A Trust Based Authentication Scheme in VANET

Farooq Javed[1], Ameer Hamza[2], Faqia Saeed[3] and Nudrat Nida[4]

[1,2]Department of Computer Science & IT, University of Sargodha, Sargodha, Punjab-Pakistan
[3,4]Department of CS&E, University of Engineering & Technology, Lahore, Pakistan
[1]farooqjavid@yahoo.com, [2]mameeerhamza@gmail.com, [3]faqiasaeed@yahoo.com

Abstract– **In vehicular network message validation is one of the key factors of Intelligent Transport System (ITS), as valid message improves the route planning, road safety and traffic management. The proposed scheme is about the validity of the message whether the message received is valid or not. Invalid message in real time urban environment can cause road side accidents, traffic jams, speed control, free passage of emergency vehicles and unseen obstacles etc at a large number that may lead to a serious/fatal results. We propose a scheme that focuses on the validity of the message by testing the trust level of the vehicle, the validity of sender vehicle's message is checked by the rating assigned to each vehicle that set by the group of receiving vehicles. If sender's rating is above the threshold value the sender vehicle will be in the trustee mode. Otherwise it will be in the list of non-trustee mode.**

Keywords– **VANET, Security, ITS, Certificate Authority (CA), On Board Units (OBU), Vehicle to Vehicle (V-to-V) and Vehicle to Infrastructure (V-to-I)**

I. INTRODUCTION

Rapidly increase of technology in automobile companies helps in many ways like improving traffic management, reducing number of destructive accidents and provides facilities like GPS, parking areas and navigation systems. One such technology that is flourishing very rapidly is VANET (Vehicular Ad-hoc Networks). In this technology vehicles and road side units are the nodes and provide useful information to each other.

Communication in VANETs can be classified as V to V and V-to-RSU (Road Side Unit). Road Side Units are the communication structures deployed by the vehicular authorities on the roadside. VANET is related to MANET as it is a subset of MANET. Nodes are mobile but in VANET, nodes have the ability to recharge their batteries frequently but not in case of MANET.

The Federal Communications Commission (FCC) has allocated VANET a frequency band of 75 MHz from 5.825-5.950 GHZ especially in US. The band is divided into 7 channels out of which 6 channels are used for communication while 7th channel is used as a control channel.

In VANETs different vehicles can exchange useful information's like traffic congestions, collision warning, road condition, weather forecast, accidents and location based services with other vehicles. This information is broadcasted by On Board Units (OBUs) [1]. This information is useful for many safety applications. For example when driver push emergency brakes, then a warning message is broadcasted to its following vehicles. All these applications jointly makes an ITS. Intelligent Traffic System aids in the organization and modernization of traffic system with the help of Vehicular Technologies.

VANET applications have many benefits, but this is the bright side of the picture. There are many security concerns as well. For example a greedy driver broadcast a false warning message that there is traffic jam ahead just to make the road clear for him as the following vehicles may change their directions. So there is huge security risk. These kinds of false messages may cause fatal results which even leads to deaths.

IEEE proposed 1609.2 [2] which uses certificates and digital signatures to prevent attacks on vehicular networks but this standard can't validate the message. For example greedy driver can still generates a false message of any accident or traffic congestion ahead on the road and receiving vehicles changes their direction as the message have valid digital signatures and certificates.

Many schemes have been proposed so far for the message validation like [3] which checks the number of vehicles reporting an event is above the certain threshold then event is considered valid otherwise invalid. The drawback of this scheme is that it has high computational overhead.

A trust based scheme helps to reduce computational overhead by checking the rating of sender vehicle. Receiving vehicles have the right to modify sender's rating upon the outcomes of events. Rating describes the trust worthiness of any vehicle, higher the rating more trustworthy the vehicle is and vice versa. For example if a vehicle broadcast a warning message about some event then the receiving vehicles checks its rating for the validation of this event. If this rating is greater than a certain threshold then the sender is considered to be trustworthy and receiving vehicle treat the message like valid event. If the rating is less than a certain threshold then the receiver confirms the information from surrounding vehicles and Road Side Units (RSUs). If the surrounding environment validates the message as true then the receiver trust the sender and increases the sender's rating otherwise decreases the rating and discard the message.

If a vehicle which broadcast a message about any event has its rating above the threshold value then the receiving vehicles just blindly trust the sender hence computational overhead is reduced as receiving vehicle doesn't need to confirm this message from its surrounding. In case if the event is not true then the rating of sender's vehicle falls down to one. If this rating falls below the certain threshold value then this vehicle is considered to be least trustworthy and its message is discarded every time.

Due to high mobility 802.11 standard protocols are not suitable for VANET; IEEE developed its extended version called IEEE 802.11p also called WAVE (wireless access in vehicular environments). This protocol is used for Dedicated Short Range Communication (DSRC). It supports many DSRC applications like collision warning and Intelligent Transportation System. This standard operates in 5.825-5.950 GHZ band divided into 7 channels with each channel of 10 MHz capable of carrying 27Mbps.

It enables reliable communication by establishing quick links and minimizing the effect of Doppler shifts, multipath propagations and exchange data in very short period of time. It also supports other higher layer protocols like 1609.2 standards.

1609.2 Standard defines security, secure message formatting, processing, and message exchange [4]. For key management, Public Key Infrastructure (PKI) is the proposed standard for VANETs. For communication and verification each vehicle has pair of key called ECDSA key: (i) private key (ii) public key.

Public key is for verification which is authorized by Certificate Authority (CA). Transportation department or car manufacturer companies can act as CA. These keys are temper proof and integrated into OBUs [5].

II. RELATED WORKS

As for the best of our knowledge there is no system that validate message like trust based event validation. We thus discuss already existing work in related topics: Threshold based event validation and VANET event validation.

Number of vehicles reporting an event is above than the threshold value determines the validity of an event [3]. This scheme focuses on both single hop and multiple hop networks, but this scheme doesn't provide desired results if number of vehicles present in a hop where any event occur are less than threshold.

The number of alerts from nearby vehicles is a strong indicator of the validity of an event [6], [7], [8]. Dietzel et al. adopts the notion of data centric [8] for event validation [9]. The main problem in this scheme is the high dissemination delay and one hop relevant. And our protocol is facilitating to distribute alerts to multi hop and provides validity indicator in them to.

III. MODEL

Fig. 1 expresses the trust based authentication in VANET. Vehicle that observes the event, broadcasts the message including its rating 'n'. Vehicles' behind the sender's vehicle certifies the event by inspecting the rating of sender vehicle as they did not observe the event by themselves i.e., it is greater than the upper threshold level. This means that rating shows the credibility of vehicle. If the rating is below upper threshold level then more proofs are needed to certify the event. If the rating is below the lower threshold level then the message is discarded. Sending vehicle cannot alter its rating; in fact the alteration is done by group of receiving vehicles depending upon the outcome of event i.e., either the event is valid or invalid. In case of valid event the rating increases by one and decreases in case of invalid event.

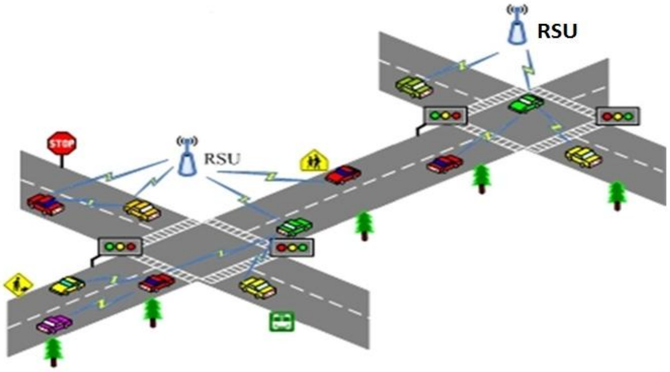

Fig. 1. VANET

IV. PROBLEM CHARACTERIZATION

Our scheme is to provide authenticated communication between vehicles in VANET. Unauthentic communication can cause serious damages. We propose trust base authentication to prevent such damages.

Threat Model: A malicious attacker may broadcast the invalid message to disturb the traffic flow. Group of nasty attackers may cause flooding and denial of services by repeatedly sending the same message and in this situation receiving vehicles may not verify every message as it exceeds the computational limit.

In our scenario, following features are already exists:

Relatively honest environment

Location of each vehicle provided by GPS

Automatic detection of event through V2V

Public Key Infrastructure (PKI) It existence means that every vehicle has valid Public and Private Key i.e., valid digital signatures.

V. A TRUST BASE AUTHENTICATION SCHEME

In trust base validation scheme a default trust (rating) level has been set to each vehicle moving in urban environment. Trust (rating) level depends upon the validation of the message forward by sender. If the message is valid, a group of vehicle will increase the rating of sender's vehicle by one, for invalid message the rating will decrease by one. Neighbour's vehicles will be responsible for the modification of sender's rating. In this scheme we define different trust (rating) level of the vehicles. Rating process will only be implemented on private vehicles. Fully trustee if the rating of the vehicle exceeds the upper threshold limit it is declared as fully trustee. Normally in urban environment public vehicles are declared to be fully trustee. Malicious vehicles are those having trust levels below the lower threshold limit. Partially trustee set to those vehicles having rating between lower and upper threshold limits. Receiving vehicle can rate only partially trustee vehicles. If the status of vehicle is fully trustee receiving vehicles blindly trust the vehicle's message and follow its instructions, such vehicles will not be rated, malicious vehicles are considered to be in danger zone and receiving vehicles will simply discard its message without any scrutiny, these vehicles will also not be rated.

In VANET every vehicle broadcasts beacon messages every 0.1 seconds, by exchanging these messages every hop will elect a 'Hop-Head' on the basis of the trust level. Selection of the hop head depends that if the vehicle is in the category of fully trustee it will be declared as a Hop-Head. If multiple vehicles are fully trustee then hop head will be selected randomly. If none of the vehicle is fully trustee then the vehicle with highest rating level will be the hop head. Vehicles will exchange their rating level by broadcasting their rating level with each other and vehicle with highest rating will select as a hop head. Now each vehicle will communicate to others through Hop-Head. This phenomenon will help to overcome the broadcasting storm.

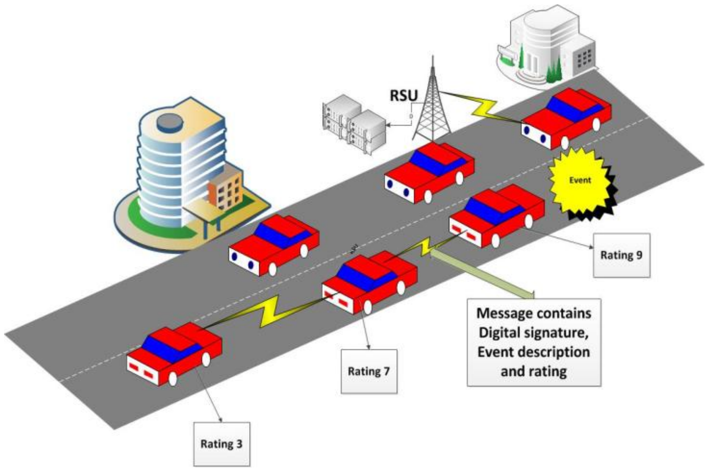
RSU
Event
Rating 9
Message contains Digital signature, Event description and rating
Rating 7
Rating 3

Fig. 2. Trust based Authentication

Flow chart of trust base authentication scheme is shown in Fig. 3.

Algorithm:

```
V(H) #set of all vehicles in a hop
R(v) #rating of sender vehicles
// beacon messages exchanged
HH# Hop-Head

HH : Rating of all vehicles checked
Hop-Head selected on the basis of highest rating

// hop-head receives alert
if (R(v) < Tmin)
drop alert
}
else
if(R(V) > Tmax)
 Forward alert
else
listen to other vehicles
 if(V(h) reporting same alert)

forward alert
increase sender's rating


else
drop the alert
decrease the rating
//check the hop head presence
goto HH
```

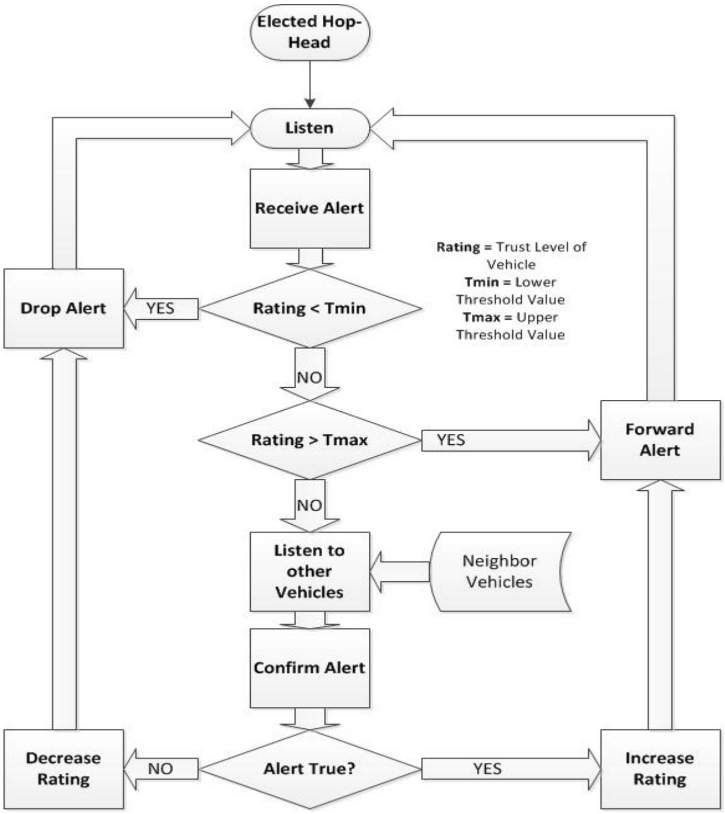

Fig. 3. Flow chart of Trust base Authentication Scheme

VI. PERFORMANCE EVALUATION

Simulations are performed in network simulator ns-2.34 [10]. Traffic file is generated in VanetMobiSim. The fixed parameter in simulation is the transmission radius 150m. Table 1 shows the simulation parameter used.

Table 1: Simulation Parameters

	Simulation Parameters	Values
1	Transmission Radius	150m
2	Simulation Time	150sec
3	Total number of Vehicles	10, 20, 30, 40
4	Packet Size	512B
5	Traffic Type	CBR
6	Traffic Load	Packet send every 1ms

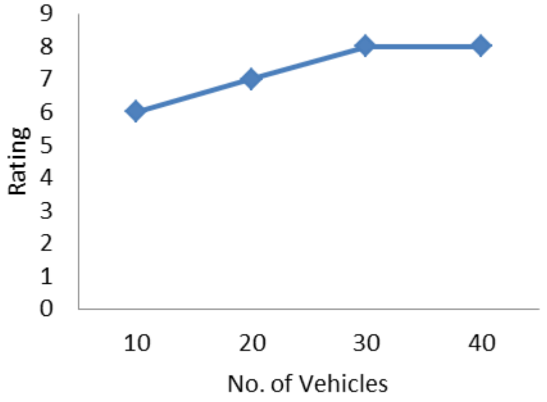

Fig. 4. Rating v/s No. of Vehicles

Fig. 4 shows that as the numbers of vehicles increases in a hop/network the average value of trust (rating) in a hop/network increases i.e., more trust full environment to report and validate an event. By increasing number of vehicles it is easy for Hop Head to validate an event and also hop head takes less time to validate an event and update the trust level (rating) of sending vehicle.

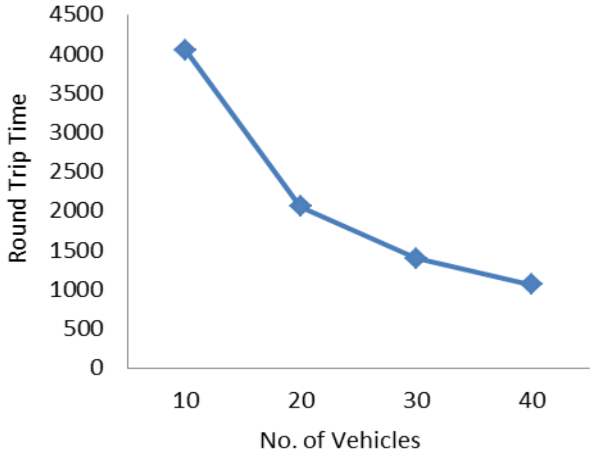

Fig. 5 Round Trip Time v/s No. of Vehicles

Fig. 5 shows that the Round Trip Time (RTT) decreases as the number of vehicles increases in a hop/network, because increasing number of vehicles causes the increase in the trustworthiness of a hop/network then it is easier for Hop Head and takes less time to authenticate an event and send back a reply message to sending vehicles to update its trust level (rating).

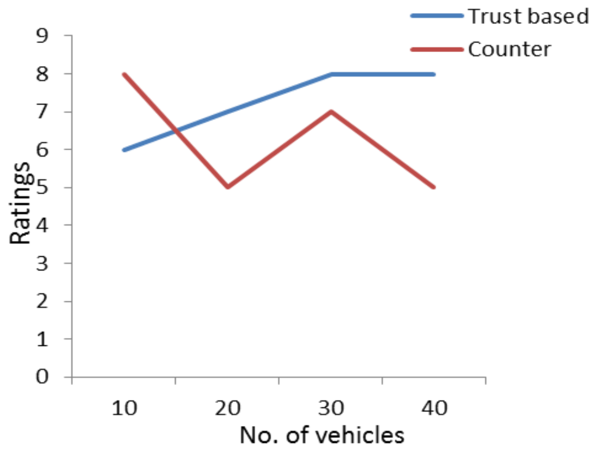

Fig. 6. Comparison of Round Trip Time by Counter-based and Trust-based

Fig. 6 shows the comparison of average trust level of a hop/network by Trust-based and counter-based scheme [3]. The behaviour of Counter-based is more abrupt as compared to Trust-based scheme. After increasing number of vehicles the trust level of Trust-based is constant while for Counter scheme it is still varying. This means that when numbers of vehicles are large in number in a hop/network then Trust-based scheme is more suitable as compared to Counter scheme.

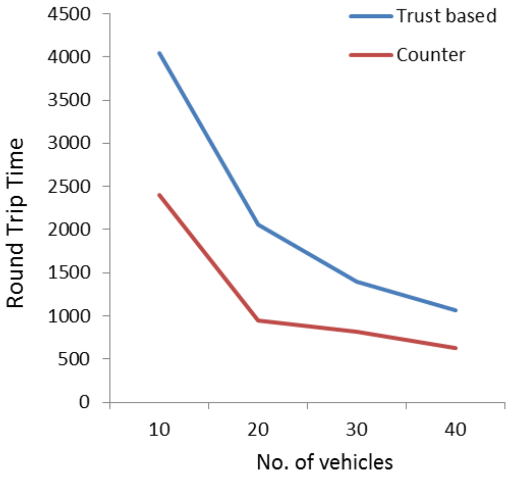

Fig. 7 Comparison of Rating by Counter-based and Trust-based

Fig. 7 shows the comparison of Round Trip Time by Trust-based and Counter-based. Counter scheme takes less amount of time as compared to Trust-based at the starting or when the numbers of vehicles are less. But as the number of vehicles increases in a hop/network the RTT of trust-based is decreases more steeply as compared to counter-based.

The novelty of the trust-based scheme is that it validates the vehicular message on the basis of the vehicle's rating. Three vehicle's rating level has been introduced fully, partially and malicious, that easily distinguishes the validity of the message. To avoid broadcasting storm in network, Hop head is also selected.

VII. CONCLUSION

The objective of this paper is to develop an efficient message authentication scheme for vehicular ad-hoc networks. Different schemes have been proposed so far but they have certain disadvantages i.e. in terms of accuracy, efficiency and bandwidth. But trust base validation scheme has overcome many problems. In comparison with Hsu-Chun Hsiao [3] scheme it has been clearly shown in graph that rating (trust) level of trust base scheme is far better than Efficient and secure threshold-based event validation scheme. Trust base scheme provides more honest and secure vehicular environment due to this factor.

In this scheme the rating level of fully trustee will not be changed, so there is need to process some checking scheme on fully trustee vehicle as well as on malicious vehicles. Malicious vehicles also got a second chance to report an event after being blacklisted.

REFERENCES

[1]. Bai, F., Krishnan, H., Sadekar, V., Holland, G. and Elbatt, T. "Towards characterizing and classifying communication-based automotive applications from a wireless networking perspective." In Proceedings of IEEE AutoNet (2006).

[2]. IEEE 1609.2 Trial use standard for wireless access in vehicular environments- security services for applications and management messages. IEEE standard 2006.

[3]. Hsu-Chun Hsiao, Ahren Studer, Rituik Dubey, Elaine Shi and Adrian Perrig. "Efficient and Secure Threshold-based Event Validation for VANETS." In Proceedings of ACM WiSEc (2011).

[4]. Ghassan M. T. Abdalla, Mosa Ali AbuRgheff and Sidi Mohammed Senouci. "Current Trends in Vehicular Ad Hoc Networks".

[5]. RAYA, M., AND HUBAUX, J.-P. "Securing vehicular ad hoc networks." J.Comput. Secur. 15 (2007).

[6]. GOLLE, P., GREENE, D., AND STADDON, J. "Detecting and correcting malicious data in vanets." In Proceedings of ACM VANET (2004).

[7]. KIM, T. H.-J., STUDER, A., ZHANG, X., DUBEY, R., PERRIG, A., BAI, F., BELLUR, B., AND IYER, A. "Vanet alert endorsement using multi-source filters." In Proceedings of ACM VANET (2010).

[8]. RAYA, M., PAPADIMITRATOS, P.., GLIGOR, V. D., ANDPIEREE HBAUX, J. "On data centric trust establishment in ephemeral ad hoc networks." In Proceedings of IEEE INFOCOM (2008).

[9]. DIETZEL, S., SCHOCH, E., KONING, B., WEBER, M., AND KARGL, F. "Resilient secure aggregation for vehicular networks." Network. Magazine. Of Global internetworking. 24 (2010), 26-31

[10]. http://www.nsnam.org/