ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 6, June 2016

A Review on Detection and Prevention of VANET from Sybil Attack Using MAC Address

Preeti rawat[1] Shikha Gupta[2]

M-Tech Student, Department of CSE, Advance Institute of Technology and Mgt, Palwal, Haryana, India1
Assit. Prof., Department of CSE, Advance Institute of Technology and Mgt. Palwal, Haryana, India 2

ABSTRACT

The communication between the vehicles in Vehicular ad hoc networks is to improve the traffic safety for decreasing number of accidents and manages traffic for saving time. The VANET security has become very important area within the research community due to concern about human lives on the roads. In vehicular ad hoc networks, vehicles communicate wirelessly so there are more chances of the attacker to fetch the information and therefore security of this network should be considered.[1] There are different types of security attacks in VANET and one of them is Sybil attack. In Sybil attack the attacker creates multiple identities which may belong to other vehicles or dummy identities and send messages to legal nodes. These fake identities are created by the attacker to gain the trust of legal node. Here is the MAC address technique to detect the Sybil nodes[18]. This paper gives an overview of the vehicular ad hoc networks, Sybil attack, and MAC address technique.

Keywords*:* VANET, MAC address, Security.

I. INTRODUCTION

As the population growth is increasing it is leading to an increase in the growth of transportation. Nowadays technology is too advancing which provides an intelligent transportation system. VANET provides communication between closer vehicles, fixed equipment, or RSUs. It allows Vehicles to connect with each other within the range of 300 meters.[4]Vehicular nodes are used as "computer on wheels". The VANET helps it to be possible that vehicles can know about the traffic situation of the route they are moving on and then quickly share that traffic information with other vehicles. This means vehicles can get certain traffic information occurred on their driving route and can react against accidental events in advance. The fixed wired Network faces a lot of problems such as access points, cell sites and many digital devices and cables. On the other side a wireless network is easy to be installed and maintained. There are many different types of attacks by which VANET is suffering from.[11,13] This Sybil attack is severe type of attack which is named after the subject of the book *Sybil*, a case study of a woman diagnosed with dissociative identity disorder. Sybil attack is a kind of security risk when a hub in a system guarantees various characters. In Sybil attack the attacker subverts the Algorithm and section IV describes related work and conclusion in V section.

This architecture of VANET, describes that vehicles are considered as nodes which can move freely with high mobility within a network and stay connected, even if they are at high speed. Each vehicle can communicate with other vehicle via DSRC (Dedicated Short Range Communication). The communication between different units of this system is achieved through a wireless medium known as WAVE (Wireless Access for Vehicular environment). WAVE provides a wide range of Information to the entities of the system and also enables safety application to enhance road safety

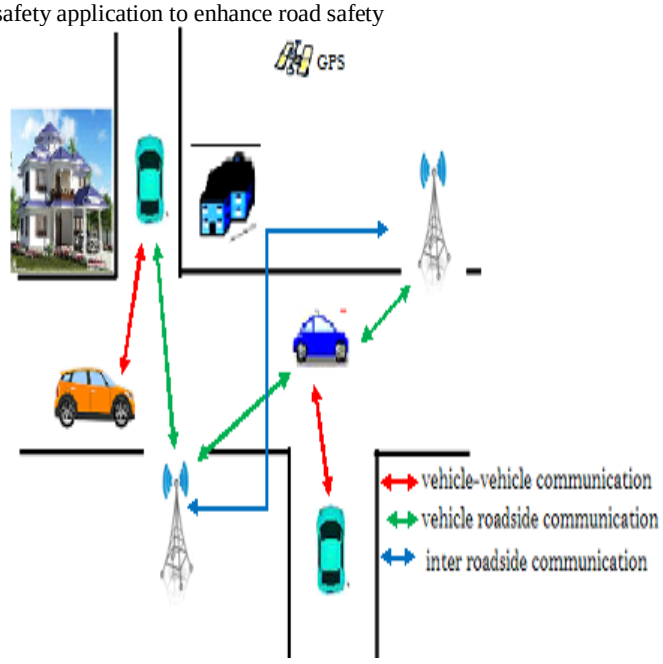

Fig 1: VANET architecture.

VANET has many applications divided into two parts Safety and Non-Safety applications[12]. These applications include distribution of multimedia information and traffic control. When VANET is used in traffic control, it helps in avoiding accidents by sharing information about the situation of road, such as road congestion and traffic

accidents Therefore, it manages city traffic, reduce number of accidents by informing the users about it and improve safety with high efficiency and high mobility[4]. Due to high mobility topology tends to change frequently. It can also helps to share some information between vehicles, such as weather forecast, petrol pumps, and restaurant addresses, music or video download services. It also allows a lot of value added services like automated toll payment, location based services like finding closest restaurant, travel lodge, fuel station.

II. ATTACKS IN VANET

Different characteristics of VANET lead to different security challenges. Some of the attacks in VANET are:

1. Black hole attack

In this attack, malicious node shows to all other nodes that it is having an optimum route to the node whose packets it wants to intercept. When the request is received the malicious node sends a fake reply with very short route. Once the node has been able to place itself between the communicating nodes, it is able to do anything with the packets passing between them.

2. Rushing attack

When compromised node receives a route request packet from the source node, it floods the packet quickly over the network before other nodes, which also receive the same route request packet can react. So in the presence of such attacks source node fails to discover any useable route or safe route without the involvement of attacker.

3. Link spoofing attack

In Link spoofing attacks, a malicious node broadcasts the information of fake route to disrupt the routing operation. The results is malicious node manipulate the data or routing traffic.

4. Denial of Service

Attackers use the network's resources preventing the important information arriving. There are two levels of this attack: Basic level and extended level [19]. In basic level attack, attackers continuously keep the nodes busy and itself keep using the network resources. In extended level attack, whole communication channel is jammed by the attackers so that other nodes cannot access the network. In this attack, important information cannot be send due to these dummy messages.

5. Alteration Attack

An attacker alters an existing data in a network. This attack includes replaying earlier transmission, altering the actual entry of the transmitted data, or delaying the information transmission. For example, message altered by an attacker that "Current route is clear" and sends this message to other nodes, but actually there is congestion on that place.

III. SYBIL ATTACK

This attack happens when a node sends multiple fake messages to other nodes and every message contains a unique source in such a way that the attacker is not known. The main goal of the attacker is to create confusion to other nodes by sending fake messages and gain trust of other nodes to leave the road for his benefit [1].We need to ensure that confidential information is neither copied nor modified by the attacker. Some of the techniques are given below:

A. Directional Antenna

This technique is used to detect Sybil attack. This method is used for direction of arriving packets and checks whether the messages has come from fake or real neighbors. This method is not perfect because sometimes it is not able to detect the attack.

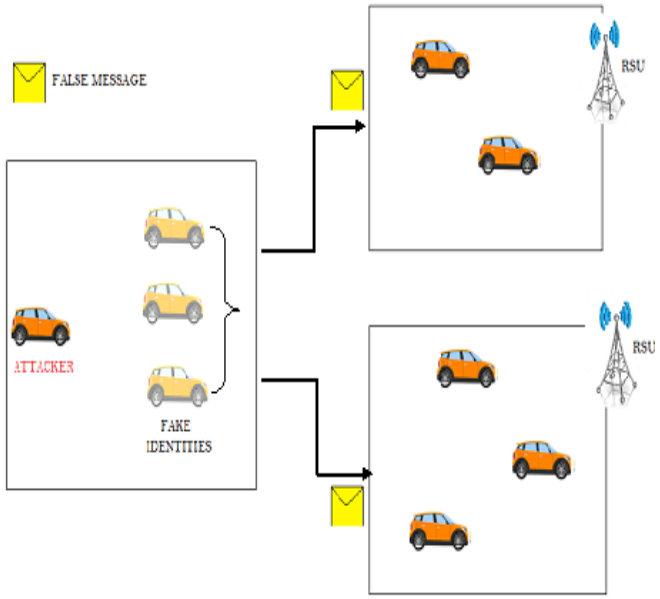

Fig 2: SYBIL ATTACK

B. Public Key Cryptography

Another mechanism of mitigating Sybil attack is by the use of public key authentication. Here the digital certificates provided by TTP and signatures using the asymmetric cryptography are combined [1].There exists a CA for each region which issues certificates and follows a hierarchy. The nodes communicate with each other by sending signed messages. This technique is able to prevent the Sybil attack because authenticated messages are kept and others are ignored. The disadvantage of this attack is that it is time consuming, very complex, and requires large memory.

C. Detection and localization of nodes

This technique detects Sybil attack by finding the physical location of nodes and comparing it with the vehicle's position. So this attack is discovered. This solution uses data obtained from GPS and is the geometric method.

IV. MAC ADDRESS

MAC (Media Access Control) address is referred to as a networking hardware address or the physical address. The MAC addresses are assigned to network interface controller and are stored in its hardware, it uniquely identifies each node and is a string of usually six sets of two digits or characters separated by colons.

Here is given the architecture to detect the Sybil node, this process follows following steps [18]:
Step 1: Start
Step 2: Detection of Sybil node can be started by any node.

Step 3: The node which want to send the message will start the detection of Sybil node before sending packet to Sybil node.
Step 4: The sender node will send request message and waits for reply packet which contains the MAC address and IP address.
Step 5: Sender node contains a table to match the addresses, if MAC address of node matches with different IP addresses the node is accepted as Sybil node and find another path to send data to destination.
Step 6: If it does not match then accept it as a legal node and send the packet.
Step 7: Stop

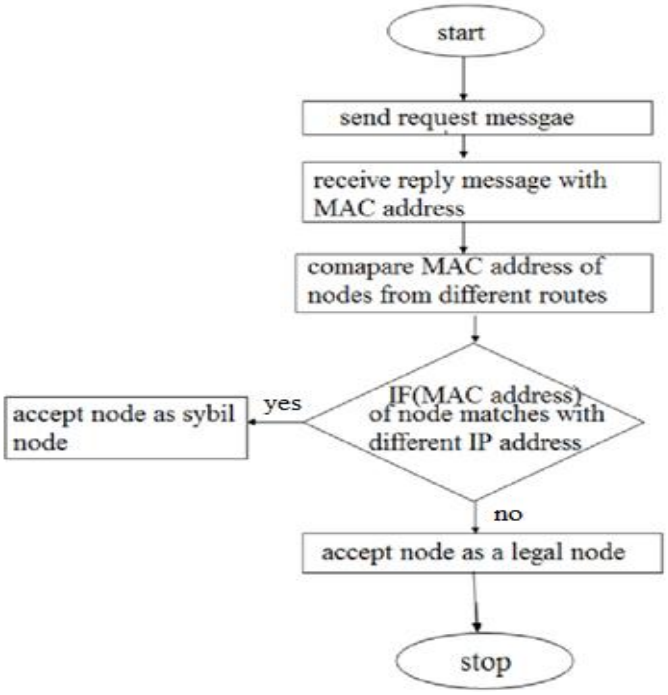

Fig 3: Architecture of detection of Sybil node

V. RELATED WORK

AUTHOR	DESCRIPTION
Ali akbar pouyan [18]	Here in this paper describing various approaches for mitigating Sybil attack in vehicular ad hoc network. In their work they had found that resource testing methods are not sufficient to implement for Sybil attack detection with high accuracy in VANETs. In contrast position based methods are easy to implement and light weight that provides high accuracy for position verification.
Anamika pareek [8]	In this paper author presented architecture for detecting Sybil attack using MAC address. From the proposed work they had found that fake sender detection, fake receiver blocking.
Sakshi gupta [14]	In this paper author proposed a privacy preserving system for detection of Sybil attack in VANET through MATLAB 7.10 environment.
Soyoung park [4]	In this paper author gives a timestamp series approach that defend to Sybil attack in a vehicular ad hoc network (VANET) based on RSUs. In this approach RSUs are the only components which issue the certificates neither it require dedicated vehicular public key infrastructure for individual vehicles, nor additional setup. This approach makes it an economical solution which very much suitable for the starting stage of VANET.
Muhammad AL-Mutaz [5]	In this paper author detecting and preventing Sybil attack in vehicular ad hoc network though platoon dispersion theory. The proposed algorithm shows similar performance for normal dispersion efficiency attack model while the minimum efficiency attack model may remain undetected at high Sybil percentages.
Harsimrat Kaur [12]	In this paper author presented a passive approach to detect a Sybil attacker by monitoring a Passive Ad hoc Sybil Identity Detection (PASID). PASID detect a single node by MAC and IP addresses.
Sohail Abbas [20]	He Proposed an RSS-based detection mechanism to secure the network against Sybil attacks. The technique worked on the MAC layer using the 802.11 protocol without using any extra hardware.
Sushmita Ruj [19]	In this paper author proposed the concept of Misbehavior Detection Schemes (MDS) to detect false messages and misbehaving nodes by observing their actions after sending out the messages. In the data-centric MDS, each node is to decide whether received message is correct or fake. Decisions of majority are not needed but the decision is based on the consistency of recent messages. When the attacker node is detected, fine is imposed on that node and not revoking identity of that node. By this scheme computation and communication costs have been reduced that were involved in revoking identity of attacker node.

Priyanka soni [11]	In this paper the author proposed a GPRS algorithm for reduction of affect of Sybil attack. By using this algorithm we are able to get the exact position of the vehicles, so that the predication of attacker node can be done. In this paper different ways like DSR, GPSR and AODV routing protocols have been described which reduces the effect of Sybil attack.

VI. CONCLUSION

VANETs is quiet not secure as well as prone to various attacks. One of the major attacks in VANET is Sybil attack which makes multiple identities to confuse other nodes and reduce the trust of legal nodes in the network. So there is requirement of a secured protocol which can be capable to rapidly organized and also use dynamic routing mechanism. Peer-to-peer systems play an ever-increasingly significant role of our daily life. Since, most of the network systems are susceptible to Sybil attacks. For designing more effective and practical Sybil defenses, we suggested an implementation depending on MAC address technique. In this paper, concerning security of the network i.e. Sybil attack has been studied. In this paper we studied prevention and detection technique using MAC address for secure network to detect Sybil attacks.

REFERENCES

[1] Preeti Rawat1, Shikha Sharma2,;" Review on Sybil Attack in Vehicular Ad Hoc Network", International Journal of Science, Engineering and Technology Research (IJSETR) Volume 5, Issue 4, April 2016.

[2] Er.Sushil Lekhi1,Gurjeet Kaur2;" A Novel Hybrid Approach of Neural Network and AOTDV for the Detection of Sybil Attack in Ad-hoc Network", International Journal of Computer Science and Communication Engineering Volume 4 issue 2(September 2015 issue)

[3] Mina Rahbari1 and Mohammad Ali Jabreil Jamali2;" efficient detection of sybil attack based on cryptography in vanet", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

[4] Soyoung Park, Baber Aslam, Damla Turgut and Cliff C. Zou,' Defense Against Sybil Attack In Vehicular Ad Hoc Network Based On Roadside Unit Support , Springer Science, Business Media.2010

[5] Samara, Wafaa A.H. Al-Salihy, R.sures, "Ghassan Security Analysis of Vehicular Ad hoc Networks"2010 International Conference on Network Applications,Protocols and Services.

[6] Nafi, N.S.; Khan, J.Y., "A VANET based Intelligent Road Traffic Signalling System," Telecommunication Networks and Applications Conference (ATNAC), 2012 Australasian , vol., no., pp.1,6, 7-9 Nov. 2012

[7] Li He; Wen Tao Zhu, "Mitigating DoS attacks against signature-based authentication in VANETs," Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference on , vol.3, no., pp.261,265, 25-27 May 2012

[8] anamika pareek," architecture for detection of sybil attack in manet using mac address", International Journal of Innovative Research in Advanced Engineering (IJIRAE) Issue 6, Volume 2 (June 2015).

[9] Biswas, S., & Misic, J to Privacy-preser. (2013). "A Cross-layer Approach ving Authentication in WAVE-enabled VANETs." Vehicular Technology, IEEE Transactions on 62(5): 2182 – 2192

[10] Mukul Saini1, Kaushal Kumar2 and Kumar Vaibhav Bhatnagar3;" Efficient and Feasible Methods to Detect Sybil Attack in VANET", International Journal of Engineering Research and Technology, Volume 6, Number 4 (2013), pp. 431-440

[11] Priyanka Soni and Abhilash Sharma, "Sybil Node Detection and Prevention Approach on Physical Location in VANET" International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 7, July 2015, pp.1161-1164

[12] Harsimrat Kaur & Preeti Bansal," Efficient Detection & Prevention of Sybil Attack in VANET" International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 9, September 2015.

[13] Jaydeep Kamani[1],Dhaval Parikh[2,"]A review on Sybil attack detection techniques", Journal for Research| Volume 01| Issue 01 | March 2015

[14] Sakshi Gupta1, Taranjit Singh Aulakh2;" Prevention of Sybil Attacks in VANETS Using Genetic Approach", International Journal of Computer Science and Mobile Computing,Vol. 4, Issue. 12, December 2015, pg.88 – 102

[15] J. R. Douceur, The Sybil attack. In Proceedings of the International Workshop on Peer to Peer Systems, March 2002, pp. 251–260.

[16] anamika pareek, " Detection and Prevention of Sybil Attack in MANET using MAC Address", International Journal of Computer Applications (0975 – 8887) Volume 122 – No.21, July 2015

[17] simranjeet kaur;" Detection and Optimisation techniques against Sybil Attack on MANET", International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 8, August 2014.

[18. Ali Akbar Pouyan, Mahdiyeh Alimohammadi;" Sybil Attack Detection in Vehicular Networks,
Computer Science and Information Technology 2(4): 197-202, 2014.

[19] Sushmita Ruj, Marcos Antonio Cavenaghi, Zhen Huang, Amiya Nayak, "On Data-centric Misbehavior Detection in VANETs", International journal of Network Security& its applications, 2011

[20] S. Abbas, , M. Merabti, , D. Llewellyn-Jones, K. Kifayat, "Lightweight Sybil Attack Detection in MANETs," IEEE, Systems Journal, Vol. 7, No. 2, 236-248, 2013.