Advances in Intelligent Systems and Computing 548

Anis Laouiti
Amir Qayyum
Mohamad Naufal Mohamad Saad
Editors

Vehicular Ad-Hoc Networks for Smart Cities

Second International Workshop, 2016

Springer

Advances in Intelligent Systems and Computing

Volume 548

Series editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland
e-mail: kacprzyk@ibspan.waw.pl

About this Series

The series "Advances in Intelligent Systems and Computing" contains publications on theory, applications, and design methods of Intelligent Systems and Intelligent Computing. Virtually all disciplines such as engineering, natural sciences, computer and information science, ICT, economics, business, e-commerce, environment, healthcare, life science are covered. The list of topics spans all the areas of modern intelligent systems and computing.

The publications within "Advances in Intelligent Systems and Computing" are primarily textbooks and proceedings of important conferences, symposia and congresses. They cover significant recent developments in the field, both of a foundational and applicable character. An important characteristic feature of the series is the short publication time and world-wide distribution. This permits a rapid and broad dissemination of research results.

Advisory Board

More information about this series at http://www.springer.com/series/11156

Anis Laouiti · Amir Qayyum
Mohamad Naufal Mohamad Saad
Editors

Vehicular Ad-Hoc Networks for Smart Cities

Second International Workshop, 2016

Springer

Editors
Anis Laouiti
Telecom SudParis
Institut Mines-Telecom
Paris
France

Amir Qayyum
Capital University of Science
and Technology
Islamabad
Pakistan

Mohamad Naufal Mohamad Saad
Universiti Teknologi Petronas
Seri Iskandar
Malaysia

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-981-10-3502-9 ISBN 978-981-10-3503-6 (eBook)
DOI 10.1007/978-981-10-3503-6

Library of Congress Control Number: 2017932010

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

Preface

It is a great honor for us to welcome you to Kuala Lumpur to participate in the Second International Workshop on Vehicular Ad hoc Networks for Smart Cities. Vehicular communication is a key technology in intelligent transportation systems. For many years, the academic and industrial research communities have been investigating these communications in order to improve efficiency and safety of future transportation. Vehicular networking will offer a wide variety of applications, including safety and infotainment. It is envisioned that communicating vehicles of the future will evolve in intelligent environments, known as smart cities. In this context, the interaction between vehicles and intelligent infrastructures will influence each other, to achieve their targets. Not only the car drivers would travel in an efficient and safe manner but the smart cities would also offer the best living conditions for citizens by reducing air and noise pollutions for the inhabitants, and reducing traffic congestion with a better traffic information system for cars. Efficient interaction between vehicles and smart cities' infrastructures is naturally needed to reach these goals.

IWVSC'2016 aims at providing a forum to bring together people from both academia and industry, to discuss recent developments in vehicular networking technologies and their interaction with future smart cities, in order to promote further research activities and challenges. We hope you will find the technical program and the keynote talk very beneficial.

Producing a conference is always a team effort involving many volunteers and we would like to thank the team that made IWVSC 2016 possible. In particular, we are greatly indebted to our Technical Program Committee members who worked hard to produce a comprehensive, high-quality program. In addition, IWVSC features one keynote speech on one of the hot topics of the moment for the VANETs namely vehicular ad hoc networks and the promising 5G.

Last but not least, we are also grateful to all authors for their submissions. We hope that you will find this program interesting and that the workshop will provide you valuable opportunities to share ideas with other researchers and practitioners around the world.

Kuala Lumpur, Malaysia
August 2016

Anis Laouiti
Amir Qayyum
Mohamad Naufal Mohamad Saad

Contents

IWVSC 2016 Workshop Organization

General Chairs

Anis Laouiti, Telecom SudParis, France
Mohamad Naufal Mohamad Saad, Universiti Teknologi Petronas, Malaysia
Amir Qayyum, Capital University of Science and Technology, Pakistan

Publicity Chair

Dhavy Gantsou, University of Valenciennes, France

Program Committee

Nasrullah Armi, Indonesian Institute of Sciences, Indonesia
Azlan Awang, Universiti Teknologi Petronas, Malaysia
Saadi Boudjit, University of Paris 13, France
Dhavy Gantsou, University of Valenciennes, France
Yacine Ghamri, University La Rochelle, France
Fatma Hrizi, Telecom SudParis, France
Anis Laouiti, Telecom SudParis, France
Saoucene Mahfoudh, King Abdulaziz University, Saudi Arabia
Paul Muhlethaler, Inria, France
Muhammad Asim Rasheed, MNS university, Pakistan
Amir Qayyum, Capital University of Science and Technology, Pakistan
Naufal Saad, Universiti Teknologi Petronas, Malaysia
Abed Ellatif Samhat, Lebanese University, Lebanon
Ahmed Soua, NIST, USA
Hajime Tazaki, IIJ Innovation Institute, Japan
Muhammad Zeeshan, NUST, Pakistan

Sponsoring

Telecom SudParis, Institut Mines-Telecom, France
Universiti Teknologi Petronas, Malaysia
Capital University of Science and Technology, Pakistan

Part I
Vanet MAC Layer and Routing Protocols Track

Hybrid MAC Protocols in VANET: A Survey

Ifa Fatihah Mohamed Zain, Azlan Awang and Anis Laouiti

Abstract Various ongoing research efforts in Vehicular Ad hoc Network (VANET) related to safety and non-safety applications have been published in academia and industry. One of the main areas in VANET that is still lacking of significant research contributions is toward designing reliable Medium Access Control (MAC) protocols. Existing surveys on MAC protocols in VANET mostly discuss general MAC methods, that include contention-based and contention-free MAC protocols. A hybrid MAC protocol that adopts both contention-based and contention-free MAC, proposed to enhance the network performance in VANET, is fruitful to be explored further. Hence, a survey of hybrid MAC protocols for VANET is presented in this paper. The benefits and limitations of the existing hybrid MAC protocols are discussed based on their classification to provide some insights into the recent advancement of high-performance MAC protocols for vehicular networks. Finally, some open research issues are highlighted as part of future research directions that need further investigations.

Keywords Hybrid MAC protocols · Multichannel · Single channel · VANET

I.F. Mohamed Zain · A. Awang (✉)
Department of Electrical and Electronic Engineering, Center for Intelligent Signal and Imaging Research (CISIR), Universiti Teknologi PETRONAS, 32610 Seri Iskandar, Perak, Malaysia
e-mail: azlanawang@utp.edu.my

I.F. Mohamed Zain
e-mail: ifafatihah@gmail.com

A. Laouiti
SAMOVAR, Télécom SudParis, CNRS, Université Paris-Saclay, 9 rue Charles Fourier, 91011 Evry, France
e-mail: anis.laouiti@telecom-sudparis.eu

A. Laouiti et al. (eds.), *Vehicular Ad-Hoc Networks for Smart Cities*,
Advances in Intelligent Systems and Computing 548,
DOI 10.1007/978-981-10-3503-6_1

1 Introduction

Vehicular Ad hoc Network (VANET) offers wireless communication between moving vehicles and has been used in Intelligent Transportation System (ITS) for driver safety enhancement [1]. Information exchange in VANET supports a wide range of safety and non-safety applications. Generally, VANET communications can be categorized into two types: vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications [2, 3]. Despite the types of communications used, medium access control (MAC) layer is a fundamental key to access the shared wireless medium for efficient sharing among multiple vehicles or nodes. The main concern at MAC layer is the probability of packet loss due to packet collisions [4]. Obstructed propagation or hidden terminal problem might contribute to the packet collisions. Nevertheless, a MAC protocol is expected to satisfy the requirements of VANET that have specific constraints such as high node movement, frequent link discontinuity, quick changing network topology, and stringent time-bounded requirements during the transportation of safety messages. Hence, the performance of MAC protocol contributes to the effectiveness of safety applications in VANET [5].

This paper presents an overview of hybrid MAC protocols in VANET. The rest of this paper is organized as follows: Sect. 2 provides VANET characteristics, Sect. 3 highlights MAC protocols in VANET and Sect. 4 explains existing hybrid MAC protocols in VANET. Then, Sect. 5 discusses future research directions, and finally, Sect. 6 concludes this paper.

2 VANET Characteristics

There are two main protocols in VANET architecture, namely IEEE 802.11p [3] and IEEE 1609.x, which are collectively called as Wireless Access in Vehicular Environments (WAVE) [6] as shown in Fig. 1. The IEEE 802.11p standard is part of an approved amendment to the IEEE 802.11 standard, which mainly focuses on the PHY layer and MAC sublayer of the stack. The IEEE 802.11p standard provides short-to-medium range connectivity to high-speed vehicles in a different environment (up to 1 km range) compared to the wireless transmission range at home or in the office [7, 8].

There are two types of communication in VANET, namely V2V and V2I. V2V focuses on communication between vehicles, and V2I deals with transmitting information between a vehicle and a fixed infrastructure such as Road Side Unit (RSU) [2, 4]. These two types of communication support non-safety applications (interactive user entertainment applications) and safety applications (emergency cases or high priority). In VANET, the network topology is frequently changing due to large speed of vehicles and it is often constrained by the road structure [9]. Hence, the unique characteristics of vehicular networks should be considered to implement an efficient MAC protocol for VANET. In the following, we highlight some unique char-

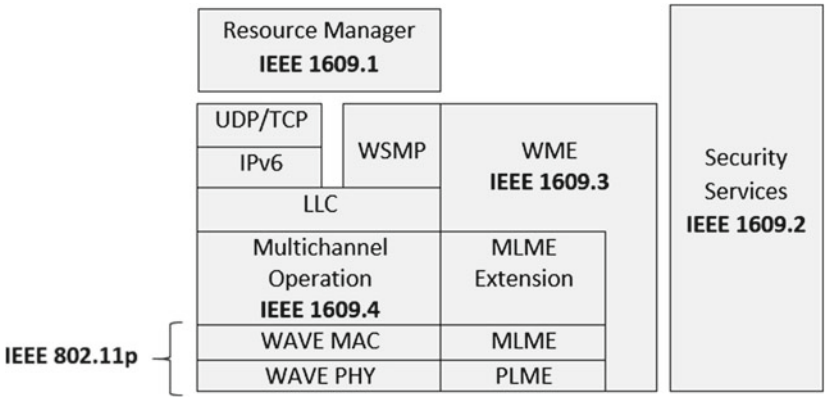


Fig. 1 Illustration of IEEE 1609.x and IEEE 802.11p in WAVE protocol stack (adopted from [6])

acteristics related to vehicular networks. For further detailed discussion on VANET characteristics, readers can refer to [2, 4, 5, 10, 11].

1. **Predictable mobility**
   In VANET, vehicles' movement is often constrained by road structure and layout; hence, their mobility is predictable. In addition, they need to obey the road signs and traffic lights, which also help in predicting their mobility.

2. **Variable network density**
   The network density can be very high during a traffic jam or in congested areas, and very low as in suburban areas. It depends on the areas and varies according to the traffic density.

3. **Large-scale network**
   The network scale in VANET is usually large, especially in dense urban areas such as on highways or in the city center.

4. **High computational ability**
   Vehicles can be equipped with a large amount of sensors, processors, Global Positioning System (GPS), large memory capacity, and advance antenna system. These resources can provide accurate information about the vehicles' current speed, direction, and position, which increase the computational ability of the vehicle.

5. **High power**
   The automotive rechargeable battery in vehicles can provide continuous power; hence, the power is not a critical issue in VANET.

3 Medium Access Control (MAC) in VANET

3.1 Overview of MAC Protocols in VANET

MAC layer protocol focuses on the mechanism to access the channel for efficient sharing between nodes to avoid packet collision. It provides the Quality of Service (QoS), for example, in terms of reliability and delay, and depends on the application layer request [4]. Basically, MAC protocols in VANET play a significant role in providing efficient message delivery, ensuring fair channel access and providing multichannel operation [12].

3.2 Classification of MAC Protocols in VANET

MAC protocols in VANET can be classified as contention-based, contention-free, and hybrid [13]. Figure 2 summarizes the broad categories of MAC protocols in VANET.

1. **Contention-based MAC Protocols**
   Contention-based MAC protocols rely on carrier sensing, backoff, and retry schemes. A node tries to access the channel with or without a little coordination. If a node wants to transmit, it must wait until the channel is idle; hence, the node needs to contend to access the channel. In summary, CSMA-based and random access protocols are categorized as the contention-based MAC protocols. However, the random access mechanism does not guarantee interference-free transmissions, especially when sender nodes are not within the transmission range of each other. Thorough analysis to investigate the impact of interfering links is needed. Hence, analysis of two-flow topologies is widely used in the literature to understand the complex interactions in multi-hop scenario for realistic wireless network deployments [14]. For example, in [15], different transmission and carrier sensing ranges are considered in two-flow topologies to mitigate the interference, thus improving the throughput.

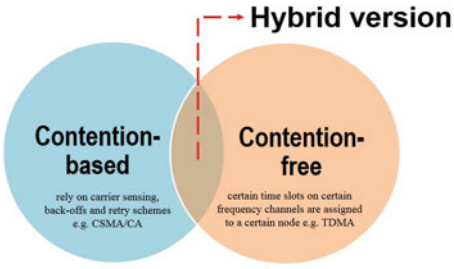


Fig. 2 Hybrid MAC protocol in VANET adopts both contention-based and contention-free approach

2. **Contention-free MAC Protocols**
   Contention-free MAC protocols basically rely on synchronization schemes. Certain time slots are assigned to a certain node on certain frequency channels. Hence, nodes do not need to contend to access the channel. The contention-free approaches might combine the fundamental multiplexing methods to ensure collision-free transmission, such as using frequency division multiple access (FDMA), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), and Space Division Multiple Access (SDMA) [10, 13]. Some examples of the TDMA-based, contention-free MAC protocols are ADHOC MAC [16], VeMAC [17], and VeSOMAC [18].

3. **Hybrid MAC Protocols**
   Hybrid protocol is usually formed by merging both contention-based and contention-free mechanisms. The combination is proposed to enhance the network performance in VANET. A hybrid MAC protocol can allocate part of its time for contention-based operation and the remainder is allocated for contention-free operation [10].

4 Hybrid MAC Protocols in VANET

4.1 Overview of Hybrid MAC Protocols in VANET

From our survey, the hybrid MAC protocols in VANET can be divided into multichannel-based [8] and single channel-based as shown in Fig. 3. Multichannel-based hybrid MAC protocols in VANET are further classified into with or without infrastructure, i.e., using RSU coordination. The term hybrid in multichannel-based is mostly referred to using one particular MAC protocol for one channel and another MAC protocol for different channel. In contrast, single channel-based hybrid MAC protocols are using both different MAC protocols in one channel, but usually divide to use them into different periods. This paper does not survey all types of hybrid MAC protocols in VANET. Our aim is to analyze current hybrid MAC protocols based on non-clustering type only.

4.2 Multichannel-Based Hybrid MAC Protocols in VANET

In [19], a hybrid MAC protocol named as Vehicle-to-vehicle and Road-to-vehicle Collaborative MAC Protocol (VRCP) has been proposed. The VRCP has two types of operation for the channel access control. The first one is Mode-A (ad hoc mode), whereas the second type is Mode-I (infrastructure mode). When the RSU is out of the communication range, Mode-A is activated and an ad hoc decentralized network is

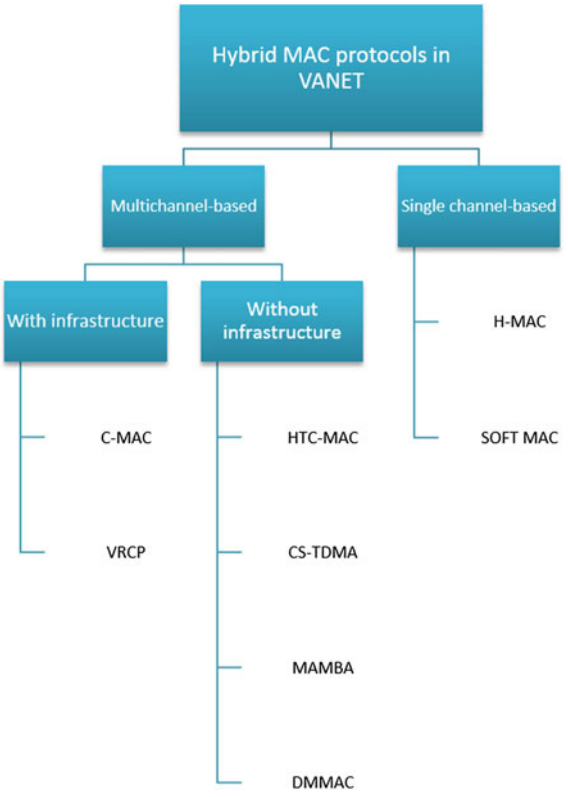


Fig. 3 Classification of hybrid MAC protocols in VANET based on multichannel and single channel

constructed using non-persistent CSMA scheme. Mode-I is activated when the RSU is within the communication range, whereby a centralized network is constructed using TDMA scheme. In VRCP protocol, each RSU holds the information map of the Message Data Slot (MDS) and shares this information map with surrounding RSUs. Hence, each access to the MDS is synchronized among RSUs. However, the collision might occur during the channel access in Mode-I if the MDS number is not equivalent to the vehicles' number. For the simulation results, the average packet loss rate is used as a performance metric in the VRCP protocol. The VRCP and non-persistent CSMA schemes are compared through simulation. However, the performance of VRCP decreases as communication traffic increases. Another comparison is made to evaluate the performance of VRCP protocol by increasing the number of RSU. The performance of VRCP improves when the number of RSU increases. Although the VRCP performance is remarkable when the number of RSU is more than two, such protocol can be implemented only within the range of RSU, which requires high cost of infrastructure. Other than the high cost of infrastructure, the RSU-dependent protocol is not an effective solution since the road topology is highly dynamic for RSU implementation which requires complex installation in certain areas such as tunnel, junctions, and bridge.

A Coordinated multichannel MAC (C-MAC) protocol is proposed in [20]. C-MAC protocol uses RSU coordination to provide safety message broadcasting through contention-free method. In C-MAC protocol, channel reservation requests will be sent by vehicles during channel reservation slots in Service Channel Interval (SCHI) through Dynamic Framed Slotted ALOHA (DFSA). After that, the RSU coordinates and schedules the transmission of the safety messages from the reservation information without the need to exchange additional information. All vehicles broadcast their information during Control Channel Interval (CCHI) using contention-free method; thus, probability to receive safety messages is increased. In addition, broadcasting time consumed is lower; thus, more time is allocated to transmit the data during SCHI duration. In the simulation analysis, delay and throughput performances of C-MAC protocol are evaluated. As the number of nodes increases, the number of collisions also increases, which contributes to higher delay and lower throughput. However, the C-MAC protocol exhibits lower delay and higher throughput as compared to WAVE and WAVE-based multichannel MAC protocols.

For a cost-effective solution, MAC protocols without RSU coordination are preferable. In [21], a Hybrid Efficient and Reliable MAC (HER-MAC) is proposed for VANET. HER-MAC protocol allows vehicles to send their safety messages without collision on the CCH within the reserved time slots. In addition, the SCH intervals are utilized during the CCHI for the non-safety message transmissions. This protocol exploits both TDMA and CSMA mechanisms for channel access. The CCH is categorized into reservation and contention periods. During contention period, various types of control packets are broadcast such as HELLO, SWITCH, and WSA/RES/ACK packets. This contributes to higher collision rate and control overhead, which decreases throughput on the CCH. To overcome this issue in HER-MAC, authors in [22] proposed a Hybrid TDMA and CSMA multichannel MAC (HTC-MAC) protocol. In HTC-MAC protocol, every node is required to reserve one time slot and transmit an announcement packet (ANC) during the reservation period through TDMA mechanism. After successfully reserving a time slot, the node constantly accesses the same slot to eliminate unnecessary control overhead and increases the throughput on the CCH. However, when node density is high, a larger ANC packet payload size is required in broadcasting neighbor's information. The comparison is made between HTC-MAC and HER-MAC using MATLAB based on the average number of nodes acquiring a time slot. Number of available time slots is fixed while number of contending nodes is varied. When the number of contending nodes is smaller, the success rate of time slot acquisition is equal for both HTC-MAC and HER-MAC protocols, while the HTC-MAC protocol exhibits better performance than HER-MAC when the number of contending nodes is higher.

A Scalable CSMA and TDMA (CS-TDMA) MAC protocol for VANET is proposed in [23]. The CS-TDMA protocol considers channel access and channel switching at the same time to provide reliable one-hop broadcast service. It combines SDMA, TDMA, and CSMA mechanism for channel access. The CS-TDMA protocol is more reliable and adaptive to reduce packet loss rate and transmission delay, while increasing network throughput. Moreover, it differs from other existing multichannel protocols because the ratio of CCH to SCH intervals is adjusted dynamically

according to vehicle density. In detail, the CCH interval is reduced in low-density scenario to guarantee a high throughput for non-safety applications. For high-density scenario, the CCH interval is fully utilized to ensure a bounded transmission delay for real-time safety applications. By using MATLAB, the CS-TDMA protocol provides an improvement in channel utilization, but the performance evaluation of this protocol has been limited only to a medium density of vehicles, i.e., 80 vehicles/km.

In [24], a Dedicated Multichannel MAC (DMMAC) protocol is proposed. The DMMAC protocol uses both TDMA and CSMA/CA for a hybrid channel access mechanism. The important mechanism of this protocol is known as Adaptive Broadcasting (AB), which allows every vehicle to construct delay-bounded and collision-free transmission for the safety applications. It also uses the Adaptive Broadcast Frame (ABF) to regulate vehicles' access behaviors, which include how to reserve a slot, how to adjust the frame length, and how to add virtual slots after the end of each frame. The DMMAC protocol has a dynamic TDMA length in CCHI and thus is adaptable to different traffic conditions. The AB mechanism gives good performance in delivery ratio of safety packets. However, its random slot assignment technique does not perform a contiguous slot allocation.

As part of the extension of the DMMAC protocol, Medium Access with Memory Bifurcation and Administration (MAMBA) protocol has been proposed in [25]. Every node needs to listen to its one-hop neighbors to determine a slot allocation during the ABF procedure in DMMAC protocol. The MAMBA protocol addresses the issue of the slot information propagating further than the one-hop neighbors in DMMAC protocol, where an extra bit is added to the Slot Allocation Table (SAT). The proposed idea in MAMBA protocol to use an extra bit is to determine whether the node number is in the correct slot as informed by the occupying node itself, or whether it was received from a different node. Transmitting node needs to inform that the allocated slot has the same ID as receiving node, so both transmitting and receiving nodes can determine their one-hop neighbors. However, due to hidden terminal issue, the information received from a single node only might not be sufficient for the receiving node to remove the allocated slot. The OMNeT++ network simulator is used to evaluate the MAMBA protocol. The DMMAC and MAMBA protocols are compared through simulation. The performance of these two protocols is comparable in terms of throughput and message delivery ratio. This is due to the fact that the number of packets generated and the vehicular parameters assigned to these protocols are equivalent for the simulated scenario. Nevertheless, DMMAC protocol exhibits high latency compared to the MAMBA during saturated SATs under high-density scenarios.

4.3 Single Channel-Based Hybrid MAC Protocols in VANET

For single channel-based, a Hybrid MAC protocol (H-MAC) is proposed in [26]. H-MAC protocol is proposed to overcome the issue of sudden burst data flow in VANET, where a frame cycle is further divided into reservation and competition

periods. Each node has its own slot in the reservation period and in this slot, the node is able to send a stable or periodic data such as beacon packets. While in the competition period, all nodes need to compete for the channel using CSMA/CA mechanism to send the burst data flow. Hence, beacon and burst data are separated, and this reduces the collision between data frames, which also decreases the delay due to collision of the burst data. However, the loss rate of beacon packets increases as the node density increases. If the number of nodes is higher than the slot number in dense scenario, the rate of packet loss will be increased. In addition, topology changes quickly as node density increases and the slot is adjusted; hence, the packet loss incremental is higher. Nevertheless, the packet loss rate of H-MAC protocol is considerably lower as compared to IEEE 802.11p.

In [27], a Space-Orthogonal Frequency Time MAC (SOFT MAC) protocol is proposed. The road is divided into cells and every cell is assigned to each of the available subcarriers. Then, vehicles within the cell share these subcarriers using TDMA mechanism. Each vehicle uses its current position to know the set of subcarriers by using the GPS system. The SOFT MAC protocol has two periods: the reservation slot (RS) and the transmission slot (TS). The RS period is accessed via a contention-based CSMA, while the TS period is accessed via a prior reservation. The RS period is used to transmit short messages and to reserve the channel resource for the coming TS period, which is used to transmit a large amount of data. The simulation analysis of SOFT MAC protocol is obtained from the mathematical model only and no mobility is considered in the performance evaluation. The SOFT MAC protocol is evaluated and compared to the basic access method of the Distributed Coordination Function (DCF). The performance of the SOFT MAC protocol in terms of throughput increases if the payload size is bigger than 500 bytes. Even the throughput increases, the possible number of TS decreases, resulting in low overhead. Although this protocol shows improvements in throughput and can support QoS requirements, the fixed interval used for the RS period is not adaptable to the varying traffic load. In addition, this protocol assumes that digital road maps are mounted on all vehicles and to guarantee its operation in situations where vehicles without digital maps are present is a challenging task.

5 Future Research Directions

1. **Dynamic interval allocation**
   Due to high node mobility in VANET, varying node densities have an important effect on the performance of the hybrid MAC protocols. Particularly in single channel-based, the fixed interval or length used in the first period (random access period) to reserve the time slot in the second period (TDMA period) needs further investigation. In a high-density network, nodes may not be able to send reservation request or only a few reservations will be made if the length of this period is too short. In contrast, if the length is too long, it might not be able to accommodate all reservations in the second period. The length of this period needs to be tuned

dynamically according to node density and also to number of the available time slots in the reservation period.

2. **Inter-RSU interference**
   Some of the hybrid protocols use RSU as a central point to coordinate channel access for the vehicles. However, the interference in vehicles might exist in the overlapping area between two neighboring RSUs if the RSUs are using the same frequency band. Future research should include the mechanism on how to reduce the inter-RSU interference effect, especially when the vehicles are entering or leaving the RSU coverage area.

3. **Mobility scenario**
   Most of the protocols have been designed to work on the highway scenario only. Urban areas, where there are obstacles such as buildings and junctions, need to be taken into account also. Hybrid MAC protocols that can operate in both highway and urban areas are still an open research issue.

4. **Alternative to GPS**
   Generally, vehicles are equipped with GPS system to determine their position, direction, and heading. Future research should consider the issue related to GPS technology, especially when vehicles encounter signal lost inside a tunnel or bridge.

6 Conclusion

In this paper, an overview and some basic description of the existing hybrid MAC protocols in VANET are discussed. Those hybrid protocols are explained based on their classification to provide some insights to the researchers in academia and industry on the recent advancement of high-performance MAC protocols for vehicular networks. Basically, the hybrid MAC protocols in VANET have been proposed to obtain superior network performance in terms of throughput, delay, packet delivery ratio, etc. The ongoing research efforts need to consider the current channel status and traffic conditions to guarantee a reliable MAC protocol in VANET environment.

Acknowledgements This research is supported by the Ministry of Education Malaysia under the Higher Institution Center of Excellence (HICoE) scheme (Cost Center: 0153CA-004).

References

1. Zeadally, S., Hunt, R., Chen, Y.S., Irwin, A., Hassan, A.: Vehicular ad hoc networks (VANETS): status, results, and challenges. Telecommun. Syst. **50**(4), 217–241 (2012)
2. Al-Sultan, S., Al-Doori, M.M., Al-Bayatti, A.H., Zedan, H.: A comprehensive survey on vehicular ad hoc network. J. Network Comput. Appl. **37**, 380–392 (2014)
3. IEEE Standard for Information technology - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments: IEEE Std 802.11p-2010 (Amendment to IEEE Std 802.11-2007 as amended by IEEE Std 802.11k-2008, IEEE Std 802.11r-2008, IEEE Std 802.11y-2008, IEEE Std 802.11n-2009, and IEEE Std 802.11w-2009), pp. 1–51 (2010)
4. Campolo, C., Molinaro, A., Scopigno, R. (eds.): Vehicular Ad Hoc Networks: Standards, Solutions, and Research. Springer, Heidelberg (2015)
5. Gupta, N., Prakash, A., Tripathi, R.: Medium access control protocols for safety applications in vehicular ad-hoc network: a classification and comprehensive survey. Veh. Commun. **2**(4), 223–237 (2015)
6. Uzcátegui, R.A., Acosta-Marum, G.: WAVE: A Tutorial. IEEE Commun. Mag. **47**(5), 126–133 (2009)
7. Gillani, S., Khan, I., Qureshi, S., Qayyum, A.: Vehicular ad hoc network (VANET): enabling secure and efficient transportation system. Technical Journal, University of Engineering and Technology, Taxila, vol. 13 (2008)
8. IEEE Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation: IEEE Std 1609.4-2016 (Revision of IEEE Std 1609.4-2010), pp. 1–94 (2016)
9. Menouar, H., Filali, F., Lenardi, M.: A survey and qualitative analysis of MAC protocols for vehicular ad hoc networks. IEEE Wirel. Commun. **13**(5), 30–35 (2006)
10. Booysen, M.J., Zeadally, S., van Rooyen, G.J.: Survey of media access control protocols for vehicular ad hoc networks. IET Commun. **5**(11), 1619–1631 (2011)
11. Stanica, R., Chaput, E., Beylot, A.L.: Properties of the MAC layer in safety vehicular ad hoc networks. IEEE Commun. Mag. **50**(5), 192–200 (2012)
12. Hadded, M., Muhlethaler, P., Laouiti, A., Zagrouba, R., Saidane, L.A.: TDMA-based MAC protocols for vehicular ad hoc networks: a survey, qualitative analysis, and open research issues. IEEE Commun. Surv. Tutorials **17**(4), 2461–2492 (2015)
13. Gillani, S.A., Shah, P.A., Qayyum, A., Hasbullah, H.B.: MAC layer challenges and proposed protocols for vehicular ad-hoc networks. In: Vehicular Ad-hoc Networks for Smart Cities, pp. 3–13. Springer, Singapore (2015)
14. Garetto, M., Shi, J., Knightly, E.W.: Modeling media access in embedded two-flow topologies of multi-hop wireless networks. In: Proceedings of the 11th Annual International Conference on Mobile Computing and Networking (ACM), pp. 200–214 (2005)
15. Zeeshan, M., Naveed, A.: Medium access behavior analysis of two-flow topologies in IEEE 802.11 wireless networks. EURASIP J. Wirel. Commun. Netw. **2016**(1), 1–18 (2016)
16. Borgonovo, F., Capone, A., Cesana, M., Fratta, L.: ADHOC MAC: new MAC architecture for ad hoc networks providing efficient and reliable point-to-point and broadcast services. Wirel. Network. **10**(4), 359–366 (2004)
17. Omar, H.A., Zhuang, W., Li, L.: VeMAC: a TDMA-based MAC protocol for reliable broadcast in VANETs. IEEE Trans. Mob. Comput. **12**(9), 1724–1736 (2013)
18. Yu, F., Biswas, S.: Self-configuring TDMA protocols for enhancing vehicle safety with DSRC based vehicle-to-vehicle communications. IEEE J. Sel. Areas Commun. **25**(8), 1526–1537 (2007)
19. Fujimura, K., Hasegawa, T.: A collaborative MAC protocol for inter-vehicle and road to vehicle communications. In: IEEE 7th International Conference on Intelligent Transportation Systems, pp. 816–821 (2004)
20. Kim, Y., Lee, M., Lee, T.J.: Coordinated multichannel MAC protocol for vehicular ad hoc networks. IEEE Trans. Veh. Technol. **65**(8), 6508–6517 (2016)

21. Dang, D.N.M., Dang, H.N., Nguyen, V., Htike, Z., Hong, C.S.: HER-MAC: a hybrid efficient and reliable MAC for vehicular ad hoc networks. In: IEEE 28th International Conference on Advanced Information Networking and Applications (AINA), pp. 186–193 (2014)
22. Nguyen, V., Oo, T.Z., Chuan, P., Hong, C.S.: An efficient time slot acquisition on the hybrid TDMA/CSMA multichannel MAC in VANETs. IEEE Commun. Lett. **20**(5), 970–973 (2016)
23. Zhang, L., Liu, Z., Zou, R., Guo, J., Liu, Y.: A scalable CSMA and self-organizing TDMA MAC for IEEE 802.11 p/1609. x in VANETs. Wirel. Pers. Commun. **74**(4), 1197–1212 (2014)
24. Lu, N., Ji, Y., Liu, F., Wang, X.: A dedicated multi-channel MAC protocol design for VANET with adaptive broadcasting. In: IEEE Wireless Communications and Networking Conference (WCNC), pp. 1–6 (2010)
25. Booysen, M.J., Zeadally, S., van Rooyen, G.J.: Performance comparison of media access control protocols for vehicular ad hoc networks. IET Network. **1**(1), 10–19 (2012)
26. Luo, J., Zha, J., Xiao, Y., Li, R.: H-Mac: a Hybrid MAC protocol for VANET. In: Wang, R., Xiao, F. (eds.) Advances in Wireless Sensor Networks, pp. 346–356. Springer, Heidelberg (2012)
27. Abdalla, G.M., Abu-Rgheff, M.A., Senouci, S.M.: Space-orthogonal frequency-time medium access control (SOFT MAC) for VANET. In: Information Infrastructure Symposium (GIIS 2009), pp. 1–8 (2009)

A Receiver-Based Forwarding Scheme to Minimize Multipath Formation in VANET

Khaleel Husain and Azlan Awang

Abstract Receiver-based data forwarding schemes are well suited for vehicular environment due to their ability of making routing decision on the fly. However, existing receiver-based schemes still face the challenges of unwanted multiple paths formation especially when contending nodes are out of transmission range of each other. In this paper, we propose an approach of the receiver-based forwarding scheme where receiving nodes decide whether to participate in contention for forwarding right based on signal-to-interference-plus-noise ratio (SINR) and forwarding zone. Upon qualifying to contend for forwarding right, the contending nodes set their waiting time based on geographical progress toward destination. We present the proposed scheme and then highlight some possible issues that require further investigation. The proposed scheme tends to minimize unnecessary formation of multiple paths toward the destination while also favors the selection of a forwarding node closer to destination.

Keywords VANET · Receiver-based forwarding · Forwarding zone · Waiting time

1 Introduction

Vehicular Ad hoc Network (VANET) is one of the emerging networking technologies aims to provide reliable communication in the road traffic environment. VANET enables Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication to allow road traffic applications relating to safety, commercial use and public services. Conventional networking technology like Mobile Ad hoc Network (MANET)

K. Husain · A. Awang (✉)
Department of Electrical and Electronic Engineering, Center for Intelligent Signal and Imaging Research (CISIR), Universiti Teknologi PETRONAS, 32610 Bandar Seri Iskandar, Perak, Malaysia
e-mail: azlanawang@utp.edu.my

K. Husain
e-mail: khsan075@gmail.com

A. Laouiti et al. (eds.), *Vehicular Ad-Hoc Networks for Smart Cities*,
Advances in Intelligent Systems and Computing 548,
DOI 10.1007/978-981-10-3503-6_2

does not perform well due to the challenges of road traffic environment such as high mobility, constrained movement pattern and frequently changing traffic density [1, 2]. In order to meet stringent Quality of Service (QoS) requirements of VANET applications, the routing must be able to deal with mobility and scalability issues while also providing satisfactory network performance in terms of end-to-end delay, packet delivery ratio and overhead. According to [3], data forwarding schemes can be classified into three categories: route-based forwarding, sender-based forwarding and receiver-based forwarding. Conventional route-based forwarding involves route establishment prior to data transmission. However, it does not work well due to high mobility and this leads to frequent changes of network topology. Routing approaches that decide the next best forwarding node toward the destination during data transmission are more suitable in vehicular environment. In sender-based forwarding approach, a sender selects the next forwarder based on the information present in a routing table. However, this approach requires periodic sharing of information among vehicles through beacon messages at the expense of high overhead. Another routing approach is the receiver-based forwarding scheme where receiving nodes are responsible for deciding whether to participate or not in the receiver-based contention. This approach offers low overhead as it does not require any periodic exchange of information for data forwarding [3, 4]. A general receiver-based data forwarding scheme has two aspects: forwarding zone and waiting time. The forwarding zone is a deciding criteria for receiving nodes to contend for a forwarding right. Once the receiving nodes satisfy the forwarding zone criteria, they contend for forwarding right by setting a waiting time determined by a certain criteria. The contending node with timer expires first become the next-hop forwarder and then broadcasts the data packet accordingly. Other contenders when overhearing the transmission cancel their timers and discard the packet.

One of the issues in the current receiver-based schemes is the unwanted multiple paths formation when two receiving nodes are out of communication range of each other. Multiple paths toward destination result in redundant packets flowing through the network which in turn lead to congestion and increasing the chances of packet collision. Hence, there is a need to define a forwarding zone to ensure the formation of only a single path toward destination. In this paper, we propose an approach of the receiver-based forwarding scheme where the eligibility criteria is based on signal-to-interference-plus-noise ratio (SINR) and forwarding zone. The forwarding zone is calculated based on forwarding angle that is set to a constant value of 60° to ensure the prevention of multipath formation. Receiving nodes that satisfy the eligibility criteria contend for forwarding right by setting a waiting time based on geographic progress toward destination. The proposed scheme tends to minimize unwanted multiple paths formation, while also reducing the number of hops by selecting the nearest forwarding node toward destination.

The rest of this paper is organized as follows. In Sect. 2, the existing receiver-based forwarding schemes in VANET are explained. Section 3 discusses the issue of unwanted multiple paths formation in the current receiver-based forwarding schemes. Section 4 briefly explains the existing solution to the problem mentioned in Sect. 3. Section 5 presents a detailed explanation of the proposed scheme involving the

proposed model, important technical terms and its work flow. Section 6 offers a brief discussion involving the theoretical comparison of the existing and proposed scheme, while also highlighting some issues that need further investigation. Finally Sect. 7 concludes the paper with a summary of key points discussed and future perspective.

2 Related Work

There exist a few receiver-based data forwarding schemes in VANET. A reactive receiver-based solution named VIRTUS [5] was proposed to allow video streaming over VANET environment. VIRTUS enables high data rate communication among vehicles without the need for any roadside infrastructure. Here, receiving nodes participate in communication based on their current location and future location estimation. The forwarding zone of VIRTUS is in the direction of the destination as shown in Fig. 1.

The forwarding zone is set based on forwarding angle θ where maximum value is 90°. The receiving nodes compute their waiting time based on geographic progress and link stability. VIRTUS provides a satisfactory video streaming performance in vehicular networks while also reducing the number of transmission. RPBL [6] is another beaconless receiver-based routing protocol where receiving nodes set their waiting time based on their closeness toward the road intersections that lie along the path to destination. However, RPBL does not make use of forwarding zone which leads to the possibility of unwanted multiple paths formation toward the destination. LIATHON proposed in [4] is a multipath receiver-based data forwarding technique developed to enable video streaming over VANET where two paths having minimum route coupling effect are discovered by making use of location information. The receiving nodes set their waiting time based on the degree of closeness, geographic progress and link stability. LIATHON fulfills the performance requirements

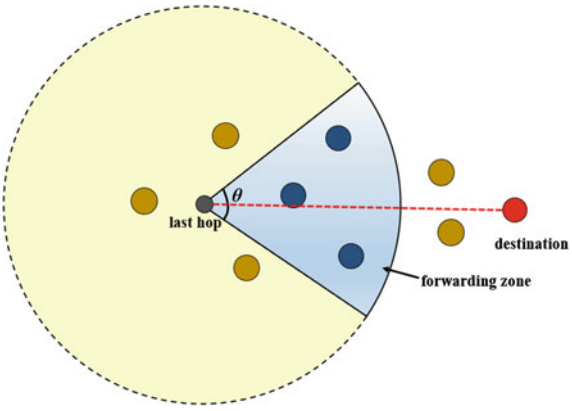


Fig. 1 Definition of the forwarding zone based on forwarding angle

of video streaming by distributing the load over the two paths. LIAITHON was further upgraded to LIAITHON+ [7] where the number of multiple paths were increased to three. Also, the impact of added redundancy was analyzed in order to further enhance the routing protocol. Finally, SLBF proposed in [3] aims to improve reliability during data transmission. Here, the forwarding zone is set based on the direction and angle size of the forwarder. The forwarding angle is determined based on the time interval from previous forwarder to current forwarder and average time for single hop. Furthermore, the receiving nodes within the forwarding zone compute their waiting time based on link quality, traffic load and greedy strategy.

3 Problem Analysis

One of the major issues in receiver-based forwarding schemes as mentioned in [6] is the unwanted multipath formation when receiving nodes are out of transmission range of each other. Figure 2, adopted from our previous work [8] depicts an instance highlighting the unwanted multipath formation issue in the current receiver-based schemes.

In Fig. 2a, the source and destination are represented by the nodes S and D, respectively whereas nodes A, X, B, Y and Z represent the intermediate nodes along the path from source to destination. As shown in Fig. 2a, S broadcasts the packets in its communication range. Since nodes A and X are within the communication range of S, they receive the packet. Let us assume both nodes A and X are within the forwarding zone and hence they contend for forwarding right by setting their waiting time. Let us assume the waiting time of node A expires first resulting in broadcasting of packet. However, as shown in Fig. 2b, nodes A and X are not in the communication range of each other and hence node X will not hear node A's transmission and will broadcast the packet once its timer expires. This will result in the formation of two paths S-A-B-D and S-X-Y-Z-D as shown in Fig. 2c. Unwanted formation of multiple paths leads to redundant packets flowing throughout the network causing network congestion. Hence, there is a need to set a forwarding zone that can prevent unwanted multipath formation in receiver-based schemes. This can be achieved if

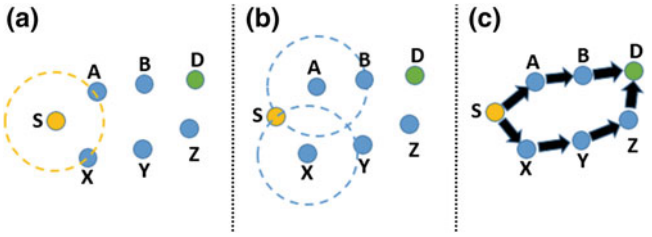


Fig. 2 Illustration of unwanted multipath formation issue in the current receiver-based schemes

the forwarding zone is set in such away that the maximum distance between any two nodes located in the forwarding zone is less than the communication range.

4 Existing Solution

Authors in [9] proposed a receiver-based scheme based on Ad hoc On-Demand Distance Vector (AODV) routing protocol [10]. Here, prior to route establishment, receiving nodes decide whether to forward or not the route request packets based on their presence in the forwarding zone. The nodes then set their waiting time according to a competing parameter which in turn depends on the hop length and link remaining lifetime. The forwarding zone of the existing solution is shown in Fig. 3.

The yellow color area represents the forwarding zone of the source S or intermediate forwarding node N_i. r is the communication range of the node. The forwarding zone is defined as the circular field with radius $r/2$ where the line connecting node S or N_i and destination D as centerline. The zone effectively eliminates multiple paths formation since the maximum distance between any two nodes in the forwarding zone is less than the communication range of the node. As shown in Fig. 3, nodes A and B are located within the forwarding zone and hence are entitled to forward the route request packets toward D. Nodes C and E since are not located within the zone discard the route request packets. However, it can be seen from this figure that node C is closer to D when compared to A and B. Hence, it can be concluded that even though the forwarding zone of the existing solution is able to solve the unwanted multiple paths formation issue to some extent, but it is inefficient in terms of selecting the closest forwarding node toward destination.

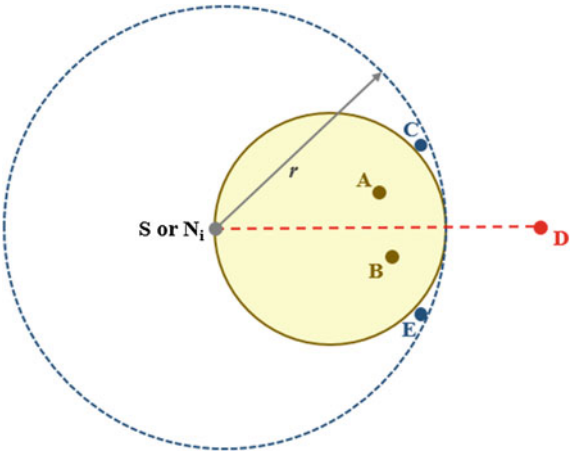


Fig. 3 Forwarding zone of the existing solution (adopted from [9])

5 Proposed Mechanism

We propose a mechanism where receiving nodes determine whether to participate in contention to be a forwarder based on its SINR and its presence in the forwarding zone. If SINR of a receiving node is greater than a threshold and the forwarding angle is less than the angle mentioned in the packet, only then it contends for its forwarding right by setting a timer based on the geographical progress toward destination. In any other case, receiving nodes discard the packet.

5.1 VANET Model

The vehicles are assumed to be moving in a single direction with different speed. Communication model used here is the WAVE architecture [11] comprising of IEEE 802.11p standard to support both physical and MAC layer while IEEE 1609 standard is used at the higher layers. V2V communication is used from source until the last hop node while V2I communication is used between the last hop node and destination. We assume that a single source vehicle transmits data to a static destination, a Road Side Unit (RSU). The data traffic type considered here is Constant Bit Rate (CBR). Each vehicle is assumed to be equipped with a Global Positioning System (GPS) and is aware of the position of itself, the last hop node and destination. The position of the last hop node is known from the received packet. For the angle computation of the vehicles, the line connecting the vehicle and destination is considered as x-axis.

5.2 Forwarding Zone

The forwarding zone of the proposed scheme is shown in Fig. 4. The forwarding zone is a fan-shaped area in the direction of destination with a constant forwarding angle θ of 60°. Here, for the angle computation, the current forwarder A is considered as the origin of a rectangular coordinate system and the line connecting the current forwarder A and destination D is considered as x-axis. As before, r is the communication range of the node. The reason for assigning θ value as 60° is to make sure that all nodes in the forwarding zone are within communication range of each other that holds true due to the nature of equilateral triangle. As shown in Fig. 4, nodes X and Y are the farthest from each other and are separated by a distance r.

The forwarding angle θ is computed in [3] as follows

$$\theta = 2 \times \left| arccos \frac{x_r - x_{lh}}{\sqrt{(x_r - x_{lh})^2 + (y_r - y_{lh})^2}} \right| \tag{1}$$

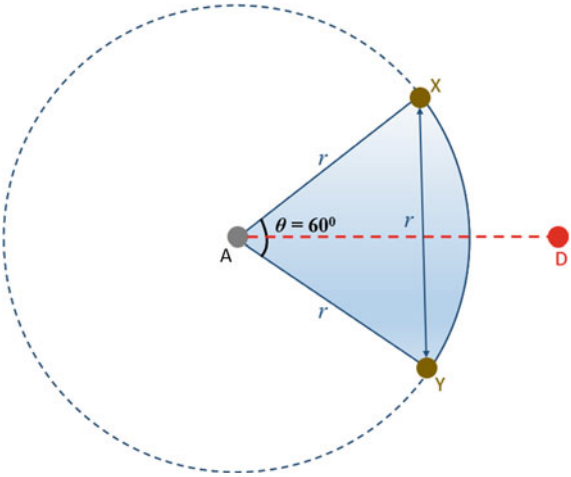


Fig. 4 Forwarding zone of the proposed scheme where θ is set to a fixed value of 60°

where (x_r, y_r) and (x_{lh}, y_{lh}) are the position coordinates of the receiving node and previous forwarding node, respectively.

5.3 Geographical Progress

The geographical progress γ_{geo} of the receiving node toward the destination is computed in [5] as follows

$$\gamma_{geo} = 1 - \frac{d(n_{lh}, n_d) - d(n_r, n_d)}{r} \tag{2}$$

where $d(n_{lh}, n_d)$ is the distance from previous forwarding node to destination, and $d(n_r, n_d)$ is the distance from receiving node to destination.

5.4 Waiting Time

Once the receiving nodes are eligible to participate in contention to be a forwarder, they contend for forwarding right by setting the waiting time which is derived from [5] as follows

$$\lambda = \gamma_{geo} \times \Gamma \tag{3}$$

where Γ is the maximum waiting time scale is the maximum waiting time scale to set the upper limit for a contending node can wait before broadcasting a packet.

5.5 Algorithm

The work flow of the proposed receiver-based scheme will be explained in two parts. Firstly, we explain the steps involved during data transmission as a source node before moving on to explain the steps involved during data transmission as an intermediate or destination node.

Source perspective Figure 5 highlights the steps involved for the source node during data transmission. Initially, source inserts its position coordinates and address in the packet. Source then sets the forwarding angle as 60° in the packet. The packet is then broadcasted and the timer is set. If the source receives the same packet or an Acknowledgment (ACK) before timeout then it discards the packet and cancels the timer. Otherwise, the source increases the forwarding angle to 180° and rebroadcasts the packet before setting the timer. In case of more than one transmission timeout, the forwarding angle is unchanged (180°) and the packet is again rebroadcasted and

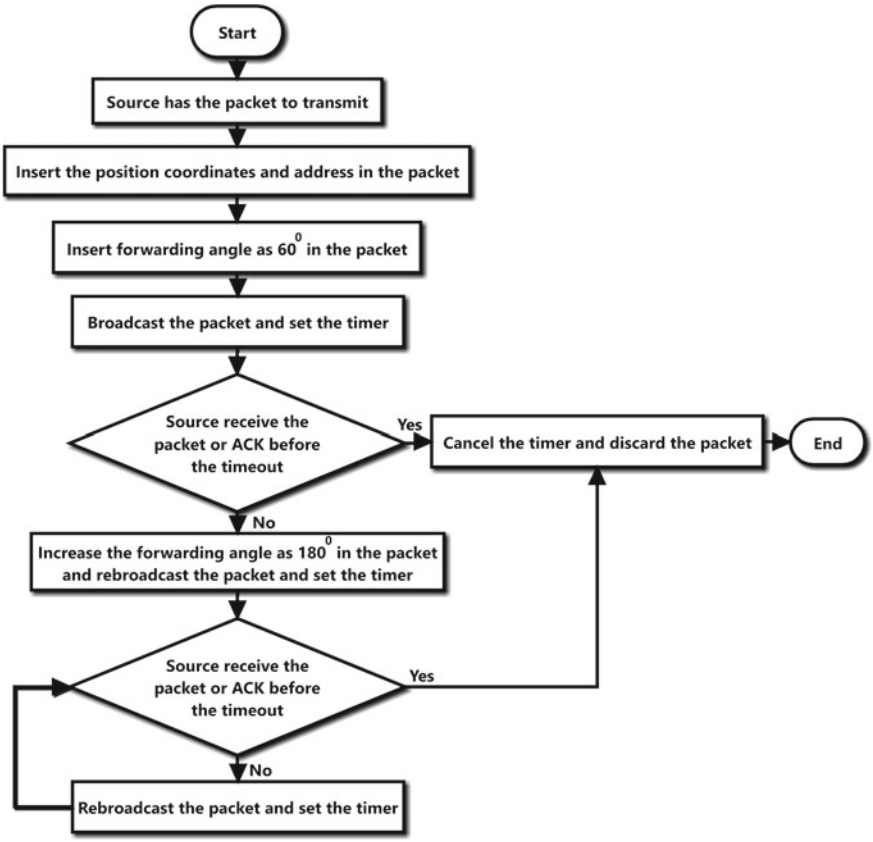


Fig. 5 Flowchart showing the steps involved for a source node during data transmission

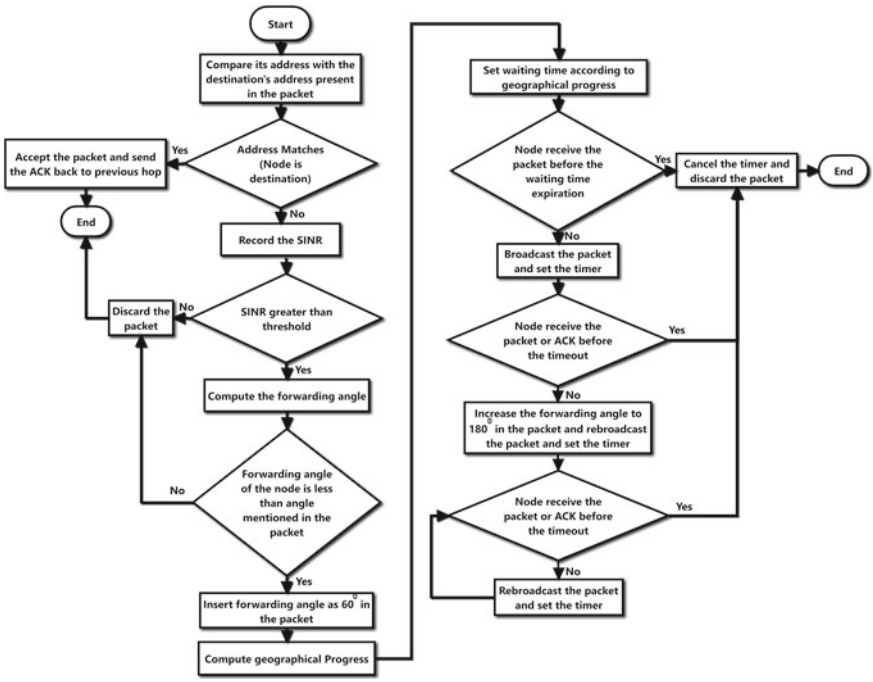


Fig. 6 Flowchart showing the steps involved for an intermediate node or destination during data transmission

the timer is set. The first transmission timeout indicate the unavailability of nodes within the forwarding zone. The intention for setting the next forwarding angle to 180° is to only select the nodes which are ahead and nearer to the destination.

Intermediate node, Destination perspective Figure 6 highlights the steps involved for an intermediate node or destination during data transmission. Once the node receives the packet it checks whether it is the destination by comparing its address with destination address present in the packet. If the receiving node is the destination then it accepts the packet and sends an ACK to previous forwarding node. If it is not the destination, it records the SINR and checks whether the recorded SINR is greater than a threshold. This threshold is the minimum signal strength required for a successful packet transmission. If the SINR is less than the threshold, that means the link does not meet the minimum signal strength requirements and the node is not eligible to participate in contention and the packet will be discarded. If it is not the case, the receiving node computes the forwarding angle and checks whether the computed forwarding angle is less than the angle retrieved from the packet. A forwarding angle less than the angle obtained from the packet implies that the receiving node is not located within the forwarding zone and similarly packet will be discarded. Otherwise, the receiving node inserts the forwarding angle as 60° in the packet, computes the geographic progress and then sets the waiting time

accordingly before broadcasting the packet. In the case when the same packet or ACK is received before the timer expires, this implies that another forwarder has already been selected. The receiving node then cancels the timer and discards the packet accordingly. Otherwise, it increases the forwarding angle to 180° in the packet before broadcasting the packet and then sets the timer. In cases when more than one transmission timeout, the receiving node keeps forwarding angle unchanged before rebroadcasting the packet and sets the timer accordingly.

6 Discussion and Future Work

In addition to forwarding zone, the use of SINR parameter in the eligibility criteria for forwarding right assists in eliminating nodes that do not meet the minimum signal strength requirement and hence makes the zone more effective. Moreover, the waiting time criteria based on geographic progress favors the proposed mechanism to select a forwarding node closer to destination. Table 1 highlights the forwarding zones of the existing protocols and our proposed receiver-based forwarding scheme.

RPBL [6] does not make use of forwarding zone concept and thus have the highest chances of multiple paths formation. LIATHON [4] and LIATHON+ [7] are multi-path receiver-based schemes aim at controlling the number of multiple paths toward the destination to two and three, respectively. The forwarding zone of VIRTUS [5] is defined by the forwarding angle which is set to 90° that allows for the possibility of multiple paths formation. The forwarding angle of SLBF [3] varies between 60° to 180° based on the time interval from previous forwarder to current forwarder and average time for single hop. Receiver-based scheme in [9] although defines a forwarding zone and free from multiple paths formation but the zone is inefficient

Table 1 A summary of forwarding zones of the existing protocols and proposed scheme

Protocol	Forwarding Zone
VIRTUS [5]	Forwarding angle of 90° in the direction of destination
RPBL [6]	–
LIAITHON [4] and LIAITHON+ [7]	Forwarding angle of 90°
SLBF [3]	Varying forwarding angle (from 60° to 180°) in the direction of destination along the road
Existing solution [9]	Circular field with the radium of R/2 with the line connecting source node/intermediate node and destination as centerline
Proposed scheme	Fixed forwarding angle of 60° in the direction of destination and in case of retransmission, forwarding angle of 180° in the direction of destination

in terms of routing as it neglects more suitable forwarders nearer to destination. The receiver-based scheme proposed in our current work, in case of no transmission timeouts, ensures single path to destination. It may also improve the routing performance by favoring more forwarders nearer to destination to be selected. However, in case of transmission timeouts, there is still chance of multiple paths formation as the forwarding angle is increased to 180°. Also, excessive retransmissions may result in an increased end-to end delay. Hence, in the future work, we would like to analyze the performance of the proposed receiver-based scheme under different conditions through simulations in a realistic VANET environment. We will also include more detailed analysis that incorporate important parameters such as communication and traffic models. In addition, performance comparison with existing receiver-based schemes will be carried out to show the improvements offered by the proposed scheme. Finally, other metrics that could further improve the waiting time criteria will be investigated.

7 Conclusion

In this paper, we propose an approach of the receiver-based forwarding scheme aims to avoid unwanted multiple paths formation. In the proposed scheme, the eligibility criteria for the receiver-based contention is based on SINR and forwarding zone. Only those receiving nodes with SINR greater than a threshold and with forwarding angle less than the angle mentioned in the packet are entitled to contend for forwarding rights by setting their waiting time based on geographic progress. All other receiving nodes discard the packet. In case of a transmission timeout, the forwarding angle is increased to 180°. In case of no transmission timeouts, the proposed scheme ensures single path to the destination thereby reducing network congestion. Also, the scheme selects a forwarding node closest to destination resulting in less number of hops and thus making routing more efficient. However, chances of multiple paths formation increase in case of transmission timeouts. In addition, excessive retransmission may significantly increase the end-to-end delay. Hence, the performance of the proposed scheme will be analyzed under different conditions through simulations which have been in progress and planned as part of the future work.

Acknowledgements This research is supported by the Ministry of Education Malaysia under the Higher Institution Center of Excellence (HICoE) Scheme (Cost Center: 0153CA-004).

References

1. Kumar, S., Verma, Ak: Position based routing protocols in VANET: a survey. Wirel. Pers. Commun. **83**(4), 2747–2772 (2015)
2. Karagiannis, G., Altintas, O., Ekici, E., Heijenk, G., Jarupan, B., Lin, K., Weil, T.: Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions. IEEE Commun. Surv. Tutor. **13**(4), 584–616 (2011)

3. Li, C., Chen, Y., Han, X., Zhu, L.: A self-adaptive and link-aware beaconless forwarding protocol for VANETs. Int. J. Distrib. Sens. Netw. Article ID 757269, 1–10 (2015)
4. Wang, R., Rezende, C., Ramos, HS., Pazzi, RW., Boukerche, A., Loureiro, AAF.: LIAITHON: a location-aware multipath video streaming scheme for urban vehicular networks. IEEE Symp. Comput. Commun. pp. 436–441 (2012)
5. Rezende, C., Ramos, HS., Pazzi, RW., Boukerche, A., Frery, AC., Loureiro, AAF.: VIRTUS: a resilient location-aware video unicast scheme for vehicular networks. IEEE Int. Conf. Commun. pp. 698–702 (2012)
6. Sasaki, Y., Lee, WC., Hara, T., Nishio, S.: On alleviating beacon overhead in routing protocols for urban VANETs. IEEE 14th Int. Conf. Mobile Data Manag. pp. 66–76 (2013)
7. Wang, R., Almulla, M., Rezende, C., Boukerche, A.: Video streaming over vehicular networks by a multiple path solution with error correction. IEEE Int. Conf. Commun. pp. 580–585 (2014)
8. Husain, K., Awang, A.: Receiver-based data forwarding in vehicular ad hoc networks. In: 6th Int. Conf. on Intelligent and Advanced Systems (ICIAS), Kuala Lumpur (2016)
9. Wang, L., Wang, Y., Wu, C.: A receiver-based routing algorithm using competing parameter for VANET in urban scenarios. Internet of Vehicles Technologies and Services. Springer International Publishing. pp. 140–149 (2014)
10. Perkins, C., Royer, E.M.: Ad-hoc on-demand distance vector (AODV) routing. Second IEEE Workshop on Mobile Comput. Syst. and Appl. pp. 90–100 (1999)
11. Uzcategui, R.A., Acosta-Marum, G.: WAVE: A Tutorial. IEEE Commun. Mag. **47**(5), 126–133 (2009)

A Novel Angle-Based Clustering Algorithm for Vehicular Ad Hoc Networks

Mohamed Hadded, Paul Muhlethaler, Anis Laouiti and Leila Azzouz Saidane

Abstract A vehicular ad hoc network (VANET) is a mobile network in which vehicles acting as moving nodes communicate with each other through an ad hoc wireless network. VANETs have become the core component of Intelligent Transportation Systems (ITS) which aim to improve the road safety and efficiency. Only if the communication scheme used in a VANET is stable can these aims be achieved. Frequent changes in network topology and breaks in communication raise challenging issues in the design of communication protocols for such networks. Currently, clustering algorithms are being used as the control schemes to reduce changes in VANET topologies. However, the design of a clustering algorithm becomes a difficult task in VANETs when there are many road segments and intersections. In this work, we propose an Angle-based Clustering Algorithm (ACA), which exploits the angular position and the direction of the vehicles to select the most stable vehicles that can act as cluster heads for a long period of time. The simulation results reveal that ACA significantly outperforms other clustering protocols in terms of cluster stability.

Keywords VANET · Cluster protocol · Ad hoc networks · Mobility direction · Angle

M. Hadded (✉) · A. Laouiti
SAMOVAR, Télécom SudParis, CNRS, Université Paris-Saclay,
9 Rue Charles Fourier, 91011 Evry, France
e-mail: mohamed.hadded@telecom-sudparis.eu

A. Laouiti
e-mail: anis.laouiti@telecom-sudparis.eu

M. Hadded · P. Muhlethaler
INRIA, BP 105, 78153 Le Chesnay Cedex, Paris-rocquencourt, France
e-mail: Paul.Muhlethaler@inria.fr

M. Hadded · L. Azzouz Saidane
RAMSIS Team, CRISTAL Laboratory, 2010 Campus University, Manouba, Tunisia
e-mail: leila.saidane@ensi.rnu.tn

A. Laouiti et al. (eds.), *Vehicular Ad-Hoc Networks for Smart Cities*,
Advances in Intelligent Systems and Computing 548,
DOI 10.1007/978-981-10-3503-6_3

1 Introduction

Vehicle-to-vehicle technology provides communication between vehicles through an ad hoc wireless network and eliminates the need for a central station to control the network topology [1, 2]. These vehicular ad hoc networks (VANETs) are characterized by the self-organization of the nodes and rapid changes in network topology due to the high speed of the vehicles. As breaks in communication links frequently occur in VANETs, ensuring communication stability is more difficult in VANETs than in standard MANETs. An effective and cheap solution to reduce the impact of mobility and improve the VANET network connectivity consists in establishing a hierarchical clustering structure within the network.

Designing of an efficient clustering protocol is not a simple task in VANETs due to the rapid changes in network topology. Several VANET research studies in the literature have focused on developing clustering protocols, most of which use the mobility direction metric to form clusters. However, the mobility direction is not always sufficient to insure clustering stability in VANETs as shown in Fig. 1 where the three vehicles v_1, v_2, and v_4 are considered to be moving in the same direction, and thus, these vehicles can be grouped together to form a cluster. Since vehicle v_4 and vehicles v_1 and v_2 are not moving on the same road, vehicle v_4 will leave the cluster after a short period and it will need to join a new cluster. In this paper, we present an Angle-based Clustering Algorithm (ACA), which uses the angle between velocity vectors of vehicles as a metric to form stable clusters. In ACA, two vehicles can form a cluster if and only if the angle between their velocity vectors is acute.

The rest of this paper is organized as follows. In Sect. 2, we present related work. Section 3 gives a detailed description of ACA. Section 4 shows the simulation results and the performance evaluation. Conclusion and perspectives are presented in Sect. 5.

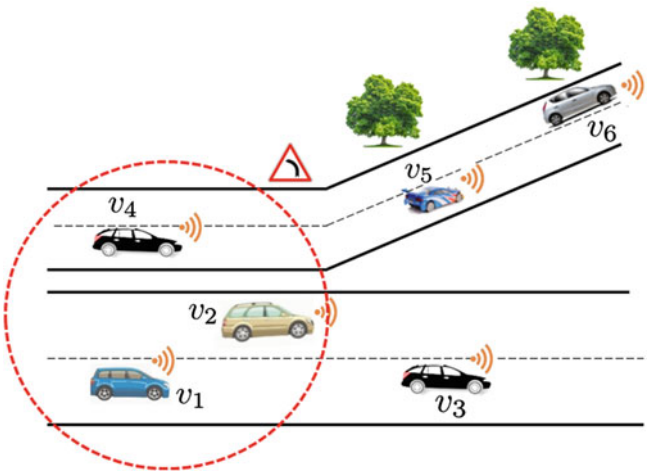


Fig. 1 Mobility direction-based clustering

2 Related Work

Clustering is the best-known method in VANETs to enable efficient resource allocation with low overhead and to reduce the relative mobility between neighboring vehicles. Several VANET research studies in the literature have focused on developing clustering protocols, most of which are based on MANET clustering techniques. Some of the most significant protocols are described below.

In [3], the authors proposed an Adaptive Weighted Clustering Protocol, called AWCP, which is road map dependent and uses road IDs and movement direction in order to make the clusters' structure as stable as possible. However, AWCP is based on the assumption that each vehicle is equipped with a digital mapping device; thus, it cannot operate in environments where vehicles without maps are present. In this work, we suppose that the vehicles are not equipped with digital road map devices, and thus, they cannot obtain the road IDs on which they are traveling. In [4] the authors have proposed a multi-metric algorithm for cluster head elections, called Threshold-based Technique (TB), suitable for highway areas. In addition to the position and the direction, this algorithm uses a speed difference metric as a new parameter to increase the cluster lifetime. The vehicles that are moving at high speed are regrouped into one cluster, while the vehicles moving at low speed are grouped into another cluster. An Adaptable Mobility-Aware Clustering Algorithm based on Destination positions (AMACAD) is proposed and evaluated by Morales et al. [5]. The goal of this work was to develop a clustering protocol with an efficient message exchange mechanism, which improves cluster stability in VANETs. AMACAD performs clustering based upon information such as current location, vehicle velocity, relative destination, and final destination of vehicles. A Multi-Head Clustering Algorithm, called Center-Position and Mobility (CPM), was proposed in [6]. This technique aims to create stable clusters and reduce re-clustering overhead by supporting single and multiple cluster heads. In the cluster head election phase, vehicles within communication range are organized into clusters and one vehicle for each cluster is elected to act as a Master Cluster Head (MCH). Then, some cluster members are selected to be Slave Cluster Heads (SCHs). In order to form stable clusters, the authors imposed that all the vehicles in a cluster are moving in the same direction.

Several other clustering algorithms designed for MANETs also work in VANETs and are frequently used for comparison with other VANET clustering protocols. For instance, the lowest-ID clustering algorithm (LID) [7] is based on electing a node with the smallest ID as a cluster head. The highest-degree algorithm (HD) [8] selects a node as a cluster head based on the nodes' connectivity. The node with the maximum number of neighbors becomes the cluster head. The Weighted Clustering Algorithm (WCA) [9] elects a node to act as a cluster head based on a combined weight which includes the number of its neighbors, their average distance and the node's average speed, and battery life. MOBIC [10] is a mobility-based clustering algorithm designed for MANETs which is also used in VANETs. MOBIC is a mobility-based version of the lowest-ID algorithm and uses a signal power-level metric to elect cluster heads. In this paper, we propose an Angle-based Clustering Algorithm in which

only the vehicles that are located on the same road segment and moving in the same direction can form a cluster by making an acute angle with the cluster heads and their members.

3 Angle-Based Clustering Algorithm

3.1 Assumptions

A VANET in a highway scenario consists of a set of vehicles moving in opposite directions and under varying traffic conditions (speed and density). ACA is based on the assumption that each vehicle in a VANET is equipped with a GPS (Global Positioning System) or a GALLILEO receiver that also allows it to obtain an accurate real-time three-dimensional geographic position (latitude, longitude, and altitude), speed, and exact time.

3.2 Description

ACA consists of three main phases: stable neighbor detection, cluster head election, and cluster maintenance.

Stable neighbor detection On the highway, vehicles traveling in the opposite direction to a reference cluster head will soon lose contact with it, but those traveling in the same direction will keep a relatively stable link state with the reference cluster head. So we should group the vehicles based on their mobility directions. In fact, the vehicles in n-road junctions are grouped into $2 \times n$ different groups $(g_1, \ldots, g_{2\times n})$ according to their directions $(d_1, \ldots, d_{2\times n})$. Figure 2 shows an example of eight possible directions $(d_1, \ldots, d_8)$ of a 4-road junction. As shown in this figure, based on direction information, the vehicles can be grouped into eight different groups; each of which is characterized by one unit vector such as (1, 0) and (0, 1). Two vehicles v and w with velocity vectors (v_x, v_y) and (w_x, w_y) can be grouped together, if the angle between their velocity vectors is acute.

As in [11], we can find whether two vehicles are moving in the same direction based on the angle θ between their velocity vectors. Let us suppose the positions of two vehicles v_1 and v_2 at time t are (x_1, y_1) and (x_2, y_2), and at time $t + \Delta t$ (where Δt is a short time) are $(\hat{x_1}, \hat{y_1})$, $(\hat{x_2}, \hat{y_2})$, respectively, as shown in Fig. 3.

The angle θ between two given velocity vectors is given by the following expression [12]:

$$\overrightarrow{OA}.\overrightarrow{OB} = ||\overrightarrow{OA}|| \times ||\overrightarrow{OB}|| \times \cos\theta \tag{1}$$

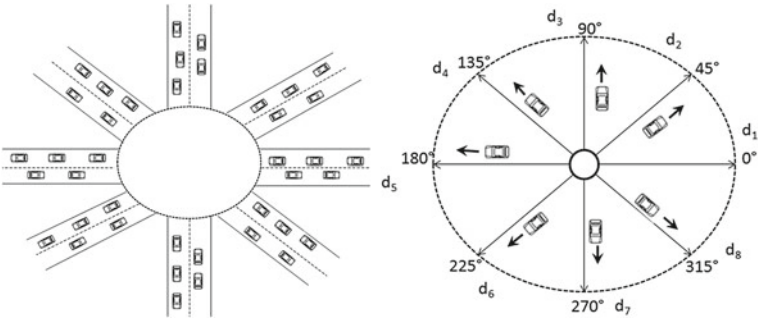


Fig. 2 Eight basic directions and their ranges at a 4-road junction

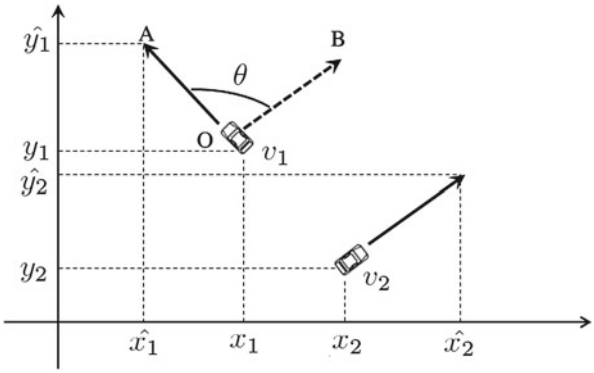


Fig. 3 Moving direction angle calculation

$$\theta = arccos\left(\frac{\Delta x_1 * \Delta x_2 + \Delta y_1 * \Delta y_2}{\sqrt{\Delta x_1^2 + \Delta y_1^2} * \sqrt{\Delta x_2^2 + \Delta y_2^2}}\right) \tag{2}$$

$$\begin{cases} \Delta x = \hat{x} - x \\ \Delta y = \hat{y} - y \end{cases}$$

After receiving of a HELLO message from all each of its one-hop neighbors, vehicle i only considers neighbors that have an angular directions equal to $\theta_i \pm \delta$, where θ_i is the angular direction of vehicle i, and δ is an angular value that represents the range of angles in which two vehicles are considered to be moving in the same direction. The authors in [11] propose that two velocity vectors are non-parallel if the smallest angle between the vectors is higher than 18°. Moreover, vehicle i ignores all HELLO messages broadcasted from neighbors that have non-parallel velocity vectors.Therefore, the direction of the vehicles velocity vectors can help to build a stable cluster structure by grouping only the vehicles that have parallel velocity vectors in the same cluster, as shown in Fig. 4.

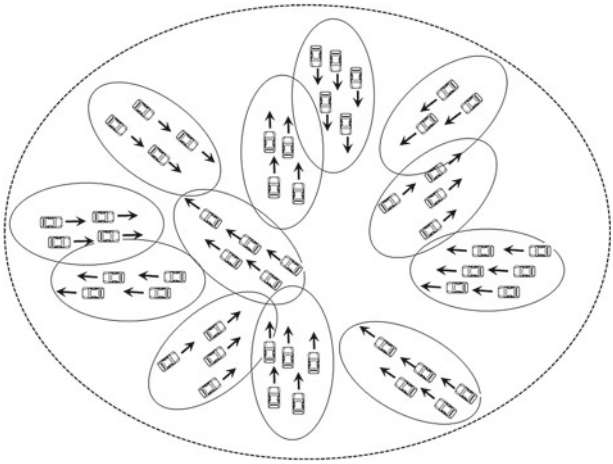


Fig. 4 Angle-based clustering

We propose an angle-based neighbor detection by exploiting the linear feature of a VANET network topology. Instead of discovering neighboring vehicles by exchanging HELLO packets over the entire communication range, we have used an angular technique that allows each vehicle to identify the stable neighbors that it can form a cluster with and does not consider neighboring vehicles that are moving at an obtuse angle. This angular methodology helps us to build stable clusters and to reduce the overhead generated by the reclustering mechanism due to the false merges at road intersections.

Cluster head election In this work, we present our cluster head election algorithm based on the one defined in [13]. Initially, all vehicles are in the undecided state (US). To divide the network into clusters, each active vehicle changes its state to Cluster Head Candidate (CHC) and it starts to broadcast a HELLO message periodically containing all the necessary information $\langle VID, old\_position, current\_position, speed\rangle$ to its one-hop neighbors (OH). Each vehicle periodically updates its *old_position* and *current_position* every 100 ms. On receiving HELLO messages from all its one-hop neighbors, each vehicle will calculate the angles between its velocity vector and those of its one-hop neighbors by using the position information received in the HELLO messages. Each pair of vehicles can find whether they are moving in the same direction based on the angle value between their velocity vectors. In order to form stable clusters, only HELLO messages received from vehicles that are moving with an angle less than ϕ are considered, and the other messages are rejected. After that, each vehicle i will update its one-hop neighbor list (OH_i) and it will calculate its current weight $\omega(i, t)$ using the following normalized weight function (3). This function consists of three parts, i.e., the average distance to the direct neighbors (i), the average speed (ii), and the number of neighbors (iii).

$$\omega(i,t) = w_1 * \frac{\delta(i,t)}{\tau} + w_2 * \frac{|\nu(i,t) - \rho(i,t)|}{\vartheta} - w_3 * \frac{n(i,t)}{\psi} \tag{3}$$

where w_1, w_2 and w_3 are the balancing factors such that $\sum_{k=1}^{3} w_k = 1$, τ is the maximum radius of the vehicles, ϑ is the maximum allowed speed on the highway, and ψ is the cluster size. We note that the three weight factors are in conflict. For simplicity, we assume that all the factors should be minimized. In fact, the multiplication of the third weight factor by (-1) allows us to transform a maximization to minimization. Then, each node i broadcasts a beacon message containing all the necessary information for the CH election algorithm $\langle VID, \omega, CH - ID \rangle$. Vehicle i announces itself as a CH by assigning its own ID to the CH-ID field of the election beacon. When a vehicle i receives beacons from its one-hop neighbors, it sorts its neighbor list OH_i according to the weights received in the beacons, and then it executes the cluster head election algorithm to change its status from CH to Cluster Member (CM), Cluster Gateway (CG), or remain CH.

$$\omega(i,t) = \{min\ \omega(j,t)\ \forall\ j \in OH_i\}, \tag{4}$$

$$n(i,t) \leq \psi \tag{5}$$

The vehicle i that satisfies the two properties (4) and (5) at instant t is elected as the CH. Then, all vehicles that are within transmission range of the CH become CMs or CGs and are not allowed to participate in another cluster head election procedure. The CH election algorithm terminates once all the vehicles become either a CH, a CM, or a CG.

Cluster maintenance In VANETs, a vehicle can join or leave a cluster at any time. These two operations will have only local effects on the topology of the cluster if the vehicle is a CM. However, if the vehicle is the CH, it must hand over the responsibility to one of the very close cluster members before leaving the cluster. The first reason for that is to maintain the cluster structure even if the current CH leaves. The second reason is to avoid using the reclustering algorithm, and thus, no reclustering overhead is generated when the CH leaves the cluster.

Joining a cluster: The cluster head periodically broadcasts an ITJ (Invite-To-Join) message to its one-hop neighbors. Once a US or CHC vehicle receives an ITJ message, and if it wishes to join the cluster, it will send an RTJ (Request-To-Join) message including the vehicles ID, *old_position*, *current_position*, and speed. When the CH receives the RTJ message, it will calculate the angle between its velocity vector and that of the requesting vehicle, and if the angle is less than ϕ, the CH sends an acknowledgment (ACK) including its ID number. After the reception of the ACK, the corresponding vehicle becomes a CM of this cluster.

Leaving a cluster: A vehicle remains in the CM state as long as it receives an ITJ and has an acute angle with its cluster head. As shown in Fig. 5, when a cluster member CM1 leaves its cluster, it will create an obtuse angle with its cluster head

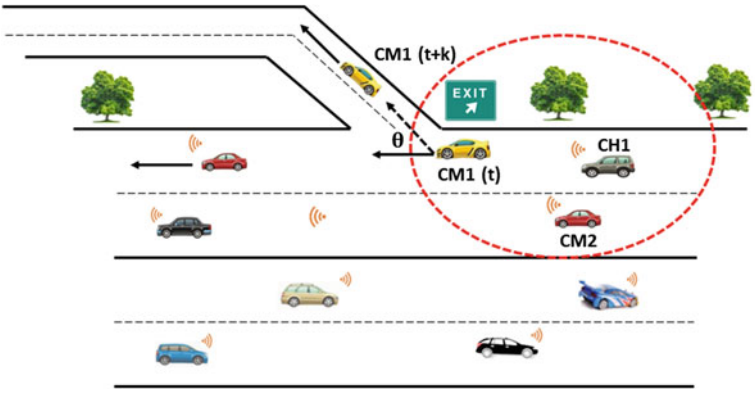


Fig. 5 Highway exit scenario

CH1. At instant $t + k$, the cluster head removes a CM1 from its cluster members list if the angle between their velocity vectors is greater than ϕ.

Clusters merging: When two or more CHs are moving in the same direction with an acute angle, only one of them will keep its cluster head responsibility while the others will switch to a cluster member status. The selection of a cluster head for merging clusters is done based on the weight $\omega(i, t)$. In order to avoid false merges (when two clusters are merged and then they are separated just after merging), we restricted the merging to clusters having the same average speed.

4 Simulation Results and Performance Evaluation

This section presents ns-2 simulation results to evaluate the performance of our proposed clustering algorithm ACA. The objectives of the evaluation are to: (1) evaluate the performance of ACA under different traffic conditions, (2) evaluate and compare the efficiency of ACA with other clustering protocols in the literature, and (3) test the efficiency of ACA in reducing the number of states changed per vehicle.

4.1 Simulation Scenarios

We generated a realistic VANET environment by selecting a real highway area from a digital map which took into account lane directions. Figure 6 shows a metropolitan area from a map of San Jose (California) of size 3000 m $\times$ 100 m exported from OpenStreetMap (OSM) and edited using Java OpenStreetMap Editor (JOSM). Then MOVE and SUMO [14] were used, respectively, to generate vehicular traffic scenarios and to simulate the area with vehicular traffic. To do that, we defined a

Fig. 6 San Jose (California) urban area captured from Google Maps (*left*) and exported to a VANET network topology by using MOVE/SUMO (*right*)

Table 1 Simulation parameters in ns-2

Parameter	Value/protocol
Simulation time	80 s
Vehicle speed	120–150 km/h
Propagation model	Two Ray Ground
Medium capacity	6 Mbps
Transmission range	310 m
Transport layer	UDP
CBR packet size	512 bytes
Vehicle density (σ)	20 40 80 120 160 200 240 280 300

vehicle flow which described a swarm of vehicles in each direction. The parameters of each vehicle flow consist of the maximum number of vehicles, the starting road and destination of the flow, and the time to start and end the flow. We assigned a random speed to each vehicle between 120 and 150 km/h. Then the traffic traces generated by SUMO were used in the *ns*2.34 simulator. The simulation parameters used in our experiments are summarized in Table 1.

4.2 Performance Evaluations

In this section, we evaluate and compare the performance of ACA with other clustering protocols proposed in the literature, namely AWCP [3], CPM [6] and HD [8]. We use the set of parameters found using the NSGA-II approach, see [13]. We simulate several scenarios by varying the vehicle density from 20 to 300 vehicles in the whole network. Figure 7 shows the cluster lifetime for the algorithms with different vehicle densities (σ). This figure clearly shows that the cluster lifetime increases as the

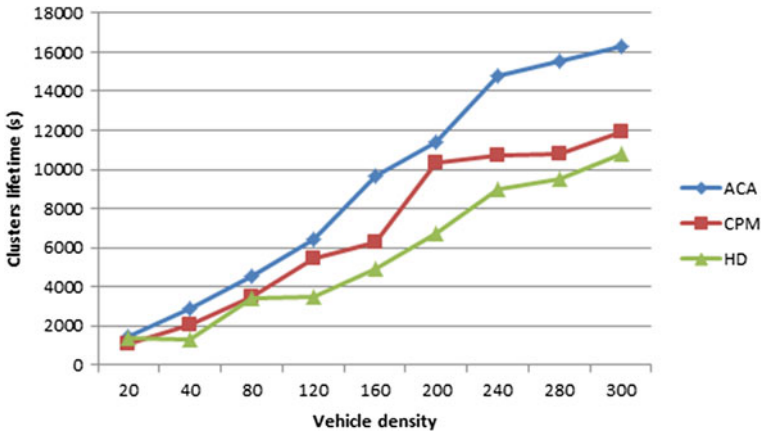


Fig. 7 Cluster lifetime under various traffic densities

number of vehicles increases. We can see that ACA achieves a considerably longer cluster lifetime than CPM and HD. For instance, for a high density (when $\sigma = 300$), the cluster lifetime is increased by 36.9 and 50.68%, respectively. These results can be explained by the fact that, in ACA, only vehicles that are moving in the same direction with an acute angle can form a cluster, and thus, the CMs will be associated with their CHs for a longer period of time. We can also note that CPM outperforms HD, because the CPM protocol forms clusters based on the mobility direction.

Figures 8 and 9 show the number of state transitions for each vehicle during the simulation for the scenarios where σ equals 120 and 200, respectively. We can note from these two figures that ACA generates the lowest number of transitions. For instance, the vehicle of ID 70 in Fig. 8 maintains its state throughout the simulation time when ACA is used, whereas it changes more than once when CPM or HD is used. These results are due to the fact that ACA avoids the problem of merging multiple clusters into a single cluster at road junctions.

In order to highlight the efficiency of ACA algorithm, we evaluate and compare it with the AWCP protocol in VANET scenarios where vehicles without maps are present. Figure 10 shows the Average Cluster Lifetime (ACL) for ACA and AWCP. These protocols are evaluated when we vary the number of vehicles which are not equipped with a digital map device between 20, 40, and 50%. As ACA is an angle-based clustering algorithm, the presence of vehicles that do not have map does not influence its performance. Moreover, when all the vehicles in the network have a map, the ACA and AWCP protocols have almost the same average cluster lifetime. However, we can note that the ACL metric decreases for AWCP as the number of vehicles that have no map increases. These results can be explained by the fact that each map-unequipped vehicle that is in the US[1] state joins any cluster without taking into account any road ID.

[1] Undecided State.

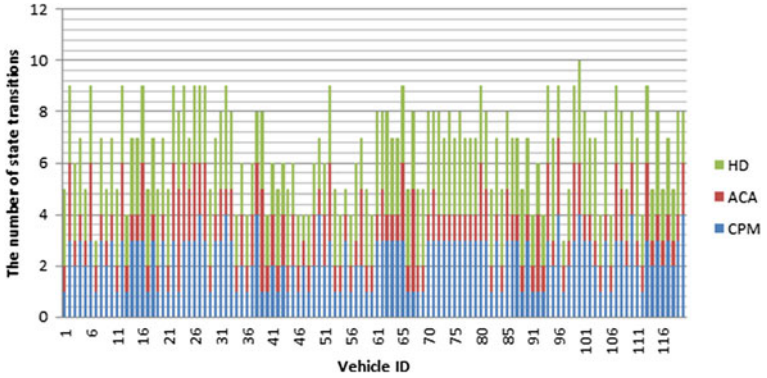


Fig. 8 Number of vehicle state transitions for $\sigma = 120$

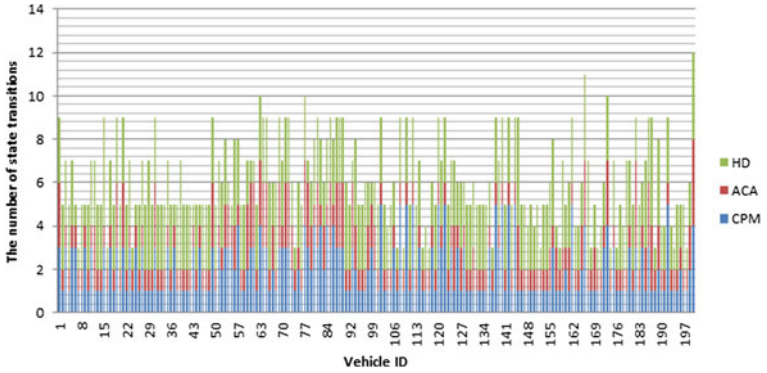


Fig. 9 Number of vehicle state transitions for $\sigma = 200$

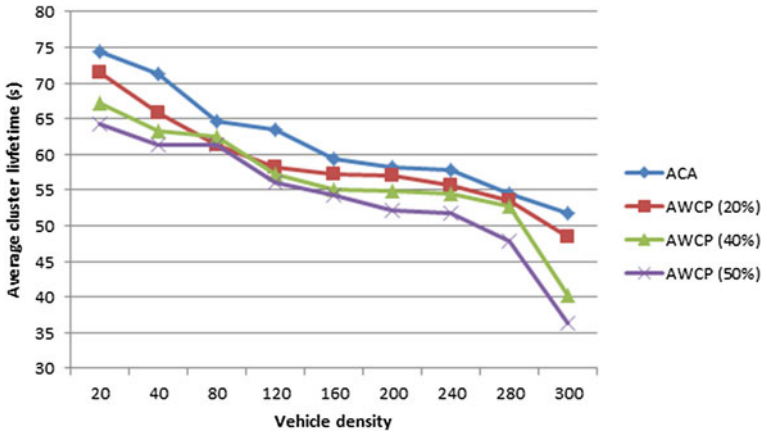


Fig. 10 Average cluster lifetime under various traffic densities

5 Conclusion

The design of a stable clustering algorithm becomes a difficult task in VANETs when there are many road segments and intersections. In this paper, we propose an Angle-based Clustering Algorithm, named ACA, in which the velocity vector angle between the vehicles participating in the cluster head election process is used as a metric to improve cluster stability in VANETs. The simulation results show that ACA clearly improves the clustering performance in VANETs in terms of cluster lifetime. As future work, we plan to design a cross-layer architecture combining a Medium Access Control (MAC) protocol and a clustering scheme to improve channel access efficiency in VANETs where cluster head would be responsible for assigning bandwidth to all the members of its cluster.

References

1. Hadded, M., Zagrouba, R., Laouiti, A., Muhlethaler, P., Saidane, L.A.: An adaptive TDMA slot assignment strategy for vehicular ad hoc networks. J. Mach. Mach. Commun. **1**, 175–194 (2014)
2. Hadded, M., Muhlethaler, P., Laouiti, A., Zagrouba, R., Saidane, L.A.: TDMA-based MAC protocols for vehicular ad hoc networks a survey. IEEE Commun. Surv. Tutor. **17**(4), 2461–2492 (2015)
3. Hadded, M., Muhlethaler, P., Zagrouba, R., Laouit, A., Saidane, L.A.: Using road ids to enhance clustering in vehicular ad hoc networks. In: IEEE IWCMC, Dubrovnik, Croatia, pp. 285–290 (2015)
4. Rawashdeh, Z.Y., Mahmud, S.M.: A novel algorithm to form stable clusters in vehicular ad hoc networks on highways. In: EURASIP Journal on Wireless Communications and Networking (2012)
5. Morales, M.M.C., Hong, C.S., Bang, Y.C.: An adaptable mobility-aware clustering algorithm in vehicular networks. In: APNOMS, Taipei, Taiwan, pp. 1–6 (2011)
6. Lo, S.C., Lin, Y.J., Gao, J.S.: A multi-head clustering algorithm in vehicular ad hoc networks. Int. J. Comput. Theory Eng. **5**(2), 242–247 (2013). Apr
7. Gerla, M., Tsai, J.C.: Multicluster, mobile, multimedia radio network. Wirel. Netw. **1**(3), 255–265 (1995)
8. Ramalingam, A., Subramani, S., Perumalsamy, K.: Associativity based cluster formation and cluster management in ad hoc networks. In IEEE HiPC, Bangalore, India, pp. 1–6 (2002)
9. Chatterjee, M., Das, S.K., Turgut, D.: A weighted clustering algorithm for mobile ad hoc networks. Clust. Comput. **5**(2), 193–204 (2002). Apr
10. Basu, P., Khan, N., Littl, T.: A mobility based metric for clustering in mobile ad hoc networks. In: ICDCS Workshop, Arizona, pp. 413–418 (2001)
11. Naumov, V., Gross, T.: Connectivity-aware routing (car) in vehicular ad-hoc networks. In: IEEE International Conference on Computer Communications, Anchorage, Alaska (2007)
12. Tian, D., Shafiee, K., Leung, V.C.: Position-based directional vehicular routing. In: Global Telecommunications Conference, GLOBECOM 2009. IEEE, hawaii, USA, pp. 1–6 (2009)
13. Hadded, M., Zagrouba, R., Laouiti, A., Muhlethaler, P., Saidane, L.A.: A multi-objective genetic algorithm-based adaptive weighted clustering protocol in vanet. In: IEEE CEC, Sendai, Japan, pp. 994–1002 (2015)
14. Karnadi, F., Mo, Z., chan Lan, K.: Rapid generation of realistic mobility models for vanet. In: IEEE WCNC, Hong Kong, China, pp. 2506–2511 (2007)

Vehicular Ad Hoc Network (VANET): A Survey, Challenges, and Applications

Asim Rasheed, Saira Gillani, Sana Ajmal and Amir Qayyum

Abstract An ad hoc network consisting of vehicles has emerged as an interesting but challenging domain where a lot of new application may find their place. Though research in this field is on since last two decades, large-scale practical implementation still require some time. In this paper, a survey of current challenges and potential applications, incorporating medium access control schemes, routing approaches, hardware and spectrum issues, and security and privacy issues for VANETs, is presented.

Keywords VANETs · Challenges · Applications

1 Introduction

Vehicular ad hoc network (VANET) is a challenging network environment that pursues the concept of ubiquitous computing for future. Vehicles equipped with wireless communication technologies and acting like computers will be on our roads soon, and this will revolutionize our concept of traveling. VANETs bring lot of possibilities for new range of applications which will make our travel not only safer, but also fun.

A. Rasheed (✉) · A. Qayyum
Center of Research in Networks & Telecom (CoReNeT), Capital University of Science & Technology, Islamabad, Pakistan
e-mail: asim@corenet.org.pk

A. Qayyum
e-mail: aqayyum@ieee.org

S. Gillani
Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan
e-mail: sairagilani@yahoo.com

S. Ajmal
Research Center of Modeling and Simulation, National University of Sciences & Technology, Islamabad, Pakistan
e-mail: sanaajmal@gmail.com

A. Laouiti et al. (eds.), *Vehicular Ad-Hoc Networks for Smart Cities*,
Advances in Intelligent Systems and Computing 548,
DOI 10.1007/978-981-10-3503-6_4

The concept of VANETs is quite simple: By incorporating the wireless communication and data sharing capabilities, the vehicles can be turned into a network providing similar services to the ones we are used to in our office or at home networks.

VANET is considered an offshoot of mobile ad hoc networks (MANET). In many ways, VANETs are similar to MANETs. For example, both networks are multi-hop mobile networks having dynamic topology. There is no central entity, and nodes themselves route data across the network. Both MANETs and VANETs are rapidly deployable without the need of an infrastructure.

VANETs have some distinguishing characteristics in many ways [1]. Both MANET and VANET are mobile networks; however, the mobility pattern of VANET nodes follows geometrical patterns. MANETs are often characterized by limited storage capacity, low battery, and processing power. VANETs, on the other hand, do not have such limitations.

In VANETs, any node may move at high relative velocity. This makes the lifetime of communication links between nodes quite short. Node density is also unpredictable; during rush hours, the roads are crowded with vehicles. Similarly some roads have more traffic than other roads.

Specialized and mixed node deployment patterns and versatile mobility have made the problem more complicated. These network topologies which are highly fluent in nature also involve large variations in node densities and relative node velocities. Scalability considerations of futuristic networks may require support for several thousands of nodes spanned in very large areas. Quality-of-service (QoS) requirements for such multidimensional and complicated networks pose another challenging dimension.

In addition to this, there are many new and unique applications emerging for VANETs, such as traffic management, emergency response services, infotainment, theft detection, law enforcement, military and commercial fleet, and convoy management [2].

Although many different solutions have been presented by research community to answer the problems, consensus has developed on four major approaches, which are given as:

- Software-defined hardware to adapt according to available resources.
- Provision of efficient MAC scheme for maximum utilization of physical resources.
- Selection of best possible route incorporating runtime changes.
- Designing of network efficient applications.

On the one hand, efficient MAC and hardware will provision maximum physical layer resources for upper layer's data, to provide best QoS. On the other hand, efficient applications and routing will try to use minimum network resources. These two pronged and mutually complimentary strategies, known as cross-layer architecture, have opened up new dimensions and possibilities for researchers. Several academic and industrial projects have been initiated to address these challenges [3].

The rest of this paper is organized as follows: Sect. 2 presents VANET applications and their requirements; Sect. 3 discusses current challenges for VANET, and Sect. 3 concludes the paper.

2 Challenges

Though, initially it was considered that VANET is a subclass of MANET, most of the research and designs related to MANET were applied to VANET. However, subsequent progress showed significant difference among both classes of networks. VANET paradigm design for communication, privacy, and provisioning coupled with security cannot be compared directly with MANET.

To highlight the peculiar VANET issues, a lot of research has already been done [4, 5]. However, many challenges are still open to researchers for the optimum solution due to non-implementation of VANET at large scale. In subsequent discussion, key challenges of the VANET are highlighted.

2.1 VANET Architecture

Architecture definition was considered as a prime problem by many standardization organizations, such as IEEE and ISO [3]. The work on formulation of four main standards started in parallel, lacking major collaboration and coordination. These standards include WAVE, C2C, CALM, and ARIB. Different regional agencies, political forces, and car manufacturers backed different standards without focusing a global harmony.

2.1.1 CALM

International Standard Organization (ISO) started its own standard named as CALM (Communications, Air-interface, and Long and Medium range). This standard is although quite complex focused on seamless inter-node and intra-node communication. The concept of CALM architecture is a heterogeneous cooperative communication framework. CALM was the first one to introduce any available interface at MAC layer. However, seamless handshake of different MAC interfaces is still open to researchers.

2.1.2 C2C

European automobile industry backed a VANET standard under the label of GEoNEt through Car-2-Car Communication Consortium (C2C-CC). It is a comprehensive architecture, mainly aiming at active safety applications. It is significantly different from Internet architecture. However, it supports many available interfaces at MAC and PHY layers.

2.1.3 WAVE

IEEE started its work under the label of WAVE (Wireless Access in Vehicular Environment). Though WAVE is a complete protocol stack labeled as 1609 protocol family and is based on current Internet model, so far no major large-scale implementation is available other than test laboratories and small-scale projects [2]. Moreover, WAVE only allows IEEE 802.11p MAC for all kinds of communication, which is considered as a bottleneck by many researchers.

2.1.4 ARIB

Japanese Standardization Agency: The Association of Radio Industries and Businesses (ARIB) defined multiple VANET architectures. Although mainly relying on WAVE, first ARIB standard named as ARIB-2001 uses only single MAC layer at 700 MHz band. Later, ARIB-2004 introduced use of 5.8 GHz band. ARIB-2008 introduced use of infrared for toll payment. Like WAVE, ARIB only focuses on emergency VANET messages. Currently, JAPAN is the most VANET compliant country in the world.

2.2 Transmission Capacity Limits

According to researchers, fundamental communication limit for mobile networks is extremely difficult [6, 7]. Researchers have defined transmission capacity as the number of successful simultaneous transmissions within a unit region [8]. Shannon in 1948 gave the formula for the capacity of the link-based networks [6]. Researchers showed that in mobile ad hoc networks, where peer-to-peer communication, interference, and mobility play an important role, Shannon's framework is not applicable [8, 9]. Andrews et al. [8] showed that the researchers have yet not been able to find a framework which can be used to find the fundamental capacity of an ad hoc network.

Interference, noise, and back-off delays are major concerns for any MAC protocol. Out of these, interference is the most limiting factor for VANETs. Interference must be mitigated to meet minimum signal-to-interference-plus-noise ratio (SINR) threshold. Current MAC protocols use techniques such as carrier sensing, random back-offs, spread spectrum and guard zone-based inhibition, to mitigate interference. Under a dense VANET environment, such as traffic jam and parking areas, the number of nodes, hence the interference, will increase overwhelmingly. There are a lot of researchers who have evaluated different MAC schemes. However, no significant work is done to check the transmission capacity under VANET architectures. Presence of hundreds of nodes will cause severe MAC issues, which will increase manifolds in case of an emergency.

2.3 Routing Techniques

Routing techniques and protocols are one of the most researched topics in VANET [1]. However, the main challenge to design a VANET routing protocols which is suitable to all scenarios and conditions is still open. More or less, researchers have consensus that static or single routing scheme cannot satisfy varying VANET network conditions. Summary of a few surveys on routing in VANET [1] is given below:

- Before determining routes, varying real traffic state is generally not considered by many protocols.
- All real-life traffic conditions cannot be met through current VANET routing protocols.
- Under rapidly changing VANET topologies, topology-based routing lacks efficiency.
- Delay tolerant networks, such as disconnected nodes, cannot be covered using vehicle-to-vehicle communication design.
- Use of non-delay tolerant routing protocols face degradation during disconnected scenarios.
- Though periodic or proactive routing approaches provide low latency, network resources are generally underutilized due to unused paths.
- Though on-demand or reactive routing protocols provide better resource utilization, latency in route determination is major limitation.
- Though geographical information is considered very helpful for VANET, mapping of geographical regions as per road layout is a big problem.
- Network partitioning and availability of accurate and updated location information causes significant network resource wastage.
- Geographical routing can form routing loops or a packet can travel longer route due to network partitioning.
- Under high-speed movement, inherent latency of GPS [10] may cause inaccurate emergency alerts, e.g., accident alert.

Efficient routing focuses on three main goals, i.e., efficiently finding most suitable route from source to destination, updating the new route at run time on availability of a better one, and lastly maintaining the route in the case of route failure. Most of the current research covers the first and third goals, whereas the second goal is generally considered as the logical outcome of the first one [1].

To find a route between two nodes, routing algorithms currently focus on three basic questions.

- What information (metrics) should be shared for determination of route?
- How and when the selected information should be shared within the network?
- How route should be determined using the shared metric?

To answer the metric issue, many different metrics for route finding have been identified by the researchers. Subsequently, hundreds of protocols have been proposed using a single or a combination of metrics. Metrics can be grouped as localized, end-to-end, and cross-layer [1].

Second issue of how to disseminate the routing information is generally simpler, and researchers have considered mainly three types:

- Through sharing of repeated/automated topology beacons regardless of situation change.
- Through sharing of topology updates, either for new route determination or on link breakage.
- Derivatives of above two approaches.

For dissemination of selected metric information from a single node perspective, choices restrict to first two only. The decision for sharing the metric to next hop is determined by the role of said node, i.e., source node or transit node. Decision for both of the roles is generally preconfigured without any significant runtime intelligence.

In the absence of any deployed VANET architecture, early research on VANET routing was based on the simulation scenarios. The main goal of this research was to provide safety information to nearby vehicles. With the advancement in research, the need emerged to incorporate roadside servers and Internet. Such requirement demanded multi-hop communication and more robust routing schemes based on realistic traffic and mobility and communication constraints.

Current routing research is primarily focused on routing algorithms with stationary route update policy, using off-time configurations only. Adaptation in routing has also been proposed by researchers through different approaches [1, 11]. The requirement of route update in the lifetime of previous route requires updated information of network conditions. Analysis of different situations shows that the route update mechanism in the current routing approaches is more or less fixed and predefined in the protocol, instead of being based on runtime network conditions.

To answer the routing challenges of dynamic networks, e.g., VANET, having range of node densities with rapid topology changes due to high mobility and scalability, there is a need of new, more flexible and adaptive route update and maintenance strategies. These new route update strategies must work efficiently, supporting a variety of realistic node deployment patterns, mobility scenarios, and QoS requirements.

2.4 Security and Privacy

Though most of the VANET security issues are same as MANETs, privacy issues are more complicated in VANETs. Security concerns are more complex due to the scalability, frequent topology changes, high mobility, and variety of applications. In addition to this, there is a compromise among authentication and non-repudiation against driver/vehicle privacy. Figure 1 enlists some of the security concerns related to the VANET.

After deployment of VANET, intelligent on-board applications may keep record of large amount of vehicle movement data and personal information. Theft or misuse of such information can lead to serious privacy and general security issues. There is a dire need to overcome these concerns before large-scale deployment of VANET.

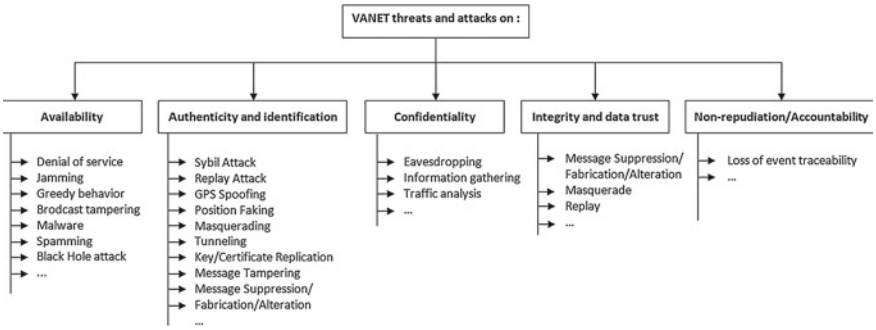


Fig. 1 Categorization of VANET Attacks

Though researchers are already doing efforts to address the security problems in VANETs, a comprehensive strategy to answer the issue is still open considering the unique characteristics of heterogeneous vehicular networks. Some characteristics of VANETs pose challenges to meet security requirements, such as low overhead, time sensitivity, minimum hops, use of stored information, and optimized data dissemination solutions.

Another major issue is to prevent attackers from interfering with both the integrity of the exchanged messages and the availability of the system. Tracking a target is a fundamental functionality in VANETs for communication protocols and also for applications and services. Tracking requires creating a mechanism to identify the path a node follows in the network and predict the next positions if necessary.

2.5 Verification and Validation

Most of the research is validated through theoretical modeling against simulative studies. Such methodology provides definition for upper and lower practical bounds prior to implementation. However, most of the research for MAC and routing strategies is based on routing scenarios defined in well-known and especially open-source simulators [11]. A survey on network simulators [12] identifies many significant limitations in scenarios, environments, and protocol patch implementations.

The fact of simulation limitations is also evident from different results even for same scenario and using same simulator. The large variations among graphs for different metrics, e.g., node density, velocity, delay, and throughput, under same environment demand clear definition and usage of simulative scenarios as well as metrics for final evaluation. Lack of such definitions leads to many questions on viability of results. The major limitations can be identified as:-

- The term of 'highly scalable' has gone beyond the scope of few hundred nodes. Traffic jams and parking areas may have thousands of nodes, heavily packed.

- The term velocity or speed cannot be compared with relative mobility. Two nodes moving in same direction even at the speed of fighter aircraft can be considered static with respect to each other.
- The active node density can be compared neither with simple node density nor with scalability, especially for networks such as VANETs. There can be scenarios with very high node density, but with very limited number of nodes practically participating in active communication.
- There can be different types of data behaviors experienced at MAC layers. Variations to single hop to multiple hop communication and versatile QoS support cannot be guaranteed in all scenarios of same network.

Accordingly, there is a need to verify and validate any VANET protocol or approach incorporating following conditions.

- Driver and vehicle model
- Traffic flow model
- Communication model
- Application model
- Driver behavior model

2.6 Software-Defined Hardware

A significant increase in VANET deployment will flood VANET applications. Such increase will be more visible in urban regions. Resultantly, large number of nodes will exhaust communication resources and may lead decrease in efficiency for safety applications. At the same time, use of bandwidth hungry infotainment applications, such as multimedia applications and information systems, can lead to spectrum scarcity.

Under congested circumstances, use of cognitive or software-defined hardware can provide efficiency in VANETs. This can enable efficient radio spectrum usage and overall vehicular communication efficiency.

As in many countries, spectrum regulators are utilizing unused license bands for unlicensed services over different space and time. Unused licensed spectrum bands include television and broadcasting. Such allocation makes software-defined hardware an attractive choice for VANET. Resultantly, cognitive radios and dynamic spectrum allocation is an open research topic to enhance the spatiotemporal efficiency of VANET PHY and MAC.

3 Applications

The most targeted and ultimate goal was to ensure safer travel by generating early warnings and timely response to the situations. However, to increase the market penetration, other classes of applications such as traffic control and provision of

Fig. 2 Categorization of VANET Applications

infotainment are also being considered [2]. Different VANET architectures support multi-channel operation for safety- and non-safety-related applications on a different channel. Based on the primary purposes, VANET applications are typically classified into two major categories [13–15] (Fig. 2):

- Safety-oriented applications
- Non-safety applications

3.1 Safety-Oriented Applications

The aim of safety applications was to ensure safer travel by generating early warnings and timely response to the situations. These applications are used to avoid the risk of road accidents by distributing information about hazards and obstacles. Safety

applications can play an important role in avoiding accidents or minimizing the impact of accidents. According to a study, if the driver gets a warning half a second before the collision, more than half of the accidents can be avoided [16].

On the road, there are many considerations for a driver, such as attention toward traffic lights, pedestrians, and other vehicles as well as following GPS directions. This is impossible for a driver to focus their full attention on all of these events at once. For example, a driver getting ready to make a right turn might easily overlook a pedestrian crossing on the left side of the street. Therefore, the number of accidents can also be reduced with the help of early warning system. Some other kinds of warning systems can also be deployed to avoid the accidents, e.g., work zone warning, stopped vehicle warning, and low bridge warning for trucks.

Some safety applications can also be helpful after accident such as to send emergency notifications to nearby emergency responders. Such applications also manage traffic flows and identify alternative routes.

Besides warning messages, safety applications are also used to provide assistance to a drive about lane change, navigation and to avoid collisions by applying automatic emergency breaks. Safety applications also guide the driver about speed limit to avoid collisions.

Safety applications demand strict time delay bounds. Even a fraction of a second is important in decision making. Thus, the requirement of hard deadline posed by the safety applications requires special handling at lower layers. As network layer is concerned, not much routing is involved in safety applications, because the target audiences for the messages are usually in the neighborhood. Therefore, the messages need not to be sent to nodes more than one hop away.

3.2 Non-safety Applications

Although the main purpose of VANET is to provide safety, however, some non-safety applications are also being considered to increase the market penetration such as traffic efficiency, control management, and some infotainment applications [2].

3.2.1 Traffic Control and Management Applications

The main purpose of traffic control and management applications is to optimize traffic flows and to minimize the travel time by avoiding traffic congestions or assist the driver about best route with updated road conditions. This can involve the use of some roadside equipment, e.g., intelligent traffic signals and e-sign boards. Information about the road congestions ahead can definitely help in reducing the congestion and improving the capacity of roads.

Some other applications can also be envisioned such as automated call to emergency services, enroute, and pre-trip traffic assistance. An interesting application is eToll plaza, where vehicles do not need to stop to pay toll fee. Vehicles can commu-

nicate with the roadside infrastructure, where it can be recognized and a fee can be charged against its account.

Congestion at road intersections can be handled in an efficient manner using intelligent traffic signals. These traffic signals can adjust themselves in response to the traffic conditions at intersection and can even communicate the status to neighboring intersections. Neighboring intersections can thus display this information on the e-sign boards and adjust their traffic signals accordingly.

Traffic management applications extensively use the roadside infrastructure. Some infrastructure may be available to be used by any user while some will need subscription. For example, eToll infrastructure will require a subscription to offer its services. For these applications, the infrastructure needs to be managed and updated. For these applications to work, the infrastructure with relevant information needs to be managed and controlled. Comfort and Infotainment Applications be managed and controlled.

3.2.2 Comfort and Infotainment Applications

Besides road safety applications, comfort and entertainment applications are also envisioned for VANETs. These applications aim to provide comfort and entertainment to travelers. Such applications can be further categorized into three types: infotainment, mobile e-commerce, and city leisure information.

The passengers in a vehicle can enjoy the facility of Internet connectivity where other traditional wireless Internet connectivity options (Wi-Fi, Wi-MAX, etc.) are not available. Even in the presence of such options, a node connected to Internet through these options can share its connectivity with other vehicles through VANET. Peer-to-peer applications can also find their place in VANETs, e.g., gaming, chatting, file sharing, and Web browsing.

Different companies use VANET for advertisements or announcements of location-based sales information; for example, gas stations can announce updated prices or different restaurant can highlight different deals to attract travelers. Beside this, some VANET applications make it easy for travelers to see the nearest service shops or restaurant, etc. The messages sent by such type of applications usually need to be delivered over multiple hops; hence, routing will be involved.

Infotainment applications in VANET can be grouped as peer-2-peer and Internet-based applications. These applications are very much useful to provide services such as sharing multimedia files, movies, and songs among the vehicles in the network. People can connect with the Internet all the time, thereby VANET provides the constant connectivity of the Internet to the users. These applications provide comfort for travelers such as advanced traveler information systems and general entertainment.

4 Conclusion

This paper presents VANETs by highlighting current challenges and applications. The applications envisioned are likely to find their place in inter-vehicular communication, hence making the widespread VANET deployment possible in near future. Although significant research has already been done, many key factors for their success are still open. There is lack of profound performance evaluation of different schemes and versatile and comprehensive real-life scenarios in VANET context. The few studies that are currently available are not only limited in scope, but also restricted to a specific scenario. Hence, some upcoming challenges are still open to researchers.

References

1. Ajmal, S., Rasheed, A., Qayyum, A., Hasan, A.: Classification of VANET MAC, Routing and approaches a detailed survey. J. UCS **20**(4), 462–487 (2014)
2. Rasheed, A., Zia, H., Hashmi, F., Hadi, U., Naim, Warda, Ajmal, Sana: Fleet & convoy management using VANET. J. Comput. Netw. **1**(1), 1–9 (2013)
3. Sajjad Akbar, M., Rasheed, A., Qayyum, A.: VANET architectures and protocol stacks: a survey. In: International Workshop on Communication Technologies for Vehicles, pp. 95–105. Springer, Berlin, Heidelberg (2011)
4. Liang, W., Li, Z., Zhang, H., Wang, S., Bie, Rongfang: Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends. Int. J. Distrib. Sens. Netw. **2015**, 17 (2015)
5. Da Cunha, F.D., Boukerche, A., Villas, L., Carneiro Viana, A., Loureiro, Antonio AF.: Data communication in VANETs: a survey, challenges and applications. Ph.D. diss., INRIA Saclay; INRIA (2014)
6. Ajmal, Sana, Jabeen, Samra, Rasheed, Asim, Hasan, Aamir: An intelligent hybrid spread spectrum MAC for interference management in mobile ad hoc networks. Comput. Commun. **72**, 116–129 (2015)
7. Ajmal, S., Adnan, S., Rasheed, A., Hasan, A.: An intelligent hybrid spread spectrum MAC protocol for increasing the transmission capacity of wireless ad-hoc networks. In: Telecommunication Networks and Applications Conference (ATNAC), 2014 Australasian, pp. 46–51. IEEE (2014)
8. Andrews, J., Shakkottai, S., Heath, R., Jindal, N., Haenggi, M., Berry, R., Guo, D., Neely, M., Weber, S., Jafar, S., et al.: Rethinking information theory for mobile adhoc networks. IEEE Commun. Mag. **46**(12), 94–101 (2008)
9. Haenggi, M.: On distances in uniformly random networks. IEEE Trans. Inf. Theory **51**(10), 3584–3586 (2005)
10. Rasheed, A., Ajmal, S.: 3D-a Doppler, directivity and distance based architecture for selecting stable routing links in VANETs. In: 2nd International Conference on Computer, Control and Communication, IC4 2009, pp. 1–5. IEEE (2009)
11. Rasheed, A., Ajmal, S., Qayyum, A.: adaptive routing update approach for VANET using local neighbourhood change information. Malays. J. Comput. Sci. 27(4) (2014)
12. Hassan, A.: VANET Simulation Master Thesis in Electrical Engineering, School of Information Science, Computer and Electrical Engineering, Halmstad University (2009)
13. Elias, S.J. et al.: A comparative study of IEEE 802.11 standards for non-safety applications on vehicular ad hoc networks: a congestion control perspective. In: Proceedings of the World Congress on Engineering and Computer Science (2014)

14. Di Felice, M. et al.: Enhancing the performance of safety applications in IEEE 802.11p/wave vehicular networks. In: IEEE International Symposium on a WoWMoM (2012)
15. Ahyar, M., Sari, R.F.: Performance evaluation of multi-channel operation for safety and non-safety application on vehicular ad hoc network IEEE 1609.4. Int. J. Simul.-Syst. Sci. Technol. **14**(1), 16–22 (2013)
16. Amadeo, M. et al.: A WAVE-compliant MAC protocol to support vehicle to infrastructure non-safety applications. In: 2009 IEEE International Conference on Communications Workshops (2009)

Novel Routing Framework for VANET Considering Challenges for Safety Application in City Logistics

Kishwer Abdul Khaliq, Amir Qayyum and Jürgen Pannek

Abstract The Intelligent Transportation System (ITS) addresses issues regarding traffic management and road safety in the domain of Vehicular Ad hoc Networks (VANETs). With the evaluation of new applications, new goals regarding efficiency and security are added for logistics and general user application, which demand time bounded and reliable services. In this paper, we discuss VANET with regards to its suitability in logistics scenarios, challenges to cope with high mobile vehicles and their short contact duration to meet the goal of efficiency. Although VANET helps to provide efficient solutions for logistics and transportation, there are still number of issues to be solved to obtain an appropriate solution. In the context of increasing number of vehicles, high bandwidth requirements for applications, and highly dynamic topology, route optimization and efficient security mechanisms requires special attention. To this regards, a number of routing protocols have been proposed, yet each routing protocol focuses on traditional topological based routing protocols. The selection of the routing methods depends upon the nature of the networks. Number of researchers argued that the most of the routing protocols focus on the particular scenario and consider particular factors for evaluation such as type of network, mobility pattern, and Quality of Service (QoS) requirements for applications. Thus, the performance of the routing protocols depends upon the particular scenario. In this paper, we focus on designing a routing protocol framework, which can provide a reliable and efficient solution for the path selection by considering different factors from application scenarios like logistics and transportation using varying parameters such as speed, number of wireless nodes, traffic loads and bit error rate. Furthermore,

K.A. Khaliq (✉) · J. Pannek
Department of Production Engineering, International Graduate School (IGS),
University of Bremen, Bremen, Germany
e-mail: kai@biba.uni-bremen.de
URL: http://www.dil.biba.uni-bremen.de

J. Pannek
e-mail: pan@biba.uni-bremen.de

A. Qayyum
CoReNeT, Capital University of Science and Technology (CUST), Islamabad, Pakistan
e-mail: aqayyum@ieee.org

A. Laouiti et al. (eds.), *Vehicular Ad-Hoc Networks for Smart Cities*,
Advances in Intelligent Systems and Computing 548,
DOI 10.1007/978-981-10-3503-6_5

we consider channel parameters for the routing protocols to render the communication to be reliable. For proof of concept, we provide and discuss basic simulation results of our proposed framework.

Keywords Routing · IEEE 802.11p · VANET · Safety application · ITS

1 Introduction

Vehicular Adhoc Networks (VANETs) [23] is the type of adhoc network, where vehicles act as a wireless nodes and have the ability to communicate with other vehicles and with the Road Side Units (RSU) wirelessly while in motion. In VANET, wireless nodes can communicate using three modes: Vehicle to vehicle (V2V), Vehicle to Infrastructure (V2I) and Infrastructure to Infrastructure (I2I). Here, infrastructure refers to road side units (RSUs), and higher order backends. It is a key technology in Intelligent Transport Systems (ITS) for achieving new goals such as road safety and efficiency [45]. It can be considered as spin-off of Mobile Ad hoc Networks (MANETs), but it differs in terms of path predictability and speed of nodes.

VANET mainly deals with driver safety applications, traffic management and non-safety applications such as commercial and infotainment applications. Safety messages are usually small in size. While developed for the latter, the next generation ITS adds the use of bandwidth hungry applications, which require less delay and high bandwidth [3]. Considering higher rate of road accidents and traffic congestion due to mismanagement of traffic, the safety applications requirement are of highest priority for many transportation companies and specially for logistics. City logistics efficiency and safety requirements are at high priority due to high demand of products and home delivery services with secure communication [41]. The requirement of these services are depicted in Fig. 1, where on time flow of goods is the key for efficiency [27]. Furthermore, requiring highly optimized routes, infotainment and lookup services are at user's top list.

Adhoc network are not only attractive because of ease, low cost and fast deployment but also because of their design. The concept of noncentralized design make it robust, self control and self organized. Though forming of network "on the fly" is attractive, the challenges to design, optimize and analyze are formidable. Moreover, with the deployment of infrastructure, mobility and flexibility, these networks have transformed into hybrid architectures, which require resource utilization and intelligence for efficiency. Never the less, the increased mobility in VANET, though it is in organized fashion, has posed challenges to the existing MAC and routing mechanisms. The involvement of highly mobile, static and mixed node deployment pattern and requirement of Quality of services (QoS) [37] have made it more complex. In addition to it, the emergence of a wide variety of new applications e.g. emergency handling services, car parking, infotainment, theft detection, safety on road, navigation, law enforcement, fleet management and health care assistance also requires efficiency and flexibility of the deployed network.

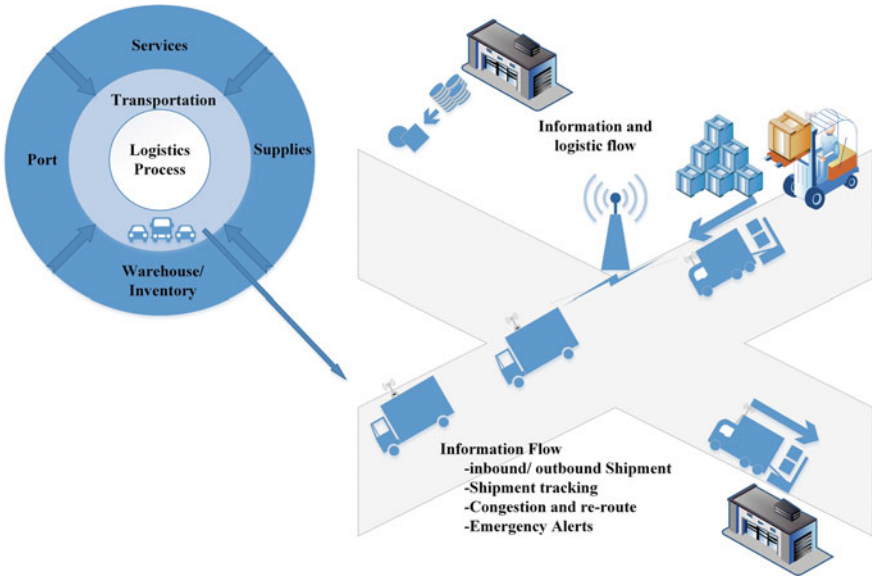


Fig. 1 Vehicular Adhoc Networks (VANET) in logistics scenario

To achieve the goal of an efficient, flexible and self organized network, the research community targets three kind of approaches. First, efficient MAC mechanisms ensure the maximal utilization of physical resources, and provide information to upper layers for QoS provisioning. Second, the efficient routing strategies find a best route between source and destination, and recover a route in case of link failure. Third, the design of efficient applications to achieve respective goals. Performance of the third depends upon the first two approaches. The MAC and routing mechanisms are not simple to define for all scenarios. In city, highway and rural area, adhoc networks face different types of challenges. In city environments, obstacles like buildings, trees, etc. and greater number of nodes cause communication loss and congestion issues. In highway scenarios, vehicles are moving with high speed, which cause link breakage and formation of new links due to change of neighboring nodes. Considering multiple scenarios reveals a broad variation in behavior of the wireless network. Therefore, routing strategies differ for respective scenarios and parameters from the physical layer can help for the best path selection. Hence, we consider properties of both layers to gather real time traffic information for path selection and optimization.

2 Literature Review

To expolite the features of MAC protocols and extract parameters for designing a new routing mechanism, the survey on MAC protocols is summarized in Table 1, which indicates the limitations of 802.11p MAC for some application scenarios, most specifically for delay sensitive and bandwidth hungry applications. The authors in

Table 1 IEEE 802.11p MAC protocols, addressed problems and limitations

Protocols	Addressed problems	Limitations
TDMA [10]	Channel access delays; Real time applications	No suitable for high mobility; Complex algorithm; Lacks a realistic mobility model; Limited throughput
W-HCF [5]	Guaranteed bandwidth and access delay for infotainment applications	Processing delays are involved for QoS management; Centralized approach; Not suitable for bandwidth hungry applications
ABS Scheme [40]	Chance of contention; Affecting throughput	Important CCH messages (emergency messages) can be missed; Not suitable for bandwidth hungry applications
Extended SCH intervals [42]	Improving channel utilization through SCH	Only suitable if vehicles avoid to listen CCH
CDS [43]	Backoff window size	Not realistic due to unknown number of high speed vehicles in a range
CBMAC [19]	Hidden node problem; High density of node	Lacks a realistic mobility model; Edge nodes of clusters cause confusions; Not suitable for bandwidth hungry applications
SDM [11]	TDMA based scheme for guaranteed channel access	Unused time slots issues
Distributed Scheme [46]	Distributed TDMA with two hop neighbors	Introduced latency when joining two groups
802.11p MAC [31]	High density scenarios for throughput degradation and increase delays	Ignored the speed of vehicles; Not suitable for bandwidth hungry applications

[25] evaluated Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) for real time applications through simulations. Their results show that under heavy traffic loads the performance deteriorates, both for individual nodes and for the whole network due to CSMA. To solve this issue, the authors proposed STDMA (Self-organizing Time Division Multiple Access) and evaluated it for VANET. The simulation showed that STDMA performs well in VANET for real time applications. Unfortunately, the authors did not discuss the causes of packet drop in CSMA/CA, which needs to be analyzed in detail. The designed algorithm is too complex and not suitable for highly mobile nodes.

In [5], the authors targeted Infotainment applications and showed through simulations that performance of bandwidth hungry applications suffers due contention based MAC scheme and delay generated due channel switching. To work on this

issue, the proposed extension is called W-HCF (WAVE-based Hybrid Coordination Function) and it provides controlled channel access on top of the contention base channel access and achieved better results. The results did not mention the overheads involved in W-HCF. However, the proposed method in [5] is centralized, introduces processing delays for the handling of QoS managements and also it offers limited bandwidth only. The authors in [40] addressed the chance of contention to increase throughput, but the resulting bandwidth was not enough for multimedia applications. Due to channel switching and channel contention, the probability of loss of emergency messages is also greater. The authors in [42] focused on SCH to improve channel utilization, but scheme failed for the CCH messages. In [43], the authors focused on the evaluation of 802.11p for V2I communication and showed via simulations that backoff window sizes are not adaptive and cause throughput degradation, particularly in dense scenarios. They proposed two solutions i.e. centralized and distributed to render the back-off window sizes adaptive. Simulations showed that both approaches improve the throughput. To solve the hidden node problem, the authors in [19] proposed a mechanism but the evaluation lacks a realistic mobility model and is not suitable for interactive applications. To give opportunity of channel access for each node in VANET, TDMA based protocols SDM [11] and Distributed Scheme [46] were proposed. As there are limited time slots, these can accommodate limited number of nodes, in some cases channel is not fully utilized. IEEE proposed 802.11p MAC and the authors in [31] focused on the high density scenarios, but they ignored speed of vehicles.

In [2], the authors proposed an enhancement in 802.11p for multimedia and delay sensitive applications, which is called Vehicular MAC Protocol Data Unit (V-MPDU) to improve the channel access efficiency. In [4], the authors evaluate the Rician and Rayleigh fading for vehicular environment and proposed suitable parameters that can help to reduce fading effects. In [26], the authors discussed the evaluation of IEEE 802.11p with IEEE 802.11n and IEEE 802.11ac and concluded that 802.11n and 802.11ac perform comparatively well for delay sensitive and bandwidth hungry applications in urban environment with limited speed. However, latest standards include frame aggregation, reverse direction algorithm and MIMO techniques to improve throughput, but can only support limited mobility and transmission range.

The performance of the adhoc network mainly depends upon the successful packet transmission to the destine node through intermediate nodes using best available path. The research shows that VANET routing protocols focused on traditional topological based routing protocols and depends upon the nature of the networks. A number of factors affect on the routing strategies like type of networks, mobility patterns, QoS requirements for different applications. Thus, a single routing method is not sufficient to meet all the different types of required scenarios. Different adhoc routing protocols proposed for the different scenarios, and were analyzed to figure out which routing metrics are considered to provide *in time* and *scalable* routing. Most researchers focused on single environment of VANET, i.e., either on highway or a city, to evaluate the performance of different routing protocols. Due to aforementioned problems there is continuous need to study various adhoc routing methods in order to select appropriate method for different environments of VANET. Routing metrics are the

basis of any routing protocol on which it selects a best path. Here, we summarize different metrics against different types, approach used for path selection, and route update mechanisms of routing protocol in Table 2.

Link life is one of the important routing metrics, as longer link life shows good link quality. Since link quality is measured on the demand of the path, this routing metrics is mostly used for reactive and flow-based scenarios [17, 30]. *Node hight* is another routing metrics, which is useful in scenarios with low mobility. Therefore, proactive protocols [33] and also flow-based protocols [17] use this metric in similar context, but with some limited benefits. Reactive protocols like Temporally-Ordered Routing Algorithm (TORA) [33] and Dynamic MANET On-demand (DYMO) [13] and proactive protocols including Dynamic Source Routing (DSR) [24], Better Approach to Mobile Ad hoc Networking (BATMAN) [1], Hierarchical State Routing (HSR) [35], Intrazone Routing Protocol (IARP) [20], Mobile Mesh Routing Protocol (MMRP) [18], Optimized Link State Routing (OLSR) [16], Optimized Link State Routing Version 2 (OLSRv2) [32], Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) [8] and Link Quality Source Routing (LQSR) [12], both types of routing protocols use *Hop Count* for the path selection, and route update is only required when it is timed out. In some scenarios, the same metric is also used where these two type of protocols are used as hybrid form, e.g., Hazy Sighted Link State Routing (HSLS) [39]. However, with the involvement of high mobility using only this metric is not enough to find a good path and may also introduce delays for larger networks. To resolve this problem, some protocols are proposed which are cluster-based. Each cluster must have a cluster head and these *Cluster Heads* take part in routing. Then *Hop Count* routing metric is used on cluster heads for the route selection. These protocols [14, 29, 34] also apply for route update on time-out. *Expected Transmission count (Expected Tx Count)* is a routing metric which is used by proactive routing protocols [22] for route selection. This routing metric count is good only for specific applications.

Proactive routing protocols build an priory table for routing path. Therefore, *Link Cost* is also a routing metric, and protocols [6, 36] use this metric to calculate the total cost of the path. The minimum cost count use for the best path selection. However, with frequent link breakage, the calculation of link cost introduces delays. Some Hybrid protocols also use *Link Cost* and *Virtual Link Predecessor* for route calculation. Table 2 summarized this analysis with the additional information of each protocol and their corresponding approach used for metric calculation.

As VANET involves the wireless communication of vehicles in adhoc mode, it consists of multiple participants including roads, Road Side Units (RSU) and On-board Units (OBU), mobile nodes (Vehicles), and taffic signals. Networks constraints exist when dealing with safety applications. As safety applications require small but frequent data packets to circulate in the network, network constraints exist. Table 3 includes some of these constraints for safety applications in VANET.

Table 2 Routing protocols comparison on the basis of selected parameter

Metric	Type	Protocols	Approach	Route Update
Link life	Reactive	LBR [30]	Signal strength	Link break
	Flow	LMR [17]	Directed acyclic graph and link reversal	
Node height	Reactive	TORA [33, 44]	Directed acyclic graph	Link break
	Flow	GB [9]	Directed acyclic graph and link reversal	Automated flow and link break
Hop count	Reactive	AODV [38]	Distance vector (DV)	Timed
	Reactive	DYMO [13]	Distance vector	Timed
	Proactive	DSR [24]	Distance vector	Timed
	Proactive	BATMAN [1]	DV and collective intelligence	Timed
	Proactive	HSR [35]	Hierarchical routing & cluster-head	Timed
	Proactive	IARP [20]	Link state (LS) and zone radius	Timed
	Proactive	MMRP [18]	Link state and sequence number	Timed
	Proactive	OLSR [16]	LS and multi point relay	Timed
	Proactive	OLSRv2 [32]	LS and multi point relay	Timed
	Proactive	TBRPF [8]	Link state with differential data	Timed
	Proactive	LQSR [12]	Weighted cumulative expected Tx time	Timed
	Hybrid	HSLS [39]	Link state timed and link break	Timed
Cluster-head/ hop count	Proactive	Guesswork [34]	Distance vector and cluster head	Timed
		DFR [29]	GPS and cluster head	
		CGSR [14]	DV and cluster head	Timed
Expected Tx count	Proactive	AWDS [22]	Link state	Timed
		Babel [15]	Distance vector	

(continued)

Table 2 (continued)

Metric	Type	Protocols	Approach	Route Update
Link cost	Proactive	DBF [6]	Bellman ford	Timed
		DSDV [36]	Bellman ford and sequence number	Timed
		WRP	Bellman ford	
	Hybrid	OORP [21]	Hierarchical routing and cluster head	Timed and link break
Virtual link predecessor	Hybrid	SSR [28]	Source routing and virtual ring routing	Timed and link break
Not specified	Hybrid	ZRP [7]	Zoning	Timed and link break

Table 3 Network constraints for safety applications

Constraint Type	Constraints Value
Aggregation bandwidth	6 Mbps
Maximum received packets/sec	4000
Maximum allowable latency	100 ms
Maximum packet size	200 bytes
Transmission channel for safety	CCH
Maximum tolerated delay (between two packets)	300 ms
Minimum delay	50 ms
Channel switching time (between CCH and SCH)	50 ms

3 Proposed Framework

Considering the literature review and evaluation of VANET in different scenarios, we selected some parameter to be considered for the path selection. The proposed solution approach is discussed in Sect. 3.

In VANET, the channel condition information is varied in different scenarios and can be very helpful for decision making for routing. If we consider quality channel parameter as a routing metric, then the results will be very different than for traditional routing protocols. We analyzed MAC and routing protocols, and identified their suitable scenarios. From our literature review, we concluded that a number of routing protocols are proposed which consider one or more routing metrics. These protocols are proposed for specific scenarios and metrics were chosen with respect to the selected scenario. Some information about channel quality can be helpful for the path selection, e.g., channel fading or Signal to Noise Ratio (SNR). Therefore, merging this information can help to improve the route selection. As routing protocols

are at the network layer and we have channel information at MAC layer, we also require a method for the flow of information from Physical Layer to Network Layer. As we can get most recent information at the MAC layer easily, and if we introduce routing mechanism at MAC layer, we can use the required information without any delay. Path selection at MAC layer can help to simplify and improve path selection on the basis of local available information. So there is need to make a link layer routing protocol for VANET. The performance of this method depends heavily on the value of the decision threshold. Yet, it is difficult to choose a value that results in good performance across all scenarios. Node density, spatial distribution pattern, and wireless channel quality all affect the optimal value. Broadcast protocols tailored to vehicular networking must be adaptive to variations in these factors. In this work, we address this design challenge by creating a decision threshold function that is adaptive regarding the number of neighbors and their speed. The proposed protocol is implemented on the Layer 2 (MAC Layer) considering SINR and rate of delivery. Based on our literature survey, we decided to consider channel quality parameters to get our initial result analysis.

We assume that the wireless channel and the medium access control protocol deliver messages between nodes located within transmission range of each other with perfect reliability. In practice, wireless signals in the system interfere with themselves and with each other in unpredictable ways, leading to apparently non-deterministic message reception. When two nodes transmit messages at the same time, the wireless signals may interfere and cause one or both of the messages to be lost at the destination node. *Fading*, the phenomenon where multiple parts of the same signal traveling along different paths interfere with each other, degrades communications even when only a single node is transmitting. Multihop wireless broadcast protocols must be abled to operate effectively even when communication reliability is poor. The *threshold function*is designed to decide about the good and bad path for routing on the basis of channel conditions. The paths with values lower than the threshold is discarded. Threshold function also included channel level metrics like SINR, packet retry rate, percentage availability of channel for measuring quality of channel Fig. 2.

The proposed framework includes four type of circulating massage format for path calculation i.e. path request (PREQ), path reply (PREP), Path Error (PERR) and path reply acknowledgement (PREP-ACK). The participating node may include three types of messages to take a decision. Figure 3 shows three decision points of the participating node. This routing protocol is working on the MAC layer, therefore, for the first proof of concept we consider MAC parameters for the path selection as discussed in the previous paragraph.

We divided protocol mechanism into two steps as it is shown in Fig. 2. In first step, we used two algorithms to compute *SINR* value and *delivery rate* (if previous link exists) of direct links and maintained table for each link. These values are computed periodically. In second step, routing algorithm identify best path on the basis of values available in the table. When a node initiates or receives a PREQ, it checks value in the tables and selects best one on the basis of available information. If node has no delivery history about a new link, it only considers SINR value to forward PREQ. If

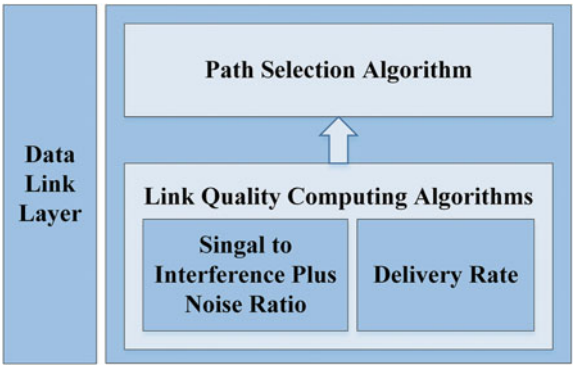


Fig. 2 Proposed routing framework

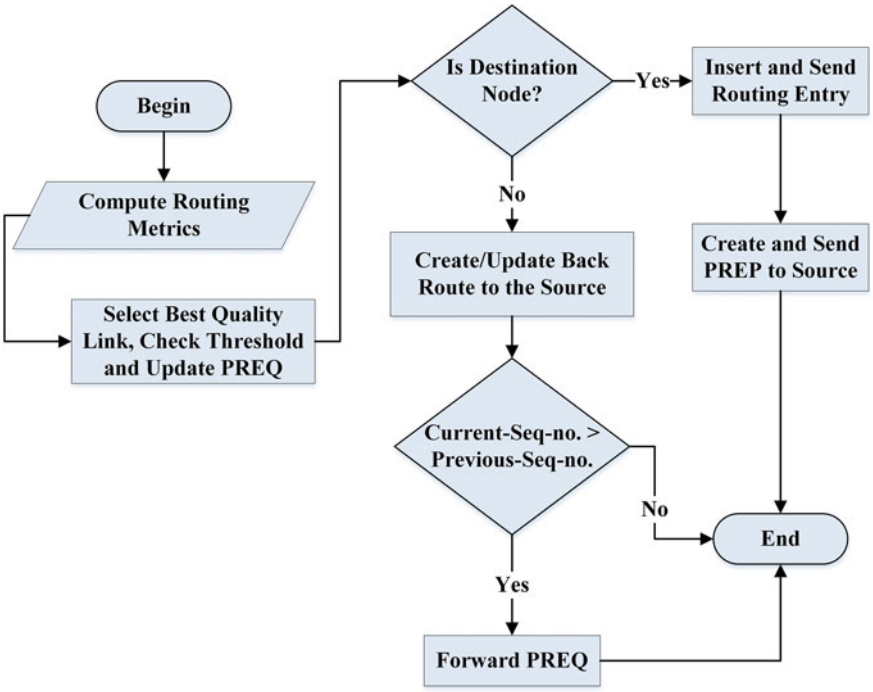


Fig. 3 Flow chart of proposed routing protocol

PREQ receiving node is a destination node, it inserts route and sends routing entry to source node using PREP. In case of intermediate node, it only creates and updates back route to the source and forwards PREQ, however, the latest copy is checked using usual procedure, i.e. sequence number. If flag is set for the reply to previous

node, then PREP-ACK is used to send reply back. PERR is used to send path error to the source node.

4 Simulation Setup and Basic Results

To analyze our problem, we used simulation implemented in Omnet++. We used *Vehicles in Network Simulation (veins)* framework, which includes a number of simulation models for VANET and used SUMO for simulation mobility pattern. This framework is open source and allows to write and test our own model and provides rich support of VANET MAC layer options like IEEE 802.11p and it also supports various routing protocols for ad-hoc networks like proactive, reactive and geographical protocols. We implemented our proposed protocol and tested it for the basic results, i.e. goodput and delay.

The proposed framework is designed considering challenges for the city, highway and rural areas. However, this paper only includes scenario of city logistic to analyze initial results for goodput and delay. For city logistic scenarios, Table 4 includes the parameter setting. The considered parameters include the environment size, total number of nodes, type and speed, packet size and type and considered simulation time. In such a scenario, where vehicles may responsible for transporting material for production unit to prepare product or delivering products from production unit to the distributors, retailers and warehouse. Consider an application, which is responsible for managing safety guideline and information flow for this particular scenario. A vehicle is performing a specific task and on each movement information is sent back to control room. Here, we are dealing only in city scenario where we considered constraints of safety application listed in Table 3 and changed speed of vehicles while moving sparse to dense network. For the comparative analysis, we selected

Table 4 Parameter setting for city scenario

Parameter	Setting
Environmental size	2000 m
Total no. of nodes	60 (variation of 10, 20, 30, 40, 50, 60)
Node type	Mobile nodes (vehicles)
Node speed	Maximum 50 Kmph and minimum 30 Kmph
Packet size	200 bytes for safety applications
Packet type	UDP
Simulation time	600 s
Number of receiver	1
No. of lanes	3
RSU	10
Traffic signals	4 in each cross

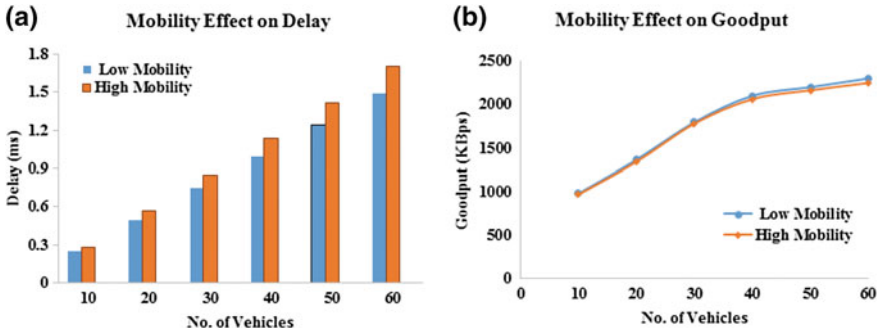


Fig. 4 **a** Effect of mobility on delay; **b** Effect of mobility on goodput

node density and speed of vehicle in urban areas and for the comparison we calculated goodput and packet delay.

For evaluation, we examined the effect on the goodput and delay at low and high mobility. Constant-bit Rate (CBR) traffic flows were used in the simulation with packet size of 200 KB, which was kept constant. We imposed two other CBR flows of 500 Kbps, which acted as background traffic. Total 60 nodes were used in the scenario, which were moving at 50 km/h maximum speed and 30 km/h minimum speed. Results are shown in Fig. 4a and b. We observe that the goodput increases with the increase in number of vehicles in the network. A constant goodput is observed for safety packets with increase in number of nodes, and when we increase the speed of vehicles, the goodput remains same as it was observed at low speed due to link quality consideration for path selection at run time. As we mentioned, we considered only safety applications and the packet size in safety applications are small. Therefore, the graph shows a constant line for small packets with increased number of vehicles. In case of delay, with increase in number of vehicles, the increase in delay is negligible.

5 Conclusion and Future Work

The Intelligent Transportation Systems (ITS) address issues regarding traffic management and road safety in Vehicular environment. VANET is the one of the enabling technology in ITS used for road safety, traffic management and logistics applications. It can also be deployed in the logistics and transportation to cope challenges of information flow with mobility of materials. With increase in number of vehicles, speed and the requirements of high bandwidth for new applications, VANET requires special attention for route optimization and security provisioning. In our work, we focused to improve routing mechanisms to tackle challenges in vehicular environment for reliable communication. Literature showed that VANET routing protocols focused on traditional topological based routing. The selection of these routing methods depends upon the nature of the networks and most focus on the

particular scenario. Thus, a single routing method is not sufficient enough in meeting all the different types of required scenarios. In this work, we rapted on designing a routing protocol, which can provide a reliable and efficient solution for the path selection. In our work, we analyzed different adhoc routing protocols proposed for the different scenarios to figure out suitable routing metrics in each case. We also designed a basic framework to cope new application requirements. However, we only included basic results for city logistics scenario considering mobility. We are focusing on designing a routing protocol considering MAC and network layer parameters to cope with challenges in multiple scenarios. We will extend this model for other scenarios with particular parameters to make it adaptive in different scenarios.

References

1. Aichele, C., Lindner, M., Neumann, S.W.A.: Better approach to mobile ad-hoc networking (batman). In: IETF Work In Progress Internet-Draft (2008)
2. Akbar, M.S., Khaliq, K.A., Qayyum, A.: Vehicular mac protocol data unit (v-mpdu): Ieee 802.11p mac protocol extension to support bandwidth hungry applications. In: Springer Vehicular Ad-hoc Networks for Smart Cities, pp. 31–39 (2015)
3. Akbar, M.S., Khan, M.S., Khaliq, K.A., Qayyum, A., Yousaf, M.: Evaluation of ieee 802.11n for multimedia application in vanet. Proced. Comput. Sci. **32**, 953–958 (2014). Elsevier
4. Akbar, M.S., Qayyum, A., Khaliq, K.A.: Information delivery improvement for safety applications in VANET by minimizing rayleigh and rician fading effect. Vehicular Ad-hoc Networks for Smart Cities, pp. 85–92. Springer, New York (2015)
5. Amadeo, M., Campolo, C., Molinaro, A.: Enhancing IEEE 802.11p/WAVE to provide infotainment applications in VANETs. Ad Hoc Netw. **10**(2), 253–269 (2012)
6. Awerbuch, B., Bar-Noy, A., Gopal, M.: Approximate distributed Bellman-ford algorithms. IEEE Trans. Commun. **42**(8), 2515–2517 (1994)
7. Beijar, N.: Networking laboratory. Zone Routing Protocol (ZRP). Helsinki University of Technology, Finland (2002)
8. Bellur, B., Ogier, R., Temlin, F.: Topology dissemination based on reverse-path forwarding (TBRPF). Technical Report, IETF Internet Draft, manet-tbrpf-08 (2003)
9. Bertsekas, D., Gallager, R.: Data Networks. Prentice-Hall, New Jersey (1987)
10. Bilstrup, K., Uhlemann, E., Strom, E.G., Bilstrup, U.: Evaluation of the IEEE 802.11p MAC method for vehicle-to-vehicle communication. In: IEEE 68th Vehicular Technology Conference, pp. 1–5 (2008)
11. Blum, J.J., Eskandarian, A.: A reliable link-layer protocol for robust and scalable intervehicle communications. IEEE Trans. Intell. Transp. Syst. **8**(1), 4–13 (2007)
12. Campista, M.E.M., Esposito, P.M., Moraes, I.M., Costa, L.H.M., Duarte, O.C., Passos, D.G., De Albuquerque, C.V.N., Saade, D.C.M., Rubinstein, M.G.: Routing metrics and protocols for wireless mesh networks. IEEE Netw. **22**(1), 6–12 (2008)
13. Chakeres, I.D., Perkins, C.E.: Dynamic MANET On-demand routing protocol. Technical Report, IETF Internet Draft, MANET-dymo-12 (2008)
14. Chiang, C.C., Wu, H.K., Liu, W., Gerla, M.: Routing in clustered multihop, mobile wireless networks with fading channel. In: Proceedings of IEEE SICON, vol. 97, pp. 197–211 (1997)
15. Chroboczek, J.: The babel routing protocol (00042011)
16. Clausen, T., Jacquet, P.: Optimized link state routing protocol (OLSR). Technical Report (2003)
17. Corson, M.S., Ephremides, A.: A distributed routing algorithm for mobile wireless networks. Wireless Networks, vol. 1, pp. 61–81. Springer, New York (1995)

18. Grace, K.: Mobile mesh routing protocol. In: IETF MANET Working Group, draftgrace-manet-mmrp-00 in Progress (2000)
19. Gunter, Y., Wiegel, B., Grossmann, H.P.: Cluster-based medium access scheme for VANETs. In: IEEE Intelligent Transportation Systems Conference(ITSC 2007), pp. 343–348 (2007)
20. Haas, Z.J., Pearlman, M.R., Samar, P.: The interzone routing protocol (IERP) for adhoc networks. In: IETF MANET Working Group, manetzone-ierp-01 (2001)
21. He, G.: Destination-sequenced distance vector (DSDV) protocol. Networking Laboratory, pp. 1–9. Helsinki University of Technology, Finland (2002)
22. Herms, A., Lukas, G.: Awds (ad-hoc wireless distribution service)
23. IEEE Standards Association and others: 802.11 P-2010-IEEE Standard for Information Technologylocal and Metropolitan Area Networksspecific Requirementspart 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments. http://standards.ieee.org/findstds/standard/802.11p-2010.html
24. Johnson, D.B.: the dynamic source routing protocol for mobile adhoc networks. In: IETF Internet-Draft, MANET-dsr-09 (2003)
25. Katrin, B., Uhlemann, E., Store, E., Bilstrup, U.: On the ability of the 802.11p MAC method and STDMA to support real-time vehicle-to-vehicle communication. EURASIP J. Wirel. Commun. Netw. **2009**(5) (2008)
26. Khaliq, K.A., Akbar, M.S., Qayyum, A., Pannek, J.: Suitability of IEEE 802.11ac/n/p for bandwidth hungry and infotainment applications for cities. In: Proceeding of IEEE SAI Intelligent Systems Conference 2016 (IntelliSys 2016), pp. 499–507 (2016)
27. Khaliq, K.A., Pannek, J., Qayyum, A.: Methodology for development of logistics information and safety system using VANET. Lecture Notes on Logistics. In: Proceedings of the 5th International Conference on Dynamics in Logistics (LDIC), pp. 173–182. Springer, Heidelberg (2016)
28. Kutzner, K., Wallenta, C., Fuhrmann, T.: Securing the scalable source routing protocol. In: Proceedings of the World Telecommunications Congress, vol. 13. Budapest, Hungary (2006)
29. Lee, Y.Z., Gerla, M., Chen, J., Caruso, B.: DFR (direction forward routing). Adhoc Sensor Wireless Networks **2**(2), 01–18 (2006)
30. Manoj, B., Ananthapadmanabha, R., Murthy, C.: Link life based routing protocol for adhoc wireless networks. In: Proceedings of IEEE Tenth International Conference on Computer Communications and Networks (2001), pp. 573–576 (2001)
31. Murray, T., Cojocari, M., Fu, H.: Measuring the performance of IEEE 802.11p using ns-2 simulator for vehicular networks. In: IEEE International Conference on Electro/Information Technology, pp. 498–503 (2008)
32. Owada, Y., Maeno, T., Imai, H., Mase, K.: Olsrv2 implementation and performance evaluation with link layer feedback. In: Proceedings of the 2007 International Conference on Wireless Communications and Mobile Computing, pp. 67–72. ACM (2007)
33. Park, V., Corson, M.S.: Temporally-ordered routing algorithm (TORA) version 1 functional specification. Technical Report, IETF Internet-Draft, MANET-TORA-Specification-00 (1997)
34. Parker, T., Langendoen, K.: Guesswork: Robust routing in an uncertain world. In: IEEE International Conference on Mobile Adhoc and Sensor Systems Conference (2005), p. 9 (2005)
35. Pei, G., Gerla, M., Hong, X., Chiang, C.C.: A wireless hierarchical routing protocol with group mobility. In: IEEE Wireless Communications and Networking Conference (IEEE WCNC 1999), pp. 1538–1542 (1999)
36. Perkins, C.E., Bhagwat, P.: Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM SIGCOMM Comput. Commun. Rev. **24**, 234–244 (1994)
37. Rizzo, G., Palattella, M.R., Braun, T., Engel, T.: Content and context aware strategies for QoS support in VANETs. In: IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), pp. 717–723 (2016)
38. Royer, E.M., Perkins, C.E.: Multicast operation of the ad-hoc on-demand distance vector routing protocol. In: Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 207–218 (1999)

39. Santivanez, C., Ramanathan, R.: Hazy Sighted Link State Routing Protocol (HSLS). Technical Report, BBN Technical Memorandum (2001)
40. Sheu, S.T., Cheng, Y.C., Hsieh, P.J., Wu, J.S.: Agent-based scheduling scheme for IEEE 802.11p wireless vehicular networks. In: IEEE 73rd Vehicular Technology Conference (VTC Spring), pp. 1–5 (2011)
41. Siddiqui, N.R., Kishwer Abdul, K., Pannek, J.: VANET security analysis on the basis of attacks in authentication. Lecture Notes on Logistics. In: Proceedings of the 5th International Conference on Dynamics in Logistics (LDIC) pp. 463–473. Springer, Heidelberg (2016)
42. Wang, C.Y., Wei, H.Y.: IEEE 802.11n MAC enhancement and performance evaluation. Mob. Netw. Appl. **14**(6), 760–771 (2009). Springer
43. Wang, Y., Ahmed, A., Krishnamachari, B., Psounis, K.: IEEE 802.11p performance evaluation and protocol enhancement. In: ICVES 2008 IEEE International Conference on Vehicular Electronics and Safety, pp. 317–322 (2008)
44. Yang, S.A., Baras, J.S.: TORA, verification, proofs and model checking. In: Adhoc and Wireless Networks Modeling and Optimization in Mobile (WiOpt 2003), p. 2 (2003)
45. Yin, J., ElBatt, T., Yeung, G., Ryu, B., Habermas, S., Krishnan, H., Talty, T.: Performance evaluation of safety applications over DSRC vehicular adhoc networks. In: ACM Proceedings of the 1st ACM International Workshop on Vehicular Adhoc Networks, pp. 1–9 (2004)
46. Yu, F., Biswas, S.: Self-configuring TDMA protocols for enhancing vehicle safety with DSRC based vehicle-to-vehicle communications. IEEE J. Sel. Areas Commun. **25**(8), 1526–1537 (2007)

Part II
Vanet Security Track

Security Risk Analysis of a Trust Model for Secure Group Leader-Based Communication in VANET

Hamssa Hasrouny, Carole Bassil, Abed Ellatif Samhat and Anis Laouiti

Abstract In this paper, we consider a Trust Model with Group Leader (GL)-based communication in VANET. This model is used to classify vehicles based on their trustworthiness and elect potential GLs. We propose a security risk assessment methodology and we apply it to our Trust Model. This methodology is used for identifying threats, assessing the risk involved, and defining approaches to mitigate them. The risk assessment includes assessment of the impact and likelihood of occurrence of attacks relevant to the identified threats, evaluation of the Trust Model design principles, validation of the built-in security, and the mitigation actions of attacks. Based on this assessment, we demonstrated the resiliency of the Trust Model to resist to many security attacks.

Keywords Risk assessment · VANET · Security · Trust · Risks

1 Introduction

VANET (vehicular ad hoc network) is a special class of mobile ad hoc networks with predefined routes. It consists of vehicles and an infrastructure. The infrastructure includes fixed RSUs (road-side units) and specific authorities for registration and

H. Hasrouny (✉) · A. Laouiti
SAMOVAR, Télécom SudParis, CNRS, Université Paris-Saclay,
9 rue Charles Fourier, 91011 Evry, France
e-mail: hamssa.hasrouny@telecom-sudparis.eu

A. Laouiti
e-mail: anis.laouiti@telecom-sudparis.eu

C. Bassil
Faculty of Science II, Lebanese University, Fanar Campus, Fanar, Lebanon
e-mail: cbassil@ul.edu.lb

H. Hasrouny · A.E. Samhat
Faculty of Engineering-CRSI, Lebanese University, Hadath Campus, Hadath, Lebanon
e-mail: samhat@ul.edu.lb

A. Laouiti et al. (eds.), *Vehicular Ad-Hoc Networks for Smart Cities*,
Advances in Intelligent Systems and Computing 548,
DOI 10.1007/978-981-10-3503-6_6

management. Vehicles with OBUs (online board units) are communicating via DSRC (dedicated short-range communication) [1] together or to the wired infrastructure. Entities are communicating directly in a single hop or multihop to afford better cooperative driving information or alert dissemination. VANET presents great challenges especially in its security due to its wireless communication mode, lack of centralization, and dynamic topology [2]. Although its main benefit is to enhance safety in vehicles by exchanging warning messages between the nodes, VANET suffers from different kinds of attacks [3], such as Sybil, DoS (Denial of Service), message modification, or suppression, injection of erroneous message.

In VANET, existing trust security approaches did not provide yet security controls to properly countermeasures the security attacks within their Trust Models. Therefore, many considerations for protecting VANET against attacks are required using trust metrics values. In newly designed architecture of Trust Models, the ability to control, configure, and combine the security services and mechanisms is the key feature for reducing the impact of security attacks.

Nodes participating in VANET must be trusted and reliable. But due to the abovementioned challenges, it is difficult to identify malicious and misbehaving nodes. Evaluating the trustworthiness of a vehicle in VANET is an open problem. Any defection in the communication and/or messages in VANET endangered people's lives. So what are the criteria that would define the trustworthiness of a node? Is it reliable to count on any node for disseminating critical messages? Then based on these criteria can we detect the misbehavior in vehicle or in the backend?

Many approaches [4–6] follow different Trust Model techniques to establish trust between the vehicles in VANET. Trust establishment approaches can be divided into infrastructure based trust or self-organizing trust. The infrastructure models are based on the certificates provided to vehicles. While the self-organizing models are a combination between direct, indirect, and hybrid trust (cooperation between the vehicles). Both models are based on the message correlation or vehicle verification and provide appropriate trust metrics values to vehicles. Based on these trust metric values, nodes can be classified and a secure and reliable communication is established between them in VANET.

We propose a Trust Model based on NHTSA security architecture [7] with cluster formation [1] and Group Leaders (GLs)-based communication that will be detailed in Sect. 3. The proposed model calculates the trust metrics values of participating nodes. It judges their trustworthiness and reports to misbehavior authority [7] in case of malicious behavior to deactivate the specific malignant node. Trust metrics value is a combination of direct and indirect calculation, centralized and decentralized authorities and in multicases (normal mode or in case of an alert). The node with highest trust metric value is considered the trustiest and will be a potential Group Leader. Using this model is crucial in VANET security, and it helps to classify vehicles, elect GLs, or deactivate others. GLs had crucial roles as they are communicating directly with specific management authorities. In this paper, we investigate the security analysis of this Trust Model and we adopt a methodology of risk assessment based on the SecRAM [8] and the ETSI TVRA (Threat, Vulnerability and Risk Analysis) [9]. This methodology includes assessment of the impact and likelihood of occurrence

of attacks relevant to the identified threats, evaluation of the Trust Model design principles, validation of the built-in security, and the mitigation actions of attacks.

The remainder of the paper is structured as follows: Sect. 2 lists the risk assessment methodologies inspiring for this security analysis. Section 3 briefly explains the Trust Model which is the context for this security analysis. Section 4 specifies the threats. The security risk assessment is described in Sect. 5 in terms of impact, likelihood, and risk level of each threat. Section 6 expands the countermeasures adopted by the Trust Model to mitigate the threats. Finally, the paper concluded in Sect. 7.

2 Risk Assessment Method

The evaluation of the threats adopted in our work is based on SecRAM methodology [8] and ETSI TVRA (threat, vulnerability, and risk analysis) [9]. SecRAM [8] is the ISO 27005-based risk assessment management methodology. It was developed by the SESAR program and was intended first for air traffic management. The assessment covers the following: establish the context and scope and identify the assets related to objectives; find threats, threat scenarios, and their likelihood; evaluate their impact of the loss of security requirements; assess the risk of each threat by combining impact and likelihood; and formulate security control implementation.

ETSI TVRA [9] is analyzing the risk of each threat attacking the ETSI architecture for VANETs. It is used to identify risks to a system by isolating its vulnerabilities, assessing the likelihood of a malicious attack on that vulnerability, and determining the impact that such an attack will have on the system. The TVRA method involves seven steps that are summarized by identify security objectives and security requirements; produce an inventory of system assets; classify system vulnerabilities and threats; quantify the likelihood and impact of attack; determine the risks involved; and specify detailed security requirements (countermeasures).

We therefore tailor both methods to apply specifically to our Trust Model. The evaluation process adheres to the following steps:

- Highlight the system (i.e., Trust Model) assets by identifying the security objectives.
- Expose the system vulnerabilities and threats.
- Security risk assessment: quantify the likelihood and impact of the attacks.
- Countermeasures or security control implementation.

We exposed the steps for the Trust Model security analysis. Now in the next section, we will start presenting the system assets related to this model.

3 Trust Model Assets

In this paper, we provide the security analysis focusing on the Trust Model and its components. We adopted the modular architecture defined by NHTSA (National Highway Traffic Safety Administration) [7] and the group (cluster) formation [1]. The NHTSA architecture is shown in Fig. 1. NHTSA security architecture is based on the PKI (public key infrastructure) and contains functional entities responsible for:

- Management and policies: SCMS (Security Certificate Management System).
- Long-term certificate enrollment for OBUs: Enrollment CA (certificate authority), device configuration manager (DCM), and certification services.
- Short-term digital certificates (pseudonyms) for OBUs: Root CA, Intermediate CA, Linkage authority 1 and 2, Pseudonym CA, registration authority (RA), and request coordinator.
- Misbehavior detection and certificate revocation: Misbehavior authority (MA), Location Obscurer Proxy, CRL (certificate revocation list) store.

This architecture assures privacy against insiders and outsiders: a single SCMS component cannot link any two certificates to the same device (no tracking) and no stored information within SCMS can link certificates to a particular vehicle or owner. MA assures the continuation of the trusted nodes only, by producing/publishing CRL and misbehavior reports in VANET. LOP acts as anonymizer proxy and shuffles

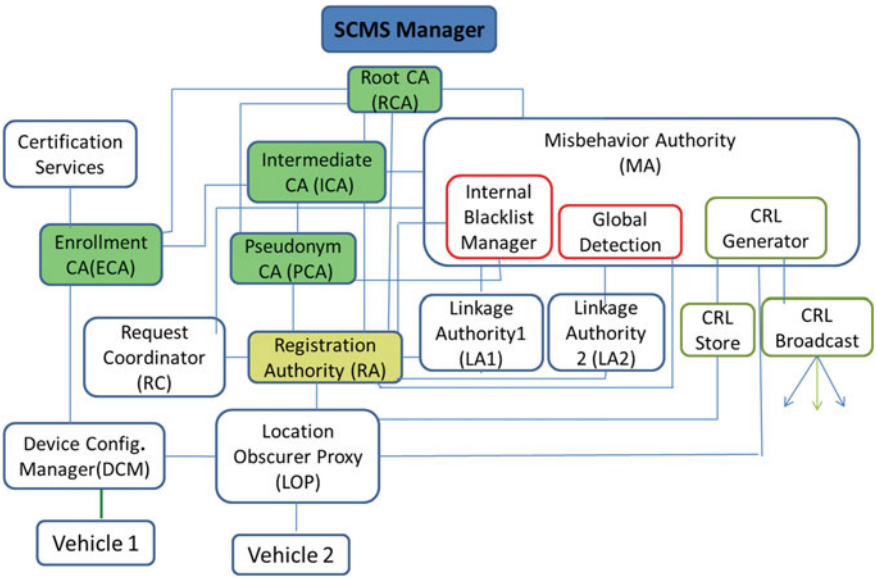


Fig. 1 NHTSA security system design

misbehavior report sent by OBUs to MA. Efficient privacy-preserving revocation exists.

In VANET and especially in V2V communications, the self-organization into groups alleviates the forth and back over the network. It affords a decentralized solution via GLs and minimizes the delays and RSU resources usage due to user verification in case of any message dissemination [1]. Furthermore, the group formation strengthens the security objectives: the anonymity using the public Pu_{gr} and private Pr_{gr} keys of the group for signature; the pseudonym and privacy ensured by those group keys changing frequently offline by the GLs; the confidentiality using the encryption, the integrity, authentication and non-repudiation using the signature.

In the group formation, the Group Leader is the center server for all nodes joining this group: It manages the group formation and generates/distributes the group keys. Thus, the GL should be a trusted node. And if this GL decides to leave the group, the newly elected GL should also be a trusted node. Hence, the need of a robust Trust Model identifies these nodes via trust metrics values. These metrics are based on parameters and cooperation between the vehicles, GLs, RSUs, and misbehavior authority.

The reference model of the Trust Model architecture and its components is briefed in Fig. 2. We built our Trust Model based on the security advantages of the NHTSA architecture and the clustering formation. The proposed Trust Model is composed mainly of two parts: A (Infrastructure) and B (Clustered vehicles). Part 'A' corresponds to NHTSA architecture mentioned in Fig. 1. Its main entities are classified based on their functionalities into four groups. These groups are policing (SCMS Manager), certificate processing, communication with vehicles, and misbehavior detection/revocation. Part B is composed of vehicles communicating with each other, with GLs and infrastructure. Many attackers can compromise the security of the infrastructure, the vehicles, the data exchanged between the vehicles and infrastructure, and the communication between the parties in VANET. In Sects. 4, 5, and 6, the risk analysis of the proposed Trust Model will detail how to resist and mitigate these attacks via the proposed Trust Model.

We propose a hybrid (vehicles' infrastructure) Trust Model which is used to determine the trust metric values of vehicles. It involves a monitoring system processing based on the cooperation of vehicles and the validity of the broadcasted data. We propose a fuzzy system to decide about the honesty of vehicles.

Each vehicle v must monitor all its 1-hop neighbors and calculates their Tm which is called direct trust of v over their neighbors. In VANET, the vehicles broadcast periodically beacons or warning messages to neighbors. So each vehicle v broadcasts its list of calculated direct trust (Tm) to all its neighbors. Then, each vehicle v possesses over a certain neighboring vehicle i, the direct trust v(i) and the direct trust of v's neighbors over i which are called indirect trusts. Note that:

- $Tm_{v(i)}$: « direct trust » judgment of v on i.
- $Tr_{v(i)}$: « indirect trust » judgment of v on i based on v neighborhood opinions.
- $Ttot_{v(i)}$: « total trust » of vehicle i calculated per v (combination of direct and indirect trust).

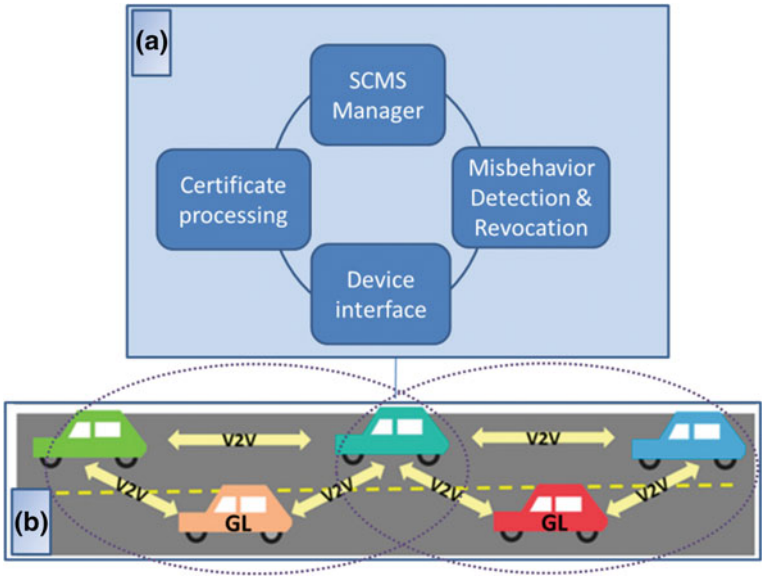


Fig. 2 Trust Model components

- $Tglob_0$ (i): initial « global trust » of vehicle i given by RSU for newly cars entering VANET.
- $Tglob_{(i)}$: « global trust » of vehicle i stored in RSU.

The trust metric in each node includes direct and indirect calculation. Then, a total result is sent to the GL. Finally, passing by the RSU, the GLs will overload all the trust metrics related to nodes. RSU as big data center will merge and update these trust metrics values and result a global trust metric for each node. The trust metric in its different stages at vehicle, GL, or RSU level has a certain threshold: when exceeded, the vehicle is considered trusted; otherwise, a fuzzy-based approach is used to filter out the malicious ones.

A new vehicle i entering the scenario will authenticate to an RSU. It will get its initial global trust from RSU, $Tglob_0(i)$ that will be modified following its behavior on the road, in addition to the certificate obtained from the CA (certificate authority). So it has $P_u i$, $P_r i$, Cert, $Tglob_0(i)$ where $P_u i$ is the public key of vehicle i, $P_r i$ is its private key, Cert is the certificate of vehicle i. The new vehicle will then join an existing group. It will get the public and private keys of this group. The car entering a certain area will broadcast beacons for its neighborhood. Certain parameters related to the communication, transmission, and reception of a vehicle, given by the GPS, sensors or by calculation of the variables are categorized into critical, intermediate, and optional. All these parameters will contribute in the calculation of the trust metrics value.

Each vehicle (including GL—vehicle with the highest confidence score) controls and sends its report directly to the misbehavior authority. We admit this because

sometimes there are some attacks or attackers detected by a certain vehicle and not immediately by the GL. Hence, we proceed by classifying vehicles between honest, intermediate, and malignant ones based on these calculated trust metrics values. Using this Trust Model, privacy is assured by the third party registration within the architecture and the mutual authentication with the RSU, trust is enforced within participants.

We exposed above the Trust Model and its assets; in the next section, we will identify the potential threats that may attack this Trust Model.

4 Vulnerabilities and Threats

The vehicular ad hoc network is exposed to many attacks [3] that mitigate the security objectives. We picked potential attacks that might affect specially the Trust Model and list them in Table 1 with their descriptions and impacts on the Trust Model.

After citing the potential attacks to the Trust Model, the next section will study their impact on the security services and outcome their security risk assessment.

5 Security Risk Assessment

For each identified threat, the impact on the security services such as authentication, availability, confidentiality, integrity, and non-repudiation within the Trust Model is assessed according to the following scale [8]:

- Scale 1: No impact/not applicable;
- Scale 2: Minor - limited impact;
- Scale 3: Sever - performance of Trust Model components is compromised; and
- Scale 4: Critical - performance of the system is compromised.

The impact is valued and assessed according to the degradation or loss of availability (Av), authentication (Au), confidentiality (C), integrity (I), and non-repudiation (Nr) for every threat related to the Trust Model assets. The overall impact is then calculated as the highest of these impacts values of Av, Au, C, I, and Nr.

Then, we estimate the likelihood of each threat to be practically realized and attacking completely the Trust Model according the following scale:

- Scale 1: Very unlikely - practically impossible;
- Scale 2: Unlikely - conceivable but unlikely;
- Scale 3: Likely - only somewhat possible;
- Scale 4: Very Likely - quite possible; and
- Scale 5: Certain - might be well expected.

Table 2 presents the assessed impact and likelihood of each threat. The scoring in this table is subjective, based on a logical analysis and the predefined scales definition

Table 1 Potential attacks on the Trust Model

Threat ID	Threat type	Description
1	Sybil	Create multiple vehicles on the road with same identity. This may affect the reliability of the calculation of the trust metrics values. An unreliable node could be elected as GL. A countermeasure is required
2	DOS	Make the resources and the services unavailable by either jamming the physical channel or 'sleep deprivation.' This threat could disturb the exchange of the trust metrics between the nodes and stop the trust service completely
3	DDOS	DOS from different locations. This threat could disturb the exchange of the trust metrics between the nodes and stop the trust service completely
4	Spamming	Injection of high volume of messages to increase transmission, latency, and bandwidth consumption. This also may disturb and delay the exchange of the trust metrics between the nodes. This leads to an inaccurate calculation of the trust metrics values within the Trust Model
5	Man in the middle (MitM)	Malicious vehicle listens to the communications between two vehicles and pretends to be each of them to reply the other and inject false information between the vehicles. This may impact the decision of the direct and indirect calculations within the Trust Model
6	Message suppression or alteration	Drops packet from the network or changes message content. This also may impact the decision of the direct and indirect trust calculation within the Trust Model. This may leads to confusion within the system
7	Message fabrication	New message is generated due to OBU malfunctioning. This may impact the decision of the direct and indirect trust calculation within the Trust Model. This may leads to confusion within the system
8	Injection of erroneous messages (bogus info)	Cause accidents or traffic redirection This may impact the decision of the direct and indirect trust calculation within the Trust Model. This leads to confusion within the system

(continued)

Table 1 (continued)

Threat ID	Threat type	Description
9	Unauthorized access	Malicious entities access the network services without having the rights and privileges. The trust metrics calculation becomes unreliable due to unauthorized nodes having access to the system for intentional selfish purpose
10	Session hijacking	Try to get cookies from other OBUs. Take control of session between the nodes. This may impact the decision of the direct and indirect trust calculations within the Trust Model. This leads to confusion within the system
11	Cheating with position info (GPS spoofing)	Hidden vehicles generate false positions that cause accidents. This may affect the result of the trust metric values within the Trust Model. The level of trust is compromised
12	Illusion attack	Adversary deceives purposefully the sensors on his car to produce wrong sensor readings. Therefore, incorrect traffic warning messages that include trust metrics are broadcasted to neighbors. Erroneous trust metric values are generated within the Trust Model. Thus, the confidence is compromised
13	Jamming	Interferes with the radio frequencies used by VANET nodes
14	Replay	Replaying old messages. It compromises the direct and indirect trust calculation within the Trust Model
15	Brute force	Attacks to get encrypted data from OBUs. Abuse of indirect trust metrics values transmitted to neighbors
16	Timing	Increasing message processing delay before forwarding. This yields in delayed messages reception by neighboring vehicles. It may delay the exchange of the trust metrics between the nodes. This leads to an inaccurate calculation of the trust metrics values within the Trust Model

above in SecRAM method [8]. For example, if we consider the Sybil attack (Threat ID 1) first row in Table 2, this attack affects only the following security services: availability (Av) and authentication (Au). No impact on confidentiality (C), integrity (I) and non-repudiation (Nr) so the impact scoring for C, I, and Nr is 1 which means

Table 2 Assessed impact and likelihood of each threat

Threat ID	Av	Au	C	I	Nr	Overall impact	Likelihood
1	4	3	1	1	1	4	5
2	4	3	1	1	1	4	5
3	4	3	1	1	1	4	5
4	4	1	1	1	1	4	4
5	3	1	3	3	2	3	3
6	3	2	1	3	2	3	5
7	3	1	1	3	3	3	5
8	3	1	1	2	3	3	5
9	4	3	4	3	3	4	4
10	2	3	3	1	2	3	3
11	3	1	1	1	1	3	3
12	3	1	1	1	1	3	3
13	4	1	1	1	1	4	4
14	1	1	1	3	2	3	4
15	1	1	3	1	3	3	3
16	4	1	1	1	1	4	5

based on SecRAM impact scale above, ‘no impact/not applicable.’ The effect of this attack on the Trust Model availability is critical and affects the trust metric calculation, so its scoring is 4 which mean ‘critical - performance of the system is compromised.’ For the authentication, it affects the performance of the authentication authorities within the Trust Model, its scoring is 3 which means ‘sever - performance of Trust Model components is compromised.’ The overall impact is then calculated as the highest of these impacts values of Av, Au, C, I, and Nr which is 4. For the likelihood of occurrence of Sybil attack is 5 which means based on SecRAM likelihood scale above ‘certain - might be well expected.’

Once the overall impact and the likelihood of each threat of the Trust Model have been assessed, the risk level can be high, medium, or low for each of the identified threats. As an example, a ‘high’ risk level is defined for impact 3 and above and likelihood 4 and above. A ‘medium’ risk level is defined for impact 2 or 3 with likelihood 3 and above. A ‘low’ risk level is defined for impact 1 or 2 and likelihood below than 3. In Table 3, we calculated the risk level of each threat within the Trust Model. For example, the risk level of the Sybil attack (Threat ID 1) is high because its overall impact is 4 and likelihood is 5.

The risk levels of the threats attacking the Trust Model are defined above in Table 3. We move in Sect. 6 to highlight their countermeasures covered by the proposed Trust Model approach.

Table 3 Calculated risk level of each threat

Threat ID	Overall impact	Likelihood	Risk level
1	4	5	High
2	4	5	High
3	4	5	High
4	4	4	High
5	3	3	Medium
6	3	5	High
7	3	5	High
8	3	5	High
9	4	4	High
10	3	3	Medium
11	3	3	Medium
12	3	3	High
13	4	4	High
14	3	4	High
15	3	3	Medium
16	4	5	High

6 Countermeasures—Detailed Security Requirements

Majority of these identified threats are mitigated using security controls. To summarize, Table 4 lists the security controls or countermeasures taken into consideration within the proposed Trust Model.

Table 4 Potential countermeasures to threats in the proposed Trust Model

Threat ID	Threat - description	Risk	Countermeasure
1	Sybil - creates multiple vehicles on road with same identity	High	Using pseudonyms for vehicle authentication within Trust Model. An association between the pseudonyms and license plate is obligatory [10]
2	DOS - make resources and services unavailable	High	Limited number of accepted received messages from neighbor in the proposed Trust Model
3	DDOS - DOS from different locations	High	Using pseudonyms and the limitation of active frequency of sending messages from neighbors
4	Spamming - injection of high volume of messages	High	Control the frequency of sending messages which is a critical factor in the proposed Trust Model
5	MitM - malicious vehicle injects false information between the vehicles	Medium	Detected by MA, using the fuzzy model and based on indirect calculation of neighboring vehicles within the proposed Trust Model

(continued)

Table 4 (continued)

Threat ID	Threat - description	Risk	Countermeasure
6	Message suppression or alteration - Drops packet from the network or changes message content	High	Detected by MA, using the fuzzy model and based on indirect calculation of neighboring vehicles within the proposed Trust Model
7	Message fabrication - new message is generated	High	Detected by MA, using the fuzzy model and based on indirect calculation of neighboring vehicles within the proposed Trust Model
8	Bogus information - cause accidents or traffic redirection	High	Detected by indirect trust calculation with the fuzzy model report to MA
9	Unauthorized access - malicious entities access network services without having rights and privileges	High	Based on the structure of the proposed Trust Model, it can be detected via GL and MA
10	Session hijacking - try to get cookies from other OBUs. Take control of session between the nodes	Medium	Using the digital signature and encryption within the architecture and the clustering, the Trust Model indirectly via the specialized parties will detect the session hijacking compromising the authentication and integrity of the data
11	GPS Spoofing - Hidden vehicles generate false positions that cause accidents	Medium	Malicious are detected by MA via trust score calculation. Transmission power compared to vehicle position is one of the critical factors that participate in trust metric calculation within the proposed Trust Model
12	Illusion attack - deceives purposefully the sensors on his car to produce wrong sensor readings. Incorrect traffic warning messages are broadcasted to neighbors	High	Malicious nodes are detected by MA via trust score calculation. Transmission power compared to vehicle position is one of the critical factors that participate in trust metric calculation within the Trust Model
13	Jamming - interferes with the radio frequencies used by VANET nodes	High	It is based on a hardware solution independent of the proposed Trust Model. It is based on channel switching or either switching between the different wireless technologies
14	Replay - Replaying old messages	High	Use Timestamp within the proposed Trust Model architecture
15	Brute Force attack - attack to get encrypted data or keys from OBU	Medium	In the OBU, keys are finished if hacked as it includes TPD (Tamper Proof Device)
16	Timing attack - adding time slots to packets to create delay	High	Detected from forwarding index which is a critical factor in the proposed Trust Model. This factor that measures the cooperativeness of each node within VANET

7 Conclusion

In this paper, we focused on security risk analysis for the Trust Model. Based on predefined security risk analysis methods, we identified possible threats of the Trust Model components, the risk level, and their countermeasures. Through evaluation of the risks related to the potential identified attacks, we conclude that the Trust Model built on the NHTSA architecture and GL-based communication provides an inherent secure environment that can mitigate the potential attacks or minimize the duration of attacks on the vehicular ad hoc network.

References

1. Hasrouny, H., Bassil, C., Samhat, A.E., Laouiti, A.: Group-based authentication in V2V communications. In: 2015 Fifth International Conference on DICTAP, pp. 173–177. IEEE (2015)
2. Shringar Raw, R., Kumar, M., Singh, N.: Security challenges, issues and their solutions for VANET. Int. J. Network Secur. Appl. (IJNSA) **5**(5), 95 (2013)
3. Hoa La, V., Cavalli, A.: Security attacks and solutions in vehicular ad hoc networks: a survey. Int. J. AdHoc Netw. Syst. (IJANS) **4**(2), 1–20 (2014)
4. Gazdar, T., Benslimane, A., Rachedi, A., Belghith, A.: A trust-based architecture for managing certificates in vehicular adhoc networks. In: International Conference on Communications and Information Technology (ICCIT), pp. 180–185. IEEE, June 2012
5. Yang, N.: A similarity based trust and reputation management framework for VANET. Int. J. Future Gener. Commun. Network. **6**(2), 25 (2013)
6. Patel, N., Jhaveri, R.: Trust based approaches for secure routing in VANET: a survey. Elsevier (2015)
7. Harding, J., Powell, G., Yoon, R., Fikentscher, J., Doyle, Ch., Sade, D., Lukuc, M., Simons, J., Wang, J.: Readiness-of-V2V-Technology-for-Application-812014. US department of transportation, NHTSA National Highway Traffic Safety Application, August 2014
8. SESAR Joint Undertaking, SESAR ATM SecRAM Implementation Guidance material-Project 16.02.03 D03, 2013, SESAR official website: http://www.sesarju.eu/
9. ETSI TR 102 893 V1.1.1-ITS-Security-Threat, Vulnerability and Risk Analysis
10. Zhou, T., Roy Choudhury, R., Ning, P., Chakrabarty, K.: P2DAP – sybil attacks detection in vehicular ad hoc networks. IEEE J. Sel. Areas Commun. **29**(3), 582–594 (2011)

Trust-BZB: Towards a Trust-Driven Routing in Vehicular Networks

Fatma Hrizi, Khalifa Toumi and Anis Laouiti

Abstract Vehicular networks are the building blocks of the intelligent transportation systems (ITS). Several applications are built to provide more safety and efficiency to users of the roads. Particularly, safety applications are the most critical and vital. This kind of application is very challenging as it is highly demanding in terms of reliability and latency. On the other hand, safety-related data should be delivered intact and in a secure manner. Vehicular technologies should therefore provide these requirements for an effective operation of these applications. In this paper, we propose an efficient receiver-based routing protocol that considers on the one hand the dynamicity and the characteristics of the vehicular environment and on the other hand the trustworthiness of the potential relays of safety data in order to secure the dissemination process. Simulations results showed that our trust-BZB reduces the delay of delivery of the information in a non-secure environment.

Keywords Intelligent transportation systems · Vehicular networks · Trust · Routing · Distance-based · Broadcast · Simulation

1 Introduction

Intelligent transportation systems (ITS) have emerged in the last years as they provide new services for users on the roads mainly to enhance safety and promote traffic efficiency. These services could be categorized into three classes, i.e. safety, efficiency and infotainment applications. The most critical application is related to

F. Hrizi (✉) · K. Toumi · A. Laouiti
SAMOVAR, Télécom SudParis, CNRS, Université Paris-Saclay,
9 Rue Charles Fourier, 91011 Evry, France
e-mail: fatma.hrizi@telecom-sudparis.eu

K. Toumi
e-mail: khalifa.toumi@telecom-sudparis.eu

A. Laouiti
e-mail: anis.laouiti@telecom-sudparis.eu

A. Laouiti et al. (eds.), *Vehicular Ad-Hoc Networks for Smart Cities*,
Advances in Intelligent Systems and Computing 548,
DOI 10.1007/978-981-10-3503-6_7

safety and security of drivers; ITS defines several safety-related applications, e.g. collision avoidance, weather and hazardous warning applications.

Vehicular technologies are specifically designed to support ITS applications. In particular, safety applications are very challenging as they are very sensitive to delay and very demanding in terms of reliability in reception. Accordingly, short-range, multi-hop communication and periodic broadcast must be used in order to transmit the safety information reliably and in brief delays. On the other hand, safety applications make use of specific types of messages for an efficient operation. In particular, periodic and event-driven messages are the mostly used ones. Following the European Telecommunications Standards Institute (ETSI) [1], periodic messages conveying location data are called CAMs (Cooperative Awareness Messages). Event-driven information is transmitted by DENMs (Decentralized Environmental Messages).

The challenge here is to efficiently convey the safety-related data taking into account on the one hand the characteristics of vehicular environment and on the other hand the existing threats in this kind of networks.

In this paper, we develop an hybrid receiver-based routing protocol for safety applications. Our routing protocol, namely trust-BZB, is an extension of our previous work in [2]. Trust-BZB is a receiver-based routing scheme that takes into account the dynamic behaviour in the vehicular environment, mostly due to the high mobility and the changing topology. Moreover, trust-BZB considers the trust degree of neighbours in the process of relay selection in order to ensure a secure dissemination of the safety-related information. Simulation studies have been conducted using iTETRIS [3] simulator. The simulation results show that our trust-BZB outperforms BZB when the vehicular environment is not secure, considering a malicious isolation attack. Accordingly, trust-BZB reduces the delay of safety information delivery.

The paper is organized as follows. In Sect. 2, we give an overview of the works done in the field of broadcasting in vehicular networks. Also, we discuss related works in trust-based routing protocols. Section 3 introduces our new routing approach trust-BZB. In Sect. 4, we present simulation results. Finally, in Sect. 5, we provide conclusions and give insights about future works.

2 Related Works

Three main research areas will be discussed in this section: the two main schemes of the multi-hop broadcast approaches (1) sender-based [4, 5] and (2) receiver-based approaches [6–10] and (3) the trust mechanism integration in the routing protocols.

In [4], authors design an adaptive and reliable broadcast scheme. The solution is based on the CSMA/CA channel access mechanism. Each sender defines a receive ACK window that is divided into many adaptive slots proportional to the number of neighbours. The retransmission will be started if any ACK from a neighbour is missing upon expiration of the ACK window. Another sender-based solution is presented in [5]. This approach defines a fully distributed adaptive algorithm. It uses the local position information to decide if it can belong or not to a connected

dominating set (CDS). Cars in a CDS will wait shorter before the retransmission of the message. This first class requires an accurate and up-to-date knowledge of the topology to build the system architecture and to maintain it. This aspect turns out to be not compatible with the highly dynamic vehicular environment and cannot cope with the requirements of traffic safety applications.

Regarding the receiver-based solutions, the broadcast relays autonomously decide whether they must transmit a message or not. Each receiver contends to be a potential relay, the node winning the contention relaying and all other nodes overhearing the relay stopping their contention. This approach, also known as Contention-based Forwarding (CBF) [9], was used with different solutions.

In [7] an analytical model of a receiver-based reliable broadcast approach was proposed. It permits to predict the performance of a packet distribution. Moreover, they propose a generic model that encourages its extension. BPAB (Binary Partition Assisted Broadcasting) [6] is another receiver-based protocol. It aims to reduce the delay of the emergency messages by using a binary partition mechanism to iteratively compose the transmission range into small segments and choose the furthest relay vehicle. Reference [8] presents a routing algorithm, called REAR, based on receipt probability of alarm messages. Each node calculates an estimate reception probability for each of its neighbours based on their position and their environment exchanged via beaconing. This solution is probabilistic-based dissemination, which means the decision of transmission depends on a given distribution that could be built on global and/or local knowledge. In [10], Blaszczyszyn et al. propose a receiver-based broadcast scheme. Active signalling is used as an acknowledgement technique and to select the relay offering the best progression.

The last part of this section discusses the integration of a trust level into the routing protocol. Indeed, the presence of attackers and malicious nodes in distributed networks may have a critical influence on the routing process. They can delete, change and drop messages. As a protection from these problems, we find several solutions proposing the integration of a trust framework into the routing protocols [7, 11].

In [7], a Trust Aware Wireless Routing Protocol (TAWRP) is proposed for wireless sensor network. It was designed in order to improve the performance of the network regarding the variety of the attacks in this heterogeneous system. The solution seeks to provide an optimal route with only trusted nodes and forward the packets from source to destination with minimum packet loss.

In mobile ad hoc networks, we can find this approach [11] that aims to propose a secure trusted routing protocol for mobile ad hoc network. The approach designs an evaluation mechanism that permits to define the trust level of a node based on the software configuration, the hardware configuration, battery power, credit history, exposure and organizational hierarchy. This trust level will be used in order to compute the next node hop.

The results presented in these works and the presence of several attacks in the vehicular environment encourage us to study this problem and to propose a new trust-driven and receiver-based routing protocol for ITS. To the best of our knowledge, there is no previous work studying this challenge in vehicular networks.

3 Trust-Driven Geographic Routing

One of the major goals considered in this paper is to design a new dissemination system that supports and improves traffic safety. It should aim to optimize the network resources usage and fit safety applications requirements in terms of delay and reception reliability. Moreover, it has to face the security issues that could be experienced in vehicular networks and accordingly detect and avoid malicious nodes that could affect the performance of data routing in the network.

The work in this paper is an extension of our previous work in [2] to consider trust as a metric in the relay selection procedure. In this section, we first give an insight about our geo-broadcast protocol proposed in [2], namely BZB (Bi-Zone Broadcast protocol) (please refer to the original publication for further details). Then, we consider the integration of trust in the routing protocol in order to secure the dissemination of data in vehicular networks.

3.1 BZB: Bi-Zone Broadcast Protocol for Vehicular Safety Applications

Bi-zone Broadcast protocol is based on a flexible and hybrid Contention-based Forwarding (CBF) scheme that mixes together, on the one hand the randomness of the standard CBF [9] and on the other hand the main concept of distance-based CBF, i.e. taking into account the progressed distance in the contention scheme. The distance-based CBF showed to be sub-optimal at close range, especially in case where no potential relay at the transmission range exists. We consider to rely on a random timer that can increase the chance of close cars to forward faster and avoid to wait wastefully for a non-existing farther relay. At the same time, the concept of distance-based CBF is preserved after a specific distance threshold (D_{th}). In other words, it is ensured that farthest nodes (after the threshold D_{th}), if they exist, will wait shorter time before transmitting. Furthermore, our approach permits to consider unknown topology and to avoid that nodes in a similar distance get the same contention timer. The main idea is to divide the potential forwarders (located in the transmission range) into two distinct groups, i.e. close and far vehicles according to their positions and given a particular distance threshold D_{th}.

In both cases, the waiting time is selected randomly between two bounds. For closer vehicles where the distance is lower than the D_{th}, the interval of contention time selection is fixed to [T2, T_{max}], T2 is given in Eq. 2 and T_{max} is the maximum waiting time. The contention interval of nodes with distance beyond D_{th} is [0, T1] where T1 is detailed in Eq. 1. Having a lower bound of 0, farthest nodes are granted the possibility to forward immediately the message upon reception without waiting a specific time. In worst cases, distance-based forwarding scheme is applied.

$$T_1 = T_{max} \times \left(1 - \frac{d}{r}\right) \tag{1}$$

$$T_2 = T_{max} \times \left(1 - \frac{D_{th}}{r}\right) \tag{2}$$

In the following, we give detailed equations of our contention approach. A node receiving the safety message computes its distance from the originator. It schedules a broadcast timer. The waiting time, as shown by Eq. 5, is randomly calculated between two bounds. The upper bound of waiting time T_{upper} and the lower bound of waiting time T_{lower} defined as expressed in Eqs. 3 and 4, respectively.

$$T_{\text{upper}} = \begin{cases} T_1 & where\ d > D_{th} \\ T_{max} & where\ d \leq D_{th} \end{cases} \tag{3}$$

$$T_{\text{lower}} = \begin{cases} 0 & where\ d > D_{th} \\ T_2 & where\ d \leq D_{th} \end{cases} \tag{4}$$

$$WaitingTime = random(T_{lower},\ T_{upper}) \tag{5}$$

where r indicates the transmission range, D_{th} is the distance threshold, T_{max} is the maximum waiting time and d is the distance from the last sender.

3.2 Trust-Driven BZB

In this section, we give details about our proposal, *trust-driven BZB*. Basically, it is an enhancement of our previously cited work *BZB*. The main purpose of this protocol is to take into account the trust aspect in the forwarding process in order to support secure forwarding in vehicular networks. We suppose here that each vehicle in the network is assigned a trust value which is evaluated beforehand. This is done by the means of a trust evaluation framework that takes into account many parameters related to the behaviour of the corresponding vehicle. The detailed operation of this trust framework is out of scope of this paper.

The main algorithm of our proposed dissemination approach is illustrated in Algorithm 1, a Decentralized Environmental Notification Message (DENM) [1] is generated when a vehicle detects an emergency event (Lines 2–4). The original message should contain all the required data such as the location data of the source and the perimeter of the dissemination area. After a successful reception of a DENM, the

vehicle checks whether the message has been received before (Line 6), whether the transmitter follows the receiver along the message propagation direction (Line 7) and if its position is located in the dissemination area (Line 8). Then, it should compare the geographic coordinates of the transmitter node with its own and determine the area it belongs (whether it is located before the distance threshold D_{th} or beyond). Accordingly, it enters the rebroadcast phase by executing the contention scheme represented by the procedure *ContentionPhase*(). The time that each node should wait before transmitting the received message depends basically on two parameters; the distance and the evaluated trust value. Following the same logic as BZB protocol, it is on the one hand inversely proportional to the distance from the last forwarder (Line 20). On the other hand, it is inversely proportional to the trust value. The total waiting time is described in Algorithm 1 (Lines 20, 21). Farthest nodes with highest trust value are given more priority to forward the DENM safety message. In addition, we define a weight w (Line 21) to adaptively evaluate the impact of considering the trust value in the calculation of the waiting time.

It is worth mentioning that we define two levels of trust:

- **Attacker**: defines the nodes with trust value equal to 0. These kinds of nodes are considered as attackers as they could conduct malicious isolation attacks.
- **Trustee**: designates the nodes with trust value equal to 1. Trustee nodes are the nodes behaving in a manner that is acceptable and in accordance with the expectations of the trustor, i.e. the surrounding nodes in the vehicular networks.

At each time step, the waiting time is decremented (Line 26). Forwarders that countdown until zero, rebroadcast the message by writing their own location information in the packet header in addition to the originator's information. Any time, while contending a node receives a valid copy of the DENM, it checks whether the message has been received before (Line 27). In this case, the vehicle aborts the rebroadcast procedure.

4 Experimentation and Evaluations

In this section, we evaluate the performance of our trust aware routing approach. We perform a comparison of trust-driven BZB against the original BZB. We consider the average information reception delay as a performance metric. It is defined as the interval from the time an application issues a DENM message and hand it over to the network layer to the time this message is firstly received by the corresponding network layer at another vehicle located at a particular distance from the source.

In the following, we introduce the simulation set-up and the configuration of mobility and network scenarios. We present then the set of performance metrics we have measured and finally the results of our experiments.

4.1 Simulation Scenario

Simulations have been performed using the simulation platform iTETRIS, where ns3 [12] and SUMO [13] are coupled together to form an integrated simulator for large-scale ITS evaluation studies. In our evaluation study, SUMO is used to create mobility scenarios which are fed then to ns-3. 40% of nodes are considered as attackers and perform a malicious isolation attack; that is, each node receiving the message does not forward it. Attackers are assigned 0 as trust value. Trustee nodes are assigned 1.

Mobility scenario We consider two different mobility scenarios for our simulations. First, to study the impact of trust in the routing process, we define a small scale static scenario where 30 vehicles are placed in two lanes road. Second, in order to model the dynamicity and the non-homogeneity of the topology and connectivity of vehicular environment, we specify an urban scenario illustrated in Fig. 1. It is a calibrated and realistic urban scenario from the iTETRIS project [3] called Acosta

Algorithm 1 pseudo-code of trust-driven BZB

Procedure: DENMMsgTx ()
if (detectEmergency) **then**
  TransmitDENMMessage ()
end if
Procedure: DENMMsgRx ()
if (notReceivedBefore) **then**
  if (inPropagationDirection (myPostion, senderPosition)) **then**
    if (myPosition *in* senderForwardArea) **then**
      ContentionPhase (D_{th})
    else
      abort
    end if
  else
    abort
  end if
else
  abort
end if
Procedure: ContentionPhase (D_{th})
Time ← Random (T_{upper} , T_{lower})
$Contention_Time \leftarrow Time * (1 - (w * (\frac{tust}{Trust_{max}})))$
Contending ← true
Contend (Time)
Procedure: Contend (Time)
while (Time > 0) **do**
  Time← Time - slotTime
  if (Time = 0 AND notReceivMessage) **then**
    TransmitMessage()
  end if
end while

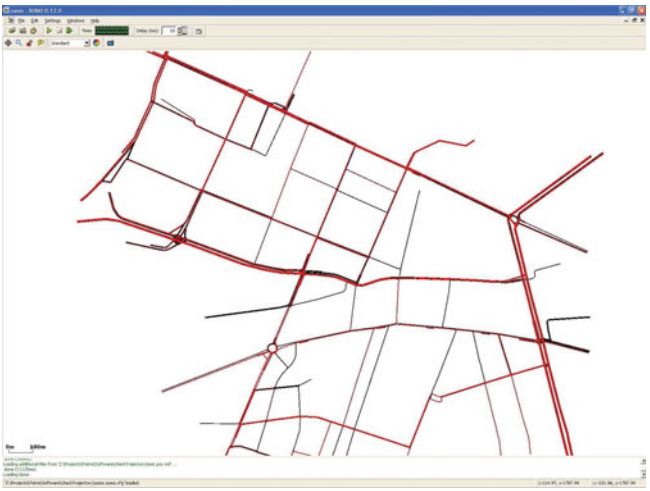


Fig. 1 Acosta mobility scenario

Table 1 Configuration parameters of the mobility scenarios

SUMO scenario	Static scenario	Urban scenario
Scenario size	3000 m × 60 m	2126 m × 2117 m
Average number of vehicles generated	30	1500–2000
Equipped vehicles rate	100%	100%
Attackers rate	40%	4%

Pasubio joined. This scenario models an urban environment and is composed of multiple intersections with different lengths of road sections connecting each other. The size of the road network is 2126 m × 2117 m. A summary of the configuration parameters of our simulations can be found in Table 1.

Network scenario In our network scenario, nodes communicate through periodic beacons and event-driven safety messages (DENM). Beacons are sent at 1 Hz frequency by all the nodes in the vehicular network. A DENM application, implemented in iTETRIS, has been used for the experiments. At the detection of an emergency event, the DENM application triggers the transmission of periodic safety messages, at the maximum allowed transmission power.

To vary the network and topology configuration, simulations have been performed multiple times (between five and ten different values of random number seed are used). Each simulation run is conducted for 100 s. At the beginning of each simulation, the dissemination area is selected randomly with a radius of 1000 m. The closest node to this area simulates an emergency event and initiates the DENM transmission.

Table 2 Configuration parameters of the network scenario

Parameter	Value
Dissemination area size	1000 m
Network beacon frequency	1 Hz
Packet size	500, 1500, 2000, 2200 Bytes
Propagation model	WINNER II LOS/NLOS
Shadowing	Correlated lognormal
Fast Fading	Rician (LOS)/Rayleigh (NLOS)
Transmission power	20 dBm
V2V maximum transmission range	400 m
V2I maximum transmission range	900 m
Simulation Time	100 s for each run
Number of simulation runs	20–40

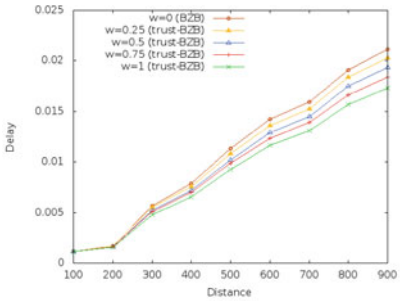
To study the impact of the overhead on the performance of the protocols, we vary the packet size. Four packet sizes have been used: 500, 1500, 2000 and 2200 Bytes. We use the WINNER B1 model for urban environment as a propagation model, which considers correlated lognormal shadowing and LOS/NLOS visibility between stations. Table 2 gives an overview of the configuration parameters for the communication scenario.

4.2 Simulation Results

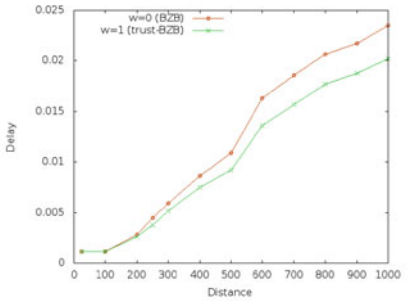
In this section, we analyse the simulation results obtained from the comparison of trust-driven BZB against BZB. Information reception delay is the performance evaluation metric examined.

Figure 2a illustrates the results in case of the small scale and static scenario. Varying the weight w of the waiting time equation in Algorithm 1, we plot the delay with regards to the distance from the source. For nodes located up to 200 m from the originator the delay does not exceed 1.7 ms for both protocols. The nodes that are covered by one hop transmission receive reliably and in short delays the DENM messages. Starting from 200 m the difference between the protocols can be distinguished. We can see that when we completely consider the trust in the calculation of the waiting time (i.e. when $w = 1$), trust-BZB achieves the lowest latencies as the average information delay does not surpass 17 ms. However, in case of BZB, the delay goes up to 21 ms. We plot the delay for different values of w. We can notice that $w = 1$ gives the best results. Indeed, our main concern is to further improve the propagation delay of the safety data as it is very critical information.

These results are explained by the fact that giving trustee nodes more priority to forward the safety messages helps to avoid waiting useless time. With trust-BZB,



(a) End to end delay with regards to the distance from the source. A static Scenario.



(b) End to end delay with regards to the distance from the source. An urban realistic scenario with mobility.

Fig. 2 End to end delay with regards to the distance from the source

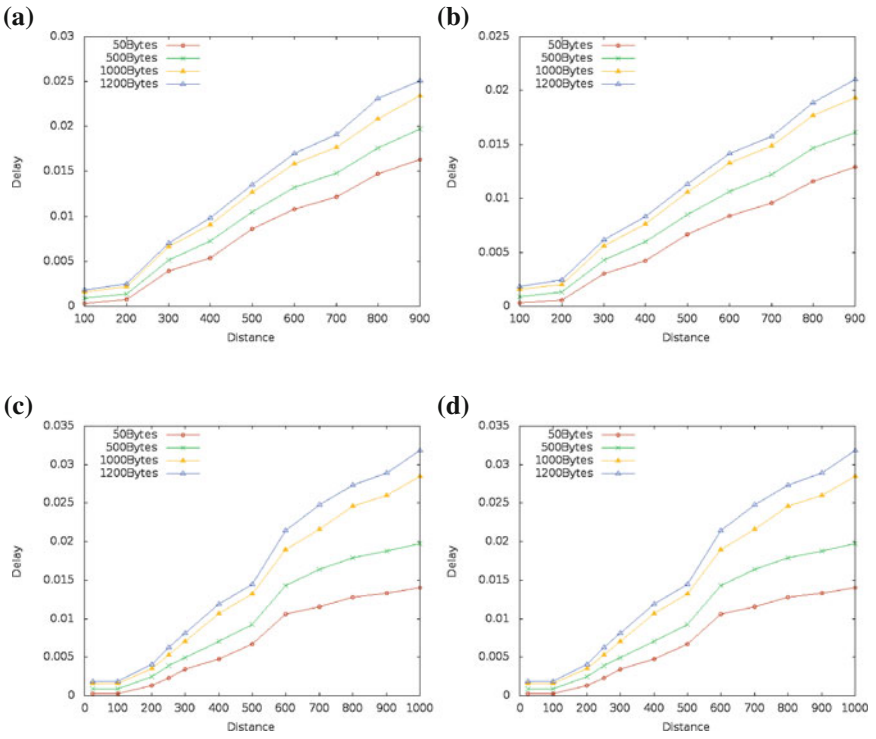


Fig. 3 Average Information reception delay with regard to the distance from the source. **a** Static scenario with w = 0 (BZB). **b** Static scenario with w = 1 (trust-BZB). **c** Urban scenario with mobility with w = 0 (BZB). **d** Urban scenario with mobility with w = 1 (trust-BZB)

trustee and farther nodes could have less waiting time than closer and attacker nodes. The forwarding scheme of trust-BZB ensures accurate relay selection in order to increase the reliability of safety data reception.

An aspect to investigate is the impact of mobility on the performance of the routing schemes. Figure 2b depicts the delay results in case of a realistic urban mobility scenario. We observe that trust-BZB outperforms BZB even in highly dynamic environments and proves again that with its design principle it enhances the dissemination delay of safety information.

Figure 3 illustrates the safety information delay with regards to the distance for several packet sizes, i.e. 50, 500, 1000 and 1200 Bytes in both mobility scenarios. Obviously, when increasing the packet size, the average information delay to reach the dissemination area increases. For example, in case of the static scenario, for a payload of 500 Bytes, nodes at 900 m from the source can receive the message after 16 ms; however, they can receive it only after 21 ms in case of 1200 Bytes of packet size. The results show that trust-driven BZB outperforms BZB for the different packet sizes. Moreover, when introducing mobility, the safety information delay increases for all the payload sizes. For instance, for packet size 1200 Bytes for static scenario the average delay at farthest distance goes up to 21 ms. However, for urban realistic scenario, it exceeds 31 ms.

5 Conclusions

In this paper, we proposed trust-driven Bi-Zone Broadcast (trust-BZB) which is a receiver-based routing protocol for safety-related data. Trust-BZB considers applying the degree of trust in the process of relay selection in order to secure the dissemination of safety messages enclosing highly critical data. The obtained simulation results showed that our trust-BZB achieves its design goal by delivering traffic safety information in a geographic area in a fast and efficient way compared to the original BZB. In future works, we plan to design a framework for trust evaluation. Moreover, we plan to further study the performance of our trust-BZB under different circumstances and considering other performance evaluation metrics.

References

1. ETSI EN 302 637-3, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service
2. Hrizi, F., Härri, J., Bonnet, C.: Adapting contention-based forwarding to urban vehicular topologies for traffic safety applications, Ann. Telecommun.
3. iTETRIS project. http://www.ict-itetris.eu/

4. Zhen, X., Wang, J., Wang, P., Wang, X., Liu, F.: A sender-initiated adaptive and reliable broadcast scheme for vanet safety message. In: IEEE International Symposium on Information Science and Engineering (ISISE) (2012)
5. Ros, F.J., Ruiz, P.M., Stojmenovic, I.: Reliable and efficient broadcasting in vehicular ad hoc networks, In: 69th IEEE Vehicular Technology Conference, VTC Spring (2009)
6. Sahoo, J., Wu, E.H.K., Sahu, P.K., Gerla, M.: Binary-partition-assisted MAC-layer broadcast for emergency message dissemination in VANETs, IEEE Trans. Intell. Transp. Syst. 12(3) (2011)
7. Gholibeigi, M., Heijenk, G., Moltchanov, D., Koucheryavy, Y.: Analysis of a receiver-based reliable broadcast approach for vehicular networks. Ad hoc Netw. **37**, 63–75 (2016)
8. Jiang, H., Guo, H., Chen, L.: Reliable and efficient alarm message routing in vanet. In: Proceedings of the 5th 28th International Conference on Distributed Computing Systems Workshops (2008)
9. Fuβler, H., Hartenstein, H., Widmer, J., Mauve, M., Effelsberg, W.: Contention-Based forwarding for street scenarios. In: Proceedings of the 1st International Workshop on Intelligent Transportation (WIT04) (2004)
10. Blaszczyszyn, B., Laouiti, A., Muhlethaler, P., Toor, Y.: Opportunistic broadcast in VANETs (OB-VAN) using active signaling for relays selection. In: Proceedings of the 8th Intelligent Transport Systems Telecommunications(ITST'08) (2008)
11. Abusalah, L., Khokhar, A., BenBrahim, G., ElHajj, W.: Tarp: trust-aware routing protocol. In: Proceedings of the international conference on Wireless communications and mobile computing. ACM (2006)
12. ns-3 simulator. http://www.nsnam.org/
13. SUMO simulator. http://sumo.sourceforge.net/
14. Anwar, R.W., Bakhtiari, M., Zainal, A., Qurechi, K.N.: Malicious node detection through trust aware routing in wireless sensor networks. J. Theor. Appl. Inf. Technol. 74(1) (2015)

Author Index

A. Laouiti et al. (eds.), *Vehicular Ad-Hoc Networks for Smart Cities*,
Advances in Intelligent Systems and Computing 548,
DOI 10.1007/978-981-10-3503-6