DOI: https://doi.org/10.24297/ijct.v20i.8852

Malicious node identification routing and protection mechanism for VANET against various attack

Er. Ritika Saini[1], Dr. Harish Kundra[2]

[1]M.Tech Student, Computer Science Engineering Department, Punjab Technical University

Rayat Institute of Engineering & Information Technology, Ropar, India

[2]Hod (CSE) Computer Science Engineering Department, Punjab Technical University

Rayat Institute of Engineering & Information Technology, Ropar, India,

[1]ritikasaini514@yahoo.in, [2]rieit_director@rgi.ac.in

Abstract: With the help of road side unit vehicles communicate among themselves. This technique termed as VANET. This network helps us to improve the safety and efficiency of the occupants during travelling in vehicles. The basic idea of this technique is to send information about the traffic information to the road side unit or other vehicles. These vehicles get safe from attacks and misuse of their private data. The objective of this paper to secure the communication among the vehicles and the road side unit. In this technique the communication mainly dependant on the safety of the road such as vehicles tracking, emergency situations and message monitoring. There are various attacks like Sybil and Gray hole attack are vulnerable to VANET. To protect from these attacks our technique provide malicious node identification mechanism that help us to provide better facility to send data to vehicles safely. To avoid these types of attacks, our propose technique include feature like key management system to prevent the communication among the vehicles. Our proposed system mostly focus on Bandwidth, packet loss and packet delivery ratio [12].

Keywords: VANET (Vehicular ad hoc network), MANET (Mobile ad hoc network), RSU (Road side unit), Access Point, OBU (On-board units).

I. INTRODUCTION

1.1 Introduction

This type of network has a property of self-configuration and this is the reason that the communication can be done in an efficient manner through this network. VANET is a part of the mobile ad hoc networks. The Vehicular ad hoc networks are the most prominent research area for the research purposes due to their increase in demand of usage. The vehicles and the elements that are present at the roadside are connected to each other for the purpose of communication and this network is self-configuring in nature. They do not require any fixed infrastructure for them. When the topology of the network is changed or there are highly moving nodes or vehicles present in the system, the routing mechanism in VANET is very difficult to perform. The attack occurs when a single node keeps sending multiple messages to other nodes which are pretended to be from different identities. In most of the cases, Sybil attack is possible. It can only be exempted from the extreme conditions and assumptions of chances of resource parity and coordination amongst the entities. A type of confusion occurs in the whole network when a single node starts sending multiple copies of it selves. The main challenge in traffic is to manage the traffic in safe and secure way. Performance can be measured by the moment of the vehicles relative to the objective of a particular transportation system and finance required [11].There is a chance that all the illegal, fake ID's and the authority are claimed. The collision within the network starts beginning which results in causing Sybil attack in the network. The main aim of the DOS attack is the prevention of a legitimate user from using the resources as well as the services. The whole channel as well as the network can be jammed in this attack. This results in an inability of not being able to access the network by the authorized vehicles. Due to its distributive nature, the DDOS attack is more harmful than the DOS attack. For the purpose of launching the attack, various types of locations are used. Various time slots can be used for the purpose of sending the messages where the natures of the message as well as the time slot are different for each vehicle. V2V and V2I can both have DDOS attack within them.In V2I technique vehicles speak with road side unit and also transmit the messages with side framework [13].

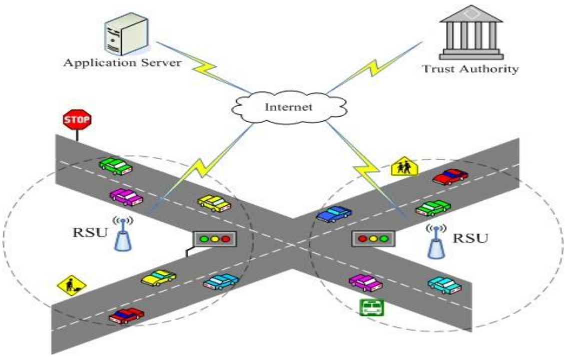


Fig: 1. VANETs Example

ATTACKS ON VANET

Incorrect information sent by a malfunctioning or attacker node might jeopardize the security and safety of the vehicles and endangers other vehicle's approaching the site. Emergency vehicle warning would have to be compromised without assurance that transmission is done from an actual emergency vehicle. Thus, it is challenging job to identify if the node spreading traffic safety information is malicious or not.

Malicious Node Identification Routing Mechanism Routing is defined as the process in which it selects best path for packet transmission from source to destination. Our proposed mechanism includes a modified AODV routing algorithm that which provide safe transmission of packets in the network. There are different scenarios for identifying attacker nodes such as Sybil attack and Gray hole attack in the network.

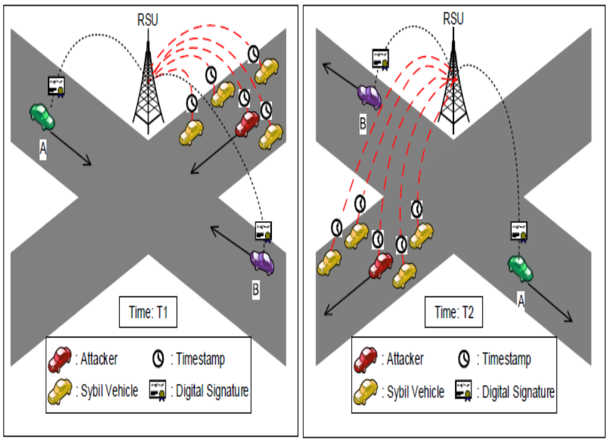


Fig: 2. Motion trajectories over time

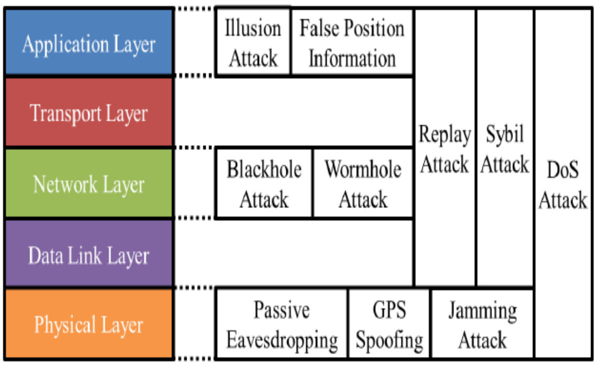


Fig: 3. Attacks with corresponding Internet Protocol Stack Layers

The above fig. shows which types of attack occur in which layer. The fig. also shows other classification such as active and passive, composite and atomic attack etc.

Sybil attack

Sensor network easily come under Sybil attack where genuine identities and forged identities used by the attackers to enter in the network. Mostly Peer-To-Peer systems face these types of attacks by faulty or hostile remote computing elements [15]. A Sybil attack is a type of attack in which a malicious node illegimately fabricates multiple vehicle identities. In a Sybil attack, there are two types of nodes that are malicious node or Sybil attacker and Sybil node as shown in fig.4

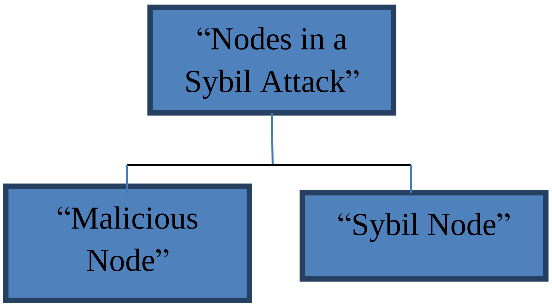


Fig: 4. Nodes participate in Sybil attack

- Malicious node/Sybil attacker: The node which spoofs the identities of other nodes.
- Sybil node: Additional identities created by the malicious node are known as Sybil node.

Fig 5 shows the typical Sybil attack in VANET scenario. Sybil attacker is spoofing the identities of A, B and C. The impact of Sybil attack gets severe when all identities created by attacker participate simultaneously in the network. Sybil attack is classified into two categories. Both of them are explained below:

Case1: When Sybil attacker creates the identities of actually existing node in the network.

Let N is the set of all vehicles in VANET and S is the set of all Sybil nodes. In this case S⊆N.

Case2: When Sybil attacker creates the identities from outside the network. Let N is the set of all vehicles in VANET and S is the set of all Sybil nodes. In this case S⊄N.

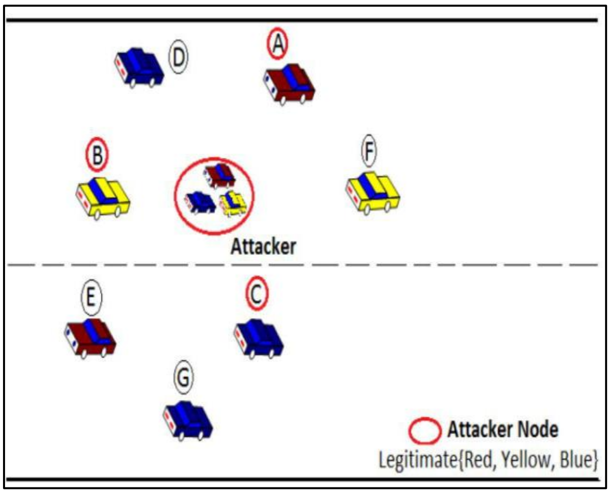


Fig: 5. Sybil attack in VANET

Due to the broadcasting feature of messages are shared over communication media. So it is easy for the attacker to get additional identity by stealing information for a malicious node. The Sybil attack mostly work on the principle that each physical node is containing only one valid identity. VANET technique is very complex in nature and its resources always need to develop lightweight security solution. So VANET required persistent and unique identity per vehicle, in order for their security protocol is in working condition. Sybil attack is the main attack in the VANET [14].

1.2 PROPOSED METHODOLOGY

Identification of Sybil attack

In our proposed mechanism Sybil attack is identified using both trusted authorities and untrusted authorities. Initially sender sends RREQ packets to their neighbour nodes. Here RSU observes RSSI (Received Signal Strength Indicator) values of all nodes that get the packets of sender node and we get the reply packets with MAC address from neighbour nodes [18]. After observing the RSSI values of nodes in the network, a signal print based Sybil classification method is used for classifying the true RSSI and false RSSI. At the end of classification, we move false RSSI values to the Department of Motor Vehicle Sector, for the accurate identification of Sybil attacker.

DMV sector consists of all information about the specific vehicle on the corresponding area[5]. The false RSSI values are verified in the DMV sector based on its MAC address and Logical address (IP address). If a node has same MAC address with different IP address then it is considered as a Sybil attacker node else it is a normal node in the network. After finding the Sybil we generate the alarm signal in the network.

```
Malicious node identification using Sybil attack:-

Input: RREQ from S, Route={a……..z}, HC[route]=0,

Timer [route]=0

Output: Identifying Sybil attack and Gray hole attack

Begin

        Step 1: S→RREQ to $I_N$

        Step 2: S←RREP from $I_N$

        //////Identifying Sybil attack

          Step 3: $I_N$ observes RSSI of RREQ

           Step 4: Each $I_N$ creates SET

           Step 5: Classify SET

           Step 6: SET→RSU

           Step 7: RSU forward DMV

           Step 8: if (RSSI==true)

                     $I_N$ Joins

                     Else

                          Create AI

       End- if

End
```

Identification of Gray hole attack

A Gray hole attack is basically the extension of black hole attack. In this, the source and monitoring systems are handled using partial forwarding. The selective data packet dropping method is presented as a normal node and this node participates in communication. A node that can behave in a complete normal manner and switch to behaving like gray hole which is actually an attacker, is known as gray hole node[4]. This gray hole node will behave completely normal and so it is difficult to identify the attacker. The routing table which contains the information of the next hop node is updated for each node. A specific route is to chosen by the node is the source node needs to route a packet to the destination node. The routing table is used to check if the route selected by the source node is available or not. A broadcasting Route Request (RREQ) message is sent to the neighbour of the node if it initiates a route discovery process. The intermediate nodes, after receiving the message, update the routing tables for reverse route to the source. When the RREQ query reaches top the destination node or any other node that has a route to the destination, a route reply message is sent back to the source node. There are two phases of the gray hole attack:

Phase 1: The AODV protocol is exploited by the malicious node. This is done to show that it has a valid route to the destination node which intends to interrupt the packets available in the spurious route.

Phase 2: In this phase, the malicious node drops the interrupted packets on the hold of certain probability. The packet selection is done on the base of this probabilistic method. The behaviour of the attacker node changes instantly which results in either transferring or dropping the packets. The malicious node creates an illusion of genuine nodes by forwarding some packets. This creates a level of difficulty of detect the attacks in the network.

Proposed Algorithm

```
Input: vehicles, RSU, malicious vehicle
Output: Malicious vehicle
Apply information gathering process
{
1.    Node send its credentials to road side units
2.     If (Matched= true)
3.    Assign identification
4.    Else
5.    Send not verified message
6.    }
7.    }
   If (Network throughput== reduced)
1.    Send ICMP messages in the network
2.    Node receive the message go to monitor node
3.    If (Node drop packets==true)
4.    Node==Malicious node
5.    Else
6.    Node=Legitimate node
7.    }
End
```

Isolation Mechanism

Security in vehicular network [1] plays a major role in an ad-hoc network to provide safe and secure communication. The security goals are authentication, integrity, robustness, confidentiality, non-reputation and anonymity. In protection mechanism, we focus on securing the VANETs from several critical attacks such as Black hole attack, Wormhole attack and Sybil attacks. To provide data confidentiality, encryption is only used for allowing honest users for reading and processing the data which are transmitted. Asymmetric algorithms such as Elliptical Curve Cryptographic algorithm are mostly preferred for packet transmission in the network; it generates private key and public key, which has higher security according. According to key base certification [7], DMV sector generates asymmetric keys for vehicles in the networks that distribute them when keys are generated. The DMV sector does a key management process which avoids the attacks in the network, by having the key table. This key table contains RSS values, MAC address and logical address and their private keys of every vehicle. During Vehicle-to Vehicle Communication and Vehicle-to-Infrastructure in the network, keys are verified.

If any vehicle enters in a VANET, it must register in a DMV sector and it gets an asymmetric key for secure communication in the network. DMV sector maintains a key management process, by recollecting all keys from every vehicle in the network and updates the new key for every vehicle at every slot K. In our routing mechanism, any vehicle suspect any malicious node in the Pseudo code: Isolation Mechanism

```
Input: Message (M)
Output: Providing secure communication
Begin
        Step 1: $Veh_i \rightarrow$ DMV
        Step 2: $Key_i$ Generation
        Step 3: Distribute $Key_i$ to all $Veh_i$
        Step 4: $Veh_1 \rightarrow M$
        Step 5: $M \rightarrow$ (Request) $Veh_2$
        Step 6: $Veh_2 \rightarrow$ (Request) RSU
        Step 7: RSU $\rightarrow$ (Request) DMV
        Step 8: DMV $\rightarrow$ (Reply) RSU
        Step 9: RSU $\rightarrow$ (Reply)  $Veh_2$
        Step 10: if (Reply is Valid)
                        $Veh_2 \rightarrow$ (Reply) $Veh_1$
                    Else
                        $Veh_2$ cancels it Reply
        Step 11: RSU generates A to $Veh_i$ and $RSU_i$
        //////Revocation process
Step 12: DMV recollects $Key_i$
Step 13: if (Key table)
          Generates new  $Key_i$
          Update $Key_i$
          Distribute  $Key_i$
 Else
          Cancel authentication to $Veh_i$
            $A \rightarrow RSU_i$
```

```
                    Generates new $Key_i$
                    Update $Key_i$
                    Distribute $Key_i$
  End
```

Network, it moves a warning message to other vehicles and again an warning signal is generated by the RSU to other RSUs. Here revocation process takes place, any malicious user have valid key, then DMV sector cancels the valid key and announces to RSU. Then every vehicle in the network cancels their connection to the specific vehicle.

If any vehicle suspects the malicious behaviour of node (i.e. malicious behaving node (Sender node) sends message to another vehicle (Receiver Node)), then it sends a message to RSU followed by DMV sector. DMV sector check the keys of the malicious node, if it is valid node, it sends a message to RSU and RSU forwards message to receiver node. Then it can continue it communication else an invalid message is received to the receiver node. Fig. 4.2 describes the pseudo code for protection mechanism. Key_i is the private keys for every vehicle, Veh_i represents the vehicles, M is the Message from sender Veh_1, Req represents the request message from Veh_1 to RSU and to DMV and Rep is the reply message from DMV to RSU and to Veh_1. A is the alarm signal that generated when malicious user communicates with other vehicle.

Fig. 7 describes the protection mechanism in our paper. In this diagram, a malicious node sends a message to normal node. Here normal node needs to check the sender is normal node or malicious node, so it sends a message to RSU, RSU sends a message by checking in the DMV Sector whether it is a valid node or invalid node. If normal node receives valid message then it continues its communication else it cancels its communication with malicious node. Then RSU sends warning signal to all vehicles and to all RSU in the network.

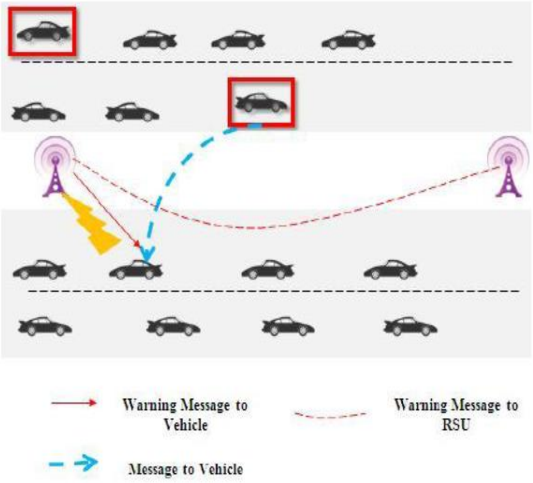


Fig: 7. Isolation mechanism

As per the security requirements and the topology we defined the output parameters will be defined**.**

NS2- It is a distinct event scheduler used to simulate wired and wireless network. It provides notable hold up to simulate bunch of vehicular protocols [2] like TCP, FTP and DSR etc. It uses TCL as its scripting language to measure and analyse performance of developed model. It run on “real time environment”. NS stands for network simulator which is primarily UNIX based it follows two groups that are event based and time based simulator. It provides collaborative environment which is responsible for freely distributed, more confidence in results. Different varieties of simulations are being done by NS like text based and animation based. Main scenario of NS is to interpret and work with a famous network simulator. For getting a better perceiving of the networking effectiveness.

Screenshots

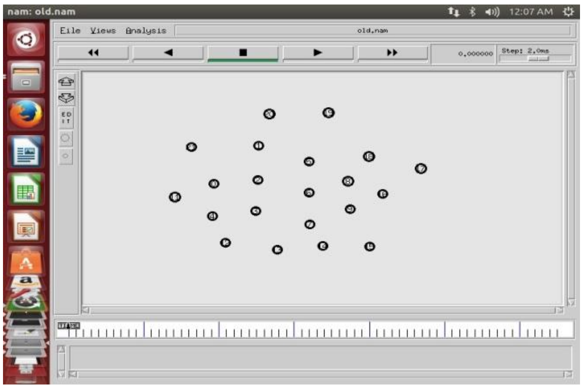
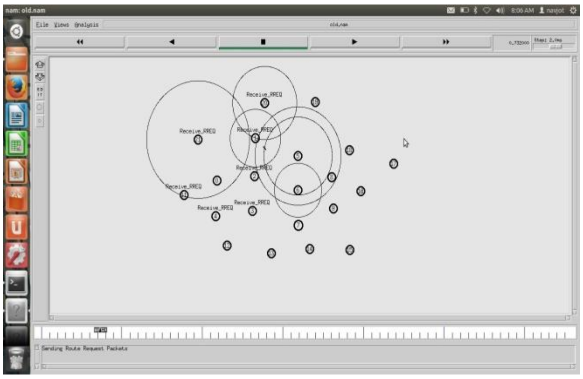


Fig: 8. Network Deployment

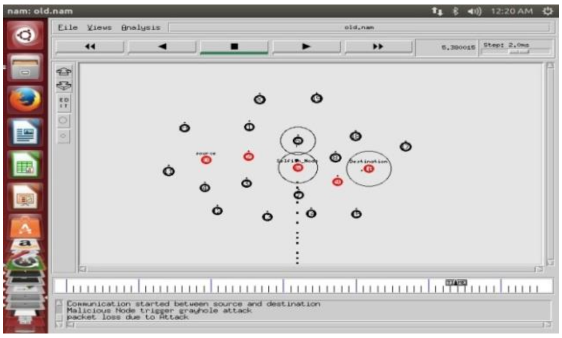
As shown in fig. 8, a fixed area is used for the placement of the “wireless adhoc network” which is responsible for the free movement of nodes from one location to another.



Sending Route Request Packets

Fig: 9. Establishing the path

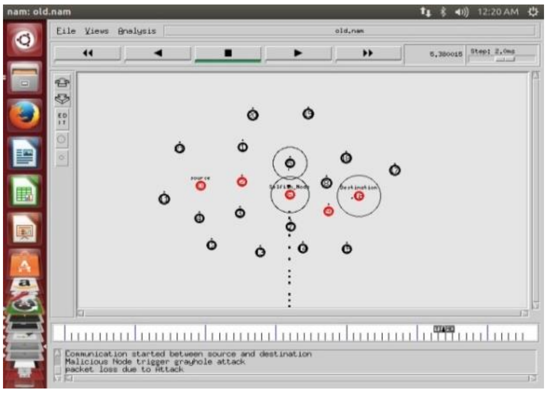
As shown in fig.9, Due to the decentralized nature of the network “nodes” can change their position freely.



Communication started between source and destination
Malicious Node trigger grayhole attack
packet loss due to Attack

Fig: 10. Triggering of attack

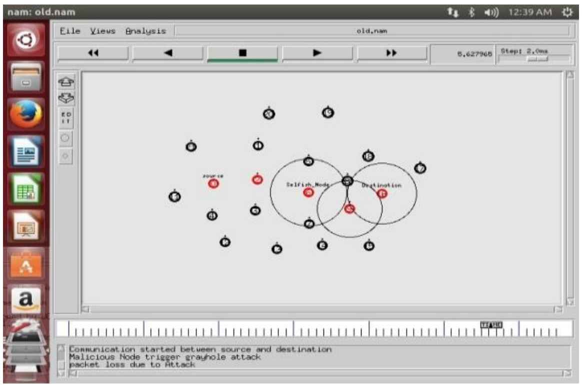
As shown in fig.10, while making the paths in between the “source and the destination nodes” the best path is being selected. The Gray hole attack will be triggered once the malicious node then it will leaves the path and this result in inclining the delay between the s and the d.



```
Communication started between source and destination
Malicious Node trigger grayhole attack
packet loss due to Attack
```

Fig: 11. Detecting the malicious node

As shown in the fig.11, the nodes which go the monitor mode will start sensing its adjacent node and node which detect the malicious node will send reply to the source about the malicious node and source will isolate that node.



```
Communication started between source and destination
Malicious Node trigger grayhole attack
packet loss due to Attack
```

Fig: 12. Isolation of malicious node

As shown in fig.12., the malicious node will be detected by the node which go the monitor mode and analyze the behavior of the node. The source will isolate the malicious node and change the path for the data transmission.

Bandwidth consumption: It is the bandwidth consumed by the vehicles at different velocities. As the no of vehicle increases the consumption also increases [10].

Table: 1. Bandwidth used

Average Velocity	Bandwidth (First)	Bandwidth (Second)	Bandwidth (Proposed)
3	15	20	15
6	28	25	24
9	55	30	28

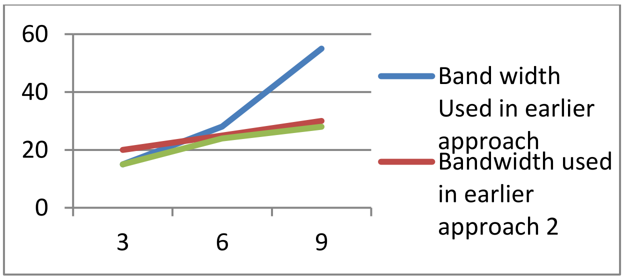


Fig: 13. Bandwidth used by different approaches

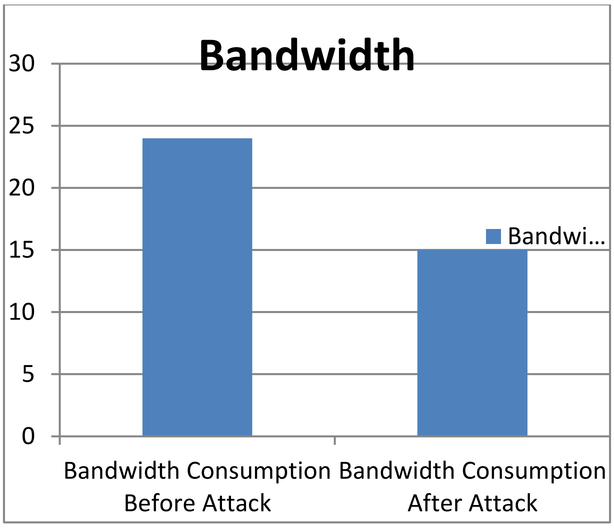


Fig: 14. Graphical Representation of Bandwidth

Table: 2. Comparisons of results

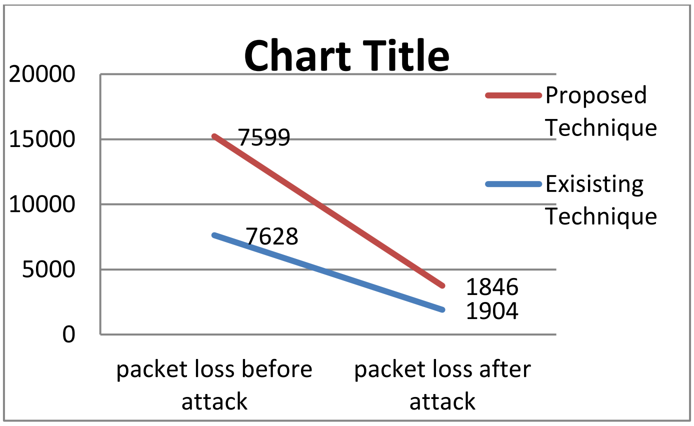
PARAMETERS	BEFORE ATTACK	AFTER ATTACK
PACKET SEND	13349	13349
PACKET RECEIVED	5721	11445
ROUTING LOAD	0.038	0.038

Packet loss in Existing approach

PARAMETERS	BEFORE ATTACK	AFTER ATTACK
PACKET SEND	13349	13349
PACKET RECEIVED	5750	11503
ROUTING LOAD	0.036	0.036

Packet loss in proposed approach

The main reason for packet loss occur only when packet are not able to reach to the destination. These occur only due to the congestion in the network. Packet loss is calculated by the ratio between number of packet send and packet loss. The transmission control protocol is the technique which is able to detect the packet loss and perform retransmission for reliable messaging. In TCP connection, packet loss is also used to avoid congestion and reduce the throughput among the connection.



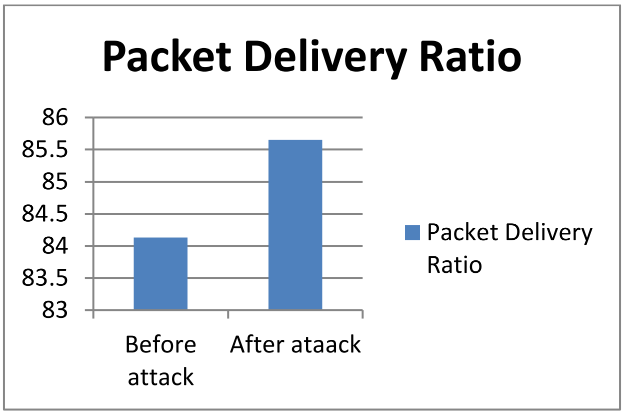
Packet delivery ratio: The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

$$\text{Packet delivery ratio} = \frac{\sum(\text{No. of packet receive})}{\sum(\text{No. of packet send})}$$

Table: 3. Packet delivery ratio

Packet Delivery Ratio (Existing work)	Packet Delivery Ratio (Proposed work)
84.13	**85.65**

the destination to the number of data packets sent by all the sources. It is calculated by dividing the number of packet received by destination through the number of packet originated from the source. It is the average at which the data is delivered successfully from one node to another over a communication network. It is usually measured in bits per second.



III. CONCLUSION AND FUTURE SCOPE

VANET is an ad-hoc network which provides links between two vehicles. It has capacity to enhance higher links and security measures. VANET has many problems in terms of security. There are various forms of attacks in VANET such as Sybil attack, Wormhole attack and black hole attack. To identify these forms of attacks we proposed a “Malicious Node Identification Routing and Protection Mechanism for VANET against Various Attacks” which comprise AODV protocol. This Routing mechanism includes three different scenarios for identifies these attacks in the network. For prevent the networks from various attacks, we introduce a Protection Mechanism that uses an asymmetric algorithm and it allows a key management based on key revocation process in the network.

Our routing mechanism provides best results in terms of packet loss, packet Delivery Ratio (PDR), Bandwidth, etc. in our future work, we enhance our routing process that identify and save VANET from endangered attacks like Gray hole attack, Sybil attack etc.

FUTURE SCOPE

- The proposed algorithm is the secure algorithm which isolate malicious nodes from the network. The proposed secure algorithm can be compared with the other secure algorithm to analyze its reliability.
- The proposed algorithm is the improvement in AODV protocol to improve security of VANET. The proposed Technique can also be tested on other routing protocols.
- In future, algorithm can be proposed which can also isolate Sybil attack using trusted and un-trusted authorities technique.

REFERENCES

[1]. Raya, M., & Hubaux, J. P. "Securing vehicular ad hoc networks", Journal of Computer Security, 15(1), pp.39-68, 2007.

[2]. Iqbal, S., Chowdhury, S. R., Hyder, C. S., Vasilakos, A. V., & Wang, C. X. " Vehicular communication: protocol design, test bed implementation and performance analysis", In Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly , pp. 410-415, 2009.

[3]. Verma Swati Bhawna Mallick Verma Poonam, "Impact of Gray Hole Attack in V ANET", 1st International Conference on Next Generation Computing Technologies (NGCT-2015) Dehradun, India, 4-5 September 2015.

[4]. Onkar V.chandure and Gaikwad V T. Article: Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol. International Journal of Computer Applications 41(5):27-32, March 2012.

[5]. Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. "Footprint: Detecting sybil attacks in urban vehicular networks", IEEE sponsored Parallel and Distributed Systems, IEEE Transactions on, 23(6), pp.1103-1114, 2011.

[6]. Zhou Tong, Roy Romit Choudhury, Peng Ning, and Krishnendu Chakrabarty, "P2 DAP –Sybil Attacks Detection in Vehicular Ad Hoc Networks", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3, MARCH 2011.

[7]. Lee, B., Jeong, E., & Jung, I. "A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET", International Journal of Security & Its Applications, 7(3), pp.1-10, 2013.

[8]. Li, M., Xiong, Y., Wu, X., Zhou, X., Sun, Y., Chen, S., & Zhu, X." A Regional Statistics Detection Scheme against Sybil Attacks in WSNs", IEEE Sponsored In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on pp. 285-291, 2013.

[9]. Praba Lakshmi V., A.Ranichitra, "Isolating Malicious Vehicles and Avoiding Collision between Vehicles in VANET", International conference on Communication and Signal Processing, April 3-5, 2013, India.

[10]. Balamahalakshmi D., & Shankar M. K. V., "Sybil Attack Detection with Reduced Bandwidth Overhead in Urban Vehicular Networks", International Journal of Engine ring Trends and Technology (IJETT)– Volume 12, pp. 578 – 584, IEEE, 2014.

[11]. Hugo Michel "Self-Organized Traffic Control", VANET'10, September 24, o, Illinois, Reena Dadhich Department of MCA, Govt. College of Engineering, Ajmer, India," Mobility Simulation of Reactive Routing Protocols for Vehicular Ad-hoc Networks" (2011)

[12]. Jason J. Haas and Yih-Chun Hu University of Illinois at Urbana-Champaign Urbana, Illinois, U.S.A," Real-World VANET Security Protocol Performance" (2007) p1-7.

[13]. Josiane Nzouonta, Neeraj Rajgure, Guiling Wang, Member, IEEE, and Cristian Borcea, Member IEEE," VANET Routing on City Roads using Real-Time Vehicular Traffic Information" (2008) p1-18.

[14]. Kelatkar, Vrushali., Dere, Pravin (2015). Lightweight Sybil Attack Detection Technique, An Overview, IJCSMC, 4 (11), (November), 173 – 180.

[15]. John R. Douceur, "The Sybil Attack", In IPTPS 01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, pp. 251-260, London, UK, 2002. Springer-Verlag.

[16]. James Newsome, Elaine Shi, Dawn Song, and Adrian Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses", In IPSN '04: Proceedings of the 3rd International Symposium on Information processing in Sensor Networks, New York

[17]. Chen C., X. Wang, W. Han, and B. Zang, "A robust detection of the sybil attack in urban vanets," in 29th IEEE International Conference on Distributed Computing Systems Workshops, 2009, pp. 270–276.

[18]. Grover J., M. S. Gaur, V. Laxmi, and N. K. Prajapati, "A sybil attack detection approach using neighboring vehicles in VANET," in Proceedings of the 4th international conference on Security of information and networks, 2011, pp. 151–158.