International Journal of Computer Architecture and Mobility (ISSN 2319-9229) Volume 3-Issue 10, December 2015

A Secure RSU based Vehicular Communication against Hole Attack in VANET

Shahnawaz. Ahmad Siddiqi
M Tech Scholar,
Department of Electronics and Communication ,
All saints' collage of Technology , Bhopal
Siddiqui.fine@gmail.com

Zaheeruddin
Assistant professor,
Department of Electronics and Communication Engineering
All Saints' collage of Technology , Bhopal
zaheeruddin18@gmail.com

Abstract—**Vehicles in Vehicular Ad hoc Network (VANET) are communicating with each other for confirming or forwarding the traffic status without any presence of centralized authority. The attacker vehicles are take advantages of it and forward the large huge amount of unwanted messages to consume the network limited bandwidth or drop the data packets or traffic status packets. In this paper we proposed the secure VANET communication in presence of RSU. RSU 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 Hole Attack Prevention (HAP) security algorithm is applied to RSU to recognize the attacker vehicle activities. The RSU after identified it block their functionality of communication. We assume that RSUs are deployed along the highway which is at least several kilometers far from each other. On the highway, maybe some vehicles travel faster or slower than average, but we assume the majority of vehicles travel in normal or similar velocities. 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 Hole 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.**

Index Terms—**RSU, VANET, Attack, Security, HAP, routing**

INTRODUCTION

VANETs are a subset of MANETs (Mobile Ad-hoc NETworks) in which communication nodes are mainly vehicles. As such, this kind of network should deal with a great number of highly mobile nodes, eventually dispersed in different roads. In VANETs, vehicles can communicate each other Vehicle-to-Vehicle communications (V to V)[1]. Moreover, they can connect to an infrastructure Vehicle-to-Infrastructure or RSU (V to I or V to RSU) to get some extra communication service. This infrastructure or RSU (Road Side Unit) is assumed to be located along the roads. VANETs are considered a subclass of MANET [1] but there some differences like as topology change rapidly with high speed vehicles, high probability of network fragmentation since there are speedy vehicles, no strict limitations of power consumption, operation at large scales inside cities and their edges and high ways, and depending on vehicles behaviors in response or reaction for delivered messages [2].

The unique characteristics [3] of VANET are the high mobility and rapidly changing network topology caused by the high travelling speed of the nodes, the constraint pattern due to the restricted roads, limitations of bandwidth due to the absence of a central coordinator that controls and manages communications between nodes, disconnection problems owing to the frequent fragmentation in the networks and signal fading, caused by objects that form obstacles between the communicating nodes.

VANET security [4, 5] is the main issue nowadays to handle because many malicious drivers are entering into the network to create disruptions and reduce the network performance. Among all the challenges of the VANET, security got less attention so far. VANET packets contains life critical information hence it is necessary to make sure that these packets are not inserted or modified by the attacker; likewise the liability of drivers should also be established that they inform the traffic environment correctly and within time. These security problems do not similar to general communication network. The size of network, mobility, geographic relevancy etc makes the implementation difficult and distinct from other network security.

In this paper we proposed a security scheme against Hole attack in VANET. Here the Hole attacker is create the 'gaps' in between vehicles by that the vehicles speed are slowed and the infection is affected the performance of normal vehicles. The proposed scheme is applied with V to RSU communication for maintaining the security and forwarded the attacker vehicle information to all rest RSU and their surrounding vehicles. The proposed prevention scheme is block the attacker malicious activities and provides secure communication in VANET.

Network Model

Network entities can be classified into three categories [6] in VANETs, the authority and application servers, road side infrastructure and nodes.

The authority and application servers:- are powerful workstations which are responsible for management and service data provision respectively. The authority knows all keys and is in charge of service scheduling. Application servers provide service data to vehicles. They can be maintained either by the authority or by third party operators. We assume that the authority and application servers have powerful processing ability. Thus, we ignore their computation time in this paper.

Road side infrastructure:- consists of RSUs deployed at the road sides which are in charge of data collection and distribution. RSUs are connected to the authority through wired network and communicate with vehicles through radio.

Nodes:- are ordinary vehicles on the road that can communicate with each other and RSUs through wireless. We assume that each vehicle is equipped with a differential GPS receiver with accuracy on the order of one meter [7] and an on board unit (OBU) which is in charge of all communication and computation tasks.

VANET Mobility Factor

Vehicular mobility is actually related to cars, railways, bicycles, motor bikes and anything that moves on wheels in roads. As for cars in VANETs, there are many factors that affect their mobility, such as [8, 9]:-

A. Street construction

Vehicles' movement is determined by the streets, their directions and traffic signs/ lights. It is also affected by the presence of intersections and whether they have single lane or multiple lanes, one way or two-way streets. Intersections will lead to speed reduction, high nodes' density and the need to assign a probability value to predict the turning direction to each vehicle in the simulation. Single lane roads do not allow overtaking and the speed is limited and affected by vehicles ahead while in multiple lane roads overtaking is allowed and driving is considered easier and safer.

B. Block size

This can be considered as one of the smallest areas surrounded by streets. The size will help defining the intersections and therefore how frequent a vehicle will reduce its speed and then stop. Additionally, streets with fewer intersections allow vehicles to accelerate to higher speeds in comparison to city blocks that contain many intersections. Vehicles will be forced to decelerate more often and more mobility details will be considered.

C. Traffic control mechanism

As mentioned in the first point, streets will differ in their traffic signs. The main signs that have their locations pre-defined and help bringing more reality to any proposed mobility model are the traffic lights and stop signs. They will lead to queue formation and reduction of speed.

D. Interdependent vehicular motion

Each vehicle is affected by the movement of the surrounding vehicles. The vehicle may be forced into speed reduction/ increment, changing lanes, changing the street or even stopping.

E. Average speed

The higher the vehicle's speed, the faster it will change its position or location. Moreover, the road's speed limit affects the vehicle's average speed. This may lead to changes in the connectivity of the network or in other words, the network topology..

Routing Protocols Overview

The routing protocols in network are required to establish the connection in between sender and receiver [3, 10]. Every routing protocol has different routing procedure for connection establishment the VANET routing protocols are totally different from the traditional wired protocols. In VANET routing protocols are divided in to three types:-

Proactive Routing Protocol

Proactive routing protocols are the table driven routing protocols that established connection in between the source to destination and maintaining the record of routing table for future used in communication. In VANET the network topology is changing frequently and the nodes in VANET is also changing their position by that the possibility of new node in route establishment is more by maintaining the record of nodes in tables is unnecessary overhead. The example of these kinds of protocols is Dynamic Source Distance Vector (DSDV) routing protocol [10].

Reactive Routing Protocols

Reactive routing protocols are ob demand routing protocols maintaining the connection if required and not maintaining the record of routes or routing table information. This type of protocol is suitable for VANET characteristics of dynamic topology. The route is only established if the sender want to communicate to receiver and the link is maintaining at the time of communication but after completing the data receiving the link is break and the whole route record is erased. The example of such type of protocol also included in this research is Ad hoc On Demand Distance Vector Routing Protocol (AODV) [10].

Hybrid Routing Protocol

Hybrid routing protocol is the combination of proactive and reactive routing protocols in VANET. The example of this kind of protocol is Zonal Routing Protocol (ZRP) routing protocol. In this protocol are particular are of communication is divided into different zones. In each zone the routing procedure is different and these routing protocols are performing routing inside the zone and outside the zone [11].

Literature Survey

In this section the recent previous work is proposed by different authors is mentioned. Here every one is contribute some new research concepts. Some of the works against attack or malicious vehicles are as follows:

In this paper [12] the author is mainly concentrates on the hole generation attack, in which the malicious or attacker drivers inside the network breaks the links by reducing their own speed or boosting their speed to create holes. Proposed a novel Robust Routing Protocol (RRP) for sending the message securely in between source to destination by surviving it from hole generation attack. RRP consists of a security module to recognize an attacker node or normal nodes and a recovery module to defend against the hole created by the malicious drivers in VANET. The whole work is done in vehicle to vehicle (V to V) communication and the attacker is continuously affected the other vehicles by that they are slow their speed and the RRP provides security from that attack.

The main drawback of this research is:-

- The loss from attacker node/s only is never mentioned and also not mentioned number of attacker node/s that flooded the false traffic information.
- The control overhead is not evaluated that contains the attacker request packets and reply packets information.
- The security algorithm is based on private key and signature based for maintain trust factor but in VANET the vehicles flooding is in large amount and if key based technique is used then overhead is enhanced.
- The attacker and security module is simulated in which simulator, not mentioned.

In this paper [13], proposed a new hybrid Position Based Secure Routing Protocol (PBSRP) and compare their security performance with Most Forward within Radius (MFR) and Border Node based Most Forward within Radius (B-MFR) routing protocols. A security module is added in this protocol by using station to station key agreement protocol to prevent the system from various attacks. It consists of three phases: initialization phase, optimal node selection phase and secure data delivery phase.

In this paper [14], proposed a security mechanism that detects blackhole attack as well as greyhole attacks in Vehicular Delay Tolerant Networks (VDTNs). Moreover this security scheme includes an inducement mechanism to support the cooperation of nodes or vehicles. Depending on the amount of information available when two nodes meet, the system will adaptively choose a suitable detection threshold to maximize detection rates while minimizing false positives. The nodes or vehicles generating the messages in network having good trust reputation will be accepted and forwarded by others, while nodes with a low trust reputation will be throw out from the network.

In this paper [15], an efficient and secure method is proposed to identify and secure against UDP end flooding attacks under different IP spoofing types. When malicious actions are detected or identified, they can further be classified into random spoofing, subnet spoofing or fixed spoofing types by analyzing a hash table for the source IP characteristics. The scheme makes utilize of a storage efficient data structure and a Bloom filter based IPCHOCKREFERENCE detection method. This frivolous approach makes it quite easy to deploy as its resource constraint is reasonably low. Unfortunately, this scheme does not work for subnet spoofing. Implementing encryption and authentication can also reduce the spoofing threats.

In this paper [16], proposed a publish/subscribe support for VANET environment. Here it is assumes that a hybrid environment of stationary or fixed information gathering and collection stations and mobile vehicles. in this approach not included the utilization of GPS or navigation systems in proposal or identified the or maintaining the vehicles location information. In this scheme, these information stations connect themselves in a DHT fashion. The information stations are understood to be connected to internet and form Distributed Hash Table (DHT) based broker overlay among them and act as assignation points for publications and subscriptions. Further, they also provide services to locate vehicles in network. Each vehicle can take the role of publisher, subscriber or broker and they communicate in cooperative manner to spread publications and subscriptions to information stations. Notifications are also disseminated to targeted vehicle using vehicle to vehicle communication.

This paper [17] proposed a wide-ranging message authentication novel scheme which enables the message authentication in intra and inters Road Side Unit (RSU) range, and the hand-off within the different RSUs. The proposed scheme maintain the balance in the overhead of computation and communication, and the security against the attacking. Vehicles’ inability to authenticate with each other across different communication ranges. Security mechanisms are also provided anonymously to avoid exposing the identities of vehicles. When accidents happen, an initial authentication RSU will provide the real identity of each vehicle.

In this paper [18], proposed a novel security scheme to prevent most of these attacks. This security scheme is try to fulfill the requirement to provide secure topology information in VANETs and to erect a secure network for applications, such as a secure communication and congestion alert system. Essentially this solution is the famous axiom “Seeing is believing”. This security scheme use on-board radar as the virtual “eye” of a vehicle. Although the “eyesight” is restricted due to a self-effacing radar transmission range, a vehicle can “notice” or "see" nearby vehicles and “hear” or "sense" reports of their GPS coordinates. By comparing what is notice to what has been heeded, a movable vehicle or nodes can substantiate the real or actual position of neighbors or surrounding vehicles and detach malicious attacker vehicles to accomplish local security. They anticipated the on-board radar device is to provide useful corroboration of reported location information, except for during short transient periods. For example, the line-of-sight that radar needs may be temporarily obstructed by a large motor vehicle like truck. Because of the dynamic nature of traffic, even if there are transient obstructions, the line of sight will be restored eventually.

PROBLEM STATEMENT

The security of Vehicular Ad hoc Network (VANET) is major concern as their awfully survival relates to decisive life threatening situations. The self-organized network is easily affected from the attacker that performs malicious activities to clash the network performance by dropping of traffic information, by consuming link capability and proving wrong traffic status. It is essential that important traffic information cannot be interleaved or modified by a malicious vehicle. The communication roadways system must be able to determine the legal responsibility of drivers while still maintaining their privacy to secure from attack but these problems are difficult to solve because of the speed of the vehicles, network size, randomness of the connectivity between vehicles and their relative geographic position. The Hole attack is initiated by flooding the fake control packets and by that the vehicles are completely disabled for taking the traffic decisions and the big hole between the network is created and the network's nodes or vehicles, On Board Units (OBU) and Road Side Units (RSUs) cannot sufficiently process the surplus data. The attacker effect in network is:-

- Extremely Enhanced the control overhead by fake packets generation that also reduces link capability and vehicles self route decision capability.
- Average end-to-end delay is enhanced by that follower vehicles is wait for the clear traffic information but this positive or clear traffic information is reached not in proper time or may be possible if the normal vehicles follow the attacker instructions then follower vehicles are stay at same position and whole network is moves very slowly.

PROPOSED WORK

In this section we apply the novel security scheme based on RSU against Hole Attack in VANET. Here we modified the RSU communication that identified the vehicles that flooding unwanted traffic wrong information. The Hole Attacker is continuously flooding the wrong traffic information by that the normal vehicles or nodes are mislaid their decision capability by that the current vehicle that is affected from attacker is also nor forwarded the correct traffic information to other vehicles in network. Because of that vehicles traffic jamming condition is occur in network and the vehicles are moves slowly towards destination point.

The Advance proposed research is required to investigate intelligent flooding schemes, secure traffic information approach from 'Hole Attack' that can efficiently handle appropriate communications among vehicles for different transmission ranges. Providing *reliable* broadcast messages for VANETs introduces several other technical challenges including the selection of the next forwarding node, the maintenance of communications among vehicles as they broadcast the traffic information of vehicles in network. In this scenario 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 wrong traffic information but the traffic conditions are different.

One of the important aspects in proposed RSU based communication is to maintain the efficiency network operation while preventing degradation of wireless channels communication. The purpose of this study is to disclose the weak points of some of these congestion control algorithm so that researchers can come up with broader algorithm to tackle the inherent problems of congestion in VAENTs. This study focused on the congestion of uni-priority of traffic status safety message in V to V VANET environment. The unwanted message is caused by the traffic of the same priority, typically the warning messages of safety applications from different transmitters. 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

4.3 Steps to minimizes the flooding in network

The description of normal VANET scenario, attack and proposed RSU is mentioned in the following points. In this research we proposed a three different scenario in same traffic system. Here the first scenario is of normal VANET communication in V to V network, second is Hole attacker scenario in V to V communication and third is applied prevention through RSU stationary unit, means the third secure scenario is of V to RSU communication. The attacker detection is based on the NRL (Normal Routing Load) value. If the NRL is more than then condition (NRL > 2*Normal) then attacker is confirm. The normal means normal VANET traffic scenario.

Proposed Algorithm for Traffic Control

The proposed algorithm is defining the steps for which the traffic status broadcasting will control and reduces traffic overhead.

Vehicle to vehicle and Vehicle to RSU communication in VANET

```
Begin
Initialization
{
T: Terrain Size (1652m*1652m) // in meters
    $V_R$: Requestor Vehicle $V_{R\ 1}$………………… $V_{R\ n}$
    $V_P$: Reply Vehicle $V_{P\ 1}$……… $V_{P\ m}$
    D = Vehicle Destination
    Routing Protocol = AODV
    Number of vehicle ($V_n$) = 69
    Total Terminals =$T_1$ to $T_9 \epsilon (V_n)$
    Number of RSU unit  = $RSU_1$ to $RSU_9 \epsilon (V_n)$ // set on
terminals in prevention scenario
```

```
        Hole Attacker Vehicles = 5  // ($V_{19,}$ $V_{25,}$ $V_{26,}$ $V_{43}$ and $V_{49}$)
        Communication range = 550 meters
        Wireless Technology Standard = WiFi
        Propagation of traffic signals = Two ray ground
  {
   Execute Traffic status Request procedure();
            $V_S$ sends route request();
               $V_D$ sends route reply();
    If (Requestor Vehicle found next neighbor = = Available) // nearby vehicles availability
        {
        Deliver traffic status & Receive Traffic Status
        }
        Else
        {Continue Sends Request}
    If (If nearest neighbors in range & $V_R$ is not reaches = = D) //Detection by RSU the Confirm the Attacker existence
        {
        RSU Capture flooding Information of all nodes;
        RSU Capture Nodes flooded unwanted packets;
        RSU Maintain information of Drop of Data Packets;
        Calculate NRL of Network;
        }
        Else
        {Destination unreachable}
    If (NRL > 2*Normal) // Hole Attack Confirm then apply prevention
          {
        Find attack information (node number, infected_packets, time)
    Block the infected node;  // by block their communication capability
        Disabled Communication;
        Remove Infection;
        }
        Else
         {
        Vehicle Sends traffic request Communicate with Next nearest neighbor and reaches to destination
                        }
                }
        }
```

SIMULATOR TOOL OVERVIEW AND PERFORMANCE PARAMETERS

The simulation is done with Network Simulator (NS-2) version 2.31[19]. This is an object oriented simulator, their back end modules are written in C++, with an OTCL interpreter as a front-end that supports to call the internal modules. The simulator supports a class hierarchy in C++ (also called the compiled hierarchy) and a similar class hierarchy within the OTCL interpreter (also called the interpreted hierarchy). The two hierarchies are closely related to each other; there is a one-to-one correspondence between a class in the interpreted hierarchy and one in the compiled hierarchy. The source of this hierarchy is the class TCL Object. The Users are create new simulator objects through the interpreter and these objects are instantiated within the interpreter and are closely mirrored by a corresponding object in the compiled hierarchy. The interpreted class hierarchy is automatically established through methods defined in the class TCL Class. User instantiated objects are mirrored through methods defined in the class TCL Object.

A. Simulation Parameters

The simulation parameters like area of simulation is 1652m*1652m in transmission range of 550m. Rest of them that are considering for simulation is mentioned in table 1.

SIMULATION PARAMETER

Area of Simulation (meters)	1652m*1652m
Mobile Nodes	69
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)	290
Packet Size	512 bytes

B. Performances Metrics

The performance of network is evaluated in case of AODV, Byzantine attack and secure IDS scheme.

1) *Traffic Load*

The number of Traffic packets delivers by the all number of vehicles for knowing the traffic information.

2) *Normal Routing Load*

The Normal Routing Load is the ratio of number of traffic request packets and the number of data traffic packets received in network.

Packet delivery ratio:

The ratio between the numbers of packets originated by the application layer to those delivered to the final destination.

3) *Average end to end delay:*

This is the average of the time taken by the packets to reach the destination in the network. The average time to packets sends by sender and received by receiver is network.

4) *contamination Packets Percentage*

The contamination packets percentage is calculated by how much percentage of data in network are infected by Hole attacker in network.

RESULTS DESCRIPTION

In this section the we presents the simulation results description in case of normal communication, Hole attack and proposed secure RSU based communication.

PDR Performance Analysis in Normal Traffic, Hole Attack and Proposed RSU Prevention

In VANET the packets receiving and forwarding is completely based on the traffic data sends and receives by the vehicles. This network communication is likely same as Ad hoc network communication but also easily affected from malicious drives and attackers. 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 normal VANET, Hole attacker presence and proposed RSU based communication is assessed and observe that the proposed scheme is really effective to identified the Hole attacker and recover about more than 98% performance as compare to normal performance. The attacker performance in network not more than 35% and also evaluated up to 260 seconds e.g. is also the enhance NRL (Normal Routing Load) and end to end delay (NRL and end to end delay always minimum better) but proposed scheme performance is almost equal to normal performance. The attacker existence is absolutely blocked by RSU for providing secure communication between vehicles.

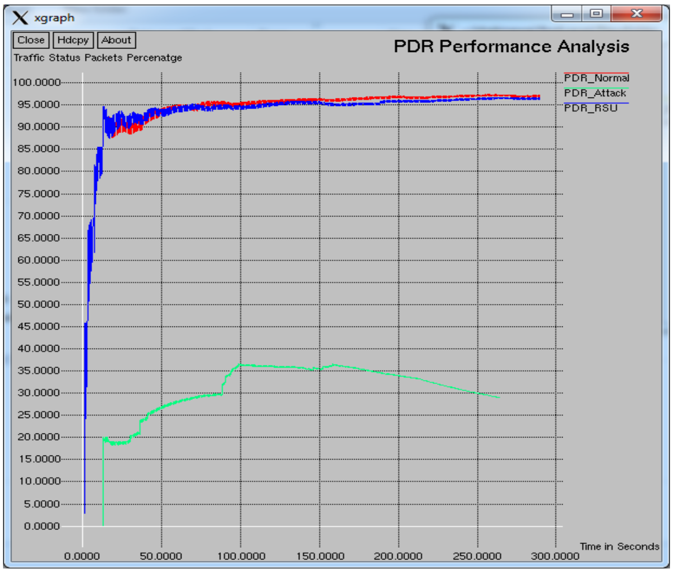

Fig.1 PDR Performance Analysis

Traffic Overhead Performance Analysis in Normal Traffic, Hole Attack and Proposed RSU Prevention

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 follower vehicles are continuously sends the traffic request for recognizes the traffic status but this information is also destructive if it will be deliver in access in network e.g. perform by Hole attacker to creating a situation that vehicles are not decided and follow to destination path very slowly. In this graph the flooding analysis Traffic overhead of vehicles is measured and observe that the attacker has flooding more than thirty lacks request packets in network but data receiving is minimizes. Their effect is NRL enhanced means delay enhanced. These packets are unwanted packets. The proposed security scheme against Hole attack is secure the network performance and providing request packets delivery as equal to normal VANET performance.

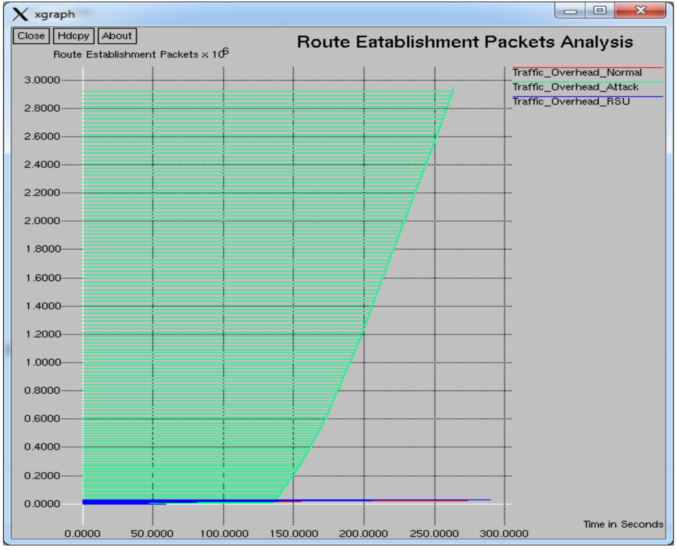

Fig.2 Route Packets Flooding Analysis

Attacker Traffic Data Drop Percentage 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 percentage of attacker vehicle is evaluated. Here the Hole attacker presence is drop the 45 % of data in network of total data of traffic is receives in network. This data is drop due to vehicles are busy in receiving the unwanted flooded data of attacker by that these data packets are dropped. But after applying secure RSU based scheme in normal V to V communication, the security criteria is enhanced for reliable communication and provides zero percent infection in network in disabled presence of attacker through RSU.

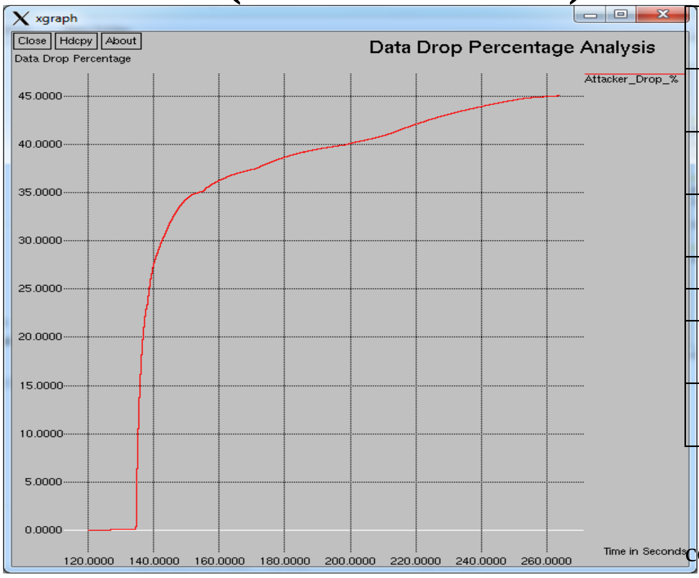

Fig. 3 Attacker Drop Percentage Analysis

Hole Attacker Nodes Flooding Packets Analysis

The attacker presence in decentralized VANET is easily destructing the whole network performance. The V to V communication is secure from applying RSU security with proposed security scheme. In this table the attacker nodes packets flooding quantity is mentioned. This flooding quantity is block the motion of vehicles because vehicles are not received the proper traffic status and also the not sends the requests of traffic. The presence of secure RSU is modified the malicious scenario in normal secure traffic communication in VANET.

ATTACKER NODES FALSE TRAFFIC STATUS FLOODING ANALYSIS

Infected Node	Total Infected Packets
19	369171
25	516591
26	262632
43	434462
49	516504

Summarized Normal Traffic Scenario Performance

The summarized and exact performance up to end of simulation time is mentioned in table 3. In this table we clearly visualized that the attacker has flooded about 29 lacks packets in network and the data packets receiving is also about one third. The Normal Routing Load (Traffic request packets by Traffic data received) is enhanced and also the end to end delay is enhanced in network. The reliable RSU units are provides the secure V to V communication (V to RSU Communication) and network performance is almost equal to normal V to V communication.

SUMMARIZED NORMAL PERFORMANCE

Performance Metrics	Normal_VANET	Hole Attack	RSU_Prevention
Traffic Data Sends	11900	10850	11900
Traffic Data Receives	11566	3149	11495
Traffic Request Packets	26375	2941697	29538
PDF	97.19	29.02	96.6
NRL	2.28	934.17	2.57
Average e-e delay(ms)	118.92	909.16	144.73
No. of dropped data (packets)	1491	7381	1567

CONCLUSION AND FUTURE WORK

In VANET mobile nodes or Vehicles equipped with wireless communication technologies and acting like computer nodes will be moves on the road. The self-organized network is provides better communication and coordination between the vehicles through established Vehicle to Vehicle (V to V) and Vehicle to Road Side Unit (V to RSU) communication in network. The previous work is discussion is provides the novel idea of simulation proposed security algorithm. In this research we proposed a new secure Hole Attack Prevention (HAP) 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 scenario of road network is based on V to V communication. Second is the Hole attack scenario and here it is observe that the network performance is almost dumped because of staying the vehicles movements but third proposed RSU based communication with including the proposed HAP scheme is not only detect but also prevent from attacker. The main advantage of applying HAP in V to RSU is that, if the attacker is detected then their particular information is easily broadcast to all the RSUs 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 RHA is recovering about 97 % performance as compare to normal VANET scenario.

The security criteria are not resolve from this particular research. 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 a mobility based communication with RSU. In this scheme try to provide clear path for high speed vehicles and identified the vehicle that modified or not follow that policy of vehicle communication.

REFERENCES

Yu Wang and Fan Li, “Vehicular Ad Hoc Networks” in Guide to Wireless Ad Hoc Networks, Book on Computer communication and Networks, Springer, 2009.

Y. Toor, P. Muhlethaler and A. Laouiti, ”Vehicle ad hoc networks: Applications and Related Technical Issues”, IEEE Communications Surveys and Tutorials, pp. 74 - 88, 3rd Quarter 2008.

Bassem Mokhtar, Mohamed Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks", Alexandria Engineering Journal, Elsevier, pp. 1-11, accepted 22 July 2015.

F. Sabahi, “The Security of Vehicular Adhoc Networks,” IEEE Third International Conference on Computational Intelligence, Communication Systems and Networks, pp. 338-342, 2011.

J. M. de Fuentes, A. I. González-Tablas, and A. Ribagorda, “Overview of security issues in Vehicular Ad-hoc Networks”, *IGI Global*, 2011.

[1] Y. Hao, Y. Cheng, C. Zhou, and W. Song, “A distributed key management framework with cooperative message authentication in VANETs,” IEEE Journal on Selected Areas of Communication, Vol. 29 , No. 3, pp. 616–629, March 2011.

[2] J. Jeong, S. Guo, Y. Gu, T. He, and D. Du, “Trajectory-based statistical forwarding for multi-hop infrastructure-to-vehicle data delivery,” IEEE Transaction on Mobile Computing, Vol. 11, Issue10, pp. 1523 - 1537, 25 August 2011.

[3] A. Mahajan, N. Potnis, K. Gopalan and A.-I. A. Wang, "Urban Mobility Models for VANETs," in Proc. of 2nd Workshop on Next Generation Wireless Networks, 2006.

[4] D. S. Gaikwad and M. Zaveri, "A Novel mobility model for realistic behavior in Vehicular Ad Hoc Networks," in 11th IEEE International Conference on Computer and Information Technology, Cyprus, 2011

[5] Kayhan Zrar Ghafoor and Marwan Aziz Mohammed, "Routing Protocols in Vehicular Ad hoc Networks: Survey and Research Challenges", Network Protocols and Algorithms, , Vol. 5, No. 4,pp. 39-83, 2013.

[6] Tarik Taleb, Ehssan Sakhaee, Abbas Jamalipour, Kazuo Hashimoto, Nei Kato, and Yoshiaki Nemoto, "A Stable Routing Protocol to Support ITS Services in VANET Networks", IEEE Transactions On Vehicular Technology, Vol. 56, No. 6, pp. 3337-3347, November 2007.

Sourav Kumar Bhoi, Rajendra Prasad Nayak, Debasis Dash and Jyoti Prakash Rout, "RRP: A Robust Routing Protocol for Vehicular Ad Hoc Network against Hole Generation Attack ", International conference on Communication and Signal Processing, pp. 1175-1179 April 3-5, 2013, India

Sourav Kumar Bhoi, Pabitra Mohan Khilar, "A Secure Routing Protocol for Vehicular Ad Hoc Network to Provide ITS Services", International conference on Communication and Signal Processing, pp. 1170-1174, April 3-5, 2013, India.

Yinghui Guo, Sebastian Schildt and Lars Wolf, "Detecting Blackhole and Greyhole Attacks in Vehicular Delay Tolerant Networks", Fifth International Conference on Communication Systems and Networks (COMSNETS), pp. 1-7, 7-10 January 2013.

[7] Karan Verma, Ashok Kumar, "An Efficient Defense Method against UDP Spoofed Flooding Traffic of Denial of Service (DoS) Attacks in VANET", IEEE 3rd International Conference on International Advance Computing Conference (IACC),pp. 550-555, 2012.

[8] Tulika, Deepak Garg. Manoj Madhav Gore, "A Publish/Subscribe Communication Infrastructure for VANET Applications" IEEE Workshops of International Conference on Advanced Information Networking and Applications, pp. 442-446, 2011.

[9] Hsin-Te,Wu, Wei-Shuo Li, Tung-Shih, Su† and Wen-Shyong Hsieh, " A Novel RSU-based Message Authentication Scheme for VANET", IEEE Fifth International Conference on Systems and Networks Communications, pp. 111-116, 2010.

[10] Gongjun Yan, Stephan Olariu, Michele C. Weigle, "Providing VANET Security Through Active Position Detection", Computer Communications , The International Journal for the Computer and Telecommunications Industry, ELSEVIER (Science Direct) Volume 31, Issue 12, pp. 2883–2897, 30 July 2008.

Network Simulator-ns-2 Tutorial Available on link, http://www.isi.edu/nsnam/ns/tutorial/index.html.