EAI/Springer Innovations in Communication and Computing

Mian Ahmad Jan
Fazlullah Khan
Muhammad Alam *Editors*

Recent Trends and Advances in Wireless and IoT-enabled Networks

Springer

EAI
RESEARCH MEETS INNOVATION

EAI/Springer Innovations in Communication and Computing

Series editor
Imrich Chlamtac, CreateNet, Trento, Italy

Editor's Note

The impact of information technologies is creating a new world yet not fully understood. The extent and speed of economic, lifestyle, and social changes already perceived in everyday life is hard to estimate without understanding the technological driving forces behind it. This series presents contributed volumes featuring the latest research and development in the various information engineering technologies that play a key role in this process.

The range of topics, focusing primarily on communications and computing engineering, includes, but is not limited to, wireless networks, mobile communication, design and learning, gaming, interaction, e-health and pervasive healthcare, energy management, smart grids, internet of things, cognitive radio networks, computation, cloud computing, ubiquitous connectivity, and more generally smart living, smart cities, and more. The series publishes a combination of expanded papers selected from hosted and sponsored European Alliance for Innovation (EAI) conferences that present cutting-edge, global research as well as provide new perspectives on traditional related engineering fields. This content, complemented with open calls for contribution of book titles and individual chapters, together maintains Springer's and EAI's high standards of academic excellence. The audience of the book consists of researchers, industry professionals, advanced level students as well as practitioners in related fields of activity including information and communication specialists, security experts, economists, urban planners, doctors, and, in general, representatives from all walks of life affected and contributing to the information revolution.

About EAI

EAI is a grassroots member organization initiated through cooperation between businesses, public, private, and government organizations to address the global challenges of Europe's future competitiveness and link the European Research community with its counterparts around the globe. EAI reaches out to hundreds of thousands of individual subscribers on all continents and collaborates with an institutional member base including Fortune 500 companies, government organizations, and educational institutions by providing a free research and innovation platform.

Through its open free membership model, EAI promotes a new research and innovation culture based on collaboration, connectivity, and recognition of excellence by community.

More information about this series at http://www.springer.com/series/15427

Mian Ahmad Jan • Fazlullah Khan
Muhammad Alam
Editors

Recent Trends and Advances in Wireless and IoT-enabled Networks

Springer

EAI
RESEARCH MEETS INNOVATION

Editors
Mian Ahmad Jan
Abdul Wali Khan University Mardan
Mardan, Pakistan

Fazlullah Khan
Abdul Wali Khan University Mardan
Mardan, Pakistan

Muhammad Alam
Department of Computer Science
and Software Engineering
Xi'an Jiaotong-Liverpool University
Suzhou, Jiangsu Province, China

ISSN 2522-8595 ISSN 2522-8609 (electronic)
EAI/Springer Innovations in Communication and Computing
ISBN 978-3-319-99965-4 ISBN 978-3-319-99966-1 (eBook)
https://doi.org/10.1007/978-3-319-99966-1

Library of Congress Control Number: 2018965488

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

To our families and friends who provided selfless support and motivation during the whole process.

Foreword

Today's world has seen significant growth in the advancement of wireless technologies, from communication to health control and monitoring applications. During the last two decades, various innovative technologies such as high-speed Internet, smart homes, smart cities, underwater sensor networks, and body area networks have emerged and many more still under consideration. The academia and industrial research groups are facing an increase in demand from the users to develop wireless applications to fulfil their needs of high data rates, error-free communication, conservation of battery power, and bandwidth efficiency. To address these demands and their underlying challenges, this book mainly focuses on presenting the new emerging paradigms in wireless communication. There is an ongoing convergence of four key technologies that are poised to transform the Information and Communications Technology (ICT) ecosystem. Those technologies are the Fifth Generation (5G) cellular, Artificial Intelligence (AI), Data Analytics, and Internet of Things (IoT). These technologies coupled with cloud computing will have a huge impact in their own right, both on ICT and on all major industry verticals that depend on telecom and IT services. However, the combination of these technologies is poised to create opportunities to significantly enhance user experiences for communications, applications, digital content, and commerce.

To this point, it seems an amazing and complicated task to connect everything; however, one can avoid the data storage problem of connecting hundreds of thousands of wireless applications. Therefore, this book focuses on how to optimally store data considering traditional and cloud storage. Cloud computing is playing an important role in storing huge amounts of data that has been processed by various cloud servers, which not only lowers the burden of storage but also the processing power of the traditional systems. To do so, many efficient machine learning algorithms are used in processing this huge amount of data.

Department of Computer Science, Ateeq Ur Rehman
Abdul Wali Khan University Mardan, Mardan, Pakistan

Preface

This book provides detailed information about the recent trends and advancements in Information and Communications Technologies. The Information and Communications Technology industry is experiencing profound changes across a broad range of research areas. More and more research is being poured into innovative technologies that aim to facilitate humans in the long run. Besides, a substantial amount of research funding is allocated by governments to provide facilities to their people at their doorsteps. For example, consumer cloud service is a concept involving the storage of various consumer electronic items in "the cloud" for the benefit of anytime, anywhere, any device access. With worldwide carriers reaching saturation of human users, network operators are looking for new ways to generate revenue and enhance profitability. At the same time, miniaturization is reaching the point in which embedded computing can be virtually ubiquitous. Many things are converging including everything from networks, services, and entire business models. One key example that is particularly poignant for enterprise is the convergence of Machine to Machine (M2M), Internet of Things (IoT), and Social and Big Data.

This book covers a diverse range of topics that are all related to recent trends in communication technologies. Due to the aforementioned trends, the industry is expected to anticipate several developments. Artificial Intelligence is becoming a part of everything. It is getting integrated into everything from machine learning, predictive analytics, security software, intelligent agents, and many more. The cloud computing is moving beyond Information Technology (IT) to include communications, applications, content, and commerce across a diverse number of industry verticals. IoT will become part of the global lexicon of indispensable things, just like smartphones and the Internet itself. Besides, Wireless Sensor Networks (WSNs) and Wireless Body Area Networks (WBANs) are contributing a lot to IoT by revolutionizing industrial automation, healthcare, agriculture, and many other sectors. Broadband, in particular wireless, is enabling key technology areas to integrate with each other. While 4G via LTE is currently the worldwide recognized standard for high-speed wireless data, it will pale in comparison to what will be commercially available by 2020 when 5G is in operation. It is expected that 5G

in near future will provide ubiquitous and pervasive communication by connecting IoT, RFID, Cloud, and many more.

Each chapter of this book is dedicated to the aforementioned tasks. Each chapter focuses on one or more of these technological trends of ICT. Except technical terms, the readability and flow of concepts make this book an easy to go for any person with some technological background.

Mardan, Pakistan — Mian Ahmad Jan
Mardan, Pakistan — Fazlullah Khan
Suzhou, China — Muhammad Alam

Acknowledgment

We would like to express our special appreciations to the Vice-Chancellor of Abdul Wali Khan University Mardan and the Patron in Chief of the University of Lahore, Pakistan, for their enduring support. We would also like to thank authors, reviewers, and committee members. Without their contributions, this book would not have been possible. Our special gratitude goes to our friends and colleagues for their technical support, especially Dr. Rodziah Binti Attan, Dr. Abid Yahya, Dr. Nabeel Younus Khan, Dr. Khalid Hussain, Dr. Aurangzeb Khan, Dr. Saeed Islam, Dr. Sajjad Khan, Dr. Mukhtaj Khan, and Dr. Ateeq Ur Rehman.

Finally we would like to thank all those who help and support us during the whole process.

Contents

Chapter 1
A Distributed Trust Management Model for the Internet of Things (DTM-IoT)

Mohammad Dahman Alshehri, Farookh Hussain, Mahmoud Elkhodr, and Belal Saeed Alsinglawi

Abstract The Internet of Things (IoT) is a paradigm that facilitates autonomous communications among various IoT devices with minimal human intervention. This raises many security challenges, which are critical and must be addressed to allow for the wide deployment of IoT. Trust must be provisioned among the various heterogeneous IoT devices. In this paper, a distributed trust management model is proposed. The model offers solutions to trust management and negotiations in the IoT. It is inspired by clustering techniques that are adopted in WSNs. After introducing the structural design and the main components of the trust model, we demonstrate how our new approach supports trust negotiations and management in the IoT.

1.1 Introduction

The management and provision of trust in the Internet of Things (IoT) are essential for the security and trustworthiness of communications in the IoT [1]. While

M. D. Alshehri
Centre for Artificial Intelligence, School of Software, Faculty of Engineering and Information Technology, University of Technology Sydney, Ultimo, NSW, Australia

Computer Science Department, Taif University, Taif, Saudi Arabia
e-mail: Mohammad.Alshehri@uts.edu.au

F. Hussain (✉)
Centre for Artificial Intelligence, School of Software, Faculty of Engineering and IT, University of Technology Sydney, Ultimo, NSW, Australia
e-mail: Farookh.Hussain@uts.edu.au

M. Elkhodr
School of Engineering and Technology, College of Engineering and Technology, Central Queensland University, Sydney, NSW, Australia
e-mail: m.elkhodr@cqu.edu.au

B. S. Alsinglawi
Western Sydney University, Sydney, NSW, Australia
e-mail: belal.alsinglawi@ieee.org

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_1

numerous IoT communication and interaction models have been the focus of various research studies, such as in [2, 3, 11], solutions that provide trustworthy communications between nodes based on a clustering technique remain unexplored. Existing research such as [3] provides a solution for the smart community for IoT by addressing low cost and power. However, adequate attention has not been given to trust and trust management establishment for IoT devices. The IoT encompasses various applications and devices such as smart products that connect to the Internet using sensors and actuators, which requires management of data, its sharing and analysis mechanisms [2, 4]. Therefore, trust management protocols are needed for trust establishment among the diverse range of IoT devices. The need for trust management in the IoT becomes apparent given the sheer size of the IoT. For instance, [5] points out that the IoT has a growing number of IoT devices, especially in storage and computation. IoT networks should also allow individual nodes to gain trust rapidly and accurately while evolving to adapt to the dynamicity involved around nodes joining and leaving the network on a regular base. The complexity in IoT communications imply that trust management protocols, designed for the IoT, should be highly resilient to trust-based attacks to ensure security protection in hostile environments. Trust management is also necessary given the heterogeneity of communications and the volume of IoT devices.

Among the various issues challenging trust management in the IoT such as lightweight characteristics of IoT devices, perhaps, scalability should be a key consideration in the design of trust protocols in the IoT [6]. This is because most of the existing trust management solutions such as those proposed in [3, 6, 7] did not address the scalability issue, thereby undermining their applicability to large-scale IoT networks.

Trust management and security in the IoT are fundamental to establish trustworthy connections [8–14]. There is a lack of research on trust management in the IoT. More specifically, previous frameworks failed to consider cluster-based approaches and focused mainly on individual solutions at the node level. In [15], the authors proposed a fuzzy reputation method for trust management in the IoT. However, this model is mainly designed to work with wireless sensor networks (WSNs). It focuses more on quality of service (QoS) metrics such as energy consumption, rather than establishing trust among IoT devices.

Similarly, other works such as [4] proposed a trust management protocol that takes into account QoS trust metrics and social trust. In order to update trust values, the authors relied, in their proposed method, on indirect recommendations and direct observations. However, the research is limited to static IoT scenarios. It does not consider the rich and dynamic interactions envisioned in the IoT. Given that the IoT is growing exponentially, solutions such as those proposed in [4] are not applicable to IoT scenarios that involve dynamic interactions.

To fill this gap, this paper introduces the Distributed Trust Management Model (DTM-IoT). The structural design of the proposed DTM-IoT is provided in Sect. 1.2. Section 1.3 presents the components of DTM-IoT. We first describe the architecture of the model, which focuses on the distribution of the IoT nodes based on the dynamic trust value of clusters. We will then elaborate in more details the

main components of the proposed model, which consists of the Cluster Node (CN) component and the Master Node (MN) component. These nodes are responsible for managing the trust management in an IoT network. Conclusion and future works are provided in Sect. 1.4.

1.2 The DTM-IoT Structural Design

The DTM-IoT provides trustworthy communication among devices that are involved in a communication as part of an IoT network. The DTM-IoT architecture allows various IoT devices and applications to establish a trusted communication among themselves, thus paving the way towards a secure communication. The architecture of the DTM-IoT is presented in Fig. 1.1. The DTM-IoT encompasses four types of devices. The first type is a general device, which is a basic physical device. It has default trust value. A device with an actuator is the second type of DTM-IoT device. The role of these devices is to receive the *trust value* command over the Internet. The third type of DTM-IoT devices have sensors which fetch the trusted data from the IoT environment and transfer the data over the Internet. A

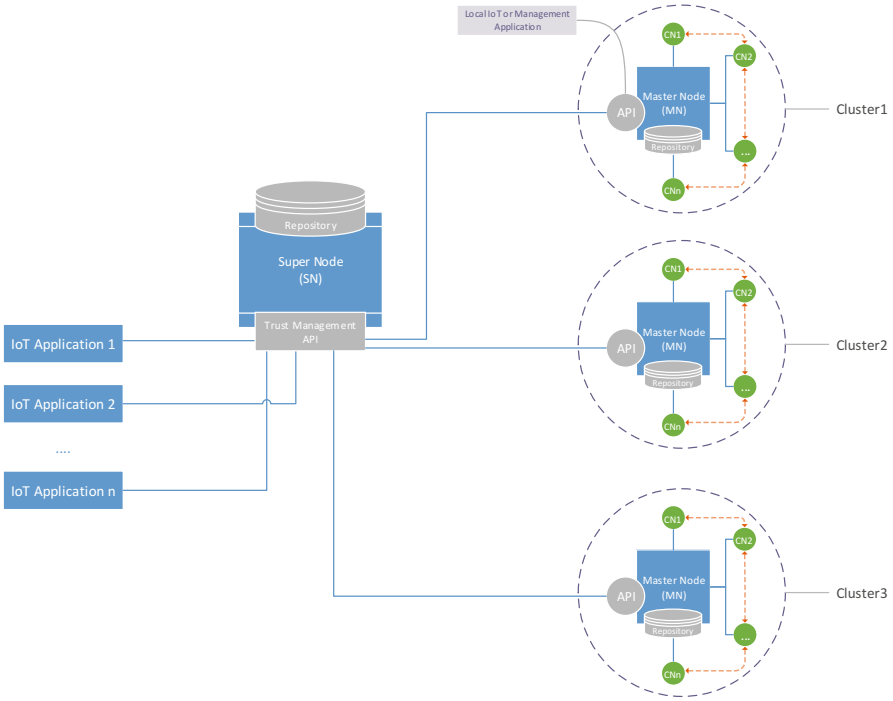


Fig. 1.1 DTM-IoT dynamic architecture

hybrid device is the last type of DTM-IoT device which has both trusted actuation and sensing capabilities. The DTM-IoT provides trustworthy communication among these nodes (devices).

The DTM-IoT architecture is a distributed architecture that consists of Cluster Node (CN), Master Node (MN) and a Super Node (SN). In this architecture, as shown in Fig. 1.1, the DTM-IoT adapts the structure that is used by traditional network management approaches. The DTM-IoT architecture consists of a Cluster Node (CN), which resides on a node, and a Master Node (MN). The Cluster Node (CN) acts as a communication node that has the responsibility for transporting the data generated or collected by CN to their MN. The MN manages many CNs in the Cluster. The MN also stores the received data, sent by CN in the cluster, in a repository at MN.

The Super Node (SN) is the base node in the DTM-IoT. It is responsible for ensuring trust in an IoT network. The SN contains an API, referred to as the trust management API. This API allows the SN to communicate with the Master Node (MN) in a given cluster. The SN also has a repository that stores the trust values and addresses of MNs and CNs. The repository of SN is hierarchical (tree-structured). Each entry relevant to a CN is addressed through the MN's unique ID. Therefore, the repository of SN does not store any data collected from the CN. It only stores its trust value and address information, i.e. through which MN and CN can be accessed. An IoT application running with the SN can provide services based on combining data collected from various CNs. Therefore, IoT applications and services are built on top of the IoT, by supporting communications among nodes through the SN.

The DTM-IoT architecture provides a centralised model of several clusters and a MN that allows for central trust management of things over local area networks. On the other hand, the DTM-IoT distributed architecture of several MNs and Clusters creates a trust distributed system where CNs communicate in a cooperative rather than a stand-alone manner. This flexibility in architecture is designed for the specific communications requirements of the IoT. This is important since IoT devices may play different roles in both centralised and distributed operation setups, especially for trust management in the IoT.

1.3 The DTM-IoT Mechanisms

In this section, we will introduce the various components of the DTM-IoT.

1.3.1 The Cluster Node (CN) Components

The Cluster Node (CN) is an IoT node which stores the trust value of a cluster in the MN repository. It stores the trust attributes of the cluster.

Table 1.1 IoT Cluster Node Trust Management Attributes

Trust Management Attributes (TMA)
ID
PKI
Trust value
Firmware version
IP, MAC address, network name or others
Battery life
Location (as a heterogeneous node)

In particular, CN is represented using the Trust Management Attributes (TMA). These attributes represent parameters such as the communication status of CN. A TMA is used to establish communication among other nodes in each cluster, based on the trust management criteria. TMAs are also used to maintain the data CN collects. They are also used to maintain information relating to CN activities. The formalisation of TMA offers a method to maintain and store CN trust information and other information collected by the MN repository. Table 1.1 shows the Trust Management Attributes (TMA) that represent a Cluster Node (CN).

We, therefore, define a CN as the IoT object that represents the device and its trust behaviour. CNs are accessed through the trust management repository by various IoT applications and the MN. CNs are a representation of IoT nodes that include not only the normal nodes, like a wireless sensor node, but also the trust communication module, software and driver (i.e. CN trust agent) that allow communication among nodes and the MN in the cluster. This is what is called the heterogeneous IoT node. A CN has a unique identification and trust attributes. The TMA can be defined and implemented for IoT nodes to the MN in the clusters. Table 1.1 shows that the TMAs are descriptions of the IoT node based on trust attributes. For instance, the ID is used to identify a unique IoT node. A public key infrastructure (PKI), trust value, firmware version and the rest of these TMAs are also used as identifiers or descriptions for IoT nodes. These trust attributes assist MNs to decide which nodes are appropriate to offer an authority to access and join the proper cluster, based on the similarity of trust value between the node and the cluster. These trust attributes support the CN in establishing a trusted communication among the CNs in the cluster. Therefore, the TMA will ultimately provide an opportunity for the CNs to be the trusted smart node.

Figure 1.2 models CNs and demonstrates that there are two main modules for a trust agent. The trust communication module is responsible for establishing communications that are trustworthy among other CNs and communicates with the MN. The trust agent services module is responsible for the services execution (such as generating low trust value level alerts or handling IoT trust actuation instructions). Therefore, the trust agent controls the communications between two important IoT nodes in the cluster. It controls the communication between CN and MN by sending the collated data to the MN and dealing out the requests sent by MN and correspondingly controls the communications between the CN and the other CNs in the cluster. The responsibilities of the CN trust agent are:

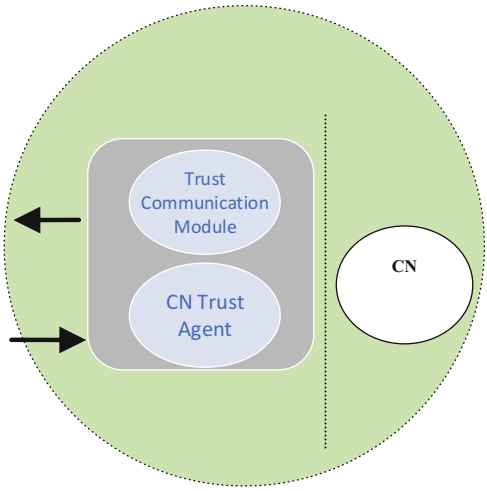


Fig. 1.2 Cluster Node (CN) components

- Establish a trust communication with the other CNs.
- Communicate and send data updates to the MN.
- Receive trust instructions of actuation from the MN.
- Manage responses and requests from/to the MN to join in/out the cluster.
- Send notifications of trust value levels to the MN.

1.3.2 The Master Node (MN) Components

Cluster is an IoT trusted CN application that performs the cluster operational roles of receiving and generating requests to retrieve trust value information from IoT nodes. A MN can also receive activity-based trust notification reports on CNs generated by their trust agent. MN controls the communication among nodes in the cluster to be trusted. It also manages the whole cluster so that it is secured and trusted. A MN maintains a trust value repository, which stores the trust value and other information about all CNs in the cluster. The MN accesses CNs' data stored in this repository. An MN also communicates with the Super Node (SN) to update it about its activity and to send a trust value of the whole cluster to be stored in SN repository.

A MN includes and provides a trust management Application Programing Interface (API) to receive IoT services from other nodes out of the cluster.

Information, which is stored in the MN repository, can be requested over the Internet once the API allows IoT applications to communicate with a MN. The API also allows trust management applications to control and monitor the CNs. The trust management API is used to communicate topology information over the Internet about the clusters and IoT network to the SN. The SN is a higher main IoT node that is responsible for the whole trust IoT network and is located above the MNs

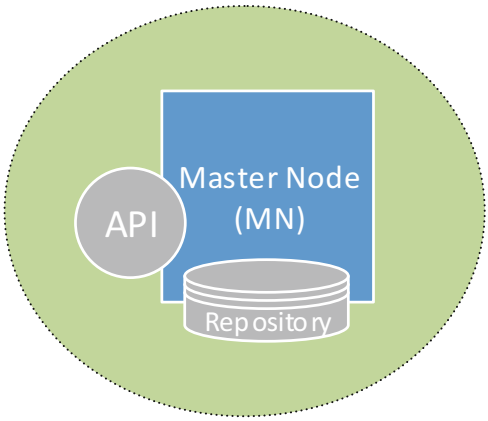


Fig. 1.3 Master Node (MN) components

and clusters. Under the supervision of the MN, the IoT applications run on top of the SN and send requests to access MN's data. Figure 1.3 shows the infarctions between MN and CNs in the cluster. To provide trustworthy communication in the cluster, the MN includes several modules that offer security, trust management and privacy abilities, among other IoT trust operational services.

1.3.3 The Cluster Components

The intention of the Trust Management IoT platform is to build upon dividing IoT nodes into different clusters based on their trust value. Based on each cluster's trust value, nodes will request to join into clusters. This method provides efficient and trusted IoT communication, by applying the trust value of the cluster for each node in the IoT. This allows for fast communication, easy control and longer battery life, since the request will be generated from nodes based on the trust value of the corresponding clusters. Nodes within the clusters contact the MNs to get authorisation to join or redirect the node. They request joining the appropriate cluster based on its trust value.

The cluster has two main functions. The first function is to maintain IoT communication by providing trustworthy communication. This allows nodes that have similar trust values to join into clusters. The cluster will then deal with other clusters rather than nodes. Another function of clusters is to provide additional communication capabilities for IoT networks through the application of trust management attributes for the cluster components (MN, CNs). Figure 1.4 shows the main components of MN.

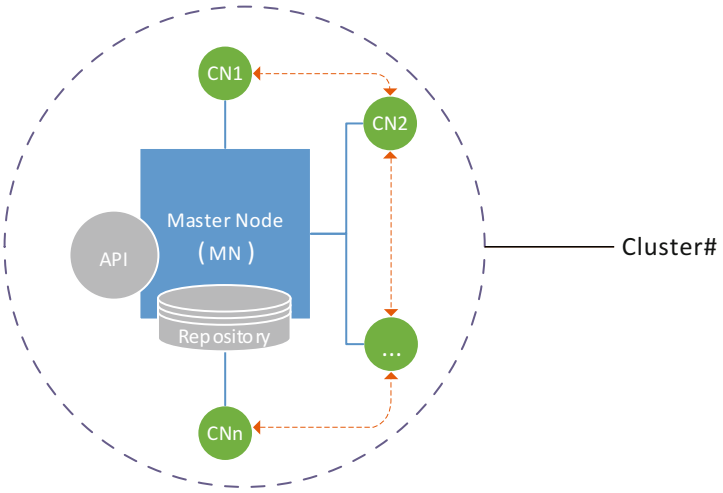


Fig. 1.4 Cluster components

1.4 Conclusion and Future Work

This paper introduced the Distributed Trust Management for Internet of Things (DTM-IoT) model. This proposed model consists of a Super Node (SN), a Master Node (MN) and a Cluster Node (CN). The DTM-IoT provides IoT devices with a mechanism that allows them to negotiate and establish trust among them. The model relies on a distributed architecture, in which the Super Node assigns trust values to cluster components. The communication between the Super Node and the Cluster component is facilitated by the Master Node. Future works involve the design of a network simulation in order to evaluate the proposed model. The simulation aims to demonstrate how a new node can join the IoT network and gains trust and thus engages in a secure communication with other nodes. The simulation work will also involve the design of a threat model to evaluate the trust management services provisioned by the DTM-IoT.

References

1. Alshehri, M. D., & Hussain, F. K. (2015). A comparative analysis of scalable and context-aware trust management approaches for internet of things. In *International Conference on Neural Information Processing* (pp. 596–605). Cham, Switzerland: Springer.
2. Alshehri, M. D., & Hussain, F. K. (2018). A centralized trust management mechanism for the internet of things (CTM-IoT). In *12th International conference on broad-band wireless computing, communication and applications. BWCCA 2017* (Vol. 12, pp. 533–543). Cham: Springer. https://doi.org/10.1007/978-3-319-69811-3_48.
3. Li, X., Lu, R., Liang, X., Shen, X., Chen, J., & Lin, X. (2011). Smart community: An internet of things application. *IEEE Communications Magazine, 49*(11), 68–75.

4. Bao, F., & Chen, I.-R. (2012). Dynamic trust management for internet of things applications. In *Proceedings of the 2012 International Workshop on Self-aware Internet of Things* (pp. 1–6). New York: ACM.
5. Chen, R., Bao, F., Chang, M., & Cho, J.-H. (2014). Dynamic trust management for delay tolerant networks and its application to secure routing. *IEEE Transactions on Parallel and Distributed Systems, 25*(5), 1200–1210.
6. Bao, F., & Chen, R. (2012). Trust management for the internet of things and its application to service composition. In *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)* (pp. 1–6). Piscataway, NJ: IEEE.
7. Chen, R., Guo, J., & Bao, F. (2016). Trust management for SOA-based IoT and its application to service composition. *IEEE Transactions on Services Computing, 9*(3), 482–495.
8. Chen, C., & Helal, S. A. (2011). Device-centric approach to a safer internet of things. In *International workshop on networking and object memories for the internet of things (NOMe-IoT)* (pp. 1–6). New York: ACM.
9. Ren, W. (2011). QoS-aware and compromise-resilient key management scheme for heterogeneous wireless internet of things. *International Journal of Network Management, 21*(4), 284–299.
10. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer, 44*(9), 51–58.
11. Alshehri, M. D., Hussain, F. K., & Hussain, O. K. (2018). Clustering-driven intelligent trust management methodology for the internet of things (CITM-IoT). *In Mobile Netw Appl., 23*, 419–431. https://doi.org/10.1007/s11036-018-1017-z.
12. Zhou, L., & Chao, H.-C. (2011). Multimedia traffic security architecture for the internet of things. *IEEE Network, 25*(3), 35–40.
13. Alam, M., Ferreira, J., Mumtaz, S., Jan, M. A., Rebelo, R., & Fonseca, J. A. (2017). Smart cameras are making our beaches safer: A 5G-envisioned distributed architecture for safe, connected coastal areas. *IEEE Vehicular Technology Magazine, 12*(4), 50–59.
14. Jan, M.A., Usman, M., He, X., & Rehman, A.U. (2018). SAMS: A Seamless and Authorized Multimedia Streaming framework for WMSN-based IoMT. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2018.2848284
15. Chen, D., Chang, G., Sun, D., Li, J., Jia, J., & Wang, X. (2011). TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Computer Science and Information Systems, 8*(4), 1207–1228.

Chapter 2
A Review of Current Security Issues in Internet of Things

Mudassar Ahmad, Tanveer Younis, Muhammad Asif Habib, Rehan Ashraf, and Syed Hassan Ahmed

Abstract The Internet of Things (IoT) is a framework in which every real-world object can be identified uniquely and has the capacity to send and receive data to the network. This paper presents analysis and survey on IOT security, also discusses the current status and challenges of IOT security. Typically, there are three layers in IoT architecture, i.e. perception layer, network layer, and application layer. For secure internet of things realization, at each layer a number of security principles should be enforced. In the future the implementation of IoT is only possible if the security issues related to each layer are resolved and addressed. A number of researchers try to address and to give corresponding countermeasures to secure each layer of IoT. This paper provides an overview on proposed countermeasures and challenges of Security.

2.1 Introduction

We are living in the age of internet where we are surrounded by many computing devices. Wired and wireless network are now existing in abundance. Future internet will be developed in such a way that every real-world object will be connected and available online everywhere each object will be able to cooperate and interact with each other. As in the future everything will be connected to the internet, we can call the future internet as an Internet of Things (IoT). In the vision of IoT the object of real world will be the part of the internet. It is observed that by 2020 the number of IoT devices will be more than 50 billion [1]. There are many application areas

M. Ahmad · T. Younis · M. A. Habib (✉) · R. Ashraf
Department of Computer Science, National Textile University, Faisalabad, Pakistan
e-mail: mudassar@ntu.edu.pk; tanveeryounis66@gmail.com; drasif@ntu.edu.pk; rehan@ntu.edu.pk

S. H. Ahmed
Department of Computer Science, Georgia Southern University, Statesboro, GA, USA
e-mail: sh.ahmed@ieee.org

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_2

of IoT such as smart home, smart transportation, smart agriculture, smart business, smart grid, smart healthcare, smart cities, smart logistics, and many more. In IoT everything will be interconnected and they must share information with each other. The transmission of information will be take place in the public places i.e. network layer and application layer. So, if there is no effective mechanism for information protection then the information could be stolen which will result in privacy risk, therefore security and privacy are the concerns of IoT enabled devices but it is difficult to implement due to the various diversity of the IoT devices. Therefore, it is very important to figure out the solution for the security of IoT devices.

2.2 Evolution of Internet of Things

Internet connectivity is becoming cheap and easily accessible all over the world [2]. In computing devices, micro and nanotechnology is being introduced which reduced their size and consumption power while enhancing their storage capabilities which makes it easy to equip them with actuators and sensors. This mishmash of small devices with multiple purpose devices enables them to communicate over the internet. RFID tags, NFC tags, or barcode are attached with the physical objects, then devices such as smart phone, tablet, and RFID/NFC readers are used to scan them. The internet capabilities can be enhanced by connecting this combination of bodily world and cyber space through the smart devices. This will result in a new era of internet which is known as Internet of Things. Figure 2.1 [3] gives the picture of future internet.

Fig. 2.1 Generic IoT scenarios

2.3 Generic Architecture of Internet of Things

Different researchers [4, 5] give different opinions about the layers of the IoT. The basic architecture of IoT can be viewed as three layers as shown in Fig. 2.2 [6]. They are named as Perception, Network, and application layers. Security issues are related to each layer. IoT will face a number of challenges in the future especially related to the security and privacy [2]. The main procedure of IoT is to connect everyone with everything to exchange information with each other and the number of communication devices will be increased exponentially. Therefore, improvement in IoT is dependent on the progress of technology and is applicable for the diverse types of application and business models.

2.3.1 Perception Layer

This layer has resemblance to the physical layer in OSI model. The perception layer consists of various types of sensors and actuators (i.e., QR code, RFID, infrared ZigBee, etc.). These sensors collect, sense, and process data (location, vibration, humidity, wind speed, dust in the air, etc.) collected from the environment and transmit this information to the network layer.

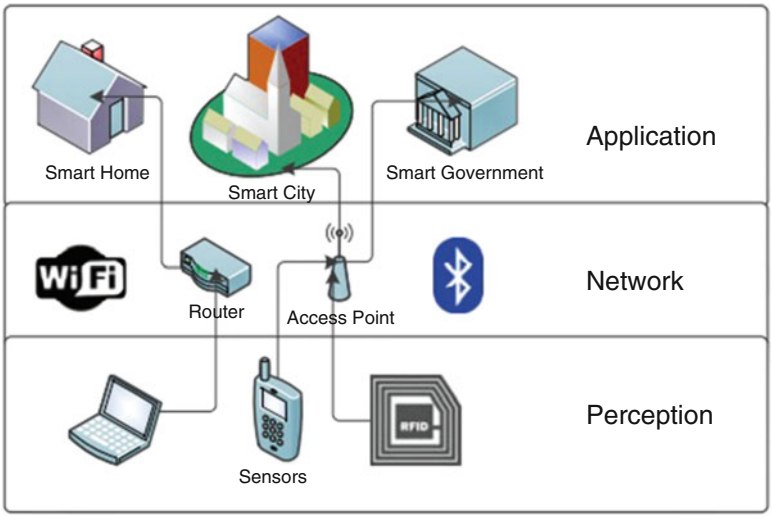


Fig. 2.2 IoT architecture

2.3.2 Network Layer

This layer is responsible for the transmission and routing of the data collected from different IoT sensors to the various IoT devices and hubs over the internet. In this layer, different technologies (i.e., Zigbee, LTE, 3G, WiFi, Bluetooth, etc.) are used to operate various network devices, i.e. router, switches, and gateways. Aggregation filtration and transmission of data take place through network gateways and they serve as a mediator between different IoT devices [7].

2.3.3 Application Layer

This layer is responsible for confidentiality, authenticity, and integrity of the data. The purpose of IoT is achieved at this layer. IoT (internet of things) applications can be smart home, smart postal, smart glasses, smart transportation, smart health, etc.

2.4 IOT Protocols

Protocols are the rules and regulations that are used for end-to-end communication of devices connected to a different or same network. This section will give a brief description about the protocols which are mostly used in machine-to-machine (M2M) communication. Message Queue Telemetry Transport (MQTT) [3] is a client–sever protocol for messaging transportation. It is easy to implement and lightweight. This protocol will run over TCP/IP. Whenever abnormal disconnection occurs MQTT will notify the interested parties about this event through an extraordinary mechanism. Constraint Application Protocol (CoAP) is an application layer protocol that is used for internet devices with resource constrained. This protocol is specially designed for M2M communication such as building automation and smart city. CoAP can be easily translated to HTTP for simplified web integration and it can also provide specialized necessities such as very small overhead, multicast support, and easiness.

2.5 Security Issues

IoT flawlessly joins two distinct worlds into one. There are many limitations and restrictions related to the IoT devices and components, i.e. their computational power and resources and even heterogeneity of devices, which arises new security issues Security challenges of IoT can be divided into two classes: security challenges and technological challenges. Heterogeneity of devices arises

the technological issues whereas security challenges arise due to the principles and functionality that must be followed to establish a secure network. According to the typical architecture of IoT as in Fig. 2.2 some devices or perception sensor is deployed openly where no monitoring system is present [8], which creates vulnerability for outside attackers. Attackers can access these devices and can program them in such a way that these sensors can send data to the register servers as well as to the group of attackers. Secure communication framework for software, processes, things, and people can be developed by following some principles and rules given below.

2.5.1 *Confidentiality*

Data of IoT should be secure and only authorized users should grant access to the data. Users of IoT can be anything it could be, the other network object, human services and machines, or the same network object. IoT sensors should be protected in such a way that they cannot reveal their collected data to other nearby nodes [9]. How the collected data should be managed is also a confidentiality issue that must be tackled. IoT user should be aware of the mechanism of data management that would be applied, and should ensure the protection of the data during the entire process of IoT.

2.5.2 *Heterogeneity*

In IoT there are multiple devices or sensors belonging to different manufacturers and with different abilities based on the complex or simple architecture. The IoT entities also have different versions of their release. They have different technical interfaces and they perform distinct functions, therefore IoT protocols should be designed in such a way that all heterogeneous entities can function together in different situations [10]. The main purpose of IoT is to connect human to device and human to human, in this way it builds a network of heterogeneous things.

2.5.3 *Integrity*

In IoT data is exchanged among many devices and that is why accuracy of data is very important, which means it should be monitored that the data is coming from the right sender and going to the concerned IoT node without any interference either intended or unintended. In IoT communication integrity feature is imposed by maintaining end-to-end security. The endpoints of IoT has very low computational

power, therefore security or cryptography algorithm implementation is difficult on the end nodes of the IoT.

2.5.4 Lightweight Solutions

As the devices of the Iota have very low computational power and lack of memory have lightweight solutions are introduced which have unique security features. These lightweight algorithms execute on IoT devices that have limited capabilities of computation, that's why they should be compatible with devices. In implementation of IoT protocols or authentication of devices, this restriction should be considered.

2.5.5 Authentication

In IoT every entity or node should be able to authenticate other objects and nodes, but this process is not simple as it requires more effort and is quite challenging due to the heterogeneous nature of IoT devices. Sometimes IoT devices have to communicate with other objects for the very first time [11]. Therefore, there is need of a universal authentication mechanism to authenticate the IoT devices in all condition.

2.5.6 Availability

The aim of IoT is to connect everything and to make everything available online. The IoT data should be available to the IoT users at any place and as any time, besides the data of IoT devices should also be accessible or reachable to the IoT users at any time.

2.6 Security Issues in Each Layer of IOT

There are many security threats related to the layers of IoT, each layer is vulnerable to many kinds of security attacks, these attacks can be active or passive and they can be caused by an internal source or external source [12]. Active attack will immediately block the service whereas passive attack can steal information from the IoT network silently without interfering the services. DoS attack can affect at each layer of IoT making the services of the network unavailable. In this section, we will discuss security issues related to each layer of the IoT.

2.6.1 Perception Layer

The most sensitive and attacking layer of IoT is perception layer, the nodes on this layer mostly operate in outdoor environment which makes it most favorite attacking area in IoT network. Wireless technology is used to transmit the signal between the nodes of IoT, therefore its efficiency can be decreased by waves disturbance. Due to the outdoor deployment of the IoT sensors, an attacker can tamper the hardware of the devices. Moreover, the devices on the perception layer consist of sensors, barcode readers, or RFID whose computation capability and power consumption are very low which make them attackable [13]. Spoofing can be used to exploit the confidentiality of this layer which can alternate identity information of IoT devices. Node capture attack can also be made on this layer in which attacker takes over the node and extracts all the information from the node. Nodes can also be replaced by the attacker on this layer.

2.6.2 Network Layer

DoS attacks can be performed easily on the network layer. Passive monitoring and network analyzing is also very common on the network layer [12]. Exchanging data of devices and mechanism of remote access give rise to these types of attacks. If eavesdropper can get the keying material of IoT devices, then secure communication will be conceded. Therefore mechanism of key exchanging should be protected for secure communication of IoT devices. The communication which takes place between the IoT devices is much different from the internet, the reason is that it is not limited to machine to human. Compatibility is the big issue for the security of IoT devices, because of the heterogeneity of the IoT devices currently available protocols cannot be used. Object protection is as important as the protection of the network. Objects should have the ability to defend themselves against any network attack. By developing good protocols this goal can be achieved. The software capabilities should also be increased to make IoT devices strong enough to handle any abnormal situation that can affect their security [14].

2.6.3 Application Layer

There are no global standards and policies for the development of IoT applications, there are many security issues related to the IoT applications. There are many applications and each application has different method of authentication, which makes difficult to ensure the authentication and privacy. The increasing number of connected devices that also share the data will result in an overhead. This overhead will cause an unavailability of the IoT services. During the process of application

development, another issue should also be considered that is who will be the user of the application and how they will interact with the application. There should be some tolls for the users that they can be used to control the data and to decide that what data should be disclosed and who will be the user of data and when they will be using the data.

2.7 Countermeasures for IoT Security

At all three layers of IoT some security measures are required; at physical layer, we need some security measures in data gathering, for transmission and routing on the network layer, and on application layer for maintaining integrity, confidentiality, and authentication [13].

2.7.1 Authentication Measures

In 2011 an authentication scheme was presented by Zhao in [14] for different IoT terminals and nodes. The basic block of the scheme is based on the feature extraction and hashing, for the avoidance of any collision attacks hashing function is combined with feature extraction. There exists irreversibility property in features extraction, this property is also necessary for the insurance of security and it also provides lightweight solution which is required in IoT. This authentication process is implemented when platform wants to transmit the data to any terminal node of IoT. This scheme will also reduce the information that must be sent while improving the security of IoT, but there is no any practical proof in the support of this scheme.

Wen et al. in [11] presented a different method of authentication for sensor node of IoT which is based on ID authentication mechanism. This works on the mechanism of request-reply based on on-time one cipher scheme. The communicating nodes uses a pre-shared matrix to implement this scheme randomly generated coordinate which are generated by nodes are used as a key coordinate. Key itself is not transferred between the parties but the things with that key coordinate are transferred. Then from this coordinate password is generated. This generated password, i.e. key, time stamp, key coordinate and device ID, is used to encrypt all the messages to be sent. Timestamp validation is then used for the communication between the devices, thus on this basis they can also cancel the session. This cipher can also be used in the situation where securing IoT does not involve sensitivity by using same key for different coordinates. For the optimization of security key coordinates can be changed regularly, for a specific structure of IoT. Protecting access controls is also very important for security, it is as important as authentication.

Mahalle addressed these two functionalities in [15]. He presented the idea of Identity Authentication and Capability Access control (IACAC). His research tries

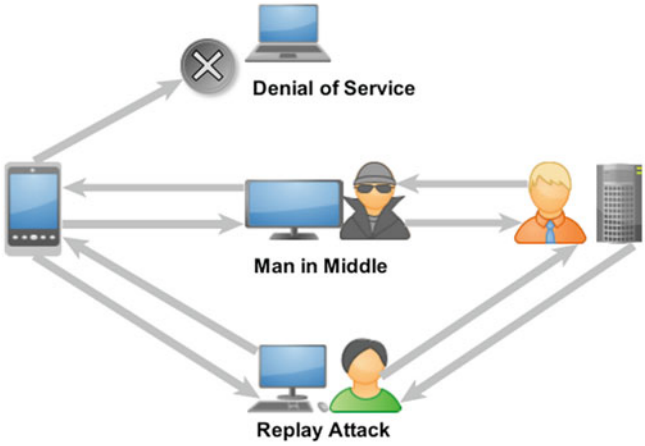


Fig. 2.3 Security attacks modeling of IoT

to achieve the mutual identity establishment in IoT based on both authentication and access control abilities. He proposed a model that uses public key approach which is compatible with distributed, mobile, lightweight, and with the limited computational nature of IoT. Man-in-the-middle attacks are prevented in his technique using a timestamp to authenticate messages between the devices, he called it MAC (Message Authentication Code). Sample use case is shown in Fig. 2.3 [16].

In IOT environment there could be three types of attacks that are Denial of Service, Man in Middle and Reply Attack which is shown in Fig. 2.3.

His scheme is based on three stages; in the first stage, a secrete key is generated, this generated key is based on Elliptical Curve Cryptography-Diffie Hellman algorithm (ECCDH) [16], in the second step identity establishment is taken place by mutual authentication protocols and one-way, at the end implementation of access control is taken place. Public key and private parameter combine to form a shared secret key, and it has low computational overhead due to the use of Elliptic Curve Cryptography (ECC). Using IACAC can minimize significantly because at one time only one ID can have access to the resources.

Perception layer of IoT is mostly based on sensor and RFID. These devices have very limited computational power, therefore on these devices implementation of any cryptography algorithm is very difficult for the network security. For the security of RFID tags, many researchers [17] presented lightweight authentication protocols. If RFID tags are not secured, then attackers can access the network by sniffing (EPC) electronic product key to the target tag and can program it to other tag. By using lightweight authentication protocol these attacks can be prohibited. These protocols ensure the authentication among RFID readers and items that are tagged. Through this mechanism large overhead on these devices is also prevented. A communication scheme is shown in Fig. 2.4 [18] in which RFID tags are to identify the items in IOT environment.

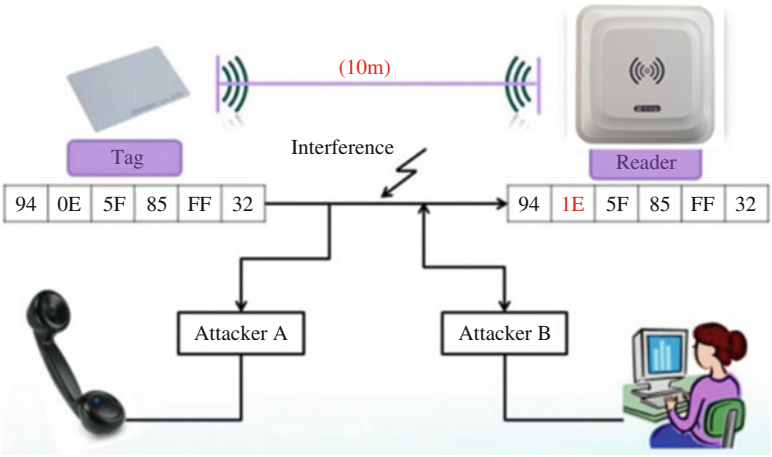


Fig. 2.4 A communication scenario in which RFID tags are used in IoT

2.7.1.1 Digital Certificate

In [19] the authors proposed the method of digital certificate which is attached to the original message to increase the security. A Certificate Authority is responsible for issuing the digital certificate. Certificate Authority verifies the user by giving it a private key. A public key is also announced by the Certificate Authority, it also has its own digital certificate which is known by all the users. This approach is used to eliminate pre-shared key for authentication and introduces digital certificate for the authentication of IOT entities. Figure 2.5 describes the process of issuing the digital certificate to the clients or IOT nodes.

The sequence of operation of the certificate authority is explained with the help of Fig. 2.5 [19].

1. Client requests a source from the server.
2. Server gives its certificate to the client.
3. Certificate contains the digital signature which is signed by Certificate Authority client who also verifies the signature by decrypting it with the CA public key.
4. After verification client also sends his certificate.
5. Digital signature of the client is also verified by the server.
6. After the completion of successful verification server and the client can communicate.

2.7.1.2 Trust Establishment

IoT devices can be moved from one place to the other or the ownership of the devices could be changed, therefore trust establishment is necessary for smooth

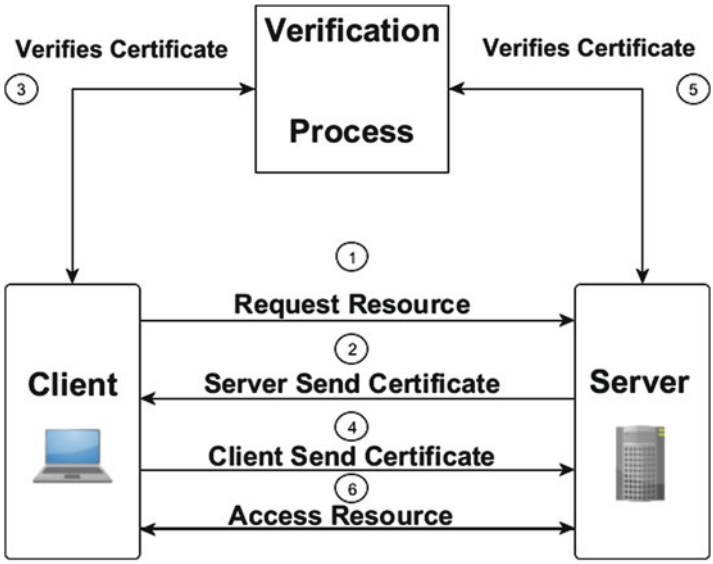


Fig. 2.5 Process of certificate authority

transition w.r.t. permissions and access controls. The concept of mutual interest for inter-system security was presented in [18]. They developed a framework based on the item level access control. In this trust is established in phases from the creation of devices to their operation and transmission. There are two steps in trust establishment; in the first step, the key creation and token. When a device is created, key is assigned to the device. Current owner or the manufacturer can create the token, then these tokens can be used jointly with RFID identification for the Iota devices. Only owner of the device can change these tokens with the condition that the old token is provided. This entire process is much like that, replacing the old key with the new one when new home is bought.

2.7.1.3 Security Awareness

Awareness of the security is very important for the success of IoT framework. Humans which are the part of the IoT network should be aware of security measures. Some researchers in [18] showed the consequences of not securing IoT with actual numbers. They gain access to the various IoT devices, printers, web cameras, etc., these devices were available publicly with no security or they have default access parameters. According to their results many devices were accessible. If in the IoT environment people keep on practicing towards unawareness of the security, by using no security or default security parameters, then the IoT environment will be more harmful than beneficial. If one of the IoT devices is not secured, then hackers can gain access to the whole network through this device.

2.8 Conclusion

Each layer of IoT is susceptible to attacks; therefore, there is need to address security challenges and requirements of IoT framework. For the dynamic mashup of internet of things topology, in the future there is need of new protocols for networking like ipv6 and 5G. Currently, researchers are only focusing on the access control protocols and authentication mechanism of IoT. Currently, the development of IoT is only restricted in small companies and business, for the large-scale development of IoT there is need to overcome many security-related issues of IoT. IoT can transform the way of life we live today. But, in this smart framework security is a big issue. There is high need of new mechanism of identification, software and hardware technology to overcome the security challenges of IoT such as trust management, identification, authentication, privacy, access controls, and confidentiality. If we could address these problems successfully, then soon IoT will transform everything.

References

1. Verizon. (2017). *Intelligent, More Meaningful Business Connections*.
2. Coetzee, L., & Eksteen, J. (2011). The internet of things-promise for the future? An introduction. In *IST-Africa Conference Proceedings, 2011* (pp. 1–9). Piscataway: IEEE.
3. Kraijak, S., & Tuwanut, P. (2015). A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends, 6–6.
4. Zhao, K., & Ge, L. (2013). A survey on the internet of things security. In *2013 9th International Conference on Computational Intelligence and Security (CIS),* (pp. 663–667). Piscataway: IEEE.
5. Mahalle, P. N., Anggorojati, B., Prasad, N. R., & Prasad, R. (2013). Identity authentication and capability based access control (iacac) for the internet of things. *Journal of Cyber Security and Mobility, 1*(4), 309–348.
6. Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I. (2015). Internet of things (IoT) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)* (pp. 336–341). Piscataway: IEEE.
7. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. In *2012 10th International Conference on Frontiers of Information Technology (FIT)* (pp. 257–260). Piscataway: IEEE.
8. Kumar, J. S., & Patel, D. R. (2014). A survey on internet of things: Security and privacy issues. *International Journal of Computer Applications, 90*(11), 20–26.
9. Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks, 57*(10), 2266–2279.
10. Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications, 111*(7), 1–6.
11. Wen, Q., Dong, X., & Zhang, R. (2012). Application of dynamic variable cipher security certificate in internet of things. In *2012 IEEE 2nd International Conference on Cloud Computing and Intelligent Systems (CCIS)* (Vol. 3, pp. 1062–1066). Piscataway: IEEE.
12. Roman, R., Najera, P., & Lopez, J. (2011). Securing the internet of things. *Computer, 44*(9), 51–58.

13. Leo, M., Battisti, F., Carli, M., & Neri, A. (2014). A federated architecture approach for internet of things security. In *Euro Med Telco Conference (EMTC), 2014* (pp. 1–5). Piscataway: IEEE.
14. Zhao, G., Si, X., Wang, J., Long, X., & Hu, T. (2011). A novel mutual authentication scheme for internet of things. In *Proceedings of 2011 International Conference on Modelling, Identification and Control (ICMIC)* (pp. 563–566). Piscataway: IEEE.
15. Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation, 48*(177), 203–209.
16. Lee, J.-Y., Lin, W.-C., & Huang, Y.-H. (2014). A lightweight authentication protocol for internet of things. In *2014 International Symposium on Next-Generation Electronics (ISNE)* (pp. 1–2). Piscataway: IEEE.
17. Xie, Y., & Wang, D. (2014). An item-level access control framework for inter-system security in the internet of things. In *Applied mechanics and materials* (Vol. 548, pp. 1430–1432). Zürich: Trans Tech Publications.
18. Patton, M., Gross, E., Chinn, R., Forbis, S., Walker, L., & Chen, H. (2014). Uninvited connections: A study of vulnerable devices on the internet of things (IoT). In *2014 IEEE Joint Intelligence and Security Informatics Conference (JISIC)* (pp. 232–235). Piscataway: IEEE.
19. Panwar, M., & Kumar, A. (2015). Security for IoT: An effective dtls with public certificates. In *2015 International Conference on Advances in Computer Engineering and Applications (ICACEA)* (pp. 163–166). Piscataway: IEEE.

Chapter 3
A Review of Internet of Things (IoT) Connectivity Techniques

Mudassar Ahmad, Atiab Ishtiaq, Muhammad Asif Habib, and Syed Hassan Ahmed

Abstract The Internet of Things (IoT) is spreading to virtually all everyday objects. Therefore, the best technology must be selected for IoT devices. This paper presents the state of the art of the best IoT connectivity technologies. The paper first discusses basic points like frequency bands, network range, and topologies that are necessary to know for the connection of IoT devices. In addition, the paper discusses basic connectivity technologies like traditional cellular networks, proprietary low-power wide-area (LPWA) technologies, cellular LPWA technologies, and short range technologies, their types, use, and range. When faced with the task of selecting any of these technologies for IoT applications, we need to understand them in all their aspects, which are divided into three main dimensions: ecosystem, technical, and commercial. Some technologies are better suited than others for different dimensions. No single technology is suitable for all purposes.

3.1 Introduction

The Internet of Things (IoT) refers to the idea of the Internet spreading into the real world, taking on everyday objects. In the quickly rising IoT, sensors and applications that are may be single electronics or industrial gears, and all are communicated to the Internet without the use of wires. The extensive range of use cases covers numerous contexts and various requests. There is long list of standards and communication technologies and selecting the most appropriate one is an interesting challenge.

M. Ahmad · A. Ishtiaq · M. A. Habib (✉)
Department of Computer Science, National Textile University, Faisalabad, Pakistan
e-mail: mudassar@ntu.edu.pk; drasif@ntu.edu.pk

S. H. Ahmed
Department of Computer Science, Georgia Southern University, Statesboro, GA, USA
e-mail: sh.ahmed@ieee.org

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_3

I will analyze the main existing commercially available connectivity technologies, discuss important official ideas and manufacturing compromises related to these technologies, and propose strategies for the choice of the correct technologies for diverse fields.

This chapter's goal is to provide an organized method for describing visions about the setting of connectivity technologies, and show how different technologies can best meet the demands in certain areas and use cases. A few terms need to be defined before commencing a discussion of IoT connectivity technologies. Two organizations, the Federal Communications Commission (FCC) and the European Conference of Postal and Telecommunications Administrations (CEPT), regulate radio transmission. The two organizations assign frequency bands for various uses [1, 2].

There are four classes of networks: personal area networks (PANs), local area networks (LANs), neighborhood area networks (NANs), and wide area networks (WANs). PANs are networks that commonly do not use wires and have a range of up to 10 m. A common example of a PAN is a smartphone that is integrated with Bluetooth (e.g., smart watches, headsets). PAN devices use less power and transmit less data. LANs may be wired or wireless and have a range of up to 100 m. For example, a local Wi-Fi network gives Internet access to personal computers, smartphones, and home appliances and thermostats. NANs are wireless and have a range of up to 25 km. They use considerable power but have low data traffic. WANs cover a large area and are a combination of wire and wireless technologies. The different classes of network ranges based on coverage area are shown in Fig. 3.1.

Fig. 3.1 Network range

Fig. 3.2 Star topology

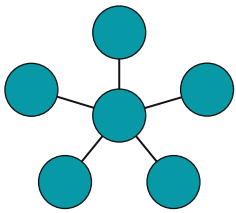
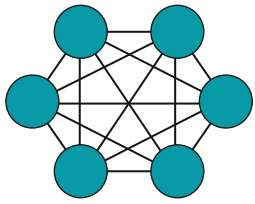


Fig. 3.3 Mesh topology



The way in which nodes are arranged and connected to each other in a network is called the topology. The two popular topologies used in the IoT are star and mesh topologies. Every node is attached to a node that is central in a star topology; for the Internet this central node is used as the gateway [3]. Figure 3.2 shows a star topology, where the central node acts as a gateway and all other nodes attach to this node. A Wi-Fi network is an example of a star topology, and the central node is AP and all remaining nodes are called stations.

All nodes can connect to many other nodes. In mesh topology, the Internet gateway may be one or more nodes. Figure 3.3 shows a mesh topology where all nodes are connected to each other. This topology is simple in real life. ZigBee is an example of a mesh topology. The one ZigBee node is a coordinator; it is an Internet gateway. Designing a mesh network is difficult and may require a long interval to move a message from a distant node in comparison to a star topology. The advantage of this topology is that it can expand the range of a network using low broadcast power. Greater consistency may be achieved by allowing many paths to send a communication in the mesh.

3.2 Description of IoT Technologies

With respect to usage, technologies are divided into four groups. The first group is LPWA networks (LPWAN). The technologies used by operators depend on their requirements. LPWANs can be used in any LTE band together withadditional

LTE services using similar bandwidth. It can be used with already existing LTE base stations but with software updates [4, 5]. A key feature of Narrowband IoT (NB-IoT) is the maintenance of a narrowband of 180 kHz. For uplinks, it supports two modes. It supports one tone with 15 or 3.75 kHz tone spacing [6] and mulitone broadcasts with 15 kHz tone spacing. The main feature of Global System for Mobile Communication (EC-GSM-IoT) is that it contains logical channels to increase coverage [7, 8]. It has other features like up to 52 min extended DSX (Discontinous Reception/Transmission DTx & DRx). It is optimized with the help of system information.

LPWANs are perfect for devices that deliver tiny amounts of data over huge ranges and that have certain restrictions regarding power depletion and power for computation. Numerous technologies are present in LPWANs. Sigfox attaches antennas from a base station on towers and performs operations with the help of local mobile network operators. It maintains communication setups and supports cloud organization policy [9]. The LoRa company has a wider bandwidth than Sigfox. LoRa compares favorably with Sigfox because it uses low amount of energy and is perfect for data transmission at rates of 300 to 5000 bps [10]. LoRa deals with operational bidirectional operations, which is why it is best for receiving and transferring messages. Ingenu is built on random phase multiple access (RPMA) technology, which provide greater data throughput than the two previously mentioned techniques. It transfers data at a rate of hundreds of thousands of bits per second but uses more power than Sigfox and LoRa. Ingenu works in the unlicensed band of 2.4 GHz, and for this reason, it has shorter coverage than Sigfox and LoRa [11, 12].

3.2.1 Traditional Cellular Networks

Traditional cellular networks that are used for IoT connectivity are GSM (2G), UMTS (3G), and LTE (4G). 2G was present in GSM policies. 2G for voice broadcasts utilizes digital signals at speeds up to 64 kbps. It enables short message service and utilizes a bandwidth of 30–200 KHz [13, 14]. As conditions worsen, digital signals completely fail, but analog slowly worsens. IMT-2000 is, widely recognized as the third generation; this generation is ideal for smartphones and broadcastings facilities. 3G utilizes WANs, which improves transparency. Data is transferred via packet switching. Circuit switches are used in voice calling. Besides spoken messages, it contains data facilities that provide access to videos [15, 16]. It functions in the 2100 MHz range, with a bandwidth of 15–20 MHz that is utilized for high-speed Internet service and for video chatting. 4G systems provide voice and other 3G services and in addition an ultra-broadband network for mobile devices [17]. Applications vary depending on the IP telephone. The characteristics of traditional cellular networks are summarized in Table 3.1.

Table 3.1 Characteristics of traditional cellular networks

Characteristics	1G	2G	3G	4G
Period	1980–1990	1990–2000	2000–2010	2010–present
Frequency	Analog signal (30 kHz)	Digital signal (1.8 GHz)	1.6–2.0 GHz	2–8 GHz
Data rate	2 kbps	64 kbps	144 kbps–2 Mbps	100 Mbps–1 Gbps
Technology	Analog cellular	GSM	CDMA,UMTS,EDGE	LTE,Wi-Fi

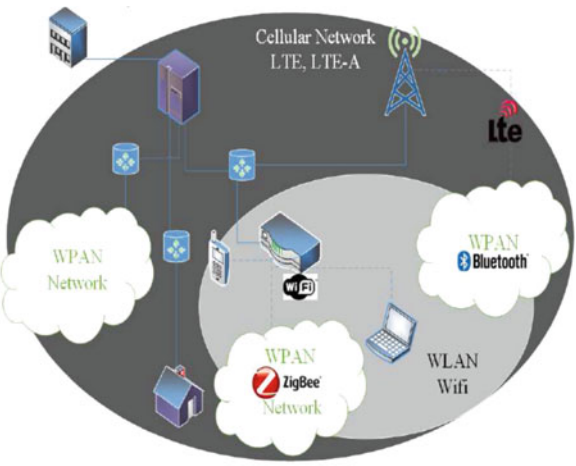


Fig. 3.4 Zigbee

In short-range technologies, Bluetooth, ZigBee, and Wi-Fi are used. Bluetooth indicates an exposed condition. ZigBee Alliance was recognized in August 2001, officially named ZigBee in 2007. ZigBee is a remote network and can be used to establish an IoT sensor network without wires [18]. The topologies of ZigBee networks are mesh, star, and tree, though the star topology is the most common. Topologies like mesh and point-to-point (P2P) can deliver great consistency because they find many paths among nodes [19]. The combination of the star and P2P topologies form the cluster tree network that is used as ZigBee topologies rely on the connectivity of the network. Figure 3.4 shows how connections are established using different technologies.

3.3 Connectivity Technologies with Respect to IoT Launch

The selection of a suitable technology is very important when deploying IoT in business. The main idea of business always lies behind the launching of IoT. This idea varies from business to business. The main vision and objective that an enterprise aims to achieve are increased revenue, made possible by establishing

an improved model of business and increased services for customers, decreasing costs by production processes and supplies. The key task is how to use connected products and data that obtained and send these data to customers and the enterprise. Then the enterprise identifies the requirements of the technologies and selects the most suitable one. Certain components of IoT are necessary to secure end-to-end technologies. These are as follows. Each of these is very important and has its own requirements, but our concern is to identify the suitable technology with respect to its use. In addition, the various actors wish to dominate their respective markets. But certain conditions are not suitable for the long run. Actors may be uncertain about conditions or the future, so they become the first to launch or wait to set standards. This depends on requirements and the environment. Many leaders emerge in their technology, but it is not necessary for one technology to be used in all use cases. Several technologies coexist to complement the standards.

3.4 IoT Connectivity Technologies

In IoT, machine-to-machine communication is done by radio technologies, including ZigBee, Bluetooth, and Wi-Fi in LANs. In WANs traditional cellular networks, GSM (2G), UMTS (3G), and LTE (4G), are used. For consumer voice and data services, many technologies are designed, including Wi-Fi and cellular networks. The aforementioned technologies are too expensive and too remote to connect to new emerging technologies that are recognized for their low power consumption and wide area coverage, the previously mentioned LPWA technologies. These technologies are divided into two main categories. The first is proprietary LPWA, in which Ingenu, Sigfox, and LoRa works on licensed spectrum. The other is cellular LPWA, in which LTECatM1, EC-GSM, NB-IoT works on an licensed spectrum. The second one introduced a new cellular option that was deployed in early 2017. When selecting one of these technologies for IoT applications, it is necessary to understand them from every aspect. Such aspects are divided into three main dimensions: ecosystem, technical, and commercial.

3.5 Considerations in Choosing the Right IoT Connectivity Technologies

The main technical requirements in transitioning to IoT connectivity are coverage, energy efficiency, and data rate. No single technology can fulfill all these requirements. All radio technologies have conflicts in objectives. All IoT applications require good coverage for devices. Some devices need to cover only certain indoor

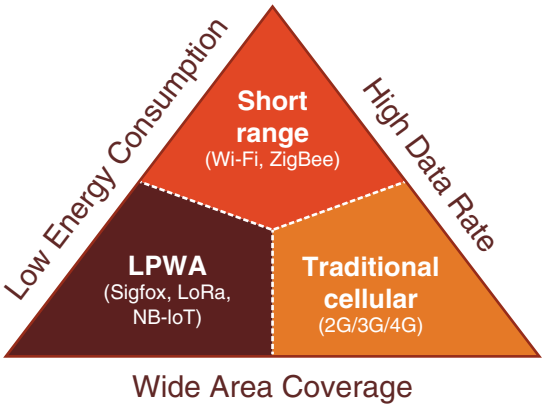


Fig. 3.5 Technical level

areas, while others need wide area coverage for rural or remote areas. A technology that has long coverage is suitable for wide areas. Cellular networks like 3G and 4G are suitable for wide area coverage. Data rate requirements in IoT vary from hundreds of bits to thousands of bits. Wi-Fi and cellular networks to support high data rate use large bandwidth with adaptive modulation,but more power is consumed or they have a shorter range. However, LPWANs have a low data rate and consume less power. Figure 3.5 shows that short-range technologies like Wi-Fi, ZigBee, and traditional cellular networks have high data rates. LPWANs like NB-IoT and traditional cellular networks have wide area coverage. Thus, LPWANs has wide coverage and low energy consumption.

By understanding the technical requirements we take the first step in selecting the right IoT connectivity technology. The IoT business model cost, scalability, and quality of assurance will dictate the choice of IoT connectivity technology [20]. The cost of IoT connectivity depends on the module and connection costs. The IoT connectivity module is the main component of IoT devices. The cost of an IoT module depends on the complexity of the technology. For LTE modules with expensive hardware, IP fees range from USD 30 to 50. For LPWA modules it is approximately USD 5. It is expected that the LPWA price will decrease further because it is being deployed at an increasing rate. As Fig. 3.6 shows, a cellular network has high Quality of Service (QoS) and security and good scalability at a high cost. Private networks like Wi-Fi and LoRA have high QoS and security and low cost but scalability is not good. Pubic proprietary networks have good scalability at a low cost but cause QoS and security issues.

Beyond the economic and technical requirements, it is very important that the technology one chooses will fit in with the healthy ecosystem and have long life and deliver economies of scale. A technology's long life is a key consideration for IoT applications with logistical and cost challenges associated with the replacement of the deployed devices. Understanding the goals of investors and the technology can

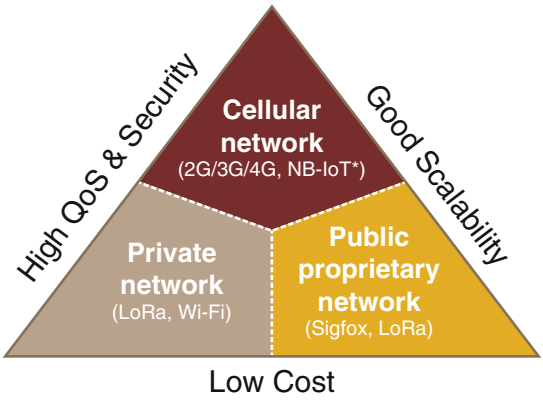


Fig. 3.6 Commercial level

help one to guess the future direction of the technology's development. For example, Ingenu and Sigfox are startups financed by risk capital, whose commitment and ability to provide long-term service have yet to be time tested. Also, a common open method accepted by the likes of LoRa assures better sustainability than technologies with closed systems. The latter poses a risk for single point of failure while the first creates opportunities for multiple service providers and dealers.

3.6 Assessment of IoT Technologies

No single technology is best in all circumstances. For IoT in wide areas, LoRA and NB-IoT are good [6]. Proprietary technologies like Sigfox is best among those. For high data rate Wi-Fi is a good option. Figure 3.7 shows the strengths and weaknesses of the three main technologies. This will help us to decide which technology is suitable for different systems.

Table 3.2 also helps in the selection of the best IoT connectivity technologies on the basis of considerations. Different technologies meet different requirements.

3.7 Challenges of IoT Connectivity

When connecting IoT devices, reliable signaling at both ends is compulsory for collecting and routing data between devices [21]. For the collection of data, devices connect to a server or vice versa. Data need to travel from one point to another quickly and reliably. Data streams must always be able to reach their destinations. Security is a huge issue and important in IoT connectivity. In a smart house, when

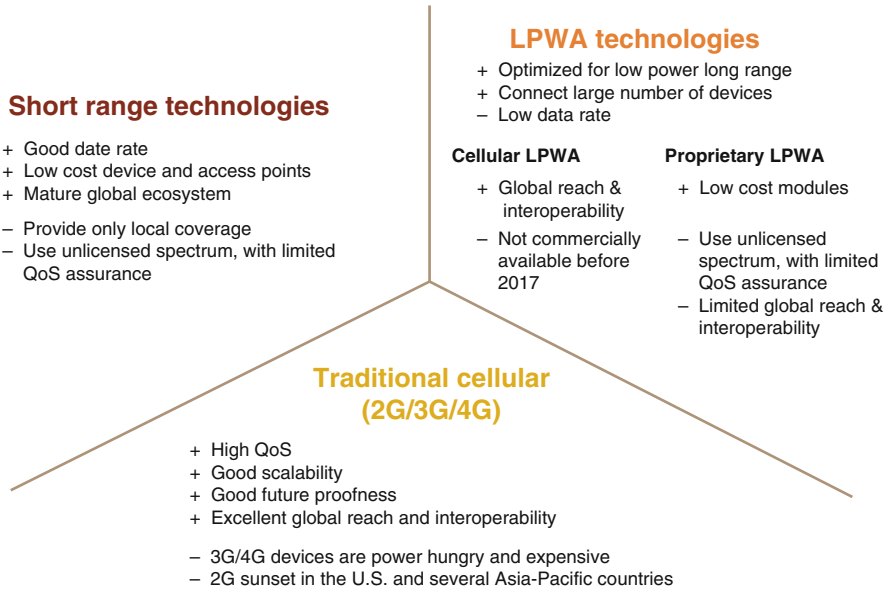


Fig. 3.7 Strengths and weaknesses of technologies

someone unlocks a door, authorization is required: when communication needs to occur between sender and receiver, both must be authorized to send and receive data streams. Open ports: IoT devices are dangerous when accessing the Internet externally through an open port. Communication must not occur outside the port.

3.8 Conclusion

Many different IoT connectivity technologies exist. Every technology has its advantages and disadvantages, and none is perfect. An issue that must be resolved has to do with which technology is the best for a particular application. In this connection, different IoT connectivity technologies belonging to traditional cellular networks, proprietary LPWANs, cellular LPWANs, and short-range groups were discussed. With respect to the presented analysis, LoRa and NB-IoT represent a good balance for wide and remote areas. LoRa is perfect for private networks with a modified arrangement, whereas NB-IoT is supported by key mobile operators offering uniform connectivity with worldwide reach. LTE, Wi-Fi, and Bluetooth Low Energy (BLE) are suitable for high data rates.

Table 3.2 Considerations of IoT technologies

Consideration	2G	3G	4G	LTE-CatM1	EC-GSM	NB-IoT	Sigfox	LoRa	Ingenu	Wi-Fi	ZigBee	Bluetooth
Outdoor coverage	>10 km	>10 km	>10 km	>10 km	>15 km	>15 km	>15 km	>10 km	>15 km	<1 km	<300 m	<100 m
Indoor coverage	High	Medium	Medium	Medium	High	High	High	High	Very low	Very high	Medium	Low
Mobility	Very high	Very high	Very high	Very high	High	High	Very low	Low	Medium	Medium	Low	Very low
Localization	Yes	Yes	Yes	Yes	Yes	n/a	No	Limited accuracy	n/a	Yes	Yes	Yes
Scalability	High	High	High	High	Very high	Very high	High	High	High	Low	Low	Very low

References

1. Reiter, G. (2014). *Wireless Connectivity for the Internet of Things*. Texas Instrument White Paper.
2. Tausif, M., Ferzund, J., & Jabbar S. (2014). Emergence of internet of things in current technological era: Multifaceted analysis and future considerations. *Journal of Platform Technology, 2*(3).
3. Mehravari, N. (1990). Performance and protocol improvements for very high speed optical fiber local area networks using a passive star topology. *Journal of Lightwave Technology, 8*(4), 520–530.
4. Rico-Alvarino, A., Vajapeyam, M., Xu, H., Wang, X., Blankenship, Y., Bergman, J., et al. (2016). An overview of 3GPP enhancements on machine to machine communications. *IEEE Communications Magazine, 54*(6), 14–21.
5. Paul, A., Ahmad, A., Mazhar Rathore, M., & Jabbar, S. (2016). SmartBuddy: Defining human behaviors using big data analytics in social internet of things. *IEEE Wireless Communications, 23*(5), 68–74.
6. Eric Wang, Y.-P., Lin, X., Adhikary, A., Grvlen, A., Sui, Y., Blankenship, Y., et al. (2016). A primer on 3GPP narrowband internet of things (NB-IoT). Preprint. arXiv:1606.04171.
7. Flore, D. (2016). LTE evolution and 5G. In *CEPT ECC Seminar on 5G, Mainz, Germany*.
8. Raza, N., Jabbar, S., Han, J., & Han, K. (2018). Social vehicle-to-everything (V2X) communication model for intelligent transportation systems based on 5G scenario. In *Proceedings of the 2nd International Conference on Future Networks and Distributed Systems*. New York: ACM.
9. Centenaro, M., Vangelista, L., Zanella, A., & Zorzi, M. (2016). Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios. *IEEE Wireless Communications, 23*(5), 60–67.
10. Vangelista, L., Zanella, A., & Zorzi, M. (2015). Long-range IoT technologies: The dawn of lora. In *Future access enablers of ubiquitous and intelligent infrastructures* (pp. 51–58). Berlin: Springer.
11. Dhillon, H. S., Huang, H., & Viswanathan, H. (2017). Wide-area wireless communication challenges for the internet of things. *IEEE Communications Magazine, 55*(2), 168–174.
12. Khan, M., Din, S., Jabbar, S., Gohar, M., Ghayvat, H., & Mukhopadhyay, S. C. (2016). Context-aware low power intelligent smart home based on internet of things. *Computers and Electrical Engineering, 52*, 208–222. https://doi.org/10.1016/j.compeleceng.2016.04.014
13. Gyrard, A., Bonnet, C., & Boudaoud, K. (2014). An ontology-based approach for helping to secure the ETSI machine-to-machine architecture. In *2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom), and IEEE Cyber, Physical and Social Computing (CPSCom)* (pp. 109–116). Piscataway: IEEE.
14. Ahmed, G., Ul Islam, S., Shahid, M., & Akhunzada, A. (2018). Rigorous analysis and evaluation of specific absorption rate (SAR) for mobile multimedia healthcare. *IEEE Access, 6*, 29602–29610.
15. Speth, M., Dawid, H., & Gersemsky, F. (2008). Design & verification challenges for 3G/3.5G/4G wireless baseband MPSoCs. In *MPSoC08*.
16. Iqbal, M. M., & Mehmood, M.T. (2018). An enhanced framework for multimedia data: Green transmission and portrayal for smart traffic system. *Computers & Electrical Engineering, 67*, 291–308.
17. Himayat, N., Talwar, S., Rao, A., & Soni, R. (2010). Interference management for 4G cellular standards [WIMAX/LTE update]. *IEEE Communications Magazine, 48*(8), 86–92.
18. Somani, N. A., & Patel, Y. (2012). Zigbee: A low power wireless technology for industrial applications. *International Journal of Control Theory and Computer Modelling (IJCTCM), 2*, 27–33.

19. Zhu, Q., Wang, R., Chen, Q., Liu, Y., & Qin, W. (2010). IoT gateway: Bridgingwireless sensor networks into internet of things. In *2010 IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC)* (pp. 347–352). Piscataway: IEEE.
20. Northstream. (2016). *Northstream-Connectivity-Technologies-for-IoT-Full-Report-1*.
21. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. In *2012 10th International Conference on Frontiers of Information Technology (FIT)* (pp. 257–260). Piscataway: IEEE.

Chapter 4
An Evolutionary Game-Based Mechanism for Unwanted Traffic Control

Jia Liu, Mingchu Li, Zitong Feng, Cheng Guo, Lifeng Yuan, and Muhammad Alam

Abstract With the development of Internet technology and the pervasive use of internet service providers (ISPs), internet users have reached an unprecedented volume. However, the existence of some malicious users seriously undermine the environment of the network by distributing a large amount of unwanted traffic, such as spam, pop-up, and malwares, which can be identified with the cooperation of individual users by installing anti-virus toolkits. In our paper, we propose an evolutionary game theoretic incentive mechanism to promote the cooperation of individual users to curb the expansion of unwanted traffic. Considering the hierarchical nature of real-world management, we model our framework as hierarchical incentive mechanism and combine reward with punishment mechanism to further incentivize cooperative behavior. Meanwhile, the acceptance condition of our framework is analyzed and we carry out a number of simulations to analyze the acceptance conditions of our framework.

J. Liu · M. Li · C. Guo
School of Software Engineering, Dalian University of Technology, Dalian, China
e-mail: mingchul@dlut.edu.cn; guocheng@dlut.edu.cn

Z. Feng
College of Electronics and Information Engineering Technology, Sichuan University, Chengdu, China

L. Yuan (✉)
School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China
e-mail: yuanlifeng@hdu.edu.cn

M. Alam
Department of Computer Science and Software Engineering, Xi'an Jiaotong-Liverpool University, Suzhou, Jiangsu Province, China
e-mail: alam@ua.pt

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_4

4.1 Introduction

In recent years, Internet has been widely used all around the world and many applications have been developed. Particularly, information sharing networks and social networks have become indispensable for daily life. However, the malicious usage of the Internet, such as spam, ad pop-ups, and plug-in software, caused an amount of unwanted traffic. Thus, how to control unwanted traffic and keep the Internet environment clean is a hot research topic.

An efficient method to solve the above problem is to require all users to install various softwares such as anti-virus tool kits. However, users need to buy those software or spare some memory. As a network entity's benefit of installing virus softwares will be shared by all, many users like to share others' software but not buy their own softwares, which leads to a social dilemma. Thus, many researchers are becoming engaged in developing incentive mechanisms to solve the dilemma [6, 7, 10, 11, 13–16].

The development of internet services bring great convenience to people's daily life. However, the existence of malicious users seriously undermines normal users' use of the Internet by hacking some individuals and distributing unwanted traffic. To tackle this problem, Al-Duwairi et al. [1], Chen et al. [3], Jan et al. [5], and Singh et al. [9] developed various security techniques and tools to combat unwanted traffic. However, those new techniques have some problems. First is that once the malicious users obtain the knowledge of new techniques, they develop new counter measures and flood the network and evolve to be more hidden and diversified and distribute unwanted traffic continuously. Second is that some users are reluctant to update their unwanted traffic (UWT) softwares. The reasons may be that learning cost is incurred with this, or if they use public devices, or if they perceive that their doing so will not bring them with direct benefit.

Some researchers adopt trust management to solve this problems. Yan et al. [14] first proposed a more general UTC method based on global trust management (GTM), and Yan et al. [15] also extend their work by introducing a hybrid trust management (HTM) to control UWT in both distributed and centralized manner. In this HTM system, not only global trust operators (GTO) and ISPs are able to detect UWT, host itself is capable of blocking traffic targeting on itself based on local traffic and behavior analysis. After this, Yan et al. [16] proposed a personalized UTC mechanism that can differentiate unwanted traffic preferences as the definition of unwanted traffic is rather subjective. Simulations show that this generic trust management-based UTC solution is robust against a number of system attacks. Although the above proposed GTM system is to some extent effective, whether ISPs and hosts are willing to adopt it or not is not very clear.

In this paper, we apply a reward and punishment incentive mechanism based on evolutionary game theory to find a way to curb the abuse of internet.

4.2 System Model

4.2.1 Incentive Mechanism Model

In this paper, we consider a network $N = (H, I)$, of which H represents the host set, I represents the set of ISPs. We assume that the number of hosts is n, and the number of ISPs is m. The network N controls unwanted traffic by the adaptation of our reward and punishment-based incentive system, and we introduce central manager (CM) to managing ISPs.

The procedure of our reward and punishment-based incentive mechanism is shown as follows:

1. If a host detects unwanted traffic from other hosts, it will send a detection report to its ISP.
2. ISPs collect and analyze the reports. If the reported unwanted traffic source host is within its subnet, the ISP will monitor the targeted host to check whether the host deliberately send out unwanted traffic. If the reported unwanted traffic source is outside its registration, the ISP will forward the report to CM to ask remote ISP to further verify the report.
3. CM collects reports and evaluates the behavior of each entity to reward or punish it. Through this, CM is able to detect malicious traffic source and add to a black list.
4. CM sends the blacklist to ISPs to control unwanted traffic.

4.2.2 Economic Model

In this section, we set up an economic model to compute the utility of hosts and ISPs. In our model, a host needs to pay p_a to its ISP as internet access fee, and c_s is the cost for installing unwanted traffic control toolbox and sending detection report to its ISP. On the other hand, hosts benefit from access to the internet, the benefit set of hosts is defined as $\mathbf{v} = \{v_1, v_2, \ldots, v_k\}$, where v_k denotes the benefit of host k by accessing the Internet. Therefore, the utility of host k can be written as:

$$u_k^t = \begin{cases} v_k(t) - p_a(t) - c_s(t) & \text{if host } k \text{ cooperate} \\ v_k(t) - p_a(t) & \text{if host } k \text{ defect} \end{cases} \tag{4.1}$$

wherein u_k^t is host k's utility at time t, $p_a(t)$ is subscriber fee of each host at time t. For an ISP, its revenue comes from the subscriber fees of fellow hosts, possible future subscriber fees incurred by sound network environment, and management expense including reward and punishment. Therefore, the utility of ISP_i can be written as:

$$U_i^t = \begin{cases} n(t)p_a(t) - m_1(t) - m_2(t) + p(t) - F & \text{if ISP}_i \text{ cooperate} \\ n(t)p_a(t) - F & \text{if ISP}_i \text{ defect} \end{cases} \tag{4.2}$$

where $n(t)$ denotes the number of hosts belonging to ISP i at time t, $p_a(t)$ denotes subscriber fees of each host, $m_1(t)$ and $m_2(t)$ denote reward expense for cooperative hosts such as cooperators and rational cooperators (RCs), respectively, $p(t)$ denotes the punishment cost for uncooperative ISPs, and $p(t) = \alpha c b_2 x_2(t) N$ and F denotes the fixed operating cost for ISPs.

4.2.3 Assumptions

1. Identity assumption: We assume that every UWT resource can be detected by IP address prefix or NAT, and unwanted traffic content can be recognized based on Hash Code.
2. Traffic assumption: We assume that unwanted traffic comes from hosts and can be sent out through its ISP.
3. Detection assumption: We assume that unwanted traffic can be detected manually or automatically by installed toolbox.
4. Privacy assumption: We assume that privacy is managed by our incentive mechanism system and ISP and CM report won't be disclosed for the public. Therefore, positively reporting unwanted traffic won't leak their information and cause damage to any network entity.
5. ISP assumption: We assume ISPs are honest and won't spread unwanted traffic for others, although some ISPs may not be cooperative in protecting network environment.
6. Damage assumption: We assume that unwanted traffic only cause damage to received hosts and related ISPs.
7. Rational cooperator assumption: We assume that rational cooperators (RC) are responsible and can actively enquire from ISPs about the network situation. If there are enough cooperators, they will choose temporary defect to save cost, and if there are not enough cooperators, they will cooperate to protect the network.
8. Interaction assumption: We assume that hosts are well-mixed and interact constantly with each other.

4.3 Public-Goods-Based Evolution Game

As we mentioned before, the performance of our mechanism depends on the contribution of every network entity. However, as some entities are selfish and are unwilling to cooperate, this will lead to social dilemma. In order to analyze the solution to this social dilemma and the performance of our mechanism, we use

public goods game to model the network environment and treat this as public goods. In our game, time is divided into slots and the game can be run many rounds. We define the network environment quality Q as:

$$Q = \begin{cases} 1 \text{ if } x_c \geq \beta \\ 0 \text{ if } x_c < \beta \end{cases} \tag{4.3}$$

For easy of reference, Table 4.1 summarizes the notations used in public-goods-based EGT game and evaluation.

4.3.1 Hosts Utility and Strategy

With the wide use and development of internet, internet users benefit from it in various kinds of ways. Therefore, we assume the utility of each host $v_k(t) - p_a(t) > 0$. For simplification, we set $p_a(t)$ of each host as the same value, and $p_a(t)$ is rather small compared with other parameters and the Internet can be accessed at very low cost, we set $p_a(t) = 20$. The mainstream internet attack is DDoS attacks in which hackers exploit botnets to provide service to malicious users to spread unwanted traffic. Without effective anti-virus toolbox, hosts will get intruded easily and become malicious nodes that spread unwanted traffic to the whole network. Additional unwanted traffic sources are from reflection attack. Normally, the owners of the hosts will not take measures until they are seriously impacted. This can help reduce cost in terms of installing toolboxes. But the majority users of the internet will be influenced by a huge amount of unwanted traffic, which will lower the quality of internet environment. Therefore, a responsible host should try to avoid control of hackers. However, selfish users that only consider the benefit of themselves will lead to social dilemma among hosts.

For a host, he or she selects strategy from strategy set $A_H = \{H_C, H_U\}$, of which H_C represents cooperate and H_U represents defect. In our mechanism, detection reports are collected from every host in every time slot. A cooperative host has the newest installed anti-virus toolbox and sends effective report, while an uncooperative host does not update toolbox or even does not have toolbox and will not send any report. If an uncooperative host is intruded successfully and become a compromised host, it will send false report or hide detection report.

Because anti-virus toolbox never stop updating, the newest toolbox always performs best, and if the toolbox is not updated it will be unable to resist new viruses. That is, in every time slot, the host has to choose whether to update anti-virus toolbox or not, as hackers are always changing and updating their attacking method.

4.3.1.1 Two-Strategy Evolutionary Game Without Incentive Mechanism

First, we only consider two pure strategies, i.e., cooperate and defect. This situation is the simplest and has been adopted by many researchers. When there are only cooperators and defectors, we denote $\mathbf{x} = \{x_1(t), x_2(t)\}$ the population structure of one ISP, of which $x_i(t)$ is the fraction of nodes adopting strategy i, and $i = 1, i = 2$ represent cooperative strategy and defective strategy, respectively. And the utility of cooperators will be $u_h^c(t) = v_k(t) - p_a(t) - c_s(t) - kx_d(t)$, where $x_d(t)$ is the fraction of defective nodes which in this case, $x_d(t) = x_2(t)$ and k is the parameter to control the influence of the fraction of defectors. And the utility of defectors will be $u_h^d(t) = v_k(t) - p_a(t) - kx_d(t)$, where $v_k(t)$ denotes the benefit of host k from the internet usage at time t and $p_a(t)$ is the access fee of a host to the internet at time t. It can be deducted easily that the utility of defectors is greater than that of cooperators. Therefore, the fitness of defectors will always be higher than cooperators. Gradually, the whole network will collapse because of the spreading of defectors.

4.3.1.2 Three-Strategy Evolutionary Game Without Incentive Mechanism

Second, we consider the case when there are RCs. It is common in some populations that some individuals do not always cooperate blindly or they just cooperate on certain condition [12]. In our work, since the network environment is shared by all hosts equally, and some hosts can enquire from its ISPs about the whole network situation, they can make wiser choices. When RC nodes are added into the network, they will select their behaviors based on the fraction of cooperators, i.e., if there are not enough cooperators, RC will cooperate to guarantee a sound network environment. However, when there are enough cooperators, they will defect. We set a threshold β to denote the minimum fraction of cooperative nodes needed to keep the network effective and define $x_3(t)$ as the fraction of RCs. Therefore, RC will cooperate with probability $x_{r,c}$ and defect with probability $1 - x_{r,c}$, of which

$$x_{r,c} = \begin{cases} 0 & \text{if } x_1 > \beta \\ \frac{\beta - x_1}{x_3} & \text{if } x_1 < \beta, x_1 + x_3 > \beta \\ 1 & \text{if } x_1 + x_3 < \beta \end{cases} \tag{4.4}$$

Thus, when $x_1 + x_3 < \beta$, RC will cooperate with probability 1, and if $x_1 > \beta$, RC will cooperate with probability 0.

Therefore, the cooperative fraction of the whole system is $x_c = x_1 + x_3 x_{r,c}$, i.e.,

$$x_c = \begin{cases} x_1 & \text{if } x_1 > \beta \\ x_1 + x_3 & \text{if } x_1 + x_3 < \beta \\ \beta & \text{if else} \end{cases} \tag{4.5}$$

and defective probability is $1 - x_c$. Also, RCs have to pay a small amount of enquiring cost r to obtain the fraction of different kinds of nodes from its ISP. For notational convenience, we further denote $\bar{u}_i$ as the average utility gained by nodes adopting the ith strategy.

Thus we update utility of the three types of nodes

$$\bar{u}_1 = v_k - c_s - kx_d$$

$$\bar{u}_2 = v_k - kx_d$$

$$\bar{u}_3 = \begin{cases} v_k - r - kx_d & \text{if } x_1 > \beta \\ v_k - c_s - r - kx_d & \text{if } x_1 + x_3 < \beta \\ (v_k - c_s)r_c + v_k r_d - r - kx_d & \text{if else} \end{cases} \tag{4.6}$$

where $r_c = \frac{\beta - x_1}{x_3}$, $r_d = 1 - \frac{\beta - x_1}{x_3}$. However, in real practice, when nodes or individuals are not totally anonymous, there exists personal loss when one get intruded, so we introduce personal loss cb_1 to defectors and RC hosts. The probability of being attacked is α. It is also worth noting that when the network is truly anonymous and one can enter or leave the network freely without any cost encountered, rational defectors will leave its current ISP to escape punishment, in which case $cb_1 = 0$. Then we update utility function as follows:

$$\bar{u}_2 = v_k - \alpha cb_1 - kx_d$$

$$\bar{u}_3 = \begin{cases} v_k - r - kx_d & \text{if } x_1 > \beta \\ v_k - c_s - r - kx_d & \text{if } x_1 + x_3 < \beta \\ (v_k - c_s)r_c + (v_k - \alpha cb_1)r_d - r - kx_d & \text{if else} \end{cases} \tag{4.7}$$

4.3.1.3 Three-Strategy Evolutionary Game with Punishment

Further, to incentivize nodes not to defect, we introduce punishment mechanism to those who defect. Long before the evolution of human populations, most species developed punishment mechanism to help deter those who are disobedient. In the whole process of human evolutionary history, the motivation to avoid punishment is strong and long-standing [8]. Thus, we also introduce this punishment mechanism to penalize those who defect. In our mechanism, defectors will be punished by cb_2 when they lead to the collapse of the system:

$$\bar{u}_2 = v_k - \alpha(cb_1 + cb_2) - kx_{d'}$$

$$\bar{u}_3 = \begin{cases} v_k - r - \alpha c b_1 - k x_{d'} & \text{if } x_1 > \beta \\ v_k - c_s - r - k x_{d'} & \text{if } x_1 + x_3 < \beta \\ (v_k - c_s) r_c + (v_k - \alpha c b_1) r_d - r - k x_{d'} & \text{if else} \end{cases} \tag{4.8}$$

In our work, we use learning mechanism and assume that each node can change its strategy with certain probability. We adopt the replicator equation of the following:

$$x_i(t+1) = x_i(t) + \delta x_i(t)(\bar{U}_i(t) - \bar{U}(t)),\ i \in \{1, 2, 3\}$$

We can see clearly from the comparing between mechanism with and without punishment that without punishment, the convergence rate to Nash Equilibrium is slower.

4.3.1.4 Three-Strategy Evolutionary Game with Punishment and Rewarding

Fourth, to further promote cooperative behaviors, we can also combine punishing mechanism with rewarding mechanism and give cooperators more incentive and advantage.

In our model, we adopt a fixed amount reward mechanism to resemble real life practice. As cooperators are critical to the well-being of the network environment, the initial cooperators are more important for the system because they can lead others to imitate their strategy. We assume the system set aside m_1 to reward cooperators, i.e., each cooperator can get $\frac{m_1}{x_1 N}$ reward, which implies that when there are only a few cooperators, they can get lots of benefits and increase their fitness to a large extent. Then the fraction of cooperators can increase. This mechanism works well when the initial fraction of cooperators is small. Thus we update the utility of the three strategies as follows:

$$\bar{u}_1 = v_k - c_s + \frac{m_1}{x_1 N} - k x_d$$

We also set aside an amount of $\frac{m_2}{x_3 N}$ to reward RCs. The utility functions will be like the follows:

$$\bar{u}_3 = \begin{cases} v_k - r - \alpha c b_1 - k x_d & \text{if } x_1 > \beta \\ v_k - c_s - r + \frac{m_2}{x_3 N} - k x_d & \text{if } x_1 + x_3 < \beta \\ (v_k - c_s) r_c + (v_k - \alpha c b_1) r_d - r + \frac{m_2}{x_3 N} - k x_d & \text{if else} \end{cases} \tag{4.9}$$

4.3.2 ISP Utility and Strategy

For an ISP, its revenue comes from the subscriber fee of fellow hosts, possible future subscriber fee incurred by sound network environment, and management expense including reward and punishment. we can model the utility of ISP as follows:

$$U_i^t = n(t)p_a(t) - m_1(t) - m_2(t) + p(t) - F$$

where $p_a(t)$ denotes subscriber fees of each host, $m_1(t)$ and $m_2(t)$ denote reward expense for cooperators and RCs, respectively, $p(t)$ denotes the punishment profit for ISPs, and $p(t) = \alpha cb_2 x_2(t)N$ and F denotes the fixed operating cost for ISPs.

Thus, if a ISP does not want to implement this incentive mechanism, its utility function will be:

$$U_i^t = n(t)p_a(t) - F$$

We can see from the above analysis, when an ISP cooperate and implement our reward and punishment mechanism, it will experience some loss in terms of hosts management, therefore, in closed boundary ISP system, wherein hosts are forced to stay in the system and pay subscriber fee, a rational ISP will not adopt the reward and punishment mechanism. However, for open boundary ISP system, the invest of incentive mechanism can improve x_c, attracting more hosts to join the system, i.e., increase $n(t)$, thus bring in more future revenue. As cooperative and uncooperative ISPs both exist in the network, the existence of uncooperative ISPs may shelter defective hosts and degrade network environment, some hosts may switch to other ISPs to escape punishment. Therefore, whether our incentive mechanism brings benefit to an ISP is not absolute and we will not analyze this open boundary situation but leave this in future work. For closed boundary network, i.e., a host cannot switch to other ISPs, the condition for ISPs adopt our incentive mechanism is $p(t) - m_1(t) - m_2(t) > 0$. And for open boundary network, where a host can switch to other ISPs, the condition is more complex, and we will show this using simulation. For different ISPs, it may choose different m_1, m_2 value or cb_2. We will analyze this in the following section.

4.4 Evolution Analysis

Let us now analyze the robustness and effectiveness of our incentive mechanism under CBLM (Current Best Learning Mechanism) learning model.

4.4.1 Evolutionary Analysis Under CBLM

In this part, to thoroughly explore the evolution of our incentive mechanism under Current Best Learning Mechanism, we classify our system statuses into nine cases. Of which, $x_3 = 0$, $x_2 = 0$, $x_1 = 0$, $x_1, x_2, x_3 \geq 0$ are conditions for case1, case2, case3, and case4 respectively, with 1, 3, 2, and 3 subcases in each case. The incentive mechanism is robust if the cooperative players can finally survive in the system. And the effectiveness of the incentive mechanism means the system can finally stay at a satisfactory cooperation level. To find the best performance strategy, we now consider their performance differences respectively and the expected utility of each strategy.

We take case1 as an example to illustrate our way of analyzing evolutionary process of the population. In case1, there are no RC, i.e., $x_3 = 0$, indicating there are only cooperators and defectors exist in the system and the ISP is cooperative, and the compromised hosts can be easily detected as unwanted traffic sources and be punished accordingly, the population dynamics will evolve in the direction of making cooperators and defectors equally beneficial [2, 4], i.e.,

$$\bar{u}_1(t) - \bar{u}_2(t) = \alpha(cb_1 + cb_2) - c_s + \frac{m_1}{x_1 N} = 0$$

Thus no matter what is the initial fraction of cooperators, as long as $x_1(0) > 0$, cooperators will stabilize at

$$x_1^{1*} = \frac{m_1}{(c_s - \alpha(cb_1 + cb_2))N}$$

Note: in the following, we use superscript $x_i^{casenumber*}$ to denote the fraction of type i player in ESS.

If ISP is cooperative, as we mentioned above, it will apply reward on cooperators and punishment on defectors. With the help of cooperator's report, and its own monitoring, ISP will be able to find out unwanted traffic sources and control them effectively, thus reducing unwanted traffic to a large extent. With enough hosts cooperating, hosts reports will be more reliable and the probability of being used as unwanted sources will be reduced dramatically. Based on the above analysis, we can see the without the protection of rational reciprocator cooperator's fraction depends purely on rewarding, punishing, and cooperation cost, implying the effectiveness of our reward, and punishment mechanism depends on rewarding, punishing, and cooperation cost in this case.

We analyze other cases in the same way and get similar results. The philosophy implications behind our work are twofold: first, like many incentive mechanisms in our society, it is difficult or even impossible for them to be perfect, but they still work with acceptable efficiency; second, reward and punishment should be implemented properly to control unwanted traffic.

4.4.2 *Impact of m_1 and m_2*

In this part, we analyze the impact of m_1 and m_2 to the efficiency of our incentive mechanism. From the above analysis, we can see that with the increasing of m_1 and m_2, hosts' utility will increase and cooperators fraction reaches a higher level, resulting in lower probability of being compromised and being used to distribute unwanted traffic. However, the utility of ISPs should also be taken into consideration for the long-term well-being of the network and they also operate for profits. Thus, we would rather find out the optimal value of m_1 and m_2 to get maximal social welfare of both hosts and ISPs. As analyzed before, we analyze the effect of m_1 and m_2 in nine cases.

Still, we take case1 as an example to calculate the critical value of m_1. Likewise, the critical value of m_2 can be obtained in the same way. In case1, there are no RRs, i.e., $x_3 = 0$, and ISP is cooperative, the compromised hosts can be easily detected as unwanted traffic sources and be punished and restricted accordingly. We can obtain the critical value of m_1 for cooperators dominate defectors by solving

$$\bar{u}_1(t) - \bar{u}_2(t) = \alpha(cb_1 + cb_2) - c_s + \frac{m_1}{x_1 N} = 0$$

Thus no matter the initial fraction of cooperators, i.e., $x_1(0) > 0$, if $\bar{u}_1(t) - \bar{u}_2(t) = 0$, $m_1^{1*} = x_1(c_s - \alpha(cb_1 + cb_2))N$. (we use superscript $k*$ to denote the critical value of m_i in case k). Thus, if we want to achieve $x_1 \geq \beta$, we should satisfy $m_1 \geq \beta(c_s - \alpha(cb_1 + cb_2))N$. This illustrates that to motivate hosts to adopt UTC toolkits, its ISP should distribute at least $\beta(c_s - \alpha(cb_1 + cb_2))N$ benefit to cooperators. The contribution of the ISP to dealing with unwanted traffic will be ruined if $m_1 \leq \beta(c_s - \alpha(cb_1 + cb_2))N$.

We analyze other cases in the same way and get similar results. To motivate enough hosts to adopt cooperative strategy in order to control unwanted traffic, an ISP should refer to other cases' critical value of m_1 and m_2 and distribute benefits to motivate hosts to cooperate.

4.5 Performance Evaluation

We carried out a number of simulations to illustrate the performance of our incentive mechanism. The network settings consist of $N = 10{,}000$ hosts. The simulations consist of two parts, game among hosts and game among ISPs. In the first set of simulations, we run the simulation to compare incentive mechanisms with or without reward or punishment. We only take into consideration the game among hosts. The second set of simulations consider the game among ISPs. Specifically, we consider the case when all ISPs cooperate, all ISPs defect, and part of ISPs cooperate.

Table 4.1 Parameters setting

Parameter	Commentate	Value
α	Attacking probability	0.1
β	Threshold probability to guarantee sound network environment	0.6
$p_a(t)$	Access fee to the internet at time t	20
$v_k(t)$	The benefit of a node from the internet usage at time t	50
$c_s(t)$	The cost of a node on toolkits for unwanted traffic detection at time t	20
cb_1	Personal loss when a host is intruded	50
cb_2	Punishment when a defector is intruded	100
$n_I^i(t)$	The number of hosts served by ISP i at time t	10,000
m_1^i	Total reward for cooperators of ISP i	20,000
m_2^i	Total reward for rational cooperators of ISP i	20,000
F	Fixed operating cost for ISPs	500

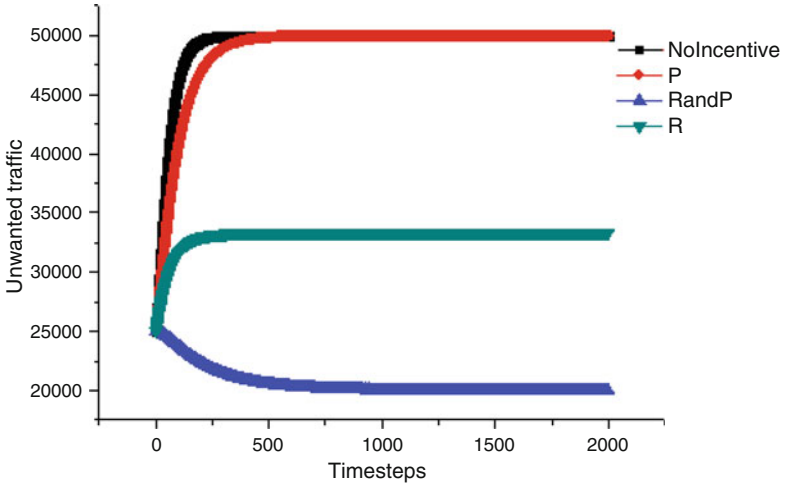


Fig. 4.1 Comparison with system without rewarding or punishment mechanism $\mathbf{x}(0) = (0.2.0.5, 0.3)^T$

We assume that the probability of hosts being attacked is fixed. In each generation, hackers select hosts randomly to attack them. When the chosen host has installed newest anti-virus toolkit, it will not be compromised, or it will be changed into bot and send unwanted traffic to other hosts. Here we assume the traffic sent from a compromised host is five times of normal traffic.

In this section, we provide numerical results to illustrate the efficacy of our proposed mechanism and validate our previous mathematical analysis. The parameters we use in the simulation are exhibited in Table 4.1, certainly we will give an explicit statement when the value of a parameter is modified.

From Fig. 4.1 we can see, systems using rewarding and punishment mechanism perform much better than those do not.

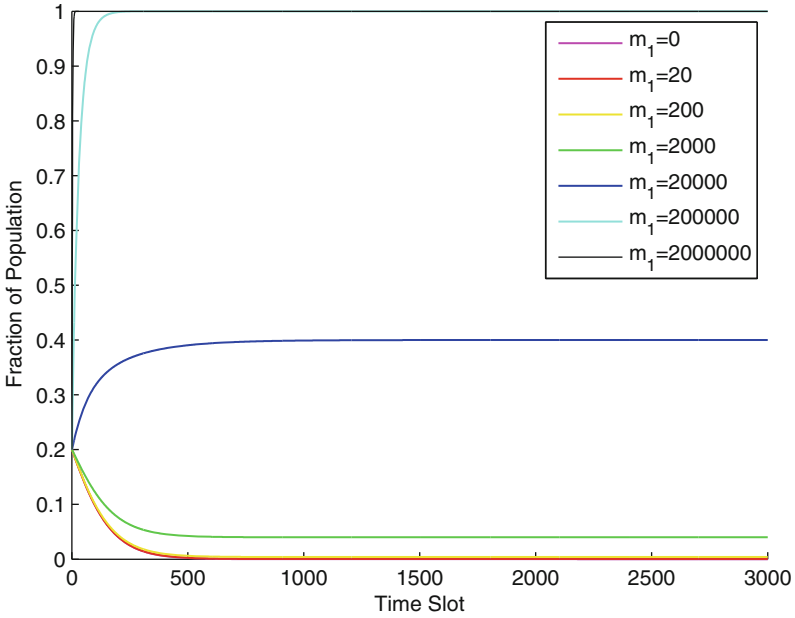


Fig. 4.2 Population dynamics with different m_1 when ISPs defect with initial state $\mathbf{x}(0) = (0.2.0.5, 0.3)^T$

Also we display the final ESS of the population with varying m_1 and m_2, in Figs. 4.2 and 4.3, respectively.

4.6 Conclusion

An increasing amount of unwanted traffic brings enormous uncertainty to ISPs and network users, which is a current challenging issue. Existing unwanted traffic control mechanisms brought up by other researchers are effective and robust but are quite difficult to implement directly in real networks. In addition, the selfish nature of network entities to maximize individual utility leads to free-riding behavior and thus results in a social dilemma. In order to solve this problem, we propose a reward and punishment incentive mechanism to control unwanted traffic based on a public goods game and evolutionary game theory. The whole network is treated as a public good and as ISPs and hosts compete for resources. A reward and punishment incentive mechanism is adopted to further promote a cooperative behavior among nodes. Simulation results suggest that the proposed incentive mechanism is effective and practical. Finally we show how we can further improve the practicality of this incentive mechanism and the performance of unwanted traffic control mechanism.

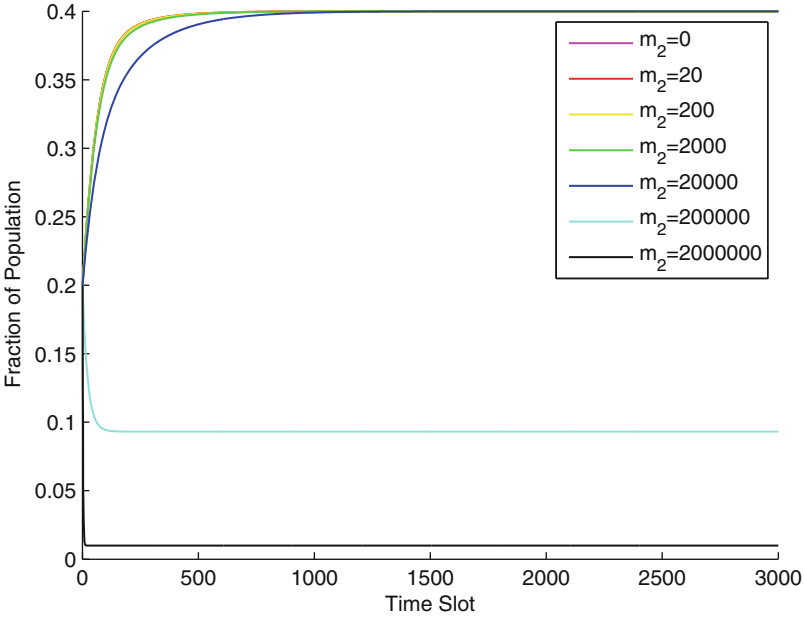


Fig. 4.3 Population dynamics with different m_2 when ISPs defect with initial state $\mathbf{x}(0) = (0.2.0.5, 0.3)^T$

Acknowledgements This work is supported by the National Science Foundation of China (Grant No. 61272173).

References

1. Al-Duwairi, B., Khater, I., & Al-Jarrah, O. (2012). Detecting image spam using image texture features. *International Journal of Information Security, 2*(3/4), 344–353.
2. Chen, Y., Crespi, N., Ortiz, A. M., & Shu, L. (2017). Reality mining: A prediction algorithm for disease dynamics based on mobile big data. *Information Sciences, 379*, 82–93.
3. Chen, Y., Lee, G. M., Lei, S., & Crespi, N. (2016). Industrial Internet of things-based collaborative sensing intelligence: Framework and research challenges. *Sensors, 16*(2), 215.
4. Chen, Y., Shu, L., Crespi, N., Lee, G. M., & Guizani, M. (2016). Understanding the impact of network structure on propagation dynamics based on mobile big data. In *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*. https://doi.org/10.1109/iwcmc.2016.7577198.
5. Jan, M. A., Khan, F., Alam, M., & Usman, M. (2017). A payload-based mutual authentication scheme for internet of things. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.08.035.
6. Pinyol, I., & Sabater-Mir, J. (2013). Computational trust and reputation models for open multi-agent systems: A review. *Artificial Intelligence Review, 40*(1), 1–25.
7. Shen, Y., Yan, Z., & Kantola, R. (2014). Analysis on the acceptance of global trust management for unwanted traffic control based on game theory. *Computers & Security, 47*, 3–25.

8. Shutters, S. T. (2012). Punishment leads to cooperative behavior in structured societies. *Evolutionary Computation, 20*(2), 301–319.
9. Singh, K., Guntuku, S. C., Thakur, A., & Hota, C. (2014). Big data analytics framework for peer-to-peer Botnet detection using random forests. *Information Sciences, 278*, 488–497.
10. Spyridopoulos, T., Karanikas, G., Tryfonas, T., & Oikonomou, G. (2013). A game theoretic defense framework against dos/ddos cyber attacks. *Computers & Security, 38*, 39–50.
11. Srivastava, V., Neel, J. O., MacKenzie, A. B., Menon, R., DaSilva, L. A., Hicks, J. E., Reed, J. H., & Gilles, R. P. (2005). Using game theory to analyze wireless ad hoc networks. *IEEE Communications Surveys and Tutorials, 7*(1–4), 46–56.
12. Szolnoki, A., & Perc, M. (2012). Conditional strategies and the evolution of cooperation in spatial public goods games. *Physical Review E, 85*(2), 1–7.
13. Tian, C., Yang, B., Zhong, J., & Liu, X. (2014). Trust-based incentive mechanism to motivate cooperation in hybrid p2p networks. *Computer Networks, 73*, 244–255.
14. Yan, Z., Kantola, R., & Shen, Y. (2011). Unwanted traffic control via global trust management. In *10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 647–654). Piscataway: IEEE.
15. Yan, Z., Kantola, R., & Shen, Y. (2012). Unwanted traffic control via hybrid trust management. In *11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 666–673). Piscataway: IEEE.
16. Yan, Z., Kantola, R., & Shen, Y. (2014). A generic solution for unwanted traffic control through trust management. *New Review of Hypermedia and Multimedia, 20*(1), 25–51.

Chapter 5
Usability Attributes for Mobile Applications: A Systematic Review

Ryan Alturki and Valerie Gay

Abstract The usability of mobile applications (apps) is an emerging area of research because of the increasing use of mobile devices around the world. App development is challenging because each application has its own purpose, and each individual user has different needs and expectations from the apps. There are various apps available for each purpose, and the success of the application depends on its usefulness. This paper presents a systematic review of some of the most contemporary apps and highlights their usability attributes. It discusses usability models, frameworks and guidelines outlined in previous research for designing apps with enhanced usability characteristics. Based on this research, comprehensive guidelines for mobile apps' usability can then be provided.

5.1 Introduction

The traditional usability guidelines used in desktop applications are not very much applicable to the apps [1]. App usability attributes are different; therefore, we need to specify usability attributes that are essential and important for apps [2]. The important usability attributes expected in any app are effectiveness, satisfaction, efficiency, learnability, errors and memorability as well as the quality characteristics outlined in ISO 9126 [3–6]. Some of the usability attributes may overlap in meaning but have been used with different names by different researchers.

Most of the guidelines are for usability testing, but most of them are not applicable to apps because mobile apps have unique features and changing context [1]. Furthermore, the work available does not have any consensus on the factors of usability. A recent study identified user, task and context as the main factors of usability [3]. However, the study was lacking due to certain limitations. The

R. Alturki (✉) · V. Gay
Faculty of Engineering and Information Technology, University of Technology Sydney, Ultimo, NSW, Australia
e-mail: Ryan.M.Alturki@student.uts.edu.au; Valerie.Gay@uts.edu.au

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_5

researchers found it hard to find the relevant papers, and it affected the results. The papers included were from 2008 to 2010 because smartphone apps had become popular during this period and there had not been much research done on mobile apps usability till that time. A review was conducted on usability characteristics of apps, but the work also lacked some of the recent developments in apps' usability [7].

This article seeks to contribute to important research concerning the usability attributes of apps. The purpose of this research is to conduct a systematic review that reveals the most prominent and recent usability attributes that have been discussed and have emerged in the research. This study will be useful in building future guidelines for developing apps that have all the essential usability attributes. This work stands out because it discusses some of the most contemporary research.

5.2 The Systematic Review

We undertook a systematic review to search for published, peer-reviewed articles that investigated usability attributes in mobile apps. We utilised the terminology outlined in the table below (Table 5.1) to look for research papers covering usability attributes in mobile devices and applications. We sought to incorporate all the related terms that could provide us with articles relevant to this topic.

We referred to ACM Digital Library, EBSCO, IEEE Xplore, PsycINFO, Communication and Mass Media Complete, Computers and Applied Sciences Complete, ProQuest Computer Science Collection, Computer Source and Web of Science.

We tried to include the most recent articles starting from 2010, which were based on app usability. We have followed the methodology from [8], and the flow chart below shows how the systematic review was undertaken (Fig. 5.1).

Table 5.1 Keywords used in the systematic review relating to usability attributes of mobile applications

Search lines	Search terms	Filtered by
Line 1	Mobile device or mobile phone or smart phone	Title/abstract
Line 2	Applications or apps	Title/abstract
Line 3	Usability	Title/abstract
Line 4	Mobile application usability or mobile app usability	Title/abstract
Line 5	Application usability attributes or apps usability attributes	Title/abstract
Line 6	Mobile application usability attributes or mobile apps usability attributes	Title/abstract

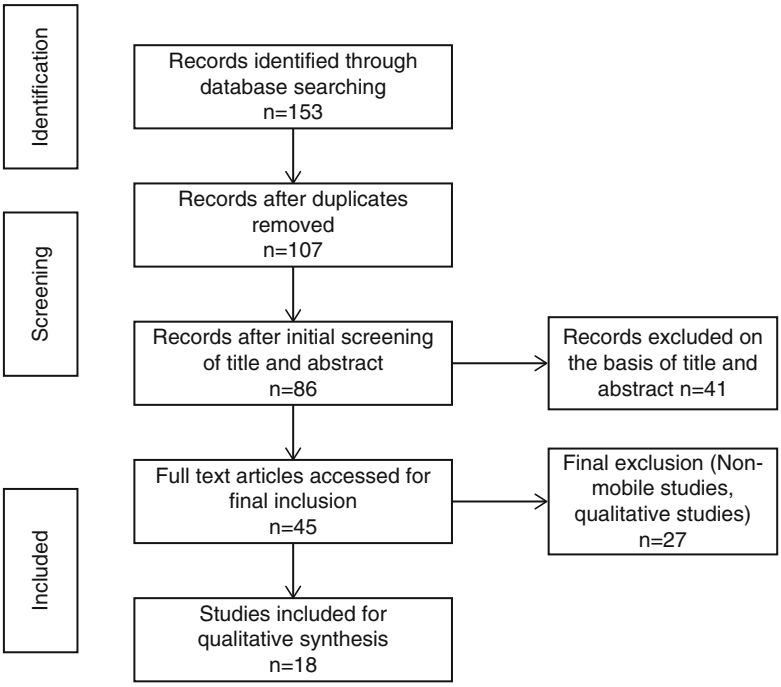


Fig. 5.1 Methodology for the systematic review

5.3 Results

We conducted a systematic review of usability attributes in mobile apps. We looked for articles that discussed usability attributes in mobile devices and applications. We also conducted a comprehensive survey on usability of apps and tried to figure out the important attributes discussed in these papers. Eighteen relevant articles were included which have been published and peer reviewed (Table 5.2).

5.4 Results Evaluation

Figure 5.2 shows the mobile apps' usability attributes. Satisfaction is the most highly mentioned amongst studies at ten times and then both effectiveness and efficiency at six times. Next, learnability was cited three times. Afterwards, simplicity, usefulness, errors, understandable and attractiveness were named two times. All the other attributes, such as memorability and cognitive load, were only cited once.

Table 5.2 Usability attributes in apps

Study's date	Usability attributes	Research
2010	Enjoyment, usefulness and ease of use	A new user interface (UI) for mobile phones is presented in this article, which makes the use of UGC services both more efficient and easier. UI has two main mobile Web 2.0 technologies, multi-display buttons and tag and tag cloud, which increase the flexibility of individual users' buttons and display size. The article not only describes the new UI interface but also investigates whether it aids in enhancing exploratory browsing within mobile user-generated content (UGC) services [9]
2010	Network connection quality, user distraction and user mobility	The article aims to fill a gap in the field of mobile information technology by coming up with clear guidelines for designing mobile information systems. Building on prior studies this research introduces a three-step conceptual model that can be used by managers to design effective information systems. The research found that a network connection's poor quality and high user distraction are very challenging features for mobile information system (IS) design; user interface should be given particular attention [10]
2010	Menu icons, text and colour	This article studied the effects of product aesthetics in usability testing on various outcome variables. The research asked whether changing the appearance of mobile phones has an impact upon usability. Sixty adolescents were asked to use two functionally identical mobile devices but with different visual appearances (highly appealing or not appealing) to find out if there is any relation between usability, perceived attractiveness and performance measures of the product. The findings were that the appealing appearance has a more highly perceived usability, perceived product attractiveness and user performance due to lower task completion time, less errors and higher interaction efficiency [11]
2011	Presentation, adaptation of Web pages, accuracy and search time	The researchers developed and tested specific mobile apps in lab research settings. Testers' performances were used to evaluate usability attributes. The results of the research showed that presentation adaptation greatly enhanced user perception and performance of mobile Web browsing. They discovered that less complexity in information search tasks improves accuracy and reduces search time [12]
2011	Icon characteristics	The study aimed to find out how mobile devices could be made easier to use for adults over 65 years of age. Specifically, alternative mobile apps were benchmarked by manipulating icon characteristics. It was found that the elderly face more problems using icons on existing mobile devices. However, icon characteristics, which have a close semantic meaning (i.e. a close relationship between the portrayed object and its connected function) and are well-known and specific were found to enhance and improve icon usability for elderly people [13]

2012	Customer needs, design, feedback, innovativeness, satisfaction and efficiency	This research developed and used a questionnaire on mobile phones to find out if there was any relationship between usability and the success of the product. The researchers reviewed the factors of product success and existing usability studies to develop a questionnaire. The usability and success factors of mobile phones were evaluated by the participants. The results showed that customer needs, design and innovativeness were not only important success factors but also increased attention ought to be given to feedback, efficiency and satisfaction to improve the usability of mobile phones [14]
2012	Screen size, colour, weight of device, text source, extra batteries, etc.	This paper aims to highlight the expected quality characteristics of apps with a detailed and reviewed discussion mostly about usability characteristics, being external characteristics of apps as according to ISO 9126 [7]
2013	Errors, task completion time and effectiveness	The article compares mobile usability in Iran and Turkey. The research concludes that usability is impacted by not only religious, ethnic or cultural issues but also contextual features which are endemic to both Turkey and Iran [15]
2013	Efficiency, satisfaction, effectiveness, aesthetic, usefulness, simplicity, learnability, understandable, intuitiveness and attractiveness	The main objective of the study is to propose a set of usability dimensions that should be considered when evaluating and designing mobile apps. The model introduced is based on the reviews of previously related studies, which were analysed by using a content analysis approach. Ten usability attributes were outlined in the model. The model introduced could be of assistance to practitioners and researchers as a guideline to design usable mobile apps [16]
2013	Security	The paper discusses the relationship between security and usability in mobile platforms; and how reducing various security threats can improve the usability of mobile apps [17]
2013	How the satisfaction attribute of apps can be improved by making them more energy efficient	The approach proposed in the paper is convenient for developers and provides a better estimate of energy consumption at code level. Pre-instruction energy modelling and program analysis are used to achieve these results. The new approach can estimate energy consumption for mobile apps to 10% of the ground truth [18]

(continued)

Table 5.2 (continued)

Study's date	Usability attributes	Research
2013	Efficiency, satisfaction, effectiveness, learnability, errors, memorability and cognitive load	Review of usability models was conducted and outlined seven usability attributes. The researchers believed cognitive load has been overlooked in previous usability models [3]
2014	Efficiency, user satisfaction and technical effectiveness	The research objective was to test the usability (efficiency, user effectiveness and technical effectiveness) of a developed mobile app (Reactivate) in obese adolescents. A field study was conducted on obese children who were asked to use the app to perform tasks to test its usability. The tasks had five categories: to create a message, to enter personal settings, to use the goal-setting feature, to find and to answer surveys and to enter descriptions or details of weight and height. Standardized SUMI was completed by each participant to determine the satisfaction of the user. SUMI measures five aspects of user satisfaction: effect, controllability, helpfulness, efficiency and learnability. SUMI scores and the mean relative user efficiency were explored using descriptive statistics. The mean scores confirmed that reactivate was a useful app, and users responded with great interest [19]
2015	Satisfaction	People with ASD (autism spectrum disorder) usually lack familiarity and experience with new technologies; therefore, usability of apps developed specifically for children with autism is very important. The paper compares the usability of two Arabic apps available on the Apple Store. Various measurement tools were used to collect quantitative and qualitative data to determine the level of user satisfaction with the apps. Recommendations were then made on how further the usability of these apps can be improved [20]

2015	Efficiency effectiveness, satisfaction, attractiveness, learnability, operability and understanding	This paper conducted a systematic literature review to investigate empirical usability evaluation processes described in different m-health app studies. The research showed that the usability attributes evaluated mostly in m-health apps were operability and effectiveness. The results showed that using automated mechanisms can improve the methods of empirical evaluation employed in usability. The paper could be useful for developers and researchers who are looking to create apps with better usability. The study also demonstrates the benefits of adapting health apps to the needs of users [21]
2015	Efficiency, effectiveness and satisfaction	This paper aimed to assess the usability of Chongqing University Library App and give recommendations for improving the usability of apps. Usability testing involved pretest questionnaires, achieving tasks and posttest surveys. Three attributes were measured: effectiveness, efficiency and user satisfaction. The results showed that app was effective, but improvement was needed for efficiency. For the user satisfaction, 'usefulness' had the highest score and 'clarity' the lowest. The descriptions were not clear and sometimes confused users. However, the services the app provided were appealing and appreciated by most users. After measuring UX, the paper recommends ways to enhance the usability of the app [22]
2016	Visibility, scrolling, navigation, interaction, satisfaction, convenience and simplicity	The paper compared four widely used mobile spreadsheet apps: Google Drive, Documents to Go, OfficeSuite Viewer 6 and ThinkFree Online. Measures for each usability attribute were gleaned from a survey. These surveys were created to address the measures based on comparative criteria supplied in the analysis. The results also indicate that there is little difference between the apps in their end results and the aspects conducted in this survey [23]
2016	Satisfaction and user feeling	The article selects all touchscreen mobile devices and various components that affect their usability. Analytic network process (ANP) and Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) were used to find which mobile devices were superior and which usability features were most important [24]

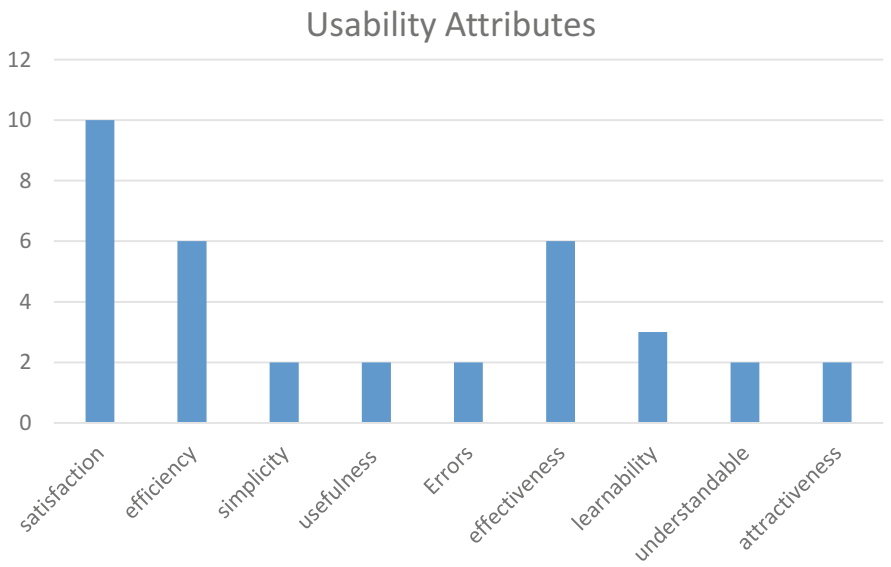


Fig. 5.2 Usability attributes in mobile apps

5.5 Conclusion

This review shows that usability in apps has been discussed from various points of view by many authors. Some studies provide guidelines for improving usability, whilst others compare usability attributes amongst different apps. Usability has been discussed from numerous angles between 2010 and 2016. Most of the work discussed in the beginning of the study involved research in lab settings; however more recent research usually took place in field settings. Earlier research was aimed at testing usability attributes in apps or emphasising the importance of certain attributes. Next, most researchers were interested in comparing different applications to test usability. Then, usability attributes have been evaluated for some practical apps, and there has been a focus on adding something new to these. Recent work has also included users' acceptance and expert reviews as evaluating procedures for determining the usability of applications. Some of the recent work focuses specifically on improving usability in apps related to various fields ranging from health to social networking. Usability criteria are always evolving, and the needs of people are changing rapidly so new dimensions of usability have been discussed in some of the recent research. The attributes that are emerging in the new research are related to the ease of use of the application when performing multiple tasks, intuitiveness, security and power consumption. These attributes can be debated as being part of those defined in the traditional literature, but in apps, there is a need to mention them separately to emphasise their importance.

The evaluation of the results shows that satisfaction is the most highly mentioned amongst studies at ten times followed by both effectiveness and efficiency at six times.

This research shows that there are numerous usability attributes and it is difficult for designers to include them all into one app. The best they can do is improve the usability of the app by keeping its nature in mind. This research will be used to outline usability guidelines for developing applications with enhanced usability. This is only possible when the developer is aware of the attributes that enhance usability.

References

1. Zhang, D., & Adipat, B. (2005). Challenges, methodologies, and issues in the usability testing of mobile applications. *International Journal of Human-Computer Interaction., 18*(3), 293–308.
2. Gafni, R. (2009). Usability issues in mobile-wireless information systems. *Issues in Informing Science and Information Technology, 6*, 755–769.
3. Harrison, R., Flood, D., & Duce, D. (2013). Usability of mobile applications: Literature review and rationale for a new usability model. *Journal of Interaction Science, 1*(1), 1–16.
4. Popa, M. (2010). Audit process during projects for development of new mobile it applications. *Informatica Economica, 14*(3), 34.
5. Pocatilu, P., & Boja, C. (2009). Quality characteristics and metrics related to M-Learning process. *Amfiteatru Economic, 11*(26), 346–354.
6. Fleming, I. (2016). An overview of the ISO 9126-1 software quality model definition, with an explanation of the major characteristics, from http://www.sqa.net/iso9126.html
7. Rabi'u, S., Ayobami, A. S., & Hector, O. P. (2012). Usability characteristics of mobile applications. In *Proceedings of international conference on behavioural & social science research (ICBSSR), Kampar, Malaysia*. (Indexed by Thomson Reuters).
8. Alturki, R. M., & Gay, V. (2016). A systematic review on what features should be supported by fitness apps and wearables to help users overcome obesity. *International Journal of Research in Engineering and Technology, 5*(9), 197–206.
9. Functionality of mobile apps in health interventions: A systematic review of the literature. *JMIR mHealth and uHealth, 3*(1), e20.
10. Kim, S., Lee, I., Lee, K., Jung, S., Park, J., Kim, Y. B., et al. (2010). Mobile web 2.0 with multi-display buttons. *Communications of the ACM, 53*(1), 136–141.
11. Gebauer, J., Shaw, M. J., & Gribbins, M. L. (2010). Task-technology fit for mobile information systems. *Journal of Information Technology, 25*(3), 259–272.
12. Sonderegger, A., & Sauer, J. (2010). The influence of design aesthetics in usability testing: Effects on user performance and perceived usability. *Applied Ergonomics, 41*(3), 403–410.
13. Adipat, B., Zhang, D., & Zhou, L. (2011). The effects of tree-view based presentation adaptation on mobile web browsing. *MIS Quarterly, 35*(1), 99–122.
14. Leung, R., McGrenere, J., & Graf, P. (2011). Age-related differences in the initial usability of mobile device icons. *Behaviour & Information Technology, 30*(5), 629–642.
15. Kim, K., Proctor, R. W., & Salvendy, G. (2012). The relation between usability and product success in cell phones. *Behaviour & Information Technology, 31*(10), 969–982.
16. Aryana, B., & Clemmensen, T. (2013). Mobile usability: Experiences from Iran and Turkey. *International Journal of Human-Computer Interaction, 29*(4), 220–242.
17. Baharuddin, R., Singh, D., & Razali, R. (2013). Usability dimensions for mobile applications—A review. *Research Journal of Applied Sciences, Engineering and Technology, 5*, 2225–2231.

18. Boja, C., Doinea, M., & Pocatilu, P. (2013). Impact of the security requirements on mobile applications usability. *Academy of Economic Studies. Economy Informatics, 13*(1), 64.
19. Hao, S., Li, D., Halfond, W. G., & Govindan, R. (2013). Estimating mobile application energy consumption using program analysis. In *2013 35th international conference on software engineering (ICSE)* (pp. 92–101). IEEE.
20. O'Malley, G., Dowdall, G., Burls, A., Perry, I. J., & Curran, N. (2014). Exploring the usability of a mobile app for adolescent obesity management. *JMIR mHealth and uHealth, 2*(2), e29.
21. Al-Wakeel, L., Al-Ghanim, A., Al-Zeer, S., & Al-Nafjan, K. (2015). A usability evaluation of arabic mobile applications designed for children with special needs—Autism. *Lecture Notes on Software Engineering, 3*(3), 203.
22. Zapata, B. C., Fernández-Alemán, J. L., Idri, A., & Toval, A. (2015). Empirical studies on usability of mhealth apps: A systematic literature review. *Journal of Medical Systems, 39*(2), 1–19.
23. Wei, Q., Chang, Z., & Cheng, Q. (2015). Usability study of the mobile library app: An example from Chongqing university. *Library Hi Tech, 33*(3), 340–355.
24. Chintapalli, V. V., Tao, W., Meng, Z., Zhang, K., Kong, J., & Ge, Y. (2016). A comparative study of spreadsheet applications on mobile devices. *Mobile Information Systems*. https://doi.org/10.1155/2016/9816152

Chapter 6
A Review on Integration of Scientific Experimental Data Through Metadata

Nur Adila Azram, Rodziah Atan, Shuhaimi Mustafa, and Mohd Nasir Mohd Desa

Abstract Data integration for scientific experiments and research is important to researchers in many research areas like biotechnology, medical, and biomedical research. This is because many experiments and research data are stored in different sources as well as involving multidisciplinary fields which make it difficult to manage and analyze the experimental data. Metadata is one of the common methods used for data integration in many different areas. This paper describes and reviewed metadata as one of the approach for data integration. Other than that, the state of research for integration of scientific experiments and research data based on metadata along with review on latest related work are also covered in this paper.

6.1 Introduction

Data integration can be defined as a process where multiple data from different sources are combined through a single access point system. In other words, data integration is an issue of related data from various sources and displaying it in a unified representation and semantic heterogeneity [1]. Data integration has become

N. A. Azram
Halal Products Research Institute, Universiti Putra Malaysia, Serdang, Malaysia

R. Atan (✉)
Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Malaysia
e-mail: rodziah@upm.edu.my

S. Mustafa
Faculty of Biotechnology and Biomolecular Sciences, Universiti Putra Malaysia, Serdang, Malaysia
e-mail: shuhaimi@upm.edu.my

M. N. Desa
Halal Products Research Institute, Universiti Putra Malaysia, Serdang, Malaysia
e-mail: mnasir@upm.edu.my

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_6

essential to different scientific experimental areas such as biology, biomedical, and medical as it involved multidisciplinary domain.

Scientific researchers need a compelling system to manage their experimental data and results as well as to share and search the data. However, with increased volume of data and experiments as well as multidisciplinary domain involved, it is challenging in the progression of gathering, establishing, interpreting, and sharing data [2].

Metadata is one of the approaches that are used to attain data integration. It can be defined as data about other data or the organized data that is used to provide the information of some sources. Metadata is generally used to depict the contents, scope, quality, administration, the data holder and other components or data sets related data. It is a basic method to achieve data discovery, administration, sharing, trade, and integration [3].

The objectives of this paper are to understand the concept of metadata as one of the possible approach for data integration and also to identify existing metadata-based approach for scientific experimental data integration. The selection of reviews and coverage of the literatures in this paper are based on the general knowledge information of metadata as data integration approach as well as the application of metadata in scientific experimental data integration.

6.2 Metadata Approach

As mentioned in Sect. 6.1, metadata is one of the methods used in data integration. It can be described as the entirety of what one can say in regard to any data objects (whatever that can be deal and operated by a human or a system as an isolated entity) at any level of combination, in a machine comprehensible representation [4]. It serves as the abstraction of data and is essential for understanding shared data [5].

Metadata can be used to accomplish data integration by making data easier to manage and promote human and machine readability. It makes data more useful to other people. It is also an important component of digital sharing and preservation because it ensures that data can be uniquely identified and accurately described to support future retrieval and reuse.

In general, three primary categories of metadata have been identified. The first is descriptive metadata which describes a resource for goals like finding and identification. The second category is structural metadata which defines how the organization of the components of an object is done (e.g., in what way pages are organized to form chapters). The third category is administrative metadata which gives information to facilitate resource management. For administrative metadata, there are two subtypes which are rights management metadata that clarify intellectual property rights and preservation metadata that contains data that is required to uphold and maintain a resource [6].

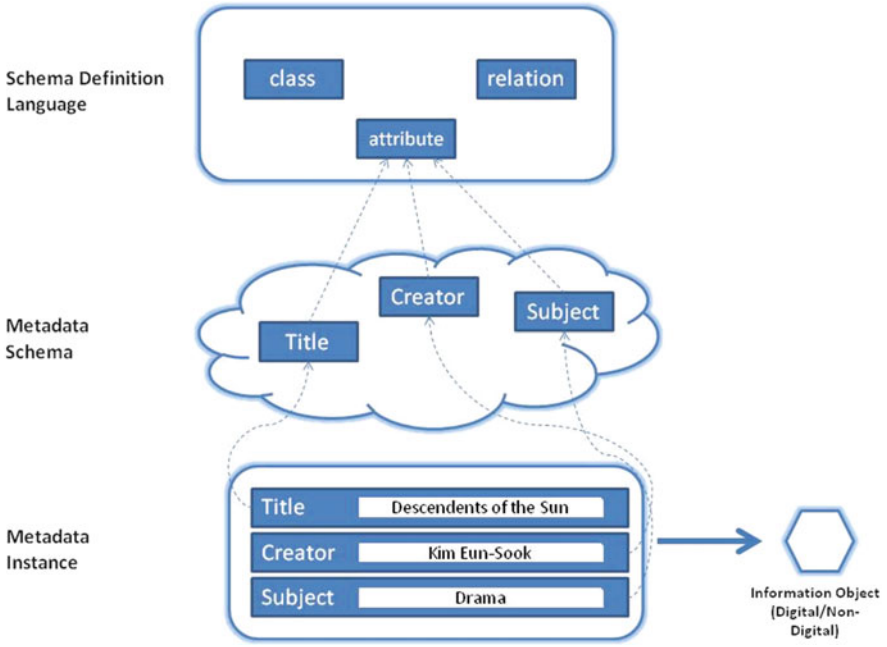


Fig. 6.1 The metadata building blocks overview

6.2.1 Metadata Building Blocks

There are three main metadata building blocks which are metadata instances, metadata schema, and schema definition language. Figure 6.1 shows the overview of metadata building blocks.

Metadata instances are the content standards set in a metadata description. It maintains a metadata component set gathered from a metadata schema and connecting content standards. Combination of these component values sets up a metadata description about a certain information object.

Metadata schema is the elements' definition. It is a set of elements with a definite semantic definition linked by some structure [7]. The meanings of schema elements define the semantics of the schema.

Schema definition language is the language for describing metadata schemes. It offers a set of language primitives. The primitives not only syntactically build but also have a semantic meaning because machines must understand the language. XML Schema, Web Ontology Language (OWL), SQL-DDL, and Unified Modeling Language (UML) are some examples of schema definition languages.

Table 6.1 Examples of metadata standard

Metadata standard	Area(s)	Description
Darwin core	Biology	Species geographic occurrence and specimens' existence in collections metadata information
Directory interchange format	Scientific data sets	Scientific data set descriptive and standardized format for interchanging information
Dublin core	Networked resources	Networked resources interoperable online metadata standard
Resource description framework	Web resources	Web resources common technique for theoretical description or presenting implemented information by utilizing a variety of syntax formats
ISO 19115:2003 geographic information—Metadata	Geographical data	Describes way to define information on geographical and connected services, including contents, data quality, access, spatial-temporal purchases, and right to use

6.2.2 Metadata Standards

Metadata standard is a prerequisite which is expected to set up a general understanding of the criticalness of information, to guarantee right and real use and comprehension of the data by its owners and users. It normally supports a number of defined functions and will specify elements. Metadata elements that are grouped into sets which intended for a particular reason are called metadata schemas.

Metadata schemas normally state names of elements and their semantics. They possibly will also state content rules for how content must be conveyed, representation rules for content, and allowable content values [6]. Many different metadata schemas have been developed as standards across disciplinary areas such as biology, scientific data sets, and networked resources. Table 6.1 shows some examples of metadata standards.

6.3 Related Work

Metadata is standard data structure applied to database set in order to ease data representation for further analysis. It can be addressed as a platform of concepts that bridges the contextual divide among heterogeneous data sources [8]. Metadata have been essential to many different areas such as medical and bioinformatics to help in integration of data or information.

In medical science, metadata has been important in integration of various medical data and information. [9] have proposed an efficient metadata schema for handling medical data through Internet applications by using Taiwanese government's medical databank as an example. The actual complex and disparate datasets could

be converted and encoded into several attributed data files and categorized in the domains of diagnosis, medication, surgical procedure, outpatient and hospitalization record, and billing record using the proposed method.

They emphasize superior performance of the proposed metadata mechanism by analyzing the comorbidity of major chronical diseases and hospitalization of diabetes patients in Taiwan through online analytical approach. Based on the results they obtained, it shows that primarily encoded metadata schema for categorizing and describing medical data could provide a possible solution for handling medical data. [10] proposed a metadata approach for data integration in medical science particularly in epidemiological study. They created a dedicated metadata repository to manage metadata centrally and consistently. It includes a matching component creating schema mappings as a prerequisite to integrate captured medical data.

Bioinformatics is another area of study that needs data integration in managing data because heterogeneity is big in respect to information accessibility, resource format, and resource availability as well as heterogeneity in tasks undertaken by bioinformatics scientists for solving biology-related problems. [11] examined the metadata element set description framework for integration of various information resources related to the field of bioinformatics available over the Internet and designed a Web-based tool for integration of bioinformatics information resources named iBIRA.

It used Dublin Core metadata element set for description of information resources and XML schema for interoperability of information resources with others. The development of iBIRA gives an opportunity for further research to develop a standard so that interoperability of information can be sought and uniformity may be achieved.

These related works used metadata as an approach to integrate various data or information related to their domains or areas of study. For scientific experimental data integration, elaboration of the metadata approaches solely for scientific experimental data is discussed in Sect. 6.4.

6.4 Metadata for Scientific Experimental Data Integration

Metadata are needed for data integration to help users to search and share data. In scientific experiment areas, often there is a need to exchange valuable data or information between different researchers or research domain [12].

It is difficult to integrate data in scientific experiment areas because it involves many multidisciplinary domains with a lot of experiment data or information. There is a need to make data integration in scientific experiment area easier to be done and applied. By using metadata approach in data integration, researchers can easily meet their research need and data sharing need.

There are many metadata approaches that have been proposed for scientific experiment data integration. There are some of the approaches general for any

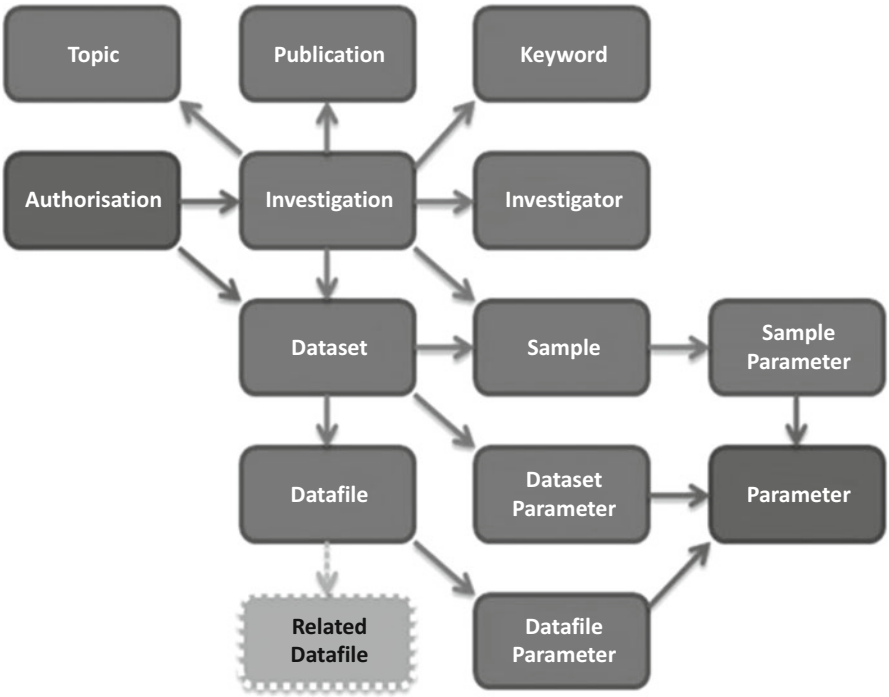


Fig. 6.2 Main entities of CSMD

domains of scientific experiment, and there are also approaches that are specific for a domain. We will summarize some of the approaches in Sect. 6.4.1.

6.4.1 Existing Metadata Approach for Scientific Experiment Data

Core Scientific Metadata Model (CSMD) is a model that focuses on study-data that is estimated to get high level information about scientific studies and the data they produce. It is an extensible model of metadata initially intended to catch a usual set of information about the data delivered by experiments, analysis, measurements, and simulations in facilities science [13]. It can also be used generically across scientific disciplines.

CSMD describes a hierarchical model of the structure of scientific research around studies and investigations with their related information. Figure 6.2 shows the main entities of the CSMD [14].

Metadata standard is a prerequisite which is expected to set up a general understanding of the criticalness of information, to guarantee right and real use

Table 6.2 The three collected metadata and their description

Metadata collected	Description
Classification metadata	The features from the research order (program ID, experiment ID, and project ID)
Transformation metadata	It defines the common properties of the transformer that are shared by all transformation instances. The transformation instance metadata define the inputs, outputs, and controls of a transformation.
Lineage metadata	Tracing former transformation Ids to connect transformation pipelines

and comprehension of the data by its owners and users. CSMD does not make presumptions about particular terminology of a domain; consequently it can be extensible and can be specific to any scientific areas which would be a significant help to the scientists in storing and sharing out their data.

SciPort is an integration system for collaborative scientific research with an experiment and metadata management [15]. Metadata in this system is defined as high-level information that illustrate experiments and transformations and then put them in a formal setting for human use. There are three metadata collected in this system. Table 6.2 shows the three collected metadata and their descriptions.

The metadata modeling of this system provides researchers with an integrated framework to describe and manage their experiments. The metadata also obtain all the essential information to recreate experiments and make it easily shared, evaluated, and repeated. It also denoted as XML documents which can be indexed and examined at the field level with standard XML query languages [16].

The EM Metadata Model is a metadata model that defines the epidemiological resources that are based on Dublin Core (DC). It provides elements for technical information, general information that relate to the digital resource, and context-specific information. The metadata model used DC as the base because DC is an interoperable metadata standard [17]. The term offered by DC can already handle many of the requirements of the EM, but because epidemiology relies on multiple domains, the metadata model must extend the core elements of DC with tags suitable for these domains. Some of DC elements have also extended with new epidemiological elements. The metadata model also specifies the expected values that can be used to fill each element. With the use of metadata model in interpreting the EM resources, it would be easier to preserve and guarantee an easier sharing of epidemic resources.

Scientific research management information resources metadata is an information resource integration technology that is based on metadata proposed by the Chinese Academy of Sciences [18]. It includes joining the source of data sources; the development of the metadata standard; extraction, transformation, and loading (ETL) operations; and data record system development. The metadata is based on Dublin Core (DC) metadata and Chinese Academy of Sciences Scientific Database Core Metadata 2.0. It includes six nonreusable core subsets and one reusable

Table 6.3 The scientific research management information resource metadata

Name	Definition
Content information	The fundamental information of title, description, topic, source, languages, cover age, date about the collection of data (e.g., name, date)
Establishing information	Information, for example, organization, associations and business associated with origination, administration, preservation, and utilization of information (e.g., production department, preservation department)
Data quality information	The general assessment of the information quality of the data set (e.g., quality report)
Form information	Information such as date, presentation, parameters, and characteristics of the data set (e.g., creation date, storage location)
Security management information	Security management information of the data set (e.g., classification of security restrictions)
Metadata reference information	The data set metadata information (e.g., metadata standard, metadata language)
Contact information	Information of individual or organization identified with data collection (e.g., names, address)
Content information	The fundamental information of title, description, topic, source, languages, cover age, date about the collection of data (e.g., name, date)

secondary subset. Table 6.3 shows the scientific research management information resource metadata.

The metadata are managed by establishment of information resource catalogue system. By using the application, users can query and preserve the metadata.

6.5 Summary and Conclusion

In this paper, we presented an overview and state of research for integration of scientific experimental data based on metadata approach. We give an overview on metadata, metadata building blocks, and metadata standards. We also summarize some existing metadata model for scientific experiment or research data. Summarizing, we found that there are few metadata models that are general for any scientific research domains and also many are for specific domains. Some of the metadata models are based on DC metadata standard because of the interoperability of DC.

Because scientific experiments involved multidisciplinary domains, scientific data varies in terms of formats, types, and structure. These make it difficult to design a general metadata for any scientific research domains.

The goal of this evaluation is to gain knowledge and understanding on the concept of metadata-based approach for data integration as well as the elements involved in creating metadata. We also want to identify existing metadata approach

for integration of scientific experimental data so that we can study and use it as a reference to establish new metadata that would suit any domains which involve scientific experimental data.

We conclude that metadata is one of the approaches that are suitable in facilitating the integration of data from various sources whether it is for scientific experimental domain or any other domain. It would help in bringing transparency and accuracy in information and also removing uncertainty in data and information especially for many scientific experiment data gathered from multidisciplinary domains.

References

1. Ae Chun, S., & MacKeller, B. (2012). Social health data integration using semantic web. In *Proceedings of the 27th annual ACM symposium on applied computing* (pp. 392–397).
2. Brahaj, A., Razum, M., & Schwichtenberg, F. (2012). Ontological formalization of scientific experiments based on core scientific metadata model. In *16th international conference on theory and practice of digital libraries. LNCS 7489* (pp. 273–279).
3. Ying, Y., & Gengda, J. (2004). Metadata-based information organization and ontology-based knowledge organization. *Journal of Academic Libraries, 4*, 43–47.
4. Gilliland, A. J. *Introduction to metadata: Pathways to digital information. Version 2.1*, Los Angeles, CA: Getty Information Institute. http://www.getty.edu/research/institute/standards/intrometadata/index.html
5. Birnholtz, J., & Bietz, M. (2003). Data at work: Supporting sharing in science and engineering. In *Proceedings of the 2003 international ACM SIGGROUP conference on supporting group-work* (pp. 339–348).
6. National Information Standards Organization, Guenther, R., & Radebaugh, J. (2004). *Understanding metadata (PDF)*. Bethesda, MD: NISO Press (pp. 1–16). ISBN 1-880124-62–69.
7. Rahm, E., & Bernstein, P. A. (2001). A survey of approaches to automatic schema matching. *The VLDB Journal, 10*(4), 334–350.
8. Lee, P. W. (2003). *Metadata representation and management for context mediation*. Working Paper CISL# 200301, May 2003.
9. Chi-Jane, C., Tun-Wen, P., Jhen-Li, H., Ying-Tsang, L., Shih-Syun, L., & Chun-Chao, Y. (2017). Construction of a metadata schema for medical data in networking applications. In *31st international conference on advanced information networking and applications workshops* (pp. 597–600).
10. Toralf, K., Alexander, K., Mathias, R., & Jonas W. (2017). Metadata management for data integration in medical sciences. *Lecture Notes in Informatics (LNI)*, 175–194.
11. Ram, S., & Rao, N. L. (2014). Metadata description framework for integration of bioinformatics information resources: A case of iBIRA. *DESIDOC Journal of Library and Information Technology, 34*(5), 384–392.
12. Chong, Q., Marwadi, A., Supekar, K., & Lee, Y. (2003). Ontology based metadata management in medical domains. *Journal of Research Practice in Information Technology, 35*(2), 139–154.
13. Yang, E., Matthews, B., & Wilson, M. (2013). Enhancing the core scientific metadata model to incorporate derived data. *Future Generation Computer System, 29*(2), 612–623.

14. Matthews, B., Sufi, S., Flannery, D., Lerusse, L., Griffin, T., Gleaves, M., et al. (2009). Using a core scientific metadata model in large-scale facilities. In *5th international digital curation conference, London, United Kingdom* (pp. 106–118).
15. Wang, F., Liu, P., Pearson, J., Azar, F., & Madlmayr, G. (2006). Experiment management with metadata-based integration for collaborative scientific research. In *Proceedings of the 22nd international conference on data engineering*.
16. W3C XML Query (XQuery). https://www.w3.org/XML/Query/
17. Ferreira, J. D., Pesquita, C., Couto, F. M., & Silva, M. J. (2013). Digital preservation of epidemic resources: Coupling metadata and ontologies. In *Proceedings of the 10th international conference on preservation of digital objects*.
18. Chen, Z., Wu, D., Lu, J., & Chen, Y. (2013). Metadata-based information resource integration for research management. *Procedia Computer Science, 17*, 54–61.

Chapter 7
Passive RFID Localization in the Internet of Things

Belal Saeed Alsinglawi, Quang Vinh Nguyen, Upul Gunawardana, Simeon Simoff, Anthony Maeder, Mahmoud Elkhodr, and Mohammad Dahman Alshehri

Abstract Smart home researches have emerged in recent years as a popular field of study in pervasive computing to suggest a solution that can be beneficial for impaired individuals and elderly on their daily life basis. Location tracking accuracy is a major research challenge in smart homes that needs much further investigation. This paper presents a review of the existing techniques and technologies in location-based systems in the Internet of things, and it identifies the research gap of localization in smart home settings. The paper proposes a localization framework for smart home healthcare as well as our preliminary implementation of the localization framework.

7.1 Introduction

The demand of the healthcare systems is rising, due to the change in the aging demographics and chronic medical conditions, and this will lead to unsustainability in the healthcare services globally [1]. According to the World Alzheimer Report,

B. S. Alsinglawi · Q. V. Nguyen · U. Gunawardana · S. Simoff
Western Sydney University, Sydney, NSW, Australia
e-mail: b.alsinglawi@westernsydney.edu.au; Q.Nguyen@westernsydney.edu.au; U.Gunawardana@westernsydney.edu.au; S.Simoff@westernsydney.edu.au

A. Maeder
Flinders University, Bedford Park, SA, Australia
e-mail: anthony.maeder@flinders.edu.au

M. Elkhodr
School of Engineering and Technology, College of Engineering and Technology, Central Queensland University, Sydney, NSW, Australia
e-mail: m.elkhodr@cqu.edu.au

M. D. Alshehri (✉)
University of Technology Sydney, Ultimo, NSW, Australia
e-mail: Mohammad.Alshehri@uts.edu.au

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_7

more than 46.8 million people are suffering from dementia today, and that number is expected to increase to 74.7 million in 2030 and 131.5 million by 2050 [2]. These problems have increased the pressures on healthcare amenities globally. Substitute solutions have been considered to address these challenges. Researchers have employed pervasive computing for smart homes for personal health monitoring, as one of the most potential affordable solutions to these challenges.

The smart home is an area in which the Internet of things (IOT) promises to reshape the healthcare domain [3]. Smart homes [4] include applications that monitor the elderly unobtrusively via interconnecting sensors to warn them or healthcare providers of abnormal conditions [5]. In personal monitoring, several wearable and environmental sensors are deployed in assistive living technologies. Smart home sensors work on the principle of sensing individual's movement to generate sequences of streaming row data. By using several location determination techniques and activity detection algorithms, this data will be interpreted to meaningful information about people's movements in the space.

Pervasive computing healthcare technologies aim to assist the elderly and impaired individuals in their living, particularly easing their daily activities and performing domestic tasks conveniently [6]. Ubiquitous homes have been studied by several researchers who have proposed promising contributions in healthcare and in supporting impaired individuals. Chan et al. [7] reviewed relevant aspects in smart homes, such as human activity recognition and efficiency of implemented sensor systems. The authors argued that smart homes are one of the favorable, cost-effective solutions for home care for the elderly and people with disabilities. However, the studies in smart homes are still in its early stages, due to the challenges that were facing smart home users and healthcare providers. Accuracy in tracking people's movements and success in detecting the activities of daily living plays are the key roles to make such a viable system solution in smart home applications.

To enable smart homes efficiently for the frail person in health assistance, several essential factors should be taken in consideration such as providing robustness cost-effective solutions; a system can differentiate between different activities that are carried on by one person or more at the same time. In addition, the smart home system should track the location of the person accurately at stationary and real-time movement. Hence, smart home is considered as a promising and affordable way to enhance the accessibility to home care and ease of living a lifestyle for elders and people with disabilities. There are still limited results in smart homes research, such as localization of movable individuals and objects. This paper highlights the smart home localization system in the Internet of things and the challenges associated with indoor localization in smart homes. Section 7.2 provides a discussion about localization systems in smart homes. Section 7.3 addresses the challenges associated with passive RFID localization systems in smart homes. Section 7.4 provides our preliminary implementation of the localization framework. The conclusion is provided in Sect. 7.5.

7.2 Localization in Smart Homes

Localization systems in smart homes work on the principle of sensing the activities performed by individuals and their locating positions and movements at a time. In Ambient Assisted Living (AAL) [7], the location-based awareness systems require indoor positioning functionalities to detect emergency situations, fall detection, and monitoring vital signs [8]. These systems work on a principle of determining the location of persons and objects and their interaction in real time.

Indoor positioning technologies are one of the core components in smart homes. A wide range of technologies for indoor environments have been used and tested in a smart space into different applications such as healthcare, medical, security, warehouse, asset management, and people tracking. There are common types of indoor tracking sensors used to track people in real time: radio-frequency-based (RF) sensors, optical sensors, sound wave sensors, and electromagnetic field sensors [9].

These technologies are widespread and used in SH settings for subject tracking and object localization. In smart homes, RF-based systems have gained significant popularity in smart environment research projects for considerable advantages such as affordability, commercial availability, and desirable coverage space in an indoor space. Therefore, smart home technologies such as RFID, Bluetooth, Wi-Fi, etc. are popularly used in the smart environment.

7.2.1 Accuracy

Accuracy (location error) in smart homes is the primary key to determining the place of the subject at any time. It refers to the user requirement of the location system. Therefore, the accuracy is defined as the average Euclidean distance between the estimated location and the real location [10].

Detecting the movable target requires careful selecting for tracking resources. The relationship between the accuracy and system is usually cost adverse. This means a more precise location to get the need to deploy more extra tracking resources, and that will lead to the more expensive solution. Therefore, researchers attempt to reduce the number of tracking records, to achieve the cost-effective way. Nevertheless, location determination and tracking algorithms need to be suitable for such an approach while the accuracy measure is achievable.

7.2.2 RFID Localization Systems

Radio-frequency identification (RFID) has been considered as a promising technology in indoor positioning for smart homes [11]. RFID systems have tremendous

benefits for smart environments: particularly (1) RFID tags are relatively small and can be easy to attach to many household tools (such as plates, spoons, cups, furniture, etc.), and (2) they are easy to wear by a person because of their small size and their light weight. RFID technology has been engaged in aged care facilities, to reduce the gap for healthcare progression and improve patient care. Several RFID localization studies have exploited subject and object localization in the past few years by many researchers in smart homes to find robustness in indoor positioning solutions for healthcare facilities, such as in [12–15]. Some of these systems have provided low localization accuracy performance with limited performance, while the others have cost concerns. Few works have investigated the challenges in cost-effectiveness, accuracy, and efficiency in RFID localization in indoor positioning for smart homes.

LANDMARC [16] introduced the concept of localization using reference tags to estimate target tag. The system measured the distances between readers and active RFID tags, using the level power method. However, LANDMARC system suffers from long latency for the position calculation and the variation in behavior of tags. VIRE [17] worked on the same principle of LANDMARC by using the virtual reference elimination method, to locate tags in a virtual reference tag and enhance the performance to avoid interference and multipath issues in indoor localization. Their system optimizes the accuracy in locating objects and achieved 0.47 m accuracy, when compared to the LANDMARC system.

TASA [18] was the first system which introduced tag-free principle in indoor localization. Their method was a hybrid approach (using passive tags and active tags), which was more cost-effective compared to other systems which used active tags such as LANDMARC and VIRE. TASA used group behavior monitoring in the large area to reduce the error of localization in passive RFID systems, which is caused by multipath. Twins [19] implemented the solution of motion detection using device-free passive RFID tags. The authors introduced the model by using two adjacent tags to optimize object localization. Twins depend on TASA principles and only used passive tags as a reference. The system achieved error location (0.75 m) compared to TASA and LANDMARC [16]. The limitations of approaches TASA [18] and Twins [19] depend on online mining frequent trajectory patterns.

Another interesting work by Ruan et al. [20] introduced a new approach which tracks moving subjects based on classification tasks. They used learning-based classification methods (GMM-based HMM model and kNN-based HMM), to localize subjects from RSSI-observed values of RSSI distributions at each grid. Moreover, they introduce a multivariate Gaussian mixture model (kNN- and HMM-based) to track moving subjects based on continuous sequences of RSSI.

Many of these solutions relied on active tags to get higher accuracy which are more expensive in indoor localization, compared to passive ones, while other solutions require deploying tracking resources, and that will result in adding more costs and more complex solutions. Since optimizing the accuracy of tracking subjects was the target of most studies, a crucial factor such as cost-effectiveness

is investigated while designing and implementing smart home solutions, especially for people with limited ability to afford to pay for an expensive system.

7.3 Limitations in Localization Systems Using RFID Tags

Although many RFID techniques have been developed to optimize the localizing accuracy in mobile tracking of subjects and objects, accuracy of the tracking is still a significant research gap in locating tracked objects and people in stationary and real-time movement using RFID sensors. In smart home settings, multiple factors can significantly affect the precision of the results, including (1) localization method used to track subjects, (2) the space of the testing (localization coverage size), and (3) the distance between targeted objects and sensing devices (e.g., sensors and readers). Also, the orientation of tagged objects (e.g., RFID tags) from the sensors also plays a significant role in getting better accuracy during the localization.

Large-scale tracking methods to determine continuous movements of an individual in indoor spaces are still a challenge in smart home systems. This requires having an effective approach that can deal with various localization scenarios at various places and coverages. Most available systems perform the localization in limited coverage spaces and hypothetical scenarios. To adopt such a system in a real-life scenario, further research needs to address large-scale localization [21, 22]. This requires designing the right approach and implementing the appropriate tools. In addition, inexpensive technologies should be taken into consideration when designing such systems.

Multi-resident tracking is another problem in indoor localization. Uncounted residents during the localization will cause noise in the data and, eventually, will lead to lower accuracy in tracking a specific target [21]. According to [23], the accuracy will decrease due to the increment in resident's occupancy. The experimental results usually show that the algorithms may be highly accurate when tracking a single resident. However, they fell rapidly once multiple residents are presented in monitoring space. It is important to investigate new methods and algorithms that track individuals accurately in the real and complex environments.

7.4 Accuracy Optimization

According to these localization works in RFID location-based systems, it has required further research on developing accurate, robust, and cost-effective solution in smart home settings in healthcare for enhancing elderly personal monitoring. In this section, we present our preliminary work toward optimizing the accuracy in subject localization in smart homes.

7.4.1 Localization Framework

Taking important factors such as cost and subject tracking's accuracy, we have proposed a localization framework using passive RFID tags [24] (Fig. 7.1). The localization platform aims to use minimal tracking recourses to optimize the accuracy. We use one RFID reader connected by three RFID antennas and one targeted passive RFID tag in the experiment. Our system obtained promising accuracy in the center of tracking area, with 16.5 cm (average error).

The proposed localization framework in Fig. 7.1 is divided into three main processes. The first is tag selection procedure to determine the best candidate tags for localization processes. This is involved in methodical sets of testing to detect the most readable candidate tags. The reading range test aims to examine the tags readability from RFID antenna-based on various tag distances from the RFID antenna. Also, it attempts to determine the best performing tags among all RFID tags. The power level evaluation aimed to find the tags that have the best RSSI readings among all tags. Tags sensitivity was to evaluate the response of the tags at various reader power levels.

In the second procedure, tags calibration is designed to evaluate the candidate tags performance on several stationary locations, tags orientations, and tags readings at various readings from each antenna. Finally, localization algorithms procedure is designed to find suitable algorithms from the proposed framework. To get the received signal strength indication (RSSI) values, Friis transmission equation [25] was examined to estimate the tag backscatter signal power received (PR). Then to determine the location of the target tag at stationary, we used trilateration algorithm [26, 27] and average moving filter for smoothness of the reading signals.

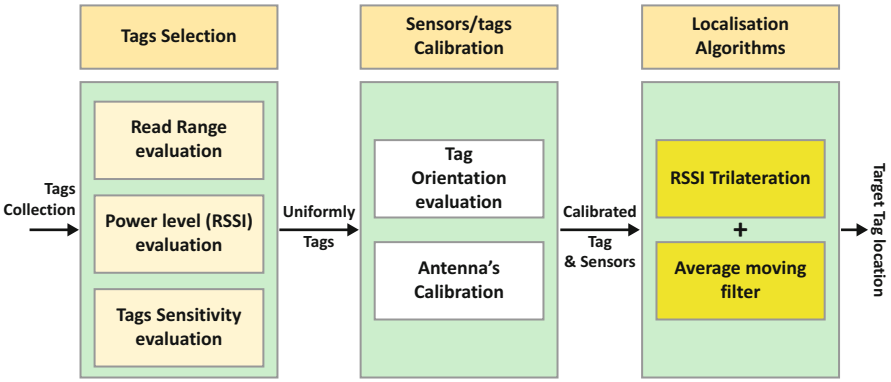


Fig. 7.1 Passive RFID localization framework for smart homes

Fig. 7.2 Platform setup and Monza 4D "target tag in the middle of the platform"

7.4.2 Localization Experiments

According to localization challenges that were mentioned in Sect. 7.3, we have introduced localization prototype (Fig. 7.2), and to validate our localization framework, several experiments were carried out using Impinj Speedway R420 development kit with UHF RFID Reader [24]. Also, we have chosen Monza 4D tag as our target tag for localization purpose (Fig. 7.2). Extensive experiments were utilized to find the best readable tag and then to decide the best tag orientation and placement from each antenna. Also, we have adjusted the tags height of each antenna and calibrated the amount of the power sent by the reader to each antenna to achieve best reading results. According to results analysis, we found that the closer the tag to the center of localization platform, the higher accuracy we received. Our system located the tag positions successfully at stationary with an average error of 16.5 cm in the center grid (size is 0.6 m $\times$ 0.6 m). The highest accuracy obtained was 2 cm at the center of the center grid. Some limitation of our system has been found, especially spots outside the central area and blind spots with the lowest accuracy results [24].

7.5 Conclusion

Smart home researches have broadened in the last few years as many studies have contributed in the pervasive healthcare system to assist impaired individuals. RFID is a promising technology due to its affordability and noninvasive tracking of individuals. Although a smart home technology such as RFID system has benefited the development of the researches in health and personal monitoring, it is not a mature field and requires further improvement. Accuracy in determining the location of an individual precisely is still a research challenge. It is important to understand

the nature of the activities that are carried on, for further healthcare assistance. In addition, cost-effective solution in smart home settings for well-being is still a significant challenge. This requires developing methods and techniques that obtain good results with lost-cost solutions.

This paper explored smart homes and related work on RFID-based localization systems. Also, this paper identified the need for improving the accuracy in localization in smart home systems and the importance of providing affordable, efficient solutions for elderly and impaired individuals. The paper proposed a localization framework and the implemented system in a simple manner and setup to demonstrate its effectiveness.

At this early stage, we are working on improving our existing system to obtain better results. We experienced problems, such as variations in RFID signals as well as angle of arrival reading differences; we aim to implement signal algorithms to optimize the RSSI readings and optimize the overall system performance. Also, we are going to investigate the fluctuations in RSSI values using phase of angle. We will investigate more about tracking individuals and their interactions with the environment and how successfully the system can differentiate between their activities of daily living.

References

1. Fafoutis, X., Tsimbalo, E., Mellios, E., Hilton, G., Piechocki, R., & Craddock, I. (2016). A residential maintenance-free long-term activity monitoring system for healthcare applications. *EURASIP Journal on Wireless Communications and Networking, 2016*(1), 1.
2. AsDI (ADI). (2015). *World Alzheimer Report 2015: The global impact of dementia*. London: Author.
3. Alsinglawi, B., Elkhodr, M., Nguyen, Q. V., Gunawardana, U., Maeder, A., & Simoff, S. (2017). RFID localisation for internet of things smart homes: A survey. arXiv preprint. arXiv:170202311.
4. Aldrich, F. K. (2003). Smart homes: Past, present and future. In *Inside the smart home* (pp. 17–39). London: Springer.
5. Wan, J., O'grady, M. J., & O'hare, G. M. (2015). Dynamic sensor event segmentation for real-time activity recognition in a smart home context. *Personal and Ubiquitous Computing, 19*(2), 287–301.
6. Alsinglawi, B., Nguyen, Q. V., Gunawardana, U., Maeder, A., & Simoff, S. (2017). RFID systems in healthcare settings and activity of daily living in smart homes: A review. *E-Health Telecommunication Systems and Networks, 6*(01), 1.
7. Chan, M., Estève, D., Escriba, C., & Campo, E. (2008). A review of smart homes—Present state and future challenges. *Computer Methods and Programs in Biomedicine, 91*(1), 55–81. https://doi.org/10.1016/j.cmpb.2008.02.001.
8. Mautz, R. (2012). *Indoor positioning technologies*. Habilitationsschrift ETH Zürich.
9. Zhao, Y., & Smith, J. R. (2013). A battery-free rfid-based indoor acoustic localization platform. In *2013 IEEE international conference on RFID* (pp. 110–117).
10. Liu, H., Darabi, H., Banerjee, P., & Liu, J. (2007). Survey of wireless indoor positioning techniques and systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 37*(6), 1067–1080.

11. Ting, S., Kwok, S. K., Tsang, A. H., & Ho, G. T. (2011). The study on using passive RFID tags for indoor positioning. *International Journal of Engineering Business Management, 3*(1), 9–15.
12. Kim, S.-C., Jeong, Y.-S., & Park, S.-O. (2013). RFID-based indoor location tracking to ensure the safety of the elderly in smart home environments. *Personal and Ubiquitous Computing, 17*(8), 1699–1707.
13. Cislo, N. (2010). Under nutrition prevention for disabled and elderly people in smart home with bayesian networks and rfid sensors. In *Aging friendly technology for health and independence* (pp. 246–249). Berlin: Springer.
14. Postolache, G., Girão, P. S., Moura, C. M., & Postolache, O. (2011). Rehabilitative TeleHealth-Care for post-stroke outcome assessment. In *2011 5th international conference on pervasive computing technologies for healthcare (PervasiveHealth 2011)* (pp. 408–413). IEEE.
15. Gu, H., & Wang, D. (2009). A content-aware fridge based on RFID in smart home for home-healthcare. In *2009 11th international conference on advanced communication technology (ICACT)* (pp. 987–990). IEEE.
16. Ni, L. M., Liu, Y., Lau, Y. C., & Patil, A. P. (2004). LANDMARC: Indoor location sensing using active RFID. *Wireless Networks, 10*(6), 701–710.
17. Zhao, Y., Liu, Y., & Ni, L. M. (2007). VIRE: Active RFID-based localization using virtual reference elimination. In *2007 international conference on parallel processing (ICPP)* (p. 56). IEEE.
18. Zhang, D., Zhou, J., Guo, M., Cao, J., & Li, T. (2011). TASA: Tag-free activity sensing using RFID tag arrays. *IEEE Transactions on Parallel and Distributed Systems, 22*(4), 558–570.
19. Han, J., Qian, C., Wang, X., Ma, D., Zhao, J., Zhang, P., et al. (2014). Twins: Device-free object tracking using passive tags. In *2014 Proceedings IEEE INFOCOM* (pp. 469–476). IEEE.
20. Ruan, W., Yao, L., Sheng, Q. Z., Falkner, N. J., Li, X. (2014). TagTrack: device-free localization and tracking using passive RFID tags. In *Proceedings of the 11th international conference on mobile and ubiquitous systems: Computing, networking and services, 2014. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering)* (pp. 80–89).
21. Crandall, A. S. (2011). Behaviometrics for multiple residents in a smart environment.
22. Bouchard, K., Bilodeau, J.-S., Fortin-Simard, D., Gaboury, S., Bouchard, B., Bouzouane, A. (2014). Human activity recognition in smart homes based on passive RFID localization. In *Proceedings of the 7th international conference on PErvasive technologies related to assistive environments* (p. 1). ACM.
23. Crandall, A., & Cook, D. (2011). *Tracking systems for multiple smart home residents. Human behavior recognition technologies: Intelligent applications for monitoring and security* (pp. 111–129). Hershey: IGI Global.
24. Alsinglawi, B., Liu, T., Nguyen, Q., Gunawardana, U., Maeder, A., & Simoff, S. (2016). Passive RFID localisation framework in smart homes healthcare settings. *Studies in Health Technology and Informatics, 231*, 1.
25. Shaw, J. A. (2013). Radiometry and the Friis transmission equation. *American Journal of Physics, 81*(1), 33–37.
26. Cook, B., Buckberry, G., Scowcroft, I., Mitchell, J., Allen, T. (2005). Indoor location using trilateration characteristics. In *Proceedings of the London communications symposium* (pp. 147–150).
27. Bouet, M., Dos Santos, A. L. (2008). RFID tags: Positioning principles and localization techniques. In *Wireless days, 2008. WD'08. 1st IFIP* (pp. 1–5). IEEE.

Chapter 8
Internet Traffic Flow Analysis in Fog Computing: An Experimental Case Study

Waleed Rafiq, Abdul Wahid, Munam Ali Shah, and Adnan Akhunzada

Abstract Fog computing (FC) is a new model, which extends cloud computing services to the edge of computing networks. Different aspects of FC, such as security, have been extensively explored in the existing research. However, the research focuses on how to identify and secure the FC devices and how these devices communicate within the intranet. We believe that it is very important to investigate how the extant infrastructure responses, when a huge amount of data is generated by FC devices. We also need to make sure that the existing network infrastructure will not be chocked, causing the existing services to block. Additionally, the security and privacy are huge concerns for FC. Consequently, by applying the security policies, how will the network respond? Will it make it even worse or improve the performance? In this research, our contribution is twofold. Firstly, we integrate the performance issues of FC network infrastructure for parameters such as throughput, delay, load, etc. Secondly, we analyze the overheads that are generated because of deploying security in FC.

8.1 Introduction

Fog computing is a new model, which extends cloud computing services to the edge of computing networks. Different aspects of FC, such as security, have been extensively explored in the existing research. However, the research focuses on how to identify and secure the FC devices and how these devices communicate within the Intranet. We believe that it is very important to investigate how this infrastructure responses when a huge amount of data is generated by FC devices. We also need to make sure that the existing network infrastructure will not be chocked, causing the existing services to block. Along with that, the security and privacy are the

W. Rafiq · A. Wahid · M. A. Shah · A. Akhunzada (✉)
Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan
e-mail: abdulwahid@comsats.edu.pk; mshah@comsats.edu.pk; a.qureshi@comsats.edu.pk

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_8

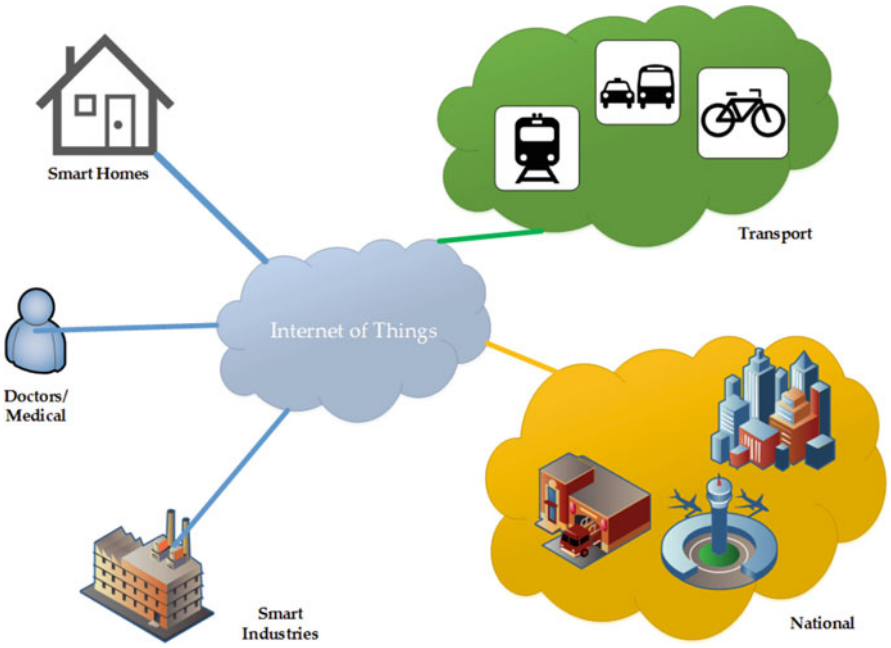


Fig. 8.1 Fog computing overview

huge concern for FC, so by applying the security policies, how will the network respond? Will it make it worse or improve the performance? In this research, our contribution is twofold. Firstly, we integrate the performance issues of FC network infrastructure for parameters such as throughput, delay, load, etc. Secondly, we analyze the overheads that are generated because of deploying security in FC (Fig. 8.1).

8.1.1 Architecture

The FC depends on many factors to communicate and exchange information between the smart objects. Smart objects are the things which can take decisions based on the sensors and the principles defined [1].

Communication Medium Naming and identification is the first step as these smart objects can't communicate without the unique identification. Internet integration is another integral part, as without any internet medium, these smart objects cannot communicate with other objects. Some of the technologies which can be used in FC for proper naming and tracking of the objects are radio-frequency identification (RFID), electronic product code (EPC), object naming service, 6LoWPAN, near-field communication (NFC), and wireless sensor networks (WPS) [2].

Network Architecture Most of the focus in FC had been given on how a specific device will communicate with the gateway which is short-ranged high-speed communication, but there is no investigation how the FC works if it has to use the Internet to communicate. In the FC, huge amount of traffic will be generated, and if the traffic is not carefully diverted, bandwidth limitation can choke the entire network [3, 4].

8.2 Literature Review

We review different papers related to our work and the overall FC network infrastructure. We divide papers into different categories.

8.2.1 FC Challenges

FC can incorporate visibly different heterogeneous end systems, while for the growth of digital services, it provides open access to different data subsets too. Because of a large variety of devices and services, it is a challenging task to build up an architecture for FC. Focusing on urban FC system, the author in [5] has discussed urban FC system as the broader category, which is being characterized specifically by its application domain. In this paper, a survey of different communication technologies, architectures and protocols of urban FC is presented. It has also been analyzed different solutions that are available nowadays for the urban FC implementation. Also Fig. 8.2 shows the current challenges for the FC network infrastructure in a graphical form.

In [1], different issues related to the FC have been addressed including the need to increase the network scale and device proximity which in turn fulfill the scalability issues. Those challenges have questioned the security, privacy, and safety of FC devices. In FC safety and security are somehow related to the behavior of FC devices, how much they are able to avoid or prevent any suspiciously behaving devices. Lack of end-host firewalls and antivirus is one of the reasons for extreme security challenges. Security in FC is meant to protect private information from leaking them without user's permission. We divided the genetic section into three main modules: (i) congestion modules, (ii) reliability module, and (iii) priority module [6].

8.2.2 Network Performances

We discuss the corporate network performances and how existing network is affecting it by an increase in delay and throughput. In [7], a case study of a

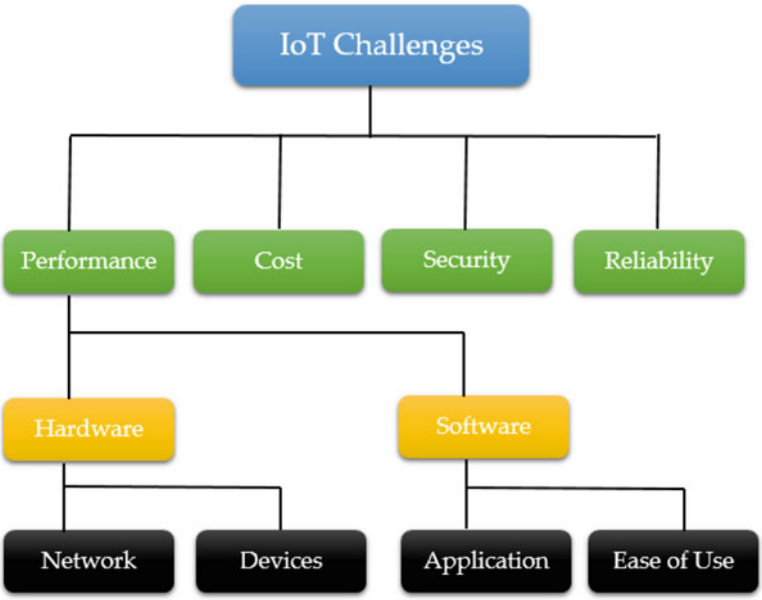


Fig. 8.2 Challenges for FC Network Infrastructure

university campus network has been considered. To achieve the better performance, the existing network needs to be optimized. The performance of the network is heavily dependent on network configuration, the device configuration, the topology of network, and the overall capacity of those networks. In this paper, the authors identified the problems in existing networks and provided the appropriate solution to overcome those limitations. The solution provided in this paper is first to deny any no prioritized traffic by enforcing the policies, second is to configure firewall, third is to use the Cisco routers, and the last one is to maximize the ISP link capacity.

FC can use wireless network virtualization to optimize its communication for the wide area networks. The wireless network virtualization can have a very broad scope. In other words, virtualization, regardless of wired or wireless networks, can be considered as a process splitting the entire network system [8]. The figure is discussed in the paper [9]; a survey is conducted for wireless network virtualization. Generally, the framework of wireless network virtualization can be composed of four main components: radio spectrum resource, wireless network infrastructure, wireless virtual resource, and wireless virtualization controller. The wireless network virtualization focuses on the throughput (bps), delay (sec), path lengths of nodes, and utilization, whereas the traditional wireless networks focuses more on the coverage, QoS, spectrum efficiency, etc. [10]. The author then discusses about the technologies for which the wireless network virtualization can be used. It can be used in existing IEEE wireless standard of 802.11, the new mobile network technologies like 3G and LTE. Also, WiMAX and other wireless standards like ad

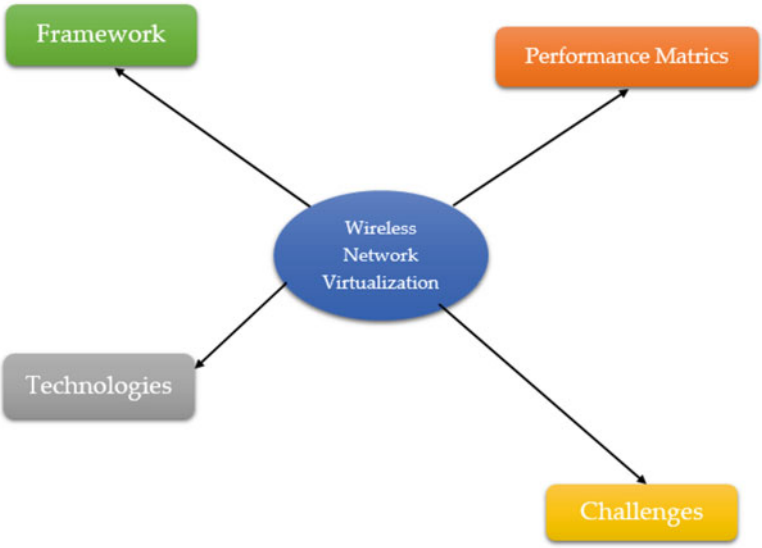


Fig. 8.3 Wireless network virtualization

hoc networks can use that virtualization as well to optimize the performance. This is somehow a relatively new technique, so there will be a number of challenges. Some security concerns along with some resource discovery and network management issues are discussed [11–16]. In summary, research on wireless network virtualization is quite broad, and it has a number of research issues and challenges. But, the wireless community can address these challenges. The FC will be very beneficial with the wireless network virtualization, and it can help the FC network to grow rapidly without compromising on any of the performance. Wireless network virtualization can be seen in Fig. 8.3.

8.3 Experimental Evaluation of the Smart Cities

We aim to simulate different network topology and network traffic scenarios to observe the performance issues for the existing network infrastructures for FC. We further aim to incorporate the security overheads in the existing network simulation scenarios.

8.3.1 OPNET Simulation

The simulation scenario is divided into two parts:

Table 8.1 Simulation parameters for intercity communication

Parameters	Without fog computing	With fog computing
Simulation time	10 min	10 min
No. of time simulation run	1	1
Time to complete simulation	23 min	3 h 23 min
Video pixel size	352 × 240	128 × 240
Video frame time	15 frames per sec	20 frames per sec
Packet size	Constant	Constant
LAN users	15 on each LAN	15 on each LAN
Type of service	Best effort	Streaming multimedia
Traffic mix	75 percent	75 percent

1. Intercity networks: A scenario where different cities communicate with each other
2. Intercity networks with fog computing: A scenario where different cities communicate with each other

8.3.2 Complete Intercity Network Scenario

In this section, we simulate both networks. The results are compared with the other FC scenarios so that we get the better idea. We are using eight applications with six profiles, and each application is set on the heavy usage of the Internet. Table 8.1 has simulation parameters for intercity communication.

This scenario represents the network performance at a larger scale. The city users from one city communicate with the other city users, and lots of routers and ISP involve in such kind of communication which can cause some delay. Figure 8.4 has the complete scenario diagram in OPNET. In this scenario, we evaluate the performance of network.

8.4 Comparative Analysis

In this section, we are comparing the simulation results based on the average delay and average throughput.

Figure 8.5a shows the average delay between the two scenarios; it shows clearly that by increasing the number of devices and the type of traffic, we have larger delays. The normal network has 0.3 s or 300 ms delay. The FC network has an average delay of about 1.3 s or 1300 ms which is quite a large delay. The average delay of the FC can be clearly seen that it is higher. We are using the live streaming

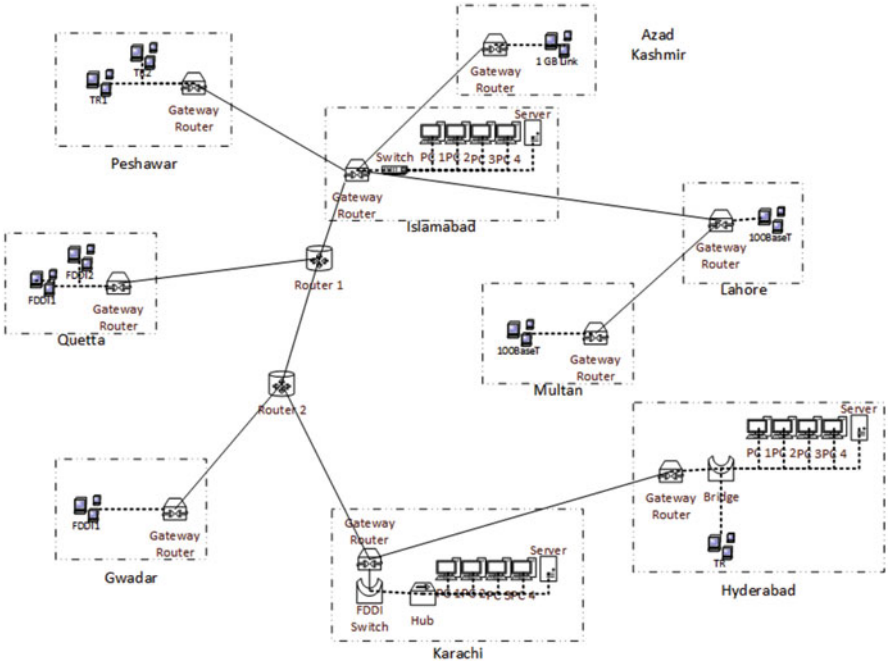


Fig. 8.4 Intercity communication complete scenario

as the type of service, so it has higher priority. This graph refers to Fig. 8.5a, the live streaming profile starts at 100, and after 300 s it restarts; that is why we are seeing a stabilized graph at 350 to 400 s, and then it suddenly peaks again. The network without the FC has two multimedia profiles which end with the simulation, so we see a smooth and stable graph.

Figure 8.5b shows the communication between the router 1 and router 2 in terms of packets/sec, and it can be clearly seen that the average throughput of the FC network is quite high as the normal network. Both are almost identical as both peak at similar time and then a small downhill progresses at the same time as well; the only difference is that FC graph has higher throughput. By comparing the different results in the intercity communication scenarios, we can conclude that the FC devices have the impact on the existing network architecture. A city-based network with the delay of 300 ms can get to the delay of 1300 ms of 1.3 s in the FC environment, which is quite large in today's world. Also, the difference between the loads on the links is higher; the average throughput in networks without FC is 315.4, and in FC environment, it is 404.5 packets.

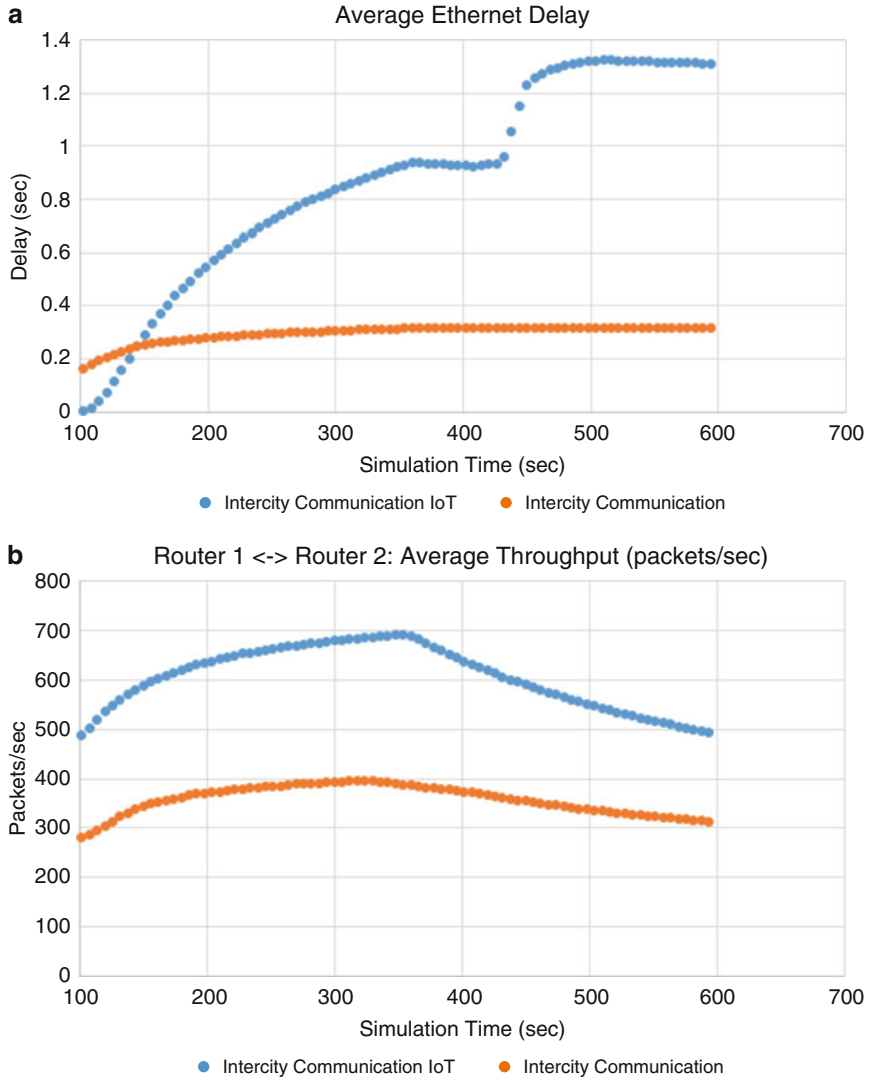


Fig. 8.5 (**a**) Average Ethernet delay. (**b**) Average throughput router 1 to router 2

8.5 Conclusion and Future Work

The main objective of this research is to explore the FC network and its compatibility with the existing networks. We reviewed the literature related to the FC networks, but no or very little work has been done in exploring what we are doing, which is performance evaluation of FC with the existing network infrastructure. For performance evaluation, we use the scenarios and simulate them in OPNET.

For intercity communication, we created a scenario in which different city users can communicate with each other. The simulation result shows little increase in delay and load on the network. In the future, we would like to introduce any routing protocol which will optimize the network traffic as well as decrease the delays on the network. Second thing is to introduce any security technique which has very little impact on the network and does not increase the delays of the network.

References

1. Khan, F., ur Rahman, I., Khan, M., Iqbal, N., & Alam, M. (2016, September). CoAP-based request-response interaction model for the internet of things. In *International Conference on Future Intelligent Vehicular Technologies* (pp. 146–156). Cham: Springer.
2. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *Communications Surveys and Tutorials, IEEE, 17*(4), 23472376.
3. Jin, J., Gubbi, J., Luo, T., & Palaniswami, M. (2012). Network architecture and QoS issues in the internet of things for a smart city. In *2012 International Symposium on Communications and Information Technologies (ISCIT)* (p. 956961). Piscataway, NJ: IEEE.
4. Khan, F., ur Rehman, A., Usman, M., Tan, Z., & Puthal, D. (2018). Performance of cognitive radio sensor networks using hybrid automatic repeat ReQuest: Stop-and-wait. *Mobile Networks and Applications*, 1–10.
5. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal*, *1*(1), 2232. [Online]. Available: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6740844
6. Jan, M. A., Jan, S. R. U., Alam, M., Akhunzada, A., & Rahman, I. U. (2018). A comprehensive analysis of congestion control protocols in wireless sensor networks. *Mobile Networks and Applications, 23*(3), 1–13.
7. Ijaz, S., & Shah, M. A. (2016). Smart cities: A survey on security concerns. *International Journal in Advanced Computer Science and Applications (IJACSA), 7*(2), 612–625.
8. Akhunzada, A., Gani, A., Anuar, N. B., Abdelaziz, A., Khan, M. K., Hayat, A., et al. (2016). Secure and dependable software defined networks. *Journal of Network and Computer Applications, 61*, 199–221.
9. Akhunzada, A., Sookhak, M., Anuar, N. B., Gani, A., Ahmed, E., Shiraz, M., et al. (2015). Man-at-the-end attacks: Analysis, taxonomy, human aspects, motivation and future directions. *Journal of Network and Computer Applications, 48*, 44–57.
10. Jan, M. A., Tan, Z., He, X., & Ni, W. (2018). *Moving towards highly reliable and effective sensor networks*. Philadelphia: Old City Publishing.
11. Usman, M., Yang, N., Jan, M. A., He, X., Xu, M., & Lam, K. M. (2018). A joint framework for QoS and QoE for video transmission over wireless multimedia sensor networks. *IEEE Transactions on Mobile Computing, 17*(4), 746–759.
12. Jan, M. A., Nanda, P., He, X., Tan, Z., & Liu, R. P. (2014, September). A robust authentication scheme for observing resources in the internet of things environment. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 205–211). Piscataway, NJ: IEEE.
13. Jan, M. A., Khan, F., Alam, M., & Usman, M. (2017). A payload-based mutual authentication scheme for internet of things. *Future Generation Computer Systems*.
14. Khan, F., Khan, M., Iqbal, Z., ur Rahman, I., & Alam, M. (2016, September). Secure and safe surveillance system using sensors networks-internet of things. In *International Conference on Future Intelligent Vehicular Technologies* (pp. 167–174). Cham: Springer.

15. Jan, M., Nanda, P., Usman, M., & He, X. (2017). PAWN: A payload-based mutual authentication scheme for wireless sensor networks. *Concurrency and Computation: Practice and Experience, 29*(17).
16. Khan, F. (2014). Secure communication and routing architecture in wireless sensor networks. In *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)* (pp. 647–650). Piscataway, NJ: IEEE.

Chapter 9
Seven Pillars to Achieve Energy Efficiency in High-Performance Computing Data Centers

Sardar Mehboob Hussain, Abdul Wahid, Munam Ali Shah, Adnan Akhunzada, Faheem Khan, Noor ul Amin, Saba Arshad, and Ihsan Ali

Abstract Nowadays, data centers and high-performance computing (HPC) systems are crucial for intensive computing environments. The energy efficiency in HPC is an evergreen problem. Moreover, energy-efficient design and energy ecology measures are core challenges in HPC. However, current research focuses on practical methods to measure power utilization to take decisions for green computing without exceeding resources and without compromising on performance. This paper surveys the issues, challenges, and their solutions over the period 2010–2016, by focusing on the energy consumption of data centers and HPC systems. We grouped existing problems in energy efficiency that data centers are currently facing. Our contribution is twofold. Firstly, with this categorization, we aim to provide an easy and concise view of the underlying energy efficiency model adopted by each approach. Secondly, we propose seven-pillar framework for energy efficiency in HPC systems and data centers for the first time.

9.1 Introduction

Performance has always been a core issue in the modern computer world which usually refers to speed [1]. Microprocessor clock rate has rapidly increased in performance; however, on the other hand, it has also caused even greater power usage [2]. About a decade ago, energy efficiency was not a main focus in most data

S. M. Hussain (✉) · A. Wahid · M. A. Shah · A. Akhunzada · S. Arshad
Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan
e-mail: abdulwahid@comsats.edu.pk; mshah@comsats.edu.pk; a.qureshi@comsats.edu.pk

F. Khan · N. ul. Amin
Department of Computer Science, Bacha Khan University, Charsadda, Pakistan

I. Ali
Department of Computer Systems and Technology, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_9

centers and HPC systems [3]. However, now it has diverted all focuses onto it and became an increasingly important consideration in HPC [4]. In data centers, where data increases in exponential manners, it is hard to possibly manipulate it.

Unlike traditional warehouses, big data is stored in different manners. The stored data needs to be rinsed first, grouped, and secured [5]. Besides, there comes the situation to access mountains of data where efficiency matters. The IT industry has to store a huge amount of data as logs to deal with the issues that can occur on and off in order to solve them. This data is kept only for a short period of time or might be stored for longer time due to importance of data [6]. Because of large volume and semi-structured nature, the traditional systems are not capable to handle with these logs. Big data analytics not only deal with mountainous data but also enrich it with long life storage [7].

In addition, these logs vary with hardware and software updates. Due to the sensor data in its two states, i.e., *motion* and *rest*, the safety, profit, and efficiency all need huge amount of data to be analyzed for good commercial consequences. As data centers consume a large amount of energy, therefore low power matters more than speed or performance [2]. It never means that performance is less important than energy efficiency but means achieving more performance using minimal power. In November 2001, NERSC's (National Energy Research Scientific Computing Centre) new 3 teraflop HPC system, consuming less than 400 KW of electrical energy, was ranked at #3 on the TOP500 lists of most powerful computers. In November 2007, NERSC's 100 teraflop successor, using almost 1500 KW, was not ranked even in the top 10 powerful computers of TOP500 list [3]. The researchers are working to develop sustainable energy-efficient HPC infrastructure. The statistical data obtained from TOP500 list is presented in Table 9.1. According to the TOP500.org list in June 2011, the power consumption of HPC has increased at higher rate than their power efficiency.

This research work elaborates the problems in energy efficiency which data centers are currently facing. The article includes elicit solutions for prescribed issues

Table 9.1 Average power consumption and average energy efficiency

	TOP500 highlights in June 2011	
	Average power consumption	Average energy efficiency
TOP500 systems	Average power consumption of a TOP500 system has increased to 543 KW, from 447 KW 6 months ago and 397 KW 1 year ago	Average power efficiency has increased to 248 W/Mflops (Mega Floating-Point Operations Per Second), from 219 W/Mflops in 6 months ago and 195 W/Mflops 1 year ago
TOP10 systems	Average power consumption of a TOP10 system is 4.3 MW (up from 3.2 MW 6 months ago)	Average power efficiency is 464 Mflops/W up from 268 Mflops/W 6 months ago

and also a critical review of relevant research work published over 2010–2015. Some standards and strategies are proposed for improvement in energy efficiency in data centers and HPC systems. Majorly, seven-pillar framework of energy efficiency in HPC systems and data centers is proposed. The rest of the paper is organized as follows. In Sect. 9.1, an introductory material of paper is provided. Section 9.2 comprises of the survey, and Sect. 9.3 consists of our contribution followed by solution to prescribed problems. Section 9.4 evaluates the performance of respected modules and the proposed solutions. Last but not the least, Sect. 9.5 ends up by concluding the research finding and future directions.

9.2 Background and Related Work

In recent years, researchers have done a lot of research in HPC systems and big data. Performance remained a core achievement in data centers, but very minimal intuition toward energy usage, consumption, and wastage was given which led toward huge wastage of power and energy. Many researchers did the research in different areas related to energy and power, but HPC systems have not focused a lot on power and energy efficiency [3] due to lack of measurement capability available for large platforms.

In 1999, Huber and Mills claimed that energy consumption by these data centers is alarming with respect to overall energy ingested by the whole USA. The study showed that energy consumption by data centers in the USA is 1–2% of the total energy uptake in the USA. Energy management has become prime consequence in HPC because energy usage and energy-associated costs of HPC are expanding for data centers and servers. So, stimulating energy-efficient design and energy ecology measures are emerging key challenges for effective development of HPC such as servers, girds, clusters, and data centers, so big data can be handled conveniently. Controlling energy or power consumption is a critical aspect for reducing operational cost of HPC in big data. Therefore, designing energy-efficient machines is the most important upcoming goal of HPC.

A data center having 1000 racks of 10MV has a total cost of nearly 7 million dollar for power generation and 4 million to 8 million for cooling [8]. Big data means bigger problems as data centers deal with 1000s of terabytes of data daily. As stated in the studies of 2010, the world lead to over 1ZB (zettabyte) of data, and by 2014, we are generating more less 72ZB of data a year [9]. It is realistic that the data centers are many times as energy exhaustive as the big office buildings. Data traffic is growing day to day in every field of science and technology. NASA database contains too much data concerning space, APIs, and climatic changes, and medical field database contains data on the cures, diagnosis, and treatment of the diseases [10]. HPC devices play an integral part in the processing of data collected from different sources like the Internet to the storage media in the data centers.

Energy efficiency in HPC and big data is influenced by two main elements which are categorized into two chunks [2]: hardware and software. So, we describe how

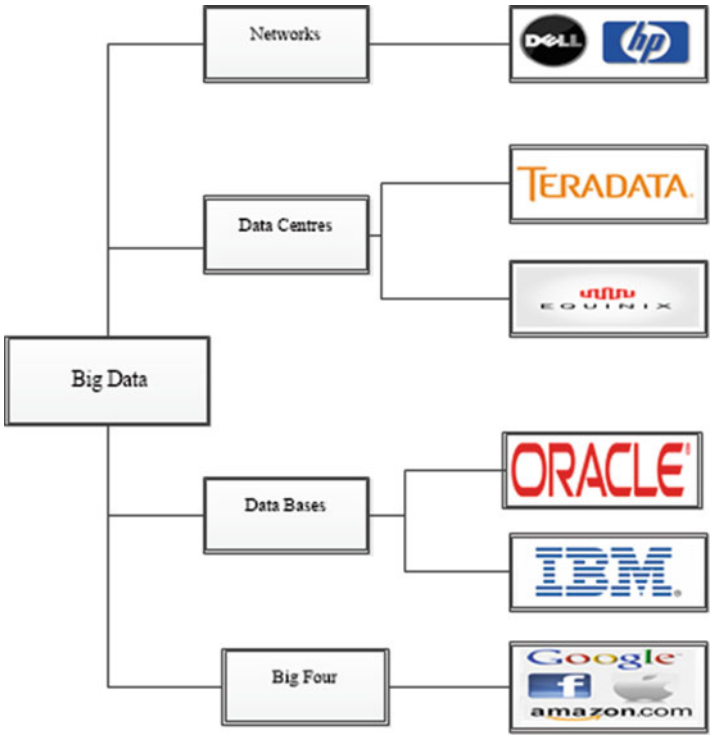


Fig. 9.1 Represents pictorial overview of organizations having big data centers, networks, and databases which are dealing with big data

these two, hardware and especially software (operating system and applications), can influence the energy efficiency. Figure 9.1 shows the organizations which have to deal with big data continuously. Figure 9.2 presents the visualization of power usage in data centers. Existing and ongoing HPC research in power management and energy efficiency has addressed the issues at different levels, consisting of resource allocation, data center design, and cooling techniques [11].

Due to the data in its two states (motion and rest), the safety, profit, and efficiency all require huge amount of data to be analyzed for good commercial consequences [12]. Financial institutes have to model data, so the risk can be calculated under a certain threshold. HPC is a broad term that works on lots of computational problems at the same time; therefore it is also known as an application of parallel processing [13]. The electrical power demands of HPC systems are reaching a limit, causing future threats [14] to the growth of advanced application programs and scientific computational tasks. Therefore, to overcome this future thread, researchers are focusing on improving energy efficiency in HPC for performing these tasks more quickly, efficiently, and reliably.

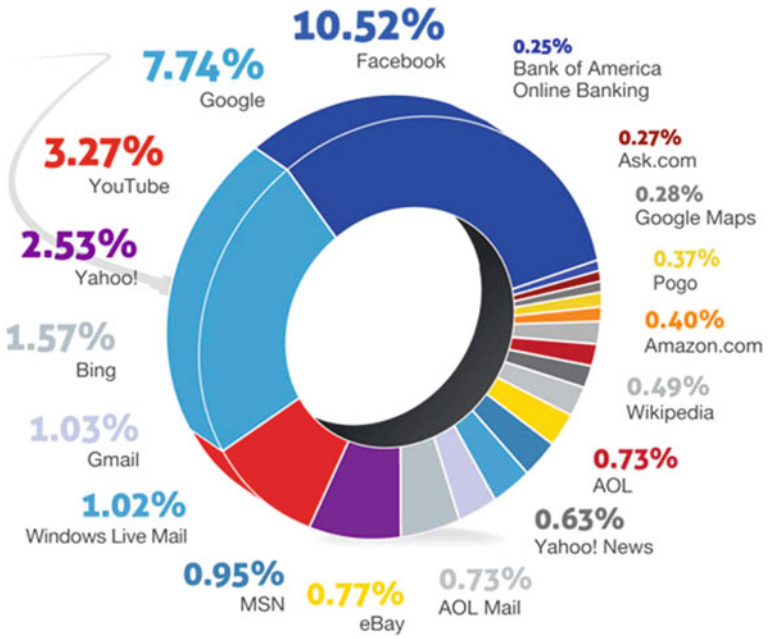


Fig. 9.2 Data center power use pattern

9.3 Seven-Pillar Framework

In [15, 16], four-pillar framework and three-dimensional approach to sustainability are proposed, respectively. This paper extends [15] and [16], and for the first time, the seven major pillar frameworks for energy efficiency in HPC and big data centers are proposed. Seven-pillar framework provides the foundation for developing energy efficiency models in HPC. Two main problems can be solved by using seven-pillar framework: first, presenting existing research efforts and works to outside stakeholders and providing base for planning future work and, second, understanding all external and internal efforts for improving the HPC data centers' energy efficiency and categorizing them. Table 9.2 shows the proposed pillars, their goals, and a short view to detail (a comprehensive view). The novel proposed seven pillars are described below.

9.3.1 Energy-Efficient Infrastructure

"Building energy-efficient infrastructure," the first pillar of HPC, is non-IT infrastructure required to operate HPC systems [17]. The objective of this pillar is to improve the energy efficiency of big data and HPC systems by carbon usage

Table 9.2 Seven proposed pillars, their goals, and details

Pillars	Goal	Details
1. EE infrastructure	Enhance major performance indicator	Minimize power leakage in the supply chain; better cooling technologies; reuse dissipated heat from IT systems; check and validate actions taken by monitoring all related information
2. EE system hardware	Minimize hardware power utilization	Use most recent semiconductor technologies; use of energy economic memory and processor technologies; use of special hardware or accelerators designed for particular problems; provide sensors for detailed power measurements
3. EE system software	Optimize resource handling tune system	Support workload management; make sure the energy-saving features of the platforms by modification in the systems relating to the applications' needs; shut down inactive requirements; examine the energy consumption of all system components
4. EE applications	Increase application performance	Use the most efficient and powerful algorithms; use the best libraries for the system; use the most proficient and efficient programming
5. EE network	Maximize hardware utilization	Use energy-efficient appliances; keep the system as busy as possible; reduce UPS and electrical power usage for cooling; lake near installation; reuse of hot and cold water
6. EE policy	Reverse engineering of network deployed	Instrumenting network for power saving; dissemination and outreach Reduce routing overhead, delay by decreasing number of retransmissions; keep track of hot and cold aisle; power supply chain monitoring
7. EE usage	Reduction in wastage of energy	Use of humidifier and dehumidified; switching system off and on as easy; energy-efficient devices; equipment replacement; insulation and air sealing; resource distribution; reuse wasted energy

effectiveness (CUE), power usage effectiveness (PUE), energy reuse effectiveness (ERE), water usage effectiveness (WUE), etc. Many industrial bodies have addressed this infrastructure [18]. It has also been discussed in research work and standardization organization. The main features of this pillar are (1) reduction of energy loss, challenges, and threats to energy-efficient HPC [19], (2) use of efficient cooling technologies, and (3) reuse of waste heat [20]. It is expected that energy reuse will turn into a significant part of any feasible exascale computing approach

[21]. By adopting energy-efficient infrastructure, a huge portion of problems can be addressed.

Architecture of the Data Center Importance should be given on the infrastructure of the data center such as arrangement of the cooling tower fans and the chiller plant that can significantly improve performance and efficiency [22]. Although after implementation it saves energy enormously to increase efficiency, implementation costs of the architectures like two-tier and three-tier are very hard and consume too much resources.

Liquid Cooling Liquid cooling gives better results than air cooling because it can efficiently transfer concentrated heat loads and because liquid has higher heat transfer coefficient. Water flow provides very efficient ways of transporting heat; moreover, water also requires less energy to move from one place to another with respect to air. Water flow carries approx. 3500 times as much heat than air [23]. Water-cooled systems can save not just energy but also space.

Chiller Systems HPC systems need chiller systems to reduce energy emission. IBM uses direct-to-rack water cooling because of the presence of vast majority of the equipment. This technique is normally not good for electricity consumption, and highly efficient cooling systems can be selected to reduce liquid cooling usage, by as much as 40–50%. The whole data center environment can be considered into three primary subsystems; in a given data center, the power delivery system includes electric power resources, the networking system includes all connectivity and racks, and the cooling infrastructure includes central chillers and computer room air conditioners. These subsystems are basically the fundamental building blocks of a data center.

9.3.2 Energy-Efficient System Hardware

"Energy-efficient system hardware," the second pillar of HPC, shows all IT systems, storage systems, and networks of HPC. What is needed is a storage architecture that delivers high performance, has the ability to scale for very large environments, and is cost-effective [24]. The main objective of this pillar is to reduce the power consumption of system hardware.

Storage System Architecture Available large-scale HPC systems are facing inadequate storage problems [25]. This pillar develops solid-state storage simulator supported by DRAM, and thus it makes HPC applications more scalable and reliable. In HPC environment, special demands are placed on the storage infrastructure. These environments have supercomputers or cluster of computers, each having unique chronological tasks that randomize when it uses shared storage infrastructure backing it [23]. So, one of the goals of this pillar is designing cost-effective and more powerful storage architecture for large-scale HPC systems by reducing hardware power consumption.

The Modern HPC Storage Architecture HPC storage infrastructures are almost completely different than conventional storage area network (SAN). Nowadays, small number of file serving storage nodes is also included in HPC designs, for supporting large number of application compute nodes. Most modern HPC systems and data centers use RAID (redundant array of independent disks) model which provides an efficient storage and improves performance by adding redundancy and striping of data.

Hardware Storage Capacity and Efficiency Improvement by Vendors Luckily, in this area, HPC systems or HPC data centers' managers need not to be involved directly because hardware vendors take steps to improve hardware efficiency and storage capacity. For example, Sandy Bridge technology by Intel provides lots of new power-saving and energy-efficient features [26]. IBM is investigating about the reusing possibilities given by hot-water-cooled supercomputers, and for memory efficiency, Intel is working on frequency scaling and dynamic voltage. Many such other institutes are working to improve their hardware technologies.

Future of HPC Hardware Future generations of HPC hardware will have higher efficiency, improved scalability, control functions, flexibility, and better monitoring. Although vendor product availability is constrained on hardware, there are ways to set up innovative advancement. For example, by adding operational (energy) costs and system costs in an acquisition plan of a business deal or agreement, the vender will actively work at more energy-efficient product development [27].

9.3.3 Energy-Efficient System Software

"Energy-efficient system software," which is the third pillar, represents all system-level software for controlling system hardware. It also provides platform for running application software. The objectives for this pillar are the best utilization of the available resources, allocation of system resources, file and disk management, and monitoring system activities. Workload management system can be used according to HPC policies and goals by taking advantage of energy-efficient and power-saving features of hardware and the application needs and by reduction of idle resources whenever it's possible. System software capabilities can also be determined by both hardware and some hardware functions that can be done with higher-level software support. For example, if CPU provides support for P-states but operating system does not provide its support, then CPU will not be able to use these.

Virtualization In HPC environments, the use of virtualization technologies has customarily been refrained due to their intrinsic performance overhead. With the use of virtualization, we can improve energy efficiency in system software. A single hardware can be used to run multiple operating systems by which every operating system will run independent of each other with very low performance degradation. Virtualized data centers are envisioned to provide better management

flexibility, lower cost, scalability, better resource utilization, and energy efficiency [28]. Even though the data center network is lightly utilized, virtualization can still cause significant throughput instability and abnormal delay variations, which in result improves overall efficiency. Sometimes the virtualization stipulates very slight performance results which depend on the type of hypervisor; however, such technologies are acute, and all virtualization techniques are not always equal. KVM hypervisor is the favorable selection for supporting HPC applications.

9.3.4 Energy-Efficient Application Software

"Energy-efficient applications," the fourth pillar, shows all user applications on HPC systems. The purpose of this pillar is to optimize an application's performance with specific hardware to improve its scalability and raw performance by selecting the best libraries that are suitable for particular architecture, the most efficient algorithm, and the right programming paradigms.

9.3.5 Energy-Efficient Network

The reprogramming becomes necessarily more and more important for a number of reasons. However, the reprogramming generates a sizeable amount of data which leads to huge energy consumption and investment. So, by using energy-efficient reprogramming scheme with Raptor code by using transmission power control, we can play with this drawback [29]. Batch architectures are inadequate to operate with big data because it causes latency. Experts made distinction between two-tier architecture and a three-tier architecture, where a third application or business layer is affixed that acts as an intermediary between the data layer and client or presentation layer. It can also eliminate many kinds of problems with confusion, which can be caused by multiuser access in two-tier architectures [30]. However, the advanced complexity of three-tier architecture may mean more cost and effort [31]. This can increase the performance of the system and can help with scalability.

9.3.6 Energy-Efficient Policy

As policy makers give a renewal attention to energy preservation issues, it has regularly been declared that a gap of energy efficiency exists between optimal and actual energy usage. Five separate and distinct notions of optimality are defined in paper [32], the economists' economic potential, the technologists' economic potential, the hypothetical potential, the narrow social optimum, and the true social optimum. Each of these has associated with it a corresponding definition of the

energy efficiency gap. An economic stance on the variety of market barriers, market failures, and behavioral failures has been quoted in the energy efficiency context. Energy efficiency and consumption are key means, but corresponding market behavior and policy reaction have led debates in the economic literature.

9.3.7 Energy-Efficient Usage and Load Balancing

Energy composition and peak power demand both are increasing and becoming major challenges in HPC. A significant part of power is devoted to cooling. It is a well-known fact that HPC and big data center spend 40% to 50% of their budget for cooling of computer rooms [33]. By using the systems according to needs, we can also save a lot of energy; a sleep mode in computer is one best example. When computer is not in use partially, moving it on sleep mode saves more or less 60% of energy used when on. So, for load balancing, we'll have to reduce this cooling energy. Execution time and temperature control come at the cost of each other [34]. Big data centers now reduce the total energy and temperature by switching the machines off and on. Another interesting example that differs energy consumption of SSD over SATA is conspicuous. So, use of SSD instead of SATA will be a better decision toward energy efficiency.

9.4 Performance Evaluation

To evaluate the performance of the respected modules/factors, we describe their properties in Table 9.3, such as the implementation cost, energy savings, and reduction in CO_2, and assume their values on the basis of details given above about them. HPC application development is different than traditional application development in different aspects as these are used for read-world simulation, modeling, and virtualization. Air cooling efficiency is lower than water cooling efficiency, and efficiency of water cooling is relatively more than 300 times higher [34] compared to efficiency of air cooling. Now, here in Table 9.4, we discussed relative data centers' issues and emerging strategies.

9.5 Conclusion

With the rapid proliferation of data centers and HPC systems around the globe, the energy requirements are increasing. Different from single PC environment, the solutions are aimed at preventing energy wastage and meaningless energy consumption in data centers. The rapid use of energy to just improve performance degrades in terms of cost and energy usage and wastage. In this work, firstly, we

Table 9.3 Issues and emerging strategies of data centers

Issues	Emerging strategies
Availability	Shift to efficient hardware: Server, storage, and network Power and cooling infrastructure
Technology advances	Design data centers for efficiency Arrange rooms Configure racks
Energy efficiency	Shift loads real time Use most efficient hardware Operate at optimum load
Dynamic infrastructure management	Turn off Manage hardware and space Asset utilization

Table 9.4 Performance comparison of energy efficiency in HPC and big data

Implementation cost (scale of economy)	Energy savings		Reduction in CO_2 emission
External factors			
Liquid cooling	Cheaper	High	40–50%
Maintenance process	Expensive	Medium	
Internal factors			
Air management	Cheaper	Medium	5–10%
Chiller systems	Expensive	High	40–50%
Early warning system model	Expensive	High	70–90%
Architecture	Expensive	Medium	40–80%

surveyed the literature published during 2010–2016 related to the current scenario of energy efficiency by summarizing its evolution along with some examples. We also outlined current and future threats and reported some predictions for the near future. Secondly, we categorized energy-efficient solutions in seven pillars and also exascale as future of HPC systems. In the future, our motivation is toward energy consumption at component level and toward the deep study of deployed hardware and network. Our focus will be to investigate the energy efficiency in storage mechanisms and storage architectures.

References

1. Liu, Y., & Zhu, H. (2010). A survey of the research on power management techniques for high-performance systems. *Software Practice and Experience, 40*(11), 943–964.
2. Computing, M. (2013). Energy awareness in HPC: A survey. *International Journal of Computer Science and Mobile Computing, 2*, 46–51.
3. Kamil, S., Shalf, J., & Strohmaier, E. (2008). Power efficiency in high performance computing. In *2008 IEEE International Symposium on Parallel and Distributed Processing* (pp. 1–8).

4. Fürlinger, K., Klausecher, C., & Kranzlmüller, D. (2011). The AppleTV-Cluster: Towards energy efficient parallel computing on consumer electronic devices. In *White paper*. Ludwig-Maximilians-Universitat.
5. Philip Chen, C. L., & Zhang, C.-Y. (2014). Data-intensive applications, challenges, techniques and technologies: A survey on big data. *Information Sciences, 275*, 314–347.
6. Katal, A., Wazid, M., & Goudar, R. H. (2013). Big data: Issues, challenges, tools and good practices. In *2013 6th International Conference on Contemporary Computing IC3 2013* (pp. 404–409).
7. Wu, X., Zhu, X., Wu, G.-Q., & Ding, W. (2014). Data mining with big data. *IEEE Transactions on Knowledge and Data Engineering, 26*(1), 97–107.
8. Xu, X., Lin, G., & Wang, J. (2014). An adaptive model of energy consumption predictor for big data centers. In *Proceedings of 2014 International Conference on Computer, Communications and Information Technology* (pp. 60–64).
9. Villars, R. L., Olofson, C. W., & Eastwood, M. (2011). *White paper big data: What it is and why you should care information everywhere, but where's the knowledge?* (pp. 1–14).
10. Reed, D. A., & Dongarra, J. (2015). Exascale computing and big data. *Communications of the ACM, 58*(7), 56–68.
11. Hpc, E. (2009). *The challenge of energy efficient HPC* (pp. 50–57). Doctoral dissertation, Louisiana State University.
12. Wilde, T., Auweter, A., & Shoukourian, H. (2014). The 4 pillar framework for energy efficient HPC data centers. *Computer Science, 29*(3–4), 241–251.
13. Lövehagen, N., & Bondesson, A. (2013). *Evaluating sustainability of using ICT solutions in smart cities – Methodology requirements*.
14. Agrawal, D., Das, S., & El Abbadi, A. (2011). Big data and cloud computing: Current state and future opportunities. In *Proceedings of the 14th International Conference on Extending Database Technology* (pp. 530–533).
15. Kambatla, K., Kollias, G., Kumar, V., & Grama, A. (2014). Trends in big data analytics. *Journal of Parallel Distributed Computing, 74*(7), 2561–2573.
16. Rodero, I., Viswanathan, H., Lee, E. K., Gamell, M., Pompili, D., & Parashar, M. (2012). Energy-efficient thermal-aware autonomic management of virtualized HPC cloud infrastructure. *Journal of Grid Computing, 10*(3), 447–473.
17. Kaisler, S., & Armour, F. (2013). Big data: Issues and challenges moving forward. In *2013 46th Hawaii International Conference on System Sciences (HICSS)* (pp. 995–1004). Maui, HI: IEEE.
18. Michel, B., Brunschwiler, T., Meijer, G. I., Paredes, S., & Escher, W. (2010). Direct waste heat utilization from liquid-cooled supercomputers. In *14th International Heat Transfer Conference, Washington* (p. 23352).
19. Torrellas, J., Quinlan, D., & Livermore, L. (2012). *Thrifty: An exascale architecture for energy-proportional computing* (pp. 2011–2012).
20. Bakshi, K. (2012). Considerations for big data: Architecture and approach. In *2012 IEEE Aerospace Conference* (pp. 1–7).
21. Valentini, G. L., Lassonde, W., Khan, S. U., Min-Allah, N., Madani, S. A., Li, J., et al. (2013). An overview of energy efficiency techniques in cluster computing systems. *Cluster Computing, 16*(1), 3–15.
22. Zimmermann, S., Meijer, I., Tiwari, M. K., Paredes, S., Michel, B., & Poulikakos, D. (2012). Aquasar: A hot water cooled data center with direct energy reuse. *Energy, 43*(1), 237–245.
23. Crump, G. (2014). The modern HPC storage architecture. *Journal of Parallel and Distributed Computing, 74*(7), 2561–2573.
24. Demchenko, Y., & Zhao, Z. (2012). Addressing big data challenges for scientific data infrastructure. In *IEEE 4th International Conference* (pp. 614–617).
25. Huber, H., Auweter, A., Wilde, T., Meijer, I., Archer, C., Bloth, T., et al. (2012). Case study: LRZ liquid cooling, energy management, contract specialities. In *2012 SC Companion: High Performance Computing, Networking Storage and Analysis* (pp. 962–992).
26. Zomaya, A., Lee, Y., Ge, R., & Cameron, K. (2012). Power-aware high performance computing. In *Energy-efficient distributed computing systems*. Hoboken, NJ: Wiley.

27. Meijer, G. I. (2010). Cooling energy-hungry data centers. *Science, 328*, 318.
28. Younge, A. J., Henschel, R., Brown, J. T., von Laszewski, G., Qiu, J., & Fox, G. C. (2011). Analysis of virtualization technologies for high performance computing environments. In *2011 IEEE 4th International Conference on Cloud Computing* (pp. 9–16).
29. Clarke, J., Kirk, K., Collins, J., Chopra, A., & Renard, K. (2011, September). *Project HPC: A multi-tier architecture for simulation and analysis*.
30. Mitra, S. (2014). Using UML modeling to facilitate three-tier architecture projects in software engineering courses. *ACM Transactions on Computing Education, 14*(3), 1–31.
31. Jaffe, A. B., & Stavins, R. N. (1994). The energy-efficiency gap: What does it mean? *Energy Policy, 22*(10), 804–810.
32. Gupta, A., Sarood, O., Kale, L. V., & Milojicic, D. (2013). Improving HPC application performance in cloud through dynamic load balancing. In *2013 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing* (pp. 402–409).
33. Tiwari, A., Laurenzano, M. A., Carrington, L., & Snavely, A. (2012). Modeling power and energy usage of HPC kernels. In *2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum* (pp. 990–998).
34. Rodero, I., & Parashar, M. (2012). Energy efficiency in HPC systems. In *Energy-efficient distributed computing systems* (pp. 81–108). Hoboken, NJ: Wiley.

Chapter 10
Scheduling Algorithms for High-Performance Computing: An Application Perspective of Fog Computing

Sidra Razzaq, Abdul Wahid, Faheem Khan, Noor ul Amin, Munam Ali Shah, Adnan Akhunzada, and Ihsan Ali

Abstract High-performance computing (HPC) demands many computers to perform multiple tasks concurrently and efficiently. For efficient resource utilization and for better response time, different scheduling algorithms have been proposed which aim to increase throughput, scalability, and performance of HPC applications. In this paper, our contribution is twofold. Firstly, the classification of scheduling algorithms on the basis of multiple factors like throughput, waiting time, fairness, overhead, etc. is presented. This paper investigates the recent research that has been carried out from 2009–2017. With this categorization, we aim to provide an easy and concise view of the HPC algorithms. Secondly, the forecasting has been done on HPC applications to predict the growth rate for 2020 and beyond.

10.1 Introduction

Nowadays, HPC infrastructure is vastly growing in commercial and financial sectors and in many domains which require high computations to assure the quality, cost, and reliability. It is evolving due to the wide demand of its applications for parallel

S. Razzaq · A. Wahid (✉) · M. A. Shah · A. Akhunzada
Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan
e-mail: sp17-rcs-010@student.comsats.edu.pk; abdulwahid@comsats.edu.pk; mshah@comsats.edu.pk; a.qureshi@comsats.edu.pk

F. Khan · N. ul. Amin
Department of Computer Science, Bacha Khan University, Charsadda, Pakistan

I. Ali
Department of Computer Systems and Technology, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia
e-mail: ihsanalichd@siswa.um.edu.my

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_10

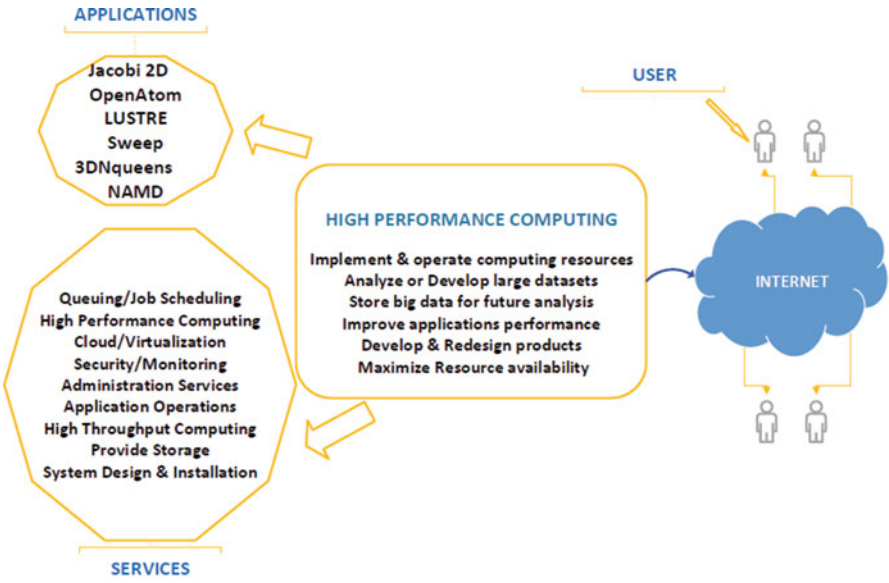


Fig. 10.1 HPC architecture with applications and services

processing which requires large amount of memory storage, high bandwidth, low latency networks, and systems at large scale specialized to fulfil high requirements of users. Its architecture has been shown in Fig. 10.1.

Some authors discussed different platforms such as cloud and cluster, and they proposed a trade-off between performance and cost for HPC applications. Due to high demand as compared to single server requirement, the HPC application requires parallel processing, while to fulfil these requirements, specialized systems are designed, which are supercomputers [1]. According to authors, the purpose of HPC applications in cloud is to reduce the work load, latency, and cost while increasing the speed, scalability, fairness, and performance. Since the early stage of cloud computing, research work is continued by considering areas of resource allocation and scheduling, high memory storage, security problems, and many more [2].

Studies have been performed among different scheduling algorithms [3]. The authors describe cloud computing performing its role to minimize the tasks execution time while improving the performance with better utilization of resources [4]. The existing algorithms perform action in different scenarios having some merits and demerits, which results in trade-off, while HPC applications require some attributes that can fulfil the requirements of an infrastructure. However, we could not provide the best one scheduling algorithm for resource allocation because it varies with increasing demands of resource requirements and particular environment needs.

In this paper, we discuss different scheduling algorithms to analyze which algorithm suits best according to the resource needed on basis of some performance parameters. They require execution or demand for resources and give users full comfort zone by fulfilling their needs and requirements [5]. As each algorithm addresses different problems and results, therefore, different scheduling algorithms have been discussed here such as GA, FCGS, SJF, RR and ACO. Also, we compare them on basis of performance parameters like throughput, CPU utilization, response time, scalability, cost effectiveness, waiting time, etc. to achieve high accuracy and compatibility for HPC applications in cloud. Different scheduling algorithms surveyed over the period 2009–2017 are presented and a comparison is made based on parameters to present their time complexity.

The paper is organized as follows. Section 10.2 presents some background study. Section 10.3 describes challenges HPC is currently facing along with the future trends and predictions in the market and the scheduling algorithms. Section 10.4 discusses the results. Finally, in Sect. 10.5, the conclusion and future work are presented.

10.2 Background Study

In this section, we discuss the previous surveys and practical work done on task scheduling algorithms. The authors used some existing techniques having comparison of performance parameters, or some had presented hybrid techniques to overcome the problems.

The authors provided a comprehensive analysis to provide a framework for three classified HPC infrastructures, cloud, grid, and cluster, for achieving resource allocation strategies. However, it would be great if they worked on analysis of system's performance [6]. The important part to be considered is the hourly cost and performance, for which they provide a fair comparison of the providers and efficiency for cloud to run applications [7]. Two points should be considered in the selection of an appropriate provider to run these applications, i.e., the behavior of the target applications and the intended usage scenario. In [8], the authors show different infrastructures with their specifications to describe the performance of HPC applications.

This paper [9] proposed a scheduling model of genetic algorithm with the comparison of three existing algorithms, i.e., round-robin, load index-based, and the ABC-based task scheduling model, to evaluate the quality of given tasks by user. Systems could become better if they minimized the cost and risk factor while increasing the adaptability factor. Authors [10] worked on a problem by making improvement with the use of hybrid genetic algorithm to achieve effectiveness. Since cloud computing has higher requirements, with the passage of time, user expectations also increased the resource allocation framework considering the control parameters (efficiency, cost, performance, execution time) to get user comfort [11]. When the problem size grew, then chances of dimensionality breakdown

also become higher in cloud computing. With the use of evolutionary algorithms like genetic algorithm (GA), particle swarm optimization (PSO), and ant colony optimization (ACO), they are more scalable, and then dynamic programming to satisfy user's QoS, application performance, and cost could be improved [12–16]. In these papers, the authors proposed ideas for improved differential evolution algorithm (IDEA) that worked for receiving, processing and waiting time. By considering the limitations and merits of scheduling algorithms, it helped many things to be done accordingly. However, algorithm limitations might be covered up slightly using hybrid approaches [17]. Cloud computing deals with workflow instances concurrently but needs efficiency in terms of execution and time cost. Authors proposed workflow scheduling algorithm to efficiently minimize both execution time and cost named compromised time cost algorithm [18].

Previously, work has been done to get high efficiency in cloud computing on global scale. Cloud providers require high power to run large computing applications while providing best services to the users [19]. The problem was tried to minimize by using many existing and proposed techniques with 1% of improvement. Superior performance optimization procedure was proposed to minimize the execution time of processor by using the insertion time scheduling policy [20]. The quantitative evaluation of all applications can be improved according to authors by identifying the characteristics required to run application and provides resources accordingly on large networks. With scheduling, the network performance could be minimized with consistent dealing of tasks efficiently [8]. Amazon is one of the infrastructure services providing solution, and here applications need to scale and speed up from Amazon HPC cloud to cluster. It could be improved with 20% efficiency. However, if it exceeds this limit, then the network interconnect bandwidth problem will occur [21].

10.3 HPC Challenges and Future Predictions

The users of HPC applications always demand high computational speed. For this purpose, operational cost varies from time to time [3]. It is in the interest of system users to tune very efficiently to make the effective use of hardware. Therefore, the system users are focused on performance optimization to give comfort zone to the application users and reduce the cost [22].

Thus, the resource scheduler performs important work, and its job is not very simple; its basic requirement is cluster utilization which needs to be improved without increasing the power budget. However, their job profiles vary for systems which are dominant in operational cost of high-performance computing to manage workloads [23]. The [24] authors briefly explain the HPC challenges in detail.

At system level, the HPC market is entering at peak level. For many years, the architecture is widely used to make an optimal balance in processor speed, I/O, and memory access. According to Goldman Sachs study, spending on cloud computing infrastructure and platforms is increasing 30% annually.

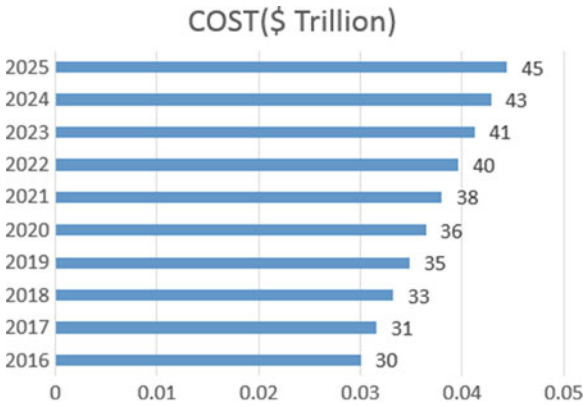


Fig. 10.2 Prediction of HPC Market Revenue

According to [25], the current growth rate of the total market value is $36.9 billion by 2020.The forecast for 2015 was $28.6 billion, while the growth rate for 2020 is $36.9 billion. At broader level, the HPC commercial and industrial market is growing by compound growth rate of 5.2% from 2016 to 2020. Figure 10.2 shows that growth rate will put the value at $45.3 billion at the end of 2025. This graph shows the HPC offerings, such as servers, storage, networks, cloud computing, and other services. From the above cited data, it can be forecasted that the HPC market will keep on increasing on the same rate, and its market value will be 45 trillion from 2016 to 2025.

10.3.1 Task Scheduling

In task scheduling the most important thing is the processor's allocation along with resources with high computation power to increase performance. To fulfil the criteria, there are certain conditions that need to be fulfilled whether the scheduler maintains the stability of the system or whether the performance metrics that are required for scheduling the tasks give the desired output [11]. In this section, the performance metrics are described and used for comparison between algorithms to find out the suitability of the algorithm according to the environment and to let the scheduling be done efficiently.

Performance Metrics There are some performance metrics to be used which are suitable for system like throughput, fairness, waiting time, scalability, performance, etc. from which some are described in Table 10.1 for making a comparison of scheduling algorithm.

Scheduling Algorithms In this section different scheduling algorithms are discussed in detail with their merits and demerits [26, 27]. In Table 10.2 the comparison of scheduling algorithms has also been discussed.

Table 10.1 Summary of performance metrics

Parameters	Description	Throughput
Throughput	Main concern of scheduling, task done per unit time, time range vary with specific process	Maximum
CPU utilization	Complete CPU cycles with 100% utilization	Maximum
Scalability	System characteristic to be competent to fulfil high operational needs	High
Turnaround time	Total time from submission of process to completion	Minimum
Fairness	Equally share CPU among processes	Equality
Fault tolerance	Check system capability to continue working of processes in case of components failure	High
Waiting time	Total time spent to wait for execution in ready queue	Minimum
Response time	Total time between submission of process to CPU and getting feedback	Minimum
Overhead	Occurs during context switching while CPU does nothing	Low

10.3.1.1 First Come First Serve (FCFS)

This algorithm works with first in first out (FIFO) queue policy in which request comes first to the CPU, which is allocated to that process straightly. It never compromises in this policy. It deals with all processes in sequence which causes starvation. Authors proposed an algorithm which includes space sharing technique to resolve the number of queues increasing to equally schedule the processes and avoid starvation [28]. Authors have applied FCFS on five processes, and the results show that average waiting time is increased [29].

- *Merits*: It fairly gives chance to each process and is executed in FIFO.
- *Demerits*: Its throughput is minimized due to longer wait of processes. Likewise, turnaround time and average time get affected for the same reason.

10.3.1.2 Round Robin (RR)

This scheduling algorithm is the concept of Round Robin that takes and gives equal share of time. It works for time sharing systems and time quantum, which equally deals with all coming processes by sharing time. It never deals on priority bases. It is almost like FCFS algorithm, but the difference is that it added preemption to switch between processes. The time quantum should never exceed from 10 to 100 milliseconds. Its performance also depends on time quantum.

- *Merits*: The benefit is that the starvation can never occur as all processes are dealt with one by one without priority.
- *Demerits*: There is a maximum chance of overhead and average waiting time also increased.

Table 10.2 Comparison of scheduling algorithms

Scheduling algorithms	Overhead	Response time	Waiting time	Fault tolerance	Fairness	Scalability	Turnaround time	Throughput	CPU utilization
FCFS	MAX	MAX	MAX	–	MAX	–	MIN	MIN	MIN
RR	MAX	MIN	MAX	–	MAX	–	–	MAX	MIN
SJF	MAX	–	MIN	–	–	–	MAX	MAX	–
GA	MIN	–	–	–	–	–	MIN	MAX	–
ACO	MAX	MAX	–	MIN	–	MAX	–	MIN	MAX

10.3.1.3 Shortest Job First (SJF)

This algorithm works like almost FCFS. It deals with shortest execution time job in sequence. It executes those processes which have short execution time. It is also called Shortest Job Next, because algorithm scheduling depends upon the length of execution time. It is basically just concerned in dealing with less time, so it places them at the start of queue and large time processes at the end of queue.

- *Merits*: The throughput and turnaround time could be high.
- *Demerits*: There is an excessive chance of starvation because it simultaneously deals with shortest execution processes.

10.3.1.4 Genetic Algorithm (GA)

This is a heuristic search algorithm in which random selection is performed to find optimal solution. GA has three basic phases, i.e., selection, crossover, and mutation. In selection, it selects two random parents from population. Their selection is based on the fittest one from the population. The roulette selection method can be used to find the fittest one. Authors took the task scheduling problem for achieving high performance as NP problem and combined the GA algorithm with CACO to propose a new algorithm which is genetic algorithm-chaos ant colony optimization (GA-CACO) to overcome the problem [26, 30].

- *Merits*: GA solves problem with multiple solutions to find optimal one.
- *Demerits*: There is no assurance that GA will produce the exact optimum solution.

10.3.1.5 Ant Colony Optimization (ACO)

It is also a metaheuristic optimization algorithm which is inspired by ant's behavior. It is used for finding the optimal path in colony like ants follows the path in search of food and return to their location by following the pheromone trails which they drop on edges of graph [31]. Ants are blind, and they navigate from nest to food by signaling each other. Its main idea is to search for minimum cost path.

- *Merits*: It is efficiently used for travelling salesman problems and gives positive feedback on achieving the solution or food.
- *Demerits*: It takes random decisions at the start, and its convergence time is uncertain.

10.4 Discussion

Based on our study, we have classified some algorithms on basis of possible optimal factors like throughput, CPU utilization, fairness, turnaround time, etc. as shown in Table 10.2. The scheduling algorithms are divided as preemptive and non-preemptive. FCFS and SJF both are non-preemptive, while RR is preemptive. These algorithms are basically used in distributed systems. Some scheduling algorithms maximize the throughput, CPU utilization, and fairness of application, while some minimize the waiting time, response time, and fault tolerance. Overhead is minimized only in case of genetic algorithm. Hence, it is cleared that algorithms can be used based on various performance factors which efficiently increase the performance of applications as per the requirements of consumers and service providers.

10.5 Conclusion and Future Work

In cloud computing, many resources are provided as a service to users and cloud providers. In this work, we presented the classification of scheduling algorithms on the basis of selected factors like throughput, waiting time, etc. to provide help in selection of algorithms according to the requirements of users and providers. We also investigate the recent research that has been carried out from 2009 to 2017, and the forecasting has been done on HPC applications to predict the growth rate from 2016 to 2025.

Research in this field is not yet saturated, and still available improvement is possible, in which various scheduling algorithms shall be implemented on factors to achieve the desired results.

References

1. Gupta, A., & Milojicic, D. (2011). Evaluation of HPC applications on cloud. In *OCS'11 Proceedings of the 2011 Sixth, Open Cirrus Summit (OCS)*.
2. Gupta, A., Kale, L. V., Gioachin, F., March, V., Suen, C. H., Lee, B.-S., et al. (2013). The who, what, why, and how of high performance computing in the cloud. In *2013 IEEE 5th International Conference on Cloud Computing Technology and Science* (pp. 306–314).
3. Balis, B., Figiela, K., Jopek, K., Malawski, M., & Pawlik, M. (2017). Porting HPC applications to the cloud: A multi-frontal solver case study. *Journal of Computational Science, 18*, 106–116.
4. Shimpy, E., & Sidhu, J. (2014). Different scheduling algorithms in different cloud environment. *International Journal of Advanced Research in Computer and Communication Engineering, 3*(9), 2278–1021.
5. Kliazovich, D., Pecero, J. E., Tchernykh, A., Bouvry, P., Khan, S. U., & Zomaya, A. Y. (2016). CA-DAG: Modeling communication-aware applications for scheduling in cloud computing. *Journal of Grid Computing, 14*(1), 23–39.

6. Georgiou, Y., Jeannot, E., Mercier, G., & Villiermet, A. (2017). Topology-aware resource management for HPC applications. In *ICDCN '17 Proceedings of the 18th International Conference on Distributed Computing and Networking* (pp. 1–10).
7. Roloff, E., Diener, M., & Carissimi, A. (2012). High performance computing in the cloud: Deployment, performance and cost efficiency. In *2012 IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom)*. Piscataway, NJ: IEEE.
8. Gupta, A., Faraboschi, P., Gioachin, F., Kale, L. V., Kaufmann, R., Lee, B.-S., et al. (2016). Evaluating and improving the performance and scheduling of HPC applications in cloud. *IEEE Transaction on Cloud Computing, 4*(3), 307–321.
9. Jang, S. H., Kim, T. Y., & Kim, J. K. (2012). The study of genetic algorithm-based task scheduling for cloud computing. *International Journal of Control and Automation, 5*(4), 157–162.
10. Kang, Y., & Zhang, D. (2012). A hybrid genetic scheduling algorithm to heterogeneous distributed system. *Applied Mathematics, 3*(7), 750.
11. Shenai, S. (2012). Survey on scheduling issues in cloud computing. *Procedia Engineering, 38*, 2881–2888.
12. Zhan, Z.-H., Liu, X.-F., Gong, Y.-J., Zhang, J., Chung, H. S.-H., & Li, Y. (2015). Cloud computing resource scheduling and a survey of its evolutionary approaches. *ACM Computing Survey, 47*(4), 1–33.
13. Dillon, T., Wu, C., & Chang, E. (2010). Cloud computing: Issues and challenges. In *2010 24th IEEE International Conference on Advanced Information Networking and Applications* (pp. 27–33).
14. Alkhashai, H. M., & Omara, F. A. (2016). An enhanced task scheduling algorithm on cloud computing environment. *International Journal of Grid and Distributed Computing, 9*(7), 91–100.
15. Abdelaziz, A., Fong, A. T., Gani, A., Garba, U., Khan, S., Akhunzada, A., et al. (2017). Distributed controller clustering in software defined networks. *PLoS One, 12*(4), e0174715.
16. Akhunzada, A., Gani, A., Hussain, S., & Khan, A. A. (2015). A formal framework for web service broker to compose QoS measures. In *2015 SAI Intelligent Systems Conference (IntelliSys)*. Piscataway, NJ: IEEE.
17. Tsai, J.-T., Fang, J.-C., & Chou, J.-H. (2013). Optimized task scheduling and resource allocation on cloud computing environment using improved differential evolution algorithm. *Computers and Operation Research, 40*(12), 3045–3055.
18. Iosup, A., Ostermann, S., & Yigitbasi, M. (2011). Performance analysis of cloud computing services for many-tasks scientific computing. *IEEE Transactions on Parallel and Distributed Systems, 22*(6), 931–945.
19. Garg, S., Yeo, C., Anandasivam, A., & Buyya, R. (2009). Energy-efficient scheduling of HPC applications in cloud computing environments. arXiv Prepr. arXiv.
20. Bahnasawy, N. A., Omara, F., Koutb, M. A., & Mosa, M. (2011). Optimization procedure for algorithms of task scheduling in high performance heterogeneous distributed computing systems. *Egyptian Informatics Journal, 12*(3), 219–229.
21. Hassani, R., Aiatullah, M., & Luksch, P. (2014). Improving HPC application performance in public cloud. *IERI Procedia, 10*, 169–176.
22. Trinitis, C., & Weidendorfer, J. (2017). *Co-scheduling of HPC applications*. Amsterdam: IOS Press.
23. Desai, N., & Cirne, W. (2014). *Job Scheduling Strategies for Parallel Processing: 17th International Workshop, JSSPP 2013, Boston, MA, USA, May 24, 2013 Revised Selected Papers* (Vol. 8429). Berlin: Springer.
24. Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big data and cloud computing: Innovation opportunities and challenges. *International Journal of Digital Earth, 10*(1), 13–53.
25. *Intersect360 publishes new five-year HPC market forecast | TOP500 supercomputer sites*. [Online]. Retrieved April 25, 2017, from: https://www.top500.org/news/intersect360-publishes-new-five-year-hpc-market-forecast/

26. Cui, H., Liu, X., Yu, T., Zhang, H., Fang, Y., & Xia, Z. (2017). Cloud service scheduling algorithm research and optimization. *Security and Communication Networks, 2017*, 7.
27. Rodriguez, M. A., & Buyya, R. (2016). A taxonomy and survey on scheduling algorithms for scientific workflows in iaas cloud computing environments. *Concurrency and Computation: Practice and Experience, 29*(8), e4041.
28. Grudenić, I. (2008). Scheduling algorithms and support tools for parallel systems.
29. Xoxa, N., Zotaj, M., Tafa, I., & Fejzaj, J. (2014). Simulation of first come first served (FCFS) and shortest job first (SJF) algorithms. *International Journal of Computer science and Network, 3*(6), 444–449.
30. Mittal, S., & Katal, A. (2016). An optimized task scheduling algorithm in cloud computing. In *2016 IEEE 6th International Conference on Advanced Computing (IACC), vol. 7, no. 4* (pp. 197–202).
31. Nosheen, F., & Bibi, S. (2013). Ant Colony optimization based scheduling algorithm. In *2013 International Conference on Open Source Systems and Technologies (ICOSST)* (pp. 18–22).

Chapter 11
A Novel Energy-Aware Design for Clustered Wireless Sensor Networks

Sohail Jabbar, Mudassar Ahmad, Abid Ali Minhas, and Syed Hassan Ahmad

Abstract In this paper, we have presented a comprehensive study on designing an aware energy architecture of clustered wireless sensor networks. In continuation to it, we have also analysed our proposed scheme, extended-multilayer cluster designing algorithm (E-MCDA), in a large network. Our novel layer-based hybrid algorithms for cluster head and cluster member selection come up to novel communication architecture. Among its components, algorithms for time slot allocation, minimization of CH competition candidates and cluster member selection to CH play underpinning roles to achieve the target. These incorporations in MCDA result in minimizing transmissions, suppressing the unneeded response of transmissions and near-equal size and equal load clusters. We have done extensive simulations in NS2 and evaluated the performance of E-MCDA. It is found that the proposed mechanism optimistically outperforms the competition with MCDA and EADUC.

11.1 Introduction

Wireless sensor network technology has woven itself into a diverse fabric of applications due to its capabilities for involvement in multidisciplinary research and its nourishing from a well-renowned group of researchers and organizations. Digging its multifaceted capabilities for efficient performance has also unfolded

S. Jabbar · M. Ahmad (✉)
Department of Computer Science, National Textile University, Faisalabad, Pakistan
e-mail: mudassar@ntu.edu.pk

A. A. Minhas
College of Computer and Information Systems (CCIS), Al Yamamah University, Riyadh, Saudi Arabia
e-mail: a_minhas@yu.edu.sa

S. H. Ahmad
Department of Computer Science, Georgia Southern University, Statesboro, GA 30460, USA
e-mail: sh.ahmed@ieee.org

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_11

a variety of issues as its by-product, and hence it has a long list of hot issues to attract researchers' mind to fix those. Among those, the most common are memory, computation issues and, the most important, energy constraint. Sensing, transmitting and receiving are the most energy-squeezing functions in the processes of sensor nodes among which transmission is the most energy-draining function. These constitute a routing phenomenon to communicate or to relay the sensed data destined to a certain destination. Since communication is wireless and mostly the deployment of nodes is random, for a well-structured and energy-efficient communication, various techniques and algorithms are devised and are presented in the literature. A well-planned survey of these techniques and algorithms with the name of factors affecting the energy-aware routing is presented.

Hence, network layer functionalities are of core importance in the communication process, and routing with energy-aware trait is indispensable for improved network performance and increased network lifetime. Designing of protocol at network layer must consider the factors above especially for energy-aware routing process. Two main types of network architectures for the dissemination of sensed data from source to destination exist in the literature, flat network architecture and clustered network architecture. In WSN, there may be hundreds or thousands of sensor nodes communicating with each other and with the base station, which consume more energy in exchanging data and information with the additive issues of unbalanced load and intolerable faults. In flat architecture-based networks, uniformity can be seen since all the network nodes work in the same mode and don't have any distinguished role [1]. So usually no conservation of energy is supported by itself from its architectural setup. Some of the well-known protocols for this network architecture are mentioned in [2–4]. The clustered network is considered to be the most energy-efficient architecture due to its ease of route discovery, fault tolerance, data aggregation and shortest possible end-to-end delay nature [5]. In this paper, we have evaluated and analysed our proposed scheme, extended-multilayer cluster designing algorithm (E-MCDA), in a large network [6]. It is an extended version of MCDA [7]. Our novel layer-based hybrid algorithms for cluster head and cluster member selection come up to novel communication architecture. Among its components, algorithms for time slot allocation, minimization of CH competition candidates and cluster member selection to CH play underpinning roles to achieve the target. These incorporations in MCDA result in minimizing transmissions, suppressing the unneeded response of transmissions and near-equal size and equal load clusters.

The rest of the paper is organized as follows. Literature survey is given in Sect. 11.2. Section 11.3 presents the summarized form of MCDA whose extended version is extended-multilayer cluster designing algorithm. Comparative analysis of E-MCDA with state-of-the-art techniques is given in Sect. 11.4 that is followed by the conclusion in Sect. 11.5.

11.2 Literature Survey

Though the available literature is rich with high-quality articles on energy-aware cluster designing, they seem to be lacking in covering key aspects to handle the energy-aware factors. Yang et al. [8] require either GPS-equipped sensors or some non-GPS technique to complete the working of their proposed solution. The former method increases the cost, while in the latter case, algorithms that correctly identify the node's location are to be implied. That is an extra overhead to face. The same is the case with the idea proposed by Li et al. [9], Yu et al. [10] and Naeem et al. [11]. Some proposed solutions have a formula with parameters like neighbour nodes' distance to BS, their energy, their nodal density, etc. that need intensive message exchange for collecting related information. The proposed solutions by Aslam et al. [12], Chen et al. [13], Naeem et al. [11] and Li et al. [9] follow the same fashion to a complete cluster designing.

Lee et al. [14] adopt a distributed cluster designing approach in their proposed solution, a self-organized and smart-adaptive clustering and routing approach for wireless sensor networks (SOSAC). The involved fitness function in the solution requires information of node degree and node energy locally (one-hop distance) and out of its local area. The rich message exchange is the inseparable part of this information collection process. Another node's energy-draining factor is centralized calculation and decision-making. The proposed solutions in [8, 9, 13] are its typical examples. The proposed solution, an energy-efficient unequal clustering mechanism for wireless sensor networks (EEUC) by Li et al. [9], requires that each node must have the value for maximum distance and a minimum distance of the node from BS among all other nodes. These values are the prerequisites to complete the calculation for identifying the maximum competition radius. On considering the worst case of this scenario, it has all the drawbacks related to the centralized cluster designing in large-scale networks, i.e. rebroadcasting of the received broadcast from the far distant node to communicate their info to the BS. BS then broadcasts the extracted info of maximum distance and minimum distance from the received information. Apart from the above major part of clustered WSN, the other constituents are cluster head selection, cluster head rotation and cluster member selection techniques. In the subsequent paragraphs, a critique on available techniques is given.

Considering the similar scenario among the competing ideas is the prime step for fair competition. Our proposed solution for CH selection takes the scenario of random deployment of homogenous nodes. The ideas for such scenarios that take energy as the CH selection criteria such as [15, 16] may suffer from network cluster with a big difference of their sizes. It may also result in either very small cluster size or very large cluster size. If the former case happens frequently, then the number of clusters is the big count. If the other case occurs, then clusters become overburdened that may result in early drainage of CHs' energy. These issues can be observed in the designed clustered networks of [9, 10, 15, 16]. Similar hazards may also exist in the idea where nodes are randomly selected as CHs such as by LEACH [17] and some of its ramifications like [18, 19].

In the initial round, network nodes' energy is almost the same. So, node degree seems to be a suitable parameter for selection of CH. This choice has the solutions for issues above that are raised due to choosing energy as the CH selection parameter. Our proposed solution, E-MCDA, follows the same strategy. Composite parameters such as node energy and node degree as is in [14] and node energy and distance to BS as is in [8] can also be used, but these are suitable in CH rotation. Most of the algorithms in the literature follow the idea to iterate the same process for CH rotation as is for the CH selection in the first round. This style is adopted in [8, 9, 14–16]. This iteration is scheduled on completing every round, such as in LEACH. Here one round means aggregation of data from CMs at CH and communication of that aggregated data to ultimately sink. This style takes a big share of node's total energy, especially in the re-clustering process. A better idea is to set a threshold to trigger the CH rotation process as is in [20] where CH rotation process is only initiated on the decrease in node density. We believe that this method is much more energy aware compared to the previous one where there is complete re-clustering on every round. This energy-aware method is adopted in [4, 20], etc. The critical point in this approach lies in selecting the threshold value of the selection parameter and the ways on how the next optimal candidate is to find for replacement of the existing CH. Choosing the threshold value of node's degree to be selection parameter for CH rotation makes the management tougher compared to choosing the node's energy for the same purpose. In the first case, triggering of the re-clustering process is dependent on changing the CH's degree that only occurs if there is death of CM. This may mean that along with the death of one node, energy of other CMs is also decreased to the lowest if not drained out since they are also participating in the sensing and communication activities of the cluster. Another dark aspect of not considering the CH's energy itself is that CH goes to die before having any change in its degree (no. of CHs' neighbours, i.e. CM). Moreover, prioritizing the first case may also result in very early initiation of the re-clustering process due to node's malfunctioning or node's death.

11.3 Extended-Multilayer Cluster Designing Algorithm (E-MCDA)

The proposed scheme, E-MCDA, is an extended version of MCDA. It is also a hybrid approach in its communication architecture perspective and architectural design perspective. In this section, we are summarizing MCDA (the prior version of E-MCDA) in brief. A detailed version of it is available in [6].

MCDA uses multilayer approach comprising of the first flat layer in the footprint of BS and the subsequent clustered layers. Designing of the former layer is initiated centrally, while distributed fashion is applied in the designing of the latter. The nodes that are deployed in the flat layer are called as flat layer nodes. The process of clustering the network is started from the second layer and continues until

the boundary of the network. The elected decision-maker nodes of the first layer select the cluster heads in the second layer. In designing the clusters, the key factors are decision-maker nodes, neighbour counter and packet sequence ID with postfix counter. Among these, decision-maker nodes play their role in selection of cluster heads, neighbour counter prefers one node over the other for the selection of decision-maker and cluster head at various steps and the last said factor is the packet ID that groups the nodes and prefers one node over the other in the group for becoming CH. The node with highest neighbouring nodes is elected by the second layer nodes as their decision-maker node. They communicate their node density to their decision-maker nodes to take part in the competition of designating as cluster head. Time division multiple access techniques are used to assign the time slots to these nodes. When the first layer node communicates its node density to the decision-maker node, a sequence number with a postfix counter '0' is assigned to this packet. The recipient nodes of the second layer become the part of the same group and save this packet sequence number. All those nodes are included in the same group that has a packet with the same packet sequence number. The node density for only those nodes is communicated to the decision-maker nodes that have the highest node density as compared to the previous nodes. These nodes increment the postfix counter. This counter separates one group member from the other group member. The first node of the next group communicates its decision-maker node, and a new packet sequence number is assigned with postfix counter '0'. Cluster head is elected by the decision-maker node after collecting the node density of the selected nodes of the second layer. The CH has the highest node density among those nodes that are addressed by the second layer nodes. The 'join request' packets are broadcast by the elected cluster heads. The sensor nodes thus come to know about the availability of specified nodes as CH. A 'join accept' message is sent in response by the recipient nodes to show the consent of becoming a cluster member. In case of receiving the 'join accept' message from multiple CHs, then the current load is the decision parameter for joining the CHs as their member. A constructive ramification of this idea is proposed with the name extended-MCDA (E-MCDA) to ameliorate the performance in network lifetime. Novel algorithms for time slot allocation, minimization of CH competition candidates and cluster member selection to CH play underpinning roles to achieve the target. These incorporations in MCDA result in minimizing transmissions, suppressing the unneeded response of transmissions and near-equal size and equal load clusters.

11.4 Results and Discussion

Considering the simulation parameters given in Table 11.1, we have evaluated the performance of E-MCDA in energy consumption at various aspects.

The impact of controlled broadcasting, selective candidate nodes for being CHs and a hybrid approach is also clearly reflected by the comparative results given in Fig. 11.1. Total energy consumption in E-MCDA is still far better compared to

Table 11.1 Simulation parameters

Parameter	Description
Routing protocols	EADUC, MCDA, E-MCDA (proposed)
Simulation area	1000 m × 1000 m
Simulator	NS 2.31
Data rate	4 packets/s
TCP/IP layer	Network layer
Node to node distance	Random
Node type	Homogenous
No. of nodes	500
Propagation model	Two-ray ground
Initial energy of node	3 J

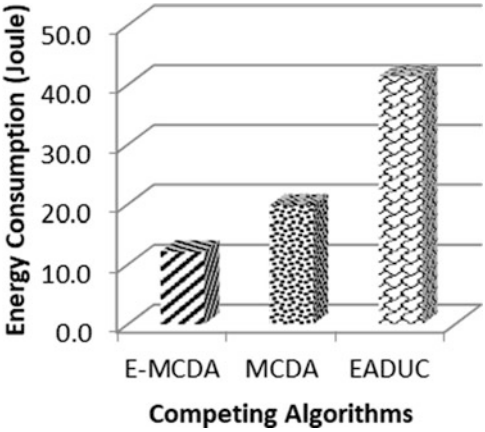


Fig. 11.1 Total energy consumption in cluster designing

MCDA and EADUC. From Fig. 11.1, it is clear that the overall consumption is decreased in the underlying sparse network. Among the effects above, the major one is less number of recipient nodes of some typical broadcast and hence less message in reply.

Hence, in Fig. 11.2, performance efficiency of E-MCDA over MCDA is a bit higher in current deployment area compared to the previous scenario. In MCDA, number of designed clusters is 70% more in 1000 m × 1000 m area compared to node deployment in 500 m × 500 m area. This aspect is stronger in EADUC compared to the other two, since in EADUC, cluster size is unequal. The farther the cluster position from the BS, the bigger is its size. Therefore, this value of the higher number of clusters in the 1000 m × 1000 m area is about 45% compared to another scenario. However, on the other end, the strategy adopted by EADUC in designing these unequal clusters is very expensive due to the information collection for the constituent parameter.

This increases the total energy consumption bar in Figs. 11.1 and 11.2 as well. This style also increases the exchange of messages (Fig. 11.3). Hence, some broadcast in EADUC is 40% higher in under discussion deployment area compared

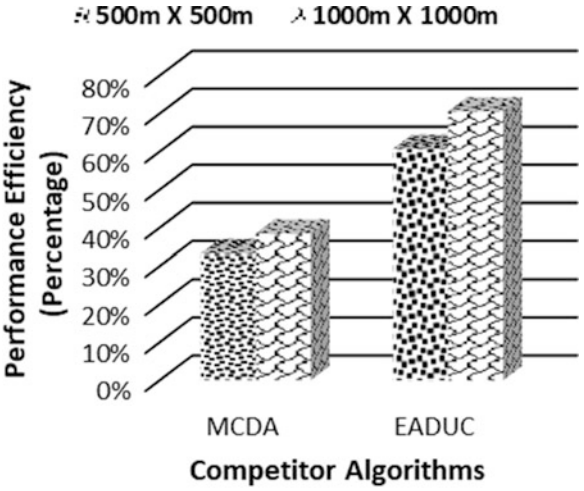


Fig. 11.2 Performance efficiency of E-MCDA in total energy consumption during cluster designing over competitor algorithms

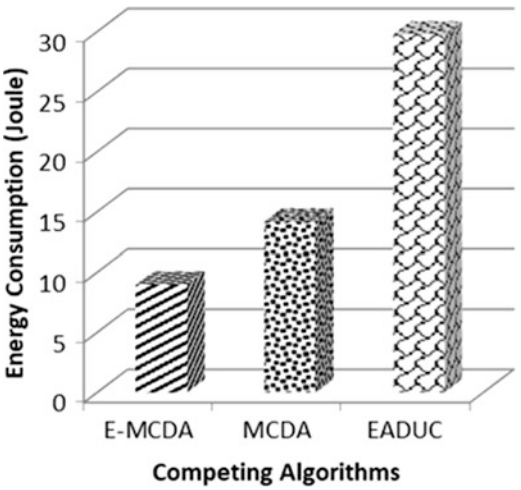


Fig. 11.3 Energy consumption in broadcast transmission

to densely node deployment in 500 m × 500 m, while in MCDA and E-MCDA, this value is 11% and 10%, respectively. Another important effect of increasing the deployment area by keeping the other aspects the same as that in the comparatively smaller area is the decrease in node density in the cluster, i.e. lesser CMs. This has a twofold effect. One is some clusters in the network, and the other is fewer nodes at the intersection point of neighbouring cluster heads' communication range. Sufficient detail has already been dedicated to the first point in previous paragraphs. So far as a decision for affiliation of nodes at intersection points is concerned, it shapes the cluster size and ultimately has its impact on CH rotation or cluster redesigning strategy (Fig. 11.4). A big value of standard deviation in case of EADUC shows higher difference in cluster size compared to that of MCDA and

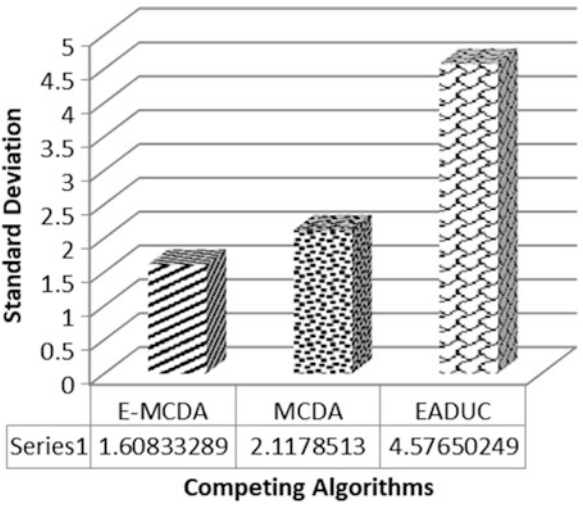


Fig. 11.4 Standard deviation of number of members per cluster

E-MCDA. This burdens the CHs with more memory and processing load in larger clusters. This further opens the numerous issues to handle.

11.5 Conclusion

Lifetime improvement of wireless sensor networks is indispensable for making the life easy in a lot of surveillances, monitoring, tracking, applications, etc. due to stringent constraint energy resource. The idea of MCDA was improved with novel algorithms for time slot allocation at network setup phase to make the cluster designing process more energy efficient, energy-efficient cluster head selection and 'required node degree' based on cluster member selection for near-equal size clusters. We named it as extended-MCDA. These ramifications play vital roles to achieve the target. Results of our experiments have shown that E-MCDA has outperformed the two competitive mechanisms.

References

1. Jabbar, S., Aziz, M. Z., Minhas, A. A., & Hussain, D. (2010). PTAL: Power tuning anchors localization algorithm for wireless ad-hoc micro sensors network. In *The 7th IEEE International Conferences on Embedded Software and Systems*. Bradford: IEEE.
2. Abid, A., Kachouri, A., & Mahfoudhi, A. (2017). Outlier detection for wireless sensor networks using density-based clustering approach. *IET Wireless Sensor Systems, 7*(4), 83–90.
3. Hassan, N., Khan, N. M., Ahmed, G., & Ramer, R. (2013). Real-time gradient cost establishment (RT-GRACE) for an energy-aware routing in wireless sensor networks. In *IEEE Eighth*

International Conference on Intelligent Sensors, Sensor Networks and Information Processing (pp. 54–59). Melbourne: IEEE.
4. Jabbar, S., Butt, A. E., Najm-us-Sehr, N., & Minhas, A. A. (2011). TLPER: Threshold based load balancing protocol for energy efficient routing in WSN. In *The 13th International Conference on Advanced Communication Technology (ICACT'11)*. Seoul: IEEE.
5. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2014). PASCCC: Priority-based application-specific congestion control clustering protocol. *Computer Networks, 02*(02), 92–102.
6. Jabbar, S., Minhas, A. A., Gohar, M., Paul, A., & Rho, A. S. (2015). E-MCDA: Extended-multilayer cluster designing algorithm for network lifetime improvement of homogenous wireless sensor networks. *International Journal of Distributed Sensor Networks, 11*(9), 902581.
7. Jabbar, S., Minhas, A. A., Paul, A., & Rho, S. (2014). Multilayer cluster designing algorithm for network life time improvement of homogenous wireless sensor networks. *Journal of Supercomputing, 70*(1), 104–132.
8. Yang, P.-T., & Lee, S. (2012). A distributed reclustering hierarchy routing protocol using socialwelfare in wireless sensor networks. *International Journal of Distributed Sensor Networks, 8*(4), 681026.
9. Li, C., Ye, M., Chen, G., & Wu, J. (2005). An energy-efficient unequal clustering mechanism for wireless sensor networks. In *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.* Washington: IEEE.
10. Yu, J., Qi, Y., Wang, G., Guo, Q., & Gu, X. (2011). An energy-aware distributed unequal clustering protocol for wireless sensor networks. *International Journal of Distributed Sensor Networks, 7*(1), 202145.
11. Naeem, M. K., Patwary, M., & Abdel-Maguid, M. (2017). Universal and dynamic clustering scheme for energy constrained cooperative wireless sensor networks. *IEEE Access, 5*, 12318–12337.
12. Aslam, M., Shah, T., Javaid, N., Rahim, A., Rahman, Z., & Khan, Z. A. (2012). CEEC: Centralized energy efficient clustering a new routing protocol for WSNs. In Conference *on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012 9th Annual IEEE Communications Society* (pp. 103–105). Seoul: IEEE.
13. Chen, G., Li, C., Ye, M., & Wu, J. (2007). An unequal cluster-based routing protocol in wireless sensor networks. *Wireless Networks, 15*, 193–207.
14. Lee, K., & Lee, H. (2012). A self-organized and smart-adaptive clustering and routing approach for wireless sensor networks. *International Journal of Distributed Sensor Networks, 8*(1), 156268.
15. Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transaction on Wireless Communications, 1*(4), 660–670.
16. Said, B. A., Abdellah, E., Hssane, A. B., & Hasnaoui, M. L. (2010). Improved and balanced LEACH for heterogeneous wireless sensor networks. *International Journal on Computer Science and Engineering, 2*(8), 2633–2640. Retrieved from www.enggjournals.com/ijcse/doc/IJCSE10-02-08-153.pdf.
17. Heinzelman, W., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. In *Proceedings of the 33rd International Conference on System Sciences*. Hawaii: IEEE.
18. Handy, M. J., Haase, M., & Timmermann, D. (2002). Low energy adaptive clustering hierarchy with deterministic cluster-head selection. In *4th International Workshop on Mobile and Wireless Communications Network* (pp. 368–372). IEEE.
19. Muruganathan, S. D., Ma, D. C., Bhasin, R., & Fapojuwo, A. (2005). A centralized energy-efficient routing protocol for wireless sensor networks. *IEEE Radio Communications, 43*(3), S8–S13.
20. Fazlullah, K., Faisal, B., & Kenji, N. (2012). Dual head clustering scheme in wireless sensor networks. In *IEEE International Conference om Emerging Technologies (ICET). 06* (pp. 1–5). Islamabad: IEEE.

Chapter 12
Internet of Things–Based Smart City Environments Using Big Data Analytics: A Survey

Muhammad Babar, Fahim Arif, and Muhammad Irfan

Abstract The intense growth and acceptance of the Internet of Things (IoT) is reflected in the trend of smart cities. Smart cities are being implemented to improve standards of living and provide higher-quality services to residents. These services may include (but are not limited to) parking, water, health, transportation, environment, and power. The varied implementations of smart cities and the IoT are challenged by the processing of gigantic data and real-time decision management. In this chapter, we explore the use of big data analytics in IoT-based smart city development and design. This chapter provides a conceptual framework for the use of big data analytics in IoT-based smart city environments.

12.1 Internet of Things

British technology pioneer Kevin Ashton first used the term "Internet of Things" (IoT) in 1999. The IoT is a system in which different devices, actuators, and sensors [1, 2] are connected by our physical world. The internet acts as a bridge between the real world and different devices for communication. Iot plays a vital role in the development of smart cities environment [3]. Equally, the cloud-based and scalable video coding is also is the key parameters for setting-up the smart environment [4].

The IoT is a new frontier for researchers. It provides computing ability and internet connections in a variety of everyday objects, sensors, and devices. The wide application of IoT has the potential to change our lives. IoT can be used for industrial applications, water management, smart traffic controls, and noise sensing in our environment. For the consumer, new IoT trends offer different services to use in home appliances, automate home objects by remote access, and manage energy

M. Babar (✉) · F. Arif
National University of Sciences and Technology, Islamabad, Pakistan
e-mail: babar.phd@students.mcs.edu.pk; fahim@mcs.edu.pk

M. Irfan
Iqra University, Islamabad, Pakistan

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_12

in secure and efficient system smart home systems. The IoT also can be used in wearable products to monitor health through different functions installed in mobile applications. The IoT can provide users with independence and quality of life in a cost-effective manner.

A large number of organizations are expected to offer IoT applications in different domains over the next 10 years. For example, according to Cisco, almost 24 billion objects will be connecting via the internet by 2019 [5]. Morgan Stanley projected that 75 billion different network devices will be connected in 2020 [6]. Huawei predicted that 100 million different devices will be connecting to the IoT by 2025 [7]. Finally, McKinsey Global forecasted a revenue gain of $3.9 to $11.1 trillion by 2025 for IoT equipment.

Even though the IoT is considered to be a new trend, the concept of using different devices, computers, and networks to monitor and control objects has existed for many years. For example, in the 1970s, commercial telephone line monitoring meters were operated remotely on the electrical grid. In the 1990s, an industrial solution for machine-to-machine IP-based wireless connectivity was proposed for monitoring and operating a variety of devices [8]. The IoT is a new approach for research into smart object networking. From a broad viewpoint, it is now possible to interconnect increasingly smaller and more numerous devices inexpensively and effectively through "smart object networking." According to the Internet Architecture Board [9–14], smart objects are defined as a large number of embedded devices connected via internet protocols that communicate with each other and offer services. Many of these devices have no need for human intervention. Instead, they extract the information from their environment, such as a building or vehicle.

Smart objects have different non-functional requirements, such as limited power, memory and processing resources, and bandwidth. The main requirement is interoperability between different devices. In the IoT, four basic communication models are is used for small device design strategy to permit communication with each other: device-to-device communication, device-to-cloud communication, the device-to-gateway model, and the back-end data-sharing model. A variety of concerns are also associated with the IoT, including security, privacy, interoperability, standards, economic development, and legal regulations.

12.1.1 IoT Applications

IoT applications can deployed for smart cities, smart homes, wearable devices, smart grids, industrial internet, connected automobiles, smart farming, smart traffic, health applications, retail, security, energy, water management, waste management, noise management, and pollution management.

12.1.2 Importance of IoT

IoT generally provides a high level of knowledge about the environment by continuously monitoring and providing information about it. The IoT can provide new services for society, allowing many fields to be managed with less effort and less time. The IoT is a new industrial revolution in the lives of common people. This innovation has changed the communication between people and devices, improving standards of living and making daily life easier.

12.1.3 Challenges of IoT

Several major challenges are facing the IoT, as follows:

Big Data Expansion IoT devices obtain different types of data from various sources. The large volume of data is a big challenge to address in IoT as applications expand.

Power Efficiency IoT devices have sensors and switches connected through power, so it is a big challenge to supply power to all connected devices over the internet.

Security The IoT also has associated security issues. Companies have a responsibility to address concerns about information vulnerability, particularly when a product is used daily by a consumer. IoT manufacturers should ensure that their devices are secure from cyberattacks and that the data are protected from access by any unauthorized person.

Privacy IoT data are collected by different sources, such as sensors and actuators, and shared with other devices. Therefore, privacy is big challenge in this context. Personal information should be safe and not shared without permission.

Interoperability/Standards Interoperability is not possible in every environment. Therefore, when a user cannot adopt IoT services with confidence, they hesitate to buy IoT services or products because of their high cost, inflexibility, and high ownership complexity. In this regard, different standard models and strategies have been proposed and implemented.

Legal Regulations and Rights The IoT is an emergent field. New technology always introduces new issues regarding laws and regulations, as well as internet-related administrative rules. Various problems can arise when different devices are interoperating with each other, transferring and receiving data over the internet. From a user perspective, it is important that information transmitted over the internet be secured from hackers and abusers. Therefore, we cannot ignore security and legal rights when adopting IOT services.

Emerging Economic and Development Issues The IoT encompasses all areas of life and promises secure social and economy lives for everyone in the future. By

2050, it is expected that several smart cities will be established, which increases the need for cost- and time-effective security. Smart cities may include transportation management, water management, sustainability, healthcare, mobility, and smart parking, among others.

12.2 Smart Cities

The smart city is a small, urban area that incorporates a variety of information technology in a modern way to manage different domains, such as schools, libraries, transportation systems, hospitals, power plants, water supply networks, waste management, law enforcement, and other community services. The purpose of the smart city is to enhance the standards of living through information technology and to offer better services within the smart city. The purpose of the information communication technology is to monitor and sense any event that occurs within a smart city. Sensors are deployed in a smart city to obtain information from the environment, thus improving the residential quality of life and saving residents both time and money.

The deployment of the IoT in an urban area in a specific domain that follows government rules and utilizes an information communication technology solution to manage residential community problems is called a *smart city* [15]. The criteria for the selection of a smart city in the very initial stages of government of India include adoption of selection criteria within the budget.

12.2.1 Why Cities Need to Become Smart

Adequate fresh water, general access to cleaner living, the capacity to travel efficiently, a feeling of well-being and security—these are some of the issues that present-day urban communities must satisfy to remain aggressive and provide personal satisfaction to their residents [11]. By 2050, 66% of the world's population is expected to have shifted to cities. Then, problems with standards of living and quality of life will arise. To address these concerns, smart cities will be established in the future.

12.2.2 Smart Traffic: Smart City Applications

Europe has encouraged many countries to adopt smart city technology for traffic management. The European Commission allocated 365 million Euros to member nations for this purpose. Paris has already benefitted from this technology by establishing an electric car smart city, called Autoli. Almost 3000 vehicles are connected by GPS to help drivers find reserved parking. London also started a

smart city many years ago so that drives could quickly access parking. The United Kingdom has deployed smart electric car and bike sharing programs. Furthermore, Copenhagen and New York have establish smart cities for traffic management.

12.2.3 Healthcare: Smart City Applications

The most important and attractive areas for IoT applications are medicine and healthcare. The IoT plays an important role in the medical field in different contexts. IoT medical applications can remotely obtain information on different diseases and recommend medications online. For this purpose, medical diagnostic equipment may be deployed in smart devices to continue monitoring patients. The IoT paradigm improves patient health and quality of life, as well as reduces costs. All patient data is stored in a central repository or cloud server. Whenever required, any health-related data can be accessed by the doctor or patient from the repository. The core idea is to collect scattered and disparate data from different sources and apply useful strategies for examining and changing raw data into useful datasets [16].

The application of big data in healthcare is not an easy task. It requires expert team members, competent vendors, and thoughtful techniques. Different challenges occur daily with the expanding use of the IoT. Different devices and connections provide patient information in different formats, so expert team members are needed to overcome this issue. Waste and abuse also play important roles in healthcare fraud that increase the economic costs. However, big data analytics can limit healthcare fraud by using different prediction techniques.

12.3 Big Data Analytics

In big data analytics, massive datasets can be analyzed in various forms, such as structure/unstructured, batch/streaming, and different sizes (zettabytes and terabytes). Big data is used where traditional systems lack the ability to process and manage the data.

12.3.1 Importance of Big Data

Big data can help companies understand customer needs, reduce costs, detect risks, monitor for fraud, make processes more efficient, facilitate faster and better decision-making, and offer new product and services. When big data is successfully and proficiently captured and prepared, a full understanding of businesses, customers, products, and competitors can result in efficient utilization, lower costs, higher performance, and increased sales. Analyzing large sets of data allows

business users, analysts, and researchers to make faster decisions on data that are not possible in traditional systems.

12.3.2 Characteristics of Big Data

Big data is popular because it allows high-volume, high-velocity, and high-variety data to be managed in an efficient manner. Data come from different sources, so it is necessary to organize raw data into meaningful forms. Various analytic techniques are used for this purpose, such as machine learning, predictive analytics, data mining, and statistics [17]. The "V"s of big data are further explained below:

The Volume In big data, a huge amount of information is involved. Data grows day by day and contains all types and sizes of information (e.g. kilobyte, megabyte, petabyte, terabyte).

The Velocity Data originate at very high speeds, so big data analytics is time sensitive.

The Variety Data are kept in different file formats and types, which are extremely heterogeneous. The data may include structured or unstructured data, such as audio, log files, or video files.

The Value Value addresses the requirement for the evaluation of data and has great importance for information technology infrastructure systems and other businesses to store a variety of values in a database.

The Veracity The increase in the choices of values represents a large data set. Unnecessary or obsolete data that are not correct should undergo further analysis.

12.3.3 Big Data Life Cycle

In this section the steps involved in the life cycle of Big Data analytics are highlighted which are different from the set of activities involved in tradition life cycle model due to high volume, velocity and variety of dataset. It is advance technique that is utilized to bring the large data in meaningful and compact form. Life cycle of Big Data comprised of nine phases which are given below:

1. Business case evaluation
2. Data identification
3. Data acquisition and filtering
4. Data extraction
5. Data validation and cleansing
6. Data aggregation and representation
7. Data analysis
8. Data visualization
9. Utilization of analysis results

12.3.4 Future Opportunities for Big Data

Big data can uncover the concealed behavior of individuals and even shed light on their future plans. More specifically, it can cross over any barrier between what individuals need to do and what they really do, in addition to how they connect with others and their conditions. These data are helpful to government offices and privately owned businesses to help basic leadership in fields ranging from law enforcement to social administration to national security. Big data will change how we live in both minor and substantial ways [15, 18–23].

12.3.5 Challenges of Big Data Analytics

The following are the major challenges faced in big data:

Big Data Format Conversion As discussed previously, there are a diversity of data sources in big data. Therefore, data heterogeneity can limits the effectiveness of data format conversion. The applications used can create more value if such format conversions can be made more effective.

Big Data Allocation Big data allocation includes data generation, acquisition, transmission, storage, and other data transformations in a specific domain [15]. Improving the transfer productivity of big data is a main factor in increasing big data computing.

Big Data Privacy Personal and private data may be leaked through storage, broadcast, and practice, even if the permission of workers is obtained.

12.3.6 Relationship Between IoT and Big Data

In the IoT paradigm, a large number of network sensors are embedded in different types of devices and machines. These sensors are deployed in numerous fields, which further gather data from various categories, such as environmental data, geographical data, and logistic data. There is a dire need for big data adoption in different IoT applications, as the development of big data is already lagging behind [15]. These two technologies are interdependent and should be working together. The extensive deployment of IoT drives and the evolution of data, both in size and type, can provide an opportunity for the application and improvement of big data. Furthermore, the application of big data technology to IoT also speeds up the research improvements and business representations of IoT.

12.3.7 Techniques

Big data requires exceptional strategies to effectively handle huge volumes of information inside constrained run times. Big data techniques involve a number of disciplines, including statistics, data mining, machine learning, neural networks, social network analysis, signal processing, pattern recognition optimization methods, and visualization approaches. Some of the most widely used approaches for big data analytics include Yarn, Map Reduce, Spark, HBase, Hive, Kafka, and Pig.

12.4 Role of IoT and Big Data in Smart Cities

There is only one way for any city to truly become a smart city—through data and analytics. The growth of big data and the advancement of IoT technologies have played a vital role in the feasibility of smart city initiatives [8]. Big data offer the potential for urban areas to obtain significant bits of knowledge from great volumes of information gathered through different sources, and the IoT allows the incorporation of different sensors in different devices using networked services. Companies are providing IoT and big data solutions for everyday operations in order to bring cities into a new era.

The IoT is fundamental when building a smart city. For a city to be entirely "smart," the devices connected to it must be able to communicate with one another. Here, IoT plays a part by providing a perfect template for device communication, hence providing smart solutions for different problems. According to Schuller, everything becomes an opportunity from a smart city perspective [11]. With more than 50% of people now living in urban areas, it is crucial for cities to think about how they can mitigate problems that arise from urbanization.

When IoT technology comes together with big data, cities can be recognized as upcoming smart cities [24, 25]. These smart cities can change the professional and personal lives of their residents on many levels, such as lowering pollution, managing waste, improving parking facility, and increasing energy savings. One of the biggest perks of creating smart cities is that resource waste will be reduced to a very large extent. Decreases in water wastage, congested streets, energy/power consumption, and pollution, among others, will certainly be a boon for the residents living in these smart cities. In fact, several smart cities around the world have already successfully tackled problems such as sewage treatment, water theft, pollution, and traffic congestion over time. Therefore, the combination of IoT technology and big data can help us to achieve the impossible.

12.5 Conclusion

The idea of the smart city is still very novel due to the revolution in conventional city functions. The smart city concept has motivated researchers and industries to construct well-organized and generic architecture. In this chapter, the use of big data analytics in the development and design of IoT-based smart cities was explored. A conceptual framework for the use of big data analytics in IoT-based smart city environments was provided.

References

1. Systems: A survey. IEEE Transactions on Industrial Informatics, vol. 1551-3203 (c) 2015 IEEE.
2. Jan, M. A., Jan, S. R. U., Alam, M., Akhunzada, A., & Rahman, I. U. (2018). A comprehensive analysis of congestion control protocols in wireless sensor networks. *Mobile Networks and Applications, 23*, 1–13.
3. Jacobs, I. S., & Bean, C. P. (2017). Innovative energy management solutions using cloud intelligence and big data analysis. *Future Generation Computer Systems, 77*, 65–76.
4. Usman, M., He, X., Lam, K. K., Xu, M., Chen, J., Bokhari, S. M. M, et al. (2017). Error concealment for cloud-based and scalable video coding of HD videos. *IEEE Transactions on Cloud Computing*. https://doi.org/10.1109/TCC.2017.2734650
5. Cisco Visual Networking. (2015). *The zettabyte era: Ctrends and analysis*. Cisco white paper.
6. Sharma, M., & Chauhan, V. (2016). A review: Map reduce and spark for big data analytics. *International Journal of Advanced Technology in Engineering and Science, 4*(6), 42–50.
7. Michael, K., & Miller, K. W. (2013). Big data: New opportunities and challenges [guest introduction]. *Computer, 46*(6), 22–24.
8. Chen, M., Mao, S., & Liu, Y. (2014). *Big data: A survey*. New York: Springer.
9. David Lake S., Rayes, A., & Morrow, M. (2013). The internet of things. *The Internet Protocol Journal, 15*, 3. Cisco Press: San Jose.
10. Jan, M. A., Khan, F., Alam, M., & Usman, M. (2017). A payload-based mutual authentication scheme for internet of things. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.08.035
11. Khan, F., ur Rahman, I., Khan, M., Iqbal, N., & Alam, M. (2016). CoAP-based request-response interaction model for the internet of things. In *International Conference on Future Intelligent Vehicular Technologies* (pp. 146–156). Cham: Springer.
12. Jan, M. A., Nanda, P., He, X., Tan, Z., & Liu, R. P. (2014). A robust authentication scheme for observing resources in the internet of things environment. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 205–211). IEEE.
13. Khan, F., Khan, M., Iqbal, Z., ur Rahman, I., & Alam, M. (2016). Secure and safe surveillance system using sensors networks-internet of things. In *International Conference on Future Intelligent Vehicular Technologies* (pp. 167–174). Cham: Springer.
14. Khattak, M. I., Edwards, R. M., Shafi, M., Ahmed, S., Shaikh, R., & Khan, F. (2018). Wet environmental conditions affecting narrow band on-body communication channel for WBANs. *Adhoc & Sensor Wireless Networks, 40*(3/4), 297–312.
15. Khan, F., ur Rehman, A., Usman, M., Tan, Z., & Puthal, D. (2018). Performance of cognitive radio sensor networks using hybrid automatic repeat request: Stop-and-wait. *Mobile Networks and Applications, 23*, 1–10.

16. Levent, T. B., & Nukamp, P. (2006). Quality of urban life: A taxonomic perspective. *Studies in Regional Science, 36*(2), 269–281.
17. Lee, I., & Lee, K. (2015). *The Internet of Things (IoT): Applications, investments and challenges for enterprises* (Vol. A247, pp. 529–551). London: Elsevier.
18. Miorandi, D., Sicari, S., De Pelligrini, F., & Chalamatic, I. (1987). Internet of things: Vision, applications and research challenges. *IEEE Translation Journal on Magnetics in Japan, 2*, 740–741. [Ad hoc Networks 10 (2012), p. 1497–1516].
19. Alam, M., Albano, M., Radwan, A., & Rodriguez, J. (2013). CANDi: Context-aware node discovery for short-range cooperation. *Transactions on Emerging Telecommunications Technologies, 26*(5), 861–875. https://doi.org/10.1002/ett.2763
20. Jan, M. A., Usman, M., He, X., & Rehman, A. U. (2018). SAMS: A seamless and authorized multimedia streaming framework for WMSN-based IoMT. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2018.2848284
21. Usman, M., Jan, M. A., & He, X. (2017). Cryptography-based secure data storage and sharing using HEVC and public clouds. *Information Sciences, 387*, 90–102.
22. Alam, M., Yang, D., Huq, K., Saghezchi, F., Mumtaz, S., & Rodriguez, J. (2015). Towards 5G: Context aware resource allocation for energy saving. *Journal of Signal Processing Systems, 83*(2), 279–291. https://doi.org/10.1007/s11265-015-1061
23. Usman, M., Jan, M. A., He, X., & Nanda, P. (2016). Data sharing in secure multimedia wireless sensor networks. In *2016 IEEE Trustcom/BigDataSE/I SPA* (pp. 590–597). IEEE.
24. Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M., & Oliveira, A. (2011). Smart cities and the future internet: Towards cooperation frameworks for open innovation. *Lecturer Notes in Computer Science, 6656*, 431–446.
25. Harris, J. M. (2000). *Basic principles of sustainable development, global development and environment institute*. Medford: Tufts University.

Chapter 13
Enhancing Integrity Technique Using Distributed Query Operation

Umar Farooq Khattak, Aida Mustapha, Muhammad Yaseen, Muhammad Arif Shah, and Asim Shahzad

Abstract Database growth and storage problems are basically the main high concerns of globally large and small enterprises, which directly have negative impact on database application performance. But something more important is that majority of it is unused in these large volumes of databases. According to industry analysts, the growth rate of enterprise databases is 125% yearly, in which 80% of the information in use is inactive. Database archiving is one of the solutions among all the solutions that are available for management. With the use of archiving database, many issues have been highlighted including selection and removal of unused data from OLTP system, integrity management, and performance. This paper introduces a methodology for where OLTP and archiving data are kept in a distributed database environment. Integrity management is important, but more significant than that is the performance of the desired query which maintains that integrity between OLTP and archiving database. The main feature of the proposed methodology is that it not only maintains data integrity for primary and unique keys between OLTP and archive database but will also focus on enhancing the query performance for maintaining that integrity by introducing a query execution plan and parallel processing in it.

13.1 Introduction

In the modern era of communication world, more and more data is being stored in OLTP system for numerous reasons by administrations. Studies have revealed that data is used to be processed and analyzed for analytical analysis. Past experiences

U. F. Khattak · A. Mustapha (✉) · M. Yaseen · A. Shahzad
Faculty of Computer Science & Information Technology, Universiti Tun Hussein Onn Malaysia (UTHM), Parit Raja, Malaysia
e-mail: aidam@uthm.edu.my; asim@honestmail.net

M. A. Shah
Faculty of Computing, Universiti Technology Malaysia (UTM), Skudai, Malaysia

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_13

have shown that larger databases have huge impact on system applications in terms of loading, unloading, etc. One of the most important factors in database application is its performance which is tremendously affected by unused large volume of data stored in it [1].

Database archiving is the type of data archiving. Data exists in numerous forms and for many different purposes, but only a tiny proportion of it is actually in a database. Documents in hard and soft form, computer files, datasets, e-mail, and other such types of files are all examples of data that at some point needs to be archived [2].

Archive database is a process of removing data records from OLTP database that are not likely to be referenced or used and then storing that into an offline data store. Data once archived will be moved to archive database and will no longer be accessed in the operational database. Database archiving drifts database information from the live production database to database archiving and then manages the integrity and accessibility of information in those archives. Note that database archiving is like information. Life cycle management (ILM) treats data differently during different stages of its life cycle. To put it in another way, database archiving can be used as a method of implementing some of the key functions of ILM on database (i.e., structured data not flat files) [3].

Archived database is different from a backup database as the novel data in the database is erased in this terminology and archive copy of the data is the single copy, which resides in archive as long as it is required. Accessibility of archive data gradually increased; we could talk about 25 to 30 years for some productions and perhaps even longer. With the rapid advancement of technology and data, increasing just the storage capacity to handle all this data is not the good solution. In today's era, data trends are evolving from speed, size, and mobility, so the simple true solution is to make certain that software and technology used in organization should fulfill the users' requirements. To achieve all of it, the first step is database [4].

Increasing data storage doesn't essentially adapt into enhanced operations, but in fact it results in the negative impact of slowing down system performances, defecting response times, and increasing complexity levels. In terms of businesses, this will affect the trust of loyal customers and new income opportunities. Therefore the commanding prime task is to have a reliable and integrated database that can manage the expandability of data that is more than double every year [5].

Many companies use archived data to mine out useful information about their customer behavior and market trends by applying different data mining techniques on archived database. The most needed strategy for the business world is facing a massive information explosion which is database archiving (Fig. 13.1).

Data integrity in the database between offline archive and OLTP can be ensured in many ways. One of the traditional ways is to check both online database and offline archive database for removing data redundancy when update and insert operation is performed. This means that DML operation not only checks OLTP for inserting or updating a record each time but also performs the same check-in procedure in the offline archive database which is a time-consuming DML operation as shown in

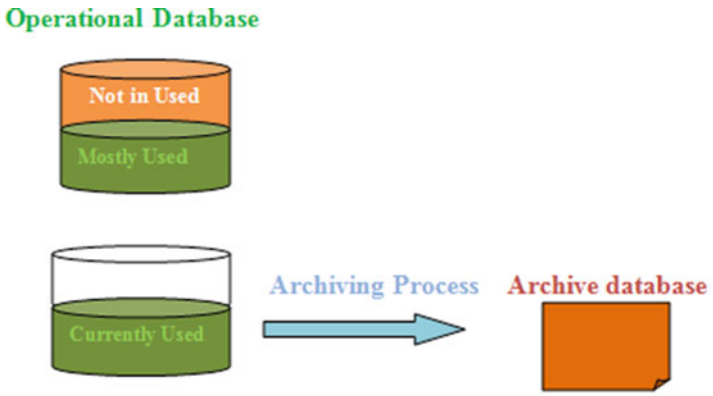


Fig. 13.1 Operational and archive database

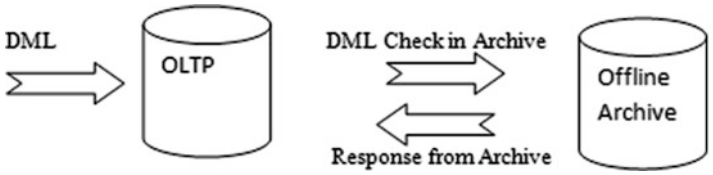


Fig. 13.2 General architecture for ensuring integrity

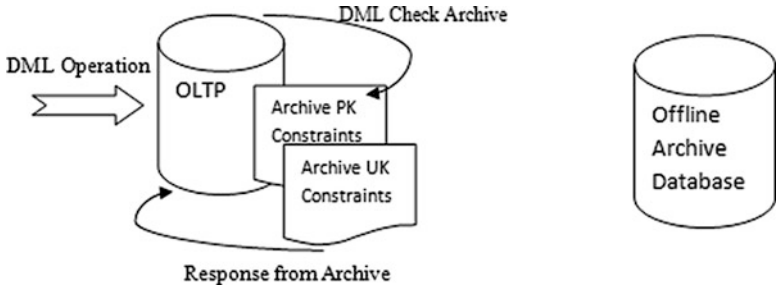


Fig. 13.3 Integrity management between archive and OLTP systems

Fig. 13.2. As a result DML operation for insertion and updating will take more time than the simple query before.

Another way initiated in "integrity management between the archive and OLTP systems" was to maintain data integrity by extracting primary and unique keys from ongoing offline database archive and inserting it in two new tables created in OLTP for each key type (primary key and unique key) as shown in Fig. 13.3 [1].

13.2 Related Work

Every year, companies devote millions of dollars in preserving and making business-critical applications up to date depending on complex relational databases. These databases store large amount of data for business operations and decision-making. As a result, databases become overloaded which cause poor performance and limit the availability of the desired functionalities. Ironically, most of this data resides online in production databases, but is hardly ever accessed [6].

According to analysts, the growth rate of enterprise databases is 125% annually. Even more interesting is that 80% of the information in those databases is not in use (in other words, it is ready for archiving). But why are we producing so much data? It's true, with the advancement of technology, data can be captured and stored in different ways. But technology alone is not the only reason behind the rate of rapid data growth [7].

Forrester estimations show that the modern database market is $27 billion—including new database licenses, technical support, facilities, and accessing—and it is probable to raise to $32 billion in forthcoming years [8]. Besides that database market is increasing rapidly. On the other hand, data growth has deeply exaggerated performance and exceptionally slowing down query run time, which is the most important deliberation for it.

The mainstream of business administrations is bound and required to save and store data for longer time period in operational database which can yet create more multifaceted setup in relation to database performance and usability, with ever increasing or expanding of operational database. It will further stress on the processing of transactions which leads to unsatisfactory query performance. As a general principle, the older the data in the OLTP system, the less efficient the transactions running against it. According to modern industry analysts and professionals, the solution to manage the large volume of data in database system lies in record database. As we know that data integrity is a fundamental part of a database system which refers to accurateness, consistency, and dependability of data that resides in the database system, therefore the fundamental rule is to preserve the data integrity while applying any archive database approach [9].

In August 2007 on behalf of BridgeHead Software, the media conducted a survey of IT executives and found that 59% of defendants were having an issue with the size of data which they were compelled to back up because it was disturbing the business activities or will do so eventually [10]. By 93% it is stated that routine backup size is progressively increasing. Several advantages were identified by the survey to deduce the volume of data regularly backed up:

- Less IT time dedicated to backup and other business operation(69%)
- A reduction in the impact of backup and replication on network utilization and capacity (60%)
- A deduction in disk resources devoted to data snapshots, replication, and mirroring (58%)
- Reduced disruption to the live application environment (45%) [11]

Life cycle management considers an overall "best practice" approach for database growth management over the long term, and database archiving is an essential component of it. By mid-1990s, long-term preservation of digital data was a major issue for organization, government agencies, scientific communities, and individual researchers. These studies have identified serious issues which needed to be solved in making reliable and efficient access to digital information over a long period of time. Besides data integrity being the primary goal, one of the challenges identified through these studies is the performance of the DBMS when ensuring data integrity between OLTP and archive database [12].

13.3 Research Method

Archiving the data from OLTP which is no longer required for an organization will be the first part of the proposed methodology. Quantity of data archiving depends upon the organization policy which varies from organization to organization. Some organizations archive their data after 1 year, other after 6 years. Mostly data archiving policy is based on time frame, in term of years rather than selecting records randomly in OLTP systems. Other organizations select their archiving policy based on the number of the records defined. In an organization, archiving ten thousand records after the end of 6 months is an example of the abovementioned policy.

A distributed database is a group of data which are spread over different sites on a network, having each site of the network an independent processing capability, and can perform local applications. Each site on the network gives response to the subqueries of global query using communication subsystem. Parallel processing improves the operation processing by executing different operation parallels, such as index building, data loading, and query evaluation. Although data are distributed over the different sites, distribution rule gives the better performance. Increasing database sizes and performance demands is easier to accommodate in a parallel processing environment. Distributed database environment is shown in Fig. 13.4, which clearly defines the distribution of database for parallel processing. Next, Fig. 13.5 shows the database archiving process across the distributed environment.

In this proposed system, query execution will be performed through parallel processing, where on one side, it will ensure integrity in OLTP system and, contemporarily on the other side, it will also ensure integrity management in the archive database in a distributed environment if an insert or update query occurs.

The database-level trigger will define detection of insertion and update DML operation for each table. The information schema view will be defined for detection of table name, value, value type, constraint type, etc. Here the query execution plan will be performed for integrity management after identification of table name, value, value type, and constraint type. The proposed methodology is shown in Fig. 13.6.

Integrity management checking between OLTP and archive database will be in parallel, which will speed up the performance of DML operation in terms of

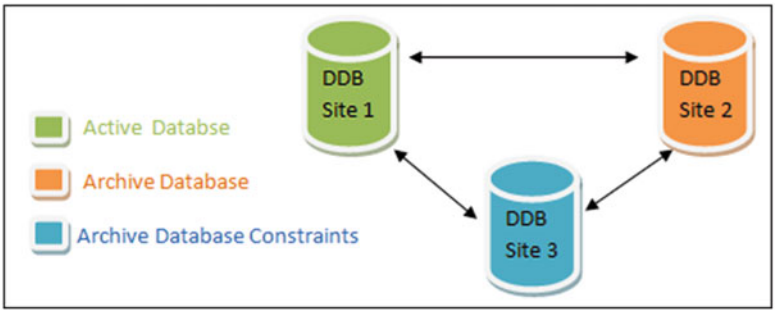


Fig. 13.4 Distributed database environment for OLTP and archive databases

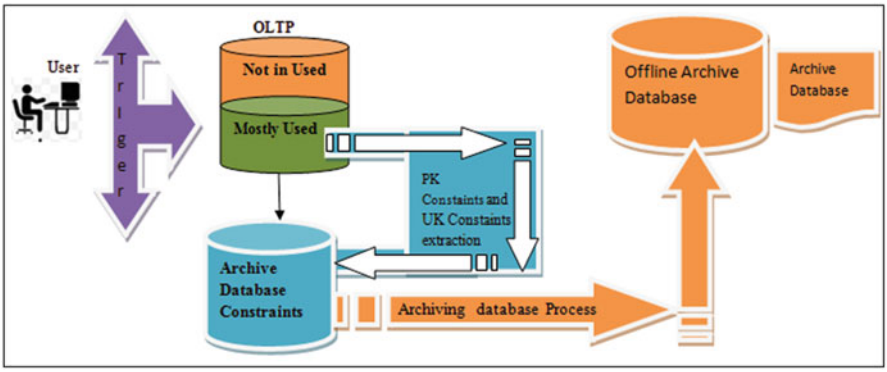


Fig. 13.5 Database archiving process over distributed database environment

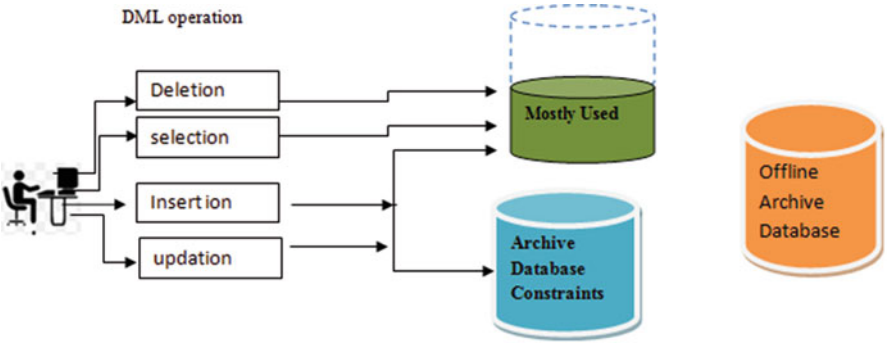


Fig. 13.6 Parallel DML operation over distributed database environment for integrity management

integrity checking. We can also access archived database data if we need it rather than using a long procedure for restoring and archiving database.

Database integrity is the major issue of data security. Database integrity means the correctness and consistency of data. Data integrity is related to the quality of data and can be ensured by the data integrity constraints. Security means that the data must be protected from unauthorized operations. Therefore, it is very important to achieve data integrity.

13.4 Conclusion and Future Work

It is clearly assumed that large volumes of database have adverse impact on database effectiveness. Database application takes longer time to load, unload, search, retrieve, reorganize, recover, and back up the required database. Several issues related to data archiving have been highlighted, including integrity management, query performance, and availability of archived data. The main concern in archiving database is integrity management, but further than that is the query performance for maintaining that integrity. The approach which I have selected ensures the integrity of primary and unique keys between OLTP and archive databases over distributed environment. On one hand is direct way for checking integrity, and on other hand integrity is checked concurrently between OLTP and archive database over a distributed situation. The proposed architecture allows the availability of data by keeping the archive data and OLTP in a distributed environment without writing long restoration procedures.

Research work helps in exploring new direction in terms of implementing and discovering new approaches. The approach which I have presented can also be expanded in many ways. This idea can also be extended ahead of primary and unique keys and can include referential integrity. New approach needs to be explored for maintaining referential integrity between archive and OLTP system. Another important new direction is the maintenance of schema synchronization between archive and OLTP system. The change that occurs in OLTP schema must be reflected to archive database schema.

References

1. Ibrahim, H., Alwan, A. A., & Udzir, N. I. (2007). Checking integrity constraints with various types of integrity tests for distributed databases. In *2007 8th international conference on parallel and distributed computing, applications and technologies, PDCAT 2007 (PDCAT)* (pp. 151–152). https://doi.org/10.1109/PDCAT.2007.14
2. Hill, D. (2006). *Database archiving: A necessity, not an option*. Commentary, Mesabi Group. Available from https://www.mesabigroup.com/English/Collaterals/Whitepapers/20060511_Database_Archiving.pdf
3. Lee, J. (2004). *Database archiving: A critical component of information lifecycle management*. Available from https://www.databasejournal.com/sqletc/article.php/3340301/Database-Archiving-A-Critical-Component-of-Information-Lifecycle-Management.htm

4. Yuhanna, N. (2009). *Enterprise database management systems*. Cambridge: Forrester Research.
5. Pfleeger, C. P., & Pfleeger, S. L. (2003). *Security in computing*. Upper Saddle River: Prentice Hall Professional Technical Reference.
6. Özsu, M. T., & Valduriez, P. (2011). *Distributed and parallel database systems*. Boston: Springer.
7. Redman, T. C. (1998). The impact of poor data quality on the typical enterprise. *Communications of the ACM, 41*(2), 79–82.
8. Norris, J. S. (2004). Mission-critical development with open source software: Lessons learned. *IEEE Software, 21*(1), 42–49.
9. Lush, M. (2017). *Getting to the bottom of data integrity Safeguarding quality systems requires understanding the thinking that drives human behaviour* (pp. 12–13).
10. Eddolls, T. (2008). *Database archiving for the future*. Available from https://www.informationtechnologycrossing.com/article/370128/Database-Archiving-for-Tomorrow/
11. Mullins, C. (2006) *Database archiving: Managing data for long retention periods*. Available from http://tdan.com/database-archiving-for-long-term-data-retention/4591
12. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2015). A sybil attack detection scheme for a centralized clustering-based hierarchical network. In *Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA* (Vol. 1, pp. 318–325). IEEE.

Chapter 14
EH-ARCUN: Energy Harvested Analytical Approach Towards Reliability with Cooperation for Underwater WSNs

Adil Khan, Sheeraz Ahmad, Mukhtaj Khan, Mian Ahmad Jan, Zahoor Ali Khan, and M. Usman Akhtar

Abstract Underwater sensor networks are ad hoc networks to monitor different underwater phenomenons such as pollution control, petrol mining, and observation of echo life. For underwater sensor networks to operate for longer duration of time, hoarding energy from background sources is viable option. One such source is harvesting energy from water currents using piezoelectric material embedded in sensor nodes. Piezoelectric materials can produce electricity when pressure is applied on it in the form of oscillating frequency produced by hydrophones. In this paper we have analyzed cooperation-based technique in underwater sensor networks containing sensor nodes which select relay nodes in their immediate vicinity with energy harvesting capabilities. These relay sensor nodes employ technique of amplify and forward (AF). As in current literature, all cooperative-based UWSN routing techniques are without integration of any type of energy harvesting schemes; considering this, we have incorporated piezoelectric energy harvesting mechanism into relay nodes in order to decrease end-to-end delay, increase stability period,

A. Khan (✉)
Abdul Wali Khan University, Computer Science Department, Mardan, KPK, Pakistan

Career Dynamics Research Centre, Peshawar, Pakistan
e-mail: adil.khan.kakakhel@awkum.edu.pk

S. Ahmad
Career Dynamics Research Centre, Peshawar, Pakistan
e-mail: adil.khan.kakakhel@awkum.edu.pk; sheerazahmad@gu.edu.pk; zahoor.khan@hct.ac.ae

M. Khan and M. A. Jan
Abdul Wali Khan University, Computer Science Department, Mardan, KPK, Pakistan

Z. A. Khan
Career Dynamics Research Centre, Peshawar, Pakistan

CIS, Higher Colleges of Technology, Abu Dhabi, United Arab Emirates
e-mail: zahoor.khan@hct.ac.ae

M. Usman Akhtar
University of Engineering and Technology, Peshawar, Pakistan

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_14

and improve packet delivery ratio. As case study, we have selected cooperation-based UWSN protocol ARCUN (Analytical Approach towards Reliability with Cooperation for Underwater WSNs) and integrated piezoelectric energy harvesting scheme with it. We compared our new scheme EH (energy harvested)-ARCUN with ARCUN and RACE (Reliability and Adaptive Cooperation for Efficient Underwater Sensor Networks). Simulation results show improvement of EH-ARCUN over ARCUN and RACE schemes.

14.1 Introduction

Operation of wireless communication networks in use today is mainly restricted by devices which use fixed batteries for energy storage. These batteries need replacement from time to time which is not only time-consuming and expensive but sometimes impossible due to harsh underwater conditions. One of the many energy harvesting techniques is piezoelectric energy harvesting. This technique can generate fair amount of voltage by applying pressure of water current on piezo-electric material which can generate electricity consequently extending duration of energy-constrained wireless networks [1, 2]. With piezoelectric energy harvesting, UWSN sensor nodes are enabled to harvest energy from hydrophones to charge their batteries [1, 2]. This technique can be integrated with cooperation-based routing in UWSNs to increase stability period, reduce end-to-end delay, and increase packet delivery ratio.

In cooperation-based routing, data from source node is cooperatively forwarded by relay node toward destination node on independent channel, whereas source node can also send data directly toward destination, thereby increasing reliability of network [3, 4].

In EH-ARCUN (Energy Harvested Analytical Approach towards Reliability with Cooperation for Underwater WSNs), relay node is now able to harvest energy from its harvesting unit. Relay node can function cooperatively for longer duration with the source node since it does not need to devour its own energy.

It is critical to supply each relay node with an energy bank (e.g., a rechargeable battery) such that they can hoard gathered energy and then perform data forwarding. Energy harvesting mechanisms have the prospective to tackle issue of performance parameters and lifetime of sensor nodes. Confrontation is present between predicting availability of energy source and amount of energy source. Intelligent selection of these two factors decides lifetime of relay node before its complete energy exhaustion and not be able to opt for next recharge cycle.

Main contributions of this paper are summarized as follows:

- We propose an energy harvesting-based Analytical Approach towards Reliability with Cooperation for Underwater WSNs (EH-ARCUN) scheme for UWSNs; relay sensor node decides when to operate between energy harvesting mode and data forwarding mode.

- We have exploited capabilities of cooperation-based communication in UWSNs to integrate energy harvesting capability in relay nodes which helps in better accumulation of signal at relay node.

The rest of the paper is organized as follows: Sect. 14.2 outlines related work about energy harvesting techniques and type of cooperation-based routing protocols. Section 14.3 presents motivation. Section 14.4 lays out our proposed protocol. Section 14.5 presents simulation results, and Sect. 14.6 concludes the paper.

14.2 Related Work

In remotely powered underwater acoustic sensor network (RPUASN) [1, 2], authors discuss integration of piezoelectric harvested sensor nodes in UWSNs. Authors showed through mathematical modeling the energy harvesting procedure of sensor nodes which can generate induced voltage which is feasible for operation of sensor nodes and extending network lifetime.

In Cooperative Energy-Efficient routing for UWSNs (Co-EEUWSN) [5, 6], authors used amplify and forward technique at relay nodes and fixed ratio combining (FRC) technique to increase energy efficiency and load balancing in network. In Cooperative Opportunistic Pressure Based Routing for Underwater Wireless Sensor Networks [7, 8], hydrocast protocol is improved by employing cooperative technique of communication with intelligent placement of sensor nodes. Calculated deployment of sensor nodes ensures precise data gathering of observed field of interest. In [9, 10] opportunistic void avoidance routing (OVAR) is proposed based on graph theory; in this technique source node selects set of nodes in any direction which can avoid holes in its path toward destination.

In [11, 12] region-based cooperative routing protocol (RBCRP) is proposed. Deficiency in this scheme lies at relay node which employs processing overhead for error checking of received data packet. In [13, 14] mobile autonomous underwater vehicle (MobiL-AUV) protocol is proposed to improve node localization in UWSNs. AUV nodes work as data-providing nodes for ordinary sensor nodes to adjust their location according to neighboring nodes. Although it improves node localization problem in UWSNs, it is not suitable for time-sensitive application because ordinary sensor nodes will have to wait for AUV to come in sight of their transmission range.

In Depth and Energy Aware Cooperative Routing Protocol for Underwater Wireless Sensor Networks (DEAC) [15, 16], sensor node depth is adjusted according to the sparsity of network, thereby improving energy consumption. In Analytical Approach towards Reliability with Cooperation for Underwater WSNs (ARCUN) [3, 4, 17], sensor node selects from a set of relay nodes which is most suitable in terms of distance and signal to noise ratio for source node and then forwards data cooperatively. In [17, 18] Reliability and Adaptive Cooperation for Efficient Underwater Sensor Networks (RACE), cooperation is employed at physical layer to

save energy consumption of network. In [8, 19] authors proposed Sink Mobility with Incremental Cooperative Routing Protocol for Underwater Wireless Sensor Networks (SMIC) which utilizes movement of sinks in order to efficiently cover monitored sensed area. Mobility of sinks is governed according to the network density.

In [8, 20] authors discussed and analyzed the use of piezoelectric energy generators for wireless terrestrial sensor networks. In [21, 22] authors proposed energy threshold based multi-relay selection (ETMRS) which harvests energy from receiving radio signal and developed mathematical model for calculating energy harvesting duty cycle and its effects on crucial network parameters like end-to-end delay and network lifetime. In [23, 24] authors presented maximizing network lifetime of wireless sensor networks: an energy harvesting approach. This scheme presents clustering algorithm for cluster heads, which selects energy harvested node, and only those nodes can forward data to cluster heads in terrestrial sensor network.

14.3 Motivation

ARCUN uses multiple relay nodes for source node in order to forward data. These relay nodes are ordinary nodes with extra energy due to its comparatively large-sized batteries. We have introduced energy harvesting capable batteries for relay nodes. In order for relay nodes to efficiently harvest energy for UWSNs, we have provided mathematical model for piezoelectric energy [1, 2] which is integrated into relay nodes of ARCUN.

Furthermore ARCUN relay nodes employ technique of amplify and forward (AF), which is based on analogue signal conversation to digital signal and feasible for acoustic signal conversion. We have also employed the same technique but with multiple cooperative relay nodes. Source node can send data to best neighboring relay nodes; additionally source node cannot send data directly toward destination node. This approach saves energy consumption as compared to ARCUN with more communication reliability.

In RACE scheme, on-demand cooperative routing is employed which is a suitable approach to balance energy consumption, but it decreases reliability when network becomes more scalable. Furthermore RACE scheme does not use relay sensor nodes; it relies on normal sensor nodes for cooperation-based communication, and this further decreases communication reliability in network.

Cooperation should be employed throughout network lifetime, and special energy harvested relay nodes should be deployed to enhance network lifetime and increase communication reliability which is demonstrated in our proposed EH-ARCUN scheme.

14.4 Proposed Protocol (EH-ARCUN)

14.4.1 Protocol Assumptions

Multiple energy harvested relay nodes are assumed to be available for single source-destination node pair. We have assumed that nodes can only forward data through relay nodes and there is no direct link available between source and destination nodes as depicted in Fig. 14.1.

In Fig. 14.1, relay nodes are represented by green color, and source-destination pair is represented by red color. g is complex channel coefficients between source and relay nodes, whereas h is complex channel coefficients between relay nodes and destination node, respectively. Relay nodes use hydrophones for energy harvesting; received signal level and calculated voltage sensitivity determine the amount of harvested energy and can be mathematically represented as [1]:

$$P_{\text{harv}} = 0.7\, n\, 10^{(\text{RL}+\text{RVS})/10}/4\, R_{\text{p}}. \tag{14.1}$$

where P_{harv} is amount of harvested energy, RL is received signal level or strength, RVS is received voltage sensitivity, and R_{p} represents hydrophone.

Equation (14.1) can be used to calculate the amount of harvested energy at relay node. We have assumed that relay node operates in two modes, one is energy harvesting mode and another one is data forwarding mode. When in data forwarding mode, data is received by relay node from source node, and relay node applies amplify and forward technique. As we do not assume direct path existence between source and destination nodes depicted in Fig. 14.1, data received at relay node can be modeled as [4]:

$$y_{\text{SiRi}} = \sqrt{P}_1 \mathbf{g}_{\text{SiRi}} x_{\text{Si}} + N_{\text{SiRi}}\,(f) \tag{14.2}$$

where P_1 is power of signal from source node, g_{SiRi} is complex channel coefficients, x_{Si} is received data at relay node, and $N_{\text{SiRi}}\,(f)$ is underwater noise.

Data received by relay node is forwarded toward destination node using amplify and forward technique modeled as [10]:

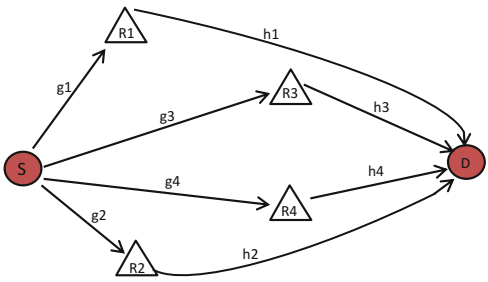


Fig. 14.1 EH-ARCUN with one source and destination node pair and four piezoelectric harvested relays

$$y_{\text{RiDi}=} \sqrt{P}_{2'} \mathbf{h}_{\text{RiDi}} x'_{\text{si}} + N_{\text{RiDi}}\,(f) \tag{14.3}$$

where P_2 is signal power of relay node, $\mathbf{h}_{\text{RiDi}}$ is complex channel coefficients of relay-destination node pair of i_{th} relay node, and x'_{si} is forwarded data of i_{th} relay node with added noise $N_{\text{RiDi}}\,(f)$.

14.4.2 Relay Selection Based on Amount of Harvested Energy

We have considered one specific scenario in which we should answer question of "which relay out of set of relay(s) will perform data forwarding? And which relay node will perform energy harvesting?" To answer these two questions, in this paper we have developed maximum energy value for each relay node which should be maintained. Each relay R_{i} stores in its local queue constant value for minimum energy that can be harvested by hydrophones denoted by P_{harv} as in Eq. (14.1). Each relay has independent choice of either to harvest energy or forward received data from source node. It will only relay data if:

$$P_{\text{harv}} >= £ \tag{14.4}$$

where £ is constant minimum attainable harvested energy value; otherwise relay node will execute duty cycle for energy harvesting. This can be mathematically modeled as [4]:

$$E_{\text{re}}\,(S) <= E_{\text{re}}\,(R_{\text{i}})^{*}\, P_{\text{harv}} \text{ where } P_{\text{harv}} >= £ \tag{14.5}$$

where $E_{\text{re}}\,(S)$ is residual energy of source node and $E_{\text{re}}\,(R_{\text{i}})$ is residual energy of relay node. If Eq. (14.5) is satisfied, then source node will forward data toward ith relay node; otherwise source node will select next relay node from its best neighboring relay node table.

Relay nodes amplify received data from source node before forwarding toward destination. This amplification can be represented by factor §, i.e., $y_{\text{RD}} = §(y_{\text{SR}})$. If Ps and Pr are transmission powers from source and relay, respectively, then § can be written as [4]:

$$§ = \sqrt{\frac{P_r + P_{\text{harv}}}{P_s \left|T_{d(\text{SR})}\right| 2 + N(f)2}} \tag{14.6}$$

Considering Eq. (14.6), signal received at destination node D, Eq. (14.3), can be expressed as [4]:

$$y_{\text{RiDi}=} \sqrt{P}_{2'} h_{\text{RiDi}} §x_{\text{si}} + N_{\text{RiDi}}(f) \tag{14.7}$$

14.4.3 Combining Relayed Signals at Destination Node

Each destination node D employs assortment integration mechanism to put together signals received from different relay nodes. We have assumed four relay nodes for specific case scenario. It is assumed that two relay nodes R_1 and R_2 are closer to source node, and two relay nodes R_3 and R_4 are closer to destination node as depicted in Fig. 14.1.

In fixed ratio combining (FRC) technique, instead of aggregating received signals, they are assigned weights based on fixed ratio. This ratio represents the average channel efficiency and reflects choice of destination node as to which relay channel should be considered for received signal and consequently the received data. In case of four relay nodes, FRC can be expressed as [4]:

$$y_{\mathrm{d}} = k_1 y_{\mathrm{R1D}} + k_2 y_{\mathrm{R2D}} + k_3 y_{\mathrm{R3D}} + k_4 y_{\mathrm{R4D}} \tag{14.8}$$

where y_{d} represents integrated signal received by destination node from four relay nodes and k_{n} represents weights assigned to four different links of relay nodes. Considering powers of these links with corresponding channel complexities and using weights of relay nodes according to their distances from source and destination nodes, there ratios can be calculated as [4]:

$$\frac{\mathrm{k3} + \mathrm{k4}}{\mathrm{k1} + \mathrm{k2}} = \frac{\sqrt{\mathrm{p3}}\ \mathrm{hR3D} + \sqrt{\mathrm{p4}}\mathrm{hR4D}}{\sqrt{\mathrm{p1}}\ \mathrm{hR1D} + \sqrt{\mathrm{p2}}\mathrm{hR2D}} \tag{14.9}$$

14.5 Simulation Results

To evaluate performance of EH-ARCUN, it is analyzed and contrasted with already proposed protocols for UWSNs, namely, ARCUN and RACE using MATLAB. In simulation we have used ten static sinks deployed at surface of water; 125 nodes are arbitrarily laid out in network. Transmission range of sensor nodes is configured at 250 meters. In each round, sensor nodes select potential relays after identical intermission of time; nodes calculate their distance from neighboring relay nodes.

Nodes forward data to next higher region using cooperation of neighboring relay nodes until data reaches at sink. Inclusion of energy harvesting relay nodes and maintaining threshold value for energy makes EH-ARCUN scheme more efficient for data critical applications.

Figure 14.2 illustrates that EH-ARCUN scheme improves stability period of network due to integration of energy harvesting relay sensor nodes. Simulation results show that in RACE first node dies after 1200 s, in ARCUN first node dies after 3000 s, and in our EH-ARCUN new scheme nodes die after 4000 s which shows improvement in stability of network.

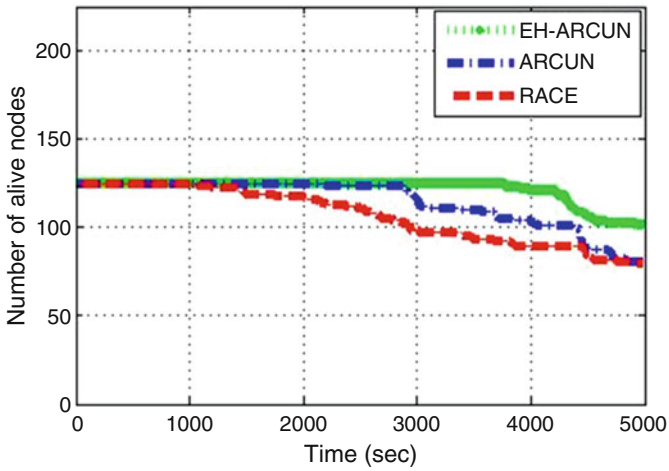


Fig. 14.2 Stability period vs. time

In ARCUN normal relay nodes are deployed, which exhausts their energy quickly, and furthermore source node transmits data not only toward these ordinary relay nodes but also toward destination node which puts extra transmission load on source node which eventually becomes cause of instability. RACE scheme does not consider any relay nodes.

All nodes are ordinary homogeneous nodes which employ cooperation technique for data forwarding which further brings down stability period.

Packet delivery ratio is shown in Fig. 14.3. Packet delivery ratio is the number of packets received at sink as compared to actually transmitted data packets by sensor nodes. PDR of EH-ARCUN and ARCUN shows similar progress up till 3000 s, where significant drop of PDR can be noted for ARCUN.

Because of amplify and forward scheme employed in ARCUN, sometimes signals are not received in their acceptable quality, amplification can saturate relay node, and consequently packets are dropped by relay nodes. In RACE PDR drop is very visible in contrast to EH-ARCUN and ARCUN, and RACE does not consider relay node mechanism, although it employs cooperation-based communication technique, but because of the decrease in inter-arrival time of packets, packet collision increases which affects delivery ratio.

End-to-end delay is plotted as shown in Fig. 14.4. End-to-end delay of our proposed scheme shows increasing trend at the end of simulation time. It is comparatively larger than ARCUN and RACE scheme. The main reason of increased delay of our scheme is time taken by relay nodes to harvest energy. Extra duty cycles are spent on energy harvesting when network becomes more and more sparse during passage of time. Initial delay of our proposed scheme is much less than the other two schemes, when relay nodes gain minimum constant energy level as in Eq. (14.4) than one or more relay nodes can cooperatively take part in forwarding data.

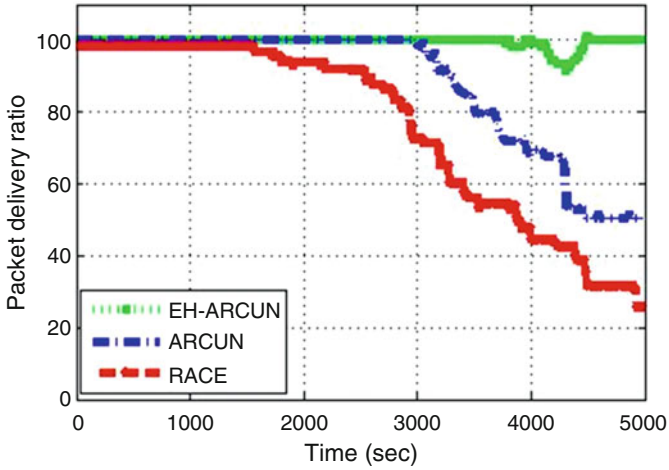


Fig. 14.3 Packet delivery ratio vs. time

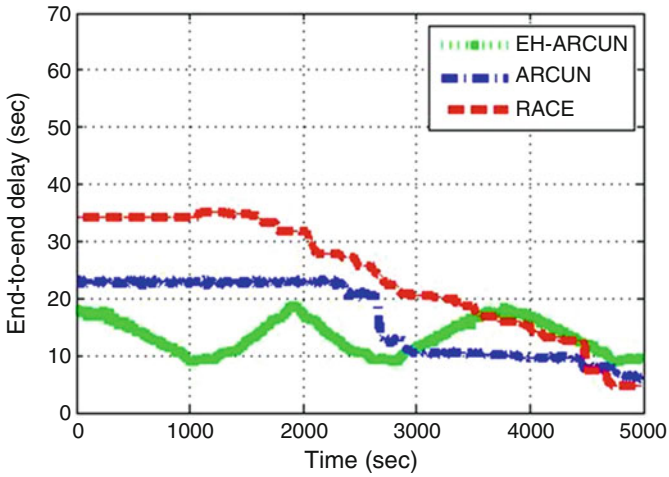


Fig. 14.4 End-to-end delay vs. time

14.6 Conclusion

In this paper we have improved existing ARCUN scheme by integrating energy harvested relay nodes which uses piezoelectric energy for harvesting. We have changed notion of cooperation in terms of cooperating relay nodes, thereby decreasing data forwarding load on source nodes.

Each relay can decide independently whether to transmit data or opt for energy harvesting duty cycles. Multiple cooperative relay nodes ensure data reliability for source node. Effective storage of threshold value of minimum harvested energy

ensures that relay nodes do not wait for extra energy harvesting duty cycles which leads to better stability period of network and efficient packet delivery ratio. It remains to be seen how much energy each relay should spend on forwarding data, because different relays would have harvested varied amount of energy and energy usage will be different for each relay. Furthermore for future research direction, developing local relay selection scheme for source nodes will provide more efficient data forwarding choice for source nodes.

References

1. Bereketli, A., & Bilgen, S. (2012). Remotely powered underwater acoustic sensor networks. *IEEE Sensors Journal, 12*(12), 3467–3472.2.
2. Khan, F., ur Rehman, A., Usman, M., Tan, Z., & Puthal, D. (2018). Performance of cognitive radio sensor networks using hybrid automatic repeat request: Stop-and-wait. *Mobile Networks and Applications, 23*(3), 1–10.
3. Ahmed, S., Akbar, M., Ullah, R., Ahmed, S., Raza, M., Khan, Z. A., et al. (2015). ARCUN: Analytical approach towards reliability with cooperation for underwater WSNs. *Procedia Computer Science, 52*, 576–583.
4. Jan, M. A., Tan, Z., He, X., & Ni, W. (2018). *Moving towards highly reliable and effective sensor networks*. Philadelphia, PA: Old City Publishing.
5. Ahmad, A., Ahmed, S., Imran, M., Alam, M., Niaz, I. A., & Javaid, N. (2017). On energy efficiency in underwater wireless sensor networks with cooperative routing. *Annals of Telecommunications, 72*(3–4), 173–188.
6. Jan, M. A., Khan, F., Alam, M., & Usman, M. (2017). A payload-based mutual authentication scheme for Internet of Things. *Future Generation Computer Systems.* in press.
7. Javaid, N., Sher, A., Abdul, W., Niaz, I. A., Almogren, A., & Alamri, A. (2017). Cooperative opportunistic pressure based routing for underwater wireless sensor networks. *Sensors, 17*(3), 629.
8. Jan, M. A., Nanda, P., & He, X. (2013, June). Energy evaluation model for an improved centralized clustering hierarchical algorithm in WSN. In *International Conference on wired/wireless internet communication* (pp. 154–167). Berlin: Springer.
9. Ghoreyshi, S. M., Shahrabi, A., & Boutaleb, T. (2016). A novel cooperative opportunistic routing scheme for underwater sensor networks. *Sensors, 16*(3), 297.
10. Jan, M. A., Jan, S. R. U., Alam, M., Akhunzada, A., & Rahman, I. U. (2018). A comprehensive analysis of congestion control protocols in wireless sensor networks. *Mobile Networks and Applications, 23*(3), 1–13.
11. Javaid, N., Hussain, S., Ahmad, A., Imran, M., Khan, A., & Guizani, M. (2017). Region based cooperative routing in underwater wireless sensor networks. *Journal of Network and Computer Applications., 92*, 31–41.
12. Alam, M., Ferreira, J., Mumtaz, S., Jan, M. A., Rebelo, R., & Fonseca, J. A. (2017). Smart cameras are making our beaches safer: A 5G-envisioned distributed architecture for safe, connected coastal areas. *IEEE Vehicular Technology Magazine, 12*(4), 50–59.
13. Javaid, N., Maqsood, H., Wadood, A., Niaz, I. A., Almogren, A., Alamri, A., et al. (2017). A localization based cooperative routing protocol for underwater wireless sensor networks. *Mobile Information Systems, 2017*, 16.
14. Khan, F., ur Rahman, I., Khan, M., Iqbal, N., & Alam, M. (2016, September). CoAP-based request-response interaction model for the internet of things. In *International Conference on future intelligent vehicular technologies* (pp. 146–156). Cham: Springer.
15. Pervaiz, K., Wahid, A., Sajid, M., Khizar, M., Khan, Z. A., Qasim, U., et al. (2016, July). DEAC: Depth and energy aware cooperative routing protocol for underwater wireless sensor

networks. In *2016 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS)* (pp. 150–158). Piscataway, NY: IEEE.
16. Fida, N., Khan, F., Jan, M. A., & Khan, Z. (2016, September). Performance analysis of vehicular adhoc network using different highway traffic scenarios in cloud computing. In *International Conference on future intelligent vehicular technologies* (pp. 157–166). Cham: Springer.
17. Naqvi, S. K. B., Ahmed, S. H. E. E. R. A. Z., Rauf, C. A., & Naqvi, S. S. (2013). Amplification and sequencing of internal transcribed regions 1 & 2, and 5.8 S rDNA from local isolates of fusarium species. *Pakistan Journal of Botany, 45*, 301–307.
18. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2018). A Sybil attack detection scheme for a forest wildfire monitoring application. *Future Generation Computer Systems, 80*, 613–626.
19. Sajid, M., Wahid, A., Pervaiz, K., Khizar, M., Khan, Z. A., Qasim, U., et al. (2016, July). SMIC: Sink mobility with incremental cooperative routing protocol for underwater wireless sensor networks. In *2016 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS)* (pp. 256–263). Piscataway, NY: IEEE.
20. Zhang, J., Fang, Z., Shu, C., Zhang, J., Zhang, Q., & Li, C. (2017). A rotational piezoelectric energy harvester for efficient wind energy harvesting. *Sensors and Actuators A: Physical, 262*, 123–129.
21. Gu, Y., Chen, H., Li, Y., & Vucetic, B. (2016). Distributed multi-relay selection in accumulate-then-forward energy harvesting relay networks. arXiv preprint arXiv:1602.00339.
22. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2013, November). Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network. In *2013 IEEE International Conference on High Performance Computing and Communications & 2013 IEEE 10th International Conference on Embedded and Ubiquitous Computing (HPCC_EUC)* (pp. 1400–1407). Piscataway, NY: IEEE.
23. Jannu, S., & Jana, P. K. (2017). Maximizing network lifetime of wireless sensor networks: An energy harvesting approach. In *Proceedings of the International Conference on signal, networks, computing, and systems* (pp. 331–339). New Delhi: Springer India.
24. Khan, F. (2014, May). Fairness and throughput improvement in multihop wireless ad hoc networks. In *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)* (pp. 1–6). Piscataway, NY: IEEE.

Chapter 15
Congestion Aware and Adaptive Routing Protocols for MANETs: A Survey

Nousheen Akhtar, Muazzam A. Khan Khattak, Ata Ullah, and Muhammad Younus Javed

Abstract MANETs contain mobile nodes that can join or leave the network during the operations intended by the network. During massive communication scenarios, congestion causes increase in transmission delay and packet loss which ultimately leads to waste of resources upon recovery. The current available routing algorithms are not congestion adaptive. Existing surveys on routing include the congestion occurrence and then its control-based techniques in a reactive manner. In this paper, we have focused to further include the congestion avoidance schemes where congestion aware and congestion adaptive protocols for MANETs are discussed. Congestion avoidance-based schemes are further subcategorized under cross-layer and rate control-based protocols. We have also categorically evaluated the existing schemes and presented in a tabular form to highlight the role of end-to-end delay, packet drop ratio, throughput, energy efficiency, data rate, and related metrics. It provides a comprehensive collection of related schemes to overview the contributions in this area and pinpoint the weaknesses for mitigating the unresolved issues.

N. Akhtar · M. A. Khan Khattak (✉)
Department of Computer Engineering, College of EME, NUST, Rawalpindi, Pakistan
e-mail: muazzamak@ce.ceme.edu.pk

A. Ullah
Department of Computer Science, National University of Modern Languages, NUML, Islamabad, Pakistan
e-mail: aullah@numl.edu.pk

M. Y. Javed
Department of Computer Science and Engineering, HITEC University, Taxila, Pakistan
e-mail: myjaved@hitecuni.edu.pk

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_15

15.1 Introduction

Mobile ad hoc networks (MANETs) consist of independent mobile nodes which communicate with each other via wireless links to exchange application-oriented information as illustrated in Fig. 15.1a. MANET applications have diverse domain ranging from small static networks to large-scale highly dynamic military operations, automated battlefield environment, and rescue operations [1]. In mobile ad hoc networks, any node can enter and leave the network. This infrastructure-less property of MANETs offers many challenges including routing in mobility scenarios. Ad hoc model specified by IEEE was a communication pattern where neighboring nodes communicate directly using wireless technologies as Zigbee, Bluetooth, Wi-Fi, and WiMAX. Initially, its applications allowed devices to set up a single-hop ad hoc network, by interconnecting devices in the same transmission range, being the simplest version of infrastructure-less/self-organizing networks [2] as shown in Fig. 15.1b. MANET was launched to enhance possibilities of information exchange through wireless nodes in an infrastructure-less manner. In MANET, nodes can either directly exchange data to sink or transmit via intermediate nodes by using routing capabilities of network as per deployment patterns.

MANETs were thought of as general purpose networks; still in real-world deployment and industrial usage, MANET applications are contemplated as specialized networks administered through single arbiter and designed to provide solutions for specific problems. Some of the applications are as follows: (1) tactical networks, military vehicles, soldiers' headquarters; (2) emergency services, disaster-struck areas; (3) vehicular network, vehicles equipped with wireless interfaces enabling them to communicate with other vehicles; (4) wireless personal area networks, mobiles, cameras, laptops to share information with each other through independent personal networks; and (5) body area networks, wireless medical body sensors that can be attached to human body for monitoring health of a person.

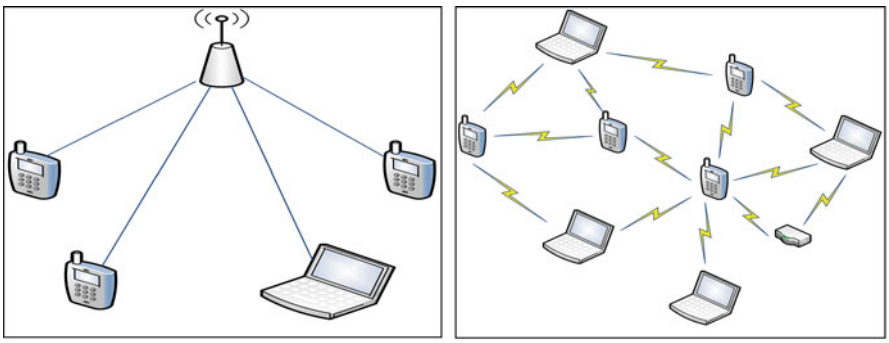


Fig. 15.1 Wireless network types: (**a**) infrastructure and (**b**) infrastructure-less wireless network

This paper presents routing schemes that handle the congestion of messages occurred when network is busy. These schemes can be subdivided into congestion aware and adaptive routing schemes where the former is further subdivided into cross-layer MAC protocols and rate control protocols. Moreover, a number of related mechanisms are discussed that mainly target to handle the congestion. We have also categorically presented the schemes in a tabular form to highlight the metrics compared along with dominating observations in schemes. It also highlights the related linkages among the schemes to proceed in this area of research.

The rest of the paper is organized as follows: Sect. 15.2 represents literature review that is subcategorized in congestion control and congestion avoidance-based schemes where the latter is divided into cross-layer protocols and rate control protocols. Moreover, congestion adaptive protocols are discussed. Section 15.3 provides comprehensive analysis of existing schemes. Section 15.4 explores conclusion and future work.

15.2 Literature Review

Routing involves the path discovery between sender and receiver nodes in MANET. It can be categorized into reactive and proactive approaches where the former involves the routing table management for all routes and the latter is about maintaining on-demand routes used currently. The main issue in all kind of routing protocols is how to transmit data from source to destination provided packet drops due to congestion and limited network resources. Most of the schemes are based on alternate path selection in occurrence of congestion on current path. The consequences of these schemes include increase in network overhead, increase in delay, and wastage of network resources. An efficient congestion aware routing technique must satisfy properties including (1) efficient utilization of network resources, (2) minimum delay, (3) maximum end-to-end throughput, and (4) efficient handling of path break.

Congestion is the compromised QoS in which network node carries data more than its capacity. In ad hoc networks, mobile nodes are connected with each other through a wireless link in a multi-hop fashion. As there is no fix infrastructure so when nodes communicate with each other, i.e., when sender nodes transmit data toward destination, any of its intermediate nodes may suffer from network overloading because the number of packets being sent on wireless links is greater than link or network capacity. This overloaded network may cause congestion on wireless links resulting in high packet loss, increase in delay, and reduced network throughput [3–5]. Congestion may also occur due to dynamic network topology in which sometimes end-to-end network connectivity may loss because of continuous movement of nodes. Congestion control routing techniques are classified as congestion aware routing and congestion adaptive routing in which congestion status routes can be changed. Congestion aware routing protocols include cross-

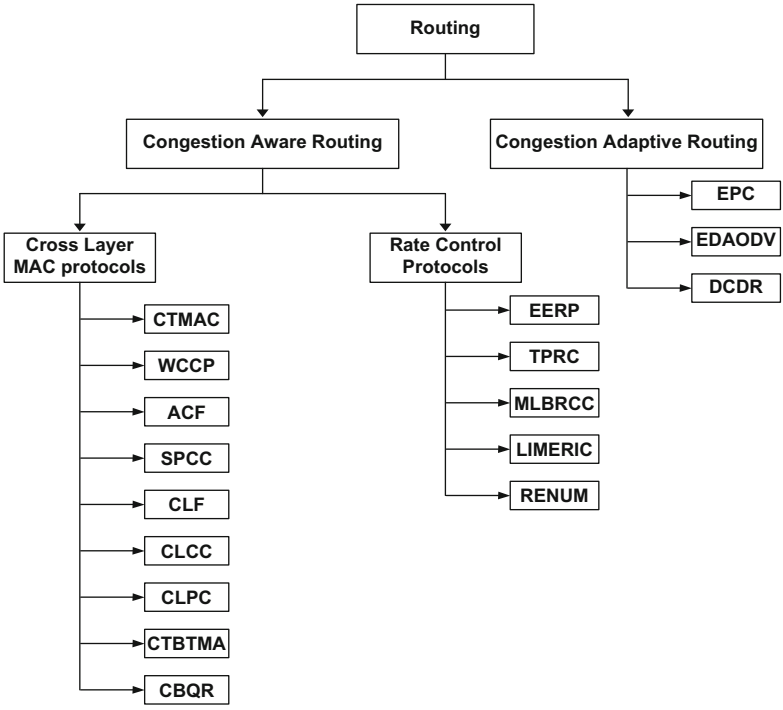


Fig. 15.2 Taxonomy of congestion aware and congestion adaptive protocols

layer MAC protocols and rate control protocols. Figure 15.2 shows the taxonomy of congestion aware and congestion adaptive routing protocols.

15.2.1 Congestion Aware Routing Protocols

These protocols consider congestion during route establishment phase. Selected route will not change unless intermediate node moves to some other location or route break happens. Protocols include cross-layer MAC protocols and rate control protocols.

15.2.1.1 Cross-Layer MAC Protocols

Cross-layer protocols normally get data from a layer and transmit it to other layers. The protocols we have chosen communicate between application layer, transport layer, and network layer. The following are some protocols of cross-layer approach: Wanrong Yu et al. have proposed an efficient throughput protocol

entitled Concurrent Transmission MAC (CTMAC) [6]. It supports transmission only when network has one transceiver, one channel, and one power architecture for transmission. An additional control gap has been introduced in CTMAC, which is basically the gap between the data packets (DATA/ACK) and control packets (RTS/CTS).

Hongqiang Zhai et al. have presented a new novel technique named Wireless Congestion Control Protocol (WCCP) [7]. The purpose of this protocol was to make transport service more fair and efficient in multi-hop ad hoc network. This protocol works on the busyness ratio of the channel, i.e., calculating the intra-node and internode allocation of available resources on fair channel and then allocating them to flow passed by and inserting feedback based on acquired busyness ratio of respective channel. Source node receives feedback from the destination node and adjusts its sending rate accordingly. That is, the incoming data rate is controlled by observing feedback received from bottleneck link.

An admission control and feedback (ACF) scheme has been embedded in a protocol named QoS-aware routing protocol, for the first time [8]. This scheme helps meeting the requirements based on QoS for any real-time application. The QoS-aware routing protocol has been used against network traffic and estimating bandwidth approximation. Mainly, the work is composed of three parts: (1) estimation of available bandwidth, (2) embedding QoS-aware scheme QoS31 with the route discovery procedure, and, lastly, using (3) cross-layer design for provision of feedback to application layer.

Vinod et al. have proposed a congestion control algorithm (SPCC) [9] which uses the shortest path using PEER approach for transmission in ad hoc networks. During path establishment link cost is considered as parameter by using transmission power and receiving power. In this way the congestion in selected path is controlled.

Anuradha et al. have proposed a cross-layer-based approach using fuzzy logic (CLF) [10]. Whenever some event in the network occurs, the algorithm detects its type and handles it accordingly. The algorithm also sets alternate paths by applying fuzzy logic; whenever congestion occurs the traffic is redirected to alternate path.

Sheeja et al. proposed a cross-layer-based congestion control (CLCC) [11] mechanism to reduce number of packet loss in network. The author defined four phases of proposed scheme. First phase ensures information sharing between different layers, while in second phase congestion is detected. In third phase, congestion control mechanism is applied which uses path gain and buffer tendency as a parameter. In final phase, the packet format is defined. Sarfaraz et al. have proposed a cross-layer approach for power control (CLPC) [12] to deal with received signal strength (RSS)-related issues. According to authors the RSS may affect physical, network, and transport layer. It is able to increase the transmission power by averaging, affecting the physical layer, the network layer, and transport layer. In [12] the designed approach selects best route between source and destination which is congestion-free.

Hangguan Shan et al. have presented an efficient grouping algorithm (CTBTMA) [13] for selecting helper node which is optimal as well. In order to increase throughput of network, MAC protocol is supported with greedy algorithm. According to

the optimal grouping of helpers, cooperation gain is accomplished and enhanced after incorporating the selection of helper module in MAC protocol. Suburah et al. presented cross-layer-based QoS routing (CBQR) [14] for the purpose of congestion control and provision of route stability in mobile ad hoc networks. The main feature of this protocol is (1) bandwidth aware, (2) congestion aware, and (3) QoS-based cross-layer architecture of network. The protocol works with physical, MAC, and network layer; when data is transmitted from source to destination, the source node chooses the path which satisfies load and link capacity. In this method the congestion is detected and controlled by the data rate adaptation. If the outgoing link is not stable, then source node selects path with less expected transmission time (ETT).

15.2.1.2 Rate Control Protocols

Rate-controlled protocols are those in which congestion is controlled by adjusting sending rate. To do this network, information is sent to source node which adjust its sending rate according to available sources at required links. The following are some rate-based congestion control protocols where sender node is responsible for injecting appropriate data rate.

Priakanth et al. have proposed a channel-adaptive energy-efficient routing protocol (EERP) [15]. In the approach, at first the channel and connection quality for each challenging stream is computed by every node. As indicated by that calculation, the weight is calculated and spread into network. The protocol permits the network for the streams having weight more than Channel Quality Threshold (CQT). A scheduling and queuing algorithm is provided by the author in order to avoid buffer.

Masaki Bandai et al. [16] have proposed a new mechanism for Medium Access Control (MAC) protocol with transmission power and transmission rate control (TPRC) in multi-rate ad hoc network. It achieves efficient energy consumption by managing transmission power and communication sequences discussed as follows:

(a) Transmission power: For every node the energy efficiency of all mixes of transmission power and rate is figured and stored in the table of each node. The most efficient grouping of calculated transmission power and transmission rate is selected by sender node.
(b) Communication sequence: Communication sequences having high energy efficiency are selected by receiver node. Each node maintains a table having values of transmission power and data rate.

Soundararajan et al. [17] have proposed multipath routing mechanism named multipath load balancing and rate-based congestion control (MLBRCC) for congestion control. In the MLBRCC mechanism, the destination node sends network information to the application which then adjusts its sending rate according to network conditions. Gaurav et al. [18] have discussed an adaptive congestion control mechanism which is applied to data rate of device. Other traditional approaches called linear message rate integrated control (LIMERIC) mechanism take the benefit

of precision control mechanism that is by default available in wireless channel. Songtao et al. [19] have developed a rate-effective network utility maximization (RENUM) algorithm which decreases the data rate on a selected route from source to destination. This framework works by associating network utility with destination node of every flow instead of informing source node about data rate.

15.2.2 Congestion Adaptive Routing Protocols

Alonso et al. [20] have proposed a routing mechanism named endpoint congestion (EPC) which improves the performance of overall network by separating congested traffic from normal traffic by using concept of adaptive routing. Endpoint congestion filter is used to separate the traffic. This filter blocks the congestion from spreading into entire network. This filter is installed in router so that it can check whether incoming packet can create congestion in network. Suppose a packet named p1 is currently sent by the route to destination node d1, meanwhile another packet named p2 arrives at router, now filter will stop this packet to get forward by router until the earlier packet p1 reached at destination. In this way congestion can be avoided by spreading into network.

Sankaranarayanan [21] has introduced early detection congestion and control routing protocol (EDAODV). This algorithm aims to provide alternate path when congestion occurs in a bidirectional manner, i.e., both forward and reverse direction of congested node. There are two phases of this algorithm: (1) route discovery and (2) congestion detection at early stages (bidirectional path discovery). Each node maintains two routing tables, one is primary routing table (PRT) which is maintained during primary path establishment phase for different destinations while the other is alternate routing table (ART) which maintains alternate paths by corresponding an entry to the PRT.

Xia et al. proposed an enhanced AODV in order to add congestion aware routing mechanism. The traditional AODV is unable to handle congestion which is one of the major disadvantages of AODV. They have improved RREQ and RREP functions of conventional AODV. Dynamic congestion detection and control routing (DCDR) [22] is a mechanism which reduces congestion by setting congestion-free paths at initial phase of route establishment phase. This algorithm configures all congestion-free paths by using CFS which is at one- or two-hop neighbor.

15.3 Comparative Analysis of Congestion Control Protocols

In this section a comprehensive analysis of some of the existing congestion control protocols is presented. Table 15.1 highlights the category, methodology, and metrics. Category includes the congestion management (CM), rate control, and congestion avoidance (CA). We have also explored the related schemes to identify the presence

Table 15.1 Comparative analysis of congestion aware and adaptive protocols

Sr no	Title	Category	Methodology	Metrics						Application
				End-to-end delay	Throughput	PDR	Packet loss	Energy efficiency	Data rate	
1	CTMAC [6]	CM	Control gap between data and control packets	_	✓	_	_	_	_	High-throughput networks
2	WCCP [7]	CM	Channel busyness ratio, channel resource allocation	✓	✓	_	_	_	_	Starvation scenario
3	ACF [8]	CM	Admission control and feedback to application layer	✓	✓	_	_	_	_	Real environment
4	SPCC [9]	CM	Shortest path using PEER approach	✓	_	✓	✓	✓	_	Low-energy networks
5	CLF [10]	CM	Select alternate path using fuzzy logic	✓	✓	✓	_	_	✓	Delay-tolerant networks
6	CLCC [11]	CM	Defined four phases for congestion control	✓	✓	✓	_	_	_	Highly congested environment
7	CLPC [12]	CM	Receiver signal strength for congestion control	✓	_	✓	_	_	_	Congestion aware routing
8	CTBTMA [13]	CM	Helper node to detect and control congestion	_	✓	_	_	_	_	High signal to noise ratio environment
9	CBQR [14]	CM	QoS-based bandwidth aware and congestion aware metric	_	✓	_	_	_	✓	Multimedia environment

10	EERP [15]	RC	Energy-based routing strategy	_	✓	_	_	✓	✓	Highly congested scenario
11	TPRC [16]	RC	Transmission power with two communication sequence	_	✓	_	_	✓	_	Low transmission power
12	MLBRCC [17]	RC	Multipath load balancing and data rate adaptation	✓	_	✓	_	_	✓	High data rate applications
13	LIMERIC [18]	RC	Channel and link quality-based weight assignment	_	✓	_	_	_	✓	Challenging flows
14	RENUM [19]	CA	Utility is used to adjust data rate rather than injecting it to source node	✓	_	_	_	✓	✓	Low power consumption and delay
15	EPC [20]	CA	Separation of congested traffic flow from normal flow	_	✓	_	_	_	✓	Bottleneck links
16	EDAODV [21]	CA	Modification of AODV. Congestion is detected using bidirectional approach	✓	_	✓	_	_	✓	Congestion aware routing
17	DCDR [22]	CA	Queue length-based congestion detection. Establish congestion-free routes	✓	_	✓	_	_	_	Applicable only at medium-level data load

and effectiveness of different metrics including end-to-end delay, throughput, packet delivery ratio, packet loss, energy efficiency, and data rate.

15.4 Conclusion

This paper presents an overview of different congestion control routing protocols for mobile ad hoc networks. In literature, it has been observed that a single algorithm can not perfectly control congestion in MANET due to limited resources in terms of bandwidth, battery life, and buffer size. It arises the need for new solutions that adopt dominating features of existing solutions for better congestion control. The efficiency of a protocol lies in a fact that it should adopt the changes of network and congestion rather than eliminating it from the network. The main purpose of this study is to explore existing congestion control techniques that can help other researchers to further explore the limitations of congestion control protocols for future research. We have also evaluated the related schemes to identify the role of metric in each scheme and its consideration for results comparison. It highlights the importance of a metric. In the future, we shall explore the impact of congestion avoidance schemes in real-time link-state routing scenarios and compare with the distance vector-based routing schemes.

References

1. Usman, M., Jan, M. A., He, X., & Alam, M. (2018). Performance evaluation of high definition video streaming over mobile ad hoc networks. *Signal Processing, 148*, 303–313.
2. Khan, F., Kamal, S. A., & Arif, F. (2013). Fairness improvement in long chain multihop wireless ad hoc networks. In *2013 International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 556–561). Piscataway, NJ: IEEE.
3. Jan, M. A., Jan, S. R. U., Alam, M., Akhunzada, A., & Rahman, I. U. (2018). A comprehensive analysis of congestion control protocols in wireless sensor networks. *Mobile Networks and Applications, 23*(3), 456–468.
4. Mamata, R., Umesh, P. R., Niharika, P., Surendra, K. N., & Sambhu, P. (2017). Congestion control mechanism for real time traffic in mobile adhoc networks. *Computer Communication, Networking and Internet Security, Springer, 5*, 149–156.
5. Umapathi, N., Ramaraj, N., Balasubramaniam, D., & Adlin, R. (2015). An hybrid ant routing algorithm for reliable throughput using MANET. *Intelligent Computing and Applications, 343*, 127–136.
6. Khan, F. (2014, May). Fairness and throughput improvement in multihop wireless ad hoc networks. In *Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on* (pp. 1–6). Piscataway, NJ: IEEE.
7. Hongqiang, Z., Xiang, C., & Yuguang, F. (2007). Improving transport layer performance in multihop ad hoc networks by exploiting MAC layer information. *IEEE Transactions on Wireless Communications, 6*(5), 1692–1701.
8. Jabeen, Q., Khan, F., Khan, S., & Jan, M. A. (2016). Performance improvement in multihop wireless mobile adhoc networks. *The Journal Applied, Environmental, and Biological Sciences (JAEBS), 6*(4S), 82–92.

9. Vinod, K. R., & Wahidabanu, R. S. D. (2013). Cross-layer based energy efficient congestion control protocol for MANETs. *International Review on Computers and Software (IRECOS), 8*(12), 2992–3001.
10. Anuradha, M., & Anandha, M. G. S. (2017). Cross-layer based congestion detection and routing protocol using fuzzy logic for MANET. *Wireless Networks, 23*(5), 1373–1385.
11. Sheeja, S., & Pujeri, R. V. (2013). Cross layer based congestion control scheme for mobile ad hoc networks. *International Journal of Computer Applications, IJCA, 67*(9), 60–67.
12. Sarfaraz, A. A., Senthil, K. T., Syed, A. S. S., & Suburam, S. (2015). Cross-layer design approach for power control in mobile ad hoc networks. *Egyptian Informatics Journal, 16*(1), 1–7.
13. Khan, F., Rahman, F., Khan, S., & Kamal, S. A. (2018). Performance analysis of transport protocols for multimedia traffic over mobile wi-max network under nakagami fading. In *Information technology-new generations* (pp. 101–110). Cham, Switzerland: Springer.
14. Saurabh, S., Dipti, J., & Rashi, A. (2017). An approach for congestion control in mobile ad hoc. *International Journal of Emerging Trends in Engineering and Development, 3*(7), 217–223.
15. Priakanth, P., & Thangaraj, P. (2009). A channel adaptive energy efficient and fair scheduling media access control protocol for mobile adhoc networks. *Journal of Computer Science, 5*(1), 57–63.
16. Masaki, B., Satoshi, M., & Takashi, W. (2008). Energy efficient MAC protocol with power and rate control in multi-rate ad hoc networks. In *Vehicular Technology Conference, 2008. VTC Spring 2008*. Singapore: IEEE.
17. Soundararajan, S., & Bhuvaneswaran, R. S. (2012). Multipath load balancing & rate based congestion control for mobile ad hoc networks (MANET). In *Digital information and communication technology and it's applications (DICTAP)*, Bangkok, Thailand.
18. Gaurav, B., John, B. K., & Charles, E. R. (2013). LIMERIC: A linear adaptive message rate algorithm for DSRC congestion control. *IEEE Transactions on Vehicular Technology, 62*(9), 4182–4197.
19. Songtao, G., Changyin, D., & Yuanyuan, Y. (2014). Joint optimal data rate and power allocation in lossy mobile ad hoc networks with delay-constrained traffics. *IEEE Transactions on Computers, 64*(3), 747–762.
20. Miguel, G., & José, F. (2015). End-point congestion filter for adaptive routing with congestion-insensitive performance. In *IEEE computer architecture letters*.
21. Fida, N., Khan, F., Jan, M. A., & Khan, Z. (2016, September). Performance analysis of vehicular adhoc network using different highway traffic scenarios in cloud computing. In *International Conference on Future Intelligent Vehicular Technologies* (pp. 157–166). Cham, Switzerland: Springer.
22. Khan, F., ur Rehman, A., Usman, M., Tan, Z., & Puthal, D. (2018). Performance of cognitive radio sensor networks using hybrid automatic repeat request: Stop-and-wait. *Mobile Networks and Applications, 23*(3), 479–488.

Chapter 16
Scalability Analysis of Depth-Based Routing and Energy-Efficient Depth-Based Routing Protocols in Terms of Delay, Throughput, and Path Loss in Underwater Acoustic Sensor Networks

Saqib Shahid Rahim, Sheeraz Ahmed, Nadeem Javaid, Adil Khan, Nouman Siddiqui, Fazle Hadi, and M. Ayub Khan

Abstract In underwater acoustic sensor networks (UWASNs), nodes are either static or dynamic depending upon the network configuration and type of application. Direct or multi-hop transmissions are used to forward data toward the sink. Alternatively, sinks can also be mobile or static, depending on whether the application is real time or passive. The variety of nodes and sink deployments greatly affect the performance of routing protocols. In this chapter, we analyze the effects of node density and scalability on the performance of routing protocols in UWASNs. Two

S. S. Rahim (✉)
Career Dynamics Research Centre, Peshawar, Pakistan

Abasyn University, Peshawar, Pakistan

Preston University, Peshawar, Pakistan
e-mail: saqib.shahid@abasyn.edu.pk

S. Ahmed · M. Ayub Khan
Career Dynamics Research Centre, Peshawar, Pakistan

Iqra National University, Peshawar, Pakistan

N. Javaid
COMSATS Institute of Information Technology, Islamabad, Pakistan

A. Khan (✉)
Career Dynamics Research Centre, Peshawar, Pakistan

Abdul Wali Khan University, Mardan, Pakistan
e-mail: adil.khan.kakakhel@awkum.edu.pk

N. Siddiqui
Career Dynamics Research Centre, Peshawar, Pakistan

Fazle Hadi
Higher Education Department, Govt. of Khyber Pakhtunkhwa, Pakistan

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_16

popular UWASNs protocols were selected for this purpose: the depth-based routing protocol (DBR) and energy-efficient depth-based routing protocol (EEDBR). DBR is a non-cluster-based technique that performs routing using only the depth of nodes, whereas EEDBR is a location-free scheme that uses both the depth and the residual energy of nodes to route data. The scalability of node deployment was used to check the efficiency of these schemes in the context of three parameters: packet delivery ratio, end-to-end delay, and path loss.

16.1 Introduction

One-third of Earth consists of oceanic areas, which are largely unexplored. Several underwater activities already exist, including underwater mining, water pollution controls, seismic monitoring, security, and sports. Conventional approaches to observe underwater environments have several limitations, such as the cost of devices and extended delays to analyze the examined data [1]. To address these issues, underwater acoustic sensor networks (UWASNs) are being developed to explore the underwater environment. UWASNs are composed of sensor nodes (also known as *nodes*). These nodes cooperatively examine different activities within a particular area [1]. A simple architecture of a UWASN is shown in Fig. 16.1.

A UWASN is composed of acoustic sensors with single multi-surface sinks that are dropped under the water to examine the underwater environment. The surface sink usually has little power restriction, whereas the sensor nodes have very restricted energy [2]. Sinks (also known as *sonobuoys*) exists at the ocean surface. These sinks contain two modems: an acoustic and a radio. For example, the nodes in the Sensor Equipped Aquatic (SEA) Swarm architecture observe nearby underwater events and report them to one of the sinks—a process known as *anycasting*. The gathered statistics are unloaded to an examination station through radiowaves for auxiliary offline processing [3, 4].

UWASNs have potential use in applications such as seismic monitoring, ocean mine exploration, and disaster prevention. UWASNs provide operational approaches for routing. This is a necessity for time-critical applications, and hence in the design of delay-sensitive protocols [5].

Radio signals are not suitable for transmissions in UWASNs because radio waves absorb in water rapidly. Hence, acoustic waves are used in this environment [6]; for high data rates in underwater communications, acoustic signals are also the best source [7]. A UWASN achieves this goal with underwater vehicles and sensor nodes. Underwater transmission has some unique challenges, such as low bandwidth, limited mobility of nodes, delays, low memory, and battery constraints. Current research on deep-water activities is based on different technologies. Because acoustic waves are used in water as a medium of communication and to transmit data, UWASNs have a greater variety of network designs than do terrestrial communication systems. Many techniques have been proposed for effective routing

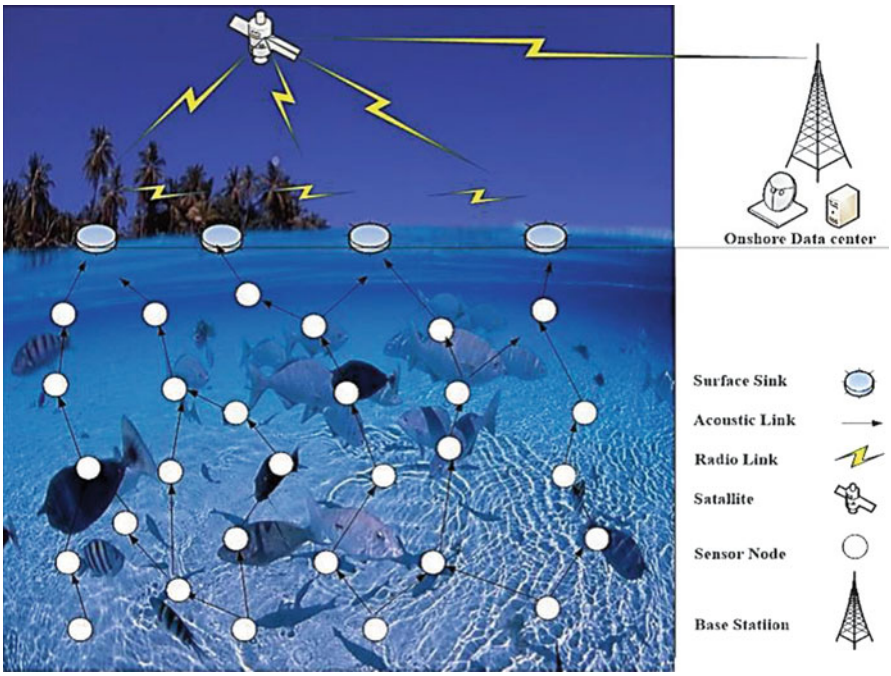


Fig. 16.1 UWASN architecture

in USWNs, such as cooperation-based routing that transmits from deep water to a surface sink by relay [8].

This chapter focuses on the scalability analysis of two well-known schemes: depth-based routing protocol (DBR) [9] and and energy-efficient depth-based routing protocol (EEDBR) [10]. DBR [9] is a non-cluster-based technique that perform routing using just the depth of nodes, whereas EEDBR [10] is a location-free scheme that uses depth along with the residual energy of nodes to route data. The scalability of node deployment is applied to examine the efficiency of these schemes in the context of three parameters: packet delivery ratio, end-to-end delay and path loss. This chapter is arranged as follows: Sect. 16.2 provides the literature review; Sect. 16.3 discusses the motivation for our work; Sects. 16.4 and 16.5 illustrate the DBR and EEDBR schemes, respectively; and Sects. 16.6 and 16.7 discuss the scalability of these schemes. Finally, Sect. 16.8 describes a cooperative node technique and the energy harvesting of nodes as future goals for researchers in this field.

16.2 Related Work

Researchers have proposed a variety of protocols and techniques to increase performance and reliable communications in UWASNs. Some of these approaches are summarized and discussed in this section.

Noh et al. [3] proposed the Void Aware Pressure Routing for Underwater Sensor Networks (VAPR) protocol, which features a pressure routing technique. This scheme uses pressure meters to deliver depths and transmit information data packets to a surface sink. A series of depth information in periodic beacons and hops are counted to establish a subsequent hop track, which makes a directional link to a nearby surface sink.

Javaid et al. [2] introduced a forwarding equation based on a routing scheme for UWASNs: Improved Adaptive Mobility of Courier nodes in Threshold-optimized Depth-based routing Protocol (iAMCTD). This protocol increases the lifetime of an underwater network through an optimal viable mobility strategy for surface sinks. The iAMCTD scheme depends on a cost function. Compared with many other depth-based underwater techniques, this approach exploits the network density for applications that are time critical. To control the transmission loss, water flooding, and transmission latency, the authors designed an equation for a depth-dependent function that also uses signal-to-noise ratio, the signal quality index, optimal holding time, and energy-cost function routing parameters. The equation computes the prime energy limit, soft threshold, and hard threshold to provide routing on demand [2].

In the Cooperative Energy-Efficient for Underwater WSN (Co-UWSN) protocol, Ahmed et al. [4] used a cooperation scheme to improve a UWASN's lifetime, enhance the delivery ratio of data, and reduce the overall energy tax, which is specifically advantageous for time-critical and delay-sensitive applications. Using cooperative communication, this technique mitigates the effects of noise and multipath fading. By changing the depth threshold, the number of eligible neighbors increases; hence, data loss is reduced in delay-sensitive applications. This cooperation technique improves the load balancing of the UWASN and the stability of the network [4].

In another study by Ahmed et al. [11], the Stochastic Performance Analysis with Reliability and Cooperation (SPARCO) technique was used to increase the efficiency of the network. Cooperative communication was introduced for routing in UWASNs to effectively consume energy. All nodes of the network were assumed to consist of a unidirectional antenna. To reduce energy consumption, several nodes transmitted their data cooperatively to take advantage of the spatial diversity [11]. In addition, the Adaptive Mobility of Courier nodes in Threshold-Optimized DBR (AMCTD) [12] achieved adaptive mobility in special mobile nodes called courier nodes to improve the life of the network. This protocol calculates the holding time based on the weight function, which controls the issue of transmission loss [12].

Javaid et al. [5] also proposed the Delay-Sensitive Depth-Based Routing (DSDBR), Delay-Sensitive Energy Efficient Depth-Based Routing (DSEEDBR), and Delay-Sensitive Adaptive Mobility of Courier nodes in Threshold-optimized

Depth-based routing (DSAMCTD) schemes. These protocols empower depth-based routing techniques. The efficiency of the proposed protocols was verified for UWASNs. These schemes use delay-efficient priority factors and delay-sensitive holding time to reduce end-to-end delays; however, a minor reduction in the throughput of the network occurred. All techniques employed an optimum weight function to compute the speed of the received signal and path loss. Moreover, a solution for the delay problem was found by forwarding the data efficiently, with nominal relative transmissions in low depth areas and the selection of an optimal forwarder. Simulation results showed that the protocols greatly reduced end-to-end delays and enhanced path loss [5].

Another study by Javaid et al. [13] proposed a scheme called the Region-Based Cooperative Routing Protocol (RBCRP). In this protocol, amplification and forwarding occur over Rayleigh worn links in UWASNs. The sender node transmits data packets, which are sensed by the sensor node to the endpoint and accessible relays. The bit error rate is tested at the end node, based on negative or positive retorts to the sender and relays. The authors used mobile sinks with energy harvesting to improve the packet delivery ratio and network stability. RBCRP was found to attain enhanced network stability, outage probabilities, and high packet delivery ratios compared with an incremental best relay scheme [13].

Ahmed et al. [14] also proposed cooperative communication to build an energy-efficient protocol for UWASNs, referred to as Cooperative Energy Efficient routing for UWSNs (Co-EEUWSN). In this protocol, all nodes of the UWASN contains a directional antenna, while several nodes coordinate with each other. At the relay, Co-EEUWSN employed the amplify-and-forward mechanism; however, at the receiving node, the fixed ratio combining was used. In a comparison of this scheme's results with those of EEDBR and cooperative DBR, Co-EEUWSN showed improved energy efficiency, decreased end-to-end delays, and enhanced throughput [14].

16.3 Motivation

Based on the literature review, most researchers [9, 10, 14, 15] use node depth as a parameter for data routing. However, they do not address node load balancing and the distribution of load when the sensor nodes are uneven. Therefore, the efficiency of energy consumption in the nodes is not properly controlled when only depth is used [9]. Wahid et al. [10] used both depth and residual energy as a metric to forward data. DBR attempts to attain a longer network lifetime but has a short stability period. The reason for this problem is due to the redundant transmission of data packets with a heavy load on the low-depth sensor nodes of the UWASN. EEDBR is not a cooperation-based protocol; hence, the packets are led from the source to the destination using a single route with a multi-hop style. Because of noise and fading of the multipath environment, many time signals suffer from a high bit error rate.

16.4 Description of the DBR Scheme

DBR is based on a greedy approach that attempts to send a data packet from a node to surface buoys. During the progression of data, the depth of the promoting nodes shrinks, even as the data reaches the sinks. If the depth of the sending node is shrunk in each step, then the data can be supplied to a sink at the surface. In the DBR technique, the node makes the decision to send data based on its own depth and the preceding sender's node depth, which is the significant concept of this protocol. According to the DBR scheme, upon receiving the data, the node first takes the depth (*dp*) of the data of the preceding hop, which resides with the data packet. Then, the receiving node matches its own depth (*dc*) to *dp*. If the node is nearer to the surface of the water ($dc < dp$), then this node will nominate itself to send the data. In other cases, the packet will be dropped because the packet came from a node that is nearer to the sink at the water surface. Multiple links cannot be fully abolished; hence, DBR use a queue known as a "priority queue." This queue decreases the number of sending nodes, as well as controls the number of sending links.

In DBR, every node also has a packet history buffer. The priority queue is denoted by Q1 and the packet history buffer by Q2. Q2 consists of a unique packet identification (ID) and packet sequence number. When correctly sending data packets, the node inserts the ID of the data packet into queue Q2; on overflow of this queue, the least recently accessed mechanism is used. Q1 is composed of data packets and the scheduled forwarding times for the data packets. The significance of an item in queue Q1 is denoted by the scheduled forwarding time. An item with a prior forwarding time has greater priority. On reception of a packet, the node first holds the packet for a specific length of time, which is known as the holding time. The scheduled sending time of a data packet is calculated based on the received time of the data packet and the holding time of the data packet [9].

The holding time is computed by using the linear function of d, where d is the difference between the depths of the recent node and the preceding node.

$$f(d) = \alpha \cdot d + \beta \tag{16.1}$$

Suppose that d_1 and d_2 are the depth differences of the n_1 and n_2 nodes, respectively, from the source node (S) as shown in Fig. 16.2. t_1 is the time that it takes to receives packet n_1 from S, whereas t_2 is the time that it takes to send from S to n_2. The propagation delay between n_1 and n_2 is t_{12}. Two situations can be expressed by the following:

$$f(d_1) < f(d_2) \tag{16.2}$$

and

$$t_1 + f(d_1) + t_{12} \leq t_2 + f(d_2) \tag{16.3}$$

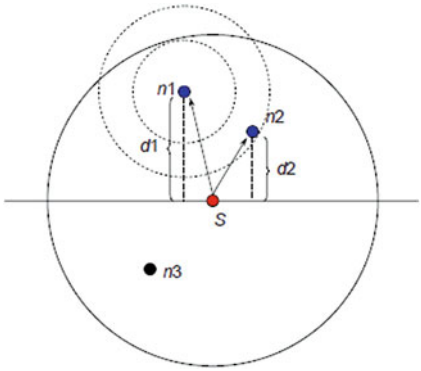


Fig. 16.2 Forwarding node selection [9]

by substituting $f(d)$ with the linear function

$$\alpha \leq (t_2 - t_1) - t_{12}/d_1 - d_2, (\alpha < 0)\,,$$

where α is non-positive.

As long as $|\alpha| \geq (t_1 - t_2) + t_{12}/(d_1 - d_2)$, the conditions of (16.2) and (16.3) can be met. α depends on the depth difference of the n_1, n_2 nodes. α can vary between 0 and R for a node with one-hop neighbors, where R is the highest range of transmission of the node. δ is a global parameter to replace the depth difference for holding time computations. Hence $\alpha = -2\tau/\delta$. Suppose the node with the least depth has a holding time of 0. β can be computed by the following expression: $-2\tau/\delta \cdot R + \beta = 0$.

By substituting α and β in (16.1),

$$f(d) = 2\tau/\delta \cdot (R - d)\,, \delta \in (0, R] \tag{16.4}$$

16.5 Description of the EEDBR Scheme

Energy efficiency is a major concern in UWASNs because the batteries have very limited energy and their replacement is costly. Thus, EEDBR is an energy-efficient scheme in which the major focus is the nodes' energy [10].

EEDBR uses two parameters for transferring data: nodes' depth and their residual energy. The nodes' residual energy is used to increase the stability period. A Hello packet is broadcast by all nodes in the information acquirement phase to its one-hop neighbors. This packet consists of residual energy and the depth of that node. When this packet is received by the neighbors, they hold the residual energy and depth information of only those nodes with lesser depths. Keeping this information from all nodes is not necessary. The updated information on depth is not so important, although residual energy is required to be updated from time to time. To solve this issue, the nodes in an EEDBR scheme check their residual energy with a time interval-based mechanism [10].

In the data forwarding phase, the data is transferred from a node to a terminus node or surface sink, depending on the residual energy and depth statistics of the nodes. In this scheme, all nodes have information on their neighbors' residual energy and depth. The forwarding node selects the optimal next hop forwarder node. The holding time (T_m) is calculated by (16.5):

$$T_m = (1 - (\text{current energy}/\text{initial energy})) * \max \text{holdingtime} + pv, \quad (16.5)$$

In (16.5), max_holding_time is a system metric and pv is the priority value. This pv is used to avoid multi-forwarding nodes. Hence, to prevent duplicated transmissions, the pv value is added to the holding time so that the differences between the holding times of sending nodes have the same residual energies. The list of forwarder nodes is arranged depending on residual energy. On the reception of data, forwarder nodes add the priority value to the holding time depending on the location within the list. The value of the priority is multiplied by two and by the increase of position in the list index. Hence, the uppermost node of the list has the maximum priority because it contains the maximum residual energy among all neighbors; this node will send data immediately on reception [10].

To balance the energies of nodes, the node that has the maximum energy is chosen. In a case where more than one node contains the same energy and depth, any node can be nominated for sending. An abundant suppression of data packet transmissions highly disturbs the delivery ratio of data, while the delivery ratio in many applications is more significant than the energy. Hence, for these applications, EEDBR uses an application-based suppression technique. When sending the data, the source node adds the number of data packets; on reception, the sink node calculates the delivery ratio. If the delivery ratio is smaller than the anticipated delivery ratio, then the sink notifies the source by transmitting a packet that consists of the delivery ratio at the sink. The source also adds the value of the delivery ratio that is received from the surface sink into the packet. On reception of the data packet, the sending nodes makes a decision on whether to suppress the packet or transmit it, depending on the value of the delivery ratio. The forwarding operation of the data is depicted in Fig. 16.3.

16.6 Scalability Analysis of DBR

In this section, we investigate and depict the scalability of DBR under different node densities during the stability period. The stability period is defined as the time period until the first network node expires. The following performance metrics for scalability were selected: throughput, end-to-end delay, and path loss.

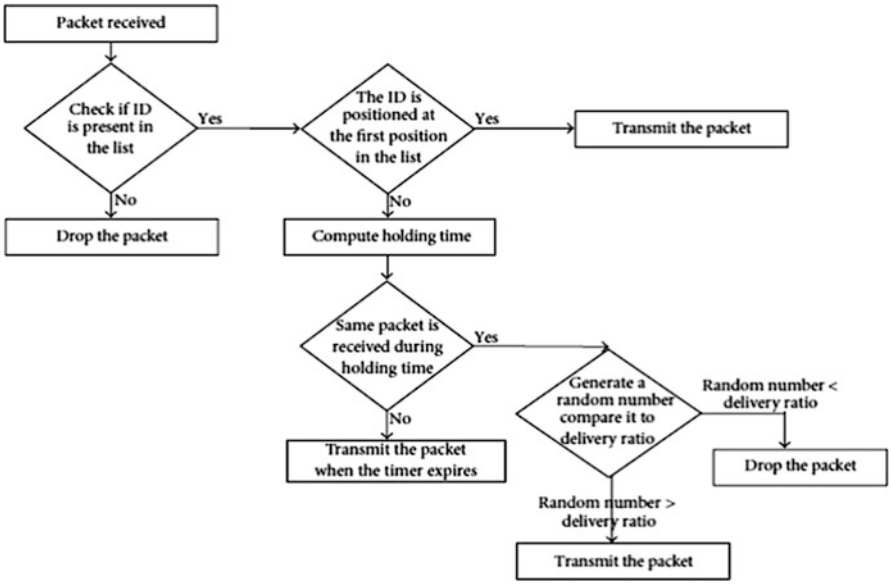


Fig. 16.3 Operation at the forwarding node [10]

16.6.1 Throughput Analysis

The throughput analysis in terms of the scalability of the DBR scheme is shown in Fig. 16.4. In first 1000 rounds, the delivery ratio was highest when the number of nodes was 100, 250, 400, or 500 (that is, 100 or near to 100). The lowest delivery ratio was 17 for 500 nodes at a round number of 5000. The optimal throughput was found for 250 nodes at each round, with an average delivery that was also better than others.

16.6.2 End-to-End Delay

The end-to-end delay analysis in terms of the scalability of the DBR scheme is shown in Fig. 16.5. The maximum delay was 133 for 500 nodes at 1000 rounds, while the minimum delay was 5 for 250 nodes at 5000 rounds. Overall, a low delay was found from 1000 to 5000 rounds for 100 nodes. The figure also depicts that delay was high at each round for 500 nodes.

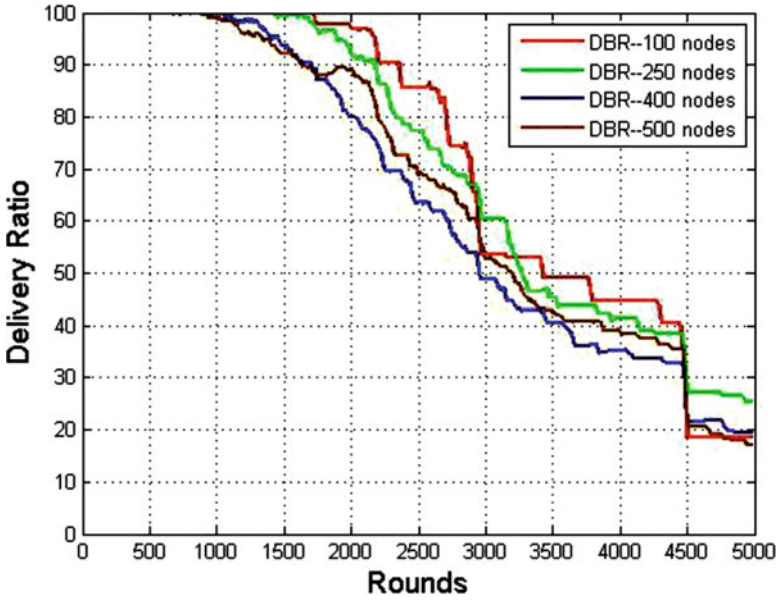


Fig. 16.4 Throughput scalability

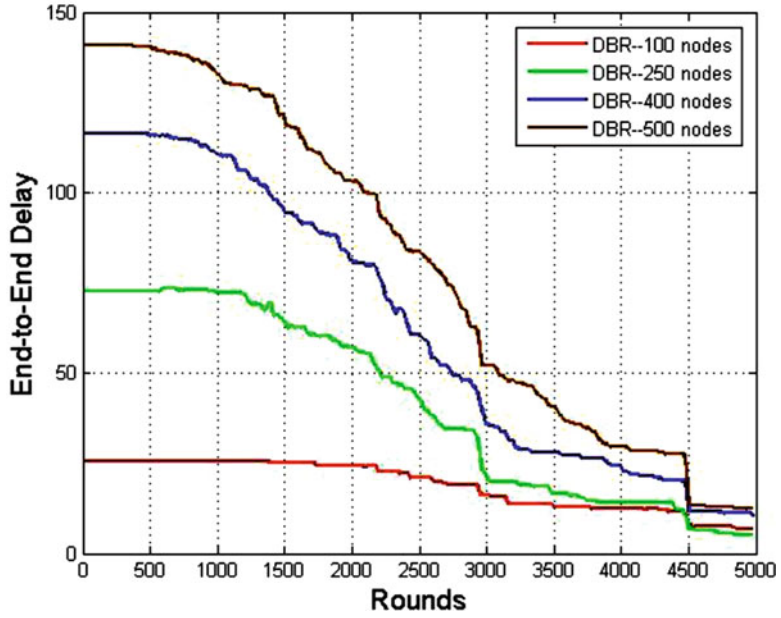


Fig. 16.5 End-to-end delay vs rounds

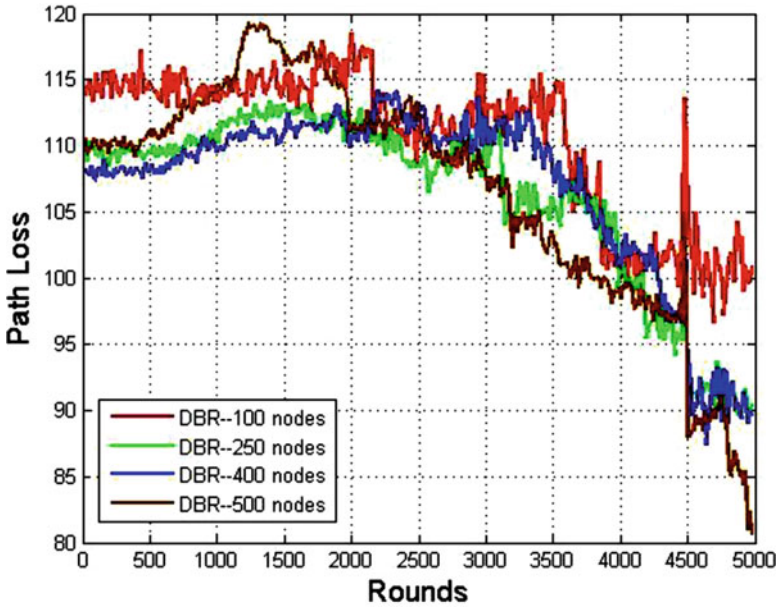


Fig. 16.6 Path loss vs rounds

16.6.3 Path Loss Analysis

The path loss analysis in terms of the scalability of the DBR scheme is shown in Fig. 16.6. As the number of nodes increased, the path loss decreased; by decreasing of the nodes, the loss increases. At round 5000, the path loss was 100 for 100 nodes; for 250, 400, and 500 nodes, this loss was 90, 88, and 79, respectively.

16.7 Scalability Analysis of EEDBR

In this section, we analyzed and discuss the scalability of EEDBR under different node densities during the stability period. The stability period is defined as the time period prior to the total energy drainage of the first node in the network. The following performance metrics for scalability were selected: throughput, end-to-end delay, and path loss.

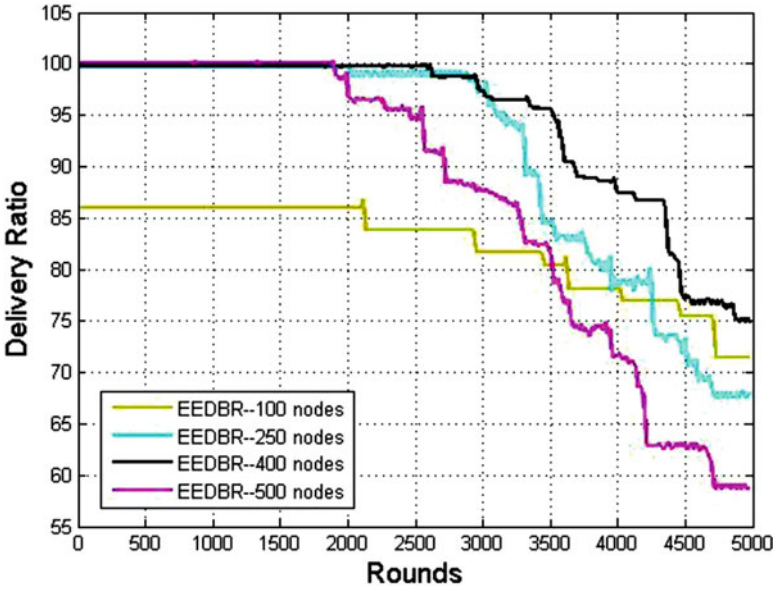


Fig. 16.7 Throughput scalability of EEDBR

16.7.1 Throughput Analysis

The throughput analysis in terms of the scalability of EEDBR is shown in Fig. 16.7. The delivery ratio remained constant until 2000 rounds, after which it decreased. With 400 nodes, the highest average throughput was obtained. With 100, 250, and 500 nodes, the average delivery ratios were 80, 88, and 82. Hence, 100 nodes had the lowest average throughput.

16.7.2 End-to-End Delay

The end-to-end delay analysis in terms of the scalability of the EEDBR technique is depicted in Fig. 16.8. The maximum delay was 80 in the case of 500 nodes at round 1000, whereas the minimum delay was 5 for 100 nodes at round 5000. Overall, the lowest delay from 1000 to 5000 rounds was for 100 nodes. With 500 nodes, the delay was higher at each round compared to the other node numbers.

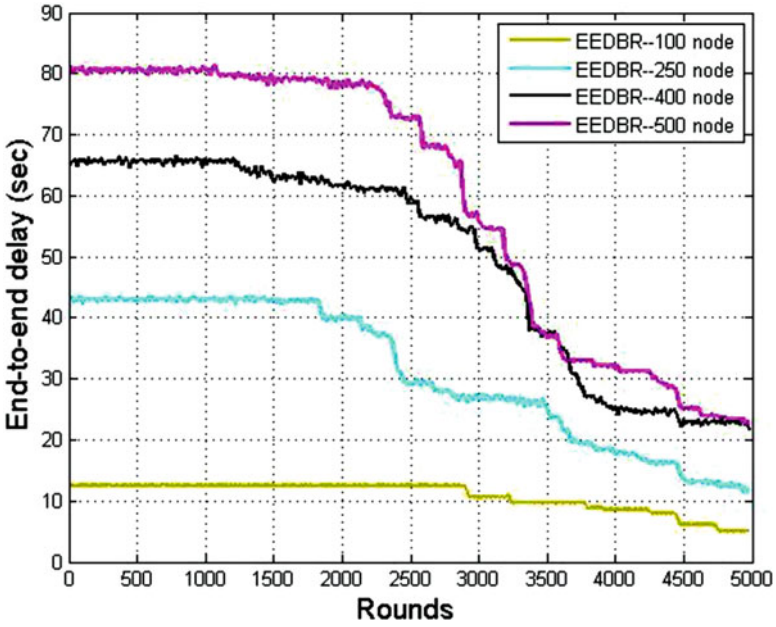


Fig. 16.8 End-to-end delay scalability of EEDBR

16.7.3 Path Loss Analysis

The path loss analysis in terms of the scalability of EEDBR is shown in Fig. 16.9. The highest average path loss was for 500 nodes. The highest path loss was at round 1000 for 100, 250, 400, and 500 nodes. The lowest path loss was at round 5000 for 100, 250, 400, and 500 nodes.

16.8 Summary of Work and Future Directions

In this chapter, we examined how to increase the stability period and throughput of UWASNs, as well as how to decrease delay. In mathematical work, we have also addressed the channel conditions and formulated three different cost functions. These cost functions were derived using the various layers of water depth. These cost functions are totally dependent on the path loss occurring in the dense underwater environment. In future, our focus will be on energy consumption and implementing energy-harvesting concepts.

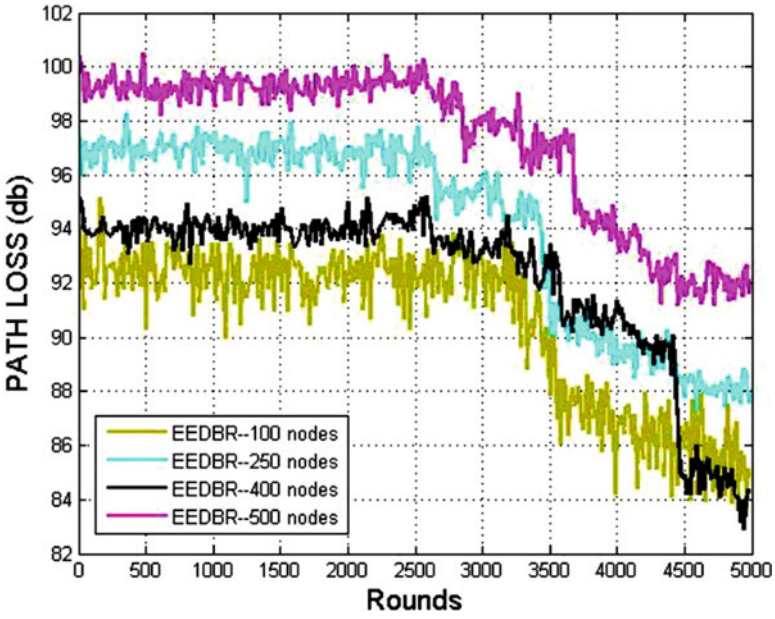


Fig. 16.9 Path loss scalability of EEDBR

References

1. Khan, F., Ur Rehman, A., Usman, M., Tan, Z., & Puthal, D. (2018). Performance of cognitive radio sensor networks using hybrid automatic repeat ReQuest: Stop-and-wait. *Mobile Networks and Applications, 23*(3), 1–10.
2. Javaid, N., Jafri, M. R., Khan, Z. A., Qasim, U., Alghamdi, T. A., & Ali, M. (2014). Iamctd: Improved adaptive mobility of courier nodes in threshold-optimized dbr protocol for underwater wireless sensor networks. *International Journal of Distributed Sensor Networks, 2014*, 1.
3. Noh, Y., Lee, U., Wang, P., Choi, B. S. C., & Gerla, M. (2013). VAPR: Void-aware pressure routing for underwater sensor networks. *IEEE Transactions on Mobile Computing, 12*(5), 895–908.
4. Ahmed, S., Javaid, N., Khan, F. A., Durrani, M. Y., Ali, A., Shaukat, A., Sandhu, M. M., Khan, Z. A., & Qasim, U. (2015). Co-UWSN: Cooperative energy-efficient protocol for underwater WSNs. *International Journal of Distributed Sensor Networks, 2015*, 75.
5. Javaid, N., Jafri, M. R., Ahmed, S., Jamil, M., Khan, Z. A., Qasim, U., & Al-Saleh, S. S. (2015). Delay-sensitive routing schemes for underwater acoustic sensor networks. *International Journal of Distributed Sensor Networks, 11*(3), 532676.
6. Zidi, C., Bouabdallah, F., & Boutaba, R. (2016). Routing design avoiding energy holes in underwater acoustic sensor networks. *Wireless Communications and Mobile Computing, 16*(14), 2035–2051.
7. Pompili, D., & Akyildiz, I. F. (2009). Overview of networking protocols for underwater wireless communications. *IEEE Communications Magazine, 47*(1), 97–102.
8. Liaqat, T., Javaid, N., Ali, S. M., Imran, M., & Alnuem, M. (2015). Depth-based energy-balanced hybrid routing protocol for underwater WSNs. In *2015 International Conference on Intelligent Networking and Collaborative Systems (INCOS)* (pp. 262–267). Piscataway, NJ: IEEE.

9. Yan, H., Shi, Z. J., & Cui, J.-H. (2008). DBR: Depth-based routing for underwater sensor networks. In *NETWORKING 2008 ad hoc and sensor networks, wireless networks, next generation internet* (pp. 72–86). Berlin: Springer.
10. Wahid, A., Lee, S., Jeong, H.-J., & Kim, D. (2011). Eedbr: Energy-efficient depth-based routing protocol for underwater wireless sensor networks. In *Advanced computer science and information technology* (pp. 223–234). Berlin: Springer.
11. Ahmed, S., Javaid, N., Ahmed, A., Ahmed, I., Durrani, M. Y., Ali, A., Haider, S. B., & Ilahi, M. (2016). SPARCO: Stochastic Performance Analysis with Reliability and COoperation for underwater wireless sensor networks. *Journal of Sensors, 2016*, 17.
12. Jafri, M. R., Ahmed, S., Javaid, N., Ahmad, Z., & Qureshi, R. J. (2013). Amctd: Adaptive mobility of courier nodes in threshold-optimized dbr protocol for underwater wireless sensor networks. In *2013 Eighth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA)* (pp. 93–99). Piscataway, NJ: IEEE.
13. Javaid, N., Hussain, S., Ahmad, A., Imran, M., Khan, A., & Guizani, M. (2017). Region based cooperative routing in underwater wireless sensor networks. *Journal of Network and Computer Applications, 92*, 31–41.
14. Ahmad, A., Ahmed, S., Imran, M., Alam, M., Niaz, I. A., & Javaid, N. (2017). On energy efficiency in underwater wireless sensor networks with cooperative routing. *Annals of Telecommunications, 72*(3–4), 173–188.
15. Ali, M. T., Rahim, S. S., Jan, M. A., Ishtiaq, A., Ahmed, S., Ahmad, M., Khan, M., & Ayub Khan, M. (2018). Dist-Coop: distributed cooperative transmission in UWSNs using optimization congestion control and opportunistic routing. *International Journal of Advanced Computer Science and Applications, 9*(6), 356–368.

Chapter 17
A Parametric Performance Evaluation of Batteries in Wireless Sensor Networks

Sana Yasin, Tariq Ali, Umar Draz, Ahmad Shaf, and Muhammad Ayaz

Abstract The use of wireless devices is increasing day by day. Most wireless devices are based on tiny sensors that gather information from their contiguous environment automatically without interacting with humans. The working of these tiny sensors basically depends upon batteries. In wireless devices, batteries play an essential role. Thus, there is a need to investigate the performance of batteries on the basis of various realistic parameters that directly or indirectly affect performance and evaluate the total lifetime of batteries. Wireless sensor networks (WSNs) are deployed in disaster areas such as military/battlefields, environmental monitoring, and intelligent building systems. They contain an extensive number of nodes that need to work normally for months to years to complete their assigned tasks. WSNs require considerable power for self-management. Due to the small size of sensor nodes, the power supply devoted to sensor nodes must be very restricted in size. Therefore, the power supply becomes a difficult issue in WSNs. Battery life is predicted under different duty cycle like low duty cycle, commissioning and packet streaming. In low duty cycle battery load is minimum due to the few number of tasks. In Commissioning mode battery perform average number of task and in packet streaming battery load is maximum due to large number of tasks. The end of this chapter presents a critical discussion of the issues.

17.1 Introduction

A wireless sensor network (WSN) consists of a varying number of sensor nodes that communicate with each other wirelessly. These nodes rely completely on batteries. Due to constant wireless communication and self scheduling of the nodes, drain

S. Yasin (✉) · T. Ali · U. Draz · A. Shaf
Computer Science Department, CIIT, Sahiwal, Pakistan

M. Ayaz
Sensor Networks and Cellular Systems (SNCS) Research Centre, University of Tabuk, Tabuk, Saudi Arabia

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_17

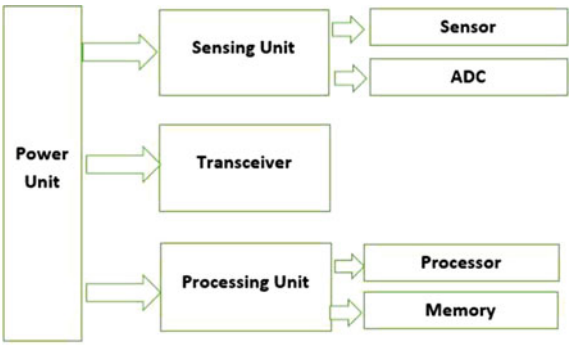


Fig. 17.1 Components of wireless sensor network

rate of the nodes is high. Thus, changing the battery is a very complicated task because these networks consist of thousands of nodes. Each node consists of certain basic elements like sensing data from the environment. Then the data are processed and sent or received by other nodes. All these tasks are performed correctly if the power supply attached to the network works well [1]. In WSNs, all nodes are self-scheduled, meaning they perform entire tasks required for the network on their own behalf means itself. There is no administration in these networks to regulate their management. Thus, for self-scheduling, these nodes consume a lot of battery power, which results in the early consumption of battery life, which forces users to come up with enhancements of battery life. Battery life is evaluated at different duty cycles to check that which mode of the battery consumes more energy. Battery life is not dependent on one or two factors; many factors influence battery life and damage it prematurely, which becomes a serious issue in WSNs [2]. Figure 17.1 presents the different components of WSNs.

Battery life is drained prematurely in WSNs for many reasons related to energy wastage. Some of them are described in [3, 4] and include, for example, retransmission, indolent snooping, packet overhead, and overhearing. Resolving these issues can save an important part of wireless networks with respect to the power issue. For example, in retransmission, when some data packets collide with each other than network do retransmission, which affects battery life and leads to energy wastage. This problem can be resolved by maintaining a distance between packets [5]. In indolent snooping, network nodes engage in idle listening and they try to receive information that is not consulted to that nodes. It increases packet overhead which becomes the cause of energy wastage. If a network sends a packet in an amount that a node can bear, then this problem can be reduced. In overhearing source node adds those nodes in their packet forwarding list that is irrelevant to that node. WSNs work in three types of duty cycles. All these cycles have a great impact on power conservation and affect battery life. In a low duty cycle, WSNs consume

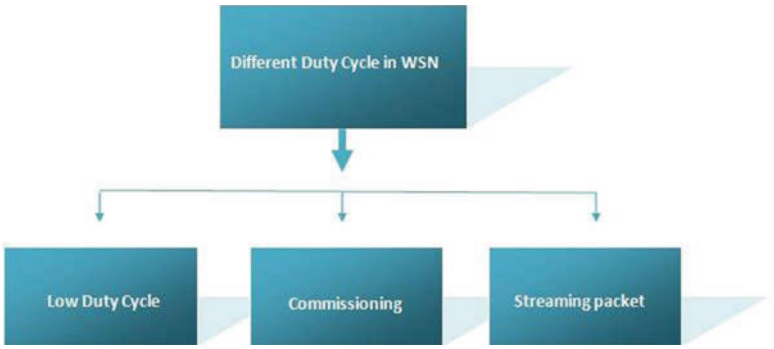


Fig. 17.2 Different duty cycles in WSNs

less power in commissioning and packet streaming. WSNs consume more power so battery life in low duty cycles is greater than in other cycles, and an inverse relationship exists between low duty cycles and battery life, as described in [6]. Figure 17.2 illustrates the different duty cycles in WSNs.

17.2 Related Work

Every duty cycle has an effect on battery life. A low duty cycle has less of an impact on battery life compared to commissioning and streaming modes because it consumes less power, and the battery is drained in very small amounts in this mode [7, 8]. If a WSN works all the time in the packet streaming cycle, then battery life will be measured in days, not years. In this chapter, the effect of different duty cycles is evaluated experimentally for rechargeable and nonrechargeable batteries. Rechargeable battery life cycle is measured against different modes in a graph of rechargeable batteries that shows that battery life is 97.2%. When a WSN is in low duty cycle mode, the remaining 2.8% is in commissioning and packet streaming modes. These results show that battery life will be low if it is in commissioning and packet streaming modes. Figure 17.3 shows the life of a rechargeable battery in different duty cycles.

The life of a nonrechargeable battery is calculated against different modes. Here is a graph of nonrechargeable batteries that shows that battery life is 37.5% when a WSN is in low duty cycle. On the other hand, the battery life is 25% when a WSN is in packet streaming mode. These results show that battery life will be maximized if WSN always operates in low duty cycle and commissioning mode and will be at its minimum if it always operates in packet streaming mode.

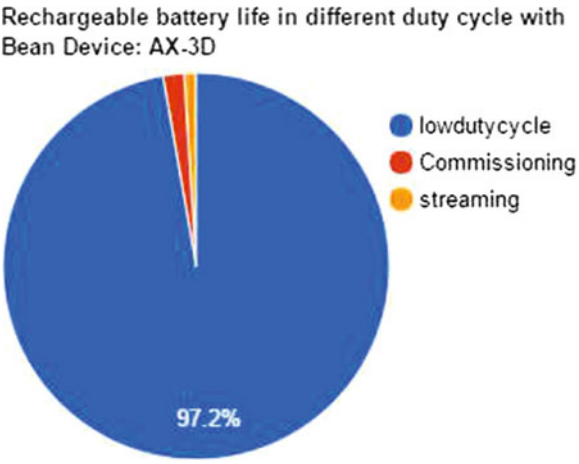


Fig. 17.3 Rechargeable battery life in different duty cycles

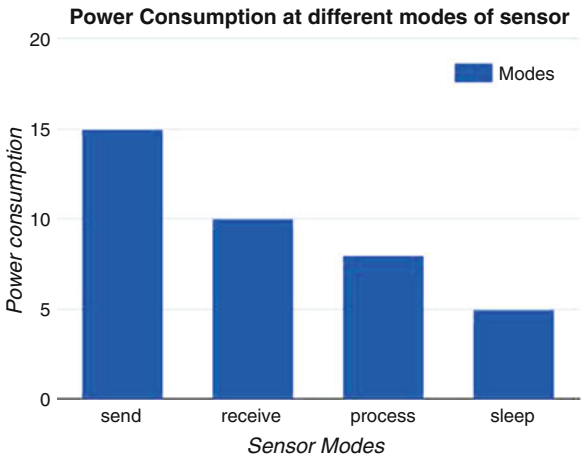


Fig. 17.4 Power consumption of sensors

17.2.1 Power Consumption in Different WSN Modes

WSNs consume different amounts of power in different modes. They consume the most power when sending and receiving modes and consume the least energy in sleep and idle modes. Figure 17.4 shows power consumption in different modes.

Power issues in WSNs are a very hot topic today. Much work has been done in this field, and more is expected. Different techniques have been proposed to resolve the issues in different ways. Some techniques focus on comparisons of different batteries and then choosing the best one that can be used in a self-scheduling network for a long time [9–11]. It is possible to use different models like physicals, empirical and abstract to compare battery life as mentioned in [12–14]. It tries to evaluate different rates of energy consumption that affects battery life and then proposes solutions to these problems. Some algorithms use fuzzy-

logic-based mechanisms, clustering, and different topological techniques to enhance system life, whereas others change the topological design of a network to enhance battery life. This involves linear programming to resolve the issue and incorporates graph-theory-based techniques [15]. Power consumption does not depend on just one factor; there are many reasons for energy wastage, such as network architecture, operating system, different protocols, and different microcontroller units. If we make them efficient to some extent, for example, if we use the best architecture, the best energy-conservation operating system, and energy-efficient protocols and microcontroller units, then the whole WSN can be made energy efficient, which will lead to decreased power wastage that causes the battery to be drained [16, 17]. A lot of work has been done on energy-harvesting techniques to obtain power from other factors like solar, temperature changes, and wind to enhance system life and make the system battery independent, because these can increase battery life through different techniques, but the battery still needs to be changed. Batteries are very limited resources in WSN and they get damaged with the passage of time due to performing self-scheduling in the networks [18–21]. This technique resolves the wireless network issue at some reasonable level.

17.3 Proposed Methodology

In this section, two categories of batteries are simulated, chargeable and non-rechargeable. Both are considered the best source of electricity in the form of a battery. Bean Air is the tool used for this simulation, which measures the effect of the duty cycle, and the XLP tool is used to measure the voltage. Both of these well-known tools are used as bean sensor devices. Table 17.1 presents the simulation parameters.

17.4 Results

The two performance parameters were evaluated using XLP and Bean Air as simulation tools. These simulation tools are mostly used in this type of experiment. Three types of duty cycle modes are used like commissioning, packet streaming,

Table 17.1 Simulation parameters

Category	Chargeable/rechargeable
Duty cycle	Three
Operation mode	RUNBUCK
Parameters	Time span, expected life
In use voltage	4 V
Output category	Year, month, days, and hours
Tool used	Bean Air and XLP

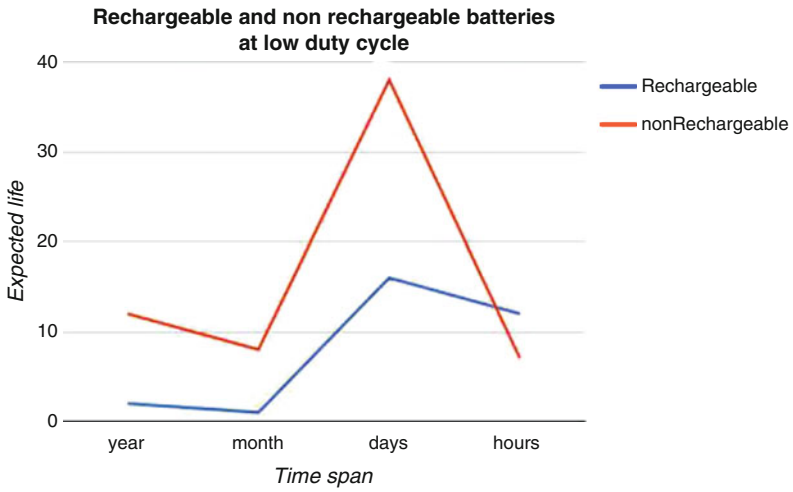


Fig. 17.5 Rechargeable and nonrechargeable batteries at low duty cycle

and low duty cycle. Before these duty cycles, the expected battery lifetime was calculated with respect to time span.

17.4.1 Effect of Duty Cycles on Battery Life

The experiments were conducted and the results calculated for rechargeable and nonrechargeable batteries at different duty cycles, and graphs were drawn against each duty cycle to show the battery predicted life against each duty cycle. There are three different types of graphs that evaluate the rechargeable and nonrechargeable battery behaviors in three WSN modes. Figure 17.5 shows that the predicted lifetime of rechargeable batteries is 2 years, 1 month, 16 days, and 12 h, and the predicted lifetime of nonrechargeable batteries is 12 years, 8 months, 38 days, and 7 h in low duty cycle. Figure 17.6 shows the rechargeable and nonrechargeable battery behavior in commissioning mode. Figure 17.6 also shows that rechargeable batteries have a lifetime of 14 h and nonrechargeable ones have a lifetime of 3 days and 16 h at commissioning. Figure 17.7 shows batteries' predicted life at packet streaming and present experimental proof that batteries have a very minimum life span in packet streaming because the WSN sends and receives packets. In this mode battery life is drained quickly.

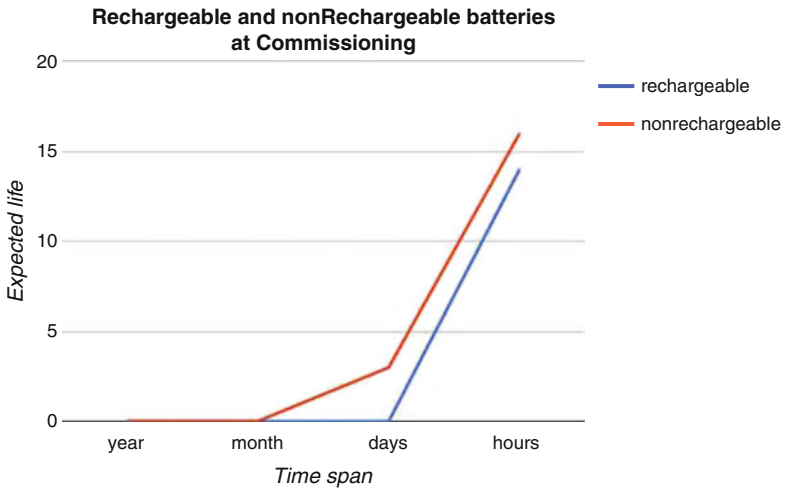


Fig. 17.6 Rechargeable and nonrechargeable batteries at commissioning

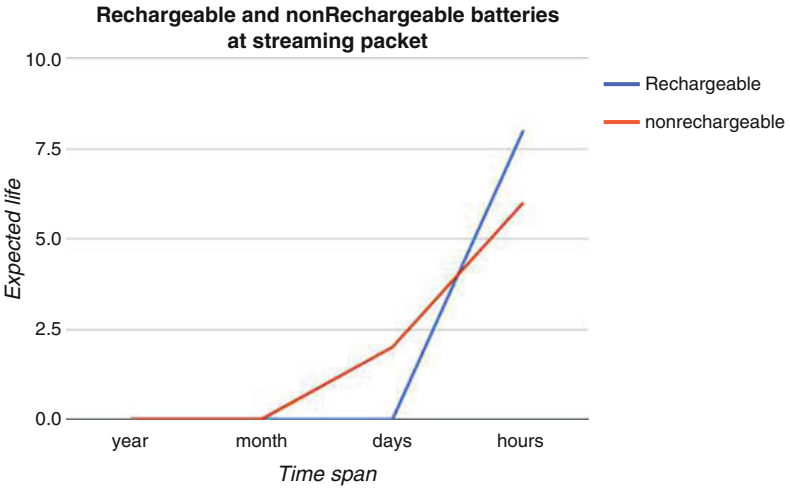


Fig. 17.7 Rechargeable and nonrechargeable batteries at packet streaming

17.4.2 Effect of Supplied Voltages on Battery Life

Supplied voltages have a strong impact on battery life. As the voltage increases, battery life also increases. Figure 17.8 shows the direct relationship between energy voltage and battery life. Figure 17.8 shows six different types of batteries – alkaline, nickel–cadmium (NICD), lithium–iron LiFes2, nickel–metal hydride (NiMH, zinc–air, lithium-ion – are examined and the effect of voltage is evaluated using two voltages, 1.8 and 3.3 V, against each battery when operation mode was RUNBUCK.

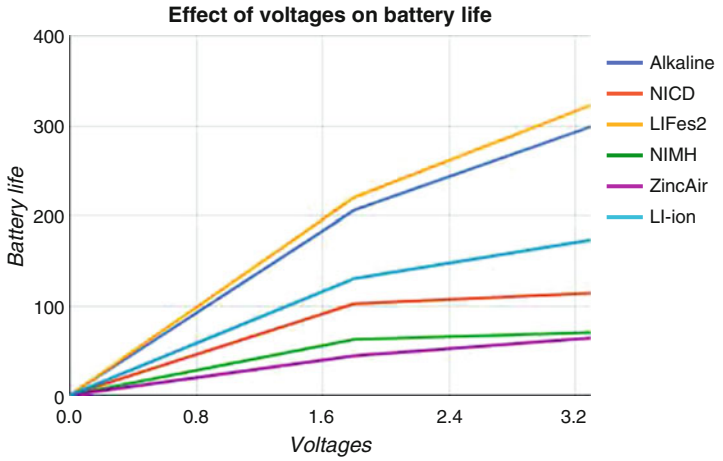


Fig. 17.8 Effect of voltage on battery life

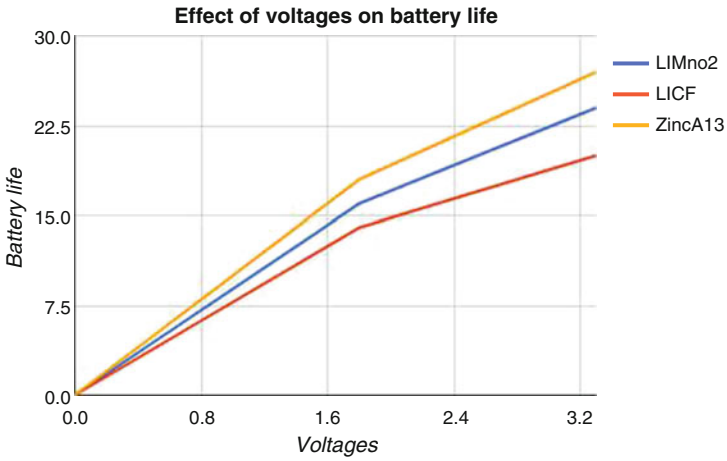


Fig. 17.9 Effect of voltage on battery life

Figure 17.8 shows the voltage effect on battery life; at 1.8 V the life of an alkaline battery would be 206 days. As the voltage is increased to 3.3 V, battery life increases to 299 days. At 1.8 V the battery life of NICD was 102 days, but at 3.3 V the life of the battery increased to 114 days. The LiFes2 battery life was 220 days at 1.8 V and increased to 323 at 3.3 V.

The NIMH battery has a life of 62 days at 1.8 V and 70 days at 3.3 V. Similarly, the zinc–air has a life of 44 days at 1.8 V and 64 days at 3.3 V. Thus, comparison of different batteries at different voltage levels experimentally proves that voltage affects battery life and that voltage is directly proportional to battery life. Figure 17.9 also shows the effect of voltage on the other three batteries and leads to the conclusion that as voltage varies, battery life increases with respect to voltage.

17.5 Conclusion

In this chapter, battery life is predicted on the basis of various factors that influence battery life. First, the life of rechargeable and nonrechargeable batteries is predicted experimentally at different duty cycles of a WSN. These duty cycles are low duty cycle, commissioning, and packet streaming. This chapter attempts to explore the notion that battery is drained rapidly in commissioning and packet streaming modes owing to high power consumption and the battery is less quickly drained in low duty cycle mode owing to less power consumption. The experimental results show that in low duty cycle, rechargeable battery life will increase with a security coefficient of 10%. In commissioning and packet streaming cycles, rechargeable battery life will increase with a security coefficient of 10%. Battery life is also predicted at different voltage levels, and it is experimentally proved that increasing the voltage leads to increased battery life as well. In future research will attempt to simulate battery performance with respect to other parameters.

References

1. Hong, S., Kim, D., & Kim, J.-E. (2005). Battery aware real time task scheduling in wireless sensor networks. In *11th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications, 2005. Proceedings*. Piscataway: IEEE.
2. Pantazis, N. A., & Vergados, D. D. (2007). A survey on power control issues in wireless sensor networks. *IEEE Communications Surveys and Tutorials, 9*(1–4), 86–107.
3. Mahlous, A. R., & Tounsi, M. (2016). Operation research based techniques in wireless sensors networks. *Communications and Network, 9*(1), 54.
4. Khan, F., ur Rehman, A., Usman, M., Tan, Z., & Puthal, D. (2018). Performance of cognitive radio sensor networks using hybrid automatic repeat ReQuest: Stop-and-wait. *Mobile Networks and Applications, 23*(3), 479–488.
5. Aakvaag, N., Mathiesen, M., & Thonet, G. (2005). Timing and power issues in wireless sensor networks-an industrial test case. In *International Conference Workshops on Parallel Processing, 2005. ICPP 2005 Workshops*. Piscataway: IEEE.
6. Barnes, M., Conway, C., Mathews, J., & Arvind, D. K. (2010). ENS: An energy harvesting wireless sensor network platform. *In 2010 Fifth International Conference on Systems and Networks Communications* (pp. 83–87). IEEE.
7. Roundy, S., Steingart, D., Frechette, L., Wright, P., & Rabaey, J. (2004). Power sources for wireless sensor networks. *In European Workshop on Wireless Sensor Networks* (pp. 1–17). Berlin: Springer.
8. Khan, F. (2014). Secure communication and routing architecture in wireless sensor networks. In *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)* (pp. 647–650). Piscataway: IEEE.
9. Gupta, S., & Roy, K. (2013). Comparison of different energy minimization techniques in wireless sensor network. *International Journal of Computer Applications, 75*(18).
10. Khattak, M. I., Edwards, R. M., Shafi, M., Ahmed, S., Shaikh, R., & Khan, F. (2018). Wet environmental conditions affecting narrow band on-body communication channel for WBANs. *Ad-Hoc and Sensor Wireless Networks, 40*, 297–312.
11. Silva, A., Liu, M., & Moghaddam, M. (2012). Power-management techniques for wireless sensor networks and similar low-power communication devices based on nonrechargeable batteries. *Journal of Computer Networks and Communications, 23*(3), 456–468.

12. Park, C., Lahiri, K., & Raghunathan, A. (2005). Battery discharge characteristics of wireless sensor nodes: An experimental analysis. *Power, 20*, 21.
13. Guo, W., Healy, W. M., & Zhou, M. C. (2012). Battery discharge characteristics of wireless sensors in building applications. In *2012 9th IEEE International Conference on Networking, Sensing, and Control (ICNSC)*. Piscataway: IEEE.
14. Jan, M. A., Khan, F., Alam, M., & Usman, M. (2017). A payload-based mutual authentication scheme for Internet of Things. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.08.035
15. Wenqi, G., & Healy, W. M. (2014). Power supply issues in battery reliant wireless sensor networks: A review. *International Journal of Intelligent Control and Systems, 19*(1), 15–23.
16. Shaikh, F. K., & Zeadally, S. (2016). Energy harvesting in wireless sensor networks: A comprehensive review. *Renewable and Sustainable Energy Reviews, 55*, 1041–1054.
17. Jan, M. A., Jan, S. R. U., Alam, M., Akhunzada, A., & Rahman, I. U. (2018). A comprehensive analysis of congestion control protocols in wireless sensor networks. *Mobile Networks and Applications 23*(3), 456–468.
18. Lattanzi, E., Freschi, V., Dromedari, M., Lorello, L. S., Peruzzini, R., & Bogliolo, A. (2017). A fast and accurate energy source emulator for wireless sensor networks. *EURASIP Journal on Embedded Systems, 2016*(1), 18.
19. Mahapatra, C., Sheng, Z., Kamalinejad, P., Leung, V. C. M., & Mirabbasi, S. (2017). Optimal power control in green wireless sensor networks with wireless energy harvesting, wake-up radio and transmission control. *IEEE Access, 5*, 501–518.
20. Deshmukh, R., Deshmukh, R., & Khokale, R. S. (2017). Techniques to improve network lifetime of wireless sensor networks-a survey. *International Journal of Advanced Research in Computer Science, 8*(3).
21. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2013). Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network. In *2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquseitous Computing (HPCC_EUC)* (pp. 1400–1407). Piscataway: IEEE.

Chapter 18
Machine Imagination: A Step Toward the Construction of Artistic World Through Storytelling

Syed Tanweer Shah Bukhari, Asma Kanwal, and Wajahat Mahmood Qazi

Abstract Development of conscious machines requires the implementation of artifacts that might enable an agent to formulate, represent, and regulate its actions and behaviors in a diverse environment. Regulation involves the rehearsal of all context-based possibilities considering emotional state and goals before execution of motor actions. It also means that an agent should be able to manipulate information that is not directly perceived through sensory stimuli. In order to incorporate these abilities, an agent is required to be constructed with cognitive memories, sensory system, sensory integration, emotion, drives, motivations, and action regulatory system. This study proposes a sub-architecture for QuBIC (cognitive architecture) to generate imaginations in QuBIC agents. The proposed architecture was implemented along with required computational constructs discussed in the paper. Furthermore, the paper presents the empirical analysis showing the potential of the proposed solution to construct imaginations in an agent. Experimental results illustrate how the aforementioned cognitive states participated in the process of machine imagination.

18.1 Introduction

Current progress in the field of machine intelligence and consciousness suggests that in the near future, machines will be requiring the characteristics to make predictions from current and already perceived information and construct imaginative thoughts in order to plan and act [1, 2]. Imagination is a manifestation of imaginary scenarios based on current and past experiences, consolidation of cognitive memories, and an ability to understand the point of views of others [3]. Various researchers have

S. T. S. Bukhari · W. M. Qazi (✉)
Intelligent Machines and Robotics, Department of Computer Science, COMSATS University Islamabad, Lahore Campus, Pakistan
e-mail: wmqazi@cuilahore.edu.pk

A. Kanwal
Department of Computer Science, Government College University, Lahore, Pakistan

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_18

discussed secretive nature of imagination in their own way [1, 4]. Kant explained imagination as a capability to simulate situations without having any physical experience [5]. In Gibson's view, it is the manipulation of mere experiences stored in the memory [6], whereas Shelley suggested that imagination is the formation of scenarios from known and unknown objects, relationships, and thoughts, i.e., the formation of *unicorn* from the experiences of horse and horn [7]. Several others emphasized on the view that it is an ability to formulate narrations, imaginary, estimation of possibilities, and phonological paths based on the experiences that are not directly perceived through sensors [3, 4, 8–10]. Studies suggested that there are other states that are responsible for the generation of imagination in the system to think and act consciously, i.e., sensory system, motivational system (goals and drives), behavioral system, cognitive memories, and emotions [11–15]. Indeed imaginations play a vital role in human cognition and consciousness. However, the question arises that, can they play a similar kind of role in machines with some kind of consciousness? In this regard, Aleksander discussed basic parameters required for the formulation of imaginative constructs in machines elsewhere [11]. Several systems have been built in the past based on some of these parameters, i.e., MAGNUS [16], CRONOS-ECCEROBOT [17], and LIDA [18]. The results obtained from these systems highlighted the need for imaginative constructs in machines. Therefore, this assumes that construction of imaginative artistic world through storytelling will help the agent to comprehend a bigger picture of the illustrated world. This may help the agent to have an experience without direct sensory input of the real world. Further advancement on this track will help in the study of Chalmer's easy and hard problem of consciousness [19]. Moreover it will also help in constructing a virtual environment for better decision making and planning (see Figs. 18.1 and 18.2).

The scope of this study is restricted to the concept of artificial imaginations in machines. This study proposes imaginative constructs in Quantum and Bio-inspired Intelligence and Consciousness (QuBIC) model which is computationally equivalent of the human brain/mind [20]. The artifacts reported here will address the issues of interaction-driven perceptual experiences, knowledge evolution in cognitive memories for the formulation of mental imagery in the coming sections.

18.2 Related Work

The pursuit of the computational equivalent of the human brain/mind raised questions about the requirements and conditions for machines carried out by the work of several researchers in the area of machine intelligence and consciousness.

Murphy, a robot having "three jointed planar arms" as an actuator and a video camera as sensor, presented for the conceptual framework of imagination by Mel [21]. Murphy worked in the workspace, where objects were scattered in randomized manner, while the video camera was placed to cover its environment [21, 22]. Murphy was designed to work in two ways: In the first mode, the robot was able

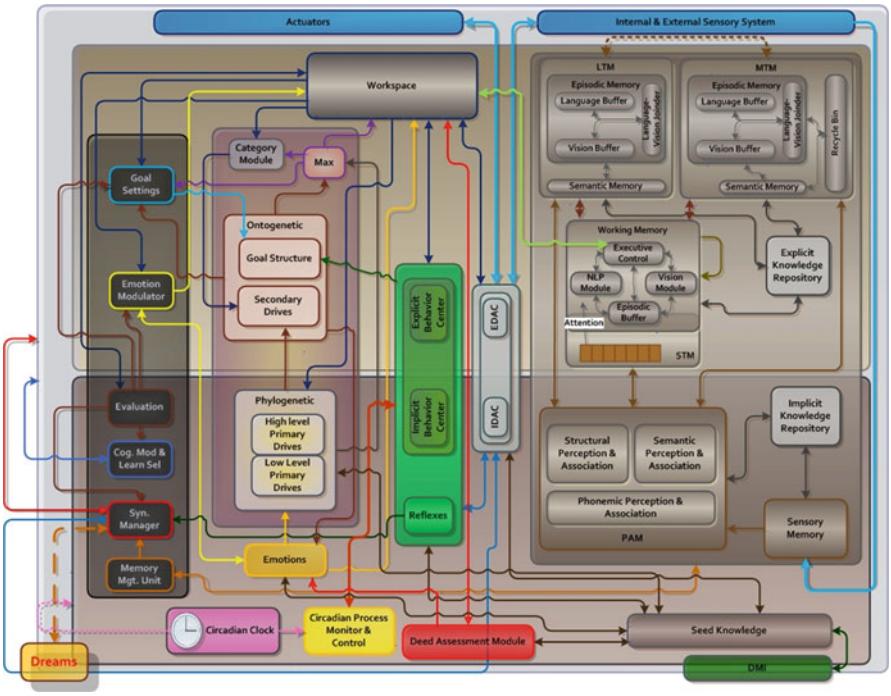


Fig. 18.1 Quantum and Bio inspired Intelligence and Consciousness (QuBIC) model

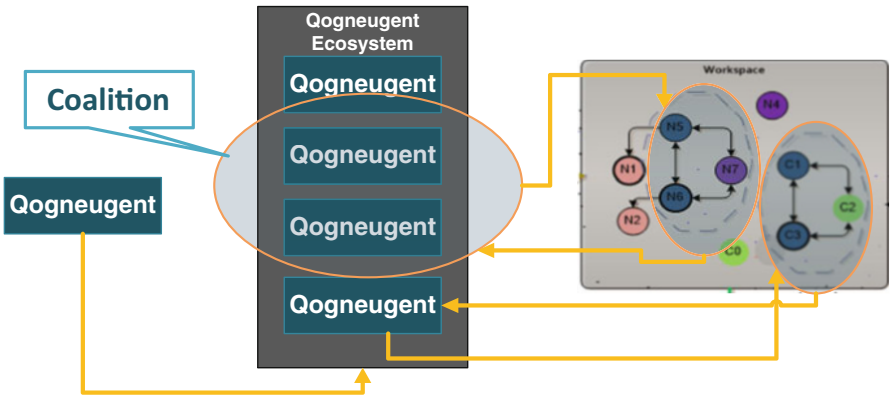


Fig. 18.2 Qogneugent—Codelets of QuBIC model

to establish associations between present image, motor control commands, and the following image to ensure collide-free grabbing of objects in an environment [21], whereas the second one is an offline mode, where the robotic arm and camera were disconnected to simulate the commands using association built in the first mode [22].

MetaToto is another robot having imagination in its weakest form introduced by Stein [23]. The main purpose of MetaToto was to navigate in immediately available surroundings, collect information regarding obstacles, and simulate it in its "cognition" for the exploration of the unknown environment [24]. MetaToto's architecture is mainly built on the work of Toto introduced by Matarić for cognitive tasks [24]. Rehearsals of tasks were controlled by its cognition (i.e., the virtual world), having the ability to work when no actuator and sensor is present. MetaToto's main purpose was to reduce the execution cost of Toto by stimulating its actions in the imagined world [23].

MAGNUS (Multi-Automaton General Neural Unit System), the system by Aleksander, could be considered as the pioneering work in artificial imagination [16]. MAGNUS is a software agent based on artificial neural network that aims to simulate the objects that were never experienced in the past [25]. The internal architecture consists of two mechanisms, one is liable for color (i.e., adjective) and the other one is for shape (i.e., noun). The "awareness area" of MAGNUS was responsible for the perceptual representations of its imagining. The associative learning was carried out by simultaneous interactions of various visual features (shape and color) [16, 25].

Ripley is a robot designed with the capability of executing verbal commands through its "compliant joint" arm [26]. The commands were usually based on the simple sentences for picking and imagining object(s) [27]. Ripley has seven degrees of freedom for the smooth execution of movements and gripping of small- and medium-sized objects [27]. The design of Ripley is distributed into three phases: understanding of scene in natural language through its auditory and visual sensors, acquisition of specific verbs to distinguish between question and information, and learning of moves using "compliant joints." The learned moves are then used in its three-dimensional virtual world for the simulation of actions for future use [28, 29]. Ripley was also capable of recognizing its copartner using Viola-Jones's face detection algorithm [30, 31].

CRONOS project was initiated by Holland for the development of human equivalent intelligence and consciousness in humanoid robot [32, 33]. In order to achieve its goals, the project began with the establishment of a musculoskeletal system to demonstrate biological realism [17, 33]. The system's learning mechanism is influenced by spike neural network [34]. For the simulation of actions performed by CRONOS (later ECCEROBOT), SIMNOS, a physics engine-based simulator, was used [34]. The execution and rehearsal of actions were controlled by a switch to support embodied imagination [35, 36]. Apart from a sophisticated design and motor control, CRONOS possess a minimalistic form of artificial imagination as per the criteria proposed elsewhere [11, 32, 37]. Marques identifies necessary conditions for artificial imaginations in machines [34]. The study shows that these conditions are not enough for the implementation of artificial imagination [18]. Cognitive theories and axioms proposed by Aleksander, Baars, and Franklin should be considered for humanlike imaginations in machines [11, 32, 37].

Learning Intelligent Distribution Agent (LIDA) is a cognitive architecture proposed by Franklin for the development of computational equivalent of the human

brain/mind [38]. LIDA includes several cognitive modules: cognitive memories, motor plan execution module, action selection, global workspace, and current situational model [39, 40]. The LIDA is further categorized into conceptual LIDA and LIDA framework. Conceptual LIDA has traces of imaginations discussed as deliberation [18, 41, 42], whereas its framework contains only the aspect of planning and previewing for the estimation of actions [18].

18.3 Cognitive Imagination Model (CIM)

Sensory input from the internal and external environment will pass to sensory memory for visual and auditory low-level feature extraction. These extracted features are transferred to PAM. PAM extracts features from coming signals in the form of object, encoding, recognition, categorization, and de-structuring. The PAM is further extended to recognize humans by detection and recognition of faces in the video stream. PAM is able to associate coming signals with past experiences by recalling memory objects from semantic and episodic memories. These attentively perceived objects transmit to WM. WM is responsible for performing face and blob detection by recollecting past experiences while imagining. WM is responsible for the formulation of scenes by reconstructing the fetched data from the episodic and semantic memory of LTM. The location and size of the object are retrieved from LTM and stored in spatial memory, whereas the object and its relevant episodes are fetched from the semantic and episodic memory of LTM, respectively, and stored in visual memory. These visual and spatial contents then pass to content generation module. Association between contents (memory objects) is built in content generation unit and further processed for evaluation in content selector unit. The evaluation takes place on the basis of goals and emotional state of the agent according to changes in the environment. Imagination is formulated based on selected content in imagination builder. Imagination formation module is responsible for the generation of imaginative scene, and this imagination depends on the strength of the emotional state. Sometimes previously designed goals are so strong that it minimizes the influence of emotions on the imaginative scene. This imaginative scene is transmitted toward WM. If any episode of episodic memory does not match with the imaginative scene, then this newly generated episode will store in LTM for future use. WM also pass this imaginative scene to action selection module. This module will select the appropriate action to express this imaginative scene. This selected action is stored in sensory-motor memory for assigning this action to the suitable actuator to generate output toward the environment (see Fig. 18.3).

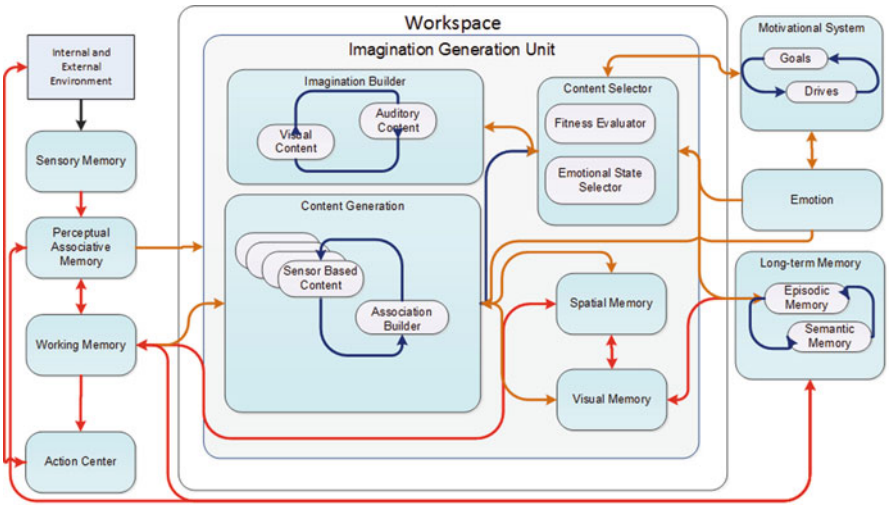


Fig. 18.3 Cognitive Imagination Model

Table 18.1 Scene generation results

No. of rounds	Object retrieval			Object placement			Scene generations
	Correct	Total	Accuracy	Correct	Total	Accuracy	
1	40	80	0.50	30	70	0.43	35
2	50	90	0.56	45	80	0.56	40
3	65	100	0.65	55	95	0.58	45
4	70	110	0.64	65	110	0.59	52
5	90	120	0.75	80	120	0.67	60

18.4 Results

Cognitive Imagination Model (CIM) is designed to differentiate between sensory information coming from external environment and sensation generated within the system. For the verification of CIM, Artificial Imagination Agent (AIA) is being developed. The implementation of AIA is based on the limited construction of imaginative scenarios using story lines. In this regard, AIA has been trained with over 150 objects. Later these objects were used in the story lines given to AIA. Table 18.1 represents the results of object retrieval, object placement, and scene generations during storytelling process. Each round contained at least 25–30 sentences for imagination. The generation was repeated for the rest of rounds. Results of first round indicate the initial recall of the memory, where retrieval and placement of objects were premature. Therefore, same story lines were given in round two to four to analyze the process of storytelling and its consequences. With the continuous recall, AIA improved its scene generation, and results can be seen in Table 18.1.

Fig. 18.4 Scene generations by AIA

Furthermore, sensory system of AIA is based on EMGU CV[1] and Microsoft Speech SDK. Additionally natural language processing techniques were used for parsing the text/speech to extract the meanings of phrases. Scenes were annotated for training the system using "is," "has," "can," and "place" tags. For example Ali is human, can walk, can talk, has two legs, and has two eyes. Parsed knowledge was stored in long-term knowledge repository implemented in Microsoft SQL Server 2012. For the initial experiment, simple sentences were used for training and testing. Simple sentences contain subject, verb, prepositions, and objects. Few of the results are shared below (see Fig. 18.4).

AIA has been given story lines to imagine, i.e., *Bird is flying in the sky*. AIA parsed story lines into noun, verb, adjective, and prepositions to build the associations between objects. Later these associations were used to construct the scenarios. The AIA is initially equipped with natural language processing toolkit (i.e., OpenNLP[2]) for the understanding of simple sentences as story lines: The results shown in Fig. 18.4 are its initial generations. The results are quite promising to further dig out the area of machine imagination. The ideas present here are still in fancy and should be seen in that context.

[1] http://www.emgu.com.

[2] https://opennlp.apache.org/.

18.5 Conclusion

This study proposes a computational model for inducing mechanism for imaginations in QuBIC-based agents. Imaginative constructs are modeled on the basis of simple sentences. For better understanding, verbal and nonverbal semantics are planned for the next phase of AIA. The work is currently in progress, and only initial results of AIA are presented in this paper. The next version of AIA will be able to understand complex and compound sentences. The study presented could be helpful for memory consolidations, planning, and prediction in future machines.

References

1. Karwowski, M., Jankowska, D. M., & Szwajkowski, W. (2016). Creativity, imagination, and early mathematics education. In R. Leikin & B. Sriraman (Eds.), *Creativity and Giftedness* (pp. 7–22). Berlin: Springer.
2. Moreton, J., Callan, M. J., & Hughes, G. (2017). How much does emotional valence of action outcomes affect temporal binding? *Consciousness and Cognition, 49*, 25–34.
3. Hunter, M. (2013). Imagination may be more important than knowledge: The eight types of imagination we use. *Review of Contemporary Philosophy, 12*, 113–120.
4. Shanahan, A. (2005). Consciousness, emotion, and imagination: A brain-inspired architecture for cognitive robotics. In *Proceedings AISB 2005 Symposium on Next Generation Approaches to Machine Consciousness*.
5. Kneller, J. (2007). *Kant and the power of imagination* (1st ed.). Cambridge: Cambridge University Press.
6. Gibson, J. J. (1986). *The ecological approach to visual perception*. Mahwah, NJ: Lawrence Erlbaum Associates.
7. Goslee, N. M. (2014). *Shelley's visual imagination*. Cambridge: Cambridge University Press.
8. Wittgenstein, L. (2001). *Philosophical investigations*. Hoboken, NJ: Wiley.
9. Taylor, M. (2011). *Encyclopedia of creativity—imagination* (S. P. Mark Runco, Ed.). New York: Elsevier Inc.
10. Faghihi, U., McCall, R., & Franklin, S. (2012). A computational model of attentional learning in a cognitive agent. *Biologically Inspired Cognitive Architectures, 2*, 25–36.
11. Aleksander, I., & Dunmall, B. (2003). Axioms and tests for the presence of minimal consciousness in agents. *Journal of Consciousness Studies, 10*, 7–18.
12. Haikonen, P. O. (2003). *The Cognitive Approach to Conscious Machines*. Exeter: Imprint Academic.
13. Haikonen, P. O. (2005). You only live twice: Imagination in conscious machines. In *Symposium on Next Generation approaches to Machine Consciousness: Imagination, Development, Intersubjectivity, and Embodiment*.
14. Aleksander, I., & Morton, H. (2007). Why axiomatic models of being conscious? *Journal of Consciousness Studies, 14*(7), 15–27.
15. Michel, M. (2017). A role for the anterior insular cortex in the global neuronal workspace model of consciousness. *Consciousness and Cognition, 49*, 333–346.
16. Aleksander, I. (2001). *How to build a mind: Towards machines with imagination*. New York: Columbia University Press.
17. Marques, H. G., Holland, O., & Newcombe, R. (2008). A modelling framework for functional imagination. In *AISB Convention of Computing & Philosophy*.
18. Madl, T., Franklin, S., Chena, K., Montaldid, D., & Trappl, R. (2016). Towards real-world capable spatial memory in the LIDA cognitive architecture. *Biologically Inspired Cognitive Architectures, 16*, 87–104.

19. Chalmers, D. J. (1995). The puzzle of conscious experience. *Scientific American, 273*, 80–86.
20. Qazi, W. M. (2011). *Modeling cognitive cybernetics from unified theory of mind using quantum neuro-computing for machine consciousness*.Punjab, Pakistan: National College of Business Administration and Economics.
21. Mel, B. (1986). A connectionist learning model for 3-d mental rotation, zoom, an pan. In *Proceedings of Eighth Annual Conference of the Cognitive Science Society*.
22. Mel, B. (1988). Murphy: A robot that learns by doing. In *Neural information processing systems*. New York: American Institute of Physics.
23. Stein, L. A. (1995). Imagination and situated cognition. In *Android epistemology* (pp. 167–182). Cambridge, MA: MIT Artificial Intelligence Lab.
24. Matarić, M. J. (1990). *A distributed model for mobile robot environment-learning and navigation* (MIT AI Lab Tech Report AITR-1228).
25. Aleksander, I., Evans, R. G., & Sales, N. (1995). Towards intentional neural systems: Experiments with MAGNUS. In *Fourth International Conference on Artificial Neural Networks*, Cambridge, UK.
26. Hsiao, K.-Y., Mavridis, N., & Roy, D. (2003). Coupling perception and simulation: Steps towards conversational robotics. In *IEEE/RSJ International Conference on Intelligent Robots and Systems 2003*.
27. Roy, D., Hsiao, K.-Y., & Mavridis, N. (2003). Conversational robots: Building blocks for grounding word meanings. In *Workshop on Learning Word Meaning from Non-Linguistic Data*.
28. Roy, D., Hsiao, K.-Y., Mavridis, N., & Gorniak, P. (2003). Ripley, hand me the cup: Sensorimotor representations for grounding word meaning. In *International Conference of Automatic Speech Recognition and Understanding*.
29. Mavridis, N., & Roy, D. (2006). Grounded situation models for robots: Where words and percepts meet. In *IEEE/RSJ International Conference on Intelligent Robots and Systems*
30. Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. In *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*.
31. Roy, D., Hsiao, K.-Y., & Mavridis, N. (2004). Mental imagery for a conversational robot. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 34*(3), 1374–1383.
32. Gamez, D. (2008). *The development and analysis of conscious machines*. Colchester: University of Essex.
33. Gamez, D. (2008). Progress in machine consciousness. *Consciousness and Cognition, 17*, 887–910.
34. Marques, H. G. (2009). *Architectures for embodied imagination*. Colchester: University of Essex.
35. Potkonjak, V., Svetozarevic, B., Jovanovic, K., & Holland, O. (2012). The puller-follower control of compliant and noncompliant antagonistic tendon drives in robotic systems. *International Journal of Advanced Robotic Systems, 8*(5), 143–155.
36. Jovanovic, K., Potkonjak, V., & Holland, O. (2014). Dynamic modeling of an anthropomimetic robot in contact tasks. *Advanced Robotics, 28*(11), 793–806.
37. Baars, B. J. (1997). In the theatre of consciousness: Global workspace theory, a rigorous scientific theory of consciousness. *Journal of Consciousness Studies, 4*(4), 292–309.
38. Franklin, S., Madl, T., D'Mello, S., & Snaider, J. (2013). LIDA: A systems-level architecture for cognition, emotion, and learning. *Autonomous Mental Development, IEEE Transactions, 6*(1), 19–41.
39. Franklin, S., Madl, T., Chen, K., & Trappl, R. (2013). Spatial working memory in the LIDA cognitive architecture. In *International Conference on Cognitive Modeling*, Ottawa, Canada.
40. Franklin, S. (1997). *Artificial minds*. Cambridge, MA: MIT Press.
41. Franklin, S., Madl, T., Strain, S., Faghihi, U., Dong, D., Kugele, S., et al. (2016). A LIDA cognitive model tutorial. *Biologically Inspired Cognitive Architectures, 16*, 105–130.
42. Paraense, A. L., Raizer, K., Paula, S. M., Rohmer, E., & Gudwin, R. R. (2016). The cognitive systems toolkit and the CST reference cognitive architecture. *Biologically Inspired Cognitive Architectures, 17*, 32–48.

Chapter 19
Geospatial Division Based Geographic Routing for Interference Avoidance in Underwater WSNs

Farwa Ahmed, Nadeem Javaid, Zahid Wadud, Arshad Sher, and Sheeraz Ahmed

Abstract In underwater wireless sensor networks (UWSNs), geographic routing paradigm seems promising choice for data transmission in severely limited acoustic communication channel conditions. The main challenge of geographic routing in sparse network conditions is communication void. In this context, we propose geospatial division based geo-opportunistic routing scheme for interference avoidance (GDGOR-IA) focusing on interference in the network. The scheme is twofold, selection of target cube and selection of optimal next hop forwarder node in the target cube.

19.1 Introduction

Underwater wireless sensor networks (UWSNs) have emerged as a promising technology for various application domains. UWSNs have gained considerable attention of research and industrial communities due to their wide application horizons, e.g., monitoring of marine life, pollutants in underwater environment and climate; to collect oceanographic data, assisted navigation, disaster prevention, and many others [1].

F. Ahmed · N. Javaid (✉) · A. Sher
COMSATS Institute of Information Technology, Islamabad, Pakistan
www.njavaid.com

Z. Wadud
University of Engineering & Technology, Peshawar, Pakistan

Capital University of Science and Technology, Islamabad, Pakistan

S. Ahmed
Career Dynamics Research Center, Peshawar, Pakistan

Iqra National University, Peshawar, Pakistan

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_19

The aforementioned constraints of acoustic communication restrict performance of conventional routing schemes. Considering this, geographic routing seems a definitive solution to design the routing protocol for UWSNs. Geographic routing with the aid of position/location information is a scalable and simple routing methodology [2]. Following the greedy forwarding approach at each hop, an optimal next hop forwarder node is selected that is closer to the destination. It continues until packet reaches destination in hop by hop manner [3].

More precisely, the significance of proposed work lies in the following contributions (1) geospatial logical division of network field in which whole network is divided into cubes. Method of forwarding is hop by hop aiming to choose shortest trail towards destination; (2) we introduce interference avoidance mechanism to reduce collision probability.

19.2 Related Work

Some of the reviewed related work are presented in this section.

In DBR, nodes greedily forward data packets to the upper nodes. If it does not find next hop forwarder node due to coverage hole or energy hole, packet drop occurs that affects packet delivery [4]. In [5], another variation of DBR is presented that formulates holding time calculations to reduce latency in the network. This protocol is intended to reduce end to end delay for delay sensitive applications. H2-DAB routing protocol in [6] uses two part information: node ID and hop ID for routing the data packet. This protocol is energy efficient because it does not store complex routing information in routing tables.

In RDBF, an efficient route search towards destination is performed using location information. For finding suitable node for forwarding process, a fitness function is defined based on distance with respect to sink [7]. The RMTG geocast routing protocol relies on multiple piece of information, such as location information of nodes and their neighbors, route discovery for selection of node closest to the destination, and route maintenance. This protocol has addressed problems like void hole and link breakage problems. A multicast shortest path is formed for packet transmission within the intended geographic region [8].

In ARP, data packets are assigned different delivery priorities that depend on application requirement. It uses location information and it is an energy efficient protocol; however, it incurs high communication overhead [9]. To avoid horizontal communication between same depth sensor nodes, DVPR opts triangular inequality theorem. According to that, same depth nodes are avoided using coordinate information of participating nodes in communication. However, accurate position information is a challenging task itself [10].

19.3 System Model

The network field is divided into cubes considering the communication range carefully. In the network architecture, a set of sensor nodes is deployed at different depths and sonobuoys known as sink nodes are deployed at the surface of the water. Our model consists of a set of sensor nodes with a communication range of R_c, so that $N_n = \{N_1, N_2, N_3, \ldots N_n\}$ represents the set of sensor nodes, and N_s is the set of sonobuoys. The sensor nodes N_n are randomly deployed in a geographic area of interest that is three dimensional (Fig. 19.1).

Potential neighbor set selection follows these steps: $n_k(t)$ be the source node having $N_k(t)$ and $S_k(t)$, its neighbor set, and its sonobuoy set at any time instant t. Packet advancement parameter (ADV) is used to determine the potential neighbor set for a source node. For the node n_k, the potential neighbor set $N_{set}(k)$ includes the neighbor nodes having the Euclidean distance with their respective nearby sinks less than the distance between n_k with its nearest sonobuoy s_n^* as mentioned in Eq. (19.1).

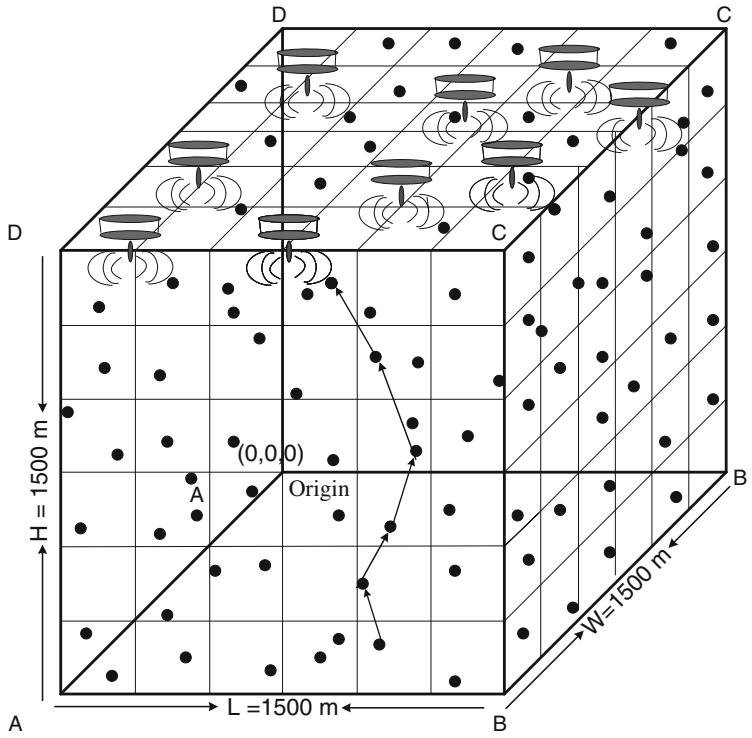


Fig. 19.1 Network architecture

$$F_{set}(k) = n_i \epsilon N_k(t) : \exists S_n \epsilon S_s(t) | D(n_i, s_{n^*}) - D(n_k, s_n) > 0 \tag{19.1}$$

19.4 GDGOR-IA

In this section, we have introduced the proposed scheme GDGOR-IA in detail. **Target cube selection** in GDGOR-IA works in two phases: at first, selection of target cube has been performed. For that purpose, a source node laying in the source cube (SC) acquires its coordinates and source cube ID. A set of neighbor cubes (NCs) of SC calculates Euclidean distance with respect to their nearby sonobuoys. NC with smallest Euclidean distance is selected as target cube (TC) for SC.

We intend to select NC with less number of nodes but within a threshold set after considering link quality in Eq. (19.2). This shows the error probability P_{BER} and collision rate probability P_{CR} when L is the size of forwarded packet. Furthermore, within the TC, selection of next hop forwarder set is based on advancement towards destination (ADVD). ADVD is calculated for the set of nodes $N_k = \{N_1, N_2, N_3, \ldots\}$ in the TC. Node with highest NADVD is selected as highest priority node and rest of the all are listed in the set according to their priority.

$$\alpha = 1/P_{CR} \times (1 - P_{BER})^L \tag{19.2}$$

$ADVD(n_i)$ is the advancement of n_i, neighbor node of source node n_k towards its closest sonobuoy as in Eq. (19.3). For any node n_i belonging to the potential neighbor set $F_{set}(k)$, normalized advancement towards destination is calculated in Eq. (19.4).

$$ADVD(n_i) = D(n_k, s_n^*) - D(n_i, s_i^*) \tag{19.3}$$

$$NADVD(n_i) = ADVD(n_i) \times P(d_k^i, m) \tag{19.4}$$

Towards the next step, neighbor nodes of source node n_a laying in target cube are put aside in another set named as $PF_{set}(n_a)$. We compare the accumulated NADVD of set of neighbor nodes and the node number in the set $PF_{\text{set}}(n_a)$. Selected set has less number of nodes within the α threshold and higher accumulated NADVD.

19.5 Simulation Analysis

In our simulations, the number of sensor nodes ranges from 150 to 450 and the number of sonobuoys is 45. They are randomly deployed in a region at the size of $1500 \times 1500 \times 1500$ m. In all experiments, the nodes have a transmission range R_c of 250 m and a data rate of 50 kbps. We consider that data packets have a payload of

Algorithm 1 Phase II: selection of next-hop forwarder

1: Procedure: select next-hop forwarder
2: **for** $n_b \in F_{set}(a)$
3: Select nodes residing in TC from $F_{set}(a)$
4: **end for**
5: Put selected nodes in potential forwarder set $PF_{set}(a)$
6: $PF_{set}(a) \leq F_{set}(a)$
7: **if** $PF_{set}(a) = \{\}$
8: **else**
9: Calculate NADVD for $PF_{set}(a)$ according to Equation (4).
10: Order all the nodes in $PF_{set}(a)$ according to their NADVD
11: Select node with highest NADVD as next hop forwarder
12: **end if**

150 bytes. Values of energy consumption associated with transmission, reception, idle state, and depth adjustment are $P_t = 2\,\text{W}$, $P_r = 0.1\,\text{W}$, $P_i = 10\,\text{mW}$,and $E_m = 1500\,\text{mJ/m}$, respectively.

19.5.1 Discussion

At low network density, distance between void nodes is high. Figure 19.2 depicts the average displacement of void nodes of GDGOR-IA and GEDAR. It can be seen that at node number 200, 15% nodes are laying in communication void region. As node number in network filed increases, displacement of void nodes decreases,

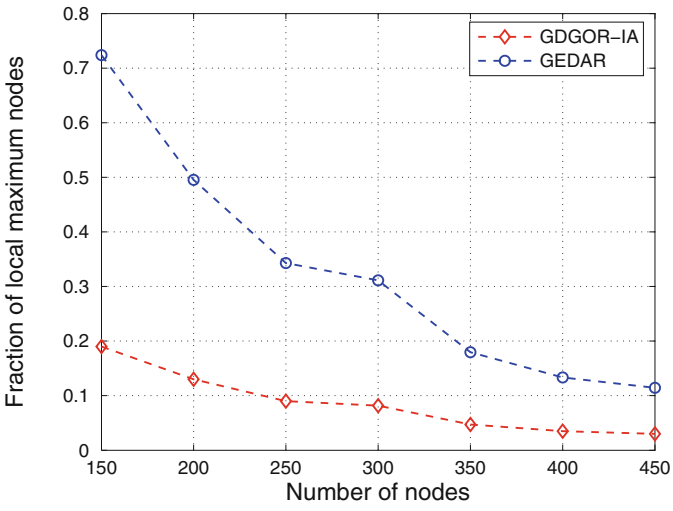


Fig. 19.2 Fraction of void nodes

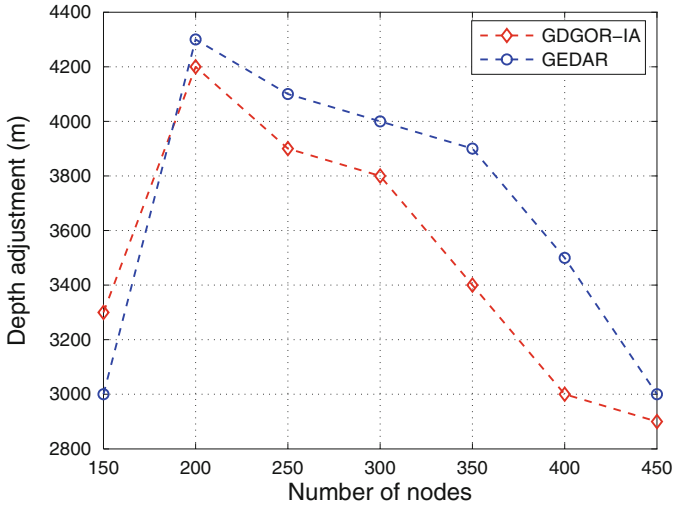


Fig. 19.3 Depth adjustment

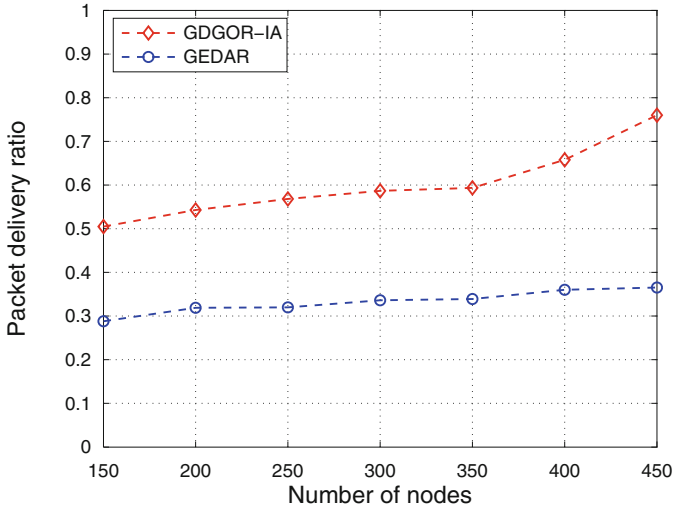


Fig. 19.4 PDR analysis

respectively. This is due to the fact that increases in node number decrease the fraction of void holes as shown in Fig. 19.3.

The PDR of both the schemes follows the same trend. It increases with the increase in network density as depicted in Fig. 19.4. Although, all the three schemes have opted void node recovery mechanism but cost associated with them is different.

In GDGOR-IA, energy consumption is mainly due to depth adjustment for recovery purpose. In the beginning, fraction of void node is high in sparse network

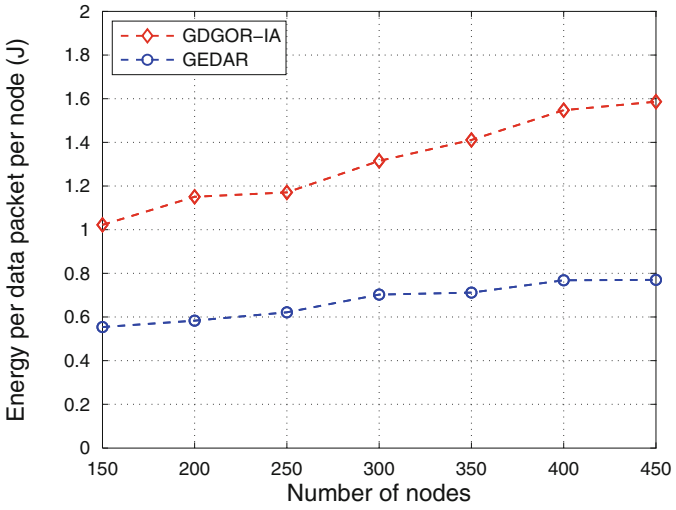


Fig. 19.5 Energy consumption analysis

density as shown in Fig. 19.5. Hence, more energy consumption occurs due to large displacement of nodes on average to recover communication voids. With an increment in node number, energy tax results concerning the GEDAR declines and that is because of reduced displacement between nodes. Above 250 node number, effect of interference avoidance mechanism opted by GDGOR-IA is more prominent. At high density network regions, chances of collisions increase and packet loss occurs. Interference avoidance mechanism reduces packet loss due to selection of optimal node with less neighbors around, thus, probability of interference among nodes reduces significantly and energy consumption gets better in dense network regions.

19.6 Conclusion

In this paper, collaborative data transmission opting 3D geospatial division is evaluated. Three dimensional division has made network scalable and forwarding is directional because of selection of upward neighbor cubes of sender cube. Moreover, interference avoidance helps in reduction of packet loss, thus it improves packet delivery. Communication void node recovery mechanism significantly improves network performance, anyhow energy consumption increases due to depth adjustment.

References

1. Akyildiz, I. F., Pompili, D., & Melodia, T. (2005). Underwater acoustic sensor networks: Research challenges. *Ad Hoc Network, 3*(3), 257–279.
2. Hong, X., Xu, K., & Gerla, M. (2002). Scalable routing protocols for mobile ad hoc networks. *IEEE Network, 16*(4), 11–21.
3. Souiki, S., Feham, M., Feham, M., & Labraoui, N. (2014). Geographic routing protocols for underwater wireless sensor networks: A survey. *International Journal of Wireless & Mobile Networks, 6*(1), 69–87.
4. Hai, Y., Jerry Shi, Z., & Cui, J.-H. (2008). DBR: Depth-based routing for underwater sensor networks. In *International Conference on Research in Networking* (pp. 72–86). Berlin: Springer.
5. Jafri, M. R., Muhammad M. S., Kamran L., Zahoor A. K., Ansar Ul H. Y., & Nadeem J. (2014). Towards delay-sensitive routing in underwater wireless sensor networks. *Precedia Computer Science, 37*, 228–235.
6. Ayaz, M., Azween A., Ibrahima F., & Yasir B. (2012). An efficient dynamic addressing based routing protocol for underwater wireless sensor networks. *Computer Communications, 35*(4), 475–486.
7. Li, Z., Nianmin, Y., & Qin, G. (2014). Relative distance based forwarding protocol for underwater wireless networks. *International Journal of Distributed Sensor Networks, 10*(2), 173089.
8. Dhurandher, S. K., Mohammad S. O., & Megha G. (2010). A novel geocast technique with hole detection in underwater sensor networks. In *Computer Systems and Applications (AICCSA), 2010 IEEE/ACS International Conference on IEEE, 2010*, pp. 1–8.
9. Guo, Z., Gioele, C., Bing, W., Jun-Hong, C., Dario, M., & Gian, P. R. (2008). Adaptive routing in underwater delay/disruption tolerant sensor networks. In *Wireless on Demand Network Systems and Services*, 31–39
10. Ali, T., Low, T. J., & Ibrahim, F. (2014). Diagonal and vertical routing protocol for underwater wireless sensor network. *Procedia-Social and Behavioral Sciences, 129*, 372–379.

Chapter 20
DEAR-2: An Energy-Aware Routing Protocol with Guaranteed Delivery in Wireless Ad-hoc Networks

Muhammad Umair Hassan, Muhammad Shahzaib, Kamran Shaukat, Syed Nakhshab Hussain, Muhammad Mubashir, Saad Karim, and Muhammad Ahmad Shabir

Abstract Nodes can connect with each other to form a self-organizing, infrastructure-less, wireless ad-hoc network, in which every node performs the actions of both host and router. The demand for wireless ad-hoc networks is growing because of their simple and quick installation. However, the limited power of nodes and continuously changing topologies of wireless networks adversely affect the performance of wireless ad-hoc networks. A major problem is maximizing the lifetime of wireless networks while ensuring that packets are delivered to their destinations. Much research has been published on the routing protocols of wireless ad-hoc networks, but most of the algorithms focus on a single performance metric of wireless networks. In this chapter, we propose a routing protocol referred to as DEAR-2 for a heterogeneous wireless ad-hoc network. We have embedded the energy and device type awareness features of the Device and Energy Aware Routing (DEAR) routing algorithm in the face routing algorithm, which focuses only on guaranteed delivery.

The original version of this chapter was revised. A correction to this chapter is available at https://doi.org/10.1007/978-3-319-99966-1_30

M. U. Hassan (✉) · M. Mubashir · M. A. Shabir
School of Information Science and Engineering, University of Jinan, Jinan, China
e-mail: umair@mail.ujn.edu.cn

M. Shahzaib
Department of Computer Science, Norwegian University of Science and Technology, Trondheim, Norway

K. Shaukat · S. N. Hussain · S. Karim
Department of Information and Technology, University of Punjab, Jhelum Campus, Jhelum, Pakistan

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_20

20.1 Introduction

An ad-hoc wireless network is collection of self-organizing and infrastructure-less nodes, connected with each other to form a network for transferring data within the network. These networks can be deployed anywhere without any special infrastructure such as a base station, which makes these networks extremely useful in emergencies (e.g., in disaster areas where no infrastructure is available). Two nodes can transfer data easily when they are in the range of each other. When a wireless network consists of more than two nodes but the sender and receiver are not in range of each other, then intermediate nodes can act as routers and forward the data packets to the next node toward the destination [1]. A common example of an ad-hoc network is a network of devices connected via Bluetooth without any central infrastructure. Ad-hoc wireless networks may be used because of their low cost and ease of installation; in addition, a problem with one device does not affect the whole network. However, these networks also have some issues, including the continuously changing topologies of networks and limited power [2]. In these networks, structures change so frequently that it may not be possible for hosts to know the topology of the network.

Much research has been done to design routing algorithms for the efficient transmission of data within ad-hoc wireless networks. However, most routing algorithms focus on a single performance metric, such as guaranteed delivery, energy conservation, or quality of service. In this chapter, we propose a new algorithm called DEAR-2 that focuses on two metrics: energy conservation and guaranteed delivery in ad-hoc wireless networks. The main objective for the algorithm is the confirmed delivery of data packets within the network while maximizing the lifespan of the network. In the proposed routing algorithm DEAR-2, we use device type and multiple paths for transmission from the Device and Energy Aware Routing (DEAR) algorithm [1] along with the path-finding techniques of the FACE routing algorithm [3], which provides the guaranteed delivery of packets to a destination in a planar graph to improve the performance of wireless ad-hoc networks. The FACE routing technique uses a planar graph of a wireless network, draws a line from sender to receiver, and sends data packets along this line. Whenever an edge intersects the line, it takes the current node and the starting node, then continues to traverse the graph until it reaches the destination. However, the FACE technique has one limitation when finding a route: it assumes that the network topology does not change during the transmission of the data packets. In our proposed protocol, we use a planar graph to find routing paths, but we use the paths that have more nodes powered by a constant power supply. The remainder of this chapter is organized as follows: Sect. 20.2 discusses related work, DEAR-2 is presented in Sect. 20.3, and the conclusion is presented in Sect. 20.4.

20.2 Related Work

Previously published research has aimed to improve the routing protocols of wireless ad-hoc networks. Major problems to solve for wireless ad-hoc networks include increasing the lifetime of the networks and ensuring reliable packet delivery to the destination [4].

20.2.1 Energy-Aware Routing Protocols

Power-Aware Routing in Ad-Hoc Networks Singh et al. [5] argued that other metrics—including the total energy consumption of a network, cost per packet delivered to the destination, and reductions to the difference in power levels among all nodes within a network—should also be considered to improve routing protocol performance, rather than just focusing on the shortness of paths in the network.

Device and Energy Aware Routing The Device and Energy Aware Routing (DEAR) protocol [1] was proposed for heterogeneous ad-hoc wireless networks. DEAR distinguishes nodes on the basis of power supply, depending on whether they are powered by a continuous supply or batteries. The main function of this protocol is to send packets through nodes with a continuous supply of power to maximize the lifespan of a network.

CLUSTERPOW and MINPOW The CLUSTERPOW protocol [6] creates clusters of nodes in the network according to their energy levels and sends packets through the routes while maintaining a maximum transmit power level for each node. The MINPOW protocol considers the total power consumption in a network rather than maintaining the power levels of individual nodes in the network.

Minimum Energy Hierarchical Dynamic Source Routing The Minimum Energy Hierarchical Dynamic Source Routing (MEHDSR) protocol is an improved version of the Dynamic Source Routing protocol. MEHDSR finds the most efficient paths for packet delivery using a flooding method. However, due to differences in the power levels of nodes and high overhead, its network lifetime is reduced [7].

20.2.2 Guaranteed Delivery Routing Protocols

Because wireless ad-hoc network topologies are continuously changing, guaranteed packet delivery to a destination is a major problem. Much research has been conducted to design a location-based protocol that ensures packet delivery. Location-based protocols are of three different types: restricted directional flooding, face routing, and greedy routing. We will be focusing on face routing. Some important face routing-based protocols include the FACE [3] first location-based

protocol, which ensures guaranteed delivery without flooding. This protocol uses a planar graph of a network to find routes for packet delivery. A line is drawn from the sender to the receiver, and the packet is delivered along the boundaries of faces.

The Greedy Perimeter Stateless Routing (GPSR) [8] protocol was designed using a combination of greedy routing and face routing. In this protocol, a node sends a packet to the closest node with respect to the destination, if the neighbor is closer to the destination than the sender node.

However, little work has been done to design a protocol that is efficient with respect to power consumption and packet delivery in the network. Therefore, we combined a newer version of the FACE routing technique with the power-aware routing features of the DEAR algorithm to obtain better performance in heterogeneous wireless networks.

20.3 Device and Energy Aware Routing Protocols

The DEAR protocol was designed with an aim to maximize the lifetime of a heterogeneous wireless ad-hoc network. In a heterogeneous wireless ad-hoc network, the nodes are of two types: internally powered by batteries and externally powered. In routing table entries, a binary attribute is the addition of device type, where 0 means that the device is battery powered and 1 means that the device is externally powered. In DEAR, the cost of passing the packet through an externally powered node is considered to be zero. DEAR works to pass the maximum traffic through externally powered nodes to increase the lifetime of a wireless ad-hoc network [9–16].

20.3.1 Network Lifetime Performance

In DEAR, most of the traffic is passed through externally powered nodes. Therefore, nodes powered by batteries maintain their energy levels and the lifetime of the heterogeneous wireless ad-hoc network is increased significantly.

20.3.2 Delivery Rate

As previously stated, the DEAR protocol attempts to send most packets through externally powered nodes. If two nodes communicate frequently, then the path with the maximum-powered nodes will be chosen every time. This will eventually drain the power of battery-powered nodes, thus causing a low delivery rate.

20.4 FACE Routing Protocol

The FACE routing protocol guarantees packet delivery in a planar graph. Guaranteed conveyance ensures the capacity to effectively send a message from a source to a destination. In a relative neighborhood and with Gabriel graphs, recovery from a failure in directing is possible without changing between any adjoining faces [17]. Most of the time, wireless ad-hoc networks use an uncontrolled path, changes in topology occur, and hosts may not know the topology of the entire framework. In this chapter, we attempt to coordinate a wireless ad-hoc network for which nothing is known about the framework, besides the range and the zones of the hosts to which the network can confer direction. Specifically, we consider a case in which all hosts have a comparatively wide conveyance [18].

FACE routing is based on location. A routing table is maintained; it contains information about the topology of the network and a planar graph of the indicating nodes of the network. FACE routing guarantees packet delivery to the destination in a fixed planar graph. As the topology of the wireless network changes, the routing table is also updated.

20.4.1 FACE Routing Constraints

FACE routing [3] requires a separately constructed subplanar graph of a wireless ad-hoc network and assumes that the subplanar graph of the network is static during the routing process.

20.4.2 Network Lifetime Performance

FACE routing does not focus on energy metrics. FACE tries to deliver packets to the destination through any possible way, without considering the energy levels of the nodes of the wireless network. Therefore, the performance of FACE is not good when considering energy or network lifetime metrics. Passing packets through the same path will decrease the lifetime of a wireless ad-hoc network.

20.4.3 Delivery Rate

The FACE routing protocol is specifically designed to ensure the delivery of packets from the source to the destination in a wireless ad-hoc network. In FACE, the main idea is to divide the network graph into planes in a localized manner, then to forward a message along one face or a sequence of adjacent faces that are progressing toward the destination node [19, 20].

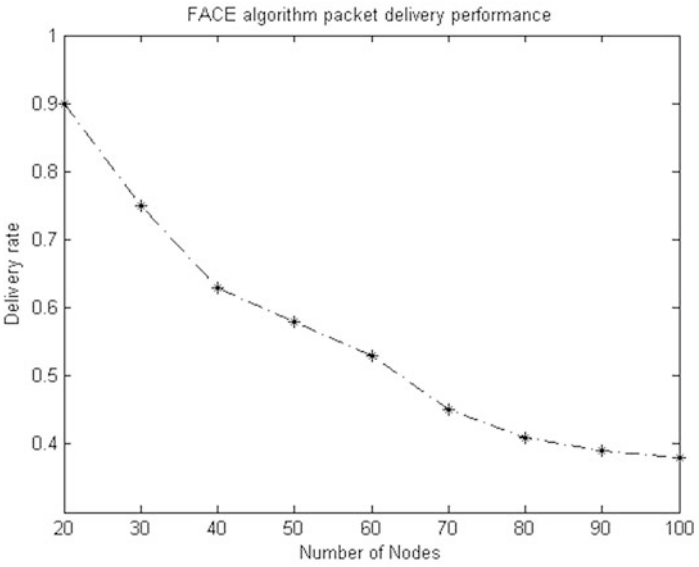


Fig. 20.1 Percentage change in the delivery rate as the number of nodes increases by a degree of 4 using the FACE routing protocol

With an increase in the degree of nodes, the delivery rate also increases (Fig. 20.1). In FACE, a packet travels through the edges that intersect the line between the source and the destination. When the packet reaches an edge intersecting with a face, then it is forwarded to the nest edge. The delivery rate is high when compared with other protocols.

20.5 DEAR-2 Protocol

20.5.1 Motivation

Most routing protocols are focused on single performance metric. For example, the FACE protocol was designed with the aim to increase the delivery rate, whereas the DEAR protocol was designed to increase the lifespan of a wireless ad-hoc network. Very few protocols focus on more than one metric to improve the routing algorithm in a network, such as to maximize the lifetime of a network and increase the delivery rate at the same time. Consider a wireless ad-hoc network for soldiers to communicate with each other; here, the maximum lifetime of the network and the maximum delivery rate are both equally important. However, no protocol has been developed yet for a wireless ad-hoc network where both metrics of energy and delivery rate are important. Here, we propose the DEAR-2 protocol, which aims to provide good performance according to both metrics.

20.5.2 Design and Operation of DEAR-2

The DEAR-2 protocol uses rules from both DEAR and FACE. All devices in the wireless network are divided into two types: battery-powered nodes and externally-powered nodes. A line is drawn from the source node to the destination node. The packets traverse through edges that intersecting lines connecting the source and destination nodes. An associated planar diagram (G) segments the plane into faces, which are limited by polygonals made up of the edges of G. Steering from the source to the destination uses these faces.

Algorithm for Packet Forwarding

```
/*Address for next node through FACE */

fAddress=FACEnext();
each entry d in routing table(RT) and redirect table(RD), do{

/* if distance from next to destination is bigger or equal
   to nearest powered node */
if(RT[d].costToDestination >=ShortestCostToPoweredNode)
RD[d].redirectToAddr = redirectPowereNode;
else
/* powered node is much distance from destination */
RD[d].redirectToAddr = fAddress;
}
```

Given a vertex v on a face f, the boundary off can be crossed in a counterclockwise course (or clockwise if f is the external face) using the notable right-hand decision [21, 22], by which it is conceivable to visit each divider in a maze by keeping your correct hand on the divider while strolling forward. A packet being forwarded from a node is calculated to find next node; it will also find the nearest powered nodes if the distance from the powered node is less than or equal to the distance of the next node selected for packet forwarding, then forward the packet to the powered node. The same method is again used to traverse through the graph to reach the destination.

20.5.3 Performance

DEAR-2 possesses the capability to increase the lifetime of a network because power is critical in a wireless ad-hoc network. This protocol also provides an increased delivery rate in wireless networks. By using externally-powered nodes to traverse through the network from the source to the destination, the lifetime of battery-powered nodes increases significantly.

Figure 20.2 indicates that the performance of the DEAR-2 protocol is similar to the performance of the FACE protocol, but provides a better delivery rate in the wireless network.

Figure 20.3 clearly shows that the lifespan of a wireless ad-hoc network increases with the use of the DEAR-2 routing protocol. This significant increase in lifespan is achieved with little overhead in calculating the distance of a powered node from the destination.

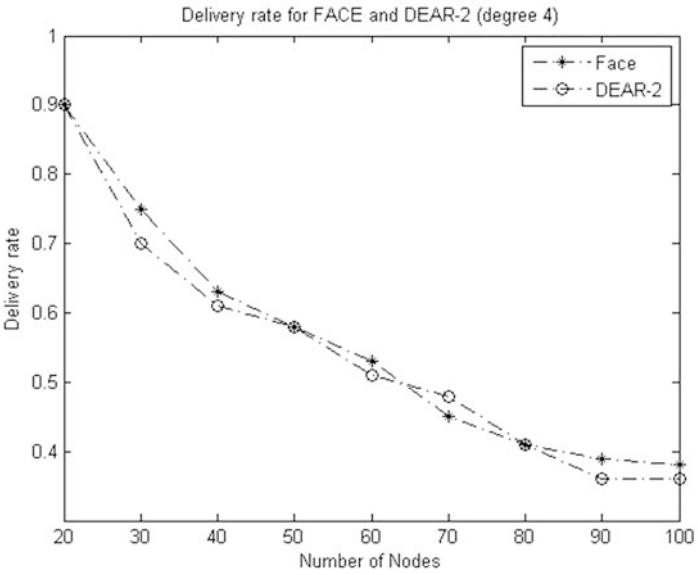


Fig. 20.2 Comparison of the delivery rates of the DEAR-2 and FACE protocols

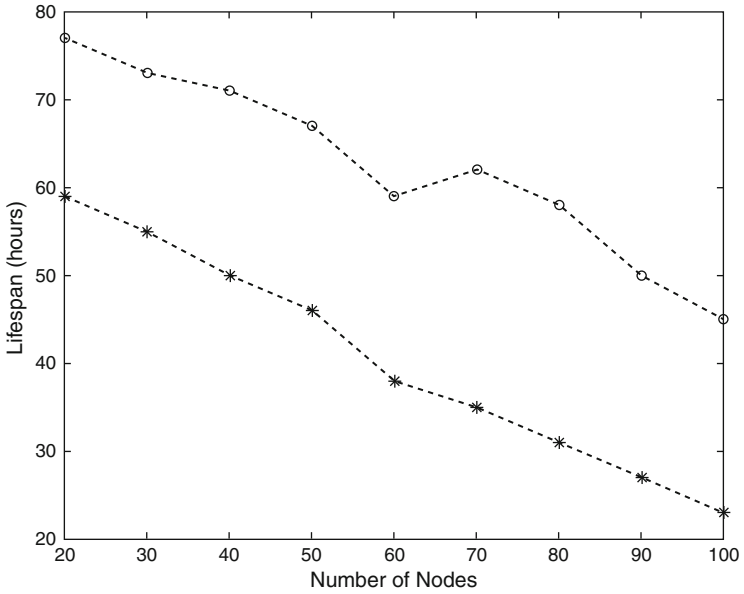


Fig. 20.3 Comparison of the network lifespans of the DEAR-2 and FACE protocols

20.6 Conclusion

In this chapter, we described the FACE routing protocol, which was designed to guarantee delivery, and the DEAR protocol, which aims to increase the lifespan of a wireless ad-hoc network. To meet the need for a protocol that focused on both the metrics of energy and delivery rate, we proposed the DEAR-2 protocol to increase the network lifetime and delivery rate. The DEAR-2 protocol was designed by adding a few steps to the FACE algorithm to use powered nodes for routing from the source to the destination.

References

1. Avudainayagam, A., Fang, Y., & Lou, W. (2002). DEAR: A device and energy aware routing protocol for mobile adhoc networks. In *MILCOM 2002. Proceedings* (Vol. 1). Piscataway, NJ: IEEE.
2. Khan, F., Rahman, F., Khan, S., & Kamal, S. A. (2018). Performance analysis of transport protocols for multimedia traffic over mobile Wi-Max network under nakagami fading. In *Information technology-New generations* (pp. 101–110). Cham: Springer.
3. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2013, November). Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network. In *2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC)* (pp. 1400–1407). Piscataway, NJ: IEEE.
4. Khan, F. (2014). Secure communication and routing architecture in wireless sensor networks. In *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)* (pp. 647–650). Piscataway, NJ: IEEE.
5. Singh, S., Woo, M., & Raghavendra, C. S. (1998). Power-aware routing in mobile adhoc networks. In *Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking*. New York: ACM.
6. Ko, Y.-B., & Vaidya, N. H. (2000). Location-aided routing (LAR) in mobile adhoc networks. *Wireless Networks, 6*(4), 307–321.
7. Tarique, M., & Tepe, K. E. (2009). Minimum energy hierarchical dynamic source routing for mobile adhoc networks. *Adhoc Networks, 7*(6), 1125–1135.
8. Karp, B., & Kung, H.-T. (2000). GPSR: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*. New York: ACM.
9. Ryu, J.-H., & Cho, D.-H. (2001). A new routing scheme concerning energy conservation in wireless home ad-hoc networks. *IEEE Transactions on Consumer Electronics, 47*(1), 1–5.
10. Bondy, J. A., & Murty, U. S. R. (1976). *Graph theory with applications*. Amsterdam: Elsevier North-Holland.
11. Alam, M., Ferreira, J., Mumtaz, S., Jan, M. A., Rebelo, R., & Fonseca, J. A. (2017). Smart cameras are making our beaches safer: A 5G-envisioned distributed architecture for safe, connected coastal areas. *IEEE Vehicular Technology Magazine, 12*(4), 50–59.
12. Jan, M. A., Jan, S. R. U., Alam, M., Akhunzada, A., & Rahman, I. U. (2018). A comprehensive analysis of congestion control protocols in wireless sensor networks. *Mobile Networks and Applications, 23*(3), 1–13.

13. Alam, M., Albano, M., Radwan, A., & Rodriguez, J. (2012). Context parameter prediction to prolong mobile terminal battery life. In *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* (pp. 476–489). Berlin: Springer.
14. Alam, M., Albano, M., Radwan, A., & Rodriguez, J. (2012). Context based node discovery mechanism for energy efficiency in wireless networks. In *2012 IEEE International Conference on Communications (ICC).*
15. Usman, M., Jan, M. A., He, X., & Alam, M. (2018). Performance evaluation of high definition video streaming over mobile ad hoc networks. *Signal Processing, 148*, 303–313.
16. Jan, M. A., Usman, M., He, X., & Rehman, A. U. (2018). SAMS: A Seamless and Authorized Multimedia Streaming framework for WMSN-based IoMT. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2018.2848284
17. Bose, P., Morin, P., Stojmenović, I., & Urrutia, J. (2001). Routing with guaranteed delivery in ad hoc wireless networks. *Wireless Networks, 7*(6), 609–616.
18. Khan, F., ur Rehman, A., Usman, M., Tan, Z., & Puthal, D. (2018). Performance of cognitive radio sensor networks using hybrid automatic repeat ReQuest: Stop-and-wait. *Mobile Networks and Applications, 23*(3), 1–10. https://doi.org/10.1007/s11036-018-1020-4.
19. Frey, H., & Stojmenovic, I. (2006). On delivery guarantees of face and combined greedy-face routing in adhoc and sensor networks. In *Proceedings of the 12th Annual International Conference on Mobile Computing and Networking*. New York: ACM.
20. Fida, N., Khan, F., Jan, M. A., & Khan, Z. (2016, September). Performance analysis of vehicular adhoc network using different highway traffic scenarios in cloud computing. In *International Conference on Future Intelligent Vehicular Technologies* (pp. 157–166). Cham: Springer.
21. Jan, M. A., Khan, F., Alam, M., & Usman, M. (2017). A payload-based mutual authentication scheme for internet of things. *Future Generation Computer Systems.*
22. Alam, M., Albano, M., Radwan, A., & Rodriguez, J. (2013). CANDi: Context-aware node discovery for short-range cooperation. *Transactions on Emerging Telecommunications Technologies, 26*(5), 861–875. https://doi.org/10.1002/ett.2763.

Chapter 21
A Lightweight Key Negotiation and Authentication Scheme for Large Scale WSNs

Mohammad Tehseen, Huma Javed, Ishtiaq Hussain Shah, and Sheeraz Ahmed

Abstract Wireless sensor networks (WSNs) are being used as remote monitoring and control systems in a number of industries, including health care, defense, agriculture, and disaster management. To ensure that their applications operate reliably, the requirements for the security and integrity of data have increased. Because WSNs are operating as backbone networks, there is a strong need to examine the security of these networks. However, the lack of administration infrastructure at the network level and scarce resources such as processing, power, and storage have made it challenging to find a proper security solution. Among the currently available solutions, single master key-based schemes have gained considerable popularity due to their lower communicational and computational burdens. Recent investigations have shown that these schemes have major drawbacks because of their susceptibility to attacks that involve the physical capture and tampering of nodes. If not handled properly, these attacks can compromise the network and cause a catastrophic situation. In this chapter, a new scheme is proposed: a lightweight system for key exchange and authentication. This scheme also contains countermeasures against physical capturing and tampering attacks. The results obtained from a simulation indicate that the scheme performs well with regard to the utilization of memory and power.

21.1 Introduction

Wireless sensor network (WSNs) are established with the help of tiny sensor nodes. Sensor nodes contain a sensor unit containing one or more sensing modules, a processing unit, a radiofrequency unit for communication, and a power unit [1].

M. Tehseen (✉) · H. Javed · I. H. Shah
Department of Computer Science, University of Peshawar, Peshawar, Pakistan

S. Ahmed
Career Dynamics Research Center, Peshawar, Pakistan

Iqra National University, Peshawar, Pakistan

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_21

The sensor nodes normally contain scarce resources, such as memory for storing data, limited power of processing, energy, and communication bandwidth, but lack any infrastructure for administering the network [2, 3]. These networks are used to communicate sensed data for this very reason. WSNs are used as the main component in a variety of applications, such as enemy tracking and targeting, battlefield monitoring systems [2], agriculture and farming [4], home intelligence [5], infant monitoring systems [6], community-based electrocardiogram monitoring systems [7], and radiation monitoring [8]. These applications require an adequate level of data security to operate properly, and the WSNs used in such applications should be completely secure. However, this level of security can only be achieved by implementing it in every aspect of a WSN, from design through the deployment phase [9, 10].

A variety of security systems have been proposed, which contain both master key-based symmetric and lightweight asymmetric algorithms. For wide-scale WSNs, master key-based systems are still considered to be the best option because these systems require less computational and communication overhead [9]. Master key-based systems contain one very major drawback: the possibility to physically capture and tampering with the node. To prevent this, special attention is required in the design phase. In such an attack, because the nodes are working unattended, an adversary can confine a node physically and retrieve the data in its storage unit; as a result, the whole network may be compromised.

This chapter proposes a key negotiation and authentication system that is both lightweight and provides resistance against physical capturing and tampering attacks. The rest of the chapter is structured as follows: Sect. 21.2 provides a brief literature review on the topic, Sect. 21.3 discusses the proposed solution, Sect. 21.4 provides implementation details and an analysis of the results, and Sect. 21.5 concludes the chapter.

21.2 Brief Overview

21.2.1 Security Challenges and Requirements

As previously mentioned, the implementation of adequate security measures in WSNs requires the security features to be implemented in every node in the network. However, some challenges need to be considered in the design phase, including wireless communication, limited resources (e.g., processing power, scarce battery, energy resources), and the lack of a fixed administrative infrastructure [11]. Because these challenges are present at the node level, the algorithms need to be lightweight in terms of computational and communication costs. The algorithms also need to fulfill the basic requirements of security, including data confidentiality, integrity, freshness, authentication, and mechanisms to deal with known types of attacks [2].

21.2.2 Schemes Presented in the Literature

The schemes that have been proposed in the literature to date can be divided into two broad categories: symmetric (key pre-distribution schemes) and asymmetric. Symmetric schemes include single master key-based schemes and pairwise key-based schemes. The single master key-based schemes are considered to be more efficient for large-scale WSNs [12, 13]. In symmetric schemes, shared keys are installed at every node in the predeployment phase of a network. These schemes require no overhead for key establishment for a secure link between the nodes.

Two approaches exist for symmetric schemes. In the first approach, a single master key is installed in all nodes [2, 14, 15]. Schemes such as SPINS, challenge and response, and the lightweight system by Delgado Mohatar are based on this approach. These types of schemes are efficient in terms of memory management and reducing the communication overhead involved in key exchange. However, they have a major drawback: If an adversary manages to retrieve the master key, then the whole network can become compromised. In the second approach for individual nodes, pairwise keys [16] related to every other node in the network are generated very carefully and stored in the memory of the node during the predeployment phase. For N nodes in a network, $N - 1$ keys need to be generated and installed at every node. Schemes such as Broadcast Session Key (BroSK) and Localized Encryption and Authentication Protocol (LEAP) [16] are based on this approach. The main drawback of this approach is the requirement for a large storage capacity because many keys need to be installed at every node.

Due to their large computational costs, symmetric key-based schemes are considered to be impractical for WSNs without elliptic curve cryptography (ECC). Different variants of ECC have been proposed and implemented to test their applicability, such as standard ECC and short ECC [17]. The National Institute of Standards and Technology (NIST) recommendation for ECC key size is 224 bits, whereas 80 bits is recommended for symmetric schemes [18]. Authors have implemented 32- to 64-bit keys for ECC, but this is not recommended by the NIST.

21.2.3 Existing Scheme Limitations

The schemes discussed in Sect. 21.2.2 have a major drawback: If any node is captured physically and all the keys present in the memory of the node are retrieved, this could cause an unimaginable loss for the data and security of the network.

21.3 Proposed Scheme

In this section, we introduce a new scheme that protects against physical capturing and tampering attacks, as well as limits the effects caused by any such attack to a subset of the network. By calculating the amount of communication that would be exposed to an adversary [19, 20], the effect of an attack can be determined. The proposed scheme works in three phases: the predeployment phase, postdeployment phase, and authentication protocol. The following sections discuss each of these phases in detail.

21.3.1 Predeployment Phase

During the predeployment phase, N bits, a sequence of numbers Seq_N, and a number *Ran* are randomly generated, where $Ran \leq (N - 1)$. They are copied into the memory of every node that will become part of the network, including the base station. A function *Func* is used to generate the master key Key_M. *Func* takes the Seq_N and *Ran* to generate the master key, as depicted in Eq. 21.1:

$$\text{Key}_M = Func\ \left(\text{Seq}_N, Ran\right) \tag{21.1}$$

Every node will then delete the random number *Ran* from its memory. The random number *Ran* will be saved only in the base station to be used for future authentication of any new nodes that want to join the network. Because all the nodes contain the same function *Func*, same sequence of numbers Seq_N, and same random number *Ran*, a single master key will be generated in every node. The key size should be at least 80 bits according to the NIST recommendation [18] to avoid brute force attacks over the network key. The size of the network key should be hidden inside the function *Func* to improve the security of the system.

At the end of this phase, every node will have a master key Key_M, a sequence of numbers Seq_N, and a function *Func*; the base station will also have a random number *Ran*. Under normal circumstances, the base station contains enough resources to secure it from any type of attack.

21.3.2 Postdeployment Phase

Soon after the predeployment phase, when the nodes are deployed in the actual environment, the postdeployment phase begins. Each node will establish a pairwise shared key *SKey* to establish a secure link with the base station. After that, all messages will pass through the base station.

Given below is the sequence of messages that will be exchanged between the base station S and an individual node A to establish a secure link. The base station S will generate message M1 and will broadcast it. The contents of the message are given in Eq. 21.2:

$$\text{M1} \ \left(S \text{ to}^*\right) : \text{Non}_s \mid \text{Iden}_s \mid \text{Hash}\left(\text{Key}_m, \text{Non}_s | \text{Iden}_s\right) \tag{21.2}$$

Here, Non_s is the nonce generated by base station S and Iden_s is the identity of base station S. Thereafter, each node will confirm the authenticity of the message received from the base station by generating a hash of Non_s and Iden_s from its own master key Key_M and matching it with the received one. After authentication, every node will then send a reply message to the base station. For example, when node A replies, node A will generate a nonce Non_A and in reply will send message M2 as shown in Eq. 21.3:

$$\text{M2} \ \left(A \text{ to } S\right) : \text{Non}_A \mid \text{Non}_S \mid \text{Iden}_A \mid \text{Hash}\left(\text{Key}_M, \text{Non}_A | \text{Non}_S | \text{Iden}_A\right) \tag{21.3}$$

This is the same message every node will send to the base station. After exchanging these messages, each node will generate a pairwise *SKey* by utilizing Eq. 21.4. Equation 21.4 will also be used at base station S to generate the respective node's pairwise *SKey*. Now consider node A again. After sending message M2, node A will have Non_S and Non_A its own nonce. Node A will concatenate them and calculate a hash from its master key Key_M.

$$SKey_{\text{as}} = \text{Hash}\left(\text{Key}_m, \text{Non}_s | \text{Non}_a\right) \tag{21.4}$$

Until now, each node has established a pairwise *SKey* for communicating securely with the base station S, whereas base station S has a table of pairwise session keys (*SKeys*) for each and every node present on the network. After establishing the pairwise session key *SKey*, each node will delete the master key Key_M.. Going forward, this pairwise session key *SKey* will be used for secure communication with the base station S.

At the end of this phase, the network is initialized. Every node will have a pairwise *SKey*, Seq_N, and *Func*. Base station S will contain a table of pairwise keys *SKeys*, Seq_N, *Ran,* and *Func*.

21.3.3 Authentication Protocol

When the postdeployment phase is finished, every node will be capable of communicating securely with the base station. If a new node wants to join the network, this protocol will help to authenticate the newly arrived node and establish a secure link with the base station. In a real environment where nodes die after completing their jobs, new nodes are deployed to replace them. Assume that node A is a recently

deployed node that wants to enter the network as a new node. The process to authenticate node A and establish a secure link will proceed as follows.

Node A will send a message M1 containing nonce Non_A and identity Iden_A to a base station S, as shown in Eq. 21.5. The new node A will have its master key Key_M generated through the procedure discussed previously.

$$\text{M1} \ \ (A \text{ to } S) : \text{Non}_A \mid \text{Iden}_A \tag{21.5}$$

M1 will serve as an indication that a new node A is trying to enter the network. As a result, base station S will reply with message M2, as given in Eq. 21.6:

$$\text{M2}\ (S \text{ to } A) : \text{Non}_A \mid \text{Iden}_A \mid \text{Non}_S \mid \text{Iden}_S \mid \text{Hash}\left(\text{Key}_M, \text{Non}_A \mid \text{Iden}_A \mid \text{Non}_S \mid \text{Iden}_S\right) \tag{21.6}$$

After authenticating the base station S, node A will send a message M3 in response, as given in Eq. 21.7:

$$\text{M3} \ \ (A \text{ to } S) : \text{Non}_A \mid \text{Non}_S \mid \text{Hash} \ \left(\text{Key}_M, \text{Non}_A \mid \text{Non}_S\right) \tag{21.7}$$

After receiving message M3, base station S will first authenticate node A. Both the base station and node A have each other's nonces. They can generate the pairwise session key *SKey* by using Eq. 21.4. After generating the pairwise *SKey*, both nodes will delete the master key Key_M. At the end of this phase, a new node has joined the network and established a secure link with the base station after they authenticated each other.

21.4 Implementation and Analysis

To test the proposed scheme, we used Network Simulator Version 2. The simulation environment was tested for networks with 64, 128, 256, 512, and 1024 nodes that were spread out in an area of 300×300 m^2. It was assumed that the same results would be produced for networks with 2048 nodes or more, on the basis of results obtained from the above-mentioned networks. Node0 was selected as the base station. The simulation implemented the proposed scheme at the application layer. For communication, a physical and data link layer with the standard 802.11 protocol was implemented, as shown in Table 21.1. The proposed scheme uses a 128-bit master key Key_M and session key *SKey*, a 2048-bit sequence of N bits Seq_N, and a 16-bit random number *Ran*. As discussed previously, after pairwise *SKey* is generated, every node deletes Key_M, Seq_N, and *Ran*, so only the 128-bit pairwise *SKey* remains.

Table 21.1 Simulation environment parameters

Protocol used	Nodes used in network	802.11 layers used	Range of radiofrequency unit	Covered area in m^2
802.11	64	Application, physical, MAC	80 m	300 × 300
802.11	128	Application, physical, MAC	80 m	300 × 300
802.11	256	Application, physical, MAC	80 m	300 × 300
802.11	512	Application, physical, MAC	80 m	300 × 300
802.11	1024	Application, physical, MAC	80 m	300 × 300

21.4.1 Proposed Scheme's Security Analysis

This section describes the results obtained from the security analysis.

21.4.1.1 Resistance Against Physical Capturing and Tampering

This scheme provides resistance against physical attacks. After establishing the pairwise *SKey*, every node deletes the master key Key_M. Therefore, if an adversary tries to retrieve Key_M, it will only end up getting the *SKey*. The whole network would not be compromised; only that particular secure link would be affected. To make the network more secure, a scheme can blacklist the nodes on the basis of trust level. Hence, instead of the whole network, only a very small portion of the network—the link between the captured node and the base station—will be exposed.

21.4.1.2 Analysis of Brute Force Attack

Due to the size of the session key (128 bits), a brute force attack can be avoided. The proposed scheme uses 128-bit keys to provide proper security. (The NIST [18] recommends 80-bit key size to avoid brute force attacks in WSNs.)

21.4.2 Performance Measurement

The performance of the proposed scheme in terms of energy consumption and memory utilization is discussed in this section.

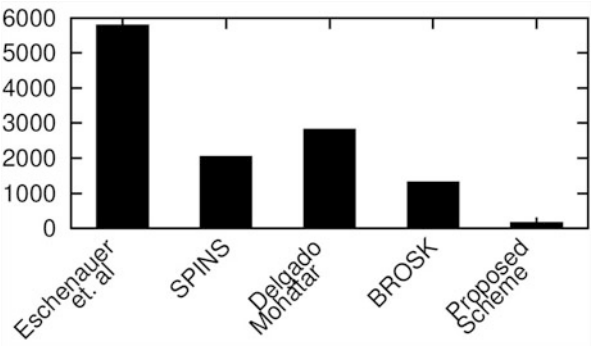


Fig. 21.1 Memory utilization for 10,000 nodes

21.4.2.1 Storage Utilization

The storage utilization of the proposed scheme is compared with other existing schemes with the same parameters, as given in Table 21.1 (one exception is the number of nodes, which are considered to be 10,000 for a wide-scale network). The proposed scheme only requires 128 bits per node to be stored in the storage area, whereas SPINS stores 2000 bits per node [2], the protocol by Eschenauer and Giglor stores 5800 bits per node [21], BROsK stores 1100–1300 bits per node [16], and a lightweight authentication protocol stores 2800 bits per node [11]. The proposed scheme is a lightweight scheme because each node only stores a pairwise *SKey* of 128 bits, so an average of 128 bits per node are stored. Therefore, the proposed scheme has better memory utilization than other existing schemes. This comparison is presented in graph form in Fig. 21.1.

21.4.2.2 Power Utilization

To compare the power consumption of the proposed scheme with other schemes, we simulated the scenario that was proposed by Delgado-Mohatar [11]. A literature review determined that 97% of power is drained by the transmission of messages [22]. Therefore, to minimize the number and size of transmitted messages, the power consumption can be reduced [23, 24]. The number of bits transmitted by an individual node in the proposed scheme is depicted in Fig. 21.2 for WSNs with different numbers of nodes. On average, the nodes in the proposed scheme require a single message of only 78 bits to establish a secure link with the base station.

Figure 21.3 depicts a detailed comparison of the proposed scheme with other schemes in terms of the number of bits transmitted by an individual node to establish a secure link for WSNs with different numbers of nodes. The results obtained indicate that the proposed scheme has better energy utilization than other existing schemes.

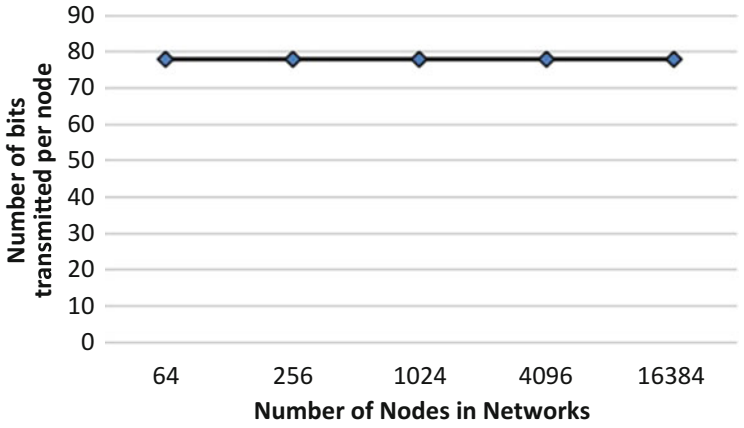


Fig. 21.2 Number of bits transmitted per node in the proposed scheme

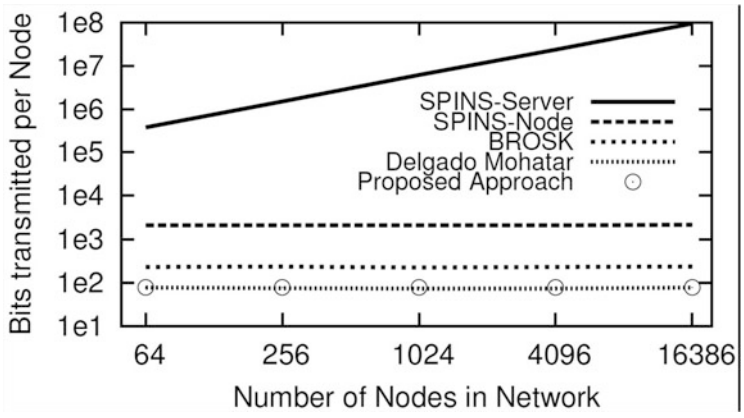


Fig. 21.3 Comparison of different schemes by number of bits transmitted per node

21.5 Conclusion

In this chapter, a lightweight key negotiation scheme was proposed. The scheme has the capability to secure a node against attacks of physical capture and tampering with the node. This scheme is a network-wide master key-based scheme that provides resistance by deleting the master key Key_M from the memory of individual nodes after the pairwise session key *SKey* is established. Because no master key exists, only that particular link will be compromised if the node is captured and tampered with physically, rather than the whole network. Additional measures can be introduced to the scheme to blacklist a node on the basis of the trust level developed with the base station.

The proposed scheme is lightweight in terms of memory and power utilization in comparison with other existing schemes. The proposed scheme only stores 128 bits per node (see Fig. 21.1), which makes it a lightweight scheme in terms of memory utilization. On average, 97% of the power is used by the communication unit. By minimizing the number of exchanged messages, much power can be saved in future applications.

References

1. Dargie, W., & Zimmerling, M. (2007). Sensor networks in the context of developing countries. In *The 3rd IFIP World Information Technology Forum (WITFOR)*. Addis Ababa, Ethiopia.
2. Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., & Culler, D. E. (2002). SPINS: Security protocols for sensor networks. *Wireless Networks, 8*(5), 521–534.
3. Stajano, F. (2002). *Security for ubiquitous computing*. Chichester, UK: Wiley.
4. Ojha, T., Misra, S., & Raghuwanshi, N. S. (2015). Wireless sensor networks for agriculture: The state-of-the-art in practice and future challenges. *Computers and Electronics in Agriculture, 118*, 66–84.
5. Batista, N. C., Melício, R., Matias, J. C. O., & Catalão, J. P. S. (2013). Photovoltaic and wind energy systems monitoring and building/home energy management using ZigBee devices within a smart grid. *Energy, 49*, 306–315.
6. Zhou, H., & Goold, B. (2015). A domestic Adaptable Infant Monitoring System using wireless sensor networks. In *IEEE 34th International Performance Computing and Communications Conference (IPCCC)* (pp. 1–2).
7. Lin, B. S., Wong, A. M., & Tseng, K. C. (2016). Community-based ECG monitoring system for patients with cardiovascular diseases. *Journal of Medical Systems, 40*(4), 1–12.
8. Gome, A., Magno, M., Lagadec, M. F., & Benini, L. (2017). Precise, energy-efficient data acquisition architecture for monitoring radioactivity using self-sustainable wireless sensor nodes. *IEEE Sensors Journal, 18*(1), 459–469.
9. Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. In *Communications of the ACM* (pp. 53–57). New York: ACM.
10. Prasanna, S., & Rao, S. (2012). An overview of wireless sensor networks applications and security. *International Journal of Soft Computing and Engineering (IJSCE), 2*(2), 2231–2307.
11. Delgado-Mohatar, O., Fúster-Sabater, A., & Sierra, J. M. (2011). A light-weight authentication scheme for wireless sensor networks. *Ad Hoc Networks, 9*, 727–735.
12. Chan, H., Perrig, A., & Song, D. (2003). Random key pre distribution schemes for sensor networks. In *Proceedings of Symposium on Security and Privacy 2003* (pp. 197–213).
13. Du, W., Deng, J., Han, Y. S., Varshney, P. K., Katz, J., & Khalili, A. (2005). A pairwise key pre-distribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC), 8*, 228–258.
14. Menezes, A. Z., van Oorschot, P. C., & Varstone, S. A. (1997). *Handbook of applied cryptography*. Boca Raton, FL: CRC Press.
15. Zhu, S., Setia, S., & Jajodia, S. (2006). LEAP efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks (TOSN), 2*, 500–528.
16. Lai, B., Hwang, D. D., Kim, S. P., & Verbauwhede, I. (2004). Reducing radio energy consumption of key management protocols for wireless sensor networks. In *Proceedings of the 2004 International Symposium on Low Power Electronics and Design* (pp. 351–356). New York: ACM.

17. Sojka-Piotrowska, A., & Langendoerfer, P. (2017). Shortening the security parameters in lightweight WSN applications for IoT-lessons learned. In *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)* (Vol. 13, pp. 636–641).
18. Barker, E., Barker, W., Burr, W., Polk, W., & Smid, M. (2007). NIST special publication. *NIST Special Publication, 800*, 1–142.
19. Gupta, A., & Kuri, J. (2008). Deterministic schemes for key distribution in wireless sensor networks. In *3rd International Conference 2008 on Communication Systems Software and Middleware and Workshop* (pp. 452–459). Banglore, India: IEEE.
20. Rautray, R., & Sarangi, I. (2011). A survey on authentication protocols for wireless sensor network. *International Journal of Engineering, Science and Technology (IJEST), 3*, 4253–4256.
21. Eschenauer, L., & Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. In *Proceedings of the 9th ACM Conference on Computer and Communications Security CCS-02* (pp. 41–47). New York: ACM.
22. Sangwan, A., Sindhu, D., & Singh, K. (2011). A review of various security protocols in wireless sensor network. *International Journal of Computer Technology, 2*, 790–797.
23. Anderson, R., Chan, H., & Perrig, A. (2004). Key infection smart trust for smart dust. In *Proceedings of the 12th IEEE International Conference 2004 on Network Protocols* (pp. 206–215). Cambridge, UK: IEEE.
24. Gupta, S., Verma, H. K., & Sangal, A. L. (2010). Authentication protocol for wireless sensor networks. *World Academy of Science, Engineering and Technology, 42*, 630–636.

Chapter 22
Distributed Monitoring Architecture for Industrial Safety Based on Gear Fault Diagnosis

Weiming Li, Yuanfang Chen, and Muhammad Alam

Abstract Real-time monitoring of machines is vital for enhanced performance and safety in industries. Gears are common components that interconnect mechanical parts that allow each part in a mechanical system to be engaged. They are mainly used to transmit kinetic energy and transform rotational speed. Due to the importance of gears, the degradation or failure of its performance affects the function of the machine resulting in the unplanned breakdown of equipment, This inevitably leads to economic losses and personnel safety issues. Therefore, it is of great significance to recognize industrial safety with respect to equipment management. In this paper, we presented a distributed architecture for monitoring the gears and reporting its faults. The monitoring of gears and gearboxes can alleviate safety issues and improve maintenance plans.

22.1 Introduction

Modern industrial safety can be divided into two categories: industrial equipment safety and industrial information control system security. The industrial production process can be safety ensured through the correct use of respective standards and instructions. The security of industrial information control systems refers to the protection of the system and the terminal equipment in the factory workshop. This

W. Li
Guangdong University of Petrochemical Technology, Maoming, China
e-mail: weiming.li@gdupt.edu.cn

Y. Chen (✉)
School of Cyberspace, Hangzhou Dianzi University, Hangzhou, China
e-mail: yuanfang_chen@ieee.org

M. Alam
Department of Computer Science and Software Engineering, Xi'an Jiaotong-Liverpool University, Suzhou, Jiangsu Province, China
e-mail: alam@ua.pt

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_22

security ensures that the industrial Ethernet and systems cannot be accessed, used, revealed, interrupted, amended, or destroyed without authorization. In 2011, the Fukushima nuclear accident promoted industrial safety to unparalleled importance, since a slight flaw in equipment may lead to an unprecedented disaster.

In industrial production, large-scale machinery and equipment is leveraged, along with a large amount of high-intensity automation. Thus, it is of great significance to ensure the safety of the equipment to continue timely production as well as the safety and well-being of the employees [1]. To achieve safe production, status of the equipment should be predicted and diagnosed early. "Many companies apply periodic preventive maintenance" to check the status of equipment. In order to ensure safety and create greater economic benefits, "forecast maintenance" provides strong support for safe production as well [2].

In industrial operations, rotating machinery is often used for many processes, thus fault diagnosis research has become popular for rotating machinery in whole fault diagnosis studies. Statistically, 80% of failures are caused by gear faults in transmission machinery failures [3]. Furthermore, root cause analysis usually has great concern with respect to continuously running operations with heavy loading and high rotational speed. This shows the significance of gearbox monitoring and diagnoses for gear faults in running machinery [4].

Gear failures are classified into different types since many factors influence them such as structural, material, and working environment conditions. Four common types of failures are as follows:

1. Tooth Damage/break: The teeth experience large loading , which results in the gear tooth base abandoning the maximum bending stress while in operation. When the fatigue limit is reached, a crack appears and extends to the broken teeth gradually, or can even directly cause instantaneous breaks.
2. Tooth Flank Pitting: The shear stress is introduced into as meshing process that results in the cracks causing small metal sheet peeling, and small pits when the shear stress exceeds the fatigue limit.
3. Tooth Flank Wearing: When lubricants are dirty or under filled, the meshing causes tooth profile changes, which result in tooth flank wear.
4. Tooth Glue: Tooth surface glue occurs when the tooth's surface temperature rises sharply along with heavy loading and high speed causing lubrication film instability.

From the list above, teeth breaking and pitting are the main sources of gear failures. As for the rest of the gear parts such as the ring gear, spoke, and hub failure typically doesn't occur since strength and rigidity requirements are attained through design [5–7].

22.2 Distributed Architecture

The proposed architecture for monitoring and fault reporting is depicted in Fig. 22.1. At lower layer, all the machines are monitored via sensors and especially the gears. The sensors constantly monitor these gears and collect the information. The collected data is forwarded to the storage via the communication technology used. The control layer, which mainly consists of servers, analyses the collected information and takes necessary decisions. These decisions are stored in the repository along with the collected data for long-term analysis and predictions. In order to provide more scalability, we have introduced the gateways that are controlled by the servers and can access the stored data and local decisions. This way, the servers can also monitor and control the far installed sensors for monitoring. The upper most layer is the application layer that presents the results to end users in visual format.

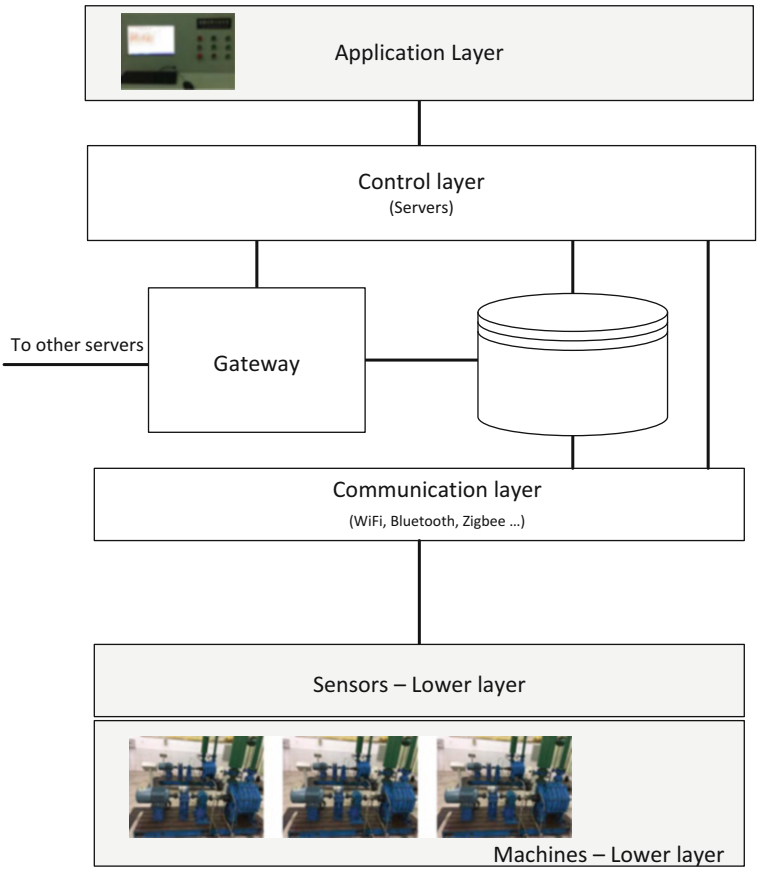


Fig. 22.1 The proposed distributed architecture

22.3 Gear Vibration Analysis

There are many fault diagnosis methods to predict gear failure such as vibration diagnosis, oil analysis, acoustic emissions, and noise analysis. However, vibration monitoring is the most important due to gear meshing vibrations that can cause noise and overheating, etc. Vibration can be divided into free vibration, forced vibration, and self-excited vibration. Vibration has two main sources. The first being normal alternating loads that are not concerned with gear error or fault which is known as the meshing vibration. The second is decided by the meshing stiffness and the fault function. Whether the status of the gear is normal or not normal, meshing vibration and harmonics always exist, but the vibration signal will be different. Therefore, it is feasible or the fault diagnosis to be leveraged from gear meshing vibration frequency and harmonic signals [8].

22.4 Intelligent Diagnosis of Equipment

Equipment performance can be maintained through key performance indicators. When various KPIs can't be determined, improving measures are adapted to ensure they are within the normal status. KPIs important system of intelligent maintenance decision-making is composed of the dynamic risk level, predictive maintenance information, and RAM (reliability availability maintainability) evaluation [9]. In recent years, condition-based maintenance decision-making has become popular. This is based on the analysis of multi-dimensional data of equipment to optimize the maintenance strategy to extend the cycle of prevent maintenance, thus reducing cost through a reliability algorithm.

22.4.1 Intelligent Decision System for Equipment Failure Maintenance

Decision-making based on intelligent diagnosis gained from vast amounts of equipment status data allows cost and safety decisions to balance. In most cases, breakdown maintenance can be performed on the standby machine through the monitoring of abnormal equipment status signals. But there are also some special operating environments in which transportation and maintenance costs restrict breakdown maintenance like offshore platforms. The equipment will need to continue production for a certain time period to reduce economic costs that are caused by unplanned shutdowns when early faults occur. However, to avoid accidents while the equipment is operating under abnormal conditions, scientific data is needed to direct the decision-making for safe equipment operation. This is called the data-based intelligent decision-making system [10].

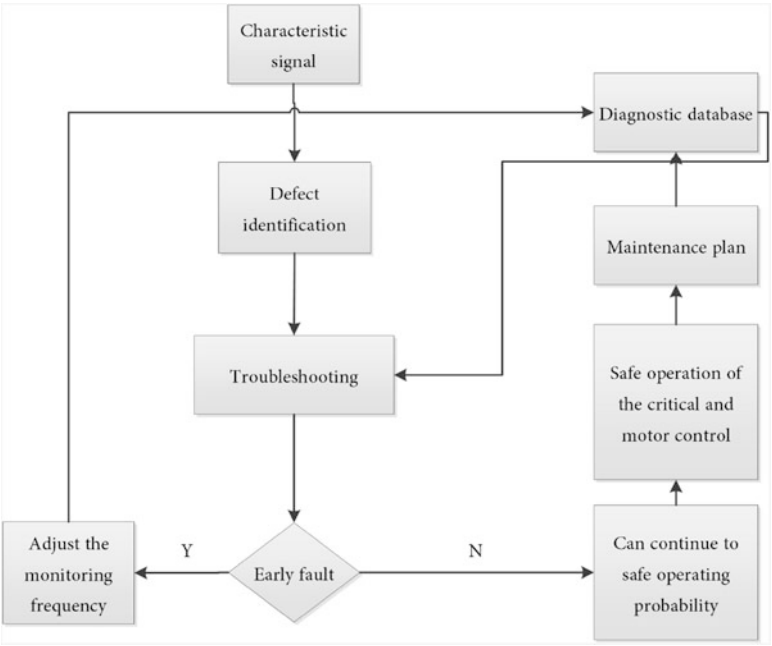


Fig. 22.2 The troubleshooting flowchart

22.4.2 Process Troubleshooting

A rational and balanced decision is needed in deciding the unexpected shutdown for minimum loss with respect to the safety status [11]. This balanced maintenance decision can be determined through the reliability of the equipment simulation, the reliability of the equipment to change the trend, and the trend itself as shown in Fig. 22.2.

22.5 Troubleshooting Examples

22.5.1 Fault Diagnosis Test Platform

Gear testing devices consist of two sets of multi-staged centrifugal fans, while one is the standard unit and the other is the testing unit. Each has an independently developed dimensionless immune composite fault diagnosis system using industrial units, as shown in Fig. 22.3. The system can diagnose gear fault types and severities, while series testing can be done on gear fault monitoring.

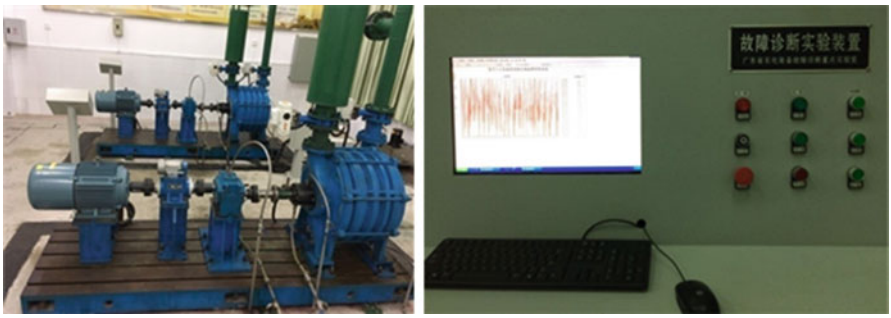


Fig. 22.3 Fault diagnosis test platform

22.5.2 Test Plan and Process

Most running machines cause vibration which can be detected with vibration sensors, and most faults can be diagnosed directly through the vibration signals at the machinery. In this test platform, the different fault types of gears were tested, while standard helical gears were used with the ratio of 1:1.25 in the experiment. The four gear states used were normal, wearing, pitting, and tooth break as shown in Fig. 22.4. Before the experiment, the two sets of units had been adjusted to the best conditions, while the vibration data was taken with sensors and used as the base. In this experiment, the vibration signals were collected at different speeds for the four gear states. The speeds were adjusted to a lower level to reduce the vibration of the faulted gears, and are shown in Table 22.1.

22.5.3 Diagnosis Decision Based on Test Signal Analysis

The vibration intensity is the root mean square value of the vibration velocity for the range of 10–1000 Hz, which reflects the characteristic indexes of the mechanical vibration. Generally, the maximum value of the vibration is taken as the vibration intensity and the expression can be written as

$$V_{\text{ims}} = \sqrt{\frac{1}{N}\sum_{n=0}^{N-1} V^2 n} \tag{22.1}$$

The two sets of units were adjusted to the best state with rotation speeds of 1800 r/min before the experiment. For every type of faulted gear, 150 data sets were attained for the 3 speeds tested, while approximately 100 data sets remained after the removal of abnormal data. After data analysis, the signals were mostly consistent between the normal unit and the standard unit. However, standard

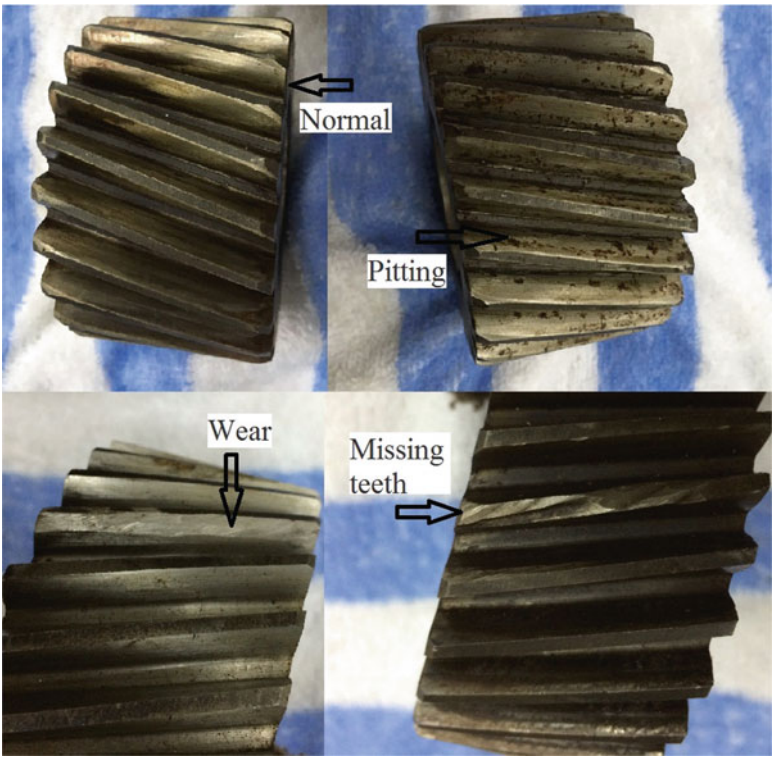


Fig. 22.4 Images of the four gears states used

Table 22.1 Fault diagnosis unit test case

Gear situation	Rotating speed (r/min)		
Standard	1800	1800	1800
Normal	1800	1800	1800
Pitting	1800	1500	1500
Wear	1800	1500	1200
Missing teeth	1800	1200	600

deviation calculations of the 100 data sets revealed that the data was 0.501 from the horizontal sensor and 1.002 from the vertical sensor.

1. For the pitted gear, the vertical vibration value was 1.022 and the horizontal vibration value was 0.511. When the speed was reduced to 1500 r/min, the vertical vibration value was reduced to 1.009, while the horizontal vibration value was reduced to 0.503.
2. For the wearing gear, the vertical vibration value was 1.158 and the lateral vibration value was 0.605. When the speed was reduced to 1500 r/min, the vertical vibration value was reduced to 1.088, while the horizontal vibration value

was reduced to 0.562. After a further speed reduction to 1200 r/min, the vertical vibration value was reduced to 1.008, while the horizontal vibration value was reduced to 0.507.

3. For gear tooth break, the vertical vibration value was 1.357 and the horizontal vibration value was 0.658. When the speed was reduced to 1200 r/min, the vertical vibration value was reduced to 1.274, while the horizontal vibration value was reduced to 0.612. After a further speed reduction to 600 r/min, the vertical vibration value was reduced to 1.153, while the horizontal vibration value was reduced to 0.542.

Based on the data for the gear tooth break, the vibration value exceeded the alarm value according to the vibration standard. After reasonable speed reduction the standard was still not complied with, therefore when such a vibration signal happens a shutdown must be conducted for. However, for the pitted and wearing gear, the vibration returned to normal levels after rotation speed reductions ensuring safe production until a timely and cost-effective shutdown and repair can occur.

22.6 Conclusions and Future Work

In this paper, we have presented a distributed architecture that reports the fault monitoring and provide on-time feedback to specific machines. The gear fault category can be identified based on the differences between the vibration signals, which can be measured at the gearbox housing. Under the same conditions, the vibration signal will increase with the increase of speed so that a quantitative relation equation can be obtained among the parameters with multiple regression analysis. As this test is still in the exploratory stage, further research can be done to more gear type failures for further exact verification. This will allow for the establishment of a more accurate characteristic parameter equation to better aid in decision-making for fault diagnosis of field rotating machinery. The future direction of this work is present more in detail the implementations and analysis of the presented architecture for distributed monitoring.

Acknowledgements The paper is supported by the Science and Technology Project of Maoming City (No. 2017316, No. 2017318).

References

1. Jin, C. (1999). *Vibration monitoring and fault diagnosis of mechanical equipment*. Shanghai: Shanghai Jiaotong University Press.
2. Pan, W., Yuan, Y., Sandberg, H., Gonçalves, J., & Stan, G.-B. (2015). Online fault diagnosis for nonlinear power systems. *Automatica, 55*, 27–36. https://doi.org/10.1016/j.automatica.2015.02.032

3. Zhigao, L., Xueqing, Q., & Haiquan, T. (2006). Domestic status and development direction of gear fault diagnosis. *Mining Machinery, 34*(1).
4. Li, W., Zhu, Z., Jiang, F., Zhou, G., & Chen, G. (2015). Fault diagnosis of rotating machinery with a novel statistical feature extraction and evaluation method. *Mechanical Systems and Signal Processing, 50–51*, 414–426. https://doi.org/10.1016/j.ymssp.2014.05.034
5. Wenyi, L. (2000). *Research on vibration monitoring and fault diagnosis of wind turbine*. Chongqing: Chongqing University.
6. Chen, Y., Lee, G., Shu, L., & Crespi, N. (2016). Industrial internet of things-based collaborative sensing intelligence: Framework and research challenges. *Sensors, 16*(2), 215.
7. Jan, M. A., Khan, F., Alam, M., & Usman, M. (2017). A payload-based mutual authentication scheme for Internet of Things. *Future Generation Computer Systems*.
8. Guoan, Y. (2016). *Practical technology of fault diagnosis of mechanical equipment*. Beijing: Petrochemical Press.
9. Qingfeng, W., Jianfeng, Y., & Wenbin, L. (2010). Development and application of intelligent decision system for press industrial equipment maintenance. *Chinese Journal of Mechanical Engineering, 24*(46), 168–177.
10. Weiming, L., Yugang, C., & Guangpei, C. (2016). Sensor-based gear vibration monitoring and reliability detection method. *Mechanical and Electrical Engineering Technology*, (5), 43–46.
11. Shufen, F., & Wenyuan, L. (2001). Research on intelligent decision support system for equipment maintenance management. *Systems Engineering-Theory and Practice*(12), 53–59.

Chapter 23
Node Density Analysis for WBAN Schemes in Terms of Stability and Throughput

Sheeraz Ahmed, Nouman Sadiq, Kamran Sadiq, Nadeem Javaid, and M. Ali Taqi

Abstract Wireless sensor applications have resulted in significant advancements in the medical sector known as body area networks. They are being heavily employed by wearable monitoring systems for detection of symptoms and indicators in order to counter harmful medical conditions while they are innocuous. The successful delivery of data whether normal or critical from the patient to his medical practitioner is still a tedious task. Various attempts at designing suitable protocols for WBANs have been made by researchers at different network layers. In this work, we have tried to present an overview of the working methodology of WBAN field, its applications, and various routing protocols designed for WBANs. What should be a suitable number of nodes to be deployed on a human body is still a challenging issue. We have considered three popular routing schemes of WBAN and presented an analysis with varying node deployments to judge their performance. The three schemes considered are SIMPLE, LAEEBA, and EENMBAN.

S. Ahmed (✉)
Career Dynamics Research Centre, Peshawar, Pakistan

Iqra National University, Peshwar, Pakistan
e-mail: sheerazahmed306@gmail.com

N. Sadiq
Career Dynamics Research Centre, Peshawar, Pakistan

K. Sadiq
Career Dynamics Research Centre, Peshawar, Pakistan

N. Javaid
COMSATS Institute of Information Technology, Islamabad, Pakistan

M. A. Taqi
Career Dynamics Research Centre, Peshawar, Pakistan

Gomal University, Dera Ismail Khan, Pakistan
e-mail: zahid.ullah@imsciences.edu.pk

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_23

23.1 Introduction

Wireless sensor networks are composed of sensor nodes that vary significantly in numbers, are sensitive to data, and serve to receive and dispatch information. The basic purpose of the sensor nodes is to observe the bodily and surrounding circumstances including humidity, temperature, noise, vibration, pressure, and movement of objects. Information gathered regarding these factors is then dispatched to the desired destination. WSN is an emergent technology with a focus on development in the field of medicine and implementation of greater process control in the industrial sector [1]. It has also found relevance in the military sector for surveillance purposes. It is also relevant in the agricultural sector for observing and analyzing surrounding factors in order to facilitate better results. Numerous routing protocols have been designed for WSNs with the intent to improve energy efficiency and information sharing among the nodes. A complete survey of the various protocols designed for WSN [2].

Energy consumption is the most significant area of interest in the general discussions surrounding WSNs. Due to the small size and intricate structure of the sensor nodes, the recharging and replacement of the battery is considerably tricky once the nodes have been placed in their designated positions. In single-hop transmission, the nodes that are distant from the BS fail to remain functional over a substantial period due to the excessive amount of transmitting power required. The same issue is encountered in multi-hop system due to the continuous transmission of information. Due to the connections between nodes being wireless, fading of data was a consistent concern. Data fading could result in errors prompting for the data to be dispatched again which would result in loss of resources including time, which would in turn result in the overall deterioration of network efficiency.

Wireless sensors have resulted in significant advancements in the medical sector. They have been heavily employed by wearable monitoring systems for detection of symptoms and indicators that may be of concern at an initial stage in order to counter harmful medical conditions while they are innocuous. Wearable monitoring systems enable patients to indulge in routine activities while their vitals are constantly observed [3–8].

A network comprising of sophisticated, low-power, and micro- and nanotechnology sensors and actuators is required for achievement of the above discussed purposes. The said network is positioned on the person's body or placed within the body in order to derive information at suitable intervals. Networks designed for this purpose are termed as wireless body area networks. In addition to proving extremely helpful in providing crucial feedback, they are also an economical option as they can replace the inhospital monitors which may be expensive. WBANs are of considerable importance as a source of accurate and prompt updates regarding the medical parameters of a patient, which in most cases form a reliable basis for the medical professional to form a diagnosis [9]. The information gathered in this manner can also be cached for future application. Figure 23.1 illustrates the operation of WBAN.

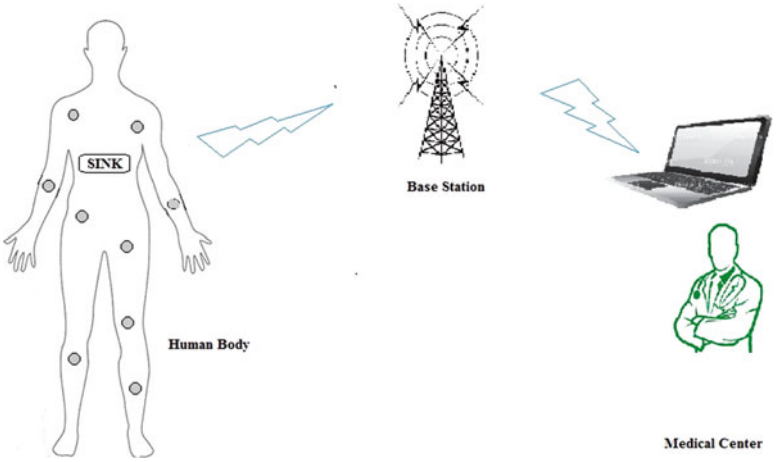


Fig. 23.1 A simple WBAN scenario

Wireless body area networks (WBANs) or wireless body area sensor networks (WBASNs) are subcategory of WSNs. WBASNs were primarily designed to aid in the medical field. However, gradually an increase in their applicability was observed, finding use in the athletic and military fields. Two major varieties of WBANs are:

- In vivo sensors which are placed inside the patient's body
- The second variety being wearable sensors which are positioned on the patient's body

Despite the expansive applicability of WBANs, there are nevertheless various obstacles that need decimation. The limited nature of the energy resources is perhaps the largest issue faced during deployment. Normally, communication between the nodes consumes a greater amount of energy as compared to observing and accumulating data. Different techniques have been proposed in order for sensors to improve energy consumption of nodes, enhancing their functional life. A leading technique employed for recharging the node batteries is induction in which the nodes are equipped with infrared light sensors (heat is generated for charging the batteries by exposing sensors to light which in turn excite the electrons). The electrons of infrared sensors can also be excited by heat produced due to exertion or movement of the patient body via mutual induction.

23.2 Related Work

Most of the protocols proposed for WSNs were unable to achieve the intended purposes of the WSNs. The evaluation criteria are often different for different protocols; various comparisons have also been made among different protocols.

Various attempts at designing suitable protocols for WSNs have been made by researchers. The salient features of some of the significant protocols have been analyzed below.

Wireless sensor networks employ multi-hop communication and comprise sensor nodes. Researchers [1] illustrate a new protocol termed as LEACH (low-energy adaptive clustering hierarchy) which relies on relaying and cooperation as means of enhancing the network's functional life. Two major functions were assigned to the relay nodes according to this model, the first being transmitting prerecorded data resulting in surplus energy which can be utilized for aiding in communication processes. The second function of the relay node is to ensure that the accumulated data is dispatched to the central device, i.e., sink or gateway or base station.

The conventional description of WSNs is that of networks that utilize sensor nodes in order to monitor and record data and dispatch it to the sink. However triggered by the limited energy resources available to the sensor nodes as illustrated in [2], A. Ehyaie and his associates introduced the concept of relay nodes. An upper bound limit was set on the number of sensor nodes and relay nodes, while the intervals between the nodes and base station/gateway were also specified. The complexities observed in relation to the joint data routing and relay positioning were scrutinized by Jocelyne Elias and other researchers for the purpose of extending the network's lifetime and presented a suitable design for WBANs as observed in [3].

A different optimal design is proposed in [9] performing joint analysis in order to address the issues encountered in relation to relay node positioning and data routing. The researchers of this paper strived to identify the most efficient locations for the relay nodes via preplanning and apposite engineering. This approach was favored over the traditional method of placing nodes on a random basis. The proposed design also scrutinized the data routing simultaneously.

In [10], researchers represented the attributes of arm movement in the form of a spherical model. Analytical channel modeling was also deducted. Four potential locations were identified for the placement of the transmitter and the receiver based on their placement inside or outside the body.

Authors in [11] presented a network protocol termed as interface aware protocol for the WBASN. This protocol enables the WBASN to monitor and record data relating to several bodily functions of numerous patients simultaneously while also providing instant analysis regarding various physical factors. Transmission of data is prioritized based on the severity of the patient's condition and how crucial the data is. The data that is of critical nature is transmitted before information that can be considered of secondary importance.

While research in [12] is related to Ambient Assisted Tool (AAT) which can recognize various physical activities, it is basically developed to identify and

register three kinds of human activities, being mobile activity recognition, ambient activity recognition, and vision-based activity recognition. Once the activity is successfully identified, the current and previously collected data is compared for any dissimilarities, with the assistance of an algorithm. AAT aids in constantly observing various relevant aspects of the person's physical condition in order to identify and locate any potential complication.

Researchers in [13] strived to monitor vital signs of patients in order to enhance end-to-end traffic. Any cast routing protocol was introduced for this purpose. Minimum network latency was achieved since information was sent to the receiver closest to the patient. The protocol serves to perform indoor positioning and ECG monitoring in addition to detecting and locating any outdoor accident.

An energy-efficient adaptive routing algorithm, as illustrated in [14], was proposed by researchers which strived to decrease the energy consumption by sensor nodes during transmission of crucial data, at the same time ensuring QoS. As a consequence of mobility, the connection between nodes and their parent nodes may be terminated. To counter that and to ensure reconnection, factors like priority and vicinity must be considered.

Authors in [15] proposed a new multi-hop routing protocol named as SIMPLE protocol. The main principle of this scheme was based on a cost function, which elects a parent node after each round as relay node for the remaining child nodes. Election depends on the residual energy of individual nodes. Represented in [16] is a protocol termed as LAEEBA (Link Aware and Energy Efficient routing protocol for wireless Body Area network) which employed features of single-hop and multi-hop communication to ascertain the transmission of information from nodes to sink. Advantages of the LAEEBA protocol include path-loss efficiency and an enhanced throughput. An enhancement in network stability and functional life of nodes was also indicated by test findings.

Authors in [17] made an attempt to introduce a follower to the LAEEBA protocol, termed as Co-LAEEBA (Cooperative Link Aware and Energy Efficient routing protocol for wireless Body Area networks). Three kinds of sensor nodes are employed in both the protocols with both relying on relay nodes for data transmission. Data transmission is achieved by employing a cost function which ascertains the most viable route for this purpose. Routing is improved, and more effective use of energy is made by making use of cooperation.

Location tracking is one of the most widespread applications of WBASNs. WBASN's performance in relation to indoor localization scheme is represented in [18]. The proper placement of the wireless sensor nodes for a given area is emphasized in the said protocol. Information regarding location tracking is communicated by the sensor nodes placed in a given area.

Chan Hong Wang and his associates introduced a distributed WBASN intended to aid in medical supervision as illustrated in [19]. It consists of three levels. The purpose of the protocol was to observe the vital signs of a patient while also serving to cache the recorded data and share it once the information was required.

In [20], a clustering-based routing method intended for heterogeneous networks was proposed termed as enhanced developed distributed energy-efficient clustering.

The proposed routing technique is based on changing of cluster heads where the most suitable cluster head is selected on basis of election probability.

Researchers in [21] illustrate personal wireless hub (PWH). The personal health information (PHI) of the patient is identified and processed by biomedical sensors. The information so gathered is received by the sink for further processing and is eventually communicated toward the healthcare unit or hospital. Results indicate that data routed by the PWH is completely relevant and eligible. To make sure that privacy is observed, the data processed is kept secure.

In their introductory phase, WBANs were intended to observe and analyze different bodily factors and were normally perceived as active monitoring technology. Albeit recently, researchers have made attempts to alter WBANs' status from active technology to proactive technology. The functionality of the sensors was therefore increased significantly as instead of merely observing and evaluating the various factors, the sensors would also react in their own capacity during crucial situations and provide critical information in relation to the emergency. The new method was aptly termed as real-time biofeedback.

In [22], the primary concept and mechanism behind biofeedback control systems is illustrated. In addition to the above, the salient features integral to the composition and functioning of biofeedback systems were also brought under consideration. Previous notable advancements made in the field were also discussed in detail.

Researchers in [23] developed a new protocol termed as EENMBAN. The proposed protocol was path-loss-aware multi-hop scheme, which ensures minimum utilization of residual energy and maximum throughput.

23.3 Motivation

Several designs for WBAN protocols have been suggested in order to improve the quality of medical aid. Sensor nodes are utilized by WBANs for analyzing and accumulating information in relation to various bodily parameters. The data gathered is dispatched to the medical server through a sink. Energy consumption is a crucial factor as the energy available is restricted. The rate of data transmission shall also be taken into consideration. SIMPLE protocol operates on the basis of the multi-hop principle [15]. The major drawback of SIMPLE protocol is the considerable amount of energy lost while designating the parent node after the completion of every round. Another disadvantage of this protocol is its inability to counter path-loss issue effectively. LAEEBA protocol [16] operates by dispatching the accumulated information to the sink either directly or via sink nodes depending on how crucial the dispatched data is. In multi-hop communication data is processed by each node after being dispatched resulting in considerable delay which may inhibit the effectiveness of the protocol. The delay is further aggravated by an overcrowding of the nodes. Cost function method is subsequently employed by the

protocol as a means of thwarting the delay albeit at the cost of significantly higher energy consumption. Despite the protocol's attempts at decimating the delay by employing the cost function mechanism, the results were still not favorable.

EENMBAN succeeds the two protocols previously discussed. It differs from LAEEBA protocol in a few major aspects including its use of different path-loss models and its preference to not employ a cost function. Instead of using cost function to determine parent nodes, relay nodes that possess a higher level of residual energy at the inception are tasked with transmitting data between nodes and sink.

The primary objective of this paper is to assess the effect of a variation in the number of nodes deployed on the overall performance of the protocol.

23.4 Protocols Selected for Analysis

23.4.1 SIMPLE Protocol

In SIMPLE protocol information regarding the location of the sink node on the patient's body and location, energy status and node ID of each sensor node are shared between the sink node and the sensor nodes via transfer of information packages. In this manner, the sensor nodes are updated with the particulars of the sink node and other neighboring nodes.

For enhancement of throughput and greater efficiency, SIMPLE protocol selects a parent node during each round based on predetermined criteria. Cost function is calculated for all nodes based on their particulars and is shared with every node, and the appropriate node is selected as the parent node. Cost function is determined with the following formula:

$$C_{\text{func}}(n) = \frac{\text{dis}(n)}{E_{\text{residual}}(n)} \tag{23.1}$$

where C_{func} represents the cost function, n represents number of nodes, "dis" represents distance between individual nodes and sink, and E_{residual} represents residual energy.

Sensor nodes share collected data with the parent node within the time duration based on time division multiple access (TDMA). Sensor nodes remain in idle mode in the absence of any data-transmitting activities. Scheduling in this manner minimizes energy dissipation.

23.4.2 LAEEBA Protocol

Information regarding neighboring nodes, location of the sink node, and the routes leading to the sink is received by each node. Each node transmits information package carrying information in relation to node ID, location, and energy resources.

Cost function is calculated by LAEEBA protocol in an almost identical manner to the SIMPLE protocol. The only difference being the fact that LAEEBA protocol considers the square root value of the distance between individual nodes and sink as shown in the following equation:

$$C_{\text{func}}(n) = \frac{\sqrt{\text{dis}(n)}}{E_{\text{residual}}(n)} \tag{23.2}$$

Routes that encompass the fewest hops to the sink are favored to ensure the efficient use of energy. Where the information is of critical nature, all procedures are put on hold until the data is successfully received at the sink node. Additionally, direct communication is established between the nodes and the base station which minimizes delay unlike multi-hop communication. In multi-hop communication, data is processed by each intermediary node which results in considerable delay. Single-hop and multi-hop communication utilize different formulae for determination of the amount of energy consumed.

Path loss is a term used to refer to the deterioration of signal strength of an electromagnetic wave during its transmission toward the receiver. Communication systems generally used include Bluetooth, ZigBee, MICS, etc. Deterioration of performance may occur due to losses observed during communication.

Path loss encompasses all the issues commonly confronted in relation to waves interacting with surrounding objects during the communication process, often resulting in decrease in power density of an electromagnetic wave. In regard to WBANs, path loss is influenced by distance and frequency.

During the transmission of data to the sink or relay nodes, one of the two path-loss models will be employed, primarily selected based on the proximity of the communicating nodes.

23.4.3 EENMBAN Protocol

Active mode, sleep mode, and transient mode constitute the three phases of sensor nodes. Information is gathered subsequent to analysis and dispatched in active mode. The node enters sleep mode in the absence of any activity. The duration between switching from active mode to sleep mode and vice versa is termed as the "transient mode." "*T*" represents the aggregate time allotted, i.e., the accumulation of time spent in active mode and time spent in sleep mode, while "*N*" denotes the number of bits to be dispatched in the aforementioned time duration [23]. In light

of the above, the energy consumed by one bit of data is determined with the help of the following formula:

$$E_{\text{bit}} = \frac{P.M_{\text{act}}T.M_{\text{act}} + P.M_{s_p}T.M_{s_p}}{N} \tag{23.3}$$

In the above equation, E_{bit} denotes energy consumed for one bit of data. The power used during active mode is represented by $P.\ M_{\text{act}}$, while power consumed during sleep mode is represented by $P.M_{s_p}.\ T.\ M_{\text{act}}$ represents time used during active mode, where $T.M_{s_p}$ denotes time eclipsed during sleep mode. Peak-to-average ratio times transmission power divided by drain efficiency (ζ), therefore, represents power consumed while in active mode.

Due to the conductive nature of the human body and inclusion of different materials with varying dielectric constants and characteristics of impedance, in its composition, no system of communication is entirely free of loss. Systems with the lowest possibility of loss are, however, favored. The reduction in the power density of an electromagnetic wave is termed as "path loss." Deterioration in the overall performance of the system occurs due to path loss. Two varying path-loss models have been employed here.

The first model was utilized to determine losses in line of sight communication. The second was used for the exact purpose in non-line of sight communication. The path-loss models put in service in this protocol were developed based on the same functional principle as received signal strength indicator. In addition to the numerous calculations made for the three protocols in discussion, bit error rate was also determined for EENMBAN. The purpose of this additional calculation is to obtain an accurate estimate of the number of bits corrupted during transmission.

23.5 Results and Discussions

23.5.1 Node Density Analysis of SIMPLE

Node density analysis for SIMPLE protocol was performed by observing its performance using varying numbers of nodes. Two nodes were dedicated for transmitting data directly to the sink, while the remaining nodes followed the multi-hop mechanism. Five thousand rounds were observed for each set of nodes. While employing a set of 6 nodes, energy loss was encountered around the completion of 500 rounds, and the first node stopped functioning, while no further nodes were lost for the remainder of the 5000 rounds. Subsequently, the performance of a 7-node set was observed.

The periodic loss of nodes was much more significant during this set of rounds as 3 nodes were lost around the 500 round mark and a further 3 were lost after another 250 rounds bringing the amount of dead nodes at 750 rounds to 6. Four nodes stopped functioning after 500 rounds for the third round of experiments in which

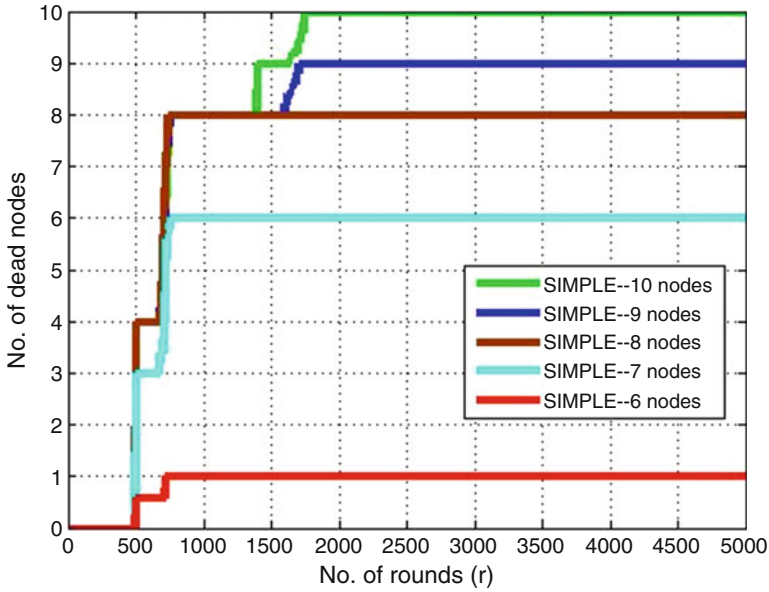


Fig. 23.2 Dead nodes after specified intervals in SIMPLE protocol

8 nodes were employed, while all the 8 nodes had expired after the completion of 750 rounds (Fig. 23.2).

For the set of 9 nodes, similar to the previous round, 4 nodes were lost after 500 rounds, and a further 4 expired after 750 rounds. The last node died at 1700 round mark. The set of 10 nodes produced results identical to the previous set of rounds in which 9 nodes were utilized, with the only exception being that the ninth node died around the 1400 round mark with the tenth node expiring at the 1700 mark. It is of particular notice that most nodes were lost after the completion of 750 rounds during all the sets. Loss was minimal after that stage with only the 9 node and 10 node set encountering losses after 750 rounds. It should be further noted that the best performance was produced by the 6 node set and the performance constantly and significantly deteriorated with the gradual increase in the number of nodes, resulting from the protocol's inability to encounter path-loss model. Another reason for the exacerbating performance was the continuous data transmission by the nodes throughout the simulation.

23.5.2 Node Density Analysis of LAEEBA

A similar node density analysis was undertaken for LAEEBA. Similar to the tests conducted for SIMPLE, groups of 6, 7, 8, 9, and 10 nodes were used. For the first set of rounds at around the 750 round mark, 3 nodes stopped functioning, while a

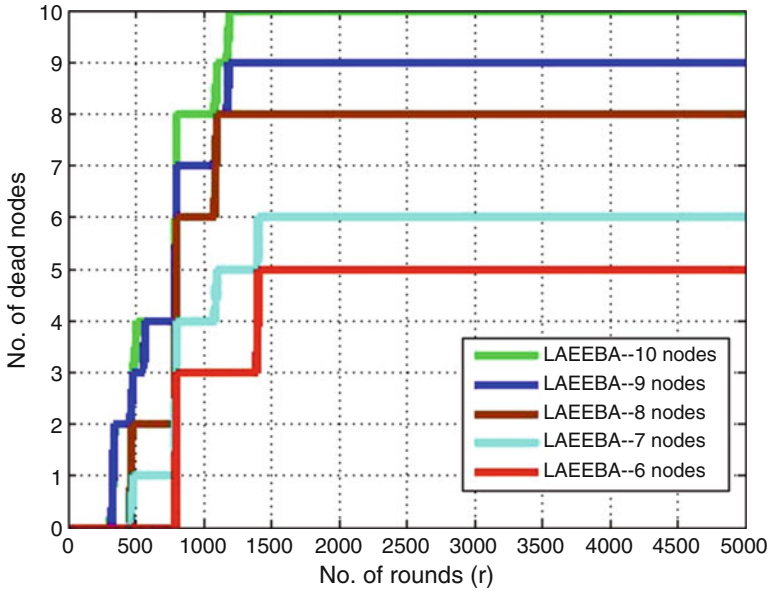


Fig. 23.3 Dead nodes after specified intervals in LAEEBA protocol

further 2 were lost after the completion of 1400 rounds bringing the total of expired nodes to 5.

For the next set of rounds in which 7 nodes were employed, the first node died at around the 500 round mark. A further 3 nodes were lost after the completion of 750 rounds. By the time 1400 rounds were completed, 2 more nodes had been rendered nonfunctional bringing the total number of dead nodes to 6. During the next set of rounds, a group of 8 nodes was employed. The first loss was encountered after the completion of 500 rounds when 2 nodes stopped functioning. A further 4 nodes expired after the completion of 750 rounds, while the remaining 2 nodes were lost after the completion of 1100 rounds (Fig. 23.3).

The first 2 nodes died during the next set of rounds after only 400 rounds. Another 1 lost after 500 rounds while the fourth node stopped functioning after 600 rounds. A further 3 nodes were lost at the 750 round mark, bringing the aggregate number of nodes lost after 750 rounds to 7. The remaining 2 nodes were lost after 1200 rounds. For the last set of rounds, a group of 10 nodes was evaluated. The results were almost identical to the last set of rounds, except for the fact that the total number of nodes lost after 750 rounds was 8 instead of 7. The remaining 2 nodes stopped functioning after 1200 rounds.

23.5.3 Node Density Analysis of EENMBAN

Node density analysis for EENMBAN produced significantly superior results as compared to the other two protocols. For the first set of rounds conducted for a 6-node group, no nodes were lost throughout the entirety of 5000 rounds (Fig. 23.4).

For the group of 7 nodes, the results were identical to the previous set of rounds with all the nodes still functional after the completion of 5000 rounds. Although no nodes were lost during the first two sets of rounds, there was insignificant loss of energy nonetheless. For the next set of rounds, a group of 8 nodes was utilized. The first loss was encountered after the completion of 1750 rounds, at which point 4 nodes stopped functioning. Three more nodes were rendered nonfunctional toward the end of the 5000 round cycle, at around the 4800 round mark.

For the next set of rounds, in which 9 nodes were used, no loss was encountered until the completion of 1750 rounds. Around this point in the cycle, 7 nodes were lost, while the remaining 2 nodes were lost at the 2000 round mark.

For the last set of rounds, a 10-node group was used. The first 2 nodes stopped functioning after the completion of 1500 rounds, while the remaining 8 nodes were lost after the completion of 1750 rounds.

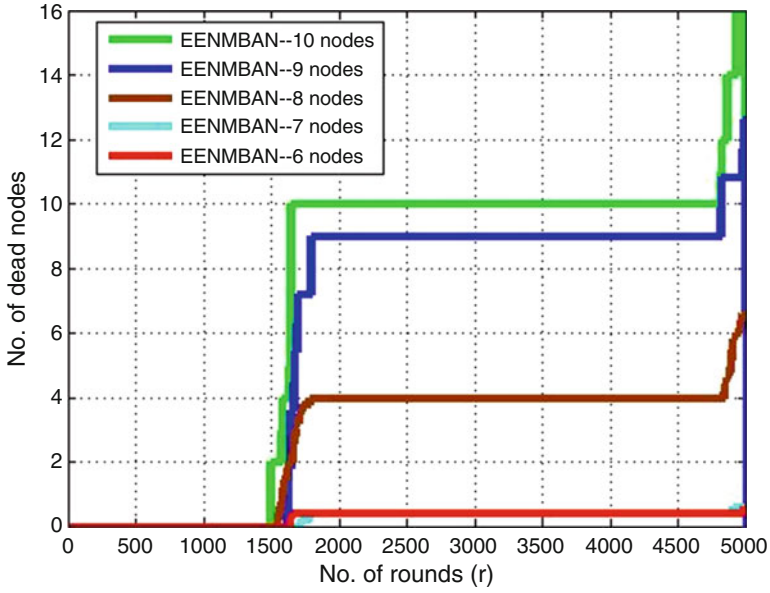


Fig. 23.4 Dead nodes after specified intervals in EENMBAN protocol

23.5.4 Throughput

Throughput represents the number of packets received at the base station after the completion of one round. The throughput of the three protocols was compared in order to gauge their performance. Similar to the previous simulations, groups of 6, 7, 8, 9, and 10 nodes were used.

For the 6-node group, LAEEBA fared better in comparison with the other two protocols with significantly superior throughput with SIMPLE and EENMBAN exhibiting an almost identical performance. For the 7-node group, LAEEBA and SIMPLE performed much better in comparison to EENMBAN with LAEEBA still registering a superior throughput than SIMPLE. For the third set of rounds, 8 nodes were employed for each protocol. EENMBAN was much better than SIMPLE and LAEEBA protocols in terms of throughput (Fig. 23.5).

In contrast to the previous two rounds, EENMBAN dwarfed SIMPLE and LAEEBA in terms of throughput displayed with the lagging protocols. Similar is the case for 9- and 10-node set, i.e., EENMBAN outperform both SIMPLE and LAEEBA by comparing their respective throughput values. However, LAEEBA performance was slightly better than SIMPLE protocol.

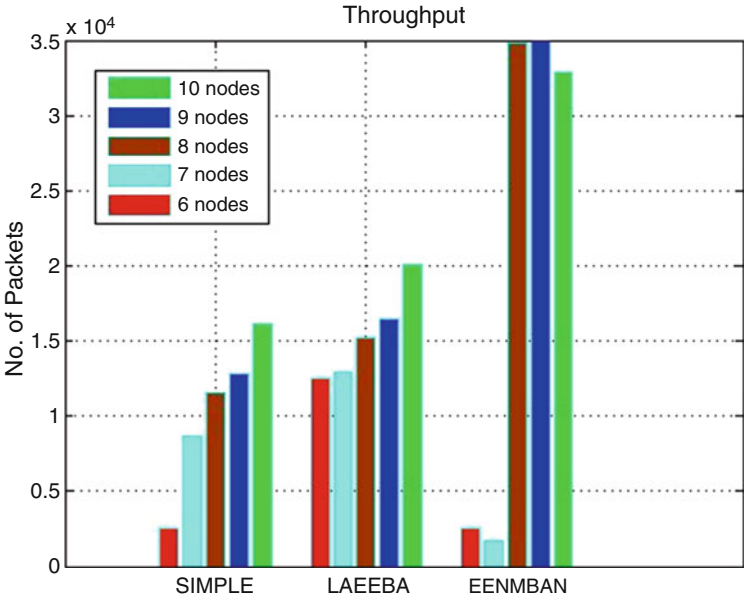


Fig. 23.5 Throughput comparison for various node densities

23.6 Conclusion

In this research, we have tried to present an overview of the working methodology of WBAN field, its applications, and various routing protocols designed for WBANs. What should be a suitable number of nodes to be deployed on a human body is still a challenging issue. We have considered three popular routing schemes of WBAN and presented an analysis with varying node deployments to judge their performance. The three schemes considered are SIMPLE, LAEEBA, and EENMBAN.

Results from the node density analysis indicated better performance by LAEEBA in comparison with SIMPLE for the 7- and 8-node groups in terms of stability period and network lifetime. However SIMPLE fared better than LAEEBA for the 6-, 9-, and 10-node groups. EENMBAN, however, produced significantly better results than both LAEEBA and SIMPLE for all the groups with no loss of nodes occurring until the completion of 1500 rounds in any set of rounds. Remarkably, no loss occurred in the 6- and 7-node groups. The nodes generally lasted much longer even after the first node expired.

However, considering throughput values of all three protocols for various sets of nodes, LAEEBA protocol showed best result for 6- and 7-node set, while EENMBAN throughput was much greater than the two protocols for the remaining set of nodes, i.e., 8-, 9-, and 10-node sets.

References

1. Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. In *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on* (p. 10). Piscataway, NJ: IEEE.
2. Khan, F., Bashir, F., & Nakagawa, K. (2012). Dual head clustering scheme in networks. In *Emerging Technologies (ICET), 2012 International Conference on* (pp. 1–5). Piscataway, NJ: IEEE.
3. Ari, A. A. A., Gueroui, A., Labraoui, N., & Yenke, B. O. (2015). *Concepts and evolution of research in the field of wireless sensor networks*. arXiv preprint arXiv:1502.03561.
4. Jan, M. A., Jan, S. R. U., Alam, M., Akhunzada, A., & Rahman, I. U. (2018). A comprehensive analysis of congestion control protocols in wireless sensor networks. *Mobile Networks and Applications, 23*, 1–13.
5. Sadiq, N., Shah, S. W., Ahmed, S., & Siddiqui, M. M. (2016). Towards an energy-efficient and throughput aware scheme for BANs. In *2nd International Conference on Emerging Trends in Engineering, Management and Sciences (ICETEMS-2016).*
6. Jan, M. A., Khan, F., Alam, M., & Usman, M. (2017). A payload-based mutual authentication scheme for Internet of Things. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.08.035
7. Khan, F., ur Rehman, A., Usman, M., Tan, Z., & Puthal, D. (2018). Performance of cognitive radio sensor networks using hybrid automatic repeat request: Stop-and-wait. *Mobile Networks and Applications, 23*, 1–10. https://doi.org/10.1007/s11036-018-1020-4
8. Alam, M., Ferreira, J., Mumtaz, S., Jan, M. A., Rebelo, R., & Fonseca, J. A. (2017). Smart cameras are making our beaches safer: A 5G-envisioned distributed architecture for safe, connected coastal areas. *IEEE Vehicular Technology Magazine, 12*(4), 50–59.

9. Wang, P., Hou, H., He, X., Wang, C., Xu, T., & Li, Y. (2015). Survey on application of wireless sensor network in smart grid. *Procedia Computer Science, 52*, 1212–1217.
10. Khan, F. (2014). Secure communication and routing architecture in wireless sensor networks. In *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)* (pp. 647–650). Piscataway, NJ: IEEE.
11. Alam, M., Trapps, P., Mumtaz, S., & Rodriguez, J. (2016). Context-aware cooperative testbed for energy analysis in beyond 4G networks. *Telecommunication Systems, 64*(2), 225–244. https://doi.org/10.1007/s11235-016-0171-5
12. Braem, B., Latre, B., Moerman, I., Blondia, C., Reusens, E., Joseph, W., Martens, L., & Demeester, P. (2007). The need for cooperation and relaying in short-range high path loss sensor networks. In *Sensor Technologies and Applications, 2007. SensorComm 2007. International Conference on* (pp. 566–571). Piscataway, NJ: IEEE.
13. Jan, M., Nanda, P., Usman, M., & He, X. (2017). PAWN: A payload-based mutual authentication scheme for wireless sensor networks. *Concurrency and Computation: Practice and Experience, 29*(17), e3986.
14. Alam, M., Albano, M., Radwan, A., & Rodriguez, J. (2013). CANDi: Context-aware node discovery for short-range cooperation. *Transactions on Emerging Telecommunications Technologies, 26*(5), 861–875. https://doi.org/10.1002/ett.2763
15. Chen, B., Varkey, J. P., Pompili, D., Li, J. K. J., & Marsic, I. (2010). Patient vital signs monitoring using wireless body area networks. In *Bioengineering Conference, Proceedings of the 2010 IEEE 36th Annual Northeast* (pp. 1–2). Piscataway, NJ: IEEE.
16. Rashidi, P., & Mihailidis, A. (2013). A survey on ambient-assisted living tools for older adults. *IEEE Journal of Biomedical and Health Informatics, 17*(3), 579–590.
17. Nadeem, Q., Javaid, N., Mohammad, S. N., Khan, M. Y., Sarfraz, S., & Gull, M. (2013). Simple: Stable increased-throughput multi-hop protocol for link efficiency in wireless body area networks. In *Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013 Eighth International Conference on* (pp. 221–226). Piscataway, NJ: IEEE.
18. Ahmed, S., Javaid, N., Akbar, M., Iqbal, A., Khan, Z. A., & Qasim, U. (2014). LAEEBA: Link aware and energy efficient scheme for body area networks. In *Advanced Information Networking and Applications (AINA), 2014 IEEE 28th International Conference on* (pp. 435–440). Piscataway, NJ: IEEE.
19. Ahmed, S., Javaid, N., Yousaf, S., Ahmad, A., Sandhu, M. M., Imran, M., Khan, Z. A., & Alrajeh, N. (2015). Co-LAEEBA: Cooperative link aware and energy efficient protocol for wireless body area networks. *Computers in Human Behavior, 51*, 1205–1215.
20. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2013, November). Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network. In *High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC), 2013 IEEE 10th International Conference on* (pp. 1400–1407). Piscataway, NJ: IEEE.
21. Javaid, N., Qureshi, T. N., Khan, A. H., Iqbal, A., Akhtar, E., & Ishfaq, M. (2013). EDDEEC: Enhanced developed distributed energy-efficient clustering for heterogeneous wireless sensor networks. *Procedia Computer Science, 19*, 914–919.
22. Abbasi, A. A., & Younis, M. (2007). A survey on clustering algorithms for wireless sensor networks. *Computer Communications, 30*(14), 2826–2841.
23. He, D., Chen, C., Chan, S., Jiajun, B., & Zhang, P. (2013). Secure and lightweight network admission and transmission protocol for body sensor networks. *IEEE Journal of Biomedical and Health Informatics, 17*(3), 664–674.

Chapter 24
Research Challenges in the Internet of Things (IoTs)

Seema Begum, Yao Nianmin, Syed Bilal Hussain Shah, Inam Ullah Khan, and Satish Anamalamudi

Abstract In the age of the technology and in the field of Computer Networking, devices integrated with the Internet of Things (IoT) resulted in a variety of popular E-Health, E-Commerce and E-Home. The Internet of Things will be next revolutionary term in the today internet. An important function of the IoT is to create various types of technologies, standards and then to integrate them. Today, the capacities of IoT are improving by establishing security for both small and large applications. To help and determine the direction of future research, IoT security challenges and privacy issues will be highlighted in this chapter. The chapter analyzes compares and consolidates the existing research, presents new findings and discusses innovations in the security of the IoT. The challenges in this chapter must be addressed, if the full potential of IoT is to be realized.

S. Begum · Y. Nianmin
School of Computer Science and Technology, Dalian University of Technology, Dalian, P.R. China
e-mail: lucos@dlut.edu.cn

S. B. H. Shah (✉)
School of Information and Communication Engineering, Dalian University of Technology, Dalian, P.R. China
e-mail: bilalshah@mail.dlut.edu.cn

I. U. Khan
Isra University, Islamabad Campus, School of Engineering and Applied Sciences (SEAS), Islamabad, Pakistan

S. Anamalamudi
Faculty of Computer Science and Engineering, SRM University, Chennai, India

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_24

24.1 Introduction

To begin let us define the Internet of Things (IoT). "The Internet of Things (IoT) is the network of physical objects-devices, vehicles, buildings and other items that are embedded with electronics, software, sensors and network connectivity, which enables these objects to collect and exchange data."

The IoT is a new and evolving concept as shown in Fig. 24.6 the investment details that is expected to be widely used in future [1]. The IoT allows the Internet to connect with applications and users by first connecting with objects. The IoT can be implemented in various domains such as retail, agriculture, home, schools and transportation, which can be accessed remotely with the use of the internet. IoT is also able to act without the human involvement in the system. The concept of the IoT is related to the remote sensor networks and remote personal area networks. Communication in IoT is through computing machines and sensors embedded in the systems. The goal of IoT is to provide a good infrastructure based on all things present in the world and also to inform users about the state of things. The evolution of the IoT will be evolving along with communication between machines. This machine-to-machine communication will occur in a variety of domains, such as smart cities, smart homes, smart schools and smart agriculture. Basically, IoT products operate on old fashioned and closed embedded operating system software. Network access needs to be restricted to improve the security terms of the IoT. The segment of the network should monitor for potential traffic and improper activities, then take action if any problem occurs. Many companies have embraced IoT technologies for their potential impact. According to Cisco, there will be 50 billion objects (i.e., devices embedded with technology) connected to the IoT by 2020, as Fig. 24.1 illustrates the world market [1].

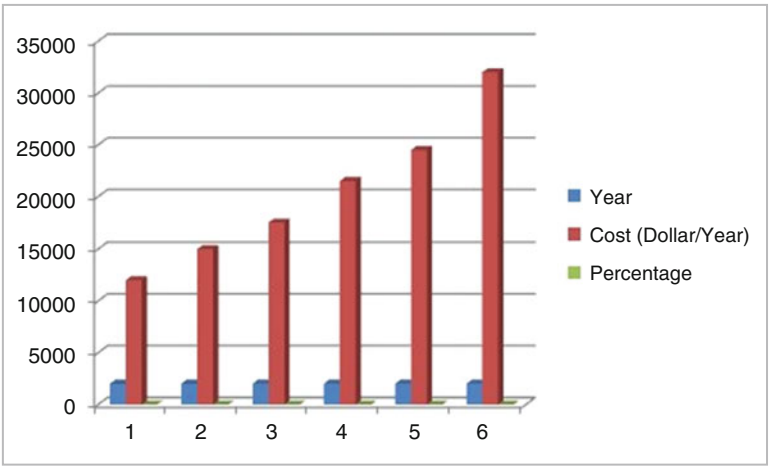


Fig. 24.1 World market for integrated equipment in IoTs

Because of this, privacy has been a hot topic in the research on the different types of technology that enable IoT.

This chapter was written to help internet companies navigate the perils and promises of IoT. We will discuss the unique aspects of the IoT in relation to the informational technology of the internet.

The rest of the chapter describes the resources needed for IoT technology based on the location where it is used. Each section focuses on security and related challenges. The topics discussed include IoT in supermarket Agriculture, schools the home, and traffic management.

24.2 IoT in Super Market

Point of sale (POS) systems are used in the super markets to provide powerful features such as warehouse hosting interfaces, enhanced reporting, file maintenance and inventory control. POS software in supermarkets is used for stock maintenance, expiry, provisioning, reordering wastage and return management. However, these POS systems have some problems including insufficient customization, intensive human resources and inefficient settlement. Currently, many super markets are using IoT technology.

The technology includes radio Frequency Identification (RFID), as shown in Fig. 24.2, smart shopping guides, self-checkout, logistics tracking, wireless and ad-hoc communication with automatic identification, and mobile advertisement [2].

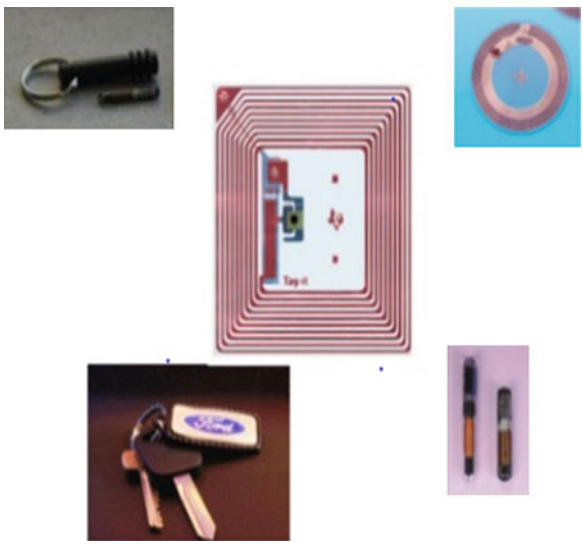


Fig. 24.2 Different designs of RFID cards

24.3 Challenges of Supermarket IoT

At present, manual stock frameworks are used for stocking, and buying items, which are then recorded in a book. Such a system is prone to errors and may lack information needed for proper operations. Data may not be appropriately recorded or managed. From the wholesaler to retailer information on charges, tickets, vouchers, and receipts are recorded in books; however, this system may not facilitate optimal operations. Thus, it is troublesome to prepare, overhaul and manage.

The issues associated with these systems include the following

1. Time consumption
2. Physical counts
3. Supply requests
4. Lack of automatic maintenance
5. Lack of proper management

24.4 IoT in Agriculture

The world of agribusiness is experiencing industrialization, but it is imperative to also to create cooperation within the industry for advancement throughout the world. Rural farmers have been concerned with improvements to advance agrarian community and increase profits.

After many years of hard work positive outcomes have been seen in horticulture framework advancements. These frameworks have the benefits of collecting and tracking rural data. For example, more emphasis has been placed on equipment than programming, without any data to address the production of needs of farmers. Furthermore, available data are not adequately used by ranchers, so the impact of data on horticulture, agriculturists and rural ranches has been minimal.

To change this situation and quickly improve farming conditions; it is important to develop a horticultural cloud data that use IoT and RFID innovations [3].

An environmental control system could incorporate water quality monitoring, programmed water quality, accurate compost treatments, soil quality and moisture monitoring, and environmental condition (e.g., air, light) monitoring. A rural asset control subsystem could incorporate an intelligent nursery that is able to program and maintain a uniform temperature, control a water system that can dispense and converse water, monitor of contamination and vermin, monitor plant and animal health, and ensure the quality product [4–6].

24.5 Different Challenges in IoT

Some of the major difficulties that should be considered when designing an IoT based system including mechanical, social, legal, financial and business issues, with an end goal to get wide acceptance from users. Guidelines and interoperability standards are critical to create markets for new advancements. When gadgets by different manufacturers are not compatible, interoperability is more troublesome, and requires additional efforts to incorporate the different standards. Furthermore, customers may tend to only purchase from a single manufacturer to avoid these comparability issues if user cannot easily exchange information when they replace a gadget with another from a different manufacturer, they will lose any benefits that occurred from aggregating their information for some time. Security allows for effective usage of the IoT with the help of inexpensive devices/gadgets to connect one or many device together. However, these additional layers of programming, middle ware, APIs, machine-to-machine communication results in more complicated setup and new security dangers. Manufactures need to address these issues with strategy driven ways to improve security and provisioning. With such a variety of players required with the IoT, there will undoubtedly be turf wars as legacy organizations attempt to protect their restrictive frameworks and as defenders of open frameworks attempt to create new principles. New models may be developed in light of requirements controlled by gadget class, control prerequisites, abilities and usage. This presents opportunities for stage sellers and open-source promoters to contribute and influence future principles [7].

24.6 IoT in Schools

The fast progression of information and Communication technologies has led to IoT advancement in schools as well [8]. School campus may be composed of many buildings constructed for different purposes. Each block of building has separate systems for air conditioning, heating, ventilation and elevators, among others as shown in Fig. 24.3. To manage these systems, IoT plays a major role in maintain their correct working order. Sensing and control units allow for better maintenance. For example RFID units can monitor the air ventilation by detecting the surrounding climate and environmental changes. If any changes to the ventilation systems are required, then the information can be automatically transmitted to the information-gathering unit that is located in each block, i.e. the wireless central control unit. Depending on the information received, the control unit may increase or decrease the air conditioning Supply [9].

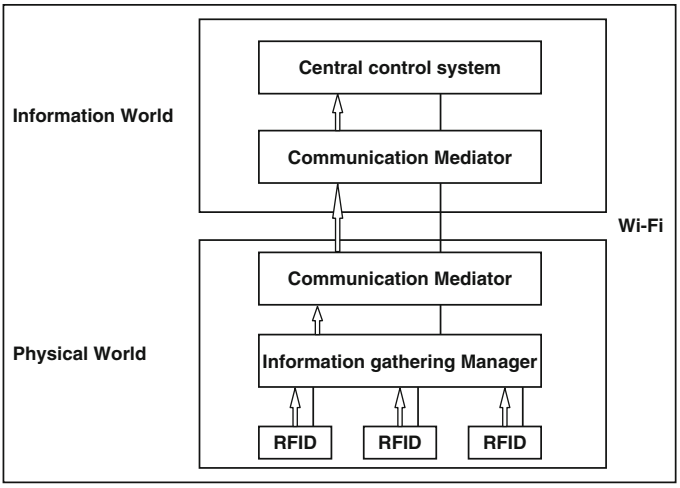


Fig. 24.3 School facilities system

24.6.1 Challenges of School-Based IoT

With the IoT, school can provide instructive results through richer learning experiences and increase access to knowledge for students [10, 11].

An increasing number of students are learning with the assistance of a remote gadget, whether it is a table brought from home or a school-issued laptop. Online lessons can also be arranged to include captivating content. However, these devices may "crash" outdated web systems in schools. To prepare, schools must upgrade to secure and fast remote systems that can handle the data transmission from complex projects being run on a large number of gadgets.

This preparation will pay off in spades. With e-learning applications, students can work at their own pace, which allows the teacher to provide one-on-one instruction to students who most require it. In addition, evaluations can be more consistent, less manual and less time-consuming. Teachers no longer need to review each examination or feed Scranton sheets into a machine. Finally, when associated with the cloud, these e-learning advancements can collect information on student progress, which can be used to enhance lesson plans for subsequent academic years [12].

24.6.1.1 Enhanced Operational Efficiency

Instructive organizations are included many moving parts. So as to prevail at what they do, they should have the capacity to monitor understudies, staff and assets; all while holding costs in line. This is conceivable by utilizing empowering

advancements that can without much of a stretch monitor individuals, resources and exercises. Beforehand tricky assets, for example, projectors or lab gear—can be outfitted with RFID peruses so that their whereabouts are unmistakable at all circumstances. Ongoing deceivability implies instructors no longer need to invest significant energy searching for these things and can rather concentrate on more critical errands like educating and arranging educational module. Furthermore, teachers can screen the state of their assets progressively so that if need be, things can be supplanted with negligible disturbance to the school day. GPS beacons can guarantee that understudies are represented progressively, minimizing tedious exercises like recording participation. With RFID prepared rucksacks, understudies can be consequently checked in as they board the transport. Likewise, the multiplication of brilliant ID cards and wristbands implies understudies can be naturally checked "present" when they stroll through the classroom entryway. With portable registering arrangements, operational barricades can be managed continuously. A support laborer who discovers a broken candy machine can utilize a handheld gadget to advise school authorities of the issue arrange the parts required as well as demand extra repair administrations—while in the field.

24.6.1.2 More Secure Campus Designs

School authorities are under expanded weight to guarantee their grounds are safe. A surge in school crises in the course of the most recent quite a long while, alongside the developing feelings of trepidation over harassing and savagery, mean it's more critical than any time in recent memory to protect understudies. The IoT's capacity to track items, understudies and staff, what's more, to interface gadgets crosswise over campuses brings another level of security to establishments.

A GPS-empowered transport framework implies that transport courses can be followed, so that guardians and chairmen can know where a given transport is at any given time. Notwithstanding making the school travel more secure for understudies (and significantly less unpleasant for guardians), understudies can be advised when the transport is close to their pickup area; not any more sitting tight outside for a late transport. ID cards and wristbands permit instructive associations to store the last-known area of an understudy or guest, making a difference to guarantee the ideal individuals are getting to the correct territories on grounds. They additionally empower cashless installments at the school cafeteria or grounds store, which makes a more streamlined exchange and can possibly demoralize tormenting and burglary. At long last, the meeting of grounds correspondences permits staff to respond all the more rapidly in a crisis circumstance. By associating portable workstations, cell phones and two-way radios, staff can in a split second talk, message or send an email to some other gadget in the system. For instance, a security monitor who spots a battle can tell instructors and chairmen promptly, with one straightforward activity. Presently, can come right away, and an acceleration of brutality can be maintained a strategic distance.

The IoT stands to significantly change the way organizations work, ensuring important resources and improving understudy learning at each level. Notwithstanding the quick advantages plot above, instructive establishments can tackle long haul esteem from these advancements by investigating the subsequent information to better arrangement asset portion, educational module and security methodology in the years to come. Challenges and Open Issues.

24.7 IoT in the Home

IoT applications are available in the market for consumer needs. IoT technology is an emerging innovation for society that will change the ways that consumers interact with other markets, such as energy, health, and transportation.

Implementation of this technology in the home will be described in this section, along with its applications, security, and potential needs of users [13, 14].

The design, installation, and setup of a professional smart home system are available only after smart electronic appliances have been integrated into the home. As such, the IoT at home is likely to be added piece by piece as the need arises. However these systems provide good insights energy savings, reducing the cost of the home improving efficiency. The functioning of this technology in the home can run in the background or foreground. The background activity of the home, can automatically process everyday tasks in a smart energy system. For example, it can adjust heating levels, by of sensing the people present in the home. When more heat is required, the energy consumed by all devices is recorded and calculated for each device separately, with approximate billing cost provided.

Security and safety can be controlled by users' smart phones. The system can also monitor for and alert users about unwanted behavior. Smoke detectors can be remotely monitored for continuous connection: the customer can remotely verify that devices are receiving powered and are turned on. Connected appliances will be operating in the foreground, with their performance increased based on previous usage. The system can provide safety and security for home that is connected with the IoT technology. When integrated into the home, this system can provide a fully automated process to control the home a true smart home as Fig. 24.4 clearly shows [15].

24.7.1 Challenges of Home-Based IoT

IoT manufacturers can demonstrate their commitment to buyers by designing and building trustworthy devices. This technology can create an advantage over other products by increasing the security and safety of users. They can also create an effective process and provide a positive customer experience that meets users' needs.

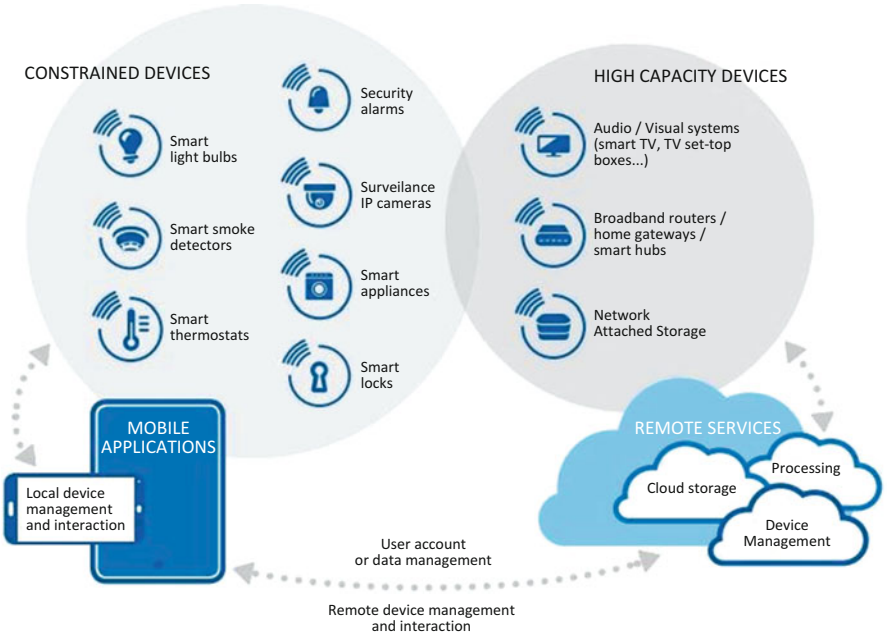


Fig. 24.4 Smart home system

24.8 IoT in Traffic Management Systems

The IoT plays a major role in intelligent traffic information systems by predicting traffic flow conditions, current traffic operations and future traffic flows. This traffic system allows drivers to find optimal routes to reduce their travel time. IoT technology provides additional benefits for an intelligent traffic system, such as high reliability, improved traffic conditions, information weather conditions, between traffic safety, reduced traffic management costs and less traffic jam. An IoT based traffic management system can be intelligent to collect of all traffic related information to support the processing and analysis of traffic information. Such a traffic system uses a number of different devices, including a global positioning system, infrared sensors, laser sensors and RFID sensors [16–32].

An intelligent traffic management system using the IoT consists of three layers: As shown in Fig. 24.5.

- Application layer
- Network layer
- Acquisition layer

Application Layer	Intelligent Traffic Management	Intelligent Driver Management	Information Collection & Monitoring	Information Services
Network Layer	Internet	WiFi, 3G/4G	WiMax	GPS, GPRS
Acquisition Layer	RFID	RFID Reader	WSN	Intelligent Terminals

Fig. 24.5 The framework of the intelligent traffic management system

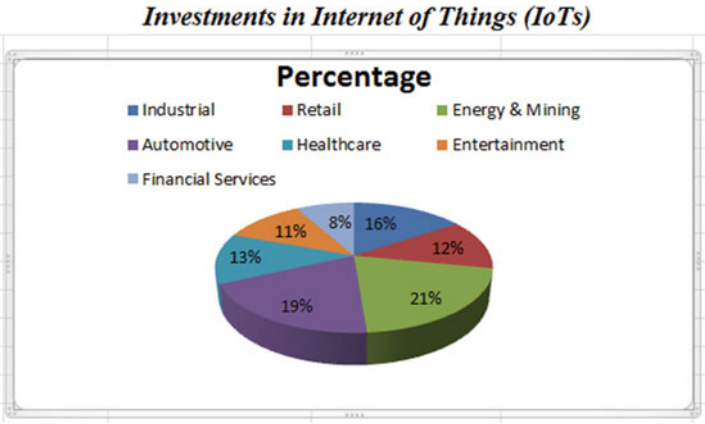


Fig. 24.6 Companies wants to invest in IoTs

24.8.1 Challenges of IoT-Based Traffic Management Systems

Due to the mobility of devices, radio frequency link variability and intermittent connectivity, the mobile devices on the IoTs may have difficulty connecting other devices on a network. For example, internet-connected cars are required to receive and send data at different locations of gateway sensor nodes. The cars need to keep the information while changing locations. To do this, IoT network paradigms should incorporate concepts from delay-tolerant networks and mobile ad-hoc networks [8, 16] (Fig. 24.6).

24.9 Conclusion

This paper has discussed IoT emerging technology in a variety of locations, where people work and study. The benefits of these technologies were summarized. When implemented correctly, they will efficiently and effectively improve the lifestyles of

the user and provide benefits for society as whole. The chapter also described the security issues and challenges associated with applications integrated in IoT. Smart technology based on the IoT has great potential. By ensuring the integration of safety and security features, manufacturer can increase the confidence of consumer while advancing society.

References

1. Archive.org. (2016). *Full text of "International Journal of Science and Research (IJSR)"*. [online] Retrieved December 26, 2016, from https://archive.org/stream/MTMwOTEzMDI/MTIwMTMzNg==_djvu.txt
2. Dlodlo, N., & Kalezhi, J. (2015). *The Internet of Things in agriculture for sustainable rural development*. [online] Retrieved December 26, 2016, from https://www.researchgate.net/publication/277713549
3. Garg, G., Goyal, D., Aggarwal, H., Baindail, K., & Verma, G. (2016). Controlling home appliances in IOT environment. *International Journal of Smart Home, 10*(8), 11–18.
4. Hongyan, L. (2015). Design and realization of smart home terminal applications based on IOT technology. *International Journal of Smart Home, 9*(8), 123–132.
5. http://citeseerx.ist.psu.edu/. (2016). *Intelligent traffic information system based on integration of Internet of Things and agent technology*. [online] Retrieved December 26, 2016, from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.695.2856&rep=rep1&type=pdf
6. https://www.uio.no. (2016). *RFID and IOT: An overview*. [online] Retrieved December 26, 2016, from https://www.uio.no/studier/emner/matnat/ifi/INF5910CPS/h10/undervisningsmateriale/RFID-IoT.pdf
7. Iot.ieee.org. (2016). *Research challenges in the internet of mobile things - IEEE Internet of Things*. [online] Retrieved December 26, 2016, from http://iot.ieee.org/newsletter/march-2016/research-challenges-in-the-internet-of-mobile-things.html
8. Jain, D., & Krishna, P. (n.d.). *A study on Internet of Things based applications*. [online] Retrieved December 26, 2016, from https://arxiv.org/ftp/arxiv/papers/1206/1206.3891.pdf
9. Journal, R. (2016). *What would be the best way for a local supermarket to transition to RFID technology?*. [online] Rfidjournal.com. Retrieved December 26, 2016, from http://www.rfidjournal.com/blogs/experts/entry?11504
10. Kim, W. (2016). The business model of IoT information sharing open market for promoting IoT service. *Journal of the Korea Society of IT Services, 15*(3), 195–209.
11. Lin, H., & Bergmann, N. (2016). IoT privacy and security challenges for smart home environments. *Information, 7*(3), 44.
12. Mehta, A., & Patel, S. (2016). IoT based smart agriculture research opportunities and challenges. *International Journal for Technological Research in Engineering ISSN (Online), 4*(3), 2347–4718. [online] Retrieved December 26, 2016, from http://www.ijtre.com/images/scripts/2016040325.pdf.
13. Rahul, G., & Patel, S. (2016). *A review of smart shopping systems*. [online] https://www.irjet.net. Retrieved December 26, 2016, from https://www.irjet.net/archives/V3/i5/IRJET-V3I5441.pdf
14. Shiryaev. (2016). *RFID technology and Internet of Things*. [online] Slideshare.net. Retrieved December 26, 2016, from http://www.slideshare.net/rushtek/rfid-and-internet-of-things
15. Vujovic, V., & Maksimovic, M. (2015). *The impact of the 'Internet of Things' on engineering education*. University of East Sarajevo Lukavica, Bosnia and Herzegovina. [online] Retrieved December 26, 2016, from http://www.citethisforme.com/cite/journal
16. Alam, M., Trapps, P., Mumtaz, S., & Rodriguez, J. (2016). Context-aware cooperative testbed for energy analysis in beyond 4G networks. *Telecommunication Systems*. https://doi.org/10.1007/s11235-016-0171-5

17. Khan, F., Rahman, F., Khan, S., & Kamal, S. A. (2018). Performance analysis of transport protocols for multimedia traffic over mobile Wi-Max network under Nakagami fading. In *Information technology-New generations* (pp. 101–110). Cham: Springer.
18. Alam, M., Albano, M., Radwan, A., & Rodriguez, J. (2013). CANDi: Context-aware node discovery for short-range cooperation. *Transactions on Emerging Telecommunications Technologies, 26*(5), 861–875. https://doi.org/10.1002/ett.2763
19. Khan, F., & Nakagawa, K. (2013). Comparative study of spectrum sensing techniques in cognitive radio networks. In *2013 World Congress on Computer and Information Technology (WCCIT)* (pp. 1–8). IEEE.
20. Zebra Technology. (n.d.). *How the Internet of Things is transforming education*. [online] Retrieved December 26, 2016, from https://www.zebra.com/ap/en.html
21. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2014). PASCCC: Priority-based application-specific congestion control clustering protocol. *Computer Networks, 74*, 92–102.
22. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2015, August). A Sybil attack detection scheme for a centralized clustering-based hierarchical network. In *2015 IEEE Trustcom/BigDataSE/ISPA* (Vol. 1, pp. 318–325). IEEE.
23. Khan, F. (2014, May). Fairness and throughput improvement in multihop wireless ad hoc networks. In *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)* (pp. 1–6). IEEE.
24. Jan, M. A., Nanda, P., He, X., Tan, Z., & Liu, R. P. (2014, September). A robust authentication scheme for observing resources in the internet of things environment. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 205–211). IEEE.
25. Jan, M., Nanda, P., Usman, M., & He, X. (2017). PAWN: A payload-based mutual authentication scheme for wireless sensor networks. *Concurrency and Computation: Practice and Experience, 29*(17).
26. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2013, November). Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network. In *2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC)* (pp. 1400–1407). IEEE.
27. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2018). A Sybil attack detection scheme for a forest wildfire monitoring application. *Future Generation Computer Systems, 80*, 613–626.
28. Jan, M. A., Nanda, P., & He, X. (2013, June). Energy evaluation model for an improved centralized clustering hierarchical algorithm in WSN. In *International Conference on Wired/Wireless Internet Communication* (pp. 154–167). Berlin, Heidelberg: Springer.
29. Usman, M., Jan, M. A., & He, X. (2017). Cryptography-based secure data storage and sharing using HEVC and public clouds. *Information Sciences, 387*, 90–102.
30. Usman, M., Jan, M. A., He, X., & Nanda, P. (2016, August). Data sharing in secure multimedia wireless sensor networks. In *2016 IEEE Trustcom/BigDataSE/ISPA* (pp. 590–597). IEEE.
31. Jan, M. A., Usman, M., He, X., & Rehman, A. U. (2018). SAMS: A seamless and authorized multimedia streaming framework for WMSN-based IoMT. *IEEE Internet of Things Journal*. https://doi.org/10.1109/JIOT.2018.2848284
32. Jan, M. A., Jan, S. R., Usman, M., & Alam, M. (2018). State-of-the-art congestion control protocols in WSN: A survey. *IoT EAI*. https://doi.org/10.4108/eai.26-3-2018.154379

Chapter 25
Managing and Processing Information in the Internet of Things-Based Smart City Environment Using Big Data Analytics

Sarah Kaleem, Muhammad Talha, and Muhammad Babar

Abstract The extensive growth of the Internet of Things (IoT) is giving the direction toward the smart cities. The smart city is preferred because it improves the living standard of the people of the society and provides quality in the services. These services are parking, health, transport, water, power, environment, and so forth. The assorted environment of IoT and smart city is challenged by data processing, decision-making, and notification management. In this research article, specific architecture is proposed for data processing and notification management in the smart city environment using IoT. The processing is carried out with Hadoop server using authentic dataset, and notification management is done based on ontology.

25.1 Introduction

The inventiveness of Internet of Things (IoT) has been advanced with the wide expansion of the smart devices, which is the backbone of the web nowadays [1, 2]. In recent times, the IoT is the center of researchers due to the smart devices and the resulting applications of smart city [3–5]. The smart city idea started to improve and optimize the quality of services provided to the citizens [6]. To manage huge data in the smart city environment, data analytics is the key. In addition, several individual works are presented to cover different smart city services [7, 8].

S. Kaleem (✉)
Iqra National University, Peshawar, Pakistan

M. Talha
Iqra University, Islamabad, Pakistan

M. Babar
National University of Sciences and Technology, Islamabad, Pakistan
e-mail: babar.phd@students.mcs.edu.pk

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_25

Thereupon, processing data and managing notification are the basic needs of smart city. For instance, cameras or sensors in a particular area collect the information which is compared with threshold based on processing, and corresponding people are notified accordingly. Processing and analytics in the smart city face a number of challenges such as interoperability issues and different formats of data, and anomalies like noise are found. In order to remove the said issues, preprocessing is required [9, 10]. In this research article, data analytics and notification management are incorporated to propose architecture for smart cities. The proposed architecture is competent for data processing, intelligent decision-making, and user-centric notification management. Hadoop is used for the processing of data in this work. The processing is followed by intelligent decision generation associated with the smart city notification management corresponding to the decisions that are executed.

25.2 Literature Review

The development of smart cities draws the attention of the researchers to work on diverse solution to demonstrate the design for smart city using IoT. Big data analytics plays a very important role in the smart city planning [11]. Different proposals are proposed to overcome the issues with regard to smart cities and IoT [12–15, 21]. Proposals are also found in literature for demonstrating the combination of social network and IoT in the last decade [11, 16, 17]. To hold an enormous data and provide services based on IoT, different proposals are given [18]. IoT uses different tools for analyzing data, for instance, NoSQL, MapReduce, Cassandra, etc. It is observed that many challenges that are to be handled, such as preprocessing and communication for notifications in a smart city. Therefore, we find out the necessities for an inventive communication model for smart city. The data analytics involves many varied stages such as data recording, data cleaning, data integration, data aggregation, data representation, and data analysis. These may be faced with many challenges such as data format challenges, separation of the valuable and helpful data, data heterogeneity, missing data, and timely processing.

To deal with aforementioned issues, the architecture proposed for smart city planning [20, 22] and also security is taken into consideration in proposal [22], but they have inefficient processing in terms of time.

25.3 Proposed Architecture

The proposed architecture is elaborated in detail in this section. The rationale of this architecture is to have efficient data processing and decision-making with proper notification management for smart city. The proposed system is connected to smart societies including smart environment, smart traffic, smart weather, smart health, and so forth. These societies are powered by a variety of communica-

tion technologies such as ZigBee, Bluetooth, Wi-Fi, and 3G/4G networks. Data collection is carried out by the corresponding smart city society. The proposed architecture is basically composed of two different units: (1) data processing and (2) decision-making and notification management. The detail description of these units of proposed architecture is given below.

25.3.1 Processing Unit

This unit is responsible for processing the data and composed of (1) data preprocessor and (2) Hadoop server shown in Fig. 25.1. Before the actual processing, we perform preprocessing. The preprocessing is carried out to remove and resolve the issue such as out-of-range, impractical data, and missing values. The preprocessing includes data clustering, normalization, and filtration. The clustering is performed using divide-and-conquer approach, normalization is performed using min-max technique, and data filtration is performed using Kalman filter to remove noise. The data processing is performed using Hadoop two nodes' cluster with MapReduce mechanism and Java programming.

The Hadoop is responsible for the actual processing which uses MapReduce. The MapR works in (1) mapping process to transform one dataset values to another set of data and (2) reducing processes which combine the data and results and reduce quantity. The proposed architecture makes use of HDFS to make possible the data storing and processing easily. The storage requirement of the proposed smart city architecture is assisted by HDFS, which is the main storage of Hadoop. Since the storage of HDFS is distributed, it supplements the MapReduce implementation on smaller subsets of larger data cluster.

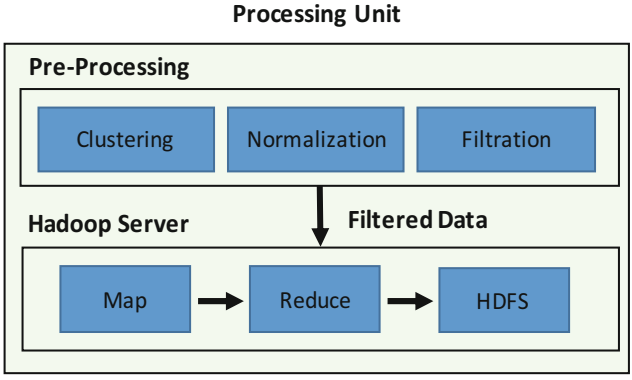


Fig. 25.1 Processing unit of proposed architecture

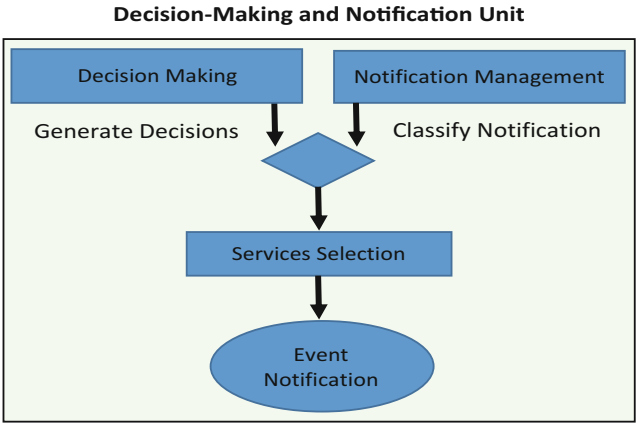


Fig. 25.2 Decision-making and notification of proposed architecture

25.3.2 Decision-Making and Notification Unit

This is responsible for performing the decision-making and notification management. It is used to generate the decisions and classify the events. The decision-making server describes the decision according to an ontology that is used to unicast the events. The corresponding society performs service selection procedure to distinguish the high and low events. The service selection unit generates the respective event and broadcasts to the implanted notification component which includes departmental, service, and subservice level. Figure 25.2 represents the overall working of this tier. Let us suppose the traffic data is processed using proposed architecture and the traffic congestion is found on the road at a specific lane A. The decision is taken, and event is produced and sent to road congestion control department of the smart traffic society to notify the corresponding users to opt a particular identified lane Y by system to avoid and control congestion.

25.4 Analysis and Results

The implementation is carried out with core i5 processor with 8GB RAM using Hadoop two nodes' cluster on Ubuntu (4GB RAM is devoted to each node) and MapReduce with Java programming. The authenticated and reliable datasets are acquired to validate the proposed architecture. To consider the fire detection situations, the data of temperature of California state in the USA is taken from the National Climatic Data Center [19]. The center of analysis is to evaluate the proposed work based on already specified thresholds. The threshold for fire detection is 45. Every time the data amount at a specific time goes beyond the normal

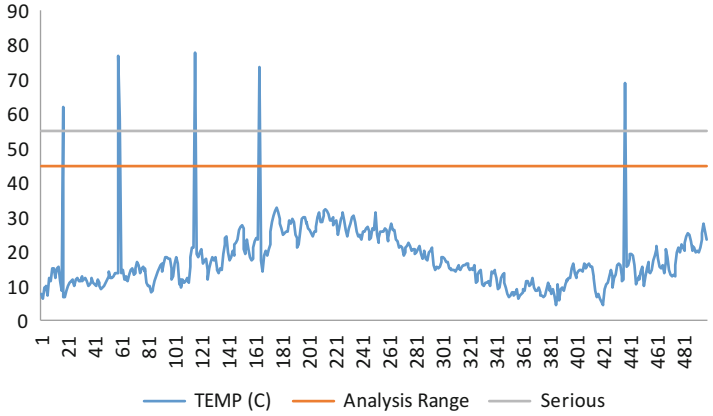


Fig. 25.3 Temperature of fire data

threshold, a particular event is initiated to the relevant department. For instance, the data is processed using proposed architecture and spawns proper events when the number of automobiles exceeds the threshold limit. Figure 25.3 demonstrates this scenario.

In order to sense or notice the fire in a specified situation based on temperature, the fire happening time is examined. It is noticed that the temperature is considerably changed from the specified range of temperature defined as normal temperature. Furthermore, the illumination is also glowing with elevated strength. It is further observed that the temperature exceeded the specified range from time to time due to different causes other than fire. For that reason, two different thresholds are set; they are (1) serious and (2) normal to sense fire as shown in Fig. 25.3. The serious threshold is 55 °C and normal is considered 45 °C.

Moreover, when the room's temperature exceeded from 55 °C (serious), the fire distress is engendered to vigilant the system. Subsequently, the information is communicated to the server, where warning signs are communicated to the respective realm for practical actions. However, when the room's temperature exceeded from 45 °C (normal), the information is forwarded to the server for analysis that considers statistical dealings to investigate the temperature. It may use discrepancy and the mean to investigate the temperature. At last, the response will be given based on statistical analysis to find the actual reason and cause of temperature increase. In addition, no response will be given if the temperature is normal. It is worth mentioning here that the serious and normal threshold differs from time to time depending upon the sensor location.

25.5 Conclusion

The understanding of the smart city is still very infant due to the revolution of the conventional city functions. The smart city notion brings the researchers and industries to the point to have well-organized and generic architecture. In this research article, an efficient architecture of smart city is proposed using data analytics which is performed using the Hadoop server with MapReduce mechanism. This research intends to open concerns of smart urban to make possible the complicated environment for analyzing real-time data. At the end, the dataset of the temperature data is taken to examine and evaluate proposed work.

References

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technolo-gies, protocols, and applications. *IEEE Communications Surveys and Tutorials, 17*(4), 2347–2376.
2. Razzaque, M. A., Milojevic-Jevric, M., Palade, A., & Clarke, S. (2016). Middleware for internet of things: A survey. *IEEE Internet of Things Journal, 3*(1), 70–95.
3. Jan, M. A., Khan, F., Alam, M., & Usman, M. (2017). A payload-based mutual authentication scheme for internet of things. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.08.035.
4. Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K.-S. (2015). The internet of things for health care: A comprehensive survey. *IEEE Access, 3*, 678–708.
5. Khan, M., Silva, B. N., & Han, K. (2016). Internet of things based energy aware smart home control system. *IEEE Access, 4*, 7556–7566.
6. Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal, 1*(1), 2–32.
7. Khan, F., Khan, M., Iqbal, Z., ur Rahman, I., & Alam, M. (2016, September). Secure and safe surveillance system using sensors networks-internet of things. In *International Conference on Future Intelligent Vehicular Technologies* (pp. 167–174). Cham: Springer.
8. Khan, M., Din, S., Jabbar, S., Gohar, M., Ghayvat, H., & Mukhopadhyay, S. C. (2016). Context-aware low power intelligent smart-home based on the Internet of things. *Computers & Electrical Engineering, 52*, 208–222.
9. Silva, B. N., Khan, M., & Han, K. (2017). Big data analytics embedded smart city architecture for performance enhancement through real-time data processing and decision-making. *Wireless Communications and Mobile Computing, 2017*, 9429676.
10. Ahmad, A., Paul, A., & Mazhar Rathore, M. (2016). An efficient divide-and-conquer approach for big data analytics in machine-to-machine communication. *Neurocomputing, 174*, 439–453.
11. Khan, F., ur Rehman, A., Usman, M., Tan, Z., & Puthal, D. (2018). Performance of cognitive radio sensor networks using hybrid automatic repeat ReQuest: Stop-and-wait. *Mobile Networks and Applications, 23*(3), 1–10.
12. Khan, F., ur Rahman, I., Khan, M., Iqbal, N., & Alam, M. (2016, September). CoAP-based Request-response interaction model for the internet of things. In *International Conference on Future Intelligent Vehicular Technologies* (pp. 146–156). Cham: Springer.
13. Rong, W., Xiong, Z., Cooper, D., Li, C., & Sheng, H. (2014). Smartcity architecture: A technology guide for implementation and design challenges. *China Communications, 11*(3), 56–69.

14. Nandury, S. V., & Begum, B. A. (2015, August). Smart WSN-based ubiquitous architecture for smart cities. In *Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI '15)* (pp. 2366–2373). Kochi: IEEE.
15. Sanchez, L., Mũ noz, L., Galache, J. A., Sotres, P., Santana, J. R., Gutierrez, V., et al. (2014). SmartSantander: IoT experimentation over a smart city testbed. *Computer Networks, 61*, 217–238.
16. Mazhar, M., Rathore, A. P., Ahmad, A., Chen, B. W., Huang, B., & Ji, W. (2015). Real-time big data analytical architecture for remote sensing application. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 8*(99), 1–12. https://doi.org/10.1109/JSTARS.2015.2424683.
17. Chung, T. Y., Mashal, I., Alsaryrah, O., Chang, C. H., Hsu, T. H., Li, P. S., & Kuo, W. H. (2014, September). MUL-SWoT: A social eb of things platform for internet of things application development. In *Internet of Things (iThings), 2014 IEEE International Conference on, and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing (CPSCom), IEEE* (pp. 296–299). Piscataway NJ: IEEE.
18. Labrinidis, A., & Jagadish, H. V. (2012). Challenges and opportunities with big data. *Proceedings of the VLDB Endowment, 5*(12), 2032–2033.
19. National climatic data center temperature data. http://academic.udayton.edu/.
20. Ahmad, A., Paul, A., Mazhar Rathore, M., & Chang, H. (2016). Smart cyber society: Integration of capillary devices with high usability based on cyber–physical system. *Future Generation Computer Systems, 56*, 493–503.
21. Jan, M. A., Jan, S. R. U., Alam, M., Akhunzada, A., & Rahman, I. U. (2018). A comprehensive analysis of congestion control protocols in wireless sensor networks. *Mobile networks and applications*, 1–13.
22. Babar, M., & Arif, F. (2017). Smart urban planning using big data analytics to contend with the interoperability in internet of things. *Future Generation Computer Systems, 77*, 65–76.

Chapter 26
Adaptive Transmission Based Geographic and Opportunistic Routing in UWSNs

Saba Gul, Nadeem Javaid, Zahid Wadud, Arshad Sher, and Sheeraz Ahmed

Abstract UWSNs are frequency selective and energy-hungry due to the underwater acoustic communication links. We propose adaptive transmission based geographic and opportunistic routing (ATGOR) for efficient and reliable communication. Opportunistic routing is utilized along with geographic routing to select a set of forwarders from the neighboring nodes instead of a single forwarder. We propose a 3D network model logically divided into small cubes of equal volume with a goal that the sensed data is transmitted by the unit of small cubes.

26.1 Introduction

In this regard, depth-controlled routing protocol (DCR) performs depth adjustment based topology control for void recovery [1]. The proposed protocol organizes the network topology and the number of connected nodes in a proactive manner to overcome the voids. Similarly, for energy efficiency, weighting depth adjustment forwarding area (WDFAD-DBR) for UWSNs is proposed to maintain the balance of energy consumption among the sensor nodes for prolonging network lifetime [7]. The selection of forwarder node based upon the depth leads to the selection of same node due to which the energy of the node depletes quickly and void hole is created.

S. Gul · N. Javaid (✉) · A. Sher
COMSATS Institute of Information Technology, Islamabad, Pakistan
www.njavaid.com

Z. Wadud
University of Engineering & Technology, Peshawar, Pakistan

Capital University of Science and Technology, Islamabad, Pakistan

S. Ahmed
Career Dynamics Research Centre, Peshawar, Pakistan

Iqra National University, Peshawar, Pakistan

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_26

In order to cater the void hole in the discussed existing state-of-the-art work, we have proposed an algorithm named adaptive transmission based geographic and opportunistic routing (ATGOR) protocol for UWSN. We have adjusted the transmission range based on the location of the neighbor node. We will consider depth and energy both parameters for the selection of the forwarder node in order to ensure that cyclic selection of the forwarder node is avoided. This selection assures that energy is efficiently utilized.

26.2 Related Work

A void aware pressure based routing technique is proposed by Noh et al. (VAPR). VAPR utilizes geographic and opportunistic routing for transmitting the sensed data from sensor nodes to the sonobuoys at water surface. The next-hop forwarder is set to continue the forwarding process by selecting the forwarders in a vertical direction towards the surface sinks based on pressure levels [4]. Noh et al. presented another pressure based anycast routing algorithm (HydroCast) for underwater sensor networks [3]. The next-hop forwarder selection is based on the pressure levels at different sensor nodes. The proposed scheme performs void recovery and limits the co-channel interference.

In [6], a depth based routing (DBR) protocol is proposed that utilizes multi-sink architecture. DBR is a greedy routing algorithm in which sensor nodes select the next-hop forwarder based on the depth of neighboring sensor nodes. Jor et al. propose focused beam routing (FBR) protocol that is suitable for both static and mobile sensor nodes [2]. In vector based forwarding (VBF) data packets are routed along a virtual pipeline of fixed radius [5]. The radius of the virtual pipeline is calculated based on the source, local distribution of sensor nodes, and the destination position location.

26.3 System Model

We assume that "i" number of sensor nodes are random uniformly distributed over a $3D$ network field forming a cube having volume "V." Network field is logically divided into uniform ''M" small cubes volume "v," denoted as $C_1, C_2, \cdots, C_M$ (Fig. 26.1).

26.4 The Proposed Transmission Scheme

In this section we describe the adaptive transmission based geographic and opportunistic routing (ATGOR) in detail.

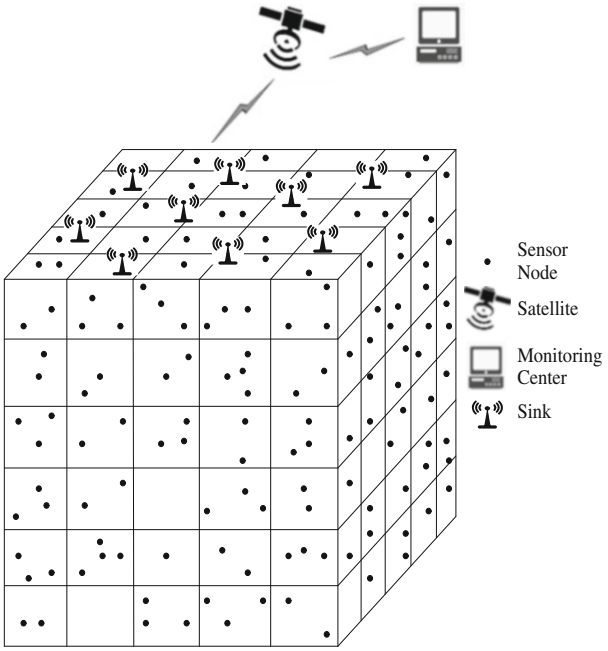


Fig. 26.1 Network model

Enhanced Periodic Beaconing The periodic beacon message of each sink includes the *sequence number*, its ID, and its X and Y location. The sequence number of beacon message is used to identify the most recent beacon of the sink. The value of Z coordinate of sinks is omitted because the sinks are deployed over the surface and the vertical movement of the sinks is negligible. Likely, each sensor node embeds a *sequence number*, the corresponding CID, node's ID, and X, Y, and Z position. Each node includes the *sequence number*, ID, and X and Y coordinate of its reachable sinks. The *sequence number* of the beacon message is incremented periodically after a fixed periodic interval of 30 s. Each entry is refreshed upon receiving the most recent beacon message based on the *sequence number*.

Determine the Next-Hop Small Cube The process of small cube selection is shown in Algorithm 1.

While choosing a **forwarder set selection**, when a forwarder is selected from the ENN other nodes suppress their communication on overhearing the packet transfer. If the highest priority node is failed to forward the packet, then the rest of the low priority nodes transmit the packet. Algorithm 2 shows all the steps of forwarder set selection.

Algorithm 1 Election of ENC

1: Node n_i receives packet from node n_j
2: Acquires its CID
3: Find ENC in its ETR
4: **if** n_i has found an ENC **then**
5: Acquire the ENC's CID
6: **else if** There is a void cube **then**
7: Choose another transmission level from T_{max}
8: Go to 5
9: **end if**

Algorithm 2 ENN set selection

1: ENN forwarder set selection;
2: Find the number of nodes within the CID of the elected ENC
3: Acquires the coordinates of nodes within the coordinates of ENC
4: Acquires its CID
5: Assign priorities to ENNs according to the distance with the nearest sink

26.5 Simulation Results and Discussion

In the simulation, we deploy 150–450 sensor nodes randomly in 1500 m × 1500 m × 1500 m region and the number of sinks is 25. Transmission ranges are set to be 150 m, 200 m, 250 m, 300 m, 350 m, 400 m, and 450 m. Each sensor node is assigned an initial energy of 10 W. In all experiments the packet size is 150 bytes and the data rate is 50 kbps. The energy consumption of transmission, receiving, and idle state are 2 W, 0.1 W, and 10 mW, respectively. We determine the performance of proposed protocol according to the following parameters: packet delivery ratio (PDR), fraction of void nodes, and energy consumption.

26.5.1 Results and Analysis

Scenario I Figure 26.2 shows the fraction of void nodes in the network. The probability of void holes reduces as the node density increases. Our proposed schemes perform better than the compared scheme. This is due to the adaptive transmission range of sensor nodes. If sensor nodes near the water surface fail to find any forwarder node in greedy strategy, then depth adjustment is performed which causes high energy consumption. While in ATGOR sensor nodes overcome the void hole by adaptively adjusting their transmission range to find the nearest sink. Our proposed adaptive transmission range strategy proves to be useful to avoid the void holes. Figure 26.3 depicts the PDR of the network. It can be seen that the PDR increases as the node density increases. The increase in node density results in reduced void nodes due to availability of high number of neighbors. The fixed transmission range causes packet failure, thus adaptive transmission range reduces

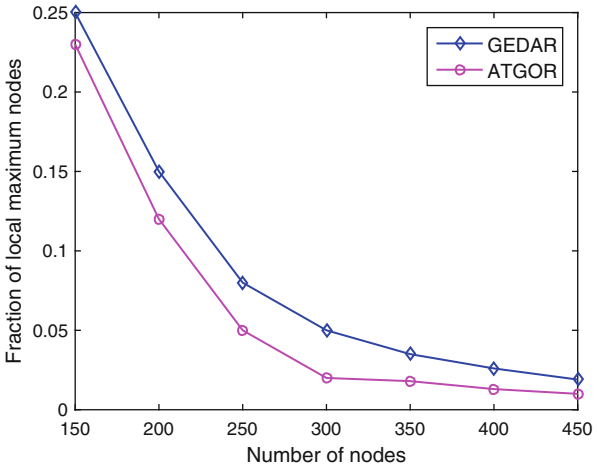
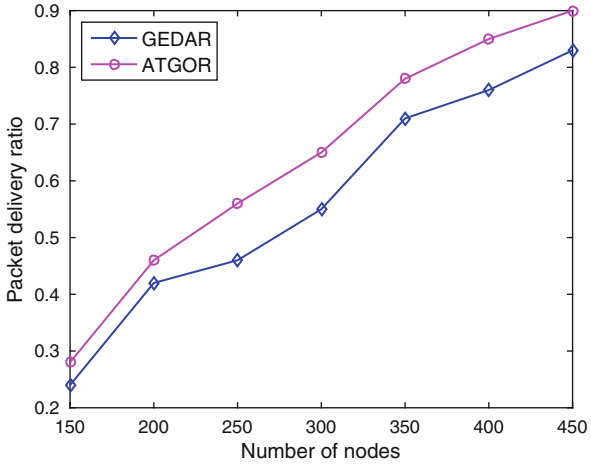


Fig. 26.2 Fraction of void nodes

Fig. 26.3 Packets received at the sinks



the packet failures. Energy consumption per packet per node is shown in Fig. 26.4. In order to avoid the void holes in GEDAR energy consumption per packet per node is high than our proposed schemes.

Scenario II Figure 26.5 shows the impact of different transmission levels on the PDR. Transmission ranges 150 m, 200 m, 250 m, 300 m, 350 m, 400 m, and 450 m are represented by T_1, T_2, T_3, T_4, T_5, T_6, and T_7, respectively. It can be seen that PDR increases as the transmission range increases. Increased transmission range overcomes the void areas in the source to destination route. In this way, it is ensured that the packet generated from the source reaches the destination. Fraction of local maximum nodes at different transmission levels is shown in Fig. 26.6. High

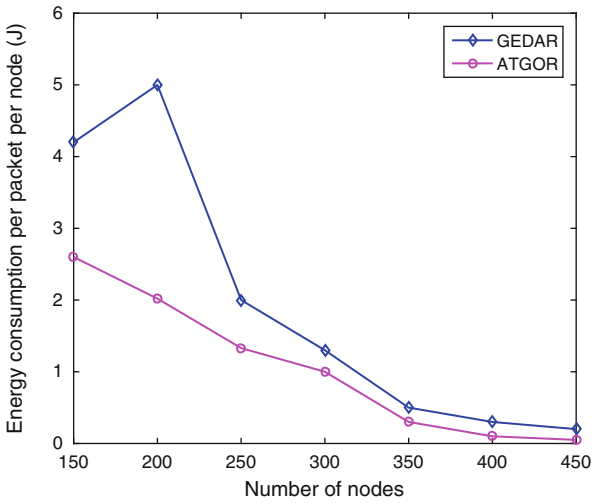


Fig. 26.4 Energy consumption per packet per node

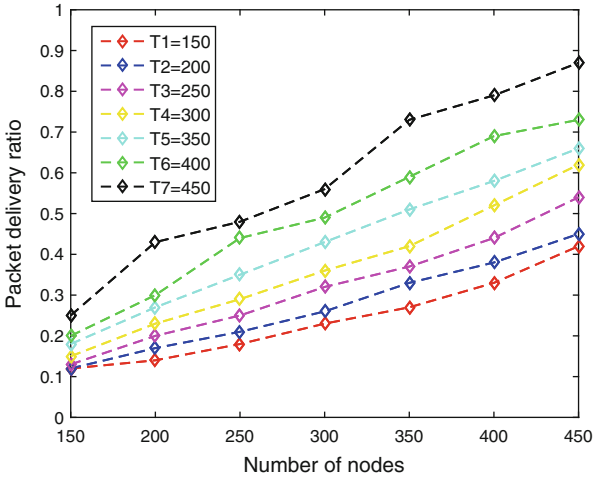


Fig. 26.5 Packets received at the sinks

transmission levels overcome the void areas and greater node density reduces the voids due to more number of neighbors. Energy consumption in the network per packet per node is shown in Fig. 26.7.

26.6 Conclusion

Our proposed scheme selects the next-hop small cube based on the distribution of neighboring nodes. In case of a zero node in the neighboring cube, ATGOR adap-

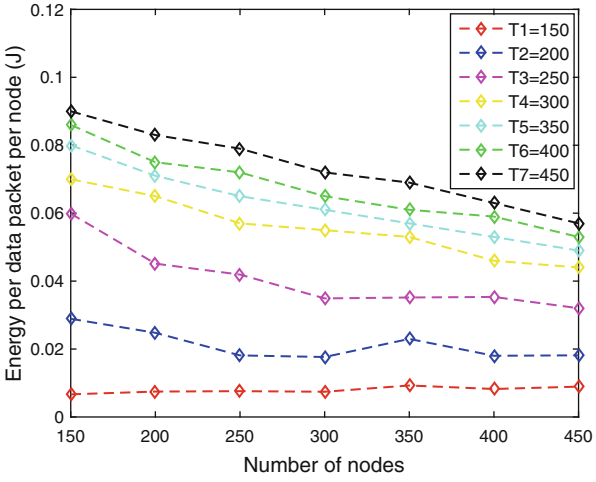


Fig. 26.6 Energy consumption per packet

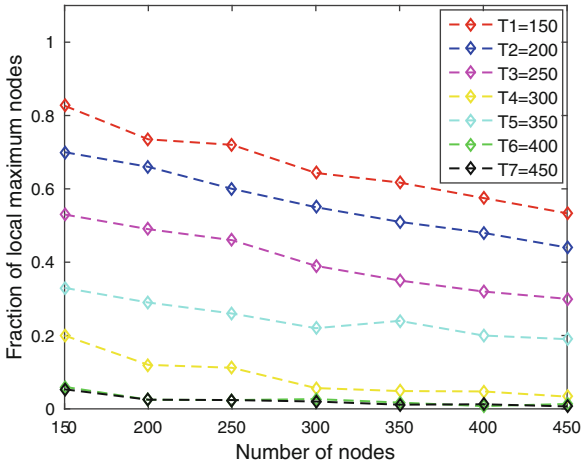


Fig. 26.7 Fraction of void nodes

tively adjusts its communication range and avoids the void nodes. Our simulation results demonstrate that the concept of adaptive transmission along with geographic and opportunistic routing lead to the improvement of network performance in terms of data delivery ratio, fraction of avoiding the local maximas and minimum energy consumption.

References

1. Coutinho, R. W., Vieira, L. F., & Loureiro, A. A. (July 2013). DCR: Depth-Controlled Routing protocol for underwater sensor networks. In *IEEE Symposium on Computers and Communications (ISCC)*, 2013 (pp. 000453–000458). Piscataway: IEEE.
2. Jornet, J. M., Stojanovic, M., & Zorzi, M. (September 2008). Focused beam routing protocol for underwater acoustic networks. In *Proceedings of the Third ACM International Workshop on Underwater Networks* (pp. 75–82). New York: ACM.
3. Noh, Y., Lee, U., Lee, S., Wang, P., Vieira, L. F., Cui, J. H., et al. (2016). Hydrocast: Pressure routing for underwater sensor networks. *IEEE Transactions on Vehicular Technology, 65*(1), 333–347.
4. Noh, Y., Lee, U., Wang, P., Choi, B. S. C., & Gerla, M. (2013). VAPR: Void-Aware Pressure Routing for underwater sensor networks. *IEEE Transactions on Mobile Computing, 12*(5), 895–908.
5. Xie, P., Cui, J. H., & Lao, L. (May 2006). VBF: Vector-Based Forwarding protocol for underwater sensor networks. In *International Conference on Research in Networking* (pp. 1216–1221). Berlin:Springer.
6. Yan, H., Shi, Z. J., & Cui, J. H. (May 2008). DBR: Depth-Based Routing for underwater sensor networks. In *International Conference on Research in Networking* (pp. 72–86). Berlin: Springer.
7. Yu, H., Yao, N., Wang, T., Li, G., Gao, Z., & Tan, G. (2016). WDFAD-DBR: Weighting Depth and Forwarding Area Division DBR routing protocol for UASNs. *Ad Hoc Networks, 37*, 256–282.

Chapter 27
Exploring IoT Applications for Disaster Management: Identifying Key Factors and Proposing Future Directions

Umara Zafar, Munam Ali Shah, Abdul Wahid, Adnan Akhunzada, and Shahan Arif

Abstract In the last few decades, disasters made a huge loss to human beings, natural resources, and other assets. As we are living in an era of technology, there can be no other way better than using ICT (information and communication technology) for disaster management, as communication is the most challenging part of it. The Internet of Things (IoT), a rapidly emerging framework, can be utilized in the best possible ways for the disaster preparedness phase to recovery phase. This paper presents the survey of the work done for disaster management using technology. A detailed analysis has performed to categorize different approaches of disaster management based on supporting phase and technologies used. The best used technology is highlighted. Moreover, forecasting about the growth of its usage and the enhancement in disaster management is also done in this paper. The paper also presents new direction of research in this most attention-grabbing topic.

27.1 Introduction

27.1.1 Internet of Things

As technology is enhancing, a society is formulating, where everyone will be connected to everything [1]. It allows real-world devices and applications to develop independent connection and exchange of data between each other. The Internet has grown tremendously in recent years as it connects billions of things worldwide. IoT technology is being increasingly applied to diverse application areas including healthcare monitoring, disaster management, and vehicular management [2].

Making the IoT paradigm more tangible requires integration and convergence of different knowledge and research domains, covering aspects from identification and

U. Zafar · M. A. Shah · A. Wahid (✉) · A. Akhunzada · S. Arif
COMSATS Institute of Information Technology, Islamabad, Pakistan
e-mail: mshah@comsats.edu.pk; abdulwahid@comsats.edu.pk; a.qureshi@comsats.edu.pk

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_27

communication to resource discovery and service integration [3]. In IoT, there are many objects, sensors, communication links, or framework and processing units that can be beneficial for decision-making and action entreating systems with the help of different technologies [4]. The basic architecture of IoT is constructed on four layers: perception, network, service, and interface layer [5].

Major elements in an IoT concept are sensors, RFID, WSN, WiMAX, etc. In a WSN environment, the components which are important to consider for WSN-monitored environment are WSN hardware, Communication Stack, WSN middleware, and Secure Data Aggregation [6, 7]. Thus, in an area of interest, it is significant to obtain the location information of sensor nodes within the margin of error [8]. Here, we highlight the Sensor Web and categorize into these types: space, underground, underwater, and creature sensors [9].

- Space sensors indicate tropical sensors such as satellites: using imagery to a hot spot to monitor the spread of forest fires, using multi-sensor data sets of remote sensing and models.
- Underground sensors are those which are usually concealed in the soil, a layer of ice, and other geographical strata or assimilated in underground pipes, to observe the mud slide disaster and to measure pore water pressure tensiometers.
- Underwater sensors state the sensors throw down into rivers and lakes or integrated sensors with pipes under the water such as undersea sensors.
- Creature sensors refer to the sensors embedded in the integral part of animals or human bodies to observe their behavior, health, locations, and other factors.

Another well-known technology for IoT is the RFID technology. It is a basic and broadly used technology in this context and considered as criterion for the IOT. RFID tags can automatically identify and track any object [10, 11].

An RFID system has three parts [12]:

- RFID tags, of two kinds either active or passive, refer to transponders attached to objects to identify and count.
- A reader or transceiver is a combination of radio-frequency interface (RFI) module and a controller.
- A data processing/application system, depending on the application, may be any application/database or any other system.

27.1.2 Disaster Management

It is an incessant process in which efforts are made to manage risks and to avoid the effects of disasters with the help of different authorities. Operative disaster management is based on full incorporation of emergency plans at all stages of participation by different authorities [13–17]. Any disaster can be managed at different levels called phases of disaster management which are shown below in Fig. 27.1. Data collected from the sensor nodes transmits to a centralized control center

Fig. 27.1 Disaster management phases

and then to emergency operations center and rescue authorities through various communication media, for example, RFID, wireless sensor networks, GIS/GPS, mobile networks, and satellites. The disaster detection and warning dissemination process in the best possible way are shown below in Fig. 27.2.

As discussed earlier, according to the stage at the time of the disaster, it could be divided into two parts: pre-disaster and post-disaster. It contains detection, monitoring, and forecasting in pre-disaster phase, or we can say it's the time when a disaster just occurred, while search, control, and rescue operations during disaster and recovery as well are the parts of post-disaster. In this paper the focus is on both the pre- and post-disaster management. Disasters cannot be eliminated, so it is very important to find solutions to damage associated with them [18–22].

The purpose of conducting this research is to review the maximum number of approaches used for disaster management in last years. Through it we categorized that which specific technology is used and which phase of disaster management is supported through any specific approach. Based on this study, we analyze and highlight the most commonly and effectively used technology and its future growth. Also, we predicted that in the coming years, improvement in people's awareness about disasters and its management will be enhanced and presented in some graphical values.

The rest of the paper is structured as follows. Section 27.2 presents the literature review of the work done for disaster management through technology. In Sect. 27.3, an overview of the technology usage in the context of disaster management and their evaluation is reported. The paper continues with an analysis and presented

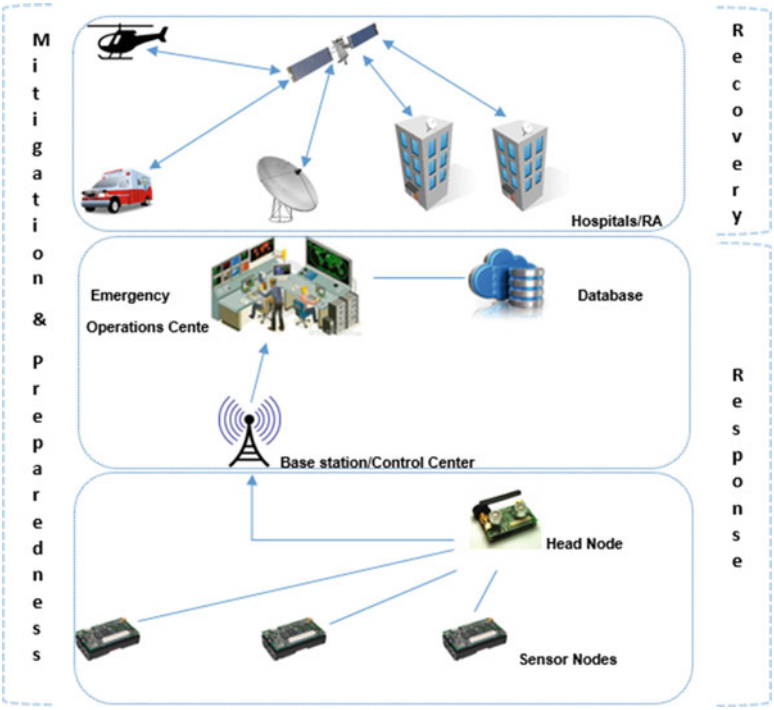


Fig. 27.2 Disaster management process

current and expected trends related to disaster management. Section 27.4 discusses the analysis, while Sect. 27.5 presents the authors' conclusions.

27.2 Disaster Management Approaches

Several disaster management approaches have been proposed in recent years to minimize the loss or damage and enhance the process. These include collaborative computer-based system or embedded system which is integrated with different ICTs. Different researchers have proposed different methodologies.

27.2.1 Pre-disaster Management

It refers to managing disaster in mitigation and pre-preparation phase. It includes mitigation measures to reduce exposure to the effects of disasters such as injuries and loss of life and property, while preparation is focused on expecting how much a

disaster can affect the community and how to react and recover from that situation. It refers to the steps taken to prepare to minimize the impact of disasters, i.e., to predict and prevent.

By analyzing flood prediction techniques built on GIS by means of ad hoc wireless sensor network [23–25], a model for flood prediction is proposed which is considered to be helpful for calculating the influence of flood damage with the use of GIS simulation tool [26]. When it comes to prime to detect prime location of ambulance and or other rescue authorities, Google Maps integrated with GIS simulation tool can help [27, 28]; moreover flood risk analysis can be performed through its use [29]. Another important factor is that for flood management GIS can utilize unit hydrographs effectively [30, 31].

An IIS (integrated information system) [32] was introduced named as '*architype*' early warning system for snowmelt floods. It works by incorporating with IoT and Geo-informatics for management of resources.

In [33] remote sensing and geographic information systems were used for the estimation of the flash flow-flood area. GIS can deliver risk assessment and public administration of natural exposures.

A framework of early warning system [34] was prototyped which integrates three components: rainfall-induced landslide prediction model (SLIDE), susceptibility model, and satellite-based forecasting model. Permutation of EEWS (earthquake early warning system) and RSMS (real-time strong motion monitoring system) was applied for response phase during an emergency in [35]. The stratagem is PDCA cycle: plan, do, check, and action.

Decentralized message broadcasting approach for sensor cooperation [36] is introduced to address the issues of message encircling in the system and event's identity confusion. Node level and network level virtualization can be practical to evade redundant placement of weather sensors [37, 38] for weather data alerts, which supports different kinds of applications for propagation of weather sensors. Earthquake alert system for Pakistan [39] was proposed which used different open-source technologies, like it takes real-time earthquake data from US Geological Survey (USGS) public API.

In [40] multi-hazard early warning and response system was considered, which focuses on reducing seismic alert time by exploring the use of vigorous seismic sensors in WSN such as Wi-Fi, WiMAX, and Zigbee which are used for different categories of networks. For detecting the earthquake, real-time wave signals are used in EEW (earthquake early warning) system [41, 42]. People are alerted on the basis of magnitude, velocity, and displacement detected. SEWAS (seismic early warning alert system) [43] warns people about imminent strong shake, so that peoples could take appropriate actions quickly, maintaining the integrity of the specifications.

27.2.2 Post-disaster Management

It includes strategies to support rehabilitation after a disaster and recovery cover which are oriented toward the reestablishment of human-centered services and infrastructure, as well as the restoration of physical and ecological veracity of the affected ecosystem.

In [44], a mini case study of occupational hazard is considered after which solutions assumed are the use of plasters by each operational unit team which can collect data about environment and sensor APIs on victim's mobile phones and finally grids, cloud, and crowd source computing for data processing and analysis through which disaster managers outside the building can get all information.

Usually Web services provide exiled, determined facilities, while grids offer state-full, transitory illustrations of objects [45]. IoT and DfPL system can account the RSSI dimensions that can perceive the presence of humans in an environment (location affected by disaster) [46]. There are many existent ways for implementing WSN in IoT scenario [47], such as smoothing algorithm "SavitzkyGolay" and classifiers like Naive Bayes, Tree Bagger, etc.

In [48], a research is conducted to support two hypotheses which are: (1) IoT technology convulsions acknowledged information requests and (2) IoT has added significance to disaster response processes. A project named SIGMA was presented [49] exploiting cloud technologies to attain, incorporate, and compute records from multiple sensor networks.

An emergency management system based on IoT architecture was proposed in China, which can monitor any disastrous situation using sensors and intelligent video [50]. In response to "Typhoon Morakot" in Taiwan, discussion research [51] suggests that a system of emergency response via the Internet can allow people to report any emergency to the government by using mobile wireless devices or computers to assist in search and rescue operations. A system [18] for evaluating disaster synthetically was designed based on seismic networks of things, which can collect data through IoT in real time and then estimate the loss and forecast by GIS. IoT may exercise the directional control function and accurate forecasting and discard sudden emergencies effectively through different technologies [52].

Development of an instinctive user interface [53, 54] to dynamically manage changes in workflow essentials of an emergency using WIFA approach incorporates the concept of IoT to enable the performance of decision-making. For consistent access to distributed database during any emergency, an emergency Role-based Authentication/Authorization Protocol (eRAAP) integrated with an RFID service (ROY) can be used [55]. RFID embedded portable devices and tags can be used to publish the collection, storage, and with fewer errors efficient way to share building assessment information to improve efficiency and effectiveness in the process of emergency management [56].

Adoption of RFID in emergency management is mainly triggered by organizations' goals to reduce response time [57]. With IoT concept real-time information and situational awareness via RFID, WSN can be gathered, and this inclusive data

can be presented to the emergency personnel [58, 59]. RFID electronic tags have been installed on cylinders of hazardous chemicals and gas bottles for dangerous goods detection as well [60]. An emergency management system based on WSID (wireless sensor identification) is designed and implemented in order to solve the inconvenience of aid persons [61]. In a disaster scenario, response time is a crucial factor, so the time required to respond should be more concerning for disaster managers [62], because quick response to any disastrous event enhances the recovery, minimizes property damage, and helps in saving a life [63]. In disaster management scenario, dynamically linked objects were used as smart resources in IoT-enabled smart environment, and its modeling through social networking analysis was proposed [64].

A WoO-based emergency fire management system integrated with ViO (virtual objects) was proposed in [65, 66] which are derivate from physical objects and interconnected in semantic ontology model. WoO kept the option of cooperation between things, humans, amenities, resources, and different sorts of concrete things such as virtual objects [67].

IoT-oriented service architecture for logistics management which is concerned to emergency response was proposed in [68, 69] employed RFID smart sensor networks as objects enabled network architecture. MyDisasterDroid [70], an android application, was developed which facilitates the rescue operations and work in response phase during a disaster. Studies revealed that cellular technology could be utilized for dissemination of pre- and post-disaster warnings effectively [71–75].

In [76] a framework was proposed for data delivery in large-scale networks for disaster management, where numerous wireless sensors are distributed over city traffic infrastructures. Smart wearable devices offer much potential to assist citizens in disasters situations [77]. A new approach proposed in [78] incorporates a mode of disaster on all mobile phones. In [79] two types of IoT-based recovery resource management processes were designed. The first is a resource information management process, and the second is a real-time management and monitoring process for resources that are implemented following disasters.

Taxonomy of the related work done in disaster management through technologies is shown below in Fig. 27.3.

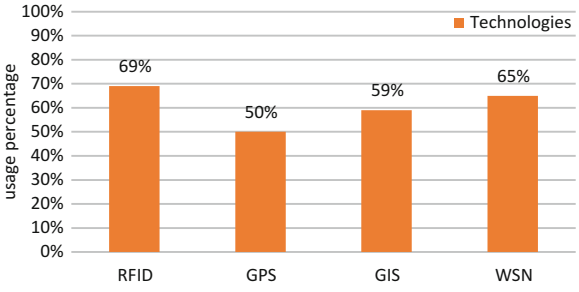


Fig. 27.3 Contribution of technologies in disaster management

27.3 Performance Evaluation

We evaluate the performance of different parameters or technologies used for disaster management in the past or used currently in this section. It provides an inclusive comparison of different characteristics. The analysis is performed using the basic parameters such as parameters for "data retrieval," "technologies," "supporting phase," and the "contributors" to that specific approach or system. Table 27.1 provides the detailed overview of the approaches used for disaster management. A comparative analysis is shown in this table by considering basic parameters which are research focus, practical implementation, data retrieval parameters, technologies used, and supporting phase (of disaster management) regarding different approaches.

27.4 Discussion

We are living in the era next to technology called the Internet of Things, or Web-of-Objects, where each and everything, from ground to high-rise building, can be integrated with technology. This concept is helping us in all fields, but in this paper, we considered it regarding disaster management. As it has multiple phases which are mitigation, preparedness, response, and recovery, we observed that technology is adding benefit to any of these phases, resulting in a contribution in the context of disaster management. For comparison and evaluation, we considered the approaches/systems, their data retrieval parameters, and technologies used in Table 27.1. It shows that a lot of work has been done in this context and the modern technologies like WSN, RFID, GPS, GIS, etc. are no doubt very helpful for reducing the effects of disasters. The analysis show that majorly using technology which is adding real contribution for managing any disastrous situation is RFID with 69% support as shown in Fig. 27.3. Secondly its WSN with a percentage of 65 and its supporting the disaster management at different phases. Then 59% and 50% for GIS and GPS respectively. On the basis of this study, we predicted that at which possible level people awareness regarding emergency situations, disaster management, and use of IoT can be increased in the upcoming years as shown in Fig. 27.4. It is predicted that "people awareness" which is currently 44% could be increased up to 65% in the coming years. "The use of IoT for disaster management" would increase by 19% from now to then, as it is 55% in 2016 and can boost up to 74% in 2020. Most importantly, the overall disaster management which refers to the reduced loss in lives and resources is predicted to increase up to 59% in the upcoming years. In Fig. 27.5, the expected growth of RFID is predicted, which shows that increment in its usage for disaster management during upcoming years is high. Disasters cannot be eliminated and different disaster management systems have been proposed, however, there is a need for more enhanced systems. Figure 27.6 shows the taxonomy of the disaster management systems found in literature.

Table 27.1 Approaches for disaster management

System/approach	Research focus	Parameters	Practical implementation	Tools and technologies	Contributors	Supporting phase
Rapid assessment of flood disaster loss	Disastrous flood area, effected population, and land use are intended by using GIS spatial analysis	Remote-sensed and land use data, basic geographic information data	Yes	GIS, spectrum photometric, remote sensing	Researchers	Mitigation and relief
GIS-based analysis of flood disaster risk	Appearances of flood disasters and the exposed population are analyzed by using ArcGIS	Gridded data from GPW, hot spots, and CAD	Yes	ArcGIS tool	Researchers, government, world population GPW	Mitigation
Flood prediction and disaster risk analysis using GIS-based WSN	Use of ArcGIS simulation tool for flood forecasting in different regions	Air, pressure, wind, snowmelt, and rainfall measurements	Yes	GIS simulation tool, WSN, GPS, remote sensing	Researchers	Mitigation and prediction
Flood risk assessment using remote sensing and GIS approach	Usage of GIS and RS technologies for flood hazard modeling	Land use data	No	GIS, remote sensing	Researchers	Mitigation
Land use effects on flood risk by using integration of GIS and RS	Analysis of flood risk analysis using remote sensing and GIS	Hydraulic modeling, stream basins	Yes	ArcGIS, HEC-RAS, remote sensing	Researchers	Mitigation
Integrated information system for snowmelt flood early warning	A prototype IIS for snowmelt flood early warning system	Meteorological, hydrological, and geographical data	Yes	GIS, GPS, cloud service, remote sensing	Researchers, public	Mitigation and preparedness

(continued)

Table 27.1 (continued)

System/approach	Research focus	Parameters	Practical implementation	Tools and technologies	Contributors	Supporting phase
Flash flood risk estimation using GIS-based morphometry	Satellite data and GIS-based morphometry for flash flood risk mapping	Drainage density and frequency	No	GIS, satellites	Researchers	Mitigation
Earthquake early warning system and real-time strong motion monitoring system in emergency response	Use of EEWS to disseminate advance alerts of ground motions and RSMS for emergency response	EEWS, RSMS	Yes	Sensors, EEWS, RSMS	Researchers	Mitigation, preparedness, and response
Integrating cloud-WSN to analyze weather data and alert users	Cloud-WSN integration to alert users during weather disasters	Sensed data	No	WSN, cloud	Researchers	Mitigation, preparedness, and response
CIVIONICS Earthquake Early Warning System	The CIVEEWS network architecture for fixing up the minimum warning time	Sensed data	Yes	Wi-Fi, WiMAX, and Zigbee	Researchers	Mitigation, preparedness, and response
Seismic early warning alert system	Seismology with the help of GPS to quickly locate an earthquake	Sensed data	No	GPS	Researchers	Mitigation, preparedness, and response
A data collective computational intelligence case proposal for managing disaster	Use of plasters to collect data about environment and monitor individual's health condition, buildings with installed sensors	Sensed data	No	Sensors, Google Maps	Researchers	Response, recovery

IoTs and DfPL in a disaster management scenario	Novel disaster management system that takes advantage of WSN and DfPL concept	Classified data, time stamps	No	Sensors, WSN, DfPL	Researchers	Preparedness, response, recovery
Application of IoT in emergency management system	Hands-free data collection, high-building firefighting, hazard monitoring, and medical and health services using technologies	Mapped, sensed, or captured data	Yes	Sensors, GPS, GPRS, RFID, WSN	Researchers, government	Response, recovery
Web 2.0 and Internet social networking as a tool for disaster management	Internet-based emergency response system based on the use of mobile devices or wireless computers	Environmental data	No	Web 2.0, Internet social networking	Researchers	Response, recovery
Quasi real-time evaluation system for seismic disaster based on IoT	Disaster real-time evaluation system to collect real-time data through IoT	Earthquake magnitude, focus, monitoring network data	Yes	Sensors, GIS	Researchers	Mitigation, recovery
Urban public safety emergency based on technologies for the IoT	Accurate prediction of emergencies through various technologies	Sensed data	Yes	RFID, Bluetooth, Wi-Fi, WSN, LAN	Researchers	Mitigation, preparedness, response

(continued)

Table 27.1 (continued)

System/approach	Research focus	Parameters	Practical implementation	Tools and technologies	Contributors	Supporting phase
RFID-based mobile communication framework for handling emergencies	RFID for emergency (ROY) approach for enhancing system's efficiency during emergency	Data	No	RFID	Researchers	Response, recovery
Supporting urban emergency response and recovery using RFID	RFID embedded portable devices and tags for gathering, storing, and sharing information	Sensed data	Yes	RFID	Researchers	Response, recovery
On-site information systems design for emergency first responders	How emerging technologies such as WSN and RFID might enable on-site dynamic information	Sensed data	No	RFID, WSN	Researchers	Response
Emergency management system based on WSID network	Emergency management system based on WSID to solve the inconvenience of aid persons and goods management in disasters	Data	Yes	WSN, Zigbee	Researchers	Response, recovery

Web-of-Objects-based context aware emergency fire management systems	WoO-based system integrated with virtual objects (ViO) interconnected in semantic ontology model	Sensed data	Yes	WSN, RFID	Researchers	Preparedness, response, recovery
Architectural design of IoT in logistics management for emergency response	IoT-oriented service architecture for logistics management which is concerned to emergency response	Resourced data	No	RFID	Researchers	Preparedness, response
A mobile disaster management system using the android technology	An android application to facilitate and take geographical locations of people directly or via sms and determine optimum route	Resourced data	Yes	Wireless mobile technology	Researchers	Response, recovery

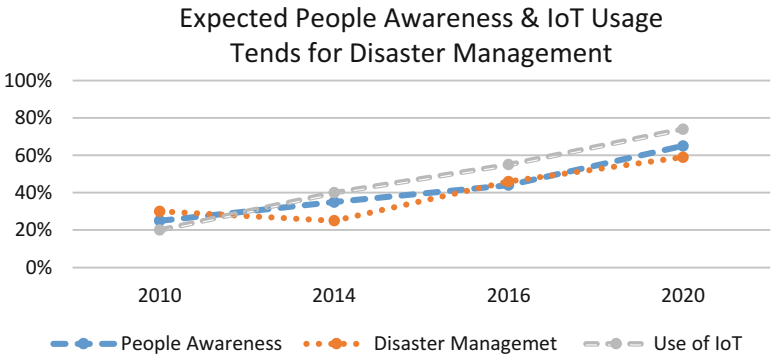
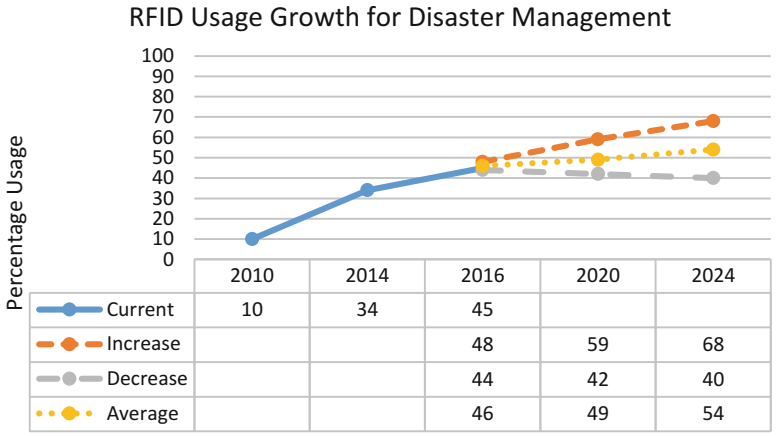


Fig. 27.4 Current and expected trends related to disaster management



	2010	2014	2016	2020	2024
Current	10	34	45		
Increase			48	59	68
Decrease			44	42	40
Average			46	49	54

Fig. 27.5 RFID usage growth in upcoming year

27.5 Conclusion

In this paper, we described the disaster management and its different phases, through which we can reduce the impacts of disasters. The Internet of Things, an evolving standard, can add a lot in this context. Major technologies of IoT, such as WSN, RFID, GIS, and GPS, are described, and we did a complete review of the existing use of these technologies in disaster management and at which level they are contributing. A detailed analysis is performed, by observing different approaches, their contribution, and supporting phases. On the basis of that evaluation, RFID is the most common and valuable technology for managing disasters. By reviewing all the work done in this field and the percentage of use of technologies and their contributions, it is predicted that disaster management would increase in upcoming years as people's awareness and usage of IoT would increase. In the future it is aimed that on the basis of this analysis, a complete IoT architecture for disaster

Fig. 27.6 Taxonomy of technologies used for disaster management

management will be proposed, in which the main focus will be on the shortest time span in which a disaster alert can be reached to all concerned authorities and the use of RFID for tracking all the "things" combined in a disaster managing environment.

References

1. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future internet: The internet of things architecture, possible applications and key challenges. In *Proceedings of the 10th International Conference on Frontiers of Information Technology (FIT) 2012* (pp. 257–260).
2. Chun, S.-M., & Park, J.-T. (2017). A mechanism for reliable mobility management for internet of things using CoAP. *Sensors, 17*(1), 136.
3. Khodadadi, F., Dastjerdi, A. V., & Buyya, R. (2017). *Internet of Things: An overview*. arXiv preprint arXiv:1703.06409.
4. Jan, M. A., Nanda, P., He, X., Tan, Z., & Liu, R. P. (2014, September). A robust authentication scheme for observing resources in the internet of things environment. In *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 205–211). Beijing, China: IEEE.

5. Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233–2243.
6. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645–1660.
7. Khan, F., Khan, M., Iqbal, Z., ur Rahman, I., & Alam, M. (2016, September). Secure and safe surveillance system using sensors networks-internet of things. In *International Conference on Future Intelligent Vehicular Technologies* (pp. 167–174). Cham, Switzerland: Springer.
8. Han, G., Yang, X., Liu, L., Guizani, M., & Zhang, W. (2017). A disaster management-oriented path planning for mobile anchor node-based localization in wireless sensor networks. *IEEE Transactions on Emerging Topics in Computing.*
9. Jan, M. A., Khan, F., Alam, M., & Usman, M. (2017). A payload-based mutual authentication scheme for internet of things. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2017.08.035.
10. Jia, X., Feng, Q., Fan, T., & Lei, Q. (2012). RFID technology and its applications in Internet of Things (IoT). In *2012 2nd International Conference on Consumer Electronics, Communications and Networks* (pp. 1282–1285).
11. Armbrust, M., Fox, A., Griffith, R., Joseph, A., & Katz, R. (2010). *Above the clouds: A Berkeley view of cloud computing* (Tech. Rep. UCB) (pp. 07–013). Berkeley, CA: University of California.
12. Khan, F., ur Rahman, I., Khan, M., Iqbal, N., & Alam, M. (2016, September). CoAP-based request-response interaction model for the internet of things. In *International Conference on Future Intelligent Vehicular Technologies* (pp. 146–156). Cham, Switzerland: Springer.
13. Wattegama, C. (2014). *ICT for Disaster Management*. http://en.wikibooks.org/wiki/ICT_for_Disaster_Management.
14. Sookhak, M., Akhundzada, A., Sookhak, A., Eslaminejad, M., Gani, A., Khan, M. K., et al. (2015). Geographic wormhole detection in wireless sensor networks. *PLoS One, 10*(1), e0115324.
15. Sookhak, M., Akhunzada, A., Gani, A., Khurram Khan, M., & Anuar, N. B. (2014). Towards dynamic remote data auditing in computational clouds. *The Scientific World Journal, 2014*, 269357.
16. Abdelaziz, A., Fong, A. T., Gani, A., Garba, U., Khan, S., Akhunzada, A., et al. (2017). Distributed controller clustering in software defined networks. *PLoS One, 12*(4), e0174715.
17. Akhunzada, A., Gani, A., Hussain, S., & Khan, A. A. (2016). A formal framework for web service broker to compose QoS measures. In *SAI Intelligent Systems Conference (IntelliSys), 2015*. Piscataway, NJ: IEEE.
18. Jan, M., Nanda, P., Usman, M., & He, X. (2017). PAWN: A payload-based mutual authentication scheme for wireless sensor networks. *Concurrency and Computation: Practice and Experience, 29*(17), e3986.
19. Akhunzada, A., Gani, A., Hussain, S., & Khan, A. A. (2015). Towards experiencing the pair programming as a practice of the Rational Unified Process (RUP). In *SAI Intelligent Systems Conference (IntelliSys), 2015*. Piscataway, NJ: IEEE.
20. Usman, N., Javaid, Q., Akhunzada, A., Choo, K. K. R., Usman, S., Sher, A., et al. (2017). A novel internet of things-centric framework to mine malicious frequent patterns. *IEEE Access, PP*(99), 1–1. https://doi.org/10.1109/ACCESS.2017.2690456.
21. Akhunzada, A., Ahmed, E., Gani, A., Khan, M. K., Imran, M., & Guizani, S. (2015). Securing software defined networks: Taxonomy, requirements, and open issues. *IEEE Communications Magazine, 53*(4), 36–44.
22. Akhunzada, A., & Khan, M. K. (2017). Toward secure software defined vehicular networks: Taxonomy, requirements, and open issues. *IEEE Communications Magazine, 55*(7), 110–118.
23. Khan, F., ur Rehman, A., Usman, M., Tan, Z., & Puthal, D. (2018). Performance of cognitive radio sensor networks using hybrid automatic repeat request: Stop-and-wait. *Mobile Networks and Applications, 23*, 1–10.

24. Liu, J., Wen, J., Yang, K., Shang, Z., & Zhang, H. (2011). GIS-based analysis of flood disaster risk in LECZ of China and population exposure. In *Proceedings of the 2011 19th International Conference on GeoInformatics, Geoinformatics 2011*, no. 40471028 (pp. 0–3).
25. Seal, V., Raha, A., Maity, S., Mitra, S. K., Mukherjee, A., & Naskar, M. K. (2012). *A real time multivariate robust regression based flood prediction model using polynomial approximation for wireless sensor network based flood forecasting systems* (pp. 432–441). Berlin/Heidelberg, Germany: Springer.
26. Ahmad, N., Hussain, M., Riaz, N., Subhani, F., Haider, S., Alamgir, K. S., et al. (2013). Flood prediction and disaster risk analysis using GIS based wireless sensor networks, a review. *Journal of Basic and Applied Scientific Research, 3*(8), 632–643.
27. Sulaiman, N. A., Husain, F., Hashim, K. A., & Samad, A. M. (2012). A study on flood risk assessment for Bandar Segamat sustainability using remote sensing and GIS approach. In *2012 IEEE Control and System Graduate Research Colloquium* (pp. 386–391).
28. Khattak, M. I., Edwards, R. M., Shafi, M., Ahmed, S., Shaikh, R., & Khan, F. (2018). Wet environmental conditions affecting narrow band on-body communication channel for WBANs. *Adhoc & Sensor Wireless Networks, 40*, 297–312.
29. Akar, Î., Kalkan, K., & Maktav, D. (2011). Determination of land use effects on flood risk by using integration of GIS and remote sensing. In *Recent advances in space technologies*.
30. Jan, M. A., Nanda, P., He, X., & Liu, R. P. (2013, November). Enhancing lifetime and quality of data in cluster-based hierarchical routing protocol for wireless sensor network. In *2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing (HPCC_EUC)* (pp. 1400–1407). Zhangjiajie, China: IEEE.
31. Sherief, Y. (2010). *Flash floods and their effects on the development in El-Qaá plain area in South Sinai, Egypt*. Diss. PhD dissertation, University of Mainz, Germany.
32. Fang, S., Xu, L., Zhu, Y., Liu, Y., Liu, Z., Pei, H., et al. (2015). An integrated information system for snowmelt flood early-warning based on internet of things. *Information Systems Frontiers, 17*(2), 321–335.
33. Jan, M. A., Tan, Z., He, X., & Ni, W. (2018). Moving towards highly reliable and effective sensor networks.
34. Liao, Z., Hong, Y., Wang, J., Fukuoka, H., Sassa, K., Karnawati, D., et al. (2010). Prototyping an experimental early warning system for rainfall-induced landslides in Indonesia using satellite remote sensing and geospatial datasets. *Landslides, 7*(3), 317–324.
35. Kubo, T., Hisada, Y., Murakami, M., Kosuge, F., & Hamano, K. (2011). Application of an earthquake early warning system and a al-time strong motion monitoring system in emergency response in a high-rise building. *Soil Dynamics and Earthquake Engineering, 31*(2), 231–239.
36. Guo, H., Liang, F., & Liu, Y. (2012). Research on sensor cooperation for distributed emergency response system. *Journal of Networks, 7*(4), 683–690.
37. Khan, I., Belqasmi, F., Glitho, R., & Crespi, N. (2013). A multi-layer architecture for wireless sensor network virtualization. In *6th Joint IFIP Wireless and Mobile Networking Conference* (pp. 1–4).
38. Arjun, D. S., Bala, A., Dwarakanath, V., Sampada, K. S., BB, P. R., & Pasupuleti, H. (2015, June). Integrating cloud-WSN to analyze weather data and notify SaaS user alerts during weather disasters. In *Advance computing conference (IACC), 2015 IEEE international* (pp. 899–904).
39. Mir, K., & Hira Fatima, S. (2014). *Earthquake auto-SMS alert system – a case study of Pakistan, The 2nd International Conference on Applied Information and Communications Technology - ICAICT*.
40. Jan, M. A., Jan, S. R. U., Alam, M., Akhunzada, A., & Rahman, I. U. (2018). A comprehensive analysis of congestion control protocols in wireless sensor networks. *Mobile Networks and Applications, 23*, 1–13.
41. Wu, Y.-M., & Kanamori, H. (2008). Development of an earthquake early warning system using real-time strong motion signals. *Sensors, 8*(1), 1–9.

42. Peng, H., Wu, Z., Wu, Y.-M., Yu, S., Zhang, D., & Huang, W. (2011). Developing a prototype earthquake early warning system in the Beijing Capital Region. *Seismological Research Letters, 82*(3), 394–403.
43. Singh, R. D., Kumari, P., Singh, P., Balwant, R., Engineering, S., & Campus, T. (2014). Seismic early warning alert system. In *International Conference on Signal Processing and Integrated Networks* (pp. 601–605).
44. Bessis, N., Asimakopoulou, E., French, T., Norrington, P., & Xhafa, F. (2010). The big picture, from grids and clouds to crowds: A data collective computational intelligence case proposal for managing disasters. In *Proceedings of the International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC 2010)*, no. Section II. (pp. 351–356).
45. Bessis, N. (2010). *Grid technology for maximizing collaborative decision management and support: Advancing effective virtual organizations*. Hershey, PA: IGI Global.
46. Deak, G., Curran, K., Condell, J., Asimakopoulou, E., & Bessis, N. (2013). IoTs (internet of things) and DfPL (device-free passive localisation) in a disaster management scenario. *Simulation Modelling Practice and Theory, 35*, 86–96.
47. Khan, F., Bashir, F., & Nakagawa, K. (2012). Dual head clustering scheme in wireless sensor networks. In *2012 International Conference on Emerging Technologies (ICET)* (pp. 1–5). Islamabad, Pakistan: IEEE.
48. Yang, L., Yang, S. H., & Plotnick, L. (2013). How the internet of things technology enhances emergency response operations. *Technological Forecasting and Social Change, 80*(9), 1854–1867.
49. Fazio, M., Celesti, A., Puliafito, A., & Villari, M. (2014). *An integrated system for advanced multi-risk management based on cloud for IoT* (pp. 253–269). Cham, Switzerland: Springer.
50. Khan, F. (2014). Secure communication and routing architecture in wireless sensor networks. In *2014 IEEE 3rd Global Conference on Consumer Electronics (GCCE)* (pp. 647–650). Tokyo, Japan: IEEE.
51. Jabeen, Q., Khan, F., Khan, S., & Jan, M. A. (2016). Performance improvement in multihop wireless mobile adhoc networks. *The Journal Applied, Environmental, and Biological Sciences (JAEBS), 6*(4S), 82–92.
52. Du, C., & Zhu, S. (2012). Research on urban public safety emergency management early warning system based on technologies for the internet of things. *Procedia Engineering, 45*(2011), 748–754.
53. Wang, J., Tepfenhart, W., & Rosca, D. (2010). Emergency response workflow resource requirements modeling and analysis. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 39*(3), 270–283.
54. Wang, J., Rosca, D., Tepfenhart, W., Milewski, A., & Stoute, M. (2011). Dynamic workflow modeling and analysis in incident command systems. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 38*(5), 1041–1055.
55. Tran, T., Yousaf, F. Z., & Wietfeld, C. (2010). RFID based secure mobile communication framework for emergency response management. In *Wireless Communications and Networking Conference (WCNC), 2010 IEEE*.
56. Aziz, Z., Peña-Mora, F., Chen, A., & Lantz, T. (2012). Supporting urban emergency response and recovery using RFID-based building assessment. *Disaster Prevention and Management, 18*(1), 35–48.
57. Fida, N., Khan, F., Jan, M. A., & Khan, Z. (2016, September). Performance analysis of vehicular adhoc network using different highway traffic scenarios in cloud computing. In *International Conference on Future Intelligent Vehicular Technologies* (pp. 157–166). Cham, Switzerland: Springer.
58. Wickler, G., & Potter, S. (2010). Information-gathering: From sensor data to decision support in three simple steps. *Information Systems Journal, 3*(1), 1–42.
59. Yang, L., Prasanna, R., & King, M. (2011). On-site information systems design for emergency first responders. *Journal of Information Technology Theory and Application, 10*(1), 5–27.
60. Du Chunquan, J., Shunbing, Z., & Qiuping, W. (2010). Study and prospect on the application of internet of things in perceiving safety. *China Safety Science Journal, 20*, 164–170.

61. Alam, M., Ferreira, J., Mumtaz, S., Jan, M. A., Rebelo, R., & Fonseca, J. A. (2017). Smart cameras are making our beaches safer: A 5G-envisioned distributed architecture for safe, connected coastal areas. *IEEE Vehicular Technology Magazine, 12*(4), 50–59.
62. Sagun, A., Bouchlaghem, D., & Anumba, C. (2010). A scenario-based study on information flow and collaboration patterns in disaster management. *Disasters, 33*(2), 214–238.
63. Shaluf, I. M. (2011). Technological disaster stages and management. *Disaster Prevention and Management, 17*(1), 114–126.
64. Zelenkauskaite, A., Bessis, N., Sotiriadis, S., & Asimakopoulou, E. (2012). Disaster management and profile modelling of IoT objects: Conceptual parameters for interlinked objects in relation to social network analysis. In *Proceedings of the 2012 International Conference on Intelligent Networking and Collaborative Systems (INCoS 2012)* (pp. 509–514).
65. Shamszaman, Z. U., Ara, S. S., Chong, I., & Jeong, Y. K. (2014). Web-of-objects (WoO)-based context aware emergency fire management systems for the internet of things. *Sensors (Switzerland), 14*(2), 2944–2966.
66. Adomavicius, G., & Tuzhilin, A. (2010). Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. *IEEE Transactions on Knowledge and Data Engineering, 17*(6), 734–749.
67. Han, S. N., Lee, G. M., & Crespi, N. (2014). Semantic context-aware service composition for building automation system. *IEEE Transactions on Industrial Informatics, 10*(1), 252–261.
68. Xu, R., Yang, L., & Yang, S.-H. (2013). Architecture design of internet of things in logistics management for emergency response. In *2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing* (pp. 395–402).
69. Yang, H., Yang, L., & Yang, S. (2011). Hybrid Zigbee RFID sensor network for humanitarian logistics Centre management. *Journal of Network and Computer Applications, 34*(3), 938–948.
70. Fajardo, J. T. B., & Oppus, C. M. (2011). A mobile disaster management system using the andriod technology. *International Journal of Communication, 3*(3), 77–86.
71. Walle, B., Eede, G. V., & Muhren, W. (2010). Humanitarian information management and systems, mobile response. In *Second International Workshop on Mobile Information Technology for Emergency Response 2008*, Bonn, Germany, May 29–38, 2008. Revised Selected Papers. Cham, Switzerland: Springer.
72. Akhunzada, A., Gani, A., Anuar, N. B., Abdelaziz, A., Khan, M. K., Hayat, A., et al. (2016). Secure and dependable software defined networks. *Journal of Network and Computer Applications, 61*, 199–221.
73. Akhunzada, A., Sookhak, M., Anuar, N. B., Gani, A., Ahmed, E., Shiraz, M., et al. (2015). Man-at-the-end attacks: Analysis, taxonomy, human aspects, motivation and future directions. *Journal of Network and Computer Applications, 48*, 44–57.
74. Sookhak, M., Gani, A., Talebian, H., Akhunzada, A., Khan, S. U., Buyya, R., et al. (2015). Remote data auditing in cloud computing environments: A survey, taxonomy, and open issues. *ACM Computing Surveys (CSUR), 47*(4), 65.
75. Alam, K. A., Ahmad, R., Akhunzada, A., Nasir, M. H. N. M., & Khan, S. U. (2015). Impact analysis and change propagation in service-oriented enterprises: A systematic review. *Information Systems, 54*, 43–73.
76. Al-Turjman, F. (2017). Cognitive routing protocol for disaster-inspired internet of things. *Future Generation Computer Systems*.
77. Cheng, J. W., & Mitomo, H. (2017). The underlying factors of the perceived usefulness of using smart wearable devices for disaster applications. *Telematics and Informatics, 34*(2), 528–539.
78. Kamruzzaman, M., Sarkar, N. I., Gutierrez, J., & Ray, S. K. (2017). A study of IoT-based post-disaster management. In *2017 International Conference on Information Networking (ICOIN)*. Piscataway, NJ: IEEE.
79. Choe, S., Park, J., Han, S., Park, J., & Yun, H. (2017). A study on the real-time management and monitoring process for recovery resources using internet of things. *International Research Journal of Engineering and Technology (IRJET), 04*(3).

Chapter 28
Spam User Detection Through Deceptive Images in Big Data

Shareena Zafar, Nawal Irum, Sidra Arshad, and Tahir Nawaz

Abstract Image mining has a very emerging sub-domain, namely, web image mining, and researchers are warmly excited towards it. This study presents a deep detail of former studies and ideas that we come up with, i.e. what is Image Mining and what are Web Image Mining techniques. In the domain of web image mining, this study also proposes an idea to recognize and cope with the deceptive images found on the web. It further helps in banning the fraudulent and annoying web users along with solutions in enhancing the users' behavior in social networking websites like Facebook, Twitter, Tumbler, etc., in blogs, and in e-shopping websites like eBay, Amazon, Daraz.pk, Kaymu.pk, etc. Apart from this, the study also mentions nearly of the conceivable future directions for the researchers in aforementioned domain.

28.1 Introduction

The advent of progressive web and multimedia technologies has made the data available on the Internet to be grown rapidly. However, in the contemporary era, the main focus is not only on storing the data but also on storing and then extracting fruitful information from it for making smart decisions in the future. Knowledge discovery is employed for this perseverance of extracting information from enormous size datasets and using it in the future in certain ways. Data is not considered a waste anymore but can be reused to produce new commercial value. The rudimentary objectives of using data mining procedures are to extract valuable knowledge patterns and information from data and to renovate it into understandable formats to be used again. It results in generation of interesting patterns, unknown previously. Data mining is an interdisciplinary field, i.e., a combination of artificial intelligence, statistics, machine learning, and databases [1].

S. Zafar · N. Irum · S. Arshad · T. Nawaz (✉)
Department of Computer Science, University of Lahore (Sargodha Campus), Sargodha, Punjab, Pakistan
e-mail: tahir.nawaz@cs.uol.edu.pk

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_28

Image mining is one of the most interesting areas in the field of data mining, which deals with image data only. The traditional data mining techniques work well with textual content, but do not process an image as it is but according to its description. Image Mining employed in un-structured content works in integration with certain other disciplines including Data Mining, Image Processing, Computer Vision, Artificial Intelligence, Pattern Recognition, Databases, Soft Computing, and Machine Learning. Image Mining is basically a technique that fetches expedient information and discovers substantial patterns from large-scale images without knowing any patterns in advance [2]. The process of image mining involves analysis of the image (including the image pre-processing, object recognition, and feature extraction), image classification by supervised classification or image clustering, and management of the data retrieved from the images [1, 3–6]. The primary objective is to gain all valuable patterns concealed inside an image without having the knowledge of image content. The gained pattern can be of any kind like classification patterns, correlation patterns, description patterns, and spatial or temporal patterns [1]. Image mining can deal with all traits of large image databases, e.g., image storages, image retrieval, and indexing methods. Commonly image mining is done in two major ways. One of them is to mine from large number of images alone, while the other one is to mine from incorporated assortments of images.

Web Image Mining is a special subdivision of Image Mining which involves useful information collection and uses pattern extraction from the huge image contents available on WWW [7]. Similarly data mining when confined to multimedia is termed as web image mining. Web image mining makes use of special image mining techniques to draw conclusions and extract patterns from the images available on the Internet which can be helpful in certain ways [8]. Websites, blogs, and other social media platforms are ample cradle of information on the World Wide Web. With each passing year, these sources of information are increasing in number, and hence their contents, especially the image contents shared on them, have also increased in number. Dealing with image contents and understanding the usage patterns of these informative portals, web image mining can serve the best. In addition, the data congregated can be in structured or unstructured format; therefore, traditional mining techniques may not easily Cope with the work. Web image mining can prove helpful especially when it deals with online shopping portals; the process of understanding and analyzing the images becomes important which can be aided by web image mining.

The Internet is a big source of data, and every passing day, the data available on the World Wide Web is increasing rapidly. This expansion of data on one hand is proving helpful to users and on the other hand is becoming difficult to manage and store. It requires construction of very large datasets referred as big data that can be analyzed to discover expedient patterns, correlations between different things, and new trends. This analysis of big data to extract useful information is what we call data mining. Fraud detection is a very important and emerging domain of mining the big data, which involves analyzing users' behavior and determining deviations from the mainstream. Any deviations from the end-user behavior would point toward a

fraud. For example, there is always a sort of pattern in which an end-user may use his or her credit card for purchasing. Any sudden change in his purchasing behavior can sound suspicious and be detected as a fraud. This detection is possible only if his general behavior is analyzed by storing his data and purchase history and then mining it using certain data mining techniques like outlier analysis. In the same way, big data on the web can be mined to detect anything suspicious.

In contemporary era of technology, the images, web-based systems, online sales/purchases, and socializing are turning out to be exceedingly imperative as the Internet has reduced the distances. The images on the web are quite a big part of the web surfing game. Every blogger, online seller, online buyer, auction administrator, education-related person, social network users, researcher, and almost everyone are somehow directly or indirectly going through billions of images on the web every day. Meanwhile, the modern man is more concerned of what is pleasing, authentic, and valued and what is annoying and fraudulent, while he uses a certain system. Hence the web image mining has become a highly attractive and rising sub-domain of image mining toward which researchers are warmly eager to indulge. This study proposes a web image mining technique to understand and improve the sale, purchase, and socializing behavior in e-shopping portals and social networking websites such as OLX, eBay, Facebook, Twitter, etc. along with some future directions. The rest of the section of this study contains literature review, proposed methodology, conclusion, and future work, respectively.

28.2 Literature Review

In web image mining, a lot of applications from multimedia to e-business have been found out in the research where understanding and improving the web usage behavior of customers, readers, sellers, bloggers, and others while interacting with a website have been made possible by mining algorithms and techniques. This Section uncovers Techniques proposed in various studies from researchers who worked on Image Mining.

One of the most interesting applications of web image mining has been proposed for automatic collection and labeling of celebrity faces from the web, for example, Xiao Zhang, Lei Zhang, Xin-Jing Wang, and Heung-Yeung Shum. A special face annotation system does so in two simple steps. The first step involves labeling an input image with celebrities by identification of the name of a celebrity from the text that appears in surroundings. In the second step, the faces are assigned with celebrity names via the label propagation on a special graph called the facial similarity graph using a name assignment algorithm. This works by first constructing a large-scale dataset called the CFW dataset. Of course there is a huge discrepancy in the appearance of facial features; process of name assignment is limited by employing context likelihood [9] (Fig. 28.1).

Mechanisms on huge visual data on the World Wide Web in the literature of multimedia and computer vision have been studied in context to some specific points

Fig. 28.1 Example of celebrity recognition with CFW dataset [9]

like web image application, visual concept web mining, and real-world sensing web mining [9].

The importance of web usage is quite obvious in business applications for which certain web usage mining techniques are used that explore the end-user's behavior while interacting with a certain website. To aid the techniques of web usage mining in industries, the web data mining algorithms can be combined with the web page's language. An Intelligent Recommender System was proposed by

Samar et al. for the quality evaluation of drinking water and performance evaluation of the recommender system that was just presented [10].

Image mining revolves around large-scale datasets, the creation of which is a hot topic of data science research. A technique for automatic construction of large-scale datasets has been proposed that works well with noisy web images. The approach proposes a rank-order distance-based density score for identification of positive seed images. It basically works according to the idea of images that belong to specific concept which are clustered firmly, while the outliers are usually much dispersed. Iterative positive and negative mining along with adaptive thresholding techniques are employed in this approach. First of all, large-scale noisy images are crawled from the web, and clean seed images are generated from those crawled images. Then by taking a start from the seeds, the dataset has grown further. In this way, the dataset is constructed automatically [11].

Another technique for large-scale image dataset construction makes use of Flicker groups for automatic building of a comprehensive visual resource and then retrieving images by using it. Special re-ranking methods are used that reduce the initial noise. The learning and prediction steps are made scalable by the use of off-the-shelf linear models. The prediction scores of distinct models are then concatenated, resulting in Semfeat image descriptions by retention of only the most noticeable reactions [11].

Christophe et al., in their study based on outlier detection tools and techniques, discussed the problem using customary techniques. They state that a survey by Simmons, Nelson, and Simonsohn [12] showed how, due to the misuse of statistical tools, significant results could easily turn out to be false positives. Identification of outliers through the intervals that span over the mean plus/minus or standard deviations remains a common practice. However, since both the mean and the standard deviation are particularly sensitive to outliers, this method is problematic. The authors highlight the limitations and issues found in using this method and present the median absolute deviation, as an alternative and more robust measure of dispersion, which is easy to implement. In their paper, a robust and easy-to-conduct method for detecting outlying values in univariate statistic, the median absolute deviation, is described. This indicator was initially developed by statisticians, but its psychology is relatively. Whatsoever the method selected, the decision-making concerning the exclusion criteria of outliers is necessarily subjective. More generally, achieving a consensus as to which method is most appropriate and which subjective threshold should be used (regardless of the method used) is of even greater importance. Otherwise, the suspicion that researchers pick the method that yields the most promising results will remain in the air even when, as in most cases, it is unjustified [13].

A mining method for determining frequent image patterns in mammogram images has been proposed with an efficient use of association rules. This approach works in two steps. The first step involves finding the region of interest by digital mammogram segmentation. Median filtering method is used to remove noise, morphological processing is used to remove background artifacts to improve the image quality that also used image enhancement techniques, and the pectoral muscle

is removed completely by using RG algorithm. The second step makes use of the association rules to determine frequent image patterns by image mining. The process involves extracting features and selecting the ones most selective. When a feature is selected, it is discredited, and transaction representation of the input images is generated, which is fed to the a priori algorithm which ultimately generates association rules. It also makes use of the ESAR algorithm. Mammogram images can be diagnosed effectively using these association rules [3].

With so many Web Mining techniques, it is still required to modify and enhance the features of Web Mining applications. Yang and Wu et al. discussed different data mining issues in their identical study underfitting, overfitting, automatic cleaning of data, data oversampling, and scalping up for high-dimensional data, sequence data, and time series data. There are other issues like networks, data stream mining, and dealing with the unstable data. The quality of web data can be improved by Web log pre-processing. But it appears quite difficult for semi-structured data. The pattern extraction techniques in data mining involve two basic approaches, predictive and descriptive mining, with certain algorithms working for this purpose, but none of them works efficiently [4].

In image mining, the preliminary objective is to extract features to acquire significant knowledge discovery from images. There are voluminous features, but to extract the best ones is important, which can be done efficiently by automated techniques. The proposed tools use automated tasks that lessen human intervention, likewise the IClass method. Others include color feature extraction, texture feature extraction, edge feature extraction, and combining features. These feature extraction techniques were also tried in integration with data mining algorithms [14].

Thomas Bayes' theorem is used in statistical influence in data mining, while a given dataset pattern can be defined with the regression theorem which helps in forecasting and predictions. The genetic algorithm invented by John Holland after getting inspired from the natural evolution process follows the principle of Charles Darwin theory of evolution. Data-based distributed systems can be managed with a special open-source software Hadoop. Clustering is performed according to the RGB values of images and patterns that are analyzed. There are a lot of applications of data mining, like neural networks, marketing, telecommunication, Medicare, banking, DNA analysis, criminal investigation, surveillance, and the most interesting image mining that can help a lot in the digital word and make the e-commerce a lot more easy and interesting [15].

CBIR has proved to be an efficient technique for mining the multimedia data available on social networks like Facebook, Flicker, etc. Certain other techniques of image mining have also made this task easier. For example, classification, clustering, CBIR, and image mining using the concepts of CBIR have a great impact [16].

By mining weakly labeled facial images, a web-based face annotation framework was investigated in order to build a database with accurately labeled facial images. With an unsupervised label refinement (ULR) technique, the label quality of web images could be improved. With special optimization algorithms, the large-scale learning tasks could be solved easily [5].

Image segmentation is a technique used for identification of identical areas in an image after it has been divided into different parts. To aid the process of segmentation, a new approach was presented involving steps like image pre-processing, Gaussian 3D blurring for image filtering, histogram equalization, image 5D process, and segmentation stage. The proposed methodology was experimented with various data mining techniques like radial basis function (RBF) neural network, wavelet transform, fuzzy discernibility classifier, harmony search, etc. [6].

Different image mining techniques have been employed in various fields. Gholap et al. proposed content-based tissue image mining as the tissue mining process could be faster if the images of tissues are indexed and mined on content. An image mining technique using pattern identification and certain data mining models were proposed by Sanhay et al. Image gathering, learning, and classification are the three basic steps of this approach. Pattnaik et al. presented an image mining approach using data compression techniques along with clustering. Decision tree-based image processing was used by Kun-Che with an aim to hide significant information in images. Image characteristics can be extracted pixel wise and changed in a table that looks like a database authorizing diverse data mining algorithms to explore them [1].

Image mining involves a few rudimentary steps: image analysis, object recognition, feature extraction, image classification, and data management. Classification of images is done either by supervised classification process or by image clustering. Data management involves storing, indexing, and retrieving images by dissimilar queries like query by associate attributes, by description, or by content [17]. Figure 28.2 gives a graphical representation of the way it all works for image mining.

With invention of more and more digital imaging devices, it has become important to recognize various categories of real-world scenes in images, and this surely needs image mining. A generic image classification system with automated mechanism of acquisition from the web is needed. A novel technique automatically gathers large number of images from the World Wide Web and classifies the images by making the gathered images the training datasets. The system is shown in Fig. 28.3. It has three basic modules: image-gathering module, image classification module, and image-learning module. The congregation module automatically gathers images, learning module extracts features from images, and the classification module classifies images [19].

In order to fold large-scale web images automatically which are relevant to specific concepts, a technique having a knowledge base with as many concepts as possible was proposed. The datasets of images with good quality are collected from analysis function of the surrounding HTML text. Images after being gathered are segmented, and an iterative algorithm then computes a model for probability distribution of the areas formed as a result of segmentation. The learned model finally identifies the visual relevancy of images with the concept [20].

One of the very interesting image mining applications is the automatic web image mining system that works to build a human age estimator based on facial information. The best feature is that it works for all groups and qualities of images. First of all, a large human aging image dataset is being crawled, and then human

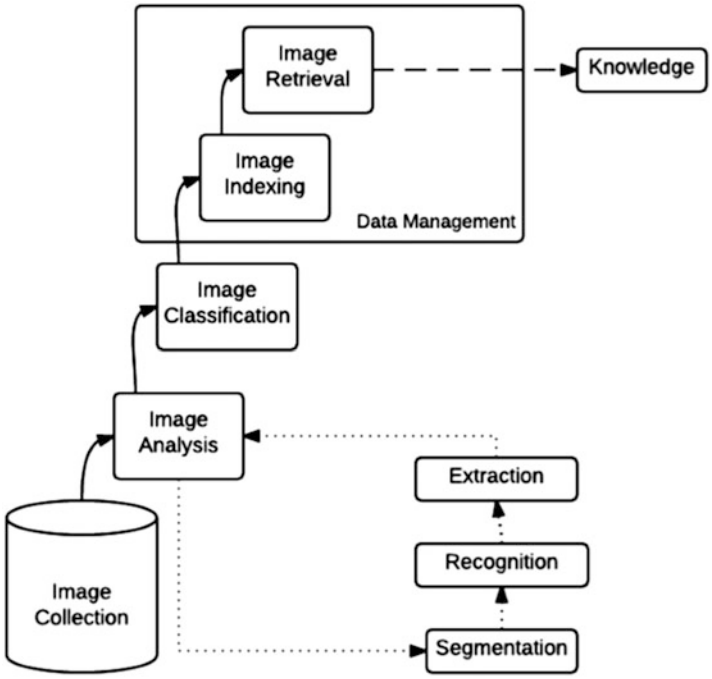


Fig. 28.2 Traditional image mining process [1]

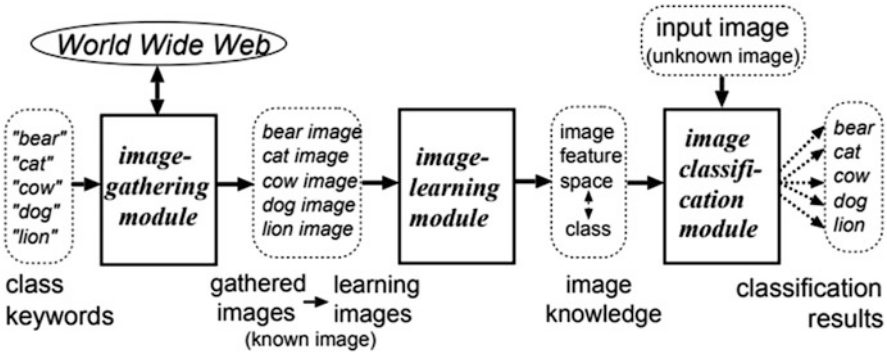


Fig. 28.3 Image-gathering module, image-learning module, and image classification module [18]

face detectors in all images are used in order to detect faces. The image is refined further by an outlier removing phase. Multi-instance regression learning algorithm learns the human age estimator based on kernel regression [8].

Web mining is subcategorized into three classes, namely, web structure mining, web content mining, and web usage mining. Web content mining refers to discovering information from the web pages and web document contents. Web structure

mining involves the analysis of relationship between web pages which are linked by information. Web usage mining is one of the most interesting categories. It involves monitoring the user activity by extracting patterns from logs [21].

Diverse web mining tools include screen-scraper, AA 6.1, WIE, Mozenda, and WCE. The screen-scraper works best for mining websites. It can search databases, and automation anywhere works for retraining the data on web. Both structured and unstructured data can be structured with the Web Info Extractor. By Mozenda, agents can be setup for web data extraction. WCE provides an interface which is friendly and wizard driven [22].

In order to attain boost productivity and success of the CBR method, a novel approach NPRF has been proposed to cope with the large-scale image data. The user query log results in certain navigation patterns in which the feedback iteration can be reduced ensuring efficiency. Effectiveness is ensured by making use of three types of query refinement approaches, i.e., QR, QPM, and QEX [23].

Another study related to automatic image annotation involves image segmentation and feature extraction where feature extraction includes shape feature, texture feature, color feature, and the spatial relationship of the contents inside the images. Furthermore, it involves neural networks and labeling to perform the automatic annotation of images which required a lot of labeled image data that are needed for training of the model using artificial intelligence [24].

28.3 Problem

Every field of life prone to fraudulent activities and deceptions is always there. No doubt the Internet has made our lives quite easy, but it does promote deception as well, misleading the web surfers. This is the reason why we also call it Web of Deception. It is not so hard for an ordinary person now to post something misleading and ambiguous. There are so many online stores whose displayed products seem quite different from the ones they actually trade and the ones they label at their platforms. Spamming is another very common and irritating activity on the web. Taking any action against spammers would require the detection process. First, detection of spammers, spamming materials, and deceptive material on Internet by mining the big data can make the Internet a reliable to surf. And secondly, there's a need to find out how to mine such big data efficiently for fraud detection? Hence the basic objective of this study is to find solutions to these.

28.4 Proposed Methodology and Framework

As per the discussion, the trends of surfing, searching, and decision-making these days have been highly bended toward self-adaption and image-driven strategies. Existing Google and Bing Image Search is improved by utilizing the visual

features of the images and click-through logs. Images on web can be used for visual knowledge and prediction of trends. The face annotations, patterns, image recognition, segmentations, classification, clustering of images, CBIR, and feature extraction are well-practiced and emerging techniques that are developing every day and being used for multiple purposes. But none of these are presently established as being used to judge the incorrect images over the social networking websites and especially in e-shopping portals.

What we are directing toward is that the techniques mentioned above can be further utilized in combination to serve the Internet community by assuring authenticity and truthfulness in online dealings. There are many recent trends and surveys showing that certain people over the World Wide Web are spreading false news images with wrong description for the sake of gaining publicity, more visitors, likes, hits, views etc. hence misleading the users and wasting one's time. To avoid such problems, even more precisely to minimize the risk of being misleader over the Internet and to improve the users' surfing capability, we recommend a way out here. Figure 28.4 shows the general working of the proposed framework, where our proposed solution comprises three parts. The first part is based on the image annotation or features/content extraction out of the images and then listing those feature out in form of a description to identify that image. The second component gets the description extracted out of the images and the actual surrounding text or tags as input and finally compares them both to evaluate whether the image contents are relevant to text or not. Finally, third component checks the spam thresh-hold value for each user post to identify a user is habitual to spam posting or not.

Let's consider an example for elaboration. Suppose somebody on Facebook displays the content like flowers and a lady, while the link or description leading to that image states that it's a shirt and tattoo, and then it can be marked as a deceptive image. In an another example of online dealing (e-shopping), while buying a Rolex watch after opening product details, it shows any local brand name inside the dial of the watch in the picture. Using the above mentioned methodology, such images can be marked as deceptive. Data mining is used to work out deceptive images over the web. This can support for furtherance in user experience in online socializing and online dealings. In this way, analyzing the long-term behavior by examining image content with their text in the huge historical repository would result in finding out the people or area from where the people mostly use to post deceptive images that can further help in taking measures of banning such users/sending clear warning to them, etc.

The details of all three components of the main model for our proposed solution "Spam User Detection Through Deceptive Images" are given below.

28.4.1 Image Feature Extraction Component

As described earlier, this component would extract the features and objects from the images posted by user against a post/product ID. This study has shown

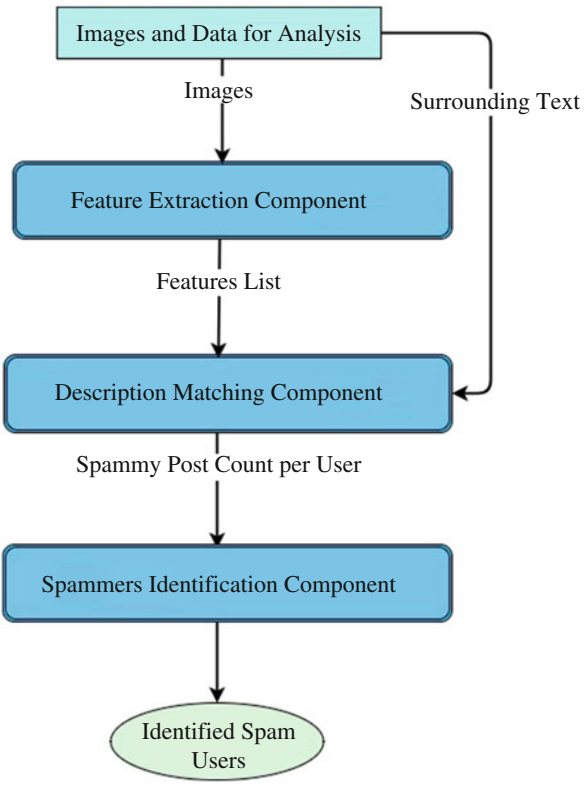


Fig. 28.4 Main model for proposed spam user detection

that techniques like color features, age estimation, texture feature, shape feature, spatial relationship, object recognition, edge recognition, near-duplicate images, segmentation-based classification, CBIR, surrounding text, and image tagging techniques are used to describe or fetch an image. Furthermore, texts tagged around the images provide alternative, helping feature extraction to recognize images and comprehend the content of images. All these in combination would work inside a module to list out the features, contents, and objects in the images in the form of a list for each post ID, and each of the post would further be classified in the third module for every user's ID. The inputs and outputs of this component are graphically represented in Fig. 28.5 where two additional sub-components are represented. These two are the base of whole working.

28.4.2 Image Data Repository

This repository is input to feature extraction module that would store and maintain data collected from target website or e-portal by using different data collecting tools

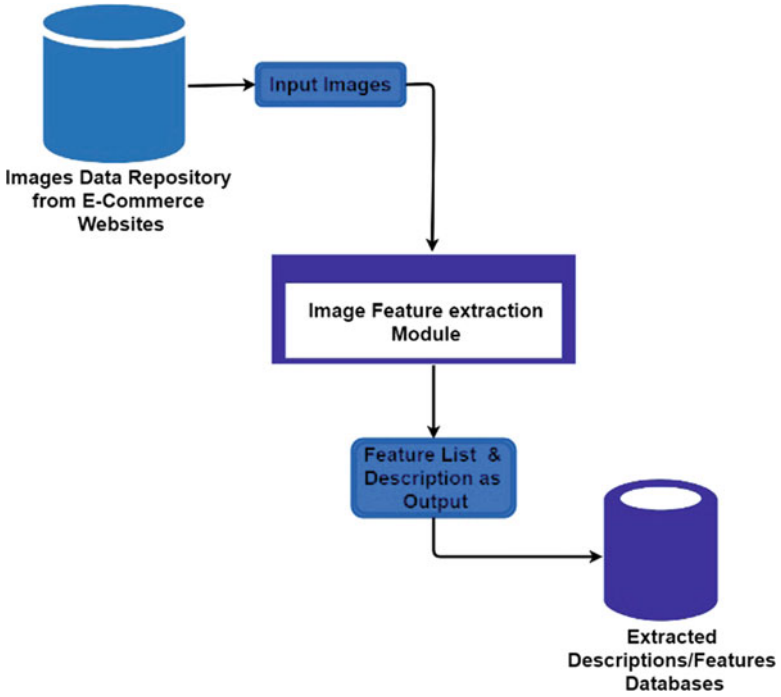


Fig. 28.5 Image feature extraction component

like web scraping and the one described by Keiji Yanai in [18]. The data to be stored in different tables of this repository against post/product ID and user's ID includes the image bytes, image dimensions, image size, image URL, post URL, user's details, top comments, total posts per user, total images per post, spam count, image per post count, posts per user count, related text, etc. The related text can be tags, keywords, category, mentioned colors, image description, title, etc. (all separated by some symbol like ";"). Note that all of the contents are not the input to feature extraction but only the images, while the rest of the data would be used by second and third module.

28.4.3 Extracted Description Repository

The second storage of data is done after the features are extracted out as the output of feature extraction module. This repository would store and maintain data generated as a result of feature extraction that would contain image dimensions, image feature/contents/object list (all separated by ";" separator), and image densities against image and post IDs. This database would be further utilized in the description matching process.

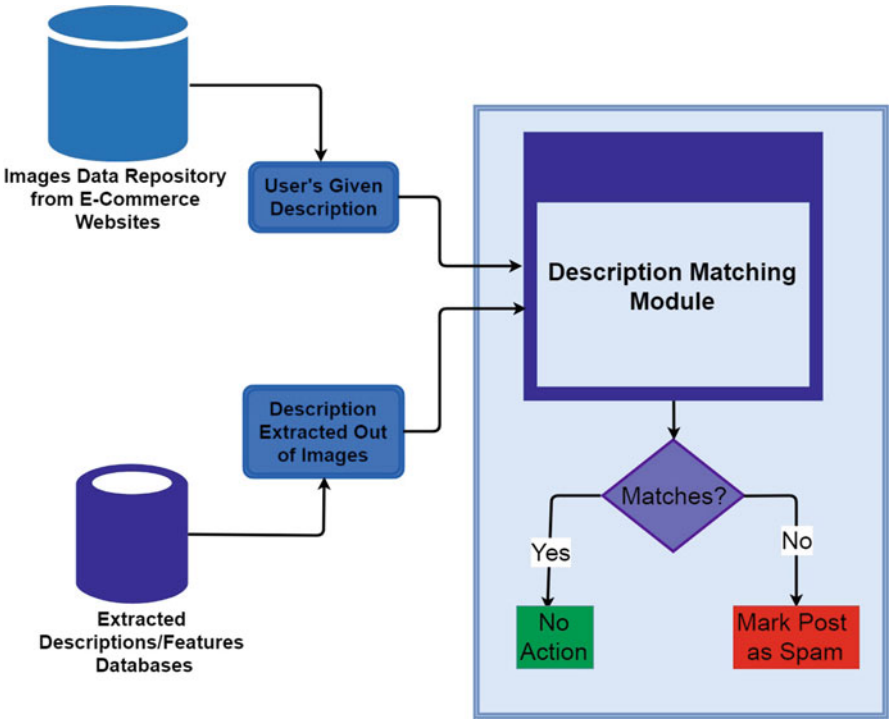


Fig. 28.6 Description matching and spam post identification component

28.4.4 Description Matching Component

Coming toward the classifying module that would decide whether an image from a post is spam or not, Fig. 28.6 demonstrates how this matching works. The module has two inputs, one is the first data store, image data repository (described in the previous section), and the other is second data store (from previous section), the extracted description repository. This module takes description given by user from first data store and objects/feature description from second data store and compares each one (after separating one) with each one, turn by turn.

The threshold for classification proposed to set would be 50% of the total features. Assuming 50% objects of the total features from first data store match with the other, no action would be taken. While if 50% of them do not match, say 65% of the extracted objects in the image didn't match the given description, then this image would be marked as spam, and all other images in the post would be examined.

Now again, if 50% of the total images didn't appear to be spam by the method described above, then the post would be marked as a spam post. Otherwise, no action would be taken (as shown in Fig. 28.6). The spam count per image and per post/product in the first data store has to be automatically updated every time this module works.

28.4.5 Spammer Classification Component

Once the spam posts are classified after a certain time lap, the spam count per post is updated. The task of this component is to analyze the long-term behavior and posting record of individual user one by one by examining the huge historical repository or big data for the spam user. This sounds really a tedious and time-taking job to minimize the time and to avoid exhaustive searching and matching for every individual; the system would be directed to examine the spam post count maintained in the user detail table per user. Figure 28.7 shows the framework for module, where to search the spam count per user from the repository is needed to define a threshold again for this module. System defines this to 50% posts/products of the total posts per user. This sounds more like calculating support and then confidence for 50% posts per user. Hence by looking up the total posts per user and the spam count of the posts per user, the system can identify the deviation from mainstream by him/her. Therefore, suppose the user's more than half posting is spam, then he/she can be considered as a habitual spammer and gets marked as a spam user in the system.

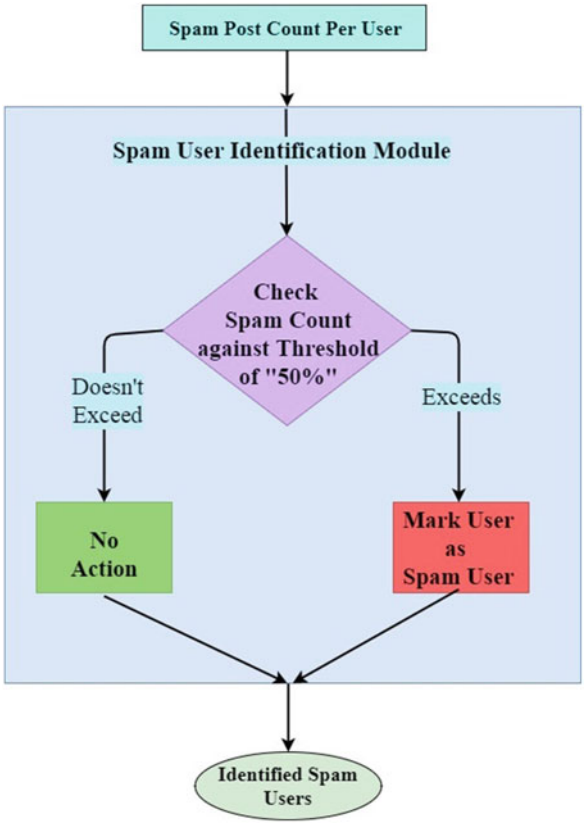


Fig. 28.7 Spam identification component

Every time when this module would work periodically, the list of such users would be returned to the owner of target URL to take action according to company/vender policies that will improve the users' experience.

28.5 Conclusion

Observing various techniques in the field of image mining, it could be concluded that there are lot of applications of image mining starting from multimedia to business applications. Understanding the web usage behavior of customer while interacting with a website has been made possible by image mining algorithms combined with web developing scripts and languages. A special face annotation system is designed with web image mining mechanism automatically collecting and labeling celebrity faces from the WWW. A similar automatic web image mining system is built according to the facial expression information available. Automatic large-scale image dataset construction has also been made possible with certain image mining techniques using rank-order distance-based density score for identification of positive seed images and use of Flicker groups and re-ranking methods. Frequent image patterns can be determined efficiently in mammogram images by using association rules in the mining technique. An automated image mining technique has made the feature extraction process easier in order to obtain significant information from images. The multimedia data available on social networks can be mined efficiently by means of CBIR. To recognize altered brands of real-world scenes in images, a generic image classification system gathers images automatically from web and classifies them. Moreover, there lie some issues in application of certain Image Mining techniques like under-fitting, over-fitting, automatic cleaning of data, data oversampling, and scalping up for high-dimensional, sequence, and time series data.

Meanwhile, contemporary sharing and online dealing community has lots of counterfeit e-business websites, scammers, etc. Even over authentic media, pretenders are always present, and proposed solution can aid the user's experience and reduce the fraud risk on web by extracting any classification of deceptive images and by listing out the images whose content doesn't match the captions or attributes mentioned (if any text related to that image exists). Hence this study proposed a new idea to make the web surfing even better and to reduce the risk of fraud. The overall user's surfing experience over the web in all kinds of social networking websites as well as in e-shopping and e-business websites is improved by collaborating a few techniques like image recognition and associated image tags/text analysis by matching the mentioned features to features extracted out of the image segments and spatial relations. Once the features and precise contents of any certain image over the web (like over blogs, social websites, or e-shopping websites) have been extracted and listed out, these listings can be further made and input to some other technique to take both the image feature and their surrounding text or tags, then finally comparing them both to check whether the images match their title and purpose

or not. The contents extracted out of the images over web and their relevance or irrelevance can then be found and displayed at any certain platform where they are presented. This relevance would then further aid in identifying spammers.

28.6 Future Work

As per the discussion, mining of the image content for advancement of web in addition to the auction behavior and online dealings can be directed to some other aspects. The implementation of the proposed methodology would make the things go smoother than before as the online dealers can then work with an enhanced understanding of their target users' and customers' behavior. However, some other future directions may include the mining of images in user profiles and tracking the long-term profile images rather than recent images to make the judgment even more accurate. This might make another way out toward the advancement in online dealings.

Other than this enhancement, another aspect of web mining can be the mining of images of social media to enhance user experience and to build every social platform to make one feel at ease. This improvement can be made by working for a resemblance search and maintaining multimedia resemblance databases for the social networking websites, i.e., Facebook. This can be achieved by mining of huge repositories and extracting the features by joining the centroid to centers and using artificial intelligence in combination to learn the images and face features adaptively as a "family face feature list." Nowadays, whenever we encounter some broken images on Facebook, it gives us the caption like image may contain two people, a bag, etc., so what we are directing toward is for Facebook to show siblings or family member suggestions through mining for resemblance of family face features in the images uploaded over the web.

Acknowledgments This work is dedicated to our parents who are the reason for us being at this point in our studies and to teachers/advisors who made our basic concepts clear enough for our efforts to be put in such a presentable form. We thank them both for encouraging us toward the research in this domain.

References

1. Sudhir, R. (2011). A survey on image mining techniques: Theory and application. *Computer Engineering and Intelligent Systems, 2*(6), 44–52.
2. Ginsca, A. L., Popescu, A., Borgne, H. L, et al. (2015). Large-scale image mining with flicker groups. In *Multimedia modeling conference*.
3. Deshmukh, J., & Bhosle, U. (2016). Image mining using association rule for medical image dataset. *Procedia Computer Science, 85*, 117–124.

4. Jayalatchumy, D., & Thambidurai, P. (2013). Web mining research issues and future directions – A survey. *Journal of Computer Engineering (IOSR-JCE), 14*(3), 20–27.
5. Wang, D., Hoi, S. C. H., & He, Y. (2011). Ming weakly labeled web facial images for search based face annotation. In *ACM SIGIR* (pp. 535–544).
6. Panda, M., Hassanien, A. E., & Abaraham, A. (2016). *Hybrid data mining approach for image segmentation based classification*. Hershey: IGI Global.
7. Yanai, K. (2015). A review of web image mining. *ITE Transactions on Media Technology and Applications, 3*(3), 156–169.
8. Ni, B., Song, Z., & Yan S. (2009). Web image mining towards universal age estimator. In *Proceedings of the 17th ACM international conference on multimedia.*
9. Zhang, X., Zhang, L., Wang, X. J., et al. (2012). Finding celebrities in billions of web images. *IEEE Transactions on Multimedia, 14*(4), 995–1007.
10. Azab, A. E., Mahmood, A., & El-Aziz, A. (2017). *Effectiveness of web usage mining techniques in business application*. Hershey: IGI Global. https://doi.org/10.4018/978-1-5225-0613-3.ch013.
11. Xia, Y., Cao, X., Wen, F., & Sun J. (2014). Well begun is half done: Generating high-quality seeds for automatic image dataset construction from web. In *Proceedings of European conference on computer vision*.
12. Simmons, J. P., Nelson, L. D., & Simonsohn, U. (2011). False positive psychology: Undisclosed flexibility in data collection and analysis allows presenting anything as significant. *Psychological Science, 22*(11), 1359–1366.
13. Leys, C., Klein, O., Bernard, P., et al. (2013). Detecting outliers: Do not use standard deviation around the mean, use absolute deviation around the median. *Journal of Experimental Social Psychology, 49*, 764e6.4.
14. Foschi, P. G., Kolippakkam, D., Liu, H., & Mandvikar, A. (2002). Feature extraction for image mining. In *Proceeding of the multimedia information systems conference* (pp. 103–109).
15. Bhateja, P., Sehrawat, P., & Bhardawaj, A. (2013). An analysis of data mining, web image mining, and their applications. *International Journal of Information and Computation Technology, 3*(6), 603–608.
16. Mishra, N., & Silakari, S. (2012). Image mining in context of content based image retrieval: A perspective. *International Journal of Computer Science Issues, 9*(4), 69–79.
17. Zahradnikova, B., Duchovicova, S., & Schreiber, P. (2015). Image mining: Review and new challenges. *International Journal of Advanced Computer Science and Applications, 6*(7), 242–246.
18. Rajeshwari, S., & Sharmila, T. S. (2013). Efficient quality analysis of MRI image using preprocessing techniques. In *2013 IEEE conference on information & communication technologies (ICT)* (pp. 391–396).
19. Yanai, K. (2003). *Generic image classification using visual knowledge on the web* (pp. 167–176). Berkeley: ACM Multimedia.
20. Yanai, K., & Barnard, K. (2005). Probabilistic web image gathering. In *ACM SIGMM workshop on multimedia information retrieval* (pp. 57–64).
21. Kumar, A., & Singh, R. K. (2016). Web mining overview, techniques, tools and applications: A survey. *International Research Journal of Engineering and Technology (IRJET), 3*(12), 1543–1547.
22. Herrouz, A., Khentout, C., & Djoudi, M. (2013). Overview of web content mining tools. *The International Journal of Engineering and Science (IJES), 2*(6), 106–110.
23. Su, J. H., Huang, W. J., & Philip, S. Y. (2011). Efficient relevance feedback for content based image retrieval by mining user navigation patterns. *IEEE Transactions on Knowledge and Data Engineering, 23*(3), 360–372.
24. Zhang, D., Islam, M. M., & Lu, G. (2012). A review on automatic image annotation techniques. *Pattern Recognition, 45*(1), 346–362.

Chapter 29
A Tool for Knowledge-Oriented Physics-Based Motion Planning and Simulation

Muhayyuddin Gillani, Aliakbar Akbari, Jan Rosell, and Wajahat Mahmood Qazi

Abstract The recent advancements in robotic systems set new challenges for robotic simulation software, particularly for planning. It requires the realistic behavior of the robots and the objects in the simulation environment by incorporating their dynamics. Furthermore, it requires the capability of reasoning about the action effects. To cope with these challenges, this study proposes an open-source simulation tool for knowledge-oriented physics-based motion planning by extending *The Kautham Project*, a C++-based open-source simulation tool for motion planning. The proposed simulation tool provides a flexible way to incorporate the physics, knowledge, and reasoning in planning process. Moreover, it provides ROS-based interface to handle the manipulation actions (such as push/pull) and an easy way to communicate with the real robots.

29.1 Introduction

Planning and simulation play an important role in robotics research. These are essential tools for the development of strategies and algorithms in various areas of robotics such as motion planning, grasping, and manipulation. Moreover, these tools allow to demonstrate the proposed strategies under different environmental conditions and constraints. The existing software for robotics can be classified into two categories: *single domain* and *multi domain* software. The former are designed to address the problem in a specific domain of robotics. For instance, *GraspitIt!* [14]

M. Gillani (✉) · A. Akbari · J. Rosell
Institute of Industrial and Control Engineering, Universitat Politècnica de Catalunya, Barcelona, Spain
e-mail: muhayyuddin.gillani@upc.edu; aliakbar.akbari@upc.edu; jan.rosell@upc.edu

W. M. Qazi
Department of Computer Science, COMSATS University Islamabad, Lahore Campus, Pakistan
e-mail: wmqazi@cuilahore.edu.pk

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1_29

is developed to study the grasp planning problems, while *MoveIt!* [19], *Robotic Library* [3], and *OpenRave* [8] are used to study the motion planning issues. On the contrary, the latter are designed in a generalized way to study the multiple domain problems, such as *Simox* [21] that is designed to study motion planning and grasping or *The Kautham Project* [17] that is used to study task and motion planning.

To capture the realistic behavior in simulation, it is required to incorporate the dynamics of the robot and the environment. Simulation of dynamics is a challenging task due to the fact that robotic systems are nonlinear in nature and due to the difficulty in determining the exact values of the parameters involved (such as forces that are acting on the system). To handle these issues the use of physics engines (such as ODE, www.ode.org and Bullet, bulletphysics.org) in robotic simulations is becoming popular. These engines provide a good approximation of rigid-body dynamics. Moreover, physics engines are also used to develop the dynamic simulators, such as Gazebo (gazebosim.org) which provide a dynamic simulation environment for robotics. Beside the core robotic software, various middle-ware frameworks (such as ROS [16] and OROCOS [6]) are proposed to manage the communication between simulation and robot hardware. These middle-wares help greatly to simplify interprocess communications and synchronization issues.

The increasing complexity in the robotic systems, such as those including collaborative robots (new generation of industrial robots) or humanoid robots, set new challenges for robotic software. These challenges involve the rich semantic description of the environment for the understanding of the scene, the incorporation of dynamics in planning, the capability of reasoning about the performed actions, and computational efficiency. It is difficult to find a software that addresses all these challenging issues. The current study contributes along this line and proposes a simulation framework for knowledge-oriented physics-based motion planning. The current proposal extends *The Kautham Project* by integrating the ontological knowledge, reasoning, and physics in the planning process.

The rest of the paper is structured as follows. The proposed framework is explained in Sect. 29.2. It involves the summary of the dependencies of the proposed simulation framework, a brief overview of *The Kautham Project*, and implementation details of how physics, knowledge, and reasoning in planning process have been incorporated. Finally Sect. 29.3 concludes the study.

29.2 Knowledge-Oriented Physics-Based Planning Framework

The proposed framework (Fig. 29.1) is developed by extending *The Kautham Project*. This section will briefly explain *The Kautham Project* and the implementation details of the proposed extensions for incorporating knowledge, reasoning, and physics in planning.

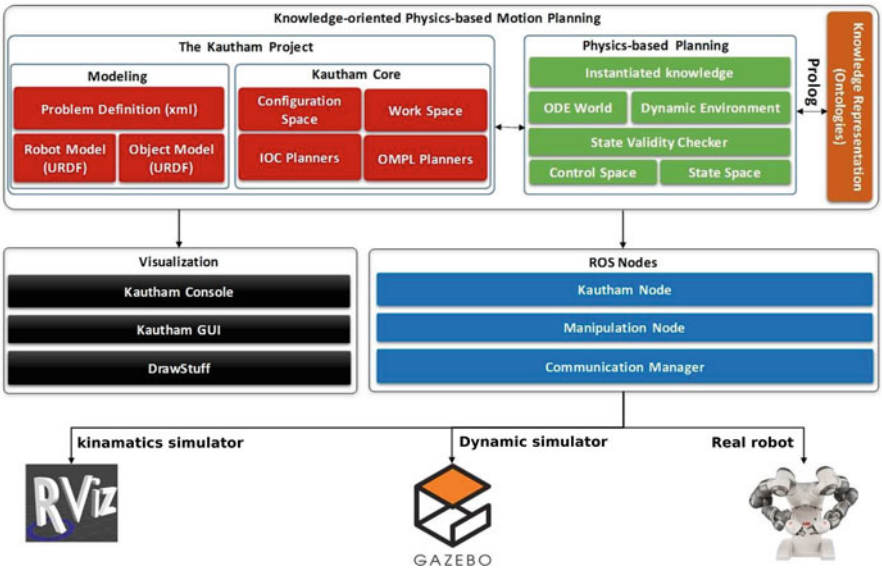


Fig. 29.1 Simulation framework for knowledge-oriented physics-based motion planning

29.2.1 Dependencies

The robotic simulation software depends on several concepts such as robot modeling, 3D rendering, and collision checking. It is difficult to develop a standalone application from scratch; and therefore, in order to incorporate such features, usually already existing libraries are used. The major dependencies of knowledge-oriented physics-based planning framework are those of *The Kautham Project*. It is developed using C++ and uses many features of C++11 such as *std* features. It uses the CMake (www.cmake.org) build system and it is available under GIT (git-scm.com) version control system, and can be downloaded from sir.upc.ed/kautham. The GUI is designed in Qt (qt-project.org), 3D rendering is performed using Coin3D (www.coin3d.org). Robots and obstacles are defined using the Unified Robotic Description Format (URDF, http://wiki.ros.org/urdf), and the Eigen library (http://eigen.tuxfamily.org/) is used for linear algebra. The Open Motion Planning library (OMPL [20]) is used as planning core. It provides various sampling-based motion planners such as RRT [13], PRM [12], and KPIECE [18]. Moreover, it also provides the capability of planning in state space where ODE is used as state propagator. The current proposal enhances the use of ODE in planning process to incorporate physics using knowledge-based reasoning. The knowledge is represented using Web Ontology Language (OWL [4]) and the Prolog language (http://www.swi-prolog.org/) is used for the reasoning over knowledge.

Fig. 29.2 (**a**) An example of a problem file. (**b**) An example of a control file

29.2.2 The Kautham Project

The Kautham Project is a C++-based open-source software for motion planning. It is used for teaching and research purposes at the Institute of Industrial and Control Engineering (IOC-UPC). For research, it is used to develop and demonstrate the motion planning algorithms, particularly for mobile and dexterous manipulators (arms equipped with anthropomorphic hands and a mobile base).

Modeling A motion planning problem is described using an XML file (Fig. 29.2). It consists of four components: robot model, object model, controls, and planner. The main parameters that are specified for robots/objects are the path to the corresponding model, translation limits (in case of mobile base), and initial position with respect to the world frame. Controls are used to define the way how the degree-of-freedoms (dof) will be actuated. In the simplest case, one control per dof is considered. Controls can also be specified for obstacles (detailed explanation of controls can be found in [17]). The final part of the problem XML file specifies the name of the planner used (such as RRT), the planning parameters (such as planning time and goal bias), and the query that contains the start and the goal configurations.

A robot is defined as a kinematic tree with optional mobile base, its configuration space is $R = SE(3) \times \mathbb{R}^n$, where n represents the number of joints of the robot. In case of fixed base, the $SE(3)$ part is represented as null. The kinematic structure of the robot is defined using URDF (Fig. 29.3). It contains the visual robot model, the collision model, transformations between the links, joints (along with limits), and dynamic parameters such as damping and masses. The visualization model is defined with triangular meshes that can be represented in *.wrl*, *.stl*, and *.dae*

```
<link name="link_1_r">
  <inertial>
    <origin xyz="0 -0.03 0.12"/>
    <mass value="2"/>
    <inertia ixx="0.1"  ixy="0"  ixz="0" iyy="0.1" iyz="0" izz="0.1" />
  </inertial>
  <visual>
    <geometry>
      <mesh filename="YuMi/link_1.stl"/>
    </geometry>
  </visual>
  <collision>
    <origin xyz="-0.003 -0.023 0.069" rpy="1 0.44 0"/>
    <geometry>
      <box size="0.075 0.082 0.08"/>
    </geometry>
  </collision>
</link>

<joint name="joint_1_r" type="revolute">
  <parent link="body"/>
  <child link="link_1_r"/>
  <origin xyz="0.05355 -0.0725 0.41492" rpy="-0.9781 -0.5716 -2.3180"/>
  <axis xyz="0 0 1"/>
<limit effort="300.0" lower="-2.9394" upper="2.9394" velocity="3.14"/>
  <dynamics damping="0.5"/>
</joint>
```

(a)

```
<?xml version="1.0"?>
<robot name="table">
   <link name="base">
   <inertial>
        <origin xyz="0 0 0" rpy="0 0 0"/>
        <mass value="3"/>
        <inertia ixx="0.0683333"  ixy="0"  ixz="0"
                 iyy="0.0683333" iyz="0" izz="0.0683333"/>
   </inertial>
   <visual>
       <origin xyz="0 0 -0.028" rpy="0 0 0" />
       <geometry>
        <mesh filename="tablewood.dae"/>
       </geometry>
    </visual>
    <collision>
        <origin xyz="0 0 0" rpy="0 0 0" />
        <geometry>
              <box size="0.1399 0.0988 0.05586" />
        </geometry>
        <material>
              <color rgba="0.5 0.5 0.5 1" />
        </material>
        </collision>
   </link>
</robot>
```

(b)

Fig. 29.3 (**a**) A part of the URDF file of the robot. (**b**) The URDF model of the table

formats. The collision model can be represented either by a triangular mesh or by primitive shapes (cylinder, box, and sphere). Obstacles are also defined as robot data structures, in case of fixed obstacles, none of its dof are actuated.

Kautham-Core It consists of the workspace, the configuration space, and a set of planners. Once a problem is loaded, it fills the data structures of the workspace (that includes the robot/obstacle models, their kinematic limits), and of the configuration space. Moreover, it contains the methods for collision checking using PQP [11] or FCL [15], and forward kinematics to move the robot to the particular configuration. To sample the configuration space various state samplers (such as random, Gaussian, and Halton) are included.

Two families of planning algorithms are implemented in *The Kautham Project*, IOC planners and OMPL planners. The former contains potential field-based planners using navigation functions [5] and harmonic functions [7]. The latter contains the sampling-based geometric and kinodynamic planners (such as RRT, PRM, and EST) offered by OMPL. The detailed explanation regarding the implementation of planners can be found here https://sir.upc.edu/projects/kautham/.

29.2.3 Physics-Based Planning

Physics-based motion planners have recently emerged as an extension to the kinodynamic motion planners, in which the robot can interact with the objects in the environment to purposefully manipulate. These interactions are modeled using rigid-body dynamics. The tree-based kinodynamic motion planners can easily be

extended for physics-based planning by replacing the state propagator with dynamic engines (such as ODE). Moreover, the extension requires the proper definition of the state validity checker, the contact dynamics, and the control space.

To enable the physics-based planning, ODE is used to handle the rigid-body dynamics during propagation. It is an open-source C++-based dynamic engine widely used in the robotics community. Moreover, OMPL provides a flexible way of using ODE as state propagator. From the input files, the robot(s) and object(s) and their properties (such as masses) are read and the ODE bodies are then created using triangular meshes, although in case of simple shapes (such as box, sphere, or cylinder), ODE primitive shapes are created. The kinematic tree that represents the robot in the dynamic world is created by adding the joints between the robot bodies. A motor (linear or angular, depending on the joint type) is added to each joint to control the joint velocities and torques. Once the ODE world is created, a dynamic environment class (with the name of the robot, such as *YumiDynamicEnviroment*) is derived from the *OpenDEEnvironment* class provided by OMPL. The derived class reimplements the functions by defining the control dimensions, control bounds, the way of applying controls, the contact parameters (such as friction, slip, bounce velocity), and the way of evaluating the collisions.

The control dimensions are set equal to the number of actuated degree-of-freedoms and the control bounds define the control (velocity or torque) limits for each joint. A method is provided to define the way of applying the controls. The controls can be joint velocities with maximum allowed torque limits (that the motor can exert to achieve the desired velocity). Contact parameters are defined between each pair of bodies in contact, describing the interactions. For instance, when an interaction takes place between two bodies, these parameters define how many contact points must be considered, what is the value of the friction coefficient, what is the bounce velocity, what is the constraint force mixing (CFM), and the error reduction parameter (ERP). CFM and ERP are ODE parameters that model the damping and spring behavior of the contact. These contact parameters must be defined carefully because inappropriate values may result in unstable behaviors.

Since physics-based planning allows the dynamic interactions in planning, the way of evaluating collision needs to be modified. Collisions with fixed objects will be forbidden, but collision with movable objects will be allowed, although collision with some movable object may be allowed only from certain parts. For instance, the collision with a car-like object is allowed only from the front or rear side and forbidden along the sides. The differentiation of the objects according to their collision properties is a challenging issue. It is handled by incorporating the contact constraints in the knowledge as explained in Sect. 29.2.4. The state validity checker will evaluate the satisfaction of the constraints that are imposed by the knowledge.

The state space of each body (robot link or obstacle) in a dynamic environment is 12 dimensional (three for position, three for orientation, three for linear velocity, and three for angular velocity). It is represented as an OMPL *OpenDEStatepace* that is a compound state space with three real vector spaces and one SO(3) space for orientation. The state space implements the distance function to measure the

distance between two states. The proposed framework provides two implementations of distance function that measure the distance in the workspace and in the configuration space. To measure the former, the position of the TCP is projected in the workspace and the Cartesian distance is measured there. Whereas the latter measures the distance between two configurations.

The implementation of the control space includes different of sampling methods. Since physics-based planning is computationally intensive, the complexity can be reduced by implementing robust control sampling strategies. The current implementation provides a random control sampler, a heuristic-based control sampler, and a power-efficient control sampler. The heuristic-based control sampler samples n controls and selects the one that results in a state closer to the goal state. The power-efficient control sampler adapts the control sampling strategy according to the region of the state space, i.e., if the robot is in contact with an object the sampling strategy computes the minimum force that is required to push the target object and sample the controls accordingly.

All control-based planners offered by OMPL can be used for knowledge-oriented physics-based planning. For every planner we need to set a pointer to the defined dynamic environment, state space, and control space. The planners such as RRT, KPIECE, EST, and SyCLoP are already available for planning. Other planners such as SST can be incorporated easily.

29.2.4 Knowledge Representation and Reasoning

Knowledge is represented with ontologies using OWL, which is a formal way of representing knowledge in terms of classes. These classes contain information about the robot (robot kinematic and dynamic properties) and about the environment (the objects and their relationship with each other). The relation among classes is defined based on axioms. The axioms are facts that are used for conceptual understanding. We used the protégé editor (http://protege.stanford.edu/) to formulate ontologies (they can be found at https://sir.upc.edu/projects/ontologies/). Domain specific ontologies can be easily defined to handle other planning domain problems, such as task planning.

To enhance the planning process with knowledge, the knowledge is fetched from the ontologies and stored in *instantiated knowledge*. The *instantiated knowledge* is a low-level representation of knowledge that contains the type of the objects, such as manipulatable or fixed, and their contact constraints. These constraints are modeled by specifying regions around the objects, such that the robot can interact with the objects only from these regions. Moreover, other types of constraints can be introduced easily such as the manipulation constraints (constraints over orientation that robot has to maintain during manipulation). The detailed explanation of instantiated knowledge can be found in [9].

The reasoning module is defined in Prolog, which is a language of facts and rules that defines predicates for the knowledge-based reasoning. The predicates are

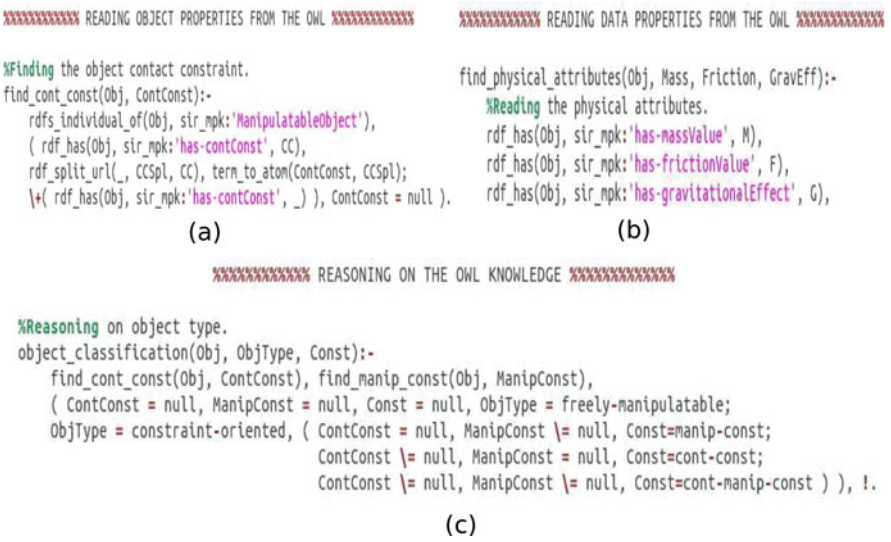


Fig. 29.4 Examples of Prolog predicates (**a**) represents the predicate for the object properties, (**b**) describes the predicate for the object data properties, and (**c**) describes the predicate for reasoning over the object types

defined in a file (with extension .pl). While creating the ODE world, the Prolog environment is initialized and reads the knowledge from the OWL using predefined predicates. Some examples of the Prolog predicates are shown in Fig. 29.4. The predicates to access object and data properties are shown in Fig. 29.4a, b, respectively. The predicate *find_cont_const(obj, ContConst)* takes the name of ODE body (from ODE world) as input and returns the associated contact constraints. *find_physical_attribute(obj,Mass.Fric- tion,GravEff)* reads the physical properties of the bodies in the ODE world. The predicate described in Fig. 29.4c is an example of the reasoning over OWL for the object classification. The predicate *object_classification(obj,objectType,Const)* reasons about the types of the object and classifies them accordingly into the manipulatable and fixed objects, along with their constraints (contact and manipulation). The Prolog predicates fetch the knowledge from the ontologies and fill the data structures of the *instantiated knowledge* that is used by the motion planner. According to the problem domain, more predicates can be easily defined.

29.2.5 Visualization

The proposed framework uses the *Kautham-GUI* tool for the visualization of the scene. It provides the visualization of the robot model, the collision model,

and the visualization of the configuration space (or a projection of it when its dimension is greater than three). The scene can also be visualized with *DrawStuff* (OpenGL-based ODE viewer). It provides the visualization of the collision model, the actual robot/object model, and the mesh views. Figures 29.5 and 29.6 depict the visualization using *Kautham-GUI* and *DrawStuff*, respectively. The numerical results of a query (such as a list of configurations of the solution path) can also be viewed using *Kautham-Console* that is a console-based interface of *The Kautham Project*.

29.2.6 ROS Nodes

The Kautham Project provides a ROS-based interface through a node called *Kautham-Node*. It provides the services such as *OpenProblem*, *SetQuery*, *Solve*, and *GetPath*. The current proposal implements two further nodes, *manipulation*

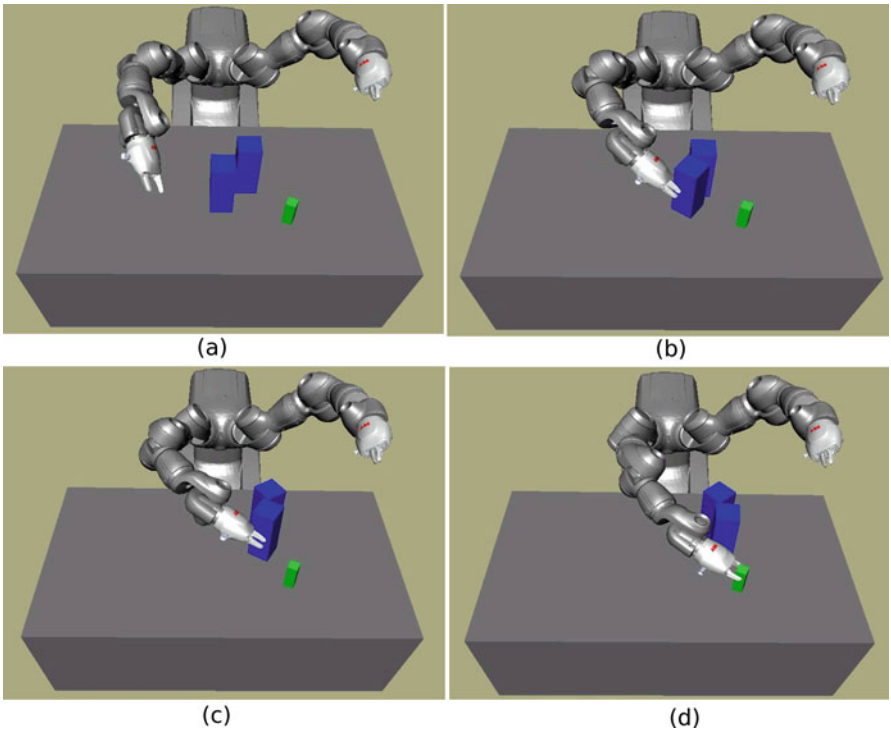


Fig. 29.5 Visualization with the *Kautham-GUI*. (**a**)–(**d**) Show the sequence of snapshots of the robot motion to grasp the green box

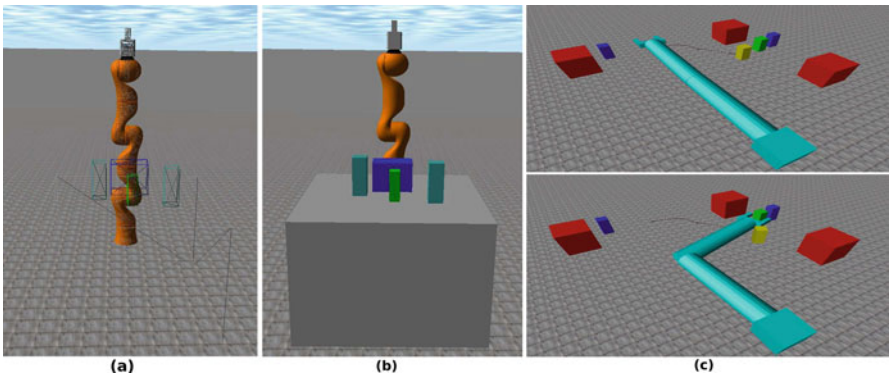


Fig. 29.6 Visualization with *Drawstuff*. (**a**, **b**) Depict the triangular mesh view and the actual view of the scene. (**c**) Show the initial and goal state of a planar robot

node and *communication manager* for handling the manipulation queries and communicating with the real robot or a third party simulation environment, such as Gazebo.

Manipulation Node The manipulation node extends the functionality of the Kautham node. It is capable of handling the manipulation queries such as push or pull queries. A manipulation query is defined by specifying a target object (that will be pushed or pulled by the robot), the type of manipulation action (such as push, pull, or move) and other planning parameters (such as planning time). In response it returns the controls and durations that are to be applied to move the robot from the start to the goal state by satisfying the constraints.

Communication Manager The communication manager is another ROS node that manages the communication between the software and the real robot. It provides the services to set the query for the manipulation node and sends the computed path to the real robot via ROS/ROS Industrial and receives the feedback from the real robot, such as joint states. Moreover, it also provides the communication between the planning framework and Gazebo or Rviz (http://wiki.ros.org/rviz) to visualize the computed path.

29.3 Conclusions

This paper described a simulation tool for knowledge-oriented physics-based motion planning by extending *The Kautham Project*. It provides an easy and reliable way to incorporate the rigid-body dynamics and the knowledge-based reasoning (about the action effects) in planning process. It also provides the manipulation node to easily handle the manipulation queries (such as push/pull). The proposed simulation tool also provides an easy way to communicate with real robot through

the ROS-based communication manager that manages the communication between the proposed tool and the real robot. This simulation tool is used in several research studies, such as [1, 2, 10].

Acknowledgment The work of the authors was partially supported by the Spanish Government through the projects DPI2013-40882-P and DPI2016-80077-R.

References

1. Akbari, A., Gillani, M., & Rosell, J. (2015). Task and motion planning using physics-based reasoning. In *IEEE 20th International Conference on Emerging Technologies Factory Automation (ETFA)* (pp. 1–7).
2. Akbari, A., Gillani, M., & Rosell, J. (2016). Task planning using physics-based heuristics on manipulation actions. In *IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA)* (pp. 1–8).
3. Andre, G. (2011). A software architecture for robot control and its application to social robotics. In *Proceedings of the IEEE International Conference on Robotics and Automation: Workshop on Open Source Software in Robotics*.
4. Antoniou, G., & van Harmelen, F. (2003). Web ontology language: OWL. In S. Staab & R. Studer (Eds.), *Handbook on ontologies in information systems* (pp. 67–92). Berlin: Springer.
5. Barraquand, J., Langlois, B., & Latombe, J. C. (1992). Numerical potential field techniques for robot path planning. *IEEE Transactions on Systems, Man, and Cybernetics, 22*(2), 224–241.
6. Bruyninckx, H., Soetens, P., & Koninckx, B. (2003). The real-time motion control core of the OROCOS project. In *IEEE International Conference on Robotics and Automation (ICRA)* (pp. 2766–2771).
7. Connolly, C. I., & Grupen, R. A. (1993). The applications of harmonic functions to robotics. *Journal of Robotic Systems, 10*(7), 931–946.
8. Diankov, R. (August 2010). *Automated Construction of Robotic Manipulation Programs*. PhD thesis, Carnegie Mellon University, Robotics Institute.
9. Gillani, M., Akbari, A., & Rosell, J. (2015). Ontological physics-based motion planning for manipulation. In *Proceedings of the IEEE International Conference on Emerging Technologies Factory Automation (ETFA)* (pp. 1–7).
10. Gillani, M., Akbari, A., & Rosell, J. (2016). Physics-based motion planning: Evaluation criteria and benchmarking. In *Robot 2015: Second Iberian Robotics Conference* (pp. 43–55). Cham: Springer.
11. Gottschalk, S., Lin, M., Manocha, D., & Larsen, E. (1999). PQP–the proximity query package. http://gamma.cs.unc.edu/SSV/.
12. Kavraki, L. E., Svestka, P., Latombe, J. C., & Overmars, M. H. (1996). Probabilistic roadmaps for path planning in high-dimensional configuration spaces. *IEEE Transactions on Robotics and Automation, 12*(4), 566–580.
13. LaValle, S. M., & Kuffner, J. J. (2001). Randomized kinodynamic planning. *The International Journal of Robotics Research, 20*(5), 378–400.
14. Miller, A. T., & Allen, P. K. (2004). Graspit! A versatile simulator for robotic grasping. *IEEE Robotics & Automation Magazine, 11*(4), 110–122.
15. Pan, J., Chitta, S., & Manocha, D. (2012). FCL: A general purpose library for collision and proximity queries. In *IEEE International Conference on Robotics and Automation (ICRA)* (pp. 3859–3866). Piscataway: IEEE.
16. Quigley, M., Conley, K., Gerkey, B., Faust, J., Foote, T., Leibs, J., et al. (2009). ROS: An open-source robot operating system. In *ICRA Workshop on Open Source Software* (Vol. 3, pp. 5).

17. Rosell, J., Pérez, A., Aliakbar, A., Gillani, M., Palomo, L., García, N., et al. (2014). The Kautham project: A teaching and research tool for robot motion planning. In *IEEE International Conference on Emerging Technologies Factory Automation (ETFA)* (pp. 1–8).
18. Sucan, I., & Kavraki, L. E. (2012). A sampling-based tree planner for systems with complex dynamics. *IEEE Transactions on Robotics, 28*(1), 116–131.
19. Suçan, I. A., & Chitta, S. (2013). MoveIt! http://moveit.ros.org.
20. Şucan, I. A., Moll, M., & Kavraki, L. E. (2012). The open motion planning library. *IEEE Robotics & Automation Magazine, 19*, 72–82. http://ompl.kavrakilab.org.
21. Vahrenkamp, N., Kröhnert, M., Ulbrich, S., Asfour, T., Metta, G., Dillmann, R., et al. (2013). Simox: A robotics toolbox for simulation, motion and grasp planning. In *Intelligent autonomous systems* (Vol. 12, pp. 585–594). Berlin: Springer.

Correction to: DEAR-2: An Energy-Aware Routing Protocol with Guaranteed Delivery in Wireless Ad-hoc Networks

Muhammad Umair Hassan, Muhammad Shahzaib, Kamran Shaukat, Syed Nakhshab Hussain, Muhammad Mubashir, Saad Karim, and Muhammad Ahmad Shabir

Correction to:
Chapter 20 in: M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing, https://doi.org/10.1007/978-3-319-99966-1_20

The original version of the book was inadvertently published with the incorrect Affiliation of Muhammad Umair Hassan, Muhammad Mubashir and Muhammad Ahmad Shabir. The Affiliation detail has now been corrected from "University of Jian, Jian, China" to "University of Jinan, Jinan, China".

The updated online version of this chapter can be found at https://doi.org/10.1007/978-3-319-99966-1_20

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing, https://doi.org/10.1007/978-3-319-99966-1_30

Index

M. A. Jan et al. (eds.), *Recent Trends and Advances in Wireless and IoT-enabled Networks*, EAI/Springer Innovations in Communication and Computing,
https://doi.org/10.1007/978-3-319-99966-1

Z