Trusted Location Selection in Vehicular ad -hoc Network

Sonam Soni

Department of CSE
ITM University
Gwalior, India
Shona1813@gmail.com

***Abstract*—VANET gives the advantage to enhance road safety and assure less or no traffic accidents. However, false messages can result in serious conditions like collision. This paper proposed a new, trust based technique for location selection in VANET. In the paper presents a trust based location selection scheme has two phases computation of direct and indirect trust. However, evaluation of direct trust system using infrastructure (RSU) and trusted authority (TA) and evaluation of indirect trust uses watchdog approach. Results show that the proposed scheme suitable for the actual situation of VANET.**

Keywords— Trust; Reputation; VANET; Watchdog; RSU; TA.

I. INTRODUCTION

VANET has become a growing area of research and development because it gives to improve traffic congestion and save time and fuel [1]. A Vehicular Ad Hoc Network (VANET) is a wireless network in which each and every node are vehicles equipped with wireless communication technology. In VANET, Communication can be established between Vehicle-to-Vehicle (V2V), when vehicles communicate directly, or V2I (Vehicle-to Infrastructure), when vehicles exchange information with access points, called Roadside Units (RSUs) [2]. The main objectives of VANET are: It provides safe and secure driving environment, assures less or no accident, save time and fuel, avoid traffic jam, provides accident report, earthquakes and flood information, weather information etc. and decrease travelling time. In VANET communication can be done between exchanges of information, so evaluating the trustworthy information is very necessary. Trust management is one well known scheme and basic need to maintain a reliable, secure faithful communication in VANET by which vehicles can believe through their close eye and could drive for a safe journey [3].

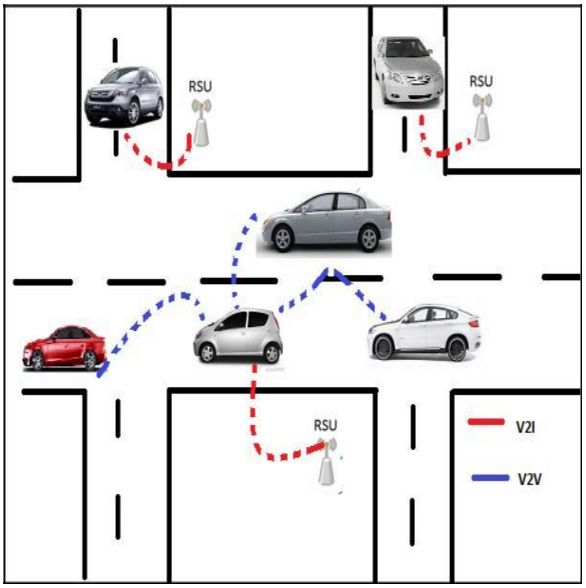

Fig.1. Types of communication in VANETs.

II. RELATED WORK

In this field researcher have effort to make strong design and implementation of trust management in VANET network environment. It is the technology of building a secure network between vehicles; i.e. vehicles communicate to each other and pass information to another vehicle. There are very few work about trust computation in VANETs [4-7]. David Antolino Rivas et al. [4] presents user signatures to transfer information about Points of interest in vehicular ad-hoc networks. In this paper [5] used for TPM for proposed a new model for chain of trust within vehicular to handle all types of attacks

American Journal of Advanced Computing, 2018, Vol-1, Issue-2, 1-6
Published Online, 2018 in AST Publishers (http://www.astpublishers.com/)
DOI: 10.15868/ajac.2018.01.02

and maintain the integrity of messages. Chaurasia et al. [6] proposed a trust computation scheme is based on formation of group. In this work presents a trust and reputation management framework [7] for VANETs based on similarities between messages and similarities between vehicles and a reputation evaluation algorithm is proposed for a new vehicle based on the similarity theory. In this propose work [8] a cooperation enhancement mechanism using "*NeighborhoodWatchDog*" to evaluate the "*Trust Token*" based scheme on the first-hand observation. The process of change point detection [9] is used to improve the watchdog monitoring mechanism is presented.

This paper established trust based technique is presented for finding the location in VANETs environment. This proposed scheme consists of two phases. In the first phase presents the direct trust computation by using access point like RSU and second phase computes the indirect trust by using watch dog.

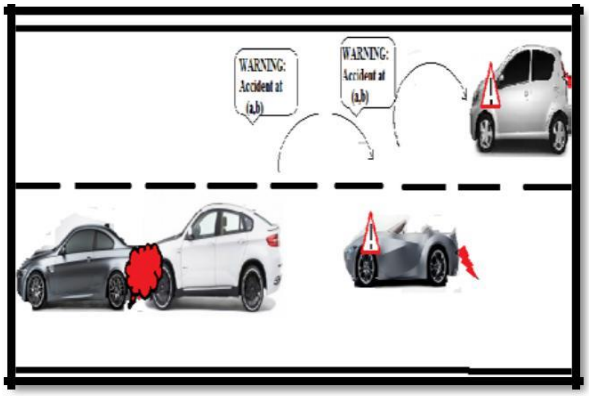

Fig. 2. Way to provide Information on VANETs environment

III. ISSUES AND DESIGN REQUIREMENTS OF TRUST COMPUTATION IN VANETS

VANETs have some unique properties which differentiate them from other ad hoc networks. The main properties of VANETs are high mobility, predictable topology, hard delay constraints, sufficient energy, storage capacity and variable network density. On the basis of characteristics of VANETs list of issues of trust establishment in VANETs are as follows:

- *Accuracy*

Evidently, a trust and reputation computation in VANETs is always expected to be accurate. Due to detect false information of vehicles.

- *Decentralized*

Decentralized is one of the main issues of trust and reputation computation in VANETs. It should also be applicable to highly dynamic and distributed environment.

- *Simple, light and fast*

Trust and reputation technique should be light weighted, fast in terms of computing and not complex or simple.

- *Scalable*

Hence, VANET is variable density and vehicular density depends on traffic conditions and locations such as traffic jam conditions, city centre, rural roads or highways. So, scalability is also an important issue of trust and reputation computation in VANETs.

IV. PROPOSED METHODOLOFY

The proposed methodology is categorized into two phases. In the first phase, computation of direct trust based location finding is presented by using infrastructure such as RSU. In the second phase, evaluation of indirect trust based location finding is presented by using watchdog. However, indirect trust system is used able to work in the absence of RSU.

Phase I: Direct Trust Computation

In this phase, vehicle wants to find some location information about its nearby hospital, petrol pump, hotels etc. then it broadcasts its request (REQ) message nearby vehicles in the network. Then the various vehicles in its transmission range reply the source query with the help of (REP) reply messages. When the source vehicle gets REP from the other vehicles within transmission range. In this proposed work, there are three cases for calculating the trustworthy location.

Case 1- Calculate the trusted location using RSU-

Source vehicle asks to RSU about location. Source vehicle will receive location information from RSU and that information will be fully trusted received by RSU. If RSU is not present in the range of source vehicle then compute the trusted location by using case 2.

Case 2- Calculate the trusted location using Vehicles-

Source vehicle broadcasts its request (REQ) message about finding the location within the communication

range in the network. Source vehicle receives the (REP) messages from the various vehicles then vehicle computes ratio of trusted information about location.

If source vehicle getting the REP messages from 20 vehicles and 18 vehicles say that in the range of 100km forward direction located a good hospital and 2 vehicles tell there is no any hospital within the range of 250km. There is a situation of the ratio is [(18/20)*100] = 90% of the trusted information about hospital location. Source vehicle may trust of broadcast location until ratio is greater than 50%. When equal to or below 50% ratio, vehicle can compute direct trust by case 3. The proposed scheme may also report to RSU or TA about malicious vehicles regarding given wrong information as in [10].

Case 3- Calculate the trusted location using TA-

If ratio equal to or below 50% then the source vehicle asks to TA (as police vans, ambulance and post office vehicles) about location. Source vehicle will receive location information from TA.

Algorithm-

TRUSTED_LOCATION_DECETION

CASE 1:

1. Source vehicle ask location to RSU
2. RSU sends location information to source vehicle
3. {
4. if (RSU is absent)
5. }
6. Go to second case

CASE 2:

1. Source vehicle broadcast REQ
2. Receive REQ by vehicles within communication entity range
3. vehicles Reply REP
4. For each (REP)
5. {
6. if (Location_present)
7. {
8. α ++ ;
9. }
10. else
11. {
12. β ++
13. }
14. }
15. Compute Ratio for α = [(α/γ)*100]
16. Compute Ratio for β = [(β/γ)*100]
17. If (α > β)
18. {
19. Path is trusted
20. }
21. else if (α ≤ β)
22. Go to third case.

CASE 3:

1. if (α ≤ β)
2. {
3. Ask to TA about location
4. }

Table 1. Notations used in algorithm

Symbol	Description
α	α is used to count of vehicle who are saying the location are present
β	β is used to count of vehicle who are denying the location are present
γ	Total number of reply by vehicles
TA	Trusted authority as police van, ambulance, post office vehicles etc.
REQ	Source node broadcast request message
REP	Nodes in the transmission range receive the REQ message and REP to source node

Phase II: Indirect Trust Computation

In the second phase, indirect trust calculates in the absence of RSU and TA by using of watchdog technique. Watchdog is used to detect the malicious vehicles. Watchdog is set in the each vehicle and maintains a buffer. Buffer maintains all the information about the vehicle. On the basis of buffer information, we calculate the misbehaving vehicles. To reduce the weakness of watchdog, we implement this proposed scheme. The proposed working of watchdog technique is divided into three steps:

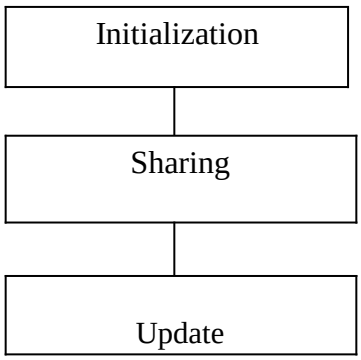

Fig.3. Steps of watchdog technique

1. **Initialization**- In the first step, source vehicle broadcasts the packet in the communication range and watchdog set in the each vehicle stores the sending packet information in own buffer. Many vehicles in the range receive the packet and forward to the next vehicle and put information in buffer.
2. **Sharing**- Second step perform sharing, each vehicle in the range of transmission sharing the buffer/table information among them.
3. **Update**- In the third step, after sharing all the information, vehicles maintains and updates the buffer. On the basis of buffer information we find out some vehicles receive the packet but do not forward to next vehicle. This type of misbehaving performance of vehicle, that vehicle is tagged as malicious vehicle.

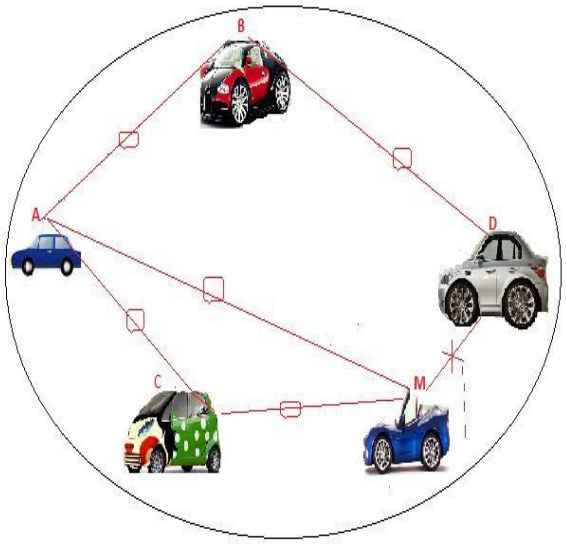

Fig.4. Watchdog Scenario.

The proposed scheme easily evaluates the malicious vehicles in the VANET scenario. If source vehicle receive 20 reply from various vehicle then calculate the trust value.

$Tv =$ 

Where, T_V is the trust value.

S_{LP} is the weighted sum of location are present.

S_{AP} is the weighted sum of location are absent.

Table 2. Trust value range

Trust value range	Vehicle category
100 to 90	5
90 to 80	4
80 to70	3
70 to 60	2
60 to 50	1
Below 50	Malicious

V. SIMULATION SETUP AND RESULTS

In this paper, we implement our experiment on a network simulator tool (NS-2.35) [11]. A field of area 2000x2000 m^2 has been considered in our experiment. All the simulation parameters that are in table 3 lists, we have used. The VANET scenario composed of 10-50 vehicles distributed in a 2 km^2 area. Vehicles considered with variable speeds between 5-55 km/hr, inclusive of accelerations and decelerations and a maximum pause time of 2s. The simulation time was setup up to 1000s and, during this time, the vehicle moves forward direction along with the road. The transmission range was setup to 250 m, with a transmission rate of 4pkts/s and a data rate of 6Mb.

Table 3. Simulation Parameters

Parameters	Values
Number of nodes	10, 35, 50
Dimension of simulated area (meter)	2000×2000
Antenna	Omni directional
Routing Protocol	AODV
Simulation time in seconds	1000
Transport Layer	UDP
Max queue length	50
Bandwidth	6Mb/s

Speed range	5-55 km/h

Figure 5 shows that if up to 50 vehicles simultaneously send information, then packet delivery rate varies from 10-50 vehicles. It is observed that when density is high then average packet delivery ratio (PDR) is very much low around 20%. However, when vehicle density in VANET is less than packet delivery ratio is high around 65%. Packet delivery ratio is decreases due to implement of watchdog over VANET scenario. The packet size is 512 bytes is considered. The average packet delivery ratio is 61% at low density and 14% at high density, but 22% at medium density environment.

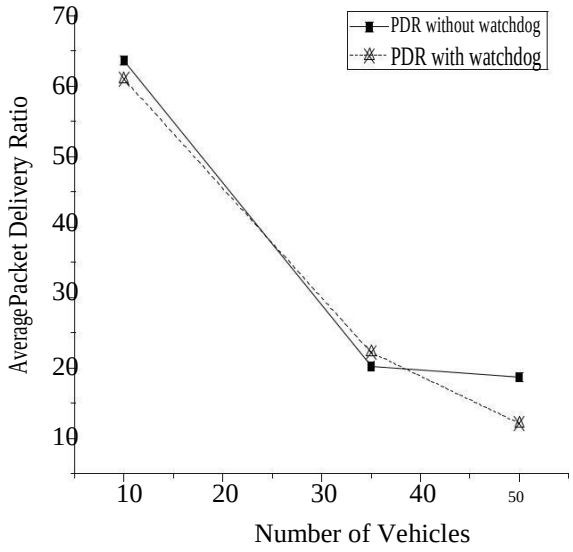

Fig.5. Packet delivery ratio for direct trust computation without using watchdog technique and with watchdog scheme.

Similarly, Figure 6 shows that the average end to end delay is high to compute indirect trust using watchdog approach. However, to compute direct trust end to end delay is less around 160 ms at high density and 28 ms at low density. After calculating packet delivery ratio we have evaluated trust computation of location finding information by two ways. Direct trust and indirect trust are two ways using infrastructure and without using infrastructure respectively Figure 5 and 6 shows the packet delay ratio and end to end delay simulation and watchdog technique is shown by dotted line after simulation we know that watchdog technique is better one to find out the malicious vehicle.

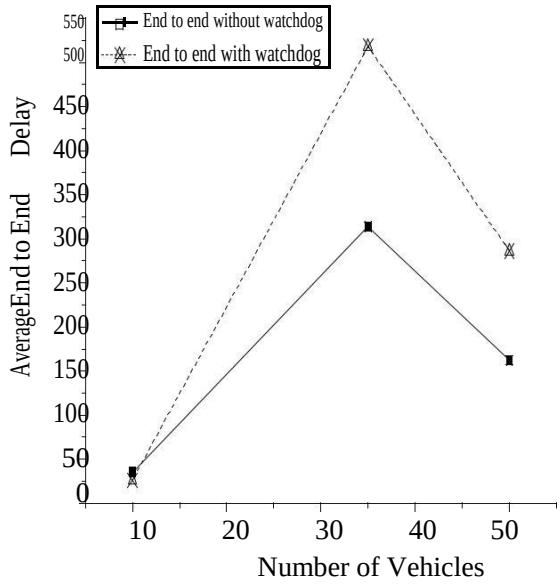

Fig. 6. End to end delay for direct trust computation without using watchdog technique and with watchdog technique.

VI. CONCLUSION

This paper concern about a trust based scheme for location finding in VANETs. This proposed scheme is used for identifying the trusted location. To evaluate the trusted location we introduce the trusted based mechanism using RSU, TA for computing direct trust and watchdog scheme for indirect scheme. In this scheme, the simulation results show that our proposed work can effectively find out the trustworthy location and this schemed performs satisfactorily in the realistic environment scheme.

REFERENCES

[1] Sabih ur Rehman, M. Arif Khan, Tanveer A. Zia and Lihong Zheng, " Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges," Journal of Wireless Networking and Communications, vol. 3(3), pp. 29-38, 2013.

[2] Md Mahbubul Haque, Jelena Misic, Vojislav Misic, Subir Biswas, and Saeed Rashwand, "Vehicular Network Security," Encyclopedia of Wireless and Mobile Communications second edition, 2013.

[3] Kapil Sharma, Sonam Soni, Brajish Kumar Chaurasia, "Reputation and Trust Computation in VANETs," IEMCON-14 Conference on Electronics Engineering and Computer Science, pp.118-122 ,2014.

[4] David Antolino Rivas, Manel Guerrero Zapata, "Chains of Trust in Vehicular Networks: a Secure Points of Interest Dissemination Strategy," Journal of Network and Computer Application Vol. 10 Issue 6, pp. 1115-1133, August 2012.

[5] Irshad Ahmed Sumra, Halabi Hasbullah, Jamalul-lail, and Masood-ur-Rehman, "Trust and Trusted Computing in VANET," Computer Science Journal Vol. 1, Issue 1, pp. 29-51, April 2011.

[6] B. K. Chaurasia and S. Verma, "Trust Based Group Formation in VANET," In International Journal of Modern Traffic and Transportation Engineering Research (MTTER), Vol. 2, No. 2, pp. 121-125, 2013.

[7] Nianhua Yang, "A Similarity based Trust and Reputation Management Framework for VANETs," International Journal of Future Generation Communication and Networking Vol. 6, No. 2, pp. 25-34, April 2013.

[8] Wang, Z. and Chigan, C. "Cooperation enhancement for message transmission in VANETs," Wireless Personal Communications, Vol. 43, Issue 1, pp. 141-156, 2007.

[9] Karuppiah, A. B. Meenakshi, T. Ranjitha, T.I.Mano & Vivitha, S., "false misbehaviour elimination in watchdog monitoring system using change point in a wireless sensor network," An International Journal Graduate Research in Engineering and Technology (GRET), pp. 31-35, 2012.

[10] B. K. Chaurasia, and Shekhar Verma, "Infrastructure based Authentication in VANETs," In International Journal of Multimedia and Ubiquitous Engineering, Vol. 6, No. 2, pp.41-54, 2011.

[11] Neha Singh, R.L. Dua, and V. Mathur, "Network Simulator NS2-2.35," International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, Issue 5, pp.224-228, 2012.