IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

A Trust Scheme based on Event Report for Communication in VANETS (TSERC)

R. Raghu[1], J. Jayanatiya[2], A. Karunya[3], M. Meena[4], A.H. Rakshana[5]

Assistant Professor, Department of IT, Adhiyamaan College of Engineering, Hosur,Tamilnadu, India[1]

UG scholars, Department of IT, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India[2,3,4,5]

Abstract: Vehicle Ad-hoc Networks (VANETs) permits vehicles to exchange running information among them. In this paper, we propose a system that can help a vehicle to judge the trustworthiness of a message. Based on the message's trustworthiness, messages are forwarded or discarded. In the proposed system the Intrusion Detection System (IDS) is used to monitor and collect information about the network traffic issues such as sudden brake, lane changing, slow down, etc. The IDS sends the messages to Road Side Unit (RSU). The RSU receives the messages from IDS and it will send the messages to the trust authority. The Trust Authority (TA) will check the messages for its trustworthiness. If the message is false, it will drop a false message. The proposed model compared with the Trust Scheme based on Vehicles Reports of Event model and simulation results shows that the proposed scheme shows better performance in all aspects than the existing model.

Keywords: VANETs, IDS, RSU, TA, and ITS.

I. INTRODUCTION

With economic and technological growth, the motor vehicle has become a mainstream of our daily transport tool for almost everyone worldwide, but this also raises the risk of traffic injuries, nearly 60 million people have died in motor vehicle collisions, people in the twentieth century suffered the same number of casualties in World War II. Road traffic accidents are estimated to kill more than 1 million people every year if no action is taken by 2020. Recently, many analysts have paid attention to the development of safe, convenient and Intelligent Transportation Systems (ITS) comfortable travel using the latest technologies like wireless communication sensors such as actuators, a global positioning system, hardware, software are smart terminal can notify the driver and help them to avoid road accidents and control the vehicles. Communication technology will be the key to ITS. Communication among organizations on the road is generally divided into two categories, i.e. Vehicles to Vehicles (V2V) and Vehicles to infrastructure (V2I). Entities are connected to create a wireless network known as vehicle ad hoc networks (VANETs) [1], which is random to create the data for data exchange.

Many types of applications can be implemented in VANETs such as electronic braking, platooning, and traffic information systems. An automatic driver is another application that can bring revolutionary changes to people driving mode, which is now under development by many companies. Some popular automobile manufacturers have already embedded some early versions of auto-drive systems in products such as the new 2014 Mercedes-Benz S-Class. All these applications need high-quality communication. There are two features to check the quality of communication between vehicles, one is authenticity, and the other is credibility. Authenticity refers to the message received by the correct recipient once a vehicle sends it out. Credibility identifies the content of the message, which is true. With these two features, attackers often want to damage the VANET. In this study, we aim to develop a mechanism that can resolve the problems and the reliability of malicious attacks from the second aspect.

The Trust Scheme based on Vehicles Reports of Event (TSVRE) will have the attackers or malicious drivers may send fake messages to fool other drivers and fool them by changing the driving routes purpose of these attackers is to minimize the number of vehicles on the road. The target of the TSERC is to find dishonest drivers and false messages to courage honest behavior and punish malicious behavior. Most trust systems are based on historical data to create trust models. They observe the communication behavior of their neighbors and speculate on the actions of those neighbors in the future. There are basic principles in the assumption that good vehicles can continue their good behavior at a high probability. Although those mechanisms can identify malicious vehicles and messages, they are the target of new attackers.

II. RELATED WORK

In the recent period, various trust models are introduced for VANETs. The trust models are entity oriented, data-oriented, and combined models.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

2.1 Entity oriented model will rely on vehicles to generate messages.

Li et al. [2] introduced a novel announcement schema based on the reputation system for VANETs. Each vehicle's score is computed by other vehicles based on vehicle behavior, and its reputation score will be stored in the reputation server. While sending the message to the vehicle, it uses the reputation score to broadcast a message. Intermediate vehicles forward the message to the receiver by comparing the trust values, which will be generated based on trust reputation. In Wei and Chan. [3] Reputation Management Center (RMC) computes vehicle reputation values. Vehicles can broadcast, its opinion about other vehicles to RMC. RMC generates reputation value based on receive opinions of the vehicles. Vehicles depend on RMC to verify the message is the trust or not.

2.2 Data-oriented models rely on message content. These models are more suitable for VANETs.

Dozer et al. [4] introduced VARS. In this model, each vehicle appends its own opinion about the trustworthiness of the message, it is called piggybacking. In piggybacking, trustworthiness can be decided based on the experiences (history). The main drawback of this method is it relays on previous experience. Chen et al. [5] Combine multiple messages about the event from different vehicles. It depends on the sender's location to verify the event is a trust or not. It may take more time to collect multiple messages for the same event. Wang et al. [6] utilize a weighted directed graph to guide the vehicles. But it demands on-road segment parameters and the local database to store message details. The use of the local database in vehicles can lead to unnecessary resource utilization.

2.3 Entity and data-oriented models are combined to frame a hybrid model. These models take the sender's reputation and content of the message to decide the trustworthiness of the messages.

Chen et al. [7] introduced a mechanism to control message propagation. In this scheme, the message is discarded, if it is not trusted. The trust value of the vehicles is decided based on their past behavior. Koster et al. [8], divides the information into many types such as government authorities, digital information boards on freeways, vehicles on roads, and GPS-based path planning services. Koster considers all vehicles as a united group, and its trust level will be the same. Koster computes different trust values for different messages. Gerlach [15], considers the RSU and VR (Virtual Ring) to generate and store vehicle reputation value. It stores vehicle reputation in local servers (vehicles). It is based on entities (vehicles). The trustworthiness is generated or decided based on the reputation value of the vehicles. The trustworthiness is verified based on data that is oriented to vehicles.

In recent years privacy-protecting of VANETs will grab researches attraction. In privacy-protecting mechanisms, the trust models are utilized to provide privacy in routing. The trust models rely on vehicle IDS during communication to provide privacy routing. But attackers can easily capture the communication between vehicles by using vehicle identities. Frequent changes in vehicle identities may break communication capture. Few related works [9, 10, 11, 12, 13, 14] utilizes pseudonyms in privacy protection mechanisms to increase security. The vehicle identities are frequently changed securely by using pseudonyms.

III. PROPOSED SYSTEM

A Trust Scheme based on Event Report for Communication (TSERC) will use the Intrusion Detection System (IDS), Roadside Unit (RSU), and Trust Authority (TA). The IDS is used to monitor the vehicles and sends the messages to RSU. Roadside units are used to facilitate the communication between vehicles transportation infrastructure, and other devices by transferring data. Trust authority is used to facilitate and judge the trustworthiness of the messages. The intrusion detection system monitors the network traffic issues and sends the message to the RSU. The RSU sends the message to verify the trustworthiness of the messages. Trust authority verifies the trustworthiness of the messages, and it drops the message if it is false otherwise unicast the trust messages to vehicles. Figure 1 depicts the architecture of the proposed system.

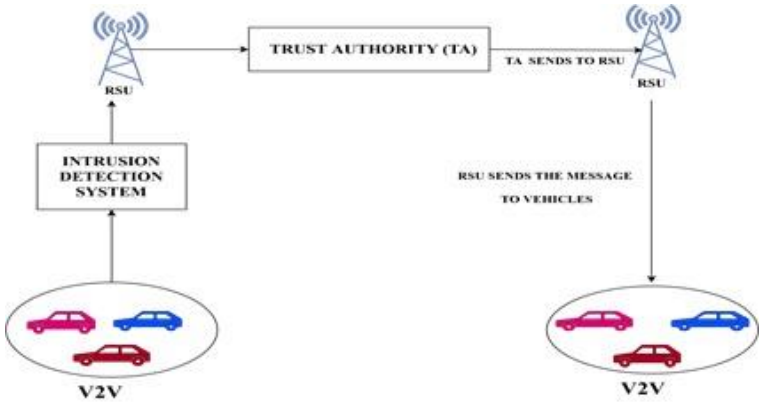

Fig. 1 Architecture of the proposed model.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

3.1 NODE CREATION:

Nodes are deployed randomly in topology. The topology consists of an "N" number of nodes with own mobility and energy. The topology referred as a graph with edges. The topology can be represented as Eq1

$$G = (N, E) \quad (1)$$

Where G indicates graph (topology), N denoted nodes and E represents edges. The edge connects the nodes.

3.2 VEHICLE TO VEHICLE COMMUNICATION:

Vehicle-to-Vehicle (V2V) Communication is a wireless network it transmits information about events. Vehicle-to-vehicle technology uses dedicated short-range communications (DSRC). Vehicles will send the message to other vehicles about the event occur in that place to change the direction of the driver.

3.3 INTRUSION DETECTION SYSTEM:

Intrusion Detection System (IDS) are alerts for detecting suspicious activity and monitoring network traffic. Although detection and reporting various primary functions, some intrusion detection systems can take action when a malicious activity or improper traffic is detected, including blocking traffic from suspicious Internet protocol (IP) addresses. IDS may conflict with an intrusion prevention system (IPS), which monitors network packets that damage network traffic, such as IDS, but with the primary goal of preventing detected and threatened. An interrupt authentication framework may help organizations in differentiating bugs or issues in their gadget systems. Now, it can be used to screen for alignment issues, and IDS is used to monitor network issues (such as braking, slowing down, and route changes).

3.4 TRUST AUTHORITY:

Trust Authority (TA) used to detect the trustworthiness of messages. TA will send only the true messages to RSU and false messages are dropped by it.

Table 1 shows the algorithm of the proposed model.

TABLE I Algorithm of the proposed model

Algorithm of the proposed model
1. Create topology ---› TP
2. Establish communication (V2V)
3. Message generation
Vehicle ---› Generate messages if event occur
if (event == true) {
generate messages
} else
no message generated
}
4. IDS ---› Monitors messages
if (message==yes) {
unicast to RSU
else
no unicast
}
5. TA ---› Receives message and verifies its trustworthiness
if (message == true){
unicast message ---› RSU
}
else
drop the message
6. RSU ---› TA
Message unicast to TA
7. RSU ---› vehicles
RSU unicasted trusted messages to vehicles.

In the algorithm, step1 to step 3 is used to create a topology for message creation and it is used to generate the message passing through the vehicles if the event occurs when vehicles crash in the road. In step 4 the IDS monitors the messages through traffic issues, and it will send the messages to RSU and in step5 the RSU sends the messages to trust

authority it will check the messages is true or false and it will send the true messages to RSU and the false messages are dropdown. The step6 and step 7 will send true messages to vehicles.

IV. SIMULATION

4.1 PARAMETERS

A. Traffic Bandwidth

The traffic bandwidth refers to the amount of data that can be sent in a certain period. It measures as a bitrate expressed in a bit per second. Traffic bandwidth calculated as in Eq2.

Bandwidth (kbps) = Receive size/ (stop time – start time)*1/60 (2)

Where kbps = kilobit per second (1 kbps =1000 bit per second)

B. Throughput

The throughput refers to the number of packets transmitted for the entire simulation time. Throughput can be calculated as in Eq3.

$T = \sum_{k=1}^{n}$ No of packets / t (3)

Where T gives throughput and t refers to the total simulation time (t=500s).

C. Bit Error Rate (BER)

The bit error rate refers to total errors occur in a transmission system. BER represented as in Eq 4.

BER = Errors / Total Number of Bits (4)

D. Network Lifetime

The network lifetime can be defined as the time from the start of simulation until the first node in the VANET runs out of energy. Eq 5 shows the mathematical model of a network lifetime.

LTN = TIE / EPS (5)

Where LTN is the Lifetime of the Network, TIE is the Total Initial Energy and EPS is the Energy / Second.

4.2 ENVIRONMENT

The network simulation is essential for a combination of VANETs on the roads and realistic computer simulations of the implementation of Apache Prior. Typically, an open-source simulator like SUMO (which handles road traffic simulation) is combined with a network simulator like TETCOS NetSim, or NS2 to study the performance of VANETs. A VANET consists of groups of moving or stationary vehicles connected by a wireless network. In table 3 simulation details are shown.

TABLE 2 Simulation details

PARAMETER DESCRIPTION	VALUE
Total number of vehicles	400
Interval starting time between two vehicles	30 s
The approximate distance of the route	2800 m
The maximum speed of a vehicle	16 m/s
The maximum speed limit on high street	24 m/s
The maximum speed limit on side pass	12 m/s
Transmit power of the radio	24m W
Sensitivity to pick up signal	-89 dB
Environment-dependent path loss exponent	4
Carrier wave frequency	7.89 GHz
Rate of malicious vehicles	0-60%
The Maximum interval time between two malicious behaviour	60 s

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

V. RESULTS

A. Traffic bandwidth:

The traffic bandwidth in the proposed system will send several messages to different vehicles at the correct time, and it will see the traffic issues that have been there in the nearer place than it will send the messages to the vehicles, it will also find the shortest path send the messages soon. But in the existing system, it will not send the messages to all vehicles at a time it will not check the messages it has been sent there will be the false messages to fool the drivers and to deviate the driver's mind-set. Fig 2 represents the performance of traffic bandwidth.

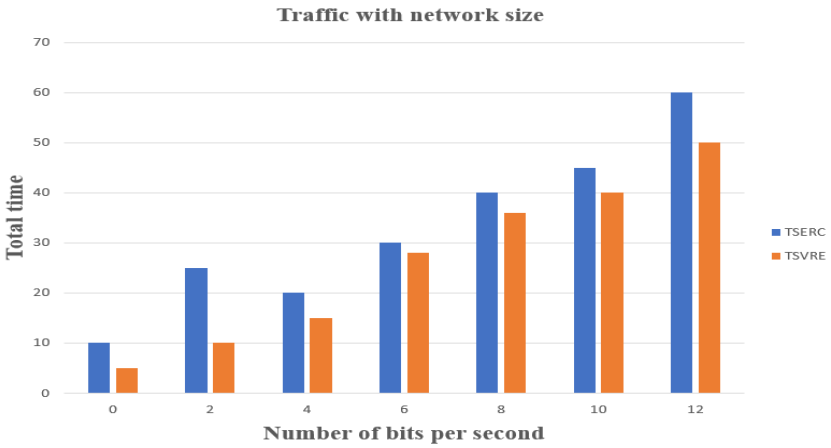

Fig. 2 Traffic Bandwidth

B. Throughput:

The TSVRE will transmit, the packets from source to destination at a slower time, it may take more time to send, a single packet to the destination. But TSERC will send the packets, as soon as it receives from the source or RSU send to other vehicles. The throughput of TSERC is higher while comparing with the TSVRE. This performance is achieved mainly due to the shortest path among the vehicles. In the proposed system, the GPSR can transmit the packets within msec. Fig 3 represents the throughput performance.

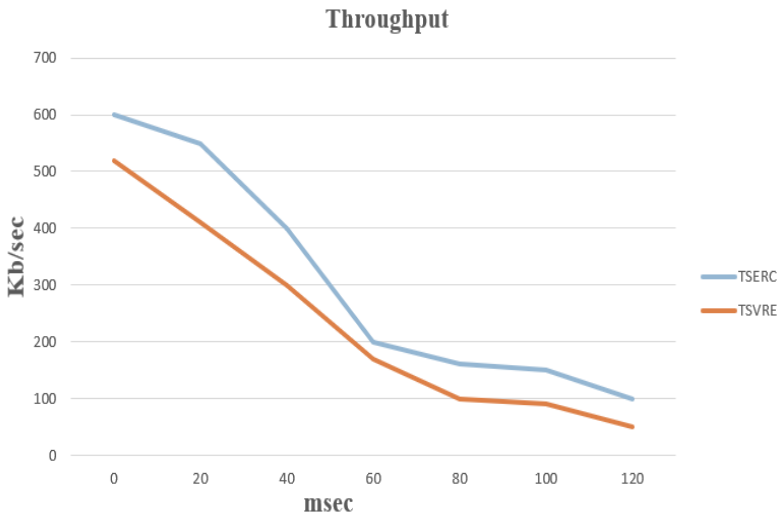

Fig 3. Throughput

C. Bit Error Rate (BER):

The BER will have no error in the proposed system will have the number of bits to transmit and receive at a time. But the existing system will have an error to transmit and receive; The messages will have an error and will affect the vehicles in that case, the traffic may also occur. The TSERC will send the bits without any error, and it will be sent in the correct time to save the vehicles. Fig 4 shows the performance of existing and proposed models with respect to BER.

IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 3, March 2020

Fig 4 Bit Error Rate

D. Network Lifetime:

In-network lifetime the TSVRE has been delayed because it as more bits up to 20, and it will not send messages quickly, it will delay due to some of the issues like a signal, slow network, etc. But TSERC as only 10 bits would not delay sending the messages that could send the messages to RSU the RSU immediately will send the messages to other vehicles without any delay. The network lifetime will have smaller bits compared with the existing system, so it will not delay sending the messages. Fig 5 represents the network lifetime.

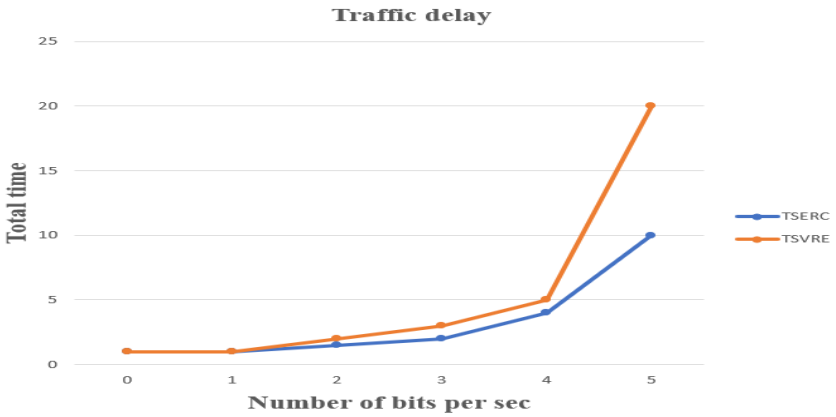

Fig 5 Traffic Delay

VI. Conclusion

In this paper, we propose a trust scheme that is used in VANETs to judge an event message's trustworthiness. In our model, the trustworthiness of the messages is verified based on events. The proposed model enforces security in message communication without relying on secure vehicle-to-vehicle communication. Without adopting authentication mechanisms our model archives better security than existing mechanisms. A simulation result shows better performance on traffic bandwidth, throughput, bit error rate and network lifetime. The usage of IDS improves throughput, bandwidth utilization. Adopting trust authority in the proposed model improves network life by avoiding attackers and reduces bit errors occurred during the transmission of messages.

References

[1]. https://slogix.in/a-trust-scheme-based-on-vehicles-reports-of-events-in-vanets.
[2]. Li, Q., Malip, A., Martin, K. M., Ng, S.-L., & Zhang, J. (2012). A reputation-based announcement schema for VANETs. IEEE Transactions on Vehicular Technology, 61(9), 4095-4108.
[3]. Wei, Y. C., & Chen, Y. M. (2014). Adaptive decision making for improving trust establishment in VANETs. In the 16th Asia-Pacific network operation and management symposium (APNOMS).
[4]. Dotzer, F., Fischer, L., and Magiera., P. (2005). Vars, a vehicle specially appointed system notoriety framework. In Proceedings of the remote versatile and sight and sound systems.

[5]. Chen, Y, - M., and Wei, Y. - C. (2013). A signal-based trust the executive's framework for improving client-driven area protection in VANETs. Diary of Communications and Networks, 15(2), 153-163.
[6]. Wang, G., and Wu, Y. (2014). BIBRM: A Bayesian derivation based street message trust model in vehicular impromptu systems. In 2014 IEEE thirteenth worldwide meeting trust, security and protection in processing and correspondence (TrustCom)(pp.481-486). IEEE.
[7]. Chen, C., Zhang, J., Cohen, R., and Ho, P. H. (2010). A trust-based message spread and assessment structure in VANETs. In Proceedings of the worldwide meeting on data innovation combination and administrations.
[8]. Koster, A. et.all, C. D. C. (2013). Utilizing trust and possibilistic thinking to manage dishonest correspondence in VANETs. In the eighth International Symposium on ISADS'07. Independent decentralized frameworks (pp.295-304).
[9]. Douceur, J. (2002). The Sybil assault. In Proceedings of the principal worldwide workshop on distributed frameworks (IPTPS).
[10]. Zhang, J. (2011) An overview of trust the board for VANETs. In 2011 International gathering on cutting edge data systems administration and applications (pp.105-112). IEEE.
[11]. J.Wan et al., "Software-de_ned mechanical web of things with regards to industry 4.0," IEEE Sensors J., DOI: 10.1109/JSEN.2016.2565621.
[12]. Z. Shu, J. Wan, D. Li, J. Lin, A. V. Vasilakos, and M. Imran, "Security in programming de_ned organizing: Threats and countermeasures," Mobile Netw. Appl., DOI: 10.1007/s11036-016-0676-x.
[13]. B. Fortz and M. Thorup, "Internet traf_c designing by improving OSPF loads," in Proc. nineteenth Annu. Joint Conf. IEEE Comput. Commun. Soc. INFOCOM, vol. 2. Tel Aviv, Israel, Mar. 2000, pp. 519_528.
[14]. Papadimitratos P, Buttyan L, Hubaux J-P, Kargl F, Kung A, Raya M (2007) Architecture for secure and private vehicular interchanges. In: IEEE ITST, pp 1–6
[15]. Gerlach, M. (2007) Trust for vehicular applications. In 8th International symposium on ISADS'07. Autonomous decentralized systems (pp. 295–304)

BIOGRAPHIES

R. Raghu[1], Working as an Assistant Professor in the Department of Information Technology at Adhiyamman College of Engineering (Autonomous), Hosur.

J. Jayanatiya[2], Pursuing B.Tech (Information Technology) in Department of Information Technology at Adhiyamman College of Engineering (Autonomous), Hosur.

A. Karunya[3], Pursuing B.Tech (Information Technology) in Department of Information Technology at Adhiyamman College of Engineering (Autonomous), Hosur.

M. Meena[4], Pursuing B.Tech (Information Technology) in Department of Information Technology at Adhiyamman College of Engineering (Autonomous), Hosur.

A.H. Rakshana[5], Pursuing B.Tech (Information Technology) in Department of Information Technology at Adhiyamman College of Engineering (Autonomous), Hosur.