International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 04, Issue: 01 (January-February, 2018)

Trust Based Data Dissemination in Vehicular Ad Hoc Network

Kalyan Singh Mewada, Dr. Satya Ranjan Patra
M. Tech. Scholar, Computer Science & Engineering Department,
Bhopal Institute of Technology & Science, Bhopal

Smita Rani Biswal
Assistant Professor, Computer Science & Engineering Department
Padmanava College of Engineering, Rourkela

Abstract: - *VANET is a special class of mobile ad hoc network. Data dissemination in VANET is a challenge due to its dynamically changing topology, 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 is come in front of researches that how they decide that information which has to be forwarding in to network is valid or not. And how can they make network trustworthy. In this paper we proposed a new approach in which vehicle can check by itself that information which comes to it for forwarding is true or not and on the basis of its decision data will be disseminate in the network. By this we can make VANET network trustworthy, our experimental results shows the same.*

I. INTRODUCTION

US DoT (Department of Transportation) introduces intelligent transportation system (ITS) for managing transportation on road, to implement communication between vehicle and stationary bodies I.T.S. uses Vehicular Ad Hoc Network (VANET), it is a special class of MANET [1], VANET enabled vehicle have on board 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 vehicle is known as Road side Unit or RSU. Dedicated Short Range Communication is used in VANET to communicate. U.S. DoT allocates range at 5.9 GHz [2]. In VANET message are categorized in to two parts, first is safety message and second is non-safety message. Safety massages carry information regarding general warnings and life critical warnings or information, where as non-safety messages are caring general messages like internet, online gaming, music, videos, electronic toll collection etc [3]. To identify which message is safety message and which one is non-safety sender adds a header with message along with this it also sends messages through some specific channels [4]. It is obvious the performance of VANET applications is depending on the reliability of the received messages. Any malicious behavior, 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 real world.

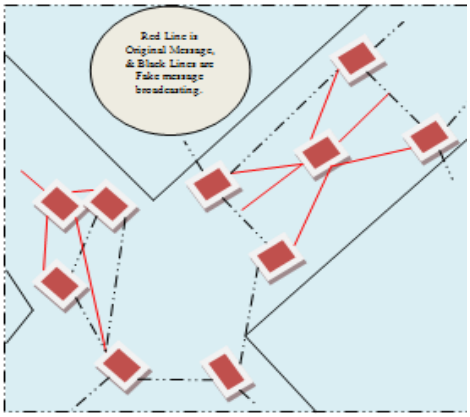

Figure 1 Data traffic load with forge and original messages

To protect VANET from these kinds of unwanted attacks there is a need of trust [5]. Before forwarding the message in a network vehicle should check the validity of the message and after confirming it, messages should be disseminate in a network. In this paper we are proposing our new approach, in which every node in a network contributes to make network trustworthy. The rest of the paper is organized as follows. Section II describes the previous approaches of data dissemination. Section III describes the proposed trust based communication scheme, followed by time complexity analysis and experimental results in section IV. Finally we conclude the paper in section V.

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. In his approach information is been checked by receiver through collection other nodes feedbacks, by this the accuracy of results is promised.

In [7] Author proposes a scheme in which a similarity based trust management scheme is applied to give trust rating for the OBU. In this scheme apriori technique (data mining) is used to find connection between OBU and its neighbor OBUs; on the definite time interval echo packets is send to the networks and receives some data from network such as speed, location etc and similarity in these values between OBUs and one hop neighbors is used to calculate similarity among the various OBUs. Then, based on this, trust value for the vehicles 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, but different data is combined to provide and by evaluating using several components validity of the data is measured. In those way properties of the data is used to provide trust in VANET. In that technique decision logics Bayesian inference and dempster-Shafer theory [9] are techniques used to evaluate the validity of the data. Then a trust assigning task is presented.

Trust Schemes mainly focus on 4 aspects which are:

- Estimate: Collection of information
- Establishment: Establishing connections
- Calculation: On the basis of similarity value
- Update values in Table

III. PROPOSED WORK

Information sharing is a most important feature of VANET. On the basis of incoming information other VANET applications are able to do their work, for e.g. after collecting information by surrounding, VANET applications will decide which route is shorter and having less traffic. As we seen in above example "information" is a critical element in VANET network. But if this information is altered by malicious user (for his personal interest), then vehicle node in network are not able to differentiate between real or altered information. Due to this life of driver on road is at risk. For the above stated problem we have proposed a new approach which relay on data based trust [7]. "Information" which is sent or forwarded in network should be real and trustworthy, for that we have developed a trust model which is based on similarity table. In network, vehicle node starts broadcasting bacon packets to its neighbor node and it will repeat this process in specified time interval. This bacon contains IP address of sender node, speed of sender node at the time of packet sending, last passed road side unit address. Address of forwarding node and information filed should be empty. On the basis of these bacons vehicle node is able to create its similarity table and update it at regular time interval. After updating of similarity table when any other information packet is come to vehicle node it starts trust calculation for particular information and after this when information trust reaches its threshold value, vehicle will broadcast that information in network, by this we are able save our network from altered or fake information.

IV. SIMULATION

We use NS-2 (2.34) simulator for simulate our trust models which is based on similarity table which is calculated by the data given by nodes neighbor. We assume that Road side units have all the valid data and they can identify data validity like information is true or false. Our model has 60 nodes, they are moving on road direction wise, simulation area is 1600*1600; we have taken results on the basis of time such as at 80sec, 120sec, up to 300 seconds. Routing protocol is AODV. Malicious node is one.

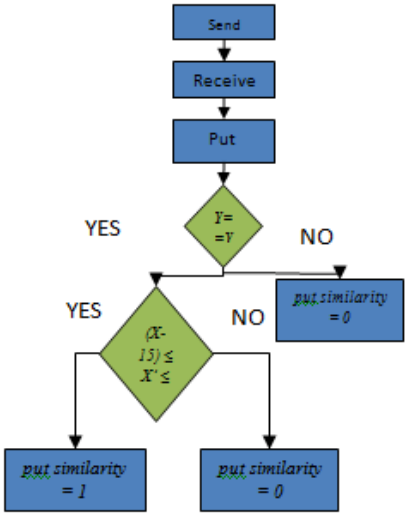

Figure 2 Algorithms for SIMILARITY Calculation

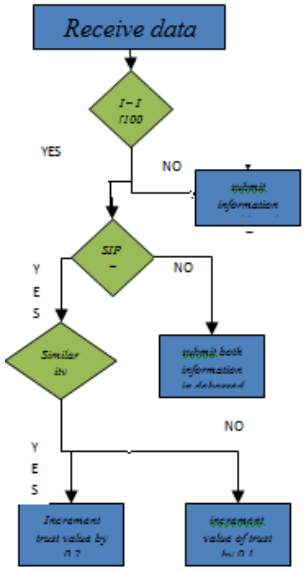

Figure 3 Algorithm for TRUST calculation

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

Performance of our approach is measured on the basis of packet delivery ratio, routing overhead, 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:

In the Figure 4 Blue line shows Trust Based Dissemination in VANET & red line shows Basic Routing Algorithm. Horizontal plane represents time in

seconds and vertical plane represents packet delivery in percentage.

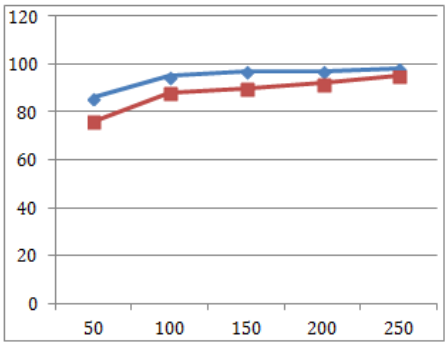

Figure 4 Packet Delivery Ratios

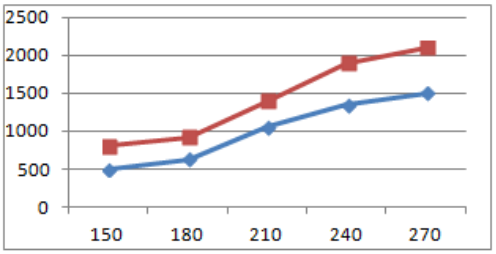

Figure 5 Routing Over Head

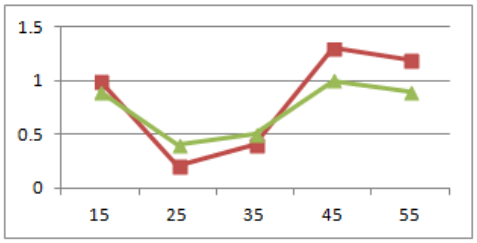

Figure 6 End to End Delays

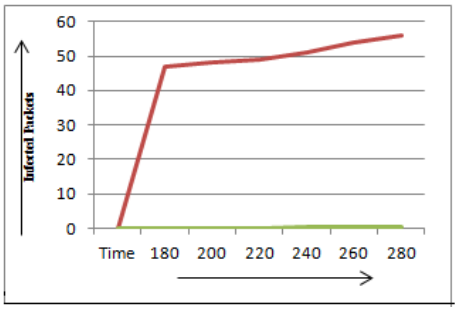

Figure 7 Forge Message Detection in network

In the Figure 5 Blue line shows Trust Based Dissemination in VANET (routing over head) & red line shows Basic Routing Algorithm (routing over head). Horizontal plane represents time in seconds and vertical plane represents routing over head. In the Figure 6 Green line shows Trust Based Dissemination using clustering in VANET (End to End Delay) & red line shows Basic Routing Algorithm (End to End Delay). Horizontal plane represents number of nodes and vertical plane represents time in seconds. Red line shows percentage of forge messages in a network over time domain using our approach.

VI.CONCLUSION

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

References

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