ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Sybil Attacks Detection in Vehicular Ad Hoc Networks

RAVNEET KAUR, NitikaChowdharyJyoteesh Malhotra
GNDU, R.C JAL assistant professor, GNDU,RC-JAL HOD-GNDU,RC-JAL

Manuscript Info

Manuscript History:

Received: 25 April 2015
Final Accepted: 22 May 2015
Published Online: June 2015

Key words:

VANET, Security, Sybil attack detection

Corresponding Author

RAVNEET KAUR

Abstract

Since few years, Vehicular Ad hoc Networks deserve much attention. The development of wireless communication in VANET implies to take into account the need of security for these networks.Vehicular communications play a substantial role in providing safety transportation by means of safety message exchange. Researchers have proposed several solutions for securing safety messages. The significant below against the security of VANET is a Sybil attack. It is an attack in which an original identity of the vehicle is corrupted or theft by an attacker and creates multiple dummy identities for stealing the vehicle. This paper briefly presents various Sybil attack detectionmechanism in VANET.

INTRODUCTION

Vehicular Ad-Hoc Network (VANET) is a specific type of Mobile Ad-Hoc Network (MANET) that provides communication between (1) nearby vehicles and (2) vehicles and nearby road side equipment's. VANETs are one way to implement Intelligent Transportation System (ITS), a technique for imparting information and communication technology to transport infrastructure and vehicles. The use of wireless communication in VANET implies an always increasing number of potential applications in these networks such as driving assistance, road traffic information or emergency braking alert.

The need of confident communications between such critical applications becomes obvious. One possible threat is the creation of multiple fake nodes broadcasting false information. This attack is known as the Sybil attack. Sybil attacks refer to a malicious node illegitimately taking on multiple identities. In this attack, an attacker node sends messages with multiple identities to other nodes in the network. The attacker simulates several nodes in the network. The node spoofing the identities of other nodes is called malicious node/Sybil attacker, and the nodes whose identities are spoofed are called Sybil nodes. Almost every other attack can be launched in a network in the presence of Sybil attack. One possibility could be an illusion of a traffic jam or accident so that other vehicles change their routing path or leave the road for the benefit of the attacker. Sybil attacker can also inject false information in the networks via some fabricated non-existent nodes. The goal of detecting Sybil attacks is to ensure that each physical node is bound with only one legal identity. We refer to a vehicle as a node in the context of VANETs. We refer to a physical node claiming multiple identities as a malicious node and, correspondingly, the malicious node's fabricated identities as Sybil nodes.The following issues are identified in Vehicular Ad-hoc Network with respect to Sybil attack.

a) It constraints more bandwidth overhead.
b) It takes revocation cost.
c) It takes time delay and message loss ratio.
d) More traffic congestion and complex roadways.

Therefore, this paper provides more safe transportation by safely exchanging the messages for the road situation and the traffic flow between vehicles for VANET by detecting a Sybil attack.

I. VANET overview

A. *Architecture of VANET*

VANET architecture is designed for Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications. There are two types of nodes in VANET; mobile nodes as OBUs (On Board Units) and static nodes as RSUs (Road Side Units).

VANET's technology uses moving cars as nodes in a network to create a mobile network. VANET turns every participating vehicle into a wireless router or node, allowing vehicles approximately 100-300 meters of each other to connect and create a network with a wide range. As cars fall out of the signal range and not able to catch the network others cars can join in, connecting vehicles to one another so that a mobile internet is created. It is estimated that the first systems to fully integrate this technology will be the police and fire vehicles to communicate with each other for safety purposes.

VANET can be used for alert the driver of emergency vehicles. These cars serving incidents may then launch alert signals which are transmitted car to car along the road. In the event of an accident, an early collision warning system could be used to prevent approaching Cars from crashing as well.

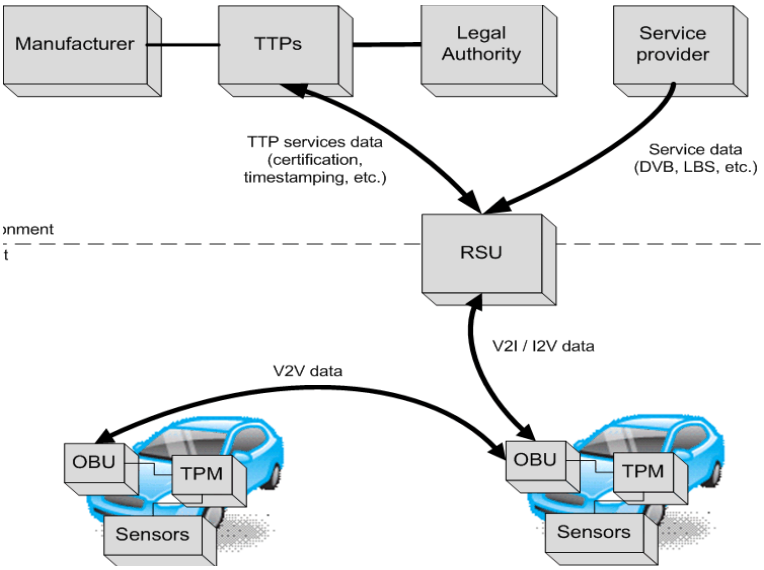

Fig. 1.1- Architecture of VANET

B. *Barriers to implementation*

(i) Financial issues: The development costs for the system are very high, but their implementation costs will be very low. The intelligence needed in the cars for processing the information also not a major cost factor. However, the first tens of thousands of cars equipped with the system in the system until there is a sufficient number of cars in the network with which to exchange information, and car owners will therefore be reluctant to spend any additional money on extras which have no use for them for years to come.

(ii) Technical barriers: High mobility of vehicles in VANET introduces frequent topology changes that negatively affect existing solutions. To develop effective localisation and data gathering mechanisms, several challenges have to be faced.

A VANET requires fully decentralised network control since no central entity could or should organise the network. Moreover, VANETs hold an additional complexity due to special conditions such as timing and reliability requirements.

Because of the number of vehicles that could be incorporated into vehicular networks, VANET may become the largest ad hoc network in history. Scalability, undoubtedly, will be a critical factor.

Protocol designers should also consider the possible consequences the protocol may have on the physical world. Protocols should be adaptable to real-time environmental changes, including vehicle density and movement, traffic flow, and road topology changes.

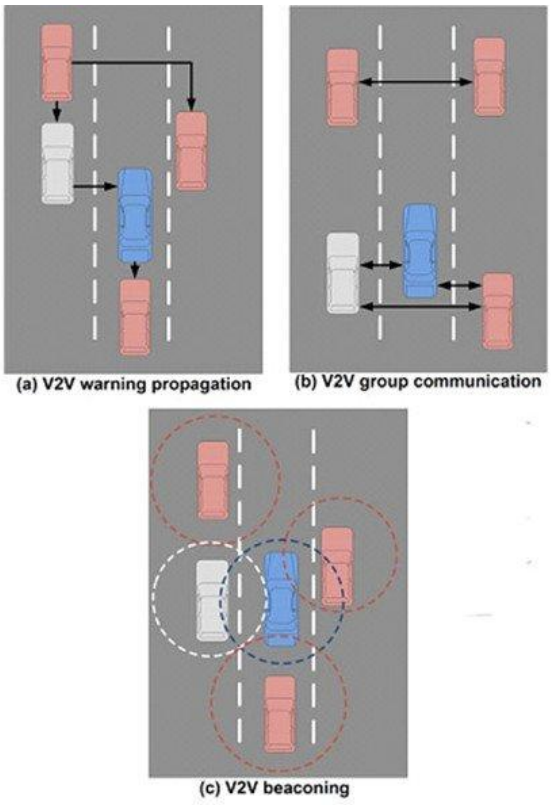

Fig 1.2: Wireless Communication Pattern in VANET

C. VANET characteristic's

In addition to the similarities to ad hoc networks, VANETs possess unique network characteristics that distinguish it from other kinds of ad hoc networks and influence research in this area. Few important characteristics of VANETs are as following:

(i) High Mobility
(ii) Rapidly changing network topology
(iii) Unbounded network size
(iv) Frequent exchange of information
(v) Wireless Communication
(vi) Time Critical
(vii) Sufficient Energy
(viii) Better Physical Protection

D. Security issues/attacks in VANET

VANET facing many attacks; these attacks are discussed in the following subsections:

(i) *Denial of Service attack:* This attack happens when the attacker takes control of vehicles, resources or jams the communication channel used by the Vehicular Network, so it prevents critical information from

arriving. Attacker is malicious, active, and local in this case. Attacker may want to bring down then network by sending unnecessary messages on the channel.

(ii) *Message Suppression Attack*: An attacker selectively dropping packets from the network, these packets may hold critical information for the receiver, the attacker suppress these packets and can use them again in other time.

(iii) *Replay Attack:* An attacker may drop legitimate packets. For example, an attacker can drop all the alert messages meant for warning vehicles proceeding toward the accident location. Similarly, an attacker can replay the packets after that event has been occurred to create the illusion of accident.

(iv) *Eavesdropping:* It is the most prominent attack over VANETs against confidentiality. To perform it, attackers can be located in a vehicle (stopped or in movement) or in a false RSU. Their goal is to illegally get access to confidential data. As confidentiality is needed in group communications, mechanisms should be established to protect such scenarios.

(v) *Sybil attack:* VANET supports the services associated with drivers' safety such as the information transmission between vehicles, the rear-end collision between vehicles, and the warning about dangerous situations in real time. In fig (1.3) & (1.4) the attacker sends wrong messages such as the information transmission between vehicles, the rear-end collision between vehicles, and the warning about dangerous situations. It throws other vehicles confusion. That is, as the objective of a Sybil attack is to make other vehicles change the route on the road or leave the road for the attacker,a Sybil attack can be a serious threat because it causes great damage to a VANET's function.

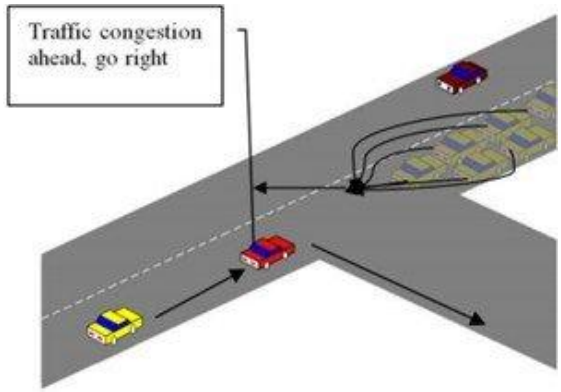

Fig. 1.3- Sybil Attack

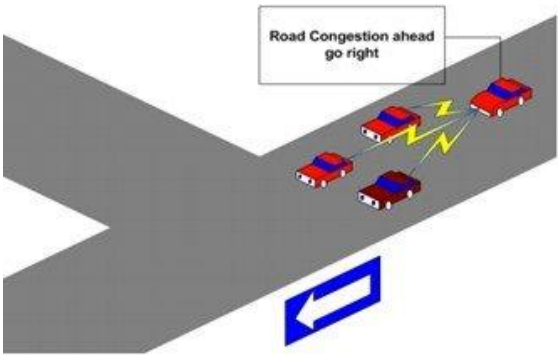

Fig. 1.4: Selfish Driver

II. Detection of Sybil attack

Different techniques are proposed for detection of Sybil attack in VANETs. Sybil attacks are always possible in the absence of any logical centralized authority. Some constraints such as validating all entities simultaneously by all nodes and strict coordination among entities are necessary for detection of a Sybil attack. Some techniques are described below.

A. *Resources testing***:** The method proposes resources testing as defences against Sybil attack. This resource testing is based on the assumption that each physical entity is limited in some resource. A typical puzzle is given to all the nodes in the network for testing computational resources. If resources of a single node are used to simulate multiple entities, any particular entity will be resource constrained in computation, storage, and bandwidth.The goal of resource testing is to attempt to determine if a number of identities possess fewer resources than would be expected if they were independent.

B. *Use of public key cryptography***:** In this scheme, each node is pre assigned a unique secret key to derive one-way key chains and an identity certificate which associates its. This technique can prevent Sybil attacks as only messages with valid certificates are considered and invalid messages are ignored. The only requirement is that each node should be assigned one certificate at a time. For privacy implementation, these certificates are changed from time-to-time.

C. *Time Stamp Series data propagation***:** On simple structured roadways that have multiple lanes and have no traffic congestions, vehicles move dynamically at different speeds and move independently. Based on this phenomenon, we discover that it would be rare for arbitrary two vehicles to pass through a few different RSUs far apart from each other always at the same time. Therefore, if a traffic message sent out by any vehicle contains several timestamps issued to this vehicle by the previously passed RSUs suspected as Sybil messages created by a single vehicle. This approach requires that only RSUs can issue timestamps and a vehicle cannot use a timestamp obtained by others.This method has challenges, for example If RSUs are located at intersections, it may make the Sybil attack detection difficult, so this method not suitable approach to detect Sybil attack
.

D. *Secure positioning***:** Another possibility to defeat Sybil attack is to provide a secure positioning system and the reliability of the position claimed by vehicles. The method uses characteristics such as signal strength and direction so it assumes directional antennas and node's cooperation. The authors present a novel approach called verifiable Multi alteration, using distance bounding protocol and base stations to provide secure positioning. They also assume that all network nodes can establish pair wise secret keys.

E. *Propagation Model:* In this technique, the received signal power from a sending node is matched with its claimed position. In, a node collects signal strength measurement from other nodes and estimates their new position according to a given propagation model. A node is considered suspect if it's claimed position is too far from the evaluated one.

III. VANET ROUTING PROCOLS

In VANET, the routing protocols are classified into five categories: Topology based routing protocol, Position based routing protocol, Cluster based routing protocol, and Geo cast routing protocol and Broadcast routing protocol. These protocols are characterized on the basis of area / application where they are most suitable. Fig. 3.1 shows the different routing protocols in VANET.

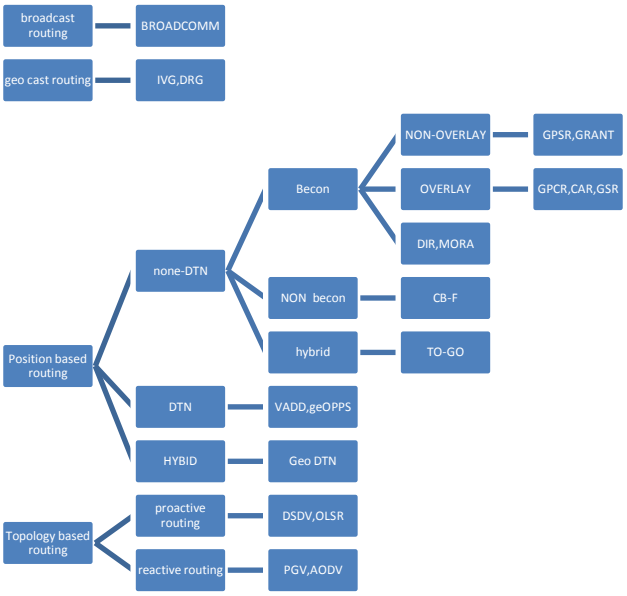

Fig 3.1: Different routing protocols in VANET

A. Simulation Based Analysis Using Network Simulator

(i) *NS-2*: Network Simulator (Version 2), widely known as ns-2, is simply a discrete event driven network simulation tool for studying the dynamic nature of communication networks. It is an open source solution implemented in C++ and Otcl programming languages. Ns-2 provides a highly modular platform for wired and wireless simulations supporting different network element, protocol (e.g., routing algorithms, TCP, UDP, and FTP), traffic, and routing types. In general, ns-2 provides users with a way of specifying network protocols and simulating their corresponding behaviour's. Result of the simulation is provided within a trace file that contains all occurred events.

(i) *Programming languages in NS-2:* The reason for having two programming languages stems from the aim to have an easy to use, yet fast and powerful simulator. Object-oriented C++ forms an efficient class hierarchy core of ns-2 that takes care of handling packets, headers and algorithms. Object Tcl or OTcl, is also an object oriented programming language utilized in ns-2 for network scenario creation, allowing fast modifications to scenario scripts. OTcl in ns-2 enables full control over simulation setup, configuration, and occasional actions (e.g. creating new TCPflows).C++ object oriented language is used for byte manipulation, packet processing and algorithm implementation.

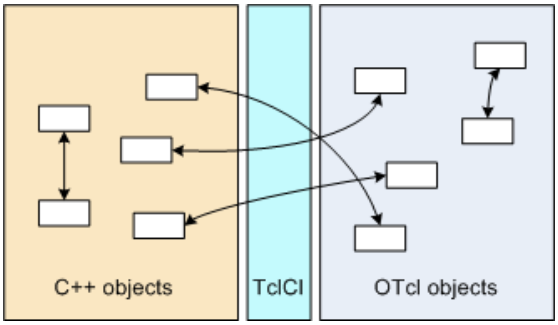

Fig 3.2: C++ and OTCL communication.

(ii) *Selection of routing protocol*: In this the analysis of ad hoc routing protocol is done in realistic scenario of VANET. After doing the simulation based analysis of AODV, DSR, OLSR and DSDV in realistic scenario of VANET we can see in fig (3.3) that the performance of AODV in terms of PDR is very good

approximate 98% and DSDV is approximate 97%. OLSR has average performance as the PDR. The Average end to end delay of AODV is very high. The DSR performs well in both of the scenario in terms of Avg. end to end delay as shown in fig (3.4). OLSR is also having low end to end delay. Packet delivery Ratio of AODV is better than other three protocols so we can say this protocol is applicable to carry sensitive information in VANET but it fails for the scenario where transmission time should be very less as it has highest end to end delay. For quick transmission DSR performs well but not suitable to carry information as packet loss is very high. The performance of OLSR is average.

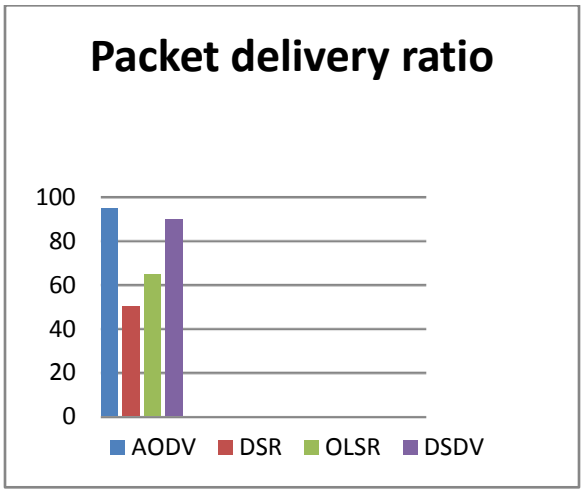

Fig. 3.3- PDR vs. node density at city low density

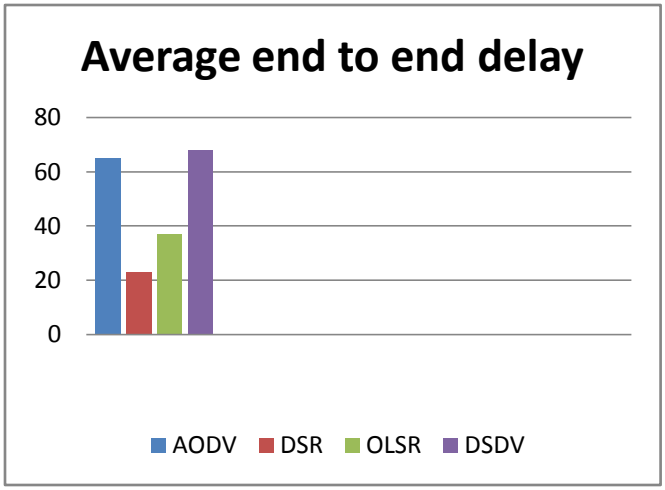

Fig. 3.4- Average E2E delay (in ms) vs. node density at city low density

B. Simulation Experiment Design

(i) Simulation Scenario: It depends mainly on the end to end throughput and average delay. Different applications place different requirements on the network. Real time applications such as voice over IP are highly sensitive to delay but function satisfactorily with little bandwidth. At the other hand data transfer applications like FTP are insensitive to delay but require as much bandwidth as possible. In this section we are going to present simulation scenario aimed at stimulating the network performance through network throughput, packet drop rate and average packets end to end delay.Within the scenario we have stated clearly the layout and configuration of our network and the simulation experiment setup.

(ii) *Network layout*: In our scenario we have two nodes of vehicles/cars and one Sybil node covered by the three towers.Three towers are considered to be RSU's in the wireless network which pass on the information from vehicles (OBU's) to central office. Additionally, the following conditions for access are presumed:
1) Each user (vehicle/car) passes its information to its respective tower whichever is in its range.
2) Each RSU is connected to the central server where whole information about the vehicles is stored.

(iii) *Determining the Throughput packet dropout and average Packets End To End delay*: The nodes in our scenario use IEEE 802.11 standards (CSMA/CA) to communicate with each other. We are going to use the simulation for:

- Determining the throughput for each node; ns-2 should calculate the bytes received by each node.
- Determining the packet loses; ns-2 should calculate the bytes that are transmitted and not receive by any node. Determining the average packets end to end delay; ns-2 should calculate the difference time of the last packet received and the number of all packets received.

C. *Simulation results:*As we know, wireless simulators provide full control to researchers in investigating traffic flow behave our, but do not always reflect real-world scenarios.Therefore, in this chapter we will present results of simulation obtained by using ns-2 simulator where the experiment setup is aimed primarily at demonstration of ns-2 features and illustrations of some basic performance for simulated network. The results of our simulation from ns-2 trace files are shown in subsequent sections.

I. *Nam Output*: The Nam class outputs at runtime in our simulation setup (Figures 3.5 and 3.6) show two networks consisting of two vehicles node_1 and node_0) and three nodes (node_2, node_3 and node_4) . In the second scenario there is additional node which is a Sybil car (node_5).

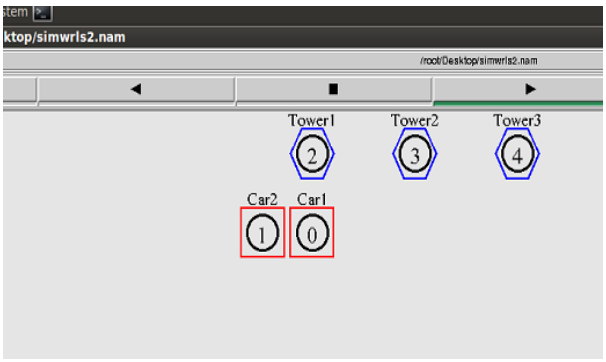

Fig. 3.5: General movement of two nodes with their towers

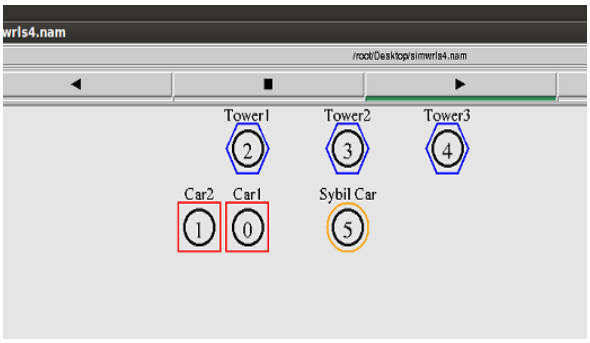

Fig 3.6: (Traffic) 2 nodes follow behind Sybil node who fakes traffic.

II. *The Network Throughput:* In this subsection we are showing the simulation results illustrating the network throughput. We will compare throughput of different scenario the one with Sybil car and other with no Sybil car as shown in Figure 3.7 and figure 3.8 here, the X axis represents the time of simulation and Y axis represents the throughput.

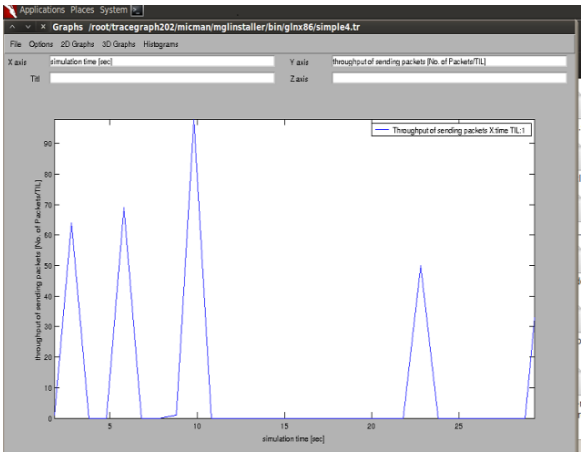

Fig.3.7: **Throughput of general movement**

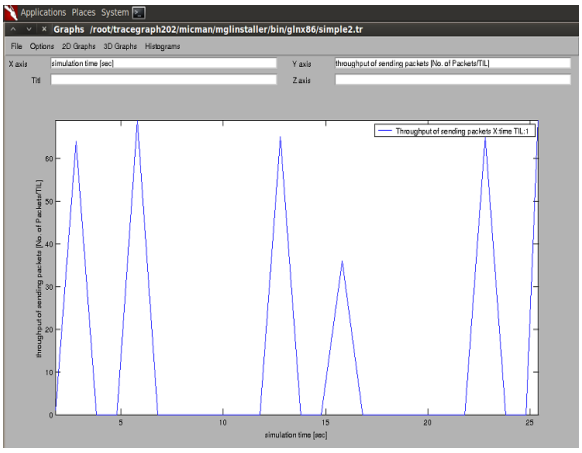

Fig 3.8: **Throughput of 3 nodes following Sybil car.**

III. *Packet Drop Rate:* Packet drop occurs when one or more packets of data travelling across a computer network fail to reach their destination. Figure 3.9 show the packets sent where X axis represents the source node Y axis represents the destination node and Z axis represent the number of packets sent. Figure 3.10 show the dropped packets where X axis represents the receiveand drop node, Y axis represents the sent node and axis Z represents the dropped packets.

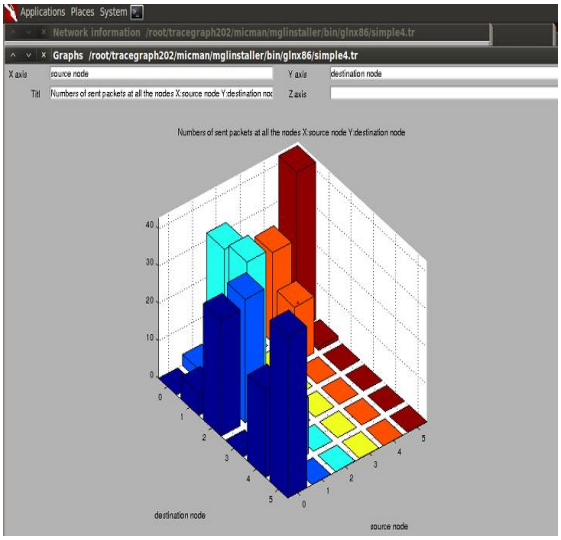

Fig 3.9: **Number of packets sent**

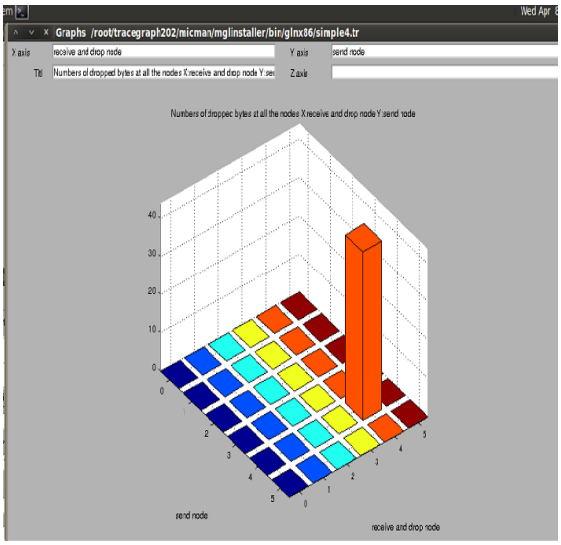

Fig 3.10: **Number of packets dropped**

IV. Conclusion

This paper include various types of attack involve in VANET and their detection mechanism also provided. We showed that only certain areas may contain cheated nodes. There is no unique method for identifying and removing the Sybil attack in the VANET. Each method has its own advantages and disadvantages. The number of issues such as detecting the presence of Sybil attacks, localizing multiple adversaries and eliminating them are not solved effectively. As we have characterized such areas, we think that the results given in this paper provide a good framework to elaborate realistic test suites for Sybil attack detection methods and to evaluate them from an objective point of view.

The simulation results in following conclusions about network behaviour:

• Another comparative study between packet drop rate and transmission rate for the different scenarios shows that the performances of the observed networks differ and there is high fluctuation for Sybil attack.

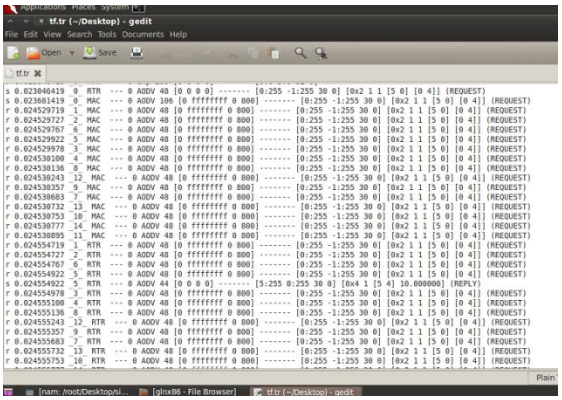

Fig.4.1: Trace file

• Third important feature of trace file is to study the average packets dropped for the node. We have implemented a module of our approach on the trace files which consist of well define Sybil attack, thus trace file is taken as input stream.The snapshot of trace file is given in Fig. 4.1

REFRENCES

[1]. S. Park, B. Aslam, C. Zou and D. Turgut, "Defense against Sybil Attack in Vehicular Ad hoc Network based on Roadside Units Support", Proceedings of Military Communications Conference(MILCOM'09), Boston, MA, USA, (2009)October 18-21.

[2]. K. Konate and A. Gaye, "A Proposal Mechanism Against the Attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in Routing Protocol of Mobile Ad Hoc", International Journal of Future Generation Communication and Networking, vol. 4, no. 2, (2011), pp. 69-80.

[3]. B. Xiao, Bo Yu and C Gao, "Detection and Localization of Sybil Nodes in VANETs," Proc. of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks, pp. 1-8, 2006

[4]. T. Zhou, R.R. Choudhury, P. Ning and K. Chakrabarty, "Privacy-Preserving Detection of Sybil Attacks in Vehicular Ad Hoc Networks," Proc. of International Conference on MobiQuitous 2007, pp. 1-8, 2007.

[5]. M. Raya, P. Papadimitratos, and JP. Hubaux,'Securing Vehicular Communications, IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, vol. 13, no. 5, pp. 8–15, 2006.

[6]. C. Piro, C. Shields, and B. N. Levine. Detecting the Sybil Attack in Mobile Ad hoc Networks.In Second International Conference on Security and Privacy in Communication Networks, 2006.

[7]. P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in ACM International Workshop on VehiculAr Inter-NETworking (VANET), October 2004.

[8] M. Raya and J.-P.Hubaux, "The security of vehicular ad hoc networks," in SASN, Nov 2005.

[9] Review Article- "Routing in Vehicular Networks: Feasibility,Modeling, and Security" IoannisBroustis and MichalisFaloutsos

[10] Department of Computer Science and Engineering, University of California -Riverside, Riverside, CA 92521, USA Correspondence should be addressed to BroustisIoannis, broustis@cs.ucr.eduReceived 11 July 2007; Accepted 19 March 2008

[11]. ByungKawn Lee, "A DTSA(Detection Technique Against A Sybil Attack) Protocol Using SKC(Session Key Based Certificate) On VANET", Electrical & Electronics Engg., Volume 3 , Issue 1; Spl. Issue of IC3T @ISSN: 2248-9584,2013.

[12] Vignesh.C, "Efficient Detection of Sybil Attack and DOS Attack in Mobile Ad-hoc Networks", International Journal of Computer Engineering & Science. ISSN: 22316590,2014.

[13].D. Balamahalakshmi and Mr. K.N. Vimal Shankar, "Sybil Attack Detection with Reduced Bandwidth Overhead in Urban Vehicular Networks", International Journal of Engineering Trends and Technology (IJETT) – Volume 12, 2014