International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 4 Apr. 2021, pp: 325-327 www.ijaem.net ISSN: 2395-5252

Advance Approach for Detection and Prevention of Sybil attack in VANET

[1]Vishwa Patel, [2]Prof. Pratik Modi, [3]Prof. Gayatri Pandi(Jain)
[1]*Research Scholar,* [2]*Professor,* [3]*Professor(HOD)*
[1] *Computer Engineering Department, LJEIT, Ahmedabad, Gujarat, India*
[2] *LDRP Institute of Technology & Research, Gujarat, India*
[3] *Computer Engineering Department, LJEIT, Ahmedabad, Gujarat, India*

Submitted: 15-04-2021 Revised: 28-04-2021 Accepted: 30-04-2021

ABSTRACT: VANET stands for Vehicular ad-hoc network, which is subgroup of MANET (Mobile ad hoc networks). VANETs are used to introduce inter communication between Vehicle nodes in the wireless network. Security of nodes is one of the major effects that exist in Vehicular ad-hoc network. Vehicular Ad-hoc networks are increasingly used to avoid accidents, traffic control and management of toll stations and public areas. VANETs are vulnerable to different types of attacks at network layer like Denial of service, black hole, gray hole, wormhole, Sybil etc. In this paper we focus on technique for detection and prevention of Sybil attack. Sybil attack is the dangerous attack inside the network layer. Most of the existing privacy schemes are susceptible to Sybil attack. In Sybil attack malicious user creates multiple identities for simulation of multiple Vehicles in network. A presented scheme uses AODV protocol which establish the route on demand and trust mechanism for detection of Sybil attack. This scheme uses an alert technique for prevention of Sybil attack.

Index Terms – AODV, Sybil attack, alert, Energy count, VANET.

I. INTRODUCTION

An Ad-hoc network is a network of individual devices communicating with each other directly. An Ad hoc network is a brief system association created for a particular reason. For example, It is used for exchanging information starting with one node then onto the next node, we utilize the Ad-hoc network. Remote specially appointed networks incorporate portable impromptu networks (MANET), vehicular specially appointed networks (VANET) and Flying impromptu networks (FANET). MANET is an adhoc network of versatile nodes while VANET is a specially appointed network of Vehicular nodes. FANET is a specially appointed network for flying nodes.

A Vehicular Ad-hoc Network (VANET) is a subgroup of Mobile Ad-hoc Network (MANET). In VANET, to make system portable, it utilizes vehicles as nodes in network. VANET transforms each vehicle which is available in the network into a remote switch or node, enabling the vehicles to interface and thus, make a system inside a wide range. It is an extraordinary sort of portable impromptu system where remote prepared component approached board unit (OBU) in vehicles structure a system with the Roadside unit (RSU) with no extra framework. VANETs purpose to provide suitable information, security and management of network. VANETs are called dynamic in nature because connection between nodes is temporary. VANET provides inter communication between vehicle to vehicle and among vehicles and road side base stations with a purpose of giving safe and effective transportation. VANET presents all the more difficult viewpoints when contrasted with MANET as a result of high portability of nodes and quick topology changes in VANET. Presently days VANET has turned into a rising region of research, development and standardization since it can possibly improve road security and vehicle safety, traffic productivity and convenience just as comfort of the two drivers and travelers. VANET can accomplish full of feeling correspondence between moving node by utilizing distinctive Ad hoc network tools, for example, Wife IEEE 802.11 b/g, WiMAX IEEE 802.10, Bluetooth, IRA. The communication range in VANET is typically 100 to 300 meter for vehicles to connecting. On the off chance that the vehicle isn't going under the range extend, the signal (flags) between vehicles will breaks and new vehicle can join if the specific vehicle is going under the system range.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 4 Apr. 2021, pp: 325-327 www.ijaem.net ISSN: 2395-5252

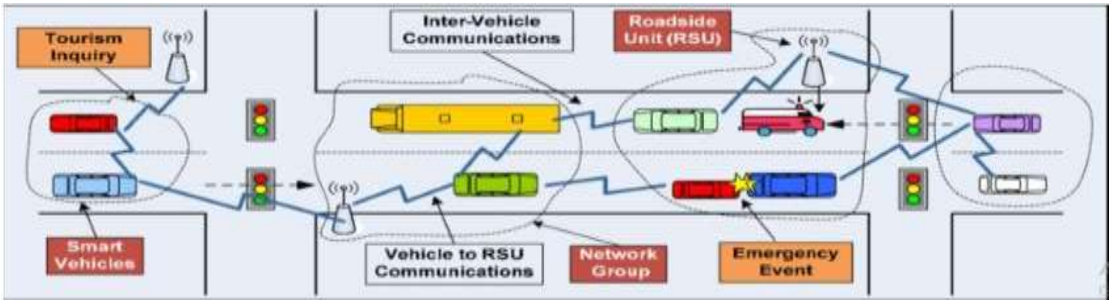

Figure 1: Basic structure of VANET[2]

Figure 1 shows the basic structure of vehicular ad-hoc network .There are various attacks like blackhole attack, denial of service attack, wormhole attack, gray hole attack, sinkhole attack and Sybil attack that can affect the entire system and modify the execution of system.

This paper is structures as follows: Section II describes about Sybil in the detailed. Section III describes Related Work presented by different authors. Section IV describes Proposed method for detection and prevention of Sybil attack. Section V we represent our analysis result. Section VI describes conclusion of our system.

II. SYBIL ATTACK.

In Vehicular ad hoc network (VANET) and in other Ad hoc network, Sybil attack is an unsafe attack. Sybil is the most dangerous attack which affect network layer. Sybil attack is a type of a security challanges when a node in a network generates multiple duplicate identities .Sybil attack have showed up in numerous scenarios with wide implications for security, safety and trust. In Sybil attack, the adversary adds a malicious node into the network or captures a legal (normal) node and reprograms it and then sends it back to the network. When this malicious node enters the network, it will start to exhibit multiple identities, represented as Sybil nodes, which will be either fabricated or stolen from legal nodes of the network.

Sybil attack can increase the traffic scenario by sending false messages in the network with multiple duplicate identities, which often creates traffic jams and also leads to Vehicular accidents in vehicular ad hoc network (VANET). When it is launched by some other conspired attackers by using their legitimate identities, It is very difficult to be detect and prevent. In this type of attack, an attacker creates multiple duplicate identities for simulation of multiple nodes. So that it will generates an illusion of traffic congestion. The Malicious nodes even misguide other vehicles, presented in the network and also takes part in voting security protocols and even it lead to loss of life.

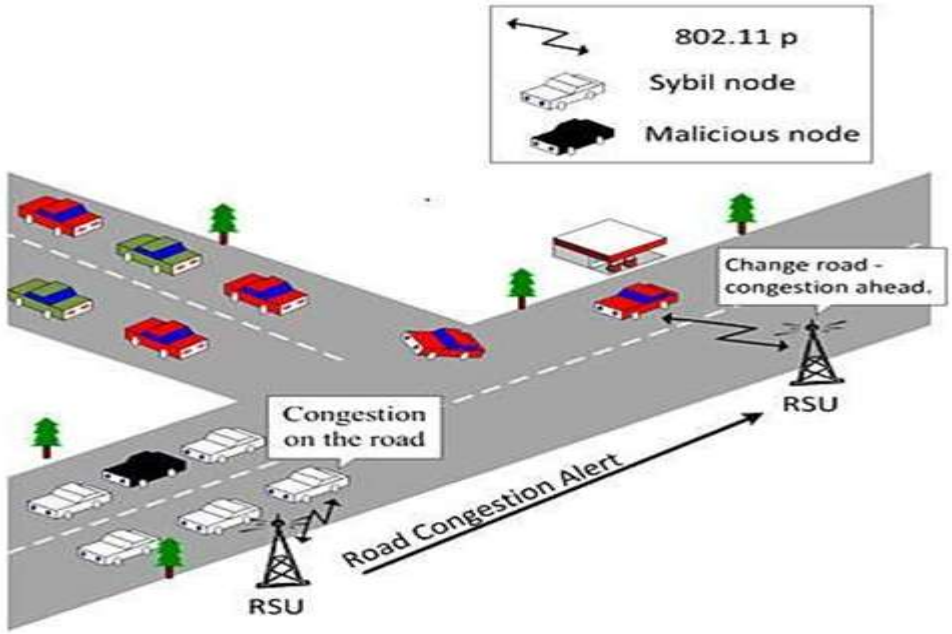

figure 2 Sybil attack

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 4 Apr. 2021, pp: 325-327 www.ijaem.net ISSN: 2395-5252

In above fig. white cars are shown as a Sybil nodes in VANET architecture. And black car is a malicious node in the network .It creates a traffic on the road.

III. RELATED WORK

In this part we deliberate some detection and prevention schemes solutions for sybil attack in VANET.

Mohamed Khalil, Marianne A. Azer [1], In this paper, Authors represents a prevention scheme for Sybil attack using identity symmetric scheme .It presents the lightweight approach for VANET. The presented protocol uses symmetric key encryption and authentication for RSUs and vehicle which are present on the road so that malicious nodes cannot generate duplicate identity in the VANET network. The lightweight protocol does not requires any managing authority for management of the vehicle and RSU communication. So that it requires less number of message for communication between vehicles. In this first of all node sends a request for authentication using Mac address. If the node is authenticated then and then it can enter the network otherwise it will discarded. Then OBU on the vehicle sends the encrypted messages using unique id of the node to RSU. If RSU can decrypt that message than the vehicle is verified. Otherwise detected as a Sybil node. Each vehicle have a unique network key when it enters the network. It requires less message for communication so that it can reduce the delay using this proposed method. Also the security of the nodes can be improved using this method.

Qing Tang, Jian Wang [2] In this paper, The Authors propose new method based on a secure positioning algorithm using number allocating scheme and mutual guarantee relying on neighbor nodes in WSN for detection of Sybil attack. Using neighbor discovery method they detect Sybil notes presented in network. In this method they use one way hash function for authentication of nodes. It provides unique number to each authenticated node. If the provided declaration number of the guaranteed node and its own unique ID doesn't match properly, then the next hop node does not allow the node to enter in the network. In this method all the nodes are statically allocated and they use identity based method for encryption. So that new node can not generate the fake identity for enter the network. Malicious node can capture the legal node in the network and attack. For detection of attack it uses random number and hash function associated with each node. This method does not requires any base station or cluster head for managing the communication ,so that communication is fast than other existing methods .Also the detection rate of this method is much more than other existing methods and the communication cost is very less .