International Journal of Innovative Research in Technology & Science

Received 2 June 2018, Received in revised form, 18 June 2018, Accepted 6 July 2018, Available online 25 July 2018

ISSN: 2321-1156 Volume VI Issue IV, July 2018

Attacks, Routing Protocols and Security challenges in VANET

Roshi Mishra, M. Tech Scholar Dept. of CSE, RGPM, Bhopal, M.P., India, roshimishra60@gmail.com;
Ratan Singh, A.P in Dept. of Computer Science & Engineering, RGPM, Bhopal, M.P., India, mr.ratan.proff@gmail.com;

ABSTRACT

Vehicular Ad hoc Networks are multichip networks with no fixed infrastructure in which the vehicles are communicate with each other (V to V) and vehicles are communicate with RSU (V to RSU) in dynamic environment. It consists of moving vehicles communicating with each other in different zones and continuously sharing traffic information for knowing traffic status. The responsibility of every vehicle is to forward the traffic status to requester vehicles. As same as MANET due to open medium security is always the major concern in VANET. The attacker vehicle/s is forward the large huge amount of unwanted messages to consume the network limited bandwidth or drops the data packets or traffic status packets. In this paper we proposed the IDS based V-RSU communication. RSU with IDS identified the attacker vehicles by that unusual interference in communication. The RSU collects the information from vehicles and forwarded to other vehicles or other RSU. The proposed IDS security algorithm is applied to RSU to recognize the attacker vehicle activities. The RSU after identified it block their functionality of communication. The proposed security scheme is identified the attacker vehicle and block their presence in network. The aim of this research is to providing security against malicious attack, to allow new proposed models to build their work on solid realistic models against packet dropping attack. In this proposed scheme, vehicles obtain traffic data when they pass by a road side unit (RSU) and then share the data after they travel out of the RSU's coverage. A basic issue of proposed security scheme is how vehicles effectively work in presence of attacker. The simulation results are confirmed that RSU provides naught dropping of packets in presence attacker e.g. the indication of secure communication. The previous research work in security are provides the guidelines in field of security to protect network from different attacks. The packet dropping attack is dropping the all traffic information and also proposed scheme is block attacker existence and improvement network performance.

Keywords: - IDS, Security, Routing, RSU, Packet dropping attacker, VANET.

Introduction

A wireless communication is ubiquitous because of its flexibility to adapt to different scenarios. Mobile Ad Hoc Networks (MANETS) is a term coined for the continuously varying network topology handheld mobiles devices. Vehicular Ad Hoc Networks (VANETS) is one of its types. It deploys the concept of continuously varying vehicular motion. The nodes or vehicles as in VANETS can move around with no boundaries on their route and rate. (VANET) involves vehicle to vehicle (V2V), vehicle to roadside (V2R) or vehicle to infrastructure (V2I) communication [1].VANET generally consist of On Board Unit (OBU) and Roadside Units (RSUs). OBUs enables short-range wireless adhoc network to be formed between vehicles. Each vehicle comprises of hardware unit for determining correct location information using GPS. Roadside Units (RSUs) are placed across the road for infrastructure communication. The number of RSU to be used depends upon the communication protocol.

VANET provide assistance to vehicle drivers for communication and coordination among themselves in order to avoid any critical situation through Vehicle to Vehicle communication [2] e.g. road side accidents, traffic jams, speed control, free passage of emergency vehicles and unseen obstacles etc. Besides safety applications VANET also provide comfort applications to the road users. Due to the dynamic nature of nodes in VANET the routing of data packets is much complex. Several factors like the type of the road, daytime, weather, traffic density and even the driver himself affect the movements of vehicles on a road. Hence, the network topology change frequently, and the routing protocol used has to adapt itself to these instantaneous changes continuously.

VANET Overview

Intelligent Transportation System (ITS)

In Intelligent Transportation Systems (ITS) [3], each vehicle broadcast the information to the vehicular network or transportation agency, which then uses this information to ensure safe and free-flow of traffic. The possible communication configurations in ITS are inter-vehicle, vehicle to roadside, and routing-based communications [4]

Received 2 June 2018, Received in revised form, 18 June 2018, Accepted 6 July 2018, Available online 25 July 2018

all this configurations requires precise and up-to-date surrounding information.

Inter-vehicle Communication

Inter-vehicle communication support multi-hop multicast/broadcast over a multiple hops to a group of receivers. ITS is generally concerned with the activity on the road ahead and not on road behind. Naive broadcasting and intelligent broadcasting [4] are the two message forwarding methods used in inter-vehicle communications Naive broadcasting believes on the periodic broadcasting of message, if the message is from a vehicle behind it then vehicle ignores the message, but if the message comes from a vehicle ahead then the receiving vehicle sends its own broadcast message to vehicle behind it. Due to the large number of messages, probability of message collision increases which lowers the message delivery rate and increases its time of delivery. The problem is overcome using intelligent broadcasting. It uses acknowledgment address limiting the number of messages broadcast for emergency events only.

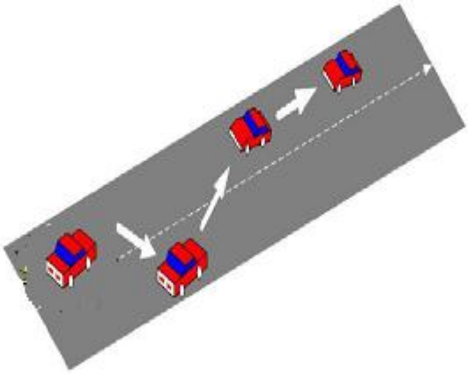

Fig.1. Inter-vehicle communication

Vehicle-to-roadside communication

In this type of communication, vehicle communication is done using single hop broadcasting method. This type of configuration provides ample amount of bandwidth link between communicating parties. In vehicle to roadside communication the maximum load for proper communication is given to the road side unit, it controls the speed of vehicle when it observes that a vehicle violates the desired speed limit, it delivers a broadcast message in the form of an auditory or visual warning, requesting the driver to reduce speed. Vehicle-to-roadside communication is shown in Fig. 2. Here RSU sends broadcast messages to all the equipped vehicles.

Routing-based communication

Multi-hop unicast method is used in routing-based communication configuration. While sending the message, the vehicle sends message using multi-hop fashion until it reaches to the desired vehicle. Receiving vehicle then sends a unicast message to the requested vehicle. Fig. 1 and Fig.2 shows the routing-based communication in VANET. Here any sender vehicle sends message to destination vehicle C using routing protocols. Standards for wireless access in VANET.

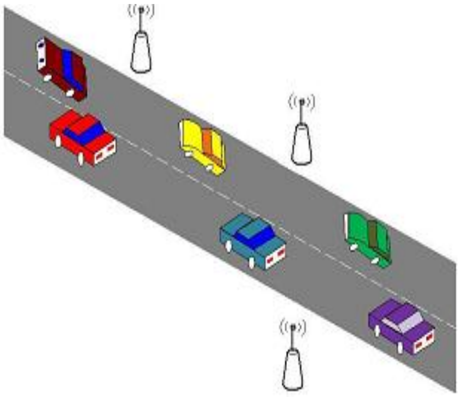

Fig. 2. Vehicle-to-Roadside Unit Communication

Standards for wireless access in VANET

Vehicular environment supports different communication standards that relate to wireless accessing. The standards are generally helpful for the development of product to reduce the cost and it also helps the users to compare competing products. These standards are as follows: Fig. 2. Vehicle-to-Roadside Unit Communication.

A. Dedicated Short Range Communication (DSRC)

It provides a communication range from 300m to 1Km. The V2V and V2R communication takes place within this range. DSRC [5, 6] uses 75MHz of spectrum at 5.9GHz, which is allocated by United States Federal Communications Commission (FCC). This provides half duplex, 6-27 Mbps data transferring rate. DSRC is a free but licensed spectrum. Free means FCC does not charge for usage of that spectrum and licensed means it is more restricted regarding of its usage. The DSRC spectrum is organized into 7 channels each of which is 10 MHz wide. Out of these 7 channels, one of the channels is reserved only for safety communication. Two channels are used for special purpose like critical safety of life and high power public safety and rests of the channels are service channels.

IEEE 1609-standards for Wireless Access in Vehicular Environments (WAVE), It is also known as IEEE 802.11p. It

Received 2 June 2018, Received in revised form, 18 June 2018, Accepted 6 July 2018, Available online 25 July 2018

supports the ITS applications, for a short range communications. In WAVE, V2V and V2R communication uses 5.85-5.925 GHz. frequency range. It provides real time traffic information improving performance of VANET. It also benefits the transport sustainability. It contains the standard of IEEE 1609 [7, 8, and 9]. This is upper layer standard. It uses Orthogonal Frequency Division Multiplexing techniques to divide the signal into various narrow band channels. This also helps to provide a data transferring rate of 3, 4.5, 6, 9, 12, 18, 24 and 27 Mbps in 10 MHz channels.

Routing Protocols Description

In MANET currently, there are mainly two types of routing protocols in MANETs, namely, topological routing and geographic routing [10, 11, 12]. In topological routing, mobile nodes utilize topological information to construct routing tables or search routes directly. In geographic routing, each node knows its own position and makes routing decisions based on the position of the destination and the positions of its local neighbors.

The investigation of topological routing has lasted for decades, and a variety of topological routing protocols have been developed. Generally, the topological routing protocols can be further divided into two categories, namely, proactive routing and reactive routing. In proactive routing, route information is propagated periodically in the network.

Thus, each node can maintain a routing table containing route entries to other nodes. When packets arrive at an intermediate node, the next hop can be selected by looking up the routing table. Destination-sequenced distance-vector (DSDV) [7] routing is referred to as a well-known example of proactive routing. In reactive routing, no routing table is maintained at the nodes. When needed, the source node triggers a route search procedure to discover the routing path to the destination. Both ad hoc on-demand distance vector (AODV) [8] routing and dynamic source routing (DSR) [9] are referred to as representative examples of reactive routing. By exploiting the strength and avoiding the weakness of each type, hybrid topological routing protocols are proposed, for example, Zone Routing Protocol (ZRP) [10], which maintains a k-hop routing zone proactively and triggers the inter-zone route discovery reactively.

Types of attack in VANET

Attacks on Mobile Ad hoc Networks can be classified as active and passive attacks, depending on whether the normal operation of the network is disrupted or not [13, 14, 15].

***Passive Attack:* -** In passive attacks, an intruder the data exchanged without altering it. The attacker does not actively initiate malicious actions to cheat other hosts. The goal of the attacker is to obtain information that is being transmitted, thus violating the message confidentiality. Since the activity of the network is not disrupted, these attackers are difficult to detect.

***Active Attack:* -** In active attacks, an attacker actively participates in disrupting the normal operation of the network services. A malicious host can create an active attack by modifying packets or by introducing false information in the ad hoc network. It confuses routing procedures and degrades network performance. Active attacks can be divided into internal and external attacks.

***External Attack:* -** External Attacks are carried by nodes that are not legitimate part of the network. In external attacks, it is possible to disrupt the communication of an organization from the parking lot in front of the company office.

***Internal Attack:* -** Internal Attacks are from compromised nodes that were once legitimate part of the network. In ad hoc wireless network as authorized nodes, they are much more severe and difficult to detect when compared to external attacks.

***Attacks Classification:* -** The types of attacks against can be classified is as follows:

***Black Hole Attack:* -** This is one of the security attack occur in VANET. In this attack the attacker node refuses to participate or even drop the data packet [16]. Hence the effect of this type of attack is most dangerous to the vehicular network.

***Malware:* -** Malware is a malicious software whose aim to disrupt the normal operation. This attack is carried out by insider. This attack is introduced in the network when the software update is received by car's VANET units and roadside station.

***Broadcast Tampering:* -** In this type of attack the attackers introduces false safety messages into the network. This message sometime hides the traffic warnings [17]. This leads to the critical situation like accidents and road congestions'.

***Spamming*: -** Spamming are the messages which are of no use to the users like advertisements. The aim of such attack is to consume bandwidth and increase the transmission

Received 2 June 2018, Received in revised form, 18 June 2018, Accepted 6 July 2018, Available online 25 July 2018

ISSN: 2321-1156 Volume VI Issue IV, July 2018

latency. Due to lack of centralized administration the controlling on such attack is difficult.

***Greedy Drivers:* -** Greedy drivers are those who try to attack for their own benefit. These drivers cause overload problem for RSU this leads to delay in service to the authorized users. On increasing number of such drivers the authorized users faced slow services.

***Denial of Service:* -** Denial of Service (DOS) [18] is one of the most serious level attacks in vehicular network. In DOS attack, the attacker jams the main communication medium and network is no more available to legitimate users. The main aim of DOS attacker is to prevent the authentic users to access the network services. DOS attack also causes the attacks like DDOS (Distributed Denial Of service) which is one of the sever attack in vehicular environment. The aim of this attack is to slow down the network. Jamming is also one of the kinds of DOS attack which jams the channel, thus not allowing other users to access the network services.

Replay Attack:-This attack happens when an attacker replays the transmission of earlier information to take advantage of the situation of the message at time of sending [19].

Tunneling: - This attack happens when an attacker connects two distant parts of the Adhoc network using an extra communication channel as a tunnel. As a result, two distant nodes assume they are neighbors and send data using the tunnel [20]. The attacker has the possibility of conducting a traffic analysis or selective forwarding attack.

***Message Tampering:* -** In this attack the valuable or even critical traffic safety messages can be manipulated. This is done by attacker by modifying, dropping or corrupting the messages [21].

Literature Survey

The work done in field of VANET security is mentioned in this section. The previous works is not very old but consider the recent researches for survey.

This paper [22] proposed a mechanism for consistent communication in VANET all the way through proficient routing protocol. If malicious nodes are there in a VANET, they may effort to reduce network connectivity and thereby undermine the network's security by pretending to be cooperative but in achieve dropping any data they are predestined to pass on. The developed protocol is capable to identify malicious node in network, and consequently change the route for packet distribution. It must compute the routes in a fast, loop free, optimal resource usage, and up to date approach. Additionally, they must keep the procedure of route continuance as confined as possible.

In this paper [23] the conviction calculation is based on position of vehicle. Sender vehicle broadcasts its route request message (RREQ) for finding the secure location within the communication range in the network. Sender vehicle receives the route reply message (RREP) from various vehicles then source vehicle computes ratio of vehicles to find out that weather a particular location is trusted or not. Computation of trusted location using RSU- Source vehicle now asks to RSU about location. Source vehicle will receive location information from RSU and that information will be fully trusted by RSU. If prerecorded information is not present to RSU about particular location. Then RSU sends Reply packet to TA (as police vans, ambulance and post office vehicles) and ask for suggestions. Now TA will send reply to RSU and then RSU will send message to source vehicle.

In this paper [23], they have understood a VANET in which nearby vehicles can communicate into the same direction only and with those vehicles which are available within the network range. Geographical positioning and timing related conditions are fulfilled with global positioning services receivers. To get the time instantaneous either at receiving side or sending side, there is no any disturbance. All the vehicles have their matchless individuality number which is also known as vehicle identity. This vehicle identity can be a permanent for a particular vehicle during its life-cycle but it can also be ruined if it is found as a malicious vehicle, a graphical overview of algorithm into the network. Vehicles have their own public key (*KX*) and private key which are useful to encrypt or to decrypt the information either at sender side or receiver side.

In this paper [24], they consider the security against DoS attacks. Actually the mobile vehicles or nodes in VANET share a wireless medium as well a radio signal can be pretentious, causing the service to be corrupted. There are a collection of different attack strategies that an attacker can carry out in order to obstruct. For each intermediate node the value of the PDR (Packet Delivery Ratio) is intended in different time instant. In the case where the packet rate successfully delivered decreases. If its value is below a certain threshold, and attacked node receives the same packet multiple times a DoS attack is detected. This mechanism can be used to improve the performance of network.

Received 2 June 2018, Received in revised form, 18 June 2018, Accepted 6 July 2018, Available online 25 July 2018

Simulator Overview And Results Description

(A) Proposed Approach: In proposed work we will work on two scenarios. First one is [1] (work of base paper) and in second one is work on detecting and preventing attacker vehicles in network. We proposed a fixed stationary Road Side Units (RSU) in network at each terminal. Here proposed work is done in Vehicle to Vehicle (V to V) and Vehicle to RSU (V to RSU) both communications. The main part of proposed work is, if the RSU is interact in communication for maintaining the secure communication and observe the conditions of traffic mismanagement. The vehicles are obtaining the incomplete or wrong traffic information but the traffic conditions are different According to if there are many nodes with network is to transmit right traffic information, in network. Furthermore, in real life various reactions from drivers will happen, it will generate multiple traffic status messages but these messages are different not related to traffic status information and the meaningful information of traffic status is drop by attacker vehicles in VANET.

(B) ***Simulator Tool:*** Network simulators conceive to model real world networks. The concept being that if a system is modeled, then options of the model are modified and therefore the results analyzed. Because the method of model modification is comparatively low price then a good form of situations is analyzed at low cost (relative to creating changes to a true network).

Network Simulator (NS-2) [38] is an Object Oriented (OO) based discrete event driven simulator that was originally developed at University of California-Berkely. The programming it uses is C++ and OTcl (Tcl script language with Object-oriented extensions developed at MIT). The usage of those 2 programming language has its reason. The most important reason is owing to the inner characteristics of those 2 languages. C++ is efficient to implement a design however it's not terribly simple to be visual and diagrammatically shown. It is not simple to change and assembly completely different parts and to vary different parameters while not an awfully visual and easy-to-use descriptive language.

(c) RESULTS DESCRIPTION:

(i) Simulation Parameters: - The simulation parameters like area of simulation are 800m*800m in transmission range of 550m. Rest of them that are considering for simulation is mentioned in table 1.

(ii) Performances Metrics: The performance of network is evaluated in case of AODV, Whole attack and Secure IDS scheme.

PACKET DELIVERY RATIO or FRACTION (PDR OR PDF) The ratio between the numbers of packets originated by the application layer to those delivered to the final destination.

THROUGHPUT ANALYSIS the numbers of senders are sends data packets to receiver and receiver is received data from intermediate nodes. The data receiving in per unit of time is counted by throughput performance metrics.

TABLE 6.1 Simulation Parameter

Area of Simulation (meters)	800m*800m
Mobile Nodes	10, 30, 50
Radio Range (meters)	550
Transferring Mode	Unicast through Unipath
Maximum Speed (ms)	50 m/s
Routing Protocol	AODV
Traffic	CBR over UDP
Simulation Time (seconds)	300
Packet Size	512 bytes

PACKET RECEIVING ANALYSIS the number of packets are received at destination is shows the actual performance of network. The better packet receiving is the sign of better performance.

(iii) Result Analysis:- Throughput Analysis: The follower vehicles are continuously sends the traffic request for recognizes the traffic status but this information is also destructive if it is not receive any response in network e.g. perform by packet dropping attacker to creating a situation that vehicles are not decided and follow to destination path very slowly. In this graph the dropping analysis throughput performance is measured and observes that the due to attacker data receiving is minimizes. Their effect is throughput is degraded. These packets receiving is very less as compare to existing (base work) and proposed work. The proposed security scheme against malicious attack is secure

Received 2 June 2018, Received in revised form, 18 June 2018, Accepted 6 July 2018, Available online 25 July 2018

the network performance and providing packets delivery as equivalent to normal VANET performance

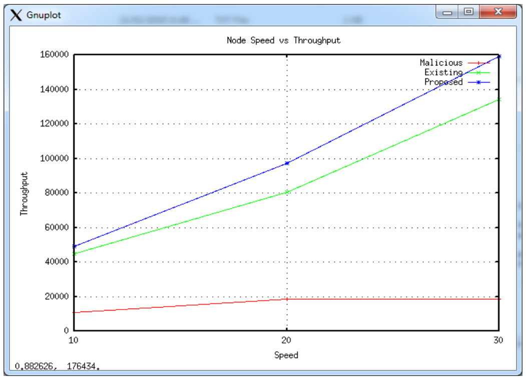

Fig.1 Throughput Analysis

Packet Dropping Analysis: The number of traffic status packets are drop in network because of attacker misbehavior. The routing protocol existence is also in VANET and the vehicles are continuously sends and receive traffic data in network for better driving facility on roads. In this graph only data drop of attacker vehicle is evaluated. Here the attacker presence is drop huge amount of data in network. This data is drop due to vehicles are chose the wrong path or misguided by attacker acknowledgement. But after applying secure RSU based scheme in normal RSU to V communication, the security criteria is enhanced for reliable communication and reduces the data drop in network.

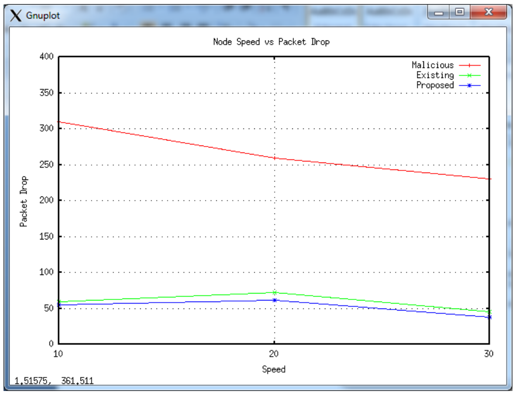

Fig.2 Packet Dropping Analysis

PDR Performance Analysis: In VANET only short information (about traffic status and something un-happened on roads like accidents) are deliver to nearby vehicles. In this graph the PDR performance of packet dropping attacker, existing scheme and proposed RSU based communication is assessed and observes that the proposed scheme is really effective to identify the existing and proposed work shows performance about more than 99% performance as compare to attacker existence in network. The attacker performance in network not more than 27% and also evaluated up to end of simulation time. The proposed scheme performance is better than the existing performance. The attacker existence is absolutely blocked by RSU for providing secure communication between vehicles

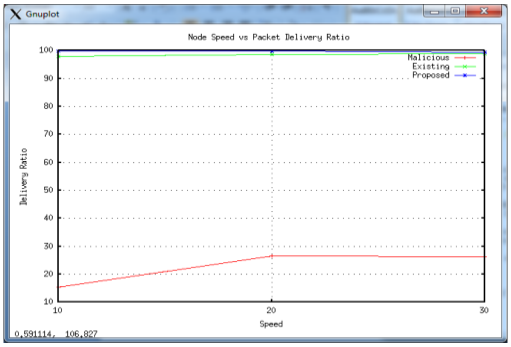

Fig.3 PDR Analysis

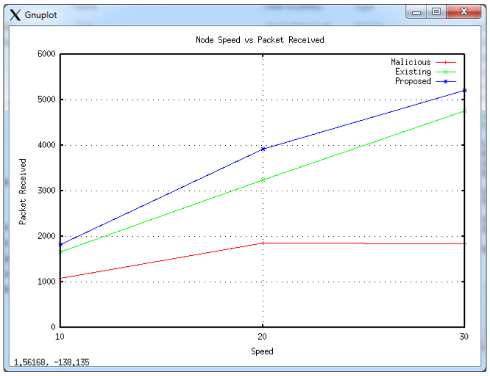

Fig.4 Packet Receiving Analysis

Packet Receiving Analysis: Each and Every vehicle is communicated with each other through established connection for receiving current traffic status. The vehicles are drive on that path according to the traffic information of beginning vehicles. The number of traffic data is received by vehicle is shows that the direction and traffic condition of road are also better. In this graph the packet receiving performance of in presence of attacker is really very poor and after applying proposed IDS security or communication done in presence of RSU is improves the performance of VANET. The packet receiving of proposed security and existing work is improves the packet receiving and reaches to more than 5000 packets in network.

Conclusion

The VANET network is designed for communication of vehicles to transfer and receive traffic status information for smart road ways. All the vehicles are containing the On Board Unit (OBU) that generate the signals of traffic status and also receive the traffic information to other vehicles. In

International Journal of Innovative Research in Technology & Science
Received 2 June 2018, Received in revised form, 18 June 2018, Accepted 6 July 2018, Available online 25 July 2018
ISSN: 2321-1156 Volume VI Issue IV, July 2018

this network also the communication is not easy because the vehicles having different mobility speed and they are communicate with each other without any administrator. The attackers are easily affected the network performance by that vehicles are not communicate properly. The previous work is discussion is provides the novel idea of simulation proposed security algorithm. In this research we proposed a new secure IDS algorithm to detect the malicious vehicles and disabled their communication capabilities for further communication in network. The three scenarios are proposed in this research. The first module of attacker presence is evaluated in different mobility speed and node density scenario in network. In Second module simulate the already implemented scheme but in third proposed RSU based communication with including the proposed IDS scheme is not only detect but also prevent from packet dropping attacker in network. The main advantage of applying IDS in V to RSU is that, if the attacker is detected then their particular information is easily broadcast to all the RSU for alert in future from that malicious vehicle. After all this information are broadcasting after block the malicious vehicle/s. The proposed security scheme is provides zero attacker infection and minimized packet dropping of traffic packets. The minimization in delay is represents the better vehicle movement. The proposed security scheme is provides better performance as compare to existing newly proposed scheme in VANET. In VANET network road accidents and road construction information issues are also affected the network performance, the malicious driver is the main obstacle for forwarding the important message to other driver. In future we proposed the novel security scheme to packet dropping attack and flooding attack in network. The security is also applied to Vehicle to Vehicle (V-V) communication and attackers are detected by the available bandwidth consumption.

References

[1]. Kawashima, Hironao. "Japanese Perspective of Driver Information Systems."Transportation 17, no. 3 (1990): 263-284.

[2]. Harsch, Charles, Andreas Festag, and Panos Papadimitratos. "Secure position-based routing for VANETs." In Vehicular Technology Conference, 2007. VTC-2007 fall. 2007 IEEE 66th, pp. 26-30. IEEE, 2007.

[3]. Sun, Jinyuan, Chi Zhang, and Yuguang Fang. "An id-based Framework Achieving Privacy and Non-Repudiation in Vehicular Ad Hoc Networks." In Military Communications Conference, 2007. MILCOM 2007. IEEE, pp. 1-7. IEEE, 2007.

[4]. Zeadally, Sherali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan. "Vehicular Ad hoc Networks (VANETs): status, results, and challenges." Telecommunication Systems, pp-1-25, 2010.

[5]. Yin, Jijun, Tamer ElBatt, Gavin Yeung, Bo Ryu, Stephen Habermas, Hariharan Krishnan, and Timothy Talty. "Performance evaluation of safety applications over DSRC vehicular ad hoc networks." In Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, pp. 1-9. ACM, 2004.

[6]. Guo, Jinhua, and Nathan Balon. "Vehicular Ad Hoc Network and Dedicated /short Range Communication Chapter. Available at link http://www. nathanbalon. com/project/cis95, 2006.

[7]. Z. J. Haas and M. R. Pearlman, “The Performance of Query Control Schemes for the Zone Routing Protocol,” IEEE/ACM Transaction Network, Vol. 9, No. 4, pp. 427–38, 2001.

[8]. Jiang, Daniel, and Luca Delgrossi. "IEEE 802.11p"' Towards an international standard for Wireless access in Vehicular environments." In Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE, pp. 2036-2040. IEEE, 2008.

[9]. "IEEE P802.11p/D3.0, Draft Amendment for Wireless Access in Vehicular Environment (WAVE)”, July 2007.

[10]. Watfa, Mohamed. Advances in Vehicular Ad-Hoc Networks: Developments and Challenges. Information Science Reference, 2010.

[11]. Paul, Bijan, Md Ibrahim, Md Bikas, and Abu Naser. "VANET Routing Protocols: Pros and Cons." arXiv preprint arXiv:1204.1201 (2012)

[12]. Kumar, Rakesh, and Mayank Dave. "A Comparative Study of Various Routing Protocols in VANET." arXiv preprint arXiv: 1108.2094 (2011).

[13]. Raya, M., & Hubaux, J. (2005). The security of vehicular ad hoc networks. In Proceedings of the 3rd ACM workshop on security of ad hoc and sensor networks (SASN 2005) (pp. 1–11), Alexandria, VA.

[14]. Sumra, Irshad Ahmed, Iftikhar Ahmad, Halabi Hasbullah, and J-L. bin Ab Manan. "Classes of Attacks in VANET." In Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, pp. 1-5. IEEE, 2011.

[15]. Fuentes, José María de, Ana Isabel González-Tablas and Arturo Ribagorda. "Overview of security issues in Vehicular Ad-hoc Networks." (2010).

[16]. Sharma, Sheenu, Roopam Gupta, M. Tech Student Reader, RGPV SOIT, and RGPV UIT. "Simulation

Received 2 June 2018, Received in revised form, 18 June 2018, Accepted 6 July 2018, Available online 25 July 2018

ISSN: 2321-1156 Volume VI Issue IV, July 2018

Study Of Blackhole Attack in the Mobile Ad hoc Networks." Executive Development 21 (2008).

[17]. Krishnamurthi, Niyant, Anurag Ganguli, Abhishek, Tiwari, Bao-Hong Shen, Joseph Yadegar, and Gregory Hadynski. "Topology control for future airborne networks." In Military Communications Conference

[18]. Ahmed Soomro, Irshad, Halabi Hasbullah, and Jamalul-lail Ab Manan. "Denial of Service (DOS) Attack and Its Possible Solution in VANET", pp. 411-415, 2010.

[19]. Parno, Bryan, and Adrian Perrig in , "Challenge in Securing Vehiclur Ad hoc Networks", In Workshop on Securing Vehicluar Communication in Wireless Topics in Networks (HotNets-IV), pp. 1-6. 2005.

[20]. Panigrahi, Sunil Kumar, Soubhik Chakraborty, and Jibitesh Mishra. "A Statistical Analysis of Bubble Sort in terms of Serial and Parallel Computation." (2012).

[21]. Leinmüller, Tim, Levente Buttyan, Jean-Pierre Hubaux, Frank Kargl, Rainer Kroh, Panagiotis Papadimitratos, Maxim Raya, and Elmar Schoch. "Sevecom-secure vehicle communication." In Proceedings of IST Mobile Summit, 2006.

[22]. Roshan Jahan Preetam Suman., “Detection of malicious node and development of routing strategy in VANET", 3rd International Conference on Signal Processing and Integrated Networks (SPIN), 2016.

[23]. Kumud Dixit Priya Pathak Sandeep Gupta, "A New Technique for Trust Computation and Routing in VANET", IEEE, 2016.

[24]. Trupil Limbasiya, Debasis Das, "Secure Message Transmission Algorithm for Vehicle to Vehicle (V2V) Communication", IEEE, 2016

[25]. Khaoula Jeffane, and Khalil Ibrahimi, "Detection and Identification of Attacks in Vehicular Ad-Hoc Network", IEEE, 2016.