International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 10 | Oct 2020 www.irjet.net p-ISSN: 2395-0072

An Efficient Detection and Prevention of Sybil Attack by using Different Parameters in VANET

Er. Poonam Arora, Er. Parminder Singh, Dr. Naveen Dhillon

M.Tech Scholar in R.I.E.T, Phagwara, Head of Computer Science Department in R.I.E.T, Phagwara, Principal in R.I.E.T, Phagwara

---

Abstract - *A Mobile Ad Hoc Network (MANET) is recognized as a useful internet protocol and where the mobile nodes are self-configuring and self-organizing in character. The Vehicular Ad Hoc Network (VANETs) is a part of mobile Ad Hoc Network. Vehicular as Hoc Network security is crucial, since application reliability and thus safety must not be compromised. One of the most severe attacks in these networks is the Sybil attack, in which a malicious nodes forges many fake identities to fool safety applications. It can locate Sybil nodes using short detection packets without adding special hardware or information exchange. The proposed techniques is based on monitor mode and distance based techniques. The simulation is been performed in NS2. NS2 is an open – source simulation tool running on Unix – like operating systems. The results shows that purposed technique shows good results in terms of various parameter. Here some perimeters are packet loss, throughput and routing overhead. Extensive simulation results demonstrate the accuracy of our analysis.*

Key Words: **MANET, VANET, NS2 and UNIX**

1. INTRODUCTION

Vehicular Ad hoc Network (VANET) is a system that has been made communication in between the vehicle to vehicle and road side unit (RSU) to vehicle in a short range of 100m to 300m. The main aim of deploying VANET is to overcome the accident issues. It has a large variety application for human safety and for drivers to drive well on the roads in the urban region. The rate of accidents are increased day by day by increasing the population of vehicles as well, therefore it is vital for the vehicles to impart the VANET system [1].

Vehicular Ad hoc Network (VANET) is a part and subgroup of Mobile Ad hoc Network (MANET). VANET is designed to offer the communication between the vehicles and close to infrastructure (RSU). This communication technique proposes to improve both safety and non-safety applications in vehicles on the road.
In recent years, researches are being focused on implementing safe VANET systems to overcome accidents from different cruel or harmful elements and situations that interrupt the network performance [2]. Many active and passive elements attack on VANET system to reduce the efficiency of vehicles. There are many secure and safe medium access control (MAC) mechanism and routing is being developed to keep away the system from these malware attacks. Various projects are being executed in the various countries to obtain the safety and security for the humans and also provide us better vehicle scenario for travelling on the road [3].

The main objective of this paper is to review the vehicle related issues and challenges during travelling on the road now days, there are many issues are being faced by people and people need safety. Moreover, people must be alert about the circumstances regarding vehicle safety and it is being arising research field for the researchers to interface between the vehicles and provide safety for humans. VANET provides numerous facilities to end users such as e-health facilities, multimedia, security and safety etc [4]. Now many researchers are working on developments and improvements of VANET system and also focus on the concerns like traffic management, routing, broadcasting, security and safety of vehicles.

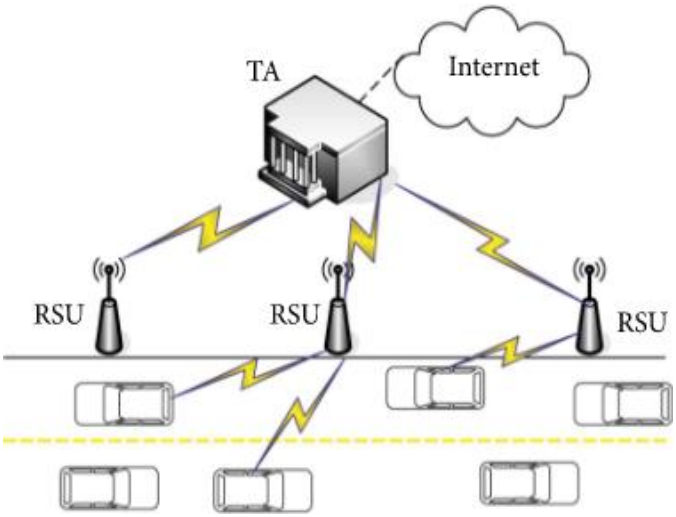

Figure 1: working of VANET.

2. OBJECTIVES OF VANET'S

2.1 Description

Nowadays, the rapid and large changes occurred in the entire domain in the world during travelling on the road. The streets are becoming dangerous by the cause of traffic

congestion and also increase road accidents. According to the survey of national road safety observatory, announced in recent years reports [5], there were 65000 above accidents in year of 2012 against that accidents had been happened in 2011. Therefore, secure traffic is not only necessity but also an essential obligation. The intelligent transport system (ITS) aims to give suitable solution to road safety of drivers and passengers and also overcome the traffic congestion problem. They enhanced also comfort and driving conditions by merging the information technology in transport systems. In intelligent transportation system (ITS), a node could be a vehicle equipped with a radio system operating in the wireless short range, and it might be also a road equipment to communicate with mobile ad hoc points, and connect them to network infrastructure [6]. The Ad hoc Network comprises of vehicle connected with sensors, on board unit (OBU) and ELP chip, where the infrastructure part includes the manufacturer, third units and service providers on board and legal authorities. The Road side unit works as a mediator between the network and infrastructure parts.

2.2 Smart Vehicle

An intelligent transport system is designed in [6], integrates basically a set of sensors that create useful environment information that generally the driver alone cannot be perceive. This intelligent vehicle finds the location by using positioning system like GPS (global positioning system), which is necessary for placing and driving support A smart vehicle integrates with communication system(multi-rate), and an event recording device which has the same function as black box of an aircraft.

2.3 VANET Standards

In addition to the services of the generation procedure, and the decrease of expenses and the time to market, standardization and institutionalization in communications and data innovation help additionally to guarantee the interoperability and the quick execution of new advancements [7]. These VANET standards are utilized for advancement of the vehicle transportation and to help clients to confirm and compare the items. There are various standards utilized as a part of VANET system, for example, dedicated short range communication protocol (DSRC) [8] and wireless access in vehicular environments (WAVE) or even IEEE 802.11p are utilized to managing the VANETs.

2.4 VANETs Characteristics

VANET is a wireless system where hubs are the settled street units or the exceptionally versatile/mobile vehicles. In foundation mode, hubs conversation with each other in ad-hoc mode and communicate with fixed hardware on the streets. Thus, the characteristic of VANET system is a mixture of remote medium attributes and the qualities of the different topologies in ad-hoc and foundation modes. These are the attributes of VANET architecture:

1. High mobility: The high versatility of VANET hubs is the imperative feature. In essential procedure of hubs communication, hubs are moving in various directions with different speed. The high versatility of hubs gives the complex topology to the system. VANET mobility range is high when contrasted with MANET. Many researchers are being committed to concentrate the effect of versatility figure specially appointed systems and particularly for vehicular systems.

2. Dynamic topology: VANET topology changes quickly, it is dynamic and unpredictable. The association time is limited particularly between hubs moving in inverse directions. This topology helps the attack of the whole system, and makes difficult the discovery of malfunction.

3. Frequent extrications: the dynamic topology and the high mobility of hubs and also different conditions, for example, atmosphere, because of movement density frequent disconnections of vehicles happened from the system.

4. Transmission medium Accessibility: In VANET system, transmission medium is air. Regardless of the way that the across the board openness of this remote transmission medium which is one of the huge points of interest in IVC, transforms into the wellspring of some security issues.

5. Limited bandwidth: The institutionalized DSRC band for VANET can be considered as constrained, whole transmission capacity range is 75 MHz. Impediment of utilization in a few nations proposes that these 75 MHz range are not all permitted. The greatest hypothetical throughput is 27 Mbps.

6. Attenuations: DSRC band has also transmission issues to computerized transmission with such frequencies, for example, diffraction, reflection, scattering, diverse sorts of blurring Doppler Impact, misfortunes and spread deferrals because of multipath reflections.

7. Restricted transmission control: The transmission power is bound in the WAVE system, which requirements the space that information can reach. This distance and space is up to 1000 m. Also, in certain particular cases for example public safety and emergency it is permit to transmit with a higher power.

3. DETECTION OF SYBIL ATTACK

Various types of malicious activities are patent in wireless sensor network. The attacks are currently classified as active and passive. The former is created by deployment of illegal information in the network that can affect it. Sybil, sinkhole, and eavesdropper are some of the active attacks. Passive

attacks are those which are meant to affect the network resources such as lifetime and network size [9].

A node or a device takes many identities that may not necessarily be lawful. It does not impersonate any node, but fast it only assumes the identity of another among several nodes, causing redundancies in the routing protocol. Sybil attacks degrade data integrity, security, and resource utilization. It can also perform storage, routing mechanisms, air resource allocation, and misbehavior detection. In a sensor network hundreds of sensor nodes form the communication network. The wireless communication between these sensor nodes passes through a central station. These nodes communicate with a specified of nodes of a specified number [10]. There are many encryption techniques available to prevent external attack on the nodes, but nodes in the communication network can also mount an attack. One of these insider attacks is called a Sybil attack [11] in which the node that spoofs the other node is called Sybil node and the other one is a normal node. In a proper communication system only nodes should communicate with one another. But here, node comes in another form of its own as an internal known node and launches an attack on the network. The Sybil node tries to communicate with neighboring nodes by using the identity of the normal node and in the process a single node gives many identities in the area to other nodes in the network which is illegal. A Sybil node can be formed as a new identity or as a pilfering legal identity. It is, therefore, considered an additional entity of a misbehaving node. This causes confusion in the network and it gets collapsed [12].

As a result Sybil attacks are classified into two forms on the basis of the manner of attack on the network. They are as follows.

(i) Direct Attack and Indirect Attack. In a direct attack, the real nodes communicate directly with Sybil nodes, whereas, in an indirect attack, the communication is done through a malicious node.

(ii) Fabricated Attack and Stolen Identity Attack. Legal identities of nodes are used to create new illegal nodes. That is to say, a sensor node which has an ID of 16-bit integers creates the same ID of 16 bits, which are fabricated nodes. The IDs stolen by the Sybil node are destroyed by checking the identity replication [13].

4. RESEARCH METHODOLOGY

The vehicular adhoc networks is the decentralized type of network in which no central controller is present and nodes can change its location any times. The vehicular adhoc networks has three major issues which are security, routing and quality of service. Due to self- configuring nature of the network, malicious nodes join the network which is responsible to trigger various type of active and passive attacks. The Sybil attack is the active type of attack in which malicious node spoof the identification of the legitimate node. The legitimate node is not able to get the required data which leads to reduction in network throughput. In this work, technique is been proposed which will detect and isolate malicious nodes from the network which are responsible to trigger Sybil attack in the network. The vehicular ad hoc network is the network which has high mobility and decentralized in nature. Due to such type of network malicious nodes enters the network which triggers various types of attacks. The security attacks can be categorized as active and passive attacks. The active attacks are those which affect network performance. The Sybil attack is the active type of attack in which malicious nodes spoof identification of the normal nodes. The normal nodes will start communicating with the malicious node instead of normal node. The Sybil attack reduces network performance in terms of certain parameters. The techniques which are proposed so far for the detection of malicious nodes have two major issues which are require extra hardware and software, accuracy of malicious node detection is low. The technique is required for the detection of malicious node which detects malicious nodes without any hardware or software and also detects malicious nodes accurately.

The proposed technique is based on the distance based technique and monitor mode technique. The distance based technique works with the beacon signals. The road side units send the beacons to the vehicle nodes in the network. The road side unit nodes, will notice the time for sending the beacon messages. The vehicle nodes receive the beacon message and reply back to the road side unit nodes. The time between sending and receiving the beacons get notes to calculate distance between road side units and vehicles. When the distance between two vehicles get mismatched then the intrusion get detected in the network. To confirm intrusion in the network, technique of monitor mode gets applied in the network. In the technique of monitor mode, the nodes start watching activities of each node in the network. The vehicle node which recently change its identification will be marked as the malicious node from the network.

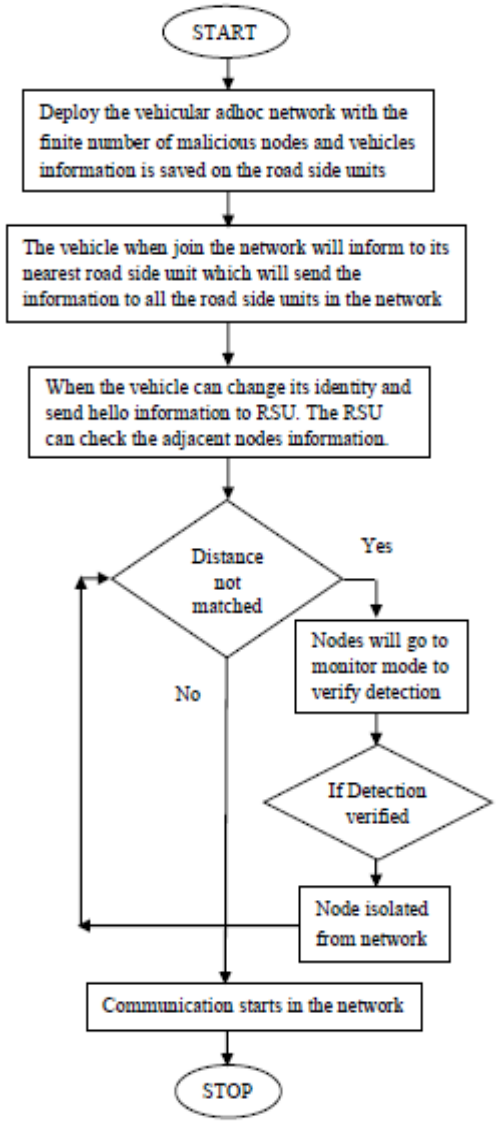

FIGURE 2: Flow chart of methodology.

5. RESULTS

The proposed technique is implemented in NS2 and the results are evaluated by making comparisons against proposed and existing techniques in terms of several parameters. Various used parameters are described below.

a. Throughput

Throughput is the number of packets sent over the network in given time. Throughput is the average rate of successful messages delivered over a communication channel. Unit: bits per second (bps).

b. Packet delivery Ratio

It is defined as the ratio of data packets received by the destinations to those generated by the sources.

PDR = (packets sent – packet dropped) / total packets sent

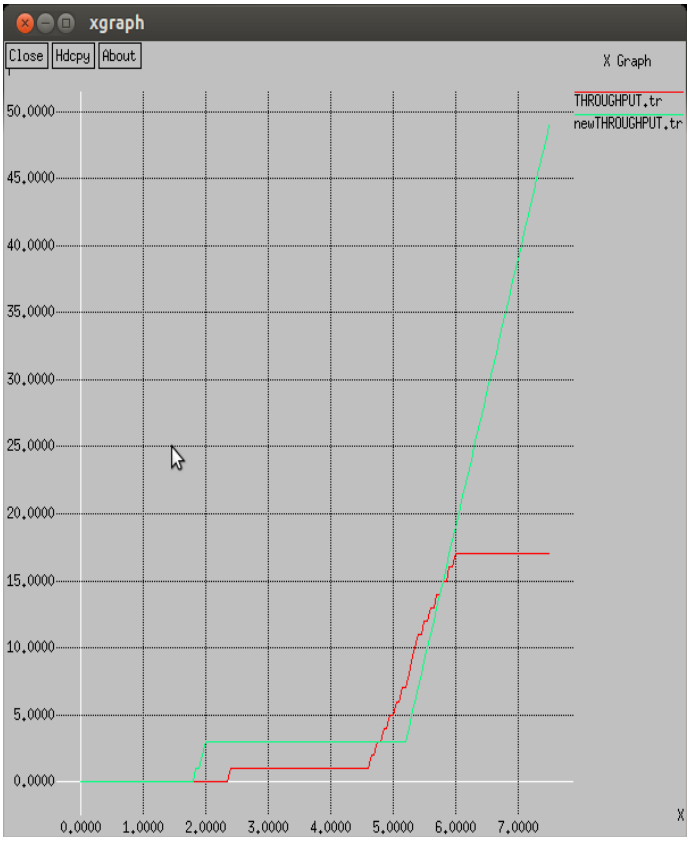

FIGURE 3: Throughput Comparison

As shown in figure 3, the throughput of the proposed and existing technique is compared and it is been analyzed that after the malicious node isolation the network throughput is increased at steady rate.

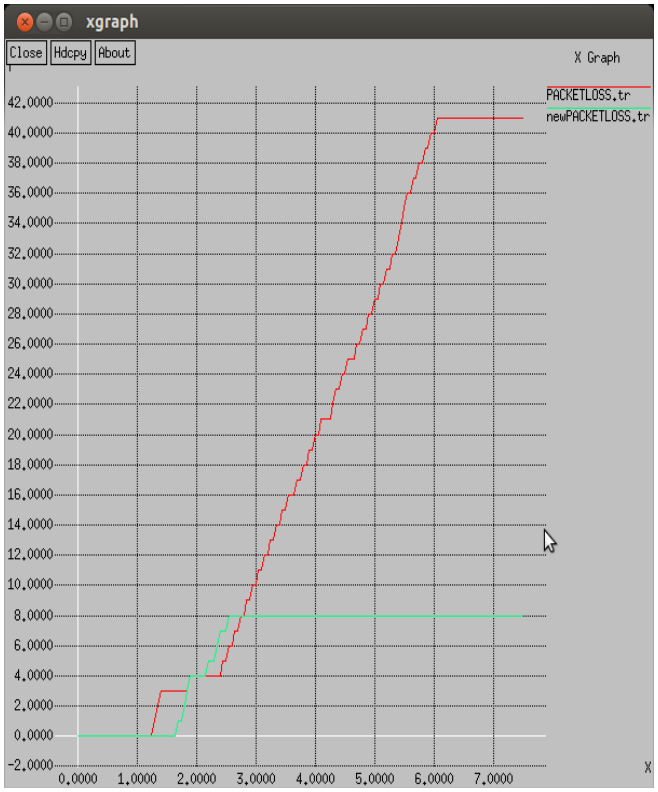

FIGURE 4: Packet loss comparison

As shown in figure 4, the packet loss of the proposed and existing technique is compared and it is been analyzed that network packet loss is reduced when Sybil attack is isolated from the network.

6. CONCLUSIONS AND FUTURE SCOPE

Vehicular Ad hoc Network (VANET) is developing into the most demanding and promising research field in wireless communication system due to its security and safety related and non-security and safety related services for users comfort. In this research paper, we have studied the fundamentals application of Vehicular Ad hoc Network, its standards, architecture, security challenges, routing issues, projects, advance VANET applications and future research issues. Scientists in everywhere throughout the world are taking a shot at the present issues of VANET system, for example, routing, broadcasting, security, safety, and implementation to extend the region of VANET. We have been clarified the VANET system models and exhibited the most recent and propelled work of VANET application which gives the best administrations to the clients. We have condensed all the security attacks and related possible approaches to overcome the security issues. This VANET study will help researchers to extend the information about VANET.

Vehicular innovation is achieving thrust as vehicles are expanding in quick away. Operation of this progress system is an essential for different safety and applications. Numerous analysts are working in this zone to give protection and security to end users. There are several research scopes which are to be studied to get innovative strategies and to give administrations to the clients. There is requiring for a few plans for controlling the measure of information deliver to the system. A key assignment for what's to come is to legitimately determine the communication requirements of vehicular applications and infer the ideal tuning of parameter of the communication system.

REFERENCES

[1] Adil Mudasir Mala and Ravi kant sahu, "Security Attack with an Effective Solution for DOS attack in VANET", International Journal of Computer Applications (0975 – 8887), Volume 66– No.22, March 2013.

[2] Ajay Rawat, Santosh Sharma, Rama Sushil, "VANET: Security Attack and its Possible Solutions", Journal of Information and Operations Management ISSN: 0976–7754 & E-ISSN: 0976–7762, Volume 3, Issue 1, 2012, pp-301-304.

[3] Jeong-Ah Jang, "A Fixed Sensor-Based Intersection Collision Warning System in Vulnerable Line-of-Sight and/or Traffic-Violation-Prone Environment", 2012, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, pp 1-11.

[4] Rakesh Kumar, Mayank, "A Comparative Study of Various Routing Protocols in VANET", 2012 pp 1-12.

[5] Reena Didcach, "Mobility simulation of Reactive protocol for VANET", IEEE, 2012.

[6] Parastoo Kafil, Mahmoud Fathy, Mina Zolfy Lighvan, "Modeling Sybil Attacker Behavior in VANETs", 2012 9th International ISC Conference on Information Security and Cryptology.

[7] Hao Wu, "An Empirical Study of Short Range Communications for Vehicles", IJSER September 2, 2011, Cologne, Germany, pp 83-84.

[8]Yuan Yao, Member, IEEE, Bin Xiao," Multi-channel based Sybil Attack Detection in Vehicular Ad Hoc Networks using RSSI". 10.1109/TMC.2018.2833849, IEEE Transactions on Mobile Computing.

[9] Surendra Nagar, Shyam Singh Rajput, Avadesh Kumar Gupta, Munesh Chandra Trivedi, "Secure Routing Against DDoS Attack in Wireless Sensor Network", 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" volume 3, issue 9, pp- 114-128, 2017.

[10] Supinder Kaur, Anil Kumar, "Techniques to Isolate Sybil Attack in VANET-A Review", 2016, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT).

[11] Anu S Lal, Reena Nair, "Region Authority Based Collaborative Scheme to Detect Sybil Attacks in VANET", 2015 International Conference on Control, Communication & Computing India (ICCC).

[12] Ashritha M, Sridhar CS, "RSU Based Efficient Vehicle Authentication Mechanism for V ANETs", 2015, IEEE Sponsored 9th International Conference on Intelligent Systems and Control (ISCO) .

[13] Mahdiyeh Alimohammadi and Ali A. Pouyan, "Sybil Attack Detection Using a Low Cost Short Group Signature in VANET", 2015, IEEE.

[14] Sebastian Bittl, Arturo A. Gonzalez, Matthias Myrtus, Hanno Beckmann, Stefan Sailer, Bernd Eissfeller, "Emerging Attacks on VANET Security based on GPS Time Spoofing", 2015 IEEE Conference on Communications and Network Security (CNS).