2019 2nd International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)

Security Attacks, Requirements and Authentication Schemes in VANET

Amit Kumar Goyal[1], Arun Kumar Tripathi[2], Gaurav Agarwal[3]
[12]KIET Group of Institutions Ghaziabad, 201206, India, [3]Invertis University Bareilly, 243123, India

***Abstract*— Vehicular Ad-hoc Networks (VANET), the promising technique, is getting attention for managing the traffic efficiently and making the road safe. The topographies and its vast applications varying from road safety, to the traffic management, payment service to infotainment. VANETs are characterized as a self-organized, distributed, highly mobile, dynamic topology, unconstrained power, computational and storage networks. The communication in VANET is performed in open-access environment which demands the security issues must be deal with utter importance. Security requirements includes authentication, availability, message confidentiality, message integrity, data availability, access control, privacy, message non-repudiation and real time guarantees of message delivery. In order to have a secure and efficient VANET infrastructure, an extensive overview of characteristics, challenges, security attacks and requirements must be dealt with. The prime objective of this paper is to provide a classification of security requirements, security characteristics and challenges.**

Keywords—VANET, Architecture, Security attacks, Challenges, Security Requirements.

I. INTRODUCTION

Vehicular Ad-hoc Networks (1) providing communication among mobile Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I), is a special category of MANET. It consists of vehicles known as nodes which are highly mobile in nature and are equipped with specialized dedicated sensors, known as On-Board Unit (OBU. Sensors collects information from other moving vehicles or stationery Road Side Units (RSU) and exchange this information with directly to other vehicles or indirectly by passing it to RSUs. VANET is there to provide safe and comfortable journey to passengers. These nodes in VANETs are equipped with sensors, which collects information in real time fashion and share this information to other moving vehicles and/or to the stationary RSUs. Though VANET helps in predicting and making decision about the future position of the vehicles, lots of challenging issues are there such as dynamic topology, potentially large scale and high mobility because most of the nodes are moving at a very high speed and thus changing their positions. Besides, scalability is very high in VANETs as nodes keep on adding and can include over the entire road of the city. Therefore, number of articles has discussed various issues related to VANET. All of these articles reviewed some of the specific research areas of VANETs.

The rest of the paper is structured as follows, section II deals with overall VANET architecture and its components, and in Section III, various characteristics of VANET are explained, section IV focuses on various attacks, in section V discussed various security requirements in VANET, VI focuses on various authentication schemes in VANET, at last, section VII summarizes the work with future trends in VANET.

II. VANET ARCHITECTURE

In VANET, vehicle consists of OBUs equipped within the vehicles, stationary RSUs and a set of sensor nodes. Fig. 1 shows generalized VANET architecture (2). The basic units involved in communication are AU, OBU and RSU. These are discussing as follows:

A. Application Unit (AU)

AU is the Graphical Interface used between user and OBU. The user can retrieve the stored messages, complete information about journey speed, traffic condition etc. for analysis.

B. On Board Unit (OBU)

It is an electronic device consisting of processor, Global Positioning System (GPS), read/write memory, sensor nodes, and Event Data Recorder (EDR) modules. Sometimes these modules may be place independently inside the vehicles. Generally, OBUs are mounted on-board and exchanges the information with nearby OBUs and RSUs. For communication, OBU uses IEEE 802.11p radio technology in ad hoc environment. On the other hand, in infrastructure-based environment, OBUs use IEEE802.11 a/b/g radio technology. Furthermore, OBUs controls ad-hoc connection, routing, IP-based mobility management, data security issues and network congestion. EDR is an electronic device and part of OBU. It stores all the transmitted and received messages to the nearby OBUs and RSUs. It also records all activities that happened in vehicle environment during the trip. For identifying the physical location acceleration and direction of movement of vehicle at specific interval of time GPS is used. A special purpose-computing device is attached with OBU. It is responsible for taking necessary action corresponding to messages received from other OBUs or RSUs. Radars and sensors are used to detect obstacles appears during movement of vehicle. An omnidirectional antenna is responsible for accessing the information on wireless channels. To identify a vehicle uniquely an Electronic License Plate (ELP) is also associated with every vehicle.

978-1-7281-1772-0

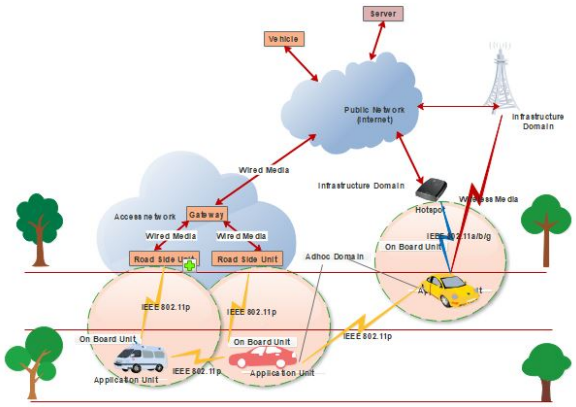

Fig. 1. VANET Architecture

C. *Road Side Unit (RSU)*

RSUs ae stationary unit mounted along roadside. RSU exchanges information through wired or wireless communication medium. For exchanging the information, VANET uses Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) modes. In V2V, vehicles may exchange information directly to another nearby vehicles using single hop technique or using multi-hop technique with the help of intermediate vehicles. In general, safety related messages are transmitted in single-hop fashion, on the other hand, non-safety related messages are transmitted in multi-hop fashion.

For this, communication media must have low latency and high transmission rate. In general, V2V mode is used for broadcasting for emergency messages such as emergency braking, collision deceleration, bottleneck alert, etc. Sometimes, V2V communication is also in a cooperative driving. On the other hand, V2I vehicles exchanges information with fixed RSUs using GSM, UMTS or WiMAX networks.

III. CHARACTERSTICS OF VANETS

VANET, special class of MANET (2), differs from MANET. The characteristics of VANET are as follows:

A. Dynamic topology

The road topology and layout are fixed and the speed and direction of vehicles changes according to it. thus, the network topology in VANET varies according to the roads and keep on changing at rapid rate.

B. Impending Large Network Size

The size of network may be large as the number of the nodes may vary involving vehicles of one city to several cities.

C. Security v/s privacy trade-of

Though security is the prime concern but the privacy of the driver is to be maintained. So, for the sake of the privacy of the driver, some kind of anonymous naming system can be used.

D. Hard time deadline

While delivering the security related messages, the delay in the delivery of the message may create havoc. Thus, the message transfer in VANET should have hard deadline.

E. Unconstrained power, computational and storage resources

VANET requires that nodes must have unconstrained amount of power as well as computational and storage capacity.

F. Intermittent Connectivity

The high mobility of the nodes may result disconnect thus creating very frequent disconnections.

G. Different models forming Routing protocol

The routing protocols for VANET depends upon the patterns formed by various traffic signals, speed limits, highway infrastructure, the congestion available on the roads.

IV. ATTACKS ON VANET

With the growth of network in VANET, security and the privacy are the major issues that must be addressed properly. VANET architecture is susceptible to various attacks (3) such as unauthorized access; fake message causing traffic jam, leaking of private information illegal use, eavesdropping, and protocol tunneling, etc. In order to discuss the possible attacks, we need to first identify the various types of attackers. Attackers may be categorized as follows:

A. Insider v/s Outsider attackers

The authenticated members of network, known as Insiders, have full knowledge about the network and hence are very dangerous whereas outsiders are the intruders have the limited competence to attack.

B. Active v/s Passive attackers

Active attackers are the those who attempt to modify the network resources or disturb their normal operation. They either generate signals or packet with an intension of some alteration of the original data or the creation of a false stream. whereas passive attackers only listen the network traffic to identify the information/pattern that is being transmitted. It is very difficult to detect passive attacks as compared to active attacks.

C. Malicious v/s rational attackers

Malicious attackers just check the security mechanisms of the network and don't have any personal benefit; whereas rational attackers may have the personal profit that's why they attack on the network.

The security mechanisms used in VANET include PKI (Public Key Infrastructure) (4), TESLA (Timed Efficient Stream Los-Tolerant Authentication) (5), TESLA++ (Modified version of TESLA) (6), ECDSA (Elliptic Curve Digital Signature Algorithm) (7) VAST (VANET Authentication using Signatures and TESLA++) (8) etc. Most of the researchers are taken above security mechanisms in consideration.

V. SECURITY REQUIRMENTS IN VANET

The security [9-18] requirements in VANET are summerized as follows:

A. Authentication

Authentication ensures that the messages to be sent by the legitimate nodes only and hence no unauthenticated node or adversary can be capable of sending the message.

B. Availability

Availability ensures that the information must be available to the users as and when required. Moreover, for specific applications the response time must be very quick, as any delay in delivering the message will make the message worthless.

C. *Message Integrity*

It ensures that the message is unaltered during the transmission and the messages received by the driver are generated by the legitimate node.

D. *Message Non-Repudiation*

It prohibits a sender from denying that he or she has not sent the message. However, everyone else cannot identify the sender rather than only authorities should be allowed to identify who has sent the message.

E. Entity authentication

It allows to checks whether the sender who has send the message is presently within the network. and also give assurance to the driver that the sender has send the message within a very short period.

F. Access control

Authorization specifies what a node can do. It is required to enforced the access control which state that all nodes will function according to the roles and privileges assigned. i.e. a node is allowed to perform a function only if a node is authorized for that.

G. Message Confidentiality

The message transmitted must be confidential i.e. free from alteration by intruders. Some nodes want to communicate secretly. But no one other than the law enforcement authority cannot do that. An example would be, to find the location of a criminal or a terrorist.

H. Privacy

Privacy ensures about unauthorized access of the private information of the driver. Location privacy assures that the past or future locations of vehicles cannot be determined in any case. Though, the various law enforcement authorities can trace user identities to determine criminal responsibilities

I. Real time guarantees

The message transmitted should have the hard deadline of delivery which is essentially required in safety related applications.

VI. AUTHENTICATION IN VANET

To provide secure and trusted V2V and V2I communication, the authentication [20-21] ensures messages from the legitimate users of VANET. In order to identify and to protect from un-authorized entities several authentication schemes were proposed by various researchers. Many authentication schemes have been proposed to provide either of Node authentications to provide node level authentication and message authentication to provide message level authentication. All of them used the principle of signing and verifying the message using one of the cryptographic techniques available. Mainly, Authentication schemes in VANET are based on: (i) Signature (22-23), (ii) Cryptography (24-25) and (iii) Verification (26-27). Fig 2. gives the classification of authentication schemes. Various cryptography authentication schemes are there based on asymmetric and symmetric key and ID-based cryptographic methods. Signature may be generated for single user or for group thus resulting the authentication schemes categorized into single user and group user signature authentication schemes. Verification based authentication schemes are divided into batch verification and cooperative massage authentication-based schemes. Various parameter namely computation overhead, communication overhead, collision detection, end to end delay can be used to analyze the performance of the various authentication schemes available.

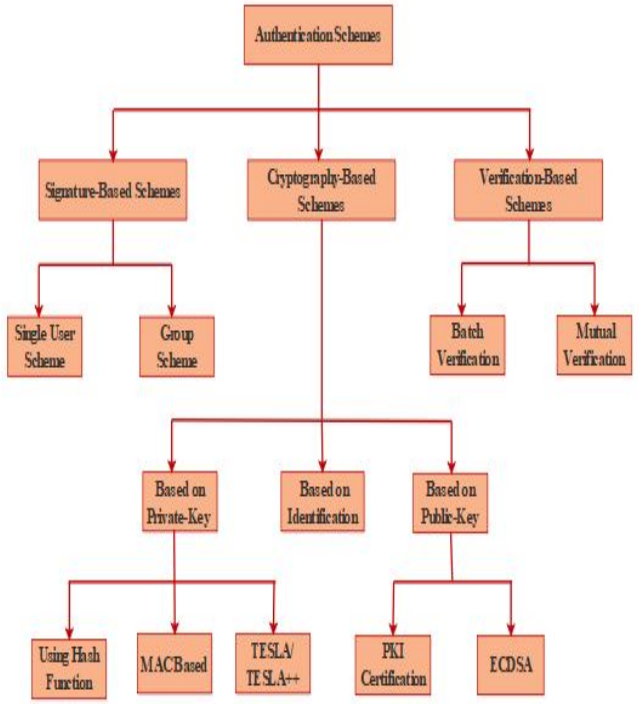

Fig. 2. Classification of authentication schemes in VANETs

VII. CONCLUSION

VANET focuses on safer, convenient, and pleasant by reducing traveling time, road congestion etc. The main focus of paper is to describe VANETs communication architectures, its various components, challenges, security attacks along with security requirements and various authentication schemes in VANET. The basic objective of paper is to introduce the VANET with respect to research point of view and motivate to researchers to explore areas in Intelligent Transportation System in smart cities.

REFERENCES

[1] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," IEEE Communications Magazine, vol. 46, no. 6, pp. 164–171, 2008.

[2] G. Karagiannis, O. Altintas, E. Ekici et al., "Vehicular networking: a survey and tutorial on requirements, architectures, challenges, standards and solutions," IEEE Communications Surveys and Tutorials, vol. 13, no. 4, pp. 584–616, 2011.

[3] S.S. Tangade, and S.S. Manvi, "A survey on attacks, security and trust management solutions in VANETs", Proc. 4th IEEE International Conference on Computing, Communications and Networking Technologies, ICCCNT-2013, pp.1-6.

[4] G. Calandriello, P. Papadimitratos, J.P. Hubaux, A. Lioy, "Efficient and robust pseudonymous authentication in VANET ", in: Proc. 4th ACM International Work-shop on Vehicular Ad Hoc Networks, September 2007, pp .19–28.

[5] Sarah Oubabas, Rachida Aoudjit, Joel J. P. C. Rodrigues, and Said Talbi," Secure and stable Vehicular Ad Hoc Network clustering algorithm based on hybrid mobility similarities and trust management scheme", Elsevier , Volume 13, July 2018, pp. 128-138.

[6] A. Studer, F. Bai, B. Bellur, A. Perrig," Flexible, extensible, and efficient VANET authentication ", Journal of Communication and Networks, Volume 11 Issue 6, December 2009, pp. 574–588.

[7] R. Kalkundri, S.A. Kulkarni, "A secure message authentication scheme for VANET using ECDSA", in: Proc. 4th International Conference on Computing, Communications and Networking Technologies, ICCCNT, January 2014, pp.1–6.

[8] M. Sivasakthi and S. Suresh, "Research on vehicular ad hoc networks (VANETs): an overview", Journal of Applied Sciences and Engineering Research, Volume 2, Issue 1, February 2013, pp. 23–27.

[9] Shihan Bao, Waleed Hathal, Haitham Cruickshank, Zhili Sun, Phillip Asuquo, and Ao Lei, "A lightweight authentication and privacy-preserving scheme for VANETs using TESLA and Bloom Filters", ScienceDirect ICT Express, Volume 4, Issue 4, December 2018.

[10] Mingzhong Wang, Dan Liu, Liehuang Zhu, Yongjun Xu, and Fei Wang, "LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication", Springer-Verlag Wien 2016, Volume 98, Issue 7, July 2016, pp: 685–708.

[11] Jie Li, Huang Lu, and Mohsen Guizani , "ACPN: a novel authentication framework with conditional privacy preservation and non-repudiation for VANETs", IEEE Transactions on Parallel and Distributed Systems , Volume 26, Issue 4, April 2015, pp. 938-948.

[12] Xiaodong Lin, Xiaoting Sun, Xiaoyuc Wang, Chenxi Zhang, Pin-Han Ho, and Xuemin (Sherman) Shen, "Timed Efficient and Secure Vehicular Communications with Privacy Preserving", IEEE transactions on wireless communications, Volume 7, Issue. 12, December 2008, pp: 4987-4998.

[13] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, and Xuemin (Sherman) Shen, "An Efficient Message Authentication Scheme for Vehicular Communications", IEEE transactions on vehicular technology, Volume 57, Issue 6, November 2008, pp. 3357 - 3368.

[14] A. Wasef, X. Shen, "EMAP: expedite message authentication protocol for vehicular ad hoc networks", IEEE Transactions on Mobile Computing. Volume 12 Issue 1, January 2013, pp. 78–89.

[15] Arun Kumar Tripathi, R. Radhakrishnan and J. S. Lather, "Secure and Optimized Authentication Scheme in Proxy Mobile IPv6 (SOAS-PMIPv6) to reduce Handover Latency", International Journal of Computer Network and Information Security, vol. 9, issue 10, 2017, pp. 1-12.

[16] Arun Kumar Tripathi and Surendra Kumar Tripathi, "A Qualitative Analysis of Secured Handover Management Schemes for Mobile IPv6 enabled Networks", International Conference on Innovative Applications of Computational Intelligence on Power, Energy and Controls with their impact on Humanity, 2018, pp. 1-8.

[17] A. Studer, F. Bai, B. Bellur, A. Perrig," Flexible, extensible, and efficient VANET authentication", Journal of Communication and Networks, Volume 11 Issue 6, December 2009, pp. 574–588, doi:10.1109/JCN.2009.6388411

[18] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie, "Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trend", International Journal of Distributed Sensor Networks Volume 2015, pp. 1-11, doi.:10.1155/2015/745303.

[19] Guo, J.; Baugh, J.P.; Wang, S. A Group Signature Based Secure and Privacy-Preserving Vehicular Communication Framework. In Proceedings of the Mobile Networking for Vehicular Environments (MOVE) Workshop in Conjunction with IEEE INFOCOM, Anchorage, AK, USA, 11 May 2007.

[20] Amit Kumar Goyal, Gaurav Agarwal, Arun Kumar Tripathi, "Network Architectures, Challenges, Security Attacks, Research Domains and Research Methodologies in VANET: A Survey" Internation Journal of Computer Network and Information Security, volume 11, issue 10, Oct 2019, pp 37-44.

[21] Arun Kumar Tripathi, R. Radhakrishnan and J. S. Lather, "Secure and Optimized Authentication Scheme in Proxy Mobile IPv6 (SOAS-PMIPv6) to reduce Handover Latency", International Journal of Computer Network and Information Security, volume 9, issue 10, 2017, pp. 1-12.

[22] Lianhai Liu, Yujue Wang, Jingwei Zhang, and Qing Yang, “A Secure and Efficient Group Key Agreement Scheme for VANET”, MDPI Sensors, Volume 19 Issue 3, January 2019, pp: 1-14.

[23] J. Jenefa, and E. A. Mary Anita, “Secure Vehicular Communication Using ID-Based Signature Scheme”, ACM, Wireless Personal Communications: An International Journal, January 2018, Volume 98, Issue 1, pp 1383–1411 , doi:10.1007/s11277-017-4923-7.

[24] Vighnesh, N.V.; Kavita, N.; Shalini, R.U.; Sampalli, S. A Novel Sender Authentication Scheme Based on Hash Chain for Vehicular Ad-Hoc Networks. In Proceedings of the IEEE Symposium on Wireless Technology and Applications (ISWTA-2011), Langkawi, Malaysia, 25–28 September 2011; pp. 25–28.

[25] Taeho, S.; Jaeyoon, J.; Hyunsung, K.; Sung-Woon, L. Enhanced MAC-based efficient message authentication scheme over VANET. In Proceedings of the 7th International Multi-Conference on Engineering and Technological Innovation, IMETI, Orlando, FL, USA, 15–18 July 2014; pp. 110–113.

[26] Vijayakumar, P.; Chang, V.; Deborah, L.J.; Balusamy, B.; Shynu, P.G. Computationally efficient privacy preserving anonymous mutual and batch authentication schemes for vehicular ad hoc networks. Futur. Gener. Comput. Syst. 2016, 78, 943–955.

[27] lina, L.; Castellà-Roca, J.; Vives-Guasch, A.; Hajny, J. Short-Term linkable group signatures with categorized batch verification. In Proceedings of the International Symposium Foundation and Practice of Security, Montreal, QC, Canada, 25–26 October 2012; pp. 244–260.