Privacy Preserving Authentication Approaches in VANET: Existing Challenges and Future Directions

Ubaidullah Rajput[†], **Fizza Abbas**[††], **Ayaz Hussain**[†††], **Dost Muhammad Saqib Bhatti**[††††] **and M. SullemanMemon** [†††††]

[†, ††, †††††] Department of Computer Systems Engineering Quaid e Awam UEST Nawabshah Pakistan,
[†††] Department of Electrical Engineering, Balochistan University of Engineering and Technology, Khuzdar, Pakistan,
[††††] Dawood University of Engineering and Technology, Karachi

Summary

The recent advent in wireless and network communication technologies has contributed greatly in people's lives. A Vehicular Ad-Hoc Network (VANET) is an application of Intelligent Transportation System (ITS) that aims towards the safety and comfort of drivers and passengers. However, the openness of this network allows attackers to jeopardize the network with a variety of attacks. Due to the catastrophic consequences of such attacks, the security and privacy of VANET is of paramount significance. In other words, the communication between network participants should be authenticated in order to allow only legitimate users to take part in the network. In this regard, this paper presents state of the art regarding the broadly used authentication techniques namely pseudonym based authentication, identity based authentication and group signature based authentication. The paper compares the significant research effort proposed by the research community and discusses the pros and cons of each of the techniques. In the end, the paper identifies various research challenges along with future directions.

Key words:

VANET Security Privacy Authentication.

1. Introduction

In 2015, the world health organization (WHO) published a global status report on road safety. According to that report, about 1.25 million humans lost their lives each year due to traffic accidents. These accidents are occurred due to many factors that include traffic congestion due to increasing population and insufficient improvements in existing road infrastructure, violation of traffic rules, negligence by the drivers, violation of traffic rules, and a lack of information of roads. The primary aim of developing Vehicular Ad-Hoc Network (VANET) is to make the driving experience more safe and pleasant. This includes (but not limited to) providing alternate routes in rush hour to reduce road congestion, information regarding nearby point of interests (such as restaurants, gas stations, accommodation etc), entertainment and enhanced road safety. VANET borrows many of the characteristics of Mobile Ad-Hoc Network (MANET). Vehicles in VANET act similarly to mobile nodes in MANET and the movement of these smart vehicles is governed by road layouts [1]. Figure 1 shows a typical VANET environment consists of infrastructure and vehicles. The communication is either vehicle-to-vehicle (V2V) or vehicle-to-infrastructure (V2I). In VANET, infrastructure is also known as Road Side Unit (RSU) that are installed alongside the roads [2]. The RSU not only helps vehicles communicate with each other (by extending the range of communication) but may also assumes a more active role of information exchange and distribution. Each smart Vehicle has an On-Board Unit (OBU) that poses the communication and processing capabilities. Smart vehicles in VANET communicate with the neighboring vehicles and with the infrastructure with the help of specific communication standard namely Dedicated Short-Range Communication (DSRC) standard [3]. The vehicles are required to periodically broadcast messages that are known as beacons. These beacons contain safety as well as traffic related information of a vehicle. This information includes (but not limited to) a vehicle's heading, speed, and geographical coordinates and used by many applications such as cooperative collision avoidance (CAA), obstacle warning, electronic emergency brake light (EEBL) and traffic events such as road congestion etc. The purpose of these applications is to provide a driver with a contextual view of his/her surroundings to help take necessary actions in case of an unexpected hazard such as sudden brake by the car in front. However, the security and privacy of the information contained in a beacon is of paramount importance. Firstly, this information may reveal the travel path of a driver and therefore, seriously hampers his/her privacy. For example, there is a high probability that the starting location coordinates and the ending coordinate of a private vehicle's travel path are the address of home and office of the driver. By eavesdropping this information, an attacker can track a vehicle and may stalk or harass the owner of the vehicle. Secondly, a more capable attacker may launch various active attacks by intercepting, forging or altering the beacon information and therefore,

Manuscript received April 5, 2018
Manuscript revised April 20, 2018

jeopardizes the information security. For example, the attacker may spoof bogus messages to provide the fake impression of a road congestion to gain an advantage. In a more worse situation, a terrorist may even cause an accident. The authors of [4,5] put forward their efforts in providing a detailed description of various security and privacy related attacks in VANET. Therefore, the authentication of legitimate users of VANET is of critical importance. During authentication, a user is required to provide valid and unique credentials. These credentials not only eliminate the possibility of attacks by outsiders but in case of an attack by insider, help tracking that malicious insider. However, the openness of a VANET environment also makes authentication of a legitimate user a non-trivial task. Since the credentials used for authentication often contain identity information such as the number plate of vehicle or driving license, unauthorize exposure of such information during an eavesdropping attack may jeopardize the privacy of the user. Therefore, the dilemma is to provide privacy preserving authentication. However, this privacy preserving authentication must be conditional, that is, the mechanism should guarantee the anonymity of a legitimate user and in case of the detection of an insider attack, the identity of the malicious user must be revealed. Although authentication of vehicles plays a vital role in dealing with many of security and privacy related issues, the task of conditional privacy preserving, that is, detection of the malicious actions and subsequent revocation of attackers while guaranteeing the privacy of honest users makes authentication a non-trivial task in VANET. Recently, many privacy preserving schemes have been put forward that include pseudonymous based schemes, identity based schemes and group signature based schemes. The study in [6] provides a more broader taxonomy, however, other categories usually serve as a subset of aforementioned broader categories. These schemes successfully resolve many of the security and privacy related issues in authentication in VANET, but each has its own limitations. This paper attempts to discuss these schemes in details, compares them, identifies unsolved issues and provide future directions for further improvements.

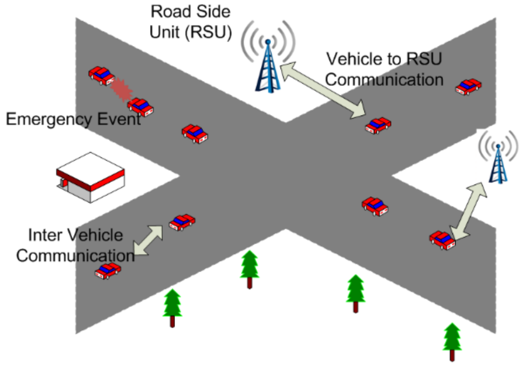

Fig. 1 VANET Overview

The paper is organized as follows. Section II briefly provides the background of VANET and related technologies. Section III discusses various privacy preserving schemes along with their pros and cons and present the comparison. Section IV identifies various challenges related to security and privacy in VANET and provides future research directions while the Section V concludes the paper.

2. VANET Background

A vehicular ad hoc network is an initiative towards safer and comfortable road travelling. VANET assumes the presence of smart vehicles that are embedded with an on-board unit or OBU equipped with processing and communication hardware enabling vehicles to form an ad hoc network environment. [7]. Roadside units (RSUs), also known as infrastructure in VANET are fixed base stations alongside the roads and intersections [8]. The main purpose of RSUs is to extend the overall network coverage. RSUs are considered to be equipped with better processing and communication hardware than OBUs and help increase network coverage by enhancing the distance propagated by the messages. The mode of communication is either vehicle-to-infrastructure (V2I) or vehicle-to-vehicle (V2V). The PHY and MAC layers of VANET are implemented with the help of dedicated-short-range-communication standard (DSRC) and IEEE 802.11p Wireless Access for Vehicular Environment (WAVE) [9] standards. In order to increase the road safety, reduced pollution and better fuel consumption [9], a dedicated 75 MHz spectrum in 5.9 GHz band, with a range of around 1000 m is allocated by the United States Federal Communications Commission (FCC) to the intelligent transportation systems (ITS) [10]. The spectrum is divided into seven 10-Mhz channels. Among them, four channels are the service channels that are used for both the safety and non-safety applications, two channels are reserved for future advanced accident avoidance applications and high power public safety communication usages and the remaining one channel is the control channel that is restricted to be used for safety communications only [10]. The WAVE/DSRC standards define rules for differentiating the usage of emergency and normal applications, fast network recognition and low delay for connection setup and therefore, help achieving high throughput communication among vehicles with low delay. Consequently, in case of some unfortunate event (such as an accident), an emergency messages can be efficiently communicated among the vehicles.

2.1 Characteristics of VANET

Apart from inheriting many of the characteristics of (MANET), VANET have the following unique characteristics of its own [11].

• Rapid change in topology

Fast moving vehicles travel with high speeds as well as change directions along the roads. This leads to rapidly changing topologies by the vehicles.

• Frequent link disconnection

Due to the high speeds, there are frequent link breakdowns. By considering the scenario where vehicles travel in opposite directions with high speed, the link will only last for a few seconds.

• No energy and storage constraints

VANET do not suffer with the energy and storage constraints that are considered as significant drawbacks of resource constraint MANET.

• Vehicle position prediction and mobility modeling

Another feature of VANET is the predictable movement (or mobility patterns) of vehicles that are governed by the specific layouts of roads, streets, intersections and speedways. Therefore, a vehicle's future position is predictable.

• City based and Highway based communication environments

Vehicles on the roads encountered with two typical communication environments. One is where the vehicles are travelling in a city environment and therefore, the communication between vehicles is affected by the obstacles such as buildings and trees. The other environment is the highways where there are less obstacles and therefore, improved line of sight (LoS) communication.

• Minimum delay requirements

One of the most critical requirement for the VANET safety applications is the minimum end-to-end delay and not the high data rates. Applications such as emergency electronic brake light (EEBL) requires immediate delivery of the message to avoid some unfortunate event such as an accident.

• On-board sensors:

Today's smart vehicles are equipped with various sensors that perform various kinds of sending tasks. These not only help drivers form a contextual view but also provide him with useful information. Examples of such sensors include “lateral proximity sensors" that assist a driver during parking by giving warnings in case of obstructions in driver's blind spot [38]. Currently, each smart vehicle is equipped around 60-100 sensors that are projected to reach 200 by the year 20203.

2.2 VANET Applications

Apart from inheriting many of the characteristics of (MANET), There is support for the safety critical and non-safety critical applications [3, 9] in VANET. The non-safety application also referred as Infotainment that is, information and entertainment. We can broadly categorized VANET applications in four categories namely “active safety applications”, “public service”, “improved driving” and “business/entertainment” [12]. Following is the description of each of these applications along with their examples.

• Active safety applications

Active safety applications are the most critical applications of a VANET environment because these are directly related to the road safety. Some of these applications include (but not limited to) blind spot warning, work-zone warning, curve speed warning, cooperative collision avoidance and electronic emergency brake light.

• Public service

The purpose of Public service applications is to provide support to the public service vehicles. These vehicles include police vehicles, emergency recovery vehicles and ambulances. Examples of such applications include emergency vehicle at scene warning, stolen vehicle tracking, approaching emergency vehicle warning etc.

• Improved driving

As the name suggests, these applications aim to assist drivers having a simplified, comfortable and improved driving experience. Examples of such applications are intelligent traffic flow control, parking lot locator service, left turn assistant, and highway merge assistant.

• Business and entertainment

These applications facilitate drivers and passengers in many ways that include both the entertainment and assistance in various kinds of business activities such as on spot payments. This includes Internet services, music download, instant messaging, software update/flashing, rental car processing and parking payment (to name a few).

3. Authentication Schemes in VANET

Shortly after the emergence of VANET, Raya and Hubaux [5], highlighted the important of privacy and security related issues in VANET. Since then, many researchers have put forward their efforts and proposed various privacy preserving authentication schemes. Most of these schemes can be broadly categorized into pseudonym based authentication, identity based authentication and group signature based authentication. In the following, we discuss in detail, schemes presented under each of these broad categories along with their advantages and disadvantages.

3.1 Pseudonymous based authentication

Raya et al. [13] proposed one of the earliest pseudonym based approaches for privacy preserving authentication in VANET. A pseudonym based authentication approach essentially employs public key cryptography concepts. These schemes attach public key infrastructure (PKI) based certificates with the beacon messages that are signed by the associated private keys. A pseudo identity is contained by each certificate and the association between the pseudo identity and the real identity of the user is known to a certification authority (CA). In the scheme of Raya et al. the CA generates and issues thousands of pseudonymous certificate and related private keys. The sender vehicle chooses a certificate among the pool of certificates and signs and broadcast the beacon message along with the related private key. The receiver of the beacon message can verify the message with the help of the attached certificate. In the event of detection of a bogus message or any malicious attempt, the CA resolves the association between the real and pseudo identity and the culprit is identified. The authors of [14] further improves the idea of [13] by introducing a Temper Proof Device (TPD) also known as hardware security module (HSM). A HSM is installed in a vehicle's OBU and secures the vehicle specific cryptographic material. However, these schemes mainly suffer from the requirements of communication, storage and distribution of thousands of pseudonymous certificates. Moreover, pseudonym based approaches also inherent another major drawback. In case of revocation of a culprit vehicle from the network, culprit's identity is included in a ever-growing certification revocation list (CRL). The CRL is continuously needed to be updated and distributed to all the network participants. The size of CRL grows exponentially. A vehicle also needs to check the CRL for each receiving beacon message. The scheme in [15] proposes an efficient distributed certificate service (DCS) that attempts to distribute CRL in an efficient way. However, a vehicle still needs to verify a large amount of certificate in an area with densely populated RSUs. Another drawback of DCS is the potential RSU compromise. Sun et al. [16] employ hash chains and proxy re-signature scheme to reduce the size of the CRL. Lu et al. [17] propose ECPP that uses bilinear maps to achieve conditional privacy for vehicles. ECPP proposes the use of multiple short life anonymous pseudonyms. A vehicle needs to obtain the short-lived pseudonyms from a nearby RSU. However, this scheme is not without drawbacks. Firstly, a vehicle needs to provide their fixed, non-changing pseudo-identities to RSU, and therefore, ECPP requires trusted RSU. However, RSU in VANET are vulnerable to physical attacks due to their deployment in open spaces. Therefore, RSU compromise may seriously hampers the vehicles' privacy. Secondly, the scheme requires a RSU to update the CRL during pseudonym issuance that becomes a significant performance bottleneck.

3.2 Identity based authentication

The schemes presented in [18] employ identity-based cryptography [19]. These schemes utilize a public key that is a known entity. The associated private key is issues by a trusted authority such as CA. However, to provide privacy, the known identity is concealed using a pseudonym and thus suffer considerably due to pseudonym management overhead. The scheme in [18] proposes an identity based signature scheme where vehicles exchange messages with RSUs and with each other. This scheme uses a batch verification scheme and therefore, messages are aggregated and quickly verified by vehicles, RSU and a traffic management authority (TMA). However, [18] requires inclusion of a common string in messages, distributed by RSU, for effective batch verification. The vehicles use short-term pseudonyms, but the revocation of the pseudonyms necessitates the use of CRL. The authors propose that the vehicle should use the short-term pseudonym for 24 hours to make the CRL shorter and therefore, allows an attacker to track a user. Sun et al. [20] propose another identity-based scheme with pseudonyms. The vehicles use these pseudonyms to get cryptographic credentials from trusted border RSUs. The scheme provides traceability but requires a vehicle to accommodate many pseudonyms and therefore, needs to maintain a CRL. Moreover, the scheme also requires vehicles to establish a shared key for communication that may prove to be time consuming process considering fast moving vehicles. The vehicles constitute an access group where the owner is authorized to revoke a member vehicle. However, [20] does not discuss the selection of owner as well as possible unfair treatment. Lu et al. [21] and Li et al. [22] propose an identity based signature and Online/Offline signature scheme that enables vehicles to use self-generated pseudonyms. The scheme employs a regional trusted authority that generates cryptographic material for the RSUs and vehicles. However, the scheme suffers from two major drawbacks. First is the use of CRL and the other is the increased computational cost in verifying the signatures. Another drawback is the unreal assumption that infrastructure (RSUs) are reliable and cannot be compromised.

3.3 Group signature based approach

The main theme of group signature based authentication schemes [23], is forming a group of vehicles and the real identity of each vehicle is concealed among the group. Each vehicle in a group signs the message with distinct private keys and the receiver of the message verifies the message with the group's public key. If a malicious message is found, then the group manager traces the malicious member and revokes it. Various schemes employ different entities as group manager such as a vehicle, RSU or trusted authority (TA). Authors of [23] propose a group signature-based scheme that provides privacy preserving communication among vehicles as well as between vehicle and RSU. However, the scheme requires a vehicle to provide its license plate number to generate an identity based signature. Moreover, the scheme employs a significantly long signature size of 192 bytes. Another drawback is the inefficient revocation mechanism. One of the proposed mechanism is like managing a CRL while the other method requires the delivery of new group credentials to the non-revoked members. Zhu et al. [24] propose another privacy preserving authentication scheme that requires the mutual authentication of RSU and vehicle and then RSU issues the group credentials to the vehicle. However, the vehicle sends an encrypted request to the RSU that contains vehicle's identity and therefore, in case of RSU compromise, vehicles' identity can compromise. The scheme in [25] employ an efficient batch verification based signature verification scheme. However, the performance of the scheme significantly decreases in the presence of a few invalid messages. This is due to the additional verification delay for a re-batch and therefore, the scheme loses its efficiency. These schemes mainly suffer from bogus messages and DoS attacks. The authors of [26] propose a combination of both the pseudonymous-based schemes and group signature-based. However, the scheme needs to check a message against the list of revoked vehicles and therefore, computationally expensive. The scheme in [27] proposes the RSUs to act as group managers. RSUs manage and maintain the vehicles. The vehicles form a group in RSU's communication area and broadcast messages that are verified by the group members and in the neighboring group. The scheme lacks in providing prevention against replay attack and DoS attacks. Another drawback is the reliance on RSU for group management tasks. This reliance poses significant security and privacy related threats on all the vehicles in a RSU jurisdiction if that RSU compromises.

4. Research Challenges and Future Directions

The related work demonstrates several short-comings in the state of the art. The pseudonym-based schemes mainly suffer from a large number of pseudonym certificates and CRL computational, communication and storage related issues. Group signature-based schemes suffer with the increased computation and communication involved in group signatures, insufficient prevention from bogus information attack and replay attacks. Moreover, another major drawback is the group management issue. Identity-based schemes use the identity information of vehicle to avoid large size certificates. However, for frequent communication they rely on short-term pseudonyms and group signatures and therefore, inherits the same issues faced by pseudonym-based or group signature-based schemes.

It is evident that the presence of CRL contributes greatly in computation, communication, storage and distribution overheads and therefore, the use of CRL is inefficient in a humongous network such as VANET. The other major performance bottleneck arises during the costly group signature verification and storage related issues. Therefore, the need is to construct signatures schemes with shorter signature and their efficient verification. The identity based scheme provides a unique way of conditional privacy preserving authentication but the trust on 3rd parties such as CA should be kept to a minimum.

5. Conclusion

The paper provides the overview of VANET, its architecture and applications. The paper also discusses the need of privacy preserving authentication by presenting various security and privacy related threats. This paper further provides an in-depth comparison of various privacy preserving authentication schemes along with their respective advantages and disadvantages. In the end, the paper outlines unsolved issues and suggest useful future directions for finding efficient solutions.

References

[1] F. J. Ros, P. M. Ruiz, and I. Stojmenovic, "Acknowledgment-based broadcast protocol for reliable and efficient data dissemination in vehicular ad hoc networks," IEEE Transactions on Mobile Computing, vol. 11, no. 1, pp. 33–46, 2012.

[2] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, “Security in vehicular adhoc networks,” IEEE communications magazine, vol. 46, no. 4, 2008.

[3] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, “A comprehensive survey on vehicular ad hoc network,” Journal of network and computer applications, vol. 37, pp. 380–392, 2014.

[4] B. Parno and A. Perrig, “Challenges in securing vehicular networks,” in Workshop on hot topics in networks (HotNets-IV). Maryland, USA, pp. 1–6, 2005.

[5] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.

[6] S. S. Manvi and S. Tangade, “A survey on authentication schemes in vanets for secured communication,” Vehicular Communications, 2017.

[7] M. S. Al-Kahtani, “Survey on security attacks in vehicular ad hoc networks (VANETs),” in Signal Processing and Communication Systems (ICSPCS), 2012 6th International Conference on. IEEE, pp. 1–9, 2012.

[8] A. B. Reis, S. Sargento, and O. K. Tonguz, “On the performance of sparse vehicular networks with road side units,” in Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd. IEEE, pp. 1–5, 2011.

[9] Q. Xu, T. Mak, J. Ko, and R. Sengupta, “Vehicle-to-vehicle safety messaging in dsrc,” in Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks. ACM, pp. 19–28, 2004.

[10] G. Dimitrakopoulos and P. Demestichas, “Intelligent transportation systems,” IEEE Vehicular Technology Magazine, vol. 5, no. 1, pp. 77–84, 2010.

[11] F. Li and Y.Wang, “Routing in vehicular ad hoc networks: A survey,” IEEE Vehicular technology magazine, vol. 2, no. 2, 2007.

[12] E. Schoch, F. Kargl, and M. Weber, “Communication patterns in vanets,” IEEE Communications Magazine, vol. 46, no. 11, 2008.

[13] R. Maxim and H. Jean-Pierre, “The security of vehicular ad hoc networks,” in Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, pp. 11–21. 2005.

[14] M. Raya, P. Papadimitratos, and J.-P. Hubaux, “Securing vehicular communications,” IEEE Wireless Communications, vol. 13, no. 5, 2006.

[15] A. Wasef, Y. Jiang, and X. Shen, “DCS: an efficient distributed-certificate-service scheme for vehicular networks,” IEEE Transactions on Vehicular Technology, vol. 59, no. 2, pp. 533–549, 2010.

[16] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, “An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications,” IEEE Transactions on Vehicular Technology, vol. 59, no. 7, pp. 3589–3603, 2010.

[17] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications,” in INFOCOM 2008.

[18] L. Zhang, C. Hu, Q.Wu, J. Domingo-Ferrer, and B. Qin, “Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response,” IEEE Transactions on Computers, vol. 65, no. 8, pp. 2562–2574, 2016.

[19] A. Shamir, “Identity-based cryptosystems and signature schemes,” in Workshop on the Theory and Application of Cryptographic Techniques. Springer, 1984, pp. 47–53.

[20] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, “An identity-based security system for user privacy in vehicular ad hoc networks,” IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227–1239, 2010.

[21] H. Lu, J. Li, and M. Guizani, “A novel id-based authentication framework with adaptive privacy preservation for vanets,” in Computing, Communications and Applications Conference (ComComAp), 2012. IEEE, pp. 345–350, 2012.

[22] J. Li, H. Lu, and M. Guizani, “ACPN: a novel authentication framework with conditional privacy-preservation and non-repudiation for vanets,” IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 938–948, 2015.

[23] X. Lin, X. Sun, P.-H. Ho, and X. Shen, “GSIS: a secure and privacy-preserving protocol for vehicular communications,” IEEE Transactions on vehicular technology, vol. 56, no. 6, pp. 3442–3456, 2007.

[24] X. Zhu, S. Jiang, L.Wang, and H. Li, “Efficient privacy-preserving authentication for vehicular ad hoc networks,” IEEE Transactions on Vehicular Technology, vol. 63, no. 2, pp. 907–919, 2014.

[25] A. Wasef and X. Shen, “Efficient group signature scheme supporting batch verification for securing vehicular networks,” in Communications (ICC), 2010 IEEE International Conference on. IEEE, pp. 1–5, 2010.

[26] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, “Efficient and robust pseudonymous authentication in vanet,” in Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks. ACM, pp. 19–28, 2007

[27] L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer, “A scalable robust authentication protocol for secure vehicular communications,” IEEE Transactions on vehicular Technology, vol. 59, no. 4, pp. 1606–1617, 2010.

Ubaidullah Rajput received his Bachelor's Degree in Computer System Engineering from Quaid-e-Awam University of Engineering, Science and Technology (Quest), Pakistan in 2005. He received his Master's in Computer System Engineering from NUST Islamabad, Pakistan in 2011. He successfully completed his PhD in Computer Engineering from Hanyang University, Korea in 2017. His research interests are security and privacy issues in crypto-currency, security and privacy issues in VANETS, Internet of Things (IoT), mobile social networks and cloud computing. He has more than 11 years of teaching and research experience and currently working as Assistant Prof. in Quest Pakistan. He has served as a reviewer in many conferences and journals. He is author of many International and national papers.

Fizza Abbas received the bachelor's degree in computer system engineering from the Quaid-e- Awam University of Engineering, Science and Technology (Quest), Pakistan, in 2007, and the master's degree in communication system and networks from Mehran University, Pakistan, in 2011. She successfully completed her PhD in Computer Engineering from Hanyang University, Korea in 2017. Her research interests are security and privacy in social network services, mobile social networks, cloud computing, mobile cloud computing, and vehicle ad hoc networks. She has ten years of teaching experience and currently working as Assistant Prof. in Quest Pakistan. She has served as a reviewer in many conferences and journals. She is author of many International and national papers.

Ayaz Hussain received the bachelor’s degree in Telecommunication Engineering from Mehran University of Engineering and Technology, Jamshoro, Pakistan, in 2006, and the master’s degree in Electronic and Electrical Engineering from Hanyang University, Ansan, Soutyh Korea in 2010. He has done his Ph.D in Electronic and Electrical Engineering from Sungkyunkwan University, Suwon, Korea. Currently, he is working as an assistant professor in department of Electrical Engineering, Balochistan University of Engineering and Technology, Khuzdar, Pakistan. His research interests include wireless communication systems; in particular, cooperative relaying, MIMO technology, D2D communications, and energy harvesting.

Dost Muhammad Saqib Bhatti is working as an Assistant Professor in Department of Telecommunication Engineering, Dawood University of Engineering and Technology Karachi. He received his Bachelors of Engineering degree in Telecommunication Engineering from Mehran University of Engineering and Technology Jamshoro Pakistan in 2011 and Ms-Ph.D. degree in Electronics and Communication Engineering from Hanyang University, Seoul, South Korea in 2017. He has worked in Huawei for 1 year as a Team Lead on CMPAK project for 3G/4G swap. During his stay at Hanyang University, he has worked on various research projects. He has wide experience of teaching, industry and research. Dr. Bhatti’s research interests are in modeling, designing and performance analysis of wireless communication system with current emphasis on spectrum sensing, fuzzy logic, multidimensional scaling, cognitive Radio Networks and Non-orthogonal multiple access (NOMA).

M. Sulleman Memon received the B.E in Computer Engineering and M.E. in Software Engineering from Mehran University of Engineering & Technology, Jamshoroin 1990 and 2004, respectively. He is now a PhD scholar at Quaid e Awam University of Engineering and Technology, Nawabshah. He has submitted thesis. He is working as Assistant Professor in the Department of Computer Engineering. QUEST, Nawabshah. He is author of many International and national papers. He has presented his work at many countries of the word in International Conferences. His field of study is Wireless communications. He is Senior Member of IACSIT and member of Pakistan Engineering Council, ACM, and IEEE.