I.J. Wireless and Microwave Technologies, **2018, 6, 73-88**
Published Online November 2018 in MECS(http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2018.06.06

***Available online at** http://www.mecs-press.net/ijwmt*

Prevention of Session Hijacking Attack in VANETs Using Intrusion Detection System

Jeevitha.R [a], Dr.N.Sudha Bhuvaneswari [b]

[a] *Research Scholar, Department of Computer Science, Dr.G.R.Damodaran College of Science, Coimbatore-641014, India.*
[b]*Associate Professor, Department of Computer Science, Dr.G.R.Damodaran College of Science, Coimbatore-641014, India.*

Received: 09 April 2018; Accepted: 02 October 2018; Published: 08 November 2018

Abstract

Vehicular Adhoc Networks (VANET) is a type of road network that provides road safety and other infotainment applications to drivers and passengers for an effective and uninterrupted communication. In this network, the communication between the vehicles are equipped with the Road Side Units (RSU). VANET is the major component of Intelligent Transportation System (ITS). Research on Vehicular Adhoc network security presents many challenging issues to the researchers. The security mechanism available for VANETs are not highly effective. Hence it is as on time requirement of new and sophisticated security solutions. This paper mainly focuses on Intrusion Detection System (IDS) for VANETs to prevent Session Hijacking Attack (SHA). The work discusses on the total number of packet generated, sent, received and dropped with varying number of nodes with the help of Network Simulator-2 (NS2) and the inferred results are discussed.

Index Terms: VANET, IDS, Session, RSU, ITS.

© 2018 Published by MECS Publisher. Selection and/or peer review under responsibility of the Research Association of Modern Education and Computer Science

1. Introduction

Mobile Computing is a technology in which variety of devices allow people to access data and information from wherever they are. This Concept involves Mobile Communication, Mobile Hardware and Mobile Software. Some of the research areas in Mobile Computing includes Wireless Local Area Network (WLAN), Sensor Networks, Mobile Adhoc Networks, Delay Tolerant Networks and Vehicular Adhoc Networks.

* Corresponding author. Tel:
E-mail address:

Vehicular Adhoc Networks is a subset of Mobile Adhoc Networks (MANETS). In VANET, a node (vehicle) can send data directly to another node (vehicle) within its transmission range. VANET aims not only in increasing traveller safety but also became an efficient communication tool for the users. It provides infotainment application to the drivers and passengers to communicate with each other by offering services such as Internet Connectivity and Media downloading. It is possible to stream the user's favourite entertainment anywhere. It is a thrust area of research with the scope to explore more on Intelligent Transportation System (ITS), Inter-Vehicular Communication, Traffic Regulation based on Network Congestion, Environment based traffic regulation, Sensor based Vehicular Traffic, Dedicated Short Range Communication (DSRC) and Applicability of MANET based routing in VANETs [1,19].

2. Security attacks in VANET

Security threats in application layer include malicious code attacks and repudiation attacks. Security threats in transport layer include SYN flooding attack, Session hijacking, and TCP ACK storm. The attacks that affect the routing protocols in the Network are Routing table overflow attack, Routing cache poisoning attack, Rushing attacks, Wormhole attack, Black hole attack, Byzantine attack, Location disclosure attack. Security threats in link layer include threats in IEEE 802.11 MAC and threats in IEEE 802.11 WEP. Security threats in physical layer include Eavesdropping, Denial of Service, Interference and jamming.

Application Layer Attack: The Application layer contains vehicle's important information related to the protocols like File Transfer Protocol (FTP), Hyper Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) that enables the vehicle communication [3]. There are two types of attacks namely malicious code attack and repudiation attack.

Malicious Code Attack: It includes virus, worms, spywares and Trojan horse. The malicious vehicles will send malicious code to attack the other vehicle, remote base station or RSU. The malicious codes will destroy the vehicle's application and affects the service access, operating system and user application [2, 3, 4].

Repudiation attack: The attacker act as a selfish node and denies the information that is meant for communication. They create the confusion for the audit entry such as RSU and Trusted Authority (TA). If this attack occurs, the data stored on log files are considered to be invalid or misleading [3, 5].

Transport layer attack: The transport layer is concerned with authentication, end-to-end secured communication using data encryption, handling end-to-end delays, loss of packet and packet corruption [3].

SYN flooding attack: The attacker creates large number of half opened Transmission Control Protocol (TCP) connection between the communicating vehicles in VANET so that handshake will not be done completely to establish connection [2]. The sender sends synchronize (SYN) message along with Initial Sequence Number (ISN) to the receiver. The receiver acknowledges the received SYN message by sending acknowledge (ACK) message which contains its ISN. The connection is established between the sender and the receiver. The malicious vehicle starts flooding SYN messages to a vehicle or RSU. That vehicle spoofs return addresses of SYN messages so that the received vehicle stores the flooded SYN messages of malicious vehicle and wait for ACK message. Since large numbers of SYN messages are received, more memory size is required in its buffer to register the SYN messages at the tables. Lot of resources is consumed and its system may be blocked for a period of time [3].

Session hijacking: The malicious vehicle acts as an authorized vehicle in VANET. It makes use of session establishment feature where no authentication is required at the beginning of the session [3].

TCP ACK storm: TCP-ACK Strom attack is created when an attacker establishes a TCP session hijacking attack. The attacker vehicle node sends the session data to vehicle V1. V1 node will acknowledge the same data to vehicle V2. This packet will not contain the sequence number that V2 expects. When V2 receives this packet, it will resynchronize the TCP session with V1 by sending it an ACK packet along with the sequence number that it is expecting. This process is repeated many times and the ACK packet is passed back and forth and thereby creating ACK Storm [3, 6].

Network Layer Attack: Due to the movement of vehicles, VANET has a dynamic topology hence maintaining a route for vehicles remains a challenge in VANET. Vehicles that are communicating should establish an efficient route so that broadcasting information will be forwarded to other vehicles in a fast manner. Any attack in the routing phase will block the overall communication and the whole network will be collapsed [3].

Routing table overflow Attack: The routing information is updated periodically in the routing table. The attacker will create routes to the nodes that do not exist to the approved nodes in the network [7]. The attacker node will send large number of route announcements to create new routes and to make the routing table overflow [3]. Proactive routing protocols are vulnerable to this attack when compared to reactive routing protocols.

Routing cache poisoning attack: On-Demand routing protocols such as Adhoc On-Demand Distance Vector (AODV) and Dynamic Source Routing (DSR) will maintain route cache for each and every node. It holds information about the routes that has been known to the node in the recent past [7]. This attack occurs when any information is altered, deleted or injected with some false information. For example, consider if an attacker node needs to poison all the nodes. The attacker will broadcast the spoofed packets with source node to all other nodes. The intermediate nodes and neighbouring nodes that are overhearing the packet will add the route to their route cache that leads to misguided routing poisoning the routing cache [3].

Rushing attack: The attacker node sends Route Request Packet quickly throughout the network than the legitimate node. Nodes that receive Route Request Packet from the legitimate node consider this packet to be duplicate and discard the packet. So the source node is not able to find the secured route [3, 7].

Wormhole attack: Two or more nodes encapsulate and exchange messages between them along the existing data routes by creating a tunnel between them [3, 8]. This tunnel is otherwise called wormhole which prevents the discovery of other route than the route through the tunnel. All the data then pass through the tunnel that results in dropping of packets and the data packets that are transferred can be altered [2, 4].

Black hole attack: The attacker nodes makes use of vulnerabilities in route discovery method of on demand routing protocols such as AODV and DSR. If a source node wants to send some data to the destination node, it broadcasts Route Request (RREQ) packet to all nodes. The node with highest destination sequence number than the current destination sequence number of node will send the reply so that the destination sequence number is higher than current destination sequence number. It is then sent to the source node. The source node receiving the fake Route Reply (RREP) packet will select the route through the malicious node. The source node assumes the new shortest path to the destination node. Now the source node rejects the entire RREP packets from other nodes and it sends packets only through the attacker node. The attacker node receives the packet and drops it instead of forwarding it [2, 3].

Byzantine attack: Byzantine attack is caused by a single malicious node or a group of nodes that work in cooperation. A set of intermediate nodes are compromised which works as individual or in groups to carry out the attacks such as creating routing loops, forwarding packets in long routes and selectively dropping packets [9]. As a result, the routing performance is degraded [8].

Location disclosure attack: This attack involves the disclosure of location information of the vehicles (nodes). The attacker node sends information about the location and uses the information for the attack. The attacker gathers information of route map and knows about which nodes are on the target route [3].

Physical layer attack: The most frequent physical layer attacks are Eavesdropping, Denial of Service, Interference and Jamming.

Eavesdropping: Reading of message and conversations by unauthorized receivers. Transmitted messages are eavesdropped and false messages are injected into the network [3].

Jamming: Jamming disrupts the communication channel by transmission of signal. The attacker senses the physical channel and gets information about the frequency at which receiver receives the signal. Then he transmits signal on the channel so that channel gets congested or jammed [10]. This type of attack affects the network by reducing the network performance.

Impersonate Attack: It makes use of network resources and disrupt the normal functioning of the network.This attack is performed by active attackers (insider/outsider). The attacker can exploit either network layer, application layer or transport layer [10]. The attacker changes the identity and acts like real originator of the message. The message from real originator node is received by the attacker node. The attacker changes the content of the message and sends the modified message to other vehicles [12].

Denial of Services (DOS): The attacker prevents the legitimate users to use service from victim node [10]. The vehicle resourses are controlled by the attackers. This prevents the arrival of critical information by jamming the session or communication medium [11]. The user cannot communicate in the network and cannot pass the information to other vehicles which may lead to miscommunication or dropping of packets [12].

3. Session Hijacking in VANET

Hijacking the session established between the source node and destination node refers to Session Hijacking. The unauthorized node steals the highly valuable and confidential information from the session, whenever the valid session is exploited [13]. The session may be hijacked mainly at the Link Layer by spoofing the Media Access Control (MAC) address and at the transport layer by spoofing the TCP sequence number. Even though session hijacking attack occurs mainly in the link layer and transport layer during session establishment [14], when an attacker gets access to the session state of a legitimate user, then it is said Session Hijacking. The attacker tries to steal a valid session ID which is used by him to get into the system and snoop the data. Active attack and Passive Attack are the two types of Session Hijacking attack. In active attack, the attacker finds an active session and takes over. In Passive attack, the attacker hijacks a session, but sits back, and watches and records all the traffic that is being sent forth.

Session Hijacking can takes place at two levels namely Network level and Application Level. In Network level, there occurs interception of the packets during the transmission between client and the server in a Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) session. At the Networking level, it provides critical information to the attacker which is used to attack application level sessions that attracts the hackers more. Networking level Hijacking includes TCP/IP Hijacking, IP Spoofing: Source Routed packets, Reset (RST) Hijacking, Blind Hijacking, Man-in- the middle: Packet Sniffer and UDP Hijacking [13].

Application level is all about gaining control on HTTP user session by obtaining the session IDs of the nodes. In this level, the hacker gains the session ID's to create a new unauthorized session and to get control of the existing session. Application level Hijacking includes obtaining Session IDs, Sniffing, Brute Force and Misdirected Trust. The users should have efficient antivirus, anti-malware software, and should keep the software up to date.

Session Hijacking can be prevented by securing the routing protocols used for communication so that attackers may not be able to get access to the packets transmitted over the routes taken by the packets. It is possible to prevent the session hijacking if the routes taken by the packets are secured.

4. Intrusion Detection System (IDS)

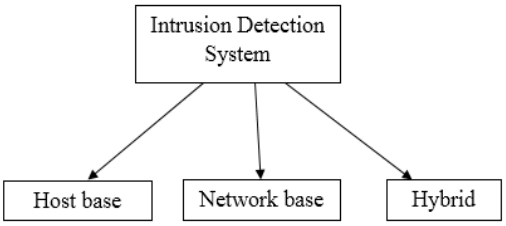

Fig.1. Classification of Intrusion Detection System [15]

Intrusion detection system (IDS) refers to the tools, methods and resources to help identity, assess and report unapproved or unauthorized network activities. IDS serve as an alarm mechanism for computer system network [17].

IDS provide security to detect the attack and to prevent the attacks [16]. IDS is classified as Host base, Network base and Hybrid. Host base IDS depends on the operating system to evaluate log files, to audit data to analyze malicious activities driven from user activities. Network based IDS depends on the data packets to analyze the malicious activity on the network [15].

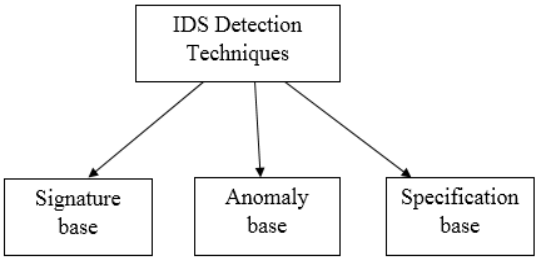

Fig.2. IDS Detection Techniques [15]

IDS Detection techniques include Signature base, Anomaly base and Specification base. Signature base IDS is used to find the malicious activity against the database. It uses preknown attack scenario and compare them with the incoming packet traffic. This detection has techniques like Expert System and Pattern recognition [15, 17]. Anomaly base IDS build its own database based on activity, behavior and inspect the traffic to mark it as malicious node. Normal vehicle can be compared with the Captured vehicle into the system along with predefined standard behavior. This detection has several techniques like data mining and neural networks. Specification base IDS has the characteristics of both Signature base and Anomaly base IDS. This type of IDS detects the zero day attacks and analyzes the behavior of vehicle at the initial time [15, 17].

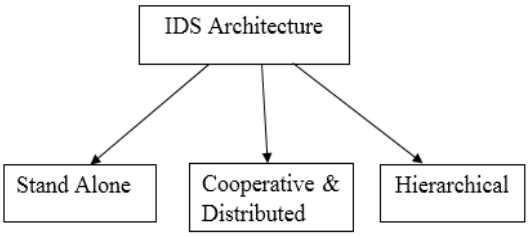

Fig.3. IDS Architecture [15]

Intrusion Detection System Architecture is of three types namely Stand alone, Cooperative and Distributed and Hierarchical. Each node is a self-governing IDS in Stand-alone architecture. They don't share the information to the other node. In Cooperative and distributed architecture, each node will be governed by IDS agent and the detection is made by decision and cooperation. They share information about the intrusion to the other nodes which is suitable for global detection [15]. In hierarchical IDS architecture, each node is controlled by Cluster Head or administrator. The Cluster head will supervise all the nodes in the clustered network and detects the malicious node in the network [15].

5. Problem Statement

Vehicular Adhoc Network are decentralized and infra-structure less network. Security is considered to be major challenging issue in VANET. There are various Security attacks in each layer. Researchers proposed many techniques for securing communication between the vehicles but there exist some drawbacks. The transfer of messages between the vehicles should be secured in any session. Some of the protocols available to secure the routes are Adhoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), Adaptive Secure AODV and Secure Efficient Adhoc Distance Vector. But there exists some drawbacks. AODV cannot sense the misbehaving nodes as well as it fail to detect the worm-hole attacks. DSR is vulnerable to the attacks if the attacker is along the route taken by the packet [17]. This paper focuses on Session Hijacking Attack which is a major threat in VANET and the steps to prevent this attack by proposing an Anomaly based Intrusion Detection System.

Finding the malicious node is the next challenging problem. They may also try to behave like normal nodes. Related works propose that the misbehaving nodes transmit false alerts, creates congestion in the network, delay, dropping and duplicating the packet. The malicious node detection schemes include Node-centric and data-centric schemes. Outlier detection technique can be used to find the anomaly node. Detection of Malicious Vehicle algorithm (DMV) is used to discover the malicious nodes that drop or duplicate the received packets more than a given threshold value. Quality of Service-Optimized Link State Routing (QOS-OLSR) clustering algorithm is used for detecting the malicious vehicles in VANET [20].

6. Proposed Algorithm

Road Side Unit (RSU) creates a strong encrypted session id along with Vehicle number for each vehicle within its transmission range in each session. Consider, the attacker tries to hack the session id. Two vehicles V1 and V2 are assumed so as to communicate securely and thus they need to agree on an encrypted session id. If the Vehicle V1 is sending frequent messages by increasing the network traffic, blocking further information exchange, overloading the network, then the vehicle V2 with the encrypted session id of Vehicle V1 is reported to the nearest RSU. RSU plays the role of IDS. A new session id is regenerated to the Vehicle V2. RSU prevents the attacker vehicle to further communicate with all other vehicles by blocking its session id.

Step 1: Vehicle V1, V2… Vn joins the Vehicular network.
Step2: RSU assigns session id to all the vehicles in the network.
Step 3: Vehicle V1 send an encrypted message M1 to nearby RSU.
Step 4: Send message M1 to next hop towards the RSU.
Step 5: Vehicle V2 receives message M1 from Vehicle V1.
Step 6: Send message M2 to next hop towards RSU.
Step 7: When RSU receives message Mn from Vehicle Vn.
Step 8: RSU retrieves the message and decrypts it.
Step 9: If Vehicle detects Vehicle Vn showing abnormal behavior or overloading the network.
Step 10: Report to nearest RSU.
Step 11: RSU sends warning message to all nodes within its transmission range.
Step 12: New session ID is regenerated to the honest vehicles.
Step 13: Update the entry of the vehicle in block list.
Step 14: Isolate the detected attacker node from the network.

7. Simulation and Analysis

NS2 is an open source tool used in wired and wireless researches. NS2 is developed as a collaborative

environment and it is a discrete event driven network simulator developed at UC Berkely written in C++ and Object Oriented Tool Command Language (OTcl). NS2 is useful for simulating local and wide area networks [21].

Table 1. Simulation Parameters

Parameter	**Values**
Simulator	NS-2 (Version 2.34)
Channel	Wireless
Number of nodes	10, 20
Routing protocol	Destination-Sequenced Distance-Vector Routing (DSDV)
MAC layer	802.11
Mobility model	Random waypoint Model
Application Type	Constant Bit Rate (CBR)
Simulation Time	10 s

Scenario 1:

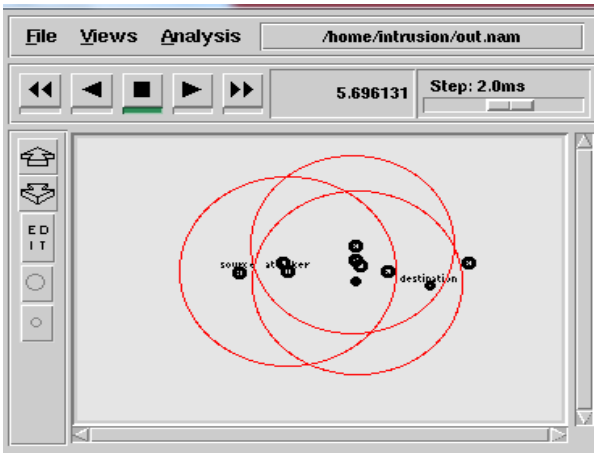

Fig.4. Simulation environment with 10 nodes

The above figure 4 shows the simulation environment of 10 nodes.

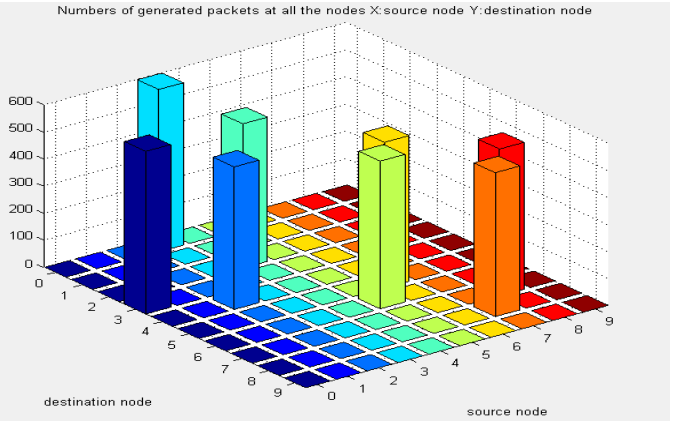

Fig.5. Number of generated packets

In figure 5, the packets are generated for 10 nodes. Total packets generated is 4427. A network packet consists of control information and user data. The packets generated will be routed and forwarded using a router from source node to destination node.

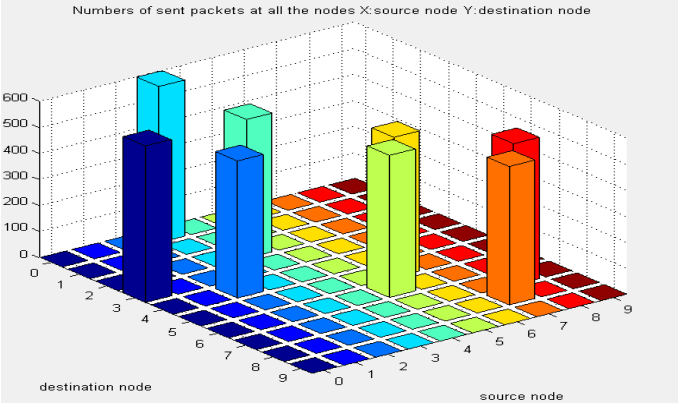

Fig.6. Number of sent packets

In figure 6, 4427 packets are sent from source to destination. If a packet is not received by the node or is dropped by a node, only the dropped packet needs to be resent.

In figure 7, the sent packets are received by the destination nodes. Number of received packets is 4325. From the packets sent and received, the packet delivery ratio can be calculated as the ratio of packets received to the packets sent.

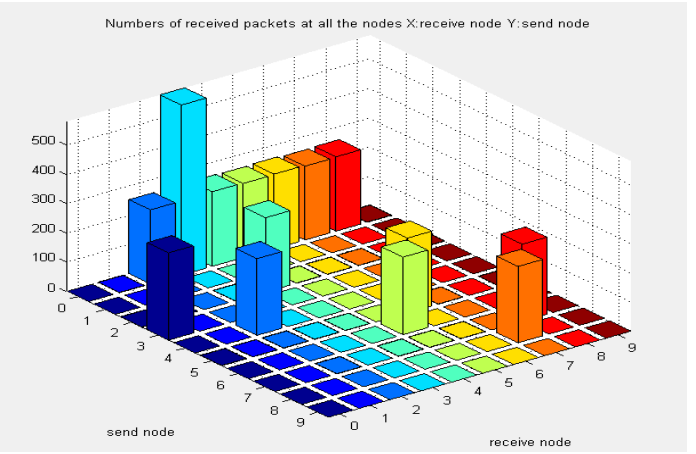

Fig.7. Number of received packets

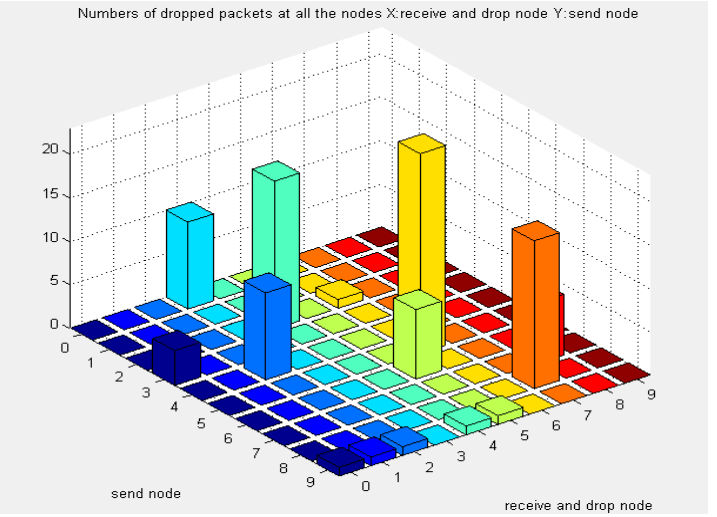

Fig.8. Number of dropped packets

From the figure 8, we can observe the dropped packets for 10 nodes. Total number of dropped packets is calculated as the difference between sending and receiving packets. 102 packets are dropped. Packet loss is calculated as the number of packets lost per 100 packets sent by a host node.

From the Figure 5 to Figure 8, we can observe that the total number of packets generated, sent, received and dropped for 10 nodes.

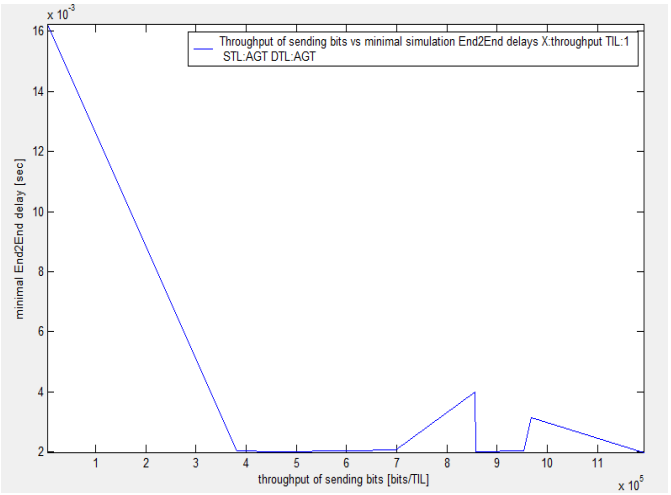

Fig.9. End to End Delay for 10 nodes

Figure 9 depicts the End to End delay for 10 nodes. End to End delay is the time taken for a packet to reach from source node to destination node. The delay time should be less for better network performance.

The network information are as follows:

Simulation information:

Simulation length in seconds:	9.482580055
Number of nodes:	10
Number of sending nodes:	10
Number of receiving nodes:	10
Number of generated packets:	4427
Number of sent packets:	4427
Number of forwarded packets:	0
Number of dropped packets:	102
Number of lost packets:	287
Minimal packet size:	28
Maximal packet size:	1618
Average packet size:	230.4098
Number of sent bytes:	1037356
Number of forwarded bytes:	0
Number of dropped bytes:	4776

Simulation End2End delays in seconds:

Minimal delay (CN,ON,PID): 0.001985515 (4,2,480)
Maximal delay (CN,ON,PID): 3.375824332 (0,3,238)
Average delay: 0.466455982

Fig.10. Simulation information for 10 nodes [23]

From the figure 10, it is analyzed that the total number of packets generated for 20 nodes is 4427 and total packets sent is 4427. 102 packets are dropped and 287 packets are lost. The average delay time is 0.46 seconds for 10 nodes.

Scenario 2:

In this scenario, 20 nodes are considered.

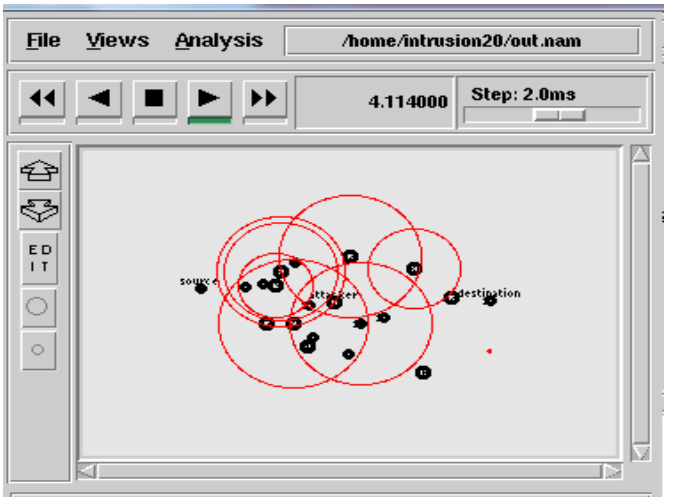

Fig.11. Simulation environment with 20 nodes

The above figure 11 shows the simulation environment of 20 nodes.

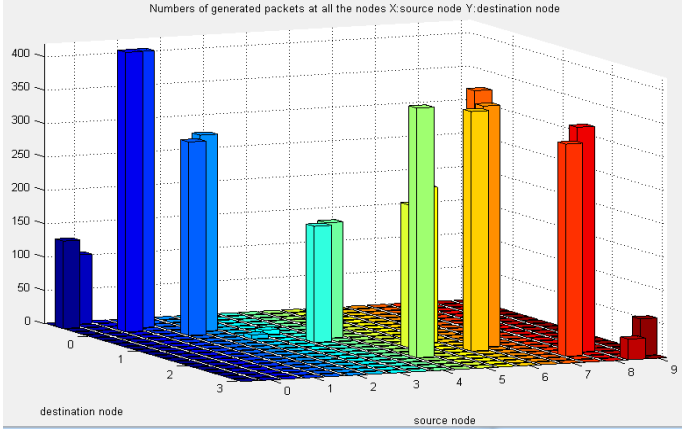

Fig.12. Number of generated packets

The above figure 12 represents the number of generated packets for 20 nodes. Generated packets tell us about how many packets are generated. Total packets generated is 4693.

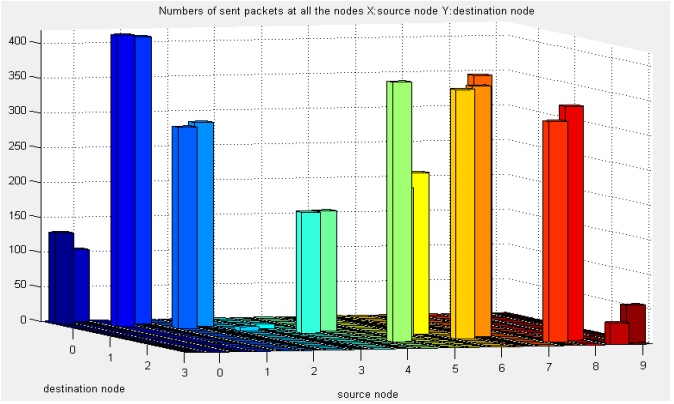

Fig.13. Number of sent packets

From the figure 13, we can observe that total packets sent is 4548. If a data transfer encounters any network congestion, then the packets are rerouted by a router using less congested path.

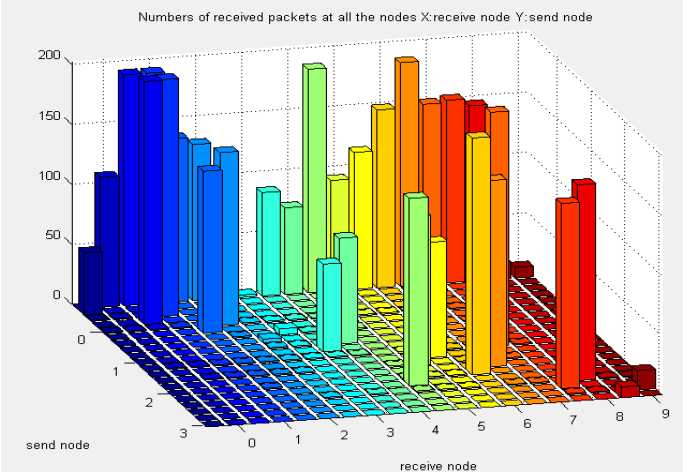

Fig.14. Number of received packets

Figure 14 represents the number of received packets for 20 nodes. Packets received are the total number of packets received by each node. The total packet received is 4157.

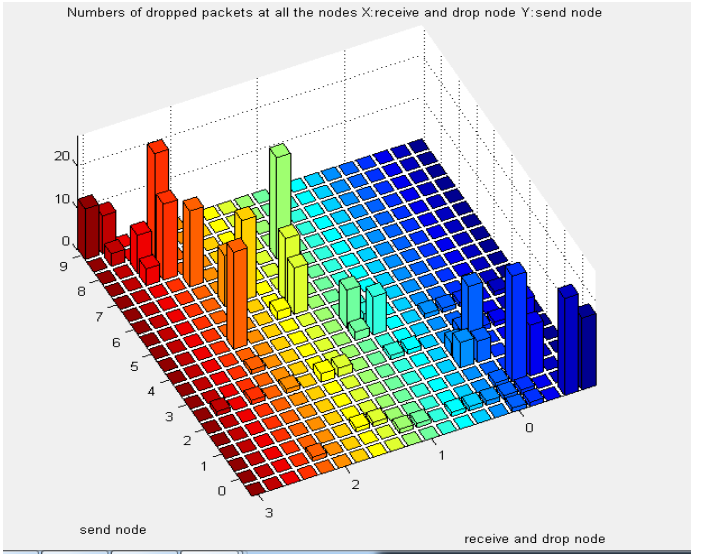

Fig.15. Number of dropped packets

From the figure 15, it is analyzed that 391 packets are dropped. As the number of node increases, total number of packets dropped will be high. The malicious nodes will be continuously dropping packets at the certain time.

From the figure 12 to Figure 15, we can observe that the total number of packets generated, sent, received and dropped for 20 nodes.

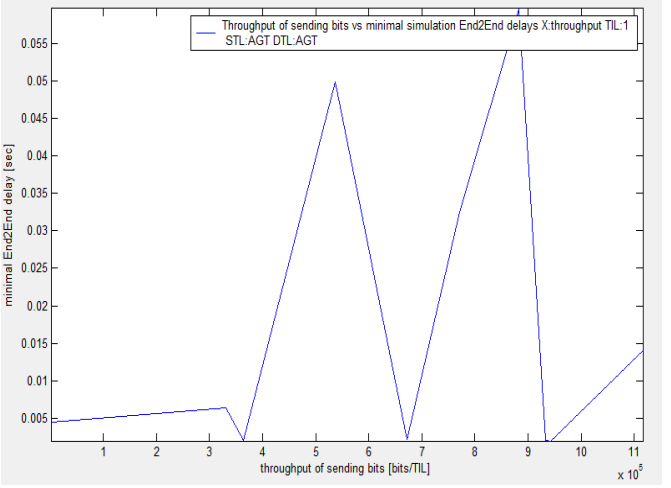

Fig.16. End to End Delay for 20 nodes

From the figure 16, it is inferred that the delay is high for 20 nodes. The delay is caused in finding the optimal route to the destination node. This may degrade the performance of the network.

Total number of packets generated is 4693 and total packets sent is 4548. 391 packets are dropped and 148 packets are lost. The average delay time is 0.70 seconds for 20 nodes.

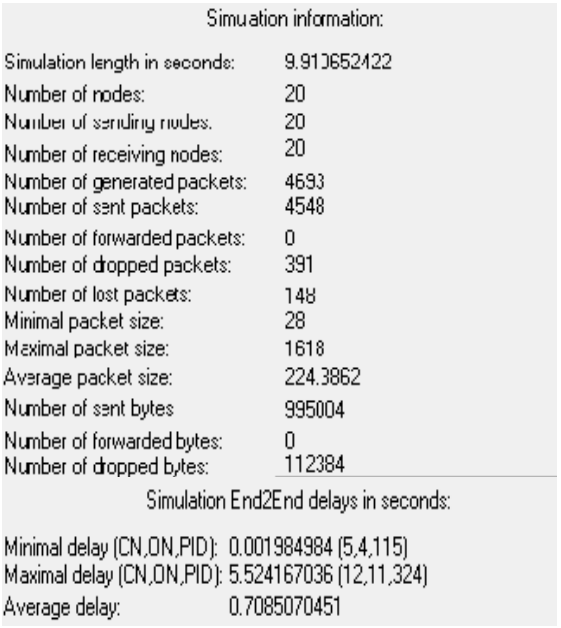

Fig.17. Simulation information for 20 nodes [23]

From the above result and analysis, it is found that the delay time for 10 nodes is less compared to 20 nodes. As the number of nodes increases, congestion will also increase. So, delay is proportional to the number of nodes.

8. Conclusions

Session hijacking affects the integrity of data on a network. Due to rapid mobility of nodes and self-routing capability, there exist issues in VANET security. Intrusion Detection System is a major challenging task because of frequently changing network topology. The attackers may also attack the entire IDS system itself. Accordingly, the study of the defense to such attacks should be explored.

References

[1] Mostofa Kamal Nasir, Mohammad Khaled Sohel , Mohammad Touhidur Rahman, A.K.M. Kamrul Islam, “A Review on Position Based Routing Protocol in Vehicular Adhoc Network”, American Journal of Engineering Research (AJER), Volume 02, Issue-02, pp.07-13,2013.

[2] Athira V Panicker, Jisha G, “Network Layer Attacks and Protection in MANET- A Survey”, International Journal of Computer Science and Information Technologies, Vol. 5 (3), pp.3437-3443, 2014.

[3] Bassem Mokhtar, Mohamed Azab, “Survey on Security Issues in Vehicular Ad Hoc Networks”, Alexandria Engineering Journal, Volume 54, pp.1115–1126, 2015.

[4] Manraj kaur and Parvinder Singh, “Detection and prevention of DOS Attacks Using Preventive Approach”, International Journal of Research (IJR), Volume 2, Issue 12, pp.211-219, 2015.

[5] M.Azees, P.Vijayakumar, L.Jegatha Deborah, “A Comprehensive Survey on Security Services in Vehicular Ad-Hoc Networks (VANETs)”, IET Intelligent Transport Systems, Vol.10 (6), pp.379-388, 2016.

[6] Al-Sakib Khan Pathan, "Security of Self-Organizing Networks: MANET, WSN, WMN, VANET", Chapter 10, Auerbach Publications, CRC Press, pp.218, 2016.
[7] B.S.Manoj and C. Siva Ram Murthy,"Ad Hoc Wireless Networks: Architectures and Protocols" Pearson Education, pp.436-456, 2004.
[8] Shikha Sharma, Shivani Sharma, "A Review: Analysis of Various Attacks in VANET" , International Journal of Advanced Research in Computer Science, Volume 7, No. 3, pp.249-253, 2016.
[9] Chetna Guntewar, Vaishali Sahare, "A Review on Byzantine Attack Detection and Prevention Using Game Theory", International Journal of Computer Science and Information Technologies, Volume 6 (1), pp.749-752, 2015.
[10] T.Ramaprabha, V.Premalatha, " A survey on security issues and challenges in VANET", International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) , Volume2, Issue 7, pp.876-879, 2016.
[11] Lavanya Sharma, Sunil Kumar Bharti, Dileep Kumar Yadav, " Vehicular Ad Hoc Networks (VANETs): A Survey on Security issues and challenges" International Journal of Advanced Research in Computer and Communication Engineering, Vol. 6, Special Issue 2, pp. 50-55, 2017.
[12] R.S.Raghav, R.Danu, A.Ramalingam, G.Krishna Kumar, "Detection of Node Impersonation for Emergency Vehicles in VANET", International Journal of Engineering Research and Technology, Volume 2, Issue 12, pp.3383-3389, 2013.
[13] Geetha.K , N.Sreenath, "Mitigation of session hijacking in mobile ad hoc networks", International Journal of Applied Engineering Research, Volume 10, pp. 34281-34287, 2015.
[14] Ravikiran Pandurang Pawar, "Detect and Prevent Session Hijacking Attacks in MANET", Journal of Networking, Computer Security and Engineering, Volume 1 Issue 1, pp.1-7, 2016.
[15] Fahad Nazir Bhatti, R.B. Ahmed, Mohamed Elshaikh and Hamid Mohammad Bhatti, "Comparison of Various Intrusion Detection Systems in VANET", Journal of Applied Sciences Research, Volume 11, Issue 24 ,pp.1-8, 2015.
[16] Ravi Shanker, Ashish Kr. Luhach and Amit Sardar, "To Enhance the Security in Wireless Nodes using Centralized and Synchronized IDS Technique", Indian Journal of Science and Technology, Volume 9, Issue 32, pp.1-5, 2016.
[17] Omkar Pattnaik and Binod Kumar Pattanayak, "Security in Vehicular ad hoc network based on Intrusion Detection System", American Journal of Applied Sciences, Volume 11, Issue 2, pp.337-346, 2014.
[18] Kuyoro Shade O., Okolie Samuel O. and Oyebode Aduragbemi, "Session Hijacking in Mobile Ad-hoc Networks: Trends, Challenges and Future", Research Journal of Mathematics and Computer Science, Volume 1, Issue 2, pp.1-8, 2017.
[19] Needhi Lathar, Shashi Bhushan and Manish Mahajan, "Enhanced Direction Based Hazard Routing Protocol for Smooth Movement of Vehicles", International Journal of Computer Network and Information Security, 2, pp.49-55, 2016.
[20] Uzma Khan, Shikha Agrawal and Sanjay Silakari, " A Detailed Survey on Misbehavior Node Detection Techniques in Vehicular Adhoc Networks", Information Systems Design and Intelligent Applications, Proceedings of Second International Conference, Volume 1, pp.11-19, 2015.
[21] http://www.isi.edu/nsnam/ns/
[22] http://www.tracegraph.com/download.html
[23] www.nsnam.com/2012/09/tracegraph-graphing-software-to-plot.html
[24] Richa Sharma, Jyoteesh Malhotra,"Performance Evaluation of AODV and GOD for Qos Aware Applications through Realistic Conditions in VANET", International Journal of Computer Network and Information Security, Volume 7, no.11, pp.64-71, 2015.

Authors' Profiles

R.Jeevitha, received her undergraduate degree at PSG college of arts and science, Coimbatore and has also completed postgraduate level courses Master of Computer Applications at Sri Krishna College of Technology, Coimbatore and M.Phil at Bharathiar University, Coimbatore. She is currently pursuing her doctorate in Computer Science in Dr.G.R.Damodaran College of Science, Coimbatore. Her field of interests include Mobile Computing and Computer Networks. She has eight Publications in International Journals to her credit. She has also presented six papers in International and National Conferences. She has also received Best Paper Presenter award in the International Conference.

Dr.N.Sudha Bhuvaneswari, is working as Associate Professor for more than 20 years in Dr.G.R.Damodaran College of Science, Coimbatore, India. She has authored 2 books and 3 Chapters and more than 80 Journal and Conference publications. Her Cyber Security Policy is accepted by the United Nations Organization of Internet Governance and she is a fellow in Asia Pacific Internet Governance Forum and Asia Pacific Network Information Centre. She is also the recipient of Marquis "Who is who in the World" award for the year 2012.

How to cite this paper: Jeevitha.R, N.Sudha Bhuvaneswari, "Prevention of Session Hijacking Attack in VANETs Using Intrusion Detection System", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.8, No.6, pp. 73-88, 2018.DOI: 10.5815/ijwmt.2018.06.06