Enhance the Security by using Hashing Technique and Trust Values in Vehicular Ad Hoc Networks

Pallavi Agarwal[1], Neha Bhardwaj[2]
[1, 2] Department of Computer Science & Information Technology
[1, 2] Madhav Institute of Technology & Science, Gwalior, India

Abstract- *Vehicular Ad hoc Network (VANET) is the favorable method to enhance the safety of divers and passengers. It becomes a basic element of the Intelligent Transportation System (ITS). It has created by applying the concepts of Mobile Ad Hoc Networks (MANETs) – which is an application of a wireless network for exchanging the data – to the domain of vehicles. They become a main element of intelligent transportation systems. In existing technique drawback is the Authentication Server (AS) gives all the working to Law Executor (LE) means AS send information to RSU, RSU send this information to law executor and then login process start but if LE behave maliciously then this authentication process fail. In our propose work, we calculate the trust of each vehicle's on the basis of their behavior. Each vehicle calculates the trust of its neighbor and send this value to AS by RSU then AS update these values and then broadcast this value by RSU, now all the vehicles have a trust value of its neighboring vehicles so that send the data by using hashing technique and use trusted path to send data source to a destination so that security enhances.*

Keywords- Vehicular Adhoc Network, AODV, Authentication Server, Road Side Unit, Law Executor, Security, Trust value.

I. INTRODUCTION

Vehicular ad hoc network (VANET) is an application of MANET that provides wireless intercommunication with nearby vehicles or the communication between vehicles and fixed roadside infrastructures.

The main aim of this technology is to give drivers more comfortable and more secure driving experience. Based on an automatic information exchange between cars and infrastructures, the drivers could know the road conditions or the details about the parking lots immediately. VANET makes Intelligent Transport System (ITS) become reality [1]. It currently provides a striking field of research that aims at upgrading everyday traffic optimization, safety and comfort. To achieve this, the development of several potential applications is envisioned. Such applications, will not only promise to provide extraordinary benefits, but will also represent important security challenges, especially due to the distinctive features of VANETs. The basics of VANETs will be briefly introduced, followed by a discussion about the routing protocols, VANETs also raise important security and privacy concerns that must be properly addressed. The problem statement and the main contributions of this paper are presented in subsequent sections, and finally at the end, the paper organization is outlined [2].

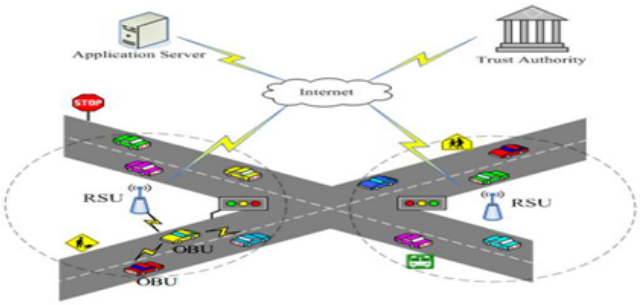

Fig.1 Overview of VANET

A. Architecture of VANET

As shown in Fig. 1, in VANET, there are three components such as On-Board Unit (OBU) which is attached with each vehicle and provide an interface between driver and RSU. OBU directly connected with the infrastructure and other vehicle's OBU. Roadside Units (RSU) which is installed along the roadside by considering it's free from attack and its number may vary with the protocol and a Trusted Authority (TA) or Authentication Server (AS) which is used for installing various security parameters on vehicles and it is more secure than others. The Dedicated Short Range Communications (DSRC) protocol [3] is used for communication among OBUs and RSUs over the wireless channel. The Internet is required to establish the communication. Every vehicle broadcast information to its neighbors periodically related to safety such as traffic alerts, accidents, vehicle speed, etc by which other vehicles can regulate their routes.

RSU is a physical stationary communication device and responsible for gathering and broadcasting critical information such as the nearest parking lots and gas price. RSU can be deployed in an intersection, it acts as a gateway between the Internet and OBU which enables vehicles to

establish connections to the Internet. RSUs also help in coordinating and collecting information about vehicle activities (e.g. red light violations). TA is actually a fully trusted party, it could be the department of government and stores the information of all vehicles. As usual, TA cannot be compromised by an adversary and has sufficient storage. Communication in VANET [15] [16] can either be vehicle-to-vehicle (V2V) (e.g. for sending warning messages) or vehicle-to-infrastructure (V2I) (e.g. When a vehicle gets some data from the TA). V2V communication allows vehicle to send and receive valuable messages; vehicles communicate with each other directly without the help of other infrastructures. V2I indicates one way for OBU to connect with RSU; vehicle can establish connections to the Internet through RSU. The message sent by one vehicle might have important security implications such as accident prevention [4].

B. Routing Protocol

Routing Protocol [18] used to define how to established communication by the routers. It creates the suitable path for sending data by efficiently using an intermediate node. Mainly, three types of protocols are available in the network such as:

1) Reactive Routing Protocol (On-Demand): It is a protocol which is a reactive or on-demand. There is no need to maintain the table to maintain the information of its neighbors. It finds the routes when required or request by sender. Because of this, it is most useful and efficient protocol, which need very less bandwidth. We used AODV in our thesis work.

2) Proactive Routing Protocol (Table-Driven): It contains the list of nodes with their routes. It updates the table periodically if any changes occur in a network. This is very fast because there is no need to find the route again and again.

3) Hybrid Routing Protocol: It is a combination of both reactive and proactive routing protocols. So its use the characteristics of both protocols.

(i) AODV Routing Protocol

AODV [6] is a reactive protocol, which is used to create the route from the source to a destination when it is needed from the source. AODV uses Hello messages to find the path. Each active node periodically broadcasts a Hello message broadcast periodically to monitor the neighbors. If a node doesn't get a response from its neighbor, then it considers that route is not available anymore. Every node of the network maintains a routing table which stores routing information.

(ii) AODV Control Messages

Three types of messages are defined here for route request (RREQ) message, route reply (RREP) message and route error message (RREQ) route discovery and maintenance.

1) **RREQ:** When a source node has a data to send then it broadcast the route request to all its neighboring. This request is forward to other vehicles by intermediate node in the network until it reaches at the destination.

2) **RREP:** When the route request has reached to the destination then a route reply is sent back to the source by the same path which has created for data traversing. It is travelled in unicast form.

3) **RERR:** If there is any breakage in a route then route error message is used. This message is used to inform all nodes so that they become aware of link breakage and update their route table.

II. LITERATURE REVIEW

Raya et al. [5], proposed a method in which every vehicle have their pre-loaded pair of key with their certificates. Each public key certificate contains fake identity to protect the vehicle's identity from others. All messages of traffic are validated by public key based scheme, and all public and private key pair has a small existence to achieve privacy.

Jorge h. et al. [10], proposed intrusion detection techniques by using a watchdog algorithm for the establishment of trust management. When the packet has sent to neighbor then source node monitors that node with ids then maintain the trust value of that node. The drawback of this technique is to create collision in network and monitor that node until that forward or drop. It has to maintain a huge history of monitoring of each neighbor node if it has a great number of neighbor nodes.

Cong et al. [9] propose the method to calculate the trust of the originator or forwarder by determining the correctness of V2V report. When a vehicle observes an incident, it broadcasts an incident report with a V2V message (e.g., accident, traffic congestion, broken bridge) to other vehicles within its communication range. After receiving the incident report by vehicle, they are required to make a

decision by using the trust score of the report originator and forwarders.

Monir et. al [8] proposed a trust management scheme for nodes. Each node is being monitored and a history record of their trust values is evaluated individually according to its interactions. If the trust value is not satisfying the criteria then it is considered as a malicious node.

Chuang et. al [20] proposed a trust extended authentication mechanism to establish an authentication among the vehicles. Hashing and XOR operations are performed which are fast and efficient. They performed various functions performed by vehicles by generating trust over the network.

III. SECURITY REQUIREMENT IN VANET

Security is a very important part of VANET as there are various possible attacks can be performed to harm the driver. There are some requirements have been mentioned which should be achieved.

A. Authentication

Authentication means the sender and receiver should know the identity [7] of each other. Every node should be authenticated before sending any data into the network. Authenticity of the sender is checked before reacting any messages. This improves the security of the network because unauthenticated node can be easily identified and they cannot send any false message in the network.

B. Confidentiality

It is not an important concern in VANET because the messages are exchanged in this network is not sensitive. Only messages should be arrived on time from or to authenticated vehicle. But confidentiality [21] should be achieved by applying encryption on messages and protect it from eavesdropping.

C. Integrity

All messages which are exchanged on the network should be protected against alteration attacks. There should be protection of messages by using hashing or digital signature so that it may not be changed during transmission. A message can be altered in several ways during its transit from source to destinations and all possible attacks must be considered.

D. Availability

When the vehicles communicate then the communication channel should be available. In this network, messages should be arrived on time so that driver took decision at the time. Denial of Service (DoS) attack is mainly performed to block the network and increase the risk of accidents.

E. Privacy

Privacy is an important concern in VANET to protect the driver's personal [13] information. When messages sent by vehicles then other information (such as vehicles identity) should be protected.

IV. TRUST IN VANET

VANET is decentralized in nature so there should be a trustful environment for communication. All vehicles are free to come and exit anytime and there is also a less chance to meet the same vehicle in future again. Trust management [11] [17] should be done in a very effective way. Trust is just a term which is calculated according to the neighbor's behavior. But if any node is untrustful then it can affect the performance of the whole network.

A. Trust can be advantageous by number of ways:

1. Trust can eliminate much of unnecessary communication that may be required. It will improve the performance [14].
2. In view of dependability, choices can be taken faster and less demanding.
3. Trust is a kind of soft security compared to hard security like encryption.

B. Trust can be estimated through a number of ways:

1. Direct Experience: It is based on direct experience.
2. Communicated Experience: It is created for recurrent communication that has been done till now between service provider and user.
3. Social Information: It is purely based on social information.
4. Reputation: It is based on the position of trustee in the society.

V. PROPOSED METHOLOGY

With the reducing costs of hardware, wireless communication technologies allow both V2V and V2I communications for information exchange. Such a network is called Vehicular Ad Hoc Network (VANET) which is very

important for various road safety and non-safety related applications. However, communication in VANET is wireless in nature due to which there is more change of attacks. Hence to realize the highest potential of VANET, the network should be free from attackers, thereby all the information exchanged in the network must be reliable i.e. should be originated from authenticated sources. To establish the route for sending data from source to destination, we used AODV routing protocol to find the path. We also used hashing to generate the hash value of the message and achieve the integrity and authentication.

In existing technique drawback is this, access server gives all the working to law executor means AS send info to RSU, RSU send this info to law executor and then login process start but if LE behave malicious than this authentication process fail.

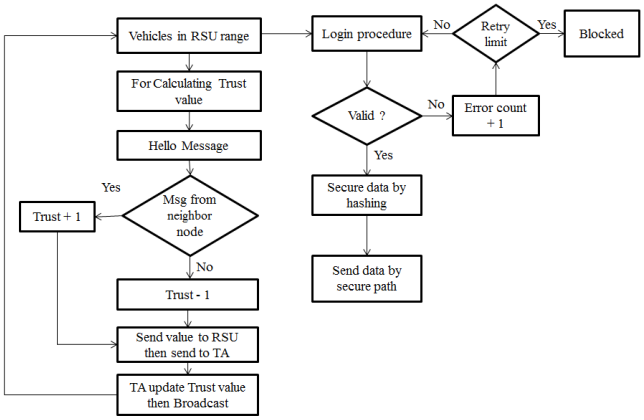

Fig.2 Flow Chart of Proposed technique

In our propose work we calculate the trust of each vehicle on the basis of their behavior. Each vehicle calculates trust of its neighbor and send this value to RSU then RSU update these values with the help of AS and then broadcast this value, now all the vehicles have a trust value of vehicles so that send data by using hashing technique and use trusted path to send the data source to a destination so that security enhance.

Proposed Algorithm:

1. Initialize network ();
2. Broadcast Hello packets to its neighbors
3. For calculating the trust value of neighboring vehicles
4. If(node sends data || send ACK || !Drop)
5. If the above conditions satisfied the we increment the trust as

   Trust++

   Otherwise, we decrement the trust as

   Trust--
6. Then we send this value to AS through RSU
7. AS store the trust values of all nodes and update it regularly
8. Trust values broadcast in the network by AS through RSU
9. Now all nodes have a trust value of its neighbors
10. If vehicle wants to send data then they start the login process whenever it comes in a range of RSU
11. Now the data send after applying hashing technique
12. Every vehicle having a trust value of its vehicles so that they send the data only to the trusted nodes
13. This method creates a trusted path which sends the data to its destination securely.

VI. RESULT ANALYSIS

The simulation is done in NS2 [22] which show the topology of 2000m x 2000m. Various parameters are described in Table 1. The performance of network analysed by PDR, throughput and routing overhead over the network.

Table 1. Simulation Parameters and their values

Parameters	Values
Network Size	2000m x 2000m
Number of Vehicles	50
Packet Size	512 Bytes
Simulation Time	100s
MAC Protocols Used	Mac/802_11
Routing Protocol Used	AODV
Traffic Type	Constant Bit Rate (CBR)

A. Packet Delivery Ratio (PDR)

Defined as the ratio of packets delivered from source to destination. The fig. 3 represents a PDR graph between base approach and the proposed approach. The packet delivery ratio of the proposed approach is better than the existing approach.

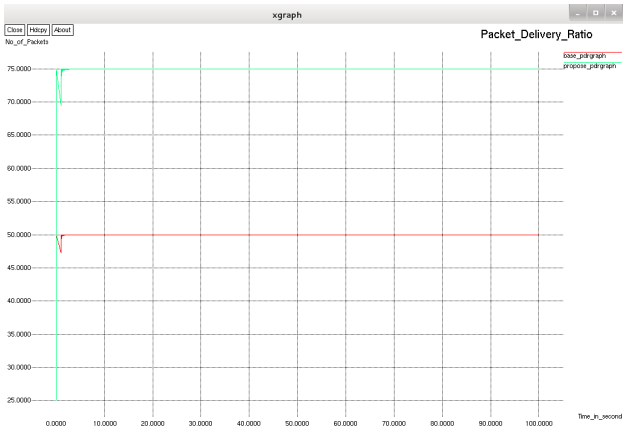

Fig 3. PDR Graph

B. Throughput graph

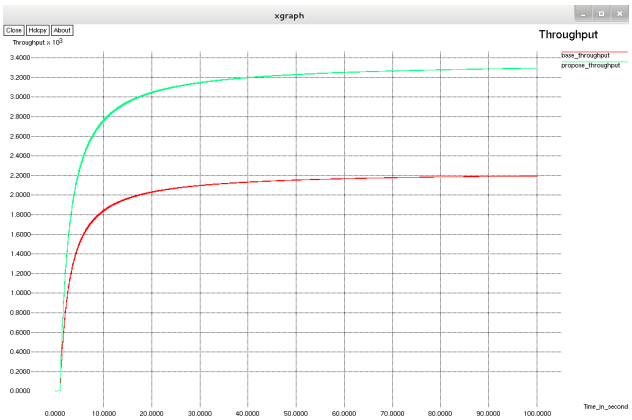

Fig 4. Throughput Graph

Per second transfer of data on bandwidth is known as throughput. The fig. 4 represents a throughput graph between base approach and the proposed approach. The throughput of the proposed approach is better than the existing approach.

C. Routing overhead

The routing overhead is defined as flooding of data in the network transmitted by an application, which utilizes a bit of accessible transfer rate of communication protocols. The fig. 5 represents a routing overhead graph between base approach and the proposed approach. The overhead of the proposed approach is less than the base approach. Since the overhead should be minimum and the routing decreases in the proposed work the overhead also decreases.

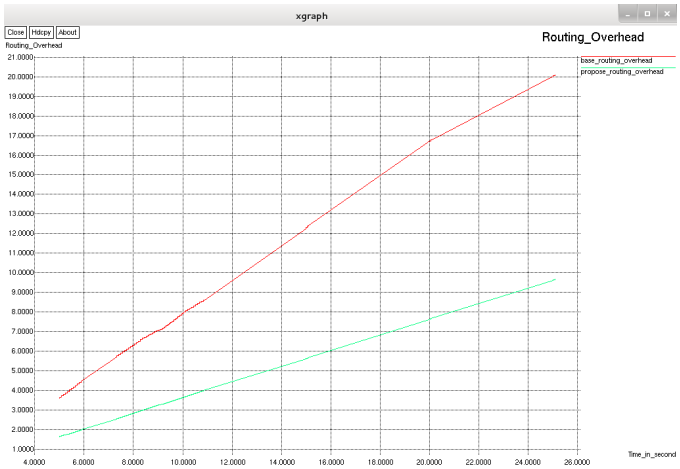

Fig.5 Routing Overhead Graph

VII. CONCONCLUSION & FUTURE WORK

In Vehicular Ad Hoc Networks (VANET), communication among vehicles should be done by the proper trust establishment to secure messages exchange and reliability. We clearly presented an application of VANET and identify the many challenges in this environment. It is a very dynamic network so it is vulnerable to attacks which considerably taken in the security section. In this survey, we mention some existing trust models for different contexts, and point out their issues when being taken to the VANET domain. 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.

In future, Artificial Neural Network can apply at every vehicle to calculate the trust value. It is based on supervised learning which take benefit from the previous detection experience by continuous. We can apply trained data set to observe the behavior of vehicles and then calculate the trust. This makes the process more accurate and fast. All the process is done on vehicles and only trust value is sent to a trusted authority to broadcast it and no updation process is required at TA.

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] Maxim Raya, “The Security of Vehicular Ad Hoc Networks”, SASN, Alexandria, Verginia, USA, (2005) November 7, pp. 11-21.

[6] Hannes Hartenstein, “A Tutorial Survey on Vehicular Ad Hoc Networks”, IEEE Communication Magazine, (2008) June, pp. 164-171.

[7] Ram 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.

[8] J. Zhang, "A survey on trust management for VANETs", International Conference on Advanced Information Networking and Applications, (2011), pp. 105-112.

[9] 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.

[10] 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.

[11] J. Zhang, "Trust management for VANETs: challenges, desired properties and future directions", International Journal of Distributed Systems and Technologies, (2012), pp. 48-62.

[12] Biswas, Subir, JelenaMisic, and Vojislav Misic, "ID-based safety message authentication for security and trust in vehicular networks", 31st International Conference on Distributed Computing Systems Workshops (ICDCSW), IEEE, (2011), pp. 323-331.

[13] Gazdar, Tahani, Abderrezak Rachedi, Abderrahim Benslimane, and Abdelfettah Belghith, "A distributed advanced analytical trust model for VANETs", Global Communications Conference (GLOBECOM), IEEE, (2012), pp- 201-206.

[14] Wei, Yu-Chih, and Yi-Ming Chen, "An efficient trust management system for balancing the safety and location privacy in VANETs", Trust, Security and Privacy in Computing and Communications (TrustCom), IEEE 11th International Conference, (2012), pp. 393-400.

[15] Gómez Mármol, Félix, and Gregorio Martínez Pérez, "TRIP, a trust and reputation infrastructure-based proposal for Vehicular ad hoc networks", Journal of Network and Computer Applications, Springer, (2012), pp- 934-941.

[16] Gazdar, Tahani, Abderrahim Benslimane, Abderrezak Rachedi, and Abdelfettah Belghith, "A trust-based architecture for managing certificates in Vehicular ad hoc networks", International Conference on Communications and Information Technology (ICCIT), IEEE, (2012), pp. 180-185.

[17] M. Chuang and J. Lee, "TEAM: Trust extended authentication mechanism for Vehicular ad hoc networks", Consumer Electronics, Communications and Networks (CECNet), IEEE International Conference, (2011), pp. 1758-1761.

[18] Jaydeep P. Kateshiya, Anup Prakash Singh, "Review To Detect and Isolate Malicious Vehicle in VANET," International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 2, February (2015).

[19] I. AhmedSumra, H. Hasbullah, I. Ahmad, and J. BinAbManan, "New card based scheme to ensure security and trust in Vehicular communications", Electronics, Communications and Photonics Conference (SIECPC), IEEE, (2011), pp. 1-6.

[20] Ming-Chin Chuang and Jeng-Farn Le, "TEAM: Trust-Extended Authentication Mechanism for Vehicular Ad Hoc Networks", IEEE, (2013).

[21] The Network Simulator 2 (NS2) [Online]. Available: http://www.isi.edu/nsnam/ns/.