IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

A Nobel approach to create trust by using similarity based scheme in VANET

Deepa Soni[1], Ravindra Gupta[2], Varsha Namdeo3

Research Scholar, Dept. of CSE RKDF IST Bhopal (M.P)[1]

Assistant Professor, Dept. of CSE RKDF IST Bhopal (M.P)[2]

HOD, Dept. of CSE, RKDF IST Bhopal (M.P)[3]

Abstract: Vehicular ad hoc network is a special kind of ad hoc network which consists of vehicles nodes. When researchers uses vehicle as a node they face some issues which are "high speed of vehicle" due to this topology changing dynamically, system needs central authority, relationship between nodes are often short lived. VANET network is introduced by ITS (Intelligent Transportation System) to protect human lives on road from accidents furthermore it focuses on providing applications which provide comforts driver during travelling. But now a day's ad hoc network is facing security issues and VANET is not an exemption. In VANET, information should be sent or receive by nodes on time and without being altered, for the reliable and efficient delivery of message. Trust is key element in network by which, one node beliefs over the other one when it receives data from it. Trust may have many faces like it can either be on the information, node, road side units, etc, but we mainly focuses on data centric trust which provided the trusted information and give some essence of entity centric trust to make system attacker free by using combined trust. In proposed approach we introduce a similarity metric which is updated and maintain by node on the basis of some specific information given by their neighbor, after that we proposes our own trust model. Results show the acceptance of our trust scheme with respect to the introduction of forge or altered data in a network.

Keywords: V2V (vehicle-to-vehicle), V2I (vehicle-to-infrastructure), RSU (road side unit**)**

I. INTRODUCTION

In the last decade wireless technology has some serious developments; by using these developments US DoT introduces intelligent transportation system (ITS) for passenger safety on road [1], to achieve the goal of passenger safety communication between vehicle is important for that purpose ITS uses Vehicular Ad Hoc Network , Which is a special class of MANET [1]. In VANET communication can be done by three ways vehicle to vehicle, vehicle to infrastructure and Infrastructure to Infrastructure [2]For communication, channel is required, so VANET uses Dedicated Short Range Communication and Wireless Access to Vehicular Environment for communication [3] Day by day attackers and malicious users are being very smart, they develop new technique to fool other passenger on road for their personal profit. As VANET is based on information sharing scenario if information is come to any node in VANET is fake, it will not able to identify it. So there is need of TRUST between nodes on road; this trust may have many faces such as Entity centric Trust, Data Centric Trust, etc [4]. By using this in VANET, information sharing on road will be trustworthy and vehicle node can able to identify which information is true and which one is false. For e.g. If any vehicle on road having a crash with other one and for escaping from any kind of penalty it sends false message that road is clear. If we not using trust than it is difficult for other vehicle to identify the validity of information whether it is true or false, but in case trust Is in scenario than receiving vehicle will cross check this information with other neighbor vehicles and then it decides information is true or false.

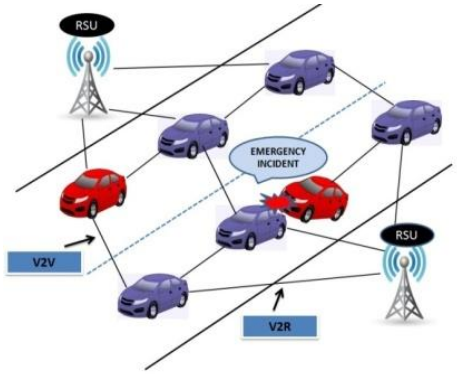


Figure 1 VANET Model

DOI 10.17148/IJARCCE.2017.61119

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

II. LITERATURE SURVEY

In [5] 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 [6] 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 [7] 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 [8] are techniques used to evaluate the validity of the data. Then a trust assigning task is presented.

Wenjie Wang, Tao Luo, Ying Hu They propose a novel routing protocol in city VANET named Landmark-based routing using global real-time traffic (LRRT), which is beaconless and AP-assisted. Initial of all, we have a tendency to present a density estimation scheme to know the worldwide density info for planning routing protocol. Vehicles in the network periodically update their locations and report back to APs, whereas APs gather these real time reports in their coverage so as to make native density table. Then the worldwide density info is available by sharing native density info between adjacent APs. Moreover, we have a tendency to style LRRT for knowledge transmission. Once upon knowledge transmission, vehicles apply to APs for the worldwide density info that is used to weight the length of all potential roads from source to destination. The shortest path algorithmic rule Dijkstra is given to output the optimized route that consists of a series of consecutive junctions on the overlay network.

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. “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.

Some definitions are as follows:
X= Speed of Node
X’= Speed of Node (Neighbor Node)
Y= Last RSU address contain by node
Y’= Last RSU address contain by node (Neighbor Node)
SIP= Source IP address
SIP’= Already stored SIP inn data base
FIP= Forwarding node IP address
I = Information ID

Bacon packet format:

SIP	FIP	Y	X	Information

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

When node sends bacon packet in a network it will not put any entry in "information" as well as "FIP" field by which receiver identify that it is a bacon packet.

Similarity Calculation:
Step 1 Send hello packets in network.
Step 2 Receive bacon packets.
Step 3 Put Entry in a table.
Step 4 If Y==Y' goto step 6
Step 5 Else put similarity = 0
Step 6 If (X-15) ≤ X' ≤ (X+15) goto step 8
Step 7 Else put similarity = 0
Step 8 Put Similarity =1, for respective IP.

For Trust Calculation:
Step 1 Receive data
Step 2 If I= I [100] goto step 4
Step 3 Else submit information in table with its SIP
Step 4 If SIP = SIP' goto step 6
Step 5 Else submit both information in debarred table.
Step 6 If Similarity value = 1 goto step
Step 7 Else increment value of trust by 0.1
Step 8 Increment trust value by 0.2

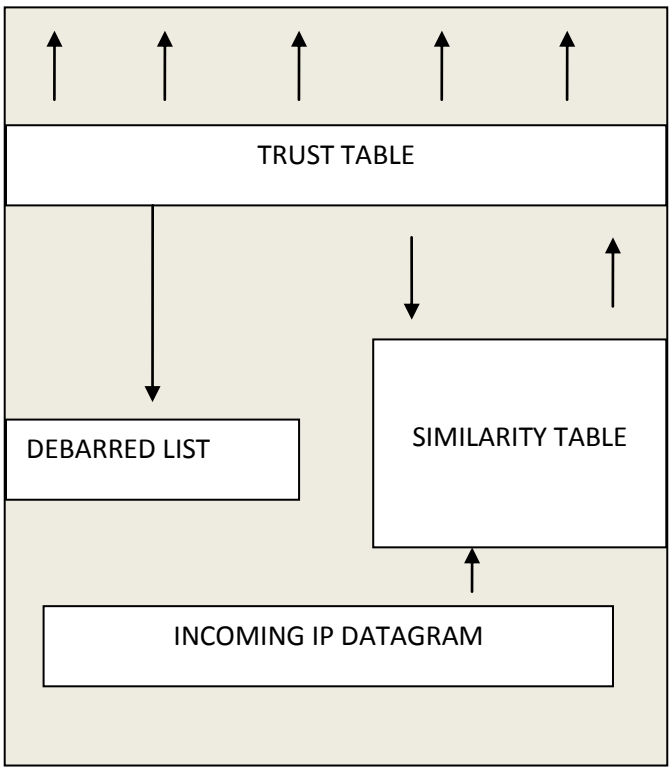


Figure 2 Logic diagram

V. 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.

Our Simulations parameters are given in the table

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

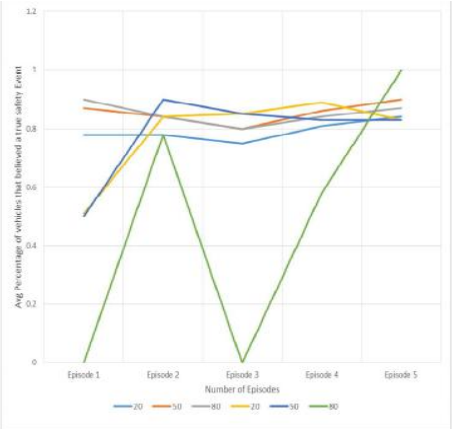
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 11, November 2017

Table 1 Parameters

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

VI. RESULTS

We compare our scheme with trust model which makes use of similarity to calculate trust.



In the figure the purple, blue and **orange** color resemble existing trust based scheme and **Dark blue, brown** and **green** resembles our proposed scheme.

VII. 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 are 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] 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]
[3] Jiang, Daniel, et al. "Design of 5.9 GHz DSRC-based vehicular safety communication." Wireless Communications, IEEE , pp. 36-43,IEEE,2008.
[4] Zhang, Jie. "A survey on trust management for vanets." 2011 IEEE International Conference on Advanced Information Networking and Applications. IEEE, 2011.
[5] Wu, Aifeng, Jianqing Ma, and Shiyong Zhang. "Rate: A rsu-aided scheme for data-centric trust establishment in vanets." WirelessCommunications, Networking and Mobile Computing (WiCOM),IEEE,pp. 1-6,IEEE,2011.
[6] 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
[7] 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.
[8] 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.
[9] Wenjie Wang, Tao Luo, Ying Hu They propose a novel routing protocol in city V ANET named Landmark-based routing using global real-time traffic (LRRT), 2016 2nd IEEE International Conference on Computer and Communications