VANET's Security, Privacy and Authenticity: A Study

Asma Parveen[1], Syed Thouheed Ahmed[2*], Raafiya Gulmeher[1], Ruksar Fatima[1]

[1]KhajaBandae Nawaz University, Kalaburgi, India
[2] Dr. T Thimmaiah Institute of Technology, Kolar, India
syed.edu.in@gmail.com

Abstract. Vehicular Adhoc Network's (VANET) has gained popularity and focus of research in recent days, due to their distinctive characteristics like frequently changing topology with predictable mobility. Much attention of Industry and academia both are attracted towards VANETs. Security of data is a crucial aspect of safety related applications of vehicular networks due to their distributed nature and mobility of vehicular ad hoc networks VANETs a critical challenge arises such as collisions of uncoordinated data transmissions and unstable topologies. This paper presents the basic vehicular ad hoc network's architecture then shows research issues. This paper provides a survey of research perspective of main aspects of VANETs such as general authentication and security techniques.

Keywords: VANETs, OBU, RSU, Secure communication

1 Introduction

Vehicular Adhoc Networks (VANETs) are Mobile Adhoc networks (MANETs) with a special type of wireless communication within short range. VANETs are self-organizing and distributed networks which have been designed for communication between the moving vehicles and road side infrastructures. In 2001 VANETSs were introduced and mentioned [1] for mobile adhoc car-to-car networking and communication applications. One of the key part of the Intelligent Transportation systems (ITS) framework is VANETs.

VANETs are being used for many applications such as providing routing information to the other vehicles efficiently, accidents, emergency warning, , broadcasting road conditions, and managing lane-changing etc. This wireless network technology is a promising one which can encounter critical vehicular safety situations. Due to these applications requirement VANETs experience fast development, as well as transpires self-driving car technologies. Transmission of a secure data is crucial in VANETs. Hence implementing data security is a critical challenge due to the frequent and rapid change of the topology in the Adhoc networks.

ICASISET 2020, May 16-17, Chennai, India

DOI 10.4108/eai.16-5-2020.2304038

Sensor devices are used to monitor the network conditions in VANET. These Sensor devices are capable of transmitting the data to others vehicles and collecting relevant information. Size of the sensor devices are very small, have low cost and can be deployed in very large numbers in the VANET. Vehicles are capable of providing themselves continuous power transmission to support functions like communication, significant computing, and sensing[2].

2 Communication in VANETs

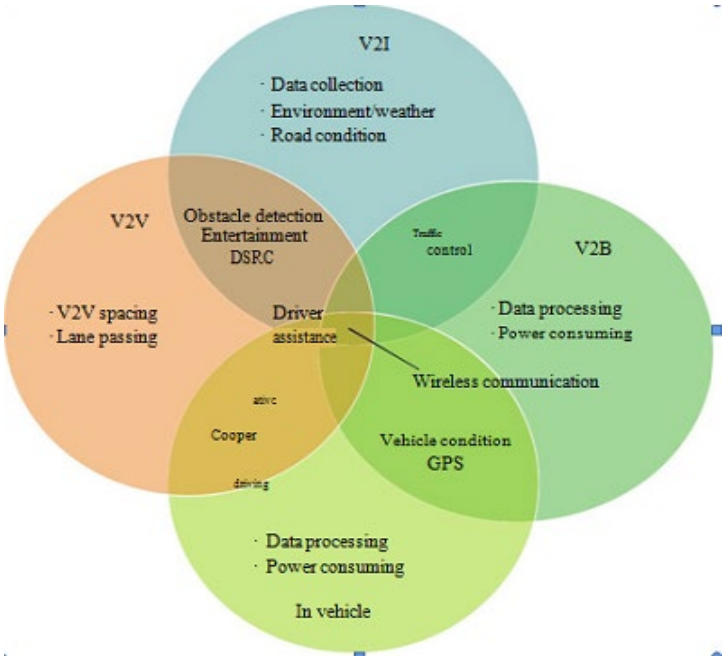

Fig.1. Key role of each communication type.

The various types of communication in VANETs can be divided in to four types. Each category is closely related to components of VANETs as discussed above. Fig. 3 gives the key Role of each communication type[1]

In-vehicle communication: In VANETs research, the vehicle communication plays a most important role, which refers to in-vehicle domain. The performance of a vehicle such as if driver is fatigue or if he feels drowsiness, these things can be encounter by vehicle communication system, that gives most for driver as well as public.

*Vehicle-to-vehicle (V2V) communication :*With the help of Vehicle-to-vehicle (V2V) communication, the drivers can exchange the data, information and warning messages that really assist the driver.

*Vehicle-to-road infrastructure (V2I) communication :*Another useful research field of VANETsis Vehicle-to-road infrastructure (V2I) communication. With this

communication, the drivers can get real time traffic and weather updates and provides monitoring and environmental sensing features.

*Vehicle-to-broadband cloud (V2B) communication :*With the help of Vehicle-to-broadband cloud (V2B) communication, the vehicles can communicate each other using wireless broadband mechanisms such as 3G/4G , because the broadband cloud will be having both information regarding traffic and monitoring the data , such type of communication will be most useful for tracking the vehicles and assisting to the drivers.

3 Security and privacy

Now a day's lot of personal information and vehicular trajectory data are stored us hybrid broad applications,which can disclose individual habits, activities and trails of system connection. The threats such as exploitation of messages or traces the trajectory of vehicles by attacker have to be overcome before communication architecture in VANETs is deployed to increase the reliability ,dependability and individual`s acceptance of the VANETs system,

Formerly many approaches have been proposed to address the security and privacy issues. Most of the literatures pay more attention to two important aspects such as architecture of VANETs and communication over it[20].

3.1 Security goals

The objectives to guarantee or secure VANETs are same as that for securing any system. The fundamental point is to give verification, trustworthiness, accessibility, privacy, and non-renouncement. Verification is affirmation that their conveying element is the one that it professes to be and empowers a hub to guarantee the personality of their imparting hub. Main task is to check , vehicle status i.e whether it is approved or not. It is vital that the hub getting information is sent from a substantial sender. Privacy manages the security of information from unapproved disclosure. Classification of information guarantees that the information is n't spilled or revealed to unapproved hubs or vehicle in the system. For eg.the data being transmitted is from enrolled vehicles . Revelation of this information may prompt recognizable proof of essential data. Integrity is especially vital for basic security. Data can be deleted or turned out to be out of reach, bringing about loss of accessibility. This implies individuals who are approved to get data can't get what they require.

Accessibility guarantees that the frame work , works appropriately and their administration is given to approved clients alone when it is required. An opponent refuse any assistance to legitimate hubs by stick their channel, by disturbing their routing rules, by depleting battery of intensity, and so forth. For eg. At essential time the services are given to vehicle by unit of road side . The elements involved in exchange of data are being participated in all or part of the transmission are provided a protection against rejection.. For eg. Subsequent to communicating something specif-

ic, the vehicle ought not deny having those sent message is called as sender non-renouncement. Additionally after getting a message, the vehicle should not deny having those gotten message is called as recipient non-renouncement [16].

3.2 Authentication Techniques in VANETs

Authentication is nothing but verification of a user's identity before granting permission for the access to the network. It is considered to be one of the basic requirement of defense against intruders.

There are different methods used to authenticate messages sent over the VANETs":

Node level authentication proves that the message is originated from certain node.

Group level authentication proves that the message is originated from a certain group of nodes.

Unicast authentication proves the message is sent to only one node.

Multicast authentication proves the message is sent to many nodes[18].

Broadcast authentication proves that the message is sent to all nodes in the network.

On the bases of trust, advanced signature and symmetric cryptography authentication techniques in VANETs are as follows. Trust based confirmation methods are Trust Extended Authentication Mechanism (TEAM) and Chameleon Hashing for shared and unknown validation. Validation methods in view of advanced signature are Elliptic Curve Digital Signature Algorithm (ECDSA) and Challenge Response Authentication utilizing Digital Signatures. Finally authentication techniques based on symmetric cryptography are Timed Efficient Stream Loss-Tolerant authentication (TESLA) and TESLA++.

4 Related work

4.1 The security, privacy and authenticity of VANETs

[10]The authors proposed a new security architecture mainly focusing on providing security to the wireless communication part of the system in the vehicles and on improving users privacy. Hence different from architecture it mainly focuses on secular vehicular communication algorithms and schemes[7,11]. A communication scheme proposed by Raya and Hubaux deals with the communication parties establishes sharing session key for longer time secure communication. Applications that are non-safety related are ignored whereas the application related to safety are given more importance in this scheme[5,12]. In[11], the authors mainly focuses on a scheme that was proposed by Raya and Hubaux for advanced secure communication, that extends the session key which can be used in applications that are non-safety

related and uses two session keys namely group keys and pairwise keys. In[13] ,the authors explains several security solutions which have been proposed in depth,like CA ,signature of group and VPKI.

[16]VANETs security is a major critical issue as the transmission of data is over wireless network. It includes short range radios that are located on road side units, vehicles and central authorities that are mainly held for managing the responsibilities and their identity registration. Several academic institutions, governments and industries in various parts of the world uses projects of Vehicular Adhoc Network. But VANETs are the most vulnerable to invaders that ranges from inactive to active attacks such as eavesdropping, tampering, interfering and spamming. This paper mainly focus on the various attacks from the VNETs and gives a most holistic protocol for transmissions of the data in more secure manner and to detect the misbehaviors of authorized users. In proposed work, the vehicle should first get registered with the nearby Road Side Unit(RSU) and then authentication is provided by the RSU using the certificate of RSU. The data is provided only after the successful authentication otherwise it will be blocked. The plausibility checks are also used to detect authorized users if they send false event. The main aim behind this paper is to give a lightweight protocol and secure data communication and the transmission against both outsider and insider attacks. Providing lightweight protocol for secure transmission of data against all kinds of insider and outsider attacks is the main motive of this paper.

[17] This paper proposes an approach to provide security to vehicular networks while privacy is being maintained. This approach makes effective use of group signature with respect to public keys are maintained by members. As the signers are unidentified in the group from which they sign so this way scheme is providing privacy. In addition, if two messages are signed by an individual, it has no link between the messages sent by the same member of the group. In other words signers cannot be identified, whether the sender of two messages is the same member or different members of the group. This proposed scheme presents anonymity, aurhenticity, accountability and data integrity.

[14]vehicle registration is done with the Certificate authority anf CA is responsible for issuing keys and vehicular node registers for its identity. VANETsthat has been using game theory for sensing attacks is not enough for security requirements. Hence this mechanism propose recently generates appropriate framework for security with an extended defensive mechanism support for VANETs which improves security. The behavior of vehicles are monitored by the neighboring vehicles and nearby RSU(Road Side Unit). A tamper proof device is attached with the vehicles and it has to check the vehicle's certificate validation. If a problematic certificate is found then revocation of Certificate happens, which avoids receiving messages by the other vehicles from the problematic certificates. Presently the responsibility of broadcasting Certificate Revocation List (CRL) for revoking certificates and tracking of the vehicle is of Road Side Unit (RSU). However this strategy causes burden on RSU and consumption of control channel by CRL. In this method of certificate revo-

cation , it will check the validity of senders certificate upon receiving a message by the vehicle. If sender does not hold a valid certificate then message from it will be ignored and if the sender do not have a certificate at all then receiver reports about the sender to the RSU. After checking the correctness of the message RSU will assign sender a valid certificate (VC), or else an invalid certificate (IC) is issued by RSU to the node and registers the ID of the vehicle to the CRL.

[15] This paper proposes two modes for basic communication -communication between OBUs with each other and with other infrastructure Road Side Units. As the communication between vehicles is through wireless channel, so there may many types of attacks take place easily such as manipulation of messages, insertion of false information etc. the system proposes Dual group key management scheme where a group key is assigned to the set of users which can also be updated during operations. By updating a small amount of information an addition or revocation of the user from group in VANET is performed efficiently in this scheme. Here various services are provided by a Trusted Expert (TE) for the online customer through Vehicular Networks. Hence it is necessary to maintain data confidentiality and authenticity that are being exchanged between TE and VANET nodes. The security issue is addressed by classifying users as unauthorized, primary and secondary by the TE. This paper proposes implementation of Dual Authentication scheme for providing high level security that prevents entering of unauthorized vehicles in the VANET.

5 Conclusion

Developing techniques ensuring Security, Privacy and Authenticity is an urgent need for implementation of a secure communication over Vehicular Adhoc Networks (VANETs). This paper presents a survey on VANET's Security, Privacy and Authenticity. An Introduction to VANETs architecture, including network components and VANET's domain view, communication types, security goals, methods and a brief discussion on authenticity techniques. It also presents research perspective for the vehicular ad hoc networks with respect to authentication, security and management under larger circumstances in increasing demand of technology.

References

1. M. Sivasakthi and S. Suresh. (2013) "Research on vehicular ad hoc networks (VANETs): an overview," Journal of Applied Sciences and Engineering Research, vol. 2, no. 1, pp. 23–27.
2. T. Kosch, C. Schroth, M. Strassberger, and M. Bechler, (2012), Automo-tive Internetworking, Wiey, New York, NY, USA.
3. M. Raya and J.-P. Hubaux, (2007), "Securing vehicular ad hoc net-works," Journal of Computer Security, vol. 15, no. 1, pp. 39–68.
4. F. Dotzer, "Privacy issues in vehicular ad hoc networks, (2005), " in Proceedings of the 5th International Workshop on Privacy Enhancing Technologies (PET '05), pp. 197–209.

5. J. M. de Fuentes, A. I. Gonzlez-Tablas, and A. Ribagorda, (2010), Overview of Security Issues in Vehicular Ad-Hoc Networks,.
6. F. Kargl, L. Buttyan, D. Eckhoff, P. Papadimitratos, and E. Schoch, (2011), Working Group on Security and Privacy, Karlsruhe Institute of Technology.
7. M. Gerlach, A. Festag, T. Leinmller, G. Goldacker, and C. Harsch, (2007), "Security architecture for vehicular communication," in Proceedings of the 5th International Workshop on Intelligent Transportation (WIT '07).
8. P. Papadimitratos, L. Buttyan, T. Holczer et al., (2008) ,"Secure vehicular communication systems: design and architecture," IEEE Com-munications Magazine, vol. 46, no. 11, pp. 100–109.
9. N. W. Wang, Y. M. Huang, and W. M. Chen, (2008), "A novel secure communication scheme in vehicular ad hoc networks," Journal Computer Communications, vol. 31, no. 12, pp. 2827–2837.
10. M. Raya and J.-P. Hubaux, , (2005), "The security of vehicular ad hoc networks, " in Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '05), pp. 11–21.
11. G. Samara, W. A. H. Al-Salihy, and R. Sures, (2010), "Security issues and challenges of vehicular ad hoc networks (VANET)," in Proceedings of the 4th International Conference on New Trends in Information Science and Service Science (NISS '10), pp. 393– 398, Gyeongju-si, Republic of Korea.
12. D.Yamini1 and J. Jayavel2, (2015), Efficient Data Transmission And Secure Communication In Vanets Using Node-Priority And Certificate Revocation Mechanism" , International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 02 Issue: 02 | p-ISSN: 2395-0072.
13. Sundareswaran, Veena&Aravindhar, John. (2018). A Secured Data Transmission in VANET using Dual Group Keys and Frequent Data Identification. Research gate publication.
14. TamilSelvan ,Komathy Subramanian , RajeswariRajendiran, (2013), "A Holistic Protocol for Secure Data Transmission in VANET ", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue .
15. JinhuaGuo, John P. Baugh, and Shengquan Wang, "A Group Signature Based Secure and Privacy Preserving Vehicular Communication Framework", Department of Computer and Information Science, University ofMichigan-Dearborn.
16. Remyakrishnan.P1, Tripti C, (2014), " Authentication techniques in VANETs-A Survey", International Journal of Advanced Research in Computer Science, Volume 5, No. 4, (Special Issue).
17. Uzma Farheen1, Dr.Ruksar Fatima,(2017), "Vehicular Protected Data Transmission over Dual Authentication Algorithm", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 5, Issue 6.
18. Kumar, S.S., Ahmed, S.T., Vigneshwaran, P. et al. Two phase cluster validation approach towards measuring cluster quality in unstructured and structured numerical datasets. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02487-w
19. Ahmed, S.T., Sankar, S. & Sandhya, M. Multi-objective optimal medical data informatics standardization and processing technique for telemedicine via machine learning approach. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-02016-9
20. Ahmed, S.T., Sandhya, M. & Sankar, S. TelMED: Dynamic User Clustering Resource Allocation Technique for MooM Datasets Under Optimizing Telemedicine Net-

work. Wireless PersCommun 112, 1061–1077 (2020). https://doi.org/10.1007/s11277-020-07091-x

21. K. Vijayakumar, Chokkalingam Arun, “Integrated cloud-based risk assessment model for continuous integration”, Int. J. Reasoning-based Intelligent Systems”, Vol. 10, Nos. 3/4, 2018.
22. J. Dafni Rose, K. Vijayakumar and S. Sakthivel, “Students performance analysis system using cumulative predictor algorithm”, Int. J. Reasoning-based Intelligent Systems, Vol. 11, No. 2, 2019.