Malicious node detection in VANET Session Hijacking Attack

Jeevitha. R
Dept. of Computer Science
Dr.G.R.Damodaran College of Science
Coimbatore, India.
jeevitha.success@gmail.com

N.Sudha Bhuvaneswari
Dept. of Computer Science
Dr.G.R.Damodaran College of Science
Coimbatore, India.
sudhabhuvaneshwari.n@grd.edu.in

***Abstract*—Vehicular Adhoc Networks (VANETs) consists of lot of or thousands of moving nodes. Maintaining network topology and protecting every node from attack is not practical. Malicious nodes might behave like legitimate vehicle by selectively dropping the packet and it is essential to detect their malicious nature. Entire operation of the VANET gets disturbed. This paper primarily focuses on detecting the malicious node that pretends to be a legitimate vehicle throughout the session hijacking attack in VANETs and also discusses on the throughput, delay at end points, total counts of packet generated, exchanged and dropped using the Network Simulator-2 (NS2) tool and appropriate inference provided.**

Keywords—Malicious node, Hijacking, Road Side Unit, OBU, TTP

I. INTRODUCTION

VANETs consider moving vehicles as nodes. One node can directly communicate with other node within its transmission range. The cars can connect approximately 100 to 300 meters in vehicular networks. The position of the nodes and clustering status are not constant. Network sessions carry sensitive and important data. The security of the nodes can be improved by protecting the information that is being sent between the vehicles [1].

There exists lot of research issues in VANET. The two major research issues in VANET are routing, security and privacy since VANETS are highly mobile with frequent changes in topology and network disconnection. The prevailing routing algorithms in MANETs don't seem to be available for many application scenarios in VANETs. The vehicular system focuses primarily on the secure communication schemes and algorithms. VANETs are far more liable to attack than wired network. This is due to the lack of centralized monitoring and absence of infrastructure and dynamically changing network topology.

The components involved within the VANET security architecture includes drivers, the unit inside the vehicle called the On-Board Unit (OBU), the road side component called the Road Side Unit (RSU) and attacker [1]. Even self-driving cars can be hacked. The hackers can disable safety features. For instance, recently the Volkswagen company vehicles have faced the key cloning attack that has resulted in easy unlocking of doors and has become a security breach.

II. LITERATURE REVIEW

A Security and Privacy Review of VANETs is done by Fengzhong Qu et al [1]. Their survey relies on architecture of VANETs, threats and necessities for the security issues in VANET. Each Vehicle and Road Side Unit (RSU) ought to be registered specifically with one Trusted Third Party (TTP). This paper provides an outlook on how to detect and revoke malicious node more efficiently.

Security analysis that is performed on VANETs is the work by Nirbhay Kumar Chaubey et al [2]. According to their analysis, if the authentication is carried out at the beginning of the session then it is easy for the hijackers to hijack the session at the time of connection establishment.

According to the survey on security issues in vehicular networks carried out by Bassem Mokhtar et al [3], malicious vehicle act as a legitimate vehicle to establish a session since there is no authentication process carried out at the beginning of the session. These malicious vehicles start spoofing the IP addresses of honest vehicles to perform a Denial of Service (DoS) attack on trusted vehicles, so that the trusted vehicles whose address are used for spoofing by the malicious vehicles become unavailable. The attackers make use of this unavailability and tries to hack the session.

A New Generation of Driver Assistance and Security is done by Shivam Srivastava et al [4]. A session is created and acknowledgement signal will be shared between legitimate node and victim node through Central Authority (CA). Local Authority (LA) acts as a group leader. CA will have information of each and every vehicle in encrypted

978-1-5386-8158-9/19/$31.00©2019IEEE

form. Tracking ID of the vehicle will be changed within fixed time duration by random generation.

Similar study on security challenges on VANETs done by S. Radhika et al [5] is based purely on real time constraint, data consistency liability and low tolerance for error. It is necessary to make sure that the VANET packets are not inserted or modified by the attacker.

According to Navid Nikaein et al [6] study on VANET security attacks and the Application Distribution Model, the two important layers responsible for security issues are Secure Sockets Layer (SSL) and Transport Layer Security (TLS). They are mainly used for protecting the problem of hijacking a session. Based on their study, this SSL/TLS demand for high computation power and also simultaneously increases the computational overhead incurred by the vehicles. Therefore, appropriate countermeasure for session hijacking still remains an interesting topic for research.

The study of Hamssa Hasrouny et al [7] on security risk analysis for VANET using the Trust Model identifies that in session hijacking, the attackers try to get cookies from other On-Board Units (OBU). The attacker takes the control of the entire session and the privacy is assured only by using the third-party security architecture.

The work done by done by Xiaobo Long et al [8] on detecting Session Hijacks in Wireless Networks analyzed that the generated sequence number for sessions will be guessed by the attackers. Signal strength is the major factor used for detecting a hijacked session. The component used for detecting the signal is the wavelet based optimal filter and the validation of the detected signal is verified using simulation results and inference are drawn.

The work of Uzma Khan et al [9] towards detecting malicious nodes in VANETs broadly detects malicious nodes and to improve the network performance. According to their work, a vehicle is identified as malicious when the vehicle's distrust value exceeds the fixed threshold limit.

Identification and eliminating malicious nodes from a vehicular network is the work done by Prashant Sangulagi et al [10]. Information of neighbour node is collected using mobile agents and the route is found from source to destination. Mobility of the nodes as well as the ratio of the power that exists between the intermediate nodes are being monitored continuously with the help of agents or brokers built through software engineering and when the monitored values are compared with the threshold values set in the system and if it is above the threshold value then the node is identified as malicious.

III. SESSION HIJACKING ATTACK (SHA) IN VANET

A session refers to interactive information exchange between the nodes. A session can be set up or it can be established at a certain point of time and later it can be torn down. Getting access without authorization into a session state of a particular user, then the unauthorized user is called as a session hijacker. Session Hijacking Attack (SHA) happens when a session is intruded by the attackers when the source and destination nodes are connected [11].

This hijacking mainly takes place at the link layer with the process of spoofing the MAC address and simultaneously at the transport layer by the process of spoofing the TCP sequence number. Since in this process, user authentication is done at the beginning of the session and it is easy to hijack or intrude during the session establishment or connected phase [12].

IV. MALICIOUS NODE DETECTION

The node which transmits false alerts is capable of creating drop of packets, packet delay and duplication of packets leading to network congestion. The node that causes this interruption is tagged as the malicious vehicle and it is removed from the network.

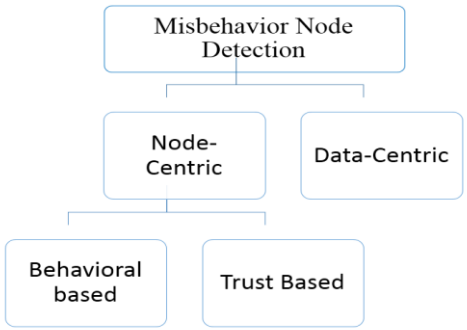

Fig. 1. Taxonomy of Misbehavior Node detection [9]

The malicious node can also behave like a normal vehicle by selectively dropping the packets. The messages that are being transmitted across the vehicles are very crucial information that includes network traffic information, road types, road conditions, information about accidents and emergency brake events and similar information. Therefore, it is critical to detect their malicious nature. Entire operation of the VANET gets disturbed.

Node-centric detection technique requires differentiating amongst specific nodes with the help of authorization. Data-centric detection technique checks the data that is being transmitted to identify misbehaviors. Node centric technique are classified into Behavioral based and Trust based detection. Behavioral based detection works towards staring at with the behavior of the node by way of

identifying trustworthy vehicles and make use of some measurements that allows to identify how effectively a node behaves. Trust based method detects a node by judging its behaviour in the past and the present and makes use of it to attain the list of nodes that misbehaves in the future [9].

V. PROPOSED WORK

All the vehicles in the vehicular network forms a cluster. A new session begins when the Road Side Unit (RSU) assigns random numeric session ID to all the nodes in the cluster. The distance between the nodes, Time gap and Traffic flow is calculated. If the distance D is less than or equal to the cluster range CR, the data transmission starts between the nodes. If the distance D is greater than the cluster range CR, the nodes are disconnected. RSU acts as Cluster Head (CH) monitors the behavior of the nodes. Machine Learning Probabilistic approach is used for detecting the malicious vehicle. The value should lie between 0 and 1. If the Traffic Flow TF is less than or equal to 1, then it is considered as honest vehicle and it is updated in registered table entry. If the Traffic Flow TF is greater than 1, then it is tagged as the malicious vehicle. The warning message is sent by RSU to all the nodes in the cluster. The entry of the malicious Vehicle V is updated in the malicious table block. Regenerate the Session Id for all other nodes in the cluster except malicious vehicle. RSU maintains the malicious node session ID as alphabetic (ASCII) value. Isolate the malicious node from the network. One RSU sends details about both registered table entry and block table entry to all other RSU in the network. Figure 1.2 explains about the workflow of the proposed work.

A. Definition of Parameters

The system uses so many parameters for finalizing the research objectives. Those parameters are listed below.

V - Vehicle
C - Cluster
D - Distance
CR - Cluster Range
TG - Time Gap
TF - Traffic Flow
S_{min} - Minimum Speed of Vehicle
S_{max} - Maximum Speed of Vehicle

B. Assumptions

S_{min} -10 Km/Hr
S_{max} – 50 Km/Hr
Transmission Range – 300 m

C. Cluster Formation

Vehicle in Cluster C = {V1, V2 …… Vn}
Co-ordinates of Vehicle1 V1= (p1, q1)
Co-ordinates of Vehicle2 V2= (p2, q2)

Distance D between vehicle V1 and vehicle V2= $\sqrt{(p1-p2)^2+(q1-q2)^2}$
where,
p1, p2 –Current Position of vehicle
q1, q2 – Position of vehicle from which distance is calculated
If (D<=CR)
Nodes are connected
Else
Nodes are disconnected
If (D>0) [No two vehicles cannot be with same speed/ velocity and same location at same time]
$TG = D_{avg} / Ve_{avg}$
where,
D_{avg} – Average distance between 2 vehicles
Ve_{avg} – Average velocity of vehicles
TF (No. of vehicles per second) = 1 /TG

D. Proposed Algorithm for Session Establishment and Malicious Node detection

Step 1: Vehicle V1, V2, V3……Vn joins the network.
Step 2: A new session begins by forming the clusters.
Step 3: Calculate the distance between the nodes, Time gap and Traffic flow.
Step 4: If (D<=CR)
Data transmission starts between the nodes
Else
Nodes are disconnected
Step 5: RSU (acting as Cluster Head) monitors the behavior of the nodes.
Step 6: If Traffic Value is lesser than or equal to 1 i.e.
If (TF<=1) then
Update the entry in registered table entry and go to step 5
Else
Go to Step 7
Step 7: Warning message is sent by RSU to all the nodes in the cluster.
Step 8: The entry of the malicious vehicle V is updated in the malicious table block.
Step 9: Regenerate the Session Id for all other nodes in the cluster except Malicious Vehicle.
Step 10: For malicious vehicle, new ASCII value is generated and stored in RSU.
Step 11: Isolate the malicious node from the network.

E. Proposed Work Flow

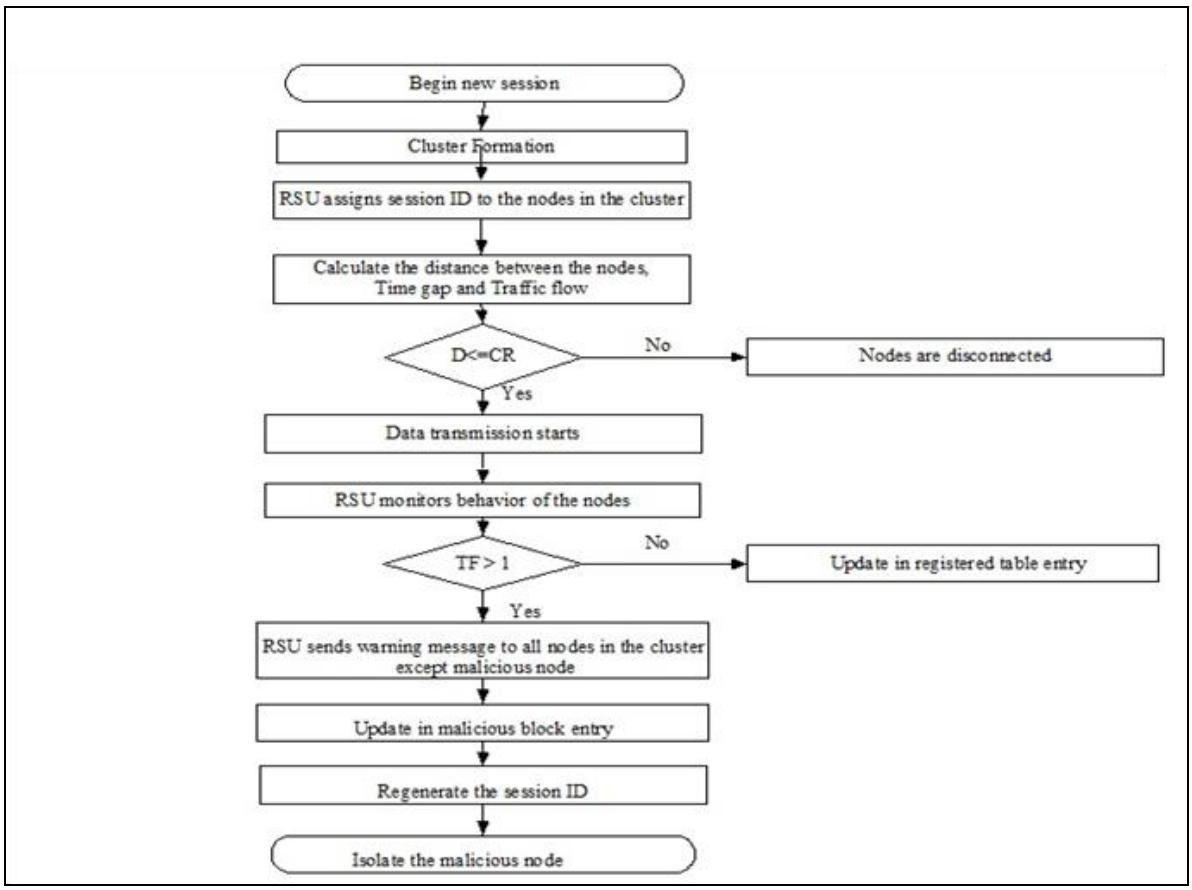

Fig. 2. Proposed work flowchart

F. Pseudo code

The proposed work is implemented in JAVA using Eclipse tool.

```
int d_n1 = rand. nextInt (10), d_n2 = rand. nextInt (10),
d_n3 =rand. nextInt (10), d_n4=rand.nextInt(10);
float d1 = (d_n1+d_n2)/2, d2=(d_n2+d_n3)/2,
d3=(d_n3+d_n4)/2, d4=(d_n4+d_n1)/2;
int d_v1 = rand. nextInt (15), d_v2=rand.nextInt(15),
d_v3=rand.nextInt(15), d_v4=rand.nextInt(15);
float v1 = (d_v1+d_v2)/2, v2=(d_v2+d_v3)/2,
v3=(d_v3+d_v4)/2, v4=(d_v4+d_v1)/2;
            timegap [0] = (d1/v1);
            timegap [1] = (d2/v2);
            timegap [2] = (d3/v3);
             timegap [3] = (d4/v4);
trafficflow [i]=(1/timegap[i]);
                    if(timegap[i]>1)
  {
            malicious_table_block [j] = temp[i];
      c1+=1;
       j++;
  }
   else
  {
     registered_table_block[k]=temp[i];
     k++;
     c2+=1;
        }
```

VI. RESULT AND ANALYSIS

As illustrated in the above pseudocode, the simulation model is set up using Network Simulator NS-2 (version 2.34). NS-2 is used for evaluating the performance of certain existed or suggested communication system, to estimate the required network parameters and metrics [13]. Total number of nodes used is 10.

Table 1. Simulation information for 10 nodes

Parameters	**Values**
Simulation length in seconds	8.688965412
Number of nodes	10
Number of sending and receiving nodes	10
Number of generated packets	3085
Number of sent packets	3010
Number of dropped packets	117
Number of lost packets	119
Minimal packet size	28
Maximal packet size	1598
Average packet size	226.8396
Minimal delay in seconds	0.001824038
Maximal delay in seconds	2.2929283225
Average delay in seconds	0.2282228487

The above table provides the simulation information for 10 nodes.

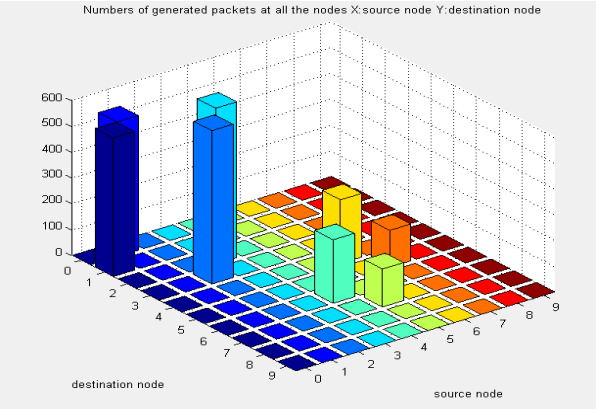

Fig. 3. Total number of packets generated

In figure 3, the packets are generated using 10 nodes and the total packets generated is 3085.

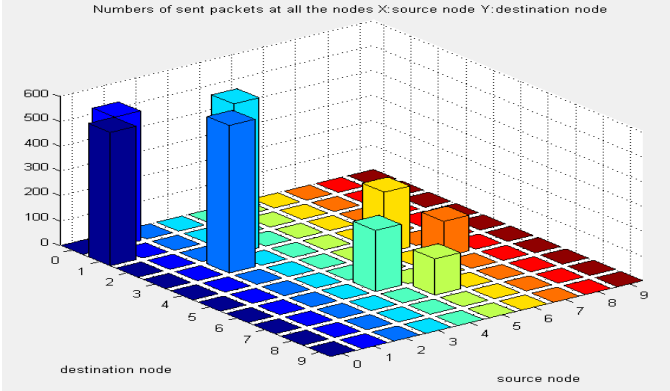

Fig. 4. Total number of packets sent

Figure 4 shows that 3010 packets are sent from source to destination node.

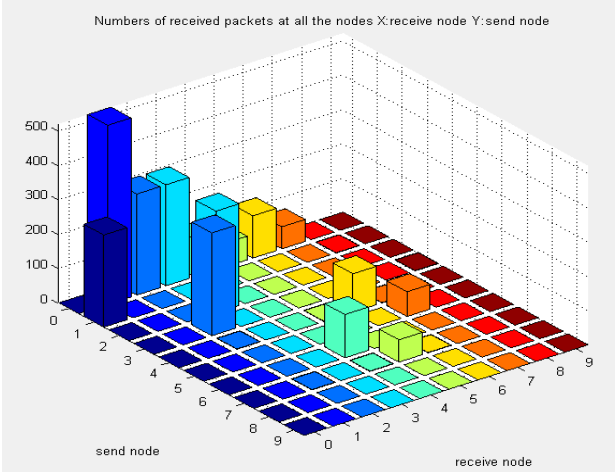

Fig. 5. Received packets

Figure 5 shows the number of packets received at the destination is 2893.

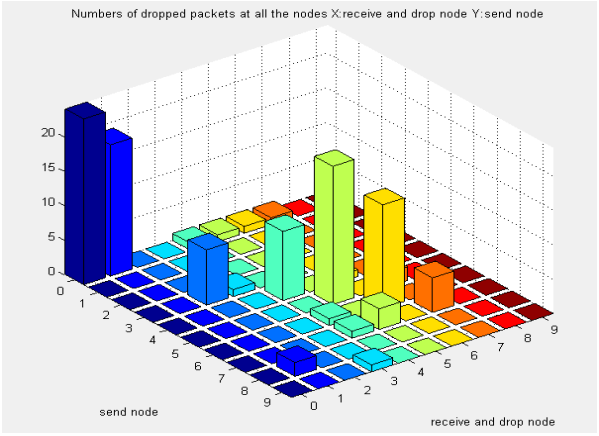

Fig. 6. Dropped packets

From the figure 6, it is inferred that totally 117 packets are dropped.

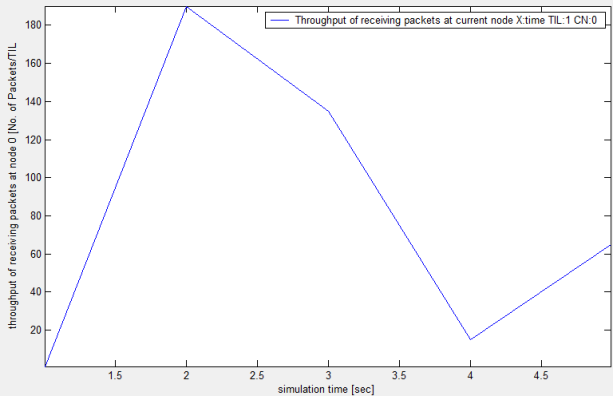

Fig. 7. Throughput

Throughput refers to the total number of successfully delivered packets at the receiver side in bits per second. The above figure shows the increase in throughput.

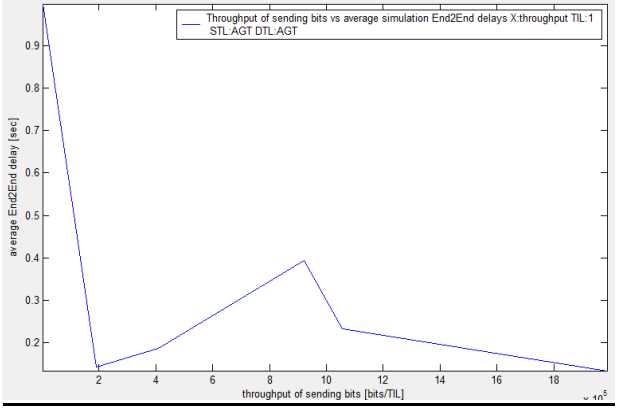

Fig. 8. End-to-End Delay for 10 nodes

End-to-End delay is the metric of time taken to transmit the packet between source and destination nodes. Delay time should be very low for better performance of network. The average delay for the proposed work is 0.2282228487 seconds.

VII. CONCLUSION

This paper discusses about how to find and isolate the malicious node in Vehicular Adhoc Networks during the Session Hijacking Attack. The proposed work shows the increased throughput, less delay and the number of dropped packet is less. This work can be further extended to include prevention technique for the malicious nodes. This research focuses on authentication level security issues in VANET. In future, other security requirements like message confidentiality, privacy, anonymity and non-repudiation can be included to the existing approach.

REFERENCES

[1] Fengzhong Qu, Zhihui Wu, Woong Cho, "A Security and Privacy Review of VANETs", IEEE Transactions on Intelligent Transportation Systems, Volume 16, Issue 6, 2015.

[2] Nirbhay Kumar Chaubey, "Security Analysis of Vehicular Ad hoc Networks (VANETs): A Comprehensive Study", International Journal of Security and its Applications, 2016.

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

[4] Shivam Srivastava, Urvashi Hasani, Vivek Kumar, Lucknesh Kumar, "A New Generation of Driver Assistance and Security", International Journal on Cybernetics & Informatics (IJCI), Vol. 6, No. 1/2, 2017.

[5] S. Radhika, S. Sindhu, "A Study on security challenges, issues and their solutions for Vehicular Adhoc Network (VANET)" International Journal of Multidisciplinary Research and Development, Vol. 2, Issue: 5, 2015, pp. 37-40.

[6] Navid Nikaein, Soumya Kanti Datta, Irshad Marecar, Christian Bonnet, "Application Distribution Model and Related Security Attacks in VANET", SPIE, Volume 8768, March 2013.

[7] Hamssa Hasrouny, Carole Bassil, Abed Samhat, Anis Laouiti. "Security Risk Analysis of a Trust Model for Secure Group Leader-Based Communication in VANET", Vehicular Ad-Hoc Networks for Smart Cities, Vol. 29, 2017, pp.71 - 83.

[8] Xiaobo Long and Biplab Sikdar, "A Mechanism for Detecting Session Hijacks in Wireless Networks", IEEE Transactions on Wireless Communications, Vol. 9, No. 4, April 2010, pp.1380-1389.

[9] 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 1,2015, pp.11-19.

[10] Prashant Sangulagi, Mallikarjun Sarsamba, Mallikarjun Talwar, Vijay Katgi, "Recognition and Elimination of Malicious Nodes in Vehicular Ad hoc Networks (VANET's)", Indian Journal of Computer Science and Engineering (IJCSE), Vol. 4 No.1, 2013, pp.16-22.

[11] R. Jeevitha, N. Sudha Bhuvaneswari, "A Session based Secured Communications for inter-networking environment in VANETs", International Journal of Advance Research in Science and Engineering, Vol. 6, Issue 12, December 2017, pp. 137-147.

[12] R. Jeevitha, 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, November 2018, pp. 73-88.

[13] http://www.isi.edu/nsnam/ns/index.html.