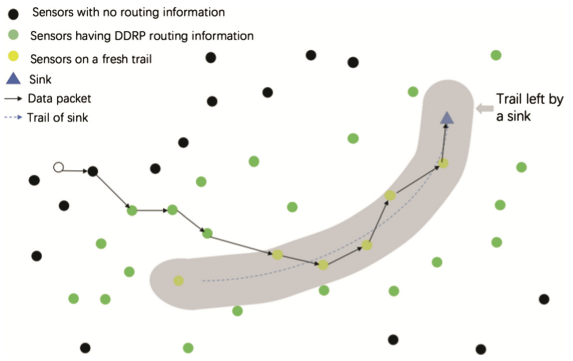


Fig. 1. An example illustrating how a packet is forwarded to a sink in TBD.

In TBD, once receiving a data packet from a neighbor sensor node or from the application layer directly, a sensor u will look up the routing entries on in its local cache, and carry out the following procedure based on which case the current packet holder is in:

Case 1: TRAIL_flag = true

In this case, we have sensor u is on a fresh trail. In this case, it will first look for sink(s) in its direct communication range. If it can find one such sink, the data packet will be forwarded directly to the mobile sink. If no sink can be found in its communication range, which means the sink has moved away, then trail based forwarding is triggered. In the trail based forwarding, the packet holder will send out a query message to see whether there is any neighbor with fresher sink-related record and start a timer. A query packet contains the identifier of the querying node and a time stamp copied from the local cache. If a reply is received before the timer expires, it will send the data packet to the sender of the reply packet. When multiple neighbors having fresher records than the packet holder, the one with the freshest record is expected to reply first via certain reply-deferring mechanism to suppress those unnecessary replies. If no reply is received, which means the trail is broken, then we use a two-hop local broadcast mechanism to find alternate route to bypass the broken point on the trail.

Specifically, the two-hop local broadcast mechanism for trail repair works as follows. The packet holder composes a new query message carrying its ID and time stamp information and then broadcasts this query to its one-hop neighbors. Upon receipt of this message, its one-hop neighbors will forward this message further. If any two-hop neighbor having fresher sink record than the packet holder, it will send a reply back to the packet holder. If multiple replies were received, the one with freshest record will be used. Upon receiving such a reply, the packet holder will send the packet to the node which sent it the reply message.

In case no reply is received in the trail repair process after certain time, sensor u will resort to its backup routing entry by going to Case 2. If no valid backup routing entry, random walk will be triggered by going to Case 3.

Case 2: DDRP_flag = true

In this case, sensor u has valid routing entry/entries learnt via overhearing of neighbor transmission(s). In this case, sensor u will perform data-driven routing by choosing the next hop from its routing entry and send the packet to the selected next hop.

Case 3: DDRP_flag = TRAIL_flag = false

In this case, node u does not have any valid routing information in its local cache, it will perform random walk routing by randomly selecting a neighbor sensor among its neighbor list and then send the packet to the selected neighbor.

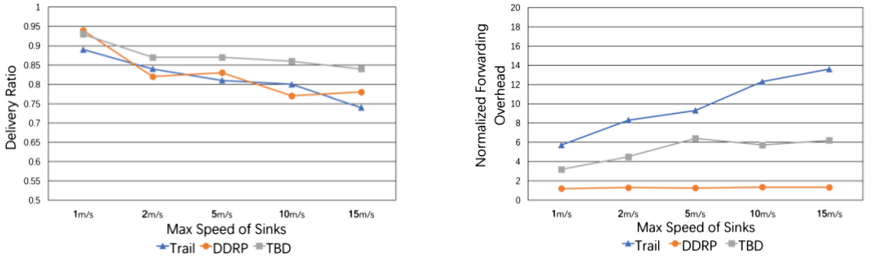
The sensor node receiving the data packet will repeat the above routing procedure until the packet reaches a mobile sink or timed out and then dropped.

4 Performance Evaluation

In this section, we conduct simulations for performance evaluation. The protocols simulated include the following: TBD in this paper, DDRP, and TRAIL. All these protocols do not require location information of nodes and they work reactively for path learning and updating. The simulation code was developed using Java. In the simulations, 200 sensor nodes and multiple mobile sinks were deployed uniformly at random initially in a 500×500 m^2 square area. Each node's communication range is 60 m. For each experiment, the simulation time is 1000 s.

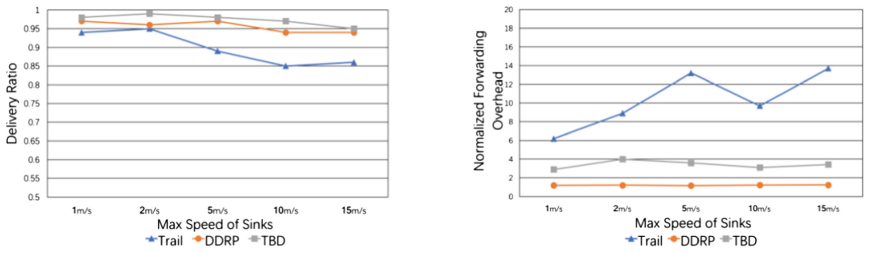
In our simulations, we used two metrics to evaluate the routing performance: Forwarding overhead and packet delivery ratio. The forwarding overhead is defined as the ratio of the total number of all packets transmitted (containing data packets and control packets) to the number of successfully delivered data packets. The number of packets transmitted is the total number of packet transmitted by all nodes (containing sensor nodes and sink nodes) and it also includes those transmissions of the packets that are forwarded, dropped, or collided. The lighter this overhead is, the more efficient a protocol will be. The packet delivery ratio is defined as the ratio of the total number of data packets successfully received by sinks to the number of data packets generated by sensor nodes. This metric represents the data delivery efficiency of a routing protocol.

In this experiment, the maximum velocity of mobile sinks varied from 1 to 15 m/s. The number of mobile sinks will be 1 and 3, respectively. Then, we will test different situations caused by the mobility of sink nodes. In the 3-sink case, we will observe routing performance when the packet generation rate in the network is 1 and 2 packets per seconds, respectively. Figure 2 shows the scenario with one sink and packet generation rate of 2 packets/s. Figure 2(a) shows the change of delivery ratio performance as the max speed of sinks change, Fig. 2(b) shows the change of overhead as the max speed of sinks change. Figure 3 shows the 3-sink situation. Figure 4 shows the 3-sink situation but changing the packet generation rate to one packet/s.



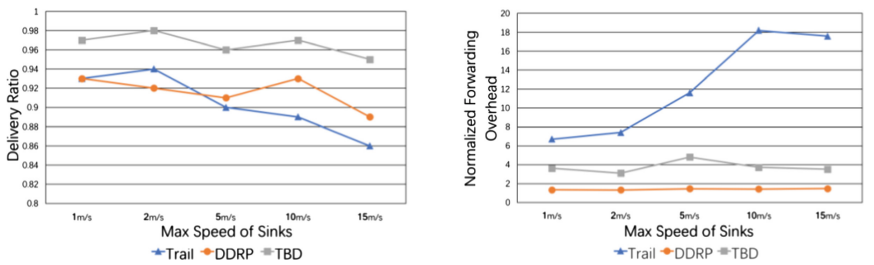
(a) (b)

Fig. 2. Performance of packet delivery ratio and normalized forwarding overhead versus sink speed. There is one sink in the network and the packet generation rate is two packets per second.



(a) (b)

Fig. 3. Performance of packet delivery ratio and normalized forwarding overhead versus sink speed. There are three sinks in the network and the packet generation rate is two packets per second.



(a) (b)

Fig. 4. Performance of packet delivery ratio and normalized forwarding overhead versus sink speed. There are three sinks in the network and the packet generation rate is one packet per second.

Through the above simulation results, we can see that TBD has the highest packet delivery ratio performance while having moderate routing protocol overhead as compared with DDRP and TRAIL. The higher protocol overhead by TBD as compared with DDRP is due to the overhead introduced for enabling trail based forwarding (i.e.,

exchanging of query-reply along trail and two-hop local broadcast for trail repair). In addition, it can be seen that sink number, sink moving speed, and packet generation rate have big impact on routing performance. Especially, in Figs. 2 and 3, we can see that as sink(s) move faster and faster, the packet delivery ratio keeps reducing while the overhead keeps increasing. Moreover, TBD has the highest packet delivery ratio performance as sink velocity increases. Figure 4 shows that, in lighter traffic situation, TBD gets even better performance on packet delivery ratio performance as compared with the other two protocols. Generally speaking, more sinks and lower moving speed lead to higher packet delivery ratio performance, and the faster sinks move, the more overhead will be caused.

5 Conclusion

In this paper, we have designed a distributed routing protocol for wireless sensor networks with mobile sinks, which integrates trail based forwarding, data-driven packet forwarding, and random walk routing. We present detailed design description of our protocol. Simulation results demonstrate that our protocol can improve the delivery ratio performance while keeping low protocol overhead.

References

1. Song, L.: Architecture of wireless sensor networks with mobile sinks: multiple access case. Int. J. Distrib. Sens. Netw. **3**(3), 289–310 (2007)
2. Liang, S., Hatzinakos, D.: Architecture of wireless sensor networks with mobile sinks: sparsely deployed sensors. IEEE Trans. Veh. Technol. **56**(4), 1826–1836 (2007)
3. Sheng, Y., Zhang, B., Li, C., Mouftah, H.: Routing protocols for wireless sensor networks with mobile sinks: a survey. IEEE Commun. Mag. **52**(7), 150–157 (2014)
4. Wang, G.J., Wang, T., Jia, W.J., Guo, M.Y. Chen, H.H., Guizani, M.: Local update-based routing protocol in wireless sensor networks with mobile sinks. In: Proceedings of the IEEE ICC 2007, pp. 3094–3099 (2007)
5. Ye, F., Luo, H.Y., Cheng, J., Lu, S.W., Zhang, L.X.: A two-tier data dissemination model for large-scale wireless sensor networks. In: Proceedings of the ACM MobiCom 2002, pp. 148–159 (2002)
6. Yu, F., et al.: Elastic routing: a novel geographic routing for mobile sinks in wireless sensor networks. IET Commun. **4**(6), 716–727 (2010)
7. Tian, K., Zhang, B., Huang, K., Ma, J.: Data gathering protocols for wireless sensor networks with mobile sinks. In: IEEE Global Telecommunications Conference (GLOBECOM 2010) (2010)
8. Shi, L., Yao, Z., Zhang, B., Li, C., Ma, J.: An efficient distributed routing protocol for wireless sensor networks with mobile sinks. Int. J. Commun. Syst. **28**(11), 1789–1804 (2015)
9. Shi, L., Zhang, B., Mouftah, H., Ma, J.: DDRP: an efficient data-driven routing protocol for wireless sensor networks with mobile sinks. Int. J. Commun. Syst. **26**(10), 1341–1355 (2013)

Delay-Aware Dynamic Barring Scheme for Massive Access in NB-IoT Network

Wenyan Liu[1], Jun Zhang[1,2(✉)], Xinghua Sun[1], and Hongbo Zhu[1]

[1] Jiangsu Key Laboratory of Wireless Communications, Nanjing University of Posts and Telecommunications, Nanjing 210003, People's Republic of China
{1015010324,zhangjun,xinghua.sun,zhuhb}@njupt.edu.cn
[2] National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, People's Republic of China

Abstract. In Internet of Things (IoT), narrow band IoT (NB-IoT) based on cellular networks is expected to play an important role for providing low power, wide area services, supporting deep indoor deployment, massive devices in one cell. However, massive access requests in resource-finite situation may bring out severe congestion and delay. To alleviate congestion and delay problems, we propose a delay-aware dynamic barring scheme in this paper. According to different delay requirements, the proposed scheme can ensure higher priority for delay-sensitive services. Compared with standard access class barring (ACB) scheme, both success probability and delay for delay-sensitive devices can be improved significantly, with several sacrifice on delay-tolerant performance.

Keywords: NB-IoT · Massive access · Delay-aware · Dynamic ACB

1 Introduction

With the development of IoT, lower power wide area (LPWA) network attracts more and more attention. The current typical LPWA technologies, for example, Lora and Sigfox, are fragmented and non-standardized, which may bring security issues. For the standardization of the LPWA market, 3GPP proposed NB-IoT based on cellular network, making some simplification both on physical and network layers [1,2]. As a reliable technology, NB-IoT can serve at least 50 thousand modules per cell [3]. With this huge load, legacy access control methods may be not efficient to handle radio access network (RAN) and core network (CN) overload, then heavy congestion and severe delay may incur [4].

In NB-IoT network, random access step must be performed first, by sending preambles in narrow band random access channel (NPRACH) for uplink synchronization. However, if more than one device select one same preamble simultaneously, then collision would be caused, which further caused access congestion. With great potential to generate huge access traffic from numerous devices, collision probability is high, causing serious RAN congestion and long delay.

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 160–170, 2018.
https://doi.org/10.1007/978-3-319-90802-1_14

To alleviate congestion and delay problems, many effective schemes have been proposed in machine-to-machine (M2M) communications [5–8]. 3GPP adopt the proposals of ACB and enhanced ACB mechanism named extended access barring (EAB) in cellular network, which is effective for RAN overload control by allowing a portion of devices to access the channel. If requests far exceeds the access channel capacity, the effect of a single barring scheme will be not obvious, thus [9] proposed a two-layer scheme combining ACB and EAB to enhance the barring performance. A cooperative ACB method is also proposed in [10], with the cooperation of base stations, the access delays can be significantly improved. Unlike the methods towards the decreasing access arrivals, in [11], another grouping scheme to reuse preambles in different groups is proposed, which may cause preamble interference between groups. Generally, the network status depends on arrivals and usable preambles in current slots, thus avoiding the access requests concurrency or exploiting preambles are the two main solutions.

In this paper, we propose an effective way to restrict preamble competitors according to different delay demands. First, a delay threshold should be set according to the acceptable delay tolerance for delay-sensitive devices, then we split devices into two sets by the threshold. Secondly, set a fixed access parameter for the delay sensitive terminals, while each delay tolerant terminal generating a random access parameter. The barring factor is also adaptive about current traffic. Without external resources, our scheme can make sure the delay-sensitive devices have priority to acquire preambles. Results show that the performance of delay-sensitive devices can be improved effectively.

2 Background and System Model

2.1 NPRACH Resource Configuration

As a clean-slate technology, NB-IoT can extend the maximum coupling loss (MCL) 20 dB more than GPRS, then NB-IoT devices can keep working in poor situation with MCL up to 164 dB. In 3GPP proposals, devices based on NB-IoT technology can be divided into 3 categories depending on MCL, called CE0, CE1, CE2 (CE, Coverage Extended), respectively supporting MCL less than 144 dB, between 144 dB and 154 dB, and MCL up to 164 dB. For supporting

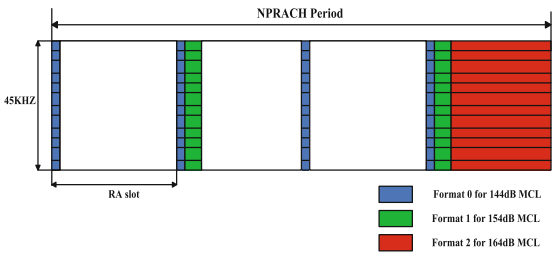


Fig. 1. NPRACH resource configuration.

extended coverage, different categories own different resource configuration. The worst condition, usually refer to basements or other places with poor channel condition, i.e., CE2 scenario, configures the longest preambles in time domain to make sure that requests can be detected by BS. The configuration can refer to Fig. 1.

Obviously, long preambles consume the uplink resources extremely, thus the number of long preambles are limited. In case of average access requests among three categories, devices in CE2 may face the most serious conflicts. In this paper, we analyze proposed schemes on CE2 devices, which is also suitable for the other two situations.

2.2 Access Barring Scheme

To resolve congestion, ACB scheme has been adopted. In each access slot, active devices need to pass through the barring process before sending preambles to BS. The barring factor δ is broadcast by BS. Each active device generates a random p (i.e., access parameter) between 0 and 1. Only if p is less than δ can the corresponding device pass the barrier. Literally, δ determines the expected percentage of active terminals which can apply for preambles. Those devices blocked by barring will be barred for a certain period called barring time, which is also broadcast by BS. The main work is shown in Fig. 2.

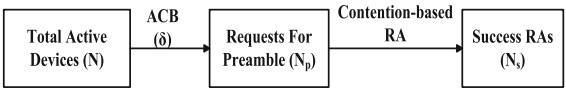


Fig. 2. Access barring scheme.

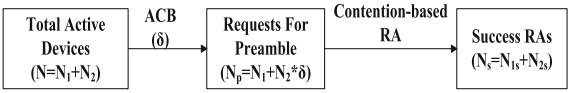


Fig. 3. Delay-aware barring scheme.

2.3 System Model

To avoid weakness on real-time service, devices supported by NB-IoT should allow a certain degree of delay. Thus, terminals with rigor delay limit will not be involved in our study. Under this premise, we present our model.

Generally most devices accept a more tolerant delay, however, the degree of acceptance are quite different among NB-IoT terminals. In rare cases, some applications which are also relatively delay-sensitive, such as alarms in poor environments, have to adopt NB-IoT due to bad channel situation. With low

proportion of entire business, although, this part is extremely important. In order to protect the efficiency of these applications, according to delay requirements, we divide all terminals into two categories and propose an access strategy.

Our target is to make sure delay-sensitive devices can pass the barring scheme with a high priority. Only several modules need a shorter delay, thus we can set a time threshold to classify devices. The threshold can be the maximum acceptable delay for delay sensitive scenarios. According to the delay requirements distribution, we split all devices into two classes, called class A and class B. Devices in class A should finish the access within the given time threshold, while others in class B can be more tolerant. In terms of quantity, devices in class A are far less than those in class B.

To ensure the priority of delay-sensitive ones, we change the way access parameter generated. Unlike the original ACB schemes with fair access parameter generation, in our work, set devices in class A with a fixed p_A equal to zero, while devices in class B need to generate random number p_B between 0 and 1. In this model, the whole period we considered, T, is divided into slots indexed by non-negative integer i ($i = 1, 2, \ldots, L$). Then, the access parameters can be described by

$$\begin{cases} p_A(i) \equiv 0, \\ p_B(i) \in (0, 1). \end{cases} \tag{1}$$

No matter how much δ is equal, those belong to class A can always break through the barrier, while part of devices in class B will be banned.

3 Delay-Aware Access Barring Scheme

3.1 Dynamic Barring Factor

To improve access success rate, we change the way barring factor generated. Preambles can be configured in advance, for analysis, assume number of preambles is K and current requests for preambles is m. If more than one select a certain preamble, then all the requests on the preamble can't be detected by BS. The collision probability can be calculated by $p_c = 1 - (1 - \frac{1}{K})^{m-1}$. According to p_c, we set a threshold about the average success requests so as to perform our following scheme. Set $M = \max\{\lceil \hat{m} \rfloor\}$, while $[1 - (1 - \frac{1}{K})^{\hat{m}-1}] < 0.1$, and $\lceil \hat{m} \rfloor$ means the closest integer near $\hat{m}$. Absolutely, more than one value can satisfy the limit of $[1 - (1 - \frac{1}{K})^{\hat{m}-1}] < 0.1$, and M is the maximum of all. The limit less than 0.1 try to make sure at this time $\hat{m}$ devices could complete the random access with 90% probability.

In following analysis, M is regarded as a threshold for adjusting barring factor. Next work is to restrict the active devices around M by designing suitable barring factor. Assume that n and n_1 denote the total active devices and class A devices, respectively, and δ is the dynamic barring factor, then let

$$\delta = \begin{cases} 1 & n \leq M \\ \frac{M - n_1}{n - n_1} & n > M > n_1 \\ 0 & n \geq n_1 > M \end{cases} \tag{2}$$

where δ can limit the preamble requests around M, ensuring success rate of access around 90%.

3.2 Adaptive Random Access Procedure

Based on our work, an adaptive random access strategy is achieved. Assume N is the number of active devices. If N is less than M, $\delta = 1$, then all the active ones can select preambles directly. If N is more than M, according to Eq. (2), each device compare their p_A or p_B with δ. Since $p_A \equiv 0$, devices in class A can always choose preambles directly, however, others in class B will be restricted by δ to some extent. Only if p_B no more than δ can the relative one pass the barrier. If the number of active A-class ones, i.e., N_1, is more than M, only these A devices can pass the barrier, while the lowest δ, i.e., 0, can block all the B-class requests. With extreme less devices in class A, the rate of initiating an access request is low, so the access resources will not be blocked by class A. The dynamic barring scheme can be described by Fig. 3.

4 Performance Analysis and Evaluation

4.1 Arrivals Distribution Model

Unlike human communications, in event-driven business, arrivals no longer satisfies the poisson distribution. Due to large-scale event-driven alarms or paging messages, lots of terminals may need to access simultaneously. As described in [12,13], this business can be modeled as beta distribution. Arrivals in a period of time, denoted as T, with probability $p(t)$, following a beta distribution

$$p(t) = \frac{t^{\alpha-1}T - t^{\beta-1}}{T^{\alpha+\beta-1}Beta(\alpha,\beta)}, \tag{3}$$

with $\alpha = 3$, $\beta = 4$, which is closest to actual situation. $Beta(\alpha,\beta)$ denotes beta function, which is only related to α and β. T can be divided into L slots evenly with τ seconds per slot.

Assume N devices need to communicate with BS in L slots. Then arrivals in each slot can be calculated by

$$N(i) = N \int_{t_{i-1}}^{t_i} p(t)dt, i = 1, 2, \ldots, L. \tag{4}$$

4.2 Performance Analysis

Some measure metrics are proposed for performance analysis. To make contrasts, we also consider the static ACB scheme with fixed barring factor η, where all the devices generate random number between 0 and 1 fairly.

Access Success Probability. Access success probability is defined as the ratio of the successful number $N_s(i)$ to total active devices $N(i)$ in continuous L slots. Thus, average success probability is calculated by

$$p_s = \frac{1}{L}\sum_{i=1}^{L}\frac{N_s(i)}{N(i)} = \frac{1}{L}\sum_{i=1}^{L} p_s(i), i = 1, 2, \ldots, L. \tag{5}$$

In original ACB scheme, with barring factor η, total k preambles available in current configuration, the success probability is calculated by

$$p_s^{ACB}(i) = (1 - \frac{1}{k})^{N(i)\cdot\eta - 1}, i = 1, 2, \ldots, L. \tag{6}$$

In our model, devices in class A and class B follow quite different access parameter patterns, thus, with different probability calculations. Define N_{1i}, N_{2i} as the active number for class A and class B devices in i-th slot. Then the success probability for class A is

$$p_s^{(A)}(i) = \begin{cases} 1 & N_{1i} = 0 \\ (1 - \frac{1}{k})^{N_{1i}-1} & N_{1i} \geq M \\ (1 - \frac{1}{k})^{N_p(i)-1} & 0 < N_{1i} < M \end{cases} \tag{7}$$

and for class B,

$$p_s^{(B)}(i) = \begin{cases} 0 & N_{1i} \geq M, N_{2i} \neq 0 \\ (1 - \frac{1}{k})^{N_p(i)-1} & 0 \leq N_{1i} < M, N_{2i} \neq 0 \\ 1 & N_{2i} = 0, \end{cases} \tag{8}$$

where $N_p(i) = N_{1i} + \delta(i) \cdot N_{2i}$, denoting the requests for preambles.

Access Delay Analysis. In fact, the delay refers to the time from the initiation request to the success of the access. Suppose there are N active devices, average delay is defined as the sum delay of successful numbers divided by the number of successful devices, thus

$$\tau_{avg} = \frac{1}{N}\sum_{j=1}^{N}\tau(j). \tag{9}$$

However, we can't promise all the active devices can access successfully in a certain period. Suppose N_i devices transmit preambles in i-th slot, the total delay is equal to

$$\tau_{tot} = \sum_{i=1}^{L} N_i. \tag{10}$$

The average delay is equal to τ_{tot} divided by the sum of successful accesses denoted as N_s, that is

$$\tau_{avg} = \frac{\tau_{tot}}{N_s}. \tag{11}$$

In our scheme, devices in class A and class B are designed with different barring time, τ for class A, $\lambda \cdot \tau$ ($\lambda > 1$) for class B. The time spent on access is calculated by the next two equations. $\tau_A(i)$ describe the total time consumption in i-th slot by N_{1i} devices while $\tau_{avg}^{(A)}$ means the average delay of $N_s^{(A)}$ class A devices. τ is a fixed time of a slot, a failed A-class device can be barred for τ, just like a new request in following slot. The detailed formula is shown below,

$$\tau_A(i) = N_{1i} \cdot \tau, i = 1, 2, \ldots, L, \tag{12}$$

$$\tau_{avg}^{(A)} = \frac{1}{N_s^{(A)}} \sum_{i=1}^{L} \tau_A(i). \tag{13}$$

For class B, the failed device should be barred for longer time. λ is an integer factor between 1 and 10, which means device should wait for $\lambda \cdot \tau$ when it was banned, with $N_s^{(B)}$ successful requests in T and success probability $p_s^{(B)}(i)$ in i-th slot, having

$$\tau_B(i) = N_{2i} \cdot p_s^{(B)}(i) \cdot \tau + N_{2i} \cdot (1 - p_s^{(B)}(i) \cdot \lambda \cdot \tau, i = 1, 2, \ldots, L, \tag{14}$$

$$\tau_{avg}^{(B)} = \frac{1}{N_s^{(B)}} \sum_{i=1}^{L} \tau_B(i). \tag{15}$$

To make contrasts, the barring time for ACB scheme is equal to τ, and the average delay is calculated by

$$\tau(i) = N_i \cdot \tau, i = 1, 2, \ldots, L, \tag{16}$$

$$\tau_{avg}^{ACB} = \frac{1}{N_s} \sum_{i=1}^{L} \tau_{(i)}. \tag{17}$$

Success Probability in Each Slot for Class A. Using the delay-aware scheme, class A devices own the priority to complete the random access requests. It means that all active devices belong to class A in one slot can possibly complete the access process all at once. Assume N_{2p} devices in class B can pass the barring and select preambles contending with class A, the success probability of first full accesses for class A is calculated by

$$P_o^{(A)}(i) = \begin{cases} \frac{C_{N_{1i}}^{k} \cdot N_{1i}!}{(k - N_{1i})} & N_{1i} \geq M \\ \\ \frac{C_{N_{1i}}^{k} \cdot N_{1i}! \cdot (k - N_{1i})^{N_{2p}}}{k^{(N_{1i} + N_{2p})}} & N_{1i} < M. \end{cases} \quad i = 1, 2, \ldots, L. \tag{18}$$

The equation means, only when N_1 devices choose different preambles from k preambles, at the meanwhile, class B devices choose the other k-N_1 preambles, can make sure all the requests from class A access successfully. To improve readability, the symbols appearing in the text are shown in Table 1.

4.3 Performance Evaluation

To evaluate the performance, we adopt the simulation parameters for NB-IoT devices that have been agreed by 3GPP. Considering 50,000 devices in a single cell with a uniform distribution geographically. In a predefined period, devices generate access attempts independently. Usually, NPRACH band occupy 180 KHZ, with subcarrier 3.75 KHZ, which means 48 preambles are available per slot. In our analysis, supposing $T = 120$ s as one specified period, let $\tau = 240$ ms, i.e., $L = 125$.

For maximizing its advantages of deep coverage, we reasonably assume CE2 terminals occupying the main part of the whole NB-IoT network, for example, half of all. Assume that each terminal randomly initiates an average of 15 access requests per day, thus, approximately 500 access requests are from CE2 in T. To meet the exploded increasing devices in future, we also evaluate the active devices up to 5,000 per period per cell.

Table 1. Symbols summary.

Symbol	Parameter
N	Total number of active devices
K	Number of preambles per NB-IoT band
M	Maximum requests for preambles satisfying $P_s \geq 0.9$
T	Specified period for one access process
p	Access parameter
δ	Dynamic barring factor
η	Fixed barring factor in ACB
τ	One access slot(240 ms)
P_s	Access success probability
τ_{avg}	Average delay
N_{fail}	Failed devices in T
$P_o^{(A)}$	Success probability for A-class devices

As Fig. 4 shows, when N is less than 1,000, the ACB with $\eta = 0.4$ works well. However, as N being larger, our scheme performs better than others. With several sacrifice on class B, the success probability of class A is improved effectively, performing well over the fixed ACB scheme with barring factor $\eta = 0.4$ and $\eta = 0.8$.

Figure 5 shows both class A and class B performs well on delay performance. With class A achieving an extreme shorter delay, B-class performs worst when N is less than 4,000. However, delay of class B is even shorter than class A while N is more than 4,000. That is because with the active number increasing, less B-class devices can pass the barrier, i.e., $N_s^{(B)}$ is limited, so the average delay seems like better than class A.

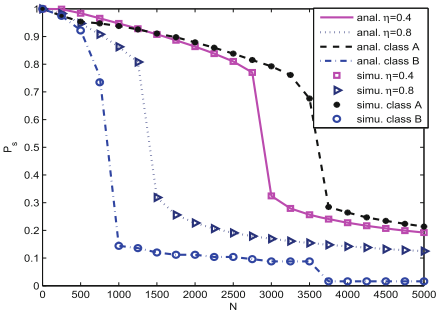


Fig. 4. Access success probability.

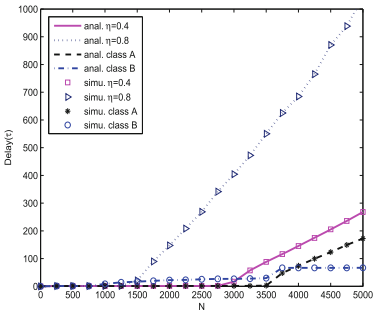


Fig. 5. Access delay for each successful device.

With exponential increasing numbers, not all of the active devices can finish the random access process in our defined period T. Surely, failed requests may continue the access procedure in the following period until finally completed the random access or gave up the packets. We observe the failed numbers and make it as another metric to assess the performance. Failed number is equal to the total active requests minus the successful ones, shown in Fig. 6.

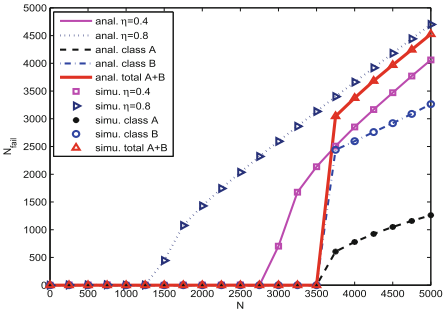


Fig. 6. Failed access numbers at the end of T.

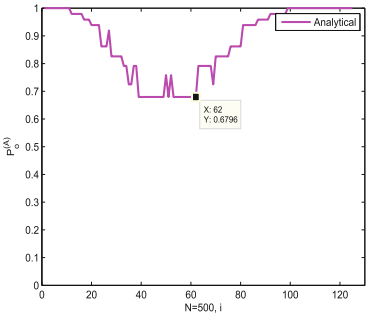


Fig. 7. Success probability of class A in appearance slot.

From the results, we can see the total failed ones, i.e., the sum of failed ones from class A and class B, is always less than the ACB method with $\eta = 0.8$. While N is larger than 3750, total failed numbers are little more than fixed barring $\eta = 0.4$ scheme, however, failed devices in class A is still limited, which mean our proposed scheme perform well on access procedure, guaranteing priority for handling delay-sensitive requests.

Figure 7 shows the probability of all class devices succeed in apparent slot. Assume the active devices in current period is equal to 500. By protecting the priority of class A to occupy preambles, the probability of all class A requests

succeed in first appearance, can be larger than 67%, which is impossible in ACB scheme. Correspondingly, both delay and re-attempts can be limited effectively.

5 Conclusion

In this paper, we have considered the critical issue of NB-IoT communication in 3GPP scenario by proposing the delay-sensitive-protected dynamic barring scheme to improve the congestion and serious delay problems. Simulation results show that the proposed scheme can effectively improve access success probability and reduce access delays for the delay-sensitive services.

Acknowledgements. This work was supported by the National Natural Science Foundation of China (NSFC) under Grants 61427801, 61671251, and 61401224, the Natural Science Foundation Program through Jiangsu Province of China under Grant BK20150852 and BK20140882, and the open research fund of National Mobile Communications Research Laboratory, Southeast University under Grant 2017D05.

References

1. Adhikary, A., Wang, Y.P.E., Lin, X.: A primer on 3GPP narrowband internet of things NB-IoT. IEEE Commun. Mag. **55**(3), 117–123 (2017)
2. Tsai, A.H., Wang, L.C., Huang, J.H., Lin, T.M.: Overload control for machine type communications with femtocells. In: Vehicular Technology Conference, Quebec City, QC, Canada, pp. 1–5 (2012)
3. Mangalvedhe, N., Ratasuk, R., Ghosh, A.: NB-IoT deployment study for low power wide area cellular IoT. In: IEEE International Symposium on Personal, Indoor, and Mobile Radio Communications, Valencia, Spain, pp. 1–6 (2016)
4. Lin, X., Adhikary, A., Wang, Y.: Random access preamble design and detection for 3GPP narrowband IoT systems. IEEE Wirel. Commun. Lett. **5**(6), 640–643 (2016)
5. Lien, S.Y., Chen, K.C., Lin, Y.: Toward ubiquitous massive accesses in 3GPP machine-to-machine communications. IEEE Commun. Mag. **49**(4), 66–74 (2011)
6. Wang, G., Zhong, X., Mei, S.: An adaptive medium access control mechanism for cellular based machine to machine (M2M) communication. In: IEEE International Conference on Wireless Information Technology and Systems, Honolulu, HI, USA, pp. 1–4 (2010)
7. Moon, J., Lim, Y.: Adaptive access class barring for machine-type communications in LTE-A. In: Eighth International Conference on Ubiquitous and Future Networks, Vienna, Austria, pp. 398–402 (2016)
8. Cheng, R.G., Chen, J., Chen, D.W., Wei, C.H.: Modeling and analysis of an extended access barring algorithm for machine-type communications in LTE-A networks. IEEE Trans. Wirel. Commun. **14**(6), 2956–2968 (2015)
9. Pang, Y.C., Lin, G.Y., Wei, H.Y.: Context-aware dynamic resource allocation for cellular M2M communications. IEEE Internet Things J. **3**(3), 318–326 (2015)
10. Lien, S.Y., Liau, T.H., Kao, C.Y., Chen, K.C.: Cooperative access class barring for machine-to-machine communications. IEEE Trans. Wirel. Commun. **11**(1), 27–32 (2012)

11. Kim, T., Han, S.J., Dan, K.S.: An enhanced random access scheme with spatial group based reusable preamble allocation in cellular M2M networks. IEEE Commun. Lett. **19**(10), 1714–1717 (2015)
12. Koseoglu, M.: Lower bounds on the LTE-A average random access delay under massive M2M arrivals. IEEE Trans. Wirel. Commun. **64**(5), 2104–2115 (2016)
13. He, H., Du, Q., Song, H., Li, W., Wang, Y., Ren, P.: Traffic-aware ACB scheme for massive access in machine-to-machine networks. In: IEEE International Conference on Communications, London, UK, pp. 617–622 (2015)

Security and IoT

Security Analysis of Authentication Overlaying Tag Signal

Song Huawei(✉), Liang Jin, and Shengjun Zhang

National Digital Switching System Engineering and Technological R&D Center, Zhengzhou, China
greatboy_song@sina.com

Abstract. This paper presents a new method for authentication based on overlaying tag signal. The tag signal and communication signal are superimposed to form the signal "watermark". From the point of view of signal transmission, the tag signal can achieve the dual "binding" of shared key and channel. Security analysis and simulation results indicate that it can achieve high authentication success rate and low failure rate. This method does not require complex cryptographic algorithms. So it can achieve security under the premise of reduce the computational amount in the communication process.

Keywords: Tag signal · Authentication · Physical layer security

1 Introduction

Authentication technology is an important part of information security [1]. Generally, authentication includes both identification authentication and message authentication. The former is used to authenticate the user identity; the latter is used to ensure the non-repudiation of communication and the integrity of the transmission of information. In the existing mobile communication system, the identity authentication and message authentication are based on cryptographic algorithm. That is to say, the authentication implementation is carried out at the high level, using the cryptographic algorithm to calculate numerical results which are difficult to be counterfeited. The eavesdropper can get the message content of the transmission, and the security is completely dependent on the difficulty of deciphering the cryptographic algorithm. Simmens summarizes this authentication security model [2], and points out that success rate of attack are related to the size of the key space |K|. It is depressing that the lower bound of the attack success rate is, which is much higher than guessing the key. Maurer further proves that the success rate of attack is also related to the times of authentication, and it may increase with the growth of times [3].

In traditional communication system, a cryptographic algorithm is used to compute MAC (Message Authentication Code). Due to both of legal sides sharing private key, the generated MAC will be the same. The receiver can determine whether the message is from legitimate senders by comparing MAC. This method is equivalent to make tag at the message level for authentication. In this paper, a new method using tag signal

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 173–180, 2018.
https://doi.org/10.1007/978-3-319-90802-1_15

realizes the physical layer authentication. Taking the advantage of legality sides sharing a private key and having coherent channel state information in short time, the sender produce tag signal from spread frequency code and measured channel state information, then overlap the tag signal on the communicational signal. The receiver can detect the correct tag signal and demodulate the communicational signal. This method can avoid using complex cryptographic algorithm, reduce the amount of calculation, and prevent passive eavesdropping and active attack effectively.

2 Related Works

In recent years, the physical layer security technology has attracted more and more attention of researchers. Wireless channel has characteristics of uniqueness, diversity and reciprocity. It provides a new direction for information security [4, 5]. Authentication in physical layer has already become a new hot spot in the authentication technology. Xiao et al. proposed the method of authentication using "channel fingerprint". Hypothesis test can check channel characteristic similarity [6]. But this kind of methods need cipher algorithm to complete authentication for the first time [7, 8]. The physical layer "challenge-response" method hidden key and authentication information in the wireless channel amplitude and phase information [9, 10]. It can be used to enhance authentication security when user access networks for the first time, but this method does not apply to the message authentication. Adding tag information on the frequency spectrum of the signal is also a good method. It has been used in the key generation [11], wireless spectrum identification and determining the interference [12, 13]. But these methods are not very applicable to wireless authentication.

3 System Model

Alice and Bob are legitimate sender and receiver and they pre-allocated the private key K. Eve is a malicious third party, who knows time slot, frequency band, and modulation mode, etc. The channel between Alice and Bob is h_{AB}, the channel between Alice and Eve is h_{AE}, and the channel between Eve and Bob is h_{EB}. Suppose that Alice sends signal x, and Bob receives signal y and Eve receives signal z, then:

$$y = x * h_{AB} + n_{AB} \tag{1}$$

$$z = x * h_{AE} + n_{AE} \tag{2}$$

In (1) and (2), n_{AB} and n_{AE} are the noise between Alice and Bob, Alice and Eve. And they are independent of each other. The asterisk represents convolution operation. In TDD (time division duplex) system, the channel parameters of the two parties are basically unchanged in a short period of time, which can be considered as short-term reciprocity. It means that $h_{AB} \approx h_{BA}$. Eve might receive a signal from Alice, or send a signal to Bob and try to make Bob accept it (Fig. 1).

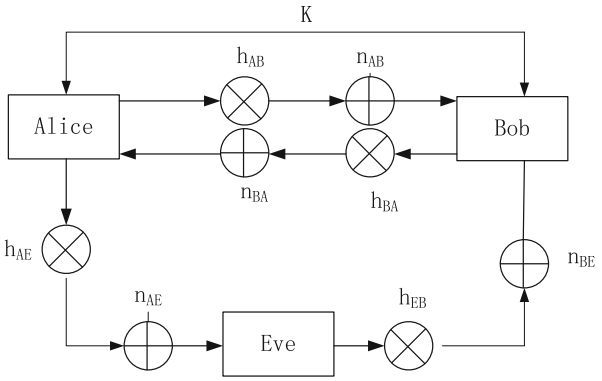


Fig. 1. System model

4 Process of Overlaying Tag Signal Authentication

Alice produces tag signal, and overlay with communication signals. Bob can normally demodulate signal, and check the correction of tag signal at the same time. Because the tag signal is generated by the shared key and reciprocity channel quantitative values through common produce m-sequence spread spectrum, Alice and Bob can generate the same tag signal. The tag signal and communication signal realize reuse in the wireless

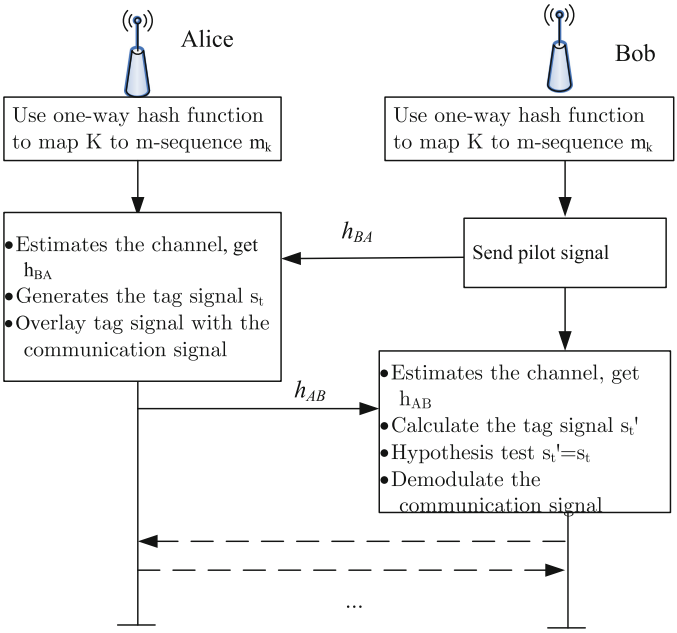


Fig. 2. Process of overlaying tag signal authentication

channel. Eve don't know the spread spectrum code, so he can only rely on guessing to fake Alice. Within limited times of attacks, it is difficult to succeed for Eve.

As shown in Fig. 2, the process of overlaying tag signal authentication has five steps.

Step 1: The preparation stage

Prior to the start of the communication, Alice and Bob pre-assigned private key K and public spread sequences $\{m_i\}$, i = 0, 1,…, N. Let's set the set space of key K is |K|. And it is satisfied that N > |K|. Alice and Bob use the same one-way hash function to map K to the same spread-spectrum m-sequence m_k. The one-way hash function should have the following properties:

(1) The randomness of hash value has no obvious statistical characteristics;
(2) Small amount of computation can be realized quickly;
(3) Unidirectional. It is difficult to obtain input in reverse according to the result of hashing, preventing secret information from being leaked;
(4) Anti-collision. It is very difficult to ensure that another input with the same hash value is found, which is to prevent Eve's dictionary attack.

Step 2: Bob sends the pilot, and Alice estimates the channel h_{BA}

Bob send pilot signal to Alice. Alice estimate h_{BA} and get approximate value $\hat{h}_{BA}$. In this course, equal probability of quantitative measurement is used. Because of the influence of the noise, $\hat{h}_{BA}$ is the noisy version of the real channel. That is: $\hat{h}_{BA} = h_{BA} + n_{BA}$, $\hat{h}_{BA} \sim CN(0, \sigma_h^2)$, n_{BA} is random variable which obey the complex Gaussian distribution. $n_{BA} \sim CN(0, \sigma_n^2)$. And the signal-to-noise ratio can be written as $SNR = \sigma_h^2/\sigma_n^2$.

Step 3: Alice generates the tag signal and sends it overlaying with the communication signal.

Alice spread spectrum for $\hat{h}_{BA}$ with m-sequence m_k, then gets tag signal s_t. The tag signal and communication signal are overlaid to send to Bob, that is:

$$s_t = m_k \hat{h}_{BA} \tag{3}$$

$$x = s_s + s_t \tag{4}$$

The signal Bob received is:

$$y = \left(s_s + s_t\right) * h_{AB} + n_{AB} \tag{5}$$

Step 4: Bob receives the signal and checks the tag

Bob estimates the channel h_{AB}, then get the approximate value $\hat{h}_{AB}$ through the same method as Alice. Bob may calculate the tag signal $s_t' = m_k \hat{h}_{BA}$. According to the principle of spread spectrum communication, communication signal can still normally despread under higher spread spectrum gain. After eliminating the tag signal s_t', the received signal can continue to demodulate. There are two alternative assumptions:

H_0: The tag signal s_t is sent by Alice;
H_1: The tag signal s_t is not sent by Alice.

Accordingly, due to the influence of channel noise, the channel characteristics of Alice and Bob may not be completely consistent. The bit strings resulting from $\hat{h}_{AB}$ and $\hat{h}_{BA}$ may be written as str($\hat{h}_{AB}$) and str($\hat{h}_{BA}$). Here quantitative difference rate is defined as ρ, which means a percentage through comparing each bit of two series of string. We set hypothesis threshold as Γ, which usually can be chosen as constant, such as $\Gamma = 99\%$. Then the hypothesis criteria may be: H_0 is accepted when $\rho \geq \Gamma$, alternatively H_1 is accepted when $\rho < \Gamma$.

Step 5: Alice and Bob correspond continuously

After the success of the authentication, Alice and Bob can continuously communicate, maintaining normal pilot signal and channel estimation. If the conditions that channel are not satisfied for the reciprocity after a long interval, we may return to step 2 for a new round of authentication.

5 Safety Analysis

For the security of the authentication, there are two type indicators of success rate and failure rate. And there are two major errors in the hypothesis test. One is that Alice superimposes the tag signal without being tested, and Bob rejected the signal that Alice sent. It is called the false alarm rate. The second is that Eve was accepted by Bob as Alice, which is called the missing alarm rate. The reason for the first type of error is similar to the successful rate, and the second error will be analyzed below.

As mentioned above, the success rate of the attacker is higher than $1/\sqrt{|K|}$ in the traditional authentication model [2]. Under the authentication method of this paper, if Eve wants to fake the tag signal, he needs to fake a spread signal that can pass the hypothesis test. According to the above assumptions, the space of m-sequence is |m|, and the space is big enough: |m| > |K|. Because of the one-way hash function, the lower bounds of attack success rate is 1/|K|. That is to say that it is worst for Eve to guess the key. Due to the mutual correlation characteristics of m-sequence, different m-sequences are unrelated. In the process of authentication, Eve even may get some sample tag signal. But Eve cannot get useful related peak. So the success rate of Eve is still limited to 1/|K|. That is the same as guessing the key. Specific analysis is made on different attacks against Eve.

5.1 Passive Eavesdropping

In some cases, it is the Contact Volume Editor that checks all the pdfs. In such cases, the authors are not involved in the checking phase.

This method realizes the hidden transmission of the tag signal. In general, due to the location of Bob and Eve won't be exactly the same, the legal channel hAB is not related to hacking channel hAE. So Eve cannot obtain legal channel information. The

assumption on position of Eve is very reasonable in actual communication system, and it is also very easy to satisfy [14]. On the other hand, Alice and Bob's key are pre-allocated safely, and Eve is not available. Since the tag signal is generated by the channel information and the key, this is equivalent to "double locks" for the tag signal. Eve cannot obtain any information about the tag signal.

In the process of signal transmission, the design of matched filter needs to know the frequency response of the signal. It is difficult for Eve to receive and detect the tag signal. Even if Eve get part information of the tag signal by using the method of statistical signal processing, it is still difficult to pose a security threat. Because the channel is time-varying, the tag signal has a natural of timeliness and it made useless for Eve's passive eavesdropping.

5.2 Substitution Attack

Eve can attack by eavesdropping and modifying the signal that Alice sends. Eve will firstly remove the legal tag signal and then attach a forged tag signal. If the signal is received and passed through authentication successfully by Bob, Eve's attack is considered successful. The probability of successful attack is represented by β, which indicates the probability that Bob will receive the signal sent by Eve.

Because the tag signal is generated by a one-way hash function based on the channel and key, Eve can generate the tag signal by guessing the channel and key, or simply forging the tag signal. For a particular key K, if the inconsistency probability of the fake tag with the legal tag is less than Γ, the attack is successful. Therefore, the attack rate can be expressed as:

$$\beta = P(\rho < \Gamma) = \sum_{i=1}^{\Gamma M} C_M^i (\frac{1}{2})^i (\frac{1}{2})^{M-i} = \sum_{i=1}^{\Gamma M} C_M^i (\frac{1}{2})^M \tag{6}$$

It is analyzed that Eve was less likely to acquire a tag signal through passive eavesdropping. So it is difficult to make a successful attack, even in a passive and alternative way.

5.3 The Attack of Man-in-the-Middle

Assuming that Eve adopts an aggressive way of amplifying and forwarding, this type of attack is also known as transparent forwarding. Eve doesn't change the signal. According to the system model, the signal Bob received is changed to:

$$y = (x * h_{AE} + n_{AE}) * h_{EB} + n_{EB} \tag{7}$$

After finishing, it becomes:

$$y = x * (h_{AE} * h_{EB}) + (n_{AE} * h_{EB} + n_{EB}) \tag{8}$$

It can be seen that both the channel and the noise of Bob have changed. In (8), $n_{AE} * h_{EB} + n_{EB}$ is considered to be new noise. The channel between Alice and Bob h_{AB} becomes the cascade of the channel h_{AE} and h_{EB}. The conditions for the reciprocity of Alice and Bob are still satisfied. At the same time, because of Eve's involvement, Bob received a signal that was mixed with Eve's noise. The increase of noise may worsen the signal-to-noise ratio, which has an impact on the performance of the authentication. But Eve is unable to implement the replacement of Alice, and there is no difference in tag signal acquisition with passive eavesdropping.

6 Simulation Analysis

BPSK is exampled as the communication signal. The m-sequence with a length of 100 bits is used as the spread spectrum sequence. The channel parameters obey 3GPP standard Urban channel model, and 10,000 times of monte-carlo simulation is adopted.

Firstly, the influence of power distribution of the tag signal and communication signal is shown in Fig. 3. Because they are superimposed in the time domain, an important measurement is the proportion of power distribution. Making SNR = 10 dB as a typical value, the simulation is carried out when spread spectrum code length is 100 bits. It can be seen from Fig. 3(a), when tag power accounted for more than 1%, false alarm rate and missing alarm rate achieve a lower level. Because the amplification gain can resist the equivalent interference, the normal demodulation of the communication signal is not affected when the label power ratio is less than 50%. And the bit error rate is stable. Keeping 10% of the tag signal power ratio, simulation is carried out under different signal-to-noise ratio in Fig. 3(b). It can be found that in low SNR, false alarm rate and the bit error rate are both high, and it can achieve good indicators when SNR is higher than 10 dB.

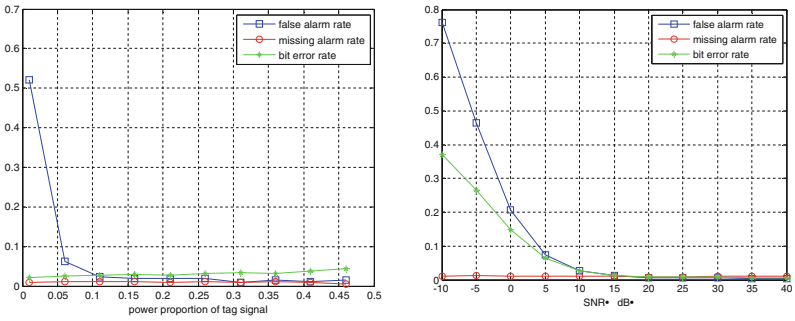


Fig. 3. Simulation diagram of performance, (a) power proportion, (b) SNR

7 Conclusion

The method of overlaying tag signal authentication in physical layer can get rid of the cipher algorithm. The dual authentication of channel and identity is realized at the signal

level. It can reduce the computational complexity in the process of communication, and achieve security enhancement to the existing authentication process. It also can be used to make up for the defect of business data authentication, and can be applied to "light-weight" authentication of the future mobile communication in low delay, high reliable scenarios.

References

1. Li, Z., Zhan, B., Yang, Y.: A survey of identification and authentication. Acta Electron. Sin. **27**(1), 98–102 (1999)
2. Maurer, U.M.: Authentication theory and hypothesis testing. IEEE Trans. Inf. Theory **46**(4), 1350–1356 (2000)
3. Yuan, H.: Research on key technologies of wireless network physical layer authentication based on radio frequency fingerprinting, Ph.D. dissertation. Southeast University (2011)
4. Paul, L.Y., Baras, J.S., Sadler, B.M.: Physical-layer authentication. IEEE Trans. Inf. Forensics Secur. **3**(1), 38–51 (2008)
5. Zeng, K., Govindan, K., Mohapatra, P.: Non-cryptographic authentication and identification in wireless networks. IEEE Wireless Commun. **17**(5), 56–62 (2010)
6. Xiao, L., Greenstein, L.J., Mandayam, N.B., et al.: A physical-layer technique to enhance authentication for mobile terminals. In: Proceedings of IEEE International Conference on Communications, Beijing (2008)
7. Tugnait, J.K., Kim, H.: A channel-based hypothesis testing approach to enhance user authentication in wireless networks. In: Proceedings of Second International Conference on Communication Systems and Networks, Bangalore (2010)
8. Shukla, M.K., Trivedi, A., Pandey, O.J.: Physical layer authentication for mobile terminals over MIMO fading wiretap channels. In: Proceedings of International Conference on Advances in Computing, Communications and Informatics, Mysore (2013)
9. Shan, D., Zeng, K., Xiang, W., et al.: PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks. IEEE J. Sel. Areas Commun. **31**(9), 1817–1827 (2013)
10. Du, X., Shan, D., Zeng, K., et al.: Physical layer challenge-response authentication in wireless networks with relay. In: Proceedings of IEEE International Conference on Computer Communications (2014)
11. Molière, R., Delaveau, F., Ngassa, C.L.K., et al.: Tag signals for early authentication and secret key generation in wireless public networks. In: Proceedings of European Conference on Networks and Communications, Paris (2015)
12. Liu, Z., Xu, J., Zhao, K.: Spectrum water printing technology based on spectrum signal. J. Hebei Univ. Sci. Technol. **S1**, 116–118 (2011)
13. Zhang, Y., Xu, J., Liu, Y., et al.: Spectrum tag embedding and extracting method based on correlation identifier. Chin. J. Radio Sci. **31**(1), 185–192 (2016)
14. Jakes, W.C., Cox, D.C.: Microwave Mobile Communications. Wiley, Hoboken (1994)

Distributed Cloud Forensic System with Decentralization and Multi-participation

Xuanyu Liu[1], Xiao Fu[1(✉)], Bin Luo[1], and Xiaojiang Du[2]

[1] State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing, China
dzl532002@smail.nju.edu.cn,
{fuxiao,luobin}@nju.edu.cn
[2] Department of Computer and Information Sciences, Temple University, Philadelphia, PA 19122, USA
dxj@ieee.org

Abstract. A considerable number of cloud forensic systems and tools have been proposed in recent years. Trust issue of digital evidence, a significant security topic, is indispensable for cloud forensics systems. In this paper, we propose a different cloud forensic system—Distributed Cloud Forensic System with Decentralization and Multi-participation (DCFS). The DCFS is set in an untrusted and multi-tenancy cloud environment, and it is assumed that cloud users, cloud employees, or forensic investigators can be dishonest. The DCFS, which is different from existing centralized cloud forensic systems, is a distributed and decentralized system that does not rely on any single node or any third party to obtain credible evidence from the cloud. Trust is divided into all participants in the DCFS, and these participants supervise each other. A distributed public ledger is maintained in the DCFS, and this ledger records all the proofs of forensic evidence along with other useful information. This ledger can enhance the credibility and integrity of forensic evidence to some degree and complete the chain of custody in forensic investigation. The forensic evidence, which are provided by the cloud employees, presented to the court of law using the DCFS will be more trustful.

Keywords: Cloud forensics · Data provenance · Byzantine faults
Distributed systems · Decentralization · Multi-participation

1 Introduction

Cloud forensics is a cross discipline of cloud computing and digital forensics. Digital forensics is the application of computer science principles to recover electronic evidence for presentation in a court of law. Most of the existing cloud forensic systems and tools are set in non-adversarial environment, and they precisely consider the

This work is supported by the National Natural Science Foundation of China (61100198/F0207, 61100197/F0207).

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 181–196, 2018.
https://doi.org/10.1007/978-3-319-90802-1_16

external threats. That is, they trust the cloud service providers completely. In return, this brings the honesty issue of the cloud service providers. Forensic investigators and court authorities may also doubt about the credibility and validity of evidence. It is undeniable that a few studies have tried to reveal the trust issues in cloud forensics. They prefer to trust the cloud service providers partially or reduce their trusted computing base by introducing some trusted components such as monitor, hardware, or database into their methods. In a multi-tenancy environment, they may attempt to pick a trusted third party [1] as an intermediary to store or verify forensic evidence. In short, these solutions are centralized so that their functions rely on a single point. Moreover, the trust of forensic evidence is established on the basis of this point. Unfortunately, neither a single component nor a third party is invariantly trustworthy. Components may exhibit loopholes or bugs and could be compromised by an adversary. A third party can also collude with malicious individuals to hide their crimes for the purpose of illegal income. Both of them can become the single failure point and can cause performance and security issues easily. Existing cloud forensic systems are unsatisfactory to some extent. It is necessary to have alternative forensic systems or tools that do not require this type of trust.

In this paper, we propose a different cloud forensic system—Distributed Cloud Forensic System with Decentralization and Multi-participation (DCFS) from another perspective. The DCFS is set in an untrusted and adversarial environment. It does not trust any single node or any single person and considers both internal and external threats. The DCFS is a distributed cloud forensic system. It does not precisely operate for a single node but for a large-scale network with numerous nodes. These nodes act together to build a more secure and more robust cloud forensic ecosystem. Decentralization indicates that the DCFS does not rely on a trusted component or a trusted third party. Trust is divided among the nodes in the DCFS, and these nodes supervise each other. Multi-participation indicates that the DCFS acts in a multi-tenancy environment with various stakeholders, including users, cloud employees, forensic investigators, and court authorities. It has the assumption that cloud customers, cloud service providers, or forensic investigators can be malicious or dishonest; they may collude with each other to provide faked forensic evidence or may frame innocent people.

Data provenance is selected as the primary raw data of forensic evidence in the DCFS. Data provenance determines and describes the lifecycle history of data sets from original resources to destruction endpoints. It is helpful for analyzing what happened to certain dataset and estimating its scope of influence among the systems. The accountability of the cloud can be enhanced using data provenance. To make data provenance more available and more credible, a public data provenance ledger is introduced into the DCFS. This ledger has something in common with the public ledger maintained in Blockchain [2] systems. A Blockchain system is essentially a distributed ledger of all transactions or digital events executed and shared among all participants in accounting systems. Each transaction in the public ledger is verified by consensus of a majority of the participants. Once recorded, these transactions can never be erased. With same purposes, the public data provenance ledger in the DCFS is a distributed ledger of all proofs of data provenance and other valuable information useful for further forensic investigation. The participants in the DCFS involve in the maintenance of this ledger and reach a consensus on its entries. Every data provenance recorded in the

ledger is verifiable, accountable, and immutable. Any misbehavior, which can be Byzantine [3], performed to the ledger is not hidden and is rejected. With this, we develop a democratic open and scalable forensic system from a centralized one. To the best of our knowledge, the DCFS is the first decentralized cloud forensic system that do not rely on any single point or third party as well as no single point or third party has absolute power to affect the forensic process. The DCFS can enhance the credibility and integrity of forensic evidence, enhance the accountability and robustness of cloud systems, and complete the chain of custody in forensic investigations. To demonstrate the practicality and security of the DCFS, we have implemented a prototype on OpenStack, which is an open source cloud computing platform. Our evaluation demonstrates the ability of the DCFS to solve the real world forensic problems, and the results reveal that the costs of the DCFS (CPU load, network latency and storage) are sufficiently low to be practical.

Motivation. Most of the existing cloud forensic systems trust their cloud service providers completely or partially and trust forensic investigators acquiescently. The DCFS, which is different from those forensic systems, does not believe in cloud employees and forensic investigators. The goals of the DCFS are as follows:

- Make forensic evidence from cloud more available and accessible.
- Enhance the credibility and integrity of forensic evidence.
- Ensure that any evidence entry presented in front of the court is verifiable.
- No one can tamper with any evidence entry and any misbehavior performed to evidence entries will be discovered and prevented.
- Malicious individuals can never repudiate evidence indicating them.
- No one can recover any valuable information from the DCFS so that the privacy of the user remains protected.

Contributions. The contributions of this paper are as follows:

- We proposed the DCFS. The DCFS is set in untrusted and adversarial multi-tenancy environment and does not rely on any single trusted node or third party. The DCFS overcomes the drawbacks of centralized cloud forensic systems and makes the cloud more accountable and robust.
- We design a public data provenance ledger for the DCFS. This ledger helps the forensic investigators and court authorities to obtain valid and credible evidence. Moreover, it can prevent malicious individuals from tampering or denying the forensic evidence after the fact.
- The DCFS is implemented and evaluated on OpenStack.

Organization. The structure of the paper is organized as follows: Sect. 2 discusses some related studies. Section 3 introduces the design of the DCFS in detail. Then, Sect. 4 provides the security analysis of the DCFS. Section 5 provides the implementation and evaluation of the DCFS, and Sect. 6 concludes this paper.

2 Related Work

There have been several studies on collecting and providing data provenance. PASS [13] is a typical provenance system in the system level. It modifies the Linux kernel and intercepts system call in the VFS level. Based on PASS, a provenance system for XEN [14] is established. SPADE [15] focuses on the related primitive operation on data input and output, and detects system calls of files and processes. LineageFS [16] associates the process ID with file descriptors and creates lineage information for files. Hi-Fi [17] includes various types of nonpersistent data into data provenance. LPM [18] is deployed in Linux kernel and is designed to collect system-wide data provenance, including process, IPC, network, and system call. Based on LSM, the LPM set provenance hooks along with LSM hooks, ensuring that the data provenance represents the proper actions of the system. DPAPI [19], CPL [20], and IPAPI [21] are set in the application level. They provide specific provenance API so that the application developers can invoke these APIs to make their applications provenance aware. HadoopProv [22] realizes a provenance system in Hadoop. In Android platform, Quire [23] extracts the provenance data from IPC and RPC to construct invocation chain. By analyzing this invocation chain, the potential attacks such as excess of authority can be discovered. Similar to Quire, Scippa [24] expands the Binder module in Android system to construct an invocation chain.

However, these systems or tools still lack in providing trustworthy data provenance. They do not consider the internal threats, and they depend only on their host systems. Some researchers tried to solve these issues. The SNP [25] is a network provenance system running in an adversarial setting. Every node manages its own tamper-evident network logs. By querying the relevant information from other nodes, fault nodes can be discovered. However, the SNP relies on some types of behaviors on the network to be observed by at least one correct node, and the error nodes can escape easily from the detection of the SNP by colluding with each other. Moreover, the efficiency of SNP will drop drastically with a reduction in the correct nodes available in the system. Another system, SecLaaS [26], assumes that users, clouds, and investigators can be malicious individually or can collude with each other. It creates the proofs of logs and publishes these proofs on the web for further verification. The drawback of this system is that the proofs are considerably coarse grained, and the proofs remain unprotected after being published. Other researchers attempt to adopt cryptography, trusted computing, or mathematics to enhance the integrity and confidentiality of data provenance, such as ABE [27] and bilinear pairing [28]. The scope of their application is small and may cause considerable resource consumption. Several papers (e.g., [29–34]) have studied related security and networking issues.

Different from them, the DCFS runs in an adversarial multi-tenancy cloud environment. It is a distributed and decentralized forensic system, and it does not rely on any single trusted node or third party. The participants in the DCFS cooperate with each other to make the evidence entries more trustworthy.

3 System Design

3.1 System Structure

In the DCFS, participants are scattered in different cloud systems. A small and smart process named DCFS Peer Agent (DPA) is allocated to every participant. The DPAs act as agents for participants and enable them to join in the DCFS membership network, involve in the DCFS cloud forensic system, manage their personal data, and conduct operation requests. Figure 1 shows the system structure of DCFS, which can be divided into three layers:

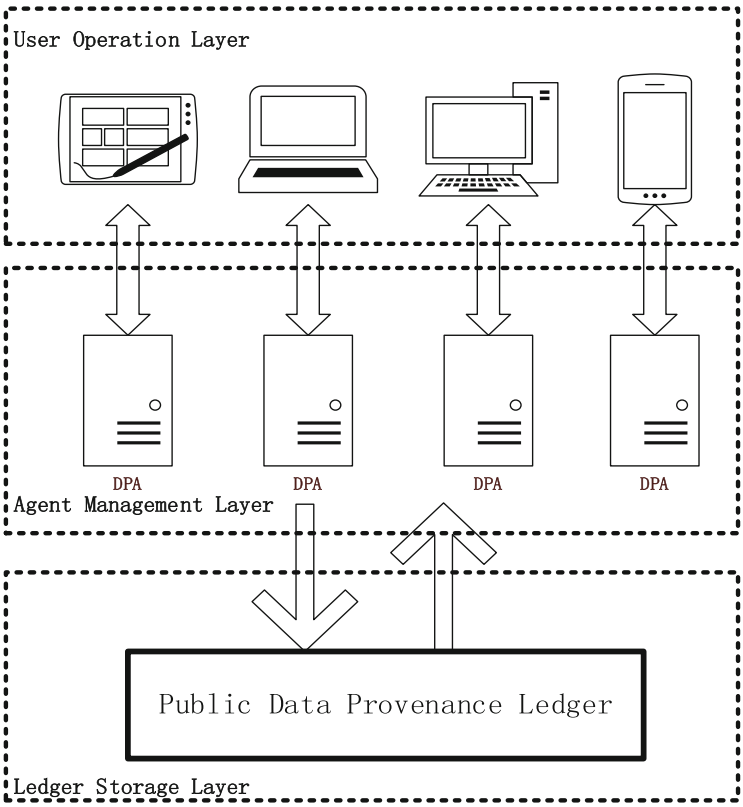


Fig. 1. System structure of the DCFS

User Operation Layer. This layer consists of all participants along with their terminal applications installed in their PCs, smart phones, or even in a third-party cloud platform. These terminals are management consoles for participants to communicate with their DPAs, commit their operation requests, and manage their personal data. They can also manage their individual accounts, check the DCFS network topology, and examine the DCFS runtime information. Investigators and court authorities can use customized terminals to verify the integrity and validity of forensic evidence.

Agent Management Layer. The DPAs are mainly located in this layer. They are independent, and they connect with each other to establish a point-to-point network. Certain consensus algorithm is adopted to ensure that these DPAs are in the same final state and reach a consensus on the public data provenance ledger. Moreover, the DPAs are responsible for managing data entries in the public ledger, acting as a gateway that evaluates all data accesses, and communicating with terminal applications to handle the received operation requests.

Ledger Storage Layer. In this layer, a public provenance ledger offers a scalable, highly available, secure, and independent storage service for data provenance against confidentiality and integrity attacks. This public ledger is not precisely located in a single node or stored on the database of a third party. Instead, it is a distributed ledger and all participants own a full copy of this ledger in their database. The DPAs of the participants reach a consensus on the ledger and ensure the contents of each ledger stored in different participants' database are consistent. Any malicious activity performed to the ledger is unacceptable to the other correct DPAs unless majority of DPAs are under control by an attacker. It is not invariantly easy to control majority of DPAs in a large-scale cloud system. This design guarantees that any data entry recorded in the ledger remains unchanged once generated. No one, including users, cloud employees, or investigators can tamper with the ledger.

3.2 DCFS Peer Agent

As Fig. 2 shows, a DPA mainly consists of three modules: Data Manager, Operation Handler, and Membership Service.

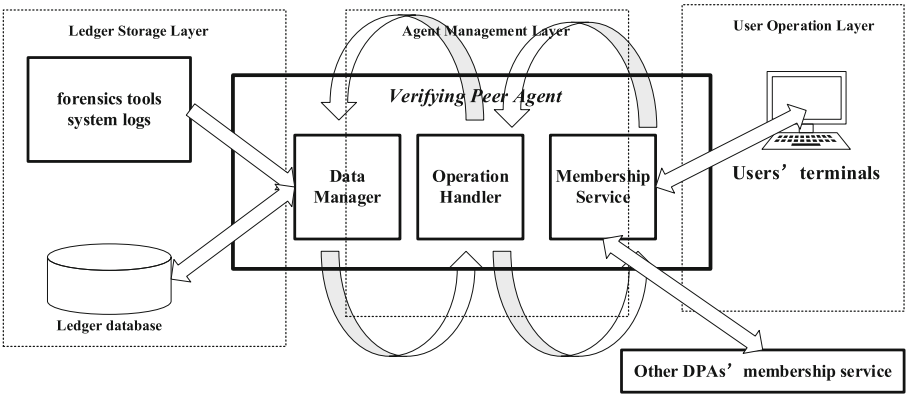


Fig. 2. Modules of the DPA. Data Manager is the medium between Ledger Storage Layer and Agent Management Layer. Membership Service is the medium between Agent Manager Layer and User Operation Layer.

Data Manager. The primary responsibility of Data Manager is to create raw proofs of data provenance using data provenance metadata from forensic tools and other useful system logs. These raw proofs of data provenance will be sent to Operation Handler for

further encapsulation and then sent to Membership Service for consensus process. Data Manager is also in charge of communicating with the database for public ledger.

Operation Handler. Operation Manager handles operation requests such as query and verification. When receiving an operation from a user, Data Manager searches satisfactory data from the public provenance ledger, verifies its validity, and packages the data in a proper manner.

Membership Service. The main duty of Membership Service module is network communication. It communicates with the terminals of the participants to receive operation requests from users and respond to them. It also connects with the other Membership Service modules of the DPAs to build the distributed forensic network. Moreover, it manages and evaluates data access policy for each participant.

3.3 Public Data Provenance Ledger

The public data provenance ledger is the core of the DCFS. Only the proofs of data provenance are included in the ledger for the following reasons:

- Raw data provide huge storage and network consumption while proofs are more lightweight.
- The main goal of the DCFS is to offer the ability to verify the correctness of evidence. The proofs of data provenance are sufficient.
- Malicious individuals may try to learn about some crucial information of other users from the ledger. If only proofs are included, nearly no valuable information can be recovered from them. The privacy of the users will remain protected.

The process from raw data to entries in the ledger includes four steps: First, a data provenance graph is generated using the raw data provided by forensic tools and system logs. Second, a new proof is created based on the data provenance graph. Third, with necessary encapsulation, the proof is added into the ledger. Finally, a consensus process is started between DPAs to ensure that all DPAs agree and accept this proof.

Data Provenance Graph. Forensic tools for cloud computing should be compatible with the cloud's characteristics of on-demand self-service, rapid elasticity, and scalability. This indicates that the data provenance model should be easy to generate and manage, be open, extensible, and scalable, and be compatible with existing forensic formats and follow existing practices and standards. Based on the above consideration, Open Provenance Model (OPM) [4] is selected as the standard data provenance format in the DCFS. The OPM defines data provenance in a precise and technology-agnostic manner and allows multiple levels of data description to coexist. It allows provenance information to be exchanged easily between systems based on a shared provenance model.

The provenance graph is a directed acyclic graph (DAG), and it implies causal relationships between states and operations. To capture transitive provenance, we can define, for any execution e, a provenance graph $G(e) = (V(e), E(e))$, in which each vertex $v \in V(e)$ represents a state or operation, and each edge (v1, v2) represents that v1 causes v2. It also indicates that the data provenance of v1 is a part of that of v2.

From the provenance graph, we can easily identify the problem's origin and estimate the scope of influence it had created to the entire system. It is helpful for forensic investigations.

The entire system may face the problem of provenance explosion. To reduce the amount and complexity of data provenance and relieve the burden of the system, methods from [5, 6] are adopted. The data provenance entries, having little or no impact on forensic analysis, will be recycled. Therefore, the size of the data provenance graph is reduced, and the proofs can be easily generated.

Proof of Data Provenance. Proofs should be easy to use and hard to forge. Many systems use Merkle trees [7] as their basic data structure for verification, such as Bitcoin and P2P network. Mostly, it is a binary tree, but it can also be a multi-way tree. The value of leaf nodes in the tree is the cell data in the dataset or its hash value. The value of a nonleaf node is calculated by hashing all its child nodes' values. Recursively, the hash value of the tree root is generated, and the entire tree is completed. Merkle tree stores the summary information about a large dataset to make the verification more efficient. It is unnecessary to reveal or transmit the entire tree, and it natively enables a user to validate the integrity of any subset of data.

The DCFS selects the Merkle tree as its data format for proofs. The steps from the data provenance graph to the Merkle tree are shown in Fig. 3. First, a topological sort of all nodes in the data provenance graph is generated. Because the topological sort of a directed acyclic graph is not unique, this step uses timestamps as another parameter. For nodes in the same topological layer, they are sorted again in ascending order by their timestamps. Second, leaf nodes in the Merkle tree are filled with topologically sorted nodes' hash value, and the other part of the tree is calculated based on these leaf nodes. Subsequently, the value at each branch node is calculated by concatenating the values of its children and computing the hash of that aggregation. Finally, the value of the root node is selected as the proof of the data provenance graph.

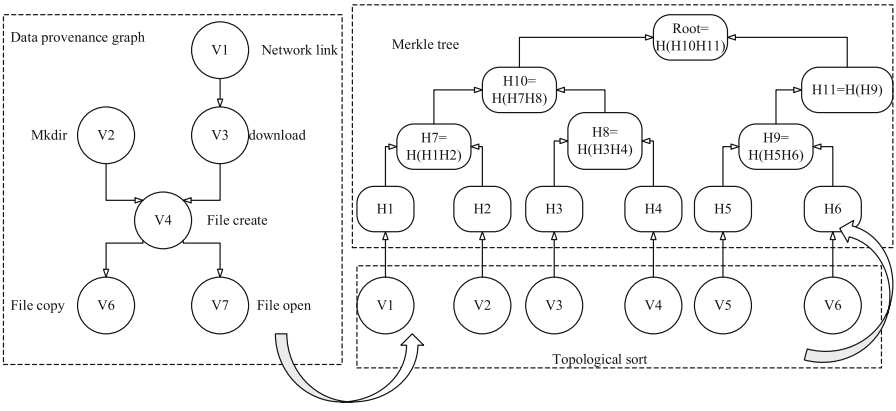


Fig. 3. Steps from data provenance graph to Merkle tree

Proof Chain. The public ledger is a chain of proof entries, and each entry contains the proof of data provenance graph and other essential information to ensure its irreversibility.

To preserve the correct order of the entries in the ledger, an Entry Chain (EC) is introduced. This Entry Chain is a hash chain. Entry Chain will be generated as follows:

$$\mathrm{EC} = <\mathrm{Hash}(\mathrm{Proof}, \mathrm{ECprev})> \tag{1}$$

where ECprev is the Entry Chain of the previous entry in the ledger, and Proof is the proof information in this entry.

A Proof Entry consists of EC, proofs of data provenance, user id, domain id, and timestamp:

$$\mathrm{Proof\,Entry} = <\mathrm{EC},\ \mathrm{Proof},\ \mathrm{UID},\ \mathrm{DID},\ \mathrm{Timestamp}> \tag{2}$$

Consensus Process. The DCFS is set in an adversarial setting and any misbehavior happened could be Byzantine. To reach a consensus on the public data provenance ledger between DPAs, the DCFS realizes its consensus process based on the PBFT [8] algorithm.

For efficiency and better management, the DPAs will be classified into different domains. For example, the DPAs in the same host machine or having the same cloud administrator will be categorized under the same domain. In each time interval, a domain itself will select a leader DPA to lead affairs. This leader DPA will convey the operation requests, guide the consensus process, and communicate with other domains. When a user desires to perform an operation request, the processing procedure is as follows: First, the DPA of this user receives the operation request and transports it to the leader DPA. Then, the leader DPA will transport the operation request to the other DPAs in its domain and the leader DPAs of the other domains. Next, all the DPAs will handle this operation request and return the results to the DPA of the user. Finally, this DPA handles the received results and return them to the user's terminal.

The pseudocode description of the consensus algorithm is showed in the Appendix.

4 Security Analysis

The cloud has full control over generating the data provenance. The DCFS functions based on an assumption that the process of generating the data provenance is trusted. It focuses on helping the investigators and court authorities to verify the evidence using the proofs included in the DCFS ledger. The participants reach a consensus on this ledger, and trustful proofs are invariantly available. The DCFS guarantees that any violation of ledger's integrity will be prevented and evidence tampered with will finally be detected during the verification process.

In the DCFS, three entities are involved: users, cloud employees, and investigators. All of them can be malicious individually or can collude with each other. However, at the verification stage, any misbehavior can be detected using the public provenance ledger. Figure 4 illustrates the detailed flow of evidence verification. Based on the evidence entries provided by a cloud employee, an investigator can calculate its proofs and fetch the corresponding proofs from the public ledger in the DCFS. If the two proofs are equal, the investigator may trust these evidence entries and present them to the court. Otherwise, he can reject them and doubt the honesty of the cloud employee. When the court receives the evidence, it first checks the ownership information from the ledger to judge whether an innocent is framed. Then, it fetches the corresponding proofs from the public ledger again to compare with the proofs of the received evidence. If they are equal, the court will accept the evidence. Otherwise, the evidence will be rejected, and the court doubts the honesty of the investigator.

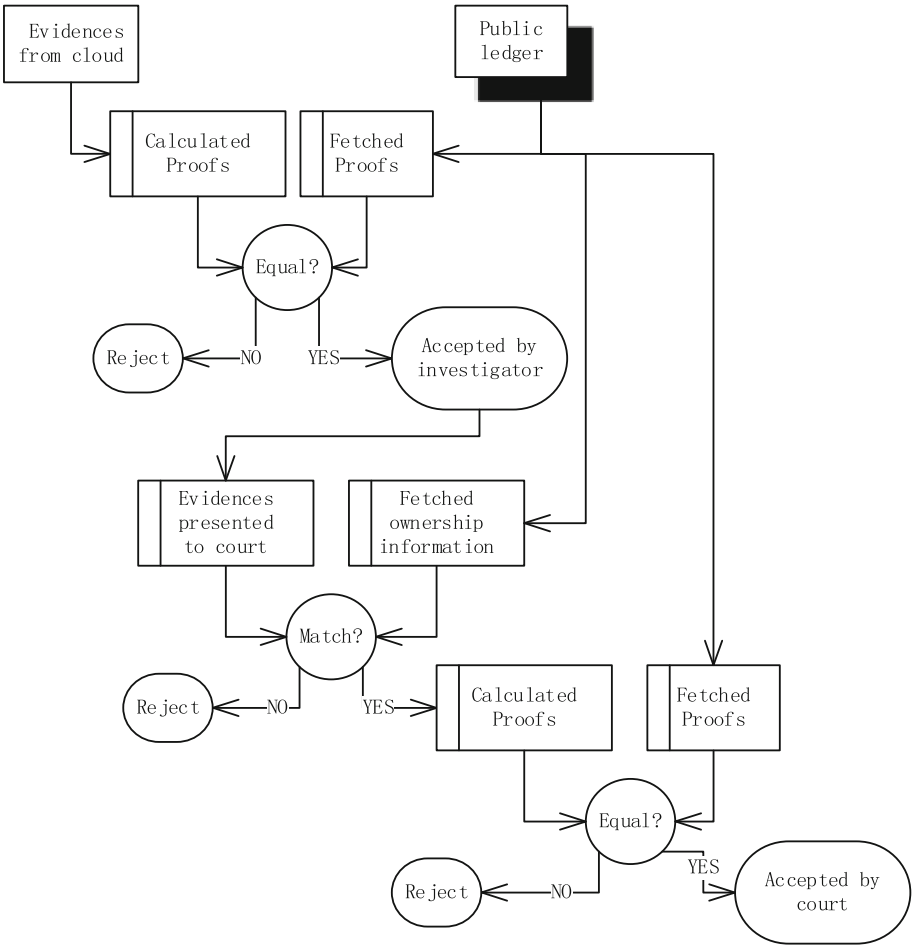


Fig. 4. Process flow of evidence verification

The DCFS is a distributed and decentralized cloud forensic system, and all participants reach consensus on a distributed public ledger. Few malicious participants have limited impact on the entire system unless they can control the majority of the DPAs. We assume that any misbehavior happened in the DCFS can be Byzantine, and we design our consensus process based on the PBFT algorithm. This algorithm guarantees liveness and safety under the premise that provides a fault tolerance of $(n - 1)/3$, where n is the total number of participants. This indicates that malicious participants should not be more than one third of all participants for safety. With a greater number of participants, the DCFS will become more secure and stable. In other words, the DCFS will be more useful in a large-scale system.

A brief proof is as follows: Define n as the number of all nodes and f as the number of faulty nodes. An assumption for asynchronous Byzantine agreement is that correct nodes will send precisely one correct message to others in each phase while the faulty nodes may send more than one message to confuse others. A minimum of $(n + f)/2$ received messages are essential to reach an agreement on a message [9]. It is invariantly possible for a node to accept $n - f$ messages. Consider a correct node n in phase p, where n has already sent a message to all the other nodes. As there exists a minimum of $n - f$ correct nodes, the n's buffer will receive a minimum of $n - k$ reply messages. The $n - k$ should outnumber $(n + f)/2$, i.e., $n - f > (n + f)/2$. Therefore, $f < n/3$.

As only hash results and some necessary identification information are included in the public ledger, the malicious individuals can barely recover any valuable information from the ledger.

5 Implementation and Evaluation

We implemented our prototype system on three desktop computers with Intel(R) Core (TM) i5-3330 3.00 GHz CPU, 8 GB main memory, and 256 KB L2 cache. Ubuntu 14.04 LTS 64-bit was used as Host Operating System, and Openstack was selected for implementation and evaluation. Virtual environment was created with XEN, and each desktop computer runs five VM instances so that there were 15 participants in total. We used SHA-2 (SHA-256) hash function for hashing. A containerization runtime environment for DPAs was established using Docker [10]. Using FROST [11], we obtained API logs from Nova nodes as metadata for generating data provenance.

For easy deployment and management, the DPAs were deployed in Docker containers and were isolated. The gRPC [12] was used for establishing point-to-point network connections between DPAs. Certainly, DPAs can be deployed anywhere as long as there are network capabilities. For example, DPAs can also be embedded into the VM instances of a user or even be located in a third party cloud platform.

The DCFS operates under a normal environment in our experiments. In order to evaluate the impact on the performance of the DCFS, we compared the CPU load, network latency, and storage consumption under the condition of running our forensic system (Table 1).

Table 1. Performance impact

	Performance impact
CPU load	Increasing 2.5% on average
Network latency	Increasing 10% on average
Storage consumption	10 MB a day for each DPA

The system delay was within an acceptable range compared with SNP [25] and SecLaaS [26]. However, at the peak of system operation, the DCFS may have a remarkable effect on the host system. To be practical in normal commercial environment, some optimizations are essential. We have left this for future research.

6 Conclusion and Future Work

Collecting forensic evidence from cloud is a challenging task because forensic investigators have considerably little control over cloud systems. Currently, forensic investigators still depend on cloud service providers to obtain forensic evidence. To the best of our knowledge, there is no procedure to verify whether the cloud service providers have provided the correct evidence to the investigators. Forensic investigators may also present invalid evidence to the court. In this paper, we proposed a different cloud forensic system DCFS from another perspective. The DCFS considers internal threats and provides the ability to securely obtain trustful data provenance for forensic purpose. It can also solve some issues existed in traditional centralized forensic systems. From our experiment, we observed that it is practically feasible to combine the DCFS with the cloud infrastructure.

One limitation of the DCFS is that it still requires some trust in the cloud. In particular, we have to trust that the generation of data provenance from the cloud is correct. This can be relieved by using tamper-evident logging such as Peer Review [35]. In future, we will investigate to make our system more efficient, practical, and expansible so that it can be compatible with more cloud architectures and based on DCFS, we will try to bring cooperative forensics and shared security into more distributed systems or IoT systems.

Appendix

The algorithm of a consensus process on an operation request is as follows:

```
if leader DPA then
   n=deployIdToOperation(received operation request)
   sendStepOneMessageToAll (leader ID, n, checksum, re-
quest)
else if not leader DPA then
   WaitForStepOneMessage()
end if
m1=receivedStepOneMessage
if m1.leaderID is right&&m1.checksum is right&&m1.n is
never used&& m1.n is within minimum and maximum then
    AcceptStepOneMessage()
    sendStepTwoMessageToOthers(leader ID, this DPA's
own ID, n, checksum, request)
    waitForStepTwoMeaasgeFromOthers()
else
    doNothing()
end if
Message[ ] m2=all receivedStepTwoMessage
na2=numOfAcceptedStepTwoMessage
define F as the tolerable maximum of fault DPAs
for all m in m2 do
    if m.leaderID is right&&m. DPA's own ID is tight&&
m.checksum is right&&m.n is never used&&m.n is within
minimum and maximum&&m.StepOneMessage is accepted then
     AcceptStepTwoMessage()
     na2++
   end if
end for
If na2>2F then
    sendStepThreeMessageToOthers(leader ID, this DPA's
own ID, n, checksum, request)
    waitForStepThreeMeaasgeFromOthers()
else
```

```
    doNothing()
end if
Message[ ] m3=all receivedStepThreeMessage
Na3=numOfAcceptedStepThreeMessage
for all m in m3 do
   if m.leaderID is right&&m. DPA's own ID is tight&&
m.checksum is right&&m.n is never used&&m.n is within
minimum and maximum&&m.StepTwoMessage is accepted then
     AcceptStepThreeMessage()
     na3++
   end if
end for
If na3>2F then
recordOperationRequestWithIDLocally(n)
else
    doNothing()
end if
```

References

1. Santos, N., Gummadi, K.P., Rodrigues, R.: Towards trusted cloud computing. HotCloud **9** (9), 3 (2009)
2. Pilkington, M.: Blockchain technology: principles and applications (2015)
3. Lamport, L., Shostak, R., Pease, M.: The Byzantine general problem. ACM Trans. Program. Lang. Syst. (TOPLAS) **4**(3), 382–401 (1982)
4. Moreau, L., Clifford, B., Freire, J., et al.: The open provenance model core specification (v1.1). Future Gener. Comput. Syst. **27**(6), 743–756 (2011)
5. Lee, K.H., Zhang, X., Xu, D.: High accuracy attack provenance via binary-based execution partition. In: NDSS (2013)
6. Lee, K.H., Zhang, X., Xu, D.: LogGC: garbage collecting audit log. In: Proceedings of the 2013 ACM SIGSAC Conference on Computer and Communications Security, pp. 1005–1016. ACM (2013)
7. Merkle, R.C.: A digital signature based on a conventional encryption function. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 369–378. Springer, Heidelberg (1988). https://doi.org/10.1007/3-540-48184-2_32
8. Castro, M., Liskov, B.: Practical Byzantine fault tolerance. In: OSDI, vol. 99, pp. 173–186 (1999)
9. Bracha, G., Toueg, S.: Asynchronous consensus and broadcast protocols. J. ACM (JACM) **32**(4), 824–840 (1985)

10. Merkel, D.: Docker: lightweight linux containers for consistent development and deployment. Linux J. **2014**(239), 2 (2014)
11. Dykstra, J., Sherman, A.T.: Design and implementation of FROST: digital forensic tools for the OpenStack cloud computing platform. Digit. Invest. **10**, S87–S95 (2013)
12. gRPC Homepage. http://www.grpc.io/
13. Muniswamy-Reddy, K.K., Holland, D.A., Braun, U., et al.: Provenance-aware storage systems. In: USENIX Annual Technical Conference, General Track, pp. 43–56 (2006)
14. Macko, P., Chiarini, M., Seltzer, M., et al.: Collecting provenance via the Xen Hypervisor. In: TaPP (2011)
15. Gehani, A., Tariq, D.: SPADE: support for provenance auditing in distributed environments. In: Narasimhan, P., Triantafillou, P. (eds.) Middleware 2012. LNCS, vol. 7662, pp. 101–120. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-35170-9_6
16. Sar, C., Cao, P.: Lineage file system, pp. 411–414 (2005). http://crypto.stanford.edu/cao/lineage.html
17. Pohly, D.J., McLaughlin, S., McDaniel, P., et al.: Hi-Fi: collecting high-fidelity whole-system provenance. In: Proceedings of the 28th Annual Computer Security Applications Conference, pp. 259–268. ACM (2012)
18. Bates, A.M., Tian, D., Butler, K.R.B., et al.: Trustworthy whole-system provenance for the Linux Kernel. In: Usenix Security, pp. 319–334 (2015)
19. Muniswamy-Reddy, K.K., Braun, U., Holland, D.A., et al.: Layering in provenance systems. In: USENIX Annual Technical Conference (2009)
20. Macko, P., Seltzer, M.A.: General-purpose provenance library. In: TaPP (2012)
21. Carata, L., Sohan, R., Rice, A., et al.: IPAPI: designing an improved provenance API. Presented as Part of the 5th USENIX Workshop on the Theory and Practice of Provenance (2013)
22. Akoush, S., Sohan, R., Hopper, A.: HadoopProv: towards provenance as a first class citizen in MapReduce. In: TaPP (2013)
23. Dietz, M., Shekhar, S., Pisetsky, Y., et al.: QUIRE: lightweight provenance for smart phone operating systems. In: USENIX Security Symposium, vol. 31 (2011)
24. Backes, M., Bugiel, S., Gerling, S., Scippa: system-centric IPC provenance on Android. In: Proceedings of the 30th Annual Computer Security Applications Conference, pp. 36–45. ACM (2014)
25. Zhou, W., Fei, Q., Narayan, A., et al.: Secure network provenance. In: Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, pp. 295–310. ACM (2011)
26. Zawoad, S., Dutta, A.K., Hasan, R.: SecLaaS: secure logging-as-a-service for cloud forensics. In: Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, pp. 219–230. ACM (2013)
27. Li, J., Chen, X., Huang, Q., et al.: Digital provenance: enabling secure data forensics in cloud computing. Future Gener. Comput. Syst. **37**, 259–266 (2014)
28. Lu, R., Lin, X., Liang, X., et al.: Secure provenance: the essential of bread and butter of data forensics in cloud computing. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 282–292. ACM (2010)
29. Cheng, Y., Fu, X., Du, X., Luo, B., Guizani, M.: A lightweight live memory forensic approach based on hardware virtualization. Inf. Sci. **379**, 23–41 (2017)
30. Fu, X., Du, X., Luo, B.: Data correlation-based analysis method for automatic memory forensics. Secur. Commun. Netw. **8**(18), 4213–4226 (2015)
31. Wu, L., Du, X.: MobiFish: a lightweight anti-phishing scheme for mobile phones. In: Proceedings of the 23rd International Conference on Computer Communications and Networks (ICCCN), Shanghai, China, August 2014

32. Wu, L., Du, X., Fu, X.: Security threats to mobile multimedia applications: camera-based attacks on mobile phones. IEEE Commun. Mag. **52**(3), 80–87 (2014)
33. Du, X., Xiao, Y., Guizani, M., Chen, H.H.: An effective key management scheme for heterogeneous sensor networks. Ad Hoc Netw. **5**(1), 24–34 (2007)
34. Du, X., Guizani, M., Xiao, Y., Chen, H.H.: A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks. IEEE Trans. Wirel. Commun. **8**(3), 1223–1229 (2009)
35. Haeberlen, A., Kouznetsov, P., Druschel, P.: PeerReview: practical accountability for distributed systems. ACM SIGOPS Oper. Syst. Rev. **41**(6), 175–188 (2007)

On the Optimal Spectrum Partitioning in D2D Enhanced Cellular Sensor Networks

Liqun Zhao[1(✉)], Hongpeng Wang[1], and Xiaoxiong Zhong[2,3]

[1] School of Computer Science, Harbin Institute of Technology (Shenzhen), Shenzhen, Guangdong, China
lxzlq2005@126.com, wanghp@hit.edu.cn
[2] Graduate School at Shenzhen, Tsinghua University, Shenzhen, Guangdong, China
xixzhong@gmail.com
[3] Guangxi Key Laboratory of Trusted Software, Guilin University of Electronic Technology, Guilin, Guangxi, China

Abstract. Device-to-Device communication is a key technique in future cellular sensor networks since it provides short range communications between two adjacent devices in terms of power consumption, green communication, and system capacity as compared to conventional homogeneous cellular network. What is more, the D2D protocol not only provides direct communication to various kinds of devices but also bridges together two devices of wireless sensor and cellular device. However, the sensors reuse licensed channels with cellular devices and potential result in severe interference from each other. In this paper, we investigate the problem of optimal spectrum partitioning and the impacts of device density on outage probability in cellular sensor networks. We convert the throughput maximization problem in to an optimal spectrum partitioning problem with signal to interference plus noise ratio constraints. Simulation results show that the proposed algorithm achieves the higher throughput.

Keywords: D2D · Cellular network · Wireless sensor network
Interference management · Resource allocation

1 Introduction

Applications rely on WSNs (wireless sensor networks), such as mobile health (m-Health), military sensing and tracking, real-time road traffic monitoring, have been rapid increase in the past few years. However, there are two drawbacks exist in current WSN networks. One is that long distance wireless communication is not suit for WSNs due to the limited battery life of nodes. The other is no platform can support Internet services to WSNs. However, the future cellular network aims to provide controlled QoS (Quality of Service) and ubiquitous MTC (machine-type communication) to various kinds of devices. D2D (Device-to-Device) or M2M (Machine-to-Machine) communications have been considered as an interface to combine cellular network and sensor network. The details can be find in release 12 of MTC-LTE [1, 2]. The collaborative applications based on sensors would benefit from the ubiquitous coverage

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 197–209, 2018.
https://doi.org/10.1007/978-3-319-90802-1_17

and Internet services offered by future cellular networks when they equipped the required LTE chip and protocol [3]. Many works have been focus on the technique of connecting sensors to cellular devices, such as smart phones and tablet computers with cellular module [4, 5]. The application of cellular sensor network in environment protection and wearable sensor has been shown in [6, 7]. D2D technique allows two proximity devices directly communicate with each other instead of traversing the BS (Base station) to offload the increasing traffic. It not only improve the spectrum efficiency but also bridge the collected data by the sensors with the cellular network [8]. Although cellular sensor network with in-band D2D communication brought various benefits to sensor applications, it still meets many challenges in resource management due to critical interferences [9].

Recently, many works research on underlay D2D communications in cellular networks focus on co-channel interference management and resource allocation algorithm with in cellular networks [10–16]. In order to mitigate co-channel interferences, most of these works mainly focus on power control or intelligent resource allocation. In [10], the authors reduce interference and optimize the system throughput through power reduction. In [11], the authors defined a SINR (Signal to Interference plus Noise Ratio) threshold to D2D receiver. This result in some cellular devices cannot reuse channels with D2D devices due to severe interference and the interference problem can be alleviated. With regards to interference mitigation solutions based on resource allocation, many of the current works utilize the information of path loss or shadowing to design superior interference alleviated schemes. In [12, 13], the position-based and distance-based interference mitigation schemes are proposed. However, these schemes need to know the locations of devices and result in high control overhead. In [14], a resource allocation scheme which considers QoS (Quality of Service) for D2D communications has been proposed. However, these channel assignment algorithms often with high computational complexity and overhead. It is hard to implement nicely in cellular sensor networks due to considerable investment to develop and deploy [15, 16]. Nowadays, modeling the locations of base station as a PPP model has been proven to be accurate in terms of SINR distribution when compared to hexagonal grid model [17, 18]. Most of current works are based on hexagonal grid network model, which is not a universal mathematical tool for analytical system performance.

In this paper, we focus on the spectrum partitioning on CUEs (cell UE) and DUEs (D2D UEs and sensors) in a PPP (Poisson point process) model. Unlike [19] which only model the locations of UEs with PPP model and not encounter in sensors, i.e., the sensors cannot communicate with base station due to low transmit power. We also claim that sensors only communication with other sensors or CUEs only by using overlay D2D communications. Our objective is to find the optimal spectrum partitioning that maximizes the network throughput. The main contributions of this paper are summarized as follows: first we provide analytical expressions for the UE outage probability and ergodic rate to characterize the performance of UEs. Then, we convert the throughput maximization problem into an optimal spectrum partitioning problem which is expressed by the outage probability and UE ergodic rate.

The rest of this paper is organized as follows. Section 2 describes the D2D enhanced cellular network model and frame structure. In Sect. 3, we derive the UE outage probabilities that help us to control the D2D interference and communication

coverage of D2D. In addition, the ergodic rate of UEs is derived to analyze the network throughput. In Sect. 4, we propose a method that makes an appropriate spectrum partitioning to optimize the system throughput. Then we give the numerical results and analysis. Concluding remarks are given at last.

2 System Model and Assumptions

Here we consider a multi-cell downlink cellular sensor network with D2D communications, as shown in Fig. 1. Each node of WSN can be thought as an UE (user equipment) in cellular sensor network. We refer to a device which communication with BS as a CUE (cellular user equipment) and a device which adopt D2D communication with other device as a DUE (D2D user equipment). Therefore, two kinds of links exist in the network. Links between BS and CUE are called direct links and links between DUEs are called D2D links. A D2D communication represents a DUE pair (i.e. a D2D transmitter and a D2D receiver) in which two DUEs work in the D2D mode. BSs are modeled as a homogeneous PPP Φ_b with density λ_b, the spatial distribution of CUEs and transmitter DUE are also generated according to another PPP with density λ_c and λ_d that is independent of Φ_b. The distance between two D2D communications DUEs follows a uniformed distribution on $(0, b)$ and the transmit powers of BSs and DUEs are P_b and P_D. α_C and α_D are the path loss exponents for direct link and D2D link. We consider a full load scenario in which the bandwidth is always fully occupied by CUEs or DUEs.

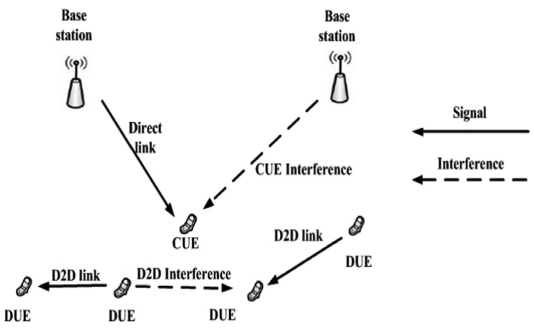


Fig. 1. System model.

In order to avoid interferences between CUEs and DUEs, disjoint spectrum allocation algorithms are adopted. As shown in Fig. 2, the total available system spectrum divided in to N orthogonal channels and each channel has a bandwidth of k Hz. A spectrum partitioning approach is considered in which the DUEs are active on η fraction of the resources in the frequency domain. i.e., the network allocates ηN channels to D2D links and allocates the rest channels to CUEs. Note that direct links operate on $(1-\eta)N$ fraction of channels, which are protected from DUE interferences. We further assume that each D2D pair randomly shares N_D channels in ηN and all D2D

links can reuse the same channels simultaneously. Recall that if it has $\eta N = N_D$, all DUEs share the same channels. If it has $\eta N > N_D$, each DUE will randomly select N_D channels form ηN fraction of channels and then the assigned channels of D2D links will not always identical. Therefore, the suffered interferences among DUEs are alleviated.

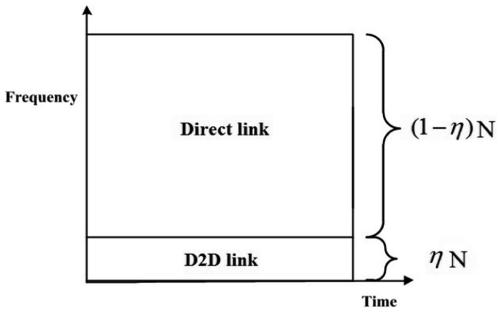


Fig. 2. Frame structure.

3 Outage Probability and Average Ergodic Rate

In this section, we derive the expressions for the outage probability and ergodic rate for CUEs and DUEs to characterize the performance of UEs which will be then used for formulating the network optimization problem.

We consider a cell association approach based on maximum received power, where a CUE is associated with the node which provides the highest reference signal receive power (RSRP). The probability that a typical UE is associated with BS is

$$A_C = \frac{\lambda_C}{\lambda_C + \lambda_D}. \tag{1}$$

The probability that a typical UE use D2D communication is

$$A_D = \frac{\lambda_D}{\lambda_C + \lambda_D}. \tag{2}$$

The average number of CUEs associates with a BS is

$$N_{CUE} = \frac{\lambda_C}{\lambda_b}. \tag{3}$$

The outage probability of a typical UE is defined as the probability that the received SINR of that UE below a certain threshold.

Lemma 1. If the CUE prescribed SINR threshold is T_C, the outage probability is given as

$$\mathbb{P}[SINR_C < T_C] = 1 - 2\pi\lambda_b \int_0^\infty x \exp\left\{-\frac{T_C}{SNR_C} - \pi x^2 \lambda_b [1 + \mathcal{Z}(T_C, \alpha_C, 1)]\right\} dx \quad (4)$$

where $\mathcal{Z}(T_C, \alpha_C, 1) = T_C^{\frac{2}{\alpha_C}} \int_{(\frac{1}{T_C})^{2/\alpha_C}}^\infty \frac{1}{1+t^{\alpha_C/2}} dt$.

Proof: If x is the distance between a random CUE and its serving BS, then we have

$$\mathbb{P}[SINR_C < T_C] = 1 - \int_0^\infty \mathbb{P}[SINR_C > T_C] f_C(x) dx. \quad (5)$$

The probability density function of x can be expressed as

$$f_C(x) = e^{-\pi\lambda_b x^2} 2\pi\lambda_b x. \quad (6)$$

This is because macro BS follows a 2D Poisson process with density λ_b in area S and its PDF is $\exp(-\lambda_b S)$.

In order calculate $\mathbb{P}[SINR_C > T_C]$, we first study the sum of interferences for the typical CUE. Let the CUE locate at the origin and its serving BS is denoted as b_0. The suffered interferences come from the BSs which follow PPP Φ_b with density λ_b. Thus, the suffered sum interferences can be expressed as

$$I_C = P_b \sum_{\Phi_b \setminus b_0} H_x d_C^{-\alpha_C} \quad (7)$$

where d_C is the distance between the typical CUE and BSs and H_x is the channel gain. According to [20], the Laplace transform of I_C is

$$\begin{aligned}
\mathcal{L}_{I_C}(s) &= E_{I_C}[\exp(-sI_C)] \\
&= E_{\Phi_b}[\exp(-sP_b \sum_{\Phi_b \setminus b_0} H_x d_C^{-\alpha_C})] \\
&= \exp(-2\pi\lambda_b \int_z^\infty \{1 - \mathcal{L}_{H_x}(sP_b r^{-\alpha_C})\} r dr) \\
&= \exp(-2\pi\lambda_b \int_z^\infty \frac{r}{1 + (sP_b)^{-1} r^{\alpha_C}} dr) \\
&= \exp(-2\pi\lambda_b \int_z^\infty \frac{sP_b r}{sP_b + r^{\alpha_C}} dr)
\end{aligned} \quad (8)$$

where z is the distance between the typical CUE and the closest interferer BS and

$$\begin{aligned}\mathbb{P}[SINR_C > T_C] &= \mathbb{P}\left[P_b H_x x^{-\alpha_C}/I_C + \sigma^2 > T_C\right] \\ &= \mathbb{P}[H_x > x^{\alpha_C} P_b^{-1} T_C (I_C + \sigma^2)] \\ &= \exp\left\{-\frac{T_C}{SNR_C}\right\} \mathcal{L}_{I_C}(x^{\alpha_C} P_b^{-1} T_C)\end{aligned} \tag{9}$$

where SNR_C is the Signal-to-Noise Ratio for CUEs and $SNR_C = \frac{P_b x^{-\alpha_C}}{\sigma^2}$. Plugging (8) into (9) gives the result

$$\mathbb{P}[SINR_C > T_C] = \exp\left\{-\frac{T_C}{SNR_C}\right\} \exp(-2\pi\lambda_b \int_d^\infty \frac{T_C x^{\alpha_C} r}{T_C x^{\alpha_C} + r^{\alpha_C}} dr). \tag{10}$$

Employing a change of variables $t = x^{-2} r^2 T_C^{-2/\alpha_C}$, we obtain

$$\mathbb{P}[SINR_C > T_C] = \exp\left\{-\frac{T_C}{SNR_C} - \pi\lambda_b \mathcal{Z}(T_C, \alpha_C, 1) x^2\right\} \tag{11}$$

where $\mathcal{Z}(T_C, \alpha_C, 1) = T_C^{\frac{2}{\alpha_C}} \int_{(\frac{1}{T_C})^{2/\alpha_C}}^\infty \frac{1}{1 + t^{\alpha_C/2}} dt$.

Combining (5), (6) and (11) gives the desired result in (4) in which the outage probability is independent of λ_b and P_b. This property is also observed in [21].

Lemma 2. If the DUE prescribed SINR threshold is T_D, the outage probability is given as

$$\mathbb{P}[SINR_D < T_D] = 1 - \frac{1}{b} \int_0^b \exp\left\{-\frac{T_D}{SNR_D} - \pi N_D \lambda_D \mathcal{Z}(T_D, \alpha_D, 1) x^2 / \eta N\right\} dx. \tag{12}$$

Proof: For a random DUE, if the communication distance is r, the probability density of r can be expressed as

$$f_d(r) = 1/b. \tag{13}$$

This is because r follows a uniformed distribution on (0, b). In practical cellular networks, a lot of D2D communications required to meet the application requirements. When a D2D UE receives signals from multiple D2D transmitters at the same time and on the same channels, the achieved SINR can be significantly reduced. Based on the above described disjoint spectrum partitioning setting, the interference for a receiver DUE is from other transmitter DUEs which reuse the same channels. The probability that a transmitter DUE use the same channels with a random receiver DUE is $N_D/\eta N$.

The derivation of DUE outage probability has a similar process as CUEs. Because a DUE suffers interferences from all the D2D pair with density $\lambda_D N_D/\eta N$. By following a similar mathematical derivation shown above, the access probability for DUEs is

$$\mathbb{P}[SINR_D > T_D] = \int_0^b \exp\left\{-\frac{T_D}{SNR_D} - \pi\lambda_D N_D \mathcal{Z}(T_D, \alpha_D, 1)x^2/\eta N\right\} dx \tag{14}$$

and the outage probability is

$$\mathbb{P}[SINR_D < T_D] = 1 - \int_0^b \mathbb{P}[SINR_D > T_D] f_D(x) dx. \tag{15}$$

Combining (13), (14) to (15), we obtain the DUE outage probability in (12). The obtained result shows that as the D2D transmission distance increases, the outage probability decrease due to high path loss. If the system allocates more sources to DUE, the outage probability can be decreased.

Lemma 3. If BSs allocate equal resources to its serving CUEs (i.e. Round Robin algorithm). The average ergodic rate of a typical CUE is

$$R_c = 2\pi\lambda_b \int_{r>0}\int_{t>0} \exp\left\{-\frac{e^t - 1}{SNR_C} - \pi\lambda_b r^2[\mathcal{Z}(e^t - 1, \alpha, 1) + 1]\right\} r dt dr. \tag{16}$$

Proof: The average ergodic rate of a CUE is defined as the data rate average over the communication distance x when all cell channels allocated to that CUE. According to Shannon's theory,

$$R_C = E_x[E_{SINR_C}[\ln(1 + SINR_C(x))]] \tag{17}$$

where

$$\begin{aligned} E_{SINR_C}[\ln(1 + SINR_C(x))] &= \int_0^\infty \mathbb{P}[\ln(1 + SINR_C(x)) > t] dt \\ &= \int_0^\infty \exp\left\{-\frac{e^t - 1}{SNR_C}\right\} \mathcal{L}_{I_c}(x^{\alpha_C} P_b^{-1}(e^t - 1)) dt \\ &= \int_0^\infty \exp\left\{-\frac{e^t - 1}{SNR_C} - \pi\lambda_b x^2 \mathcal{Z}(e^t - 1, \alpha_C, 1)\right\} dt. \end{aligned} \tag{18}$$

Plugging (18) to (17), we have

$$R_C = \int_0^\infty E_{SINR_C}[\ln(1 + SINR_C(x))] f_c(x) dx. \tag{19}$$

After plugging (6) into (19), we get the desired result in (16). By following a similar mathematical derivation shown above, the average ergodic rate of a typical DUE is

$$\begin{aligned} R_D &= \int_0^\infty E_{SINR_D}[\ln(1+SINR_D(x))]f_D(x)dx \\ &= \frac{1}{b}\int_0^b \int_0^\infty \exp\left\{-\frac{e^t-1}{SNR_D} - \frac{\lambda_D N_D r^2}{\eta N}\mathcal{Z}(e^t-1,\alpha_D,1)\right\}dtdr \end{aligned} \tag{20}$$

where SNR_D is the Signal-to-Noise Ratio for DUEs and $SNR_D = \frac{P_D x^{-\alpha_D}}{\sigma^2}$. Obviously, the average ergodic rates of DUE can be determined by the parameter η which denoted the amount of channel resources assign to D2D links. This indicates that the appropriate channel partitioning can improve the network throughput.

4 Problem Formulation

In this section, we derive the overall system throughput in terms of outage probability and ergodic rate. Our objective is to find the optimal spectrum partitioning parameter η that maximizes the network throughput with the constraint of UE SINR threshold. The throughput of a typical CUE and DUE is given below:

$$T_{CUE} = \mathbb{P}[SINR_C > T_C]R_c\frac{(1-\eta)Nk}{N_{CUE}} \tag{21}$$

where $(1-\eta)N/N_{CUE}$ represents the number of channels allocated to each CUE in average and

$$T_{DUE} = \mathbb{P}[SINR_D > T_D]R_D N_D k. \tag{22}$$

Using (21) and (22), we are able to calculated the per cell throughput which is the sum of CUEs and DUEs throughput in a cell, that is

$$T_{total} = A_C T_{CUE} + A_D T_{DUE} \tag{23}$$

Note that ηN must be an integer. The optimal spectrum partitioning parameter η^* can be get by calculate by

$$\eta^* = \begin{cases} \arg\limits_{\eta} T_{total}(\lfloor \eta N \rfloor) & if \quad T_{total}(\lfloor \eta N \rfloor) \geq T_{total}(\lceil \eta N \rceil) \\ \arg\limits_{\eta} T_{total}(\lceil \eta N \rceil) & if \quad T_{total}(\lfloor \eta N \rfloor) < T_{total}(\lceil \eta N \rceil) \end{cases} \tag{24}$$

where $\lceil x \rceil$ is the smallest integer bigger that x and $\lfloor x \rfloor$ is the biggest integer small than x. Thus, the problem of maximize network throughput convert to a spectrum partitioning problem which is shown in (23) and the optimal channel partitioning parameter η^* can be calculated according to (24).

5 Simulation Results and Analysis

We present numerical results on the performance of the proposed approach under different network scenarios. In all the results that follow, the transmit powers are P_b = 46 dBm, P_D = 8 dBm and channel bandwidth k is 1000 Hz. The number of total channels is 100. Assumed densities are $\lambda_b = 1/\pi 500^2$ m^2 and path loss exponents are $\alpha_C = 3.5, \alpha_D = 4$.

Figure 3 shows the outage probability under different DUE communication distance b. It can be observed that at any SINR threshold, as DUE communication distance increases, the outage probability also increases. Fewer D2D communications can be provided due to high path loss. This verified that communication distance is a key factor that affects the system performance. We adopt b = 25 m in the following studies. Because it seems make an appropriate tradeoff between outage probability and communication distance.

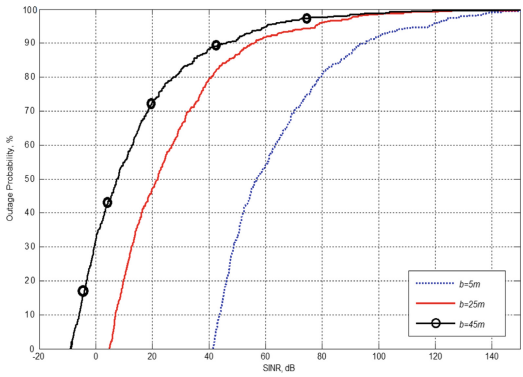


Fig. 3. Outage probability comparison under different DUE communication distance.

We set the SINR threshold T_C = 2 dB and T_D = 8 dB. The impact of UE density on outage is shown in Fig. 4. The x-axis indicated the CUE density and DUE density. We first observe no obvious changes in outage probability for increasing CUE density. Because adding CUEs to network cannot make interference to each other. This validates (4) that adding CUE to the network does not change the SINR distribution of CUEs. For DUEs, as the DUE density increases, the outage probability also increases because the interferences are increasing. This implies that D2D interference is a dominant factor in system performance. This shows that deployment D2D communications with high density are more likely to suffer from D2D interference, which will actually limit the achievable system throughput.

Figure 5 shows the DUE outage probability when b = 25 m and the density of DUE is 5 * λ_b. As the value of ηN increases, the outage probability of DUE decrease. This figure further confirms that the reduction interference can improve the DUE SINR distribution.

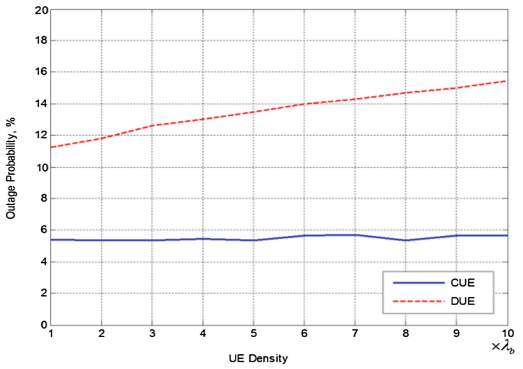


Fig. 4. Outage probability for varying density of CUEs and DUEs.

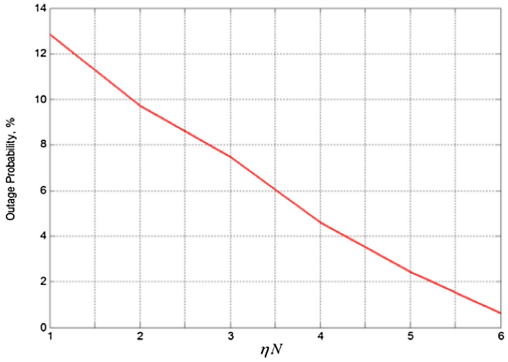


Fig. 5. The DUE outage probability under different value of ηN.

Figure 6 shows the varying value of η versus the total throughput of CUEs and DUEs. The density of CUEs is 5 * λ_b and the density of DUEs is 10 * λ_b. We first observe that the CUE throughput linearly increase with the value of η since the SINR distribution of CUEs is independent with η. The throughput of DUE decreases as the value of η increases, but the rate of decrement increases due to the more D2D interferences generated in the network as the number of candidate channel is limited by the value of η.

Figure 7 shows the total system throughput under different UE density and the optimal value obtained according to (24). The system gets the maximum throughput only and only if it has $\eta = \eta^*$. When it has $\lambda_C = \lambda_D = \lambda_b$, the total throughput increases as the value of η increases. When $\lambda_C = \lambda_D = 5\lambda_b$ and $\lambda_C = 5\lambda_b, \lambda_D = 10\lambda_b$, the total system throughput increases at first but then decreases for a sufficiently large value of η. It can be observed that different UE density corresponding different optimal η and the value of η^* decrease with increasing DUE density. These results can be explained by noting that increasing DUE density increases D2D interferences and more resources are needed to reduce these interferences, leading to a decrease in η^*.

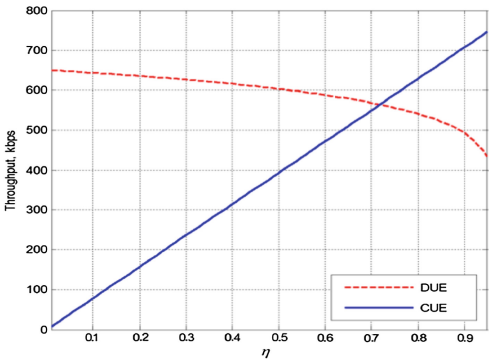


Fig. 6. Throughput with varying values of η.

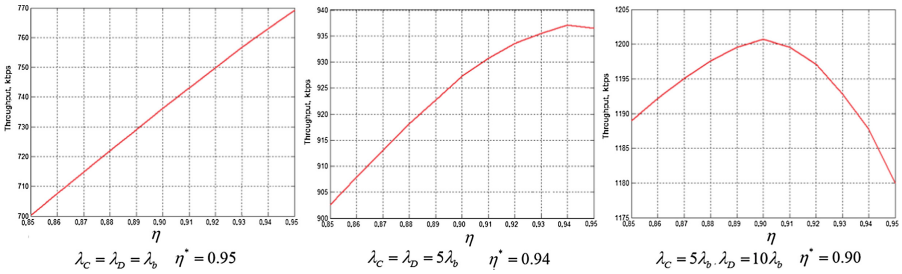


Fig. 7. Optimal value of η under varying UE density.

6 Conclusion

This paper provides an analytical framework for frequency partitioning in D2D enhanced cellular sensor networks. We convert the throughput maximization problem in to an optimal spectrum partitioning problem with SINR constraints and propose an optimal resource partitioning algorithm with UE SINR constraints. Simulation results show that the channel allocation schemes and DUE density strongly affects the overall system throughput due to interference and our proposed scheme effectively optimize the network throughput.

Acknowledgments. This research was supported in part by Shenzhen IOT key technology and application systems integration engineering laboratory and the Natural Science Foundation of Guangxi Province under grant 2016GXNSFBA380010. We would like to acknowledge the reviewers whose comments and suggestions significantly improved this paper.

References

1. 3GPP TR 37.869: Study on enhancements to Machine-Type Communication (MTC) and other mobile data applications. v.12.0.0, March 2013
2. Ozduran, V., Ozdemir, N.: 3GPP Long Term Evolution (LTE) based cooperative communication in wireless sensor networks. In: 4th International Congress on Ultra Modern Telecommunications and Control systems and Workshops (ICUMT), pp. 900–905 (2012)
3. Goratti, L., Steri, G., Gomez, K.: Connectivity and security in a D2D communication protocol for public safety applications. In: 11th International Symposium on Wireless Communications Systems (ISWCS), pp. 548–552 (2014)
4. Zhang, J., Shan, L., Hu, H., Yang, Y.: Mobile cellular networks and wireless sensor networks: towards convergence. IEEE Commun. Mag. **50**, 164–169 (2012)
5. Crosby, G.V., Vafa, F.: Wireless sensor networks and LTE-A network convergence. In: 38th IEEE Conference on Local Computer Networks (LCN), pp. 731–734 (2013)
6. Durresi, M., Durresi, A., Barolli, L., Uchida, K.: Using cellular sensor networks for environment protection. In: 29th International Conference on Advanced Information Networking and Applications Workshops (WAINA), pp. 326–331 (2015)
7. Steri, G., Baldini, G., Goratti, L.: LTE D2D communication for collaborative wearable sensor networks: a connectivity analysis. In: European Conference on Networks and Communications (EuCNC), pp. 403–407 (2016)
8. Lin, X.Q., Andrews, J.G., Ghosh, A., Ratasuk, R.: An overview of 3GPP device-to-device proximity services. IEEE Commun. Mag. **52**, 40–48 (2014)
9. Yin, R., Zhong, C.J., Zhang, Z.Y., Wong, K.K., Chen, X.M.: Joint spectrum and power allocation for D2D communications underlaying cellular networks. IEEE Trans. Veh. Technol. **65**, 2182–2195 (2016)
10. Yu, C.H., Doppler, K., Ribeiro, C.B., Tirkkonen, O.: Resource sharing optimization for device-to-device communication underlaying cellular networks. IEEE Trans. Wirel. Commun. **10**, 2752–2763 (2011)
11. Min, H., Lee, J., Park, S., Hong, D.: Capacity enhancement using an interference limited area for device-to-device uplink underlaying cellular networks. IEEE Trans. Wirel. Commun. **10**, 3995–4000 (2011)
12. Bao, P.C., Yu, G.D.: An interference management strategy for device-to device underlaying cellular networks with partial location information. In: 23th International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), pp. 465–470 (2012)
13. Wang, H., Chu, X.: Distance-contrained resource-sharing criteria for device-to-device communications underlaying cellular networks. Electron. Lett. **48**, 528–530 (2012)
14. Asheralieva, A., Miyanaga, Y.: QoS-oriented mode, spectrum, and power allocation for D2D communication underlaying LTE-A network. IEEE Trans. Veh. Technol. **65**, 9787–9800 (2016)
15. Wang, F., Li, Y., Wang, Z.C., Yang, Z.X.: Social-community-aware resource allocation for D2D communications underlaying cellular networks. IEEE Trans. Vel. Technol. **65**, 3628–3640 (2016)
16. Peng, B., Hu, C.J., Peng, T., Yang, Y., Wang, W.B.: A resource allocation scheme for D2D multicast with QoS protection in OFDMA-based systems. In: 24th IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), pp. 2383–2837 (2013)
17. Andrews, J.G., Baccelli, F., Ganti, R.: A tractable approach to coverage and rate in cellular networks. IEEE Trans. Commun. **59**, 3122–3134 (2011)

18. Lin, X.Q., Ganti, R.K., Fleming, P., Andrews, J.G.: Towards understanding the fundamentals of mobility in cellular networks. IEEE Trans. Wirel. Commun. **12**, 1686–1698 (2013)
19. Lin, X.Q., Andrews, J.G., Ghosh, A.: Spectrum sharing for Device-to-Device communication in cellular networks. IEEE Trans. Wirel. Commun. **13**, 6727–6740 (2014)
20. Bao, W., Liang, B.: Structured spectrum allocation and user association in heterogeneous cellular networks. In: 33th International Conference on Computer Communications (INFOCOM), pp. 1069–1077 (2014)
21. Dhillon, H.S., Ganti, R.K., Baccelli, F., Andrews, J.G.: Modeling and analysis of k-tier downlink heterogeneous cellular networks. IEEE J. Sel. Areas Commun. **30**, 550–560 (2012)

LQI-DCPSec: Secure Distributed d-Cluster Formation in Wireless Sensor Networks

Cherif Diallo(✉) and Maimouna Tedy Sow

Laboratoire Algèbre, Cryptographie, Codes et Applications (ACCA),
UFR Sciences appliquées et de Technologies (UFR SAT),
Université Gaston Berger, BP 234, Saint-Louis, Senegal
cherif.diallo@ugb.edu.sn

Abstract. In wireless sensor networks (WSN), grouping of small group nodes, called clusters, is an effective technique for facilitating scalability, self-organization, energy saving, access channels, routing, data aggregation, etc. Several clustering protocols have been proposed for WSN. Depending on the order in which the formation of clusters and the election of cluster leaders are performed, these protocols can be subdivided into two categories: the Leader-First (LF) and the Cluster-First (CF) approaches. In LF approaches, clusterheads are first elected according to certain metrics (e.g., degree of connectivity, remaining energy), and then agree to assign the other nodes to different clusters. While in CF techniques, all sensors first form clusters, and then each cluster chooses its leader. In previous work, we proposed LQI-DCP, which is a non-secure distributed protocol for multihop clustering with an LF approach. During the clustering process, one or more malicious nodes could attempt to disrupt the cluster leader election by electing illegitimate nodes. In this paper we propose LQI-DCPSec which is a secure version of LQI-DCP that we will compare, in terms of energy consumption, to SEFA which is another secure clustering algorithm using an LF approach. Simulation results show that LQI-DCPSec is more energy-efficient than SEFA.

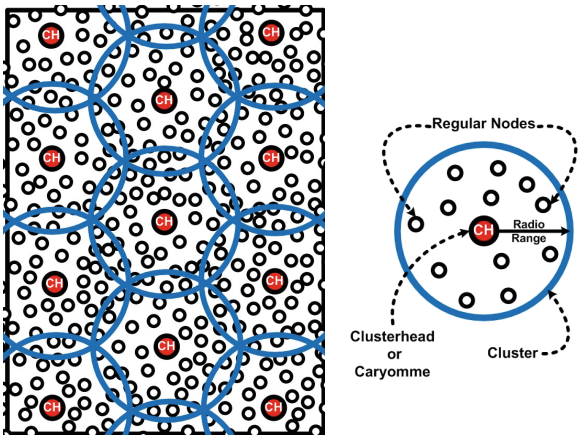
Keywords: WSN · Clustering · LQI-DCP · Security · LQI-DCPSec

1 Introduction

A WSN application often requires a clustering protocol to partition (Fig. 1) the network in order to guarantee scalability and better performance [1]. When cluster leaders are required, the nodes of each cluster will be able to execute an election protocol to determine their cluster leader [1–3].

Many clustering protocols have been proposed. However, most of them, such as LQI-DCP [1], LCA, LCA2, MaxMin [3], LEACH [4], LSCA [5] and SOS [6], assume healthy networks and are not resistant to attacks from malicious participants in hostile environments. In Leader-First approaches, malicious nodes

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 210–220, 2018.
https://doi.org/10.1007/978-3-319-90802-1_18



(a) *WSN Clustering* (b) *Cluster*

Fig. 1. Clusters formation [2,3]

may lie about their metrics (for example, increasing the criterion value to be elected as clusterhead, when the node sends it to its respective neighbors in the first step of the LQI-DCP process [1]). As a result, such kind of nodes could control all nodes in their clusters. Similarly, none of the Cluster-First protocols can guarantee a consistent view of group memberships when malicious nodes send erroneous information.

In [7], Vasudevan et al. have proposed two secure leader election algorithms using a trusted authority to certify the metrics of each node used in the leader election process. However, these algorithms assume that all participating nodes are reliable and that no messages are lost or delayed, which can not be guaranteed in case of malicious nodes.

In [1], we have proposed a distributed multihop clustering protocol, called LQI-DCP, which is based on the Link Quality Indicator (LQI). Intended to dense wireless sensor networks, its basic idea is to enhance the network efficiency by selecting the best located sensors as clusterheads. It takes place in 2 rounds. The first round consists of information exchanges to initialize the algorithm and to preselect preferable nodes as clusterheads. In this round, the undesirable nodes with respect to the preselected ones are identified. In the second round, caryommes are elected among the remaining non-clusterized nodes and then among the previous identified undesirable nodes in last resort, while avoiding having single-node clusters [8] in the network.

This previous work [1] have shown that LQI-DCP helps in producing clusters of which each clusterhead has a better positioning regarding the locations of other clusterheads. Therefore in cluster formation, LQI-DCP has shown that it is quite important to sufficiently outspread the clusterheads (or caryommes) in order to improve the network efficiency. However, producing a secure clustering protocol was not part of our objectives in [1]. This is precisely what we are

trying to achieve in this paper by proposing LQI-DCPSec which is a secure version of LQI-DCP. Because like most WSN protocols, LQI-DCP clustering protocol should meet security requirements. However, sensors are constrained by limited energy resources and the need to manipulate simple data for the cluster-head election process poses major challenges in implementation of security mechanisms and data processing.

To carry out our work, this paper is organized as follows: in Sect. 2, we will consider an attacker's model. Then, we present LQI-DCPSec security mechanisms in Sect. 3. Finally, LQI-DCPSec is compared with SEFA protocol [7] regarding to network performance in Sect. 4.

2 Attacker's Model

We consider an attacker who is in the vicinity of the nodes to listen to traffic during the clustering process. In other words, in this attacker model, the attacker snoops the network communications and then records the messages sent by the legitimate nodes during the clustering process. Then, he could produce adequate messages that would allow him to be illegitimately elected as clusterhead (with a better metric, for example). The attacker could also try to insert one or more malicious nodes in the network in order to disrupt the cluster-head election process.

With this simple model, an attacker could perform, during the LQI-DCP clustering process, the most of common WSN attacks described in [9,10] such as: passive listening or eavesdropping attack, traffic analysis attack, man-in-the-middle attack, message alteration attack, sybil attack, black hole attack, selective forwarding attack and many others kind of attacks. Therefore, the LQI-DCPSec protocol is intended to prevent such attacks in the WSN by adding confidentiality and integrity features to secure the messages exchanged during the clustering process.

3 LQI-DCPSec Security Mechanisms

LQI-DCP is described in detail in [1,3]. Further results concerning LQI-DCP are published in [11]. Here, we pursue the objective of ensuring the integrity and confidentiality of the messages exchanged (sending of the criterion value in the first step of LQI-DCP, PN-INFORM-MSG, WBN-SELECTION-MSG and CH-INFORM-MSG) during the cluster formation process by LQI-DCP. This is that updated version of the LQI-DCP protocol that we have called LQI-DCPSec.

3.1 Initialization Phase

Prior to the deployment of the network, the base station assigns to each node u a unique identifier Id_u and a key pair (private key and public key). In addition, each node u knows the public key of all its neighbors. In addition, the base station generates a unique secret key shared by all the sensors in the network.

3.2 Hash and Encryption Functions

To secure LQI-DCP, we will use the hash and encryption functions of the PRESENT protocol [12]. PRESENT is an ultralight block encryption algorithm that runs on 31 rounds [12]. This algorithm works on blocks of 64 bits and uses keys of 80 or 128 bits length. These two versions are called PRESENT-80 and PRESENT-128 depending on whether the key size is 80 or 128 bits. For a better application, the authors of [12] propose the use of 80-bit keys. Therefore, we will use PRESENT-80 for messages encryption. We will also use the DM-PRESENT-80 hash function to calculate the messages digest for each packet: sending of the criterion value in the first step of LQI-DCP, PN-INFORM-MSG, WBN-SELECTION-MSG and CH-INFORM-MSG. Such as PRESENT-80, DM-PRESENT-80 uses 80-bit keys inputs and returns a message digest of 64-bit.

3.3 Signing and Encrypting a Message from Node A to Node B

In this section we use the following notations:

- $K_{Priv}(A)$: The private key of a node A
- $K_{Pub}(A)$: The public Key of a node A
- $K_{WSN}(t)$: The shared key, at time t, by all the nodes of the network
- F_{Hash}: The hashing function, Hash algorithm.

Signing a Message from Node A to Node B

- **Message digest computation:** The main purpose of the message digest computation is to ensure the integrity of the message. $\textbf{Digest} = [\textbf{Message}]F_{Hash}$
- **Signature of the digest:** The sender (node A in this case) generates a signature digest by using its private key. Moreover, the name of the hashing algorithm used by the transmitter is sent with the generated signature. With this information, anyone could decrypt and verify the signature using the sender public key and the hash algorithm. Given the properties of public key encryption and hashing algorithms, the recipient has the proof that:
  1. The digest was encrypted using the transmitter private key.
  2. The message is protected against any alteration.
  3. At this step, one has the initial message and the computed digest which is signed with the sender private key: $\textbf{Message} + [\textbf{Digest}]K_{Priv}(A)$.

Message Encryption

- We use a single encryption/decryption key because cryptographic algorithms that use asymmetric keys are too slow and symmetric key algorithms are more energy efficient in WSNs.
- Then, the entire message (the initial message and its digital signature) is encrypted using the network shared key $K_{WSN}(t)$.
- At this step, one has the entire message which is signed with the WSN shared key: $[\textbf{Message} + [\textbf{Digest}]K_{Priv}(A)]K_{WSN}(t)$

3.4 Deciphering and Verifying the Signature of the Received Message

Message Decryption. The message (which includes the message itself and the digital signature) is then decrypted using the network shared key $K_{WSN}(t)$.

Signature Verification. The signature verification includes the three following steps:

- Deciphering the message digest. The digest was encrypted using the private key of the sender (node A). The digest is now decrypted using the transmitter's public key.
- Evaluation of the digest. Since hashing is a one-way process, in other words, it is impossible to retrieve the original message from the digest, the recipient must re-evaluate the digest using exactly the same hashing algorithm as the sender.
- Comparison of condensed matter. The deciphered condensate and the evaluated condensate are compared. If they agree, the signature is verified and the recipient can then be sure that the message has been sent by the sender and has not been altered. If they do not agree, it is possible that:
  1. The message has not been signed by the issuer or it was corrupted.
  2. In either case, the message must be rejected.

3.5 Generating the Unique Key

As in [13], we propose a solution which consists of using a generation key. For each period or generation t, the base station sends a new key $K_{WSN}(t)$ to the entire network. This key serves as a certificate for each node to prove its membership in the network. If a malicious node tries to enter the WSN and does not have this generation key, it could not be accepted within it. This technique also makes it possible to limit the substitution attacks of a sensor and its reprogramming in order to be reinserted into the network. If a node is stolen at time 0 with the generation key $K_{WSN}(0)$, the time an attacker reprograms it to put it back in the WSN, it will have elapsed a time x. When the sensor is reinserted in the network, the new generation key would then be $K_{WSN}(x)$. The malicious node will ask its neighbors to enter the network with the generation key $K_{WSN}(0)$ and not $K_{WSN}(x)$ because it could not having receive the new generation key. As $K_{WSN}(0)$ is different from $K_{WSN}(x)$, neighbors will not accept its request and the malicious node will not then be able to enter the network.

4 LQI-DCPSec Performance Evaluation

To evaluate the performance of LQI-DCPSec, we compare it to the SEFA protocol. Some clustering protocols are more suitable for some deployment strategies than others [11]. So, in this section performance evaluation are done by using

in results (Figs. 2 and 3) a random deployment type without constraint [14], in results (Figs. 4 and 5) a deployment type with a remoteness constraint λ between nodes as defined in [14], and a grid topology deployment in the result of Fig. 6.

4.1 SEFA Algorithm

In [7], authors consider the problem of secure leader election and propose Secure Extrema Finding Algorithm (SEFA) as a cheat-proof election algorithm. SEFA assumes a synchronous distributed system in which the various rounds of election proceed in a lock-step fashion. SEFA assumes that all elector-nodes share a single common evaluation function that returns the same value at any elector-node when applied to a given candidate-node. The details of SEFA protocol are described in [7].

4.2 Simulation Parameters

In the simulation model N sensors are deployed over an area of length L, and width l. The transmission range of each sensor (including the Base Station) is R = 20 m. As in [1–3], we use the same energy consumption model. Let $E_{Tx}(k, d)$ the energy consumed to transmit a *kbits* message over a distance d [4]:

$$E_{Tx}(k, d) = E_{elec} * k + \varepsilon_{amp} * k * d^2 \tag{1}$$

Let E_{Rx} the energy consumed to receive a *kbits* message:

$$E_{Rx}(k, d) = E_{Rx-elec}(k) = E_{elec} * k \tag{2}$$

$$E_{elec} = 50\,\text{nJ/bit}\ and\ \varepsilon = 100\,\text{pJ/bit/m}^2 \tag{3}$$

The main parameters are summarized in the Table 1.

Table 1. Simulation parameters used for each result

Parameters	Figure 2	Figure 3	Figure 4	Figure 5	Figure 6
Radio range R	20 m	20 m	20 m	20 m	20 m
Area length L	100 m	100 m	100 m	100 m	100 m
Area width l	60 m	60 m	100 m	100 m	100 m
Number of sensors	50 to 200	20	50 to 200	50	50
λ			0.25	0.25	
Step					10

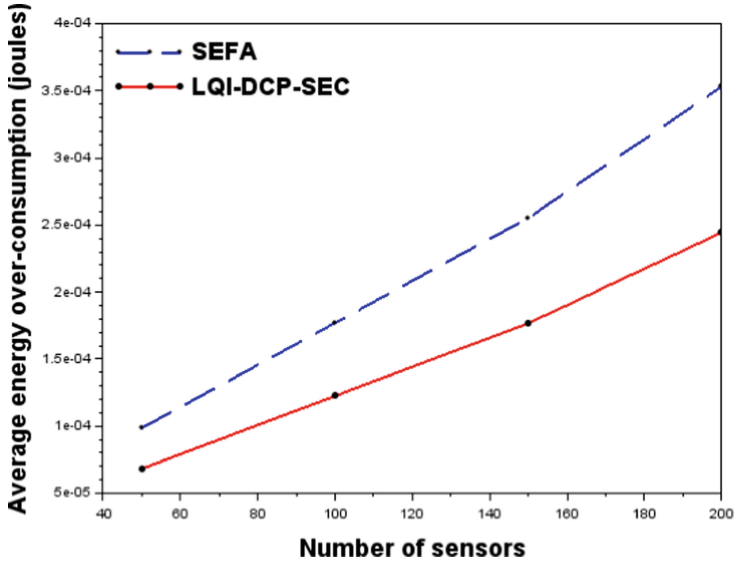


Fig. 2. Total average energy consumption as a function of the number of sensors deployed according to the random deployment without constraint (Color figure online)

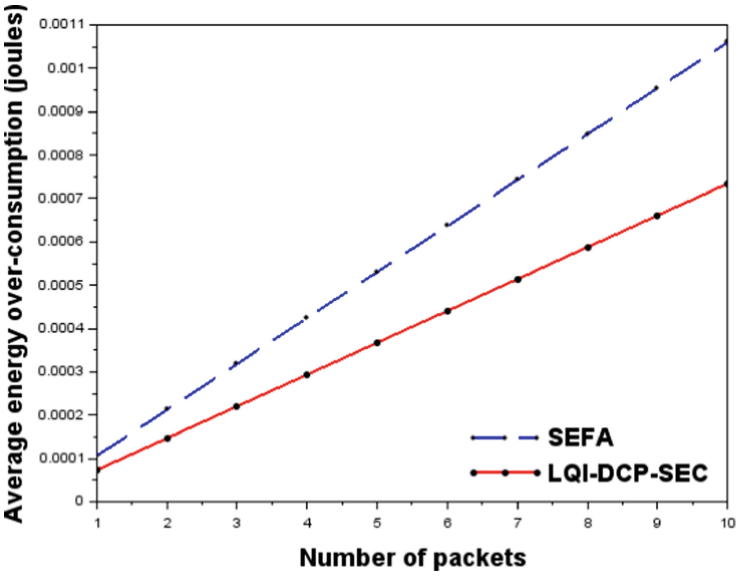


Fig. 3. Total average energy consumption as a function of the number of packets sent per sensor following random deployment without constraint (Color figure online)

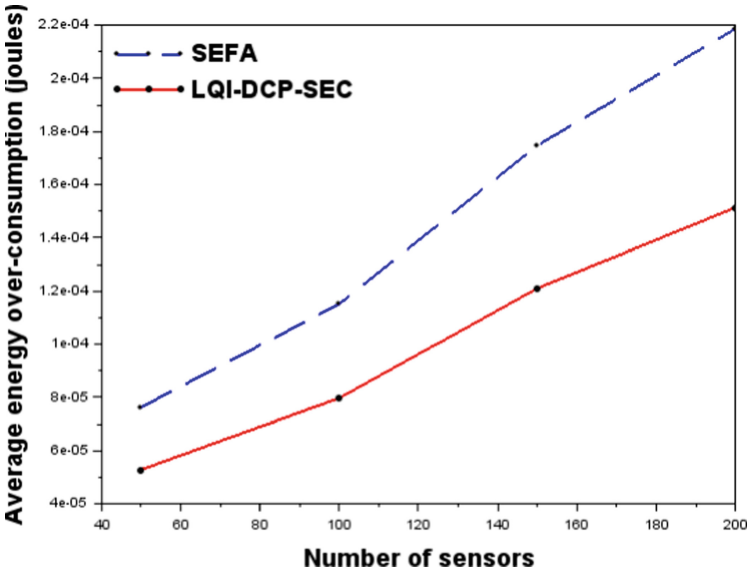


Fig. 4. Total average energy consumption as a function of the number of sensors deployed according to a deployment type with a remoteness constraint λ between nodes (Color figure online)

4.3 Simulation Results

In each Figs. 2, 3, 4, 5 and 6, we have two curves: the first one, in red and in continuous lines (LQI-DCPSec), outputs the total average energy consumption using the LQI-DCPSec protocol for forming clusters; and the second one in blue dotted lines (SEFA) is obtained by using the SEFA protocol.

To compare the energy cost of the LQI-DCPSec and SEFA clustering protocols, we calculated the total average energy over-consumption in the case where the number of packets sent per sensor varies from 1 to 10 in each case of random deployment without constraint (Fig. 3) and deployment type with a remoteness constraint λ (Fig. 5) as well as in the case of the grid deployment (Fig. 6). We also calculated the total average additional energy expenditure in the case where the number of sensors varies from 50 to 200 according to the LQI-DCPSec and SEFA clustering protocols in the case of random deployment (without constraint (Fig. 2) and with a remoteness constraint λ (Fig. 4)).

The results of Figs. 3, 5 and 6 show that the more the packet exchanges increase in the network, the greater the gap between energy over-consumption becomes greater between SEFA and LQI-DCPSec. SEFA consumes up to 57% more energy than LQI-DCPSec (Fig. 3). Similarly, this difference increases up to 55% in Fig. 5. On the other hand, in the case of the grid topology SEFA consumes up to 33% more energy compared to LQI-DCPSec (Fig. 6). This means that when the average number of neighbors per node decreases, the gap also decreases. It could be concluded that SEFA is more suitable for less dense

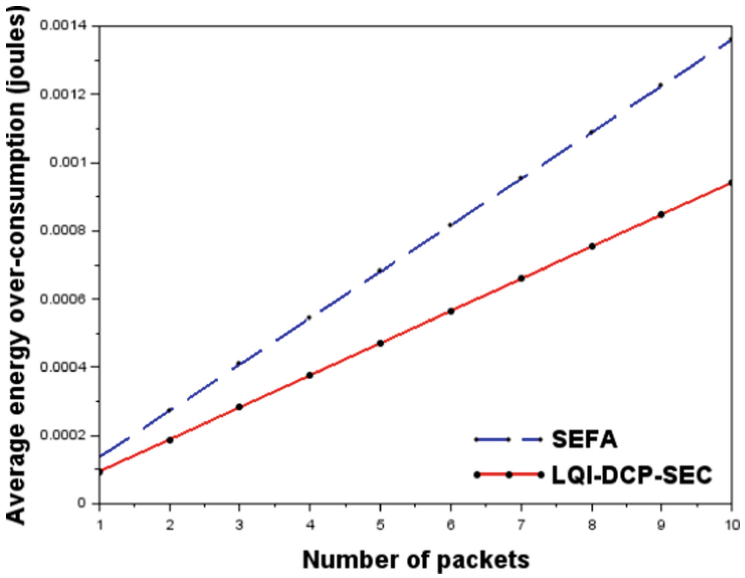


Fig. 5. Total average energy consumption as a function of the number of packets sent per sensor following a deployment type with a remoteness constraint λ between nodes (Color figure online)

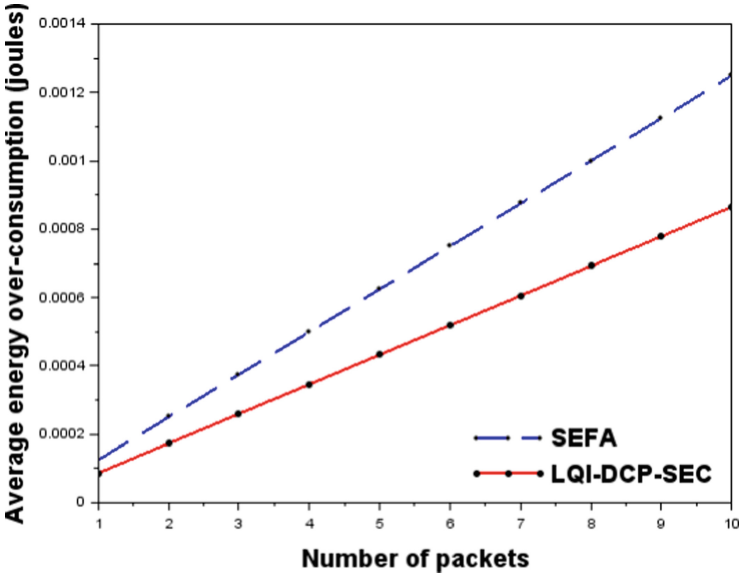


Fig. 6. Total average energy consumption as a function of the number of packets sent per sensor following the grid deployment (Color figure online)

networks even though in this case LQI-DCPSec still offers better performances. This is confirmed by the results of Figs. 2 and 4 where it should also be noted that when the density increases, the additional energy expenditure of SEFA with respect to LQI-DCPSec increases up to 45% for the result of Fig. 2, and up to 57% in the case of the result of Fig. 4.

We note that, in all cases, the total average energy consumption of the SEFA protocol exceeds that of LQI-DCPSec protocol. By observing the evolution of the curves, we note that protocol LQI-DCPSec succeeds, beyond the questions related to the security and the optimization of resources, in significantly reducing the overall average energy consumption of the network. Thus, LQI-DCPSec protocol is far better than SEFA from an energy expenditure point of view, which is a very important resource in the WSN. This does not mean that LQI-DCPSec is the best algorithm for secure cluster formation in terms of energy consumption, because we always have to think about decreasing the size of the used keys [14].

5 Conclusions and Future Works

As we can see, the LQI-DCPSec protocol guarantees the integrity of each message. This is facilitated by hashing the message content and signing the hash using the sender's private key. This allows the recipient of the message to verify the signature using the sender's public key that is known by everyone. Therefore, if a malicious node tries to corrupt a message from another node, it will be detected by the recipient. Moreover, beyond the integrity feature, authentication of the sender is also ensured with LQI-DCPSec. Finally, given the fact that all the messages are encrypted, which guarantees the confidentiality of the data, LQI-DCPSec protocol is also resistant to many attacks such as passive listening or eavesdropping, traffic analysis, man-in-the-middle, message alteration, sybil, black hole, selective forwarding, etc. Likewise, given the mechanism of unique network key generation, LQI-DCPSec prevents any malicious nodes insertion in the network. In addition, compared to SEFA, LQI-DCPSec offers better performance with much lower energy consumption.

However, from another point of view, since the messages exchanged during LQI-DCPSec clustering process are signed and encrypted, the packet size has increased. With an initial 64-bit packet size, one added the 64-bit digest obtained with the hash function DM-PRESENT-80, making a total of 128 bits. One adds to this the size of the PRESENT-80 encryption key which is 80 bits, which leads to a total packet size of 208 bits. That means to say that the package size has increased by 225%. This is high given our previous results [14]. Therefore, in our future work, we will try to propose our own lightweight integrity and privacy schemes lighter than the PRESENT algorithm in order to significantly reduce the size of exchanged packets and to gain much more performance.

Acknowledgment. This work is supported by CEA-MITIC (http://www.ceamitic.sn/), UFR SAT, Université Gaston Berger, Saint-Louis, Sénégal.

References

1. Diallo, C., Marot, M., Becker, M.: A distributed link quality based d-clustering protocol for dense ZigBee sensor networks. In: Proceedings of the Third IFIP/IEEE Wireless Days International Conference, WD 2010, Venice, Italy (2010)
2. Diallo, C., Marot, M., Becker, M.: Using LQI to improve clusterhead locations in dense ZigBee based wireless sensor networks. In: Proceedings of the 6th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2010, Niagara Falls, Canada, October 2010, pp. 137–143 (2010)
3. Diallo, C.: Techniques d'amélioration du routage et de la formation des clusters multi-sauts dans les réseaux de capteurs sans fil. Ph.D. Télécom SudParis (2010)
4. Heinzelman, W.B., Chandrakasan, A., Balakrishnan, H.: An application-specific protocol architecture for wireless microsensor networks. IEEE Trans. Wirel. Commun. **1**(4), 660–670 (2002)
5. Gao, C., Jantti, R.: Link-state clustering based on IEEE 802.15.4 MAC for wireless ad-hoc/sensor networks. In: Proceedings of IEEE Wireless Communications and Networking Conference, WCNC 2006, Las Vegas, USA, vol. 1, pp. 499–504 (2006)
6. Shin, K., Abraham, A., Han, S.Y.: Self organizing sensor networks using intelligent clustering. In: Gavrilova, M.L., Gervasi, O., Kumar, V., Tan, C.J.K., Taniar, D., Laganá, A., Mun, Y., Choo, H. (eds.) ICCSA 2006. LNCS, vol. 3983, pp. 40–49. Springer, Heidelberg (2006). https://doi.org/10.1007/11751632_5
7. Vasudevan, S., DeCleene, B., Kurose, J., Towsley, D.: Secure leader election in wireless ad hoc networks. UMass Computer Science Technical report 01-50 (2010)
8. Diallo, C., Marot, M., Becker, M.: Single-node cluster reduction in WSN and energy-efficiency during cluster formation. In: Proceedings of the 9th IEEE/IFIP Annual Mediterranean Ad Hoc Networking Workshop, Med-Hoc-Net 2010, Juan-Les-Pins, France, June 2010. IEEE Communications Society (2010)
9. Diallo, C., Sawaré, A., Sow, M.T.: Security issues and solutions in wireless sensor networks. Int. J. Comput. Sci. Inf. Secur. IJCSIS **15**(3), 6 (2017). ISSN 1947-5500
10. Diallo, C.: Security issues and solutions related to data aggregation process in WSN. Int. J. Comput. Sci. Netw. Secur. IJCSNS **17**(4), 59–71 (2017). ISSN 1738–7905
11. Diallo, C.: Deployment strategies and clustering protocols efficiency. Sens. Transducers **213**(6), 9–23 (2017). International Journal ISSN 2306–8515, e-ISSN 1726–5479
12. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74735-2_31
13. Bekara, C., Laurent-Maknavicius, M.: A new resilient key management protocol for wireless sensor networks. In: Sauveron, D., Markantonakis, K., Bilas, A., Quisquater, J.-J. (eds.) WISTP 2007. LNCS, vol. 4462, pp. 14–26. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-72354-7_2
14. Sow, M.T., Diallo, C.: Energy over-consumption induced by securing network operations. In: Proceedings of 2nd IEEE International Conference on Frontiers of Sensors Technologies, IEEE-ICFST 2017, Shenzhen, China, April 2017, pp. 154–160. IEEE (2017). ISBN 978-1-5090-4858-8/17/

Swarm of Networked Drones for Video Detection of Intrusions

Mustapha Bekhti[1(✉)], Nadjib Achir[1], and Khaled Boussetta[1,2]

[1] Université Paris 13, Sorbonne Paris Cité – L2TI (EA 4303), Villetaneuse, France
{bekhti.mustapha,nadjib.achir,khaled.boussetta}@univ-paris13.fr
[2] Inria URBANET, INSA Lyon, 69621 Villeurbanne, France

Abstract. Border control, sensitive area monitoring and intrusion detection are surveillance problems of practical import that are well suited to wireless sensor networks. In this paper, we study the application of a swarm of Unmanned Aerial Vehicles to an intrusion detection and tracking problem. We introduce the Boids scheme to maintain the drones team formation in order to deal with coverage issue and collision problem. A contribution of our work is that we do not assume a ground centralized control of the drones; on the contrary, the swarm is considered as a set of autonomous and self organized entities.

Keywords: UAV · Swarm · Intrusion · Detection · SINR · Coverage

1 Introduction

Unmanned aerial vehicles, shortly named UAVs are defined as autonomous entities with no pilot on board. They are a part of a global system called Unmanned System which also includes elements such as a control station, relays etc.

Due to them flexibility and mobility, these flying machines become the ideal tool for carrying out technical inspections of constructions, buildings, industrial sites, highway structures in a fast but also at low-cost way. Capable of going in places difficult of access or simply wide area, the drone allows a simplified but a precise technical inspection. With the aerial shots taken by a drone, it is possible to obtain a precise image of the building and thus allows to localize and to diagnose the defects of constructions. In another hand, borders and sensitive area control and monitoring is a key issue that every state is considering carefully, whether for security or economic reasons. The main challenge is to control borders and areas outside regulated zone crossings, which are always considered as open doors for intrusion. Thus, in order to improve the time and the quality of the response, the UAV could allow a rapid assessment of the situation but also to contribute to the processing of the operational information concerning the threats.

Basically, these flying machines are designed to fulfill the requirements of assigned missions individually or among a set of drones, called swarm. Since complex mission cannot be accomplished with a single entity, the use of a set

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 221–231, 2018.
https://doi.org/10.1007/978-3-319-90802-1_19

of drones is required. Thus, the drones forming the swarm have to cooperate in order to achieve the global mission and to avoid collision with each others. Thus, the main objective of flight in formation is to make a link between the decisional and functional level, in other words, to produce a configuration of formation based on the constraints of the mission. However, such cooperation requires robust communications and a good strategy to avoid obstacles and collision between the drones as well.

Different control strategies have been presented in robotics to control the movement of entities among a swarm, such the ones based on the potential field presented by [2,5,6]. Other visual methods have been developed for mobile robots on the ground, but it is difficult to transpose them to the three-dimensional environment of drones with a much faster dynamics [4].

However, simple target tracking is not sufficient to ensure the stability of the swarm. This requires closing the loop by slaving the drones one against the others. Thus, three behaviors are sought, namely intruder localizing, collision avoidance and configuration compliance. The effectiveness of this control depends on the possibility at which the position of the drones can be obtained.

When flying at high speed in formation with small spacing, the safety of the flight becomes difficult to guarantee, especially in events related to communication systems failures. In fact, communications are the major problems of unmanned aircraft. In order to ensure the safety of the flight, the data must be exchanged continuously between drones themselves and the ground control station, thus excluding the radio silence is more than necessity [1].

Our current research is mainly motivated by emerging applications such as border surveillance, reconnaissance, environmental monitoring and search-and-rescue tasks in areas without a permanent communication infrastructure. In this paper, we present a deployment strategy of a fleet of quad-copters for area monitoring, intrusion detection and video stream reporting. It is evident that the drones should not collide and keep a safety distance from each other during the mission. Thus, our solution is based essentially on the well known model proposed by [7] where the movement of the swarm is inspired from the motion of a flock of birds.

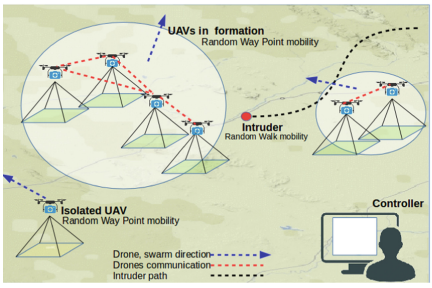
This choice is motivated by the simplicity and robustness of the method. Moreover, it does not increase the use of bandwidth for communications, considering that drones must only exchange their positions to maintain the swarm formation, to cover a large area and to avoid collision as well.

2 Scenario

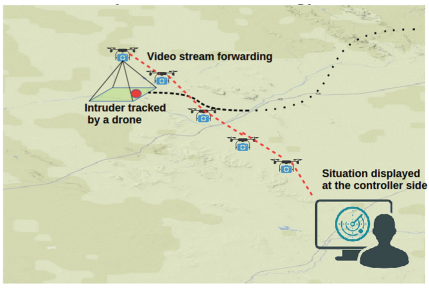
We address the problem of mobile target localizing and tracking by the use of a fleet of drones. Our goal is to determine the intruder position, to keep the fleet in a certain formation in order to avoid collision between drones and to forward video situation to the controller side. To this end, a behavioral approach based on the quality of signal between drones of the same swarm is proposed. In addition, we deal with one of the assumption commonly made about wireless networks

that says that the signal strength is just a simple function of distance, which is not always the case.

The following scenario provides the motivation of this work. We consider a sensitive area to monitor. A set of ground detectors is deployed at the border of the area. In the case of intrusion, the ground sensors send an alarm to the security forces in charge of the area surveillance. The security forces need to localize the intruder and to get a real time video of the situation for a better threat evaluation. To this end, the security forces resort to the use of a set of small scale drones equipped with cameras and wireless communications devices. The Figs. 1a and b give an overview of the scenario and illustrate the drone's behavior during the different phases of the mission.



(a) UAVs fleet for intruder localizing



(b) UAVs fleet for video stream reporting

Fig. 1. Intruder search and report scenario

3 Problem Formulation

3.1 Problem Statement and System Description

As mentioned earlier, we are dealing with a sensitive area surveillance. The main objective of this paper is to localize the intruder and to report the situation to the security forces in the shortest possible time in order to evaluate the threat and to deploy the adequate forces. Basically, this mission is given to a set of autonomous small scale drones, denoted by $D = \{D_1, D_2, \ldots, D_n\}$. Each drone D_i is equipped with a camera and wireless devices to communicate with the other drones and the base station BS situated at the controller side. We assume that all the communication devices have the same characteristics and have a short sensing range compared to the size of the region of interest. In addition all the cameras have the same field of view that we denote by FoV. We also consider that the drones have a limited flight autonomy Υ. Finally, we assume that the intruder is localized once it is within the FoV of any drone D_i.

In this frame, the system is modeled as 2D area A without any obstacle since the drones are flying at the same altitude h. The projection of the flying area is represented by a rectangular with length of x_{max} and a width of y_{max}.

Our goal is to present a solution that minimize the search localization, optimize the number of the used drones for a given mission. Moreover, during the mission, and in no cases, the drones must not collide with each other. Furthermore, and in order to cover a large area, drones shall flight in formation and maintain the maximum distance possible between the rest of drones of the same swarm. For this purpose, we assume that after each period P drone generates a message of size D bits containing its identification, its position and speed. The on-board wireless interface tries to send each generated message to the other UAVs. For some reasons, a message can be corrupted or lost due to possible interference and collisions. The opportunity to transmit also depends on the radio coverage, the capacity of the related wireless technology and the drone's location.

The following is how the mobile target search problem is resolved. A swarm of mini drones with autonomous behaviors is capable of performing low cost and distributed sensing functions such as the one described in the preceding scenario. A first drone is sent to the direction where the attacker was initially reported by the ground detectors that are deployed at the border of the area. After a period time p, and if the situation is not received at the controller side, another drone takes off and moves towards a random position looking for the intruder. This step is repeated after each period p, until the intruder is localized or the maximum number of the drones is reached. In the case where the drone identification and position message D is received by one or different drones, the sender and the receivers drones create a new swarm. The cohesion of this swarm is a function of the signal quality of the wireless network created by the swarm drones. Thus, the drones forming a swarm maintain the largest distance between them in order to cover a large area. In this case, a low signal strength could guarantee the position messages exchange in the network. Whereas, a high data rate is needed to report the video situation to the controller. However, a good quality of signal should be assured when the drones are being closer enough.

In addition, if a drone D_i consumes a 70% of its energy it goes back to the start position. Moreover, if a drone identifies the intruder based on its camera, it reports and notifies the nearby UAVs of its location. The UAVS alter their flight paths and align themselves between the intruder position and the BS at the controller side. As the intruder moves, the drones update them positions to keep the target in sight. Through coordination, the UAVs should be able to complete tasks that each could not have done alone. With these new capabilities, UAVs can plan missions collaboratively and can re-plan adaptively based on real-time changes in UAV availability, camera FoV and target movement. The flow chart in Fig. 4 depicts clearly the different steps of our algorithms, namely, localization, swarming and collision avoidance, and video reporting.

3.2 Problem Formulation

We have n autonomous drones flying at the same altitude h at an instant t. For simplicity we denote the position of a single drone D_i at time step t by the coordinate $(x_{i,t}, y_{i,t})$. The movement of a drone D_i is discretized in space and

time allowing the drone to make its own decision to move to adjacent position or to hover at the same position via the information gained from the nearby drones.

Our main objective is to minimize the search time of the intruder:

$$\text{minimize} \sum_{i=1}^{N} t_i x_i \tag{1}$$

subject to:

$$\sum_{i=1}^{N} x_i = 1 \tag{2}$$

where N is the number of UAVs, t is an estimate of the time needed by the drone D_i to intercept the target, and x is an assignment variable that is equal to 1 if the intruder is within the D_i FoV, and zero otherwise.

As we assumed that the drones are flying at a constant altitude h, they therefore have a collision avoidance constraint which can be quantified as

$$(x_{n+1,t}, y_{n+1,t}) - (x_{n,t}, y_{n,t}) > A, n = 1, \ldots, N-1. \tag{3}$$

where A is the minimum safety separation between two drones.

In addition, when performing area coverage for intruder detection and for video stream reporting, it is important to define the range boundary of the drones swarm based on signal-to-noise (SNR) ratio, which is the signal level (in dBm) minus the noise level (in dBm). For example, to maintain the UAV swarm in formation, drones need to know the other nearby drones position, a small SNR and low data rate are enough to guarantee a reliable data exchange. However, a healthy value for wireless network is more than necessary for video streaming.

$$SNR_{n,n+1} < \delta, n = 1, \ldots, N-1. \tag{4}$$

3.3 Communications

Assuming a transmission power P_t for the UAV, the received power P_r is easily calculated using an appropriate propagation model depending on the distance d between UAVs. As we consider an open field area, and UAV to UAV communications, the appropriate model could be the free space model.

$$P_r = Att(d).P_t \tag{5}$$

In the ideal case and in its simplest form, the Friis equation is expressed as the ratio of power available at the input of the receiving antenna P_r, to the output power of the transmitting antenna P_t:

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi R}\right)^2 \tag{6}$$

where G_t is the antenna gains of the transmitting antenna, G_r is the antenna gains of the receiving antenna, λ is the wavelength, and R is the distance between the transmitter and the receiver antennas.

Once P_r is determined, the signal-to-noise ratio SNR is computed using the noise/interference power value. In this case, the SNR is equal to:

$$SNR = 10.log\left(\frac{P_r}{P_{Noise} + P_{Interf}}\right) \tag{7}$$

The SNR is an indicator of the quality of transmission of the data. It impacts in a direct manner on the performance of the network. Thus, a lower SNR decreases the throughput and lead the network to operate at a lower data rate with a low throughput. However, a higher SNR value allows a higher data rate, a better throughput and fewer retransmissions [3,8].

The use of a particular SNR value as a requirement for signal coverage, collision avoidance between drones but for keeping the warm in a formation is certainly a difficult choice, and the rule of thumb given in this paper is to test the algorithm with a set of SNR range values.

3.4 Swarm Formation

The basic flocking model presented by [7] consists of three simple steering behaviors. Each behavior is based on the position and the velocity of the nearby agents.

– Cohesion (R1): steer to move toward the average position of local flockmates. The center of the swarm is simply the average position of all the drones. We assume we have N drones in one swarm, then the center c of all N drones is given by:

$$\text{c} = (D_1.\text{position} + D2.\text{position} + \ldots + D_N.\text{position})/\text{N}$$

The positions here are vectors, and N is a scalar.

However, the center of swarm is a property of the entire flock; it is not something that would be considered by each drones. Thus, each individual drone moves toward its perceived center, which is the center of all the other drones, not including itself. Thus, for D_i (1 <= i <= N), the perceived center D_ipc is given by:

$$\begin{aligned} D_ipc = (&D_1.position + D_2.position + \ldots \\ &+D_{i-1}.position + D_{i+1}.position + \ldots \\ &+D_N.position)/(N-1) \end{aligned} \tag{8}$$

– Separation (R2): steer to avoid crowding local flockmates
– Alignment (R3): steer towards the average heading of local flockmates

Algorithm 1. Separation

Input:
V ▷ vector
D_i ▷ Drone
$SNR_{i,j}$ ▷ SNR

function SEPARATION(D_i , $SNR_{i,j}$)
  Vector vector = 0
  for each drone $D_j \in swarm$ **do**
    if thenD_i != D_j
      if $SNR_{i,j} > \delta$ **then**
        $vector \leftarrow vector - (D_i.position - D_j.position)$
      end if
    end if
  end for
  return *vector*
end function

Algorithm 2. Alignment

Input:
V ▷ vector
D_i ▷ Drone

function ALIGNMENT(D_i , $SNR_{i,j}$)
  Vector $vector_i = 0$
  for each drone $D_j \in swarm$ **do**
    if thenD_i != D_j
      $vector_i \leftarrow vector_i + D_j.velocity$
    end if
  end for
  $vector_i \leftarrow vector_i/N - 1$
  return $vector - D_i.velocity$
end function

3.5 Pattern Formation

The formation pattern is one of the most important coordination issue in swarm formation. The geometric pattern to be formed is a set of points in the plane, represented by the drones cartesian coordinates after messages exchange and computation process. For drones, the suited formation can be one of the following pattern:

- arbitrary pattern where all shapes are allowed.
- circle pattern, in this case drone place themselves on the plane to form a circle.
- line pattern: the drones are required to place themselves on a line.
- V pattern: inspired from V-shaped flight formation of migratory birds.

At the end of the coordination and computation, each drone has to broadcast its new localization to the other drones in the same swarm.

4 Results

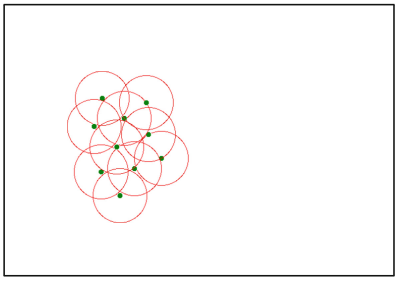
In this section we evaluate our proposed algorithm. Two main objectives were fixed, first, to minimize the intruder localization by the use of less number of drones, while the second one was avoid collision between these drones.

Thus, we assess the algorithm in different scenarios. Using Omnet simulator we generate two traces of the intruder trajectory. Since intruders follows unpredictable path and in order to make it more realistic, we opt for Random Way Point (RWP) mobility model. In addition, as we didn't discretize the area of interest, a drone can move freely to the all adjacent positions. Here again a drone follows a RWP mobility model on its way of intruder localization. Thus, once a set of drones form a swarm, the swarm follows a mobility model resulted of different behaviors, namely separation, cohesion, alignment and the RWP mobility model as well. The Table 1 summarizes the predefined variables.

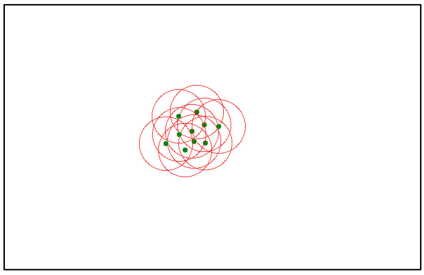
Table 1. Simulation parameters

Designation	Value
Area	X = Y = 1000 m
Number of drones	1..N
UAV altitude	20 m
D	200 bytes
P_t	20 dBm (100 mW)
Path loss type	Free space
Pnoise + Pinterf	−60 dBm (Constant)
Antennas gains	Ge = Gr = 10 dBi
Carrier frequency	2.4 GHz
Drone' packet sending interval	1 s
Intruder mobility model	RWP
Single drone mobility model	RWP
Swarm mobility model	Cohesion, separation, alignment and RWP

The result of the Fig. 2 shows the influence of the SNR parameter on the swarm connectivity and the area size covered by the swarm. As illustrated in Fig. 2a, a low SNR value allows to cover a larger area and therefore, the drones of the same swarm maintain the maximum distance possible. In the same logic, a higher SNR result a small size area covered by the swarm, since the distances that separate the drones is small. In addition, the Fig. 3a illustrates two separate swarms and having two different bearing. In fact, our algorithm can generate more than one swarm at the same time t. When communication between two different swarms is possible, these latter constitute a single one swarm as depicted



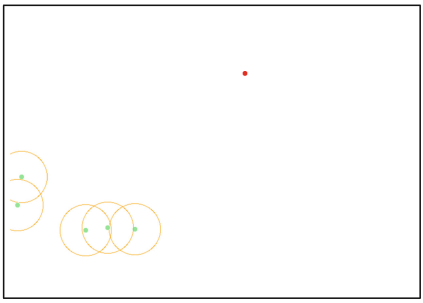
(a) SNR Separation parameter = 10dBm



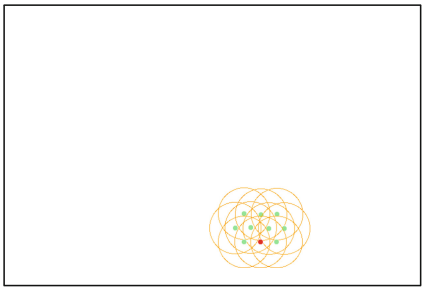
(b) SNR Separation parameter = 16dBm

Fig. 2. UAVs swarm formation with different SNR separation parameters

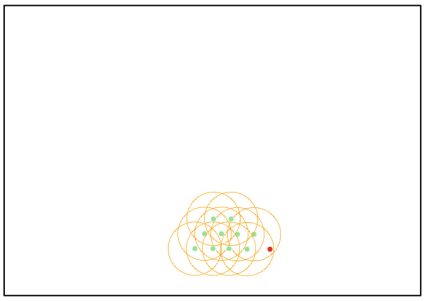
in Figs. 2, 3b and c. The intruder localization is illustrated by Fig. 3b and c. Indeed, when an intruder is within one drone camera field of view, the swarm change its topology and the drones become closer to each other in order to ensure a high data rate for video forwarding to the controller side.



(a) Two separate swarms for intruder search



(b) Intruder localized by the swarm



(c) UAVs fleet for video stream reporting

Fig. 3. Intruder search and report scenario

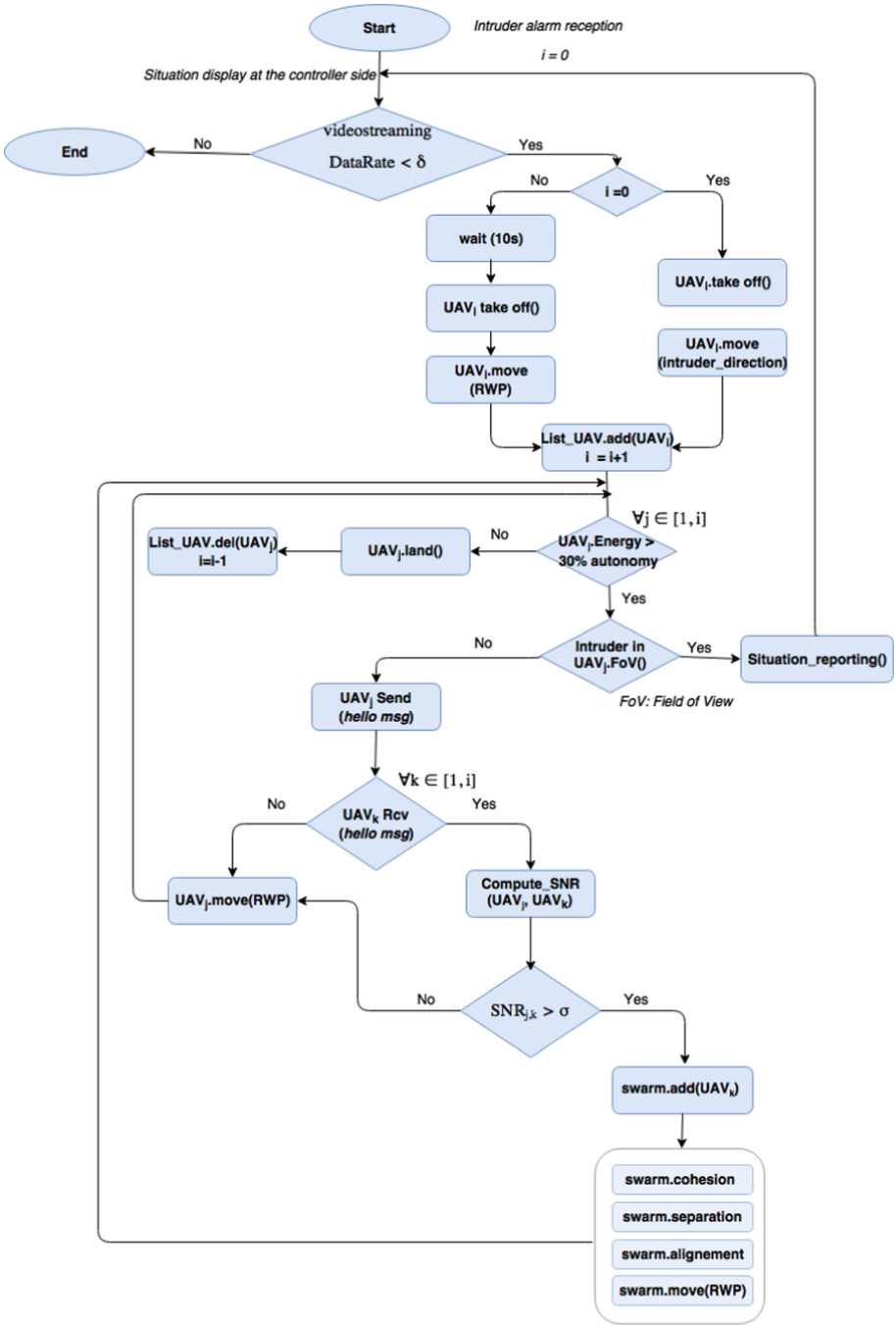


Fig. 4. UAVs swarm intruder tracking and video stream reporting flow chart

5 Conclusion

We propose a comprehensive solution for borders and sensitive areas control and monitoring through the use and the exploitation of the communications and imaging capabilities of a team of drones. The proposal should improve the response time between intruder detection and interception, and thus allows to better compare the nature and level of the threat, and consequently yield to optimize the deployment of resources and enhance their values. We showed the flocking scheme based on the quality of the received signal between drones of the same swarm enable to avoid collision end to cover a large area.

Nevertheless other methods deserve to be explored for faster execution, in particular the potential field, only the solution mentioned above has been tested. In addition, the video stream reporting needs to be evaluated, either by simulation or with experiments to assess the influence of multi hops video forwarding on the quality of the situation displayed at the controller side and the. This is left for future work.

References

1. Bekhti, M., Abdennebi, M., Achir, N., Boussetta, K.: Path planning of unmanned aerial vehicles with terrestrial wireless network tracking. In: Wireless Days (WD), pp. 1–6. IEEE (2016)
2. Gazi, V., Passino, K.M.: Stability analysis of swarms. IEEE Trans. Autom. Control **48**(4), 692–697 (2003)
3. Geier, J.: How to: Define Minimum SNR Values for Signal Coverage (2008). http://www.wi-fiplanet.com/tutorials/article.php/3743986
4. Hattenberger, G.: Vol en formation sans formation: contrôle et planification pour le vol en formation des avions sans pilote. Ph.D. thesis, Université Paul Sabatier-Toulouse III (2008)
5. Khatib, O.: Real-time obstacle avoidance for manipulators and mobile robots. In: Cox, I.J., Wilfong, G.T. (eds.) Autonomous Robot Vehicles, pp. 396–404. Springer, New York (1986). https://doi.org/10.1007/978-1-4613-8997-2_29
6. Leonard, N.E., Fiorelli, E.: Virtual leaders, artificial potentials and coordinated control of groups. In: Proceedings of the 40th IEEE Conference on Decision and Control, vol. 3, pp. 2968–2973. IEEE (2001)
7. Reynolds, C.W.: Flocks, herds and schools: a distributed behavioral model. ACM SIGGRAPH Comput. Graph. **21**(4), 25–34 (1987)
8. Techaccess. Pre-installation Wi-Fi Site Survey Report. https://www.techaccess.be/wp-content/uploads/2013/10/Pre-Installation-WLAN-Site-Survey-Report-VOORBEELD-BE.pdf

Ring of Scatterers Based Localization Using Single Base Station

Zengshan Tian, Yueyue Shu(✉), Yong Li, Mu Zhou, and Ze Li

Chongqing University of Posts and Telecommunications, Chongqing 400065, China
{tianzs,zhoumu}@cqupt.edu.cn, shuyueyue6@163.com,
ly94ong@163.com, lizecqupt@yahoo.com

Abstract. In this paper, a new Mobile Station (MS) Localization approach based on Ring of Scatterers (ROS) is proposed in response to the Non-Line-of-Sight (NLOS) environments. By exploiting the geometrical relations among the MS, scatterers, and the single base station, we present a Geometric Characteristics Based (GCB) localization algorithm with ROS model which provides conditional information for accurate location estimation of MS and scatterers. Simulation results illustrate the superior performance of proposed algorithm in typical NLOS environments.

Keywords: Mobile Station Localization · Non-Line-of-Sight
Single Base Station · Ring of Scatterers

1 Introduction

The Federal Communication Commission (FCC) released an act in 1996 which required cellular service providers to estimate subscribers locations for Enhanced-911 (E-911) demand [1]. And this act inspired significant research enthusiasm on the modern cellular mobile communication system which is utilized as a new positioning mechanism in people's daily travel, transportation navigation, and national information security [2]. By using measurements such as Time of Arrival (TOA) [3], Angle of Arrival (AOA) [4], or their joint adoption [5], the Mobile Station (MS)s position can be estimated with accurately collected data. However, in the actual scenario, the measured data are dramatically deteriorated due to Non-Line-of-Sight (NLOS) effect. And the absence of a direct Line-of-Sight (LOS) path between MS and Base Station (BS) also makes traditional LOS-based positioning methods unavailable. In order to alleviate the localization errors in the NLOS situation, a lot of work has been done, such as using the scattering model [6], or reconstructing the major positioning parameters [7]. Authors in [6] designed the single base station positioning method based on two layer scattering model. In [7], by analyzing the polynomial fit curve of TOA, authors reconstructed the TOA in LOS path to reduce the NLOS error. Most of related solutions above assume that either there is at least one BS with

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 232–238, 2018.
https://doi.org/10.1007/978-3-319-90802-1_20

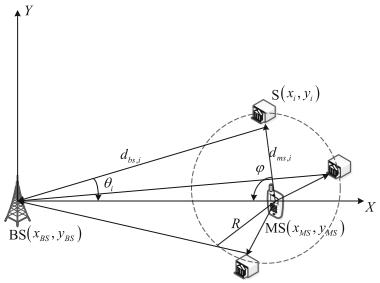


Fig. 1. ROS model.

LOS path or there are more than three BSs available. But the measurements are always associated with NLOS path from a single BS at a given MS location in many practical cases.

In this paper, a new localization approach is proposed based on the single BS to tackle the NLOS involved problem. Using the one-bounced Ring of Scatterers (ROS) model, the Geometric Characteristics Based (GCB) algorithm is designed without the LOS path and the feasible region is constricted for optimal location estimations corresponding to MS position and scatterers.

The remaining of this paper is organized as follows. In Sect. 2, the ROS model is presented. And the GCB algorithm is described in Sect. 3. Section 4 shows the associated simulations and numerical results. Finally, some concluding remarks are given in Sect. 5.

2 Scattering Model: ROS Model with a Single Base Station

In the ROS model, the signal undergoes a single reflection from the mobile station to the base station through the scatterers witch are uniformly distributed on a MS centered ring with the radius, R. The angle φ between MS to BS and scatterers is uniformly distributed within $[0, 2\pi]$ as shown in Fig. 1. In this model, the height of antennas are relatively high. Thus, there is no scatterer near the base station. At the same time, there is no LOS path, and only one base station is used for positioning here.

In Fig. 1, the BS is assumed to locate at the origin with coordinate $(0, 0)$ and the line from BS to MS is the x axis. The signal are reflected by m scatterers from MS and BS. And the TOA and AOA measurements at BS corresponding to $i-$th scatterer are denoted by τ_i and θ_i respectively. The associated propagation distance in (1), L_i, includes the distance $d_{ms,i}$ between the MS location, (x_{MS}, y_{MS}), and the $i-$th scatterer location, (x_i, y_i), and the distance between BS location, (x_{BS}, y_{BS}), and (x_i, y_i).

$$L_i = c\tau_i = d_{ms,i} + d_{bs,i}\,,\ i = 1, \cdots, m \tag{1}$$

where m is the number of scatterers on the ring. $c = 3 \times 10^8$ m/s. Meanwhile, the coordinate of $i-$th scatterer (x_i, y_i), also can be expressed as

$$\begin{cases} x_i = d_{bs,i} \times \cos\theta_i \\ y_i = d_{bs,i} \times \sin\theta_i. \end{cases} \tag{2}$$

Then, (1) is equal to

$$\sqrt{\left(x_{MS} - d_{bs,i} \cdot \cos\theta_i\right)^2 + \left(y_{MS} - d_{bs,i} \cdot \sin\theta_i\right)^2} + d_{bs,i} = c\tau_i\,,\ i = 1, \cdots, m\,. \tag{3}$$

Equation (3) contains m equations and $m+2$ unknown parameters which involve $d_{bs,i}\,(i = 1, \cdots, m)$ and (x_{MS}, y_{MS}).

3 The Proposed GCB Algorithm

3.1 MS Location Model

From ROS model in Fig. 1, we have

$$c\tau_1 - d_{bs,1} = c\tau_{j+1} - d_{bs,j+1}\,,\ j = 1, \cdots, m-1\,. \tag{4}$$

Thus, combining (3) and (4), we can convert the underdetermined equations in (3) into the overdetermined ones as if $m > 3$ as shown in (5).

$$\begin{cases} \sqrt{\left(x_{MS} - d_{bs,i} \cdot \cos\theta_i\right)^2 + \left(y_{MS} - d_{bs,i} \cdot \sin\theta_i\right)^2} + d_{bs,i} = c\tau_i\,,\ i = 1, \cdots, m \\ c\tau_1 - d_{bs,1} = c\tau_{j+1} - d_{bs,j+1}\,,\ j = 1, \cdots, m-1\,. \end{cases} \tag{5}$$

Here (5) provides $2m-1$ independent equations with $m+2$ unknown parameters. Since the AOA and TOA measurements are generally with errors due to multipath effect, we utilize NLOS propagation by considering the errors into range estimation, thus the localization towards target can be obtained by minimizing the Nonlinear Least Squares Problem (NL-LS) in (6).

$$F(\mathbf{x}) = \frac{1}{2}\sum_{p=1}^{2m-1} {f_p}^2(\mathbf{x}) = \frac{1}{2}\left(\varepsilon_1, \varepsilon_2, \cdots \varepsilon_m, \xi_1, \xi_2, \cdots, \xi_{m-1}\right)\left(\varepsilon_1, \varepsilon_2, \cdots \varepsilon_m, \xi_1, \xi_2, \cdots, \xi_{m-1}\right)^T \tag{6}$$

where $\mathbf{x} = \left(x_{MS}, y_{MS}, d_{bs,i}\right)^T$, $\chi = \left(d_{bs,1}, d_{bs,j+1}\right)^T$. The $\varepsilon_i(\mathbf{x})$ and $\xi_j(\chi)$ are derived by moving the right hand side of the two equations in (5) to the left and making the equation equal to zero.

In our system, the minimum range $L_{\min} = c\tau_{\min}$ implies that the MS is inside a BS centered circle with radius $L_{\min}$. And the maximum and minimum of AOA measurements constrain MS to a fan-shaped area with angle α as shown by dash lines in Fig. 2. Thus feasible region of MS can be expressed as

$$\begin{cases} \sqrt{\left(x_{MS} - x_{BS}\right)^2 + \left(y_{MS} - y_{BS}\right)^2} \le c\tau_{\min} \\ \alpha_1\left(x_{MS}, y_{MS}\right) \le \alpha \\ \alpha_2\left(x_{MS}, y_{MS}\right) \le \alpha \end{cases} \tag{7}$$

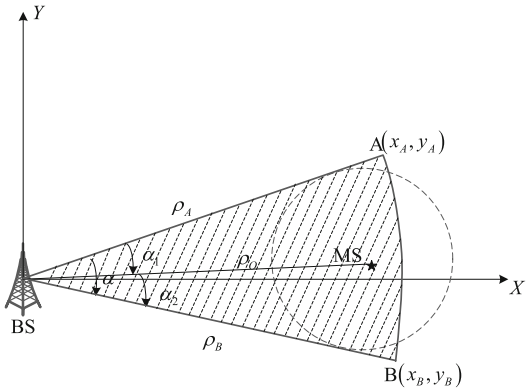


Fig. 2. Feasible region of MS.

and $d_{bs,i} \leq c\tau_{\max}$, where α denotes the maximal angle formed by vectors $\overrightarrow{\rho_A}$ and $\overrightarrow{\rho_B}$ with equal length $L_{\min}$. $\alpha_1\left(x_{MS}, y_{MS}\right)$ and $\alpha_2\left(x_{MS}, y_{MS}\right)$ are the functions of x_{MS} and y_{MS} corresponding to α_1 and α_2 respectively.

Thus, the above localization problem is transformed into a nonlinear constrained least squares problem.

3.2 The LM-BFGS Algorithm

We adopt Levenberg-Marquard (LM) method to solve the nonlinear least squares problem. Specifically, the increment of variants $\Delta\mathbf{x}$ is formed as follows.

$$\Delta\mathbf{x}_k = -(\mathbf{H}_k + \mu_k\mathbf{I})^{-1}{\mathbf{A}_k}^T\mathbf{b}_k, \tag{8}$$

where $\Delta\mathbf{x}_k = (\Delta x, \Delta y, \Delta L_i) = \mathbf{x} - \mathbf{x}_k$, $\mathbf{H}_k = {\mathbf{A}_k}^T\mathbf{A}_k$ is the approximate Hessian matrix, k is the number of iterations, $\mathbf{I}$ is the identity matrix, μ_k is a scalar. $\mathbf{A}_k$ is Jacobean matrix and $\mathbf{b}_k = \left[\, f_1\left(\mathbf{x}_k\right)\ f_2\left(\mathbf{x}_k\right) \cdots f_{2m-1}\left(\mathbf{x}_k\right)\right]^T$. As a consequence, successive location estimations are updated according to the recursion

$$\mathbf{x}_{k+1} = \mathbf{x}_k + \lambda_k\Delta\mathbf{x}_k, \tag{9}$$

where λ_k is learning rate which is updated according to the Armijo criterion [8].

However, the LM algorithm obtains the approximate Hessian matrix only by $\mathbf{H}_k = {\mathbf{A}_k}^T\mathbf{A}_k$ which ignores the term with second order, $\mathbf{M}\left(\mathbf{x}\right) = \sum_{p}^{2m-1} f_p\left(\mathbf{x}\right)\nabla^2 f_p\left(\mathbf{x}\right)$, and thus causes a greater error with large residuals. Based on quasi-Newton updating [9] we conduct the Broyden-Fletcher-Goldfarb-Shanno (BFGS) to update the approximate value of the second order according to [10]. Thus the the approximate Hessian matrix can be rewritten as $\tilde{\mathbf{H}}_k = {\mathbf{A}_k}^T\mathbf{A}_k + \mathrm{B}_k$, where $\mathrm{B}_k \approx \mathbf{M}_k$. The use of BFGS generally has better performance for full Hessian approximations in nonlinear programming objective function [11]. Based on LM-BFGS algorithm, the final estimate position $(\hat{x}_{MS}, \hat{y}_{MS})$ is obtained by minimizing the cost function.

4 Simulations and Numerical Results

Simulations are performed to validate the efficiency of the proposed GCB localization algorithm. Specifically, 1000 independent simulations are conducted. The BS and MS are located at $(0, 0)$ and $(1000, 0)$. The TOA and AOA measurements are added by Gaussian noises with standard deviations σ_{TOA} and σ_{AOA} respectively. And we use the Root Mean Square Error (RMSE) $RMSE = \frac{1}{1000}\sum_{n=1}^{1000}\sqrt{(\hat{x}_{MS}(n) - x_{MS})^2 + (\hat{y}_{MS}(n) - y_{MS})^2}$ to evaluate the positioning accuracy.

Firstly, we discuss the variations of positioning accuracy with respect to the number of scatterers and the radius of ROS. We set $\sigma_{TOA} = 5\,\mathrm{m}$ and $\sigma_{AOA} = 2^\circ$. From Fig. 3, we can observe that the positioning performance is improved with increased number of scatterers, and the improvement is insignificant when the number of scatterers is greater than 12. Besides, the RMSE decreases as the radius of ROS increases.

In the second experiment, we vary the standard deviations of TOA and AOA to evaluate the performance behavior of our method with $m = 12$ and $R = 100\,\mathrm{m}$.

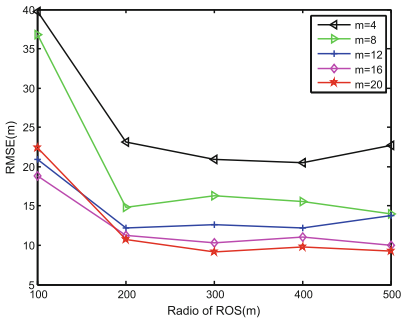


Fig. 3. RMSE with respect to the different number of scatterers and the different radius of ROS.

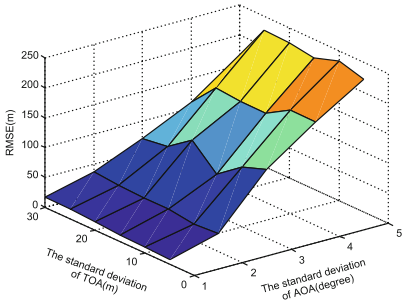


Fig. 4. RMSE with respect to the different standard deviations of TOA and AOA.

As illustrated in Fig. 4, the AOA error has a significant effect on the position error. TOA error also has certain influence on the positioning accuracy which is not obvious when the AOA error is large.

5 Conclusion

This paper presents a new MS positioning approach based on single BS in NLOS environment. The proposed GCB algorithm fully utilizes the geometrical characteristics of ROS to make localization problem resolvable with a simple LS method. Specifically, the positioning error will decrease as the radius of ROS increases which is different from the usual case. However this feature is beneficial for macrocell based positioning.

Acknowledgment. This work was supported by the National Natural Science Foundation of China (61301126, 61471077), Program for Changjiang Scholars and Innovative Research Team in University (IRT1299), Special Fund of Chongqing Key Laboratory (CSTC).

References

1. Federal Communications Commission: Revision of the commissions rules to ensure compatibility with enhanced 911 emergency calling systems, report and order and further notice of proposed rulemaking, Technical report CC Docket, pp. 94–102 (1996)
2. Bill, F.: Global positioning system and telematics. IEEE Veh. Technol. Mag. **5**(2), 4–7 (2016)
3. Abu-Shaban, Z., Zhou, X., Abhayapala, T.D.: A novel TOA-based mobile localization technique under mixed LOS/NLOS conditions for cellular networks. IEEE Trans. Veh. Technol. **65**(11), 8841–8853 (2016)
4. Nguyen, T.L.N., Shin, Y.: A new approach for positioning based on AOA measurements. In: IEEE International Conference on Computing Management and Telecommunications, pp. 21–24. IEEE Press, New York (2013)
5. Chang, J.C., Shen, C.C.: Hybrid TOA/AOA measurements based on the Wiener estimator for cellular network. In: IEEE 12th International Conference on Networking, Sensing and Control, pp. 9–11. IEEE Press, New York (2015)
6. Tian, Z., Yao, L., Zhou, M., Zhou, F., Zhang, L.: Scattering model based hybrid TOA/AOA/AOD localization in NLOS environment. In: Zhang, B., Mu, J., Wang, W., Liang, Q., Pi, Y. (eds.) The Proceedings of the Second International Conference on Communications, Signal Processing, and Systems. LNEE, vol. 246, pp. 893–901. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-00536-2_103
7. Lei, Y., Wang, M., Xiao, N.: NLOS error mitigation in mobile location based on TOA reconstruction. In: IET International Conference on Information and Communications Technologies, pp. 475–480. Institution of Engineering and Technology, United Kingdom (2013)
8. Wardi, Y., Egerstedt, M., Hale, M.: Switched-mode systems: gradient-descent algorithms with Armijo step sizes. Discrete Event Dyn. Syst. **24**(4), 571–599 (2015)
9. Dennis, J.E., Gay, D.M., Walsh, R.E.: An adaptive nonlinear least-squares algorithm. ACM Trans. Math. Softw. (TOMS) **7**(3), 348–368 (1981)

10. Yaping, X., Pengfei, C.: The application of a presented hybrid BFGS-based method for data analysis in automation system, In: IEEE International Conference on Computational Intelligence and Communication Networks, pp. 973–976. IEEE Press, New York (2015)
11. Powell, M.J.D.: How bad are the BFGS and DFP methods when the objective function is quadratic? Math. Program. **34**(1), 34–47 (1986)

Wireless Networking (II)

An Enhanced Listen Before Talk (e-LBT) Mechanism for Avoiding Hidden Nodes in an LTE-U and WiFi Coexistence System

Liangyu Chu, Jun Zheng(✉), and Jie Xiao

National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, Jiangsu, People's Republic of China
{lychu,junzheng,jiexiao}@seu.edu.cn

Abstract. This paper considers the hidden node avoidance problem in an LTE-U and WiFi coexistence system operating in unlicensed bands. An enhanced Listen Before Talk (e-LBT) mechanism is proposed for coordinating the LTE-U and WiFi systems. To support the e-LBT mechanism, we first enhance an LTE-U node by introducing a WiFi module in the LTE-U eNB and redefining the RRC and MAC functional blocks in both LTE-U eNB and LTE-U UE in order to enable information exchange between an LTE-U node and a WiFi node. Moreover, the e-LBT mechanism incorporates an RTS/CTS handshaking mechanism in the basic LBT mechanism to resolve the hidden node problem. Simulation results show that the proposed e-LBT mechanism can significantly improve the performance of the coexistence system in terms of LTE-U system throughput as compared with the basic LBT mechanism.

Keywords: Coexistence · Hidden node · LBT · LTE-U · WiFi

1 Introduction

Unlicensed spectrum bands are being considered as the supplement of licensed spectrum for cellular networks [1]. The third Generation Partnership Project (3GPP) is currently studying Licensed-Assisted Access (LAA) using LTE in the unlicensed spectrum (LTE-U), and the LTE-U and WiFi coexistence in the unlicensed bands [2]. A critical issue that arises with the use of unlicensed spectrum for cellular users is the coexistence of an LTE-U system and a WiFi system in the same unlicensed band. Due to the different channel access mechanisms employed by the two systems, how to coordinate the channel access of users from the different systems becomes a challenging issue for the coexistence of LTE-U and WiFi. According to the study results in [3], if there is no additional mechanism to coordinate LTE and WiFi coexistence, an LTE system will occupy the majority of channel access opportunities and thus significantly affect the performance of a WiFi system. To address this issue, several MAC mechanisms have been proposed to improve the performance of LTE-U and WiFi coexistence, such as Almost Blank Subframe (ABS), Carrier Sense Adaptive Transmission (CSAT), and Listen Before Talk (LBT) [4–6].

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 241–249, 2018.
https://doi.org/10.1007/978-3-319-90802-1_21

LBT was originally proposed in 3GPP LAA specifications [2]. In some regions, like Europe and Japan, LBT is one of mandatory regulations in LTE-U implementation. The main idea of LBT is to allow an LTE-U node to sense a channel for a while before starting transmission. If the channel is idle, the node will transmit after a predefined time interval. Otherwise, the node needs to keep quiet and periodically sense the channel in the subsequent subframes until the channel becomes idle. However, as the range that the node can sense is limited, the classical *hidden node* problem is unavoidable with LBT. In the IEEE 802.11 (WLAN) standard [6], a node is referred to be hidden from other node(s) when it is out of the sensing or detection range of other node(s). When more than two hidden nodes transmit data simultaneously, often referred to as *collision*, the transmitted packets cannot be successfully decoded at the receivers with a high probability. To address this problem, request to send/clear to send (RTS/CTS) was introduced in the IEEE 802.11 standard. Two communicating nodes need to *handshake* by exchanging RTS and CTS messages before transmission to avoid collision. For an LTE-U and WiFi coexistence system, however, different channel access mechanisms are employed in LTE-U and WiFi, which makes an LTE-U node unable to exchange RTS/CTS messages with a WiFi node, and cannot resolve the hidden node problem to an extent as expected.

In this paper, we consider the hidden node avoidance problem in an LTE-U and WiFi coexistence system operating in an unlicensed spectrum band. We first enhance LTE-U nodes by introducing a WiFi module in the LTE-U eNB and redefine the RRC and MAC functional blocks in both LTE-U eNB and LTE-U UE in order to enable information exchange between an LTE-U node and a WiFi node. Based on the enhanced LTE-U nodes, we further propose an enhanced listen-before-talk (e-LBT) mechanism, which incorporates an RTS/CTS handshaking mechanism in the basic LBT mechanism to resolve the hidden node problem. Simulation results are shown to evaluate the performance of the proposed e-LBT mechanism in terms of LTE-U system throughput.

The rest of this paper is organized as follows. Section 2 reviews recent related work. Section 3 presents the proposed e-LBT mechanism. Section 4 shows simulation results to evaluate the performance of the e-LBT mechanism. Section 5 concludes this paper.

2 Related Work

LTE in Unlicensed bands (LTE-U) has become a hot research area in recent years and considerable work has been conducted in this area. In [2], 3GPP recommends LTE-U deployment scenarios, introduces unlicensed spectrum band ranges in different countries, and defines indoor and outdoor channel models. For LTE-U, a main concern is how to coordinate LTE and WiFi systems coexisting in the same unlicensed band. To address this concern, a variety of coexistence mechanisms have been proposed in the literature [4–6]. In [4], Almeida et al. introduced Almost Blank Subframes (ABS) in LTE-U to coordinate the LTE-U and WiFi coexistence. In [5], Qualcomm proposed a carrier sense adaptive transmission (CSAT) mechanism, in which an LTE-U eNB dynamically activates and deactivates its transmission in a time cycle based on the sensed

channel status. In [6], 3GPP proposed a listen before talk (LBT) mechanism, in which an LTE-U node senses an unlicensed channel before data transmission.

As mentioned in Sect. 1, a MAC mechanism based on channel sensing, such as LBT and CSMA/CA, will inevitably cause the hidden node problem due to the limited sensing coverage of a node. In [7, 8], Panasonic and Samsung evaluated the influence caused by hidden nodes when LBT is employed. Moreover, they used UE reporting and RTS/CTS signaling to detect hidden nodes. However, no specific MAC mechanism is presented in [7, 8]. In [9], however, Lien et al. pointed out that RTS/CTS cannot be used in an LAA-WiFi coexistence scenario due to the lack of a unified information exchange interface between an LTE-U system and a WiFi system. Regardless of the above work, the hidden node problem in an LTE-U and WiFi coexistence system has not been well studied and resolved, which motivated us to conduct this work.

3 Enhanced Listen Before Talk (e-LBT) Mechanism

In this section, we present the proposed e-LBT mechanism for an LTE-U and WiFi coexistence system.

3.1 System Model

We consider a basic LTE-U and WiFi coexistence system consisting of multiple LTE-U networks and multiple WiFi networks, as shown in Fig. 1. Both the LTE-U networks and WiFi networks operate in the same unlicensed band. The LTE-U network uses the LBT mechanism to access the channel, while the WiFi network uses the CSMA/CA access mechanism.

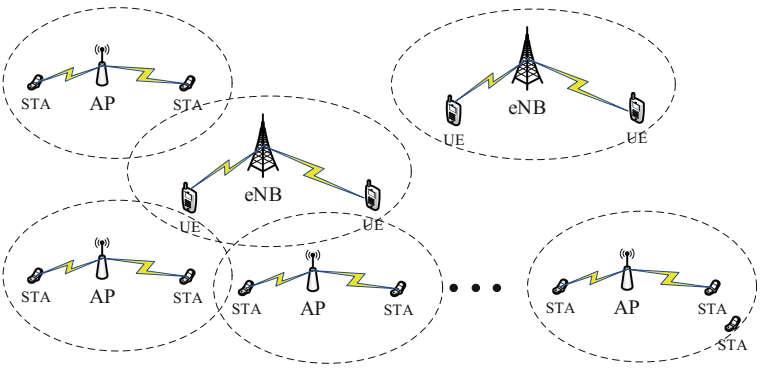


Fig. 1. System model

In Fig. 1, the dotted lines stand for the transmission ranges of different networks. The LTE-U eNB senses the channel before transmission. However, the access points (APs) of the WiFi networks are out of the sensing range of the LTE-U eNB. Thus the LTE-U eNB cannot sense the existence of the APs. When the APs and eNB transmit

simultaneously, the hidden node problem will occur. Similarly, the hidden node problem will also occur when a WiFi node has data to transmit and an LTE-U node is out of the sensing range of the WiFi node.

3.2 Enhanced LTE-U Nodes

In the system model described in Fig. 1, the LTE-U networks and WiFi networks employ different channel access mechanisms. Typically, an LTE-U node and a WiFi node cannot implement information exchange between each other. As indicated in [9], without a universal air interface for information exchange between a Wi-Fi network and an LTE-U network, RTS/CTS cannot be used to resolve the hidden-node problem. To enable the information exchange between the two different networks, we introduce a WiFi module in the LTE-U eNB to enhance the functionality of the eNB, and redefine the RCC functional block in the LTE module of the eNB, renamed e-RRC, as shown in Fig. 2. For an LTE-U UE, we redefine the RCC functional block in its LTE module and the MAC functional block in its WiFi module [10], which are renamed e-RRC and e-MAC, respectively.

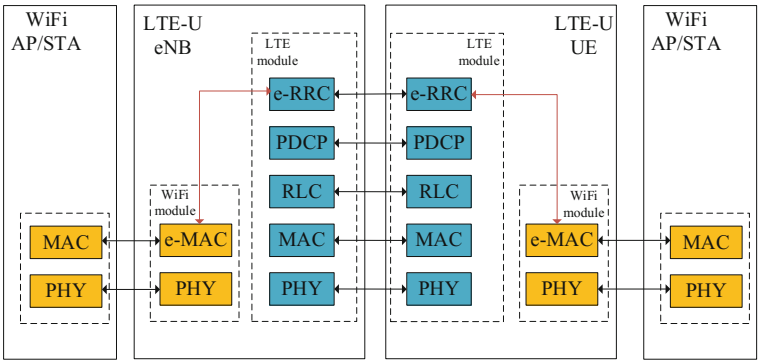


Fig. 2. Functional blocks of enhanced LTE-U nodes

The enhanced eNB is composed of two components, LTE module and WiFi module. The LTE module is used to transmit data, and determine whether the LTE node needs to transmit and whether it can transmit. The WiFi module is used to sense a channel, receive/send WiFi signaling messages, reserve a channel, and exchange relevant information with the LTE module. In the LTE module, a new function is added in e-RRC to implement the information exchange with e-MAC in the WiFi module. Similarly, in the WiFi module, a counterpart function is added in e-MAC to implement the information exchange with e-RRC.

3.3 Enhanced Listen Before Talk (e-LBT) Mechanism

The e-LBT mechanism is a channel access mechanism for resolving the hidden node problem in the LTE-U and WiFi coexistence system. It is based on the enhanced LTE

eNB and UE nodes described in Sect. 3.2. Meanwhile, it introduces RTS/CTS in the basic LBT mechanism.

In the e-LBT mechanism, each LTE-U node will sense the channel through the WiFi module before data transmission. If the channel is idle, the e-MAC of the WiFi module will report the channel status to the e-RRC of the LTE module. Once the LTE module receives the channel status, it will send the destination address, source address, and transmission length information to the WiFi module. Once the WiFi module receives the information, it will send an RTS message to all neighbor nodes within its transmission range, and includes all the information in the RTS message. After the destination node receives the RTS message, it will reply with a CTS message after a short interframe space (SIFS) duration. Once the LTE-U node receives the CTS message, the e-MAC of the WiFi module will report the information contained in the received CTS message to the LTE module. After the LTE module receives the reported information, it will start to transmit data after another SIFS duration. If the RTS/CTS exchange is unsuccessful or the ACK message is absent, the node will wait a backoff time and then start the RTS/CTS exchange again. The RTS and CTS messages include a time field to inform other nodes of the length of the current transmission. All neighbor nodes that receive the RTS or CTS messages will update their Network Allocation Vector (NAV) fields with the value of the time field in the RTS and CTS messages. A neighbor node will not access the channel until the value of its NAV field reaches 0 [6]. Figure 3 illustrates the signaling procedure of the e-LBT mechanism when an LTE-U eNB has data to transmit to an LTE-U UE.

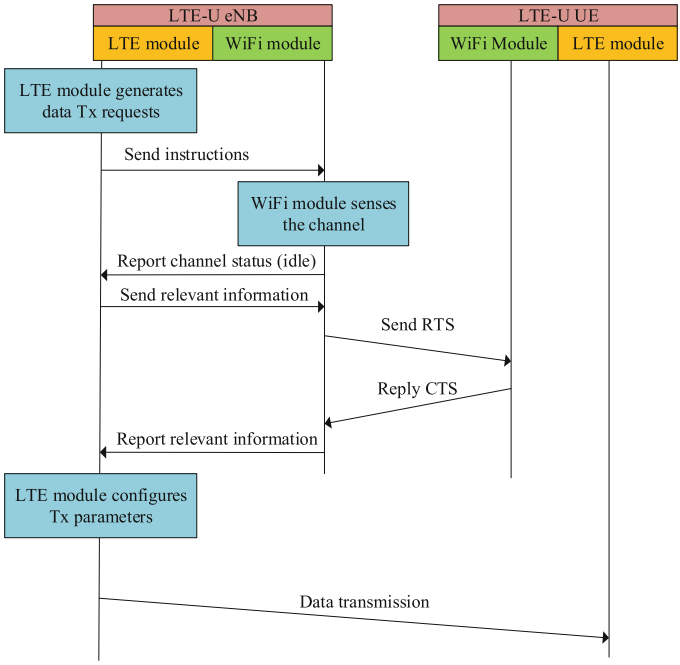


Fig. 3. Signaling procedure of LTE-U transmission

4 Simulation Results

In this section, we evaluate the performance of the proposed e-LBT mechanism through simulation results. The simulation experiments were conducted on a simulator developed using NS3 [11]. We use the LTE-U system throughput and WiFi system throughput as the performance metrics, which are defined as the average number of bits that LTE-U users transmit and the number of bits that WiFi users transmit in a second, respectively. The parameters used in the simulation experiments are given in Table 1.

Table 1. Simulation parameters

Parameter	Value
Network layout	Indoor
eNB/AP transmission power	18 dBm
Unlicensed channel bandwidth	20 MHz
Unlicensed spectrum frequency	5.18 GHz
Antenna type	2D omnidirectional
eNB antenna height	6 m
UE antenna height	1.5 m
Number of UEs	20
Traffic model	FTP model-1

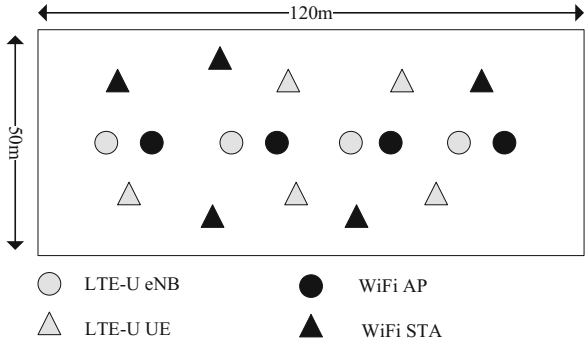


Fig. 4. Center placement

We consider two simulation scenarios, "center placement" and "corner placement", to evaluate the influence of hidden nodes. In both scenarios, four eNBs and four APs are placed in a 120 m*50 m room, and 20 UEs are randomly distributed in the rectangular region, without redropping [2]. In the center placement, the eNBs and APs are evenly spaced and centered in the shorter dimension of the room, as shown in Fig. 4. The distances between two neighbor eNBs or APs are equal. If we set the bottom-left corner as the origin of the coordinate system, the eNBs (LTE-U) are placed in (15,25), (40,25), (75,25) and (100,25), and the APs (WiFi) are placed in (20,25), (45,25), (80,25) and (105,25), respectively. In the corner placement, the eNBs and the APs are placed at the corners of the room, as shown in Fig. 5. In the same coordinate system, the eNBs are

placed at (0,0), (0,50), (120,0) and (120,50), and the APs are placed at (1,1), (1,49), (119,1) and (119,49) [11], respectively.

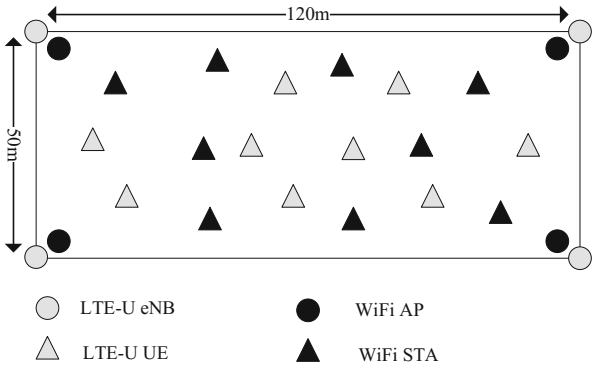


Fig. 5. Corner placement

The simulation results are shown in Figs. 6 and 7, where we use "center" and "corner" to represent the center placement and corner placement, respectively, and use "LBT" and "e-LBT" to represent the basic LBT mechanism and the e-LBT mechanism, respectively.

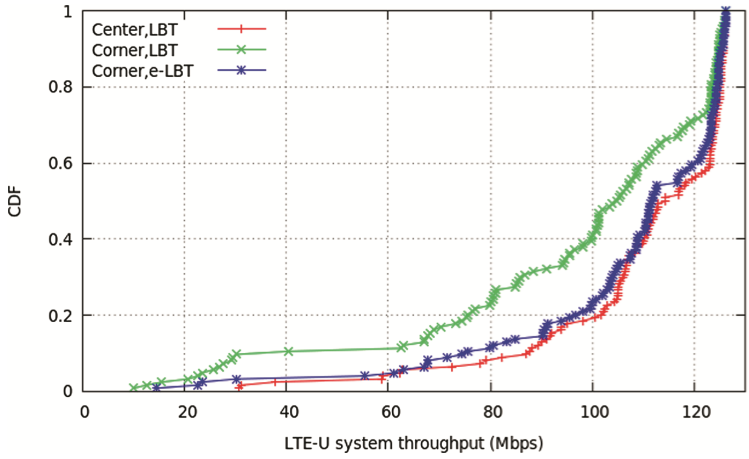


Fig. 6. LTE-U system throughput

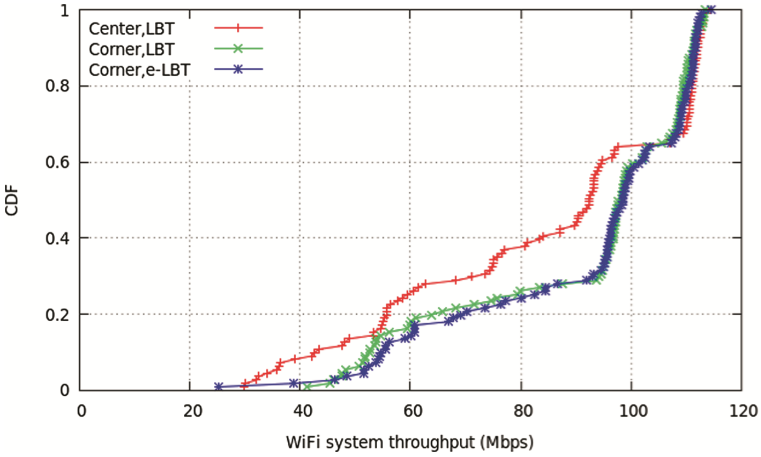


Fig. 7. WiFi system throughput

Figure 6 shows the LTE-U system throughput with the basic LBT mechanism and the e-LBT mechanism in the two scenarios, respectively. It is seen that with LBT the LTE-U system throughput is larger in the center placement than that in the corner placement. This is because that the distance between eNBs and UEs in the corner placement are much larger than that in the center placement, which results in more hidden nodes in the corner placement and thus causes more serious interference. On the other hand, in the corner placement, the LTE-U system throughput with e-LBT is larger than that with LBT. This is because that with e-LBT an LTE-U node is enhanced with an additional WiFi module which can exchange signaling information with the WiFi nodes. Meanwhile, the RTS/CTS mechanism is introduced to avoid the collisions caused by the hidden node problem.

Figure 7 shows the WiFi system throughput with the basic LBT mechanism and the e-LBT mechanism in the two scenarios, respectively. It is seen that with LBT the WiFi system throughput in the corner placement is larger than that in the center placement. This is because the distances between WiFi nodes are smaller than those in LTE-U nodes in the corner placement. As a result, there are less hidden nodes with the WiFi systems in the corner placement. According to Fig. 6, there are more hidden nodes with the LTE-U systems in the corner placement, which would degrade the throughput of the LTE-U system and thus improve the WiFi system throughput. On the other hand, it is seen that the WiFi system throughput with e-LBT in the corner placement is larger than that with LBT in the center placement, but does not have much difference as compared with that with LBT in the corner placement.

5 Conclusions

In this paper, we considered the hidden node avoidance problem in an LTE-U and WiFi coexistence system operating in unlicensed bands. An e-LBT mechanism was proposed

for coordinating the LTE-U and WiFi systems. To support the e-LBT mechanism, an LET-U node was first enhanced by introducing a WiFi module in the LTE-U eNB and redefining the RRC and MAC functional blocks in both LTE-U eNB and LTE-U UE to enable information exchange between an LTE-U node and a WiFi node. To resolve the hidden node problem, the e-LBT mechanism incorporates a RTS/CTS handshaking mechanism in the basic LBT mechanism. Simulation results show that the proposed e-LBT mechanism can significantly improve the performance of the coexistence system in terms of the LTE-U system throughput as compared with the basic LBT mechanism.

References

1. Huawei: Discussion paper on unlicensed spectrum integration to IMT systems. 3GPP RAN 62 RP-131723 (2013)
2. 3GPP TR 36.889: Study on licensed-assisted access to unlicensed spectrum (Release 13) TR 36.889v13.0.0 (2015)
3. Nihtila, T., et al.: System performance of LTE and IEEE 802.11 coexisting on a shared frequency band. In: IEEE Wireless Communications and Networking Conference, pp. 1038–1043. IEEE Press, New York (2013)
4. Almeida, E., et al.: Enabling LTE/WiFi coexistence by LTE blank subframe allocation. In: IEEE International Conference on Communications, pp. 5083–5088. IEEE Press, New York (2013)
5. Qualcomm: LTE in unlicensed spectrum: harmonious coexistence with WiFi. White Paper (2014)
6. IEEE Std 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY). Specification (2012)
7. Panasonic: Hidden and exposed station statistics and implications in LAA Scenarios. 3GPP TSG-RAN R1-151018 (2015)
8. Samsung: Discussion on hidden node issue for LAA. 3GPP TSG-RAN R1-151047 (2015)
9. Lien, S.Y., et al.: Resource-optimal licensed-assisted-access in heterogeneous cloud radio access networks with heterogeneous carrier communications. IEEE. Trans. Vehi. Technol. **65**(12), 9915–9930 (2016)
10. Song, H., et al.: A spectrum etiquette protocol and interference coordination for LTE in Unlicensed Bands (LTE-U). In: IEEE International Conference on Communication Workshop, pp. 2338–2343. IEEE Press, New York (2015)
11. Giupponi, L., et al.: Simulating LTE and Wi-Fi coexistence in unlicensed spectrum with NS-3. https://arxiv.org/abs/1604.06826

A Space-Time Graph Based Unpredictable Interruptions-Resilient Routing Algorithm in Satellite Disruption-Tolerant Networks

Nan He(✉), Peng Yuan, Zhihua Yang, and Qing Guo

Communications Engineering Research Center, Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen, China
henan930906@163.com, yuanpl990@163.com, {yangzhihua,qguo}@hit.edu.cn

Abstract. In a satellite Disruption-Tolerant Network (DTN), unpredictable interruptions from node malfunction and link disruption will lead to severe postponements and even failure of bundles delivery mission due to incapability of originally planned paths. In this paper, we propose a space-time graph based multicast routing algorithm for coping with an unpredictable interruption in the network. In particular, the proposed algorithm could find a group of new paths with minimal cost by re-planning the two-dimensional global topology in the updated space-time graph. As a result, the residual volume of target data could be successfully delivered in time even if there is an unexpected interruption in the network. The simulation results show that the proposed interruptions resilient routing algorithm can achieve as short as possible, given a defined data volume to be delivery in a certain time latency.

Keywords: Satellite Disruption-Tolerant Network · Space-time graph Interruption · Routing

1 Introduction

Recently, satellite network has played an important role in the next generation network, due to its advantages of global coverage and realistic-time communication with their inter-satellite links (ISL). Compared with terrestrial networks, a satellite network confronts with a serial of unique challenges, i.e., intermittent links, limited resources and highly dynamic platforms, which probably cause no-existence of end-to-end paths for a delivery mission. Currently, Disruption Tolerant Network (DTN) is developing into a promisingly candidate solution for architecture of space information network especially satellite network, with its well-known store-carry-forward mechanism [1]. With the ever-increasing space scientific missions, massive amounts of various types of data require to be downloaded from orbits [2]. As a result, in a satellite DTN network, it is necessary to find reliable and efficient routes to deliver those bundled data for specific mission, considering full utilizations of transfer capability of network. Research on space DTN network routing algorithm has always been an important problem in space information network communication research. In recent years, most

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 250–260, 2018.
https://doi.org/10.1007/978-3-319-90802-1_22

of the research optimize the space information network routing algorithm, so as to improve the satellite network link utilization, shorten the end to end delay, balance the amount of data and other purposes. In [3], with regarding to the unbalanced load and the multimedia service of multimedia QoS requirements in GEO/LEO double layer satellite networks, a GEO/LEO double layer satellite networks multi-service routing algorithm is proposed. An optimized layered routing algorithm based on TORA and Dijkstra's algorithms is customized for the hybrid GEO/LEO satellite networks and aimed at balancing between data traffic and end-to-end delay in [4]. [5] proposes a Light Weight Security algorithm that forwards messages only to the trusted nodes, thus prevents the malicious or selfish nodes from affecting the entire DTN communication. However, in these routing algorithms, there is no solution to the problem of data transmission when a link is interrupted suddenly in a space information network.

However, in a found end-to-end path of delivery, unexpected interruptions, such as node malfunctions or link disruptions, will produce potentially catastrophic even fatal challenges for the bundles delivery mission, since they will destroy originally planned routes on the network topology and possibly incur complete failures of bundles forwarding mission in extreme case. For example, if a DTN endpoint encounter a malfunction leading to a reject for incoming bundles in the satellite network, the to-be-forwarded bundles at those previous endpoints on the associated routes will be carried for waiting recovery of the local endpoint. In extreme case, if it is a permanent damage event, the pre-configured routing table is disabled for all related routes without any prior sign. If we do not employ specific routing strategy for distributing these bundles into other feasible routes, prolonged waiting time will lead to a total failure of certain mission with a rigid latency requirements. Moreover, a prolonged sojourn time possibly inflicts loss of bundles since a Time-To-Live criterion constrains a life time for a bundle on the way. More important, a certain portion of forwarded data are on the way at many intermediate nodes, while another part of original data are still waiting to start at the source node. Therefore, preplanning them with specific routing strategies is quite indispensable for the success of target delivery mission. Unluckily, we do not find effective approaches among current routing strategies in the satellite networks. Recently, a two-dimensional directed graph, called as space-time graph, is developed for describing the satellite network with time-varying topology, which could discretize a time-evolving topology into a serial of snapshots in time by assuming quasi-static in discrete time intervals. With an excellent capability of capturing the connectivity and disconnection of each node in a time-varying network, therefore, a space-time graph can be conveniently used for modelling a sequence of time and space-related unexpected interrupting events in the satellite network, especially for a specific design of routing strategy. In this paper, we present a space-time graph based unpredictable interruptions-resilient routing policy in Space Disruption-Tolerant Networks, which could efficiently achieve a successfully completion of a given delivery mission of bundled message even though an unexpected interrupt occurs in the network. In particular, a group of optimization algorithms, involved with source node, interrupted node and other related nodes, are respectively proposed for re-planning those residual bundles un-arrived to the destination node with respect to the minimal cost of energy.

The rest of this article is organized as follows. Section 2 describes the space-time graph model and the problem formulation. Bundled data transmission and interrupt

routing algorithm is given in Sect. 3. Numerical results and discussions are seen in Sect. 4. Finally, Sect. 5 concludes.

2 System Model

2.1 Space-Time Graph

In this section, we use a space-time graph to describe the time-varying topology of satellite network. In the space-time graph [6–9], a time span of interest is discretized with a sequence of sufficiently small time intervals. In each time interval, a static graph *G (V, E)* can be used to describe the current topological relationship of network, in which *V* and *E* is the node and edge set respectively. We call this series of static images as snapshots of satellite network. Given a satellite network with n nodes $V = \{v_1, v_2, \ldots, v_n\}$, the time span of a transmission mission is divided into K equal time intervals. In order to represent the interconnection of K topological snapshots, the space-time graph (denoted as $\mathcal{G}$) is constructed with a hierarchical graph of $K + 1$ layers, each with a copy of all nodes. The node set of the l-th layer ($l \in [0, K]$) is $V^l = \{v_1^l, v_2^l, \ldots, v_n^l\}$. For a t-th snapshot of $G^t(V, E)$, if the node pair of $v_i, v_j (i, j \in [1, n])$ has a connection $v_i \leftrightarrow v_j$ ("$\leftrightarrow$" on behalf of a two-way link), we add two directional edges in the $\mathcal{G}$: $v_i^t \rightarrow v_j^{t+1}$ and $v_j^t \rightarrow v_i^{t+1}$, respectively. Neighbors of two adjacent nodes v_i^l and v_i^{l+1} can be connected by directed edges $v_i^l \rightarrow v_i^{l+1}$.

For a given task (φ, t_0, γ) of single source and multiple destination node, φ and t_0 represent the total amount of task data and required temporal duration of delivery respectively, while γ is the delay tolerance. We assumed that the sequential number of network node is defined by an integer from 1 to N. In particular, the first node with number "1" represents the source node, while those nodes from $N - NG + 1$ to N represents a group of NG ground stations. In addition, those remaining numbers represent a series of NS relay satellites. To construct a space-time graph of the target network, we will firstly determine an appropriately sampling interval τ to separate the time line into multiple time slots. Then, we will divide all the nodes in the network into different layers, in which N nodes of the i-th layer are sequentially numbered from integer $i \cdot N + 1$ to $i \cdot N + N$. With the start and end time t_{start} and t_{end}, it is possible to infer that $\mathcal{G}$ spans a group of discretized snapshots of $(t_{end} - t_{start})/\tau$ from the t_{start}/τ layer to the t_{end}/τ layer. Note that the node $\{i \cdot N + j | i = 0, \ldots, \gamma/\tau\}$ in the space-time graph exactly denotes the j-th node in the realistic network. Then, we add a serial of time and space links into the space-time graph, thus construct a complete graph.

2.2 Problem Formulation

Firstly, we will make analysis on the optimization problem without unexpected interruptions in the network. For a given task (φ, t_0, γ), we attempt to find a series of feasible paths $\mathrm{P} = \{p_1, \ldots, p_n\}$ in the space-time graph $\mathcal{G}$ for the complete delivery of task data. Through these paths, a global minimal cost of delivery (i.e. energy) $\mathcal{C}$ for the task is achieved. In particular, p_m is defined as the planning path in the network, f_{p_m} indicates the amount of data that passes through p_m, and w_{mn} is the energy cost required

for the unit data transmitted by the link, respectively. Then, the problem could be formulated as a minimum-cost constrained routing problem

$$\begin{gathered}\textbf{Min } C = \sum_{(v_m,v_n)\in p_m, p_m\in P} w_{mn}\cdot f_{p_m};\ \text{s.t.} \sum_{p_m\in P} f_{p_m} = \varphi; \\ 0 \le f_{mn} \le c_{mn},\ \text{for } \forall (v_m, v_n) \in E; \sum_{(v_m,v_n)\in E} f_{mn} = \sum_{(v_n,v_k)} f_{nk},\ \text{for } \forall v_n \in V\backslash\{s,d\},\end{gathered} \tag{1}$$

where s and d represent the source and destination nodes, respectively. In (1), first constraint makes sure that the amount of data from the source node s is equal to φ. The second constrain is the capacity constraint, which means the amount of data flowing through a certain edge is not greater than the capacity of that edge. The third constraint is a traffic-constrained condition, meaning that the amount of data flowing out a node, other than the source node and destination node, is equal to the amount of data flowing into it. In the space-time graph, the cost will be exploited for an objective function to find the shortest path, then update the network capacity in turn until finishing the residual amount of data.

Now, we will discuss about the above problem with interruptions in the network. We assume that an unexpected interrupt happens in the i-th node at time t, which is exactly on the end-to-end path for the task. For the source node, those to-be-sent data at the source node will lose a feasible path to the destination, if those data has been planned to go exactly through the interrupt node i at time t. Besides, a certain portion of ongoing data will make sojourn at those preceding nodes connected directly with the interrupted node, due to no feasible ways for forwarding. For the convenience of analysis, here we do consider those lost data due to hardware damages during the interruption. As a result, we assume that there is no data at the interrupt node i after time t since the previous hop nodes linked directly with i are rejected by node i. Therefore, for a given $\mathcal{G}$ we attempt to find a series of feasible paths $\mathrm{P} = \{p_1, \ldots, p_n\}$ after node i is interrupted, in order to efficiently finish the task data of size with the originally planned requirements. The optimization model with the interruption is divided into two parts. In particular, one is the optimization for the data φ_s that the source node has not transmitted at the time of the interruption, while another is a certain portion of ongoing data φ_i to make sojourn at those preceding nodes connected directly with the interrupted node. In addition, we define the data that has been ongoing in the network with the planned path not passing through the interrupt node after the interrupt occurs as φ_d. Here, φ_s, φ_i and φ_d satisfy the following relationship:

$$\varphi = \varphi_s + \varphi_i + \varphi_d \tag{2}$$

First, we analyze the data that has not yet been sent at the source node optimization problem.When the interrupt occurs, update the network space-time graph. $\mathcal{CS}$ indicates the energy cost of the data that the source node does not transmit after the space-time graph is updated. p_s indicates the path to which the data is not transferred at the source node from the time of the interruption. f_{p_s} indicates the amount of data that passes through the p_s.

$$\text{Minimize} \quad \mathcal{CS} = \sum_{(v_m,v_n)\in p_s, p_s\in P_s, m\neq i, n\neq i} w_{mn}\cdot f_{p_s}\ ; \textbf{s.t.} \quad \sum_{p_s\in P_s} f_{p_s} = \varphi_s$$
$$0 \le f_{mn} \le c_{mn},\ \text{for}\ \forall (v_m,v_n)\in E_s,\ \ m\neq i, n\neq i;\ \sum_{(v_m,v_n)\in E_s} f_{mn} = \sum_{(v_n,v_k)} f_{nk},\ \text{for}\ \forall v_n \in V_s \setminus \{s,d,i\}, \tag{3}$$

Next, we analyze the data that is ongoing to make sojourn at a group of preceding nodes connected with the interrupted node. p_i is defined as the replanning path the data of passing through the interrupt node after the time of the interruption. Where path p_i is the last hop of the interrupt node as the source node, and the bottleneck capacity of the path f_{p_i} is used as the flow. Because at this time the data has been transmitted in the network, only the last hop node of interrupt node as a new source node re-plan the path. $\mathcal{Ci}$ indicates the energy cost of the data that last hop nodes of the interrupt node transmit after the space-time graph is updated. l indicates the set of last-hop nodes for the original scheduled path through the interrupt node. f_{lmn} indicates the flow that has flowed out of a last hop node of the interrupt node.

$$\text{Minimize} \quad \mathcal{Ci} = \sum_{(v_m,v_n)\in p_i, p_i\in P_i, m\neq i, n\neq i} w_{mn}\cdot f_{p_i}\ ; \textbf{s.t.} \quad \sum_{p_i\in P_i} f_{p_i} = \varphi_i$$
$$0 \le f_{mn} \le c_{mn},\ \text{for}\ \forall (v_m,v_n)\in E_s,\ \ m\neq i, n\neq i\ ;\ \sum_{(v_m,v_n)\in E_s} f_{mn} = \sum_{(v_n,v_k)} f_{nk},\ \text{for}\ \forall v_n \in V_s \setminus \{s,d,i,l\}, \tag{4}$$

3 Routing Algorithm

3.1 Bundle Transport Mechanism

In a space network implemented with a DTN architecture, a bundle protocol layer will incorporated between application layer and transport layer, with a Custody Transfer mechanism. In particular, bundle, as BP Protocol Data Unit (PDU), is a basic message storage and forwarding unit. In the proposed stack, a flow of Application Data Unit (ADU) will be encapsulated into a serial of bundles as payloads, with corresponding bundle headers. By calling the proposed algorithmic procedure, a group of address, as a calculated end-to-end route by the algorithm, will be appended and encapsulated together with the payload. Then, these bundles will be delivered down to the lower layer for delivery, i.e., LTP protocol proposed by DTNRG. The LTP protocol takes the bundle as an LTP block and divides it into multiple sub-blocks, which are encapsulated into the segments. In the receiver nodes, after receiving the segments over the space channel, LTP protocol will check them with an interaction mechanism of checkpoints and acknowledgments for reliable delivery. In particular, if the segments data are lost, receiver sends the report to the sender (RS) for feedback.

As an edge's weight in the space-time graph, we define a capacity of one space (time) link as the maximum number of DTN bundles n that can be transmitted (stored) within the duration of each edge in $\mathcal{CC}$ quantized by discrete time intervals. Besides, one unit transmission (storage) cost of space (time) link is defined as the amount of

energy consumed to transmit (store) a DTN bundle within those discrete time intervals. In the following, we provide mathematical analysis on the spatial link capacity and unit transmission cost. The variables used are shown in Table 1.

Table 1. Declarations of variables

Variable symbol	Definition
PER (PERRS)	Segment (RS) packet loss rate
cj	The number of the j-th segment transmissions
M	The maximum number of transmissions for all segments
N	The total segments in bundle

Here, we only consider those energy costs for transmitter side sending packets and receiver feed-backing RS. In specific, the energy costs of sending a segment and a RS is respectively defined as e_s and e_{rs}, then the unit transmission cost of space link $i \rightarrow j$ is recorded as

$$w_{ij} = \mathrm{E}[\sum_{j=1}^{N} c_j \cdot e_s + \sum_{k=1}^{M} i \cdot e_{rs}] = \frac{N \cdot e_s}{1 - PER} + \frac{M \cdot e_{rs}}{1 - PER_{RS}}. \tag{5}$$

3.2 Interruption Resilient Routing

In a space network, nodes confronts frequently with abrupt events, such as platform failure, link outage and resource exhausted, leading to expected disruptions in the delivery mission. For example, in Fig. 1, *i*-th node is exactly interrupted at time t with a duration of *len* time slots, as

$$k = (t - t_{start})/\tau \tag{6}$$

Here, we assume that a discrete time interval τ can totally capture the connection and interruption of the link. And γ can be divisible by τ. If the space link contact time can not be captured by τ in the network, the time of the space link is rounded off. The τ mentioned in the following section satisfies the above requirements. In the graph, firstly, we delete the time link.

$$\{j \cdot N + i \rightarrow (j + i) \cdot N + i | j = k, \ldots, k + len\} \tag{7}$$

and define $\{j \cdot N + i | j = k, \ldots, k + len\}$ as the start point and $\{j \cdot N + i | j = k, \ldots, k + len\}$ as the end point of the space link, respectively. The new space-time graph is shown in Fig. 2. The new source node in the figure indicates that the previous hop node before the interrupt node will reallocate the data.

To solve the above problem, we propose a multicast routing algorithm to deal with the interruption in the constructed space-time graph. In particular, the main idea is to

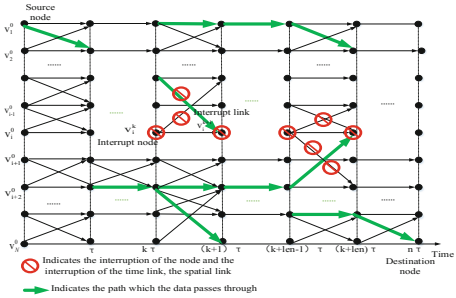


Fig. 1. Space-time graph with interruptions

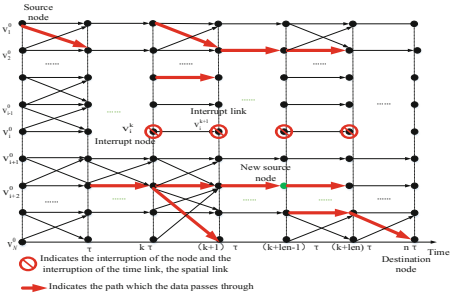


Fig. 2. New space-time graph after interruptions

Table 2. Interruptions resilient routing algorithm

The pseudo-code algorithm

1: **INPUT:** $\mathcal{G}(V,E,C,W)$, $\mathcal{C}, \mathcal{T}$, P
2: **OUTPUT:** $\mathcal{C}$_NEW, $\mathcal{T}$_NEW, P_NEW
3: **For each** $j = N - NG + 1,\mathrm{L}\ ,N$ **and** $i = 1,\mathrm{L}\ ,\left\lfloor \frac{t_0}{\tau} \right\rfloor$
4: find（P== $i \cdot N + j$ ）=（i,j）//find the path associated with the interrupt node
5: P_DIS ⟵ P(i,:) ; // Extract the path
6: $\mathcal{G}$_NEW ⟵ **SETUP_GRAPH** ($\mathcal{G}$, p, c_p , N_i) //Update
7: $\varphi = \varphi - \sum c_p$,$\mathcal{C}$_NEW= $\mathcal{C}$- $\mathcal{C}$_DIS;// update the capacity
8: $p \leftarrow$ **FIND_PATH** ($\mathcal{G}$_NEW); //The source node at the time of the interruption and the interrupt hop node as the source
9: **while** $f < \varphi$ **and** $p \neq \varnothing$ **do** // flow is less than data
10: P_NEW ← P-P_DIS ∪ p;
11: $f \leftarrow f + c_p$;
12: **if** $f > \varphi$ **do** //
13: $c_p \leftarrow c_p - (f - \varphi)$ //The last path transmission data is less thanc_p
14: $f \leftarrow \varphi$;
15: **end if**
16: $\mathcal{C}$_NEW ⟵ $\mathcal{C}$_NEW+ $w_p \cdot c_p$;
17: $\mathcal{G}$_NEW ⟵ **UPDATE_GRAPH** ($\mathcal{G}$_NEW, p, c_p)
18: $p \leftarrow$ **FIND_PATH** ($\mathcal{G}$_NEW) // Find w_p the smallest path
19: **end while**
20: **if** $f < \varphi$ **do**
21: **Return** –*f*; // The return transmission task can't complete the flag
22: **else do**
23: $\mathcal{T}$_NEW ⟵ **CALCULATE_DELAY_DIS** (P_NEW) ;
24: P_NEW ⟵ **TRANSLATE_PATHS_DIS** (P_NEW);
25: **Return** $\mathcal{C}$_NEW, $\mathcal{T}$_NEW, P_NEW;
26:**end**

update the space-time graph from the time t interruption happens, and reallocate the residual data in the network after the interruption occurs with a group of re-planned routes. In the algorithm, we define the capacity and cost as two weights of one edge and update these weights after the interrupt occurs. For source node s, those residual data waiting to transmit will be re-planned with a new group of end-to-end routes between the source and the final destination node from time of the interruption. For an intermediate node exactly at the original route, if it is at one preceding hop from the interrupted node with a connection, it will re-plan a new group of route from it to the destination for its sojourned data by the proposed algorithm in the following section. By the update of graph, all the data in the network is redistributed to find the optimal route after interruption, with a Bellman-Ford algorithm of finding the minimum cost path. Once the interruption happens, each node with sojourned data before the disrupt node would be considered as a new source node. As a result, the path re-planning problem for residual data of given task is transformed into a shortest path of multi-source and multi-destination routing problem with respect to energy cost. Table 2 provides a pseudo-code routing algorithm.

4 Numerical Results

In this section, we will compare the performances on several given data volumes with different interrupt lengths with respects to the energy costs and time delays in MATLAB. The simulation parameters are listed in Table 3. In the simulation, we assume that the interrupt time can be exactly captured by a serial of integral time intervals. In particular, the evaluation metrics are mainly the delay $\mathcal{T}$ and the transmission overhead $\mathcal{C}$. Typically, we study an experimental scenario of Earth observation satellite network as follows: an Earth remote sensing satellite of China remote sensing satellite with high resolution (GF-II), which operates at a height of 631 km in the sun synchronous orbit with an inclination of 97.908°; six relay satellites distributed in a constellations of Walker (6/6/4), where the seed satellites runs on a circular orbit with a height of 1414 km (using the global orbit height) and inclination of 52°; three ground stations are located in China's Miyun (40.3°N, 116.8°E), Kashi (39.5°N, 76°E) and Sanya (18.2°N, 109.5°E) respectively; the observation target in the experiment is

Table 3. Simulation parameters

Parameter	Value	Parameter	Value
Bundle size	100 kbytes	*Different types of links BER*	GF-*RS*: 10^{-6}; GF-*GS*: 10^{-7}; *RS-RS*: 10^{-6}; *RS-GS*: 10^{-7}
Segment size	1250 bytes	*Time and space link unit energy cost*	10^{-3} kJ; 10^{-4} kJ; 10^{-5} kJ
Data transmission rate	GF-II: 20 Mbps; *RS*: 50 Mbps; *GS*: ∞	e_s	2.5×10^{-5} kJ
RS feedback rate	*RS*: 10 Mbps; *GS*: 5 Mbps	T_{prop}	GF-*RS*: 30 ms; GF-*GS*: 10 ms; *RS-RS*: 30 ms; *RS-GS*: 10 ms
Storage	GF-II: ∞; *RS*: 10^5; *GS*: ∞		

located in Sahara (28°N, 11.5°E) corresponding to the transmission task $(\varphi, 12:00(\mathrm{UTC}), 2\mathrm{h})$. The start time of the task is selected based on the contact time between GF-II and the observed target. Given a mission of delivering remote sensing image data encapsulated in bundles, φ is determined as 10000, 12500, 15000 and 16000, respectively.

In particular, the time instant t_{start} and t_{end} of all links are rounded to the nearest integer minute, in which t_0 is the starting point of time as "0". The time span is $[0, \gamma]$ with discrete time interval τ of 1 min. As can be seen in Fig. 3, with the duration length of interruption increasing, the energy cost becomes larger, since it is possible to find a smaller energy cost path than the previous path after recovery of interruption. Give the interrupted node on the path of the minimum energy cost, when the interrupt stops, data flow can still be re-allocated. On the other side, given a small amount of missioned data, with time length of interruption changing, energy costs do not change obviously.

As can be seen from Fig. 4, when the amount of data is large, the interrupt length becomes larger, the time delay will be larger. Because the available path in the space network is reduced when the interrupt time of the interrupt node becomes longer. So that the transmission delay may be increased at the same amount of transmission data.

Table 4 shows the original and resulted routing paths in the network when the interrupt time is 20 min. According to the connections between nodes within the observation time range, 20 min can be regarded almost as a permanent interrupt. It can be seen that some of the data of the interrupt node is transmitted by other relay nodes, resulting in a longer time delay and a larger network energy cost Table 5 shows two comparative paths with an interruption time of 1 min (actually within one time interval). We can see that, once the interrupt stops, the energy cost and time delay becomes smaller due to a different path produced by the proposed routing strategy. Table 5 shows two comparative paths with an interruption time of 1 min (actually within one time interval). We can see that, once the interruption stops, the energy cost and time delay becomes smaller due to a different path produced by the proposed routing strategy.

Table 5 shows two comparative paths with an interruption time of 1 min (actually within one time interval). We can see that, once the interrupt stops, the energy cost and time delay becomes smaller due to a different path produced by the proposed routing strategy.

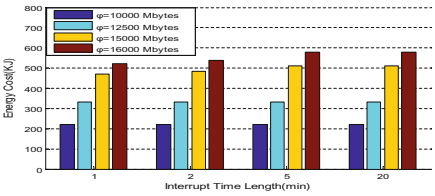


Fig. 3. Comparison of energy under different interrupts

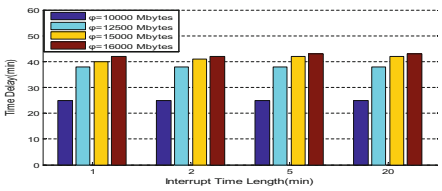


Fig. 4. Comparison of time delay under different interrupts

Table 4. Routing paths

	Start node	End node	Start time	End time	Data
Original routing path table	1	5	16min	24min	6887
	5	8	17min	25min	6887
	1	9	17min	23min	8113
Interruption –resilient routing path table	1	5	16min	18min	1656
	5	8	17min	19min	1656
	1	6	30min	40min	5231
	6	8	31min	41min	5231
	1	9	17min	23min	8113

	Start node	End node	Start time	End time	Data
Original routing path table	1	5	16min	24min	6887
	5	8	17min	25min	6887
	1	9	17min	23min	8113
Interruption–resilient routing path table	1	5	16min	18min	1656
	5	8	17min	19min	1656
	1	6	30min	38min	4403
	6	8	31min	39min	4403
	1	9	17min	23min	8113
	1	5	21min	24min	2484
	5	8	22min	25min	2484

5 Conclusion

In this paper, we design a routing algorithm for dealing with unpredictable interruption in space DTN network. The algorithm uses the space-time graph as the network model, and find the minimum energy cost paths for the given data volume after the interruption occurs. The simulation results verified the proposed algorithm.

Acknowledgment. The authors would like to express their high appreciations to the supports from the National Natural Science Foundation of China (91538110), Natural Science Foundation of Guangdong Province (2016A030313661), and Basic Research Project of Shenzhen (JCYJ20150625142543458 and JCYJ20150403161923521).

References

1. Lin, B., Li, H., Long, Y.: A buffer-limited maximum throughput routing algorithm for satellite network. In: 22nd International Conference on Telecommunications (ICT 2015) (2015)
2. Liu, R., Sheng, M., Xu, C., Li, J., Wang, X., Zhou, D.: Antenna slewing time aware mission scheduling in space networks. IEEE Commun. Lett. **21**(3), 516–519 (2017)
3. Yang, L., Sun, J.: Multi-service routing algorithm based on GEO/LEO satellite networks. In: International Conference on Network and Information Systems for Computers (2016)
4. Jiang, M., Liu, Y., Xu, W., Yang, Y., Kuang, L., Tang, F.: An optimized layered routing algorithm for GEO/LEO hybrid satellite networks. In: IEEE TrustCom-BigDataSE-ISPA. https://doi.org/10.1109/trustcom.2016.186
5. Juyal, V., Pandey, N.: A heuristic light weight security algorithm for resource constrained DTN routing. In: IEEE International Conference on Computational Intelligence and Computing Research (2016)
6. Liang, Q., Modiano, E.: Survivability in Time-varying Networks. Laboratory for Information and Decision Systems Massachusetts Institute of Technology, Cambridge (2016)
7. Huang, M., Chen, S., Zhu, Y., et al.: Topology control for time-evolving and predictable delay-tolerant networks. IEEE Trans. Comput. **62**(11), 2308–2321 (2013)

8. Li, F., Chen, S., Huang, M., et al.: Reliable topology design in time-evolving delay-tolerant networks with unreliable links. IEEE Trans. Mob. Comput. **14**(6), 1301–1314 (2015)
9. Merugu, S., Ammar, M.H., Zegura, E.W.: Routing in space and time in networks with predictable mobility. Georgia Institute of Technology, CC Technical report, GIT-CC-04-07 (2004)

An Improved Cluster Routing Algorithm Based on ZRP Protocol

Xuefeng Lv(✉), Xinxi Le, and Kui Ding

Laboratory of Low-frequency Electro-magnetic Communication Technology, WMCRI, CSIC, Wuhan, China
eslxf@163.com

Abstract. Hybrid routing protocol combines proactive with reactive techniques, with the advantages of high reliability and low routing overhead. The Zone Routing Protocol (ZRP) is a typical hybrid routing protocol. This paper presents an improved ZRP routing protocol based on cluster domain mechanism. This protocol replaces partition in ZRP routing protocol with clusters in hierarchical network, and proposes a new domain routing method to avoid redundant or duplicate route requests. Theory analysis and simulations show that the ETE delay, routing overhead and packet delivery ratio performance of the protocol proposed here are superior compared to the traditional ZRP protocol.

Keywords: Ad-hoc · Zone routing protocol · Clustering
Hierarchical network structure

1 Introduction

Mobile Ad-hoc network, a special wireless mobile communication network system, consists of a set of wireless mobile nodes. In such a network, each node is free to move randomly and acts as router and server. Because of these, such a wireless network topology may change rapidly and unpredictably, which is the greatest feature of Ad-hoc network. Ad-hoc networks has broad application prospects, which with flexible networking modes and robustness. Existing routing protocols based on the wired network are not suitable for dynamically changing network environment of the Ad-hoc networks. So routing technology becomes one of the key technologies of the Ad-hoc network. At present, the routing protocol used by Ad-hoc network mainly includes proactive routing protocol, reactive routing protocol, and hybrid routing protocol combining the above two routing ideas. In the proactive routing protocol, the node maintains the latest and consistent routing information of all nodes in the network through the periodic broadcast routing information grouping. The advantage of this is that when a node needs to send data packets, the node maintains the routing information table in real time through interactive information, so the data delay is very small [1]. Though it performs well in data delay, it needs a large number of storage spaces. However, the reactive routing protocol is just the opposite. In the reactive routing protocol, when the source node needs to communicate with the destination node, the node of this protocol does not need to maintain the routing table at all times, thus makes

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 261–271, 2018.
https://doi.org/10.1007/978-3-319-90802-1_23

it save storage space. The reactive routing protocol needs periodic broadcast information to update the routing. The advantage is that the routing overhead is small, but it may cause a little more time to transmit data. To solve the problems of these two kinds of protocols, hybrid ones tend to exploit the advantages of both proactive and reactive approaches. We focus on a typical hybrid routing protocol called ZRP (Zone Routing Protocol) [2].

Zone routing protocol is a hybrid routing protocol. It uses two different protocols in the web: the nodes in the region use the proactive routing protocol to maintain routing information; the external nodes out of the region adopts reactive protocol. And the size of the region can be adjusted to adapt to the changes of the network dynamically. So the overall performance of the network can be the best [3].

2 The Zone Routing Protocol

2.1 Architecture

Generally speaking, the ZRP protocol is mainly composed of three parts: IARP, IERP and BRP, and its architecture is shown in Fig. 1. Figure 1 shows how these three sub protocols interact to provide an efficient routing protocol that acts proactively in zone and reactively out of zone.

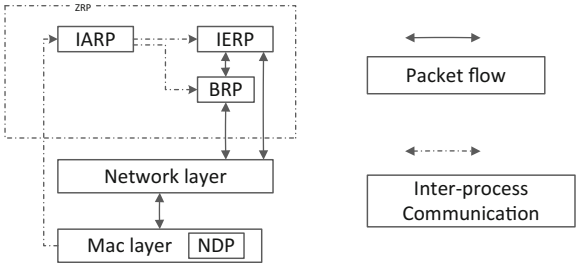


Fig. 1. ZRP components

All nodes in the ZRP network are based on their own center, and the number of nodes in the zone is related to the set radius. The IARP protocol maintains a routing table for other members within the region using a proactive routing algorithm in the region [4].

Interval routing protocol IERP is used to set up temporary routing. Packet delivery radio is implemented through the BRP protocol. ZRP declares an NDP protocol in order to detect whether new neighbor nodes and connections fail [5].

2.2 IARP

The intra-area routing protocol (IARP) is a pre-routing protocol within a limited area. It maintains routing information and routing tables between nodes through periodic broadcasts. It proactively monitors the connectivity of the regional network and provides

support for route discovery and routing maintenance for nodes as needed. If a node needs to communicate with the nodes in the area, it can provide the route directly, thus reducing the cost of route discovery [6].

2.3 IERP

IERP is an inter-regional routing protocol. The protocol routes the communication of nodes in different regions and is responsible for reactively creating routes for nodes out of the zone. When the node is communicating, the target node and the source node are detected weather in the same area. If the destination node is outside of the region, we will enable the IERP protocol and send the routing request to the boundary nodes. After receiving the routing request, the boundary node looks up the routing table. If the destination node is found, it sends a routing reply to the source node. If not, it continues to forward the routing request to its boundary node, so that it can be searched until the destination node is found.

2.4 BRP

The Border-cast Resolution Protocol (BRP) is proposed to improve the efficiency of routing queries in IERP, thereby reducing the waste of radio resources due to redundant or repeated broadcasts. The BRP is responsible for forwarding the IERP routing request to the peripheral nodes of the border broadcast nodes. Although only the neighbor nodes receive the boundary broadcast packets, the BRP sends a query to the IERP at each hop. BRP records the node path that the request has been overwritten. When a node receives a query packet, it reconstructs the boundary broadcast tree to mark the peripheral node of the previous boundary broadcast node. Then the node becomes a new border broadcast node. The connection status is saved so that the query can be forwarded correctly from the higher layer before the query is sent to a higher level.

2.5 Discussed Problems

Though ZRP performs well in large scenarios, it still has some problems. The traditional ZRP protocol has planar structure, and the planar structure is not scalable. As each node in the scenario maintains a route table, there are lots of overlapping areas in the whole scenario. Those overlapping areas produce redundant or duplicate route requests. The best way to solve this problem is to use the appropriate clustering algorithm to construct a hierarchical topology. A group of nodes that are adjacent to each other form a cluster. The members of the cluster can be divided into cluster heads, cluster members and gateways. The communication between the cluster members is done through the cluster head, and the communication between the clusters is forwarded through the gateway. This reduces redundant routing requests.

3 A Strategy for Generating Clusters

The election of cluster heads is critical to the performance of the network, and a node's ability is affected by a lot of factors. Based on the above considerations, a self-adaptive on-demand weighted clustering algorithm is adopted. We give a certain weight to the various factors that affect the performance of the algorithm, and obtain the comprehensive weight [7] (Fig. 2).

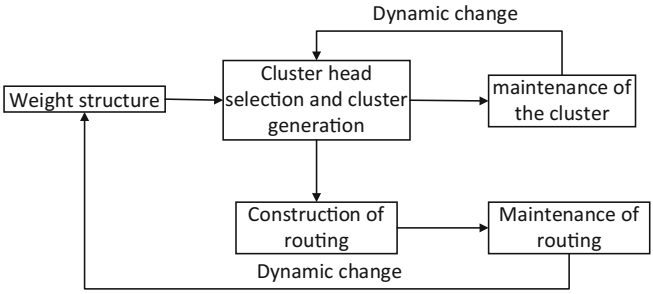


Fig. 2. Clustering algorithm

Because the cluster head node has to carry out its own information transmission, and also responsible for cluster message, group information maintenance and so on, so energy consumption is generally higher than the ordinary nodes. We put the node's residual energy as a factor. In addition, the node connectivity, that is, the number of neighbors is also an influencing factor. Based on the above factors, we define a value named N to measure the ability of the node to manage the network. When N is bigger, it is more capable of becoming a cluster head node. We have that

$$N = d \times T_{\mathrm{i}} \tag{1}$$

Where d is the degree of the node i, T_{i} is the time of the node i to be the head. The average energy consumption rate of the group is

$$E_{\mathrm{avg}} = \frac{E_{\mathrm{s}}}{T_{\mathrm{s}} - T_{\mathrm{e}}} \tag{2}$$

Where E_{s}, T_{e} refer to the node is selected as the first group of energy and time respectively. T_{s} indicates the current time. Assuming the node's node set be N_{i}, e_{ij} is the amount of energy that the unit data is sent to its neighbors. K_{ij} is the data flow from node i to j. Then the total energy consumption of node i is

$$E_{\mathrm{i}} = \sum_{\mathrm{j} \in N_{\mathrm{i}}} e_{\mathrm{ij}} k_{\mathrm{ij}} \tag{3}$$

The time T_{i} that node i can serve as the head is

$$T_{\mathrm{i}} = \frac{E_{\mathrm{ic}} - E_{\mathrm{i}}}{E_{\mathrm{avg}}} \tag{4}$$

The cluster formation algorithm can be described as follows:

Step 1: Each node checks its own value N within a specified radius of the area. Then the node whose N is the maximum is selected to be a managing node. If there are more than one node owning the maximum value, we choose the node whose ID number is smaller.
Step 2: We consider the selected cluster head as the center. The nodes within the specified radius of the center form a zone.
Step 3: The cluster head node broadcasts information to the neighbor nodes and announces the establishment of a new cluster. The neighbor node sends a join message to the cluster head node, which includes itself and the group number to be added. If the node receives more than two messages, the node is a gateway node. The gateway node needs to send its own degrees, energy and other group numbers that can be reached to the cluster head node.
Step 4: Repeat the above process until all nodes join a cluster (Fig. 3).

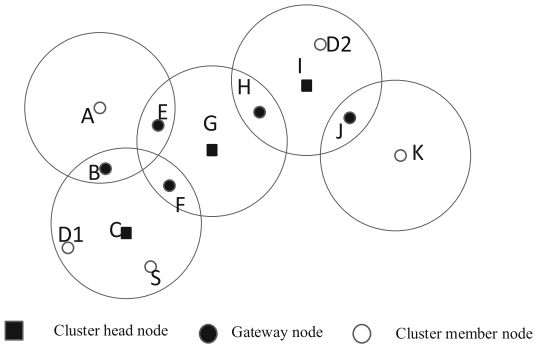


Fig. 3. Example of clustering algorithm

4 Improved Cluster Zone Routing Protocol

4.1 Improved Routing Mechanism

By clustering the network structure, the ZRP protocol has obvious advantages compared with the direct division of the network structure directly on the plane network structure. The characteristics of the improved cluster-based ZRP are: (1) by using cluster algorithm to form a domain, it is avoided that each node forms the domain by itself, thus reducing the number of domains and avoiding the entry of one node into multiple domains. (2) In the improved IARP protocol, only the central node maintains the route table in the cluster, and other nodes do not maintain the route table. So that the overhead of the node is reduced, the efficiency is improved, and the location information is used to trigger the

update messages. (3) In the improved IERP protocol, inter-domain routing uses a hierarchical structure to reduce the number of routing request packets and improve the efficiency of the boundary nodes. This method has a good network scalability, and the joined nodes are only related to the cluster structure they join, so they will not affect the topology of the whole network. All in all, the improved IERP protocol is suitable for large-scale network [8].

When the data packet arrives at the node, the route discovery process can be described as follows:

Step 1: The source node firstly sends the request data to the cluster head node, then the cluster head node finds whether the destination node is in the region. If there is a route to the destination node in the same area, the source node then finds the route and send the data packet to the target node. If there is no route to the destination node, then skip to Step 2.
Step 2: Perform reactive inter-domain route discovery. The cluster head node of the cluster where the node resides sends the routing request information RREQ to the neighbor cluster head node through the gateway node. The cluster head node that receives the RREQ information determines whether the destination node is in the area maintained by finding its own route table. If there is routing information of the destination node, the destination node sends the RREP message to the source node; if it does not exist, the head node continue to send routing request information RREQ to its neighbor cluster head node. Repeat these steps until you find the path to the target node (Fig. 4).

4.2 Example

The network contains 15 nodes, which are divided into five clusters. Nodes A, C, G, I, K are the cluster head nodes of the cluster, nodes B, E, F, H, J are the gateway nodes of the cluster. The source node is S, the destination node is D1, D2.

(1) When the source node S is to communicate with the destination node D1, the node S firstly sends request data to the cluster head node C to find out whether there is routing information of node D1 in the route table. Since the node S and the node D1 are in the same cluster, the node S can communicate directly with the destination node D1 through the information in the route table.
(2) When the node S needs to communicate with destination node D2, there is no routing information for node D2 in cluster head node C. At this time, the cluster head node C sends the routing request information RREQ to the cluster A and the cluster G through the gateway nodes B. It is found that there is no information of D2 in the route table maintained by A and G, then the routing request information is forwarded through gateway node H. When node I receives the route request information RREQ sent by node C, node I checks to find the routing information of node D2 in the route table by checking it. At this time, node G sends a route reply information RREP to node C, then the cluster head node C forwards the information to the node S. So that the node S can receive the RREP information and communicate with the node D2.

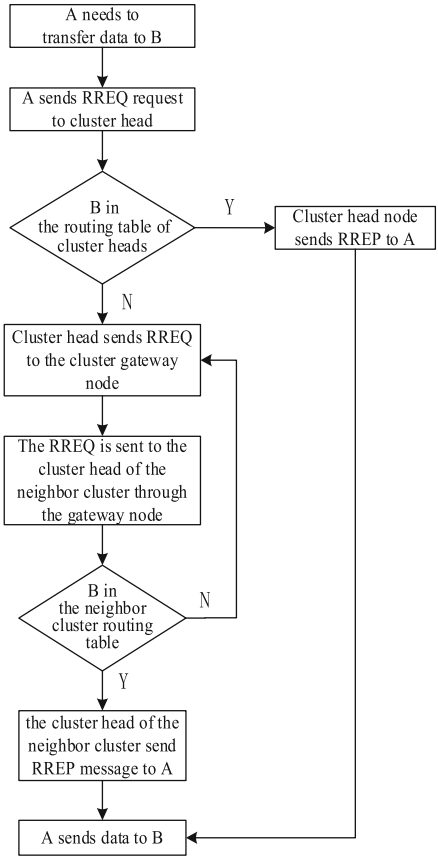


Fig. 4. Improved ZRP routing algorithm process

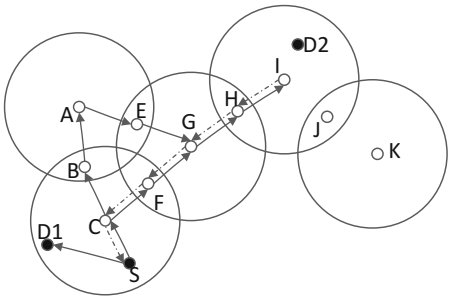


Fig. 5. Routing request process diagram

When the cluster head node broadcasts the routing request information to its neighbor nodes, the neighbor node may receive duplicate broadcast information and discard it for duplicate information. As shown in the Fig. 5, when the cluster head node C wants to find

the routing information of the node D3, the gateway node broadcasts the routing request message RREQ to the neighbor cluster head nodes A and G. The node A does not have the routing information of node D2, then it will continue to forward routing request information RREQ to its neighbor cluster head node G. When node G receives the RREQ message, it finds that it is a duplicate routing request message and discards it.

The head node of the cluster where the source node resides may receive multiple routing reply information RREP after issuing the routing request information RREQ. When the repeated routing reply message is received, only the first received RREP message is selected as the routing information for the destination node, while other information is simply discarded. When the destination node is not present in the network or the existing network structure can't overwrite the destination node, the source node will receive a request error message RRER and notify the destination node that it is unreachable.

5 Analysis of Protocol Performance

In order to analyze the changes made and compare the performance between improved cluster-based ZRP and traditional ZRP, we evaluated both routing protocols in a simulation environment. Our simulations were conducted by OMNET Simulator. In the simulations, mobile nodes move around a square region of size 2000 m × 2000 m according to random waypoint mobility model. The node's speed is between 0 m/s to 10 m/s. The data packets are sent after 30 s the simulation starts. The packet size is 512 Bytes. The simulation time is 300 s. We analyze the performance between the two protocols from three aspects: end-to-end delay, packet delivery ratio and routing overhead.

Figure 6 shows the comparison of the end to end delay of the two route protocols. End-to-end delay refers to the time taken for a packet to be transmitted across a network from source to destination.

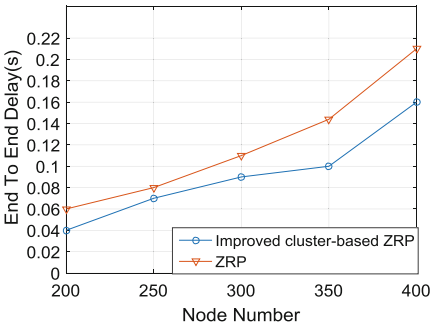


Fig. 6. End to end delay

As shown in Fig. 6, the improved cluster-based ZRP performs better than ZRP in end to end delay. It can be seen that the average end-to-end delay of the two protocols increases with the number of nodes increases. However, at the same number of nodes,

the end-to-end delay of the improved ZRP protocol is always smaller than the delay of the ZRP routing protocol, and more obvious when the number of nodes is more. The improved protocol adopts a clustering-based partitioning method. It performs better for less overlapping zones and less request packets than ZRP. So it shows a smaller end-to-end delay than the ZRP protocol.

Figure 7 reflects the change of the packet delivery ratio of the two routing protocols with the increase of the number of nodes in the simulation scenario. Packet delivery ratio is the fraction of packets sent by the application that are received by the receivers and is calculated by dividing the number of packets received by the number of packets originated from the source.

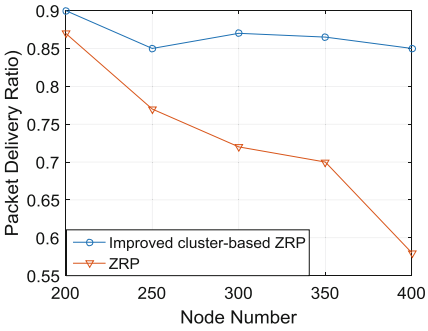


Fig. 7. Packet delivery ratio

As shown in the Fig. 7, with the increase of the number of nodes, packet delivery rate gradually reduces. Because the network topology changes more frequently, there are more route request packets in the network, which makes the network load heavier and influences the transmission of the data packets. So partial packet data may fail to send. But packet delivery ratio of the improved routing protocol is still higher than the original protocol.

Figure 8 compares the routing overhead of networks by using the two route protocols. Routing overhead is an important indicator of the efficiency of routing protocols. It is the total number of routing groups to be sent. In ZRP protocol, the nodes in the area adopt proactive route, regardless of whether you need to reach the routing of other nodes, these routes will be maintained in advance and regularly updated. As shown in the Fig. 8, as the size of the network continues to expand, the routing overhead increased significantly. Improved routing protocols can be used to cluster nodes in the network, so the number of messages that need to be sent for proactive routing maintenance in the region is reduced. Therefore, it can reduce the routing overhead and shows a lower routing load than the ZRP protocol.

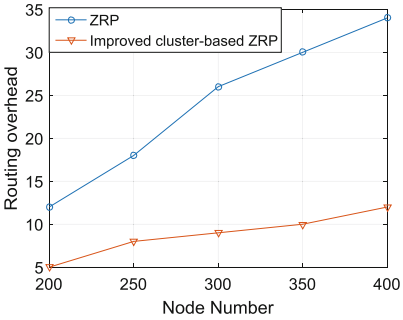


Fig. 8. Routing overhead

6 Conclusions

ZRP is a typical hybrid routing protocol which combines two completely different routing methods into one protocol. This paper proposes an improved cluster-based ZRP routing protocol, which solves the problem of poor extensibility and high overlap of routing area in traditional ZRP routing protocol. The improved cluster-based ZRP presents a new generation algorithm for cluster in hierarchical network, and proposes a new domain routing method to avoid redundant or duplicate route requests. Using this method, the improved cluster-based performs better in ETE delay, routing overhead and packet delivery ratio than ZRP.

Acknowledgements. This paper is supported by National Natural Science Foundation of China (Grant no. 61701130) and the Fundamental Research Funds for the Central Universities of China (Grant no. HEUCFD1509). Meantime, all the authors declare that there is no conflict of interests regarding the publication of this article.

References

1. Hass, Z.J., Pearlman, M.R., Samar, P.: The zone routing protocol (ZRP) for Ad Hoc Networks, IETF Internet Draft, draft-ietf-manetzone-zrp-04.txt, July 2002
2. Tsirigos, A., Haas, Z.J.: Multipath routing in the presence of frequent topological changes. Commun. Mag. **39**(11), 132–138 (2001)
3. Sethi, S., Rout, A., Mishra, D.: A robust cluster based routing protocol for MANET. In: Proceedings of ACM the 2011 International Conference on Communication, Computing & Security, pp. 26–31 (2011)
4. Yélémou, T., Meseure, P., Poussard, A.M.: Improving ZRP performance by taking into account quality of links. In: Wireless Communications and NETWORKING Conference, pp. 2956–2960. IEEE (2012)
5. Pathak, S.K., Upadhyay, R., Bhatt, U.R.: An efficient query packets forward algorithm in ZRP protocol. In: International Conference on Issues and Challenges in Intelligent Computing Techniques, pp. 592–595. IEEE (2014)

6. Sumit, S., Mitra, D., Gupta, D.: Proposed intrusion detection on ZRP based MANET by effective k-means clustering method of data mining. In: International Conference on Optimization, Reliability, and Information Technology, pp. 156–160. IEEE (2014)
7. Zhang, X., Xu, C., Xu, J.: Hierarchical ZRP's performance vs ZRP's performance in MANET. In: IEEE International Conference on Communication Software and Networks, pp. 423–426. IEEE (2015)
8. Arora, N.: Performance analysis of DSDV, AODV and ZRP under Blackhole attack. Int. J. Eng. Res. Technol. **3**(4), 2000–2004 (2014)

Key Management Scheme for Wireless Sensor Networks

Yongjian Wang and Jing Zhao(✉)

National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, People's Republic of China
zhaojing_is_me@hotmail.com

Abstract. The paper designs a key management scheme for wireless sensor network that can resist key attack against the network. The scheme gives full play to the cluster head's resources such that the head can carry most of the computation, storage and communication overhead by the cluster head, and thereby achieves the minimum energy consumption of the cluster members and anti capture target, and key attack can resist wireless sensor network effectively. Through the simulation of the key management program in the authorization certificate issuance mechanism, and the development of the corresponding changes in the value of the parameters to assess the performance of each mechanism, it comes to the overall performance of the mechanism ultimately and how the value should be set to get the best performance. Simulation results show that compared with the traditional scheme, the proposed model can effectively improve the node's anti capture ability and reduce the node energy consumption.

Keywords: Wireless sensor networks · Key management
Authorization certificate issuing

1 Introduction

The wireless sensor network is a new type of wireless network technology that is completely different from the traditional wireless network. It relies on the wireless link to transmit data, which relieves the dependence on the wired network. It is more efficient, with high coverage, scalability and Reliability and other advantages to overcome the Ad Hoc network, wireless LAN, wireless personal area network, wireless MAN some restrictions, so wireless sensor networks are increasingly concerned by academics and the industry, especially wireless sensor network security issues [1–3]. The wireless sensor key management scheme is the security foundation of the wireless sensor network. In essence, the classical cryptographic scheme is used to solve the security of the wireless sensor network and prevent the network from being attacked.

In the paper, the wireless sensor network is distributed in a cluster, a cluster has a cluster head and a plurality of cluster members, the topology can be seen in Fig. 1. The cluster head is no special line communication equipment, computing, storage, communication and energy in other areas have higher ability; cluster members are ordinary sensor capacity low, to reduce the energy consumption, the provisions in the cluster members can only communicate with the cluster head.

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 272–283, 2018.
https://doi.org/10.1007/978-3-319-90802-1_24

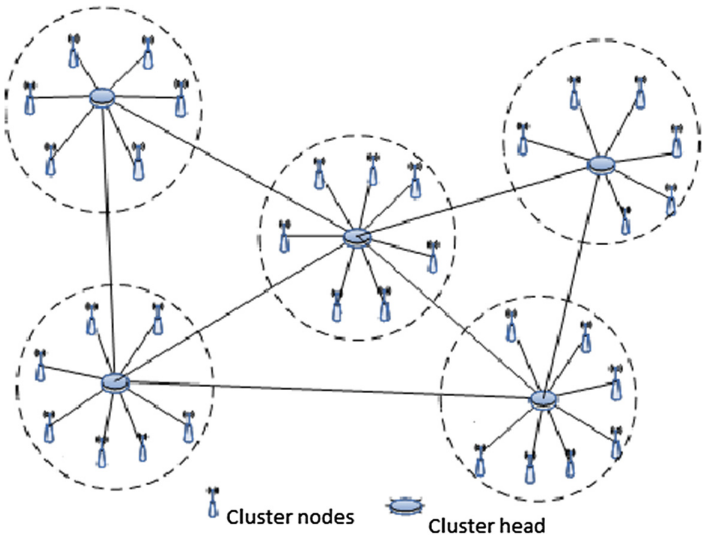


Fig. 1. Topology of wireless sensor network

There is a great difference in the wireless sensor network in this cluster and the cluster members of the allocation of resources, because the cluster head can carry high computation and communication overhead, so the key management can be used between a plurality of cluster head nodes distributed management, which can improve the anti capture and reduce storage. The cluster head is not balanced with the members of the cluster, and the traditional scheme of the flat network is directly applied to the inner layer with low efficiency and poor security. For example, Boujelben et al. Proposed probabilistic scheme is difficult to achieve full connectivity of the network, and the cluster head and cluster members have a large amount of key storage [4].

2 Key Management Architecture

Key management architecture mainly includes the initial key and certificate distribution module, identity based private key and certificate distribution module, key and storage module, key and certificate update module and authentication service module.

In the initial key and certificate assignment module, the following functions are mainly included: the offline CA assigns the public and private key pairs and the public key certificate for itself and each registered system member (user, regional router, backbone router); the offline CA assigns public and private key pairs for the system, and shares the system private key in the backbone router. The main function of identity based private key and certificate allocation module is the virtual CA which is formed by the backbone router. The main function of key and certificate storage module is to store public key certificate, authorization certificate and identity based private key. The main function of the key and certificate update module is to update the public key pair, the identity based private key, the public key certificate and the authorization certificate

when the system is abnormal and the system members join or leave. The main function of the authentication service module is to authenticate the user and authenticate the identity of each other before the members in the same area, adjacent or non-adjacent areas communicate with each other [5–8].

2.1 Preparation Knowledge

The N protocol is a set of N interactive probability algorithms. Each algorithm is a probabilistic polynomial complexity of interactive Turing machine, with participants Ji expressed the i algorithm. Each participant Ji input $\alpha i \in \{0,1\}^*$. Random input $ri \in \{0,1\}^*$ and safety parameter k input length. Non adaptive actual attacker A is another interactive Turing machine, described by participants in the behavior of the adversary intrusion. The attacker's A input includes the identity of the affected party and their respective inputs. The additional auxiliary input received by attacker A is represented by z. The random input for A is $r0$. If an attacker controls at least λ participants, the attacker is bounded by λ. In each round of the calculation process, the honest party first generates the round of messages according to the protocol. The attacker mastered all the messages sent to the invaded participant. Then the adversary generates a message that is sent by the invading party. If the attacker is passive, then these messages are determined by the protocol. The active attacker generates the message sent by the participating party in any malicious way. The result is that all participants generate their own local output. The Honest Party's output is completely in accordance with the agreement, and the participants are exposed to a special symbol that they have been invaded. The attacker outputs an arbitrary function of its view. The attacker's view is composed of the following parts: auxiliary input, random input, input and random input of the participating party, and the message sent and received by the participating party during the whole calculation. Without losing generality, the attacker's output is assumed to consist of all of its views [9–12].

$ADVR\pi, A(k, \vec{\alpha}, z, \vec{r})$ represents the output of an attacker in the actual model, where z is an auxiliary input π is running protocol, $\vec{\alpha} = (\alpha 1, \alpha 2 \ldots . \alpha n)$, $\vec{r} = (r0, r1 \ldots . rn)$, αi and ri are the input and random input of the Ji, $r0$ is the random input of the attacker. $EXEC\pi, A(k, \vec{\alpha}, z, \vec{r})i$ is the output of the participant Ji. If Ji is honest, then its output follows the protocol execution; If Ji is invaded, then $EXEC\pi, A(k, \vec{\alpha}, z, \vec{r})i = \perp$. In the actual protocol security model, the output of the protocol is $(EXEC\pi, A(k, \vec{\alpha}, z, \vec{r})1, EXEC\pi, A(k, \vec{\alpha}, z, \vec{r})2 \ldots . \ldots EXEC\pi, A(k, \vec{\alpha}, z, \vec{r})n)$

Definition 2-1 Calculates indiscernibility. Called two random variable family $\{Xi|Xi \in Di, i \in I\}$, $\{Yi|Yi \in Di, i \in I\}$ polynomial time calculation cannot be distinguished (Use $\stackrel{c}{\equiv}$ to express), If the probability algorithm for each polynomial level is M', each polynomial $P(n)$, and all the big integers n, it will have $|pr\{M'(Xi, i) = 1\} - pr\{M'(Yi, i) = 1\}| < 1/p(|i|)$

Definition 2-2 Probabilistic polynomial computing Turing machine. Given polynomial $P : N \rightarrow N$, for any interactive Turing entity M, at any time it runs (that is, any configuration of M), M the total number of steps up to $p(n)$, and $n = k + nI - no - k * nN$, k is a security parameter, nI is the total number of bit that is

currently written to the M input tape, nN is the number of different Turing machines that have been written by M.

2.2 Key Distribution Management Scheme

Set Ga, Gb as the P order large prime multiplication group, g as the generator of Ga, the bilinear pairings is $e(Ga, Ga) \rightarrow Gb$, where $e(R, g^r PK) = I$, H is a collisionless hash function. The publicly parameters are $(Ga, Gb, g, P, e(R, g^r PK) = I)$. Cluster members (except cluster heads) use the formula $h = H(ID)$ to calculate the value of the cluster member ID, and make $PK = g^h$, then register PK as identification of the cluster member in the cluster header.

2.2.1 Initialization Phase

The initial stage is implemented in the robust subset of cluster head in the wireless sensor network. The so-called robust subset means: Each cluster member is communicated with a subset of the cluster head to obtain a session key, each such set of cluster header is called a robust subset. Cluster head that satisfies the condition randomly selects σ where $\sigma \in Zp^*$, the cluster head generates the shared value $\{\sigma i\} i \in P$ of their $\sigma \in Zp^*$ according to the access structure Γ (A subset of ownership structure). Sharing scheme to resist active attackers, active attackers can invade a subset of the attacker structure A. Each cluster head can get the share value $\{\sigma i\} i \in P$ of $\sigma \in Zp^*$, but the cluster head which not in the Γ can't get any information about $\sigma \in Zp^*$. For every robust subset R, to meet any $B \in A$, there are $R - B \in \Gamma$. The process of generating shared value $\sigma \in Zp^*$ in R in a distributed manner is as follows:

Each cluster head $Ji \in R$ randomly selects a $x \in Zp^*$ and uses the vector space verifiable secret sharing scheme to distribute the fragments of x in the cluster head set J. p and q are prime numbers, and satisfy the conditions $q|p-1$. g is a generator of q order multiplication subgroup of Zp^*. Select a random vector $\vec{\eta} i = (\eta i^{(1)}, \eta i^{(2)} \ldots \eta i^{(r)}) \in (Zq)^r$, so that $\vec{\eta} i \cdot \psi(E) = xi$ is established, where $\psi : S \cup \{E\} \rightarrow (Zq)^r$ is a function that makes $P \in \Gamma$ if and only if $\psi(E) \in \langle \psi(Ji) \rangle Ji \in P$, E is an entity outside the set J. Ji sends fragment $xij = \vec{\eta} i \cdot \psi(Sj)$ to each cluster head Jj in J, and Ji also broadcasts a the promised value $\eta tt = g^{\eta i^{(t)}}$ for $\eta i^{(t)} (1 \leq t \leq r)$. Each participant $Jj \in J$ verifies the correctness of the fragment xij that sent by Ji by verifying whether the equation $g^{xij} = \prod_{t=1}^{r} (\eta it^{\psi(Jj)^{(t)}})$ is established. If the verification is not passed, Jj opens a complain to the Ji. If the set of participant which have sent a complain to $Ji \in J$ does not belong to a subset of A, that is, there is an honest participant sends a complain to Ji, then the Ji is rejected (terminated); Otherwise, that is, the complaint received by the $Ji \in J$ only from the attacker, then Ji open the fragments xij which be complained. If the above equation is not valid, then the Ji is rejected (terminated). $Con \subset R$ represents the set of participants through the validation phase. The secret key $\sigma = \sum_{i \in Con} xi$ is randomly generated by $Con \subset R$. Each cluster head $Jj \in J$ calculates the fragmentation of σ, the fragmentation formula is $\sigma j = \sum_{i \in Con} xij$. Where

$Ej = g^{\sum_{i\in Con} xij} = \prod_{i\in Con} g^{xij} = \prod_{i\in Con}\prod_{t=1}^{r}(\eta it^{\psi(Sj)^{(t)}})$, The initial stage of cluster heads is defined as $(\ldots.xi,\ldots..\perp\ldots) \rightarrow (\sigma 1, \sigma 2\ldots.\sigma n)$, Where xi is the input of the participants in R, the attacker no input.

2.2.2 Key Computation Phase

After generating the secret sharing value σ, all cluster heads can know the public commitment value $Ei = g^{\sigma i}(1 \le i \le n)$ of the σi, and the current cluster member can get a session key K. Each cluster head $Ji \in Con$ broadcasts a ciphertext (ri, si). The goal of this stage is to obtain the ciphertext (ri, si) of plaintext $h^{\sigma i}$. The keyquery and calculation process is defined as $(\ldots.(ai, bi, h), \ldots.) \rightarrow (\ldots..(ri, si), \ldots.)$, where $ai, bi \in Zp^*$.

2.2.3 Key Generation and Distribution Phase

Each cluster head which output (ri, si) (other outputs is L.) can form a subset of Γ. The cluster head selects $l \in RZ_P^*$ to send to the trusted network requester at first, cluster member calculates $R = g^{\frac{1}{h+l}}$ and sends it to the cluster head, the cluster header to verify whether the $e(R, g^l PK) = I$ is established to determine whether the members of the cluster are legitimate, then the cluster head in the permission set $C \in \Gamma$ can calculate the ciphertext (r, s) of the session key $K = h^{\sigma}$:

$$r = \prod_{Ji\in C} ri^{\lambda i^Q} = g^{\sum_{Ji\in Q}\lambda i^Q \cdot bi} \bmod p, \quad s = \prod_{Ji\in C} si^{\lambda i^Q} = h^{\sigma}(yj)^{\sum_{Ji\in Q}\lambda i^Q \cdot bi} \bmod p$$

where λi^Q is the reconstruction factor, to make $\psi(E) = \sum_{Ji\in Q}\lambda i^Q \psi(Ji)$, $\sigma = \sum_{Ji\in Q}\lambda i^Q \cdot ai \bmod q$ is established, the cluster head $Ji \in Q$ will send the ciphertext (r, s) to the cluster member Uj.

3 Authorization Certificate Issuing Mechanism

Before the two node communication, it will first go through the verification of each other's license certificate is legitimate before the formal communication. Authorization certificate is issued by the backbone router virtual CA. The paper uses the threshold-based multi-signature mechanism to issue the authorization certificate, and the reliability of the certificate is proved by mathematics. Authorization certificate issuing mechanism is as follows. N backbone router nodes choose to calculate open parameters; select a secure hash function; select a large prime p, q is a prime factor of p − 1. α is a q order generator of Z_p^*, Z_p^* is a modular P integer group. Generally, $2^{511} \le$ p $\le 2^{512}$; $2^{159} \le$ q $\le 2^{160}$; calculation and disclosure $y = \alpha^s \bmod$ p; participant $B_i \in A$, calculation and disclosure $y_{\mathrm{r}} = \alpha^{s_{i_r}} \bmod$ p; The user U sub-signature is given by the formulas (3-1) and (3-2):

$$\delta_r = \mathrm{H}\ (\mathrm{m})b_r + (c_{i_r} + 1)s_{i_r} \bmod \mathrm{q} \tag{3-1}$$

$$sig_r(\mathrm{m}) = (w_r, \delta_r) \tag{3-2}$$

In the formula (3-1), b_r is an integer randomly chosen [0, q − 1], m is user information, c_{i_r} and s_{i_r} can be obtained by formulas (3-3) and (3-4):

$$c_{i_r} = \prod_{1 \le j,r \le t, j \ne r} \frac{x_{i_j}}{x_{i_j} - x_{i_r}} (x_{i_r} = i_r) \tag{3-3}$$

$$s_{i_r} = h(x_{i_r}) \bmod \phi\ (x_{i_r} = i_r) \tag{3-4}$$

In the formula (3-2), $w_r = \alpha^{b_r} \bmod \mathrm{p}$ is published to all users, $sig_r(\mathrm{m})$ is the signature of the end user U. After receiving the sub-signature $sig_r(\mathrm{m})$, the end user U verifies whether the sub-signature is valid by the formula (3-5).

$$\alpha^{\delta_r} = w_r^{H(m)} y_r^{(c_{i_r}+1)} \bmod \mathrm{p} \tag{3-5}$$

Proof of formula (3-5):

$$\alpha^{\delta_r} = \alpha^{[H(m)b_r + (c_{i_r}+1)s_{i_r} + n_0 q]}$$

(Parameter n_0 is an integer; the other parameters are the same as the previous description)

$$= \alpha^{H(m)b_r} \alpha^{(c_{i_r}+1)s_{i_r}} \alpha^{n_0 q}$$

($\alpha^{n_0 q}$ equal unit element)

$$= \alpha^{H(m)b_r} \alpha^{(c_{i_r}+1)s_{i_r}}$$

$$w_r^{H(m)} y_r^{(c_{i_r}+1)} \bmod \mathrm{p}$$

$$= (\alpha^{b_r} + n_1 \mathrm{p})^{H(m)} (\alpha^{s_{i_r}} + n_2 \mathrm{p})^{(c_{i_r}+1)} \bmod \mathrm{p}$$

$$= \alpha^{H(m)b_r} \alpha^{(c_{i_r}+1)s_{i_r}} \bmod \mathrm{p}$$

If the Eq. (3-5) is established, the sub-signature is legal, otherwise the sub-signature is illegal.

4 Experiment Simulation and Result Analysis

4.1 Simulation Scenarios

Under the Window XP system, the paper uses the OPNET 10.5A simulation software to simulate the authorization of the key management scheme of wireless sensor network. The time distribution of authorization certificate issued by the main simulation

obtaining the initial key in different interval time and different requests and different threshold T, success rate and average distribution trend of delay, how to set the retransmission interval time, request time distribution and the threshold value of t to ensure the best performance of authorization certificate issued [13, 14].

An authorization certificate is issued for a simulation scenario with the following parameters:

(1) Scene scale: 300 m × 300 m;
(2) Main node types: 1 CA (Offline-CA), 32 Backbone-Router, 2 Zone-Route, 16 gt;
(3) Auxiliary node type: role configurator, application configurator, statistics center;
(4) Node transmission rate: backbone network using 54 Mbps, the regional network using 11 Mbps;
(5) The interval of retransmission (0.01 s, 0.60 s) (Fig. 2).

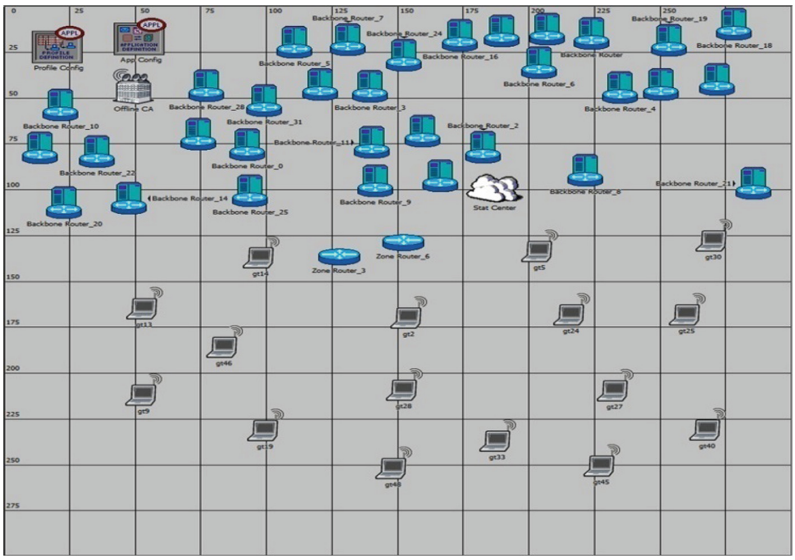


Fig. 2. Authorized certificate issued simulation scene

4.2 Simulation Results and Analysis

The simulation results of the success rate and average delay of the authorization certificate are shown in Figs. 3, 4, 5, 6, 7 and 8 in the case of the retransmission interval, the time distribution and the different thresholds of the different request issuing certificates: the abscissa is the time interval request issued by thee certificate of authorization; the success rate in the e curve diagram, the ordinate is the success rate in thee diagram, the average delay; authorization certificate issued, the ordinate is the average delay time distribution, unit is the second (s).

When the limit of system t value is 1, from the graph presented in Figs. 3 and 4 certificate success rate and average delay, the following conclusions can be drawn:

(1) When the interval is less than or equal to 0.03 s, the success rate is 0, and the average delay is also 0, which shows that when the t = 1, the backbone of the router in the shortest distance between the two adjacent routers is longer than 0.03 s.
(2) When the time interval is greater than 0.04 s, (0–1) to (0–5) the distribution of the success rate of the curves, and they were 100%, this shows that in the interval time is greater than 0.04 s, the success rate is not affected by request time distribution and retransmission interval time issued by the certificate of authorization.
(3) When the time interval is greater than 0.04 s, the average delay of the authorization certificate is not affected by the request time distribution and retransmission interval time issued by the certificate of authorization, the average delay of floating around 0.034 s, it will have a little change.

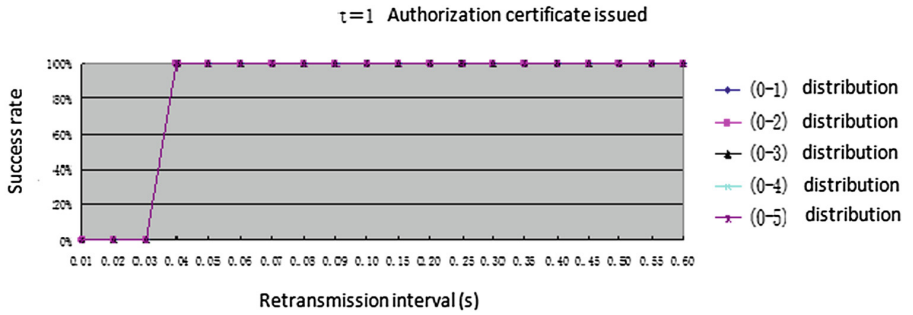


Fig. 3. t = 1 The success rate of the certificate issued

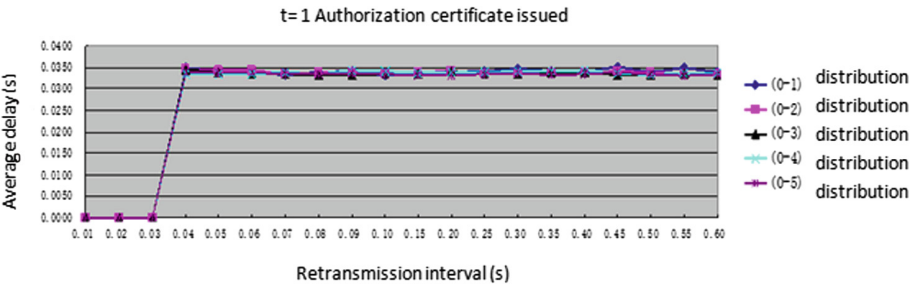


Fig. 4. t = 1 Average delay of authorization certificate

When the value of the threshold system t is 2, the success rate and the average delay graph of the certificate issued from Figs. 5 and 6 can be concluded as follows:

(1) As with t = 1, the success rate and average delay are 0 when the interval is less than or equal to.
(2) Retransmission interval is greater than 0.04 s, the interval time is 0.04 s, request distribution (0–1) distribution of the pole, (0–1) to (0–5) the distribution of the success rate was 100% and the curves, the success rate is: success rate is not affected by the request issued by the certificate of authorization of the time distribution of the cause; this is because the poles when t = 2, request authorization certificate for the 0.04 s and the retransmission interval (0–1) issued by the time in the distribution, there is a conflict caused by the relatively large, the success rate is 57%.
(3) Retransmission interval is greater than 0.04 s (0–1), in addition to the distribution of the average delay of volatility is relatively large, (0–1) to (0–5) at about 0.07 s the average delay distribution, it will have little change..

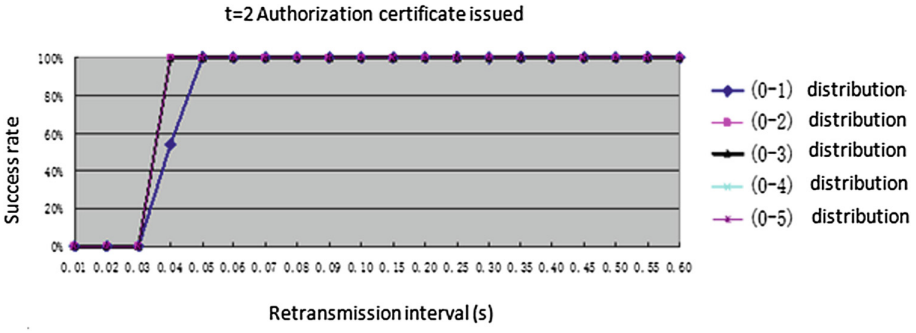


Fig. 5. t = 2 The success rate of the certificate issued

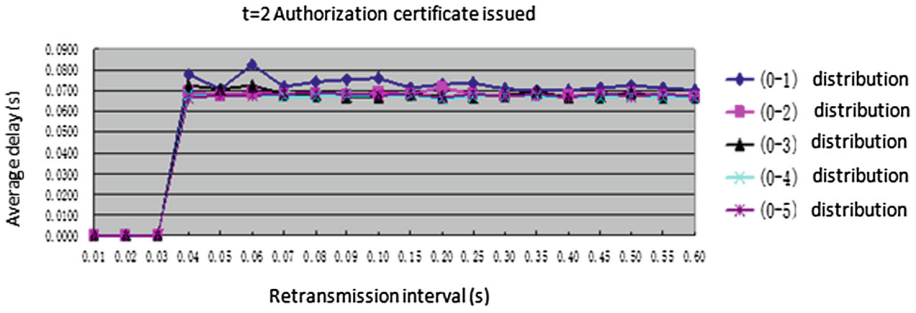


Fig. 6. t = 2 Average delay of authorization certificate

When the value of the threshold system t is 3, the success rate and the average delay graph of the certificate issued from Figs. 7 and 8 can be concluded as follows:

(1) When the interval is less than or equal to 0.03 s, the success rate is 0; after the interval is greater than 0.05 s, the success rate curve of (0–1) to (0–5) distribution coincidence, and the success rate of 100%;
(2) Retransmission interval between 0.03–0.05 s, (0–1) to (0–5) the success rate distribution curves are extreme, that when t is 3, interval between 0.03–0.05 s, (0–1) to (0–5) Certificate Authority issued certificate issued by the authorized distribution of failure process due to the existence of conflict;
(3) Retransmission interval is greater than 0.05 s, in addition to (0–1) the average delay curve fluctuates much distribution, (0–2) to (0–5) the average delay distribution curve is smooth, and are concentrated in the vicinity of 0.105 s.

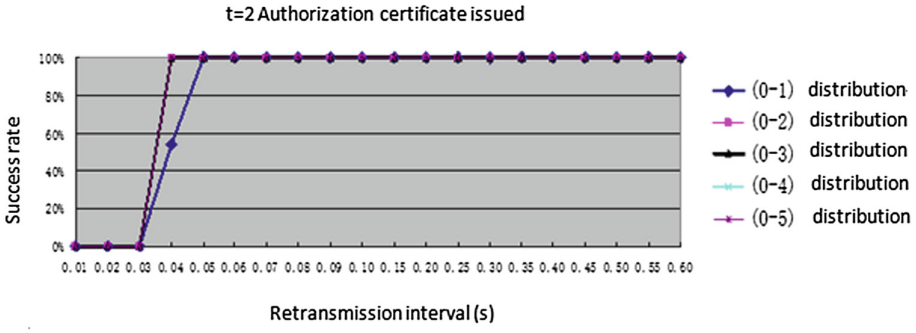


Fig. 7. t = 3 The success rate of the certificate issued

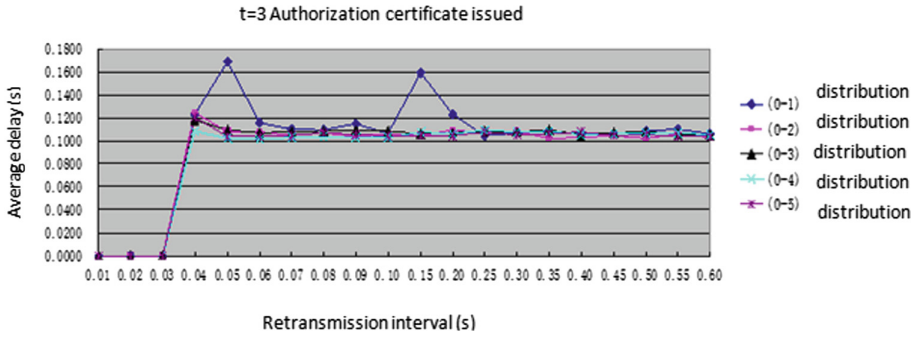


Fig. 8. t = 3 Average delay of authorization certificate

From the longitudinal comparison of the success rate and the average delay in Figs. 3, 4, 5, 6, 7, 8, 9 and 10, the following conclusions can be drawn:

(1) The retransmission interval should be at least greater than the distance between the nearest node of the backbone router and the backbone router;
(2) When the retransmission interval is greater than a certain threshold, the time distribution of the issuing certificate will have little effect on the success rate and the average delay;
(3) Retransmission interval is greater than a certain threshold value, the success rate of 100%, with the increase of t value, the threshold is more and more big, such as when t = 1, the threshold is 0.04 s; when t = 2, the threshold is 0.05 s; when t is 3, the threshold is 0.06 s;
(4) When the t value is low, the time distribution of the issuing certificate has little effect on the success rate, especially when t = 1, but with the increase of t value, the influence is more and more big;
(5) When the average delay is large, it will eventually approach a certain value. And with the increase of t value, this value is getting bigger and bigger;
(6) When t is the value, the greater the retransmission interval, the higher the success rate of the certificate issued, when the retransmission interval reaches a certain threshold, the success rate is 100%, the retransmission interval value is not the bigger the better, Otherwise it affects the delay in issuing a certificate of authorization.

5 Conclusion

The paper designs a set of wireless sensor network key management scheme, associating key information and node ID, which can effectively resist key attack in wireless sensor network, at the same time, the wireless sensor network model based on region can be used to deal with any scale of wireless sensor network and integrate different characteristics of subnet (such as sensor networks, Ad Hoc network access). When an area router suspects that a user's authorization certificate is false, the public key certificate issued by the offline CA can be used to verify the validity of the user; the user can grant the identity based private key and authorization certificate by any *t* backbone routers in *n* backbone routers; there are at least two backbone routers connected to Internet in the backbone network, and there are two regional routers connected to the backbone network, which improve the fault tolerance of the system.

References

1. Huanyi, C., Qingsong, C.: Ad hoc technology and WMANET network architecture. Commun. World **1**, 44–45 (2003)
2. Brunno, R., Conti, M., Gregori, E.: Mesh networks: commodity multi-hop ad hoc networks. IEEE Commun. Mag. **43**(3), 123–131 (2005)

3. Whitehead, P.: Mesh networks: a new architecture for broadband wireless access systems. In: Radio and Wireless Conference, Denvor, CO, USA, pp. 43–46. IEEE Press, Piscataway (2000)
4. Li, C.: Study and research on wireless network authentication technology security based on 802.1x protocol. Comput. Secur. (10), 4–12 (2006)
5. Fowler, T.: Mesh networks for broadband access. IEE Rev. **47**(1), 17–22 (2001)
6. Rayner, K.: Mesh wireless networking. Commun. Eng. **1**(5), 44–47 (2003)
7. Tabata, K., Kishi, Y., Konishi, S., Nomoto, S.: A study on the autonomous network synchronization scheme for mesh wireless network. In: 14th IEEE 2003 International Symposium on Personal, Indoor and Mobile Radio Communications Proceedings, Beijing, China, pp. 829–833. IEEE, Piscataway (2003)
8. Kishi, Y., Konishi, S., Nanba, S., Nomoto, S.: A proposal of millimeter-wave multi-hop mesh wireless network architecture with adaptive network control features for broadband fixed wireless access. In: Proceedings RAWCON 2001, IEEE Radio and Wireless Conference, Waltham, MA, USA, pp. 17–20. IEEE, Piscataway (2001)
9. Akyidiz, I.F., Wang, X., Wang, W.: Wireless mesh networks: a survey. Comput. Netw. **47** (4), 445–487 (2005)
10. Prasad, N.R., Alam, M., Ruggieri, M.: Light-weight AAA infrastructure for mobility support across heterogeneous networks. Wirel. Pers. Commun. **29**(3–4), 205–219 (2004)
11. Houyou, A.M., De Meer, H., Esterhazy, M.: P2P-based mobility management for heterogeneous wireless networks and mesh networks. In: Cesana, M., Fratta, L. (eds.) EuroNGI 2005. LNCS, vol. 3883, pp. 226–241. Springer, Heidelberg (2006). https://doi.org/10.1007/11750673_18
12. Luo, H., Lu, S.: Ubiquitous and robust authentication, services for ad hoc wireless networks. Technical report 200030. UCLA Computer Science Department (2000)
13. Mizrak, A.T., Chen, Y.C., Marzullo, K., et al.: Detecting and isolating malicious routers. IEEE Trans. Dependable Secure Comput. **3**(3), 230–244 (2006)
14. Karlof, C., Wagner, D.: Secure routing in wireless sensor networks: attacks and countermeasures. In: First IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK 2003, pp. 113–127 (2003)

Wireless Communications

A Novel Channel Model for Molecular Communications Based on Inter-cellular Calcium Wave

Hengtai Chang[1], Ji Bian[1], Jian Sun[1,2], Wensheng Zhang[1], and Cheng-Xiang Wang[3(✉)]

[1] Shandong Provincial Key Lab of Wireless Communication Technologies, Shandong University, Jinan 250100, Shandong, People's Republic of China
hunter_chang@126.com, bianjimail@163.com, {sunjian,zhangwsh}@sdu.edu.cn
[2] State Key Laboratory of Millimeter Waves, Southeast University, Nanjing 210096, People's Republic of China
[3] School of Engineering and Physical Sciences, Institute of Sensors, Signals and Systems, Heriot-Watt University, Edinburgh EH14 4AS, UK
cheng-xiang.wang@hw.ac.uk

Abstract. Calcium signalling is a good bio-inspired method for molecular communication due to the advantages of biocompatibility, stability, and long communication range. In this paper, we investigate a few channel characteristics of calcium signaling transfer systems including propagation distance and time delay based on a novel inter-cellular calcium wave (ICW) propagation model. Our model is the first one that can investigate the impact of some exclusive parameters in ICW (e.g., the gap junction permeability). Understanding the channel transfer characteristics of ICW can provide a significant reference for the calcium signaling application in molecular communication. In the future, theoretical and simulation results in this paper can help in the design of molecular communication systems between nanodevices.

Keywords: Molecular communication · Inter-cellular calcium wave
Channel characteristics

1 Introduction

In recent years, the rapid development of nanotechnologies provides many new applications in biomedical, industrial, and military fields [1]. In nanometer scale, the most basic unit is called nano-machine [2] and each nano-machine can only perform simple tasks like sensing, computing, and drug delivery. Therefore, cooperation of different nano-machines is significant for nano-machines to do complex tasks. Nano-sized communication allowing nano-machines to pass instructions and sharing informations is an important part of cooperation of nano-machines.

Molecular communication is a type of promising nano-sized communication technology and can be a good compensation to traditional communication mode

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 287–299, 2018.
https://doi.org/10.1007/978-3-319-90802-1_25

due to advantages of biocompatibility, small scale, and high energy efficiency [3]. In the molecular communication system, transmitted information is encoded in molecules and communicated by diffusion or molecular motor. By means of molecular communications, nano-networks between nano-machines can enable nano-machines to exchange messages and work cooperatively [4].

This paper concentrates on the bio-inspired molecular communication approach, which means that develop molecular communication from communication mechanism existing in biological structures. In nature, cells in organism transfer significant information to other cells using information objects. Bio-inspired approach utilizes communication mechanism existing in organism such as intercellular Ca^{2+}, Na^{+} wave propagation, and hormone traveling, to develop new advanced molecular communication technology. For this approach, bio-inspired molecular communication can work on both bio-organism and nano-machines that offer compatible solution for in-body communication scenario.

Calcium signal is a type of bio-inspired molecular communication method based on ICW [5]. Many studies suggested that this kind of communication method exists widely in nature [6,7]. As shown in Fig. 1, human smooth muscle coupling in intestines and stomach is mediated by Ca^{2+} release. In human astrocytes, the calcium wave plays an important role in information transfer in remote parts of the brain. Calcium signal is also a common phenomenon in epithelial cells, the calcium oscillation resulting from a simple regenerative is of vital importance for system equilibrium. In Ca^{2+} signaling, connected cells array can serve as a communication channel connecting the transmitter and receiver. The inter-cellular calcium wave can be transferred to the touching neighbor cells through the gap junctions, which results in the intercellular Ca^{2+} wave propagation.

Calcium signal have been studied by many researchers for a long time. In [10], a relay channel model based on ICW was proposed and communication capacity of a Ca^{2+} relay channel was computed. In [11], a linear channel model for intra/inter-cellular Ca^{2+} molecular communication based on Ca^{2+} signal was investigated and some channel characteristics were derived. However, these Ca^{2+} channel models mainly considered the effect of Ca^{2+} diffusion and Ca^{2+} induced Ca^{2+} release (CICR). Inositol 1, 4, 5-triphosphate (IP3) induced Ca^{2+} release was rarely taken into account in these channel models. According to the latest study [5], in some certain type of cells such as epithelial cells, ICW is mainly caused by transmission of IP3 between adjacent cells instead of calcium itself. This paper investigates the molecular communication channel model based on IP3 induced ICW. Close-form solutions for channel characteristics and channel capacity based on information theory are obtained, which will play important roles in communication system design and performance evaluation.

The rest of this paper can be divided in four parts. In Sect. 2, the mathematical model of cytosolic Ca^{2+} concentration oscillation and gap junction relevant to channel modeling is described and analyzed. In Sect. 3, some significant channel characteristics are analyzed based on a mathematical model. Binary channel capacity is computed in Sect. 4. Section 5 concludes the whole paper and points out the future works.

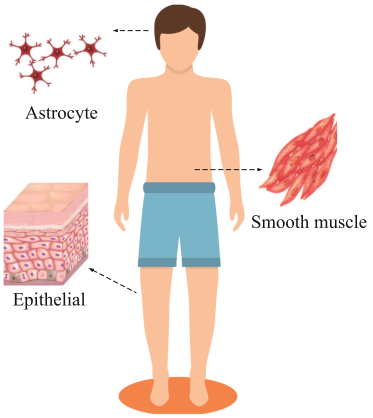


Fig. 1. Locations of cells having inter-cellular Ca^{2+} wave propagation.

2 Channel Models Based on ICW

2.1 Ca^{2+} Oscillation Model

Cytosolic Ca^{2+} serves as a kind of crucial second messenger in inter/inner cellular communications. The principle of this communication method has been studied by many researchers and different dynamic models have been proposed to explain the mechanism of ICW [8,9]. However, most communication channel models based on ICW mainly considered CICR to describe ICW communication mechanism, which dose not conform to the reality very well. In this paper, we refer to the ICW model proposed in [14], which takes IP3 as the main factor triggering the ICW, and apply this dynamic model to a molecular communication scenario, i.e. lots of cells connected with each other via gap junction. Then, we simulate the molecular communication process to get the ICW propagation characteristics based on the Ca^{2+} channel model.

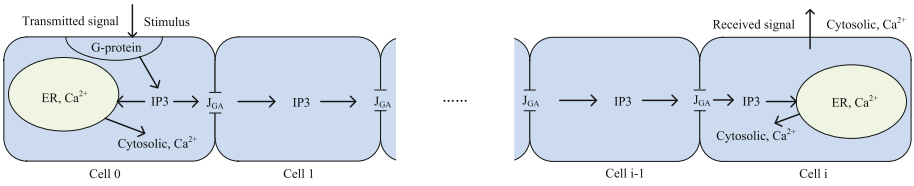


Fig. 2. Mechanism of inter-cellular Ca^{2+} wave propagation.

The basic mechanism of cytosolic Ca^{2+} oscillation is shown as Fig. 2 in Cell 0. Firstly, external stimulus applied on G-protein receptors induces the discharge of PLCβ molecules. Then, PLCβ molecules trigger the release of IP3 molecules initiating a rapid release of Ca^{2+} from the endoplasmic reticulum (ER) through IP3

and Ca^{2+} sensitive channels. Finally, with the repeated release and absorbtion of cytosolic Ca^{2+}, Ca^{2+} concentration in cytosol starts to perform an oscillation state.

This model contains three variables, namely, the concentrations of free Ca^{2+} in the cytosol (Z) and in ER (Y), and the IP3 concentration in the cytosol (A). The time evolution of these variables is governed by the following ordinary differential equations

$$\frac{dZ}{dt} = J_{\text{in}} + J_{\text{rel}} - J_{\text{pump}} - KZ + K_{\text{f}}Y \tag{1}$$

$$\frac{dY}{dt} = J_{\text{pump}} - J_{\text{rel}} - K_{\text{f}}Y \tag{2}$$

$$\frac{dA}{dt} = J_{\text{s}} + J_{\text{GA}} - \varepsilon A. \tag{3}$$

For cytosolic and ER Ca^{2+} concentration, J_{in} means the influx of Ca^{2+} from the extracellular media, J_{rel} and J_{pump} refer to IP3 induced Ca^{2+} release from ER and pumping of cytosolic Ca^{2+} into the ER, respectively, Ca^{2+} oscillation is mainly based on the balance between these two fluxes, KZ means the leak flux Ca^{2+} from cytosol to extracellular media which is proportional to cytosolic Ca^{2+} concentration, and $K_{\text{f}}Y$ is the leak flux of Ca^{2+} from ER to cytosol. For cytosolic IP3 concentration, J_{s} refers to stimulus induced IP3 release, ε refer to IP3 degration coefficient, and J_{GA} is the gap junction IP3 flux that will be discussed in next subsection. The function expressions of the participating fluxes are shown as follows:

$$J_{\text{s}} = \beta V_4 \tag{4}$$

$$J_{\text{in}} = V_0 + V_1\beta \tag{5}$$

$$J_{\text{pump}} = V_{\text{M2}}\frac{Z^2}{K_2^2 + Z^2} \tag{6}$$

$$J_{\text{rel}} = V_{\text{M3}}\frac{Z^m}{K_2^m + Z^m}\frac{Y^2}{K_{\text{Y}}^2 + Y^2}\frac{A^4}{K_{\text{A}}^4 + A^4}. \tag{7}$$

In these equations, V_0 refers to a constant input of Ca^{2+} from extracellular space and V_1 is the maximum rate of stimulus-induced influx of Ca^{2+} from the extracellular medium. Parameter β reflects the degree of stimulus that only varies between 0 and 1, V_4 is the maximum rate of stimulus-induced synthesis of IP3. V_{M2} and V_{M3} denote the maximum values of J_{pump} and J_{rel}, respectively. Parameters K_2, K_{Y}, and K_{A} are threshold constants for pumping, release, and activation of Ca^{2+} release by Ca^{2+} and by IP3, respectively. These parameter values are shown in Table 1.

2.2 Gap Junction Model

In the nature, one of the important cell-to-cell communication methods is the gap junction communication. In this way, the communication between different cells is achieved by the exchanges of message molecules like ions, protein,

Table 1. Simulation parameters.

Parameter	Value
Transport coefficient of cytosolic Ca^{2+}, k	$10\,s^{-1}$
Threshold constant for J_{pump}, K_2	$0.1\,\mu M$
Threshold constant for J_{rel} correlated to A, K_A	$0.2\,\mu M$
Coefficient of leak flux, K_f	$0.1\,\mu M$
Threshold constant for J_{rel} correlated to Y, K_Y	$0.2\,\mu M$
Threshold constant for J_{rel} correlated to Z, K_Z	$0.5\,\mu M$
Ca^{2+} from the extracellular medium, V_0	$2\,\mu M\,s^{-1}$
Maximum rate of stimulus-induced influx of Ca^{2+}, V_1	$2\,\mu M\,s^{-1}$
Maximum value of J_{pump}, V_{M2}	$6\,\mu M\,s^{-1}$
Maximum value of J_{rel}, V_{M3}	$60\,\mu M\,s^{-1}$
Maximum value of J_{in}, V_4	$2\,\mu M\,s^{-1}$
Coefficient of IP3 degration, ε	$0.3\,s^{-1}$
Hill coefficient, m	2

and organelles at the coupling channels of adjacent cells. This communication mechanism is a meaningful part of ICW propagation.

In our model, IP3 is transmitted by a transmitter cell, and then propagates through the gap junction crossing a few cells by means of diffusion. During this period, IP3 induces Ca^{2+} oscillation in passing cells and suffers decay in propagation process. Finally IP3 is received by the receiver cell and excites the Ca^{2+} oscillation. The IP3 flux between gap junction coupling cells is proportional to the IP3 concentration gradient and gap junction permeability [6]. Therefore, the IP3 gap junction transmitting mechanism is determined as

$$J_{GA} = P_{IP3}(Z^+ - Z) + P_{IP3}(Z^- - Z) \tag{8}$$

where Z^+ and Z^- are Ca^{2+} concentration in two different adjacent cells, P_{IP3} is the IP3 gap junction permeability and P_{IP3} is usually unaffected by the IP3 concentration. So, we consider that P_{IP3} is independent of IP3 concentration.

3 Results and Analysis

In this section, we study the ICW channel characteristics like maximum propagation distance, propagation time delay, and calcium oscillation frequency as the function of gap junction permeability P_{IP3} and stimulus intensity β using numerical and simulation methods.

3.1 Calcium Oscillation Condition

Refering to the model expression in Sect. 2.1, Ca^{2+} oscillation is mainly based on the balance between J_{pump} and J_{rel}. IP3 concentration increasing causes

the increasing of J_{rel} and breaks the steady state of cytosolic Ca^{2+}. Then CICR causes the positive feedback of J_{rel} and finally gives rise to Ca^{2+} oscillation. The condition of Ca^{2+} oscillation can be expressed as $J_{\text{pump}} > J_{\text{rel}}$, and substituting (6) and (7) into this condition we can get

$$V_{\text{M2}} \frac{Z^2}{K_2^2 + Z^2} > V_{\text{M3}} \frac{Z^m}{K_2^m + Z^m} \frac{Y^2}{K_{\text{Y}}^2 + Y^2} \frac{A^4}{K_{\text{A}}^4 + A^4} \tag{9}$$

$$\frac{A^4}{K_{\text{A}}^4 + A^4} > \max \left\{ \frac{V_{\text{M2}}({K_Z}^2 + Z^2)}{V_{\text{M3}}({K_2}^2 + Z^2)} \right\}. \tag{10}$$

Through proper simplification, the condition can be written as

$$A > (\frac{EK_A^4}{1-E})^{\frac{1}{4}} = K'_{\text{A}} \tag{11}$$

$$E = \begin{cases} V_{\text{M2}}{K_Z}^2 / V_{\text{M3}}{K_2}^2, & K_Z > K_2 \\ V_{\text{M2}}/V_{\text{M3}}, & K_Z \leq K_2 \end{cases} \tag{12}$$

which means that the sum of cytosolic Ca^{2+} fluxes forms the positive feedback and E is the critical condition of oscillation state and steady state for variable $\frac{A^4}{K_{\text{A}}^4 + A^4}$.

We take IP3 induced Ca^{2+} release threshold as K'_{A}. In order to prove that a certain IP3 concentration K'_{A} excites the calcium concentration oscillation, numerical method is used to simulate IP3 induced calcium oscillation. We use the system parameters from [14] and assume that all the cells in the system have the same biological parameters. Utilizing Runge-Kutta method, we get three variables time evolution of IP3 induced Ca^{2+} oscillation of different cells. Figure 3 indicates that the existence of Ca^{2+} oscillation is controlled by IP3 concentration. The same IP3 concentration threshold enable the oscillation in different cells. The relationship between IP3 concentration and Ca^{2+} oscillation amplitude or frequency is shown in Fig. 4. From this numerical simulation, Ca^{2+} oscillation amplitude Z_{AM} and frequency f_o are related with IP3 concentration and once IP3 concentration surpasses the threshold value K'_{A}, Z_{AM} and f_o tend to be a constant.

3.2 Intercellular IP3 Concentration Propagation

Since cytosolic Ca^{2+} oscillation is mediated by IP3 concentration in our model, ICW propagation time delay and distance can be calculated based on IP3 propagation differential equations. The variation of IP3 concentration due to the gap junction IP3 exchanging between Cell i and Cell i-1 can be illustrated as

$$\frac{dA_{\text{i}}}{dt} = \begin{cases} P_{\text{IP3}}(A_{\text{i-1}} - A_{\text{i}}) - \varepsilon A_{\text{i}} - P_{\text{IP3}}(A_{\text{i}} - A_{\text{i+1}}), & i \neq 0 \\ \beta V_4 - P_{\text{IP3}}(A_{\text{i}} - A_{\text{i+1}}) - \varepsilon A_{\text{i}}, & i = 0. \end{cases} \tag{13}$$

The IP3 in each cell can be described by steady-state and transient-state based on (13). Setting time derivative of A_{i} to 0, the steady-state of IP3 concentration

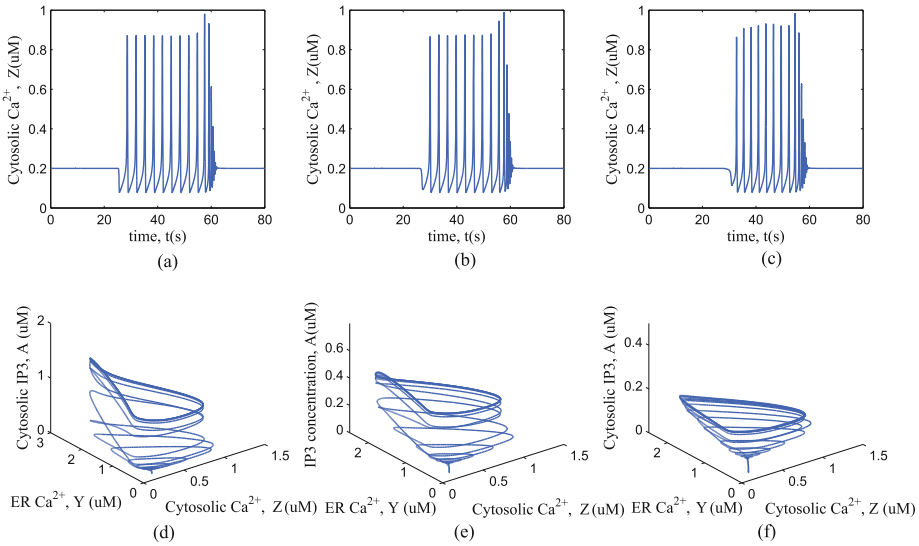


Fig. 3. Time evolutions of cytosolic Ca^{2+} concentration, (a) in Cell 2, (b) in Cell 4, and (c) in Cell 8 with transmitter cell subject to agonist stimulus representing the sequence '010' and symbol duration of 25 s. The relationships of three variables (A, Z, Y) are shown as (d) in (a), (e) in (b), and (f) in (c), respectively. Simulation parameters are the same as Table 1.

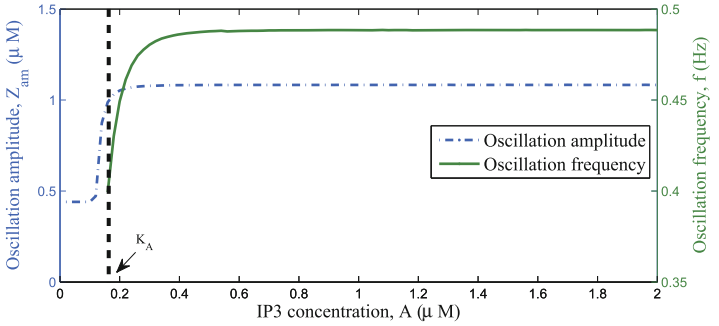


Fig. 4. Ca^{2+} oscillation amplitude or frequency affected by IP3 concentration.

in Cell i, A_i', can be obtained by solving the first order linear equations in matrix formation as below

$$\mathbf{Ax} = \mathbf{b} \tag{14}$$

where $\mathbf{A}$ is an infinite matrix with the formation

$$\mathbf{A} = \begin{bmatrix} (P_{\mathrm{IP3}}+\varepsilon) & -P_{\mathrm{IP3}} & 0 & \cdots & \\ -P_{\mathrm{IP3}} & (2P_{\mathrm{IP3}}+\varepsilon) & -P_{\mathrm{IP3}} & 0 & \cdots \\ 0 & -P_{\mathrm{IP3}} & (2P_{\mathrm{IP3}}+\varepsilon) & -P_{\mathrm{IP3}} & 0 \ \cdots \\ \vdots & \ddots & \ddots & \ddots & \end{bmatrix}.$$

Here, $\mathbf{x}$ and $\mathbf{b}$ are infinite vectors, i.e. $\mathbf{x} = \begin{bmatrix} A'_0 & A'_1 & A'_2 & \cdots \end{bmatrix}^T$, $\mathbf{b} = \begin{bmatrix} \beta V_4 & 0 & 0 & \cdots \end{bmatrix}^T$. By solving these equations, it can be found that steady-state IP3 concentration attenuation a_{in} between Cell i and Cell i+1 is a function of P_{IP3} and ε, and can be expressed as

$$a_{in} = 1 - \frac{\sqrt{\varepsilon^2 + 4\varepsilon P_{\mathrm{IP3}}} - \varepsilon}{2P_{\mathrm{IP3}}}. \tag{15}$$

Therefore, steady-state of IP3 in each cell can be obtained as

$$A'_i = a_{in} A'_{i-1} = a_{in}^i A'_0 \tag{16}$$

and A'_0 is written as

$$A'_0 = \frac{\beta V_4 (\sqrt{\varepsilon^2 + 4\varepsilon P_{\mathrm{IP3}}} - \varepsilon)}{2\varepsilon P_{\mathrm{IP3}}}. \tag{17}$$

Once the IP3 concentration steady-states in each cell is determined, IP3 induced ICW propagation distance N can be determined as

$$N \log a_{in} = \log \frac{\mathrm{K_A}}{\mathrm{A'_0}}. \tag{18}$$

Because of the time consumption of IP3 diffusion in the cytosol, we assume that inter cellular IP3 propagation starting from cytosolic IP3 concentration is equal to steady state. Then, the overall response of IP3 concentration in each cell can be written as

$$A_i(t) = \begin{cases} 0, & t \le (i-1)\tau_{in} \\ P_{\mathrm{IP3}} A'_{i-1}(1 - \exp(-\lambda (t - (i-1)\tau_{in}))/\lambda, & (i-1)\tau_{in} < t \le i\tau_{in} \\ a_{in} A'_{i-1}, & t > i\tau_{in} \end{cases} \tag{19}$$

where $\lambda = P_{\mathrm{IP3}} + \varepsilon$ is the time coefficient and τ_{in} is the IP3 propagation time delay for each cell that can be written as

$$\tau_{in} = \frac{1}{\lambda} \ln\left(\frac{\mathrm{P_{IP3}} - a_{\mathrm{in}}\lambda}{\mathrm{P_{IP3}}}\right). \tag{20}$$

Then, the time delay τ_i for ICW propagation of Cell i can be calculated by solving $A_i(\tau_i) = K_{\mathrm{A}}$ and the solution is

$$\tau_i = (i-1)\tau_{in} - \frac{1}{\lambda} \ln\left(1 - \frac{\mathrm{K_A}}{\mathrm{A'_i}}\right), \quad \mathrm{i} \le \mathrm{N}. \tag{21}$$

ICW propagation distance and delay can be calculated base on (18) and (21), respectively.

3.3 Effect of Gap Junction Permeability and Stimulus Intensity

In this subsection, we examine the ICW propagation distance and time delay with the variation of both junction permeability and stimulus intensity. The propagation distance for the ICW process is computed with both theoretical and numerical methods. It can be seen that theoretical and numerical values match well as shown in Fig. 5. Propagation distance is shown with respect to both the gap junction permeability and stimulus intensity. Increase of gap junction permeability and stimulus intensity can enhance the ICW propagation distance obviously.

ICW propagation time delay of Cell i is calculated in (21) as a function of number of cells along the path and simulated with Euler algorithm. From Fig. 6, ICW propagation time delay, τ_i, increases proportionally with the rising number

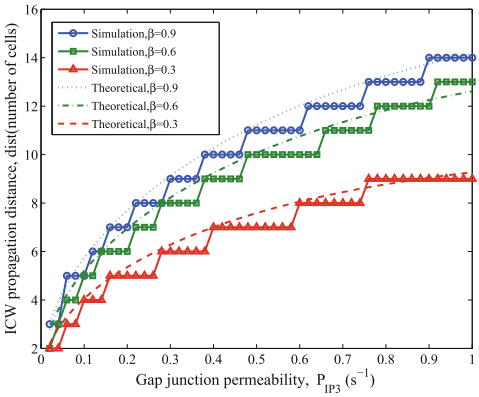


Fig. 5. ICW transmit distance with varying stimulus intensity and gap junction permeability.

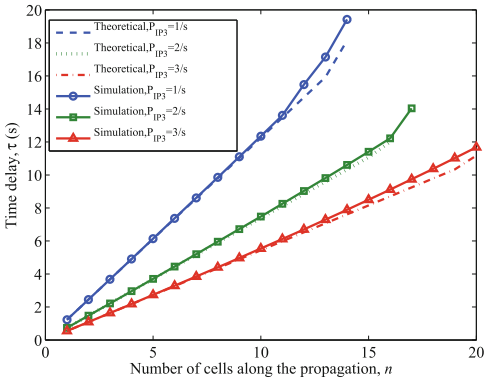


Fig. 6. ICW transmission delay with varying propagation distance and gap junction permeability.

of cells along the propagation. Meanwhile, gap junction permeability increase causes the decrease of time delay, indicating that gap junction permeability is another crucial factor affecting the calcium wave propagation delay. Therefore, it is a reasonable approach to optimize the communication channel by increasing the gap junction permeability.

4 Channel Capacity

Channel capacity can be calculated as the maximum mutual information value between the transmitter and the receiver. Considering a binary channel in our system, mutual information can be calculated as

$$\mathrm{I}(X;Y) = \sum_{\mathrm{X}} \sum_{\mathrm{Y}} \mathrm{P(x,y)} \log_2 \frac{\mathrm{P(x,y)}}{\mathrm{P(x)P(y)}}. \tag{22}$$

A symbol '1' is transmitted when continuous stimulus is applied to the transmitter cell. Detection of symbols at the receiver side is realized by detection of Ca^{2+} concentration pulses number. If the cytosolic Ca^{2+} concentration shows more than $M/2$ pulses within a symbol duration at receiver cell (M is the total number of pulses in a symbol duration with oscillation state, $M = f_0 T_s$), then we judge the received signal as '1'. If not, the received symbol will be detected as '0'. A symbol '0' is transmitted when no stimulus to transmitter cell and if the cytosolic Ca^{2+} concentration shows more than $M/2$ pulses without IP3, received symbol will be judged false as '1'. If not, the received symbol will be judged correctly as '0'. The probability of Ca^{2+} pulse occurring in unit time can be calculated as [12]

$$P_w = 1 - \exp(-\frac{P_{\max} Z_{\mathrm{init}}^2}{K_p^2 + Z_{\mathrm{init}}^2} T_u) \tag{23}$$

where $P_{\max}$ is the maximum probability of Ca^{2+} pulse occurrence in unit time T_{u}, $\mathrm{Z_{init}}$ is the initial Ca^{2+} concentration in cytosol, and K_p is the threshold constant. Here, we take $Z_{\mathrm{init}} = 0.2\,\mu\mathrm{M}$, $T_{\mathrm{u}} = 1\,\mathrm{s}$, $T_s = 25\,\mathrm{s}$, $f_o = 0.44\,\mathrm{Hz}$, and $K_p = 0.6\,\mu\mathrm{M}$. The error probability P_E of transmitting '0' and receiving '1' can be calculated as probability of more than $M/2$ pulses occurring in a symbol duration, i.e.

$$P_E = \Pr(m > \frac{M}{2}). \tag{24}$$

The pulse number without the IP3 in a symbol duration, m, can be approximated by poisson distribution as

$$m \sim \mathrm{Pois}(\frac{T_{\mathrm{s}} P_{\mathrm{w}}}{T_{\mathrm{u}}}). \tag{25}$$

The probability of Ca^{2+} oscillation occurring at receiver cell P_s due to ICW can be represented by probability of IP3 successful propagation. As mentioned in [13], gap junctions may be blocked due to virous factors such as connexin protein phosphorylation, which causes the ICW propagation to fail to transmit. We assume that different gap junctions have the same probability P_{block} to be blocked. Thus, the probability of IP3 induced ICW occurring at Cell n can be represented as

$$P_S(n) = \begin{cases} (1 - P_{\text{block}})^n, & n \leq N \\ 0, & n > N \end{cases}. \tag{26}$$

The joint probability distribution of the transmitted symbol and received symbol from Cell 0 to Cell n can be obtained as equation below

$$P_n(X, Y) = \begin{cases} P_0(1 - P_E), & X = 0, Y = 0 \\ P_0 P_E, & X = 0, Y = 1 \\ P_1(1 - P_S(n))(1 - P_E), & X = 1, Y = 0 \\ P_1 P_S(n) + P_1(1 - P_s)P_E, & X = 1, Y = 1 \end{cases} \tag{27}$$

where P_0 and P_1 are probabilities of transmitted symbols to be '0' and '1', respectively. Finally, the channel capacity can be calculated as maximum of mutual information value shown in Fig. 7. It can be seen that channel capacity reduce with the increase of propagation distance and maximum probability of Ca^{2+} pulse occurrence. Gap junction blocking greatly decreases the channel capacity in the long range ICW communication.

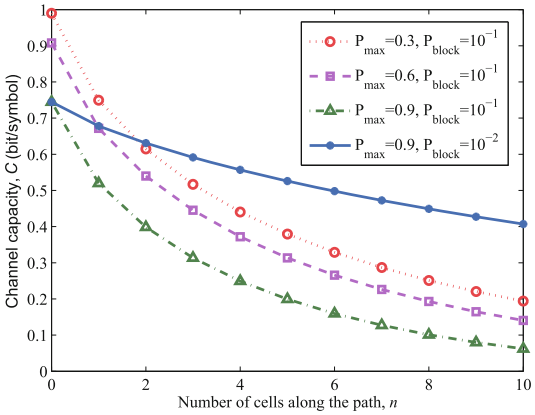


Fig. 7. Channel capacity between transmitter cell and receiver cell. $P_{\max}$ is set to be 0.3, 0.6, 0.9 and effect of P_{block} is also tested from 10^{-1} to 10^{-2} with $P_{\max} = 0.9$.

5 Conclusions

In this study, the mechanism of molecular communication via ICW has been illustrated and a few channel characteristics have been investigated based on the theory of IP3 induced inter-cellular calcium wave. The main contributions of this paper is offering close-form solutions for channel characteristics like IP3 propagation attenuation, ICW propagation distance, and ICW propagation time delay. Besides, channel capacity considering the binary channel has also been calculated. A few parameters affecting ICW propagation have been analyzed. We believe that theoretical and simulation results in this paper can offer significant reference to the design of ICW based molecular communication systems. However, most parameters in this study were set to be ideal which do not accord with the practical conditions. More practical parameters and models will be investigated in our future works.

Acknowledgment. The authors gratefully acknowledge the support from the EPSRC TOUCAN project (Grant No. EP/L020009/1), the EU FP7 QUICK project (Grant No. PIRSES-GA-2013-612652), the EU H2020 5G Wireless project (Grant NO. 641985), Natural Science Foundation of China (Grant No. 61210002 and 61371110), and Key R&D Program of Shandong Province (Grant No. 2016GGX101014).

References

1. Akyildiz, I.F., Brunetti, F., Blazquez, C.: Nanonetworks: a new communication paradigm. Comput. Netw. **52**(12), 2260–2279 (2008)
2. Akyildiz, I.F.: Nanonetworks: a new frontier in communications. In: Proceedings of the 2010, SECRYPT, Athens, Greece, p. IS-5 (2010)
3. Atakan, B., Akan, O.B., Balasubramaniam, S.: Body area nanonetworks with molecular communications in nanomedicine. IEEE Commun. Mag. **50**(1), 28–34 (2012)
4. Nakano, T.: Biologically inspired network systems: a review and future prospects. IEEE Trans. Syst. Man Cybern. C **41**(5), 630–643 (2011)
5. Kuran, M.S., Tugcu, T., Edis, B.O.: Calcium signaling: overview and research directions of a molecular communication paradigm. IEEE Wirel. Commun. **19**(5), 20–27 (2012)
6. Barros, M.T.: Ca^{2+}-signaling-based molecular communication systems: design and future research directions. Nano Commun. Netw. **11**, 103–113 (2017)
7. Barros, M.T., Balasubramaniam, S., Jennings, B.: Comparative end-to-end analysis of Ca^{2+} signaling-based molecular communication in biological tissues. IEEE Trans. Commun. **63**, 5128–5142 (2015)
8. Fink, C., Slepchenko, B., Moraru, I.: An image-based model of calcium waves in differentiated neuroblastoma cells. Biophys. J. **79**(1), 163–169 (2000)
9. Sobie, E., Dilly, K., Dos, S.: Termination of cardiac Ca(2+) sparks: an investigative mathematical model of calcium-induced calcium release. Biophys. J. **83**(1), 59–63 (2005)
10. Bicen, A.O., Akyildiz, I.F., Balasubramaniam, S., Koucheryavy, Y.: Linear channel modeling and error analysis for intra/inter-cellular calcium molecular communication. IEEE Trans. NanoBiosci. **15**(5), 488–498 (2016)

11. Nakano, T., Liu, J.Q.: Design and analysis of molecular relay channels: an information theoretic approach. IEEE Trans. NanoBiosci. **9**(3), 213–221 (2010)
12. Kilinc, D., Akan, O.B.: An information theoretical analysis of nanoscale molecular gap junction communication channel between cardiomyocytes. IEEE Trans. Nanotechnol. **12**(2), 129–136 (2013)
13. Nakano, T., Suda, T., Koujin, T., Haraguchi, T., Hiraoka, Y.: Molecular communication through gap junction channels. In: Priami, C., Dressler, F., Akan, O.B., Ngom, A. (eds.) Transactions on Computational Systems Biology X. LNCS, vol. 5410, pp. 81–99. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-92273-5_5
14. Houart, G., Dupont, G., Goldbeter, A.: Bursting, chaos and birhythmicity originating from self-modulation of the inositol 1, 4, 5-trisphosphate signal in a model for intracellular Ca(2+) oscillations. Bull. Math. Biol. **61**(3), 507–530 (1999)

Spatial-Temporal Distribution of Mobile Traffic and Base Station Clustering Based on Urban Function in Cellular Networks

Tong Wang(✉), Xing Zhang, and Wenbo Wang

Wireless Signal Processing and Network Laboratory,
Beijing University of Posts and Telecommunications,
Beijing 100876, People's Republic of China
zqwt199439@bupt.edu.cn

Abstract. With the rapid development of mobile internet, it's essential to understand the spatial-temporal distribution of mobile traffic. Based on the mobile traffic data collected from a large 4G cellular network in northwestern China, this paper presents detailed analyses of the traffic data on base stations in two aspects: (1) spatial-temporal distribution, (2) clustering based on physical context, i.e., urban function. We introduce the concept of traffic density to measure the traffic level, according to the Voronoi diagram to partition the covering area of BSs. Both spatial and temporal dimensions show distinct inhomogeneity property of mobile traffic. Furthermore, we cluster BSs utilizing urban function information, which enables us to identify and label base stations. The diverse application usage patterns of each cluster of BSs are obtained, which could be applied in resource cache policy and BS loading allocation.

Keywords: Spatial-temporal distribution · Mobile traffic
BS clustering · Urban function · Application usage pattern

1 Introduction

Global mobile data traffic has reached 7.2 exabytes per month at the end of 2016. And with the increasing scale of the cellular network, the fourth-generation (4G) traffic has increased up to 69% of mobile traffic [1]. Hence, from the network operators' point of view, to implement high-efficiency network planning and intelligent base station sleeping mechanisms are now in urgent need, which are key elements of establishing a green network.

For each single base station (BS), it has a specific covering area determined by its configuration and surrounding BSs, making it quite difficult for us to find a specific traffic usage pattern. As a result, through learning the spatial-temporal distribution of traffic, we understand the network traffic distribution, resource consumption and so on, thus making it easier for the resource allocation and efficiency promotion.

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 300–312, 2018.
https://doi.org/10.1007/978-3-319-90802-1_26

Models of spatial-temporal patterns and traffic load of BSs have both been studied in various existing works. For the spatial distribution of traffic load, it has been studied respectively for 2G [2] and 3G cellular networks [3]. Among those studies, applying log-normal distribution is the most common method to characterize the spatial traffic variations. But few papers study the spatial-temporal distribution of 4G cellular network traffic, and they often neglect the factor of covering area of the BSs. Besides, existing literatures focus on behavior modeling and prediction mainly from the perspective of users. However, those works don't focus on the BSs from application usage perspective, which is more important for network planning and optimizing. Cranshaw *et al.* [4] proposed an approach to discover urban functional regions based on the check-in data in FourSquare. However, the penetration rate of FourSquare is very low in China.

Based on the above-mentioned limitations of the related works, we utilize the 4G network traffic data and analyze the integral BSs of a metropolis from both temporal and spatial dimension. Furthermore, we cluster BSs utilizing the data of Points of Interest (PoIs) [5] so as to get the application usage patterns. The main contributions of our work are summarized as follows:

- **Both temporal and spatial distribution of traffic are analyzed in 4G cellular networks:** We utilize the 4G HTTP data and analyze the BSs of a metropolitan in temporal dimension by comparing the traffic data between weekday and weekend. And in spatial dimension, based on the Voronoi diagram to partition the covering area of BSs, we introduce the concept of traffic density to measure the traffic level.
- **The PoIs data are used to depict the physical context of BSs:** By crawling PoIs data through the Amap's application programming interface (API), We depict the BSs using a PoIs vector and cluster BSs by applying K-means algorithm, which is much easier to be generalized to other cities.
- **Diverse application usage patterns of each cl uster of BSs are obtained through horizontal and vertical comparison:** With a view to the heterogeneous usage of BSs on different applications, we employ the horizontal and vertical comparison to mine the diverse application usage patterns and verify our clustering results.

The rest of the paper is organized as follows. Section 2 introduces our dataset, details of application catalogues and data preprocessing. In Sect. 3, we analyze the distribution of traffic in temporal and spatial dimension. In Sect. 4, we cluster BSs using the PoIs and analyze the application usage patterns of each cluster. Finally, we discuss the conclusions in Sect. 5.

2 Dataset and Preprocessing

2.1 Dataset

In this section, we will introduce the dataset in detail, also including the application catalogues. The collected traffic data come from a large Chinese 4G-LTE

service provider, which covers over 25,000 cells in a northwest province in China. The billions of HTTP records last for 2 days (April 3–4, 2015), spanning from weekday to weekend. The fields 'etac' and 'eci' identify a specific cell.

Moreover, we crawl the PoIs via the Amap's API. As we choose one city (provincial capital) to analyze, the number of PoIs is about 9,600. PoIs are divided totally into 10 class: business, recreation, hospital, hotel, scenic spot, residence, government, education, transportation and company.

2.2 Preprocessing

Application Catalogue Update. Due to the inaccuracy of the application (APP) label, we update it by analyzing the following three fields: 'URL', 'host', 'user agent'. Enough key words are extracted to match more than 85 percent traces. Finally, we categorize the applications to 15 service types: instant messaging (IM), reading, blog, navigation, pic & video, music, app store, game, e-commerce, e-mail, social network, news, download, search and others. Table 1 shows the detailed statistic information about the new application catalogues.

Table 1. The percentage of metrics for each application category.

Application category	Traffic			Packets number			User number	Flow number	Duration
	Uplink	Downlink	Up & down	Uplink	Downlink	Up & down			
Instant messaging	13.50%	9.50%	9.64%	13.84%	11.34%	12.40%	90.92%	17.11%	8.27%
Reading	1.06%	0.51%	0.53%	0.70%	0.57%	0.62%	23.20%	0.95%	1.21%
Blog	1.17%	1.77%	1.75%	1.84%	1.64%	1.72%	19.43%	2.09%	1.63%
Navigation	2.59%	0.42%	0.49%	1.46%	0.96%	1.17%	77.72%	3.07%	3.71%
Pic & video	12.23%	46.06%	44.91%	30.95%	39.52%	35.91%	86.30%	12.92%	16.06%
Music	1.34%	2.59%	2.55%	1.92%	2.38%	2.19%	42.63%	1.06%	1.66%
App store	4.07%	9.08%	8.91%	7.59%	8.39%	8.05%	91.69%	5.26%	4.57%
Game	3.17%	1.12%	1.19%	1.79%	1.43%	1.59%	62.28%	2.89%	2.01%
E-commerce	10.91%	4.45%	4.67%	6.64%	5.32%	5.88%	63.96%	9.04%	12.56%
E-mail	0.24%	0.07%	0.08%	0.10%	0.09%	0.09%	5.95%	0.13%	0.13%
Social network	10.64%	5.31%	5.49%	8.46%	6.34%	7.23%	82.15%	11.23%	12.14%
News	7.95%	3.83%	3.97%	5.67%	4.45%	4.97%	83.92%	8.14%	7.73%
Download	7.90%	9.21%	9.17%	7.25%	8.72%	8.10%	85.19%	5.45%	5.49%
Search	8.95%	2.52%	2.74%	4.30%	3.29%	3.71%	87.26%	6.41%	8.96%
Others	14.28%	3.56%	3.92%	7.48%	5.57%	6.38%	90.92%	17.11%	8.27%

Data Aggregation. To analyze the traffic consumption from the view of BSs, we aggregate the data records to 1-h granularity. Each BS's traffic is characterized by a 48*14 matrix (2 days correspond to 48 h, and application numbers are 14 without regard to the unmatched traces).

3 Spatial-Temporal Traffic Analysis

In this section, we will describe our analysis result for mobile traffic on BSs from the temporal and spatial dimension using the 4G traffic data of a metropolis including downtown, suburb and subordinate rural area.

3.1 Temporal Dimension

As for the temporal dimension, we compare the traffic of different time slots in a day, along with the same time slot between weekday and weekend. To reflect the objective law, we choose five typical time slots, i.e., midnight (2:00–3:00), morning (7:00–8:00), noon (11:00–12:00), afternoon (17:00–18:00), evening (20:00–21:00), and aggregate the traffic for each BS and each time slot.

Figure 1 shows empirical CDFs of the traffic on all BSs. The 5 solid lines represent traffic on weekday, and the 5 dotted lines represent traffic on weekend. Blue lines on the top show that most of the BSs consume less traffic during midnight. However, dotted blue line is a little low, which means that BSs consume more traffic during midnight on weekend than that on weekday and we conclude that users tend to sleep late. But in the morning, BSs become more active during weekday. And among those 5 time slots, BSs consume more traffic during noon and afternoon than other time slots, which may be led by the behaviors of users to eat lunch and get off work. In summary, those results conform with people's daily activities and can be used to optimize the traffic resource allocation between BSs on temporal dimension.

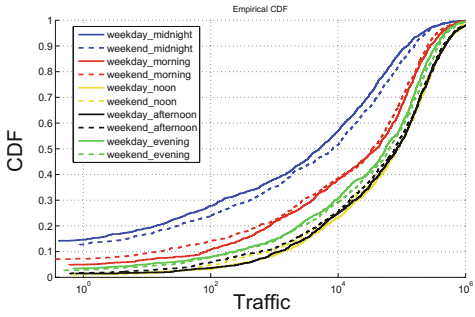


Fig. 1. The distribution of traffic on BSs. (Color figure online)

3.2 Spatial Dimension

Voronoi. While the BSs have a specific geographic location which could be identified by longitude and latitude, we use a software to transform them into Cartesian coordinate system and use x and y value to represent the BSs' position. Moreover, due to the complex practical environment such as the topography and

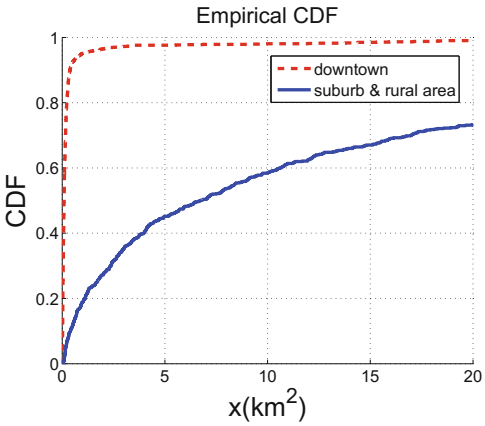


Fig. 2. The distribution of covering area.

buildings' distribution, the covering area of BSs are quite anomalous. To simplify the schematic diagram, we use Voronoi [6] to divide the covering area.

Utilizing the API of Amap, we divide the BSs of one city into two groups: (1) downtown, (2) suburb & rural area. Figure 2 evidently shows that the covering area of BSs in downtown are remarkable smaller than that in suburb & rural area. That means, the developed area has a higher BS density than developing area.

In order to combine the covering area and mobile traffic, we define the traffic density as the ratio of traffic and covering acreage to reflect the traffic consumption level [7]. Figure 3 shows a scatter diagram of traffic density versus BS covering area (including BS in both downtown and suburb & rural area). Traffic per BS and BS covering area exhibit some degree of negative correlations. The Spearman's correlation coefficient and the Pearson's correlation are -0.5208 and -0.0947, respectively. We check correlations between them by using a linear regression function to fit the dots and get a rough relation:

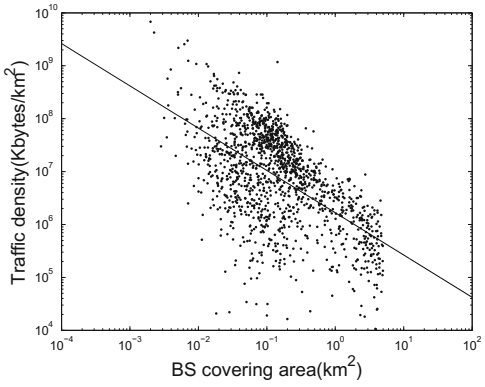


Fig. 3. A scatter diagram of traffic density versus BS covering area.

$$\log_d \rho = -0.7989 * \log_d s + 6.2231 \tag{1}$$

where ρ represents the BS traffic density and s represents the BS covering acreage. We conclude that the number of deployed BSs and BS locations are closely affected by the traffic density of a specific area. So in reality, when deploying a new BS, the network operators will take the traffic density of this area into account.

Traffic Density Distribution. Figure 4 shows the empirical CDFs of the traffic density and its fitting with log-normal, Weibull, gamma and exponential distributions. For both downtown and suburb & rural area, the log-normal and Weibull distribution show a better fitting result. We introduce K-S test [8] to measure the fitting performance and the test results are shown in Table 2. The last column 'cv' represents the critical value of the test. The Weibull distribution is accepted at the 5% significance level for downtown ($0.0406 < 0.0407$), while the log-normal distribution is accepted for suburb & rural area ($0.0316 < 0.0773$).

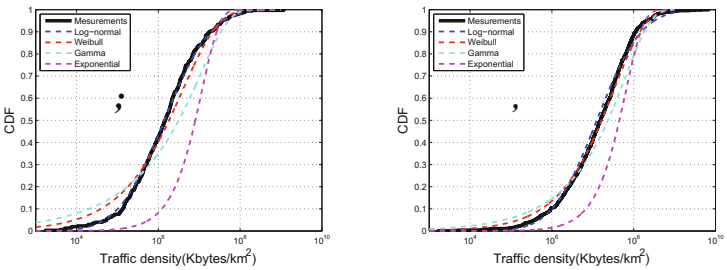


Fig. 4. The distribution of traffic density in (a) downtown, (b) suburb & rural area.

Table 2. Fitting result in k-s test.

	Log-normal	Weibull	Gamma	Exponential	cv
Downtown	0.0488	0.0406	0.1141	0.2939	0.0407
Suburb & rural area	0.0316	0.0847	0.1878	0.4365	0.0773

4 BS Clustering and Application Usage Patterns

In this section, we combine the cellular network traffic data with the PoIs data crawled from Amap's API to cluster BSs. Besides, in view of the advantage that traffic data contain APP types, horizontal and vertical comparison are applied to help us understand the APP patterns existing in different BS clusters.

4.1 Methodology

Normalization Utilizing TF-IDF. The traffic pattern of BSs largely depends on the area they cover, so we utilize the PoIs data to cluster BSs and allocate labels. The PoIs are classified into 10 class: business, recreation, hospital, hotel, scenic spot, residence, government, education, transportation and company. By counting the PoIs in the area the BS covers, we get a 1*10 PoI vector to characterize each BS: $X_i = \left[p_i^1, p_i^2, ..., p_i^{10}\right]$. In consideration that the numbers of different PoI types vary considerably, term frequency inverse document frequency (TF-IDF) [9] is used as a method to balance the weights between those PoI categories. TF-IDF is a non-linear transformation, which is widely used in document classification to reflect how important a word is to a document. It's the product of term frequency (TF) and inverse document frequency (IDF). In our research, it's used to measure the importance of a specific PoI type to the BS. Specifically, for a BS $i \in \{1, 2, \ldots, N\}$ and a PoI type $j \in \{1, 2, \ldots, 10\}$, the TF-IDF value (F_i^j) can be calculated as follows:

$$F_i^j = \mathrm{TF}_i^j \cdot \mathrm{IDF}_i^j \tag{2}$$

$$\mathrm{TF}_i^j = p_i^j / \sum_1^{10} p_i \tag{3}$$

$$\mathrm{IDF}_i^j = \log_d(N/n) \tag{4}$$

where N is the total number of BSs and n is the number of BSs that have the PoI type i in their area ($p_n^i \neq 0$). Multiply the TF and IDF factor, the final TF-IDF vector can be described as: $F_i = \left[F_i^1, F_i^2, ..., F_i^{10}\right]$.

K-Means++ Clustering. As for the clustering algorithm, we cluster the BSs based on the classic K-means algorithm. Taking into consideration of relevance of 10 kinds of PoIs, Pearson correlation is adopted as the distance depiction. Due to the randomness of initial seeds selection in standard K-Means algorithm, we use K-Means++ [10] instead and set 10 linearly independent vectors as initial cluster centers. Table 3 shows the BS clustering result when k = 10. Through observing the mean TF-IDF value, we conclude that each cluster has a unique dominant PoI type. In Fig. 5, each color represents a specific BS cluster, which reveals that the BS clusters don't have aggregation effect but truly contain some adjacent BSs. This clustering method based on the urban function could be applied to many researches. Take traffic prediction for example, when building the prediction model, the label of BSs should be taken into consideration, thus models with various parameters are built for different clusters to enhance the accuracy.

Table 3. The BS clustering result.

BS label	BS number	PoI type (TF-IDF value)									
		Business	Recreation	Hospital	Hotel	Scenic spot	Residence	Government	Education	Transportation	Company
Business	130	**0.3137**	0.0007	0.0233	0.0126	0	0.0546	0.0269	0.0362	0.0019	0.0396
Recreation	19	0.0586	**0.5277**	0.0313	0.0130	0.0146	0.0389	0.0273	0.0637	0	0.0437
Hospital	109	0.0146	0.0017	**0.2812**	0.0136	0.0014	0.0456	0.0270	0.0535	0	0.0255
Hotel	101	0.0349	0.0035	0.0261	**0.3081**	0.0066	0.0540	0.0361	0.0481	0.0014	0.0290
Scenic spot	44	0.0279	0.0109	0.0439	0.0145	**0.4442**	0.0483	0.0521	0.0378	0	0.0414
Residence	137	0.0094	0	0.0221	0.0078	0.0028	**0.2210**	0.0249	0.0450	0.0013	0.0181
Government	138	0.0133	0	0.0191	0.0160	0.0060	0.0382	**0.2744**	0.0521	0.0014	0.0391
Education	179	0.0069	0	0.0148	0.0064	0.0030	0.0275	0.0153	**0.2135**	0.0008	0.0220
Transportation	27	0.0195	0	0.0260	0.0319	0.0056	0.0327	0.0601	0.0350	**0.6018**	0.0634
Company	116	0.0207	0	0.0099	0.0094	0.0033	0.0335	0.0149	0.0306	0.0009	**0.3316**

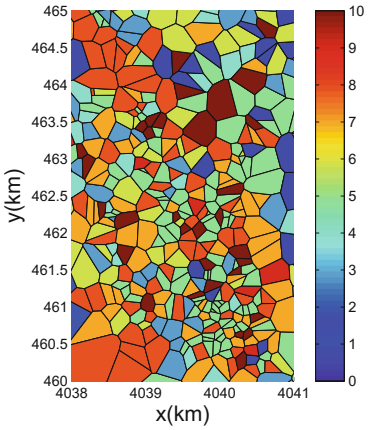


Fig. 5. Voronoi cells with BS clusters padding.

4.2 Traffic Patterns

Entropy of APPs. Just as the Table 1 shows, the proportion of 14 kinds of APPs differ significantly. To characterize the specific distribution of those APPs, we import entropy to measure their diversity, which is defined as below:

$$H(x) = -\sum_{1}^{N} p(x_i) \log_b p(x_i) \tag{5}$$

where N is the number of BSs, each different i represents a specific BS, and x represents an APP category. $p(x_i)$ is the proportion of the APP traffic consumption on one BS. The entropy reaches maximum when the distribution is uniform. Here, we use the normalized entropy as below to compare the different patterns between APP categories.

$$H_{norm}(x) = H(x)/H_{max}(x) \tag{6}$$

$$H_{max}(x) = \log_b N \tag{7}$$

Figure 6 shows the normalized entropy of each APP for every hour in two days. The trend of the entropy for 14 kinds of APP catalogues are approximately

similar, which is high in the day and low during the night, but their average levels exhibit considerable divergence. The entropy of IM is the highest, with a maximum of 0.9042, which means IM is most popularized. But e-mail exhibits a quite low entropy, with a maximum of 0.6992 and a minimum of 0.1926. It reveals that e-mail is mainly used on a small proportion of BSs, more likely in workplaces.

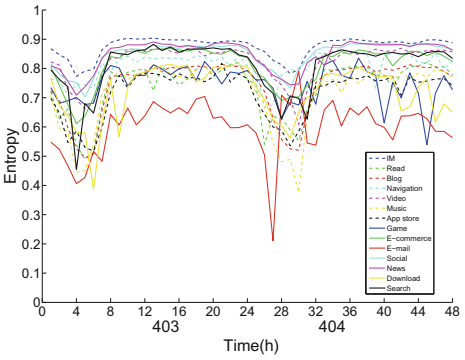


Fig. 6. The entropy of APPs with time varying.

Horizontal Comparison Between Clusters. According to the above result using entropy, the 14 kinds of applications exhibit high difference in mobile traffic and flow numbers due to their natural properties. To break through this limitation, we use horizontal comparison method to observe the traffic patterns of each BS cluster without normalization. Specifically, the overall traffic consumption ratio of each kind of application is calculated as a baseline, then we compare the traffic of a specific application in each cluster based on the baseline. Figure 7 describes the traffic pattern of each cluster, where red pillars are applications exceeding the baseline and blue ones on the contrary. To illustrate them more clear, we set a threshold to filter the histogram. That means, we only take the red ones with value bigger than 0.1 as dominant services and blue ones with value smaller than -0.1 as weak services. Table 4 gathers all the filtered information, some objective law and interesting phenomena are revealed:

- In hotel and scenic spot areas, navigation APPs are dominant. Tourists and the people on a business trip are main users in those areas, and they tend to be unfamiliar with the local traffic information. In those condition, Navigation APPs such as Amap and Didi Taxi are frequently used.
- Cluster shopping doesn't show a specific preference on APPs. It may be because that BSs in shopping areas have a large number of floating population. No regular application usage pattern is acquired.
- Recreation area is mainly constituted by theater, bar and so on. Users are more likely to use entertainment APPs to relax such as games and videos.

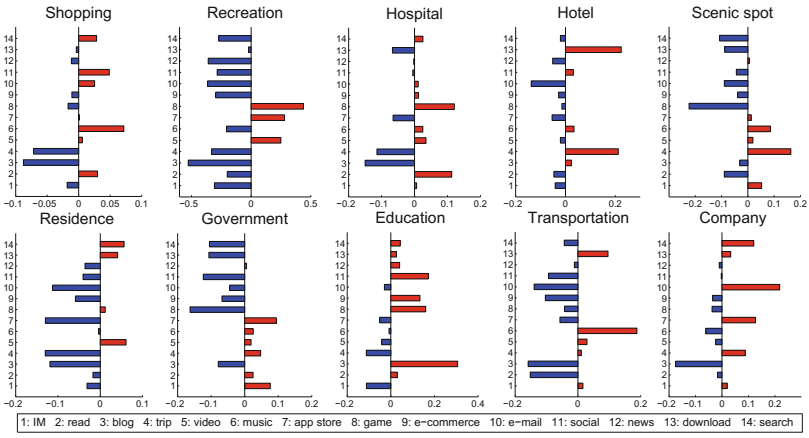


Fig. 7. APP pattern – horizontal comparison result.

- BSs in education area cover many middle school students and undergraduates. They show a preference on blog, game and social network APPs, while social networking and navigation APPs are in a weak position.
- In transportation area such as railway station, bus station and airport, people listen to music more than other places. It shows a popular user behavior about music service.
- Games are played less in the government, while companies use more e-mail service. Both of them show their characteristic of workplaces.

For BS clusters under different urban function, they show various preference on APP usage, which conform to the distribution of urban PoIs. Those above APP patterns answer to popular user behaviors, and can be utilized to help network operators understand the traffic distribution, such as applying some targeted resource cache policy. For example, because of the preference that people tend to listen to music in transportation junctions, we could buffer more music information on BSs in those areas and let the people nearby access to those BSs preferentially when they request music information. In this way, the requests to core network will decrease, which will both save the network energy and promote the network efficiency.

Vertical Comparison Between Weekday and Weekend. In order to understand the APP patterns comprehensively, we also apply the vertical comparison thought. Specifically, the data records on April 3 and 4 are used to represent the traffic on weekday and weekend, and we compare the APP patterns using the ratio of the weekend service traffic to weekday service traffic. In Fig. 8, the APP patterns acquired through vertical comparison are showed by aggregating the red pillars and blue pillars separately, which is more intuitive. The whole traffic of cluster shopping, recreation, residence, government, transportation grow

Table 4. Filtration result in horizontal comparison.

BS clusters	Dominant	Weak
Shopping	/	/
Recreation	Game, app store, pic & video	Blog, e-mail, navigation
Hospital	Read, game	Blog, navigation
Hotel	Navigation, download	e-mail
Scenic spot	Navigation	Game, search
Residence	/	App store, navigation, blog
Government	IM, navigation	Game, social networking, download
Education	Blog, game, social networking	IM, navigation
Transportation	Music	Read, blog, e-mail
Company	Email, app store, search	Blog

rapidly on weekend, with the traffic of cluster hotel, scenic spot and education on the contrary. As for cluster company and transportation, plot the detailed comparison histogram and some interesting phenomena emerge. In company area, the traffic of blog, music and e-commerce increase 21.36%, 8.29% and 9.32% respectively, while the traffic of e-mail reduces more than 22%. The traffic of transportation cluster BSs increases clearly on all APP types, as the traffic on weekend is almost 1.5 to 3 times of that on weekday for every application. It reveals that the number of traveling people has an alarming rise on weekend.

Through vertical comparison between weekday and weekend, we obtain the APP patterns on each BS cluster. Depend on the activities of users in each BS's covering area, the app usage patterns show a certain degree of periodicity. Those would give us an essential cognition of their APP patterns, which could be used to optimize the BS loading with day-varying allocation. Based on this, for a dataset that lasts more than one week, the periodicity of traffic pattern for those clusters could be extracted. And due to the differences of urban planning and economic development degree among cities, more studies are further needed to compare the traffic patterns between cities of varying degrees of development.

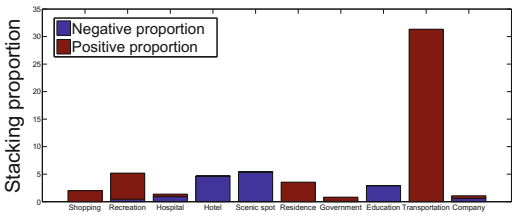


Fig. 8. APP pattern – vertical comparison result.

5 Conclusion

In this paper, through utilizing the mobile traffic data collected from 4G cellular networks in northwestern China, we comprehensively study the temporal and spatial distribution of mobile traffic data on BSs. The Voronoi diagram and traffic density are imported in order to make the results more clearly. The result shows quite an obvious heterogeneous distribution of traffic data on both temporal and spatial dimension. Based on the Voronoi diagram, we combine the traffic data with the PoIs data crawled from Amap to cluster BSs into 10 groups, which give each BS a specific label. The methodology of combining datasets could be applied to many research. And the APP patterns obtained by horizontal and vertical comparison are very practical and meaningful in resource cache policy and BS loading allocation.

We are continuing our research focusing on various interesting and practical dimensions, including predicting the traffic trend of BSs and introducing various complex network theories. We hope our research result inspire you for further research in this area.

Acknowledgements. This work is supported by the National Science Foundation of China (NSFC) under grant 61571054, 61771065 and 61631005, by the New Star in Science and Technology of Beijing Municipal Science and Technology Commission (Beijing Nova Program: Z151100000315077).

References

1. Cisco visual networking index: Global Mobile Data Traffic Forecast Update, 2016–2021. https://www.cisco.com
2. Gotzner, U., Rathgeber, R.: Spatial trac distribution in cellular networks. In: Vehicular Technology Conference, VTC 1998, Ottawa, vol. 3, pp. 1994–1998 (1998)
3. Paul, U., Subramanian, A.P., Buddhikot, M.M., Das, S.R.: Understanding traffic dynamics in cellular data networks. In: 2011 Proceedings IEEE INFOCOM, Shanghai, pp. 882–890 (2011)
4. Cranshaw, J., Schwartz, R., Hong, J., Sadeh, N.: The livehoods project: utilizing social media to understand the dynamics of a city. Social Science Electronic Publishing (2012)
5. Xu, F., Zhang, P., Li, Y.: Context-aware real-time population estimation for metropolis. In: ACM International Joint Conference on Pervasive and Ubiquitous Computing ACM, pp. 1064–1075 (2016)
6. Guruprasad, K.R.: Generalized Voronoi partition: a new tool for optimal placement of base stations. In: 2011 Fifth IEEE International Conference on Advanced Telecommunication Systems and Networks (ANTS), Bangalore, pp. 1–3 (2011)
7. Zhou, S., Lee, D., Leng, B., Zhou, X., Zhang, H., Niu, Z.: On the spatial distribution of base stations and its relation to the traffic density in cellular networks. IEEE Access **3**, 998–1010 (2015)
8. Woodruff, B.W., Moore, A.H., Dunne, E.J., Cortes, R.: A modified Kolmogorov-Smirnov test for Weibull distributions with unknown location and scale parameters. IEEE Trans. Reliab. **R–32**(2), 209–213 (1983)

9. Leng, B., Liu, J., Pan, H., Zhou, S., Niu, Z.: Topic model based behaviour modeling and clustering analysis for wireless network users. In: 2015 21st Asia-Pacific Conference on Communications (APCC), Kyoto, pp. 410–415 (2015)
10. Agarwal, S., Yadav, S., Singh, K.: Notice of violation of IEEE publication principles K-means versus k-means ++ clustering technique. In: 2012 Students Conference on Engineering and Systems, Allahabad, Uttar Pradesh, pp. 1–6 (2012)

Research on Irregular Carrier Aggregation in Complex Electromagnetic Environment

Jingning Wang[1,2(✉)] and Meng Liu[1]

[1] The 54th Research Institute of CETC, No. 589 West Zhongshan Road, Shijiazhuang, Hebei, China
wjnhit@126.com

[2] Science and Technology on Communication Networks Laboratory, No. 589 West Zhongshan Road, Shijiazhuang, Hebei, China

Abstract. In order to take full advantage of the discontinuous and irregular frequency in complex electromagnetic environment, an irregular carrier aggregation method is proposed. In the proposed method, several frequency bands from 1 MHz to 20 MHz can be combined to a wideband channel, witch can transmit HD image etc. The process and the key technologies are introduced, including channelized spectrum, resource allocation, synchronization and channel estimation. Analysis shows that the proposed carrier aggregation method has effective anti-jamming ability and the spectrum resources can be utilized efficiently.

Keywords: Complex electromagnetic environment
Irregular carrier aggregation · Channelized spectrum · Resource allocation

1 Introduction

Carrier Aggregation (CA) is one of the key technologies of Long Term Evolution Advanced (LTE-A) systems, consists of distributing the information over several frequency bands to achieve a very large bandwidth. According to the CA approach, the User Equipments (UEs) can access a wider transmission bandwidth by using CA to aggregate a number of individual Component Carriers (CCs) shaping heterogeneous contiguous and non-contiguous frequency bands. In LTE-A, at most 5×20 MHz carrier aggregation is adopted.

There are three methods of frequency aggregation; the first method is contiguous intraband frequency aggregation in which the information is transmitted over frequency subbands placed next to each other, within one frequency band. The second method consists of transmitting information over separated subbands within a frequency band, which is called noncontiguous intraband frequency aggregation. In the last method, the information is transmitted over different subbands placed at different bands [1, 2].

In complex electromagnetic environment, there are not 20 MHz or 5 MHz frequency spectrum without interference. The available frequency spectrum in frequency band is discontinuous and irregular. The CA methods for several regular frequency band in LTE-A are not applicable. Cognitive Radio (CR) and Non-Contiguous Orthogonal Frequency

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 313–318, 2018.
https://doi.org/10.1007/978-3-319-90802-1_27

Divison Mutilplex (NC-OFDM) are effective solution for this scene. NC-OFDM is a highly efficient multi-carrier modulation technology which has a good anti-jamming performance by selecting the sub-band without interference to transmit data in interference environment [3, 4]. But the frequency band of NC-OFDM is limited, such as 20 MHz or 40 MHz, and the available frequency spectrum band is distributed in one or several hundred MHz.

In order to apply the discontinuous and irregular frequency resource in wide frequency band, a new carrier aggregation method is proposed, which can combine several irregular frequency band distributing in 100 MHz or more.

The rest of the manuscript is organized as follows. In Sect. 2, the system model description and parameter setting are given. In Sect. 3, the proposed CA method and the research points are introduced. And Sect. 4 concludes the work.

2 Parameter Setting and Flow

The LTE is consulted in this paper, such as the sub-carrier bandwidth, synchronization and resource allocation. The sub-carrier bandwidth is 15 kHz and one resource block (RB) contains 12 sub-carrier (180 kHz). The primary synchronization signal (PSS) and the secondary synchronization signal (SSS) need to occupy 6 RBs (1.08 MHz). UEs receive the PSS and SSS to get time and frequency synchronization, and obtain the UE physical layer cell ID, the length of the Cyclic Prefix (CP) (Fig. 1).

Spectrum sensing is the first step, frequency occupancy is obtained. The available frequency spectrum distributes in 100 MHz discretely. A threshold is set and the frequency spectrum with interference lower than the given threshold is available. There are 4 available frequency band in Fig. 2.

The spectrum is periodic and the available frequency spectrum is dynamic changing. The operating bandwidth is 100 MHz, and at least 2 carriers can be converged and at least 5 MHz frequency can be used. The bandwidth of one band is at most 20 MHz.

Resource allocation is the second step, the available frequency spectrum is allocated to multi-user. The spectral efficiency and energy efficiency should be considered in this step.

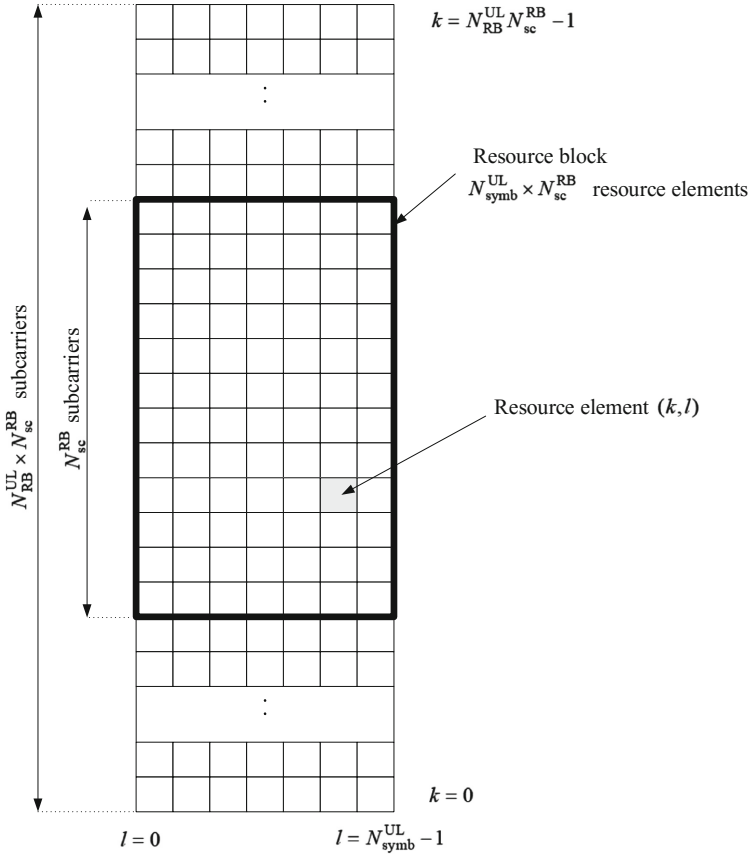


Fig. 1. The RB in LTE, which is consulted in this paper.

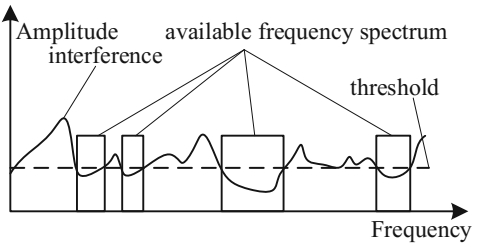


Fig. 2. There are 4 available bands where the interference is lower than the given threshold.

3 Key Technologies

3.1 Channelized Spectrum in Spectrum Sensing and Using

In spectrum sensing, the spectral resolution is related to complexity. Consult the LTE standard, 2048 points FFT is used and the spectral resolution is 15 kHz. The filter bandwidth is finite, so frequency sensing should be segmented to several 20 MHz for 100 MHz frequency band. The sensing result should be coupled together.

Because of the smallest distributable resource unit is RB in LTE, the sensing result is added up by 180 kHz (one RB). If there are more than 12 continuous RBs are usable, the spectrum is marked as usable, as in Fig. 3. The spectrum band is integer multiple for 180 kHz, which is consistent with LTE.

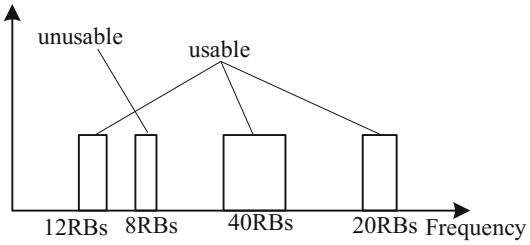


Fig. 3. Band more than 12 continuous RBs is usable.

If the available frequency spectrum is larger than 20 MHz, it should be split into several parts, and each part is at most 20 MHz.

3.2 Synchronization and Channel Estimation

Synchronization is important in communication systems and there are 2 synchronization symbols in LTE, which are PSS and SSS. The PSS, SSS and packet broadcast channel (PBCH) are all occupied 6 RBs, so the least usable band is 1.08 MHz.

The interference minimum channel is selected as the "main channel", and the PSS, SSS and the PBCH are arranged here, which is the "center frequency" such as LTE. See Fig. 4, the "center frequency" of irregular CA is in the center of the "best" channel. And in the PBCH, frequency bandwidth and center of the other channels are broadcast.

Channel estimation is different in LTE and irregular CA system, because the spectrum is discontinuous and irregular. The pilot arrangement scheme is not the same as the OFDM in LTE, see as Fig. 5. In irregular CA system, the pilot should consider the irregular band.

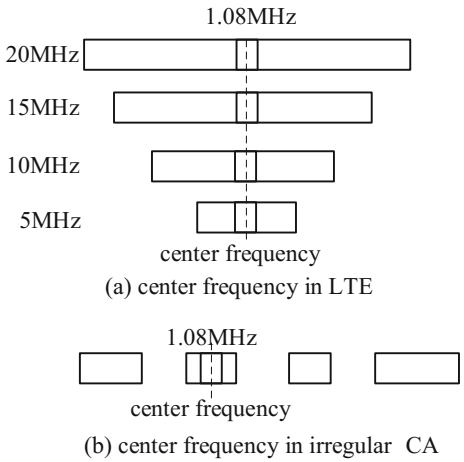


Fig. 4. The "center frequency" of irregular CA is in the center of the "best" channel.

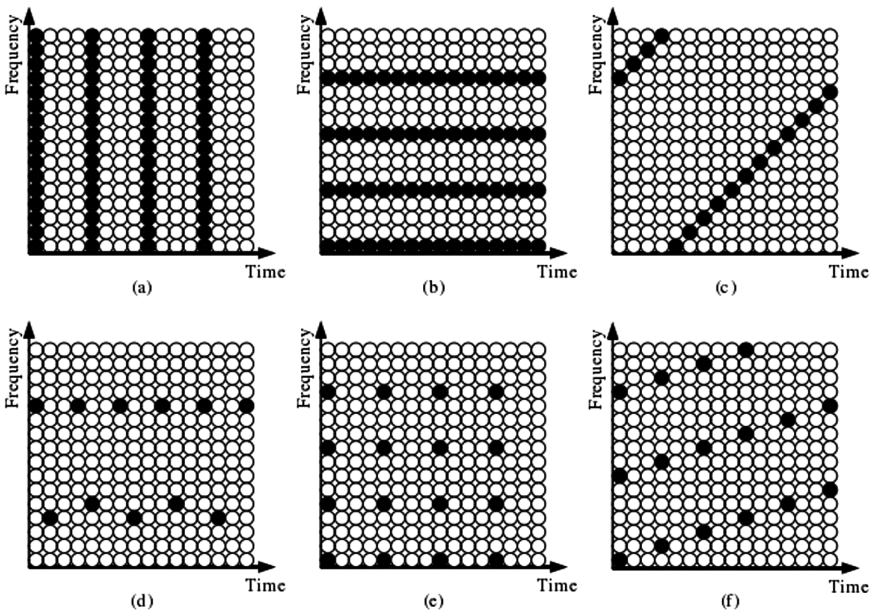


Fig. 5. The comb-type pilot, block-type pilot, equal interval pilot in OFDM

3.3 Resource Allocation

Under carrier aggregation, resource scheduling gets more complicated for the existence of multiple carriers. On the other hand, since a Quality-of-Service (QoS) protection mechanism has been adopted, the QoS-based resource scheduling has become a very important research direction [5].

Distinguish from the CA in LTE-A, in irregular CA, the resource allocation should consider UE's complexity. UE occupies as few as possible frequency band in addition to the band contains "center frequency". For each UE, it can work at least occupying 2 bands.

Fairness and throughput should be considered, each UE should retain minimum bandwidth to transmit high priority service.

Hybrid algorithm should be used and the amount of CA, Fairness and throughput are all should be considered. An evaluation function can be proposed, which is like that

$$F = a * N_{CA} + b * Throu + c * Fair. \quad (1)$$

Here, a, b and c are coefficient, N_{CA} is carrier number of one UE, Throu is throughput of the system, Fair is fairness factor.

4 Conclusion

In this paper, an irregular CA scheme is introduced in complex electromagnetic environment, when there is no continuous 5 MHz or 20 MHz spectrum. There are some differences between irregular CA and CA in LTE-A. In order to consistent with LTE, spectrum band more than 1.08 MHz can be used. NC-OFDM can be combined to irregular CA in the future, which can use narrower spectrum band, such as 180 kHz.

References

1. Abyaneh, M.A., Huyart, B., Cousin, J.-C.: Carrier aggregation of three OFDM signals using a single oscillator and I/Q modulator. IEEE Trans. Microw. Theory Tech. **65**(9), 3351–3359 (2017)
2. Tsinos, C.G., Foukalas, F., Tsiftsis, T.A.: Resource allocation for licensed/unlicensed carrier aggregation MIMO systems. IEEE Trans. Commun. **65**(9), 3765–3779 (2017)
3. Li, D., Dai, X., Zhang, H.: Sidelobe suppression in NC-OFDM systems using constellation adjustment. IEEE Commun. Lett. **13**(5), 327–329 (2009)
4. Xu, G., Zhu, Y.W., Han, M.: Broadband cognitive radio transmission based on sub-channel sensing and NC-OFDM. Int. J. Commun. Netw. Inf. Secur. **2**(2), 98–102 (2010)
5. Zheng, Y.: Research on resource scheduling for LTE-A carrier aggregation. Dissertation for the Master's Degree of Harbin Institute Technology (2013, in Chinese)

Performance Analysis of Frequency Division Multiplex Complementary Coded CDMA Systems

Siyue Sun[1(✉)], Kun Wang[2], Guang Liang[1], Feng Tian[1], and Zaiyang Jiang[1]

[1] Shanghai Engineering Center for Micro-satellites, Shanghai, China
sunsiyue@hit.edu.cn
[2] Huawei Technologies Co., Ltd., Shanghai, China

Abstract. As a kind of two-dimensional spreading codes, complementary codes (CCs) are able to provide ideal correlation properties, which is an attractive feature for CDMA systems to eliminate multiple access interference (MAI) and multi-path interference (MPI). Based on modeling the frequency selective fading channel for a kind of frequency division multiplex (FDM) CC-CDMA system, this paper provides a detailed performance analysis of such kind of CC-CDMA systems and proves the limits of channel conditions for the interference-free character of such systems, which is verified by the simulated results at the end of this paper.

Keywords: Complementary codes · CDMA · Correlation properties
Multiple access interference · Multi-path interference

1 Introduction

As one of the most popular multiple access techniques in the past 50 years, Code Division Multiple Access (CDMA) provides higher frequency efficiency and security with lower radiation for wireless communications. However, due to its interference-limited problem, CDMA has lost competitiveness compared with Orthogonal Frequency Division Multiplexing Access (OFDMA) in ground cellular systems, although it is still the preferred multiple access technique in satellite communications.

It has been widely approved that all existing CDMA systems are interference-limited, particularly in the presence of multiple access interference (MAI) and multi-path interference (MPI) due to the undesirable properties of the spreading sequences. In order to improve the performance of CDMA technique, [1–3] proposed a new kind of spreading sequences — complementary codes (CCs) which

This work was partly supported by National Nature Science Foundation Program of China (No. 61601295), Shanghai Sailing Program (16YF1411000) and CAS Innovation Fund (No. CXJJ-16S033).

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 319–327, 2018.
https://doi.org/10.1007/978-3-319-90802-1_28

are able to realize both idea auto- and cross- correlation properties relying on the two-dimensional code structure and the definition of complementary correlation.

Owing to such desired properties, the complementary coded CDMA (CC-CDMA) system has become one of the research hotspots, especially during discussing the candidates for 4G cellular systems. In [4], we have present a survey on the history of CCs and a deeply studies on the correlation properties of CCs with realistic communication environment was presented in [6]. However, the two-dimensional code structure and definition of complementary correlation make it hard to implement a CC-CDMA architecture. In [5], we have divided the existing CC-CDMA solutions into two categories according to the kinds of independent sub-channels and compared them in terms of resist of MAI and MPI, implementation complexity and spread and spectrum efficiency. In the last decade, CC-CDMA systems have been widely studied and reported by a large number of works [8–12] which showed their superior performance compared with the traditional CDMA systems. However, the desired interference-free features of CC-CDMA relies mainly on the same fading pattern on each sub-channel, which is almost impossible in realistic communication environment.

In this paper, based on modeling the frequency selective fading channel for a kind of frequency division multiplex (FDM) CC-CDMA systems, a detailed performance analysis of such kind of CC-CDMA systems is provided and the paper will prove the limits of channel conditions for the interference-free character of such systems, which will be verified by the simulated results at the end of this paper. The analysis and simulated work in this paper will provide theoretical bases and new ideas for future research work.

2 Definitions

2.1 Definitions of Complementary Codes

A family of CCs is denoted as $\mathcal{C}(K, M, N)$ which contents K CCs each with M element sequences. A CC can be represented by a $M \times N$ matrix $\mathbf{C}^{(k)}$, which is unfold as

$$\mathbf{C}^{(k)} = \begin{bmatrix} \mathbf{c}_0^{(k)} \\ \mathbf{c}_1^{(k)} \\ \vdots \\ \mathbf{c}_{M-1}^{(k)} \end{bmatrix} = \begin{bmatrix} c_{0,0}^{(k)} & c_{0,1}^{(k)} & \cdots & c_{0,N-1}^{(k)} \\ c_{1,0}^{(k)} & c_{1,1}^{(k)} & \cdots & c_{1,N-1}^{(k)} \\ \vdots & \vdots & \ddots & \vdots \\ c_{M-1,0}^{(k)} & c_{M-1,1}^{(k)} & \cdots & c_{M-1,N-1}^{(k)} \end{bmatrix},$$

where $c_{m,n}^{(k)} \in \{1, -1\}$, $k \in \{0, 1, \cdots, K-1\}$, $n \in \{0, 1, \cdots, N-1\}$, and $m \in \{0, 1, \cdots, M-1\}$. M is called flock size and N is the code length. In a CC-CDMA system, MN is the "congregated length" of a CC, and it determines the corresponding processing gain.

2.2 Definitions of the Complementary Correlation

The correlation properties of CCs are characterized by the complementary aperiodic correlation function which is calculated as the sum of the aperiodic correlation functions of all element sequences with the same delay τ, or

$$\rho\big(\mathbf{C}^{(k_1)}, \mathbf{C}^{(k_2)}; \tau\big) = \sum_{m=1}^{M} \phi\big(\mathbf{c}_m^{(k_1)}, \mathbf{c}_m^{(k_2)}; \tau\big) \tag{1}$$

where $\mathbf{C}^{(k_1)}, \mathbf{C}^{(k_2)} \in \mathcal{C}(K, M, N)$, $k_1, k_2 \in \{1, 2, \cdots, K\}$, and $\phi\big(\mathbf{c}_m^{(k_1)}, \mathbf{c}_m^{(k_2)}; \tau\big)$ is the aperiodic correlation function of $\mathbf{c}_m^{(k_1)}$ and $\mathbf{c}_m^{(k_2)}$. When $k_1 = k_2$, (1) is the complementary aperiodic auto-correlation function (ACF); otherwise, it gives the complementary aperiodic cross-correlation function (CCF).

A CC is said to be perfect if and only if its ACF is a delta function. A set of perfect CCs are considered to be perfect, if and only if the CCF of any two CCs is a zero function. The correlation properties of a perfect set of CCs, $\mathcal{C}(K, M, N)$, which are also called ideal correlation properties throughout this paper, can be expressed as

$$\rho(\mathbf{C}^{(k_1)}, \mathbf{C}^{(k_2)}; \tau) = \begin{cases} MN, & k_1 = k_2 \text{ and } \tau = 0 \\ 0, & \text{elsewhere} \end{cases} \tag{2}$$

where $\forall k_1, k_2 \in \{1, \cdots, K\}$.

3 System Model and Performance Analysis

3.1 The Transmitter Mode

In this paper, a kind of FDM CC-CDMA system [7] will be studied. A family of CCs $\mathcal{C}(K, M, N)$ is employed as the spreading codes for a system with K users and let $\mathbf{C}^{(k)}$ be the spreading code for user k. The transmitter mode of an FDM CC-CDMA system is shown in Fig. 1.

The original data is serial/parallel conversed into $b^{(k,1)}, b^{(k,2)}, \cdots, b^{(k,N)}$. Then the N streams of data are spread by the same CC and they are summed after delayed different number of chips latency.

The spreading wave of mth element code of user k is

$$C_m^{(k)}(t) = \sum_{n=1}^{N} c_{m,n}^{(k)} q(t - nT_c + T_c) \tag{3}$$

where, $q(t) = \frac{1}{\sqrt{MNT_c}}$, $0 \le t < T_c$, T_c is the chip duration. Let $b^{(k,\eta)}(i)$ be the ith BPSK symbol of ηth stream of data after S/P operation, $\eta \in \{1, 2, \cdots, N\}$, $i \in \{0, 1, \cdots, B-1\}$ and B is the length of each stream of data burst. Then the spread signal after delayed $\eta - 1$ chips latency is

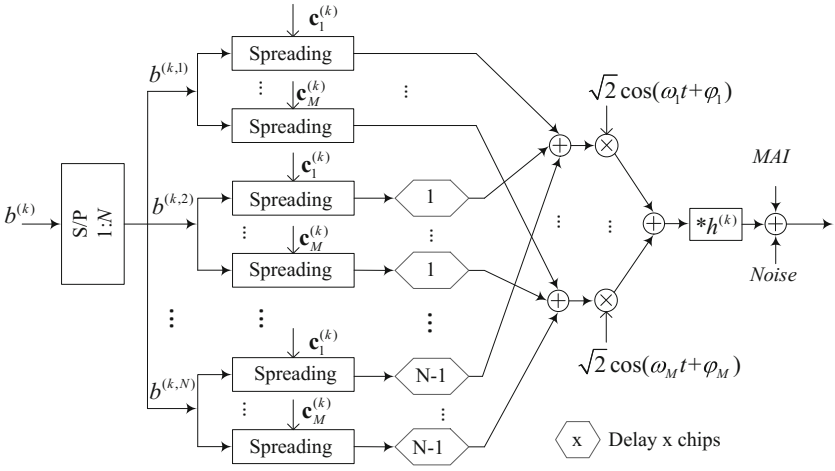


Fig. 1. The transmitter mode of parallel frequency-division-multiplexed CC-CDMA systems.

$$s_m^{(k,\eta)}(t) = \sqrt{p_t} \sum_{i=0}^{B-1} b^{(k,\eta)}(i) C_m^{(k)} \left[t - iT_b - (\eta - 1)T_c \right] \tag{4}$$

where, p_t is the transmitting power, $T_b = NT_c$ is the bit duration.

As shown in Fig. 1, combine the above N streams of data, we get

$$s_m^{(k)}(t) = \sum_{\eta=1}^{N} s_m^{(k,\eta)}(t) \tag{5}$$

Finally, the M combined signal will be modulated on M sub-carriers, as

$$s^{(k)}(t) = \sum_{m=1}^{M} s_m^{(k)}(t) \sqrt{2} \cos(\omega_m t + \varphi_m) \tag{6}$$

3.2 The Receiver Mode

In this paper, a tap-delay-line model is used to describe the multi-path channel and we get

$$\begin{aligned} r(t) &= \sum_{k=1}^{K} \Gamma_k h^{(k)}(t) * s^{(k)}(t) \\ &= \sqrt{2} \sum_{l=1}^{L} \sum_{k=1}^{K} \sum_{m=1}^{M} \Gamma_k h_l^{(k)} s_m^{(k)}(t - \tau_{k,l}) \cos \left[\omega_m (t - \tau_{k,l}) + \widehat{\varphi}_m \right] \end{aligned} \tag{7}$$

where Γ_k is channel coefficient of user k, $h_l^{(k)}$ and $\tau_{k,l}$ denote the channel coefficient and the time delay of lth channel.

Assuming ideal carrier-synchronization, the received signal on ω_ith sub-carrier is coherent demodulated in the receiver, as

$$r_i(t) = \left\{ r(t) \cdot \sqrt{2}\cos(\omega_i t + \widehat{\varphi}_i) \right\}_{LPF} = \sum_{l=1}^{L} \sum_{k=1}^{K} \sum_{m=1}^{M} \Gamma_k h_l^{(k)} s_m^{(k)}(t - \tau_{k,l}) \cos(\omega_i \tau_{k,l}) \tag{8}$$

where $\{\cdot\}_{LPF}$ means low pass filtering. Therefore, the equivalent baseband multi-path channel model is

$$h_m^{(k)}(t) = \sum_{l=1}^{L} h_l^{(k)} \cos(\omega_m \tau_l)\delta(t - \tau_{k,l}) = \sum_{l=1}^{L} h_{l,m}^{(k)} \delta(t - \tau_{k,l}) \tag{9}$$

This paper considers an asynchronous multi-path channel with each sub-band suffering flat fading. Based on such channel condition, the carrier-demodulated signal from sub-carrier m can be written as

$$r_m^{(g)}(t) = \sum_{k=1}^{K} \Gamma_k h_m^{(k)} s_m^{(k)}(t - \tau_k) + n_m(t) \tag{10}$$

where $n_m(t)$ is the complex additive white Gaussian noise with the power spectrum density N_0 which is independent over M sub-carriers. The receiver mode of such CC-CDMA system is shown in Fig. 2.

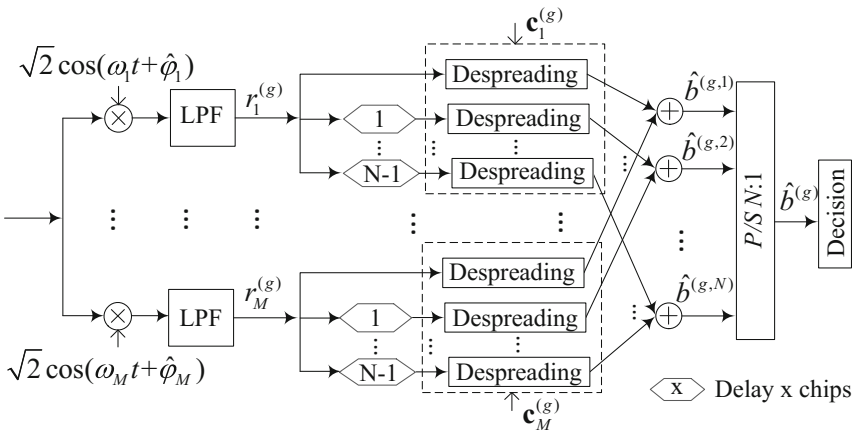


Fig. 2. The receiver mode of parallel frequency-division-multiplexed CC-CDMA systems.

Step 1. De-spreading (assuming ideal carrier-, bit- and chip-synchronous)

$$
\begin{aligned}
y_m^{(g,\eta')}(j) &= \int_0^{NT_c} r_m^{(g)}\big[t + jT_b + (\eta'-1)T_c + \tau_g\big] C_m^{(g)}(t)dt \\
&= \int_0^{NT_c} \sum_{k=1}^{K}\sum_{\eta=1}^{N} \Gamma_k h_m^{(k)} s_m^{(k,\eta)}\big[t + jT_b + (\eta'-1)T_c + \tau_g - \tau_k\big] C_m^{(g)}(t)dt + v_m \\
&= \sum_{k=1}^{K}\sum_{\eta=1}^{N}\sum_{i=0}^{B-1} \int_0^{NT_c} C_m^{(k)}\big[t + (j-i)T_b + (\eta'-\eta)T_c + \tau_g - \tau_k\big] C_m^{(g)}(t)dt \\
&\times \sqrt{p_t}\Gamma_k h_m^{(k)} b^{(k,\eta)}(i) + v_m \\
&= \frac{1}{M}\sqrt{p_t}\Gamma_g h_m^{(g)} b^{(g,\eta')}(j) + I_m^{(g)} + I_m^{(K)} + v_m
\end{aligned} \tag{11}
$$

where $v_m = \int_0^{NT_c} n_m(t) C_m^{(g)}(t)dt$ is the noise, $I_m^{(g)}$ is the interference from η'th stream of signal of user g on mth subcarrier, as

$$
\begin{aligned}
I_m^{(g)} =& \sqrt{p_t}\Gamma_g \sum_{\eta=1,\eta\neq\eta'}^{N} h_m^{(g)} b^{(g,\eta)}(j) \frac{1}{MN}\phi(\mathbf{c}_m^{(g)}, \mathbf{c}_m^{(g)}; \delta_\eta) \\
&+ \sqrt{p_t}\Gamma_g \sum_{\eta=1,\eta\neq\eta'}^{N} h_m^{(g)} b^{(g,\eta)}\big[j + \mathbf{sgn}(\delta_\eta)\big] \frac{1}{MN}\phi(\mathbf{c}_m^{(g)}, \mathbf{c}_m^{(g)}; N - \delta_\eta)
\end{aligned} \tag{12}
$$

where $\delta_\eta = \eta' - \eta$, $\mathbf{sgn}(x)$ equals to 1 when $x \geq 0$, and equals -1 when $x < 0$.

$I_m^{(K)}$ denotes the interference from other users on mth subcarrier, as

$$
I_m^{(K)} = \sum_{k=1,k\neq g}^{K}\sum_{\eta=1}^{N} \sqrt{p_t}\Gamma_k h_m^{(k)} \frac{1}{MN}\left\{\alpha_m^{(k,\eta)} b^{(k,\eta)}(j) + \beta_m^{(k,\eta)} b^{(k,\eta)}\big[j + \mathbf{sgn}(\delta_{k,\eta})\big]\right\}
$$

where $\delta_{k,\eta} = (\tau_g - \tau_k + \eta' - \eta)/T_c$.

$$
\begin{cases}
\delta_{k,\eta} > 0 : \alpha_m^{(k,\eta)} = \phi(\mathbf{c}_m^{(g)}, \mathbf{c}_m^{(k)}; \delta_{k,\eta}),\ \beta_m^{(k,\eta)} = \phi(\mathbf{c}_m^{(k)}, \mathbf{c}_m^{(g)}, N - \delta_{k,\eta}) \\
\delta_{k,\eta} < 0 : \alpha_m^{(k,\eta)} = \phi(\mathbf{c}_m^{(k)}, \mathbf{c}_m^{(g)}; -\delta_{k,\eta}),\ \beta_m^{(k,\eta)} = \phi(\mathbf{c}_m^{(g)}, \mathbf{c}_m^{(k)}, N + \delta_{k,\eta}) \\
\delta_{k,\eta} = 0 : \alpha_m^{(k,\eta)} = \phi(\mathbf{c}_m^{(g)}, \mathbf{c}_m^{(k)}; 0),\ \beta_m^{(k,\eta)} = 0
\end{cases} \tag{13}
$$

Step 2. Combination

$$
\begin{aligned}
\widehat{b}^{(g)}(j) &= \sum_{m=1}^{M} y_m^{(g,\eta')}(j) \\
&= \frac{\sqrt{p_t}}{M}\Gamma_g \sum_{m=1}^{M} h_m^{(g)} b^{(g,\eta')}(j) + \sum_{m=1}^{M} I_m^{(g)} + \sum_{m=1}^{M} I_m^{(K)} + \sum_{m=1}^{M} v_m \\
&= \frac{\sqrt{p_t}}{M}\Gamma_g \sum_{m=1}^{M} h_m^{(g)} b^{(g,\eta')}(j) + I^{(g)} + I^{(K)} + \omega
\end{aligned} \tag{14}
$$

where $I^{(g)}$, $I^{(K)}$ and ω are interference and noise respectively.

Step 3. Despreading and combination with different chip delays according to step 1 and 2, and then after serial/parallel conversion, we get the decision signal.

4 Analysis on Interference-Elimination Performance

Simplify the interference in (11), we get

$$\begin{aligned} I^{(g)} =& \frac{\sqrt{p_t}\Gamma_g}{MN}\sum_{m=1}^{M}\sum_{\eta=1,\eta\neq\eta'}^{N} h_m^{(g)} b^{(g,\eta)}(j)\phi(\mathbf{c}_m^{(g)},\mathbf{c}_m^{(g)};\delta_\eta) \\ &+ \frac{\sqrt{p_t}\Gamma_g}{MN}\sum_{m=1}^{M}\sum_{\eta=1,\eta\neq\eta'}^{N} h_m^{(g)} b^{(g,\eta)}\left[j+\mathbf{sgn}(\delta_\eta)\right]\phi(\mathbf{c}_m^{(g)},\mathbf{c}_m^{(g)};N-\delta_\eta) \\ =& \frac{\sqrt{p_t}\Gamma_g}{MN}\sum_{\eta=1,\eta\neq\eta'}^{N}\left\{b^{(g,\eta)}(j)\Psi_1 + b^{(g,\eta)}\left[j+\mathbf{sgn}(\delta_\eta)\right]\Psi_2\right\} \end{aligned}$$

where $\Psi_1 = \sum_{m=1}^{M} h_m^{(g)}\phi(\mathbf{c}_m^{(g)},\mathbf{c}_m^{(g)};\delta_\eta)$, $\Psi_2 = \sum_{m=1}^{M} h_m^{(g)}\phi(\mathbf{c}_m^{(g)},\mathbf{c}_m^{(g)};N-\delta_\eta)$.

$$\begin{aligned} I^{(K)} &= \frac{\sqrt{p_t}}{MN}\sum_{m=1}^{M}\sum_{k=1,k\neq g}^{K}\sum_{\eta=1}^{N}\Gamma_k h_m^{(k)}\left\{\alpha_m^{(k,\eta)}b^{(k,\eta)}(j)+\beta_m^{(k,\eta)}b^{(k,\eta)}\left[j+\mathbf{sgn}(\delta_{k,\eta})\right]\right\} \\ &= \frac{\sqrt{p_t}}{MN}\sum_{k=1,k\neq g}^{K}\sum_{\eta=1}^{N}\Gamma_k\left\{b^{(k,\eta)}(j)\Psi_3 + b^{(k,\eta)}\left[j+\mathbf{sgn}(\delta_{k,\eta})\right]\Psi_4\right\} \end{aligned} \tag{15}$$

where $\Psi_3 = \sum_{m=1}^{M} h_m^{(k)}\alpha_m^{(k,\eta)}$, $\Psi_4 = \sum_{m=1}^{M} h_m^{(k)}\beta_m^{(k,\eta)}$.

Substitutes (13) into Ψ_3 and Ψ_4. Comparing $\Psi_1 \sim \Psi_4$ and (2), it is proved that when the channel is flat fading, i.e., $h_1^{(k)} = h_2^{(k)} = \cdots = h_M^{(k)}$, $k \in \{1,2,\cdots,K\}$, $\Psi_1 = \Psi_2 = \Psi_3 = \Psi_4 = 0$. Therefore, the interference $I^{(g)} = I^{(K)} = 0$ and we get

$$\widehat{b}^{(g)}(i) = \sqrt{p_t}\Gamma_g h^{(g)} b^{(g)}(i) + \sum_{m=1}^{M} v_m \tag{16}$$

Since $\{v_m\}_{m=1}^{M}$ are M dependent Gaussian random variables, their sum is also a dependent Gaussian random variable. Let $p_t = \frac{E_b}{MNT_c}$, $\Gamma_g = 1$, we get

$$\gamma_b = |h_g|^2 \frac{E_b}{N_0} \tag{17}$$

In Rayleigh channel, the probability density of γ_b is

$$p(\gamma_b) = \frac{1}{\overline{\gamma}_b} e^{-\gamma_b/\overline{\gamma}_b} \tag{18}$$

where $\overline{\gamma}_b = \frac{E_b}{N_0}$ is the average signal-noise ratio. We can get the corresponding bit error rate (BER) as

$$P_2(\gamma_b) = \int_0^{\infty} Q(\sqrt{2\gamma_b}) p(\gamma_b) d\gamma_b = \frac{1}{2}\left[1 - \sqrt{\frac{E_b/N_0}{1 + E_b/N_0}}\right] \tag{19}$$

Then we compared the BER performance of CDMA systems with different spreading codes, as shown in Fig. 3. $NFR = 20lg(\Gamma_k/\Gamma_g)$ denotes the near-far effect.

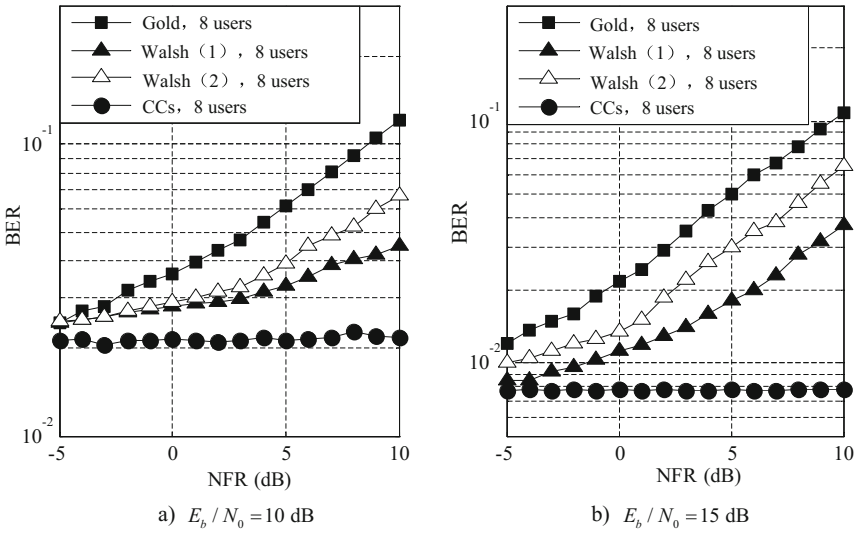


Fig. 3. Influence of near-far effect on BER of CDMA systems with three different codes.

As can be seen in Fig. 3, the CC-CDMA system performs better than that with traditional spreading codes, especially with serious near-far effect. However, when the channel is frequency selective fading, i.e., $h_1^{(k)}, h_2^{(k)}, \cdots, h_M^{(k)}$ are not equal, the equal gain combination defined in (2) can not be realized. Therefore, none of Ψ_1, Ψ_2, Ψ_3 and Ψ_4 equal to zero and CC-CDMA will suffer self-interference $I^{(g)}$ and MAI $I^{(K)}$ over the frequency selective fading channels.

5 Conclusions and Discussions

This paper has present a detailed analysis of an FDM CC-CDMA system and proves the limits of channel conditions for the interference-free character of such system. As can be seen from the analytical work, we get the conditions of the interference-free feature of CC-CDMA systems. As for the future work, we will study on new combining algorithms for such system to improve its performance over such frequency selective fading channels.

References

1. Golay, M.: Complementary series. IRE Trans. Inf. Theory **7**(2), 82–87 (1961)
2. Tseng, C.-C., Liu, C.L.: Complementary sets of sequences. IEEE Trans. Inf. Theory **18**(5), 644–652 (1972)
3. Suehiro, N., Hatori, M.: N-shift cross-orthogonal sequences. IEEE Trans. Inf. Theory **34**(1), 143–146 (1988)
4. Sun, S.-Y., Chen, H.-H., Meng, W.: A survey on complementary-coded MIMO CDMA wireless communications. IEEE Commun. Surv. Tutor. **17**(1), 52–69 (2015). Please check and approve the edit made in the article title in Ref. [4]
5. Sun, S., Han, S., Yu, Q., Meng, W., Li, C.: A survey of two kinds of complementary coded CDMA wireless communications. In: 2014 IEEE Global Communications Conference, pp. 468–472 (2014)
6. Sun, S., Liang, G., Wang, K.: Study on correlation properties of complementary codes and the design constraints of complementary coded CDMA systems. In: Gu, X., Liu, G., Li, B. (eds.) MLICOM 2017. LNICST, vol. 227, pp. 61–70. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-73447-7_8
7. Turyn, R.: Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings. J. Comb. Theory Ser. A **16**(3), 313–333 (1974)
8. Chen, H.-H., Zhang, H.-M., Huang, Z.-K.: Code-hopping multiple access based on orthogonal complementary codes. IEEE Trans. Veh. Technol. **61**(3), 1074–1083 (2012)
9. Chenggao, H., Suehiro, N., Hashimoto, T.: A systematic framework for the construction of optimal complete complementary codes. IEEE Trans. Inf. Theory **57**(9), 6033–6042 (2011)
10. Chen, H.-H., Yeh, J.-F., Suehiro, N.: A multicarrier CDMA architecture based on orthogonal complementary codes for new generations of wideband wireless communications. IEEE Commun. Mag. **39**(10), 126–135 (2001)
11. Suehiro, N., Kuroyanagi, N., Imoto, T., Matsufuji, S.: Very efficient frequency usage system using convolutional spread time signals based on complete complementary code. In: Proceedings of the PIMRC, vol. 2, pp. 1567–1572 (2000)
12. Lu, L., Dubey, V.: Performance of a complete complementary code-based spread-time CDMA system in a fading channel. IEEE Trans. Veh. Technol. **57**(1), 250–259 (2008)

A Novel Optical Index Modulation Aided DCO-OFDM Scheme for VLC Systems

Haodong Li[1], Jian Sun[1], Wensheng Zhang[1(✉)], and Cheng-Xiang Wang[2]

[1] School of Engineering, School of Information Science and Engineering, Institute of Sensors, Signals and Systems, Shandong University, Jinan 250100, Shandong, People's Republic of China
392467887@qq.com, {sunjian,zhangwsh}@sdu.edu.cn
[2] Physical Sciences, Heriot-Watt University, Edinburgh EH14 4AS, UK
cheng-xiang.wang@hw.ac.uk

Abstract. In this paper, a novel optical index modulation (OIM) aided direct-current (DC) biased optical OFDM (OIM-DCO-OFDM) scheme for visible light communication (VLC) systems is proposed. Different with traditional index modulation schemes, the proposed OIM-DCO-OFDM scheme uses index bits to determine which subcarrier transmit original signals and which subcarrier transmit conjugate signals. The constellation of traditional phase-shift keying (PSK) and quadrature amplitude modulation (QAM) is symmetrical about the real axis. It means that we cannot distinguish the original signals and conjugate signals. In order to recover index bits at the receiver, we propose a unipolar pulse amplitude modulation (PAM) scheme for the modulation of constellation bits, and design a zero-forcing (ZF) based detector. Compared with dual-mode index modulation aided DCO-OFDM (DM-DCO-OFDM) scheme, the proposed scheme has 1 dB and 2 dB performance gain at the bit error rate (BER) level of 10^{-4} when the spectral efficiency is 1.21 bits/s/Hz and 2.18 bits/s/Hz, respectively. The proposed OIM-DCO-OFDM scheme can achieve 80% spectral efficiency improvement than the DM-DCO-OFDM scheme at the modulation order of $M = 4$.

Keywords: Visible light communication · Optical index modulation
DC-biased optical OFDM · PAM

1 Introduction

VLC is a green communication technology without electromagnetic interference by using light-emitting diodes (LEDs) and photodiodes (PDs) to transmit and receive information. Moreover, VLC has many other advantages compared with radio frequency communication, such as wide bandwidth with no license application, energy efficiency and low deployment cost [1,2].

Orthogonal frequency division multiplexing (OFDM) has been widely used in radio frequency communication because it can combat the inter-symbol interference (ISI) effectively. OFDM has been used in VLC [3,4]. Since the signal only

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 328–337, 2018.
https://doi.org/10.1007/978-3-319-90802-1_29

can be transmitted by the intensity of light and no phase can be transmitted simultaneously, conventional OFDM cannot be adopted in VLC. Many optical OFDM schemes have been proposed, such as DC-biased optical OFDM (DCO-OFDM) [5], asymmetrically clipped optical OFDM (ACO-OFDM) [6], unipolar OFDM (U-OFDM) [7] and Flip-OFDM [8]. All of the above schemes make use of Hermitian symmetry to create real signal before IFFT operation. Thus a half of carriers cannot transmit efficient signals, which leads to low spectral efficiency.

IM was recently studied for 5G wireless communication systems in [9]. Recently, optical OFDM-IM (O-OFDM-IM) scheme was proposed [10]. Compared with traditional optical OFDM schemes, O-OFDM-IM scheme transmits the information bits by the M-ary signal constellation and the indices of subcarriers. The subcarriers are divided into G groups. For each group, the subcarriers are activated by index bits to transmit constellation signals. It means that some subcarriers transmit nothing. The O-OFDM-IM scheme represents better performance compared with classical DCO-OFDM and ACO-OFDM. However, the O-OFDM-IM scheme has a low spectral efficiency since not all the subcarriers are used to transmit constellation signals.

Motivated by the O-OFDM-IM scheme, authors of [11] proposed a dual-mode index modulation aided DC-biased optical OFDM (DM-DCO-OFDM) scheme. Same as O-OFDM-IM, DM-DCO-OFDM divides the subcarriers into two parts according to different index bits, and this two parts of subcarriers transmit different constellation mapping signals. After index modulation, the OFDM block is created. By using Hermitian symmetry operation and adding DC-bias, complex signals can be translated to real and positive signals. Finally, the unipolar signals are transmitted by LEDs. Compared with DCO-OFDM scheme, the DM-DCO-OFDM scheme achieves higher spectral efficiency and improves BER performance significantly. DM-DCO-OFDM has higher spectral efficiency than O-OFDM-IM. The reasons are that all subcarriers are used to transmit constellation signals in DM-DCO-OFDM.

In this paper, we propose a novel optical index modulation aided DC-biased optical OFDM scheme. In the OIM-DCO-OFDM scheme, the index bits are used to determine which subcarriers transmit original signals or their conjugate signals. Because the constellation of the conventional M-ary modulation schemes such as PSK and QAM, are symmetrical about the real axis. In other words, index bits are not recovered by distinguishing transmitted the original signals and their conjugate signals at the receiver. In order to detect index bit effectively, we employ unipolar PAM to map constellation bits. After PAM mapping operation, every two unipolar PAM signals constitute a complex signal. Only the real and unipolar signals can be transmitted in the VLC system, so we use Hermitian symmetry operation to get real signals. After adding DC-bias, the generated real and non-negative signals can be transmitted by LEDs. At the receiver, we design a low computational complexity detector which is called ZF based detector. After obtaining estimated signals by ZF estimator, the index bits can be recovered by judging the sign of the imaginary part of received signals, and constellation bits can be demodulated by unipolar PAM de-mapping. The

simulation results confirm that the proposed scheme has significant BER performance gains compared with the DM-DCO-OFDM scheme at the same spectral efficiency. Under the condition of same modulation order, the proposed scheme has higher spectral efficiency improvement than DM-DCO-OFDM.

The rest of this paper is organized as follows. In Sect. 2, the system model of DM-DCO-OFDM is reviewed. The OIM-DCO-OFDM system model is presented in Sect. 3. The simulation results and spectral efficiency analysis are given in Sect. 4. Section 5 shows the conclusions.

2 Review of DM-DCO-OFDM

In DM-DCO-OFDM, N subcarriers are divided into G groups, each group contains n subcarriers and p_{DM} bits, $p_{DM} = p_1 + p_2$. p_1 bits are fed into index selector to determine index pattern and p_2 bits are modulated by two different constellations, M_{A}-ary A and M_{B}-ary B. For each group, k subcarriers out of n subcarriers are selected to transmit the constellation A signals, and other $n-k$ subcarriers transmit the constellation B signals. The transmitted bits in each group can be calculated by $p_{DM} = \lfloor \log_2 (C(n,k)) \rfloor + k\log_2(M_A) + (n-k)\log_2(M_B)$, where $\lfloor \rfloor$ is the floor function, $C(n,l)$ is the binomial coefficient. Noted that the symbol of constellation A and constellation B should be differentiated with each other. Otherwise, the index bits cannot be recovered at the receiver, which will lead to bad BER performance. After index modulation and constellation mapping, Hermitian symmetry operation is used to obtain real signals before IFFT operation. The Hermitian symmetry property can be represented by

$$\begin{cases} X_i = X_{N-i}^*, 0 < i < N/2 \\ X_0 = X_{N/2} = 0 \end{cases} \tag{1}$$

where $X_i \in \mathbf{X}$, $\mathbf{X} = [X_0, X_1, \ldots, X_{N-1}]$ is the frequency-domain complex signals after constellation mapping. Then IFFT and parallel-to-serial operation are employed to generate time-domain signal. Finally, a suitable DC-bias should be added on the time-domain signals to create unipolar signals, i.e., only the time-domain unipolar signals can be transmitted via LEDs. At the receiver side, the reverse operations are used to obtain transmitted frequency-domain signals. The maximum likelihood detector or the log-likelihood ratio detector can be selected to recover index bits and constellation bits.

3 System Model of OIM-DCO-OFDM

Motivated by DM-DCO-OFDM, the proposed OIM-DCO-OFDM scheme also uses all of subcarriers to transmit signals, which can achieve higher spectral efficiency than O-OFDM-IM scheme. The block diagram of OIM-DCO-OFDM transceiver is given in Fig. 1 For each OFDM block, m bits and N carriers are divided into G groups, each group contains p bits and n subcarriers i.e., $m = pG$, $N = nG$. For each group, p bits are split into three parts, p_1, p_2 and

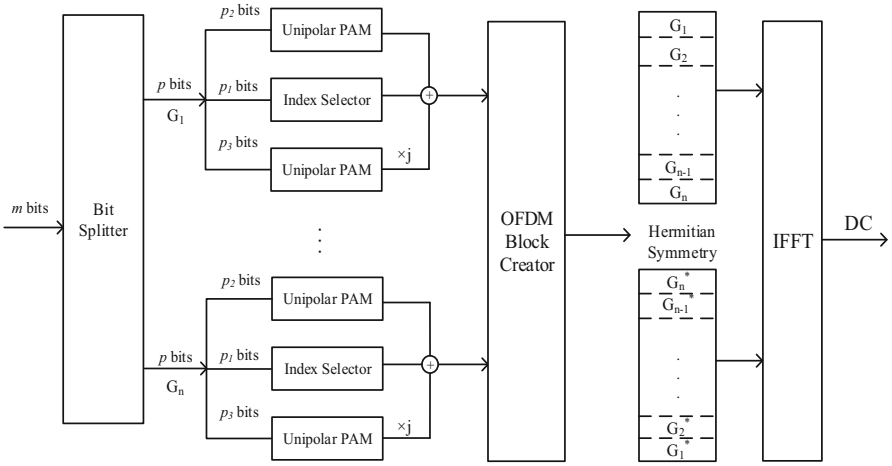


Fig. 1. The block diagram of the OIM-DCO-OFDM transmitter.

p_3, i.e., $p = p_1 + p_2 + p_3$. The index bits p_1 are fed into index selector to choose l subcarriers from n subcarriers, and these l subcarriers will transmit original signals while other $n - l$ subcarriers will transmit conjugate signals. Then p_1, p_2 and p_3 can be calculated by

$$p_1 = \lfloor \log_2 (C(n, l)) \rfloor \tag{2}$$

$$p_2 = p_3 = n \log_2 (M) \tag{3}$$

where M is the modulation order of unipolar PAM. The bits p entered into each group can be calculated by

$$p = \lfloor \log_2 (C(n, l)) \rfloor + 2n \log_2 (M). \tag{4}$$

Noted that the index bits cannot be detected successfully if use QAM or PSK to modulate constellation bits. Because conventional PSK and QAM constellation symbols are symmetrical about the real axis, it cannot distinguish original signals and its conjugate signals at the receiver, where we use the difference between original constellation signals and their conjugate signals to transmit index bits. In order to recover index bits, we use two unipolar PAM symbols to form a complex signal. p_2 and p_3 are modulated by unipolar M-ary PAM constellation. The unipolar PAM constellation symbols are denoted as $\mathbf{S} = [S_1, S_2, \ldots S_M]$. Every two unipolar PAM symbols form a complex signal, i.e., $X = S_\alpha + jS_\beta$, $S_\alpha, S_\beta \in \mathbf{S}$. The conjugate signal of X can be represented by $X^* = S_\alpha - jS_\beta$.

In OIM-DCO-OFDM scheme, the look-up table method is used to index selected procedure [12]. We illustrate the implementation by an example. The initial settings are assumed that $M = 2$, $\mathbf{S} = [1, 3]$, $n = 4$ and $l = 2$. Calculating Eq. (4), we can get $p = \lfloor \log_2 (C(4, 2)) \rfloor + 2 * 4 * \log_2 (2) = 10$ bits. The index bits p_1 can be obtained by Eq. (2) and we can get that $p_1 = 2$. The look-up table is illustrated in Table 1, and the first column of the table denotes the combination of binary bits. The second column is the indices pattern I generated according to the input index bits, where "1" denotes the subcarriers transmitting original signals X and "0" denotes the subcarriers transmitting conjugate signals X^*. The last column is the signal subblocks which generated by index modulation. For example, if input bits are "1011011001", the index pattern can be determined by Table 1. The index bits are "10", which indicates that the index pattern is "1,0,0,1" which means that the first and the fourth subcarrier transmit the original signals X, and the rest of subcarriers transmit conjugate signals X^*. The rest of bits are modulated by unipolar PAM and the generated complex signal subblock is $[3 + 3j, 1 - 3j, 3 - 1j, 1 + 3j]$.

After index modulation and unipolar M-ary PAM mapping, the generated complex signal in γ-th subblock can be represented by

$$\mathbf{X}_\gamma = [X_{\gamma-1}, X_\gamma, \ldots, X_{\gamma+n-1}]^{\mathrm{T}}. \tag{5}$$

Since in VLC system only real and unipolar signals can be transmitted, Hermitian symmetry is used to generate real-value signal aforementioned in Eq. (1), which means that half of subcarriers transmit no information bits. Hence the spectral efficiency of OIM-DCO-OFDM can be calculated by $\eta = \frac{pG}{2N}$ bits/s/Hz and the spectral efficiency of DM-DCO-OFDM also can be obtained by this equation. After Hermitian symmetry operation, the frequency-domain signals in an OFDM block can be represented as

$$\mathbf{X} = [0, X_1, X_2, \ldots, X_{N-1}, 0, X_{N-1}^*, \ldots, X_2^*, X_1^*]^{\mathrm{T}}. \tag{6}$$

The real-value time-domain signals are obtained by IFFT operation of $\mathbf{X}$ and can be denoted as

$$\mathbf{x} = [x_1, x_2, \ldots, x_{2N}]^T. \tag{7}$$

Before transmitting signals by LEDs, a suitable DC-bias U_{DC} is adopted to obtain real and unipolar signals by

$$U_{DC} = \mu \sqrt{E\{(x_i)^2\}} \tag{8}$$

where $x_i \in \mathbf{x}$, μ is a proportionality constant, and U_{DC} is defined as a bias of $10\log_{10}(\mu^2 + 1)$ [13].

Figure 2 is the scenario model. In order to simplify the model, we only consider the line-of-sight (LOS) component [14]. The optical channel can be modeled as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}_{\mathrm{A}} \tag{9}$$

Table 1. A Look-up Table for OIM-DCO-OFDM with $n = 4$ and $l = 2$.

Index bits	Indices pattern	Subblocks
[0, 0]	[1, 1, 0, 0]	$[X, X, X^*, X^*]$
[0, 1]	[0, 1, 0, 1]	$[X^*, X, X^*, X]$
[1, 0]	[1, 0, 0, 1]	$[X, X^*, X^*, X]$
[1, 1]	[0, 1, 1, 0]	$[X^*, X, X, X^*]$

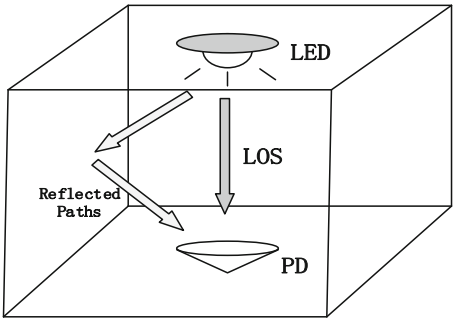


Fig. 2. The scenario model.

where $\mathbf{y} = [y_1, y_2, \ldots y_{2N}]$ is a received signal vector, $\mathbf{H}$ is the optical channel gain, and $\mathbf{n}_\mathrm{A}$ denotes $2N \times 1$ real-valued additive white Gaussian noise (AWGN) vector.

At the receiver, in order to recover index bits and information bits, we design a ZF based detector. Firstly, the ZF estimator is used to yield an estimation of $\mathbf{x}$ which can be obtained as

$$\hat{\mathbf{x}} = \mathbf{H}^{-1}\mathbf{y}. \tag{10}$$

Then, $\hat{\mathbf{x}}$ is fed into FFT operation and performs the inverse operation of Hermitian symmetry to obtain the frequency-domain estimated signal $\hat{\mathbf{X}}$. Secondly, the index pattern of ξ-th group can be determined by judging the sign of $\hat{\mathbf{X}}^\xi$ imaginary part, which can be represented by

$$I_i^\xi = \begin{cases} 1, \text{if Imag}(\hat{X}_i^\xi) \geq 0 \\ 0, \text{if Imag}(\hat{X}_i^\xi) < 0 \end{cases} \tag{11}$$

where $\text{Imag}(\hat{X}_i^\xi)$ denotes the imaginary part of $\hat{X}_i^\xi$. Then, inputting index pattern into the look-up table, the index bits p_1 can be recovered. The constellation bits p_2 and p_3 can be recovered by putting the real part and imaginary part of $\hat{\mathbf{X}}$ into unipolar M-PAM demodulator respectively. We summarize the step of the designed ZF based detector in Algorithm 1. The computational complexity of ZF based detector is about the order of $O(3n)$ per group.

Algorithm 1. ZF based detector for OIM-DCO-OFDM.

Input: Received signals $\mathbf{y}$, number of groups G, number of subcarriers in each group n, number of subcarriers modulated by original signals l.
Operation: Calculating the frequency-domain estimated signals $\mathbf{X}$ by Eq. (10), FFT and removing Hermitian symmetry operation.
Recovering index bits:
for $\xi = 1; \xi \leq G; \xi++$ **do**
  for $i = 1; i \leq n; i++$ **do**
    if $\mathrm{Imag}(X_i^{\xi}) \geq 0$ **then**
      $I_i^{\xi} = 1$
    else
      $I_i^{\xi} = 0$
    end
  end
  Input index pattern $\mathbf{I}_i^{\xi}$ to look-up table, index bit p_1 can be obtained.
end
Recovering constellation bits:
for $\xi = 1; \xi \leq G; \xi++$ **do**
  for $i = 1; i \leq n; i++$ **do**
    p_2 = demodulate the real part of X_i^{ξ}
    p_3 = demodulate the imaginary part of X_i^{ξ}
  end
end

4 Simulation Results and Analysis

In this section, the performance of the proposed OIM-DCO-OFDM scheme is validated. The simulation results are compared with the DM-DCO-OFDM scheme results under optical AWGN channel. The simulation parameter settings are same as [11]. The number of carriers is $N = 128$, and efficient carriers are split into $G = 31$ groups which contains $n = 4$ subcarriers. For each group, $l = 2$ subcarriers are selected to transmit original symbols, and the rest of subcarriers transmit conjugate originals. The size of IFFT is 256. The proportionality constant $\mu = 1.05$. The signal-to-noise ratio (SNR) is defined as E_b/N_0 in the OIM-DCO-OFDM scheme.

Figure 3 presents the BER performance comparison between OIM-DCO-OFDM and DM-DCO-OFDM in same spectral efficiency of 1.21 bits/s/Hz and 2.18 bits/s/Hz. When the spectral efficiency is 1.21 bits/s/Hz, the proposed scheme uses unipolar 2-PAM to modulate constellation bits, and the set of unipolar 2-PAM constellation can be represented by $\mathbf{S} = [1, 3]$. As for DM-DCO-OFDM scheme, the two distinguished QPSK constellation sets $\mathbf{S}_{\mathrm{A}}$ and $\mathbf{S}_{\mathrm{B}}$ are $[1+\mathrm{j}, -1+\mathrm{j}, -1-1\mathrm{j}, 1-\mathrm{j}]$ and $\left[1+\sqrt{3}, (1+\sqrt{3})\mathrm{j}, -1-\sqrt{3}, -(1+\sqrt{3})\mathrm{j}\right]$ [15]. The spectral efficiency is 2.18 bits/s/Hz, and the unipolar 4-PAM constellation set can be represented by $\mathbf{S} = [1, 3, 5, 7]$. For DM-DCO-OFDM scheme, the two distributed 16-QAM constellation sets $\mathbf{S}_{\mathrm{A}}$ and $\mathbf{S}_{\mathrm{B}}$ are $[3+3\mathrm{j}, 1+3\mathrm{j}, -1+3\mathrm{j}, -3+$

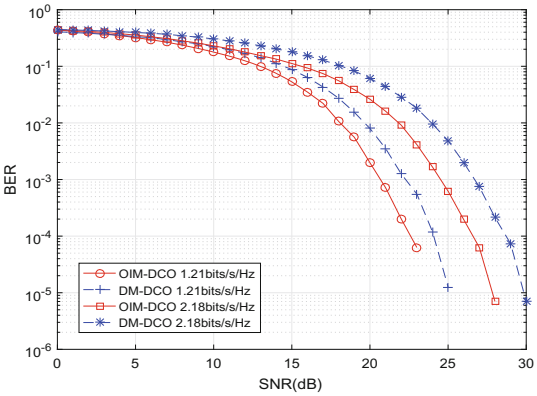


Fig. 3. Performance comparison of OIM-DCO-OFDM and DM-DCO-OFDM schemes under AWGN channels with the spectral efficiency of 1.21 bits/s/Hz and 2.18 bits/s/Hz.

3j, −3+j, −1+j, 1+j, 3+j, 3−j, 1−j, −1−j, −3−j, −3−3j, −1−3j, 1−3j, 3−3j] and [5 + j, 5 + 3j, 3 + 5j, 1 + 5j, −1 + 5j, −3 + 5j, −5 + 3j, −5 + j, −5 − j, −5 − 3j, −3 − 5j, −1 − 5j, 1 − 5j, 3 − 5j, 5 − 3j, 5 − j] [15]. We can observe from Fig. 3 that the proposed OIM-DCO-OFDM scheme has 1 dB and 2 dB performance gain over DM-DCO-OFDM scheme at the BER level of 10^{-4} when the spectral efficiency is 1.21 bits/s/Hz and 2.18 bits/s/Hz, respectively. The wrong recovered index bits have no impact on constellation bits recover at low SNR level. The index bits and constellation bits can be recovered successfully by the ideal ZF estimator at high SNR level. Other reason is the proposed scheme has low order constellation at same spectral efficiency with DM-DCO-OFDM, which is more robust to the noise. Therefore, the proposed scheme achieves better BER performance gains than DM-DCO-OFDM scheme.

Then, we focus on comparing the spectral efficiency between OIM-DCO-OFDM and DM-DCO-OFDM scheme. We assume both of two schemes have same system parameters and adopt the same subcarrier parameter settings. In the DM-DCO-OFDM scheme, the different signal constellations have same modulation order. As description in Sect. 3, the spectral efficiency can be obtained. Noted that the length of CP is not considered in spectral efficiency. In Fig. 4, the spectral efficiency between OIM-DCO-OFDM and DM-DCO-OFDM scheme are compared. At same modulation order, OIM-DCO-OFDM has higher spectral efficiency than DM-DCO-OFDM scheme. For example, the spectral efficiency of the proposed scheme is $\eta_{\mathrm{OIM}} = 2.18$ bits/s/Hz at the modulation order $M = 4$, while the spectral efficiency of DM-DCO-OFDM is $\eta_{\mathrm{DM}} = 1.21$ bits/s/Hz. The proposed scheme has 80% spectral efficiency improvement than DM-DCO-OFDM. Because the signals transmitted by each subcarrier in OIM-DCO-OFDM, are constituted by two unipolar M-ary PAM symbols, but DM-DCO-OFDM only transmit one M-ary QAM symbol. It means that proposed scheme can transmit twice information bits on per subcarriers than DM-DCO-OFDM scheme.

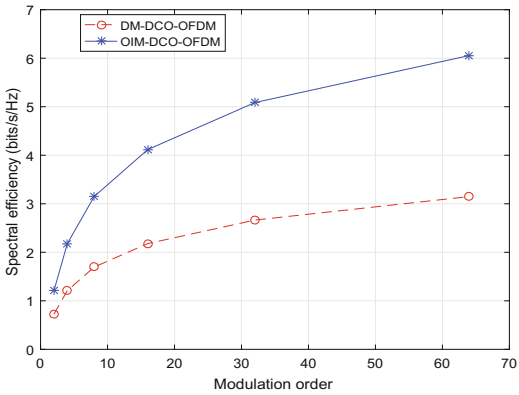


Fig. 4. Spectral efficiency comparison between OIM-DCO-OFDM and DM-DCO-OFDM schemes.

5 Conclusions

In this paper, a novel OIM-DCO-OFDM scheme has been proposed. Same as the DM-DCO-OFDM scheme, the proposed OIM-DCO-OFDM scheme have used all subcarriers to transmit constellation signals. But the index bits in the proposed scheme are used to select which subcarrier to transmit the original signals or their conjugate signals. Since conventional PSK and QAM constellation schemes are symmetry about the real axis, they cannot be used in the proposed scheme. In order to recover index bits at the receiver, we have used two unipolar PAM symbols to constitute a complex signal. Generated complex signals and their conjugate signals can easily be distinguished by the sign of the imaginary part of signals. After index selection and constellation mapping, Hermitian symmetry operation and DC-bias have been adopted to translate bipolar complex signals to unipolar real signals. Then, the generated unipolar real signals can be transmitted by the LEDs. At the receiver, a ZF based detector has been designed for demodulation of index bits and constellation bits. It has been demonstrated via simulations that the proposed OIM-DCO-OFDM scheme has a performance gain compared with the conventional DM-DCO-OFDM scheme at the same spectral efficiency of 1.21 bits/s/Hz and 2.18 bits/s/Hz under AWGN channels. Moreover, we have analyzed the system spectral efficiency of the proposed scheme and DM-DCO-OFDM scheme. The proposed scheme can achieve 80% more spectral efficiency gain than the DM-DCO-OFDM scheme when the modulation order equals to four. In the future, we will investigate the upper bound of the BER of the proposed scheme as well as analyze the performance of OIM-DCO-OFDM under actual communication environments.

Acknowledgement. The authors gratefully acknowledge the support from Natural Science Foundation of China (No. 61371110), Fundamental Research Funds of Shandong University (No. 2017JC029), Key R&D Program of Shandong Province

(No. 2016GGX101014), Shandong Provincial Natural Science Foundation (No. ZR2017MF012), Science and Technology Project of Guangzhou (No. 201704030105), EPSRC TOUCAN project (Grant No. EP/L020009/1), and EU H2020 RISE TESTBED project (Grant No. 734325).

References

1. Karunatilaka, D., Zafar, F., Kalavally, V., Parthiban, R.: LED based indoor visible light communications: state of the art. IEEE Commun. Surv. Tutor. **17**(3), 1649–1678 (2015)
2. Cailean, A., Dimian, M.: Current challenges for visible light communications usage in vehicle applications: a survey. IEEE Commun. Surv. Tutor. **PP**(99), 1 (2017)
3. Afgani, M., Haas, H., Elgala, H., Knipp, D.: Visible light communication using OFDM. In: International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, Barcelona, pp. 129–134 (2006)
4. Zhang, G., De, M., Leenheer, A., Morea, B.M.: A survey on OFDM-based elastic core optical networking. IEEE Commun. Surv. Tutor. **15**(1), 65–87 (2013)
5. Carruthers, J., Kahn, J.: Multiple-subcarrier modulation for nondirected wireless infrared communication. IEEE J. Sel. Areas Commun. **14**(3), 538–546 (1996)
6. Armstrong, J., Lowery, A.J.: Power efficient optical OFDM. Electron. Lett. **42**(6), 370–372 (2006)
7. Tsonev, D., Sinanovic, S., Haas, H.: Novel unipolar orthogonal frequency division multiplexing (U-OFDM) for optical wireless. In: Vehicular Technology Conference, pp. 1–5. IEEE, Yokohama (2012)
8. Fernando, N., Hong, Y., Viterbo, E.: Flip-OFDM for unipolar communication systems. IEEE Trans. Commun. **60**(12), 3726–3733 (2012)
9. Patcharamaneepakorn, P., Wang, C.-X., Fu, Y., Aggoune, H., Alwakeel, M.M., Tao, X., Ge, X.: Quadrature space-frequency index modulation for 5G wireless communication systems. IEEE Trans. Commun. (accepted for publication)
10. Basar, E., Panayirci, E.: Optical OFDM with index modulation for visible light communications. In: International Workshop on Optical Wireless Communications, pp. 11–15. IEEE, Istanbul (2015)
11. Mao, T., Jiang, R., Bai, R.: Optical dual-mode index modulation aided OFDM for visible light communications. Optics Commun. **391**, 37–41 (2017)
12. Basar, E., Aygolu, U., Panayirci, E., Poor, H.V.: Orthogonal frequency division multiplexing with index modulation. IEEE Trans. Sig. Proc. **61**(22), 5536–5549 (2013)
13. Dissanayake, S.D., Armstrong, J.: Comparison of ACO-OFDM, DCO-OFDM and ADO-OFDM in IM/DD systems. J. Lightw. Technol. **31**(7), 1063–1072 (2013)
14. Kahn, J.M., Barry, J.R.: Wireless infrared communications. Proc. IEEE **85**(2), 265–298 (1997)
15. Mao, T., Wang, Z., Wang, Q., Chen, S., Hanzo, L.: Dual-mode index modulation aided OFDM. IEEE Access **5**, 50–60 (2016)

Wireless Networking Algorithms and Protocols

Analysis of Crowdsourcing Based Multiple Cellular Network: A Game Theory Approach

Yan Yan, Ye Wang(✉), Jia Yu, Shushi Gu, Siyun Chen, and Qinyu Zhang

Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China
wangye@hitsz.edu.cn

Abstract. Multihop cellular network (MCN) is a feasible scheme to help enlarge network coverage and enhance signal strength in the way of deploying heterogeneous network (HetNet). However, it is challenging for mobile network operators (MNOs) to expedite the implementation of MCN. On the one hand, it is prohibitively expensive to deploy and manage a large-scale intermediate nodes which is essential in MCN; on the other hand, traditional intermediate nodes are usually autonomous and self-interested, which has negative effect on the transmission efficiency and reliability. To address this issue, we discuss a new paradigm of MCN based on crowdsourcing-HetNet (CHetNet). In this paradigm, MNOs recruit the third-parties (TPs) to participate in the construction and maintenances of intermediate nodes by means of rational incentive mechanism. In this article, we mainly focus on a two-hop cellular network in CHetNet. A game-theory approach is used to discuss the whole process of crowdsourcing in this two-hop cellular network and detailed proofs of Nash equilibrium and Stackelberg equilibrium is provided. It is concluded that MCN in CHetNet can help MNOs ease the pressure on the deployment of HetNet and further promote development of 5G.

Keywords: Crowdsourcing · Game theory · HetNet

1 Introduction

With mobile devices increasing explosively and various network applications/services emerging endlessly, it has become more and more difficult for 4G networks to bear the load [2]. Naturally, the new vision for 5G which aims to gain at least a thousand times larger capacity per km^2, a hundred times higher data rates and seamless coverage has been a hot pot [8]. However, as the infrastructure gradually becomes ripe and takes shape, it is a big challenge for mobile network operators (MNOs) to proceed with the innovation of 5G.

To realize the vision of 5G, there have emerged many feasible solutions. Among these, heterogeneous network (HetNet) which can greatly enlarge network capacity and make sure seamless coverage by increasing the density of cell sites has been recognized as an effective scheme in communication field [3].

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 341–353, 2018.
https://doi.org/10.1007/978-3-319-90802-1_30

In HetNet, different kinds of low-power nodes (also called small cell sites) including remote radio heads (RRHs), micro/pico nodes, femto node and relay nodes are expected to distribute around the macro station [4]. Generally speaking, the macro station is mainly in charge of seamless coverage, while low-power nodes have responsibility for some of the network traffic and complementing the coverage holes [1]. What is more, as ubiquitous small cell sites, relay nodes (RNs) play a much important role in the HetNet, because their deployment is fairly flexible and transmission distance is shorter.

However, it is much challenging for MNOs to deploy such large-scale small cell sites. First, it becomes harder for MNOs to gain satisfying profits under heavy operating and capital expenditure (OPEX and CAPEX) [7]. Second, complicated networking topological relation makes it harder to realize seamless coverage and switching among kinds of access ways. For example, seamless coverage from indoor to outdoor areas is still hard to realize. Even the most precise GPS, it has not reached a degree of position in every corner inside buildings. Last but not least, because of regulatory issues, MNOs might face hindrances in obtaining new deployments on existing sites and seeking for new cell sites.

MNOs has been in a dilemma where they have not feasible scheme to proceed the deployment of large-scale small cell sites. Fortunately, a hot concept "Crowdsourcing" appears in recent years which may bring about a favourable turn. Recently, "crowdsourcing" has been widely developed in communication field. Huawei announced a "Crowdsourcing Small Cell" solution at Mobile World Congress 2014. The solution aims to form a new exciting business mode to generate revenue between MNOs and crowdsourcing partners. Partners including facilities owners, building proprietors, network integrators and enterprises can gain rewards which may be money or high-quality service at their locations by participating in the small cell construction and operation. Moreover, MNOs can achieve rapid and large-scale small cells deployment to increase system capacity and energy efficiency (http://pr.huawei.com/en/news/hw-327762-ict.htm#.WZg4BZp96Ul).

In addition, we have witnessed many other practical realization of network deployment based on crowdsourcing. For example, FON (https://fon.com/), a brand about sharing-WiFi routers, aims to build a network where people connect to millions of WiFi hot spots: seamlessly, securely, and everywhere in a crowdsourcing-mode. FON members by using FON devices can choose a voluntary or paid way to provide fractional bandwidth to other FON members. In return, they can enjoy the free WiFi at any corner where there are signals provided by FON members. FON makes good use of crowdsourcing-based mode and has built the world's largest WiFi network, comprised of people sharing their WiFi in recent 10 years. Apart from network deployment, crowdsourcing can also be used for network measurement. GPS tracking unit uploaded by drivers and passengers can be utilized to generate real time traffic statistics [6].

Inspired by these successful examples, allowing the third-parties to participate in the small cell construction and operation may be a significant scheme. In [9], author presents a paradigm called CHetNet which applies crowdsourcing to

distributed HetNet deployment. In this paradigm, author discusses roles of crowdsourcer and crowd in the CHetNet in detail and lists four applications scenarios for CHetNet. In this article, we continue the study of CHetNet based on [9]. Our work focuses on multihop cellular networking (MCN), an application scenario presented for CHetNet. We discuss a two-hop cellular network in CHetNet and increase the number of RNs distributed around the mobile networking operator (MNO)-deployed layer. Furthermore, we present an incentive mechanism and build a game-theory model based on Stackelberg game to seek for a win-win situation. The closed solution of Nash equilibrium and proof of Stackelberg Equilibrium are given in detail. At last, we discuss the influence on utility of the Donor evolved nodeB (DeNB) and RNs when increasing greatly the number of RNs and conclude that too many RNs participating in crowdsourcing would not benefit as anticipated.

The rest of this article is organized as follows: we first analyze the specific case about two-hop cellular networks based on crowdsourcing. Following we form a game-theory model to discuss an intelligent incentive mechanism and specifically prove its rationality. Then, we describe the simulation environment and results. Finally, concluding remarks are given.

2 System Model

With low-cost and feasible-deployment of RNs, it is significant to study MCN for crowdsourcing. MCN has attracted a lot of attention as an effective transmission strategy for future cellular networks because it can effectively increase data rate and enhance coverage [5]. However, the RNs in traditional MCN are usually passive and self-interested that delay the implementation of MCN in terms of transmission efficiency and reliability. This hindrance can be addressed in CHetNet by recruiting TPs as the intermediate nodes instead of voluntary RNs. When a multi-hop communication is formed, the DeNB will employ some potential reliable TPs which play the role of RNs to transmit the information to

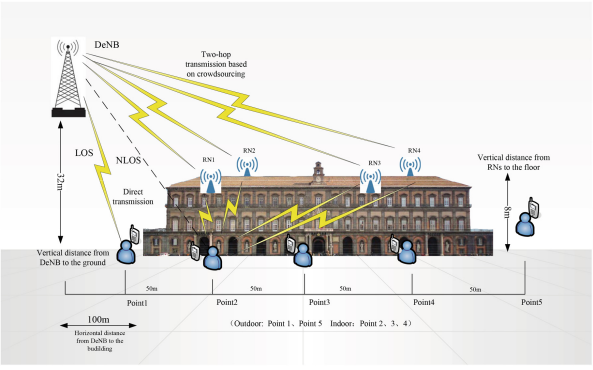


Fig. 1. The model of the two-hop cellular networks

the target UEs. Taking MCN into account, we present a model of two-hop cellular networks in CHetNet using a game-theory approach. The model is composed of an MNO-deployed DeNB, four TP-deployed RNs, and an ordinary user equipment (UE), as shown in Fig. 1. It is evident that the crowdsourcer is the DeNB and crowd is TP-deployed RNs. RNs are deployed on the height of the ceiling in the hall. There are five observation points where the UE walks from outdoor into the hall. When the UE asks for a request, the DeNB has two ways to serve: UE-direct transmission or two-hop transmission, i.e. crowdsourcing way. Note that there is a precondition that only when the task that the DeNB wants to announce is decomposable and sub-tasks are independent, would crowdsourcing scheme proceed [12]. Specifically, when receive a service request from the UE, the DeNB first gathers the network information, including traffic type, channel state information (CSI), potential RNs, resource block (RB), and so on. Depending on these information, orientation process has a decision on a direct transmission way or outsourcing the task to RNs. If outsourcing is determined, the DeNB will start the negotiation with potential partners on the details of the transmission task including transmission parameters, cooperative mode, and the specific incentive mechanism. At last the DeNB and partners reach an agreement in terms of transmission parameters and rewards, and so on. Once an agreement is reached, the DeNB is responsible to transmit traffic data to the recruited RNs in the first time slot, and then these recruited RNs forward the data to the target UE in the second slot [10]. Along with this framework, a general utility function of the DeNB can be written as follows:

$$\begin{aligned} u_{MNO} &= \max\{u_{MNO}^{Direct}, u_{MNO}^{Two-hop}\} \\ u_{MNO}^{Direct} &= \alpha W \log_2\left(1 + SNR^{Direct}\right) \\ u_{MNO}^{Two-hop} &= \frac{1}{2}\alpha W \log_2\left(1 + \sum\nolimits_{i=1}^{N} SNR_i^{Relay}\right) - R \end{aligned} \tag{1}$$

where α is the profit per Mbps of the MNO, and W is the transmission bandwidth assigned to the UE. SNR^{Direct} is the signal-to-noise ratio (SNR) from the DeNB to the UE; N is the number of crowdsourcing RNs, and we assume $N \geq 2$; SNR_n^{Relay} is the received SNR after amplify-and-forward (AF) by RN n; and R is the total reward announced by the MNO. If two-hop transmission is adopted, let p_i denote the transmission power of RN i, the reward allocation can be done using a proportional method, and we can write the reward paid for the i-th RN as

$$r_i = \frac{p_i}{\sum_{j=1}^{N} p_j} \times R \tag{2}$$

Due to the battery-powered form, energy consumption is nonnegligible for RNs to deploy. Let c_i denote the unit power cost of RN i, Accordingly, the cost of RN i participating in the crowdsourcing transmission can be defined as $c_i p_i$, and the utility function of each participating RN can be written as

$$u_i = \frac{p_i}{\sum_{j=1}^{N} p_j} \times R - c_i p_i \tag{3}$$

3 Incentive Mechanism

As MNOs and RNs are the relationship of the employer and employees, an intelligent incentive mechanism is essential to stimulate RNs to participate in crowdsourcing. By means of game-theory model, we can objectively analyze the utility of the two parties and find an optimal scheme for each party and facilitate a win-win situation. In this model, the incentive mechanism of the system using two-hop relay transmission can be modeled as a Stackelberg game. There are one leader and N followers in this game. Obviously, the leader is the DeNB and followers are N relay nodes. Generally speaking, a Stackelberg game can be composed of two stages: In the first stage, the DeNB announces its strategy about the reward R; in the second stage, N relay nodes strategize its transmission power p_i to maximize its own utility and this stage can be considered a non-cooperative game.

In the following parts, we first proves that there exists a unique Nash Equilibrium when R is fixed. On this basis, we further proves that the game between DeNB and recruited RNs has a unique Stackelberg Equilibrium.

3.1 The Determination of Nash Equilibrium

Let a set $\mathcal{U} = \{1, 2, \ldots n\}, n \geq 2$ denote the attached RNs that are interested in participating the transmission task. The strategy of RN i is represented by p_i. The transmission cost of RN i is $c_i p_i$, where $c_i \in \Theta$ is its unit cost. And the set of unit costs is $\Theta = \{\theta_1, \theta_2, \cdots, \theta_l\}$. We assume that the DeNB knows Θ and the distribution of RNs with corresponding unit cost according to the analysis about the historical data. Meanwhile, we assume that RNs with the same unit cost have the same strategy. Based on above descriptions and assumptions, we can transform the utility of RN i (3) to

$$u_i = \frac{p_i}{\sum_{j \in \mathcal{U}} p_j} \times R - c_i p_i \tag{4}$$

The utility of the DeNB is

$$u_0 = g(\widetilde{p}_1, \widetilde{p}_2, \cdots \widetilde{p}_n; n) - R \tag{5}$$

$$g(\widetilde{p}_1, \widetilde{p}_2, \cdots \widetilde{p}_n; n) = \frac{1}{2} \alpha W \log_2 \left(1 + \sum_{i=1}^{n} SNR_i^{Relay}\right) \tag{6}$$

Where $\widetilde{p}_j$ is the transmission power of RNs with unit cost c_j, and $g(\widetilde{p}_1, \widetilde{p}_2, \cdots \widetilde{p}_n; n)$ is the DeNB's valuation function of RNs' transmission power. When $\forall \widetilde{p}_j \leq 0, g(\widetilde{p}_1, \widetilde{p}_2, \cdots \widetilde{p}_n; n) = 0$.

Note that all RNs are willing to provide service for a positive utility, so RN i will not participate in the game when $u_i \leq 0$.

With the strategy of RN i being its own transmission power p_i, we denote $p = (p_1, p_2, \ldots p_n)$ the strategy profile consisting of all RNs strategies. In addition, let p_{-i} denote the strategy profile excluding p_i. Based on it, $p = (p_1, p_2, \ldots p_n)$ can be denoted by $p = (p_i, p_{-i})$.

Definition 1 (Nash Equilibrium). *A set of strategies* $p^{ne} = (p_1^{ne}, p_2^{ne}, \dots p_n^{ne})$ *is a Nash Equilibrium (NE) if for* $\forall$ *RN* i*,*

$$u_i(p_i^{ne}, p_{-i}^{ne}) \geq u_i(p_i, p_{-i}^{ne})$$

for $\forall p_i \geq 0$.

Definition 2 (Best Response Strategy). *Given* p_{-i}*, a strategy of RN* i *is the best response strategy, denoted by* $\beta_i(p_{-i})$*, if it maximizes the utility* $u_i(p_i, p_{-i})$ *of RN* i *for all* $p_i \geq 0$.

Based on above definitions, we firstly prove the existence of the Nash Equilibrium according to computing the best response strategy.

Obviously, every RN will play the best response strategy to gain profit in a NE. To study the best response strategy, we firstly compute the derivatives of u_i with respect to p_i:

$$\frac{\partial u_i}{\partial p_i} = \frac{-Rp_i}{(\sum_{j\in\mathcal{U}} p_j)^2} + \frac{R}{\sum_{j\in\mathcal{U}} p_j} - c_i \tag{7}$$

$$\frac{\partial^2 u_i}{\partial p_i^2} = \frac{-2R\sum_{j\in\mathcal{U}} p_j + 2Rp_i}{(\sum_{j\in\mathcal{U}} p_j)^3} = -\frac{2R\sum_{j\in\mathcal{U}_{-i}} p_j}{(\sum_{j\in\mathcal{U}} p_j)^3} < 0 \tag{8}$$

Since the second-order derivative of u_i is negative, the utility u_i is a strictly convex function with respect to p_i. It indicates that RN i can maximize its own utility according to changing its transmission power p_i when other RNs' transmission power p_{-i} is fixed. Note that we should set $\beta_i(p_{-i}) = 0$ when the best response strategy $p_i \leq 0$.

We let the first-order derivative of u_i be zero, we can obtain

$$\frac{-Rp_i}{(\sum_{j\in\mathcal{U}} p_j)^2} + \frac{R}{\sum_{j\in\mathcal{U}} p_j} - c_i = 0 \tag{9}$$

$$p_i = \sqrt{\frac{R\sum_{j\in\mathcal{U}_{-i}} p_j}{c_i}} - \sum\nolimits_{j\in\mathcal{U}_{-i}} p_j \tag{10}$$

when $p_i \leq 0, \sqrt{\frac{R\sum_{j\in\mathcal{U}_{-i}} p_j}{c_i}} - \sum_{j\in\mathcal{U}_{-i}} p_j \leq 0$, $R \leq c_i \sum_{j\in\mathcal{U}_{-i}} p_j$, we will set $\beta_i(p_{-i}) = 0$. Hence we can obtain the best response strategy of RN i

$$\beta_i(p_{-i}) = \begin{cases} 0. & if\ R \leq c_i \sum_{j\in\mathcal{U}_{-i}} p_j; \\ \sqrt{\frac{R\sum_{j\in\mathcal{U}_{-i}} p_j}{c_i}} - \sum_{j\in\mathcal{U}_{-i}} p_j & otherwise \end{cases}$$

Since the best response strategy of RN i is solved, we have proved that the existence of a NE. Then, we should prove that the NE is unique according to proving the theorem below. The idea of demonstration about NE is learned from [11].

Theorem 1. *Let $R > 0$ be given. Let $\overline{p} = (\overline{p}_1, \overline{p}_2, \ldots \overline{p}_n)$ be the strategy profile of an NE, and let $\overline{\mathcal{S}} = \{i \in \mathcal{U} | \overline{p}_i > 0\}$, $|\overline{\mathcal{S}}| = n_0$, we have*

1. $|\overline{\mathcal{S}}| > 1$
2. $\overline{p}_i = \begin{cases} 0, & if\ i \notin \overline{\mathcal{S}}; \\ \frac{(n_0-1)R}{\sum_{j\in\overline{\mathcal{S}}} c_j}\left(1 - \frac{(n_0-1)c_i}{\sum_{j\in\overline{\mathcal{S}}} c_j}\right), & otherwise \end{cases}$
3. *if* $c_q \leq \max_{j\in\overline{\mathcal{S}}}\{c_j\}$, *then* $q \in \overline{\mathcal{S}}$
4. *Assume that RNs are ordered in a ascending way such that* $c_1 \leq c_2 \leq c_3 \leq \cdots \leq c_n$. *Let* h *be the largest integer in* $[2, n]$ *that meets* $c_h < \frac{\sum_{j=1}^{h} c_j}{h-1}$. *Then* $\overline{\mathcal{S}} = \{1, 2, \ldots h\}$

By means of proving these statements, we can obtain the closed-form solution of $\overline{p}_i$ and then prove the unique NE.

Proof. Firstly we prove $|\overline{\mathcal{S}}| > 1$. We assume $|\overline{\mathcal{S}}| = 0$, obviously it is impossible, as RN 1 can increase its utility by increasing its transmission power. So $|\overline{\mathcal{S}}| > 0$. Then we assume $|\overline{\mathcal{S}}| = 1$, it shows there is only RN $k (k \in \overline{\mathcal{S}})$ participating in the game. However, the first-order derivative of u_k is $-c_k$ and it is unequal to zero. It indicates the strategy of the RN k is not a best response strategy. In other words, it has not reach a NE. It contradicts the NE assumption. So $|\overline{\mathcal{S}}| > 1$.

Then we prove the second one. Based on $|\overline{\mathcal{S}}| > 1$ and (9), we can replace p_i with $\overline{p}_i$ and replace $\mathcal{U}$ with $\overline{\mathcal{S}}$. We can obtain

$$\frac{-R\overline{p}_i}{\left(\sum_{j\in\overline{\mathcal{S}}} \overline{p}_j\right)^2} + \frac{R}{\sum_{j\in\overline{\mathcal{S}}} \overline{p}_j} - c_i = 0, \quad i \in \overline{\mathcal{S}} \tag{11}$$

Summing up (11) over the $|\overline{\mathcal{S}}|$ and we can obtain

$$\frac{-R + n_0 R}{\sum_{j\in\overline{\mathcal{S}}} \overline{p}_j} - \sum\nolimits_{j\in\overline{\mathcal{S}}} c_j = 0 \tag{12}$$

$$\sum\nolimits_{j\in\overline{\mathcal{S}}} \overline{p}_j = \frac{(n_0 - 1)R}{\sum_{j\in\overline{\mathcal{S}}} c_j} \tag{13}$$

Then substituting (13) into (11), we can obtain

$$\overline{p}_i = \frac{(n_0 - 1)\, R}{\sum_{j\in\overline{\mathcal{S}}} c_j}\left(1 - \frac{(n_0 - 1)\, c_i}{\sum_{j\in\overline{\mathcal{S}}} c_j}\right) \tag{14}$$

Besides, we set $\overline{p}_i = 0$ when RN i does not belong to $\overline{\mathcal{S}}$. Thus, we can get

$$\overline{p}_i = \begin{cases} 0, & if\ i \notin \overline{\mathcal{S}}; \\ \frac{(n_0-1)R}{\sum_{j\in\overline{\mathcal{S}}} c_j}\left(1 - \frac{(n_0-1)c_i}{\sum_{j\in\overline{\mathcal{S}}} c_j}\right), & otherwise \end{cases} \tag{15}$$

From the above statement, we find that $\overline{p}_i$ only depends on reward R, the set of unit cost Θ and the number n_0 of RNs participating in the game. The reward R

is fixed and the set of unit cost Θ can be learned. Thus, only when we confirm the number n_0, would we prove the unique NE. The next work is to find the certain RNs that belongs to $\overline{\mathcal{S}}$.

The third one was proved as follows: Since $\overline{p}_i > 0$ for every RN i belongs to $\overline{\mathcal{S}}$. Then from the (15), we can know $1 - \frac{(n_0-1)c_i}{\sum_{j\in\overline{\mathcal{S}}} c_j} > 0$ which implies $\frac{(n_0-1)c_i}{\sum_{j\in\overline{\mathcal{S}}} c_j} < 1$. Thus we can obtain

$$c_i < \frac{\sum_{j\in\overline{\mathcal{S}}} c_j}{n_0 - 1}, \qquad \forall i \in \overline{\mathcal{S}} \tag{16}$$

And then

$$\max_{i\in\overline{\mathcal{S}}} c_i < \frac{\sum_{j\in\overline{\mathcal{S}}} c_j}{n_0 - 1} \tag{17}$$

We assume that $c_q \leq \max_{j\in\overline{\mathcal{S}}}\{c_j\}$, but $q \notin \overline{\mathcal{S}}$. Since $q \notin \overline{\mathcal{S}}$, we know that $\overline{p}_q = 0$. Using the (13), we can obtain the first-order derivative of u_q with respect to p_q when $p = \overline{p}$

$$\frac{\partial u_q}{\partial p_q} = \frac{R}{\sum_{j\in\overline{\mathcal{S}}} \overline{p}_j} - c_q = \frac{\sum_{j\in\overline{\mathcal{S}}} c_j}{n_0 - 1} - c_q > \max_{i\in\overline{\mathcal{S}}}\{c_i\} - c_q \geq 0 \tag{18}$$

It indicates the RN q has not reach a NE and it can increase its utility by increasing its transmission power. It conflicts the previous assumption. So $q \in \overline{\mathcal{S}}$.

Finally the proof of last one was given. Since we have proved that if $c_q \leq \max_{j\in\overline{\mathcal{S}}}\{c_j\}$, then $q \in \overline{\mathcal{S}}$, we know that $\overline{\mathcal{S}} = \{1, 2, \cdots, q\}$ for some integer q in $[2, n]$. Because of $c_h < \frac{\sum_{j=1}^{h} c_j}{h-1}$ and (16), we can make sure that $h \geq q$. Firstly we assume $h > q$, so we can find that $c_{q+1} < \frac{\sum_{j=1}^{q+1} c_j}{q}$. Then we have $q \cdot c_{q+1} < \sum_{j=1}^{q} c_j + c_{q+1}$ which implies $c_{q+1} < \frac{\sum_{j=1}^{q} c_j}{q-1}$. In a similar way, we get the first-order derivative of u_{q+1} with respect to p_{q+1} when $p = \overline{p}$ is $\frac{\partial u_{q+1}}{\partial p_{q+1}} = \frac{R}{\sum_{j\in\overline{\mathcal{S}}} \overline{p}_j} - c_{q+1} = \frac{\sum_{j=1}^{q} c_j}{q-1} - c_{q+1} > 0$. It shows the contradiction to the NE assumption which proves that $h = q$.

3.2 Stackelberg Equilibrium of the DeNB

Based on the above analysis, the DeNB that is the leader in the Stackelberg game knows that there exists a unique NE for the RNs when the reward R is announced. Thus the DeNB can strategize its R to maximize its utility. Next we will prove that there must exist a unique Stackelberg.

Theorem 2. *There exists the unique Stackelberg Equilibrium* $(\overline{R}, p^{ne})$ *in the first stage of the Stackelberg game, where* $\overline{R}$ *is the unique maximizer of the utility of the DeNB over* $R \in [0, \infty)$*, and* $p^{ne} = (\widetilde{p}_1, \widetilde{p}_2, \cdots \widetilde{p}_n)$ *which is a set of NE is given in the part A.*

Proof. Let $u_0 = g(X_1R, X_2R, \cdots, X_nR; n) - R$.

And $g(\widetilde{p}_1, \widetilde{p}_2, \cdots \widetilde{p}_n; n) = \frac{1}{2}\alpha W \log_2\left(1 + \sum_{i=1}^{n} SNR_i^{Relay}\right)$. We can get:

$$X_i = \begin{cases} \frac{(n_0-1)}{\sum_{c_j \in \overline{\mathcal{S}}} c_j}\left(1 - \frac{(n_0-1)c_i}{\sum_{c_j \in \overline{\mathcal{S}}} c_j}\right) & i \in \overline{\mathcal{S}}; \\ 0 & i \notin \overline{\mathcal{S}} \end{cases}$$

Besides, we know that $SNR_i^{Relay} = \frac{p_0\gamma_i^1 p_i \gamma_i^2}{1+p_0\gamma_i^1+p_i\gamma_i^2}$ in a two-hop relay transmission system, where p_0 is transmitting power of the DeNB and p_i is RN i's transmitting power. And $\gamma_i^1 = \frac{|h_i^1|^2}{\sigma^2}, \gamma_i^2 = \frac{|h_i^2|^2}{\sigma^2}$ are respectively the SNR from the DeNB to RN i and RN i to the UE, where h_i^1, h_i^2 refers to their channel coefficients and σ^2 is the variance of additive white gaussian noise. Then let $h_i(R) = \frac{p_0\gamma_i^1\gamma_i^2 X_i R}{1+p_0\gamma_i^1+\gamma_i^2 X_i R}, h_i(R) > 0$ thus $u_0 = \frac{1}{2}\alpha W \log_2(1 + \sum_{i=1}^{n} h_i(R))$. Then we can obtain:

$$\frac{\partial u_0}{\partial R} = \frac{1}{2}\alpha W \ln 2 \frac{\sum_{i=1}^{n} \frac{\partial h_i(R)}{\partial R}}{1 + \sum_{i=1}^{n} h_i(R)} \tag{19}$$

$$\frac{\partial^2 u_o}{\partial R^2} = \frac{1}{2}\alpha W \ln 2 \frac{(1 + \sum_{i=1}^{n} h_i(R)) \sum_{i=1}^{n} \frac{\partial^2 h_i(R)}{\partial R^2}}{(1 + \sum_{i=1}^{n} h_i(R))^2} \tag{20}$$

$$\frac{\partial h_i(R)}{\partial R} = \frac{p_0\gamma_i^1(\gamma_i^2)^2 X_i(1 + p_0\gamma_i^1)}{(1 + p_0\gamma_i^1 + \gamma_i^2 X_i R)^2} \tag{21}$$

According to (21), it is evident that $\frac{\partial^2 h_i(R)}{\partial R^2} < 0$, and we know $h_i(R) > 0$, so $\frac{\partial^2 u_o}{\partial R^2} < 0$. Thus $u_0 = g(X_1R, X_2R, \cdots, X_nR; n) - R$ is a strictly convex function in variables R when $p^{ne} = (\widetilde{p}_1, \widetilde{p}_2, \cdots \widetilde{p}_n)$ is given. When $R = 0, u_0 = 0$. $R \to \infty, u_0 \to -\infty$. So a unique maximizer $\overline{R}$ must exist. We can find the maximal u_0 and then obtain $\overline{R}$ according to traversing the R in the Matlab.

Based on above analysis, it has been proved that there exists a unique NE of the strategy RNs and a unique Stackelberg equilibrium about the strategy of the DeNB. Thus MNOs can adjust their transmission way based on the maximal utility of direct or relay transmission.

4 Simulation and Results Analysis

In this section, we introduce the environment and results of the simulation about the two-hop cellular networks. The model consists of an MNO-deployed DeNB, four TP-deployed RNs and an ordinary UE. Both the DeNB and RNs are equipped with four uniform linear antenna arrays (ULA-4), and the UE is equipped with ULA-2. We set the transmission power and the profit per Mbps of the DeNB are respectively $p_0 = 1\,\mathrm{W}$ and $\alpha = 20/\mathrm{Mbps}$; Besides, we set the transmission bandwidth $W = 1\,\mathrm{MHz}$; and we set $C = [10, 20, 15, 25]$ that is respectively the unit transmission cost of RNs in order. We use WINNER Phase II channel as the environment and the mode of RNs is amplify-and-forward (AF). Maximal ratio combining (MRC) is adopted when multiple replications are received by the UE. As for

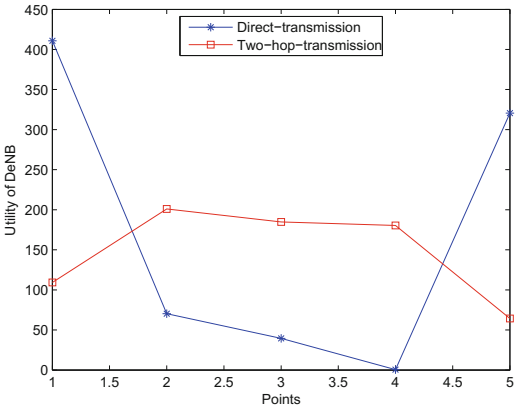


Fig. 2. The utility of the DeNB at different observation

the UE, there are five observation points where points 1 and points 5 are typical urban macrocells with line-of-sight (LOS) condition from the DeNB to the UE. For point 2, 3, 4, the UE moves from outdoor into a large indoor hall and across it. The four RNs are deployed at the four corners of the ceiling. At point 2, 3, 4, transmission from the DeNB to the UE experiences non-LOS (NLOS) outdoor-indoor propagation. As for the two-hop relay transmission, on the first slot, we can consider it LOS macrocell propagation from the DeNB to RNs; and on the second slot, for point 1 and point 5, they are NLOS indoor-outdoor propagation from RNs to the UE, and for the points indoor, they are LOS large-indoor hall propagation from RNs to the UE. Relevant parameters are shown in the Table 1. As unit transmission costs of RNs that plan to receive the transmission task are different, those RNs that have lower unit transmission cost tends to gain higher profits, while RNs which need much more cost would quit the game. In this model, the fourth RN with higher unit cost would not participate in the game because of negative utility. Thus the DeNB and RN $1, 2, 3$ form a cooperative relation to proceed a win-win situation at last.

Table 1. Parameters of layout

Parameter	Value
p_0	1 W
α	20/Mb/s
W	1 MHz
C	10 20 15 25
Height of the DeNB	32 m
Height of RNs	8 m
Height of the UE	1.5 m

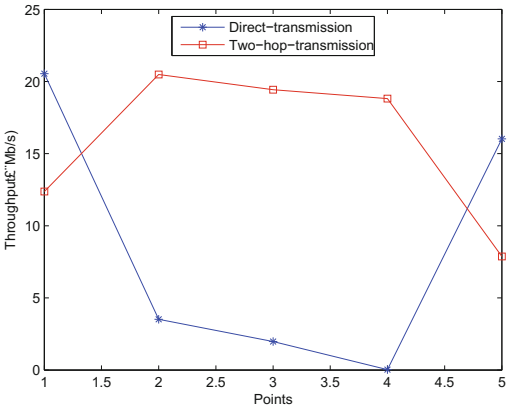


Fig. 3. The throughput of the UE at different observation

Figure 2 shows the variations of utility of the DeNB with different observation points in the way of direct and two-hop transmission. It is evident that when the UE stands at the point 1 or 5, the utility of the DeNB in the direct transmission way is much higher than the two-hop transmission way. However, when the UE enters the mall, the utility of the DeNB in the direct transmission way drops rapidly and even approximates to zero. In this condition, the DeNB will prefer the two-hop transmission way. Figure 3 shows the throughput of the UE, which seems like the trend of graphs about the utility of the DeNB. According to jointly using direct and two-hop transmission, We can find that not only the DeNB can always maintain relatively high utility, but the UE can always experience greater than 15 Mb/s data rate.

Figure 4 shows the relationship between the utility and reward when the UE respectively stands at point 2, point 3 and point 4. The square points labeled on every curve refer to the Stackelberg equilibrium strategy for the DeNB which means the optimal reward offered to RNs. It can be seen that a small amount of reward that is less than 10% of the utility of the DeNB can stimulate the participation of RNs in crowdsourcing task transmission. Thus we can conclude that all participants including the DeNB, RNs and the UE can get what they call for. The DeNB gains more profits and ease the deployment pressure. RNs earn satisfying reward and get higher quality service. And the UE enjoys a better service experience. However, it will not be more profitable when more and more low-cost RNs try to participate in crowdsourcing in a noncooperative competition. We assume all RNs' unit transmission cost is 15/W and gradually increase the number of RNs that are sure to participate in the transmission task one by one when the UE stands at point 3. Figure 5 is the simulation result of utility about the DeNB and RNs and the throughput of the UE in a two-hop transmission way when we add RNs to fourteen. We can find more RNs only make the utility of the DeNB increase little (less than 5%). Meanwhile, the utility of RNs decrease gradually and even approximate to zero as more and

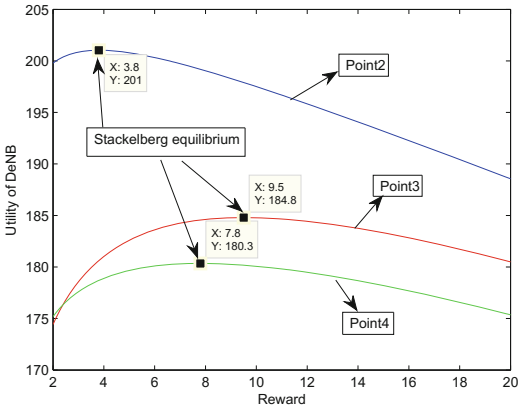


Fig. 4. The utility of the DeNB vs. Reward of RNs.

more competitors take part in the crowdsourcing while the experience data rate of the UE increase barely 2 Mb/s and even improve little at last. Thus, choosing more RNs to participate in a single transmission task benefits little to any party of DeNB, RNs and UEs, it is more worthy to study how to allocate rationally which RNs to which task.

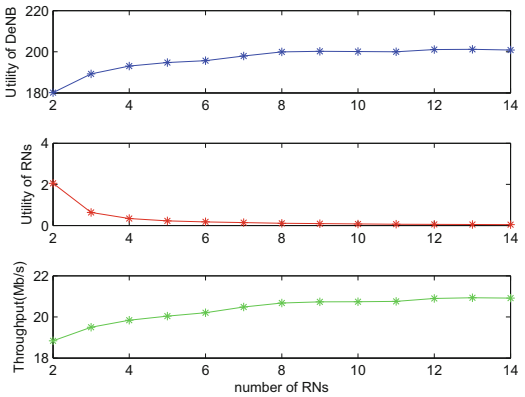


Fig. 5. The utility of the DeNB and RNs, the throughput of the UE

5 Conclusion

In this article, we mainly discuss a two-hop cellular network based on crowdsourcing and its incentive mechanism. By means of a game-theory model, Concrete processes of proof about Nash equilibrium and Stackelberg equilibrium are given to verify the feasibility of the incentive mechanism. The results of simulations

verify that the crowdsourcing mode prompts MNOs and TPs to form a win-win situation and helps accelerate deployment of HetNet, and further promote the development of 5G.

However, MCN in CHetNet still faces many challenges in the way of implementation. How to organize and manage a large scale of unplanned TPs in a convincing and legal way is a critical issue to solve. And how to optimize the incentive mechanism and allocate transmission tasks rationally which can ensure equity for TPs needs further research. In addition, security problem becomes particularly important and MNOs should protect the privacy of UEs from revealing through TPs.

Acknowledgements. This work has been supported in part by the National Natural Sciences Foundation of China (NSFC) under Grants 61501140, 61701136, and 61525103.

References

1. Cai, S., Che, Y., Duan, L., Wang, J., Zhou, S., Zhang, R.: Green 5G heterogeneous networks through dynamic small-cell operation. IEEE J. Sel. Areas Commun. **34**(5), 1103–1115 (2016)
2. Cisco: Cisco visual networking index: global mobile data traffic forecast update, 2013 to 2018. Technical report, February 2014
3. Ge, X., Tu, S., Mao, G., Wang, C.X., Han, T.: 5G ultra-dense cellular networks. IEEE Wirel. Commun. **23**(1), 72–79 (2015)
4. Ghosh, A., Mangalvedhe, N., Ratasuk, R., Mondal, B., Cudak, M., Visotsky, E., Thomas, T.A., Andrews, J.G., Xia, P., Jo, H.S., et al.: Heterogeneous cellular networks: from theory to practice. IEEE Commun. Mag. **50**(6), 54–64 (2012)
5. Jangsher, S., Li, V.O.K.: Power control in multihop cellular networks with multiple radio access technologies. In: IEEE International Symposium on Personal, Indoor, and Mobile Radio Communication, pp. 1674–1678 (2014)
6. Kanhere, S.S.: Participatory sensing: crowdsourcing data from mobile smartphones in urban spaces. In: Hota, C., Srimani, P.K. (eds.) ICDCIT 2013. LNCS, vol. 7753, pp. 19–26. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36071-8_2
7. Machuca, C.M.: Expenditures study for network operators. In: International Conference on Transparent Optical Networks, pp. 18–22 (2006)
8. Osseiran, A., Boccardi, F., Braun, V., Kusume, K., Marsch, P., Maternia, M., Queseth, O., Schellmann, M., Schotten, H., Taoka, H.: Scenarios for 5G mobile and wireless communications: the vision of the METIS project. IEEE Commun. Mag. **52**(5), 26–35 (2014)
9. Wang, Y., Lin, X.: CHetNet: crowdsourcing to heterogeneous cellular networks. Netw. IEEE **29**(6), 62–67 (2015)
10. Wang, Y., Lin, X.: User-provided networking for QoE provisioning in mobile networks. Wirel. Commun. IEEE **22**(4), 26–33 (2015)
11. Yang, D., Xue, G., Fang, X., Tang, J.: Incentive mechanisms for crowdsensing: crowdsourcing with smartphones. IEEE/ACM Trans. Netw. **24**(3), 1732–1744 (2016)
12. Zhang, H., Sugiyama, M.: Task selection for bandit-based task assignment in heterogeneous crowdsourcing. In: Technologies and Applications of Artificial Intelligence, pp. 164–171 (2015)

A Markov Decision Based Optimization on Bundle Size over Two-Hop Inter-satellite Links

Yue Li(✉), Zhihua Yang, and Peng Yuan

Shenzhen Graduate School, Communications Engineering Research Center,
Harbin Institute of Technology, Shenzhen, China
liyue1234566@126.com, yangzhihua@hit.edu.cn, yuanp1990@163.com

Abstract. In a satellite Disruption-Tolerant Network (DTN), bundle delivery is obviously affected by time-varying parameters, i.e. bit error ratio and propagation latency, due to constantly changing distance and connectivity between consecutive orbital nodes. In this paper, we proposed a Markov decision based optimization approach for bundle size, which could efficiently improve the expected time of delivery over a dynamic two-hop Inter-Satellite Link (ISL). In particular, a sequence of optimal bundle sizes are adaptively selected according to distance-dependent current channel parameters, which could make full utilization on intermediate node's memory. The simulation results verified the proposed method with different conditions with comparison.

Keywords: DTN · Markov decision · Bundles · Memory

1 Introduction

Due to high error ratio and frequent interruption, typical TCP/IP protocol cluster are not suitable for a satellite network with inter-satellite links (ISL), since scarcely continuous end-to-end paths exist for reliable delivery in the network. In these years, Disruption-Tolerant Network (DTN) architecture is proposed for an attractive candidate solution on those above challenges in satellite networks. In a DTN, as a main protocol of stack, bundle protocol (BP) exploits a custody transfer mechanism which could store bundling data temporarily in local endpoint's storage until forwarding them to next hop successfully. Typically, bundle is employed for a basic unit of delivery by BP agent, thus its size has an obvious impact on the transfer performance with respect to the latency and throughput over hop-by-hop links.

At present, a bulk of works focus on the optimization of bundle size in various scenarios of DTN. In [1, 2], one realistic application in DTN scenario is proposed for a so-called Ring Road networks with the improvements of delivery time. In [3, 4], a file delivery model in a single-hop link is proposed with a method to calculate round-trip time. An expedited scheme for bundle transfer is designed in [5] for coping with sudden link failures, which enables partially received segments to be forwarded towards the next node within a new bundle during previous-hop transfer cessation. Jiang and Lu in [6] establish a multi-hop transmission model in static link and propose an optimization method for bundle and segment size. In [7], a bundle distribution mechanism is

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 354–364, 2018.
https://doi.org/10.1007/978-3-319-90802-1_31

constructed by a birth-death Markov process, in which the probability of successful delivery for a bundle is theoretically derived. Currently, these above works on bundle size optimization discuss mainly on static environments with a couple of fixed link parameters. In a DTN based satellite network, however, relative distance between satellite nodes changes instantly with node's orbital motions, which will cause correspondingly time-varying properties of channel parameters. In addition, periodically intermittent connectivity between satellite nodes also make obvious impacts on the bundles delivery. As a result, a fixed size of bundle possibly leads to inefficiency of link usage and long latency of delivery, due to incapability of filling up dynamic contacts, especially over a two-hop link with an intermediate node. Extremely, there could be no forwarding of a bundle due to unsuitable size compared with a short duration of contact. In this paper, therefore, we propose a Markov decision based optimization method for bundle size over a two-hop ISL, which could find a series of optimal sizes of bundle by adjusting the decisions accordingly with various channel parameters, given a constrained storage memory at the intermediate node. The simulation results verified that the proposed algorithm significantly improve the performance of bundle delivery with respect to the transfer latency.

The remainder of the paper is organized as follow: Sect. 2 describes bundle delivery model and delay metric. In Sect. 3, Markov decision model is presented and numerical results are discussed in Sect. 4. Finally the conclusion is drawn in Sect. 5. In this paper, the used abbreviation are specified in Table 1.

Table 1. Abbreviation

Abbr	Definition	Abbr	Definition
ISL	Inter-satellite links	*ACK*	Acknowledgement signal
BP	Bundle protocol	LEO	Low earth orbit satellite
LTP	Licklider Transmission Protocol	MEO	Medium earth orbit satellite Medium Earth Orbit
CAi	the *i*-th reverse link	GEO	Geosynchronous

2 System Model

2.1 DTN over Two-Hop ISL

In a DTN in-built satellite network, a flow of application messages, i.e. image files, will be transferred with a bulk of bundles encapsulated by BP (Bundle Protocol) and LTP (Licklider Transmission Protocol) agents. Initially, a target file is sent from application layer to BP layer, which will be divided into a series of bundles according to the optimal bundle size obtained by the proposed algorithm in this paper. Then, LTP agent receives bundles from BP layer and encapsulates them into blocks, which are subsequently sliced into segments as basic transmission units. Due to a custody transfer mechanism, these bundles are stored in the endpoint's permanent storage before transferred successfully to the next endpoint. Normally, local endpoint will delete one bundle if its next-hop node receives the entire bundle successfully.

In a scenario with two consecutive links, delivery of bundles from sender node to receiver node will experience two individual contacts with differently dynamic channel parameters, i.e., bit error ratio (BER) and propagation delay. As a result, the performance of delivery will present an obvious inefficiency if with a fixed set of bundle size in two links. In this section, therefore, we propose a Markov decision model in BP layer to calculate a couple of optimal bundle sizes for two-hop delivery, by making analysis on the dynamic of memory at intermediate node during the whole delivery. In particular, the optimal size of bundle will be adaptively selected from a limited candidate set according to current status of channels.

2.2 Bundle Delivery Time

Typically, bundle is a basic protocol data unit in BP layer. In a delivery, a round-trip time (RTT) consists of propagation delay, bundle and ACKs transmission delay and random delay, respectively.

Figure 1 shows a temporal sequence of one bundle delivery in a dynamic space channel, which is developing worse with time. In the figure, transmission delay $T_b(i)$ and propagation delay $T_p(i)$ progress larger respectively. Generally, a successful delivery of bundle in a single-hop link means that the entire bundle has been received reliably by destination node with a transferred custody. At the same time, source node removes the bundle copy from memory. As a result, a RTT of bundle at time t is expressed as follow

$$RTT(t) = 2 \cdot T_p(t) + T_{ca} + T_b(t) + T_{random}, \tag{1}$$

in which the used notations are specified in Table 2.

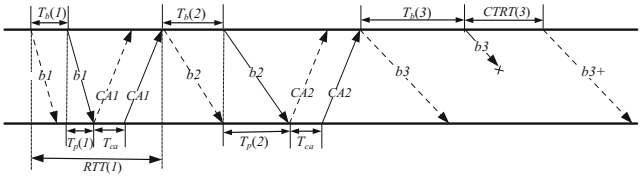


Fig. 1. Bundle delivery procedure

In Fig. 1, bundle *b3* is lost during a spurt due to bad link conditions, which will start a re-transmission immediately after a corresponding timer *CTRT* is timeout. Hence, if a bundle is transferred with one spurt successfully, the delivery time of this bundle is same as a RTT. Otherwise, it is equal to the value of custody-confirm timer (*CTRT*). As a result, the delivery time of one bundle can be represented by an expectation of RTT as follows

$$RTT_{ev}(t) = (1 - P_{ef}(t)) \cdot RTT(t) + P_{ef}(t) \cdot CTRT(t), \tag{2}$$

in which

$$CTRT(t) = 2 \cdot T_p(t) + T_{ca}. \tag{3}$$

Table 2. Notations

T_p	Propagation delay	L_{space}	Free space path loss
T_b	Transmission time of bundle	E_0	Sum of constant variables about *SNR*
T_{ca}	Transmission time of ACK signal	f	Frequency
CTRT	Timeout length	D	Distance
RTT	Round-trip time	RTT_{ev}	Expect of round_trip time
P_{ef}	Bundle lost probability	T_{random}	Random noise
P_e	Error bit rate	N_0	Unilateral noise power spectral density
Lbundle	Bundle size	B	Bandwidth
SNR	Signal to noise ratio	E_b	Energy per bit
L_{ca}	The size of ACK signal	R_{ca}	The rate of ACK signal

In particular, $P_{ef}(t)$ is a bundle loss probability obtained by a specific function coupling bundle size with bit error rate of P_e, which is determined by both modulation technique and signal-to-noise ratio together. With a BPSK modulation, the bundle loss probability is expressed as follow

$$P_{ef}(t) = 1 - (1 - P_e(t))^{8 \cdot Lbundle}, \tag{4}$$

in which

$$P_e(t) = 0.5 \cdot erfc(\sqrt{SNR(t)}). \tag{5}$$

In (5), $SNR(t)$ is calculated by channel parameters in a ISL. Defining a main variable of $L_{space}(t)$ with other constant variables, we express $SNR(t)$ as

$$SNR(t) = E_0 - 10 \lg L_{space}(t). \tag{6}$$

Due to relative motion of two satellites, the range of $D(t)$ changes over time t, which determines the free space path loss $L_{space}(t)$ and $T_p(t)$ as

$$\lg(L_{space}(t)) = 92.45 + 20 \lg D(t) + 20 \lg f. \tag{7}$$

With (6) and (7), $P_e(t)$ can be express:

$$P_e(t) = 0.5 \cdot erfc(\sqrt{E_0 - (92.45 + 20 \lg D(t) + 20 \lg f)}). \tag{8}$$

In addition,

$$T_p(t) = D(t)/C. \tag{9}$$

For T_b, it is related with bundle size and a transmission rate, as

$$T_b(t) = L_{bundle}(t)/R_{data}(t) \tag{10}$$

in which

$$R_{data}(t) = \frac{SNR(t) \times N_0 \times B}{E_b}. \tag{11}$$

In conclusion, one RTT can be rewrote as

$$\begin{aligned} RTT_{ev}(t) = {} & (1 - 0.5 \cdot erfc(\sqrt{C_0 - 20\lg D(t)}))^{Lbundle} \times (2 \cdot T_p(t) + T_{ca} + T_b(t) + T_{random}) \\ & + (1 - (1 - 0.5 \times erfc(\sqrt{C_0 - 20\lg D(t)}))^{Lbundle}) \times CTRT(t) \end{aligned}, \tag{12}$$

where

$$C_0 = E_0 - (92.45 + 20\lg f). \tag{13}$$

3 Markov Decision Model

In a two-hop ISL, we could make an optimization of bundle size in order to get a shorter latency of file delivery. In a general optimization method, a bundle size is uniquely determined according to current link state, until the entire file is transferred. In a satellite network, especially with two-hop ISL, however, link state changes dynamically, leading to an inefficiency of fixed size in the transmission process. Therefore, in this paper, we propose a Markov decision based optimization model for finding a couple of suitable bundle sizes, by making different decisions in a set of candidate actions with a constrain of intermediate node memory.

3.1 Problem Formulation

Firstly, source node delivers a series of bundles to intermediate node in a two-hop ISL. If one entire bundle is received by intermediate node successfully, it will be stored in the memory of intermediate node. With convenience of analysis, in this paper, we assume that the memory of intermediate node has exactly a volume of one bundle. As a result, the intermediate node could receive another bundle from the sender, only after it has forwarded successfully that store-in-memory bundle to the next-hop destination node. It is means that, the intermediate node could accept new bundles only when memory becomes empty. Hence, the dynamic of memory in intermediate node can reflect the delivery performance of one bundle over the two-hop ISL. Comprehensively, a small size leads to a faster transfer of bundle, which could pass the intermediate node quickly and be delivered to the destination node. However, a smaller bundle size will cause more bundles need to be sent for a target file, which will enlarge the total delivery time. Therefore, an adaptive bundle size is necessary for improving delivery efficiency and shortening the file end-to-end delivery time.

In this section, we consider a Markov decision model to select a bundle size, by which a rate of memory utilization at the intermediate node is improved as largely as

possible. The progress of Markov decision model is shown as Fig. 2. In the proposed algorithm, when the time t is updated, a new bundle size according to a related decision is outputted at time t. Finally, we can obtain a set of bundle sizes based on different link states at each moment. In Fig. 4, *RTT* (State of Link I) and *RTT* (State of Link II) can be calculated by a reward function expressed in (17), respectively.

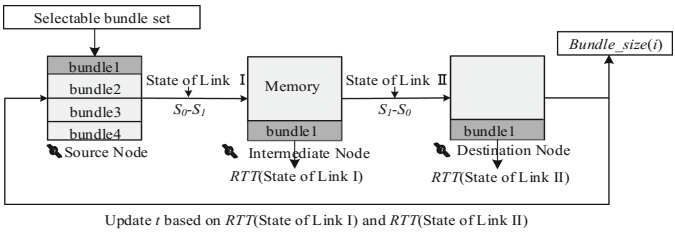


Fig. 2. Markov decision model based file delivery in a two-hop link

3.2 Markov Decision Strategy

Typically, the proposed Markov decision model consists of five associated parts as follows.

Part One: a state set S is defined as S: $\{S_0, S_1\}$.

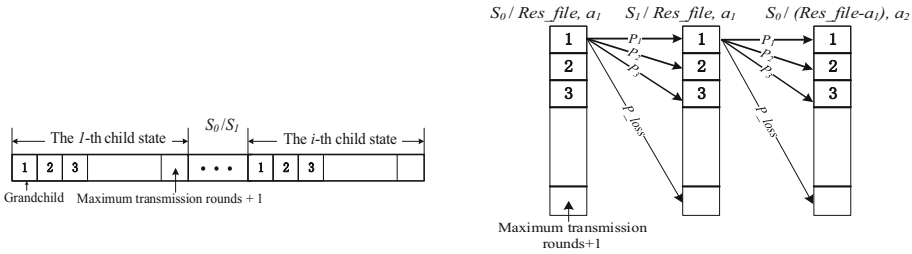
In the set, S_0 represents that the memory of intermediate node is empty without bundle. On the other side, S_1 represents that there is exactly an entire bundle in the memory. That is, S_0 and S_1 also express two transport processes of first hop and second hop, respectively. Here, the state of S_0/S_1 is determined by two following rules.

(a) Once the entire file is transferred completely, we need an absorbing state to stop the procedure. Therefore, we divide S_0 and S_1 individually into i child states, which is calculated according to file size and minimum bundle size. As a result, the i-th child state means that the remained file size is $Lfile - i \cdot Lb_{\min 1}$. If the remained file size is zero, a corresponding state is an absorbing state;

(b) Due to two bad channels, bundles are successfully delivered with differently uncertain latency. Therefore, time span of transition is accordingly different from one state to another state. Hence, we need further divide i-th child state in (a) into a certain number of grandchild states, which is exactly equal to the maximum transmission rounds of one bundle plus 1. In particular, the additional "1" means the transmission failed. The number of child state of S_0/S_1 shown in Fig. 3(a) is calculated by

$$NUM = Lfile/Lb_{\min 1} \times (max\_trans\_round + 1). \tag{14}$$

Part Two: an action set A includes all alternative bundle sizes. Defining a minimum bundle size of $Lb_{\min}$ as a basic unit, we determine a selectable set of bundle size with an adaptive step of $Lb_{\min}$ by A:$\{Lb_{\min 1}, Lb_{\min 2}, Lb_{\min 3}, \ldots\}$ and $Lb_{\min i} = i \times Lb_{\min 1}$.



(a) S0 /S1 child state (b) State transition diagram.

Fig. 3. S0/S1 child state and state transition diagram.

Part Three: a Markov strategy set π is the set of all selected bundle sizes at each state outputted by the proposed decision model.

Part Four: a transition probability P_i is calculated collectively by transmission rounds, bundle loss probability and bundle size in current link state.

By the transmission rounds, we can find the next state *s_next* and consequently calculate the transition probability from *s_current* to *s_next*, based on bundle loss probability. Figure 3(b) provides a state transition diagram. If the residual file size is *Res_file* within the current state of a child state S_0, then the next state must be the child state of S_1 and the residual file size is same as S_0 when we take action a_1. That is, next state and probability of transition are collaboratively determined by action and bundle loss rate P_{ef} in current link state.

In particular, the transition probability can be calculated as (15). In addition, *P_loss* represents a probability that one bundle is abandoned once transmission rounds exceeds the maximum rounds, as (16).

$$P_i = (1 - P_{ef}) \cdot P_{ef}^{i-1} \tag{15}$$

and

$$P\_loss = P_{ef}^{i}. \tag{16}$$

Part Five: a reward function r is the RTT of bundle under action a and transmission round i, as

$$r = RTT(s\_current, a) + (i - 1) \times CTRT(s\_current, a) \tag{17}$$

where *RTT* and *CTRT* are calculated respectively by (2) and (3), and *s_current* shows the current link state.

With two-hop dynamic ISL, we will obtain a group of link state at each time in the experiments by sampling the distance between two related nodes with an interval of Δt. In specific, we record a sequence of delivery times of each bundle during the file transfer. By accumulating the recording results until the sum of accumulation is more than Δt, we consider that the link state changes exactly at that time. Then, we input a

set of new parameters of link state I and link state II. Based on the new states, we can get a series of optimized bundle sizes by solving the proposed Markov decision model.

3.3 Value Iteration Algorithm

Generally, an optimal policy of Markov decision is solved by value iterative equation. In this paper, we design a corresponding Value Iterative Equation for the proposed decision model.

(1) If the current state is S_0,

$$v0(s) = \min_{a} \sum_{n} P(s\_next|s)\{r(s|\pi(s)) + v1(s\_next)\}, \tag{18}$$

in which $a \in A$ and $s\_current$ is rewritten as s in (18) and (19).

(2) If the current state is S_1,

$$v1(s) = \sum_{n} P(s\_next|s)\{r(s|\pi(s)) + v0(s\_next)\}. \tag{19}$$

The detailed Value Iterative Algorithm is shown in Table 3.

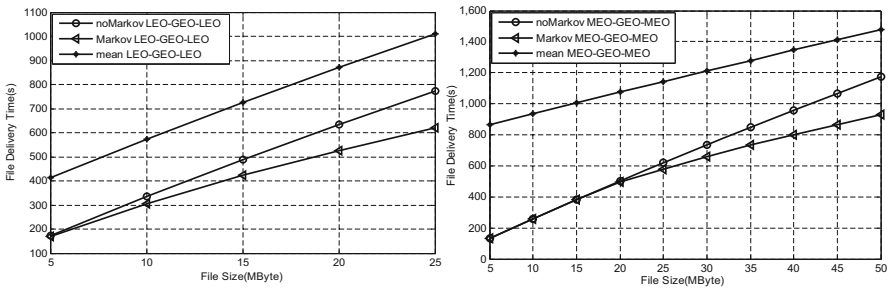
Table 3. Value iterative algorithm

Input matrix *S0,S1,A* $v0(num) \leftarrow 0;\ v1(num) \leftarrow 0;\ p(num) \leftarrow 0;$ // p is the action set
$loop \leftarrow num + max\_trans\_round + 1;$
While(*loop*){
  For each $s \in num$ {
    $(p\_trans1, trans\_round1) \leftarrow link\_state(s\_current\_link1, a);$
    $(p\_trans2, trans\_round2) \leftarrow link\_state(s\_current\_link2, a);$
    If $(trans\_round1 \le max\_trans\_round) \cup (trans\_round2 \le max\_trans\_round)$
      $v0(s) \leftarrow \min_a \sum_{n\_next} p\_trans1 \times (r(trans\_round1, a) + v1(s\_next));$ //calculate $v0$
      $p(s) \leftarrow a;$
      $(p\_trans2, trans\_round2) \leftarrow link\_state(s\_current\_link2);$ //calculate $v1$
      $v1(s) \leftarrow \sum_{n\_next} p\_trans2 \times (r(trans\_round2, a) + v0(s\_next));$
    End If
      $Refresh\_state(s\_current\_link1, s\_current\_link2);$ }
  End For
  $loop \leftarrow loop - 1;$ }
End While

4 Numerical Results

In this section, we make performance comparison with respect to bundle end-to-end delivery time. In the simulations, we assume the rate of CA_i is constant, and we sample link distance at 60 s interval. Furthermore, the number of state S_0/S_1 is calculated by (14).

The rounds of transmission can be calculated by bundle loss probability P_{ef}. In general, with the increasing of transmission rounds, the transmission failure probability decreases exponentially. When the failure probability is less than a threshold value, we consider that the bundle is sent successfully. Here, we set the threshold of 0.001, thus we can get the transmission rounds of one bundle. If the transmission round is more than a maximum value, however, we think the related bundle size is not accepted. In particular, L_{ca} is set by 100 Byte, R_{ca} is 8000 bps and C_0 is set with 104.22, respectively. The simulation results are presented in Figs. 4, 5 and 6.



a) LEO1-GEO-LEO2 b) MEO1-GEO-MEO2

Fig. 4. File delivery time in scenario LEO1-GEO-LEO2 and MEO1-GEO-MEO2

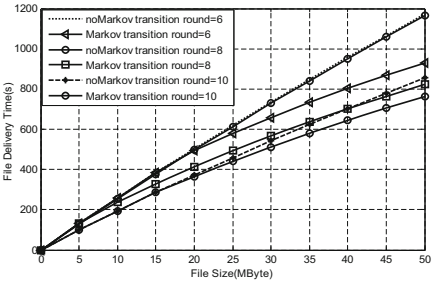


Fig. 5. Under different rounds.

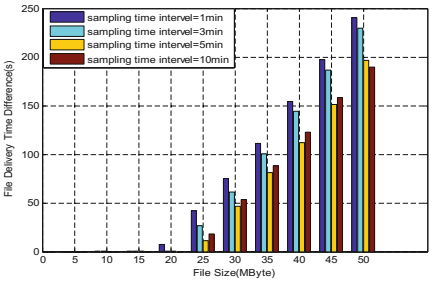


Fig. 6. Under different sampling intervals

The scenarios in Fig. 4(a) are defined by ISLs of LEO1-GEO-LEO2. Here, we set a maximum transmission rounds of six. In particular, we select a traditional optimal method and a mean value method separately as comparisons. The traditional optimal method is that we choose an optimum bundle size according to a set of constant link parameters. On the other side, the mean value method expresses the average value of all file delivery time under a group of fixed bundle sizes. If a bundle with chosen size is not able to be sent under the current link state due to its transmission round more than the allowed maximum round, the algorithm needs to wait for the arriving of next sampling time, which leads to an extra sampling time on file delivery time. Comparing the results from Fig. 4(a), we can observe that both traditional optimal method and Markov decision model have obvious optimization effects. It is noted that, with a file size less than 5 Mbyte, the delivery time under the two methods are equal. The reason

is that, since the end-to-end delivery time is less Δt, those trivial changes of link state during the delivery do scarcely make realistic impacts on the transmission. However, with the file sizes more than 5Mbyte, Markov decision can obtain relatively less delivery time than traditional method. With file size increasing, the optimization effect is more obvious, which is quite suitable for those bulk-data return missions over space links, such as disaster surveillance and remote imaging.

In Fig. 4(b), the scenario is defined by a MEO1-GEO-MEO2 link with maximum rounds of six. In particular, we assume that the two consecutive links do not increase or decrease synchronously. From the results, with file sizes less than 20 Mbyte, the delivery time is very short, since the change of distance is not enough to make effects. That is, Markov decision choose only one optimal value of bundle size in the current state, which will keep unchanging until the entire file is transmitted. When the variation of distance is enough large, Markov decision will adaptively change the strategy to get more reward. Hence, larger file size will obtain better optimization than unchanging strategy for all the different states.

In Fig. 5, with one of MEO1-GEO-MEO2 links, the results show that, if the maximum round increases in a proper range, the delivery delay will decrease accordingly. Because more bundle sizes in set A can be chose, Markov decision model will choose the better one on different states. In Fig. 6, the sampling interval are 1 min, 3 min, 5 min and 10 min respectively. The result shows that, if the sampling time interval is much smaller, the optimal effect is more obvious. However, when the sampling interval is too much, traditional method and Markov decision model will are nearly same under different sampling time intervals.

5 Conclusion

In this paper, we proposed a Markov decision base optimization model to achieve optimal bundle size for bundle end-to-end delivery over a dynamic two-hop ISL. By comparing delivery time of files with different sizes, respectively by using Markov decision, fixed optimal parameter and the mean method in end-to-end transmission, the simulation results show that the Markov decision model can effectively reduce file end-to-end delivery delay than traditional optimization method as the increasing of file size. Moreover, a greater file size can obtain better effects of the proposed algorithm. Besides, increasing a maximum transmission rounds or decreasing the sampling time of link distance can improve the optimization effects in certain degree.

Acknowledgment. The authors would like to express their high appreciations to the supports from the National Natural Science Foundation of China (61571156), National Science and Technology Major Project (91538110), and Natural Science Foundation of Guangdong Province (2016A030313661).

References

1. Feldmann, M., Walter, F.: Refining the ring road – delays and path lengths in a LEO satellite message-ferry network. In: IEEE International Conference on Communications, ICC 2017, May 2017, pp. 1–7 (2017)
2. Fraire, J.A., Feldmann, M., Burleigh, S.C.: Benefits and challenges of cross-linked ring road satellite networks: a case study. In: IEEE International Conference on Communications, ICC 2017, May 2017, pp. 1–7 (2017)
3. Yu, Q., Wang, R.: Modeling RTT for DTN protocol over asymmetric cislunar space channels. IEEE Syst. J. **10**(2), 556–567 (2016)
4. Yu, Q., Burleigh, S.C., Wang, R.: Performance modeling of Licklider transmission protocol (LTP) in deep-space communication. IEEE Trans. Aerosp. Electron. Syst. **51**(3), 1609–1620 (2015)
5. Jiang, F., Yang, Z., Li, Y.: Disruption-resilient bundle delivery mechanism in space DTNs with partial segments aggregation. IET Commun. **10**(13), 1646–1654 (2016)
6. Jiang, F., Lu, H.: Packet size optimization in delay tolerant networks. In: 2014 IEEE 11th Consumer Communications and Networking Conference, CCNC, pp. 392–397. IEEE, January 2014
7. Abdellaoui Alaoui, E.A., Agoujil, S., Hajar, M.: Stochastic modeling and analysis of DTN networks. In: Conference Proceedings, pp. 1–6. The Institute of Electrical and Electronics Engineers, Inc. IEEE, March 2016

An Energy-Efficient Localization-Based Geographic Routing Protocol for Underwater Wireless Sensor Networks

Kun Hao[1(✉)], Haifeng Shen[2], Yonglei Liu[3], and Beibei Wang[4]

[1] School of Computer and Information Engineering, Tianjin ChengJian University, Tianjin, China
Kunhao@tcu.edu.cn
[2] College of Science and Engineering, Flinders University, Adelaide, Australia
haifeng.shen@flinders.edu.au
[3] School of Electronic and Information Engineering, Tianjin University, Tianjin, China
sanxiong_1@163.com
[4] School of Control and Mechanical Engineering, Tianjin ChengJian University, Tianjin, China
wbbking@163.com

Abstract. An efficient routing protocol for data packet delivery is crucial to underwater sensor networks (UWSNs). However, design of such a protocol is a challenging task due to the characteristics of the acoustic channel used for communication by UWSNs. In this paper, we present a novel energy-efficient localization-based geographic routing protocol EEL, which uses location information and residual energy of sensor nodes to greedily forward data packets to sink nodes. EEL periodically updates the location information of nodes in an UWSN and effectively adapt to the dynamic topological changes of the network. Simulation results show that EEL can effectively locate the nodes and significantly improve the packet delivery ratio and reduce the energy consumption in a routing process.

Keywords: Underwater acoustic sensor networks · Localization
Geographic routing · Energy consumption

1 Introduction

Recently, underwater sensor networks (UWSNs) [1, 2] have received a great deal of attention from the wireless communication and networking communities. This technology is expected to mark a new era of scientific and industrial underwater monitoring and exploration applications, such as oceanographic data collection, disaster prevention, and pollutant content monitoring. As communication in a UWSN is through acoustic waves and high frequency radio waves are strongly absorbed in water, underwater communication has high bit errors, limited bandwidth capacity and high energy consumption. Further because GPS does not work underwater as the radio signals on which it depends cannot penetrate into water, it is non-trivial to obtain the exact location of each node in a UWSN. These issues lead to excessive data retransmission, high energy

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 365–373, 2018.
https://doi.org/10.1007/978-3-319-90802-1_32

consumption and low packet delivery ratio, which all contribute to the difficulties of designing an efficient and reliable routing protocol for UWSNs.

The routing protocols for UWSNs can be classified into categories of active routing, passive routing and geographic routing [3–5]. A geographic routing protocol is more energy-efficient than an active or passive protocol and thus able to prolong the lifespan of a UWSN as it can reduce flooding by exploiting the location information of sensor nodes, which is getting easier to acquire thanks to the development of localization technology.

The VBF (Vector Based Forwarding) [6] protocol defines a route vector comprising nodes from the source node to the destination node. During a routing process, each node does not save status information; instead it uses a forwarding factor to calculate the suppression time before forwarding is carried out in order to increase network energy efficiency by avoiding unnecessary forwarding, while the routing information is included in each data packet. The data forwarding of VBF is limited to a "virtual pipe". VBF can take full advantage of the location information for both the source and destination nodes to improve the efficiency of both routing and forwarding, thus saving energy. However, VBF may make local nodes to undertake excessive forwarding tasks, which results in fast energy consumption of these nodes and reduces the lifespan of the sensor network. In addition, the radius of pipe may significantly influence the routing performance.

In DBR (Depth Based Routing) [7], through specialized sensors (such as pressure sensors) that can obtain their own depth information, packets are forwarded from bottom to top with a threshold depth defined to control the efficiency of packet forwarding. The DBR protocol can achieve good performance in dense networks but may cause long transmission delay and high energy consumption in sparse networks.

Clearly the acquisition of location information on sensor nodes is indispensable to geographical routing algorithms. For static networks, nodes are usually deployed at fixed locations and as such the location information is known. However, an UWSN is usually deployed in a dynamic environment where the location information of the nodes has to be provided by a localization algorithm. The nodes on the surface can usually have their position information measured by means of GPS, but the underwater nodes have to be located using measurement algorithms. In Teymorian et al.'s work [8], the authors proposed to transform the three-dimensional underwater sensor network localization problem into its two-dimensional counterpart by using sensor depth information. Cheng et al. [9] proposed a positioning scheme TDOA, a time difference of arrival based localization scheme that does not require synchronizing the time of the nodes. However, a drawback is that it can not locate the nodes that reside outside the enclosed area by four anchor nodes.

This paper presents a novel geographic routing protocol EEL (Energy Efficient Localization-based), which uses location information and residual energy of sensor nodes to greedily forward data packets to sink nodes. Selection of a forwarding node is based on its NADV (Normalized Advancement) determined by its depth difference relative to the sending node and the residual energy of the node. Candidate nodes are sorted according to their NADV, and the node with the highest NADV is selected first to forward data packets. The protocol can periodically update the location information

of the nodes in an UWSN and effectively adapt to the dynamic topological changes of the network.

The rest of this paper is organized as follows. Section 2 presents a localization model and a NADV link metric model. Section 3 describes the EEL routing algorithm, followed by its performance evaluation in Sect. 4. Finally, Sect. 5 concludes the paper with a summary of major contributions.

2 Localization and Link Metric Models

2.1 TOA (Time of Arrival) Localization Model

The TOA localization [10] method is widely adopted for the positioning of underwater sensor nodes. It measures distance between nodes and can usually achieve higher positioning accuracy than other methods. TOA ranging is a simple form of communication between two nodes, where a timestamp is placed in each frame. The distance between the nodes is obtained through multiplying the signal transmission time by the average propagation speed of the signal. We assume that the depth information of sensor nodes can be obtained through auxiliary means, such as pressure sensors and as such the three-dimensional underwater sensor node localization problem is reduced to a two-dimensional positioning problem in which only three beacon nodes are required to complete a localization process.

Considering three beacon nodes A, B, and C, their position coordinates are denoted (x_a, y_a, z_a), (x_b, y_b, z_b), and (x_c, y_c, z_c) respectively and their underwater acoustic signal transmission time are denoted Δt_a, Δt_b, and Δt_c respectively. The underwater acoustic signal transmission time Δt is subject to time measurement errors, signal reflection, anti-radiation and other unknown factors. For the sake of simplicity yet without losing generality, we assume that the time measurement error follows a Gauss distribution of zero mean, that is $t_n \sim N(0, \sigma_t^2)$. The time measurement error of nodes A, B and C are denoted t_{na}, t_{nb} and t_{nc}. For node U whose position coordinates are (x_u, y_u, z_u) in which z_u is known through pressure sensors, its location is derived through Eq. (1):.

$$\begin{cases} \sqrt{(x_u - x_a)^2 + (y_u - y_a)^2 + (z_u - z_a)^2} = v(\Delta t_a + t_{na}) \\ \sqrt{(x_u - x_b)^2 + (y_u - y_b)^2 + (z_u - z_b)^2} = v(\Delta t_b + t_{nb}) \\ \sqrt{(x_u - x_c)^2 + (y_u - y_c)^2 + (z_u - z_c)^2} = v(\Delta t_c + t_{nc}) \end{cases} \tag{1}$$

2.2 NADV Link Metric Model

NADV (Normalized Advancement) [11] is a link metric model used in multi-hop wireless networks. The purpose of the NADV model is to find an optimal balance between the proximity of the destination and the cost of the link. In this paper, the link cost is the

energy consumed by a node to transmit data, while the proximity to the destination is the distance from a transmitting node to the sink node on the surface.

As shown in Fig. 1, node B has a packet to send to node S, which however is not within B's communication range. Therefore B has to rely on its neighboring nodes to relay the packet. Neighboring nodes A and C are both within B's communication range, so the same energy is consumed by B to send data to A or C. However, as the distance from A to S is shorter than that from C to S, B would choose node A to relay data to destination S in order to reduce the number of data forwarding and consequently minimize the energy consumption in the whole data transmission process. Nonetheless, if node A has a higher transmission error rate than C does, it would be more probable for node B to retransmit lost data, resulting in additional power consumption and consequently high link cost. This scenario particularly illustrates the importance of finding a balance between the proximity of the next hop and the link cost.

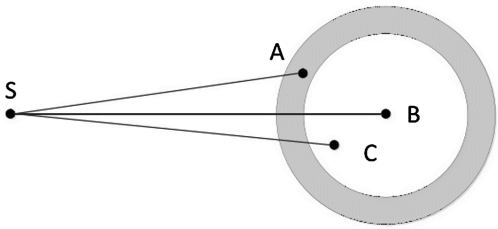


Fig. 1. NADV model diagram

In the NADV model, the distance between the source node B and the neighboring node n relative to the destination node is defined by Eq. (2):

$$\mathrm{ADV}(n) = D(B) - D(n) \tag{2}$$

where D(n) represents the distance from node n to destination node S. The larger ADV(n) is, the closer node n can forward the packet to the target node. Assuming that the link cost from node B to node n is denoted Cost (n), NADV of the neighboring node n represents the distance of transmitting data from node n with one unit energy consumption, which is defined by Eq. (3):

$$\mathrm{NADV} = \frac{ADV(n)}{Cost(n)} \tag{3}$$

Suppose the probability that the data will be successfully passed on to the neighboring node n is., which is calculated using the models described in previous work [11, 12]. If the link cost is expressed by $1/P(n)$, then

$$\mathrm{NADV} = ADV(n) * P(n) \tag{4}$$

3 The EEL Routing Algorithm

In the three-dimensional dynamic network architecture adopted in this paper, the beacon nodes are deployed on the water surface, and their location information is obtained through GPS. The position coordinates of the nodes to be located can be obtained by Eq. (1). According to the different depth of work, location of nodes needs to consider two cases: shallow sea and deep sea. Figure 2 depicts the localization of underwater sensor nodes.

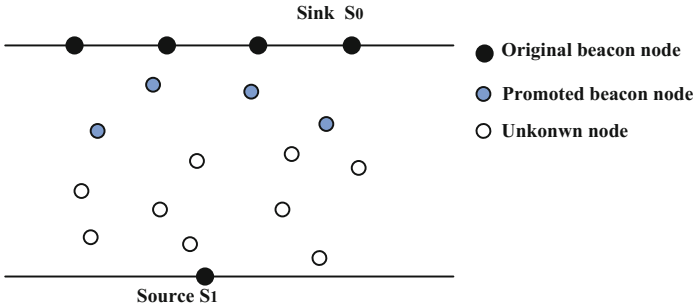


Fig. 2. Schematic diagram of underwater sensor node diffusion localization

When all nodes of a network are working in a shallow sea, any unknown node in the network can communicate directly with at least three beacon nodes to complete its localization. For a node in a deep sea, it has to rely on diffusion localization. In Fig. 2, the original beacon nodes are deployed on the surface of water and periodically broadcast their location information by sending location packets. For an unknown node near the surface of water, its localization starts with the three edge location and after that it becomes a "promoted beacon node". Other unknown nodes carry out localization through original beacon nodes or enhanced beacon nodes before being converted to "promoted beacon nodes". Each beacon node broadcasts its location information to be obtained by an unknown node in the network, which is subsequently transformed into a "beacon node". The localization process proceeds as such until all unknown nodes in the network are identified.

A sensor node can calculate the relative distances between itself and its neighboring nodes through the TOA localization algorithm in order to generate a set of next-hop candidate nodes from which the next hop node is selected for forwarding data packets. In this paper, we improve the NADV algorithm by introducing the residual energy of nodes so that nodes with higher residual energy are more likely to be selected as the next hop, which can balance the energy consumption and extend the lifespan of nodes in the network.

To avoid energy consumed by data wandering between nodes of similar depth, we also define a depth threshold to control the next hop selection as defined in Eq. (5) [13]: if the depth difference is less than the threshold of the neighboring node, only the depth and the depth difference are considered; however if the depth difference is larger than

the threshold value of the neighboring node, the residual energy of the node is also considered.

$$\mathrm{ADV}(n) = \begin{cases} |D - D(n)|/R, & |D - D(n)| < \theta \\ |D - D(n)|/R + Energy(n)/E, & |D - D(n)| \geq \theta \end{cases} \tag{5}$$

where D is the depth of the sending node, D(n) is the depth of the neighboring node n, R is the communication radius of the node, θ is the depth threshold, Energy(n) is the residual energy of the neighboring node n, and E is the initial energy of the node. Thus, candidate nodes with higher residual energy have a higher probability to be selected to relay data when they have similar depths. When the neighboring nodes are close to the sending nodes, the distance difference is used as a reference so that short distance relay of data can be avoided as it would generate unnecessary energy consumption. The candidate nodes are sorted according to NADV, and the node with the highest NADV is first selected to forward packets.

4 Simulation Results

To evaluate the performance of the proposed EEL routing algorithm, we compare it with the existing protocols of Flood and VBF using Aqua-Sim [14] as the routing protocol simulator. We randomly deploy 800 sensor nodes in a three-dimensional region of 2000 m * 2000 m * 2000 m and 64 sink nodes at a sea surface region of 2000 m * 2000 m. Each sensor node has an initial energy $E_0 = 100$ J, a transmission range of R = 600 m, a positioning time of 100 s, and a maximum/minimum movement speed of 3 m/s and 0.2 m/s respectively. Assume that the packet size is 100 kB and energy consumption rate of transmitting data is at 60 uJ/bit.

4.1 Effect of the Number of Sink Nodes on Positioning Accuracy

Figure 3 shows the effect of the number of underwater nodes on the average positioning error. With diffusion positioning, unknown nodes may be converted into “promoted beacon nodes” in the process of localization, which consequently increases the intensity of beacons in the network. Therefore, increasing the number of unknown nodes can also improve positioning accuracy. It is worth mentioning that node density may have a negative influence on positioning accuracy, which however is relatively low as compared to the positive influence of beacon intensity.

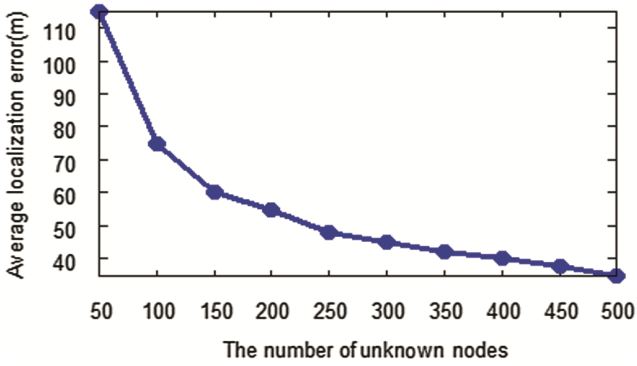


Fig. 3. The influence of the number of underwater nodes on the average localization error

4.2 Packet Delivery Radio

Figure 4 shows the data transfer rate of the three protocols, where the flood routing is optimal, while the packet delivery ratio of EEL is higher than that of the VBF protocol, thanks to the positioning technology used in the protocol. For all the three protocols, with the increase of network nodes, the density of nodes gets higher and as such the distance between nodes becomes shorter, the connectivity rate gets higher, and so does the data delivery rate.

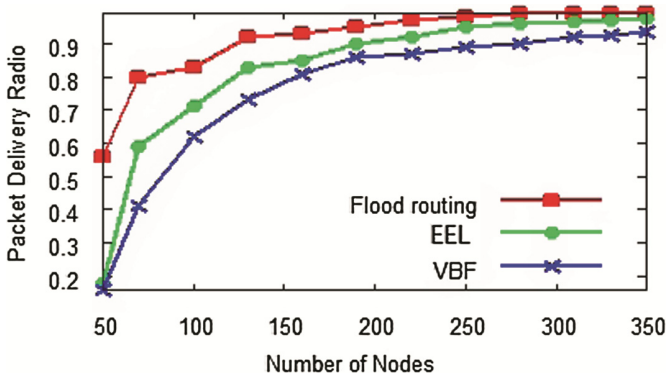


Fig. 4. The influence of the number of nodes on packet delivery radio

4.3 Energy Consumption

As shown in Fig. 5, flood routing has the highest energy consumption, VBF routing performs better than flood routing, while EEL routing performs the best. The total energy consumption in the network includes the energy consumed by the routing process and the energy consumed by the localization process. When the network is sparse, the average energy consumption of the network would be high as the packet delivery rate

is low in the routing process and as such the positioning process would dominate the energy consumption. With the increase of the number of nodes in the network, the packet delivery rate in the routing process increases and consequently the average energy consumption decreases. When the number of nodes reaches a certain level, routing instead of positioning becomes dominant in the energy consumption and as such the average energy consumption starts to increase with the number of nodes.

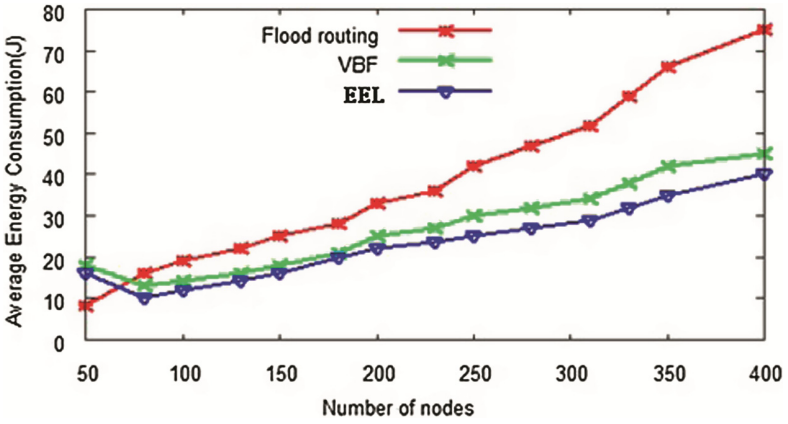


Fig. 5. The influence of the number of nodes on average energy consumption

5 Conclusion

The location and routing issues are two major challenges for UWSNs. In this paper, we have proposed a novel routing protocol EEL using geographic and location information of nodes in a UWSN. Considering the three-dimensional dynamic UWSNs, we have combined these two aspects to design the routing protocol. During the localization process, the diffusion localization can effectively locate the nodes in UWSNs. During the routing process, EEL uses a new greedy approach to deliver packets to sink nodes, thus improving data transmission ratio and reducing energy consumption. However, high energy consumption is a drawback of this algorithm. As future work, we intend to investigate other important geographic routing features, such as average end-to-end delay and average number of candidates, in order to improve the performance of EEL.

Acknowledgments. This research was supported by a National Natural Science Fund Project (61571318), Hainan Technology Project (2014ZDXM0236), Qinghai Technology Project (2015-ZJ-904), and China Postdoctoral Science Foundation (2016M601265).

References

1. Xu, W., Yan, S., Ji, F.: Marine information gathering, transmission, processing, and fusion: current status and future trends. Sci. Sin. Inf. **46**(8), 1053–1085 (2016)
2. Guo, Z., Luo, H., Hong, F., Yang, M., Ni, L.M.: Current progress and research issues in underwater sensor networks. J. Comput. Res. Dev. **47**(3), 377–389 (2010)
3. Cho, H.H., Chen, C.Y., Shih, T.K., Chao, H.C.: Survey on underwater delay/disruption tolerant wireless sensor network routing. IET Wirel. Sens. Syst. **4**(3), 112–121 (2014)
4. Han, G., Jiang, J., Bao, N., et al.: Routing protocols for underwater wireless sensor networks. IEEE Commun. Mag. **53**(11), 72–78 (2015)
5. Sabbineni, H., Chakrabarty, K.: Location-aided flooding: an energy-efficient data dissemination protocol for wireless-sensor networks. IEEE Trans. Comput. **54**(1), 36–46 (2005)
6. Xie, P., Cui, J.-H., Lao, L.: VBF: vector-based forwarding protocol for underwater sensor networks. In: Boavida, F., Plagemann, T., Stiller, B., Westphal, C., Monteiro, E. (eds.) NETWORKING 2006. LNCS, vol. 3976, pp. 1216–1221. Springer, Heidelberg (2006). https://doi.org/10.1007/11753810_111
7. Yan, H., Shi, Z.J., Cui, J.-H.: DBR: depth-based routing for underwater sensor networks. In: Das, A., Pung, H.K., Lee, F.B.S., Wong, L.W.C. (eds.) NETWORKING 2008. LNCS, vol. 4982, pp. 72–86. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-79549-0_7
8. Teymorian, A.Y., Cheng, W., Ma, L., Cheng, X., Lu, X., Lu, Z.: 3D underwater sensor network localization. IEEE Trans. Mob. Comput. **8**(12), 1610–1621 (2009)
9. Cheng, X., Shu, H., Liang, Q., Du, D.H.C.: Silent positioning in underwater acoustic sensor networks. IEEE Trans. Veh. Technol. **57**(3), 1756–1766 (2008)
10. Han, S., Yue, J., Meng, W., Wu, X.: A localization based routing protocol for dynamic underwater sensor networks. In: IEEE GLOBECOM, pp. 1–6 (2016)
11. Coutinho, R.W.L., Boukerche, A., Vieira, L.F.M., Loureiro, A.A.F.: Geographic and opportunistic routing for underwater sensor networks. IEEE Trans. Comput. **65**(2), 548–561 (2016)
12. Hao, K., Jin, Z., Shen, H.: An efficient and reliable geographic routing protocol based on partial network coding for underwater sensor networks. Sensors **15**(6), 12720–12735 (2015)
13. Shi, Y.: Energy-aware pressure routing for underwater sensor networks. Master Degree thesis, Xidian University (2014)
14. Zhu, Y., Martin, R., Cui, J.H.: Aqua-Sim 2.0: an NS-2 based simulator for underwater sensor networks. In: The Eighth ACM International Workshop on Underwater Networks, WUWNet (2013)

Power Allocation for Full Duplex Decode-and-Forward Cooperative Relay System

Shuai Han, Yi Zhang, Weixiao Meng(✉), and Ningqing Liu

Communications Research Center, Harbin Institute of Technology, Harbin, China
wxmeng@hit.edu.cn

Abstract. The 5G communication system requires higher data rates and energy efficiency. Full-duplex (FD) communications can double the spectral efficiency in ideal conditions and in full-duplex relay systems the relay node works under full-duplex mode. There is a trade off between the signal and interference at the relay node because the transmitting signal of the node can be interference signal and desired signal in different links in the system, respectively. Proper power allocation can both suppress the residual self-interference for better performance and save power of the FD system. In this paper, we propose a power allocation approximation algorithm and a power allocation method based on genetic algorithm (GA) for a FD decode-and-forward (DF) cooperative relay system with residual self-interference. The end-to-end outage probability is chosen as the criterion of power allocation problem. Both the global power constraint and individual power constraint are investigated. The approximation algorithm shows great simplicity and has better performance with high SNR. For GA algorithm, numerical results show that the proposed power allocation scheme obviously improves the performance of the FD relay system with good convergence performance.

Keywords: Full-duplex · Power allocation · Relay · Genetic algorithm

1 Introduction

Full duplex which means transmitting and receiving simultaneously in the same frequency band has become a promising technique in 5G communication [1]. It can double the spectral efficiency in ideal conditions at the side of conventional half duplex schemes. However, the most crucial issue is its strong self-interference (SI). Lots of work has been done and self-interference cancellation techniques make full duplex feasible in communication systems. In practice, the SI can not

N. Liu—This work is supported by National Natural Science Foundation of China (61471143) and the Provincial Natural Science Foundation of Heilongjiang, China (No. ZD2017013).

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 374–386, 2018.
https://doi.org/10.1007/978-3-319-90802-1_33

be eliminated completely and residual SI must be taken into account in FD relay systems [2].

In [3–5], the outage probability of full duplex decode-and-forward relay system for both dual-hop and multi-hop is derived. A new distributed FD Alamouti scheme for cooperative relay system is proposed in [6] and the outage probability and the diversity-multiplexing tradeoff are obtained. In addition, the optimization problem of power allocation for dual-hop full duplex DF relay system under power constraint conditions is solved in [7]. For full duplex decode-and-forward (DF) relay system, there is a performance tradeoff between the link from the source to the relay and the link from the relay to the destination [2]. This is because, the transmitting power of the relay node is not only the desired signal for the destination node but also the SI power for the relay node itself which degrades the performance of the link from the source to the relay. Thus, an effective power allocation strategy is necessary for performance improvement and power conservation.

In this paper, we aim at power allocation for the FD cooperative DF relay system and acquire quasi-optimal transmitting power for the nodes. Considering the FD cooperative relay system with self-interference, the outage probability of the system we derived is non-convex which is quite complex to solve through numerical methods. We use taylor expansion to obtain an approximate objective function which is easy to be optimized and it has a good performance in high SNR region. In order to get more accurate results for general conditions, we adopt GA algorithm to solve the problem. Compared with traditional search algorithms, the genetic algorithm (GA) is a global optimization technique that avoids many of the shortcomings exhibited by local search techniques on difficult search spaces [8]. Moreover, the GA has been modified for our problem as follows: (1) We introduce a penalty function to fulfill the constraint conditions and avoid local convergence. (2) Variable fitness function parameter is employed in the fitness value calculation operator which can avoid premature convergence. Simulation results show that our proposed algorithm can obtain feasible solutions with satisfying convergence performance.

The remainder of this paper is outlined as follows. In Sect. 2, we illustrate the system model of the FD relay system. And the power allocation problem is proposed and solved in Sect. 3. The simulation results are presented in Sect. 4 and the conclusion is drawn in the last section.

2 System Model

In this section, we will introduce the basic system model of the full duplex DF cooperative relay system, then derive the mathematical model of the FD system with different power at transmitting antennas. Figure 1 shows the system model of the FD relay system. It contains a source node R_0, a relay node R_1 and a destination node R_2. In FD relay mode, the received signal of relay node R_1 consists of two parts: the desired signal from source node R_0 and the self-interference signal from its own transmitting antenna. The received signal of destination node

also contains two different signals: the desired signal from source node R_0 and the desired signal from relay node R_1. According to [6], the source transmission is ordered into frames and blocks. And compared with half-duplex (HD) mode, FD only needs 3/4 of half-duplex symbols. We assume Rayleigh frequency non-selective fading channel and it can be expressed as $h_{i,j} \sim CN(0, \Omega_{ij})$ where $i \in \{0,1\}, j \in \{1,2\}$ means the channel fading coefficient from node R_i to node R_j, and $h_{1,1}$ denotes residual self-interference of the relay node from its transmitting antenna to its receiving antenna [6]. The transmission of the cooperative scheme is divided into three phases. In the first phase, the source node R_0 transmits symbol x_1 and the received symbol at node R_1 and R_2 can be written as

$$y_{R11} = \sqrt{p_T} h_{0,1} x_1 + n_{R11}, \tag{1}$$

$$y_{R21} = \sqrt{p_T} h_{0,2} x_1 + n_{R21}, \tag{2}$$

where p_T denotes the transmit power of node R_0 in the first phase and n_{Rij} denotes the normalized AWGN at receive nodes. In the second phase, R_0 transmits symbol x_2 and R_1 transmits symbol x_1 in the meantime. The received symbol at node R_1 and R_2 can be written as

$$y_{R12} = \sqrt{p_0} h_{0,1} x_2 + \sqrt{p_1} h_{1,1} x_1 + n_{R12}, \tag{3}$$

$$y_{R22} = \sqrt{p_1} h_{0,2} x_2 + \sqrt{p_2} h_{1,2} x_1 + n_{R22}, \tag{4}$$

where p_0 and p_1 denote the transmit power of node R_0 and R_1 respectively. In the third phase, R_0 transmits symbol $-x_1^*$ while R_1 transmits symbol x_2^*, where $(\cdot)^*$ denotes the conjugate. The received symbol at node R_2 can be written as

$$y_{R23} = -\sqrt{p_1} h_{0,2} x_1^* + \sqrt{p_2} h_{1,2} x_2^* + n_{R23}. \tag{5}$$

By using the equivalent MIMO channel model, the scheme above can be expressed as

$$Y_{R2} = Hx + n_{R2}, \tag{6}$$

where $Y_{R2} = [y_{R21}\, y_{R22}\, y_{R23}^*]^T$; $H = \left[\sqrt{p_T} h_{0,2} 0;\ \sqrt{p_1} h_{1,2}\ \sqrt{p_0} h_{0,2};\ \sqrt{p_0} h_{0,2}^*\ \sqrt{p_1} h_{1,2}^*\right]$; $x = [x_1\ x_2]^T$; $n_{R2} = [n_{R21}\, n_{R22}\, n_{R23}^*]^T$. Then the capacity can be derived as

$$\begin{aligned} C_{FD} = \tfrac{1}{3}\log_2 \Big[&\left(1 + p_0 |h_{0,2}|^2 + p_1 |h_{1,2}|^2\right) \\ &\left(1 + (p_0 + p_T)\, |h_{0,2}|^2 + p_1 |h_{1,2}|^2\right) \Big], \end{aligned} \tag{7}$$

The outage probability of this scheme can be formulated as

$$P_{out} = P_{FD}\,(1 - P_{SR}) + P_{SD} P_{SR}, \tag{8}$$

with

$$P_{FD} = P\{C_{FD} < R\}, \tag{9}$$

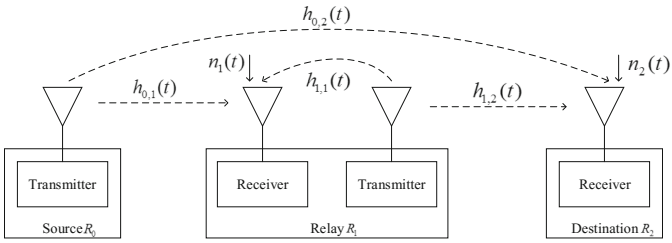


Fig. 1. System model of the full duplex DF cooperative relay system.

$$P_{SR} = P\left\{\log_2\left(1+\frac{p_0|h_{0,1}|^2}{1+p_1|h_{1,1}|^2}\right) < \frac{3}{2}R\right\}, \tag{10}$$

$$P_{SISO} = P\left\{\log_2\left(1+p_T|h_{0,2}|^2\right) < R\right\}, \tag{11}$$

where P_{FD} and P_{SISO} denote the outage probability of FD cooperative and SISO mode, respectively. And P_{SR} denotes the outage probability of the source to relay link.

For Rayleigh fading channel, $|h_{i,j}|$ is Rayleigh distributed and we can express the PDF of $|h_{i,j}|^2$ as

$$f_{|h|^2}(y) = \frac{1}{\Omega_{i,j}} e^{-\frac{y}{\Omega_{i,j}}}, \tag{12}$$

Through (12) we can calculate the three parts of P_{out} as follows: The outage probability of SISO mode with transmitting power p_T can be derived as

$$\begin{aligned} P_{SISO} &= P\left\{\log_2\left(1+p_T|h_{0,2}|^2\right) < R\right\} \\ &= \int_0^{\frac{2^R-1}{p_T}} \frac{1}{\Omega_{0,2}} e^{-\frac{y}{\Omega_{0,2}}} dy \\ &= 1 - e^{-\frac{2^R-1}{p_T\Omega_{0,2}}}. \end{aligned} \tag{13}$$

And P_{SR} can be derived as

$$\begin{aligned} P_{SR} &= P\left\{\log_2\left(1+\tfrac{p_0|h_{0,1}|^2}{1+p_1|h_{1,1}|^2}\right) < \tfrac{3}{2}R\right\} \\ &= \int_0^{\infty}\int_0^{\frac{p_1}{p_0}(2^{\frac{3R}{2}}-1)y+\frac{2^{\frac{3R}{2}}-1}{p_0}} \frac{1}{\Omega_{0,1}} e^{-\frac{x}{\Omega_{0,1}}} dx \frac{1}{\Omega_{1,1}} e^{-\frac{y}{\Omega_{1,1}}} dy \\ &= 1 - \frac{1}{1+\frac{\Omega_{1,1}p_1}{\Omega_{0,1}p_0}(2^{\frac{3R}{2}}-1)} e^{-\frac{2^{\frac{3R}{2}}-1}{p_0\Omega_{0,1}}}. \end{aligned} \tag{14}$$

Because P_{FD} can not get a closed-form solution, we derive a lower and an upper bound for it. Based on $C_{FD} < \frac{1}{3}\log_2\left[1+(p_0+p_T)|h_{0,2}|^2+p_1|h_{1,2}|^2\right]^2$

and $C_{FD} > \frac{1}{3}\log_2\left[1 + p_0|h_{0,2}|^2 + p_1|h_{1,2}|^2\right]^2$, the lower and upper bound for the outage probability of the FD scheme are obtained, respectively. Thus, P_{FD} can be expressed as

$$P_{FD} = P\left\{p|h_{0,2}|^2 + p_1|h_{1,2}|^2 < Z\right\}, \tag{15}$$

where $Z = 2^{\frac{3R}{2}} - 1$. Moreover, when $p = p_0$, it denotes the upper bound and when $p = p_0 + p_T$, it denotes the lower bound. Finally, the outage probability of the cooperative scheme can we written as

$$\begin{aligned} P_{FD} &= \int_0^{\frac{Z}{p}} \int_0^{\frac{Z}{p_1} - \frac{p}{p_1}y} \frac{1}{\Omega_{1,2}} e^{-\frac{x}{\Omega_{1,2}}} dx \frac{1}{\Omega_{0,2}} e^{-\frac{y}{\Omega_{0,2}}} dy \\ &= \begin{cases} 1 - e^{-\frac{z}{p\Omega_{0,2}}} - \frac{z}{p\Omega_{0,2}} e^{-\frac{z}{p_1\Omega_{1,2}}} & p\Omega_{0,2} = p_1\Omega_{1,2} \\ 1 - \frac{1}{1-\frac{\Omega_{1,2}p_1}{\Omega_{0,2}p}} e^{-\frac{z}{p\Omega_{0,2}}} - \frac{1}{1-\frac{\Omega_{0,2}p}{\Omega_{1,2}p_1}} e^{-\frac{z}{p_1\Omega_{1,2}}} & p\Omega_{0,2} \neq p_1\Omega_{1,2} \end{cases}. \end{aligned} \tag{16}$$

3 Power Allocation Algorithm

In this section, we adopt a approximation algorithm and a GA to solve the power allocation problem of the FD cooperative relay system. Our target is to minimize the end-to-end outage probability and two different constraint conditions are defined: global power constraint and individual power constraint.

3.1 Global Power Constraint and Individual Power Constraint

There are three nodes in the relay system and two of them transmit symbols. Global power constraint means the total power of the source node R_0 and the relay node R_1 does not exceed the P_{Total}. The power allocation problem which is an optimization problem can be expressed as

$$\begin{aligned} \min\ & P_{out} = P_{FD}(1 - P_{SR}) + P_{SD}P_{SR} \\ \text{s.t.}\ & p_0 + p_1 = P_{Total} \end{aligned}, \tag{17}$$

where P_{FD}, P_{SR} and P_{SD} are referred to (16), (14) and (13), respectively. P_{Total} denotes the total power of the system and $p_T = P_{Total}$ means the source node's transmitting power in the first phase.

Individual power constraint means the power of each node does not exceed the P_{Max}. The optimization problem can be expressed as

$$\begin{aligned} \min\ & P_{out} = P_{FD}(1 - P_{SR}) + P_{SD}P_{SR} \\ \text{s.t.}\ & 0 < p_0 \leq P_{Max} \\ & 0 < p_1 \leq P_{Max} \end{aligned}, \tag{18}$$

where P_{Max} denotes the maximum power of a single node and $p_T = P_{Max}$ means the source node's transmitting power in the first phase.

3.2 Power Allocation Approximation Algorithm

We choose the upper bound of P_{FD} as the objective function. The objective function can be written as

$$P_{out} = P_{FD}\left(1 - P_{SR}\right) + P_{SD}P_{SR}\,, \tag{19}$$

where $P_{FD} = 1 - \frac{1}{1-\frac{\Omega_{1,2}p_1}{\Omega_{0,2}p_0}}e^{-\frac{z}{p_0\Omega_{0,2}}} - \frac{1}{1-\frac{\Omega_{0,2}p_0}{\Omega_{1,2}p_1}}e^{-\frac{z}{p_1\Omega_{1,2}}}$. The objective function is consist of fraction and exponential function which make it difficult to solve. By applying taylor expansion we can rewrite the exponential function in P_{FD} as

$$\begin{aligned} e^{-\frac{z}{p_0\Omega_{0,2}}} &= 1 - \frac{z}{p_0\Omega_{0,2}} + \frac{z^2}{2p_0^2\Omega_{0,2}^2} + \cdots . \\ e^{-\frac{z}{p_1\Omega_{1,2}}} &= 1 - \frac{z}{p_1\Omega_{1,2}} + \frac{z^2}{2p_1^2\Omega_{1,2}^2} + \cdots . \end{aligned} \tag{20}$$

By substituting (20) into P_{FD}, P_{FD} can be expressed as

$$\begin{aligned} P_{FDAL}(R) &= 1 - \left(\frac{1}{1-\frac{\Omega_{1,2}p_1}{\Omega_{0,2}p_0}}e^{-\frac{z}{p_0\Omega_{0,2}}} + \frac{1}{1-\frac{\Omega_{0,2}p_0}{\Omega_{1,2}p_1}}e^{-\frac{z}{p_1\Omega_{1,2}}}\right) \\ &= 1 - \left[1 - \frac{z^2}{2p_0\Omega_{0,2}\Omega_{1,2}p_1}\right] \\ &= \frac{z^2}{2p_0\Omega_{0,2}\Omega_{1,2}p_1}. \end{aligned} \tag{21}$$

Through ignoring the 1 in the denominator of (10), we can obtain approximate P_{SR} as

$$\begin{aligned} \pi(R) &\approx P\left\{\log_2\left(1 + \frac{p_0|h_{0,1}|^2}{p_1|h_{1,1}|^2}\right) < \frac{3R}{2}\right\} \\ &= P\left\{|h_{0,1}|^2 < \frac{p_1}{p_0}(2^{\frac{3R}{2}} - 1)|h_{1,1}|^2\right\} \\ &= 1 - \frac{1}{1+\frac{\Omega_{1,1}p_1}{\Omega_{0,1}p_0}(2^{\frac{3R}{2}}-1)}. \end{aligned} \tag{22}$$

Then the outage of the system can be written in a simplifying form as

$$\begin{aligned} &P_{out} = P_{FDAL}(R)(1-\pi(R)) + P_{SISO}(R)\pi(R) \\ &\approx \frac{z^2}{2p_0\Omega_{0,2}\Omega_{1,2}p_1}\frac{1}{1+\frac{\Omega_{1,1}p_1}{\Omega_{0,1}p_0}z} + \left(1 - \frac{1}{1+\frac{\Omega_{1,1}p_1}{\Omega_{0,1}p_0}z}\right)\left(1 - e^{-\frac{2^R-1}{p_T\Omega_{0,2}}}\right) \\ &= \frac{A - Kp_0p_1}{p_1(p_0 + Bp_1)} + K, \end{aligned} \tag{23}$$

where $z = 2^{\frac{3R}{2}} - 1, A = \frac{z^2}{2\Omega_{0,2}\Omega_{1,2}}, B = z\frac{\Omega_{1,1}}{\Omega_{0,1}}, K = 1 - e^{-\frac{2^R-1}{p_T\Omega_{0,2}}}$. The function (23) will be the new objective function of the power allocation algorithm.

First, we consider global power constraint problem. By substituting the constraint condition $p_0 = P_{Total} - p_1$, we can get the final problem

$$\min F = \frac{A - K(P_{Total} - p_1)p_1}{p_1(P_{Total} + Cp_1)}, \tag{24}$$

where $C = B - 1$. It can be turn into a quadratic function optimization problem. The power allocation results are as follows

$$\begin{aligned} p_1 &= \frac{2AC + \sqrt{4A^2C^2 + 4ABKP_{Total}^2}}{2BKP_{Total}} \\ p_0 &= P_{Total} - p_1, \end{aligned} \tag{25}$$

For individual power constraint conditions, we can get

$$\begin{aligned} p_1 &= \sqrt{\frac{2AB \pm \sqrt{4A^2B^2 + 4\frac{KB^2}{A-1}\frac{A^2}{(A-1)K}}}{2KB^2/(A-1)}} \\ p_0 &= \frac{KBp_1^2 + A}{(A-1)Kp_1}. \end{aligned} \tag{26}$$

If the results beyond the scope of the constraint, the power will be set as P_{Max}.

3.3 Power Allocation Based on Genetic Algorithm

The objective function (19) reveals to be a non-convex function which is difficult to get an analytic solution. GA is a global searching algorithm with low complexity. It is an iterative procedure which mainly contains four parts: a genetic representation, a fitness function, genetic operators and control parameters. The basic structure of GA is shown in Fig. 2. In GA, each solution to the problem is coded as a fixed-length binary string which is called a 'chromosome' and every bit of the strings is called a 'gene'. A group of chromosomes are called population. For every iteration, the population produce new chromosomes and get close to the best solution gradually.

(1) Fitness value is a way to evaluate the quality of the solution which is related to the objective function and decided by fitness function. In our design, the objective function is the outage probability of the FD relay system P_{out} which is in the interval $[0, 1]$. In GA, we apply $1 - P_{out}$ as our basic fitness function. As a result, we consider larger value as better results. For the two different constraint conditions we use linear scaling (27) and exponential scaling (28), respectively.

$$f_{fitness} = b\left(1 - P_{out}\right), \tag{27}$$

$$f_{fitness} = e^{c(1-P_{out})}. \tag{28}$$

In addition, in order not to surpass the restriction of the global power constraint, we adopt a penalty function to fulfill the constraint conditions. If power of the two nodes does not satisfy the conditions in (17), the fitness value of this chromosome will shrink by (29) and be marked as a infeasible solution.

$$f_{fitness}^{*} = f_{fitness}\left[1 - \left(\frac{\Delta}{\Delta_{\max}}\right)^{a}\right], \tag{29}$$

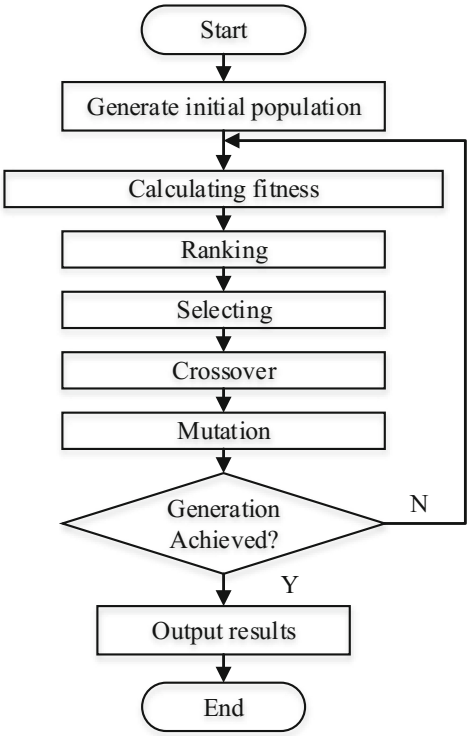


Fig. 2. The flow chart of GA.

where $\Delta = p_0 + p_1 - P_{Total}$ and $\Delta_{\max}$ is the maximum of the whole population. In this way, these infeasible solutions can be appropriately reserved for the next generation to ensure genetic diversity. Moreover, the parameter a in (29) varies with generation according to (30)

$$a = \frac{1 - a_0}{G - 1} g + \frac{a_0 G - 1}{G - 1}, \tag{30}$$

where a_0 is an initial value, G and g are total generation and current iteration generation, respectively.

(2) After finishing calculating the fitness values of the population, we will rank the chromosome and find the best one in this generation. Certainly, the chromosomes which are marked during fitness value calculation can not be chosen as the best. The best chromosomes of every generation will be recorded and the final solution is one of the best chromosomes.

(3) Selection operator has many strategies. In this paper, we employ a competition method to generate new population. Two of the chromosomes will be chosen at random, the one with higher fitness value will be one of the chromosomes in the next generation. In this way, we can keep outstanding chromosomes and maintain diversity in the meantime.

(4) Crossover operator is the core of GA which is controlled by crossover rate P_c. It chooses a pair of chromosomes and exchange some of their genes with the probability P_c. We choose single-point crossover to break old chromosomes and recreate next new population. Crossover operator balances premature convergence and diversity which is decided by P_c, and we choose two different crossover rate for different constraint conditions.
(5) Mutation operator has a parameter P_m called mutation rate. A chromosome change one of its genes with the probability of P_m and create new chromosome with new characteristic. Mutation rate should be small or GA will become a random search algorithm with low efficiency. We choose 0.1 as our mutation rate.

The five steps above are the basic components of GA's loop structure. One loop is one generation and we need 100 generations for both global power constraint and individual power constraint.

4 Numerical Results

In this section, simulation results are shown to verify the theoretical analysis and the performance of the power allocation scheme. The effect of residual self-interference are also illustrated based on simulation results. We will illustrate the parameters for the two different conditions respectively and show improvements and advantages of power allocation.

4.1 Global Power Constraint

Under the condition of global power constraint, the parameter initial value a_0 in (30) is 15 and linear scaling parameter $b = 10$ in (27). The population size is 40 and total generation of this GA is 100. The length of chromosomes is determined by precision of answers, that is, high precision needs longer chromosomes with the cost of time. Crossover rate and mutation rate are 0.85 and 0.1, respectively.

Figure 3 shows simulation results of outage probability for uniform power allocation, power allocation based on GA and approximation power allocation. We calculate three series of curves with different colors. The red one represents uniform power allocation and the blue curves are power allocation results based on GA. The black curves show performance of approximation power allocation. There are three curves in each series. They represent upper bound (UB), lower bound (LB) and simulation (S) results, respectively. It is obvious that simulation curves are in the region limited by the two bounds and it proves the correctness of the theoretical analysis above. The power allocation approximation algorithm has a poor performance when power is low but it is still better than uniform power allocation. And it will achieve a better performance in high SNR region. The GA can achieve better performance in both high and low SNR region but it has higher complexity than the approximation algorithm. Through power allocation, outage performance of this FD cooperative relay system has improved.

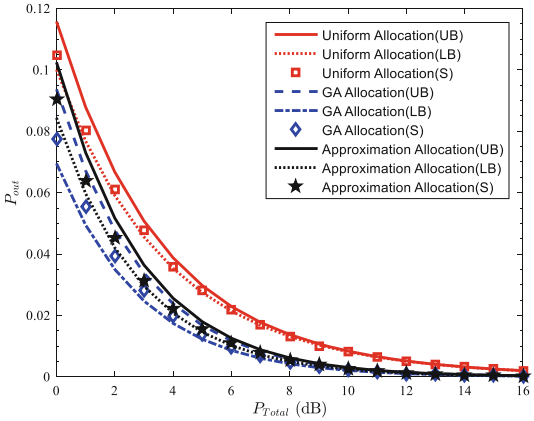


Fig. 3. Outage probability of global power constraint. ($\Omega_{0,1} = 10\,\text{dB}$, $\Omega_{0,2} = 2\,\text{dB}$, $\Omega_{1,1} = 8\,\text{dB}$, $\Omega_{1,2} = 10\,\text{dB}$, $R = 0.5\,\text{bit/s/Hz}$) (Color figure online)

4.2 Individual Power Constraint

Different from global power constraint using a penalty function, we adopt exponential scaling with parameter $c = 15$ in (28). The population size is 30 and total generation of this GA is 100. Crossover rate and mutation rate are 0.75 and 0.1, respectively. Figure 4 illustrates maximum power allocation compared with GA power allocation and approximation power allocation. Different from global power constraint, approximation power allocation has a good performance with no SNR limitations and achieve similar performance as GA power allocation. The outage performance has a significant promotion and transmit power is saved in the meantime.

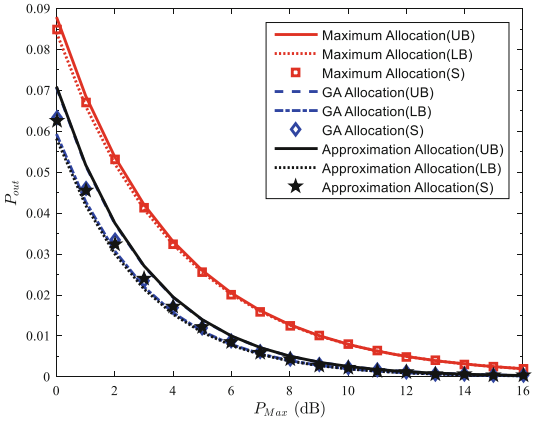


Fig. 4. Outage probability of individual power constraint. ($\Omega_{0,1} = 10\,\text{dB}$, $\Omega_{0,2} = 2\,\text{dB}$, $\Omega_{1,1} = 8\,\text{dB}$, $\Omega_{1,2} = 10\,\text{dB}$, $R = 0.5\,\text{bit/s/Hz}$)

4.3 Self-interference

In Fig. 5, results of power allocation with different intensity of self-interference are illustrated. Different kind of curves represent different intensity of self-interference. As it is shown in Fig. 5, the power allocation scheme gets evident performance improvement when $\Omega_{1,1} = 8\,\mathrm{dB}$. Nevertheless, it can not achieve significant gain when the self-interference is comparatively small. This result can be explained in (8–11) where $h_{1,1}$ denotes the only interference in this system. Therefore, the power allocation scheme should be applied when there is enough self-interference.

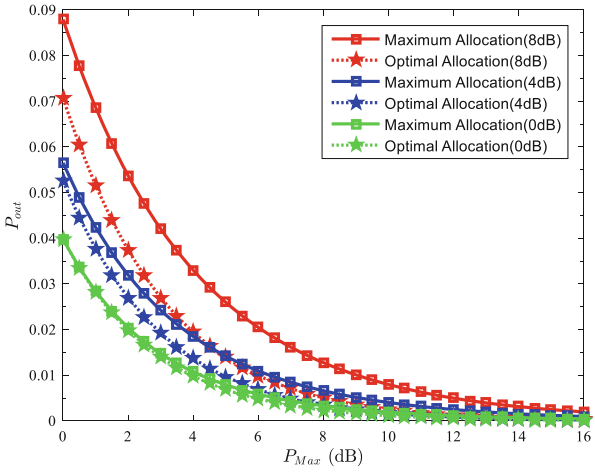


Fig. 5. Power allocation with different intensity of self-interference

4.4 Convergence of Genetic Algorithms

Figures 6 and 7 illustrate convergent performance of the proposed algorithm compared with original GA and traversal search results are regarded as optimal results.

We can clearly see that the proposed GA has a better convergence performance than original GA for individual power constraint condition. There is a premature convergence problem in original GA for global power constraint condition while the proposed GA has a good performance in both convergence and optimal value. From the results, the proposed algorithm shows superior performance for the power allocation problem. However, increasing the number of generation and population size can get further performance improvement at the expense of complexity.

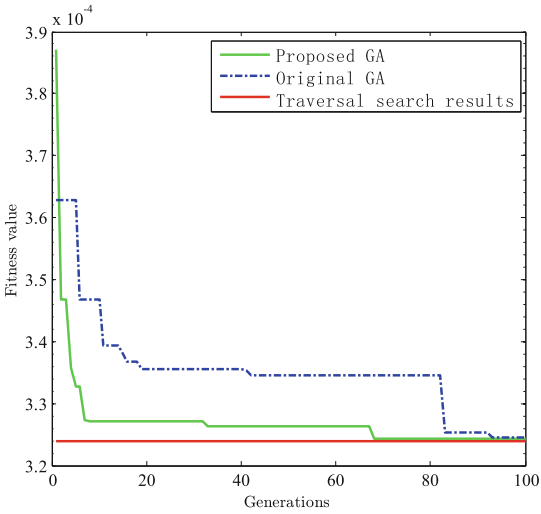


Fig. 6. Convergence of genetic algorithm for individual power constraint condition

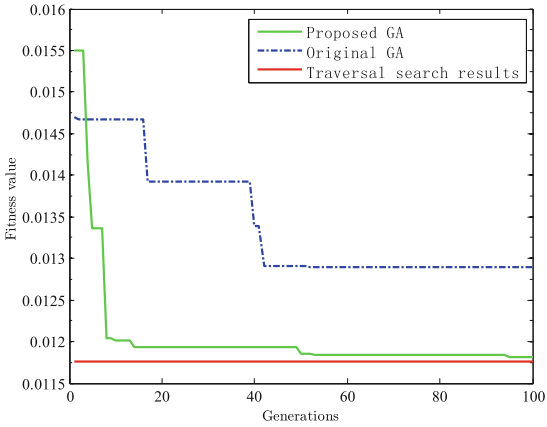


Fig. 7. Convergence of genetic algorithm for global power constraint condition

5 Conclusion

In this paper, we show a power allocation model for the FD cooperative relay system and propose a power allocation method based on GA and a power allocation approximation algorithm. Under two different constraint conditions: global power constraint and individual power constraint, we solve the optimal problem by adopting the two algorithms. Simulation results verify the theoretical analysis and show evident performance improvement. Under global power constraint, approximation algorithm has better performance under high transmitting power

condition while GA has no such limitation. GA based allocation can achieve good performance under any SNR condition. Under individual power constraint, approximation algorithm is better than the algorithm based on GA for its low complexity and power allocation can also achieve energy conservation. The self-interference intensity influences the effectiveness of power allocation. When self-interference is comparatively small, there is no need to allocate power. Simulation results also show that the proposed GA has a good performance in both convergence and optimal value.

References

1. Sabharwal, A., Schniter, P., Guo, D., Bliss, D.W., Rangarajan, S., Wichman, R.: In-band full-duplex wireless: challenges and opportunities. IEEE J. Sel. Areas Commun. **32**(9), 1637–1652 (2014)
2. Liu, G., Yu, F.R., Ji, H., Leung, V.C.M., Li, X.: In-band full-duplex relaying: a survey, research issues and challenges. IEEE Commun. Surv. Tutor. **17**(2), 500–524 (2015)
3. Kwon, T., Lim, S., Choi, S., Hong, D.: Optimal duplex mode for DF relay in terms of the outage probability. IEEE Trans. Veh. Technol. **59**(7), 3628–3634 (2010)
4. Baranwal, T.K., Michalopoulos, D.S., Schober, R.: Outage analysis of multihop full duplex relaying. IEEE Commun. Lett. **17**(1), 63–66 (2013)
5. Khafagy, M., Ismail, A., Alouini, M.S., Aissa, S.: On the outage performance of full-duplex selective decode-and-forward relaying. IEEE Commun. Lett. **17**(6), 1180–1183 (2013)
6. Krikidis, I., Suraweera, H.A.: Full-duplex cooperative diversity with Alamouti space-time code. IEEE Wirel. Commun. Lett. **2**(5), 519–522 (2013)
7. Chen, L., Han, S., Meng, W., Li, C.: Optimal power allocation for dual-hop full-duplex decode-and-forward relay. IEEE Commun. Lett. **19**(3), 471–474 (2015)
8. Grefenstette, J.J.: Optimization of control parameters for genetic algorithms. IEEE Trans. Syst. Man Cybern. **16**(1), 122–128 (1986)

Application Scheme of PKI System in Wireless Medical Data Transmission Network

Hui Wang and Chenming Gu(✉)

College of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, Jiangsu, China
gcm0621@hotmail.com

Abstract. With the rapid development of Internet of Things (IoT) and medical informatization, various kinds of intelligent medical devices have emerged in the market. Intelligent medical devices are capable of monitoring the health condition of the patient through sensors and sending those information to third parties. However, if there are no management and encryption of the information to ensure accuracy, those devices will not be able to monitor health condition accurately or even cause medical accidents. Under the circumstances, a secure data transmission scheme based on Public Key Infrastructure (PKI) is proposed. This scheme controls energy efficiency by transferring the high energy consumption of asymmetric encryption calculation to third parties. This paper also estimates the data transmission energy consumption of certain kind of wireless device, which implements the scheme to ensure feasibility.

Keywords: Internet of Things · Public key infrastructure · Data security
E-health

1 Introduction

With the rapid development of computer information technology and Internet of Things (IoT), while medical information systems such as Hospital Information System (HIS), Picture Archiving and Communication Systems (PACS), Electronic Medical Record (EMR) have becoming increasingly mature. Hospitals are heading the direction of information, modernization, digitization. A wide range of intelligent medical equipment emerging under the concept of IoT. Those data will be diagnosed and stored by hospital information systems. The patients' private data and diagnostic information provided by medical institutions are sensitive information and it is critical to implement data encryption for these information during transmission. Apart from patient health data, the doctor's diagnosis became incomplete or tampered, which will cause serious consequences such as medical malpractice. Public Key Infrastructure (PKI) is the foundation and core of network security construction, which is the basic guarantee for the implementation of e-commerce security. PKI system can achieve identity authentication, secure transmission, non-repudiation and data integrity. Certification Authority (CA) is responsible for the application, production, distribution, updating, certification and management of various digital security certificates for units, individuals or equipment. A lightweight end-to-end medical data

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 387–395, 2018.
https://doi.org/10.1007/978-3-319-90802-1_34

transmission scheme is proposed in this paper to establish a secure data transmission between intelligent medical devices and servers [1–4].

2 Scheme Overview

In this chapter, we will demonstrate the network model of the scheme, then provide a macroscopic review of the protocol and the keywords used in this paper. Finally, provide a detailed description of the data transmission process.

2.1 Network Model

The network model of the scheme consists of four main components: intelligent medical devices based on mobile interactive sensors, third parties, remote servers and CA companies (Fig. 1).

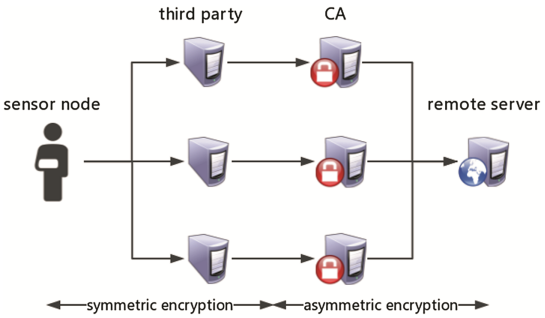


Fig. 1. The network model of the proposed scheme.

(1) Mobile interactive sensors: Through the implantation or adsorption of human body, this kind of sensor access to the patient's health data such as blood pressure, blood sugar and so on. Devices equipped with these sensors mostly adopt embedded architecture. They can perform wireless data transmission through WIFI, Bluetooth and so on [5].
(2) Third party equipment: Third parties are the key links in the scheme. A certain third party is any entity that can provide high-speed data process for the sensor nodes, such as the HIS and PACS systems of the hospital. Resource constrained sensors rely on these hardware and software for data formatting and corresponding encryption operations. Third party is denoted by TP_i [6].
(3) Certification Authority: CA mechanism ensures that third parties and remote servers communicate through certificate-based authentication, and verify the accuracy of the data by signing and verifying the data through the relevant method provided by the trusted CA authorities.

2.2 Scheme Elaboration

The proposed scheme provides a continuous message interaction process, through which the message body containing different information to complete the data encryption and transmission. Figure 2 summarizes the system message exchange process, which is divided into five phases, including 11 interactive message bodies.

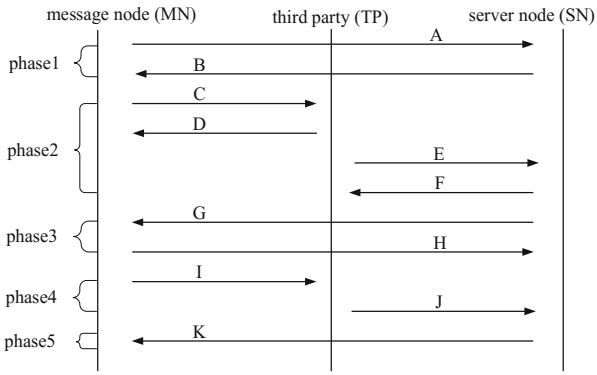


Fig. 2. Message exchange process of the data transmission

Table 1 shows the descriptions of some variables used in the scheme, they will be used mostly in the message formula.

Table 1. Notation and description of the variables in the scheme

Notation	Description
MN	Message node
SN	Server node
TP_i	Third party
CA	Certification authority
N_x	Data generated by node x
$K_{x,y}$	Symmetric key between x, y
K_x	Public key of node x
K_x^{-1}	Private key of node x
$[data]_k$	Data encrypted with key k
$SIGN_x$	Node x's digital signature
S	Credential between MN and SN

Phase 1 (initialized interaction):

Due to the limited computing power of wireless sensor nodes, MN can only perform symmetric encryption function. Node MN initiates the exchange by sending a HELLO message A to SN. This message informs SN about the security policies such as AES encryption algorithm, SHA algorithm and so on. If the server node responds, SN will

select one of the proposed security policies, SN responds with a HELLO message and generates a symmetric key for selected symmetric encryption method.

$$\text{A: } MN - hello\left(N_{MN}, SecurityPolicy\right) \tag{1}$$

$$\text{B: } SN - hello\left(N_{SN}, SecurityPolicy\right) \tag{2}$$

Phase 2 (Secure connection between nodes):

After a successful connection between the MN and the SN, this phase requires the establishment of a secure channel between TP_i and MN or SN. MN sends a message C to a TP_i device to inform its presence, this message includes a Message Authentication Code (MAC), which is encrypted by the symmetric encryption key K_{MN,TP_i} generated in phase 1, and send message D to agree to join the information exchange process. It is worth noting that in the message E, each TP_i sends public key along with certificate to the SN, meanwhile requests server certificate from SN. If the certificate provided by TP_i is certified, SN will return the certificate requested by TP_i.

$$\text{C: } \forall_i \in \{1, n\}\left[MN, N_{MN}, N_{SN}\right]_{K_{MN,TP_i}} \tag{3}$$

$$\text{D: } \forall_i \in \{1, n\}\left[TP_i - hello\left(N_{TP_i}\right)\right] \tag{4}$$

$$\text{E: } \forall_i \in \{1, n\}\left[CertRequest, Cert, N_{MN}, N_{TP_i}\right] \tag{5}$$

$$\text{F: } \forall_i \in \{1, n\}\left[Cert_{SN}, N_{TP_i}\right] \tag{6}$$

Phase 3 (Proving third party representativeness of MN to SN):

At this stage, it is necessary to prove to SN that TP_i represents a specific MN and verify the representative relationship. As response, MN will perform a hash function on each key to ensure data confidentiality and send it to the SN in message H. TP_i will send the data to the SN in the next phase and Hash value of the MN symmetric key K_{MN,TP_i}. The matching of the data proves the representation of specific MN node by perform a data comparison.

$$\text{G: } HashRequest\left(N_{SN}\right) \tag{7}$$

$$\text{H: } \left[Hash\left(K_{MN,TP_1}\right), Hash\left(K_{MN,TP_2}\right), \ldots Hash\left(K_{MN,TP_m}\right), N_{MN}\right] \tag{8}$$

Phase 4 (Encryption and transmission of critical data):

Through the first few stages of exchange, network entities have successfully established connections. At this point, MN generates medical information data S, which will be divided into m segments. Through the message I, each piece of data uses the symmetric encryption key K_{MN,TP_i} to perform symmetric encryption and sent to the specific TP_i. After received message I, TP_i will use the public key of the SN to asymmetrically encrypt the message J, and message J contains the hash value of the original

data message segment S_i, K_{MN,TP_i} along with the signature values of signing these data. SN decrypts data with its own private key after received message J, meanwhile uses verify signature method in API provided by CA to validate the accuracy of data and credential. By comparing the signature value and the original data in the message J to verify whether the data is accurate and non-repudiation. The hash value of the K_{MN,TP_i} in the message J is compared with those in message H, and if it matches, SN will recognize the data and reorganize the raw data S [7–10].

$$\text{I: } \forall_i \in \{1, m\} \left[S_i, N_{TP_i}\right]_{K_{MN,TP_i}} \tag{9}$$

$$\text{J: } \forall_i \in \{1, m\} \left[S_i, Hash\left(K_{MN,TP_i}\right), N_{MN}, N_{SN}, Sign_{TP_i}\right]_{K_{SN}} \tag{10}$$

Phase 5 (Termination phase):

SN informs the MN that the data has been received by the message K to terminate a complete data exchange process.

$$\text{K: } \left[Terminate\left(N_{MN}\right)\right]_S \tag{11}$$

3 Scheme Energy Analysis

This chapter is about energy feasibility on integrating PKI system into the data transmission. As the wireless acquisition equipment are mostly self-powered rechargeable equipment, so we must calculate the overall energy consumption.

3.1 Energy Estimation Model

In [11], the author proposed an energy consumption model for wireless sensor nodes (WSN) in data transmission. By introducing this model into the network model proposed in previous chapter, to estimate sending, receiving and listening energy consumption. The energy consumption values of Elliptic Curve Cryptography (ECC) elliptical algorithm was given [11], along with the energy consumption of ECDSA (ECC-DSA)

Table 2. Energy estimation model variables in the scheme

Message operation	Cost
Transmit 1 bit	0.72 μJ
Receive 1 bit	0.81 μJ
Listen for 1 ms	0.29 μJ
AES-128 encryption	28.11 μJ
SHA-1 128 bits MAC	23.9 μJ
ECC-160 encryption	17 mJ
ECDSA-160 signature algorithm	15 mJ

signature algorithm. In [12], the author provided the energy consumption of wireless sensor node equipped with AES encryption algorithm and SHA-1 encryption algorithm. Based on the energy calculations in these two papers. The energy estimations listed in Table 2 will serve as energy models for different data operations in the scheme.

3.2 Energy Detail Estimation

Sending energy consumption: The energy consumption of the transmission is calculated based on the length of the message of the MN and the number of third parties involved in the operation of the data. Table 3 summarizes the effect of the number of third parties on the energy consumption.

Table 3. Table of sending energy consumption using energy estimation model

Number of third parties	Size (bytes)	Energy consumption (μJ)
0	319	1831.68
2	545	3133.44
4	920	5299.34
6	1298	7464.97
8	1673	9630.56
10	2049	11796.45

Receiving energy consumption: Similar to the sending consumption, the receiving energy consumption is affected by the total length of the received message and the number of third parties. Table 4 lists the effect of the number of third parties on the receiving energy consumption.

Table 4. Table of receiving energy consumption using energy estimation model

Number of third parties	Size (bytes)	Energy consumption (μJ)
0	213	1374.4
2	258	1671.76
4	395	2553.34
6	530	3434.5
8	669	4316.67
10	803	5198.89

Listening energy consumption: The length of time that a MN is monitored is equal to the sum of the packet transmission delay (Δ), packet calculation time ($Comp$) transmission delay (T) and the reception delay (R). It is estimated that the packet transmission delay between different entities is 150 ms, and third parties and the server node have sufficient computational power and do not need to concern too much about energy efficiency. The transmission delay is calculated as follows:

$$T_{Listening} = \Delta(MN \rightarrow SN) + R(SN) + Comp(SN) + T(SN) + \Delta(SN \rightarrow MN) \quad (12)$$

Where: $\Delta(MN \rightarrow SN)$ denotes packets propagation delay from MN to SN; $R(SN)$ denotes Reception latency of SN; $Comp(SN)$ denotes Computational time of SN; $T(SN)$ denotes Transmission latency of SN; $\Delta(SN \rightarrow MN)$ denotes Packets propagation delay from SN to MN. The energy consumption monitored by the number of third-party impact is given in Table 5.

Table 5. Table of listening energy consumption using energy estimation model

Number of third parties	Listening time (ms)	Energy consumption (μJ)
0	942.27	273.12
2	2408.34	698.43
4	4215.36	1222.44
6	6023.25	1746.95
8	7830.79	2270.45
10	9637.56	2794.82

Encryption energy consumption: Encryption energy consumption is estimated by calculating the total length of the message that needs to be encrypted by the MN node, then applying the energy model to estimate the energy consumption generated by symmetric encryption and asymmetric encryption operations. It changes accordingly to the increase in the number of third parties. The asymmetric encryption algorithms adopted in China are SM series algorithms (SM2, SM3). These algorithms are improved and strengthened compared to the original ECC algorithm, but the energy consumption of this algorithm is basically similar [13] (Table 6).

Table 6. Table of encryption energy consumption using energy estimation model

Number of third parties	Size (bytes)	Energy consumption (μJ)
0	35	34000
2	132	231.56
4	264	456.87
6	388	681.45
8	517	906.53
10	640	1131.56

3.3 Scheme Energy Analysis

The scheme estimated overall sending, receiving and listening energy consumption as communication cost, and overall encryption energy consumption as computational cost, the final estimation is given in Fig. 3.

When estimating the energy consumption of communication, if there is no third party, the energy consumption on MN will be quite tremendous. Symmetric encryption and asymmetric encryption are completed in the wireless device in this case. It is technically difficult to achieve, it has certain requirements for the hardware and software conditions of the wireless devices. There must be at least one third party involved in the application to ensure that the wireless device has the highest energy efficiency. We also

find out that the energy consumption value is within reasonable range in the case where third parties are limited in number and the non-symmetric encryption operation is completed by the third party, and the feasibility of the system is verified.

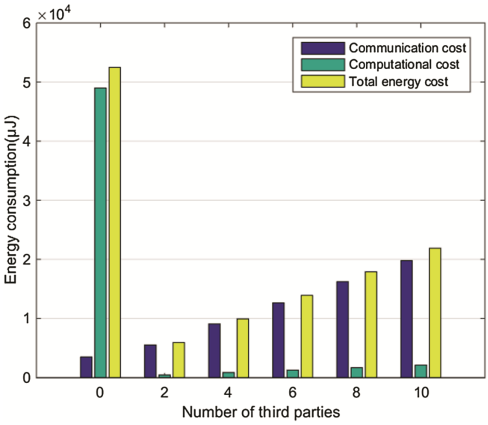


Fig. 3. Final energy consumption estimation summary

4 Conclusion and Further Work

This paper provides a feasible solution, detailed description and scheme feasibility verification of a data exchange scheme based on PKI system, with wireless intelligent medical equipment as message source. Set message nodes sending data to third party medical information system secured and unabridged as goal. Introducing PKI system into E-health applications in the context of IoT, meanwhile verified the feasibility of the system through the estimation of the energy consumption required by wireless message nodes. We have not researched on the efficiency of data transmission and the choice of data transmission channel, which will be consummated in the trailing research.

References

1. Lin, J.W.: Recent advances in PKI technologies. J. Cryptol. Res. **27**(1), 487–496 (2015)
2. Mullgan, G.: The internet of things: here now and coming soon. IEEE Internet Comput. **14**, 35–36 (2010)
3. Zen, H., Jiang, X.H., Sun, Y.F.: Research on a PKI-based IoT security model. Comput. Appl. Softw. **6**, 271–274 (2013)
4. Chowdhury, A.R., Baras, J.S.: A lightweight certificate-based source authentication protocol for group communications in hybrid wireless. In: IEEE GLOBECOM, pp. 56–59 (2008)
5. Qian, Z.H., Wang, Y.J.: Internet of things-oriented wireless sensor networks review. J. Electron. Inf. Technol. **1**, 215–227 (2013)
6. Abdmeziem, M., Tandjaoui, D.: Tailoring mikey-ticket to e-health applications in the context of internet of things. In: International Conference on Advanced Networking, Distributed Systems and Applications (Short Papers), pp. 72–74 (2013)

7. Millán, G.L., Pérez, M.G., Pérez, G.M., Skarmeta, A.F.G.: PKI-based trust management in inter-domain scenarios. Comput. Secur. **29**(2), 278–290 (2010)
8. Ning, J., Zhao, Y., Zhuang, L., Li, Y.: Design and implementation of removable storage device end-to-end encrypt system. Comput. Eng. Des. **34**(1), 1–7 (2013)
9. Braun, J., Volk, F., Classen, J.: CA trust management for the Web PKI. J. Comput. Secur. **22**(6), 913–959 (2014)
10. Delignat, L.A., Abadi, M., Birrell, A.: Web PKI: closing the gap between guidelines and practices. In: ISOC Network and Distributed System Security Symposium—NDSS (2014)
11. Meulenaer, G.D., Gosset, F., Standaert, F., Pereira, O.: On the energy cost of communication and cryptography in wireless sensor networks. In: IEEE International Conference on Wireless and Mobile Computing, Networking and Communication, pp. 580–587 (2008)
12. Kaps, J.-P., Sunar, B.: Energy comparison of AES and SHA-1 for ubiquitous computing. In: Zhou, X., Sokolsky, O., Yan, L., Jung, E.-S., Shao, Z., Mu, Y., Lee, D.C., Kim, D.Y., Jeong, Y.-S., Xu, C.-Z. (eds.) EUC 2006. LNCS, vol. 4097, pp. 372–381. Springer, Heidelberg (2006). https://doi.org/10.1007/11807964_38
13. Sun, R.Y., Cai, C.S., Zhou, Z., Zhao, Y.J., Yang, J.M.: The comparision between digital signature based on SM2 and ECDSA. Netw. Secur. **2**, 60–62 (2013)

One Division-Multiplexed of Control Code Based on Quantum Secure Direct Communication

Jinlong Liu, Zhilu Wu(✉), and Jianbo Zhao

School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150006, China
{yq20,wuzhilu,zhaojianbo}@hit.edu.cn

Abstract. As a subject of the quantum information science, Quantum Secure Direct Communication (QSDC) has been different from Quantum Key Distribution (QKD), QSDC makes the cryptograph to be transmitted directly in the quantum channel. Quantum non-cloning theorem and the indeterminacy principle insure its security. So QSDC has an important research value for the quantum communication. This letter proposed one division-multiplexed of the control code based on QSDC, the simulation is realized, utilizes the division-multiplexed of the control code to encrypt the quantum subsequence, and further improves the security. Two steps of the quantum communication are optimized to be one step. The division-multiplexed of the control code improves the efficiency of QSDC.

Keywords: QSDC · Division-multiplexed · Control code Order-rearrangement

1 Introduction

Long and Liu firstly proposes Quantum Secure Direct Communication: Efficient two-step-quantum-QSDC, then the scientists take the advantage of Single-Photon, Polarization-entangled twin photons, Quantum teleportation is proposed for QSDC [1]. The literatures on Quantum Secure Direct Communication in recent five years are summarized and analyzed, the theoretical research of QSDC towards system utility, how to simplify the procedure and how to improve the efficiency become the innovation and the research focus, so how to solve these two problems is the key method for QSDC. The researchers on the study propose Measuring-Base-Encryption Quantum Key Distribution (MBE-QKD) and Quantum Key Distribution based on the controlled order rearrangement encryption (CORE-QKD) [2–6]. The core concepts of two methods both are that how to use the control code, this paper proposes one division-multiplexed of the control code on the architecture of Quantum Secure Direct Communication.

1.1 Advantages of Using QSDC

QSDC directly transmits both the secret key and the cryptograph in the quantum channel to achieve a higher security, but QKD only sends the quantum key with quantum

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 396–404, 2018.
https://doi.org/10.1007/978-3-319-90802-1_35

channel, the cryptograph transmission also depends on the classical electromagnetic channel. The research based on quantum secure direct communication can break away from the current situation that QKD is subject to the classical security communication. QSDC is fit for transmitting confidential information in some emergencies, for example, the power grid where is an attack needs the secure and instant communication. QSDC is beneficial to simplify Distributed Blind Quantum Computation (DBQC).

1.2 Measuring Base Encryption-QKD

Measuring-Base-Encryption Quantum Key Distribution (MBE-QKD) of Hwang, Koh and Han improved BB84-QKD, as both communication sides, Alice and Bob first create a bunch of random binary number password as the control code, the code-length was N_k. Under the action of the control node, both Alice selects the measurement basic to encrypt the polarization states, Bob also selects the same measurement basic to demodulate these polarization states. Therefore, under the environment of noise-free and no eavesdropping, Bob can accurately receive the encrypted message from Alice [7–9]. Because Eve doesn't know the composition of the control code, so there is no way to judge the measurement basic which Alice selects to encrypt the polarization states, Eve only selects the random measurement basic to eavesdrop the cryptograph. Whether Eve selects any measurement basic, he cannot obtain the accurate information. The principle of MBE-QKD was shown in Fig. 1.

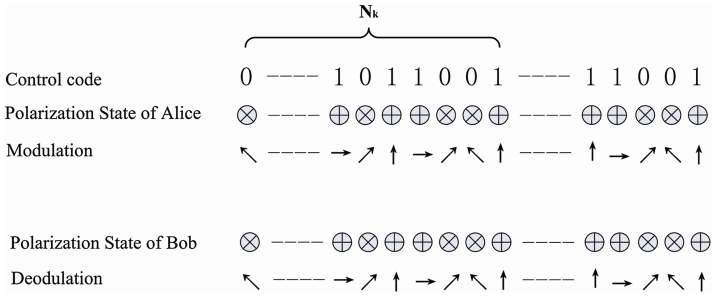


Fig. 1. The principle of MBE-QKD

Whether Eve selects any measurement basic, it cannot obtain the accurate information,so the control code becomes a key of secure communication between Alice and Bob. Before Alice and Bob compare the results by the classical channel, Eve cannot decode any message of the key with the control code. Alice and Bob reuse their control code, Eve can only obtains less than 50% of the cryptograph. If Eve taps the process of the quantum communication, by comparing the quantum bit error rate (QBER) between Alice and Bob, the two parties easily detect Eve, so Alice and Bob get up this transmission, Eve never obtains the useful information of the key with the control code. Due to MBE-QKD and BB84-QKD contain exactly the same coding method, so Hwang proves that this scheme of MBE-QKD is secure. For Alice and Bob, the control code is a secure key of QSDC to detect Eve.

1.3 Controlled-Order-Rearrangement-Encryption-QKD

Before Einstein-Podolsky-Rosen (EPR) enters into the quantum channel, Alice changes the particle transport order of the entanglement with Controlled Order Rearrangement Encryption (CORE), so the chronological locations of the two quantum photons which are located in the upper channel and the lower channel are not one-to-one, and the two quantum photons do not come from the identical EPR. The control code and the order rearrangement are the key technology in CORE-QKD. One bunch of the keys which are shared by Alice and Bob is the control code, for Eve, the control code is one bunch of the random binary sequence [10]. Figure 2 shows the principle of CORE-QKD.

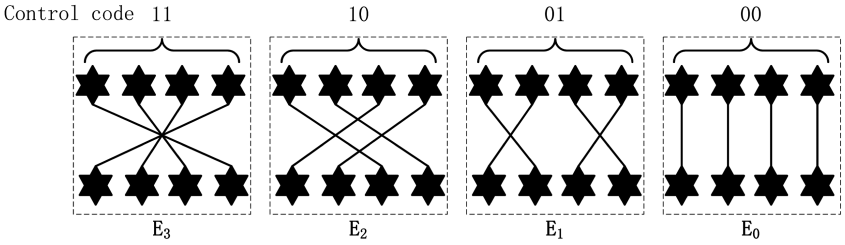


Fig. 2. The principle of CORE-QKD

Alice and Bob can transfer the effective and secure information in the quantum channel after they determines the order rearrangement of EPR, when they begin to assign the quantum key. The encryption and the decryption both utilize the order rearrangement of the control code. As shown in Fig. 2, the two quantum photons which are connected with the straight lines for one EPR. The four EPR contained 24 (4!) kinds of the order rearrangement. For example, Alice and Bob choose four kinds of the order rearrangements to transfer every EPR, they are E_0, E_1, E_2 and E_3. 2 bits of binary values of the control code are 00, 01, 11, and 10, the four binary numbers are respectively corresponded to E_0, E_1, E_2 and E_3.

1.4 Division-Multiplexed of Control Code

Through the analyses of the control code in the methods of MBE-QKD and CORE-QKD, the researchers conclude that the control code is the key technology for the two methods. The control code is used to select the same measurement basic in MBE-QKD; to select the mode of the order rearrangement [11]. Based on the key technology of the control code in MBE-QKD and CORE-QKD, this letter proposes one division-multiplexed of the control code (DMCC) on Quantum Secure Direct Communication-architecture, this method not only makes the control code to select the measurement basic, but also to select the mode of the order rearrangement, in the communication process of QSDC.

2 Establish Model on Division-Multiplexed of the Control Code

In the signal generator, Alice uses the polarization controller (Line-Conjugate-base ⊕, Diagonal-Conjugate-base ⊗) to modulate the quantum particles, Line-Conjugate-base ⊕ modulates the horizontal polarization state "→" and the vertical polarization state "↑", Diagonal-Conjugate-base ⊗ modulates the 45° polarization state "↗" and the −45° polarization state "↘", the horizontal polarization state "→" and the vertical polarization state "↑" encode the quantum bit (Qbit) 0, the 45° polarization state "↗" and the −45° polarization state "↘" encode Qbit 1.

The double multiplexing function is that the two parties determine the order rearrangement and select the polarization conjugate base. The sequence of the control code is one string of data bits of binary system, the string of data bits and the code block of the single photon cryptograph contain the same length cryptograph, the cryptograph sequence contains k single photons, the control code sequence is denoted by N_k.

When N_k performs the control function, "0" in N_k selects the polarization ⊕ to modulate the horizontal polarization state "→" and the vertical polarization state "↑", "1" in N_k selects the polarization ⊗ to modulate the 45° polarization state "↗" and the −45° polarization state "↘". When N_k performs the rearrangement, the binary value range divides the interval to map the rearrangement of E_m. Assumes $k = 8$, the binary value range of N_8 is {00000000-11111111}, N_8 contains eight equal intervals: {E_1, E_2, E_3, E_4, E_5, E_6, E_7, E_8}, Table 1 shows the corresponding relation, Fig. 3 shows the geometric rearrangement of E_m (For example: E_5 and E_8).

Table 1. Interval of N_8

Model of rearrangement	Section of N_8
E_1	00000000-00011111
E_2	00100000-00111111
E_3	01000000-01011111
E_4	01100000-01111111
E_5	10000000-10001111
E_6	10100000-11011111
E_7	11000000-11011111
E_8	11100000-11111111

Alice first executes the rearrangement based on E_m which the binary value range of N_k selects, when Alice modulates the quantum particles. Then Alice chooses the polarization to code the cryptograph with "0" and "1" from N_k. Figure 4 shows the modulation mode of Alice. Bob uses the same method to demodulate the photons sequence which it receives.

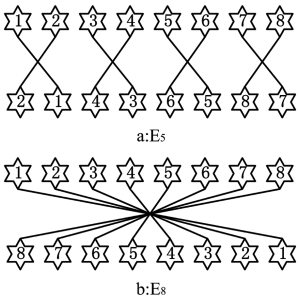


Fig. 3. The order rearrangement E_5 and E_8

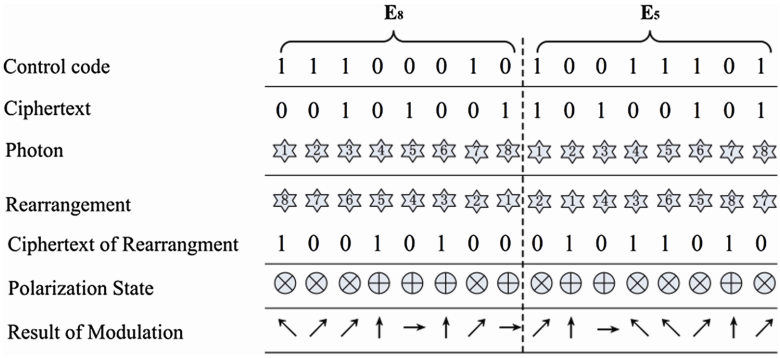


Fig. 4. The modulation mode of Alice

3 Experimental Results

The program flow chart of the principle based on DMCC is as shown in Fig. 5. According to the flow chart, Alice (the transmitting end) first prepares the random matrices $\{a_k\}$ and $\{b_k\}$, Bob (the receiving end) prepares the random matrices $\{c_k\}$, the random matrices $\{a_k\}$, $\{b_k\}$ and $\{c_k\}$ values "0" or "1", $k = 1, 2, \ldots, n$. Alice transmits the quantum states $\{|\varphi a_k b_k\rangle\}$ to Bob, in accordance with an evaluation of the random matrices $\{a_k\}$ and $\{b_k\}$, there are four kinds of the quantum states. The evaluation of random matrices $\{a_k\}$ expresses the cryptograph, if $b_k = 0$, the orthonormal basis I modulates the quantum states of Alice; if $b_k = 1$, the orthonormal basis Z modulates the quantum states of Alice. After Bob receives the quantum states, according to the evaluation of the random matrices $\{c_k\}$, if $c_k = 0$, Bob makes the orthonormal basis I to demodulate the quantum states; if $c_k = 1$, makes the orthonormal basis H to demodulate the quantum states.

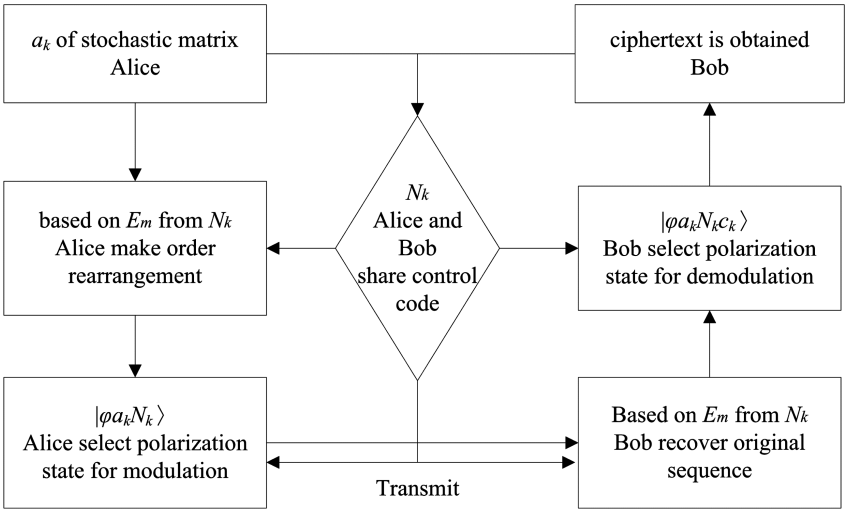


Fig. 5. The program flow chart of the principle based on DMCC

3.1 The Simulation of the Division-Multiplexed Based on the Control Code

As shown in, Alice (the transmitting end) prepares the random matrices $a_k = [1\ 1\ 0\ 1\ 0\ 0\ 1\ 0]$ in Fig. 6, Alice and Bob share the division-multiplexed of the control code $b_k = [1\ 0\ 0\ 0\ 0\ 0\ 1\ 1]$. Because the decimalism of b_k is: $m = 131$, so Alice selects the fifth rearrangement interval E_5.

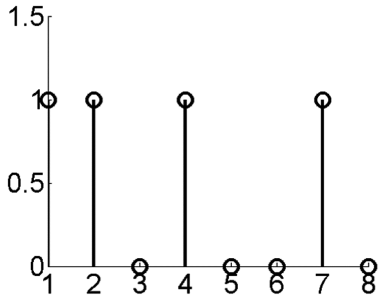


Fig. 6. Alice prepare the random matrices a_k

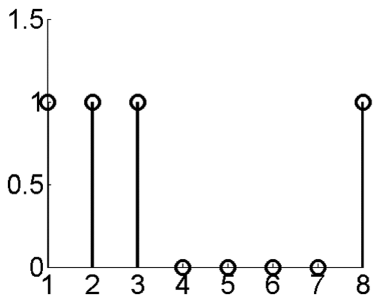


Fig. 7. The result of rearrangement

Alice first executes the order rearrangement, exchanges the first quantum photon and the second quantum photon; exchanges the third quantum photon and the fourth quantum photon; exchanges the fifth quantum photon and the sixth quantum photon; exchanges the seventh quantum photon and the eighth quantum photon, Fig. 7 shows the result of rearrangement.

After the rearrangement, if $b_k = 0$, Alice selects the orthonormal basis I to modulate the quantum; if $b_k = 1$, the orthonormal basis Z to modulate quantum. Figure 8 shows

the result of the modulation. Then, Alice transmits the cryptograph of the modulation to Bob, according to the division-multiplexed of the control code, as shown in Fig. 9. Bob recovers the original marshalling sequence of the quantum, then demodulates the final cryptograph, Fig. 10 shows the result of the cryptograph.

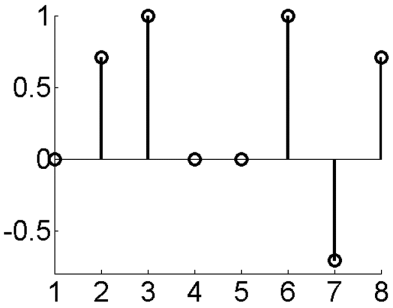


Fig. 8. The result of the modulation

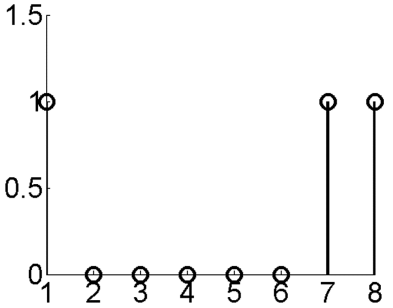


Fig. 9. The control code shared

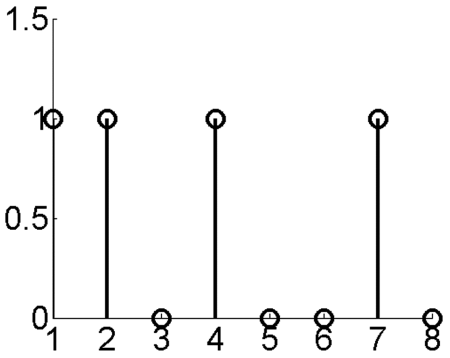


Fig. 10. The cryptograph which Bob demodulates

3.2 Compare QBER

There are eavesdrop-retransmission attacks, Trojan horse attacks, photon-number-splitting attacks, quantum channel noise and channel attenuation in the quantum communication, all reasons also can break the security for QSDC. In the experiments, QBER is employed to compare the security between DMCC and other algorithms, [10] chooses 0.13 as the threshold value. If the threshold value less than 0.13, the eavesdropping, the noise/attenuation cannot be differentiated.

QBER from all 1000 times experiments are more than 0.29 in DMCC, DMCC can detect the eavesdropping effectively. QBER from 118 times experiments are lower than 0.13 in the other algorithm, it cannot differentiate between the eavesdropping and the other reasons in the quantum channel. The comparison between the proposed DMCC and the other algorithm is shown in Table 2.

Table 2. The comparison between the proposed DMCC and another algorithm

QSDC	QBER	Less than 0.13	0.13–0.25	0.25–0.33	More than 0.33
The proposed DMCC	Frequency occurrence	0	0	16	984
Another algorithm	Frequency occurrence	118	280	0	602

4 Conclusion

This letter proposes one division-multiplexed of the control code based on the quantum secure direct communication, the experiments are done, according to the analysis of the simulation result, the proposed algorithm can select the polarization conjugate base to encrypt the quantum, and can execute the order rearrangement. This approach can effectively detect the eavesdropping.

Above all, this paper puts forward one kind of the transmission method in the field of quantum secure direct communication, the main innovative points as follows:

(1) Establish one theory model which put the control code into the block to select the polarization conjugate base.
(2) Design the approach of the order rearrangement based on the control code.
(3) Propose one division-multiplexed of the control code after summarizing the advantages of the control code from MBE-QKD and CORE-QKD.
(4) According to the analysis of the simulation result, this paper proves that the process of division-multiplexed of the control code can effectively detect the eavesdropping.

Acknowledgement. This work is supported by the Professor Zhilu Wu of School of Electronics and Information Engineering in Harbin Institute of Technology.

References

1. Deng, F.G., Long, G.L., Liu, X.S.: Two-step quantum direct communication protocol using the Einstein- Podolsky- Rosen pair block. Phys. Rev. A **68**(4), 042317 (2003)
2. Yadav, P., Srikanth, R., Pathak, A.: Two-step orthogonal-state-based protocol of quantum secure direct communication with the help of order-rearrangement technique. Quantum Inf. Process. **13**, 2731–2743 (2014)
3. Zhu, C., Hu, Q., Fu, M.: Cryptanalysis and improvement of the controlled quantum secure direct communication by using four particle cluster states. Int. J. Theor. Phys. **53**, 1495–1501 (2015)
4. Xun, R.Y., Wen, P.M., Dong, S.S.: Efficient three-party quantum secure direct communication with EPR pairs. J. Quantum Inf. Sci. **3**, 1–5 (2013)
5. Chen, W., Han, Z.F., Zhang, T.: Field experimental "star type" metropolitan quantm key distribution network. IEEE Photonics Technol. Lett. **21**(9), 575–577 (2009)

6. Liu, D., Pei, C., Quan, D.X.: A new quantum secure direct communication scheme with authentication. Chin. Phys. Lett. **27**(5), 503–506 (2010)
7. Liu, X.Y., Nie, M.: Satellite quantum communication system based on quantum repeating. In: 2011 International Conference on Consumer Electronics, Communications and Networks, pp. 2574–2577 (2011)
8. Jiang, L.N., Zhang, J.L., Ma, J., Yu, S.Y.: Entanglement dynamics between two atoms within different W-like initial states. Int. J. Theor. Phys. **53**(3), 942–951 (2014)
9. Ma, J., Jiang, L.N., Yu, S.Y.: Entanglement dynamics of the mixed two-qubit system in different noisy channels. Int. J. Theor. Phys. **53**(11), 3843–3855 (2014)
10. Guoan, Z., Geng, S., Fan, N.: Quantum secure direct communication using checking sequence coded. Int. J. Secur. Appl. **9**, 333–340 (2015)
11. Zhang, W., Ding, D.S., Sheng, Y.B., Zhou, L.: Quantum secure direct communication with quantum memory. Phys. Rev. Lett. **118**(22), 1–4 (2017)

A New Model for Cooperative Cognitive Radio Network Using Coalitional Game

Sara Gmira[1(✉)], Abdellatif Kobbane[1], Mouna El Machkour[1], and Jalel Ben-othman[2]

[1] MIS Team, SIME Lab, ENSIAS, Mohammed V University of Rabat, Rabat, Morocco
sara.gmira@um5s.net.ma, {abdellatif.kobbane,mouna.elmachkour}@um5.ac.ma
[2] Laboratoire L2TI University of Paris13, Paris, France
jalel.ben-othman@univ-paris13.fr

Abstract. In this paper we study the resources access problem in cognitive radio networks, especially we are interested in the large number of secondary users (SUs) present in the system. We propose a model based on channel access process when the PU is active, respecting the level of interference authorized by the operator. In this paper, we take secondary users as positive potential cooperators for the primary users. SUs negotiate with PUs for the acquisition of underutilized channels with exceeded interference caused to the PU. The PU will support additional interference Δ but will benefit from the cooperation of SUs to relay its data. In each transmission frame, one or more secondary users are selected to act as a relay for the primary user and also transmit its own data. We model this cooperation as coalitional game. The utility function considers various factors such as transmission power and noise level. A distributed coalition formation algorithm is also proposed, which can be used by SUs to decide whether to join or leave a coalition. Such a decision is based on whether it can increase the maximal coalition utility value. The objective of this work is to demonstrate that the proposed scheme is able to enhance the network throughput while increasing the opportunity that SUs can access the licensed spectrum owned by PUs.

Keywords: Cognitive radio · Dynamic spectrum access
Cooperative relaying · Coalitional game

1 Introduction

Cognitive radio is an innovative approach to wireless communication, which can improve spectrum utilization by spectrum sharing between primary users (PUs) and secondary users (SUs). Cognitive radio has been proposed in recent years to promote the spectrum utilization by exploiting the existence of spectrum holes [1]. According to Federal Communications Commission (FCC)[1,2], the secondary users would sense the activities of the primary users periodically.

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 405–415, 2018.
https://doi.org/10.1007/978-3-319-90802-1_36

When a channel is not occupied by a primary user, a secondary user can use the channel opportunistically after sensing. In a cognitive radio network, the SUs are allowed to access the spectrum in overlay or underlay model [3–5]. In underlay spectrum sharing scenario, the SU and the PU can access a licensed spectrum simultaneously as long as the interference caused to PU is kept below a predefined threshold [2]. SUs' transmission power is constrained strictly. Accordingly, the SUs' quality of service (QoS) can not be guaranteed and enhancing the SUs' performance becomes a challenging issue.

For better exploitation of spectrum resources, and with the evolution of cognitive radio technologies, dynamic spectrum access [2,3] becomes a promising approach to increase the efficiency of spectrum use, allowing an unauthorized wireless users (secondary users) to dynamically access the bands of spectrum holders (primary users). This efficiency can be improved considerably when dynamic spectrum access is associated with spectrum leasing. Dynamic spectrum leasing (DSL) [6] is proposed on the basis of DSA. In DSL model, spectrum licensees (called primary users) have the rights to sell or trade their spectrum to the third party. So primary users can lease their owned spectrum resources for a fraction of time to the secondary users to exchange reasonable remuneration. The authors in [9] proposed an improved cognitive radio (CR) model in which the secondary system can harvest energy from the primary system and access the spectrum of the primary system to transmit its own data in an underlay mode.

In this paper, we study the cooperation between PU and SU where PU use SUs to relay their message in exchange for spectrum access. We focus on designing an effective cooperation strategy for SUs to form a coalition so that the overall system performance (primarily, the throughput) can be improved. A distributed coalition formation algorithm for each SU is proposed in this paper to decide whether to join or leave a coalition based on the split and merge rules [7]. Such a decision is based on whether it can increase the maximal coalition utility value.

The rest of this paper is organized as follows. The network model and the cooperative transmission mechanism are illustrated in Sect. 2. We formulated the relay selection problem as coalitional game with transferable utility in Sect. 3 and also proposed the distributed game formation algorithm. In the Sect. 4, we analyze the performance of our proposed cooperative cognitive framework. Finally the Sect. 4 concludes the paper.

2 System Model

In our proposed framework, we assume that:

- The network is dense where many SUs have the objective to access the channel.
- The PU is willing to cooperate with the SUs and grant to a subset of secondary transmitters in exchange for cooperation (relaying) in the form of transmission.
- The messages exchanged between the PU and the SU during the negotiation phase are not addressed in this paper.

- Most of the SUs have best effort traffics (like web surfing, mails,...), these users will be authorized by the PU to share the canal with it even if the interference threshold is not respected. They will not waste time in sensing to check the presence of the PU and will leave the spectrum holes for SUs with real time services.
- In the secondary network, each transmitter has information to deliver to a given secondary receiver (interference channel).

In this paper, we explore the ability of cognitive radio to provide sufficient capacity to support additional interference for the PU in exchange for cooperation. The PU will be willing to support additional noise level Δ *(presented in* Fig. 1) in his owned bandwidth for a fraction of time if, in exchange for this concession, they will benefit from enhanced quality of service (e.g., in terms of rate and also of outage probability). When the PU is active, he decides its strategy on the level of the additional noise level that he can support from the SUs, and also the number of successive time slots **X** granted of SUs in this cooperation. This cooperation is modeled as a game, specifically, as a ***coalitional game***.

The proposed system involves N Primary Network (owner of the spectrum rights) and M Secondary Users. The set of PUs and SUs are denoted by $\mathcal{N} = \{1, 2, ..., N\}$ and $\mathcal{M} = \{1, 2, ..., M\}$, respectively (Fig. 2).

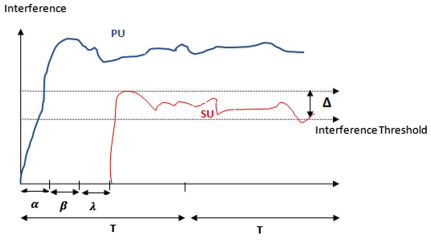


Fig. 1. Cooperative spectrum sharing

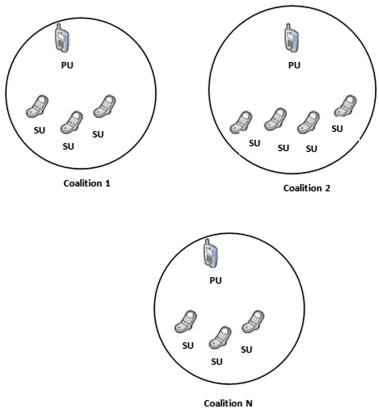


Fig. 2. Coalition formation for collaborative spectrum access

In this paper, we consider a model where the SUs act as cooperative relays to assist the PUs transmission in exchange for spectrum accesses in overlay or underlay mode. The PU can coexist with one or more secondary systems and sharing the same frequency band. Both these two networks operate autonomously. Thus, the Primary Network is aware of the spectrum occupancy by PUs and the same for the Secondary Network. SUs can make use of free

channels, or use the occupied channels under SINR constraints. Every PU in the $\mathcal{N} = \{1, 2, ..., N\}$ will form a collation with one or more SUs, The coalition head is represented by the PU. The number of coalitions formed in our proposed model is equal to N.

The PU has two transmission modes: direct transmission and cooperative transmission. If PU selects direct transmission mode, it sends the data to its receiver directly over the entire primary portion.

In our proposed system, the time resource is partitioned into discrete time slots (Fig. 1). We suppose every channel is slot Rayleigh channel which means that the channel coefficient is constant in a slot and all transmissions are assumed to be slot synchronized. During the primary time slot, each PU may use the entire slot for direct transmission or to employ cooperation with SUs which determined by the coalition algorithm described in the next section.

The data transmission slot is divided into four portions, α, β, λ and $T - \alpha - \beta - \lambda$.

- The Sensing phase with duration: α.
- The Reporting phase with duration: β.
- The Negotiation phase with duration: λ (Coalition Formation).
- The Data Transmission Phase with duration: $T - \alpha - \beta - \lambda$.

The contributions of this paper can be summarized as follows:

(1) We present a cooperation framework between primary users and secondary users.
(2) Coalitional game theoretic model of spectrum access/sharing is presented.
(3) We investigate the coalition formation and discuss the NE solution for our coalition game.

Algorithm 1. Coalition Formation Algorithm

Initial Coalition Formation:
PU broadcasts pilot traffic to each SU, and select candidate relays based on the geographic location
Initial coalition formation $C_{j_{initial}} = \{PU_j, SU_1, ..., SU_i, ...SU_{q_{initial}}\}$
The PU sets a value for the additional accepted interference Δ and the number of time slots X granted for SUs' access using the underlay mode.
Coalition Transformation:
SUs get the value of Δ
Apply merge-split rules on coalitions
Repeat after X time slot
$\Pi^{'}$ = merge (Π), Coalitions in C merge into a new coalition based on the merge rules
Repeat until no more merge possible
Π = split ($\Pi^{'}$), Coalitions in F split into different coalitions based on the split rule
Repeat until no more split possible $C_j = \{PU_j, SU_1, ..., SU_i, ...SU_q\}$
SUs calculate the transmission power's value

3 Proposed Cooperative Relay System

3.1 Coalition Game Overview

Coalition formation is a branch of game theory that investigates algorithms for studying the coalitional structures that form in a network. It's recognized as an important tool in many fields, such as social sciences, biology, engineering, political science [13]. Coalitional games approaches can achieve better results in terms of performance and stability in cooperative communications networks. Coalitional games was classified in a tutorial paper [7] into three categories: canonical (coalitional) games, coalition formation games, and coalitional graph games.

3.2 Framework Conception

In this section, an algorithm for the coalition formation of our proposed framework is presented. The SU will start by sensing the canal in the sensing phase α (presented in Fig. 1). If the PU is idle, then the SU will access the canal in its free spectrum holes using the Overlay Mode. The access will be granted for the current time slot. Otherwise, if the PU is active in the canal, the SU will share the same spectrum with the PU using the Underlay access mode. In our proposed model, SUs are authorized to exceed the predefined threshold with an additional interference Δ. In turn, they will collaborate with the PU by relaying its data to their destinations. When the PU is active, one or more SUs can coexist with the PU in the same canal for X time slots. The values of Δ and X are defined by the PU during the negotiation phase λ. In this case, for the next X time slots, the SUs will not waste energy in the sensing and the reporting phases, and will use the whole time slot with duration T.

Incorporating cooperation into cognitive radio networks, the SUs not only look for idle time slots to transmit their own data, but they may also relay the PUs' packets. Thus, cooperation in cognitive radio networks can be regarded as a win-win situation. In our paper, the cooperation between the PU and the SUs is used when the PU is present in the canal and is willing to support additional interference. In general, the more SUs in the selected coalition, the less spectrum's portion access. In turn, each SU may obtain less access time for its own data transmission. On the other hand, each SU may acquire more access time for its own data transmission if there is a fewer number of SUs in the coalition. Consequently, each SU in the game has the incentive to team up with the best partners so as to produce the maximal coalition utility value. This value depends also on the value Δ fixed by the PU at the beginning of the negotiation phase λ. The coalition formation algorithm is detailed in Algorithm 1 based on the split and merge rules.

3.3 Throughput Calculation/Coalition's Utility

As presented in the paper [11], a coalitional game G is uniquely defined by the pair $(K;U)$, where K is the set of players (PU and his SUs relay nodes),

any non-empty subset $\mathscr{C} \subseteq N$ is called a coalition, and U is the coalition value, it quantifies the worth of a coalition in a game. The strategy of each player is to decide on which coalition to join, and the payoff is the function $U(\mathscr{C}_j; \Pi_i)$.

The utility (denoted by U) is the aggregated utility value of a coalition. Specifically, $U(\mathscr{C}_j)$ denotes the total coalition utility value of the coalition $\mathscr{C}_j$, where $j \in \{1, 2, ..., N\}$ and $\mathscr{C}_j \subseteq (N \cup M)$, which is defined as below:

$$U(\mathscr{C}_j) = \sum_{i=1}^{q_j+1} U_i \tag{1}$$

Where $q_j + 1$ denotes the number of players in the coalition $U(\mathscr{C}_j)$: one PU and q_j SUs.

The utility value U_i of each player is the difference between reward and cost, which is defined as:

$$U_i = R_i - C_i \tag{2}$$

Where R_i and C_i represent respectively the reward and the cost given to SU_i/PU_i.

In our proposed coalition game, the throughput is considered as reward of the PU_j and SU_{ij} $(1 \leq i \leq q_j)$ in the coalition.

The cardinal of the coalition $\mathscr{C}_j$ is equal to $q_j + 1$, so we have:

$$U(\mathscr{C}_j) = \sum_{i=1}^{q_j+1} (R_i - C_i) \tag{3}$$

The aggregated utility value of each coalition is composed of the utility of the PU and the other SUs in his coalition. Then, after substitution:

$$U(\mathscr{C}_j) = (R_{PU_j} - C_{PU_j}) + \sum_{i=1}^{q_j} (R_i - C_i) \tag{4}$$

Then we have :

The primary transmission rate is giving by :

$$R_{PU} = \begin{cases} R_{Direct(PU)} & , no\ cooperation \\ R_{Direct(PU)} + R_{Coop(PU)} & , with\ cooperation \end{cases} \tag{5}$$

In the equations below, W denotes the communication bandwidth, P_s and P_p the transmission power for the SU and the PU respectively, G_i^j the channel gain between node i and j and is modeled as independent zero mean complex Gaussian random variable with variance σ^2.

The achievable rate from PU transmitter-receiver over the channel on the direct link (without using the SU for relaying its data) is:

$$R_{Direct(PU)} = W * log_2 \left(1 + \frac{P_p G_p^p}{\sigma^2}\right) \tag{6}$$

We assume that when the PU is active in the canal, it has many services in his queue to send to their destinations. He will benefit from cooperation with SUs and transmit some services to his coalition in order to relay them to their destinations. The achievable rate from Primary transmitter (PT) to Primary receiver (PR) over the channel with cooperative relay is:

$$R_{Coop(PU)} = L_j * \delta_{Succ(j)} * R_{Coop(SUij)} \tag{7}$$

Where L_j denotes the packet length delivered by the PU of the coalition $\mathscr{C}_j$ to its SUs in his coalition in order to deliver it (the packet) to PU's receiver, and $\delta_{Succ(j)}$ denotes the probability of successful delivery of a message by the SUs of the coalition $\mathscr{C}_j$. According to [13], we have:

$$\delta_{Succ(j)} = 1 - \Pi_{.} Q_{SUij} \tag{8}$$

Where is the Q_{SUij} probability that a $SUij$ fails to deliver the copy of the PU's packet to the destination. Thus, the throughput of SU_{ij} when relaying the PU's data is:

$$R_{Coop(SUij)} = (T - \alpha - \beta - \lambda) * W * log_2 \left(1 + \frac{P_s G_s^s}{\sigma^2}\right) \tag{9}$$

The achievable rate from ST to SR over the channel in the overlay mode for **one time slot** is ($\lambda = 0$ in this case because there is no negotiation on the value of X between the PU and the SU):

$$R_O(SU) = \frac{T - \alpha - \beta}{T} * W * log_2 \left(1 + \frac{P_{si} G_{si}^{si}}{\sigma^2}\right) \tag{10}$$

As explained above, the PU will grant access to his formed coalition for X time slots in the underlay mode. In the first time slot, SUs will negotiate with the PU in the negotiation phase λ on the value of X and the additional value Δ. At the remaining time slots $X - 1$, SUs will exploit the whole time slot (without the sensing, the reporting and the negotiation phases). Then, the achievable rate from ST (Secondary Transmitter) to SR (Secondary Receiver) for all the SU_{ij} ($1 \leq i \leq q_j$) in the coalition in the underlay mode for X **time slot**s is:

$$R_U(SU_i, X) = \frac{T - \alpha - \beta - \lambda}{T} W log_2 \left(1 + \frac{P_{si} G_{si}^{si}}{\sigma^2 + \Delta}\right) + (X - 1) W \sum_{i=1}^{q_j} log_2 \left(1 + \frac{P_{si} G_{si}^{si}}{\sigma^2 + \Delta}\right) \tag{11}$$

Then we have the average throughput for the SU in the underlay mode for the X time slot :

$$R_U(SU_i Avrg) = \frac{1}{X} * R_U(SU_i, X) \tag{12}$$

Thus,

$$R_U(SU_iAvrg) = \frac{T-\alpha-\beta-\lambda}{T*X} * W * log_2\left(1+\frac{P_{si}G_{si}^{si}}{\sigma^2+\Delta}\right) + \frac{X-1}{X} * W * \sum_{i=1}^{q_j} log_2\left(1+\frac{P_{si}G_{si}^{si}}{\sigma^2+\Delta}\right) \tag{13}$$

The SU will access in Overlay mode if the PU is idle in the canal and access in Underlay mode of he's active. Let's denote Π_p, the probability of the presence of the PU in a given band, and Y the number of time slots when SU access in the Overlay mode. Thus, the total average throughput of the SU in our proposed model is presented below:

$$R_{Total(SU_i,Avrg)} = \frac{Y}{X+Y} * (1-\Pi_p) * R_O(SU_i) + \frac{X}{X+Y} * \Pi_p * R_U(SU_iAvrg) \tag{14}$$

3.4 Existence of Nash Equilibirum

The Nash equilibrium [15] is an important concept to measure the outcome of a non-cooperative game, which is a set of strategies, one for each player, such that no selfish player has incentive to unilaterally change his/her action.

According to [8], a Nash equilibrium exists if it satisfies the following conditions: $\forall i \in N$:

(1) The action strategy profile (A_i) is a nonempty, convex, and compact subset of some Euclidean space.
(2) The utility function (U_i) is a continuous and quasi-concave function over the strategy set of the players.

Proof: this can be achieved by showing the two conditions offered are met and the poof can be shown according to:

- Since each CR user has a strategy profile that is defined by a spectrum access type with some transmission power, thus the first condition is readily satisfied.
- To prove the second condition is also satisfied, we have to show that the given price based utility function (A_i) is quasi-concave $\forall i \in N$.

The utility function is continuous and strictly concave because we have:

$$\frac{\partial^2 U_{ab}^{\gamma}}{\partial p_{\gamma}} > 0 \tag{15}$$

Nash equilibrium of a game G is a strategy profile $s^* \in S$ such that $\forall i \in I$ we have the following

$U_i(s_i^*, s_{-i}^*) >= U_i(s_i, s_{-i}^*) \forall s_i \in S_i, s_i \neq s_i^*, \forall i \in I$

4 Simulations and Numerical Results

In this section, we provide and discuss numerical results about the system performance for $N = 2$ and $M = 5$. We aim to show by these simulations that both the PU and the SU can achieve reasonable throughput in our proposed cooperative model. For our simulations, we choose the default parameters as follow: $K = 200\,kHz$, $Pp = 10\,mW$, $Ps(underlay) = 0.1\,mw$, $n0 = 10^{-15}\,W; SINR = 10\,dB$.

In Fig. 3, we plot the throughput's variation for both PU and SU as a function of the variation of the Δ. We note that the throughput of the PU without the cooperation decreases if the value of the Δ is increased, while it increases if the PU cooperates with SU. We can clearly see that the SU's throughput is enhanced for higher value of Δ.

In our game, every player is a general entity individual and uses a strategic learning algorithm to learn the best coalition and finally the system converge to Nash equilibrium. We use the imitative Boltzmann-Gibbs weighted strategy [11,13]. In our paper, we are interested in SU's strategies. Those of the PU will be studied in a future work.

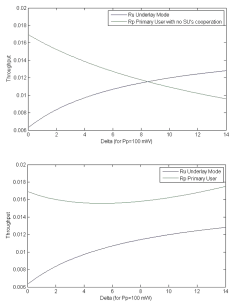


Fig. 3. SU's and PU's throughput variation without and with cooperation

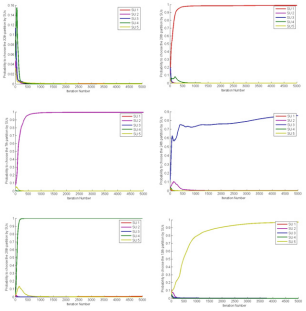


Fig. 4. Convergence of partition choice for five SUs

In Fig. 4, we plot the probability of partition's convergence ($N = 2, M = 5$). It shows that each SU can make a good decision on which partition to choose. SU1 to SU5 choose respectively partitions: Π_{28}, Π_7, Π_{24}, Π_{28} and Π_{13}. For the strategy Π_{32}, no user converge to this strategy, because the reward for this one is the lowest one (all the SUs with the same PU that offers the lowest value of Δ).

From these simulations we can conclude that having a maximum utility (throughput) for players is due to the partition's choice, which takes into account the value of Δ predefined by the PU and the number of the SUs present in the current coalition with the PU (Table 1).

Table 1. Possible Coalitions Structure for $N = 2$ and $M = 5$

$\Pi_1 = \{\{PU_1, SU_1\}, \{PU_2, SU_2, SU_3, SU_4, SU_5\}\}$	$\Pi_{17} = \{\{PU_1, SU_1, SU_2, SU_4\}, \{PU_2, SU_3, SU_5\}\}$
$\Pi_2 = \{\{PU_1, SU_2\}, \{PU_2, SU_1, SU_3, SU_4, SU_5\}\}$	$\Pi_{18} = \{\{PU_1, SU_1, SU_2, SU_5\}, \{PU_2, SU_3, SU_4\}\}$
$\Pi_3 = \{\{PU_1, SU_3\}, \{PU_2, SU_1, SU_2, SU_4, SU_5\}\}$	$\Pi_{19} = \{\{PU_1, SU_1, SU_3, SU_4\}, \{PU_2, SU_2, SU_5\}\}$
$\Pi_4 = \{\{PU_1, SU_4\}, \{PU_2, SU_1, SU_2, SU_3, SU_5\}\}$	$\Pi_{20} = \{\{PU_1, SU_1, SU_3, SU_5\}, \{PU_2, SU_2, SU_4\}\}$
$\Pi_5 = \{\{PU_1, SU_5\}, \{PU_2, SU_1, SU_2, SU_3, SU_4\}\}$	$\Pi_{21} = \{\{PU_1, SU_1, SU_4, SU_5\}, \{PU_2, SU_2, SU_3\}\}$
$\Pi_6 = \{\{PU_1, SU_1, SU_2\}, \{PU_2, SU_3, SU_4, SU_5\}\}$	$\Pi_{22} = \{\{PU_1, SU_2, SU_3, SU_4\}, \{PU_2, SU_1, SU_5\}\}$
$\Pi_7 = \{\{PU_1, SU_1, SU_3\}, \{PU_2, SU_2, SU_4, SU_5\}\}$	$\Pi_{23} = \{\{PU_1, SU_2, SU_3, SU_5\}, \{PU_2, SU_1, SU_4\}\}$
$\Pi_8 = \{\{PU_1, SU_1, SU_4\}, \{PU_2, SU_2, SU_3, SU_5\}\}$	$\Pi_{24} = \{\{PU_1, SU_2, SU_4, SU_5\}, \{PU_2, SU_1, SU_3\}\}$
$\Pi_9 = \{\{PU_1, SU_1, SU_5\}, \{PU_2, SU_2, SU_3, SU_4\}\}$	$\Pi_{25} = \{\{PU_1, SU_3, SU_4, SU_5\}, \{PU_2, SU_1, SU_2\}\}$
$\Pi_{10} = \{\{PU_1, SU_2, SU_3\}, \{PU_2, SU_1, SU_4, SU_5\}\}$	$\Pi_{26} = \{\{PU_1, SU_2, SU_3, SU_4, SU_5\}, \{PU_2, SU_1\}\}$
$\Pi_{11} = \{\{PU_1, SU_2, SU_4\}, \{PU_2, SU_1, SU_3, SU_5\}\}$	$\Pi_{27} = \{\{PU_1, SU_1, SU_3, SU_4, SU_5\}, \{PU_2, SU_2\}\}$
$\Pi_{12} = \{\{PU_1, SU_2, SU_5\}, \{PU_2, SU_1, SU_3, SU_4\}\}$	$\Pi_{28} = \{\{PU_1, SU_1, SU_2, SU_4, SU_5\}, \{PU_2, SU_3\}\}$
$\Pi_{13} = \{\{PU_1, SU_3, SU_4\}, \{PU_2, SU_1, SU_2, SU_5\}\}$	$\Pi_{29} = \{\{PU_1, SU_1, SU_2, SU_3, SU_5\}, \{PU_2, SU_4\}\}$
$\Pi_{14} = \{\{PU_1, SU_3, SU_5\}, \{PU_2, SU_1, SU_2, SU_4\}\}$	$\Pi_{30} = \{\{PU_1, SU_1, SU_2, SU_3, SU_4\}, \{PU_2, SU_5\}\}$
$\Pi_{15} = \{\{PU_1, SU_4, SU_5\}, \{PU_2, SU_1, SU_2, SU_3\}\}$	$\Pi_{31} = \{\{PU_1\}, \{PU_2, SU_1, SU_2, SU_3, SU_4, SU_5\}\}$
$\Pi_{16} = \{\{PU_1, SU_1, SU_2, SU_3\}, \{PU_2, SU_4, SU_5\}\}$	$\Pi_{32} = \{\{PU_1, SU_1, SU_2, SU_3, SU_4, SU_5\}, \{PU_2\}\}$

5 Conclusion

In this paper, we study the cooperation strategy for SUs in a CRN based on the coalition formation game theory. We focused on designing an effective cooperation strategy between PU and SU to form a coalition so that the overall system performance (primarily, the throughput) can be improved. We formulate the problem of cooperative spectrum access as a coalition game, which is solved by a proposed distributed coalition formation algorithm utilizing the split and merge rules. The simulation results showed that networks performances increase with the proposed scheme especially in terms of the throughput enhancement.

References

1. Haykins, S.: Cognitive radio: brain-empowered wireless communications. IEEE J. Sel. Areas Commun. **23**(2), 201–220 (2005)
2. FCC Spectrum Policy Task Force: Report of the spectrum efficiency working group, November 2002. http://www.fcc.gov/sptf/reports.html
3. Zhao, Q., Sadler, B.M.: A survey of dynamic spectrum access. IEEE Signal Process. Mag. **24**(3), 79–89 (2007)
4. Gmira, S., Kobbane, A., Sabir, E.: A new optimal hybrid spectrum access in cognitive radio: overlay-underlay mode. In: WINCOM 2015, Marrakech, Morocco, pp. 1–7 (2015)
5. Mitola, J.: Cognitive radio for flexible mobile multimedia communications. In: Proceedings of the IEEE International Workshop Mobile Multimedia, Communication, pp. 3–10 (1999)
6. Etkin, R., Parekh, A., Tse, D.: Spectrum sharing for unlicensed bands. In: Proceedings of the 1st IEEE Symposium New Frontiers Dynamic Spectrum Access Networks, pp. 251–258 (2005)
7. Saad, W., Han, Z., Debbah, M., Hjørungnes, A., Basar, T.: Coalitional game theory for communication networks. IEEE Signal Process. Mag. **26**, 77–97 (2009)
8. Huo, Y., Liu, L., Ma, L., Zhou, W., Cheng, X., Jing, T., Jiang, X.: A coalition formation game based relay selection scheme for cooperative cognitive radio networks. J. Wirel. Netw. 1–12 (2016)

9. Le, T.-D., Shin, O.-S.: Wireless energy harvesting in cognitive radio with opportunistic relays selection. In: Proceedings of the IEEE International Symposium Personal Indoor and Mobile Radio Communication (PIMRC), pp. 949–953, August 2015
10. Al Sukkar, G., Shafeeq, Z.A., Al Amayreh, A.: Best relay selection in a multi-relay nodes system under the concept of cognitive radio. In: ICICS 2015, Amman, Jordan, April 2015
11. Oualhaj, O.A., Kobbane, A., Elmachkour, M., Sabir, E., Ben-Othman, J.: A coalitional-game-based incentive mechanism for content caching in heterogeneous Delay Tolerant Networks. In: 2015 International Wireless Communications and Mobile Computing Conference (IWCMC), pp. 987–992, August 2015
12. Belghiti, I.D., Elmachkour, M., Berrada, I., Kobbane, A., Ben-Othman, J.: Coalitional game-based behavior analysis for spectrum access in cognitive radios. Wirel. Commun. Mob. Comput. J. **16**(14), 1910–1921 (2016)
13. Tembine, H.: Distributed Strategic Learning for Wireless Engineers. CRC Press/Taylor Francis, Boca Raton/London (2012)

Cloud and Big Data Networking

Improving Multiple-Instance Learning via Disambiguation by Considering Generalization

Lu Zhao[1(✉)], Youjian Yu[1], Hao Chen[1], and Liming Yuan[2]

[1] Tianjin Chengjian University, Tianjin 300384, China
zhaolu6892@163.com
[2] Tianjin University of Technology, Tianjin 300384, China

Abstract. Multiple-instance learning (MIL) is a variant of the traditional supervised learning. In MIL training examples are bags of instances and labels are associated with bags rather than individual instances. The standard MIL assumption indicates that a bag is labeled positive if at least one of its instances is labeled positive, and otherwise labeled negative. However, many MIL problems do not satisfy this assumption but the more general one that the class of a bag is jointly determined by multiple instances of the bag. To solve such problems, the authors of MILD proposed an efficient disambiguation method to identify the most discriminative instances in training bags and then converted MIL to the standard supervised learning. Nevertheless, MILD does not consider the generalization ability of its disambiguation method, leading to inferior performance compared to other baselines. In this paper, we try to improve the performance of MILD by considering the discrimination of its disambiguation method on the validation set. We have performed extensive experiments on the drug activity prediction and region-based image categorization tasks. The experimental results demonstrate that MILD outperforms other similar MIL algorithms by taking into account the generalization capability of its disambiguation method.

Keywords: Multiple-instance learning · Disambiguation
Generalization ability

1 Introduction

Multiple-instance learning (MIL) copes with the classification of training bags each of which is composed of one or more training instances [5,7]. Labels are associated with bags rather than any individual instance. The standard multiple-instance assumption indicates that a bag is labeled positive if *at least* one of its instances is positive, and otherwise labeled negative.

Several researchers have made a more general multiple-instance assumption that a bag is labeled as a ceratin class only when several different instances co-appear in the bag. Under this general assumption, they further proposed

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 419–429, 2018.
https://doi.org/10.1007/978-3-319-90802-1_37

several embedded-space MIL algorithms [3,4,8,10]. The basic idea can be summarized as: (1) selecting some instance prototypes from the training set to form an embedded-space, (2) embedding every bag into the embedded-space by computing the distances/similarities between this bag and those instance prototypes, (3) using the new bag-level features for training bags to learn an support vector machine (SVM).

MILD is a very efficient and robust embedded-space MIL algorithm, which has been demonstrated by Li and Yeung [10]. MILD focuses on the ability of a candidate instance prototype in separating positive and negative training bags. However, it ignores the discriminative ability of an instance on the validation set, or in other words does not consider the generalization capability of its disambiguation method, leading to inferior performance as compared to other similar algorithms.

In this paper, we attempt to improve the performance of MILD by taking into account the generalization ability of its disambiguation method. The main idea is dividing the training set into a training set and a validation set, and using the discrimination of a candidate instance prototype on the validation set as the evaluation standard of its discriminability. We name the new variant of MILD Multiple-Instance Learning via Generalized Disambiguation (MILGD). The experimental results show that MILGD outperforms other embedded-space MIL algorithms with respect to classification accuracy and robustness to labeling noise.

The remainder of the paper is organized as follows. In Sect. 2, we review some work related to our research. In Sect. 3, we first analyse the characteristics of MILD and then propose our new algorithm. We then compare our MILGD algorithm with other baselines using two kinds of MIL data sets in Sect. 4. We conclude this paper in the last section.

2 Related Work

Dietterich et al. [6] proposed the first MIL algorithm called Axis-Parallel Rectangle (APR). The main idea is trying to find an APR in the feature space, which includes *at least* one instance from every positive training bag but excludes all instances from the negative training bags. Before long, Maron and Lozano-Prez [12] presented a similar concept named Diverse Density (DD) to solve the MIL problem. DD actually describes the likelihood that a possible concept appears in all positive bags and does not appear in any negative bag at the same time. Zhang and Goldman [19] extended the DD concept into the Expectation Maximization (EM) framework and proposed the EM-DD algorithm in order to locate the target concept in a more efficient way. Since learning a single concept may be insufficient to capture the multi-modal distribution, GEM-DD applies the Quasi-Newton approaches to search for a group of concepts in an iterative way [14].

Ramon and De Raedt [15] adapted the neural networks to the MIL context. Later on, Zhang and Zhou [18] derived a similar framework to tackle the MIL

problem. Wang and Zucker [17] used the Hausdorff distance to measure the distances between different bags and extended the standard k-Nearest Neighbor (kNN) algorithm into the multiple-instance setting. Gärtner et al. [9] developed a multiple-instance kernel function such that SVMs can be applied directly for the training bags. Andrews et al. [1] regarded the unobservable instance labels as hidden variables and formulated MIL as mixed integer quadratic programs. Settles et al. [16] constructed a multiple-instance framework with active learning and showed that instance labels are beneficial for improving the performance of an MIL learner. Motivated by the subgradient-based approaches for SVMs, Bergeron et al. [2] proposed a non-convex bundle method for optimizing the multiple-instance objective. Li et al. [11] assume that the distribution of instances is a mixture of the concept and non-concept. Under this assumption, they constructed an ensemble of several classifiers for classifying bags. Nguyen et al. [13] provided a generic framework used to convert the rule-based algorithms into MIL algorithms.

Several researchers have attempted to use the embedded-space algorithms to solve the MIL problem. Various embedded-space algorithms are different with each other in that they choose from training bags the instance prototypes. Specifically, DD-SVM [4] depends on DD for choosing the instance prototypes. DD-SVM regards the instances with the local maximal DD value as prototypes. MILES [3] regards all instances in the training set as valid prototypes and selects a subset of them via learning a 1-norm linear SVM that is known to produce sparse solutions for feature weights [20]. MILD [10] depends on a conditional probability model for the instance selection. The instance possessing the highest capability in classifying the training bags is considered as a prototype. MILIS [8] achieves the initial instance selection by modeling the distribution of the negative population with a Gaussian-kernel-based kernel density estimator. Then it depends on an iterative optimization framework for the instance selection and classifier learning.

3 MILGD: A Variant of MILD

In this section, we first analyse the characteristics and bias of the MILD algorithm in order to introduce our MILGD algorithm. Then MILGD algorithm is proposed to improve the performance of MILD by considering the discrimination of its disambiguation method on the validation set. Let B^+ denote all positive training bags and B^- all negative training bags. m^+ and m^- are the size of B^+ and B^-, respectively. B is the union of B^+ and B^-, and m is the sum of m^+ and m^-. We denote the i^{th} positive bag in B^+ as B_i^+ and the j^{th} instance in that bag as B_{ij}^+. The bag B_i^+ is composed of n_i^+ instances B_{ij}^+, $j = 1, \ldots, n_i^+$. When the label of a bag does not matter, we simply denote the bag as B_i and its instances as B_{ij}. $l(B_i) \in \{+1, -1\}$ denotes the label of B_i and $l(B_{ij}) \in \{+1, -1\}$ that of B_{ij}. Note that the instance labels are not directly observable.

3.1 Analysis of MILD Characteristics

From the MIL formulation, we know that instances in each negative bag are all negative, so for negative bags there is no ambiguity on the labels of instances. However, a positive bag may contain not only positive instances but also negative instances and the labels of instances are unknown therein. Therefore, the ambiguity in instance labels in MIL arises in the positive bags and MILD is thus aimed at identifying the *true* positive instances in the positive bags.

Assumption 1. *Given a true positive instance t, the* ***probability*** *that an instance B_{ij} is positive is calculated as*

$$\Pr(l(B_{ij}) = +1 \mid t) = \exp(-\frac{\parallel t - B_{ij} \parallel^2}{\sigma_t^2}), \tag{1}$$

where $\parallel x \parallel \triangleq \sqrt{\sum_k x_k^2}$ denotes the 2-norm of the vector x, and σ_t is a parameter larger than 0.

Assumption 1 is used to compute a conditional probability. From (1), we can easily see that $0 \leq \Pr(l(B_{ij}) = +1 \mid t) \leq 1$, $\Pr(l(B_{ij}) = +1 \mid t) = 0$ when $\parallel t - B_{ij} \parallel = +\infty$ and $\Pr(l(B_{ij}) = +1 \mid t) = 1$ when $\parallel t - B_{ij} \parallel = 0$. This is well consistent with our intuition. If t is a true positive instance and $\parallel t - B_{ij} \parallel = 0$, B_{ij} will definitely be a true positive instance since B_{ij} is just equal to t, which indicates that $\Pr(l(B_{ij}) = +1 \mid t) = 1$ is reasonable. Similarly, if $\parallel t - B_{ij} \parallel = +\infty$, B_{ij} will be infinitely far away from the true positive instance t, which means that $\Pr(l(B_{ij}) = +1 \mid t) = 0$ is also reasonable. The farther B_{ij} is away from t, the lower is the probability that B_{ij} is positive given t, which is reasonable based on our intuition. Based on Assumption 1, MILD defines the probability that a bag is positive as follows.

Definition 1. *The* ***most-likely-cause estimator*** *for estimating the probability that a bag B_i is positive given a true positive instance t is defined as*

$$\begin{aligned} Pr(l(B_i) = +1 \mid t) &= \max_{B_{ij} \in B_i} Pr(l(B_{ij}) = +1 \mid t) \\ &= \max_{B_{ij} \in B_i} \exp(-\frac{\parallel t - B_{ij} \parallel^2}{\sigma_t^2}) \\ &= \exp(-\frac{d^2(t, B_i)}{\sigma_t^2}), \end{aligned} \tag{2}$$

where

$$d(t, B_i) = \min_{B_{ij} \in B_i} \parallel t - B_{ij} \parallel . \tag{3}$$

In other words, the distance $d(t, B_i)$ between an instance t and a bag B_i is simply equal to the distance between t and its nearest instance in B_i.

The definition of the most-likely-cause estimator implies that the label of a bag is most probably determined by a specific instance in it which is nearest to

the true positive instance t. In general, the larger $d(t, B_i)$ is, the lower is the probability that B_i is positive given the true positive instance t. Based on the definition of the most-likely-cause estimator, MILD gives the following theorem.

Theorem 1. *Given a true positive instance t, there exists a threshold θ_t which makes the decision function defined in (4) label the bags according to the Bayes decision rule.*

$$h^t_{\theta_t}(B_i) = \begin{cases} +1, \ d(t, B_i) \leq \theta_t, \\ -1, \ otherwise. \end{cases} \tag{4}$$

For simplicity, we ignore the proof of Theorem 1 and refer the interested readers to [10] for details. Therefore, if t is a true positive instance, there must exist a decision function as defined in (4) to label the bags well, implying that the distances from the true positive instance t to the positive bags are expected to be less than those to the negative bags. Since the positive bags may also contain negative instances just like the negative bags, the distances from a negative instance to the positive bags may be as random as those to the negative bags. Thus, for a negative instance its distances to the positive and negative bags do not exhibit the same distribution as those from t. MILD thus uses this distributional difference to identify the true positive instances. The following definition and theorem form the basis of its disambiguation method.

Definition 2. *The **empirical precision** of the decision function in (4) is defined as*

$$P_t(\theta_t) = \frac{1}{m} \sum_{i=1}^{m} \frac{1 + h^t_{\theta_t}(B_i) l(B_i)}{2}. \tag{5}$$

The empirical precision essentially measures how well the decision function $h^t_{\theta_t}(\cdot)$ with threshold θ_t mimics $l(\cdot)$ in predicting the bag labels. If t is a true positive instance, it can label the bags well according to Theorem 1, and thus the best (maximum) empirical precision $P^*(t)$ for t will be high. In contrast, if t is a negative instance, it cannot label the bags well, and thus $P^*(t)$ for t will be low. In essence, $P^*(t)$ reflects the ability of instance t in discriminating the training bags. The larger $P^*(t)$ is, the more likely t is a true positive instance. The remaining issue is how to compute $P^*(t)$ given an instance t. Theorem 2 provides the solution to this problem. Note that

$$P^*(t) = \max_{\theta_t} P_t(\theta_t), \tag{6}$$

$$\theta^*_t = \arg\max_{\theta_t} P_t(\theta_t). \tag{7}$$

Theorem 2. *The best empirical precision $P^*(t)$ for t is achieved when θ_t is an element in the set $\{d(t, B^+_i) \mid B^+_i \in B^+\}$.*

Therefore, to obtain the best empirical precision $P^*(t)$ given an instance t, we only need to compute the distance from t to every positive training bag. Given all

of the above knowledge, Li and Yeung [10] proposed their MILD algorithm. In their algorithm, they select from every positive training bag the instance with the largest P^* value as a candidate true positive instance (instance prototype).

When the disambiguation process is completed, MILD maps every training bag B_i to a point $D(B_i)$ in the embedded-space composed of all the instance prototypes, and then learns a SVM with a Gaussian kernel on all new features for bags. The new bag-level features for a bag B_i is defined as

$$D(B_i) = [d(t_1, B_i), \ldots, d(t_{m^+}, B_i)]^{\mathrm{T}}, \tag{8}$$

where $t_k \in T$ and T is the set of instance prototypes.

3.2 MILGD

Following the above description, we know that $P^*(t)$ describes the ability of an instance t in classifying the training bags. MILD just uses $P^*(t)$ as its instance selection principle. However, MILD computes $P^*(t)$ for an instance t with all the training examples and does not consider the discriminative ability of t on unknown examples. As we know, this kind of practice cannot guarantee the generalization ability of a method, specifically, the disambiguation method of MILD herein.

To solve this problem, we can group all the training bags into a training set and a validation set. Given an instance t, we first compute the best threshold θ_t^* on the training set, which corresponds to the maximum empirical precision $P^*(t)$. Then we compute the value of $P_t(\theta_t^*)$ on the validation set. This process can be considered as one fold of n-fold cross-validation. When the cross-validation approach is applied, we use the mean of $P_t(\theta_t^*)$ on all the folds to estimate the discriminability of the instance t. This is the main idea of our MILGD algorithm. Algorithm 1 summarizes the disambiguation process presented here. Note that MILGD assumes that a target concept (instance prototype) can be related to either positive bags or negative bags, whereas, in MILD the target concept is defined for positive bags only. As in DD-SVM [4], negative instance prototypes can be computed in exactly the same fashion after negating the labels of positive and negative bags.

Following Algorithm 1, we know that the main difference of MILD and MILGD lies in the instance selection standard. MILD regards the discriminative ability of an instance t on the training set as its instance selection standard, and thus MILD does not consider the discrimination of unknown examples. In contrast, MILGD regards the discriminability of t on the validation set as its instance selection standard, and hence MILGD takes into account the generalization ability of its disambiguation method. As shown in Sect. 4, this transition of instance selection standard can lead to improved performance and robustness to labeling noise. As for the bag-level feature mapping and classifier learning, there is no difference between MILGD and MILD.

Algorithm 1. Instance-Selection Method of MILGD

Input: Set of training bags B and fold number n
Output: Set of instance prototypes T

$T_p = \textbf{LearnIPs}(B, n)$
Negate labels of all bags in B
$T_n = \textbf{LearnIPs}(B, n)$
$T = T_p \cup T_n$

LearnIPs

Partition B into n subsets $\{B_1, \ldots, B_n\}$
for $B_i^+ \in B^+$ **do**
  for $B_{ij}^+ \in B_i^+$ **do**
    for $k = 1$ to n **do**
      Compute $\theta^*_{B_{ij}^+}$ on $\{B_1, \ldots, B_{k-1}, B_{k+1}, \ldots, B_n\}$ according to (7)
      Compute $P^k_{B_{ij}^+}(\theta^*_{B_{ij}^+})$ on B_k according to (5)
    end for
    $P(B_{ij}^+) = \frac{1}{n}\sum_{k=1}^{n} P^k_{B_{ij}^+}$
  end for
  $t = arg\,max_{B_{ij}^+ \in B_i^+} P(B_{ij}^+)$
  Add t to T
end for

4 Experiments

In this section, we compare the performance and efficiency of the proposed MILGD algorithm with that of other MIL algorithms using two kinds of data sets.

4.1 Drug Activity Prediction

Experimental Setup. The MUSK data sets, MUSK1 and MUSK2, are standard benchmarks for MIL, which are publicly available from the UCI Machine Learning Repository (http://archive.ics.uci.edu/ml/). These data sets consist of descriptions of molecules and the task is to predict whether a given molecule is active or inactive. Each molecule is viewed as a bag, the instances of which are the different low-energy conformations of the molecule. Surface properties of a conformation are extracted as its feature vector that has 166 dimensions. If one of the conformations of a molecule binds well to the target protein, the molecule is said active, and otherwise inactive. MUSK1 contains 47 positive bags and 45 negative bags, with an average of 5.17 instances per bag. MUSK2 contains 39 positive bags and 63 negative bags, with 64.69 instances per bag on average. MUSK2 shares 72 molecules with MUSK1, but contains more conformations for those shared molecules.

The parameter n (fold number in Algorithm 1) was set to be 2 for MILGD. We used LIBSVM (http://www.csie.ntu.edu.tw/~cjlin/libsvm/) to train all the SVMs in our experiments. We chose the regularization parameter C and

Gaussian kernel parameter γ from $\{2^{-10}, 2^{-8}, \ldots, 2^{10}\}$ using a twofold cross-validation on the training bags. As for other embedded-space MIL algorithms used for comparison, we asided by the same parameter selecting principle described here.

For the MUSK data sets, we applied ten different random runs of tenfold cross-validation to test various embedded-space MIL algorithms. We thus reported the mean and 95% confidence interval of the results of ten runs of tenfold cross-validation.

Classification Results. Table 1 reports the classification accuracies for different embedded-space MIL algorithms on the MUSK data sets. We also list some other results on the same data sets for comparison. From Table 1, we can see that APR gives the best performance on MUSK1 and MUSK2. However, the APR algorithm chooses the parameters to maximize the performance on the test set rather than the training set, and thus the superiority of APR should not be interpreted as a failure. It can also be observed from Table 1 that our MILGD algorithm is superior to other algorithms in terms of the average prediction accuracy over the two data sets, in particular, the embedded-space MIL algorithms. Furthermore, the classification accuracies of MILGD are much higher than those of MILD, which demonstrates that considering the generalization ability is indeed very helpful for MILD.

Table 1. Classification accuracies (%) for various MIL algorithms on MUSK.

Algorithm	MUSK1	MUSK2	Avg.
MILGD	87.7:[86.2, 89.2]	88.1:[86.6, 89.5]	87.9
MILD [10]	85.0:[82.8, 87.1]	85.0:[83.6, 86.5]	85.0
DD-SVM [4]	85.6:[83.9, 87.2]	87.3:[86.3, 88.2]	86.5
MILES [3]	86.6:[84.9, 88.4]	88.3:[86.8, 89.9]	87.5
MILIS [8]	86.4:[84.6, 88.2]	88.3:[87.2, 89.5]	87.4
APR [6]	92.4	89.2	90.8
DD [12]	88.9	82.5	85.7
EM-DD [19]	84.8	84.9	84.9
MI-SVM [1]	77.9	84.3	81.1
mi-SVM [1]	87.4	83.6	85.5

Computation Time. Then we evaluate the efficiency of our MILGD algorithm. Following the description of MILGD, we know that MILGD divides the whole training set into different parts (or folds) for instance selection, and then uses one part for validating and the remaining parts for training in each iteration. Therefore, the more the fold number n is, the slower MILGD is. In general, MILGD is less efficient than MILD. However, the disambiguation process of

Table 2. Computation time (minutes) for various embedded-space MIL algorithms on MUSK.

Algorithm	MUSK1	MUSK2
MILGD	0.06	2.70
MILD [10]	0.03	0.42
DD-SVM [4]	8.74	122.57
MILES [3]	0.11	4.14
MILIS [8]	6.02	3091.39

MILD itself is very fast, and thus MILGD can still accomplish the instance selection process very quickly. Table 2 reports the computation time of tenfold cross-validation for different embedded-space MIL algorithms on the MUSK data sets. From Table 2, we can see that MILD is the most efficient one while DD-SVM and MILIS are the least efficient ones among all the embedded-space MIL algorithms. But other than that, the computation time of other algorithms (i.e., MILGD and MILES) is on the same order of magnitude.

4.2 Region-Based Image Categorization

Experimental Setup. The COREL data sets have been widely used for region-based image categorization. The data sets contain 20 thematically diverse image categories with 100 images of size 384×256 or 256×384 in each category. Each image is segmented into several local regions and features are extracted from each region. The data sets and extracted features are available at http://www.cs.olemiss.edu/~ychen/ddsvm.html. Details of segmentation and feature extraction are beyond the scope of this paper and interested readers are referred to [4] for further information.

Two tests have been performed for the COREL data sets, i.e., 10-category and 20-category image categorizations. In the first test, we used the first 10 categories. In the second test, we used all 20 categories. we randomly chose from each category half of images as the training bags, and we used the remaining half as the test bags. The SVM parameters were tuned in the same way as for the MUSK data sets and the fold number n was still set to be 2. We repeated the above procedure five different times. Thus, we reported the classification accuracy over five different test sets and the corresponding 95% confidence interval. Since this is a classification problem for multi-class, the simple one-against-the-rest strategy is applied for training 10/20 binary SVMs. Therefore, the category having the largest decision value given by the SVMs is assigned to the unknown bag.

Categorization Results. We provide the classification accuracies for MILGD and other embedded-space MIL algorithms on the COREL data sets in Table 3. On both data sets, the performance of MILGD is better or highly comparable with that of other algorithms. With respect to the average accuracy over the two

Table 3. Classification accuracies (%) for various embedded-space MIL algorithms on COREL.

Algorithm	COREL_{10}	COREL_{20}	Avg.
MILGD	83.2:[81.4, 85.0]	69.9:[68.8, 71.0]	76.6
MILD [10]	80.1:[77.9, 82.3]	66.8:[65.5, 68.1]	73.5
DD-SVM [4]	73.0:[71.8, 74.1]	54.3:[51.0, 57.7]	63.7
MILES [3]	82.0:[81.2, 82.9]	69.9:[68.3, 71.6]	76.0
MILIS [8]	81.2:[79.3, 83.2]	69.7:[67.2, 72.1]	75.5

tests, MILGD outperforms all the other embedded-space MIL algorithms. Particularly, the performance of MILGD is significantly better than that of MILD, which indicates again that taking into account the generalization ability is very important for the MILD algorithm. Based on the better results on the COREL data sets, we can conclude that our MILGD algorithm is very promising for the applications satisfying the general multiple-instance assumption mentioned in Sect. 1.

5 Conclusions

In this paper, we have proposed a variant of MILD called MILGD. The goal of the study was to improve the performance of MILD via the consideration of the generalization capability of its disambiguation method. The experimental results indicate that its prediction ability can be significantly improved when taking into account the generalization capability. Moreover, due to the transition of instance selection principle (from focusing on the discriminative ability on the training set to focusing on that on the validation set), MILGD achieves the best performance as compared to other state-of-the-art embedded-space MIL algorithms.

Acknowledgements. This research has been supported by the Open Project of Key Laboratory from Ministry of Education (TJUT-CVS20170001), the Tianjin Technology Project (14ZCZDGX00868), Science and Technology Transformation Award Special Fund Project of Tianjin Chengjian University in 2017 (KJZH-A1-1709), and the Basic Research Foundation of Tianjin Chengjian University (2016CJ11).

References

1. Andrews, S., Tsochantaridis, I., Hofmann, T.: Support vector machines for multiple-instance learning. In: Advances in Neural Information Processing Systems, pp. 561–568. MIT Press (2003)
2. Bergeron, C., Moore, G., Zaretzki, J., Breneman, C.M., Bennett, K.P.: Fast bundle algorithm for multiple-instance learning. IEEE Trans. Pattern Anal. Mach. Intell. **34**(6), 1068–1079 (2012)

3. Chen, Y., Bi, J., Wang, J.Z.: MILES: multiple-instance learning via embedded instance selection. IEEE Trans. Pattern Anal. Mach. Intell. **28**(12), 1931–1947 (2006)
4. Chen, Y., Wang, J.Z.: Image categorization by learning and reasoning with regions. J. Mach. Learn. Res. **5**, 913–939 (2004)
5. Cinbis, R.G., Verbeek, J., Schmid, C.: Weakly supervised object localization with multi-fold multiple instance learning. IEEE Trans. Pattern Anal. Mach. Intell. **39**(1), 189–203 (2016)
6. Dietterich, T.G., Lathrop, R.H., Lozano-Pérez, T.: Solving the multiple instance problem with axis-parallel rectangles. Artif. Intell. **89**(1), 31–71 (1997)
7. Durand, T., Thome, N., Cord, M.: WELDON: weakly supervised learning of deep convolutional neural networks. In: Proceedings of the 29th IEEE Conference on Computer Vision and Pattern Recognition, pp. 4743–4752. IEEE, Washington (2016)
8. Fu, Z., Robles-Kelly, A., Zhou, J.: MILIS: multiple instance learning with instance selection. IEEE Trans. Pattern Anal. Mach. Intell. **33**(5), 958–977 (2011)
9. Gärtner, T., Flach, P.A., Kowalczyk, A., Smola, A.J.: Multi-instance kernels. In: International Conference on Machine Learning, pp. 179–186. Morgan Kaufmann (2002)
10. Li, W.J., Yeung, D.Y.: MILD: multiple-instance learning via disambiguation. IEEE Trans. Knowl. Data Eng. **22**(1), 76–89 (2010)
11. Li, Y., Tax, D.M.J., Duin, R.P.W., Loog, M.: Multiple-instance learning as a classifier combining problem. Pattern Recogn. **46**(3), 865–874 (2013)
12. Maron, O., Lozano-Pérez, T.: A framework for multiple-instance learning. In: Advances in Neural Information Processing Systems, pp. 570–576 (1998)
13. Nguyen, D.T., Nguyen, C.D., Hargraves, R., Kurgan, L.A., Cios, K.J.: mi-DS: multiple-instance learning algorithm. IEEE Trans. Syst. Man Cybern. Part B-Cybern. **43**(1), 143–154 (2013)
14. Rahmani, R., Goldman, S.A., Zhang, H., Cholleti, S.R., Fritts, J.E.: Localized content-based image retrieval. IEEE Trans. Pattern Anal. Mach. Intell. **30**(11), 1902–1912 (2008)
15. Ramon, J., De Raedt, L.: Multi instance neural networks. In: International Conference on Machine Learning Workshop on Attribute-Value and Relational Learning (2000)
16. Settles, B., Craven, M., Ray, S.: Multiple-instance active learning. In: Advances in Neural Information Processing Systems, pp. 1289–1296. MIT Press (2008)
17. Wang, J., Zucker, J.D.: Solving multiple-instance problem: a lazy learning approach. In: International Conference on Machine learning, pp. 1119–1126. Morgan Kaufmann (2000)
18. Zhang, M.L., Zhou, Z.H.: Improve multi-instance neural networks through feature selection. Neural Process. Lett. **19**(1), 1–10 (2004)
19. Zhang, Q., Goldman, S.A.: EM-DD: an improved multiple-instance learning technique. In: Advances in Neural Information Processing Systems, pp. 1073–1080. MIT Press (2001)
20. Zhu, J., Rosset, S., Hastie, T., Tibshirani, R.: 1-norm support vector machines. In: Advances in Neural Information Processing Systems, pp. 49–56. MIT Press (2004)

Research on Interference Energy Harvesting Based on SWIPT Relay System

Jianxiong Li[1,2], Ke Zhao[1,2], Xianguo Li[1,2(✉)], Xuelong Ding[1,2], and Weiguang Shi[1,2]

[1] School of Electronics and Information Engineering, Tianjin Polytechnic University, Tianjin 300387, China
{lijianxiong,lixianguo,shiweiguang}@tjpu.edu.cn, 1140350591@qq.com, 1206737984@qq.com

[2] Tianjin Key Laboratory of Optoelectronic Detection Technology and Systems, Tianjin 300387, China

Abstract. Simultaneous wireless information and power transfer (SWIPT) is a promising communication solution for energy-constrained wireless network. In the practical environment, the interference often results in a loss of the system rate, but it also brings energy at the same time. This paper proposes the scheme of interference energy harvesting (IEH) which can compensate for the loss of the SWIPT relay system rate caused by the interference. Based on the existing two operation strategies, time switching (TS) and power splitting (PS), we investigate the effect of IEH on the relay system rate. The interference energy is divided among subsequent transmission blocks, which can reduce the duration of energy harvesting (EH) slots. In addition, the optimal points are investigated in the different interference factors and interference power. The results show that IEH can effectively improve the relay system performance under an interference channel.

Keywords: SWIPT · Relay system · Interference energy harvesting (IEH)

1 Introduction

In recent years, energy harvesting (EH) has become a potential solution to prolong the lifetime of energy-constrained wireless network [1]. Besides other commonly used energy sources such as solar and wind, ubiquitous radio frequency (RF) signals have become another available source for wireless power transfer (WPT). So, simultaneous wireless information and power transfer (SWIPT) has drawn a great deal of attention. It can provide green energy [2] and information for the energy-constrained users simultaneously.

SWIPT first was introduced by Varshney [3]. In [3], the fundamental tradeoff between the information transmission rate and power transfer has been investigated. Two practical receiver operation strategies, time switching (TS) and power splitting (PS), have been presented in [4]. In [5], Liu et al. studied the optimal switching strategy of EH/information decoding (ID) mode under a single-input-single-output (SISO) channel subject to the time-varying interference.

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 430–439, 2018.
https://doi.org/10.1007/978-3-319-90802-1_38

Wireless relay communication system has been widely used, because it can extend the coverage of communication [6]. The relay system based on SWIPT has also attracted the attention of scholars. In [7], Krikidis et al. studied an amplify-and-forward (AF) relay system based on TS strategy. The goal was to design the optimal TS factor which minimized the probability of interruption. In [8], the AF and decode-and-forward (DF) SISO relay system based on TS strategy was discussed, and the optimal TS factor was designed to maximize the system throughput. A low complexity algorithm of the resource allocation for DF relay system was presented in [9], but it did not involve harvesting the interference energy.

In this paper, we focus on the SISO relay system based on TS or PS operation strategy and propose the scheme of interference energy harvesting (IEH). During the strong interference, the signal-to-noise ratio (SNR) sharply drops so that the information transmission (IT) is interrupted. Generally, the relay system does not operate until the end of the interference which results in a decrease of the system rate. In order to alleviate the problem, we propose the IEH scheme that the relay harvests the interference energy and then evenly divides the harvested interference energy among the subsequent transmission blocks. IEH can reduce the duration of EH slots so as to compensate for the loss of the system rate caused by the interference and improve the system performance under an interference channel. Of course, it is assumed that the channel state information (CSI) is perfectly known at the relay.

2 System Model

This paper considers a wireless relay system including a transmitter (Tx), a relay and a receiver (Rx). The Tx and the Rx are active without energy limit, while the relay is passive. The Tx and the Rx are equipped with single antenna, and the relay is equipped with double antennas. The relay works in the AF mode and employs TS or PS strategy. The link from the Tx to the relay is referred to as the downlink with channel gain $h > 0$, and the link from the relay to the Rx is referred to as the uplink with channel gain $g > 0$.

2.1 Time Switching Relay System Model

The relay system model based on TS is shown in Fig. 1. At the Tx side, the baseband signal is expressed as x, and $\mathrm{E}[|x|^2] = 1$, where $\mathrm{E}[\cdot]$ and $|\cdot|$ denote the mathematical expectation and absolute value, respectively. The RF band signal is expressed as $\sqrt{P}x$ with the average transmit power P. At the relay side, the noise n_A is a circularly symmetric complex Gaussian random variable [5], i.e. $n_A \sim CN(0, \sigma_A^2)$. y_r is the signal received by the relay. The fraction of time that the relay operates in the EH mode is defined as $\alpha \in [0, 1]$. The AF power P_r from the harvested energy in the EH mode is used to amplify the information signal y_r' to x_r, where y_r' is equal to y_r in the IT mode. At the Rx side, the received signal is expressed as y. Similarly, the noise $n_R \sim CN(0, \sigma_R^2)$ is introduced.

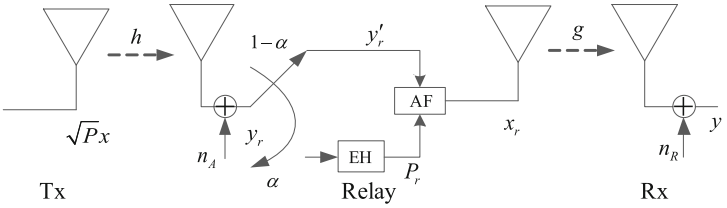


Fig. 1. Time switching relay system model

2.2 Power Splitting Relay System Model

The relay system model based on PS is shown in Fig. 2. Unlike the TS relay model, due to the use of the power splitter, new noise n_P is introduced at the relay. The fraction of energy harvested by the relay in the EH mode is defined as $\rho \in [0, 1]$.

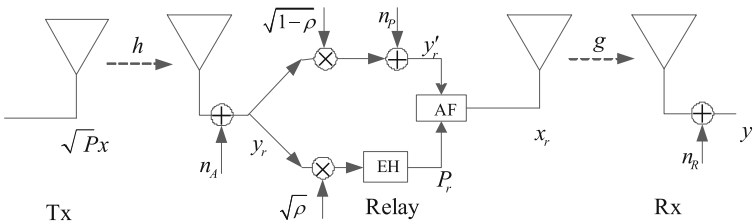


Fig. 2. Power splitting relay system model

2.3 Allocation of Blocks

As shown in Fig. 3, the TS relay system is taken as an example to illustrate the allocation of blocks. The interference lasts for mT blocks and its energy is harvested by the relay. Subsequently, a block of T is split into an EH slot and an IT slot. The relay harvests energy in the EH slot and transmits information in the IT slot. The energy harvested from the interference is evenly divided among n subsequent EH slots. New variable $\xi = m/n$ is introduced and defined as the interference factor.

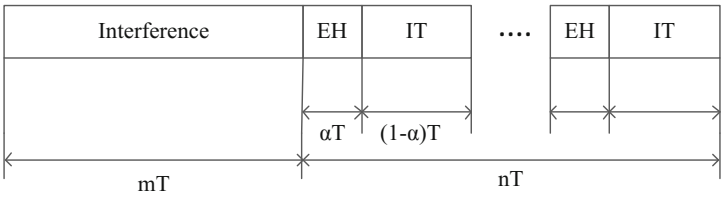


Fig. 3. Allocation of blocks

The average power of the interference is defined as P_I, and the energy harvested from the interference is expressed as $E_I = \eta P_I mT$, where η indicates the energy conversion efficiency. Therefore, the energy of each EH slot from the harvested interference energy can be expressed as

$$E_I' = \frac{\eta P_I mT}{n} = \eta \xi P_I T. \tag{1}$$

3 Problem Formulation

3.1 Time Switching Model

Frist, we consider the TS relay system shown in Fig. 1. Through the downlink, the signal y_r received by the relay is expressed as

$$y_r = \sqrt{hP}x + n_A. \tag{2}$$

The average AF power of the relay is

$$P_r = \frac{E_{EH} + E_I'}{(1-\alpha)T}, \tag{3}$$

where E_{EH} denotes the energy harvested in the EH slot and can be expressed as

$$E_{EH} = \eta hP\alpha T. \tag{4}$$

By substituting (1) and (4) into (3), we obtain

$$P_r = \frac{\eta hP\alpha T + \eta \xi P_I T}{(1-\alpha)T} = \frac{\eta(h\alpha P + \xi P_I)}{1-\alpha}. \tag{5}$$

Then, the signal x_r transmitted by the relay can be expressed as

$$x_r = \sqrt{\frac{P_r}{hP + \sigma_A^2}}(\sqrt{hP}x + n_A). \tag{6}$$

Through the uplink, the signal y received by the Rx can be expressed as

$$y = \sqrt{g}x_r + n_R = \sqrt{\frac{gP_r}{hP + \sigma_A^2}}(\sqrt{hP}x + n_A) + n_R. \tag{7}$$

Thus, the SNR of the signal y is obtained as

$$SNR = \frac{hg\eta P(h\alpha P + \xi P_I)}{g\eta(h\alpha P + \xi P_I)\sigma_A^2 + (1-\alpha)(hP + \sigma_A^2)\sigma_R^2}. \tag{8}$$

The system rate is given by

$$R_{TS} = \frac{1-\alpha}{1+\xi} \cdot \log_2\left(1 + \frac{hg\eta P(h\alpha P + \xi P_I)}{g\eta(h\alpha P + \xi P_I)\sigma_A^2 + (1-\alpha)(hP + \sigma_A^2)\sigma_R^2}\right). \tag{9}$$

Then, we consider the following optimization problem (P1),

$$\begin{aligned} \text{(P1)} \quad & \max_{\alpha} \quad R_{TS} \\ & s.t. \quad 0 < \alpha < 1 . \end{aligned}$$

Problem (P1) can be solved by the extremum method. With the first derivative $R'_{TS}(\alpha) = 0$, the extreme point can be obtained as $\alpha = \alpha^*$. At the same time, we verify whether the second derivative $R''_{TS}(\alpha^*)$ is less than zero. If $R''_{TS}(\alpha^*) < 0$, it can be determined that α^* is the maximum point, i.e., the optimal point. The maximum system rate at the optimal point α^* is defined as R^*_{TS}.

3.2 Power Splitting Model

Through the downlink, the signal y_r received by the relay shown in Fig. 2 is expressed as (2). The signal y'_r is expressed as

$$y'_r = \sqrt{1-\rho}(\sqrt{hP}x + n_A) + n_P. \tag{10}$$

The average AF power of the relay is

$$P_r = \frac{E_{EH} + E'_I}{T}, \tag{11}$$

where E_{EH} in (11) is the harvested energy by the relay in a block and expressed as

$$E_{EH} = \eta h \rho P T. \tag{12}$$

Substituting (12) and (1) into (11), we obtain

$$P_r = \frac{\eta h \rho P T + \eta \xi P_I T}{T} = \eta(h\rho P + \xi P_I). \tag{13}$$

Then, the signal x_r can be expressed as

$$x_r = \sqrt{\frac{P_r}{(1-\rho)(hP + \sigma_A^2) + \sigma_P^2}} \cdot [\sqrt{1-\rho}(\sqrt{hP}x + n_A) + n_P]. \tag{14}$$

Through the uplink, the signal y received by the Rx can be expressed as

$$y = \sqrt{\frac{gP_r}{(1-\rho)(hP+\sigma_A^2)+\sigma_P^2}} \cdot [\sqrt{1-\rho}(\sqrt{hP}x + n_A) + n_P] + n_R. \tag{15}$$

Thus, the SNR of the received signal y is obtained as

$$SNR = \frac{(1-\rho)hgP}{(1-\rho)g\sigma_A^2 + g\sigma_P^2 + \frac{\left[(1-\rho)(hP+\sigma_A^2)+\sigma_P^2\right]\sigma_R^2}{\eta(h\rho P + \xi P_I)}}. \tag{16}$$

The system rate is given by

$$R_{PS} = \frac{1}{1+\xi} \cdot \log_2 \left(1 + \frac{(1-\rho)hgP}{(1-\rho)g\sigma_A^2 + g\sigma_P^2 + \frac{\left[(1-\rho)(hP+\sigma_A^2)+\sigma_P^2\right]\sigma_R^2}{\eta(h\rho P + \xi P_I)}} \right). \tag{17}$$

Then, we consider the following optimization problem (P2),

$$\text{(P2)} \max_{\rho} \quad R_{PS}$$
$$s.t. \quad 0 < \rho < 1 .$$

The solution method of (P2) is the same as that of (P1), and the optimal point is $\rho = \rho^*$. The maximum systen rate at the optimal point ρ^* is defined as R_{PS}^*.

4 Simulation Results

Unless otherwise specified, the simulation parameters are set as follows: $h = 1$, $g = 1$, $P = 200$, $P_I = 100$, $\xi = 0.1$, and the noise power is set to be $\sigma_A^2 = \sigma_R^2 = \sigma_P^2 = 1$. For convenience, the energy conversion efficiency is set to be $\eta = 1$.

4.1 The Effect of IEH on the System Rate

The relay system rates based on TS and PS are shown in Figs. 4 and 5, respectively.

As shown in Fig. 4, the relay system rate based on TS with IEH is higher than that without IEH in [8]. Furthermore, the optimal point α^* with IEH is smaller than that without IEH, since the harvested interference energy reduces the duration of the EH slot. Therefore, the duration of the IT slot increases, and the system rate naturally rises. The same conclusions can be obtained by analyzing Fig. 5. Compared with [10], the system performance based on PS is improved effectively.

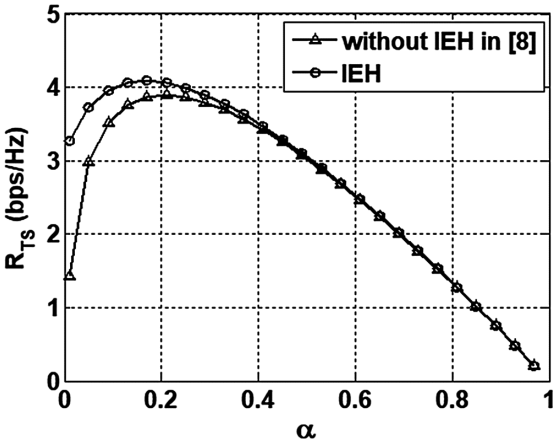


Fig. 4. The system rate based on TS

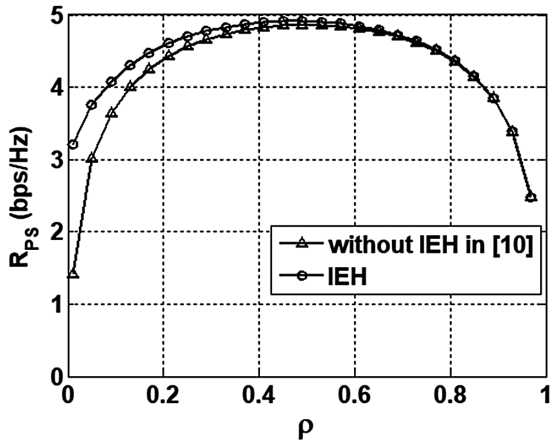


Fig. 5. The system rate based on PS

4.2 The Effect of the Interference Power on the Optimal Points

The optimal points α^* and ρ^* in the different interference power are shown in Figs. 6 and 7, respectively. They decrease gradually with the increase of the interference power, since the stronger interference can supply more energy. Hence fewer resources are allocated for EH and more resources are allocated for IT. In other words, the optimal point decreases and the system rate increases. As such, IEH reduces more loss of the system rate caused by the interference if the interference power is larger.

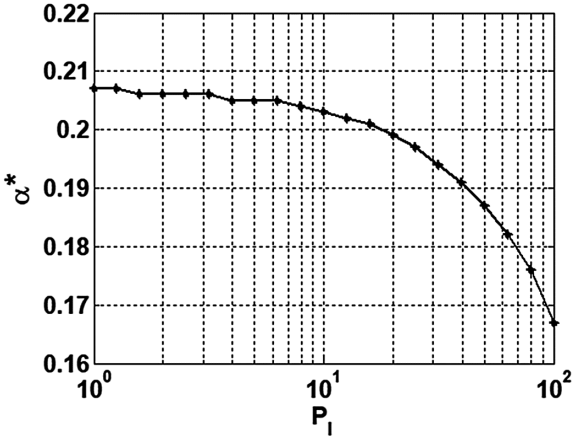


Fig. 6. The optimal point α^* in the different interference power

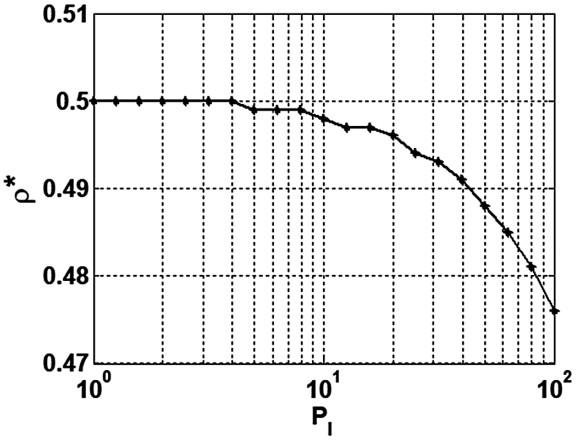


Fig. 7. The optimal point ρ^* in the different interference power

4.3 The Effect of the Interference Factor on the Optimal Points and the Corresponding Maximum System Rates

When other parameters are fixed, the optimal points α^*, ρ^* and the corresponding maximum system rates in the different interference factors are shown in Figs. 8 and 9, respectively. With the increase of ξ, the optimal points and the maximum system rates decrease simultaneously.

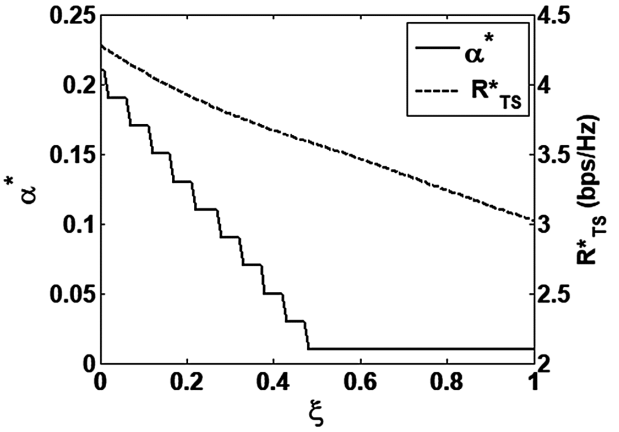


Fig. 8. The optimal point α^* and the maximum system rate R_{TS}^* in the different interference factors

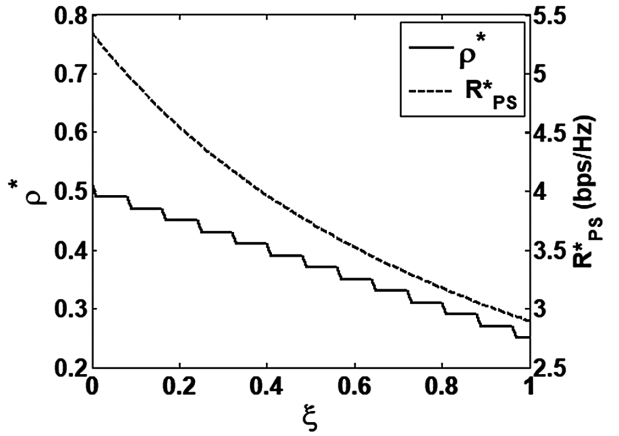


Fig. 9. The optimal point ρ^* and the maximum system rate R_{PS}^* in the different interference factors

5 Conclusion

This paper proposes the scheme of IEH based on SWIPT relay system. The optimal points α^* and ρ^* are investigated in the different interference power and interference factors. For the relays based on TS or PS operation strategy, the simulation results show that IEH can compensate for the loss of the system rate caused by the interference and effectively improve the system performance.

Acknowledgments. This work was supported by the National Natural Science Foundation of China (Grant No. 61372011), Natural Science Foundation of Tianjin (Grant No. 16JCTPJC46900) and Tianjin Research Program of Application Foundation and Advanced Technology (Grant No. 15JCYBJC16300).

References

1. Sudevalayam, S., Kulkarni, P.: Energy harvesting sensor nodes: survey and implications. J. IEEE Commun. Surv. Tutorials **13**, 443–461 (2011)
2. Mahapatra, R., Nijsure, Y., Kaddoum, G.: Energy efficiency tradeoff mechanism towards wireless green communication. J. IEEE Commun. Surv. Tutorials **18**, 686–705 (2016)
3. Varshney, L.R.: Transporting information and energy simultaneously. In: IEEE International Symposium on Information Theory, pp. 1612–1616. IEEE Press, Toronto (2008)
4. Zhang, R., Ho, C.K.: MIMO broadcasting for simultaneous wireless information and power transfer. J. IEEE T Wirel Commun. **12**, 1989–2001 (2013)
5. Liu, L., Zhang, R., Chua, K.C.: Wireless information transfer with opportunistic energy harvesting. J. IEEE Trans. Wirel. Commun. **12**, 288–300 (2012)
6. Wireless Relay Communication System and Method. http://www.freepatentsonline.com
7. Krikidis, I., Timotheou, S., Sasaki, S.: RF energy transfer for cooperative networks: data relaying or energy harvesting. J. IEEE Commun. Lett. **16**, 1772–1775 (2012)
8. Nasir, A.A., Zhou, X., Durrani, S., Kennedy, R.A.: Wireless energy harvesting and information relaying: adaptive time-switching protocols and throughput analysis. J. IEEE Trans. Commun. **63**, 1607–1622 (2015)
9. Huang, G., Zhang, Q., Qin, J.: Joint time switching and power allocation for multicarrier decode-and-forward relay networks with SWIPT. J. IEEE Sig. Proc. Lett. **22**, 2284–2288 (2015)
10. Chen, Z., Xia, B., Liu, H.: Wireless information and power transfer in two-way amplify-and-forward relaying channels. In: IEEE Global Conference on Signal and Information Processing, pp. 168–172. IEEE Press, China (2014)

Optimization of Density-Based K-means Algorithm in Trajectory Data Clustering

Mei-Wei Hao[1(✉)], Hua-Lin Dai[2], Kun Hao[1], Cheng Li[1], Yun-Jie Zhang[1], and Hao-Nan Song[3]

[1] College of Computer and Information Engineering, Tianjin Chengjian University, Tianjin 300384, China
angelsamle@126.com, littlehao@126.com, licheng.mum@gmail.com, zhangyunjietj@163.com

[2] Computing Center, Tianjin Chengjian University, Tianjin 300010, China
99871382@qq.com

[3] Department of Electrical Engineering, Tsinghua University, Beijing 10000, China
shn14@mails.tsinghua.edu.com

Abstract. Since the amount of trajectory data is large and the structure of trajectory data is complex, an improved density-based K-means algorithm was proposed. Firstly, high-density trajectory data points were selected as the initial clustering centers based on the density and increasing the density weight of important points, to perform K-means clustering. Secondly the clustering results were evaluated by the Between-Within Proportion index. Finally, the optimal clustering number and the best clustering were determined according to the clustering results evaluation. Theoretical researches and experimental results showed that the improved algorithm could be better at extracting the trajectory key points. The accuracy of clustering results was 24% points higher than that of the traditional K-means algorithm and 16% points higher than that of the Density-Based Spatial Clustering of Applications with Noise algorithm. The proposed algorithm has a better stability and a higher accuracy in trajectory data clustering.

Keywords: K-means algorithm · Based on density
Characteristics of vehicle activity · Weighted density · Initial clustering center
Between-Within Proportion (BWP) index

1 Introduction

With the advent of the era of big data and the rapid development of mobile location services, trajectory data has become an important digital resource. Since the amount of trajectory data is very large and the quality of trajectory data is usually poor, it is becoming a hot issue that how to obtain the deep semantics of trajectory data by data mining and visualization analysis. Clustering algorithm as an effective technique for trajectory data feature extraction is widely used in trajectory data mining.

The K-means algorithm [1] as a typical partition-based clustering algorithm is widely used because of its simplicity and high efficiency. However, it requires users to determine the clustering number and the initial clustering centers based on the relevant

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 440–450, 2018.
https://doi.org/10.1007/978-3-319-90802-1_39

experience or background field, and performs sensitively to the selection of the initial clustering centers and the order of the data input, which may result in unstable and inaccurate clustering results. Aiming at these problems, many scholars have proposed different improvement programs. There are density-based improvements: the literature [2] proposed the cluster center initialization algorithm (CCIA), which clusters according to the density-distribution information of sample data points to obtain the initial clustering centers, the literature [3] proposed selecting the sample data points with farthest from the global sample data center in the high-density area as the initial clustering centers. However, these algorithms are not applicable in the sample datasets of which the data distribution is relatively uniform. When filtering the sample data points according to the density, they need to add other parameters for auxiliary judgements. There are distance-based improvements: the literature [4] proposed the method of dynamically adjusting the selection of the initial clustering centers based on the principle that the distance within the cluster is less than the distance between clusters, the literature [5] proposed the algorithm which clusters by giving every sample data point the specific weighting factor according to the distance between the data and the initial clustering center to cluster, the literature [6] proposed determining the initial clustering centers based on minimal maximum algorithm and partitioning the sample dataset based on Euclidean distance. However, these algorithms when used in larger datasets increase the algorithm time complexity and reduce the operation efficiency. In addition, the clustering results are susceptible to interference of outliers. There are also density-distance-based improvements: the literature [7] proposed the algorithm which is local clustered by dividing the sample dataset into several small subsets with the centroid and weight, but the computational complexity increases in high-dimensional sample datasets, the literature [8] proposed selecting the initial clustering centers based on the square error criteria, but the efficiency of the algorithm obviously decreases in large-scale datasets.

Since the amount of trajectory data is very large and the structure of trajectory data is relatively complex, this paper proposed an improved density-based K-means algorithm. The improved algorithm this paper proposed can automatically obtain the clustering number and the initial clustering centers, and has a strong anti-noise interference ability. In addition, because of filtering the sample trajectory data points by characteristics of vehicle activity, the accuracy of the clustering results is effectively improved. This algorithm not only has important significance for the research of regular changes in road traffic, but also has positive significance for the exploration of human activity hotspots area.

2 Related Description and Definition

Assume the set of trajectory data points $P = \{p_1, p_2, p_3, \ldots, p_n\} \in R^{d*n}, d = 3$, d means the number of the sample trajectory dataset dimension, which is three in this paper. The three dimensions include spatial longitude coordinates, spatial latitude coordinates and time dimension. n means the total number of the trajectory data points.

The following is some of the important concepts proposed in this paper:

Definition 1 (Density of a trajectory data point). The density [9] $Dens_r(p_i)$ of any one of the trajectory data points p_i is defined as follows:

$$Dens_r(p_i) = \sqrt{\frac{1}{N-1}\sum_{j=1,j\neq i}^{N}(r - Dist^2(p_i, p_j))} \tag{1}$$

r means the effective density radius; N means the total number of the trajectory data points contained within the radius; p_j means the j-th trajectory data point in the circle with the center p_i and radius r; $Dist(p_i, p_j)$ means Euclidean distance between p_i and p_j, that is, the real distance between p_i and p_j in the map, $Dist^2(p_i, p_j)$ means the square of Euclidean distance $Dist(p_i, p_j)$.

Definition 2 (Weighted density of a trajectory data point in turning state). After recognizing the straight or turning state of the trajectory data points (that is, the straight or turning activity state of the corresponding vehicle in this point), it is necessary to increase the filtering probability of the turning state of the trajectory data points by increasing the weight density. Thus, the concept of the weighted density of a trajectory data point in turning state is introduced. The weighted density [5, 9] $WDens_r(p_i)$ of any one of the trajectory data points in turning state p_i is defined as follows:

$$WDens_r(p_i) = \sqrt{\frac{1}{N-1}\sum_{j=1,j\neq i}^{N}(r - Dist(p_i, p_j))^2(1 + \frac{r - Dist(p_i, p_j)}{r})} \tag{2}$$

Definition 3 (Average distance of the trajectory data points). The average distance of the trajectory data points is defined as follows:

$$avgDist = \frac{1}{n(n-1)}\sum_{j=1}^{n}\sum_{i=1,i\neq j}^{n}(Dist(p_i, p_j)) \tag{3}$$

i and j means subscript, having. The average distance of the trajectory data points can effectively reflect the overall degree of the discretization of the trajectory dataset, and provide a valid basis for the better determination of the neighborhood radius.

Definition 4 (Neighborhood radius). The neighborhood radius as the effective density radius is not only directly involved in the calculation of the density value, but also determines how many points of the trajectory data points may be contained within the radius. Therefore, the appropriate neighborhood radius is critical to the density calculation. The neighborhood radius γ is defined as follows:

$$\gamma = \sqrt{\frac{1}{n-1}\sum_{j=1}^{n}\sum_{i=1,i\neq j}^{n}(Dist(p_i, p_j) - avgDist)^2} \tag{4}$$

The smaller the neighborhood radius is, the closer the trajectory data points in the neighborhood are.

Definition 5 (Length of trajectory step). The vehicle trajectory data are usually sampled at even time intervals. The length of trajectory step is used to reflect the average length of each sub-trajectory segmented by the trajectory data points. It also can be used to indirectly reflect the rate and other attributes of the vehicle's activity in the trajectory. The trajectory step ε is defined as follows:

$$\varepsilon = \frac{\sum_{i=1}^{m} L_i}{\sum_{i=1}^{m} P_i - m} \tag{5}$$

m means the total number of the trajectory; L_i means the length of each trajectory; P_i means the total number of the trajectory data points in each trajectory. The length of trajectory step is shorter, the rate of the vehicle is lower, and the density of the trajectory data points contained within the length is higher. It is generally considered that when the vehicle in the turning process the density of trajectory data points is high, and the rate of the vehicle is low.

3 Improved Density-Based K-means Algorithm

3.1 Selection of Initial Clustering Centers Based on Density

The improved algorithm was described as follows:

Input: The trajectory dataset X containing n objects, the predicted clustering number K, the minimum density threshold $minDen$, the neighborhood radius γ, the length of trajectory step ε

Output: The set T of the initial clustering centers containing K objects, the set P of the trajectory data points without noise

Begin:

1. Make sets $D = \{\}$, $D' = \{\}$, $W = \{\}$, $T = \{\}$, $P = \{\}$;
2. According to the formula (3) and the formula (4), calculate the neighborhood radius γ; according to the formula (5), calculate the length of trajectory step ε;
3. ***For*** $x_i \in X$, ***Do*** Give x_i a density label, and taking $r = \gamma$, according to formula (1), calculate the initial density $Dens_r(x_i)$ of x_i;
4. Calculate the minimum density threshold $\min Den = \frac{1}{n}\sum_{i=1}^{n} Dens_r(x_i)$; select the first 2K objects with the large initial density, which are put into the set D;
5. ***For*** $x_i \in X$, **Do**
   5.1 Taking $r = \varepsilon$, according to the formula (1), calculate the density $Dens_r(x_i)$ of x_i;
   5.2 ***If*** $Dens_r(x_i) \geq \min Den$, ***THEN*** Put x_i into the set D';

6. Take the objects in the set D into the set W (These objects only with the spatial and time attributes are the same as those of the set D' in the spatial dimension and the time dimension);
7. ***For*** $x_i \in W$, ***Do*** Give x_i a turning state label, and taking $r = \gamma$, according to the formula (2), calculate the weight density $WDens_r(x_i)$ of x_i, updating its density label in the set X and D;
   Repeat:
8. Take the first object d_i with no center point or boundary point label in the set D;
   8.1 Let d_i be a center of a new cluster, and give d_i and the corresponding x_i a center point label;
   8.2 ***For*** $x_i \in X$ and $x_i \neq d_i$, ***Do***
   If x_i is the point of direct density-reachable of d_i and x_i has no center point or boundary point label, ***Then*** Give x_i a boundary point label, and put it in this cluster;
   8.3 Update d_i's density label, ***If*** d_i has the turning state label, ***THEN*** Taking $r = \gamma$, according to the formula(2), calculate the weight density $WDens_r(d_i)$ of d_i, Else THEN Taking $r = \gamma$, according to the formula(1), calculate the density $Dens_r(d_i)$ of d_i;
   Until: Traverse all the objects in the set D, until each object in the set D has a central point or a boundary point label;
9. In the set D, select the first K objects with the center point label and the large density, which are put into the set T;
10. ***For*** $x_i \in X$, ***Do If*** x_i has no center point or boundary point label, ***THEN*** Give x_i a noise label, ***Else THEN*** Put x_i into the set P;
11. Output the results;

End

3.2 Optimized Selection of the Number K of Clusters

A lot of experiments and experience show [10] that the best clustering number K should be in the $[2, \sqrt{n}]$, n meaning the total number of sample data. Based on this, many scholars proposed a simple and effective way to select the clustering number K. The basic idea of it is searching for the K optimal value in the $[2, \sqrt{n}]$. That is, the sample dataset is clustered for each determined K_{opt} value, then evaluate the clustering results corresponding to the K_{opt} value by clustering validity function. When the clustering results are optimal, the corresponding K_{opt} value is the best clustering number K.

This paper used the BWP index [11] $BWP(j, i)$ as the clustering validity function to reflect the tightness within the cluster and the separation between clusters by the ratio of the clustering deviation distance $bsw(j, i)$ and the clustering distance $baw(j, i)$. j and i meaning the i-th sample data of the j-th cluster. The specific description of $BWP(j, i)$ is as follows:

$$BWP(j,i) = \frac{bsw(j,i)}{baw(j,i)} = \frac{b(j,i) - w(j,i)}{b(j,i) + w(j,i)} \tag{6}$$

b(j, i) means the minimum distance between clusters of the *i*-th sample data of the *j*-th cluster, that is, the minimum value of the average distance between the sample data and each other clusters. The specific description of *b(j, i)* is as follows:

$$b(j,i) = \min_{1 \le k \le C, k \ne j} \left(\frac{1}{n_k} \sum_{p=1}^{n_k} Dist(x_p^{(k)}, x_i^{(j)})\right) \tag{7}$$

C means the number of clustering; *k* and *j* means the cluster index; n_k means the total number of the sample data of the *k*-th cluster; $x_p^{(k)}$ means the *p*-th sample data of the *k*-th clusters; $x_i^{(j)}$ means the *i*-th sample data of the *j*-th clusters; $Dist^2(x_p^{(k)}, x_i^{(j)})$ means the square of Euclidean distance between $x_p^{(k)}$ and $x_i^{(j)}$. From the viewpoint of the degree of separation between clusters, the minimum distance between clusters *b(j, i)* is the bigger the better.

w(j, i) means the distance within the cluster of the *i*-th sample data of the *j*-th cluster, that is, average distance between the sample data and each other sample data in this cluster. The specific description of *w(j, i)* is as follows:

$$w(j,i) = \frac{1}{n_j - 1} \sum_{q=1}^{n_j} Dist^2(x_q^{(j)}, x_i^{(j)}) \tag{8}$$

From the viewpoint of the degree of tightness within clusters, the minimum distance between clusters *b(j, i)* is the smaller the better.

The higher the average BWP of all the sample data points is, the higher the quality of clustering results is. When the average BWP is maximum, the best clustering number *K* is K_{opt} (the clustering number corresponding to the clustering results). The specific description of the best number *K* of clusters is as follows:

$$K = K_{opt} = \max_{2 \le k \le \sqrt{n}} \left(\frac{1}{n} \sum_{j=1}^{k} \sum_{i=1}^{n_k} BWP(j,i)\right) \tag{9}$$

n means the total number of the sample data; n_k means he total number of the sample data of the *k*-th cluster.

3.3 Improved Density-Based K-means Algorithm with BWP Index

The basic idea of the algorithm this paper proposed was as follows. Firstly, successively selected the number K_{opt} of clusters in the $[2, \sqrt{n}]$, *n* meaning the total number of the trajectory data. Secondly, according to the selected clustering number K_{opt}, the improved density-based clustering algorithm selected the initial clustering centers by clustering iteration. Then the selected clustering number K_{opt} and the obtained initial clustering

centers were used for the improved K-means algorithm, to cluster the trajectory data and evaluate the clustering results by BWP index. Finally, when the BWP maximum, the corresponding clustering number K_{opt} was taken as the best clustering number K, and the corresponding clustering results were taken as the optimal clustering results.

The improved algorithm was described as follows:

Input: The trajectory dataset X containing n objects, the minimum density threshold *minDen*, the neighborhood radius γ, the length of trajectory step ε

Output: The best clustering number K, the set T of optimal clustering results

Begin:

1. Make sets $X = \{\}$, $T' = \{\}$, $T = \{\}$, $S = \{\}$;
2. ***For*** $k = 2$ ***To*** $[\sqrt{n}]$;
   - 2.1 According to the improved density-based clustering algorithm, select the k initial clustering centers;
   - 2.2 According to the improved K-means algorithm, the trajectory dataset without noise is clustered and the clustering results are put into the set T';
   - 2.3 According to the formula (6), calculate average BWP value *avgBWP* of the clustering results, and put (k, *avgBWP*) into the set S;
   - 2.4 Put the set T' into the set X, then make set $T' = \{\}$;
3. Comparing the *avgBWP* values of the objects in the set S, take the object *target* where the max *avgBWP* is located and record the subscript *index* of the object;
4. K is k of *target*; $T = X_{index}$, X_{index} means the *index*-th object of the set X;
5. Output the results;

End

The algorithm this paper proposed was optimized based on the traditional K-means algorithm. It ensured that the initial clustering center could be generated in the high-density trajectory data points, reduced the interference of outliers in the trajectory dataset on the clustering results, avoided the clustering results falling into the local optimal solution, and improved the accuracy of the clustering results. In addition, under the BWP index intervention, this algorithm could automatically obtain the best clustering number and highly effectively select the high-quality clustering results. It solved the big problem that when the structure of the trajectory dataset unknown, the best clustering number was difficult to be determined.

4 Experimental Results and Analysis

4.1 Experimental Platform and Data

The paper was selected from 8:00 to 10:00, 12:00 to 14:00, 16:00 to 18:00 and 20:00 to 22:00 from 4th to 14th August 2015, in Beijing Dongcheng District taxi GPS data provide by DataTang as four sets of experimental data. Each sample experiment data points included vehicle ID number, latitude and longitude coordinate point and time information. A detailed description of the data set is shown in Table 1.

Table 1. Trajectory dataset used in the experiment

Trajectory dataset	Period	Dimension	Total number of sample data	Number of trajectory path
Data1	8:00–10:00	3	21078	619
Data2	12:00–14:00	3	25162	675
Data3	16:00–18:00	3	23179	634
Data4	20:00–22:00	3	19764	596

4.2 Comparison and Analysis of Three Kinds of Clustering Algorithms

To verify the feasibility of the algorithm this paper proposed, it was compared with the traditional K-means algorithm and DBSACN algorithm, including comparison of clustering result and algorithm efficiency.

The analysis of clustering results included five aspects: the accuracy of clustering results, the distance within the cluster, the distance between clusters, the best number of clusters and the number of clustering iterations. To guarantee the reasonable validity of the traditional K-means algorithm, each dataset would repeat the experiment 50 times and take the average value as the final clustering result, when clustering experiments using the traditional K-means algorithm. The results of the three algorithms are shown in Table 2.

Table 2. Comparison of clustering results of three algorithms

Algorithm	Trajectory dataset	Accuracy	Distance within the cluster	Distance between clusters	Best number of clusters	Number of clustering iterations
Traditional K-means algorithm	Data1	58.17%	0.46	1.23	81	13
	Data2	64.83%	0.35	1.10	80	10
	Data3	63.02%	0.33	1.20	85	11
	Data4	62.17%	0.42	1.25	83	11
DBSCAN algorithm	Data1	62.08%	0.43	1.25	73	12
	Data2	74.50%	0.30	1.13	85	8
	Data3	73.11%	0.37	1.30	63	9
	Data4	70.02%	0.39	1.29	65	9
The algorithm this paper proposed	Data1	83.07%	0.41	1.32	75	10
	Data2	90.52%	0.30	1.15	85	8
	Data3	86.03%	0.36	1.30	61	9
	Data4	85.53%	0.37	1.33	63	9

It could be seen from Table 2 that the accuracy of clustering results of the proposed algorithm was 24.45% points higher than that of the traditional K-means algorithm and 16.36% points higher than that of the Density-Based Spatial Clustering of Applications with Noise algorithm. To further verify the clustering results of the three algorithms in the trajectory dataset, choose the clustering results of the trajectory dataset Data3 as shown in Figs. 1, 2 and 3.

Fig. 1. Heat map of clustering results based on the algorithm this paper proposed

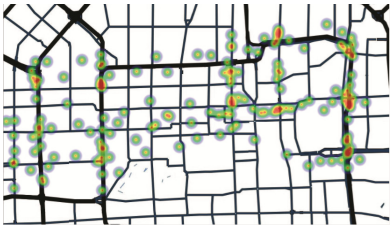


Fig. 2. Heat map of clustering results based on the DBSCAN algorithm

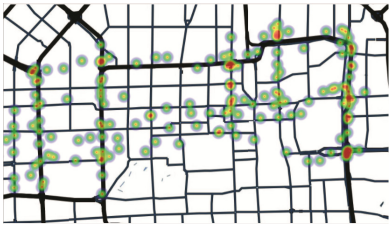


Fig. 3. Heat map of clustering results based on the traditional K-means algorithm

Compared with Figs. 1, 2 and 3, the proposed algorithm and DBSCAN algorithm were more reasonable in clustering than traditional K-means algorithm, and could better highlight the path of traffic in the trajectory distribution. In addition, the proposed algorithm had better anti-noise interference ability than the other two algorithms, and the clustering results of the trajectory data were more suitable for the actual road.

The analysis of three algorithm efficiency was analyzed by comparing the time (including the shortest, longest and average time) spent in a single cluster iteration CPU in different trajectory data sets. The results of the three algorithms were shown in Table 3.

Table 3. Comparison of operational efficiency of three algorithms

Algorithm		Traditional K-means algorithm	DBSCAN algorithm	The algorithm this paper proposed
Data1	Best/s	1.032	0.650	0.545
	Worst/s	2.998	1.695	1.572
	Average/s	2.579	1.312	1.246
Data2	Best/s	1.352	0.853	0.818
	Worst/s	4.013	3.720	3.712
	Average/s	3.188	2.641	2.575
Data3	Best/s	1.201	0.809	0.722
	Worst/s	3.913	3.263	3.38
	Average/s	3.062	2.372	2.346
Data4	Best/s	1.175	0.672	0.678
	Worst/s	3.113	2.086	2.033
	Average/s	2.473	1.492	1.498

The experimental results showed that at each iteration, the average consumption time of the proposed algorithm was similar to that of the DBSCAN algorithm. Although the time complexity was higher when searching for the initial clustering centers, in the complex trajectory datasets, the proposed algorithm could effectively reduce the number of iterations and improve the operating efficiency to a certain extent.

5 Conclusion

The improved density-based K-means algorithm was proposed in this paper. Combining the BWP index, the proposed algorithm selected the key trajectory data points in high-density area as the initial clustering centers, to ensure obtaining the high-quality clustering results which were tightness within the cluster and separation between clusters. The experimental results showed that the proposed algorithm was more accurate and highly efficient, and the simulation results showed that the proposed algorithm could extract the key points of the trajectory data well. In this paper, the time complexity is increased when calculating the sample spacing and selecting the initial clustering center. In the future research, the computational efficiency of this part will be improved.

Acknowledgments. This research was supported by the Fundamental Research Funds for the Universities in Tianjin, Tianjin Chengjian Universities (2016CJ11)

References

1. Wang, Z.C., Yuan, X.R.: Visual analysis of trajectory data. J. Comput.-Aided Des. Comput. Graph. (1), 9–25 (2015)
2. Khan, S.S., Ahmad, A.: Cluster center initialization algorithm for K-means clustering. Expert Syst. Appl. **25**(11), 1293–1302 (2004)

3. He, Y.B., Liu, X.J., Wang, Z.Q., et al.: Improved K-means algorithm based on global center and nonuniqueness high-density points. J. Comput. Eng. Appl. **52**(1), 48–54 (2016)
4. Zhu, M., Wang, W., Huang, J.: Improved initial cluster center selection in K-means clustering. Eng. Comput. **31**(8), 1661–1667 (2014)
5. Zhang, T., Ma, F.: Improved rough K-means clustering algorithm based on weighted distance measure with Gaussian function. Int. J. Comput. Math. 1–17 (2015)
6. Zhang, S.Q., Huang, Z.K., Feng, M.: An optimized K-means algorithm. Microelectron. Comput. **32**(12), 36–39 (2015)
7. Capó, M., Pérez, A., Lozano, J.A.: An efficient approximation to the K-means clustering for massive data. Knowl.-Based Syst. **117**, 56–69 (2017)
8. Zhang, S.J., Zhao, H.C.: Algorithm research of optimal cluster number and initial cluster center. J. Appl. Res. Comput. **34**(6), 1–5 (2017)
9. Rodriguez, A., Laio, A.: Machine learning. Clustering by fast search and find of density peaks. Science **344**(6191), 1492 (2014)
10. Rezaee, M.R., Lelieveldt, B.P.F., Reiber, J.H.C.: A new cluster validity index for the fuzzy c-mean. Pattern Recogn. Lett. **19**(3–4), 237–246 (1998)
11. Zhou, S.B., Xu, Z.Y., Tang, X.Q.: Method for determining optimal number of clusters in K-means clustering algorithm. J. Comput. Appl. **46**(16), 27–31 (2010)

A Haze Prediction Algorithm Based on PCA-BP Neural Network

Dong Li(✉), Shudong Liu, Rong Liu, Cheng Li, and Yunjie Zhang

School of Computer and Information Engineering,
Tianjin Chengjian University, Tianjin, China
328848806@qq.com

Abstract. In this paper, we proposed a novel haze forecast model, which combine the principal component analysis with back-propagation neural network to solve the air quality problem in China. Comprehensive variables are obtained by dimension reduction on many predictive factors through principal component analysis (PCA). Then we use the comprehensive variables as the input of back-propagation (BP) neural network. Through this process, the correlation among the original predictors can be eliminated and the structure of neural network can be simplified. The simulation results show that the average prediction error of the prediction model by using principal component analysis combined with BP neural network is less than 10%, far lower than the results of the traditional prediction method which only use a single index, $PM_{2.5}$ daily average concentration, to judge whether it is haze day.

Keywords: Haze forecast · PCA · BP neural network
Comprehensive variables

1 Introduction

The solving of the air pollution problem is imminent with the intensification of urbanization in China, especially the air quality in the Beijing-Tianjin-Hebei region. According to statistics, the number of heavy pollution days up to 29 all the year round in Tianjin and the average concentration of $PM_{2.5}$, PM_{10} and NO_2 is above the national standard. Among them, the average concentration of $PM_{2.5}$ is 69 μg/m^3, which exceeds 0.97 times to the normal; the average concentration of PM_{10} was 103 μg/m^3, which was 0.47 times higher.

Because of the vast territory, complex terrain and capricious climate in China, it is very important to monitor and forecast the weather conditions and make corresponding countermeasures. In recent years, domestic and foreign scholars have put a lot of energy in haze prediction research and proposed a variety of prediction methods and models and also achieved a series of research results. Hou used the cubic exponential smoothing model to analysis and forecast haze weather [1]. According to the characteristics of BP artificial neural network, Ai proposed a haze weather forecasting system based on the BP artificial neural network, which can approximate any nonlinear function [2]. Haze forecast method of selective ensemble based on glowworm swarm optimization

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 451–460, 2018.
https://doi.org/10.1007/978-3-319-90802-1_40

algorithm is proposed by Ni [3]. Fu presented a method to predict the haze based on multiple linear regression analysis, whose sample is online update [4]. Miao establish the haze prediction model and diffusion model with the six ambient air parameters of Changchun City in 2013 October and November [5]. These parameters are analyzed statistically under the environment of MATLAB and pay close attention to $PM_{2.5}$ values, which is defined as a good reference to evaluate and analysis of the air quality [6]. However, the performance of the model is seriously reduced when historical data is different from the predicted data in variation, which is not suitable for such a sudden and strong situation.

Many researchers in the field of haze weather prediction have been seeking a method of high reliability and accurate prediction results at present, however, the researchers are continuing to improve the performance of existing forecasting methods due to the high nonlinearity and complexity of the prediction. Various methods and models need further verification in practice [7]. Therefore, in this paper, the PCA is used to process the original multi-dimensional data. Then, input the extracted principal components to the BP neural network, which have powerful nonlinear function mapping capabilities. Finally, the neural network are trained through a lot of historical data. Through this way, either the dimensions of input variables can be reduced or correlativity among input variables can be eliminated, thus both convergence and stability of neural network can be improved.

The sections of this paper are arranged as follows:

1. The Sect. 1 introduces the research background and research significance of this paper and summarizes the model of prediction models of haze forecast in recent years.
2. The Sect. 2 introduces the fundamentals and steps of principal component analysis method.
3. The Sect. 3 introduces the fundamentals of BP neural network.
4. The Sect. 4 raised a model of haze forecast based on the combination of principal component analysis with BP neural network, which is used to evaluate the air quality of Tianjin.
5. The Sect. 5 summarizes the contents of the whole paper and look forward to the improvement of this model of haze forecast.

2 Principal Component Analysis

The principal component analysis method (PCA) is a statistical analysis method which transforms many variables into a few integers by linearly changing the factors. It greatly reduces the computational workload in the analysis process and eliminates the correlation between the original factors $x_1,x_2,\ldots,x_p$. Through the PCA, the original factors can be mapped into a set of integrated variables Z_m with less numbers than original predictor.

The steps of principal component analysis are as follows:

1. Data standardization. At first, the original variables were normalized to eliminate its extreme variation and different dimension. Assuming that there are n sets of data, each group of data has p variables which makes up n × p order matrix:

$$X_{n*p} = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1p} \\ x_{21} & x_{22} & & x_{2p} \\ \vdots & \vdots & & \\ x_{n1} & x_{n1} & \cdots & x_{np} \end{bmatrix} \tag{1}$$

Generate the standard matrix Z by formula (2):

$$Z_{ij} = (x_{ij} - \frac{1}{n}\sum_{i=1}^{n} x_{ij}) \Big/ \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_{ij} - \bar{x}_j)^2}, i = 1, 2, \cdots, n; j = 1, 2, \cdots p \tag{2}$$

2. Establish the correlation coefficient matrix:

$$R = Z^T Z \big/ (n-1). \tag{3}$$

solve the eigen equation of the sample correlation matrix $\left|R - \lambda I_p\right| = 0$, we can obtain the eigen value and vector a_i.

3. Calculate principal component contribution rate and determine principal component:

$$\alpha_i = \lambda_i \Big/ \sum_{i=1}^{p} \lambda_i. \tag{4}$$

Principal component contribution rate is used to reflect the amount of information what original variable factor contains. Normally, the 1st, 2nd,…,nth principal components are fetched, which are respectively matched with the eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_m$, whose accumulative contribution rates are up to 85–95%. In other word, the value of m in $F_1, F_2, \ldots, F_m$ is determined by accumulative contribution rate of variance, G(m).

$$G(m) = \sum_{i=1}^{m} \lambda_i \Big/ \sum_{k=1}^{p} \lambda_k. \tag{5}$$

4. Calculate the main composition score:

$$l_{ij} = \lambda_i a_{ij}. \tag{6}$$

$$F_i = a_{1i}x_1 + a_{2i}x_2 + \cdots + a_{pi}x_p, i = 1, 2, \cdots, m. \tag{7}$$

$$PCA = \sum_{i=1}^{m} \alpha_i F_i \Big/ G(m). \tag{8}$$

Comprehensive score *PCA* as input variable of BP neural network is the main basis for judging whether it is haze day.

3 BP Neural Network

The model adopted multilayer perceptron neural network of BP algorithm is called Back Propagation Neural Network, which is consisted of an input layer, single or multiple hidden layers and an output layer. There are two stages for learning process of BP Neural Network. In the first stage, output signals can transmit along the formed network to the output layer via hidden layers, during which the weight value of neurons of hidden layers is constant; the conditions of neurons of each layer can only influenced by the neurons from last layer. In the second stage, the difference between the output value from output layer and the expected value will be regarded as an error signal and transmitted back layer by layer, during which the connection weight value between each layer will be modified, which can ensure the error values drop into the allowed error range. Fig. 1 is BP neural network structure.

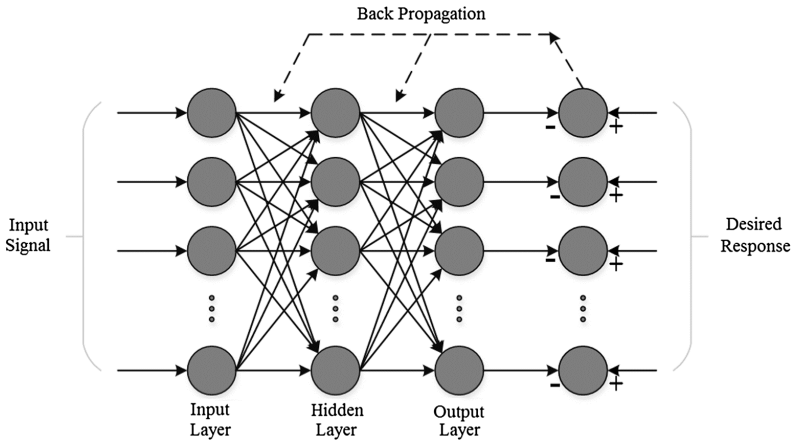


Fig. 1. BP neural network structure.

The output of each layer neuron is shown in formula (9), which show that the mapping between n dimensional space to m dimension space. The connection weight value between each layer: $\omega_{ij}, \theta_j, \omega'_{jk}, \theta'_k, \omega''_{kl}, \theta''_l$.

$$\begin{cases} x'_j = f(\sum_{i=0}^{n-1} \omega_{ij} x_i - \theta_j), j = 0, 1, \cdots, n_1 - 1 \\ x''_k = f(\sum_{j=0}^{n_1-1} \omega'_{jk} x'_j - \theta'_k), k = 0, 1, \cdots, n_2 - 1 \\ y_l = f(\sum_{k=0}^{n_2-1} \omega''_{kl} x''_k - \theta''_k), l = 0, 1, \cdots, m - 1 \end{cases} \tag{9}$$

The steps of BP neural network are as follows:

1. Weight initialization.
2. Enter each learning sample.
3. Calculate the output of each layer: x'_j, x''_k, y_l.
4. Find the back propagation error of each layer and record the values of $x_k^{''(p)}$,$x_j^{'(p)}$ and $x_i^{(p)}$ according to formula (10).

$$\begin{cases} \delta_{ij}^{(p)} = \sum_{k=0}^{n_2} \delta_{jk}^{(p)} \omega'_{jk} x_j^{'(p)} (1 - x_j^{'(p)}), j = 0, 1, \cdots n_1 \\ \delta_{kl}^{(p)} = (d_l^{(p)} - y_1^{(p)}) y_1^{(p)} (1 - y_1^{(p)}), l = 0, 1, \cdots m - 1 \\ \delta_{kl}^{(p)} = \sum_{l=0}^{m-1} \delta_{kl}^{(p)} \omega''_{kl} x_k^{''(p)} (1 - x_k^{''(p)}), k = 0, 1, \cdots n_2 \end{cases} \tag{10}$$

5. Record number of samples that have been learned. If $p < P$, go to step (2) to continue the calculation, if $p = P$, go to step (6).
6. Adjust the weight of each layer according to the weight correction formula.
7. Calculate the new x'_j, x''_k, y_l, and E^T, according to the obtained new weights. If any end conditions satisfied, end the learning process, or else go to step (2) and start a new round of learning. End conditions: $\left| d_l^{(p)} - y_l^{(p)} \right| < \varepsilon$ or $E_T < \varepsilon$.

4 Simulation Analysis

The existing haze forecasting models used to be established by a single factor $PM_{2.5}$ value. This is the main drawback to reduced the prediction accuracy. On the one hand, single factor cannot clearly define the fog and haze weather and it cannot take the complexity of haze components into account.

4.1 Data Source

Daily mean concentrations of 6 kinds of pollutants which affect actually air quality in Tianjin are chosen as predictor in this paper including $PM_{2.5}$, PM_{10}, SO_2, NO_2, O_3 and CO by Tianjin Environmental Protection Bureau in 2016. Part of original monitoring data is shown in Table 1.

Table 1. Original monitoring data in Tianjin (μg/m^3).

Date	AQI	$PM_{2.5}$	PM_{10}	SO_2	CO	NO_2	O_3
1/1	220	172.4	237.4	62.7	1700	78.2	22
1/2	395	336.4	480.5	64.5	3488	138.2	7
1/3	129	97.5	109.7	34.5	1254	52.9	25
1/4	140	106	148	36.3	1533	63.2	43
1/5	53	33.8	62.3	25	875	43.5	44
1/6	74	47.8	84.4	31.5	1071	53.8	55

4.2 Principal Component Extraction

According to the steps of principal component analysis in Sect. 2, the correlation coefficient matrix between each factor which is calculated by formula (3) is shown in Table 2.

Table 2. Correlation coefficient matrix

	$Z_{PM2.5}$	Z_{PM10}	Z_{SO2}	Z_{CO}	Z_{NO2}	Z_{O3}
$Z_{PM2.5}$	1	0.864	0.672	0.746	0.778	−0.011
Z_{PM10}	0.864	1	0.595	0.644	0.695	0.084
Z_{SO2}	0.672	0.595	1	0.784	0.808	−0.325
Z_{CO}	0.746	0.644	0.784	1	0.835	−0.313
Z_{NO2}	0.778	0.695	0.808	0.835	1	−0.181
Z_{O3}	−0.011	0.084	−0.325	−0.313	−0.181	1

Table 2 show that there is the correlation between original indicators. As can be seen from Table 2, according to a single indicator, $PM_{2.5}$ daily average concentration, is unable to accurately determine whether it is haze day.

Table 3. Total variance explained.

Component	Total variance explained		
	Total	Variance %	Contribution rate %
1	4.011	66.846	66.846
2	1.164	19.408	86.254
3	0.346	5.762	92.016
4	0.215	3.58	95.596
5	0.146	2.427	98.024
6	0.119	1.976	100

According to the formula (4) to calculate the correlation coefficient matrix eigenvalues, eigenvectors and cumulative contribution rate in Table 3.

As can be seen from Table 3, the contribution rate of the first two principal components has reached 86.274%, which is more than 80%, which can represent the majority of information of the original data, so it can be determined that the number of principal components is 2. According to formulas (6) and (7), the linear combination between two principal components and each variable can be obtained:

$$\begin{cases} F_1 = 0.23Z_{PM2.5} + 0.21Z_{PM10} + 0.22Z_{SO_2} + 0.23Z_{CO} + 0.23Z_{NO_2} - 0.05Z_{o_3} \\ F_2 = 0.23Z_{PM2.5} + 0.33Z_{PM10} - 0.18Z_{SO_2} - 0.14Z_{CO} - 0.02Z_{NO_2} + 0.81Z_{o_3} \end{cases}. \tag{11}$$

Comprehensive score PCA:

$$PCA = (0.66846F_1 + 0.19408F_2)/0.86254. \tag{12}$$

4.3 Simulation Results

The model 1 used PCA based on the principal component analysis as input of BP neural network to predict the haze weather prediction model. The model 2 was established only by using the daily average concentration of $PM_{2.5}$ in the original sample as the input of the BP neural network is called the traditional prediction method which is widely used in many fields.

BP neural network can fit any nonlinear curve if there are more hidden layers in theory. BP network structure with two hidden layers was adopted in this paper after several contrast experiments in order to improve prediction accuracy. Each hidden layer contains 10 nodes, the first hidden layer neurons use logsig transfer function, the second hidden layer neurons use pure linear function, the training function using trainlm. Training parameters are set as follows: learning rate 0.01, the maximum number of training 5000, the target error 0.00000001, display step 50.

There are 91 sets of effective data, 70 groups as a training neural network, 21 groups as predictive comparison data from January 2016 to March 2016. Table 4 shows the forecast values, measured values and prediction errors of haze weather indicators in the first three days of April though two models. According to the $PM_{2.5}$ standards set by our country, the average daily concentration is more than 35 μg/m^3, which is regarded as the haze weather. While the PCA value is determined to be greater than 0.15 when compared with actual air quality index AQL, it is considered to be the haze weather. For example, the actual calculation of AQL on April 1 was given in Table 4 is 105, which is considered to be lightly haze day, but the $PM_{2.5}$ daily concentration predicted by the traditional prediction method is 34.19 μg/m^3, it is not haze days according to the detection standard. Based on the model 1, the error calculated according to the error formula (13) is 6.25% less than the traditional prediction method of prediction error of 29.93%, so that the forecasting accuracy is improved.

$$Errors = (MeasuredValue - ForecastValue)/MeasuredValue. \tag{13}$$

Table 4. Comparison of network forecast value and measured value.

Date	AQL	Indicator	Measured value	Haze day	Forecast value	Haze day	Errors%
04.01	105	$PM_{2.5}$	48.8 μg/m^3	√	34.19 μg/m3	×	29.93
		PCA	0.16	√	0.17	√	6.25
04.02	51	$PM_{2.5}$	17.4 μg/m^3	×	20.54 μg/m^3	×	18.06
		PCA	−0.56	×	−0.58	×	3.57
04.03	78	$PM_{2.5}$	29.7 μg/m^3	×	15.46 μg/m^3	×	47.94
		PCA	−0.32	×	−0.27	×	15.62

As Table 4 shown, it can be seen that the prediction $PM_{2.5}$ content of traditional forecasting methods has great errors in determining whether it is haze day. But the average prediction error of the prediction model that combination the principal component analysis with BP neural network is less than 10%, and the predicted value is closer to real value. The main reason is that the new synthetic variables are obtained by principal component analysis eliminate the correlation between original predictive factors, reduce influence of redundant information, greatly simplify the neural network structure and improve the prediction accuracy.

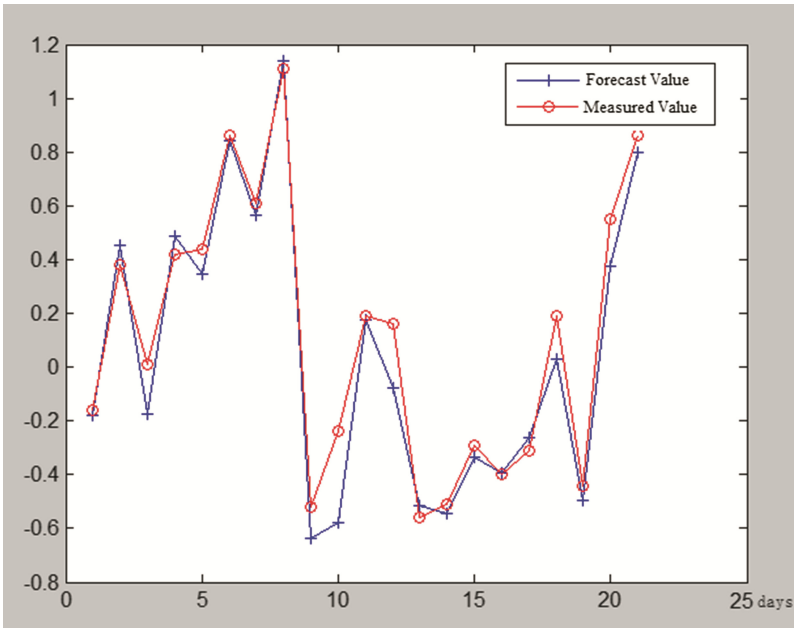


Fig. 2. The curve fitting of the comprehensive variable PCA.

Figures 2, 3 shows the compare results of the predicted value and measured value from 21 days after march 2016. The Y-axis of Fig. 2 is the value of the integrated score of PCA, and the Y-axis of Fig. 3 is the daily average of $PM_{2.5}$ predicted by traditional

prediction method.As shown in Fig. 2, the trend of the predicted and measured values of haze is basically the same. Although there is same error between the predictive value and the true value of the comprehensive variable, but the overall curve fit is higher when the data changes dramatically, the prediction curve can respond quickly to changes in the real curve. Figure 3 is a traditional prediction method for single haze factor $PM_{2.5}$ forecast. Contrast Figs. 2 and 3, there are much more error in the traditional prediction results. Actually, the number of iterations of the traditional prediction method reaches the maximum value after many training and contrast. Indicating that the learning accuracy can not meet the requirements.

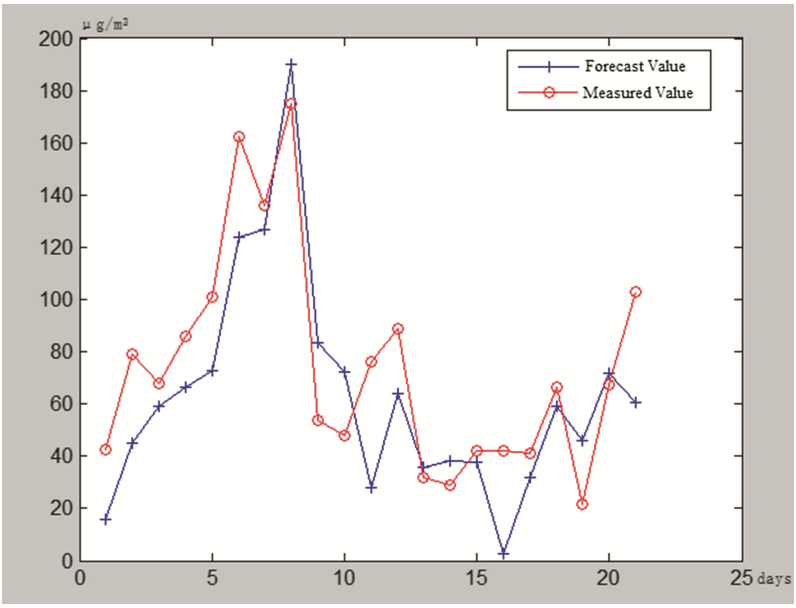


Fig. 3. The curve fitting of traditional forecasting

5 Conclusion

A haze forecast model based on the combination of PCA and the BP neural network is proposed in this paper. Principal components analysis is used to decreases the dimensions of the six predictive factors. Then, the comprehensive variables are taken as input variable for back-propagation neural network, which eliminates the correlation among the original predictors and simplifies the structure of neural network, Results show that complexity of training and training time is reduced and the prediction accuracy had improved, prediction of the fitting curve is much closer to the true value. Although the BP neural network is widely used, it still has some shortcomings, such as the convergence rate is slow, easy to fall into the local minimum etc., in the future, BP neural network can be further optimized to build a more completed prediction model.

Acknowledgments. This research was supported by the Fundamental Research Funds for the Universities in Tianjin (2016CJ11), Projects of the national "863Program" (NO. 2015BAF09B02-3).

References

1. Hou, Q., Yang, H.: Analysis and forecasting of haze weather based on the cubic exponential smoothing model. J. Environ. Prot. Sci. **38**, 73–77 (2014)
2. AI, H., Ying, S.: Study on prediction of haze based on BP neural network. J. Comput. Simul. **32**, 402–405 (2015)
3. Ni, Z., Zhang, C., Ni, L.: Haze forecast method of selective ensemble based on glowworm swarm optimization algorithm. J. PR AI **29**, 143–153 (2016)
4. Fu, Q.: Research on Haze prediction based on multivariate regression. J. Comput. Sci. **43**, 526–528 (2016)
5. Miao, Y.N.: Research on Haze ARIMA-GM Forecast and Diffusion Model Based on the Kalman Filtering (2016)
6. Li, L., Sun, Y.: Haze environment analysis and research based on equalization of PCA. J. Appl. Res. Comput. **42**, 1373–1375 (2015)
7. AI, H., Pan, H., Li, Y.: Research on optimization of PM2.5 content prediction in air haze. J. Comput. Simul. **34**, 392–395 (2017)

Stabilization Control Design for Network Switched System with Communication Constrains

Yi Liu[1], Yuheng Pan[1(✉)], Weijia Lu[1], and Zhiyan Xue[2]

[1] School of Computer and Information Engineering, Tianjin Chengjian University, Tianjin 300384, China
yuheng0616@sina.com
[2] School of Electronic Information Engineering, Suzhou Vocational University, Suzhou 215006, Jiangsu, China

Abstract. Switching laws based on average dwell time method and switched state feedback controller are designed for a network switched control system with communication constrains. The networked control system is modeled as a discrete-time switched system with time delay and parametric uncertainties. If feedback control access rate is higher than the stability condition, then the designed scheduling strategy can guarantee every subsystem reaches exponential stability. Sufficient condition for exponentially stability is also presented, and the result shows systems can be stabilized under the designed switch laws. Finally, the effectiveness of the proposed approaches is demonstrated through MATLAB simulation.

Keywords: Communication constrains · Average dwell time
Exponential stability · Network control

1 Introduction

The network control system (NCS) is a closed-loop control system composed of controller, actuator and communication network, which applies network communication to the decentralized control system and achieve resource sharing and remote operation. Therefore it can meet requirement of large-scale and complicated systems. Therefore this control method has a promising future and will be an important tendency for the control systems [1]. However for practical systems, controllers cannot manage the whole objects all along due to the constraint of the equipment and resources. So in the limited communication network partial subsystems remain open-loop condition at the same time. This question can be described as the medium communication constrains (MCC) [2–6].

To achieve stable control, an appropriate switched strategy is designed for the switched system, so NCS can be analyzed using switched method [7–11]. The average dwell time is one of the most effective methods, therefore a new dynamic scheduling strategy and feedback control designing method based on mode-dependent average dwell time is proposed in the literature [12]. The system is modeled as a discrete

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 461–470, 2018.
https://doi.org/10.1007/978-3-319-90802-1_41

switched system with uncertain parameters. This method not only considers the influence caused by random short time delay but also presents the average dwell time conditions of all the subsystems. The existing research about the network control of MCC is focused on constrains of media access, digit ratio and information ratio. In the literature [13], the NCS with fixed time delay is modeled as discrete switched system with uncertain parameters and under quantizers are modeled as multiple modals the MEF-TOD (Maximum Error First-Try Once Discard) dispatch strategy. And then according to Lyapunov theory the digit ratio conditions that enable quantization errors convergent can be verified. Aiming at the random-delay NCS with MCC, a design method based on the TOD dynamic dispatch strategy and state feedback controller is presented in the literature [14]. While the literature [15] presents a technique using TOD dynamic dispatch strategy and H∞ quantization control, which manages errors using sector bound approach and models the close-loop NCS as discrete switched system with uncertain parameters. The uncertain network-induced time delay is modeled as polytope-type uncertainty in the literature [16]. In this system the robust control method based on the parameter-correlated Lyapunov stability is used to design network discrete controller and simultaneously adopt control and dispatch to ensure the stability of every subsystem in NCS. For the NCS with delay and parameter uncertainty under the MCC few scholar researches non-linear network switch system using average swell time switch law.

This paper researches the stability of NCS with communication constrains utilizing average swell time method. The state feedback controller and the average swell time condition, which assures the system exponential stable, are presented in the form of linear matrix inequation using Lyapunov function. Finally, the effectiveness of the proposed approaches is demonstrated through MATLAB simulation.

2 Problem Statement

If the state equation of NCS is of the form

$$x(t) = A_p x(t) + B_p u(t) \tag{1}$$

where, $x(t) \in R^n$, $u(t) \in R^m$ are respectively the state variable and the input of the controlled object. A_p and B_p are the optimal dimensional matrixes.

The structure diagram of NCS is shown in Fig. 1. The controlled object is composed of umpty sensors and actuators. The network-induced time delay between sensors and controllers is τ_k^{sc} while the one between actuators and controllers is τ_k^{ca}. Suppose the system satisfies with the following terms.

Hypothesis 1: Sensors are time-driven and the sampling period is h, controllers and actuators are both event-driven.

Hypothesis 2: $\tau_k = \tau_k^{sc} + \tau_k^{ca}$ is time-varying and $0 < \tau_k < h$.

Hypothesis 3: All signals from sensors or controllers cannot be transferred simultaneously because of the restrictions of network bandwidth. The transferred

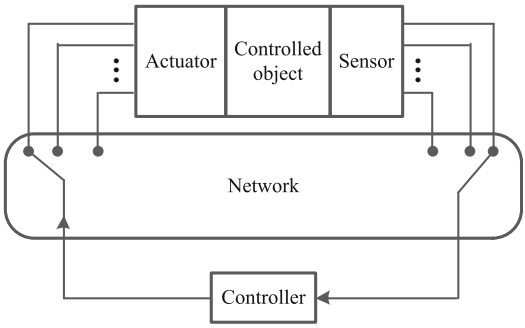


Fig. 1. The structure diagram of NCS

numbers of state vector and control signal every time are $d_s(0<d_s\leq n)$ and $d_c(0<d_c\leq m)$ respectively.

Discrete the state equation of the controlled objects

$$x(k+1)=Ax(k)+B_0(\tau_k)\hat{u}(k)+B_1(\tau_k)\hat{u}(k-1) \tag{2}$$

where, $A=e^{A_p h}$, $B_0(\tau_k)=\int_0^{h-\tau_k} e^{A_p t}Bdt$

Because of network restrain in the hypothesis 3, the scheduling network nodes are required in every transmission. Introduce the sensor-control scheduling vectors $\theta(k)$ and the control-actuator ones $\delta(k)$ and then

$$\theta_i(k)=\begin{cases}1, & \textit{if } x_i(k) \textit{ is transmitted}\\ 0, & \textit{otherwise}\end{cases} \qquad i\in(1,2,\ldots,n) \tag{3}$$

$$\delta_i(k)=\begin{cases}1, & \textit{if } u_i(k) \textit{ is transmitted}\\ 0, & \textit{otherwise}\end{cases} \qquad i\in(1,2,\ldots,m) \tag{4}$$

During the kth sampling period, the sensors and control nodes allowed to transmit are respectively determined by the scheduling vector $\theta(k)=[\theta_1(k),\theta_2(k),\ldots,\theta_n(k)]$ and $\delta(k)=[\delta_1(k),\delta_2(k),\ldots,\delta_m(k)]$.

Define $\Lambda(k)=diag(\theta(k))$, and then the effective updated data received by the control nodes are $\Lambda(k)x(k)$, while the data that are not updated hold the last value through the zero-order holder (ZOH). So the input of the controller is as follows

$$\hat{x}(k)=\Lambda(k)x(k)+(\mathrm{I}-\Lambda(k))\hat{x}(k-1) \tag{5}$$

Similarly, define $\Pi(k)=diag(\delta(k))$ and then the output is

$$\hat{u}(k)=\Pi(k)u(k)+(\mathrm{I}-\Pi(k))\hat{u}(k-1) \tag{6}$$

The total numbers of sensors and actuators are n and m respectively in this NCS, but only d_s sensors and d_c actuators are allowed to transmit data. Take each scheme as a modality, and the system provides N types of modality.

Where, $N = [n!/(n-d_s)!] \times [m!/(m-d_c)!]$

Each modality corresponds to a group of $\Lambda_i(k)$ and $\Pi_i(k)$, $(i = 1, 2, \ldots, N)$. So the generalized discrete modal of NCS is as follows

$$\begin{cases} x(k+1) = Ax(k) + B_0(\tau_k)\hat{u}(k) + B_1(\tau_k)\hat{u}(k-1) \\ \hat{x}(k) = \Lambda_i(k)x(k) + (\mathrm{I} - \Lambda_i(k))\hat{x}(k-1) \\ \hat{u}(k) = \Pi_i(k)u(k) + (\mathrm{I} - \Pi_i(k))\hat{u}(k-1) \end{cases} \tag{7}$$

The system includes N types of modality, i.e. N subsystems, which are switched using TOD strategy.

Define $s_i(k) = [\theta_i(k), \delta_i(k)]$ and $s_i(k) \in \{0,1\}^{n+m}$, $i = 1, 2, \ldots, N$, $s_i(k)$ indicates ith modality of the system during kth sapling period.

Let $\Gamma_i = diag(s_i(k))$, i.e. $\Gamma_i = diag(s_i(k))$, then the errors are as follows

$$e(k) = \begin{bmatrix} e^x(k) \\ e^u(k) \end{bmatrix} = \begin{bmatrix} x(k) - \hat{x}(k-1) \\ u(k) - \hat{u}(k-1) \end{bmatrix} \tag{8}$$

According to TOD dynamic scheduling algorithm, the switch function is $\sigma = \arg max\{\Gamma_1(k)e(k), \Gamma_2(k)e(k), \ldots, \Gamma_N(k)e(k)\}$, $\sigma \in \{1, 2, \ldots, N\}$ where arg is subscript function, $\Gamma_i(k)(i = 1, 2, \ldots, N)$ corresponds the ith modality.

The form of the designed discrete state feedback controller is

$$u(k) = K_\sigma \hat{x}(k) \tag{9}$$

where, $\hat{x}(k) \in R^n$, $u(k) \in R^m$ are respectively the input and output of the controller. K_σ is the state feedback gain after introducing TOD scheduling strategy.

From hypothesis 2, $\tau_k \in [0, h]$ varies randomly. $B_0(\tau_k)$ and $B_1(\tau_k)$ are also time varying, then

$$\begin{aligned} B_0(\tau_k) &= B_0 + DF(\tau_k')E \\ B_1(\tau_k) &= B_1 - DF(\tau_k')E \end{aligned} \tag{10}$$

where, $\tau_k' \in [-h/2, h/2]$.

Suppose $\bar{F}(\tau_k') = \int_0^{-\tau_k'} e^{A_p t}dt$, $\beta = max \int_0^{-\tau_k'} e^{A_p t}dt = \int_{h/2}^{h} e^{A_p t}dt$ then $B_0 = \int_0^{h/2} e^{A_p t}B_p dt$, $B_1 = \int_{h/2}^{h} e^{A_p t}B_p dt$, $D = \beta e^{A_p(h/2)}$, $E = B_p$ are both constant matrixes, $F(\tau_k') = \beta^{-1}\bar{F}(\tau_k')$ changes with τ_k, and $F^T(\tau_k')F(\tau_k') \le I$.

Let $z(k) = [x^T(k)\hat{x}^T(k-1)\hat{u}^T(k-1)]$, then the equation of the close-loop control is as follows

$$z(k+1) = \Phi_\sigma z(k) \quad \sigma \in \{1, 2, \ldots, N\} \tag{11}$$

where

$$\Phi_\sigma = \begin{bmatrix} a_1 & b_1 & c_1 \\ \Lambda_\sigma & I-\Lambda_\sigma & 0 \\ \Pi_\sigma K_\sigma \Lambda_\sigma & \Pi_\sigma K_\sigma (I-\Lambda_\sigma) & I-\Pi_\sigma \end{bmatrix}$$
$$= \mathrm{G}_\sigma + H\Pi_\sigma K_\sigma \Lambda_\sigma + D_0 F\left(\tau_k'\right) E\Pi_\sigma (K_\sigma \Lambda_\sigma - I)$$

$$a_1 = A + B_0(\tau_k)\Pi_\sigma K_\sigma \Lambda_\sigma$$

$$b_1 = B_0(\tau_k)\Pi_\sigma K_\sigma (I-\Lambda_\sigma)$$

$$c_1 = B_0(\tau_k)(I-\Pi_\sigma) + B_1(\tau_k)$$

$$G_\sigma = \begin{bmatrix} A & 0 & B_0(I-\Pi_\sigma)+B_1 \\ \Lambda_\sigma & I-\Lambda_\sigma & 0 \\ 0 & 0 & I-\Pi_\sigma \end{bmatrix}$$

$$H = \begin{bmatrix} B_0 \\ 0 \\ I \end{bmatrix},\ D_0 = \begin{bmatrix} D \\ 0 \\ 0 \end{bmatrix},\ \Lambda_\sigma = \begin{bmatrix} \Lambda_\sigma \\ I-\Lambda_\sigma \\ 0 \end{bmatrix}^T,\ \bar{I} = \begin{bmatrix} 0 \\ 0 \\ I \end{bmatrix}^T \quad \sigma \in \{1,2,\ldots,N\}$$

Definition 1 [17]**.** In any time $t_2 > t_1 \geq 0$, $N_r(t_1,t_2)$ means the switch times during $[t_1,t_2]$. If there is $T_\alpha > 0$, $N_0 \geq 0$, which can satisfy the following inequality

$$N_r(t_1,t_2) \leq N_0 + \frac{t_2-t_1}{\mathrm{T}_\alpha} \tag{12}$$

T_α is average swell time, N_0 is buffering boundary.

Lemma 1 [18]**.** H, E and I are the optimal dimensional matrixes and Q is symmetric matrix. For all the matrixes satisfy with $F_{ri}(k)^{\mathrm{T}} F_{ri}(k) \leq I$, when $\varepsilon \geq 0$, $Q + \varepsilon^2 HH^T + \varepsilon^{-2} E^T E \leq 0$, then $Q + HF_{ri}(k)E + E^T F_{ri}(k)^T H^T \leq 0$.

3 Main Results

Theorem 1. The positive definite matrix P and constant $\lambda \in (0,1)$ satisfies the matrix inequality

$$\begin{bmatrix} -P^{-1} + \varepsilon_\sigma D_0 D_0^T & * & * \\ \mathrm{G}_\sigma P^{-1} + H\Pi_\sigma K_\sigma \Lambda_\sigma P^{-1} & -(1-\lambda)P & * \\ 0 & E\Pi_\sigma (K_\sigma \Lambda_\sigma - I)P^{-1} & -\varepsilon_\sigma I \end{bmatrix} < 0 \tag{13}$$

If the visiting rate and frequency are

$$\frac{\alpha_c(k)}{k} \geq \frac{\ln \lambda_o - \ln \lambda^*}{\ln \lambda_o - \lambda_c} \tag{14}$$

$$\begin{aligned} &N(k) \leq N_0 + k/\mathrm{T}_\alpha,\ N_0 = \frac{\ln c}{\ln \mu}, \\ &\mathrm{T}_\alpha > \mathrm{T}_\alpha^* = \frac{\ln \mu}{2\ln \rho - \ln \lambda^*} \end{aligned} \tag{15}$$

then there are feedback controllers (13) to make the system expressed by Eq. (1) stable, and the estimated state of the system is $\|x(k)\| \leq \sqrt{\frac{bc}{a}}\rho^k \|x(0)\|$. Where, * represents the transposition of the symmetric position, $0 < \lambda_c < 1$, $\lambda_o > 1$ are the feedback coefficients of close-loop and open-loop respectively, T_α is the average swell time. $\lambda_c < \lambda^* < \rho^2 < 1$, $c > 0$ and $V_c(k) \leq \mu V_o(k)$, $V_o(k) \leq \mu V_c(k)$.

Proof. The piecewise quadratic Lyapunov-like function is as follows

$$V(k) = \begin{cases} V_c(k), & close - loop \\ V_o(k), & open - loop \end{cases} \tag{16}$$

If $V_c(k) = z^T(k)Pz(k)$, then

$$\begin{aligned} &\Delta V_c(k) + \lambda_c V_c(k) \\ &= z^T(k+1)Pz(k+1) - z^T(k)Pz(k) + \lambda_c V_c(k) \\ &= z^T(k)\Phi_\sigma^T P \Phi_\sigma z(k) - z^T(k)Pz(k) + \lambda_c V_c(k) \\ &= z^T(k)\left(\Phi_\sigma^T P \Phi_\sigma - P + \lambda_c P\right)z(k) \\ &= z^T(k)\begin{bmatrix} -P^{-1} & \Phi_\sigma \\ \Phi_\sigma^T & -(1-\lambda_c)P \end{bmatrix} z(k) \end{aligned}$$

According to Schur complement lemma and the above equations, $\Delta V_c(k) + \lambda_c V_c(k) < 0$. Similarly, the above conclusion is tenable for the open-loop system. So

$$\begin{aligned} V_c(k+1) &\leq \lambda_c V_c(k) \\ V_o(k+1) &\leq \lambda_o V_o(k) \end{aligned} \tag{17}$$

Suppose during the time interval $[k_{2j}, k_{2j+1})$, $j = 0, 1, 2, \ldots$, the system control channel is close-loop, while during the time interval $[k_{2j+1}, k_{2j+2})$, $j = 0, 1, 2, \ldots$ it is open-loop. For any $k > 0$, according to the Eq. (17),

$$V(k) \leq \begin{cases} \lambda_c^{k-k_{2j}} V_c(k_{2j}), & k_{2j} \leq k < k_{2j+1} \\ \lambda_o^{k-k_{2j+1}} V_o(k_{2j+1}), & k_{2j+1} \leq k < k_{2j+2} \end{cases} \tag{18}$$

So when $k \in \left[k_{2j+1}, k_{2j+2}\right)$, according to the Eq. (18) and definition

$$\begin{aligned} V(k) &\le \lambda_o^{k-k_{2j+1}} V_o\left(k_{2j+1}\right) \\ &\le \mu \lambda_o^{k-k_{2j+1}} V_o\left(k_{2j+1}\right) \\ &\le \mu \lambda_o^{k-k_{2j+1}} \lambda_c^{k_{2j+1}-k_{2j}} V_o\left(k_{2j+1}\right) \\ &\le \cdots \\ &\le \mu^{N(k)} \lambda_c^{\alpha_c(k)} \lambda_o^{k-\alpha_c(k)} V(0) \end{aligned}$$

Similarly when $k \in \left[k_{2j}, k_{2j+1}\right)$,

$$V(k) \le \mu^{N(k)} \lambda_c^{\alpha_c(k)} \lambda_o^{k-\alpha_c(k)} V(0) \tag{19}$$

According to the Eq. (19),

$$(\ln \lambda_0 - \ln \lambda_c)\alpha_c(k) \ge (\ln \lambda_0 - \ln \lambda^*)k$$

Namely

$$\lambda_c^{\alpha_c(k)} \lambda_0^{k-\alpha_c(k)} \le (\lambda^*)^k \tag{20}$$

According to the Eq. (20),

$$\mu^{N(k)} \le \mu^{N_0 + \frac{k}{T_\alpha}} \le \mu^{N_0} \mu^{\frac{k(2\ln\rho - \ln\lambda^*)}{\ln\mu}} = c\left(\frac{\rho^2}{\lambda^*}\right)^k$$

From Eqs. (16), (19) and (20) $V(k) \le c\rho^{2k} V(0)$

Because of quadratic form Lyapunov-like function, then the constants $a_c > 0, a_0 > 0, b_c > 0, b_0 > 0$ make the following inequation established.

$$\begin{aligned} &a_c x(k)^2 \le V_c(k),\ a_o x(k)^2 \le V_o(k) \\ &V_c(0) \le b_c x(0)^2,\ V_o(0) \le b_o x(0)^2 \end{aligned} \tag{21}$$

Then

$$a x(k)^2 \le V(k),\ V(0) \le b x(0)^2 \tag{22}$$

where $a = \min\{a_c, a_o\}$, $b = \min\{b_c, b_o\}$.

Finally, according to Eqs. (21) and (22),

$$x(k) \le \sqrt{\frac{bc}{a}} \rho^k x(0)$$

Due to the uncertain item in Φ_σ, transform $\begin{bmatrix} -P^{-1} & \Phi_\sigma \\ \Phi_\sigma^T & -(1-\lambda)P \end{bmatrix}$ into

$$\begin{bmatrix} -P^{-1} & \Phi_\sigma \\ \Phi_\sigma^T & -(1-\lambda)P \end{bmatrix} = \begin{bmatrix} -P^{-1} & \mathrm{G}_\sigma + H\Pi_\sigma K_\sigma \Lambda_\sigma \\ * & -(1-\lambda)P \end{bmatrix} + \begin{bmatrix} D_0 \\ 0 \end{bmatrix} F(\tau_k') \begin{bmatrix} 0 \\ E\Pi_\sigma(K_\sigma\Lambda_\sigma - I) \end{bmatrix}^T + \begin{bmatrix} 0 \\ E\Pi_\sigma(K_\sigma\Lambda_\sigma - I) \end{bmatrix} F^T(\tau_k') \begin{bmatrix} D_0 \\ 0 \end{bmatrix}^T$$

According to the lemma, further transform the above equation into

$$\begin{bmatrix} -P^{-1} & \mathrm{G}_\sigma + H\Pi_\sigma K_\sigma \Lambda_\sigma \\ * & -(1-\lambda)P \end{bmatrix} + \varepsilon_\sigma \begin{bmatrix} D_0 \\ 0 \end{bmatrix} \begin{bmatrix} D_0 \\ 0 \end{bmatrix}^T + \varepsilon_\sigma^{-1} \begin{bmatrix} 0 \\ E\Pi_\sigma(K_\sigma\Lambda_\sigma - I) \end{bmatrix} \begin{bmatrix} 0 \\ E\Pi_\sigma(K_\sigma\Lambda_\sigma - I) \end{bmatrix}^T + \begin{bmatrix} -P^{-1} + \varepsilon_\sigma D_0 D_0^T & * & * \\ \mathrm{G}_\sigma + H\Pi_\sigma K_\sigma \Lambda_\sigma & -(1-\lambda)P & * \\ 0 & E\Pi_\sigma(K_\sigma\Lambda_\sigma - I) & -\varepsilon_\sigma I \end{bmatrix}$$

Let $X = P^{-1}$, multiply it by $diag(I, X, I)$ in both left and right sides, the above equation can be changed into the equation in the theorem. So the system can be exponent stability.

4 Simulation Example

Consider the equation of NCSs $x(t) = A_p x(t) + B_p u(t)$, where $\mathrm{A_p} = \begin{bmatrix} -0.8 & -0.01 \\ 1 & 0.1 \end{bmatrix}$, $\mathrm{B_p} = \begin{bmatrix} 0.4 \\ 0.1 \end{bmatrix}$

And in the Eq. (2),

$A = \begin{bmatrix} 0.852 & -0.0019 \\ 0.1867 & 1.02 \end{bmatrix}$, $B_0 = \begin{bmatrix} 0.0384 \\ 0.0032 \end{bmatrix}$, $B_1 = \begin{bmatrix} 0.0355 \\ 0.0055 \end{bmatrix}$, $D = \begin{bmatrix} 0.0355 & 0 \\ 0.0037 & 0.0389 \end{bmatrix}$, $E = \begin{bmatrix} 0.4 \\ 0.1 \end{bmatrix}$

The system includes one control input and two states. When $d_s = d_c = 1$, the system have two types of modals, i.e. $s_1 = [1 \quad 0 \quad 1]$ and $s_2 = [0 \quad 1 \quad 1]$. Use Matlab the LMI (Linear Matrix Inequality) in theorem can be solved.

$$K_1 = [-1.1065 \quad 0.11577]$$
$$\mathrm{K_2} = [-0.0169 \quad -1.3888]$$

Suppose that the time delay is the random number within (0, 0.1) and the original state is $[0.3, -0.3]^{\mathrm{T}}$. The state response curve of the above network switch control system is shown in Fig. 2.

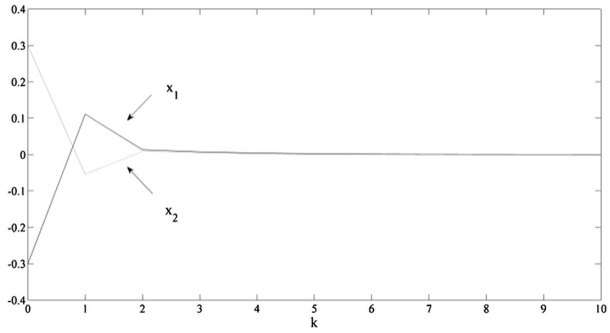


Fig. 2. Response of state curve

As shown in the Fig. 2, the system can be stable with the designed controller and switch laws.

5 Conclusions

In conclusion, the stability control of network switch system with MCC is researched. The switch laws are designed using the average dwell time method and the conditions to ensure the system exponential stability. The results show the system can be stable if the visiting rate of a feedback control system is greater than a value.

References

1. Wen, D.L., Wand, K.S., Chen, Z.X.: Dynamic quantization H∞ control for networked control systems. Control Eng. China **20**(5), 960–965 (2013)
2. Xu, Y., Su, H.Y., Pan, Y.J.: Stability analysis of networked control systems with round-robin scheduling and packet dropouts. J. Frankl. Inst. **350**(8), 2013–2027 (2013)
3. Xie, C.X., Hu, W.L.: Analysis and design of a class of networked-control systems with long time-delay and data-packet-dropout. Control Theory Appl. **27**(9), 1207–1213 (2010)
4. Dong, Y., James, L.: Non-fragile guaranteed cost control for uncertain descriptor systems with time-varying state and input delays. Opt. Control Appl. Methods **26**(2), 85–105 (2005)
5. Zhang, H., Wu, Z.J., Xia, Y.Q.: Exponential stability of stochastic systems with hysteresis switching. Automatica **50**(2), 599–606 (2014)
6. Zhai, S.D., Yang, X.S.: Exponential stability of time-delay feedback switched systems in the presence of asynchronous switching. J. Frankl. Inst. **350**(1), 34–49 (2013)

7. Wang, M., Fan, Y.G., Qiu, J.B.: Static output feedback control of saturated uncertain discrete-time switched systems with average dwell-time. Control Decis. **25**(10), 1479–1483 (2010)
8. Zhao, X.D., Yu, Q., Zhang, J.F., et al.: A novel approach to stability analysis for switched positive linear systems. J. Frankl. Inst. **351**(7), 3883–3898 (2014)
9. He, T., Zhang, X.M., Zhou, R.J.: Fuzzy control for networked systems via average dwell-time method. Chin. J. Eng. Math. **30**(2), 184–196 (2013)
10. Fu, J., Ma, R.C., Chai, T.Y.: Global finite-time stabilization of a class of switched nonlinear systems with the powers of positive odd rational numbers. Automatica **54**(4), 360–373 (2015)
11. Lu, Q.G., Zhang, L.X., Karimi, H.R., et al.: H∞ control for asynchronously switched linear parameter-varying systems with mode-dependent average dwell time. IET Control Theory Appl. **7**(5), 673–683 (2013)
12. Zhu, X.C., Zhou, C., Chen, Q.W.: Model-based average dwell time scheduling and control for networked control system. Control Theory Appl. **32**(1), 86–92 (2015)
13. Ren J., Zhou C.: Simulations design of dynamic scheduling and quantized control for networked control system with communication constraints. 31st Chinese Process Control Conference **03**, 20–25 (2013)
14. Du, M.L., Zhou, C., Chen, Q.W., Ren, J.: Coordinate design of dynamic scheduling and H-infinity control for networked control systems with communication constraints. Control Theory Appl. **29**(9), 1132–1138 (2012)
15. Yu, C., Zhou, C., Chen, Q.W.: Dynamic scheduling and H∞ quantized feedback stabilization for networked control systems with communication constraints. Journal of Central South University **44**(1), 103–108 (2013)
16. Dai, S.L., Lin, H., Ge, S.S.: A switched system approach to scheduling of networked control systems with communication constraints. In: Proceedings of the Joint 48th IEEE Conference on Decision and Control and 28th Chinese Control Conference, Shanghai, China, pp. 4991–4996 (2009)
17. Lin, J.X., Fei, S.M.: Robust exponential admissibility of uncertain switched singular time-delay systems. Acta Autom. Sin. **36**(12), 1773–1779 (2010)
18. Tong, S.C., Tang, J.T., Wang, T.: Fuzzy adaptive control for multivariable nonlinear systems. Fuzzy Sets Syst. **111**(2), 153–167 (2000)

Fuzzy Logic Load-Balancing Strategy Based on Software-Defined Networking

Guoyan Li(✉), Tianying Gao, Zhigang Zhang, and Yadong Chen

School of Computer and Information Engineering, Tianjin Chengjian University, Tianjin 300384, China
{ligy,gty,zzg,cyd}@tcu.edu.cn

Abstract. Traditional load balancing hardware is expensive and lacks scalability and flexibility. We propose a load balancing strategy based on fuzzy logic (LBSFL), which exploits the control and forwarding separation architecture characteristics of software-defined networking (SDN). First, the fuzzy membership function that affects the performance parameters of the server load is analyzed. Based on this, the load state of the virtual server is evaluated through fuzzy logic. Then the centralized control capability of SDN's controllers for the whole network is utilized to monitor virtual server information in real time and to schedule virtual server tasks. Individual servers can be hibernated or restarted, to save power or to increase performance as necessary. Finally, the dynamic balance between the overall load, performance and energy consumption is realized. Simulation experiments showed that the proposed strategy improves overall performance of the network, especially when dealing with communication-intensive tasks and using a high-latency network.

Keywords: SDN · OpenFlow protocol · Load balancing · Fuzzy logic

1 Introduction

In recent years, with the development of internet, e-commerce and big data technology, the scale, flow and user base of the internet has exploded. To meet the needs of network users, many internet service providers use load-balancing technology to provide high-quality and reliable service through the rational use of resources. However, traditional load-balancing devices are expensive and lack adequate scalability and flexibility.

Software-defined networking (SDN) is a clean slate project by a Stanford University study group [1] that proposes a new network architecture paradigm. Its core technology is the OpenFlow network protocol, which creates an interface between the device control plane and the data plane [2–7]. The resulting platform provides flexible network traffic control, innovation and application of the core network. In an SDN network, each switch has a flow meter, which is primarily a collection of process data streams for all actions, such as looking up and forward. The main flow table contains headers, counters and actions, three fields in which the actions field is represented, forwarding rules, and flow meters, which are updated intermittently. Because the SDN controller determines the

C. Li and S. Mao (Eds.): WiCON 2017, LNICST 230, pp. 471–482, 2018.
https://doi.org/10.1007/978-3-319-90802-1_42

traffic forwarding rules, the load balancing algorithm is in the controller, meaning that load balancing takes place at each link.

Several scholars have studied load balancing technologies based on SDN. In [8], the authors proposed an SDN-based publish/subscribe system that constructed and fine-tuned topic-connected overlays to disseminate events efficiently and non- redundantly, based on a global topology overview. Handigol [9] proposed a web traffic model founded on SDN. Based on the Openflow environment, Kaur [10] achieved network load balancing using a polling algorithm. Similarly, Zhang [11] determined the minimum number of network connections using a load balancing polling algorithm under an SDN framework. However, although [10, 11] applied traditional load balancing algorithms to the SDN architecture, they could not effectively reduce the server response time.

Shang [12] overcame this response time drawback by incorporating a middlebox, based on SDN architecture, to achieve load balancing by collecting server information. While this scheme effectively reduced server response time, it increased the complexity of the server architecture. In [6], a load balancing algorithm was proposed, based on server response times by using the advantage of SDN flexibility. Its lack of reliability depended on only server response times.

Fuzzy logic, where fuzzy sets are expressed with mathematical formulas, can solve many complicated problems which are not accurately represented by mathematical models [13]. In this task-scheduling model of SDN, the load status of each node is nonlinear and unpredictable. Given the technical limitations associated with collecting node information, extra time is required to obtain and report information. The information stored in this middleware can represent only past node load information, rather than the current load situation, because the system has an inherent delay. Considering the accuracy of the virtual server, the load state of the node is evaluated and the estimated quantity is more effectively expressed in fuzzy terms.

In the present paper, we propose a load balancing strategy based on fuzzy logic (LBSFL). Initially, we analyze the correlation among several parameters that impact load balancing and obtain the load of multiple virtual servers through a fuzzy logic algorithm. We then examine the virtual servers' load status in real time, select the lightest virtual server to handle the request, and, if necessary, set the sleep/restart policy of server. Finally, to verify the correctness and effectiveness of this load balancing algorithm, we constructed an SDN simulation platform. The experimental results show that the proposed strategy is stable and highly effective, resulting in faster and more consistent system response times.

2 System Architecture

The controller, or network operating system, is the heart of an SDN and is responsible for controlling and managing all of the OpenFlow switches [14–16]. We deployed the OpenDayLight SDN controller in our scheme. With the control plane and the data plane being separated in the OpenFlow environment, software configurations are customized through the controller to achieve effective load balancing. OpenFlow switches provide a unified interface and data forwarding function to the controller, so the controller unifies

control of the flow table of OpenFlow. The controller periodically obtains the running state of the virtual server and utilizes the load balancing algorithm to calculate the desired state of the server. To improve overall system performance, the load balancing algorithm migrates tasks from overloaded virtual servers to lightly-loaded virtual servers. If necessary, this strategy sleeps or restarts the virtual server to achieve load balance. We show the proposed system architecture in Fig. 1.

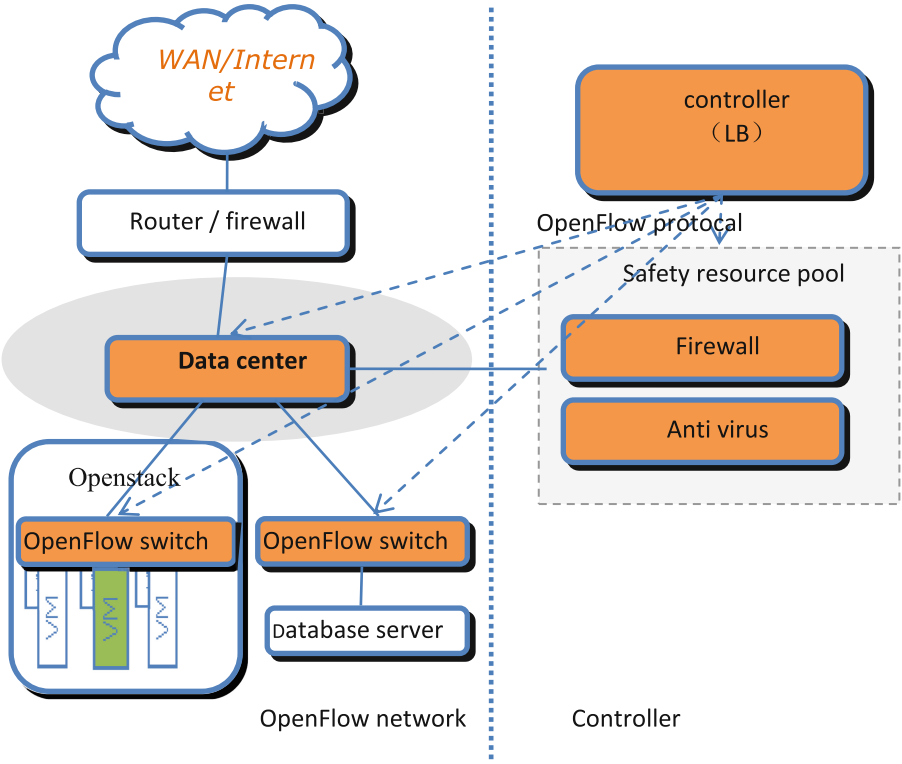


Fig. 1. System architecture

3 Load Balancing Algorithm Based on Fuzzy Logic

The current load condition of the virtual server can be calculated by using parameters such as CPU utilization and IO utilization. However, the load represented by these parameters is a fuzzy concept, meaning that there are no accurate mathematical models or control rules. When monitoring load condition, we considered the advantage of describing emergent problems and uncertainty problems in fuzzy mathematics, and introduced fuzzy-logic theory to solve load balance problems. The fuzzy logic system can be divided into three parts: fuzziness, fuzzy reasoning and solution.

3.1 Fuzziness

Fuzziness scale-transforms the input values to scope of the domain expressed by the fuzzy set. In addition, it determines the corresponding fuzzy rank sequence for each type of input value, e.g. {high, mid, low}, and determines a membership degree between the input parameters and fuzzy grade. Therefore, we need to select the membership function to map the membership relation between the variables and the sequence.

Many factors can be used to characterize the load condition of the server in the virtual server cluster environment, such as the frequency and utilization of the CPU, size and utilization of memory, response times of each server and the number of the current implementation of the process. The network request call and the returned result must be transmitted through the network, taking additional time, CPU and memory resources to complete. Thus, CPU utilization, memory utilization and I/O utilization are chosen as the load parameters for performance evaluation of server nodes. OpenFlow switches regularly submit virtual server load status to the controller. Load index value based on a given threshold is classified into three categories and allocated a value between 0 and 1. Three fuzzy sets are used to describe the load index value, and the fuzzy membership functions for each parameter are defined below in the following sections.

3.1.1 CPU Utilization

In the present study, we use the current server's CPU (C) utilization as the domain. We define fuzzy memberships $\mu_h(C)$, $\mu_m(C)$ and $\mu_l(C)$ as parts of the fuzzy subset of the current server CPU load, indicating membership in "highly-loaded," "moderately-loaded" and "lightly-loaded," respectively. Thus, $\mu_h(C)$, $\mu_m(C)$ and $\mu_l(C)$ are computed according to the following:

$$\mu_l(C) = \begin{cases} 1 & C \le 25\% \\ 1.5 - 2 * C & 25\% < C \le 75\% \\ 0 & C > 75\% \end{cases} \tag{1}$$

$$\mu_m(C) = \begin{cases} 0 & C \le 25\% \\ 4 * C - 1 & 25\% < C \le 50\% \\ 3 - 4 * C & 50\% < C \le 75\% \\ 0 & C > 75\% \end{cases} \tag{2}$$

$$\mu_h(C) = \begin{cases} 0 & C \le 25\% \\ 2 * C - 0.5 & 25\% < C \le 75\% \\ 1 & C > 75\% \end{cases} \tag{3}$$

3.1.2 Memory Utilization

We use the current server's memory (M) utilization as the domain. We define fuzzy memberships $\mu_h(M)$, $\mu_m(M)$ and $\mu_l(M)$ as parts of the fuzzy subset of the current server

memory load, indicating membership in "highly-loaded," "moderately-loaded" and "lightly-loaded," respectively. Thus, are computed according to the following: $\mu_h(M)$, $\mu_m(M)$ and $\mu_l(M)$ are computed according to the following:

$$\mu_l(M) = \begin{cases} 1 & M \leq 25\% \\ 1.5 - 2 * M & 25\% < M \leq 75\% \\ 0 & M > 75\% \end{cases} \tag{4}$$

$$\mu_m(M) = \begin{cases} 0 & M \leq 25\% \\ 4 * M - 1 & 25\% < M \leq 50\% \\ 3 - 4 * M & 50\% < M \leq 75\% \\ 0 & M > 75\% \end{cases} \tag{5}$$

$$\mu_h(M) = \begin{cases} 0 & M \leq 25\% \\ 2 * M - 0.5 & 25\% < M \leq 75\% \\ 1 & M > 75\% \end{cases} \tag{6}$$

3.1.3 I/O Utilization

We used the current server's I/O (IO) utilization as the domain. We define fuzzy memberships $\mu_h(IO)$, $\mu_m(IO)$ and $\mu_l(IO)$ as parts of the fuzzy subset of the current server I/O load, indicating membership in "highly-loaded," "moderately-loaded" and "lightly-loaded," respectively. Thus, $\mu_h(IO)$, $\mu_m(IO)$ and $\mu_l(IO)$ are computed according to the following:

$$\mu_l(IO) = \begin{cases} 1 & IO \leq 30\% \\ 1.75 - 2.5 * M & 30\% < IO \leq 70\% \\ 0 & IO > 70\% \end{cases} \tag{7}$$

$$\mu_m(IO) = \begin{cases} 0 & IO \leq 30\% \\ 5 * IO - 1.5 & 30\% < IO \leq 50\% \\ 3.5 - 5 * IO & 50\% < IO \leq 70\% \\ 0 & IO > 70\% \end{cases} \tag{8}$$

$$\mu_h(IO) = \begin{cases} 0 & IO \leq 30\% \\ 2.5 * IO - 0.75 & 30\% < IO \leq 70\% \\ 1 & IO > 70\% \end{cases} \tag{9}$$

After fuzzy processing of the four input variables by their respective membership functions, we comprehensively evaluate the load status of the virtual servers. The only output of the fuzzy logic inference system is the probability that a request should be

allocated to a virtual server, indicated by R. The set of factors is taken to be $E = \{C, M, IO\}$ and the collection of comments as {high, medium, low} when comprehensive fuzzy evaluation is used for internet quality of service.

3.2 Fuzzy Reasoning

Fuzzy reasoning is the core of the fuzzy controller, based on the relation of the fuzzy logic and the rule of inference. It provides the ability to simulate based on the fuzzy concept. The fuzzy control rules database is the most important component of fuzzy logic inference. The classical fuzzy rules are composed of numerical or linguistic variables. We construct a fuzzy matrix to represent memberships of the input parameters in each fuzzy subset, and perform comprehensive fuzzy evaluation according to the following steps:

(1) In a parallel manner, we establish a comprehensive fuzzy evaluation model to evaluate a single factor of each index. The output of the fuzzy logic is the possibility of assigning the network request to the virtual server in the case of overload. The evaluation results of each factor have the following fuzzy vectors:

$$R1 = [u_h(C), u_m(C), u_l(C)],$$
$$R2 = [u_h(M), u_m(M), u_l(M)],$$
$$R3 = [u_h(IO), u_m(IO), u_l(IO)],$$

where the three vectors constitute a fuzzy matrix from the factor set to the comment set, $R = [R1, R2, R3]$.

(2) We determine weight vector $P = [p1, p2, p3]$, where $p1$, $p2$ and $p3$ represent the importance of CPU, memory and I/O, respectively, in u, and $p1 + p2 + p3 = 1$.

(3) We define a fuzzy transformation $Q = P \cdot R$, where Q is the evaluation result of each virtual server in the comment collection of fuzzy vector $F = (L, M, H)$. Three of these components represent the extent to which the virtualserver is a candidate.

3.3 Defuzzification

Because the output of fuzzy inference is fuzzy vector F, it is necessary to solve the model to obtain the exact output value. We adopt the classical area center method for defuzzification. It takes the centroid of the membership function of each fuzzy rank as the exact output of the fuzzy grade. The corresponding centroid of the fuzzy grade L is 0.15, the corresponding centroid of the fuzzy grade M is 0.5, and the corresponding centroid of the fuzzy grade H is 0.85. Finally, we use the following formula to calculate the exact value of the output of the fuzzy logic:

$$Fuzzy\_out = \frac{\sum_i w_i M_i}{\sum_i M_i}, \tag{10}$$

where, M_i represents the centroid of each output fuzzy level, and wiindicates the weight of the corresponding output fuzzy level for M_i.

3.4 Load Balancing Strategy Based on SDN

Our proposed LBSFL is based on SDN. This strategy attains load balance among multiple servers while saving energy. When the overall load is low, the server with the lightest load is set to sleep; when the overall load is high, the server is restarted. The following is the specific implementation strategy:

(1) Initialize the OpenFlow network. The system responds to the web requests through a classic polling algorithm. The load balancing module obtains server status information through SDN switches and calculates the load of the server through a classic polling algorithm, then calculates the load balancing parameter of the OpenFlow network.

(2) Set the load balance adjustment threshold. The minimum threshold of the server's average load is assumed to be 0.2 and the maximum threshold to be 0.8. The adjustment threshold for load balancing will be obtained experimentally. The fuzzy logic algorithm adjusts the load balance. When δ is greater than the threshold value, the current web request is forwarded to the server with the lowest load. When δ is lower than the threshold and F_{avg} is lower than 0.2, the server load is idle and the server migration strategy [5] is executed to sleep the server with the smallest load. When δ is lower than the threshold and the F_{avg} is greater than 0.8, the server load is saturated and the server migration strategy [5] is executed to restart a virtual server. When δ is lower than the threshold and the F_{avg} is between 0.2 and 0.8, it shows that the current load of the virtual server is balanced, and the status of the server continues to be monitored. The execution flow chart of the strategy is shown in Fig. 2:

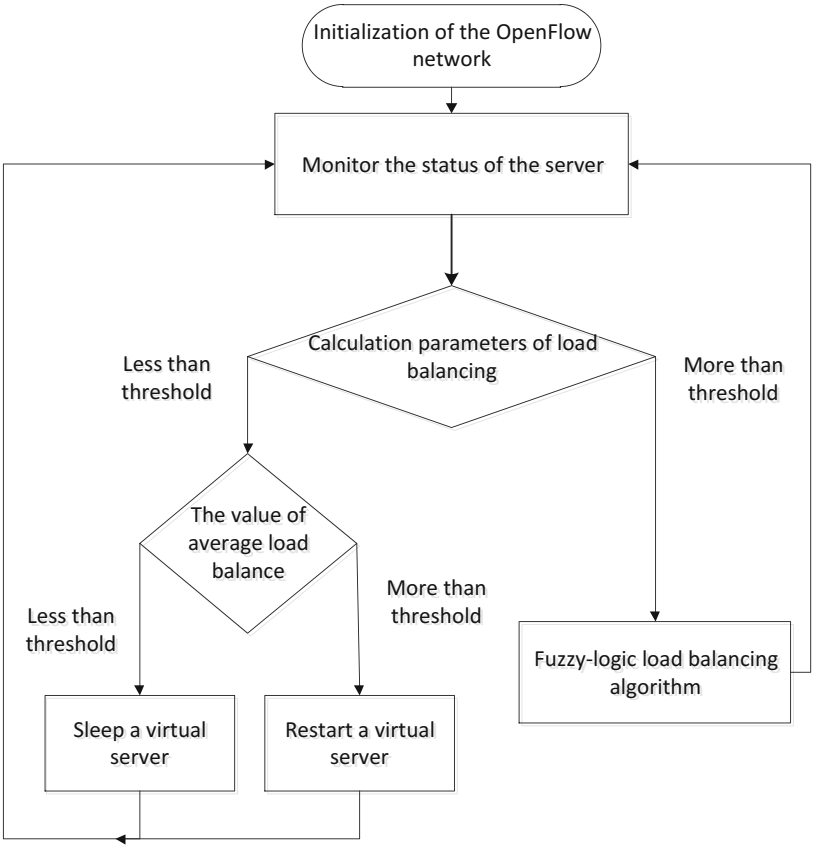


Fig. 2. Proposed load balancing strategy based on fuzzy logic

4 Experimental Analysis

To review the performance of the LBSFL based on SDN, we used the following experimental environment: Ubuntu version 11.04, running on an Intel Pentium E2180 dual-core 4-GHz processor. We used open source software Mininet 2.0 to build the OpenFlow network, the H3C5510_34C switch that supports the OpenFlow1.3 protocol, and a Java-based OpenDayLight controller to implement the load balancing strategy. To test the performance of the algorithm, we installed iperf, a network performance testing tool, which generated traffic pressure in the Mininet environment.

The simulation testing system structure is shown in Fig. 3. Four virtual machines with identical configurations were assigned as web servers. Taking into account that frequently sleeping and restarting the server impacted the performance of the system, we set a minimum of four virtual servers.

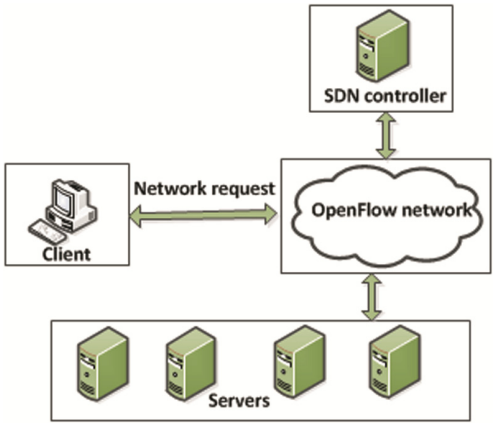


Fig. 3. Hardware simulation platform

We first evaluated the efficiency of LBSFL against traditional round-robin (WRR) and weighted least connections (WLC) schemes. The input data of the fuzzy system included CPU utilization, memory utilization and I/O utilization. The empirical values of the three parameters were 0.4, 0.3 and 0.3, respectively. In the test, the load was increased linearly for the first 10 min, adding 2000 connection requests per minute; followed by a linear reduction by 2000 connection requests per minute for the next 10 min. The total experimental time was 20 min. Samples were taken every 1 min, and the test was repeated five times. The average of these values was assumed to be the value of system response time at that time. The test results are shown in Fig. 4.

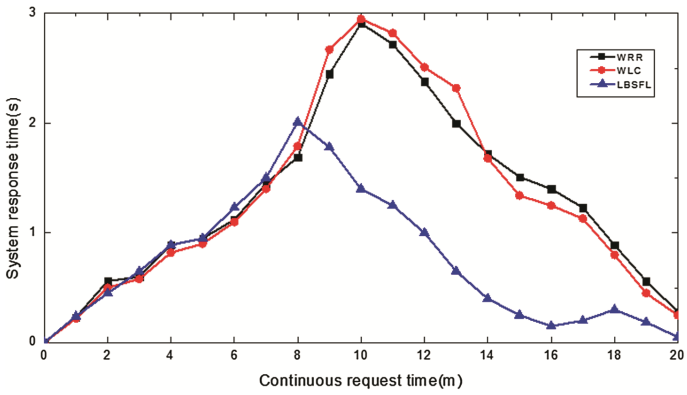


Fig. 4. Response time of system

At the same time, to achieve a more prominent load balancing effect in LBSFL, we also extracted the CPU, memory utilization, I/O average utilization rates of each server. Figures 5, 6 and 7 present the CPU, memory and I/O usage graphs of the four servers (h1, h2, h3, h4) under WRR, WLC and LBSFL schemes, respectively.

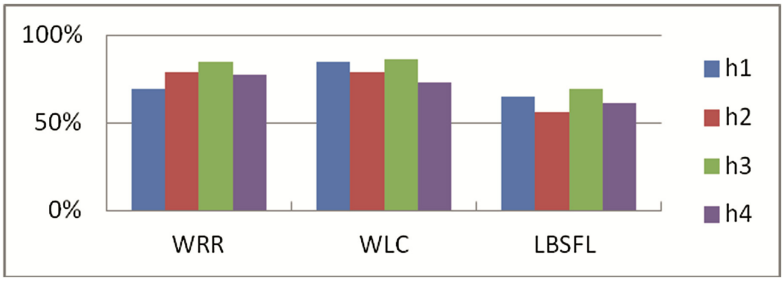


Fig. 5. CPU utilization

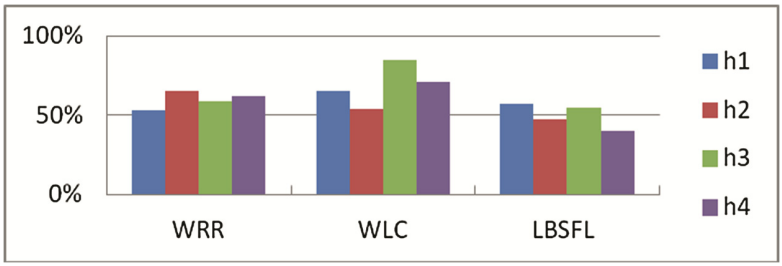


Fig. 6. Memory utilization

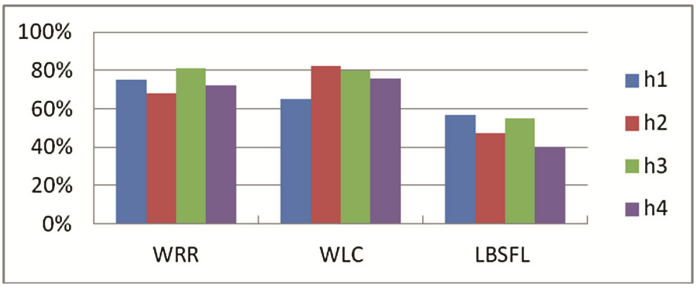


Fig. 7. I/O utilization

From the experimental results we can see:

(1) From Fig. 4, the average server response times for the three schemes, WRR, WLC and LBSFL were 1.434 s, 1.532 s and 0.83 s respectively. It is evident that the average server response times of the server in LBSFL was the lowest among the three schemes. This is because LBSFL always chooses the server characterized by a fuzzy logic algorithm to provide services to the users. Moreover, WRR and WLC do not consider the real-time status of the servers. From Figs. 5, 6 and 7, we also found that the load balancing effect of LBSFL is better than that of WRR and WLC.

(2) With the parameters shown in Fig. 4, the number of requests was small, the task management and scheduling was relatively simple, and there was not much

difference between the three strategies with respect to system response time. However, as the number of requests increased, task management and scheduling became more and more complex. The response time of LBSFL was shorter than those of WRR and WLC. With its simplified task management and scheduling, LBSFL provided more advantages than WRR and WLC.

(3) The LBSFL system response time curve shows two obvious wave peaks, the first at about 8 min. With increasing requests, the current load capacity of all virtual servers peaked. To reach system dynamic balance, the controller triggered the load scheduling mechanism to start a virtual server, after which the response time of the system appeared to decline and stabilize. The second peak was at about 18 min. With decreasing requests, the current server load continually reduced until the controller triggered the load scheduling mechanism to sleep a virtual server. After this, the system response time again appeared to decline and stabilize. Because of the sleep of a server, the system request processing ability was weakened, so there was a small wave crest, and with the task management and scheduling becoming simpler, the response time of the system appeared to decline. Server sleep and restart also resulted in system energy saving.

5 Summary

Traditional load balancing hardware is expensive and lacks adequate scalability and flexibility. We propose a load balancing strategy in SDN networks that successfully enhanced the load balancing effect and improved network resource utilization.

Acknowledgments. The author would thank the support from projects of the national "863Program" (NO. 2015BAF09B02-3); the natural science fund of Tianjin city (NO. 17JCQNJC00500); Tianjin education science planning project of 13th five-year plan (HE3045); the fundamental research fund for the university in Tianjin, Tianjin Chengjian university (2016CJ12) and the fund of Tianjin Education Committee (20110813).

References

1. McKeown, N.: Software-defined networking. INFOCOM Keynote Talk **17**(2), 30–32 (2009)
2. McKeown, N., Anderson, T., Balakrishnan, H., et al.: OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Comput. Commun. Rev. **38**(2), 69–74 (2008)
3. Namal, S., Ahmad, I., Gurtov, A., et al.: SDN based inter-technology load balancing leveraged by flow admission control. In: 2013 IEEE SDN for Future Networks and Services (SDN4FNS), pp. 1–5. IEEE (2013)
4. Marconett, D., Liu, L., Yoo, S.J.B.: Optical FlowBroker: load-balancing in software-defined multi-domain optical networks. In: Optical Fiber Communication Conference. Optical Society of America (2014): W2A. 44
5. Muñoz, P., Barco, R., de la Bandera, I.: Load balancing and handover joint optimization in LTE networks using fuzzy logic and reinforcement learning. Comput. Netw. **76**, 112–125 (2015)

6. Zhong, H., Fang, Y., Cui, J.: LBBSRT: an efficient SDN load balancing scheme based on server response time. Future Gener. Comput. Syst. **68**, 183–190 (2017)
7. Gandhi, R., Liu, H.H., Hu, Y.C., et al.: Duet: cloud scale load balancing with hardware and software. ACM SIGCOMM Comput. Commun. Rev. **44**(4), 27–38 (2015)
8. Wang, Y., Zhang, Y., Chen, J.: SDNPS: a load-balanced topic-based publish/subscribe system in software-defined networking. Appl. Sci. **6**(4), 91 (2016)
9. Handigol, N., Seetharaman, S., Flajslik, M., et al.: Plug-n-serve: load-balancing web traffic using OpenFlow. ACM Sigcomm Demo **4**(5), 6 (2009)
10. Kaur, S., Singh, J., Kumar, K., et al.: Round-robin based load balancing in software defined networking. In: 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), pp. 2136–2139. IEEE (2015)
11. Zhang, H., Guo, X.: SDN-based load balancing strategy for server cluster. In: 2014 IEEE 3rd International Conference on Cloud Computing and Intelligence Systems (CCIS), pp. 662–667. IEEE (2014)
12. Shang, Z., Chen, W., Ma, Q., et al.: Design and implementation of server cluster dynamic load balancing based on OpenFlow. In: 2013 International Joint Conference on Awareness Science and Technology and Ubi-Media Computing (iCAST-UMEDIA), pp. 691–697. IEEE (2013)
13. Pakzad, F., Portmann, M., Tan, W.L., et al.: Efficient topology discovery in OpenFlow based software defined networks. Comput. Commun. **77**, 52–61 (2016)
14. Scott-Hayward, S.: Design and deployment of secure, robust, and resilient SDN controllers. In: 2015 1st IEEE Conference on Network Softwarization (NetSoft), pp. 1–5. IEEE (2015)
15. Hoang, D.B., Pham, M.: On software-defined networking and the design of SDN controllers. In: 2015 6th International Conference on the Network of the Future (NOF), pp. 1–3. IEEE (2015)
16. Kang, S.B., Kwon, G.I.: Load balancing strategy of SDN controller based on genetic algorithm. Mech. Eng. **129**, 219–222 (2016)

Author Index