ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

A Novel Approach to Detect Sybil Attack in VANET

D. P. Mishra[1], G. M. Asutkar[2]

Research Scholar, Department of Electronics Engineering, G. H. Raisoni College of Engineering, Nagpur, M.S., India [1]

Professor and Head, Dept. of Electronics & Communication, PIT, Nagpur, M.S, India[2]

ABSTRACT: Vehicular Ad-hoc Network (VANET) is vulnerable to many security threats including Sybil attack due to its open infrastructure. In this paper we have proposed a scheme to detect Sybil attacks using Digital Signature. The infrastructure needed includes vehicles, Road Side Units (RSUs) and Department of Motor Vehicle (DMV). In Sybil attack the malicious node, called Sybil attacker, illegally claim multiple identities which are called Sybil nodes. In this paper a Sybil attacker has been designed and a simulation environment on real world conditions has been implemented using OSM maps, SUMO mobility generator and NS2 network simulator. The detection using Digital Signature does not require any vehicle to disclose its identity. Thus this scheme also preserves the privacy of vehicles.

KEYWORDS: VANET, Sybil, SUMO, NS-2.

I. INTRODUCTION

VANET is a technology that employs moving vehicles as nodes in a network to create a mobile network to provide communication among vehicles, nearby fixed Road Side Units (RSUs) and Regional Trusted Authorities (RTAs). VANETs are used for broad range of safety applications and non-safety applications such as collision warning, road navigation, traffic information and mobile infotainment. In VANETs, user authentication is important security services for access control in both inter vehicle and vehicle to road side communication [1].

VANET enables vehicles plying on roads to communicate with each other and with fixed infrastructure. This can make roads secure and accidents can be avoided by use of VANET technology, which is still in research stage. VANET is attracting a lot of research interest and a hot topic of research. Vehicle speed, traffic density, continuously changing network topology is some of the challenges VANETs are facing. VANETs also face security threats because it uses distributed wireless communication channel. Most severe threat is in the form of Sybil attack, which can lead to many attacks. These attacks can lead to loss of human life. A network where there is no central authority is more susceptible to Sybil attack. In Sybil attack a malicious vehicle can acquire multiple identities and gives an illusion that there are more vehicles on roads than actually present. Malicious vehicle can cause a illusive traffic jam or can participate in a voting protocol rigging the results [2].

VANETs have following salient features:
(1)Node movements are restricted by road and speed limits.
(2)Frequent changes in network topology.
(3)Signals can be blocked by buildings.
(4)There is no power constraint with nodes.
VANET has numerous applications such as real time traffic information sharing (traffic jam). They face all traffic threats of wireless communication network. A Sybil attack can be easily launched if there is no central authority in network. Many attacks can be launched after getting illegal identities and fake positions in network such as providing bogus information and dropping packets. All these lead to degradation of QoS in VANET. A Sybil attacker can give the illusion of traffic jam or an accident, subsequently all other vehicles will change their route and attacker will get pass quickly. In VANET vehicles are able to sense their neighbouring traffic environment. Vehicle share their

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

information with other vehicles on road. Thus vehicles are able to get prior information about the events on their driving route. Thus they are able to react to events in advance. Sybil attack is the root cause of many security problems. Most of the VANET applications such as collision warning, route guidance and navigation and pre- crash sensing and warning need communication and cooperation among vehicles. If similar view is sensed by many vehicles, for some traffic situation, then it can be a reliable proof about certain traffic situation for other vehicles [3].

A Sybil attack can deteriorate the functionality of a network such as:

(1) Data Aggregation: A Sybil attacker can send more data to change outcome of data aggregation.

(2) Fair resources allocation: In general resources to be allocated equally to every node in a network, but due to presence of Sybil nodes a Sybil attacker is allocated more resources.

(3) Routing: Disjointed paths are established in multipath routing protocol. Sybil nodes on these paths can interfere with routing. Sybil attacker can appear in more than one place as Sybil nodes at same time. Hence geographic routing is most affected by Sybil attack.

(4) Voting: Sybil attacker can rig the voting process by voting many times using its Sybil identities, while honest nodes can vote only once. Legitimate and honest nodes can be eliminated from network if Sybil nodes participate in voting process to determine and eliminate misbehaving nodes.

Major challenge in VANET is that the receiving node must ensure the authenticity and trustworthiness of message source before reacting to it. Alert messages require authenticity, but not encryption [4].

In this paper we have proposed a system based on Digital signature. The system enhances security in VANET by detecting Sybil attack. Vehicles are assigned IDs. Detection is performed at two levels that is at Road Side Unit (RSU) level and at the level of central authority like Department of Motor Vehicle (DMV).

Rest of the paper is organized as follows: Section II describes related earlier research work on Sybil attack detection in VANETS. Section III material and methods used in our experimentation. Section IV deals with experimentation and results. Section V presents conclusions drawn.

II. RELATED WORK

Sybil attack was introduced by **Douceur [5] in 2002** for the peer to peer network. It can easily defeat the protocols and systems designed to prevent it and protect the system against it. A solution for detecting and defence against Sybil attack is having a central authority in the system. This authority makes sure that there is only one identity for each vehicle.

In the year, **2006, Bin Xiao et al [6]** had proposed a lightweight system for detecting and localizing Sybil attack. The approach is based on statistical analysis of distribution of signal strength of the vehicles. Each vehicle detects the potential Sybil vehicle by verifying the difference between their claimed and estimated position. Authors first proposed signal-strength-based position verification scheme, but it is not accurate. Position verification scheme is based on monitoring the signal strength of periodic beacons. Hence, there was a need for more accuracy. Authors proposed two statistical algorithms to increase the accuracy of position verification scheme. The algorithm detects potential Sybil nodes by observing distribution of signal strength over a period of time. Simulation results show that when number of witness is more than 5 and observation period is 10 units, a detection rate is greater than 95% was achieved with false positive rate less than 5%. All vehicles in the system play three type of roles namely claimer, witness and verifier. Each node plays all three roles at different time moments for different purposes. Complete detection process comprise of three phases:

Phase 1: Each node broadcast and receive beacon messages to/from neighbouring nodes and perform signal strength measurements. These measurements are saved in memory.

Phase 2: When nodes collect sufficient signal strength measurements from neighbours, they execute enhanced position verification algorithm on nodes.

Phase 3: If a node is detected as Sybil node in phase 2, then the node which has detected Sybil node executes classification algorithm on detected node and other neighbouring nodes. This is done in order to find all Sybil nodes originating from same malicious node. In this phase estimated position of malicious node is found out including its trajectory.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

In the year **2009, Soyoung Park et al [3]** proposed a time stamp series approach for defence against Sybil attack in VANETs. This approach uses Road Side Units (RSUs). RSUs are the only components issuing certificates to vehicles. It is very rare to find that two vehicles passing by various RSUs at precisely the same time. This is because of the difference of movement dynamics among vehicles. The approach uses digital certificates, but avoids using Vehicular Public Key Infrastructure (VPKI) for individual vehicles. The vehicles obtain certified time stamps, signed by RSU, whenever they pass by any RSU. A message sent out by a vehicle must contain a series (two or more) of latest time stamps certificates, showing when it crossed the last RSUs. The approach uses temporal and spatial correlation between vehicles and RSUs. When a vehicle receives message with identical time stamp series, a Sybil attack is suspected. No long term ID or certificate is used in traffic messages, thus vehicles privacy is protected.

In the year **2010, Jyoti Grover et al [7]** proposed a simple security system that uses the difference in movement patterns of Sybil and normal nodes. Each RSU calculates and stores parameter values such as received signal strength distance and angle of nearby vehicle when it receives beacon packet from it. If some vehicles have same value of parameters during the period of observation, then such vehicles can be classified as Sybil nodes. Simulation results show 99% accuracy.

RSU play important role in detecting Sybil attack and are assumed to be honest. Each vehicle broadcasts beacon packets containing vehicle ID (in encrypted form), time stamp and its position. In an average 3-10 packets are sent/second. Whenever a RSU receives beacon it calculates the distance and angle of vehicle. RSUs then calculate the difference between signal strength of received beacon with its estimated signal strength based on claimed position. If there is difference the vehicle is classified as suspected. In this way each RSU puts record of all vehicles passing across them. Observations of RSUs are collected by observer RSU and difference between motion trajectories is estimated. If some vehicles follow same trajectories, then they are classified as Sybil vehicles. All vehicles having same trajectories are placed in a group. In this way number of groups is equal to number of Sybil attacker. All Sybil nodes are discarded from network by central authority.

In the year **2011, Jyoti Grover et al [8]** proposed a distributed approach to defend against Sybil attack. The approach localizes the fake identities of malicious vehicles by analysing the consistent similarities in neighbourhood information. Each node periodically keeps record of its neighbours. It sends and receives beacon messages to announce its position and receive information about neighbours. If some nodes find that they have neighbours for particular interval of time then the same neighbours are identified as Sybil nodes. Thus in this approach Sybil nodes are quickly detected. The approach does not need any special hardware. Two vehicles cannot have exactly same set of neighbours for some specified long time interval. This is only possible in case of high vehicular density. The fake identities created by Sybil attacker are always bounded physically by Sybil attacker. They share the same set of neighbours at same instant of time. The proposed scheme does not use RSUs to perform detection. All vehicles take part in detection process by making group of neighbouring nodes at fixed interval of time. Analysis of groups is done instead of investigating each node independently. All nodes in communication range of sender receive beacon packets and form a group. All Sybil nodes originating from an attacker have same malicious node and same set of physical neighbours. However, communication neighbours of Sybil node may be different because they use different transmission power while sending packets.

Detection process is divided in four steps:

1. ***Periodic communication***: Each time a node broadcast beacon message, it attaches its neighbours list in it. Also beacon message contains identity of sender (in encrypted form), its position and time stamp.
2. **Group *formation***: When a node receives enough beacons, it makes record of neighbour nodes at regular interval of time.
3. ***Exchange of records***: The nodes exchange the record of neighbouring nodes with other nodes in their vicinity.
4. ***Identification of nodes having same neighbours***: Record of neighbouring vehicles is compared with other vehicles. If some nodes are observed simultaneously by other nodes for a time interval greater than some threshold value, then these nodes are put under Sybil group category. Thus all fake nodes originating from a Sybil attacker are detected.

In the year **2011,Yong Hao et al [9]** proposed a security protocol to detect Sybil attack using position based applications in privacy preserved VANET. Vehicles detect Sybil node cooperatively. They do so by examining the

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

rationality of vehicle position to their own neighbours. The detection is done by using the parameters of communication and vehicle's GPS position. The GPS position of vehicle is embedded in periodically broadcasted safety related messages. No extra hardware is needed but a little communication and computational overhead. Vehicles, in a cooperative way, detect and quarantine suspected Sybil nodes by analysing the correlation of their geographic information. While detecting Sybil nodes privacy of vehicles is protected. All communication parameters are embedded in safety related messages. Only small computational resources are required for detection. Simulation result shows that for higher security level longer time duration is needed.

There are three phases in protocol namely: probing, confirmation and quarantine. Once the vehicle is suspected, other vehicles start cooperative confirmation. When the number of vehicles confirming the suspected vehicle reaches a threshold value then the suspected vehicle will be quarantined.

In the same year **2011, Tong Zhou et al [10]** proposed a light-weight, scalable protocol "Privacy Preserving Detection of Abuses of Pseudonym (P2DAP)". In this protocol as soon as Sybil attack is detected the malicious vehicle is revoked. The detection is performed by a set of fixed nodes called Road-Side- Boxes (RSB). They simply passively overhear the communication in the network. Authors have presented simulation results for a realistic case to highlight overhead for central authority such as Department of Motor Vehicles (DMV), false alarm rate and detection latency. In P2DAP scheme, most of DMV's task is performed by RSB in order to reduce communication overhead of DMV. P2DAP also preserves privacy even if a RSB compromise with attacker. DMV is only involved when a suspected by RSB need to be confirmed as a Sybil node. It generates two level xxxx of pseudonyms which helps in saving storage memory of DMV. DMV can link a pseudonym to a vehicle by calculating its coarse-grained and fine-grained hash value and then comparing them with secure plate number. There is a need of maintaining a vehicle secure plate numbers and their pseudonym association (mapping).

In the year **2012, Parastoo Kafil et al [11]** modelled the Sybil attacker in VANET in various scenarios and traffic models. Traffic models used in their work include Highway, Uniform and Urban models. The attacker may be near to source or destination in each model or it can be out of route. It has been concluded that Sybil attacker near source of route is more dangerous because there are fewer hops between sender and receiver of a packet. Here the attack can be deeper with more packet loss. Sybil attacker in Highway model is more successful than in Urban model. This is because in highway model movement of vehicle is more predictable. In Urban model attacker is not aware of movement and is also hard to know about routing algorithm.

In the year **2013, Bayrem TRIKI et al [12]** proposed a solution to prevent and detect Sybil attack based on RFID tags which are embedded in vehicle. These RFID tags authenticate vehicle to RSUs. They obtain short life time certificates from RSU. These certificates are used to authenticate vehicles by other vehicles present in network as neighbours. The network is divided in different zones. These zones are managed by different certification authorities. When a vehicle moves from one zone to another it has to get new certificate from the first RSU it comes across in its route. The proposed solution also prevents the vehicle from the attacker tracking the mobility of vehicles. One of the RSUs is selected as a controller of that zone and called as Road Side Controller (RSC). The solution detects Sybil attacks occurring in and out of the coverage range of RSUs because observer components are deployed in vehicles. RFID tags in vehicles contain Vehicle Identification Number (VIN). RSUs and RSCs authenticate the moving vehicles when they go across them. RSUs and RSCs prevent unauthorized vehicles from getting certificates. The privacy is preserved because VIN contained in RFID tag is never transmitted in network.

The vehicle cannot be tracked as they change their certificates as they move from one zone to another. The vehicles request the new certificate from the first encountered RSU in newly entered zone. The detection mechanism is distributed among RSUs and in-vehicle observers. This reduces the overhead on RSU and allows detection beyond RSUs coverage range. Detection is instantaneous and fast. Traffic simulator (SUMO) is used with NS-2to generate mobility traces of vehicles and simulate communication respectively. MOVE tool is used to convert SUMO traffic traces in to NS-2 compatible traces.

In the year **2013, Kenza Mekliche et al [13]** proposed a privacy preserving approach to detect Sybil attack. They have used RSUs and DMV in their approach. LP2DSA algorithm proposed in the paper is an improvement to C-P2DAP. The scheme is an infrastructure based scheme. Vehicles are assigned a pool of pseudonyms which are hashed to a common value. Detection is performed in two-level manner. First level of detection is done by RSUs. They overhear the vehicular communication and find out the position of each vehicle with the help of adjacent RSUs. These

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

positions are used when suspicious vehicles, having same coarse grained hash, are found. RSUs compute the degree of distinguishability between them. If the degree of distinguishability is higher than a threshold value, then the corresponding RSU report the suspicious vehicles to DMV. At second level of detection, DMV computes the fine grained hash of suspicious vehicles to separate them between real attacker and false positive. Thus load on DMV is reduced. The detection scheme does not mandate any vehicle to disclose its identity. Thus privacy of vehicles is preserved.

In the year **2014, P. Vinoth Kumar et al [14]** proposed Priority Batch Verification Algorithm. It classifies requests obtained from multiple vehicles, at RSU level. The scheme provides immediate response to emergency vehicles like police, ambulance or fire service. In the proposed model of Sybil attack prevention, the algorithm puts restrictions on providing multiple time stamps to the particular vehicle within short time duration. The RSU set the timer ON when it provides time stamp to a particular vehicle for first time. If the vehicle, before expiry of set time, once again sends request for time stamp, then there is a suspicion that the vehicle may be an attacker. In such conditions RSUs deny the request for time stamp and subsequently track the vehicle to find out whether the vehicle is an attacker or a legitimate one.

The proposed Priority Batch Verification Algorithm (PBVA) is installed in each RSU. When RSU receives simultaneous requests from vehicles, PBVA starts searching simultaneous requests if they are from emergency vehicles. RSUs classify vehicles using identifier found in received requests. In VANET each vehicle is given its type identifier. Only RSU can identify whether a vehicle is an emergency vehicle or a general one.

In the same year **2014, Dongxu Jin et al [4]** proposed a novel scheme, ”Traffic Flow Aided Sybil node Detection Mechanism (PMSD)” to detect Sybil nodes. The scheme uses physical measurements of beacon messages. These measurements are not modifiable. It is an infrastructure less scheme and hence easy to implement. This scheme reduces overheads for detection. Safe guard distance is introduced to increase detection rate. Detection rate is 97% with only about 2% error rate. Time Difference of Arrival (TDoA) technique is used to locate source of message. If the location is different from claimed location included in beacon message, then the node will be judged as Sybil node.

In the same year **2014, Thago M. de SALES et al [15]** proposed a protocol for privacy- preserving authentication and Sybil attack detection in VANET. The protocol uses multilevel K-anonymity architecture, with group signature and pseudonyms. The proposed protocol is divided in to three phases: (1) Registration phase; (2) Temporary identity (pseudonym) assignment phase and (3) Sybil detection phase. According to properties of multilevel anonymity sets, it is impossible for two different vehicles to announce the same event with the same anonymity set digital certificates.

In the year **2015, Jie Li et al [1]** proposed ACPN a novel authentication frameworkwith conditional privacy-preservation and non-repudiation for VANET. This approach uses Identity Based Signature (IBS) schemes based on ID-Based Cryptography (IBC) for authentication. Pseudonym based scheme for privacy preservation is used which uses Public Key Cryptography (PKC) based scheme for pseudonym generation.
IBS is used for authentication between vehicles and RSU. IBOOS (ID-based on-line/off-line signature) for authentication among vehicles. Important property of ACPN is its reusability. It can be utilized with other new schemes for security and performance improvements. Typical performance evaluation has been conducted using IBS and IBOOS schemes [1].

III. MATERIALS AND METHODS

A. SIMULATION OF URBAN MOBILITY:

SUMO software has been chosen by the authors to simulate the scenarios in which the vehicles ply on the roadways. This is open source software [16]. It is a macroscopic as well as microscopic continuous TS developed by Institute of Transportation System at the German Aerospace Centre. It can operate at the level of each vehicle. Each vehicle with explicit definition has unique path and identification. Vehicle movements can be described by Origin Destination Matrix (O/D Matrix). Trip file can be generated from O/D Matrix using od 2 trips. For simulation to run SUMO needs network files and road network. Network file define the road map on which the vehicle travels.

(a) Importing maps: One can manually generate network file by writing route. But these networks are very basic. It is very difficult to create complex network manually. Some basic networks are Grid Network and Spider Network. But for realistic simulation one has to create network file which represent conditions of real world. SUMO incorporates

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

facility for this purpose. It can handle large simulation maps imported from reality. Initially, SUMO is given with a list of intersections, road segments, traffic control lights, routes and vehicles. One can download real world roadmap from [17]. These downloaded maps are OSM files. OSM file can be edited using Jawa Open Street Map (JOSM) editor. In this step all undesired routes can be removed to simplify the network file.

(b) Generation of Network file: After editing OSM file, it can be converted into net.xml file using net convert command line application available in SUMO. Input is .osm file and output is net.xml.

(c) Edge: It defines the connection between starting point to destination point. Parameters of Edge are as follows: (i) Id – Gives unique Id to each edge (ii) From – Id of node where edge begins. (iii) To – Id of the node where edge ends. Edge has lanes. Lane parameters are as follows: (i) Id – Unique Id for a lane. (ii) Index – Define sides of lanes e.g. 0 for right most (iii) Speed – Maximum speed at which vehicles can travel on it. (iv) Shape - Set of coordinates for centre line of lane.

(d) Trip File: Creation of Trip file is followed by creation of route on which vehicle travels. This is done in two steps: (i) Creation of trip file. (ii) Creation of route file. Trip file contains the parameters like route Id, departure Id of vehicles, starting lane and ending lane. Creation of trip file is a difficult task. Therefore, SUMO provides Python script called random trips. Using this facility one can create random link between two nodes. Route file contains information about the route, which a vehicle would traverse through. It contains Edge IDs encountered in travel. One can write route files but for large network with high density of vehicles, it is not possible to make route files manually. With trip file and network file as input one can generate route file using duarouter.exe application. Duarouter is part of SUMO suite. SUMO's TraCI protocol is required to integrate (couple) with it during concurrent simulation in NS-2. TraCI allows the control of vehicles, road, intersections and traffic lights.

B. NS2:

It is one of the most popular open source simulator. NS2 is a discrete event and object oriented network simulator. It was developed at the University of California- Berkley in 1989. It uses two languages. Core modules such as protocols and channels or agents are written and implemented in C++. Simulation models are developed in Tool command language (Tcl). Users write script containing commands for setting up network topology, wireless parameters and recording statistics. Some mobility simulators can generate vehicular trace files suitable for NS2. NS2 generates event trace output file and an animation trace file. NS2's Network Animation Utility uses animation trace file to produce visualization of simulation. NS2 can be used for wired and as well as wireless networks routing protocols and IEEE 802.111 MAC layer can be implemented in NS2. The NS2 is widely used for research on vehicular network, but does not work well for big topologies (more than 300 nodes). It requires large memory per simulation. It cannot be extended, because it does not support hierarchical models [18].

Since its inception, NS2 has gained tremendous interest from industry and academia. NS2 contains modules for network components such as routing, transport layer protocol, applications etc. to investigate network performance one can use scripting language Tcl to configure a network and then observe the results generated by NS2. An event driven simulator is started and run by a set of events. A list of events is maintained and updated throughout the simulation. The simulation has to sequence through this list and execute one event after the other until either list is empty or stopping condition is reached. In an event driven simulator, all events in an entire simulation cannot be created at initialization step. As the simulation advances one event may generate one or more events. The new events are inserted in the list of events.

As shown in figure 1 the architecture of NS2 provides executable command ns. This command takes on arguments as name of the Tcl scripting file. Output generated by NS2 is a trace file which can be used to plot graph and create animation.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

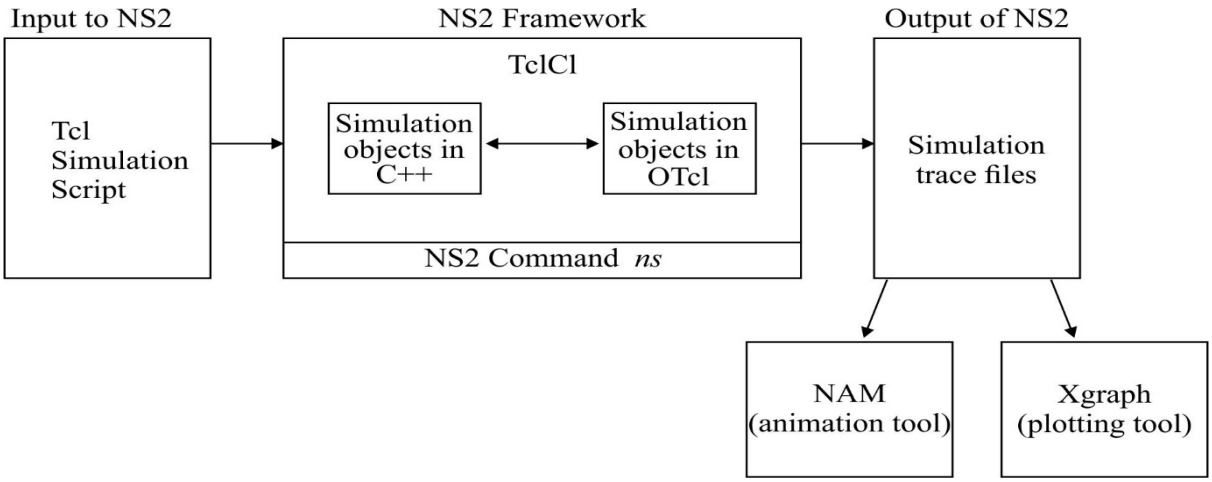

Figure1: Architecture of NS2

NS2 is based on two language i.e. C++ and Object oriented Tool Command Language (OTcl).C++ defines internal mechanism of simulation objects (at backend). OTcl is used to set up simulations by assembling and configuring objects and scheduling the events (at frontend). C++ and OTcl are linked by TclCL. Variables in OTcl domain are referred as handles which are mapped to C++ objects. A handle is just a string in OTcl domain and does not contain any functionality. Functionality is defined in mapped C++ object (such as class connector). Handle acts at frontend with users and OTcl objects. It may define its own procedures and variables for interaction. Member procedures and variables in OTcl arena are called instance procedure (instprocs) and instance variables (instvar) respectively. NS2 provides large number of built-in C++ objects. One can use these objects to set up simulation using Tcl simulation script.

After running simulation NS2 generates a text-based or animation based outputs. To interpret these outputs graphically or using animation, the utilities like network animator (NAM) or XGraph are used.

NS2 runs on various platforms such as UNIX, Windows and Mac systems. NS2 has smoothest ride in UNIX. Cygwin (UNIX emulator) is activated in Windows systems. NS2 source codes are divided in two forms: all-in-one suite component wise. With all-in-one package users get all components along with some special components. The package provides an "install" script, which configure NS2 environment and create NS2 executable file using the 'make utility.

After installation an executable file **ns** is created in NS2 home directory. NS2 can be invoked by executing the following statement from shell environment.

>> ns [<file>] [<args>]

While <file> and <args> are optional arguments. If no argument is given the command **ns** will invoke NS2 environment. Then NS2 waits to receive the commands from keyboard line-by-line. If first input argument <file> is given, NS2 interprets the input script file. To run a simulation one requires defining a network scenario in a Tcl script file. Then this Tcl script with .tcl extension is given as input to **ns** executable file. After simulation the packet flow information can be obtained through text-based tracing or NAM tracing. An AWK program or a Perl program can be used to analyse a text-based trace file. NAM program utilizes NAM trace file to replay network simulation using animation.

Defining simulation of a scenario in NS2 is done in three steps:

1 Simulation Design

In this step all planning has to be made. User should define the purposes and objectives of the simulation. How is the network to be configured? What are the assumptions? What are the parameters to be measured? Which type of results is expected?

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

2. **Configure and run simulation**
In this step the designed simulation is implemented. In configuration phase chosen components are created and configured. Events in simulation are scheduled at certain instant of time. In second phase the user get the simulation run in configured network. Sequenced events are executed in chronological order. The simulation runs until all events in the list are executed. The simulation scenario is described in Tcl script file. This file is given as input argument while executing " >>ns<file> " command.

3. **Debugging and Packet tracing.**
In this step, the first task is to debug the problems encountered while preparing the Tcl script file. In second step collection and compilation of result is done. Packet tracing process records the details of packet flow during simulation. There are two types of packet tracing. (1) Text-based (2) NAM packet tracing.
Text-based packet tracing make record of details of packets passing through network components. The general format of each trace line is show below in figure 2 which consist of 12 columns.

1	2	3	4	5	6
Type Identification	Time	Source Node	Destination Node	Packet Name	Packet Size
7	8	9	10	11	12
Flags	Flow ID	Source Address	Destination Addr.	Sequence Number	Packet Unique ID

Figure 2: General format of trace line.

The type identifier field has four possible event type that a packet has experienced: r (received), + (enqueued), - (dequeued) and d (dropped). Time field shows at which time the event occurred. Remaining fields are self-explanatory. Having only trace file in meaningless. An analysis is to be performed on these data. One has to extract a subset of data of interest and further analyse it. The languages used for the purpose of analysis are AWK and Perl.
Network **A**ni**M**ation (**NAM)** Trace
NAM trace is the record of simulation details in text file. After obtaining a NAM trace file the animation can be initiated at command prompt by using following command.
>> nam file name. nam
Various visualisation features are available in NAM. They include animating coloured packet flow, dragging and dropping nodes, labelling of nodes, colouring of links etc.
Many times, while developing an NS2 simulation it is necessary to create special C++ modules. Whenever a change is made to one file, it is required to recompile other files that depend on it. Manual recompilation of each such file is not practical. The 'make' utility tool automatically keep track of all files created throughout development process wherever inter dependency exists. The 'make' utility is a simple tool to include a newly developed module in NS2. After developing C++ code, one simply add an object file name into the dependency and re-run make. After running 'make' an executable file **ns** is created. Then this **ns** file is used to run simulation [19].

C.DIGITAL SIGNATURE:
Paper documents are authenticated by putting signatures. Nowadays there is wide use of electronic documents. For electronic documents a similar system of authentication is needed. Digital signatures are widely used for this purpose. Digital signature is a string of zeroes and ones generated by digital signature algorithm. The digital signature serves the purpose of validation and authentication of electric document. Validation means certifying the contents of document,

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

while authentication means certifying the sender of document or message. Digital signature has the following characteristics:
(1) Signature is a bit pattern that is determined for a message (thus for different messages from the same sender, digital signature will be different).
(2) Signature must have some information that is unique for sender. Thus forgery and denial can be prevented.
(3) Signature should be easily produced.
(4) The process of recognition and verification of authenticity of digital signature should be easy.
(5) It should not be feasible to forge a digital signature.
(6) It should be practically possible to get copies of digital signatures so that they can be stored to make future arbitration possible in case of later disputes.
Several authentication techniques have been developed to verify that the received message is sent from claimed sender. Digital signature is computed based on the message and some private information held only by sender. A hash function is applied to message to get the message digest. The message can be of any arbitrary length but message digest is of fixed size. MD5 (message digest 5) and SHA (secure hash algorithm) are commonly used hash functions. Symmetric key cryptosystem and public key cryptosystem are used in digital signature computation. In symmetric key cryptosystem a common key is known only to sender and receiver. When the number of user pair increases it becomes extremely difficult to generate, distribute and keep track of keys. In case of public-key cryptosystem a pair of keys is used. A private key is only known to its owner (assume A) and a corresponding public key is known to everyone else in the system who want to communicate. A message to be sent to owner (A) is encrypted by with owner's (A) public key. This message can only be decrypted by the owner who has the corresponding private key. No other person can decrypt the message because they do not have the private key corresponding to the public key used for encryption. For authentication, the message is encrypted with the private key of sender this message can be decrypted by anyone using public key of sender. If message is decrypted by the public key of sender (A). Now it is clear that the message was only encrypted by the private key of sender (A) and authenticates that only (A) has sent it.

Creation and verification of digital signature

A simple method for creation and verification of digital signature is depicted in figure 3 and figure 4respectively. A hash function is applied on message and corresponding fixed size message digest is generated. On this message digest the signature function of the private key of sender is applied and thus a digital signature is generated. The message and digital signature is sent to receiver. The message can be decrypted by anyone. The digital signature ensures the authenticity of sender. At receiver end the inverse signature function (public of sender) is applied on digital signature to generate message digest. On received message the same hash function is applied, which was applied on message at sender's end. Resulting message digest is compared with the corresponding one recovered from digital signature. If the two digest match then it is ensured that the message has been only sent by claimed sender, and the message has not been altered during transmission [20].An ITS requires authentication and integrity among vehicles. Vehicle IDs are issued by Central Authority such as RTO or DMV. Hence, IDs are generated by central authority. For implementing an ITS system AODV Protocol has been used for communication.

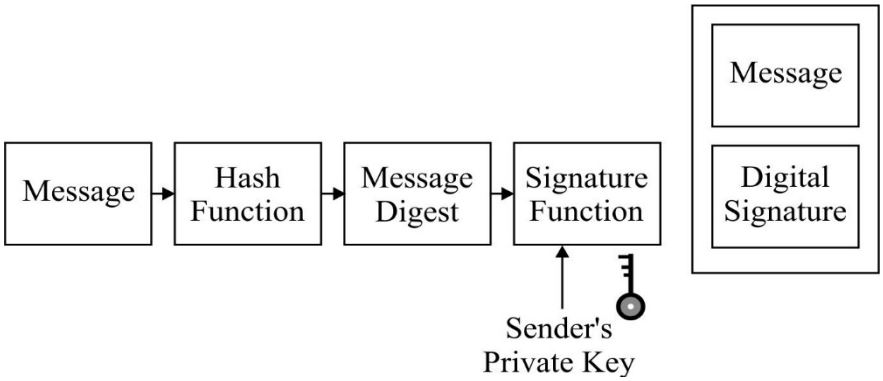

Figure 3: Generation of digital signature at sender's end.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

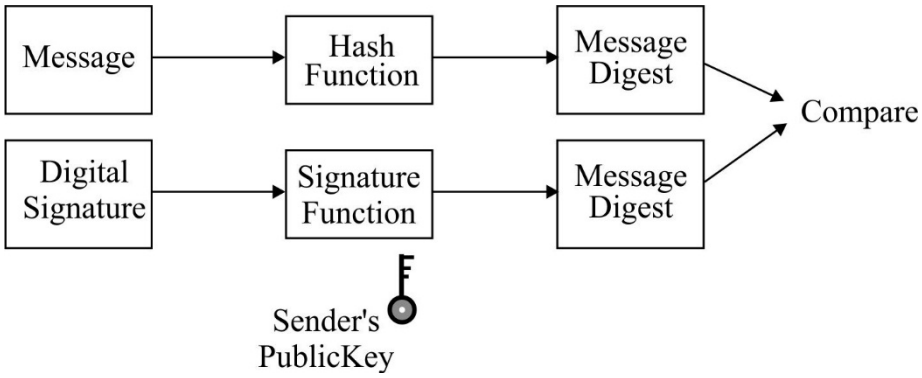

Figure 4: Verification at receiver end.

The modification of AODV file for inclusion of digital signature and corresponding hash function developed for the purpose. The AODV.CC file and AODV.H file modification and corresponding screenshots are shown in figure 5 and Figure 6 below.

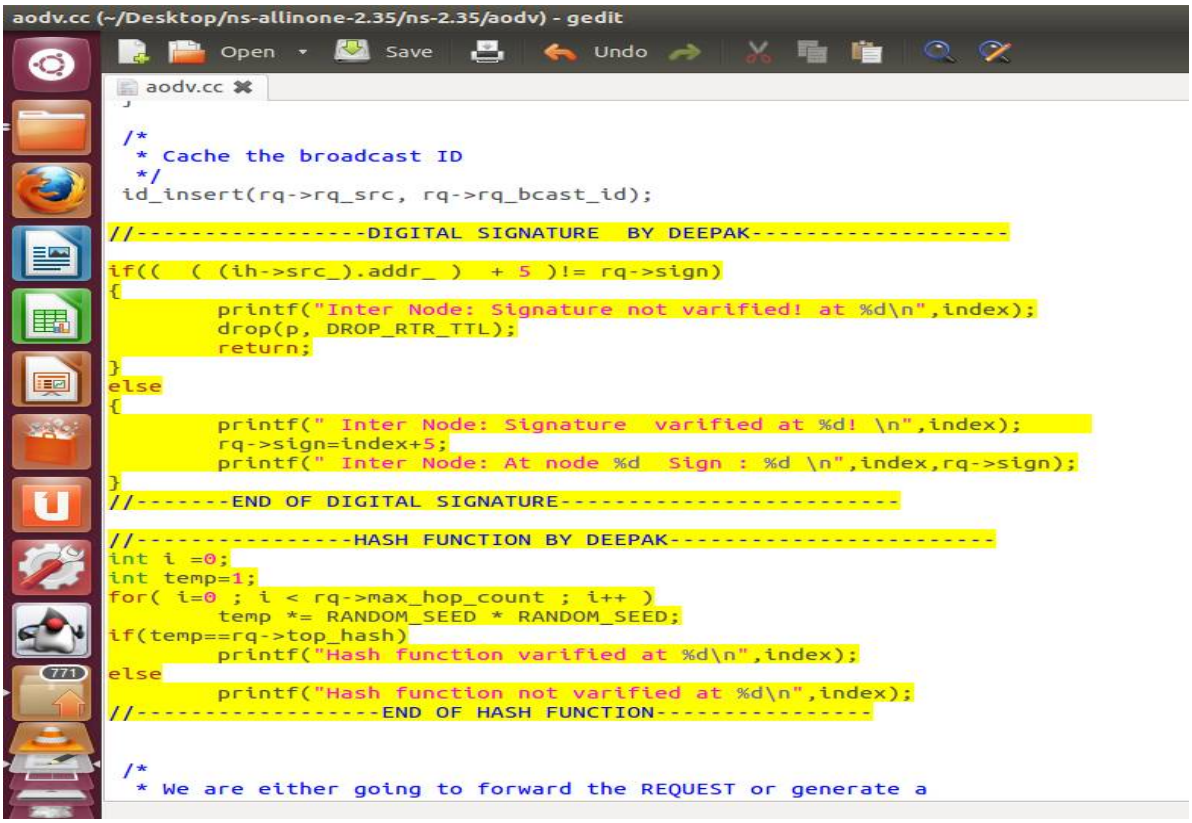

Figure 5: Screenshot of modification in AODV.CC file.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

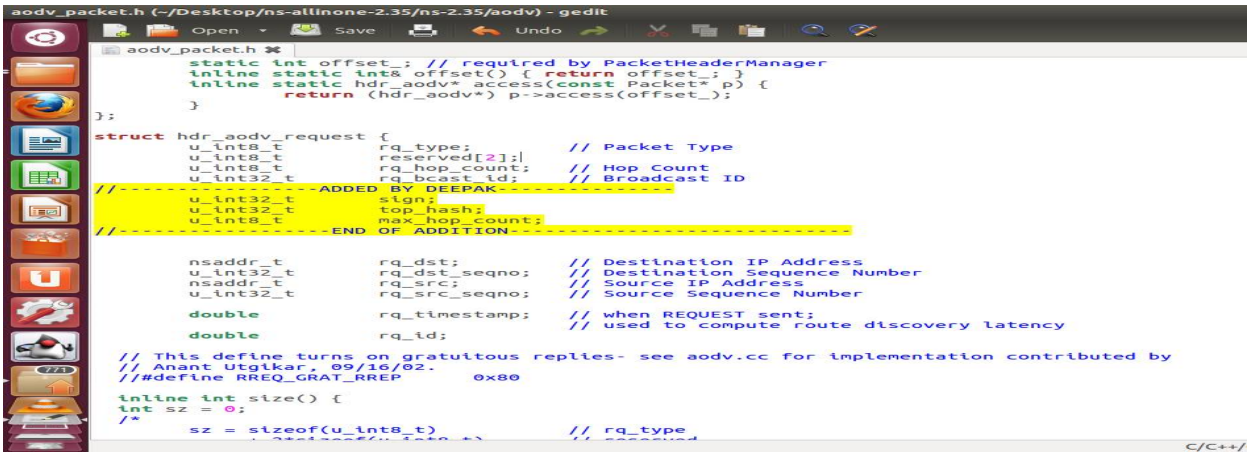

Figure 6: Screenshot for modification in AODV.H file

This simulation environment is similar to real world traffic conditions. The performance of AODV protocol under Sybil attack has been evaluated. In presented simulation Digital Signatures are used for verification of vehicle IDs so that only honest vehicles could participate in communication and Sybil nodes can be detected and revoked from communication process. The output screenshot showing the list of verified and non-verified nodes is depicted in figure 7.

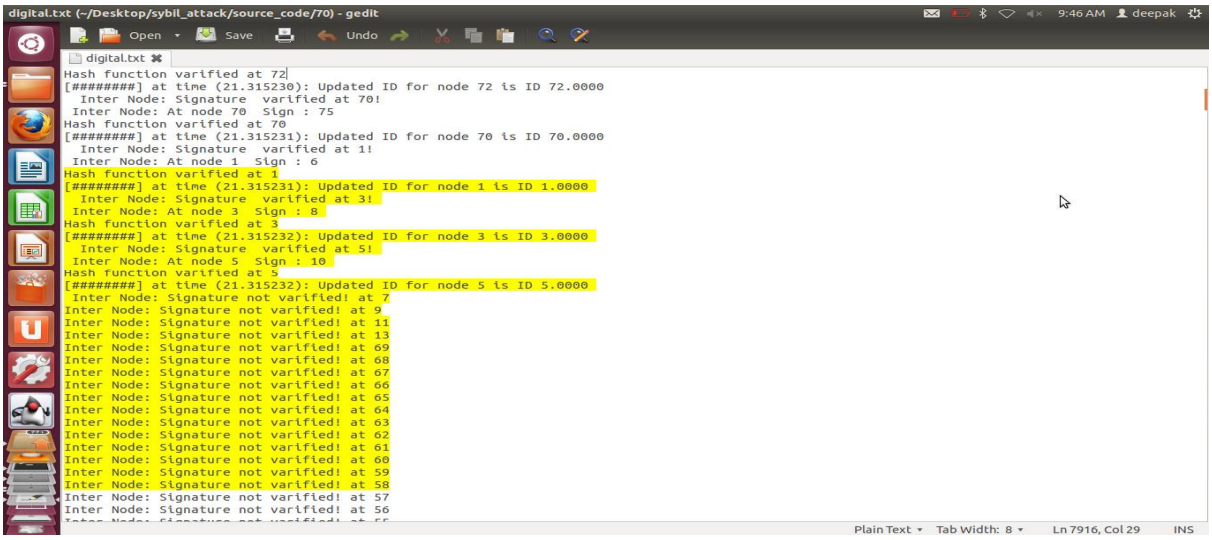

Figure 7: Screenshot for Verified and non-verified Signatures of node.

IV. SIMULATION & EXPERIMENTATION

A. SOFTWARE INSTALLATION:

For the purpose of simulation and experimentation following platforms/simulators need to correctly install sequentially given in Table 1.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

Table 1: Simulation software and versions

Sr. No	Software	Platform/ Version
1	Linux	Ubuntu 12.04
2	SUMO	Version0.21.0
3	NS-2	Version 2.35

B.EXPERIMENTATION:

A comprehensive experimentation has been performed to evaluate the detection of Sybil nodes in an environment which uses AODV protocol. At the start of experimentation, a Sybil attacker has been designed to be included in simulation. The experimentation has been divided in two phases. In phase1 a Sybil attacker is designed and its performance has been evaluated. In phase2 an environment on Nagpur-Mumbai highway has been implemented to evaluate the performance of Sybil detection scheme using digital signature.

Phase1.

Following algorithm shown in figure 8 is implemented in NS-2 to generate Sybil attacker.

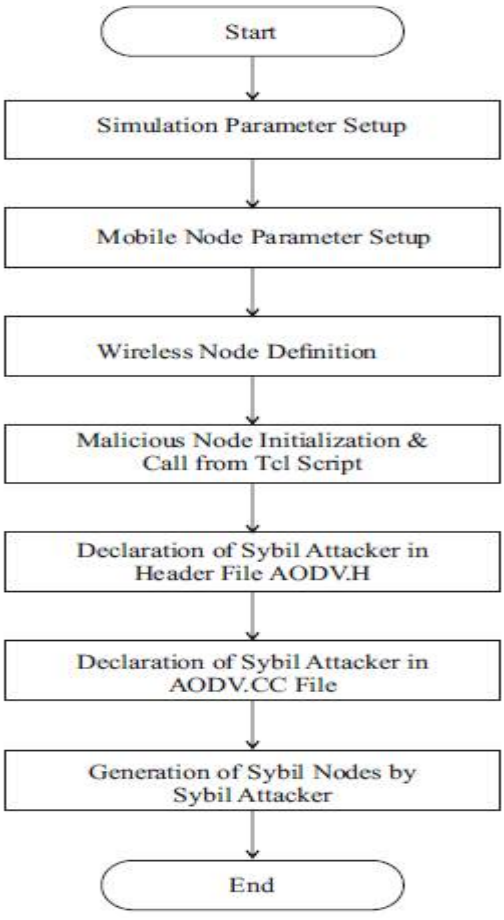

Figure 8: Algorithm for Design of Sybil Attacker

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

(1) Simulation Parameters Setup: Screenshot for simulation Parameter Setup is shown in figure 9.

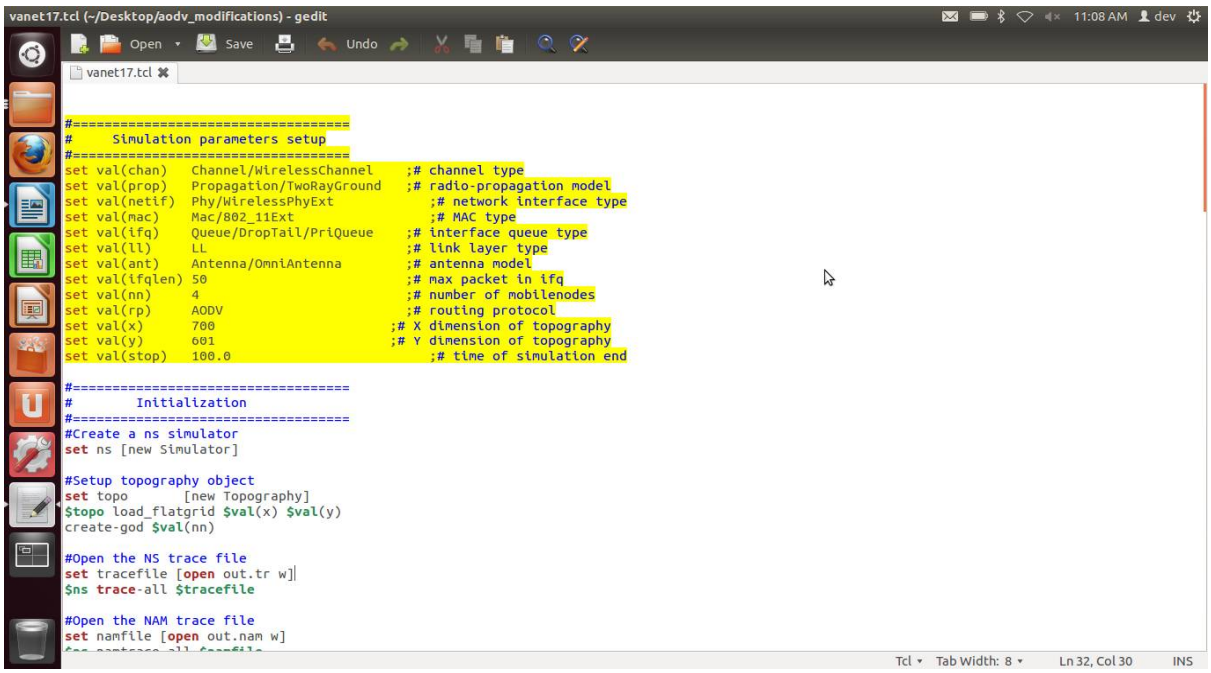

Figure 9: Screenshot for simulation parameter setup

(2) Mobile node parameter setup: Screenshot for mobile node parameter setup is shown in figure 10.

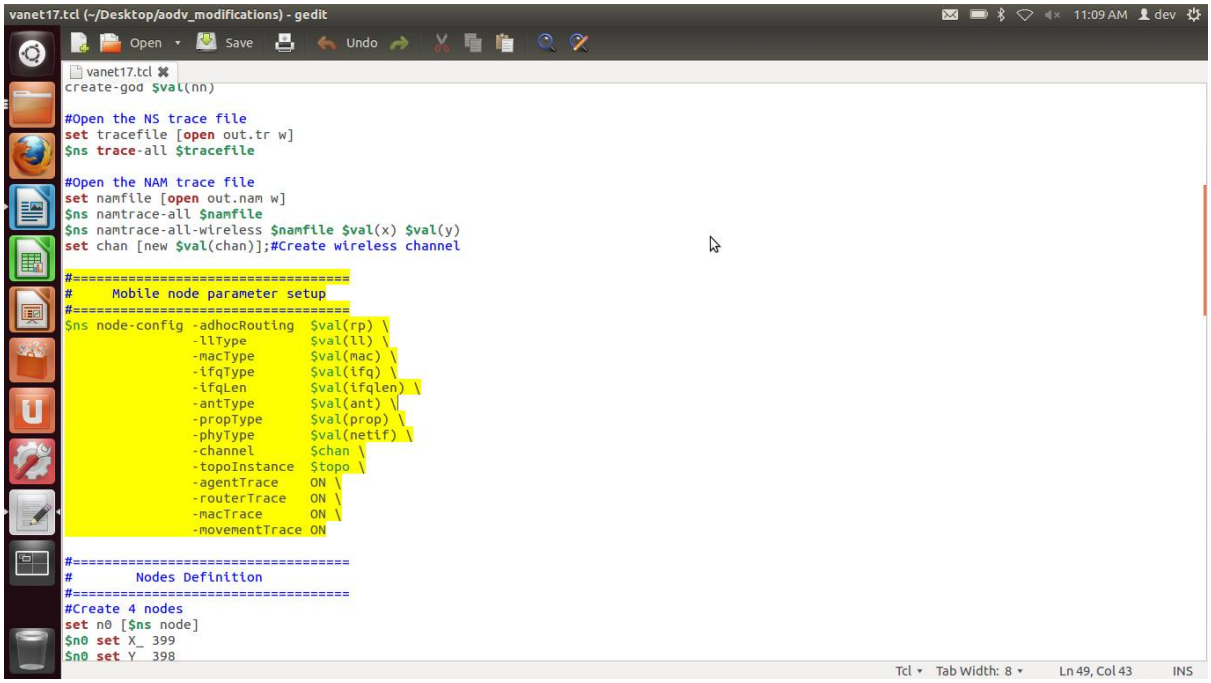

Figure 10: Screenshot for mobile node parameter setup.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

(3) Wireless node definition: Screenshot for wireless node definition is shown in figure 11.

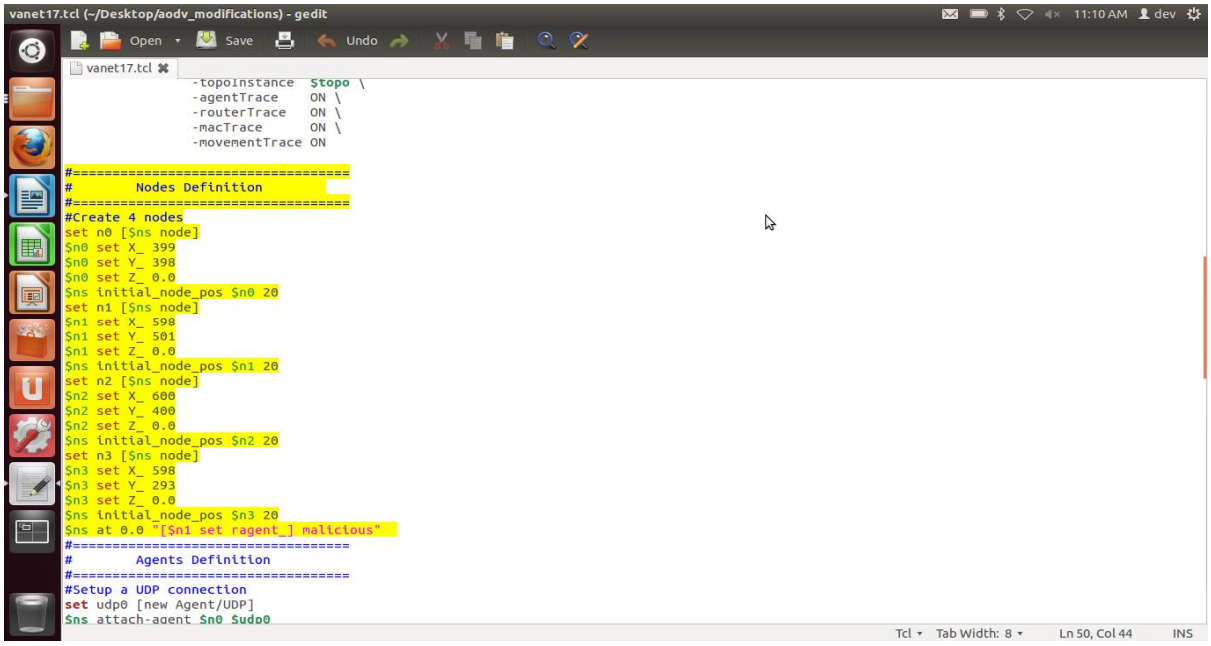

Figure11: Screenshot for wireless node definition

(4) Malicious attacker initialization/ calling from TCL script: The screenshot for initializing malicious attacker which is done from TCL script is shown in figure 12.

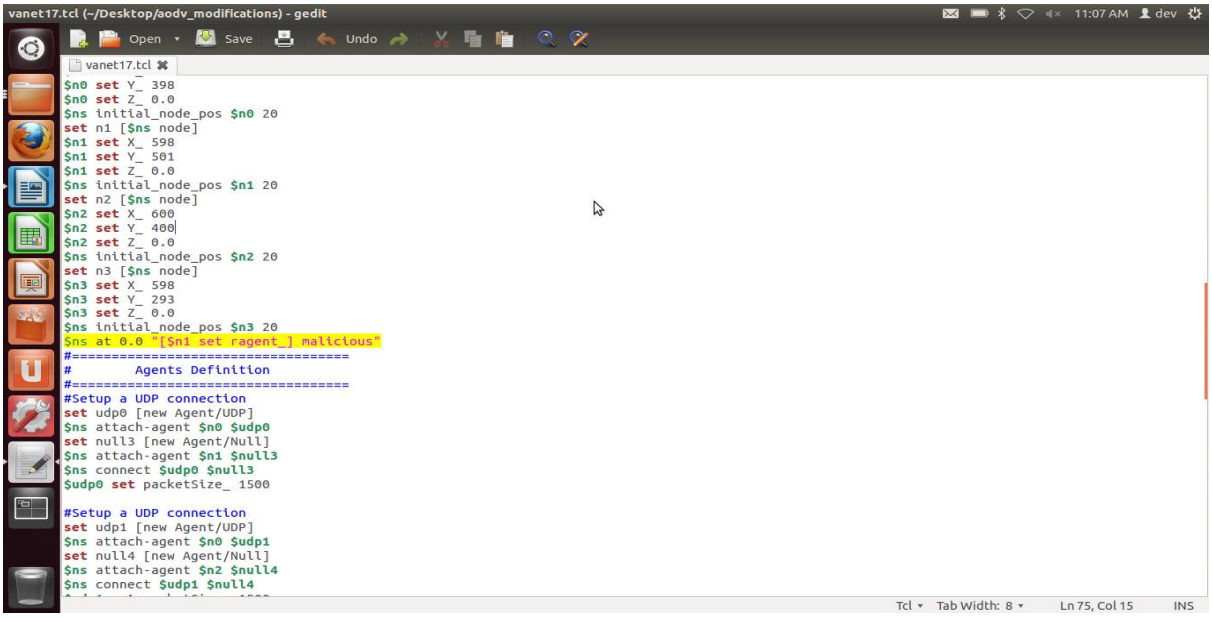

Figure 12: Screenshot for initializing malicious attacker.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

(5) Declaration of attacker in header file aodv.h: Declaration of attacker is also to be made in aodv.h file. The screenshot for the same is shown in figure 13.

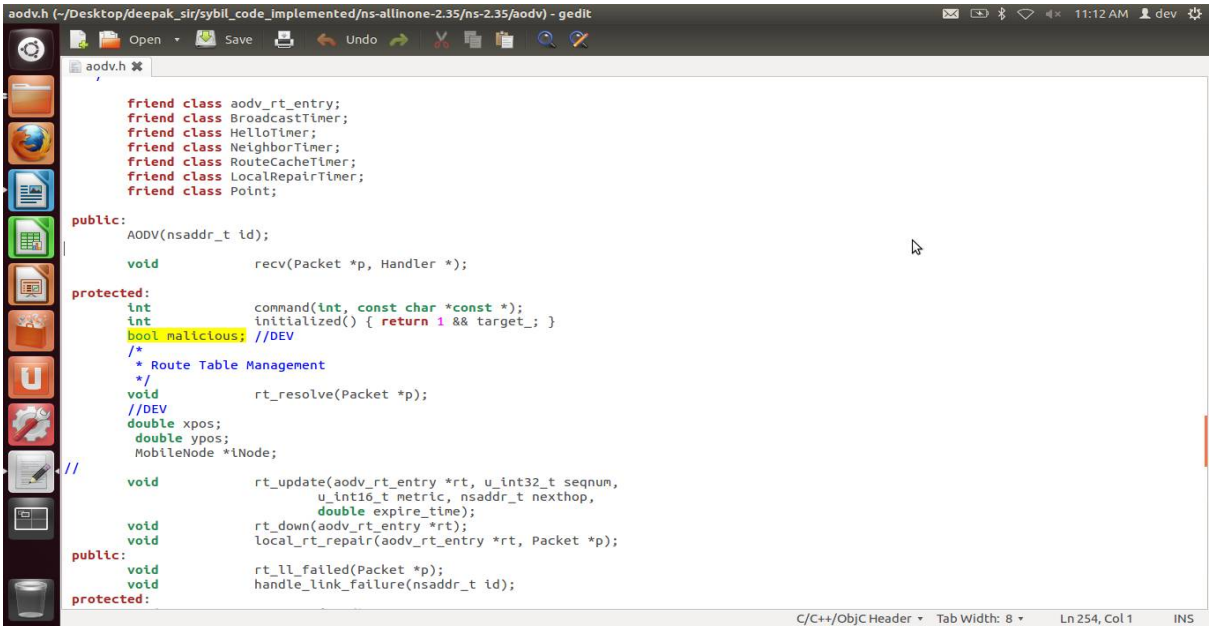

Figure 13: Screenshot for declaration of attacker in aodv.h header file.

(6) Definition of attacker in aodv.cc file: The definition of attacker in aodv.cc file is shown in the screenshot depicted in figure 14.

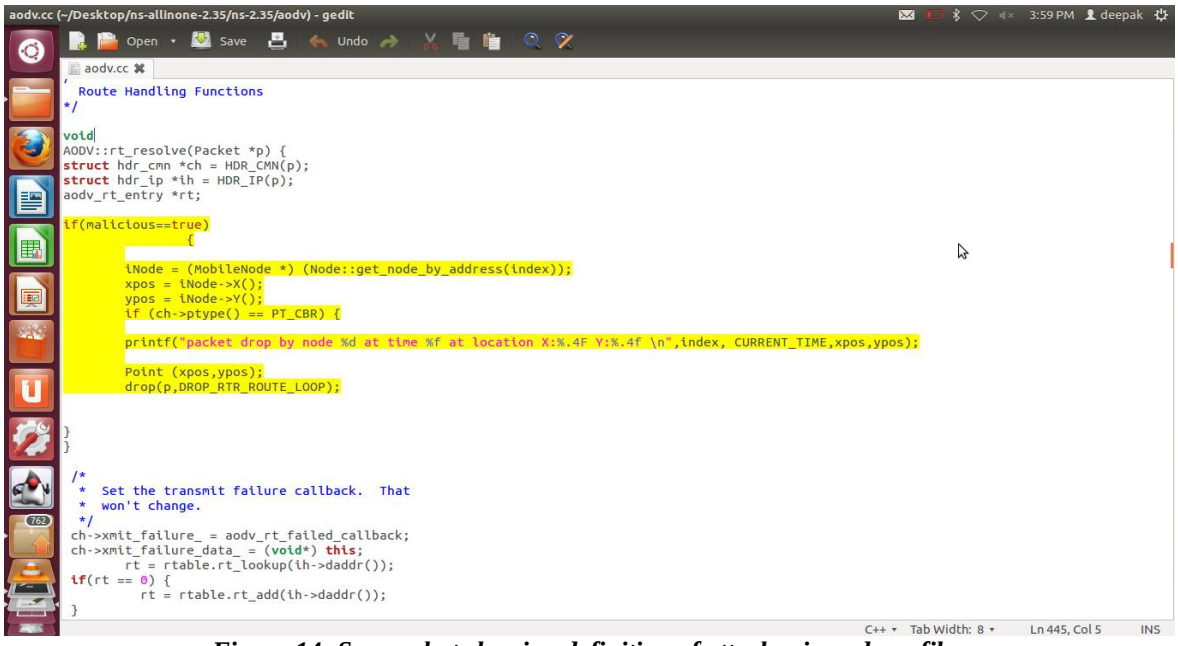

Figure 14: Screenshot showing definition of attacker in aodv.cc file.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

(7) Generation of Sybil identities (nodes): Screenshot for generation of Sybil identities is shown in figure 15.

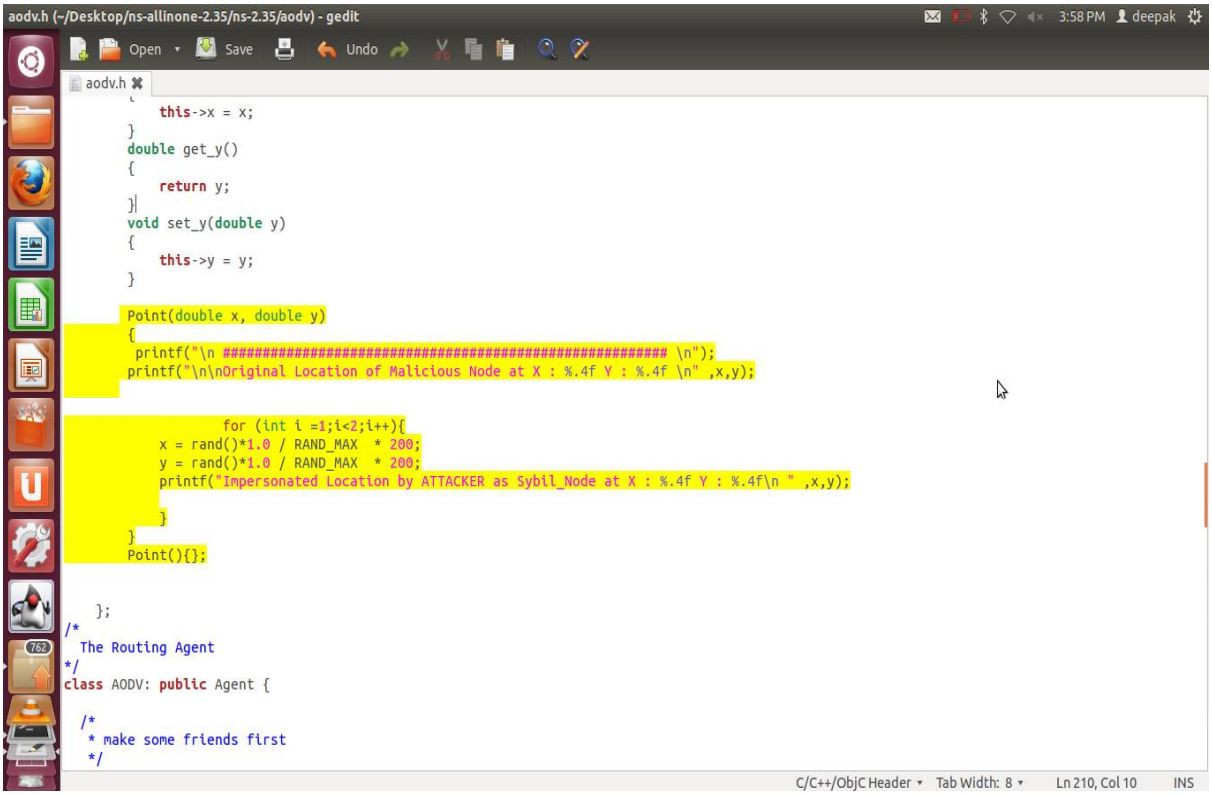

Figure 15: Screenshot for generation of Sybil identities.

With NO Attack in the network, only one packet loss was observed while with Sybil Attack in network most of the packets were lost (117/167).

Phase2.

In phase2 of the experiment Open Street Map(OSM) and SUMO (Simulation of Urban Mobility) have been used to create realistic mobility model and NS-2.35 is used for analysis of sybil attack in VANET scenario of Nagpur-Mumbai Highway.

For Simulation has been developed in three steps:

I. Extraction of Nagpur-Mumbai Highway Map from OSM.

II. Extracted MAP is used as input to SUMO simulator for visualization.

III. SUMO generated mobility and Traffic files and the same are used as input to NS-2 for Sybil attack performance analysis.

Observation parameters:

1. Detection rate = Number of true positive detected by RSU/Number of attack
2. False Positive rate = Number of false positive reported to DMV/Total number of messages analysed by RSUs
3. DMV load = (False Positives + True Positives) / Total number of incidences reported to DMV

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

V. OBSERVATION & RESULT

Following figures show our observations:
Figure 16 shows the relationship between percentage Detection Rate on Y-axis and number of vehicles and number of attackers in network on X-axis. Five observations have been recorded. Figure 16 shows the relationship between DMV load in percentage on Y-axis and number of vehicles and number of attacker on X-axis. Five observation points have been recorded in this figure.
Figure 17 shows the relationship between DMV Load in percentage on Y-axis and number of vehicles and number of attackers on X-axis. This figure also records five observations.
Figure 18 shows the relationship between False Positive Rate in percentage on Y-axis and number of vehicles and number of attackers on X-axis. This figure also records five observations.

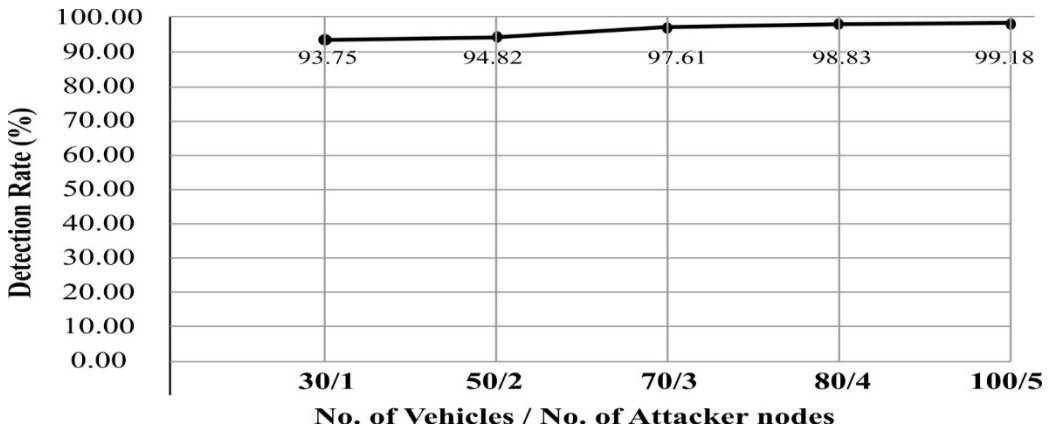

Figure 16: Relationship between percentage detection rate and number of vehicles and attacker.

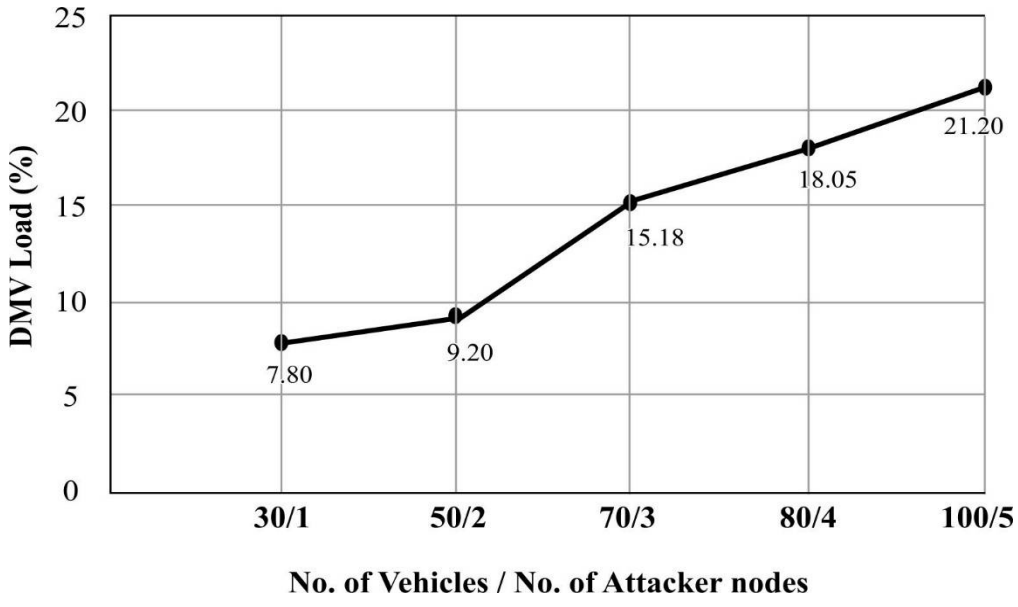

Figure 17: Relationship between DMV load and number of vehicles and attacker.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

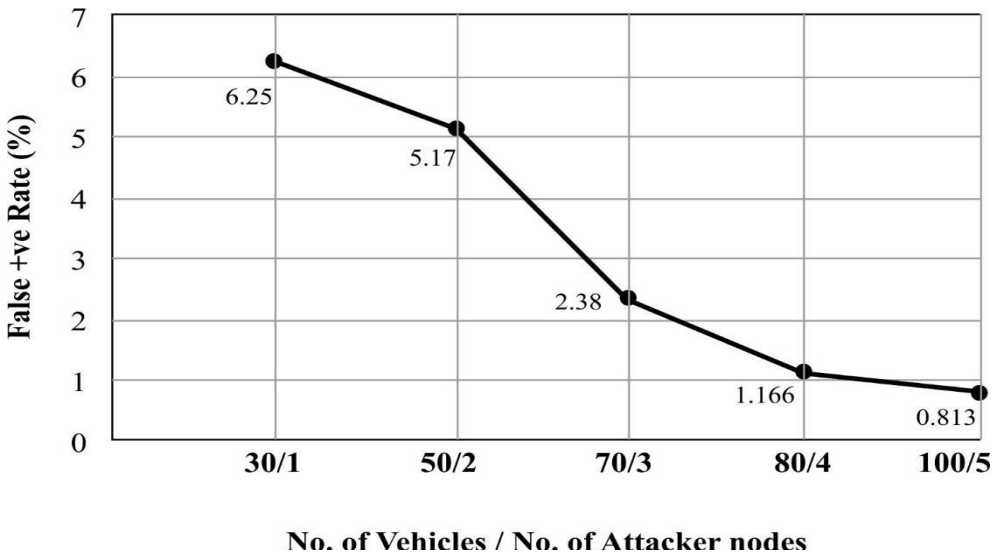

Figure 18: Relationship between false positive rate and number of vehicles and attacker.

From the above placed observation following results have been obtained.
1. The detection rate increases with increase in number of nodes.
2. The DMV load increases as number of attackers increases.
3. False negative rate reduces as number of nodes increases.

VI. CONCLUSION

In this paper a scheme has been presented to detect Sybil attack using Digital signature. A malicious node has been designed to act as Sybil attacker. When there was no attacker in the system no packet loss was observed, but with inclusion of Sybil attacker almost all packets were dropped by attacker. Detection rate increases with an increase in number of nodes. DMV load increases with increase in number of attackers in the system. False negatives decrease as number of nodes increase in the system.

REFERENCES

[1] Jie li, Huang Lu and Mohsen Guizani. ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs. IEEE Transactions on parallel and distributed systems, Vol. 26, No. 4, April 2015, pp. 938-948.
[2]Kenza Mekliche and Dr. Samira Moussaoui.L-P2DSA: Location-based Privacy-Preserving Detection of Sybil Attacks. 11th international Symposium on Programming and System (ISPS), 22-24 April 2013 IEEE pp. 187-192.
[3] Soyoung Park, Baber Aslam, Damala Turgut and Cliff C. Zou. Defence Against Sybil Attack in Vehicular Ad hoc Network Based on Roadside Unit support. IEEE, Military Communications Conference (MILICOM) 2009, 18-21 October.
[4] Dongxu Jin and JooSeok Song. A Traffic flow Theory Aided Physical Measurement-Based Sybil Nodes Detection Mechanism in Vehicular Ad hoc Networks. IEEE, 13th International conference on Computer and Information Science (ICIS) 2014, June 4-6 2014, Taiyuan, China.
[5] J. R. Douceur, The Sybil attack. The International Workshop on Peer to Peer Systems, March 2002, pp. 251-260.
[6] Bin Xiao, Bo Yu and Chuanshan Gao, Detection and Localization of Sybil Nodes in VANETs. In proceedings of ACM Workshop on Dependability Issues in Wireless Ad hoc Networks Sensor networks 2006 (DIWANS-06) Los Angeles USA 25-9-2006, pp. 1-8.
[7] Jyoti Grover, Manoj Singh Gaur and Vijay Laxmi, A Novel Defence Mechanism against Sybil Attacks in VANET, in the proceedings of 3rd International ACM conference on Security of Information and Network (SIN' 10), Sept.7-11, 2010, Taganrog, Rostov-on-Don Russian Federation pp. 249-255.
[8] Jyoti Grover, Manoj Singh Gaur and Vijay Laxmi, A Sybil Attack Detection Approach using Neighbouring Vehicles in VANET, presented at 4th International ACM conference on Security of Informationand Networks (SIN' 11) Nov. 14-19, 2011, Sydney, Australia, pp.151-158.
[9] Yong Hao, Jin Tang and Yu Cheng, Cooperative Sybil Attack Detection for position Based Applications in Privacy Preserved VANETs presented at IEEE Global Telecommunication Conference (GLOBECOM 2011), Dec. 5-9 2011.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 10, October 2016

[10] Tong Zhou, Romit Roy Choudhury, Peng Ning and Krishnendu Chakrabarty, P^2DAP – Sybil Attacks Detection in Vehicular Ad Hoc Networks, IEEE Journal on selected areas in communications, VOL. 29 No. 3, March 2011, pp. 582-594.
[11] Parastoo Kafil, Mahmoud Fathy and Mina Zolfy Linghvan, Modelling Sybil Attacker Behaviour in VANETs, IEEE 9th International Conference on Information Security and Cryptology (ISC) 2012, Sept. 13-14 pp.
[12] Bayrem TRIKI, Slim REKHIS, Mhamed CHAMMEM and Noureddin BOUDRIGA, A Privacy Preserving Solution for the Protection Against Sybil Attacks in Vehicular Ad Hoc Network, IEEE Conference: Wireless and Mobile Networking at 6TH IFIP (WMNC'2013) April 2013.
[13]Kenza Mekliche and Dr. Samira Moussaoui, L-P2DSA: Location-based Privacy- Preserving Detection of Sybil Attacks, IEEE 11Th International Symposium on Programing and System (ISPS) 2013, pp. 187-192. prevention of Sybil
[14] P. Vinoth kumar and M. Maheshwari, Prevention of Sybil Attack and Priority Batch Verification in VANETs, IEEE Conference ICICES2014- S. A. Engineering College, Chennai, India.
[15] Thiago M. de SALES, Hyggo O. ALMEDIA, Angelo PERKUSICH, Leandro de SALES, and Marcello de SALES, A Privacy-Preserving Authentication and Sybil Detection Protocol for Vehicular Ad Hoc Networks, IEEE International Conference on Consumer Electronics (ICCE) 2014, Jan 10-13 2014, pp. 426-427.
[16]SUMO, Project SUMO available fromhttp://sumo.sourceforge.net/.
[17]Available from: www.openstreetmap.
[18] Ricardo Jorge Fernandes, Large-scale simulation of Vehicular Ad Hoc Network, Doctoral Thesis, University of Porto, Minho and Aveiro, May 2014.
[19] Teerawal Issariyakul, Ekram Hossain, Introduction to Network Simulator NS2, Spinger,2009.
[20] S.R.Subramanya, Byung K Yi, Digital Signatures, IEEE POTENTIAL march/april 2006 Vol. 25, issue 2, pp.5-8.