True and Reliable Information Sharing in VANET Environment

Mohit Saxena, Sweta Sharma
Computer Science & Engineering Department,
Bhopal Institute of Technology & Science, Bhopal

Abstract: - *VANET is a special class of mobile ad hoc network. Data dissemination in VANET is a challenge due to its dynamically changing topology, and researcher's works very hard to minimize this problem and new approaches from them have done this. Now data dissemination in VANET is easy as compared to five years back. But now a new challenge comes in front of researchers that how they decide that information which has to be forwarded into the network is valid and how can they make the network trustworthy. In this paper, we proposed a new approach in which a vehicle can check that information that comes to it for forwarding is true or not and, on its decision, data disseminated in the network. By this, we can make the VANET network trustworthy, and our experimental results show the same.*

I. INTRODUCTION

US Department of transportation introduces intelligent transportation systems for managing transportation on the road to implement communication between vehicle and stationary bodies. ITS uses Vehicular Ad Hoc Network [1], VANET enabled the vehicle to have the onboard unit installed in it, to communicate with other vehicles (known as V2V communication) and with infrastructure (known as V2I communication). Infrastructure which can communicate with the vehicle is known as Roadside Unit or RSU. Dedicated Short Range Communication is used in VANET to communicate. US DoT allocates range at 5.9 GHz [2].

In VANET, messages are categorized into two parts: safety message and non-safety message. Safety messages carry information regarding general warnings and life-critical warnings or information. In contrast, non-safety messages are caring general messages like the internet, online gaming, music, videos, electronic toll collection[3]. To identify which message is a safety message and a non-safety sender adds a header with the message. It also sends messages through some specific channels [4].

The performance of VANET applications depends on the reliability of the received messages. Any malicious behaviour, such as injecting false information, modifying and replaying disseminated messages, discarding routing packets in the network, and impersonation, has irreversible effects on people's lives. Moreover, drivers show prime interest in privacy to protect their private information leading to unique identification in the network. So, it is clear that security and privacy preservation are two critical challenges for VANET deployment in the real world. There is a need for trust to protect VANET from these kinds of unwanted attacks [5]. Before forwarding the message to a network, the vehicle should check the message's validity, and after confirming it, messages disseminated in a network. In this paper, we are proposing our new approach, in which every node in a network contributes to making the network trustworthy. The rest of the paper is organized as follows. Section II describes the previous approaches to data dissemination. Section III describes the proposed trust-based communication scheme, followed by time complexity analysis and experimental results IV. Finally, we conclude the paper in section V.

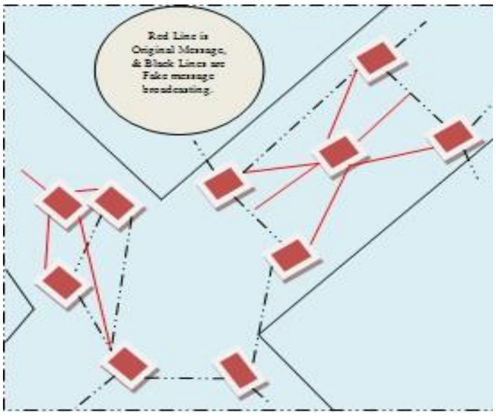
Red Line is Original Message, & Black Lines are Fake message broadcasting.

Figure 1 Data traffic load with forge and original messages

II. LITERATURE SURVEY

In [6] Author proposes a scheme in which roadside unit plays an important role for Trust Establishment. This scheme is based on trusted information instead of the entity that is providing that information. Given approach, the receiver's information has been checked through the collection of other nodes feedback, and accuracy of results is promised.

In [7] Author proposes a scheme in which a similarity-based trust management scheme is applied to give a trust rating for the OBU. Here apriori technique is used to find a connection between OBU and neighbour OBUs. On the definite time interval, echo packets are sent to the networks and receive some network data. Such as speed, location, and similarity in these values between OBUs and one-hop neighbours are used to calculate similarity among the various OBUs. The vehicles' trust value is calculated, which is used to prevent false information dissemination in VANETs.

In [8], a data-centric trust management technique is presented. In that technique, first individual trust for the data is calculated, then multiple. Still, different data are combined to provide and by evaluating using several components, the validity of the data is measured. In that way, properties of the data are used to provide trust in VANET. In that technique, decision logics, Bayesian inference, and dempster-Shafer theory [9] are techniques used to evaluate the data's validity. Then a trust assigning task is presented. Trust Schemes mainly focus on four aspects which are:

- Estimate: Collection of information
- Establishment: Establishing connections
- Calculation: Based on the similarity value
- Update values in the table

III. PROPOSED WORK

Information sharing is the most important feature of VANET. Other VANET applications can do their work; e.g., after collecting information by surrounding, VANET applications decide which route is shorter and have less traffic. As we saw in the above example, "information" is a critical element in the VANET network. But if this information is altered by a malicious user (for his interest), then the vehicle node in the network cannot differentiate between real or altered information. Due to this life of the driver on the road is at risk.

We have proposed a new approach for the above-stated problem that relies on data-based trust [7]. "Information" which is sent or forwarded in the network should be real and trustworthy; for that, we have developed a trust model based on a similarity table. The vehicle node starts broadcasting beacon packets to its neighbour node in the network, repeating this process in a specified time interval. This bacon contains the sender node's IP address, the sender node's speed at the time of packet sending, and the last-passed roadside unit address. Address of forwarding node and information filed should be empty. Based on these kinds of bacon, the vehicle node can create its similarity table and update it regularly. After updating of similarity table, when any other information packet comes to the vehicle node, it starts trust calculation for particular information. After this, when information trust reaches its threshold value, the vehicle broadcast that information in the network; by this, we can save our network from altered or fake information.

IV. SIMULATION

We use the NS-2 simulator to simulate our trust models based on a similarity table that the data given by node neighbour calculates. We assume that Roadside units have all the valid data, and they can identify data validity like information is true or false. Our model has 60 nodes, and they are moving in road direction wisely; simulation area is 1600*1600; we have taken results based on time, such as at 80sec, 120sec, up to 300 seconds.

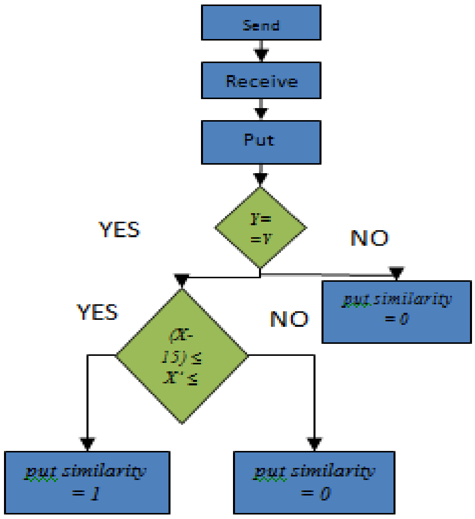

Figure 2 Algorithms for SIMILARITY Calculation

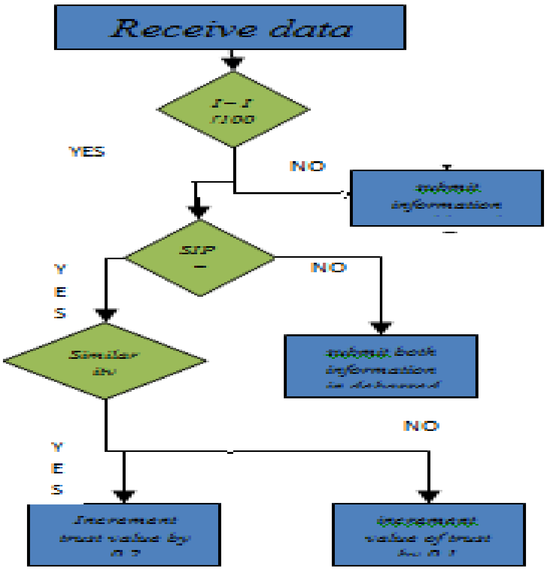

Figure 3 Algorithm for TRUST calculation

Table 1 Our Simulations parameters are given in the table.

Simulation Area	1600 *1600
Simulation Time	80,120,160,200, 250,300
Routing Protocol	AODV
Number of Nodes	60
Number of Malicious Node	01

V. RESULTS

Our approach's performance is measured based on packet delivery ratio, routing overhead, and false message detection. There are two different approaches for which we measure packet delivery ratio. Those two approaches are 1) Basic Routing Algorithm, 2) Trust-Based Dissemination. Simulation graphs are as follows: Figure 4 Blue line shows trust-based dissemination in VANET & the red line shows Basic Routing Algorithm. The horizontal plane represents time in seconds, and the vertical plane represents packet delivery in percentage.

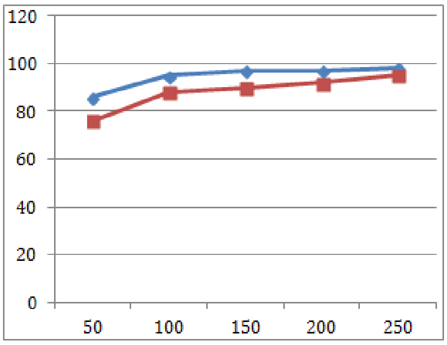

Figure 4 Packet Delivery Ratios

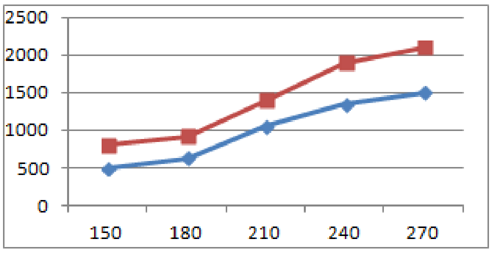

Figure 5 Routing Over Head

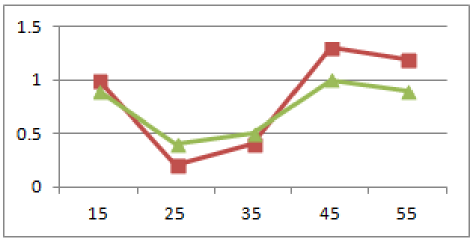

Figure 6 End to End Delays

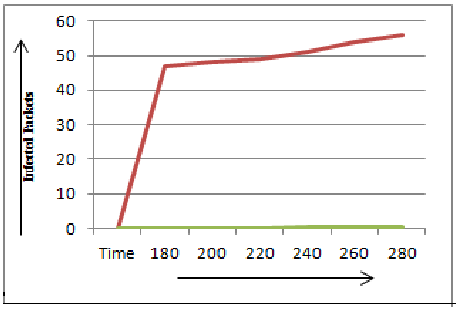

Figure 7 Forge Message Detection in network

Figure 5 Blue line shows Trust-Based Dissemination in VANET (routing overhead) & the red line shows Basic Routing Algorithm (routing overhead). The horizontal plane represents time in seconds, and the vertical plane represents routing overhead. Figure 6 Green line shows Trust-Based Dissemination using clustering in VANET (End to End Delay) & the red line shows Basic Routing Algorithm (End to End Delay). The horizontal plane represents the number of nodes, and the vertical plane represents time in seconds. The Redline shows the percentage of forged messages in a network over time domain using our approach.

VI. CONCLUSION

As per our proposed scheme, trust is building through similarity, and the roadside unit has all the valid data by which can assist the vehicle to identify genuine data. The RSU. helps in increasing the overall performance of our proposed scheme. Our scheme also identifies and debarred the node that broadcast altered information in the network. The proposed scheme results show better performance as compared to the existing scheme. The proposed scheme shows minimum variation in trust value in the network overall, even when 80% of the network information is false.

REFERENCES

[1] Guan, Quan Sheng, et al. "Topology control in mobile ad hoc networks with cooperative communications." Wireless Communications on, IEEE, pp. 74-79, IEEE, 2012.

[2] Jiang, Daniel, et al. "Design of 5.9 GHz DSRC-based vehicular safety communication." Wireless Communications, IEEE, pp. 36- 43, IEEE, 2008.

[3] Belton "Electronic Toll Collection System in the Republic of Belarus" [Online]. Available: http://www.beltoll.by/index.php/en/faq/all- about-the-obu [Accessed May 25 2016]

[4] Yi Qian; Kejie Lu; Moayeri, N., "A Secure VANET MAC Protocol for DSRC Applications," Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE, vol., no., pp.1, 5, Nov. 30 2008-Dec. 4 2008.

[5] Zhang, Jie. "A survey on trust management for Vanets." 2011 IEEE International Conference on Advanced Information Networking and Applications. IEEE, 2011.

[6] Wu, Aifeng, Jianqing Ma, and Shiyong Zhang. "Rate: An RSU-aided scheme for data-centric trust establishment in Vanets." Wireless Communications, Networking and Mobile Computing (WiCOM), IEEE, pp. 1-6, 2011.

[7] Al Falasi, Hind, Nader Mohamed, and Hesham El- Syed. "Similarity-Based Trust Management System: Data Validation Scheme." Hybrid Intelligent Systems. Springer International Publishing, pp.141- 153, Springer, 2016

[8] Raya, Maxim, et al. "On data-centric trust establishment in ephemeral ad hoc networks." INFOCOM 2008. The 27th Conference on Computer Communications. IEEE, pp. 1912 – 1920, IEEE, 2008.

[9] Jothi, K. R., and A. Ebenezer Jeyakumar. "Optimization and quality-of-service protocols in VANETs: a review." Artificial Intelligence and Evolutionary Algorithms in Engineering Systems. Springer India, pp. 275-284, Springer, 2015.