International Journal of Grid and Distributed Computing
Vol. 9, No. 7 (2016), pp.301-306
http://dx.doi.org/10.14257/ijgdc.2016.9.7.30

Vehicular Ad Hoc Networks: Hashing and Trust Computation Techniques

Pallavi Agarwal[1] and Neha Bhardwaj[2]

[1]*Research Scholar, CSE & IT Dept., Madhav Institute of Technology & Science, Gwalior, India*
[2]*Assistant Professor, CSE & IT Dept., Madhav Institute of Technology & Science, Gwalior, India*
[1]*pallaviagarwal015@gmail.com,* [2]*bhardwaj.neha08@gmail.com*

Abstract

Vehicular ad-hoc networks (VANETs) technology has come out as an important research field over the last few years. VANETs are the likely an influencing approach to provide safety of driver and other applications for the traffic conditions as well as passengers. Being dynamic in nature, it establishes the network, according to the situation and need of the users and provides reliable communication among the vehicles. Due to its great benefits, it is highly vulnerable to various attacks and security in VANET should be taken into consideration. This paper presented the security attacks between vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Many research works have been done to improve the performance and security of this network. The main aim of this paper is the security using hashing and techniques to calculate the trust in VANETs.

Keywords*: Vehicular Adhoc Network, Attacks, Hashing, Road Side Unit, On Board Unit, Security, Trust Computation.*

1. Introduction

Vehicular ad hoc network (VANET) may be a specific form of Mobile Ad-Hoc Network (MANET) that provides communication between the vehicles and the vehicles and roadside infrastructure. VANET differs from MANET because it provides higher quality of nodes, larger scale networks, geographically unnatural topology and frequent network fragmentation. There is not any fixed infrastructure networks and have confidence the vehicles themselves for implementing any network practicality. A VANET may be a redistributed network as each node performs the functions of host and router. It is the technology [1] of building a secure network between vehicles; i.e. vehicles communicate to every alternative and pass information to another vehicle. The most advantage of VANET communication is the enhanced driver's safety by virtue of exchanging warning messages between vehicles. VANET security is crucial as a result of a poorly designed VANET is susceptible to network attacks and this successively compromises the protection of drivers. Security systems have to make sure that transmission comes from an authorized source and not tampered in the route by different sources.

Accidents can be avoided if the vehicles follow the traffic rules and road limit. The malicious node could spread out spam messages and send false messages to make issues like false information of collision and theft and heavy traffic. VANET has become a growing space of analysis. Researchers have put lots of efforts [2] in this field to create robust plan and the implementation of VANET network environment. With the increasing quantity of the vehicles, roads can probably get more rushful. Thus, it is very necessary to extend road safety and reduce traffic congestion. In VANET, the communication is established by transferring the updated information about the road and traffic conditions

ISSN: 2005-4262 IJGDC

to avoid road accidents and efficient result of traffic. VANET is employed to give the protection and traffic reports to the users about traffic jams, earthquake, tsunami, etc. for lessening the road accidents, fuel consumption and provides safe driving atmosphere.

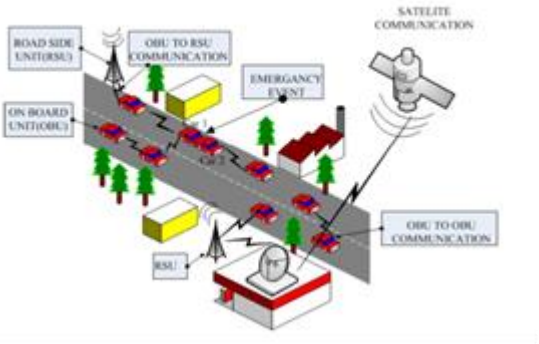

Figure 1. Overview of VANET

In intelligent transportation systems, every vehicle broadcast data [3] to the vehicular network or transportation company by having the role of sender, receiver, and the router by using the data to validate safe, free-flow of traffic. Vehicles should be equipped with some variety of radio interface or Onboard Unit (OBU) for communication to occur between vehicles and Road Side Units (RSUs) that enables adhoc short-range wireless networks to be created [4]. Vehicles should even be fitted with hardware that allows the data with the exact position of the vehicle such as global Positioning System (GPS) or a Differential Global Positioning System (DGPS) receiver. RSUs are fixed and are connected to the backbone network, which should be in place to promote communication. The distribution and amount of roadside units should be relying on the communication protocol is to be used. However, some protocols need roadside units to be allocated equally throughout the full road network, some need roadside units solely at intersections, while others need roadside units solely at region borders. Though it's safe to assume that infrastructure exists to some extent and vehicles have access to that periodically.

The possible communication structure of intelligent transportation systems includes inter-vehicle and vehicle-to-roadside communications. Inter-vehicle and vehicle-to-roadside communications depend on correct and up-to-date data concerning the surrounding geographical area, which in turn, needs the employment of accurate positioning systems and elegant communication protocols for exchanging data. In this network, the communication medium is shared, highly unreliable, and with restricted bandwidth. The elegant communication protocols should guarantee quick and reliable delivery of information to all or any vehicles within the section.

2. Literature Review

Uzma Khan et al. [5], surveyed a method to detect misbehavior or malicious nodes. It creates a reliable and secure environment for communication. Verma et al. [6], proposed secure group communication method in which vehicles communicate by two ways. In the first way, they authenticate y RSUs and secondly communicate by creating a group. Raya et al. [7], presented a method to protect the privacy of vehicles from the other vehicles by generating fake identity of vehicles. Jorge h. et al. [8], proposed a scheme to detect the behavior of the neighbor node by watching them continuously. It used intrusion detection of a watchdog to differentiate the malicious node. Chuang et al. [9], proposed a scheme TEAM to enhance the authentication among the vehicles in less time and compute the keys by using hashing techniques. Monir et al. [10], proposed a mechanism to establish the trust by using trust management among the nodes. Every node is monitored and then calculate the trust value of that node.

3. Security Attacks in VANET

Security attacks are performed in VANET to violate the privacy and also harm the vehicle's driver [11].

3.1. Denial of Service (DOS)

DOS is very common attack to block the network and unable the users to use the services. This attack is very harmful for the vehicles as it stops the communication totally. The whole network gets jammed by this attack and this decrease the reliability of the network.

3.2. Sybil Attack

Sybil attack performs by creating multiple identities of the single vehicle and sending the messages by the node. But the receiver thinks that they are getting messages from the multiple senders. This creates the confusion of multiple nodes in the network and also increase the routing overhead.

3.3. Eavesdropping Attack

Eavesdropping attack is a passive attack in which the attackers did not perform any changes. This attack is used to violate the confidentiality of the messages. It is very difficult to detect this attack as the attacker only analyze the data like vehicles location or identity.

3.4. Fabrication Attack

Fabrication attack is performed to broadcast the false messages in the network. An attacker changes the data and then transfer it to other vehicles and send it by using another identity [12].

3.5. Impersonation Attack

Impersonation attack means the attacker takes the identity of another user and try to impersonate. This attack is very dangerous if they send any false information about the accident happened in any location.

4. Hashing

Hashing is a technique which is used in cryptography for achieving the authentication and integrity of the sender or messages. It is very useful and fast method to ensure the security in the network. It takes an input message of variable length and generates the hash value (or known as message digest) of fixed length.

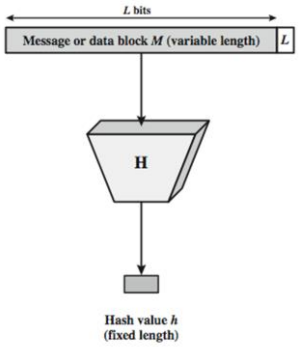

Figure 2. Hashing in Cryptography

There are different variants available according to the need of users in which the key sizes are different and some are fast, but less secure and vice versa [13]. At the sender's side, when user input the message and it produce the hash value (h) then encryption performed to make it more secure. After transmitting it from the secure channel, receiver decrypts it by using the key and generate the hash value of the received message. Then it compared the hash value contained in the message and it creates. If both the values are equal, then it verifies that the data is not altered during the transmission and it is sent by an authenticated user.

5. Trust in VANET

In VANET, each vehicle communicates with other vehicles securely if there is a confidence in that vehicle. It is based on the behavior of the nodes in the network if they forward the message, then they considered to be trustful otherwise malicious [14]. Every vehicle calculates the trust values according to its requirements and this can be vary with the time also. In the beginning, each vehicle has a default value which is increased or decreased with every interaction.

Trust establishment can be done in various ways of creating the trustful environment. Vehicles individually calculate the trust value of other vehicles by sending the messages to the neighbor's node [15]. Figure 3. describes various techniques to establish trust in the network.

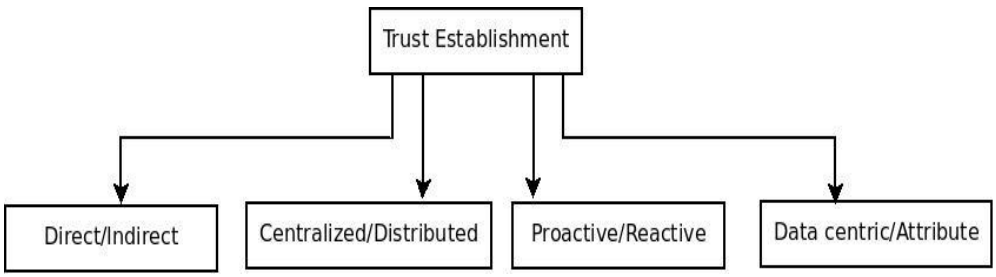

Figure 3. Trust Establishment

6. Conclusion

In Vehicular Ad Hoc Networks (VANET), communication among vehicles should be done by the proper trust establishment to secure messages exchange and reliability. We presented an attack of VANET and hashing to maintain the security by maintaining the integrity of the messages and authentication of sender. In this survey, we discussed some

some trust calculation techniques to secure communicate among the vehicles We mention some important properties that should be archived by proper management of trust for VANET, setting a specific outcome for researchers in this area.

References

[1] S. K. Sood, A. K. Sarje, and K. Singh, "A secure dynamic identity based authentication protocol for multi-server architecture," J. Netw. Comput. Appl., vol. 34, pp. 609–618, (**2011)** March.
[2] F. We and X. Li, "An improved dynamic ID-based remote user authentication with key agreement scheme," Comput. Electr. Eng., vol. 38, pp. 381–387, **(2012)** March.
[3] C. Chen, J. Zhang, R. Cohen, and P. Han Ho, "A trust-based message propagation and evaluation framework in VANETs", International Conference on Information Technology Convergence and Services, **(2010)**.
[4] Ding, Qing, Xi Li, Ming Jiang, and XueHai Zhou, "Reputation-based trust model in Vehicular ad hoc networks", Wireless Communications and Signal Processing (WCSP), International Conference on IEEE, **(2010)**, pp. 1-6.
[5] Uzma Khan, Shikha Agrawal and Sanjay Silakari, "A Detailed Survey on Misbehavior Node Detection Techniques in Vehicular Ad Hoc Networks," Advances in Intelligent Systems and Computing, Vol. 339, pp 11-19, **(2015)**.
[6] Verma, Mayank and Dijiang Huang, "SeGCom: secure group communication in VANETs." In Consumer Communications and Networking Conference, 2009, CCNC 2009, 6th IEEE, pp. 1-5. IEEE, **(2009)**.
[7] Maxim Raya, "The Security of Vehicular Ad Hoc Networks", SASN, Alexandria, Verginia, USA, **(2005)** November 7, pp. 11-21.
[8] Hortelano, Jorge, Juan Carlos Ruiz, and Pietro Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs", Communications Workshops (ICC), IEEE International Conference, **(2010)**, pp. 1-5.
[9] Ming-Chin Chuang and Jeng-Farn Le, "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks", IEEE, **(2013).**
[10] Merrihan Monir, Ayman Abdel-Hamid and Mohammed Abd El Aziz, "A categorized trust-based message reporting scheme for VANETs", Advances in Security of Information and Communication Networks, pp. 65-83.
[11] Hannes Hartenstein, "A Tutorial Survey on Vehicular Ad Hoc Networks", IEEE Communication Magazine, **(2008)** June, pp. 164-171.
[12] Am Shringar Raw, Manish Kumar, Nanhay Singh, "Security challenges, issues and their solutions for VANET", International Journal of Network Security & Its Applications (IJNSA), vol.5, **(2013)** September.
[13] J. Zhang, "A survey on trust management for VANETs", International Conference on Advanced Information Networking and Applications, **(2011)**, pp. 105-112.
[14] Liao, Cong, Jian Chang, Insup Lee and Krishna K. Venkatasubramanian, "A trust model for vehicular network-based incident reports", Wireless Vehicular Communications (WiVeC), IEEE 5th International Symposium on IEEE, **(2013),** pp. 1-5.
[15] J. Zhang, "Trust management for VANETs: challenges, desired properties and future directions", International Journal of Distributed Systems and Technologies, **(2012)**, pp. 48-62.

