TO PROPOSE ALGORITHM TO DETECT AND ISOLATE MALICIOUS VEHICLE IN VANET

A DISSERTATION

Submitted

By

JAYDEEP PRAVINCHANDRA KATESHIYA

(11307449)

To

Department of Computer Science

In Partial Fulfilment of the Requirement for

Award of the Degree of

Master of Technology in Computer Science & Engineering

Under the guidance of

MR ANUP PARKASH SINGH

2015

PAC FORM

LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

School of: Computer Science and Engineering

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the student	:Jaydeep P. Kateshiya	Registration No	:11307449
Batch	:2013-2015	Roll No	:RK2307A03
Session	:2014-2015	Parent Section	:KE2307

Details of Supervisor:

Name	:Anup Parkash Singh	Designation	: Assistant Professor
UID	:16790	Qualification	: M.Tech
		Research Exp.	:3 years

Specialization Area: Networking

Proposed Topics:-

1. Analysis of security attack in Vehicular Ad-Hoc networks.
2. Analysis of routing protocols of wireless sensor network.
3. Security issues in wireless sensor networks.

Anup VRK 16790
Signature of supervisor

PAC Remarks:

Topic (1) is approved

APPROVAL OF PAC CHAIRMAN Signature: Date: 29/9/2014

*Supervision should finally encircle one topic out of three proposed topics and put up for an approval before Project Approval Committee (PAC).
*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.
*One copy to be submitted to supervisor.

ABSTRACT

A Sybil attack is notorious security problem in wireless Vehicular Ad-Hoc network (VANET). A vehicular Ad-Hoc network is wireless networks without any pre-existing infrastructure and centralizes control. They have self-organizing capabilities with vehicular nodes. Ad-Hoc network contains multi-hop routes capabilities within short transmission range. Because of openness nature VANET is malicious by attacker. Several approaches have been proposed for finding malicious activity in VANETs. Due to nonexistence of VANETs infrastructure and well defied perimeter VANETs are susceptible to variety of attacker types. To develop a mechanism which provide strong security and understand the malicious node activity in the VANETs. A new mechanism presented is called Monitoring Method, which isolate malicious node on selective path in AODV routing protocol and secure the channel. This new methodology is named as "To Isolate and prevent Sybil Attack in VANETs". It is based on ICMP message and monitor mode technique. Experimental result will be drone with use of NS-2 simulator and simulate result for Throughput, Fuel Emission, Delay and compare the result with existing technique.

.

ACKNOWLEDGEMENT

I am very grateful to my guide **Mr Anup Parkash Singh,** Assistant Professor in Department of Computer Science & Technology, Lovely Professional University, Punjab. For his extensive patience and guidance throughout my project work. Without his help I could not have completed my work successfully .I would like to thank **Mr Dalwinder Singh**, Professor and Head, Department of Computer Science and Engineering ,Lovely Professional University, Punjab, for having provided the freedom to use all the facilities available in the department, especially the library. I would like to thank my classmates for always being there whenever I needed help or moral support. Finally, I express my immense gratitude with pleasure to the other individuals who have directly or indirectly contributed to my need at right time for the development and success of this work.

Jaydeep P. Kateshiya

DECLARATION

I hereby declare that the dissertation proposal entitled, "**To Propose Algorithm To Detect and Isolate The Sybil Attack in VANET**" submitted for the M. Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

DATE: **Investigator**

Reg. No._____

CERTIFICATE

I hereby certify that the work which is being presented in the Dissertation-II entitled **" To Propose Algorithm to Detect and Isolate Sybil Attack In VANET "** in partial Fulfilment of the requirement for the award of degree of **Master of Technology** and submitted in Department of Computer Science and Engineering, Lovely Professional University, Punjab is an authentic record of my own work carried out during period of Dissertation-II under the supervision of **Mr Anup Parkash Singh**, **Assistant Professor**, Department of Computer Science and Engineering, Lovely Professional University, Punjab.

The matter presented in this dissertation-II has not been submitted by me anywhere for the award of any other degree or to any other institute.

Date: **(Anup Parkash Singh)**

Supervisor

CONTENTS

LIST OF FIGURES

LIST OF TABLE

CHAPTER 1

INTRODUCTION

1.1 Networks

A group of independent systems or persons to share the information and hardware is said to be a network. In a network each and every node is connected by a path where the communication can be done. Networks are broadly categories as wired network and wireless network. In wired network all the devices are connected to each other where we connect a USB storage, printer , LAN cables etc. to represent wired network there are many topologies such as star,bus,mesh .These networks follow some fixed infrastructure. Wireless networks are quite equal to wired network but the devices are connected without using any wires and cables to decrease the mobility and increase the range. These types of networks does not have any fixed infra-structure .the devices can connect to the computer without any wires through signals such adhoc networks, Wi-Fi access. Basically networks are divided as Local area network, Control area network, Wireless local area network, Wide area network, Metropolitan area network. This mainly deals with many forms like local, global.

1.2 MANET

Mobile Ad hoc Network basically called as MANET. It's ability of an algorithm to continue operating despite abnormalities in input, calculations, etc. means robustness infrastructure less wireless network and it will be either by mobile nodes or by both fixed structure and mobile nodes. Mobile nodes are randomly connected with each other means near and within area and forming arbitrary topology. They act like as both as intermediate node for sending and receiving packet which basically like router and host. Their ability to self-arrangement makes this technology suitable for provisioning communication with in range and out of the range, for example flood or disasters areas where there is no contact point or communication infrastructure where we can communicate or in emergency type. In MANET routing protocols are available for both fix and dynamic topology are used for routing the packet or

data via mobile node to destination. An ad hoc network is a wireless network describe by the none any centralized which can control and fixed infrastructure. The not present of an infrastructure in ad hoc networks poses great difficult task in the functionality of these networks. [1]

1.2.1 Types of MANET

Vehicular Ad Hoc Networks (VANETs): VANET is basically use for vehicle communication in city and highway. These are used for the communication among the mobile vehicles and road side unit. The communication being carries on same direction and also in if the vehicles are moving in the different direction with in the range of that area.

Intelligent vehicular ad hoc networks (InVANETs): It is used in case like destruction of the vehicles or also used for media communication and track the automotive vehicle. It is uses the scheme brilliantly and the less communications flow goes on.

Internet Based Mobile Ad hoc Networks (iMANET): It is an ad hoc networks that connection mobile nodes and fixed nodes of Internet entrance. For this Ad hoc routing algorithms don't apply directly in this class of network where another protocols is used.

1.3 VANET:

VANET's is basically a part of MANET and best example of VANET is Transport System of any travel agency or any company which is joined internally. These Transport System of a vehicles are moving in any parts of city and different routes to pick or drop client or employees if they are connected together, which make an Ad hoc Network and connected wireless.

In ad hoc network most capable areas of research is the investigation of the communications among vehicles called Vehicular Ad-hoc Networks (VANETs). The networks are self-configuring networks together of a collection of vehicles and elements of roadside unit structure connected with each other without need any infrastructure, sending and receiving in data of current traffic situation and the way from where it's easy to go. Nowadays, Wi-Fi (*IEEE 802.11 based*) technologies are used for the initialization of VANETs which most frequently today.

The communications standard specifically for VANETs is DSRC (Dedicated Short-Range Communication) has been proposed presently. Its attempt very low discontinuation and high data rate for a short medium range communications service. In some scenarios in which buildings and distances discontinue communication channels frequently and where the reachable time for connecting to vehicles could be really very short-lived are especially true in certain time of a VANET. In this without using automatic intelligent design tools is practically impossible efficient protocol configuration for VANETs because of the enormous number of possibilities problem (*NP-problems*). When considering multiple design issues, such as highly dynamic topologies which change very rapidly and reduced scope, it is especially difficult (e.g., for a network designer) [2].

Vehicular adhoc network are wireless networks where all the vehicles are basically called node or mobile node in MANET. It is for the driver comfortable when any certainly action done and road infrastructure safeties, the vehicle to vehicle communications provide them.. It is very bottom line for all the vehicles. Vehicular ad hoc network is individual form of MANET which is vehicle to vehicle roadside wireless changing topology for communication network. It is functioning as independent and self-arranging wireless communication network, where exchanging data and sharing information for all the nodes in VANET involve themselves as servers or client . The VANET network architecture can have three different types of categories such as pure cellular network architecture, pure ad-hoc network architecture and hybrid network architecture.

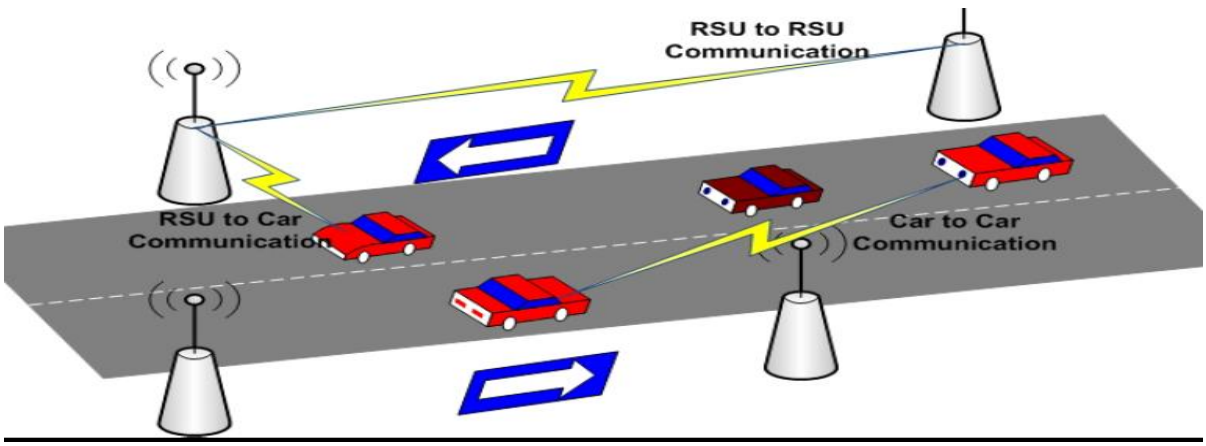


Figure 1 : VANET Structure

1.3.1 Application and uses of VANET:

- **Safety applications:** There are so many accident happened in road due to the collision of vehicles due to some minor mistake. That's why Safety applications are most important factor to reduce the road accident and loss of life of the occupants of vehicles. The class of application which provide people life safety and active road safety to avoid collisions by assisting the drivers with timely and accurate information and with care of all security.
- **Car speed warning:** The combinations of GPS and digital maps with help of protocols are used to judge threat level for driver approaching a curve quickly.
- **Traffic signal violation warning:** It is also pattern to send a warning message when driver detects the vehicle is in risk of running the traffic signal or any accident case. The timing to send a message is made on the basis of traffic signal light status and timing the vehicle position and speed.
- **Collision risk warning:** On collision of a vehicle risk time the system vehicle and RSU detect chances of collision between multiple vehicles are not able to communicate amongst them. The system will collect data about vehicles that are coming in opposite direction and are approaching towards their destination.
- **Lane change warning:** In this application vehicle sensor monitor the position of vehicle within a roadway lane and warn a driver to change lanes or not.

1.3.2 V2V Communication:

Possible Deployment regarding the C2C-CC (Car-to-Car Communication Consortium) reference architecture together with the advances in different communication technologies, the vehicular networks in all likelihood have two main types of communication types: vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication [5].

These types of communication scenarios allow a vehicular network number of deployment options. Vehicular network deployment can be included into the existing cellular systems or Vehicular network deployment can also be combined into wireless hotspots along with road and near to most accident road. Such hotspots can be operated individually at office or at

home, or by wireless Internet service providers or can be combined operator with any one [5].

Vehicles with other vehicle can even communicate or transfer data or message directly without any communication with infrastructure or RSU unit, where vehicles can co-operate and forward the data on behalf of near the vehicle [5].

The technologies for the vehicular communication can be classified in the following three types based on the specific characteristics of vehicle [5]:

i. **In-vehicle communication**
ii. **Vehicle-to-roadside/vehicle-to-infrastructure communication**
iii. **Inter-vehicle communication (single- and multi-hop)**

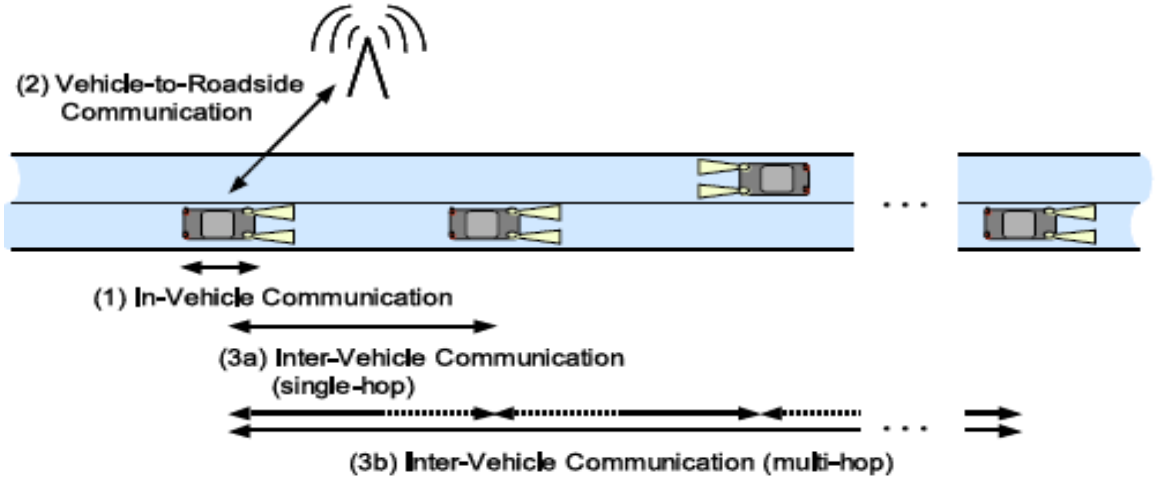


Figure 2 : Communication Architecture

- **In-Vehicle Communication:** In-vehicle communication (InVC) enables the data exchange between different components within a vehicle for better performance and is widely used in any modern and luxurious car. Such example as sensor of distance between within vehicles which connect in mirror or display [5].
- **Vehicle-to-Roadside Communication (VRC):** It is also called as vehicle to infrastructure or RSU communication. It is used for any amiable of communication from the vehicle to a fixed infrastructure or vice versa. This communication can be single way or in two ways directional [5]. In vehicle to road side communication is

also called a vehicle to RSU communication. In this time vehicles communicate from the vehicle to a fixed infrastructure. This communication in the two forms which can be an unidirectional or bidirectional fixed infrastructure. Simulcast system support the unidirectional transfer of information from simulcast station to the vehicle. In this system the entire vehicle communicates point to point with the base station or access point. Base station make a coordinating the communication by using the physical synchronization and medium access. Base station balances the extra load and provides the access control in proper channel. Bidirectional technologies further divide into the cellular mobile phone system and small range system. Existing cellular infrastructure like GMS and UTMS and provide information required infrastructure always available. The small area which within the range which can provide high data rates at a low cost. It's also depending on the type of air interface and infrastructure, the range in which VRC is possible varies from small range of meters for wireless local area technologies to high range of kilometres for public radio systems.

1.3.3 Major Issues in VANET:

There are some issues in VANET. These are as follow:

High Mobility: Due to high mobility all the nodes are not interacted properly with each other because they have to learn about others behaviour first according to learn based scheme. It also decreases efficiency of the system.

Real-time Guarantee: VANET applications are used for hazard warning, vehicle accident warning information, and collision avoidance, so applications involve strict deadlines for proper message delivery.

Privacy and Authentication: It is required to follow the vehicles for the identification of vehicles from which they send the message for authentication of all message transmission, which most consumers will dislike others to know about their personal identification. Therefore a system wants to be introduced which enables message to be unknown to the common vehicles but also recognition by central authorities which handle in cases like accidents.

Location Awareness: For the proper location awareness GPS system is required to handle the VANET application for location awareness. If there is no Proper system for location identification, delay is there automatically.

Delay in VANET: In a VANET delay issue should be minimum for the new path identification. The chances of collision between multiple vehicles are not able to communicate amongst themselves can detect by both vehicle and infrastructure. The system will collect data about vehicles that are coming in opposite direction and are approaching towards the destination. For this, there are many safety applications are present in VANET to minimise the road accident and loss of life by vehicle accident. Collision leads the jam problem. To overcome this problem delay should be minimum.

1.3.4 Characteristics of vehicular network:

Vehicular network have some special type of behaviour and characteristics, which distinguishing them from other types of network. As compare to other networks vehicular network have unique and interesting features as follow:

- **Unlimited transmission power:** In the ad-hoc devices power issues is main constrain but in the case of this network nodes/vehicle provide continuous and sufficient power to computing and communication devices for doing other task.
- **Computational capacity very high:** Operating vehicles can have very significant computing capacity which done by sensor and circuit in the vehicle with sufficient energy, communication and sensing capabilities.
- **Predictable mobility:** In the mobile ad-hoc network where the vehicle mobility is very hard to predict, vehicles have very predictable movements that are limited to roadways. Roadways information is often available from positioning systems and map based technologies such as GPS. It can give brief about the vehicle average speed with according to some distance, current speed of the vehicle and path of the future position of vehicle can also be finding them.
- **High mobility:** vehicular networks operate extremely dynamic and their configurations. If take the example of highway where relatively speed of up to 190-230 Km/h may occur while density 1-2 vehicle in 1 Km on other side where relative speed up to 65-70 Km/h and in rush hours especially very high density of nodes.

- **Partitioned network:** vehicular network will be frequently divided and dynamic nature of traffic may result in large inter vehicle gaps in sparsely populated scenarios in several unusual clusters of nodes.
- **Network topology and connectivity:** In the vehicular network scenarios are vary from location to location. When vehicle move and change their position constantly in the dynamic scenarios. As the link between the nodes connect and disconnect very often because of network topology changes frequently. As the network is connected is hugely depend upon the two factors which are the range of wireless links and the fraction of participant vehicles, where only a fraction of vehicle on the road could be equipped with wireless interfaces [8].

1.4 VANET Applications:

VANETs applications scenarios very huge learning and designing phase is very difficult may become a very nasty job. They are classified into in such a way such as set of protocol will work for applications from a given class. The benefits of classifying them as follow:

- Develop some applications models to represent a large number of applications with similar properties belonging to same class for application simulation and validations.
- Identification of key performance metrics relevant to each identified applications class, as benchmarks for evaluating whether designed application mechanism can meet common requirements mandated by application classes.
- Create a networking protocol stacks for each class of applications, with the consideration of improving reusability of common mechanistic modules or networking protocols.

1.5 Attacks in VANET:

There are different types of attacks in VANET. These attacks are as follow:

Sybil Attack in VANET:

This attack happens when an attacker creates a large number of pseudonyms and claims or acts like more than a hundred vehicles in order to tell other vehicles that there is a jam ahead and forces them to take an alternate route. Sybil attack depends on firstly, how

cheaply identities can be generated, secondly the degree to which the system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity and thirdly whether the system treats all entities identically. For instance an attacker can act like hundred vehicles to convince the other vehicles on the road that there is congestion and instruct them to go to another route, so that the road will be clear for him/her. A Sybil node may send a high rate of association request messages to an AP, using random medium access control (MAC) values to emulate a large number of clients. The result is that legal clients are denied access once the Sybil node has consumed an AP's association slots or channel slots. As a special kind of denial-of-service attack, Sybil attacks seriously endanger the availability of network services for wireless systems.

It consists of sending multiple messages from one node with multiple identities. Sybil attack is always possible except the extreme conditions and assumptions of the possibility of resource parity and coordination among entities. When any node creates multiple copies of itself then it creates confusion in the network. Claim all the illegal and fake ID's and Authority [21]. It can create collision in the network. This type of situation is known as Sybil attack in the network. This system can attack both internally and externally in which external attacks can be restricted by authentication but not internal attacks. As there is one to one mapping between identity and entity in the network.

A, B, C, D nodes are Sybil nodes which create fake or similar identity in the network and collapse the network. Sybil attack is a critical attack. In this type of attack attackers generate multiple messages from different ids to other vehicles. Other vehicles are thinking in this way that messages are coming from different vehicles with different ids, so there is condition of jam occurs.

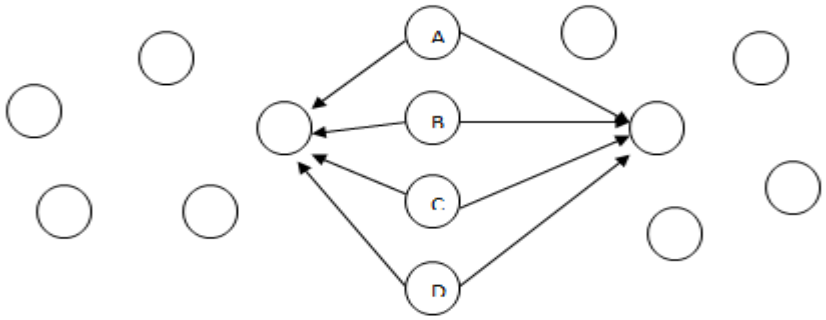


Figure 3 : Sybil Attack

In this way attacker produce illusion of other vehicle and force them to choose another path and leave the road for the benefit of the attacker. Overall it is concluded that Sybil attack is performed or launched by sending multiple messages from different ids. In fig. 4 red colours cars have same id that is A which are responsible for trigger Sybil attack in the network. It is of two types delay sensitive and throughput sensitive.

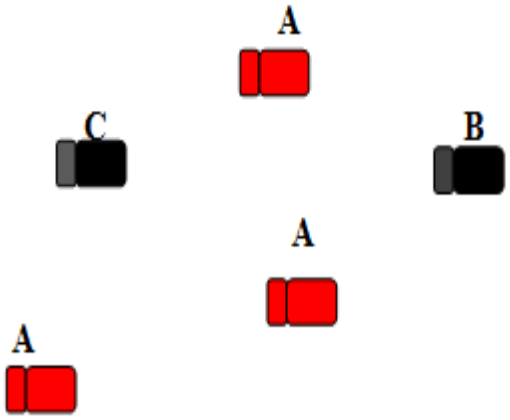


Figure 4 : Sybil Attack in the Network

Denial of Service Attack:

In DOS attack the main objective is to prevent legitimate user from accessing resources and services. This attack can be trigger by jamming the whole channel and network so

that no authorized vehicle can access the network. It is serious problem in which user is unable to communicate with the user due to DOS attack. At the basic level, attacker forces node and make it busy to do unnecessary tasks by overwhelming it so that it could not do necessary tasks. So it is responsible for packet dropping [22].

Distributed Denial of Service Attack:

DDOS is more harmful than DOS attack because it is in distributed manner. Different types of locations are used by the attacker to launch the attack. It might be possible that they use different time slots for sending messages. The nature of the message and time slot varied from vehicle to vehicle. DDOS is possible at V2V and V2 I. Its main objective is to slow down the network and jam the network [22].

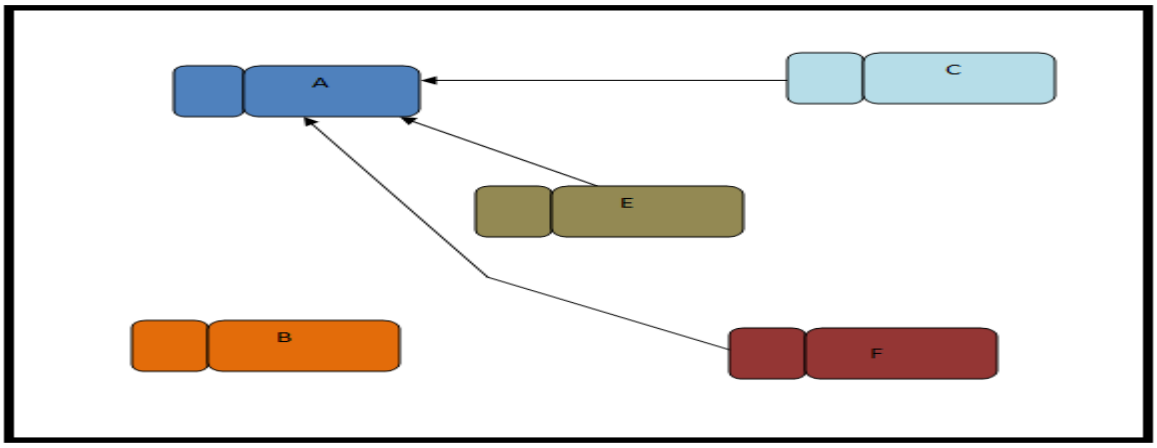


Figure 5 : DDOS attack

Spamming:

In spamming, attacker tries to spam number of messages in the network to consume more bandwidth and increase the latency of the network. Attacker send number of messages to the group user which are not concern with their work it just load the network [23].

Black hole Attack:

In this type of attack the requests is listen by an attacker for the routers in a flooding based protocol .When a request is received by the attacker to the destination node for a route, it

creates a reply for the short route and enters into the passageway to do something with the packets passing between them [10].

Wormhole Attack:

In wormhole attack, a malicious node, at one location in the network receives packets and to another location in the network tunnels them, to the location where packets are present into the network. When the control messages are routing are tunnelled it create disrupted. It is a network layer attack. The two colluding attacker's tunnel between them is referred as wormhole [8].

Node Impersonation Attack:

In Vanet network, each vehicle is identified by its ids. Each vehicle has a unique id which helps to communicate with these vehicles. Id is more important to identify accident's reason. In node impersonation attack, attacker can hide or change his original id and acts like original originator of the message. Attacker can change the content for his benefits. After this attack, attacker can easily send message to the any of the vehicle [23].

Replay attack:

Reply attack is used by unauthorized users and malicious user to masquerade as a legitimate user or Road side unit. This attack is happen only when attacker replay the transmission of already generated frames to the new connection. Attacker's captures generated frames and used it as a part of frame. Its main aim is to give false information regarding the identity of vehicle responsible for accident [24].

GPS Spoofing:

Table is maintained in the network to update all the information regarding identify of the vehicle and geographic location of the vehicle. Attacker generate GPS satellite signal to fool vehicle which are more effective than the original signals.

Timing Attack:

There should be accuracy in the time for the best performance of the network so delay should be less in any application. Timing attack is an issue in ITS safety application. In

this attack, attacker instead of modify the data; add more content in the original data. Due to addition message takes more slot to reach to the destination rather than required time. So ITS application is crucial application which is dependent on time and it requires data transmission on time otherwise serious accident may happen [22].

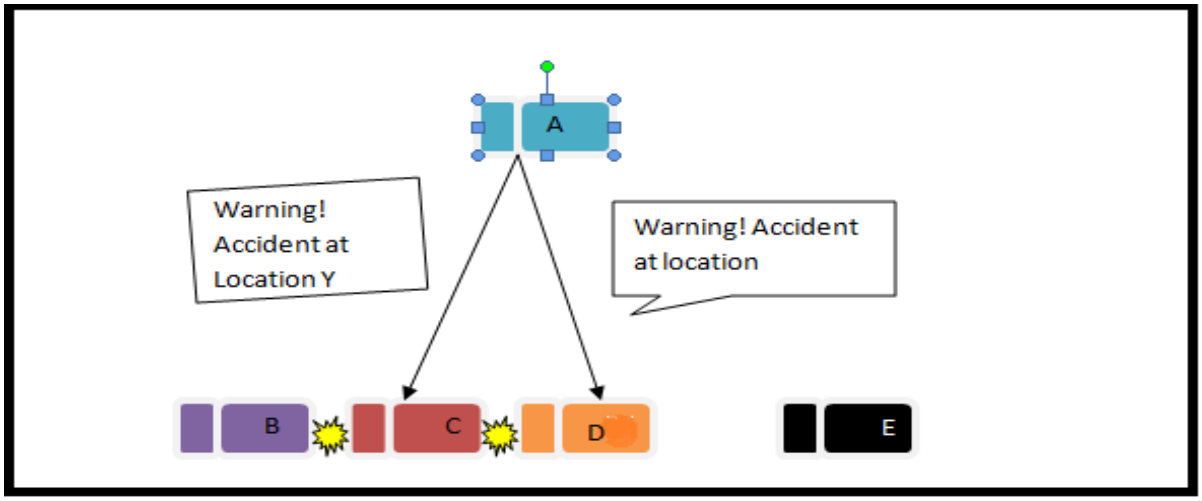


Figure 6 : Timing Attack

Social Attack:

The main idea of this attack is to confuse and bedazzle the victim by sending unnecessary, non-informative, unmoral message so that driver gets disturb. The authorized user gets annoyed by receiving such kind of message which is the main concern of the attacker. It automatically disturbs the driver which is responsible for distribution in the network.

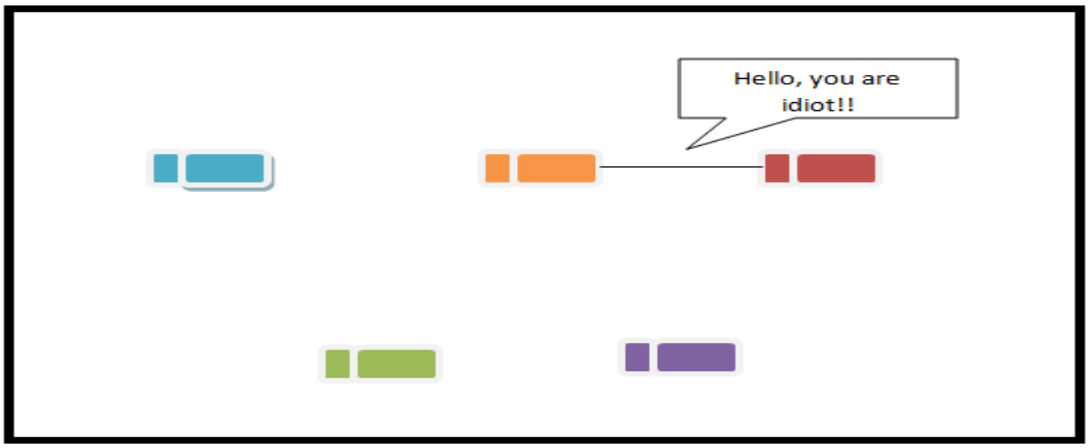


Figure 7 : Social Attack

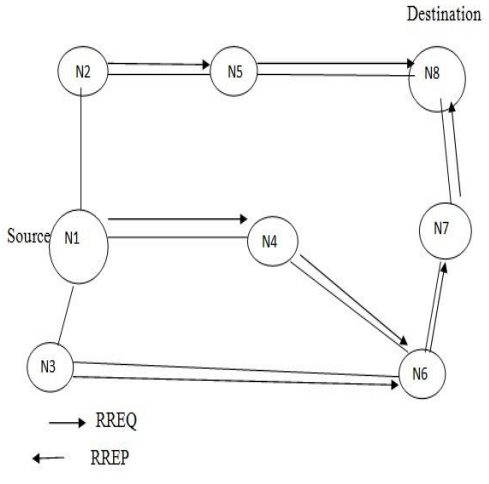
1.6 Routing Protocol in VANET:

Routing protocol specifies how to communicate with the help of routers. It shares information among intermediate nodes then with the whole network. It helps to search shortest route from source to destination. There are various routing protocol in VANET. These protocols are as follow [25]:

Ad-Hoc On-Demand Distance Vector (AODV):

AODV is an on-demand routing protocol utilized in ad hoc networks. This protocol is like any other on-demand routing protocol which facilitates a smooth adaptation to transmutations in the link conditions. In case when a link fails, messages are sent only to the affected nodes. With this information, it enables the affected nodes invalidate all the routes through the failed link. AODV has low recollection overhead, builds unicast routes from source to the destination and network utilization is less. There is least routing traffic in the network since routes are built on demand. When two nodes are in an ad hoc network wish to establish a connection between each other, it will permit them build multi-hop routes between the mobile nodes involved. It is loop free protocol which uses Destination Sequence Numbers (DSN) to avoid counting to illimitability. This one is the distinguishing feature of this protocol. Requesting nodes in a network send Destination Sequence Numbers (DSNs) together with all routing information to the destination. It culls the optimal route predicated on the sequence number [7].

AODV defines three messages: Route Requests (RREQs), Route Errors (RERRs) and Route Replies (RREPs). These messages are used of UDP packets to discover and maintain routes across the network from source to destination. Whenever there is need to produce a new route to the destination, the node which is requesting broadcasts Route Requests. A Route is determined when this message reaches the next hop node (intermediate node with



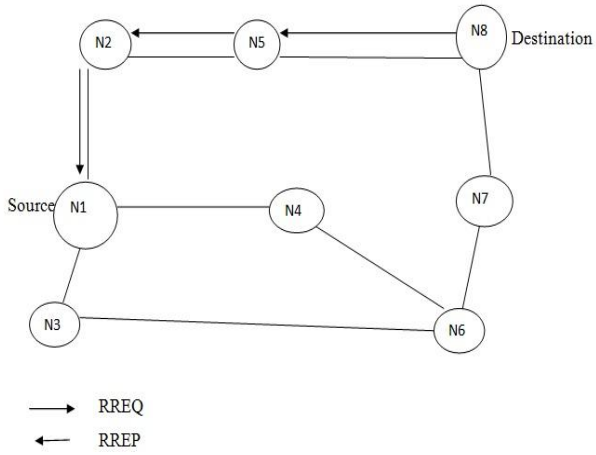


Figure 8 : AODV Route Discovery Process Figure 9 : Best path with minimum Hop Count

routing information to the destination) or the destination itself and the RREP has reached the originator of the request. Routes from the originator of the RREQ to all the nodes that receive this message are cached in these nodes. When a link failure occurs, Route Errors (RERRs) message is generated [29].

In the fig: 8 N1 nodes broadcast the packets to its neighbour nodes with RREQ and update its table. Then these nodes further forwards packets to its neighbour until the destination find outs and fresh route ascertain. Each node maintains its sequence number and broadcast ID. For every RREQ the node initiates broadcast ID which is incremented and together with the node's IP address uniquely identifies an RREQ. At last that route will be the final route that has the minimum hop count from source to destination.

LAR Protocol:

Location based routing protocols have characteristics along with deign architecture which make vehicular communication more challenging. There are three broad categories of networks as cellular, adhoc and hybrid. Cellular network supports infotainment, for example, latest news, information of locality. This is based on vehicle to infrastructure paradigm. As the existing infrastructure is present and support wide range of vehicular applications. But still there is a drawback that the requirement of fixed infrastructure deployment. It is solved by adhoc networks where there is no need of the prior infrastructure. This is more suitable for vehicle to vehicle communication. But it also faces problems due to

network partitioning and routing link failures and rapid topology changes. The solution of this problem is the deployment of the access points along the road and in case there is no issue regarding energy consumption. In hybrid communication, cellular network is based on centralized architecture which collects traffic information from road through access point. Access point processes acquired information and make available to drivers. The dynamic nature of vehicular communication, high speed of vehicles, and mobility results in degraded performance in traditional routing protocols. Traditional ad hoc routing protocols [25], [26], [27], [28] addressed the issues of mobile ad hoc network and are applicable for MANET applications. Following are the forwarding strategies:

- Greedy forwarding: According to the scenario depicted in Fig.1, if greedy forwarding strategy is used then, source node forwards the packets to a node closest to the destination 'D'. In this case 'S' sends packet to 'A'.
- Improved greedy forwarding: In this case, source node first consults its neighbour table and computes new predicted position of all its neighbours based on direction and velocity and then selects a node which is closest to the destination. 'S' computes new predicted position of its neighbours and suppose at time t2, vehicle 'B' over takes the vehicle 'A', then'S' selects 'B' as its next hop instead of 'A'.
- Directional greedy forwarding: Directional greedy approach only considers those nodes which are moving towards destination. It selects a node which is moving towards destination and is closest to the destination. Thus, it selects vehicle 'B' as its next hop.
- Predictive directional greedy forwarding: In this strategy, forwarding node maintains the information of its 2-hop neighbours. Before forwarding the packet, forwarding node consults its neighbour table and computes predicted position of all its neighbours (one- hop and 2-hop neighbours) and then selects a node whose one-hop neighbour is moving towards the destination and is closest to the destination. In this case, 'S' selects vehicle 'A' because its one-hop neighbour 'C' is moving towards destination 'D'.

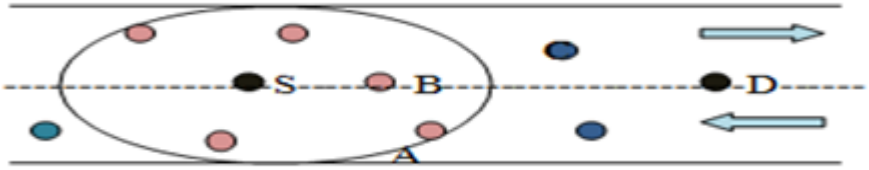


Figure 10 : Forwarding Strategies

DGR (Directional Greedy Routing):

DGR reduces hop count during routing by choosing the node moving towards the destination. Further, PDGR (Predictive Directional Greedy Routing) enhances the Directional Greedy Routing protocol by predicting the mobility of the vehicle and getting this mobility information from traffic pattern and street layout [25].

GSR (Geographic Source Routing):

GSR uses Dijkastra's shortest path algorithm on a map from GPS system. It calculates shortest path on each junction and by using greedy forwarding strategy along the path to next junction until destination is reached. Although, in this case no real time traffic information is used for path selection of the next node may stop at local maximum and for recovery it select another vehicle outside that road using greedy forwarding. GSR is combination of position based and topology based routing and it is reactive location service. It has high overhead on network due to use of beacons but more scalable and suitable for sparse network. [26]

A-STAR:

A-STAR is the position based routing scheme called as Anchor-based-street and Traffic Aware Routing. It uses city bus routes to identify an anchor path for packet delivery with high connectivity. By considering number of bus line on road, it provides traffic awareness for better decision making towards selected path as more vehicle density lowers down the chances of local maximum situation. If local maximum occurs then road is marked as out of service and recalculation of path takes place [25] [26].

GyTAR (Greedy Traffic Aware Routing):

GyTAR proposes for city environments which is based on intersection and makes use of geographical routing protocol. It has two parts: junction selection and forwarding data between two junctions. Digital maps are used to identify the position of junctions and also to find the shortest path towards destination via Dijkastra's shortest path algorithm [27].

EGySTAR:

EGySTAR is the modified version of GySTAR routing protocol. It selects junction dynamically as it is based on vehicular traffic density in the direction of the destination and curvamertic distance to the destination. It eliminates limitation of GySTAR by considering the direction of the vehicles before selecting the next junction. The score is assigned to each junction accordingly and junction having highest score is selected as next destination junction has higher vehicular traffic moving in direction of destination [28]

1.7 Disadvantages of LAR:

The use of positioning information has been widely used for location tracking and navigation. For example, GPS is commonly used in cars to assist drivers in navigating through foreign land. It is also used for military and defence operations. However, GPS availability is not yet worldwide and positional information does come with deviation, i.e., errors. In addition, it is not necessarily true that all future mobile devices will be equipped with GPS receivers. Heterogeneous devices will exist and hence some devices will not have GPS receivers. In such situations, location based routing will suffer and fail to operate. Positional errors can also cause problems in routing. In addition, without considering signal strength, power life, and connectivity information, communication performance will suffer if data are routed based on location information alone. Lastly, prior and advance information about the positional information of the destination node may not be readily available at the source.

CHAPTER 2

REVIEW OF LITERATURE

Gañán, C., Muñoz, J. L., Esparza, O., Mata-Díaz, J., & Alins, J."PPREM: privacy preserving revocation mechanism for vehicular ad hoc networks". This Paper represents one of the critical security issues of Vehicular Ad Hoc Networks (VANETs) is the revocation of misbehaving vehicles. While essential, revocation checking can leak potentially sensitive information. Road Side Units (RSUs) receiving the certificate status queries could infer the identity of the vehicles posing the query. An important loss of privacy results from the RSUs ability to tie the checking vehicle with the query's target. They propose a Privacy Preserving Revocation mechanism (PPREM) based on a universal one-way accumulator. PPREM provide explicit, concise, authenticated and unforgettable information about the revocation status of each certificate while preserving the users' privacy. They have proposed PPREM for VANETs, which enhances the certificate status checking process by replacing the time-consuming CRL with a fast revocation checking process employing a one way accumulator. PPREM not only satisfies the security and privacy requirements of VANETs but can also significantly reduce the revocation cost [**9**].

This paper proposed a compromised RSU detection mechanism for Sybil attack detection. A footprint concept is used in proposed method to detect the Sybil attack by using the trajectory information which is generated by multiple RSUs and the location of the vehicle is preserved. **Balamahalakshmi D. & Shankar M. K. V** says that the RSU will generate the location and timing information to vehicle while it passes through RSU. Using this message, the verification is carried and the number of adjacent RSUs is eliminated to reduce message size. The result showed that the length of the trajectory information is reduced without loss of information and the bandwidth overhead is also reduced [10].

Byung Kawn Le et al. , Proposed a Detection Technique Against a Sybil Attack (DTSA) protocol using Session Key based Certificate (SKC) to validate inter-vehicle IDs in VANETs. In DTSA, the SKC (Session Key based Certificate) used to verify the IDs among vehicles,

and also generates a vehicle's anonymous ID, a session Key, the expiration date and a local server's certificate for the detection of a Sybil Attack and the verification time for ID.

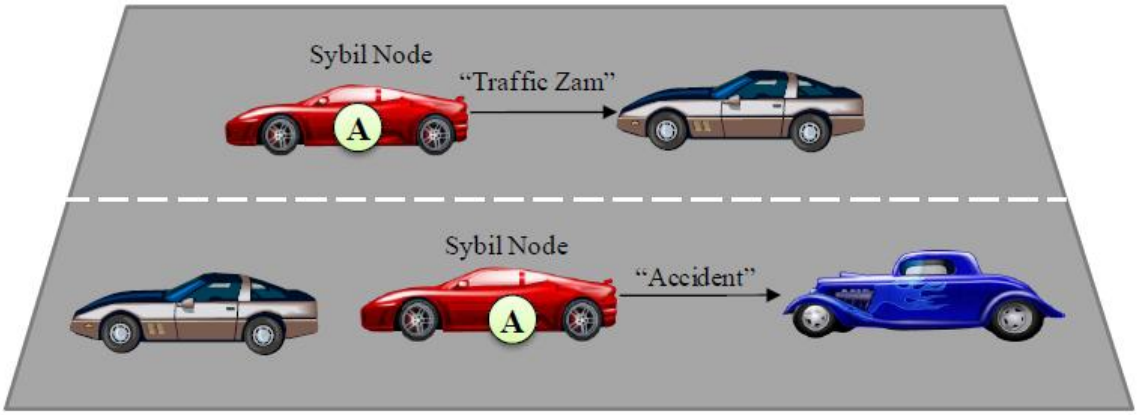


Figure 11 : Sybil Node

This DTSA reduces not only the detection time against a Sybil attack but also the verification time for ID by using a hash function and an XOR operation. Besides, a drivers' privacy can be protected by using an anonymous ID. This DTSA helps drivers drive safely with the reliable information of VANET and reduce traffic accidents [**7**].

The detection of replication attacks in wireless sensor networks (WSNs) has been a long-standing problem. Many variants of replication attacks were spawned such as the sybil attack. In this paper **Li, M., Xiong, Y., Wu, X., Zhou, X., Sun, Y., Chen, S., & Zhu.xX** , they proposed a regional statistics detection scheme (RSDs) against sybil attacks, which is an effective solution to three key issues: firstly, they address the sybil attack by a RSSI-based distributed detection mechanism, secondly, their protocol can prevented the network from a large number of nodes failure caused by sybil attacks, Thirdly, the RSDs has been verified can maintain a high detection probability with low system overhead by implement experiments. Finally, they run our protocol in a prototype detection system with 32 nodes that the experiment result confirmed its high efficiency [**8**].

Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. , they propose a novel Sybil attack detection mechanism, Footprint, using the trajectories of vehicles for identification while still preserving their location privacy. More specifically, when a vehicle approaches a road-side unit (RSU), it actively demands an authorized message from the RSU as the proof of the

appearance time at this RSU. They design a location-hidden authorized message generation scheme for two objectives: first, RSU signatures on messages are signer ambiguous so that the RSU location information is concealed from the resulted authorized message; second, two authorized messages signed by the same RSU within the same given period of time (temporarily linkable) are recognizable so that they can be used for identification. With this scheme, vehicles can generate a location-hidden trajectory for location-privacy-preserved identification by collecting a consecutive series of authorized messages. Utilizing social relationship among trajectories according to the similarity definition of two trajectories, Footprint can recognize and therefore dismiss "communities" of Sybil trajectories

Tong Zhou et al. proposed a lightweight and scalable protocol called Privacy Preserving Detection of Abuses of Pseudonyms protocol to detect Sybil attacks in VANET. In this protocol, a malicious user pretending to be multiple (other) vehicles can be detected in a distributed manner through passive overhearing by s set of fixed nodes called road-side boxes (RSBs). The detection of Sybil attacks in this manner does not require any vehicle in the network to disclose its identity; hence privacy is preserved at all times. he results also quantify the inherent trade-off between securities, i.e., the detection of Sybil attacks and detection latency, and the privacy provided to the vehicles in the network. From the results, we see our scheme being able to detect Sybil attacks at low overhead and delay, while preserving privacy of vehicles. Using this protocol, the multiple vehicles which are affected by malicious user can be detected in a distributed manner through passive listener using set of fixed nodes called road-side boxes (RSBs). The detection of Sybil attacks in this manner does not require any vehicle in the network to explore its identity; hence privacy is preserved at al times [**6**].

In this paper, **Hao, Y., Tang, J., & Cheng, Y.** propose a security protocol to detect Sybil attacks for position based applications in privacy preserved vehicular ad hoc networks (VANETs). Vehicles in our protocol identify Sybil attacks locally in a cooperative way by examining the rationality of vehicles' positions to their own neighbours. The attack detection utilizes the characteristics of communication and vehicles' GPS positions which are included in the periodically broadcasted safety related messages. No extra hardware and little communication and computation overhead will be introduced to vehicles. Therefore, their

protocol is very light weighted and suitable for real applications. Moreover, a smart attacker scenario in which a malicious vehicle may adjust its communication range to avoid detection and the malicious vehicles' collusion scenario are also considered. Simulation results based on NS2 are presented to demonstrate the performance of the proposed protocol [**4**].

In this paper, they present a lightweight security scheme for detecting and localizing Sybil nodes in VANETs, based on statistical analysis of signal strength distribution. Their scheme is a distributed and localized approach, in which each vehicle on a road can perform the detection of potential Sybil vehicles nearby by verifying their claimed positions. **Xiao, B., Yu, B., & Gao, C, They** first introduce a basic signal-strength-based position verification scheme. In this technique, traffic patterns and support from roadside base stations are used to their advantage then, propose two statistic algorithms to enhance the accuracy of position verification. The statistic nature of our algorithms significantly reduces the verification error rate. In GPS and RSSI signal measurements are used for detecting Sybil nodes. The proposed scheme uses Vehicle-to-Vehicle (V2V) communications to confirm reported positions of vehicles by referencing the RSSI measurements. To correct inaccuracies arising from RSSI measurement, caused by vehicle mobility, traffic patterns and support from roadside base stations are used [**3**].

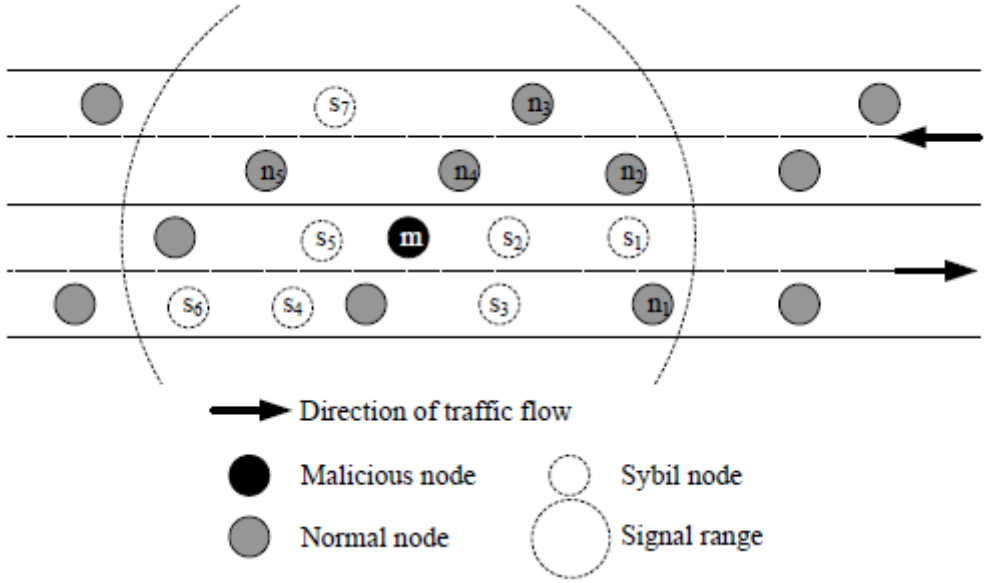


Figure 12 : VANET under Sybil Attack

Rajesh Rajamani has proposed on spacing policies for highway vehicle automation [11] a spacing policy which is a nonlinear function of speed. It provides string stability and traffic flow stability as well as a higher traffic flow capacity compared to the standard time-gap controller. The spacing policy used autonomously available information. Analytical calculations showed that the spacing policy would guarantee string stability and traffic flow stability while maintaining smaller steady state spacing and hence providing larger traffic flow capacities in the speed range 20–65 m/h. this spacing policy can be readily implemented on ACC vehicles on today's highways.

Hao Wu has presented An Empirical Study of Short Range Communications for Vehicles [14] a work on short range of communication over the vehicles. The work includes both V2V and V2I communication under highway scenario. The network characteristics in driving environment is been discussed in this work.

Josiane Nzouonta, Neeraj Rajgure represents a paper based on routing protocols called RBVT, road based using vehicular traffic information routing which is based on the existing routing protocol in city based vehicular ad-hoc networks (VANETs). RBVT protocols leverage real time traffic information to create road based paths consisting of successions of road intersection and high probability, network connectivity among all the systems. In this paper use the geographical forwarding is used to send the packets between intersection paths, reducing the sensitivity within the paths to individual node movements. In the dense network high contention and optimize the forwarding using a distributed receiver based election of next hops, it is based on the multi-criteria prioritization function taking into account non-uniform radio propagation. This paper designs the reactive protocol RBVT-R and proactive protocol RBVT-P and compared them against MANETs protocols like AODV, OLSR, GPRS. Other protocol representative is like VANET. In the simulation result shows that in the urban settings shows that RBVT-R protocol best in term of delivery rate, with up to 40% increase compared to some existing protocols. In the protocol terms of average delay, RBVT-P performs best and 85% decreased as compared to other protocols [19].

Jason J. Haas and Yih-Chun Hu represent a paper based on the performance measurements obtained from simulations of the (VANETs) vehicular ad-hoc networks. These simulations

use as input traces of vehicle movements that have been generated by traffic simulators which is based on the traffic model theory. In this paper mainly work based on the actual large scale recordings of vehicle movements. To our knowledge, no one has published any work on actual large scale recording of vehicle movements. In order to enable analysis on this scale, we have developed a new VANET simulator which handles more vehicle than ns2. To enable us simulator and present results of cross validation between ns2 and our simulator showing the both simulation produce result that are statistically the same. This simulator use to analyse the proposed authentication mechanism, which relies on ECDSA signatures comparing it to broadcast authentication using TESLA. In this paper perform our evaluations using real vehicle mobility. Our comparison shows its strength and weakness for each of these authentication schemes in terms of the resulting reception rates and latency of broadcast packets [18].

Su-Jin Kwag has proposed Performance Evaluation of IEEE 802.11 Ad-hoc Network in Vehicle to Vehicle Communication performed a work to [15] analyses the performance of the IEEE 802.11 Ad-hoc network for v2v communication under a vehicular environment, focusing on the fairness which very crucial to the safety related services, and the effect of mobility. Some suggestions for future researches are followed.

Kung has proposed a survey of mobility models for ad hoc network research [13] they proposed security architecture for vehicular communication. The primary objectives of the architecture include the management of identities and cryptographic keys, the security of communications, and integration of privacy enhancing technologies. Their design approach aims at a system that relies on well-understood components which can be upgraded to provide enhanced security and privacy protection in the future.

Gang Liu and Han have proposed some aspects of road sweeping vehicle automation [12] a design of framework of intelligent transports system is proposed. The main task of the road condition information transferring module is deal with the information exchange of the car inside, car to car and car to road. They concern the security issues of VANETs from some aspects and provide the appropriate solving measures. To make sure the Its can be used under the security pattern.

CHAPTER 3

PRESENT WORK

3.1 Problem Formulation

The introduction of IEEE 802.11 along with advanced wireless ad-hoc networks and location-based routing algorithms makes vehicle-to-vehicle communication viable/possible. Applications for inter-vehicle communication include intelligent cruise control, lane access and emergency warning systems among others. The Vehicular systems employ wireless ad-hoc Networks and GPS to determine and maintain the inter-vehicular separation necessary to ensure the one hop and multi hop communications needed to maintain spacing between vehicles. Location based routing algorithms are flexible and efficient enough with regards inter-vehicular communication so, they form the basis of any VANET (R. A. Santos et al.). Some of location-based algorithms are Greedy Perimeter Stateless Routing (GPSR), Grid Location Service (GLS), Location Aided Routing (LAR) and Distance Routing Effect Algorithm for Mobility (DREAM). Location-Based Routing Algorithm with Cluster-Based Flooding (LORA-CBF) is an option for present and future automotive applications. A vehicle to vehicle communication for cooperative collision warning as proposed by Xue Yang et al. (2004) provides such facilities to a large extend but the wireless communication used is unreliable due to channel fading, packet collisions, and communication obstacles, can prevent messages from being correctly delivered in time.

The necessary condition for the support of message differentiation is that underlying MAC protocol should provide service differentiation among different classes of messages. The 802.11e EDCF (Enhanced Distributed Coordinated Function), an extension to IEEE 802.11 provides such a function (G. Chesson et al., 2002). In 802.11e EDCF, different levels of channel access priorities can be provided through different choices of Inter Frame Space (IFS) and contention window (CW) sizes. Corresponding to different delay requirements, three classes of messages are defined, where class 1 messages have the highest priority to be transmitted and class 3 messages have the lowest priority.

TO PROPOSE ALGORITHM TO DETECT AND ISOLATE MALICIOUS VEHICLE IN VANET

The VANET is the self-configuring type of network, in which the vehicles can move freely in the network. In such type of network, there are more chances that malicious vehicles can join the network and trigger some type of attack. Among the possible attacks Sybil attack is the most harmful attack which is possible in the network. This attack will reduce the network performance. In this work, we will work on to detect malicious vehicles in the network which is responsible to trigger such type of attacks.

3.2. OBJECTIVES:

- To analyse and study various type of routing protocols and attack in VANETs.
- To analyse the performance of AODV protocol when Sybil attack will be triggered by the malicious node in the network.
- To propose enhancement in AODV protocol to detect malicious vehicle and isolate Sybil attack from the network.
- To implement existing and proposed protocols under simulated environment and analyse network performance in terms of throughput, delay and fuel emission.

3.3. SCOPE OF STUDY:

Traffic accidents have been taking thousands of lives each year, outnumbering any deadly diseases or natural disasters. Studies show that about 60% roadway collisions could be avoided if the operator of the vehicle was provided warning at least one-half second prior to a collision. So, based on these statistic figures, researchers and scientists switch to computerize and automate the vehicular transportation system to reduce this accident rate as the human driver suffers from following problems:

- Line-of-sight limitation of the brake light: Most often, a driver can only see the brake light from the vehicle directly in front.
- Large processing/forwarding delay for emergency events: Driver reaction time typically ranges from 0.7 seconds to 1.5 seconds which results in large delay in propagating the emergency warning.

So, VANET is one of the solutions to remove these problems but that too needs a mechanism so as to avoid collision, achieve congestion control and low latency in delivering of emergency warning messages. A vehicle to vehicle communication for cooperative collision warning provides such facilities to a large extend but the wireless communication used is unreliable due to channel fading, packet collisions, and communication obstacles, can prevent messages from being correctly delivered in time. So, there are many effective protocols for V2V communication like vehicular Collision Warning Communication (VCWC) protocol to support the following application challenges:

- Stringent delay requirements immediately after the emergency.
- Differentiation of the emergency events and elimination of redundant EWMs.

Keeping in view above challenges we are trying to further improve the efficiency of VCWC protocol so that it may be able to control both, the factors which makes wireless communication unreliable and also support the above application challenges to a large extent. All the problems discussed above can be raised if some of the wrong information can be flooding in the network. The wrong information can be flooding in the network by malicious vehicles. These malicious vehicles can degrade the network performance by triggering some security attack. In this work, we will detect malicious vehicles and isolate Sybil attack from the network.

3.4 Research Methodology:

In this work, the new scheme had been proposed which will be based on to detect malicious nodes from the network which are responsible to trigger Sybil attack in the network. The Sybil attack can harm the network throughput and delay. The throughput of the network can be reduced because network resources get wasted. The delay can be raised because packets are routed to wrong destination or long paths get followed. In this work the techniques which will be proposed are based on some assumptions. These assumptions are:

1. The speed of the mobile nodes is fixed on the defined roads.
2. The RSU's are responsible to maintain the information about all vehicles.
3. The mobile nodes have to present its neighbour node information to RSU's.
4. The RSU's can maintain the neighbour node information about all the nodes.

The malicious vehicles can change its identity every time and send hello messages to RSU's for network join. The vehicles which are on the network can register itself with the server, in the registered information the unique vehicle number and its identification number will be defined. This registered information can be available on all RSU's. When any join the network, is have to send hello message to RSU and then RSU ask nodes for their identification number. When the identification number will be successfully verified the RSU gather all the information about neighbouring or adjacent nodes of the registered nodes. The RSU will also define the speed limit of the vehicle on the road for which it is registered. When any malicious node will can its identity can send hello message to RSU, the RSU will register the malicious node but when RSU checks the adjacent node and that are different from the legitimate node. The malicious node can be detected from the network. To verify the detection process, the RSU's will flood the monitor mode messages in the network , and adjacent nodes of the malicious nodes can start monitoring the malicious nodes and detect that it is the malicious nodes

Algorithm:

Input: Road side units, smart cars, malicious car

Output: Detection of Malicious car

Set registration process
{
Cars send its credentials to road side units
If (stored credentials == send credentials)
{
Assign identification number;
Else
{
Repeat step of registration
}
If (Identification== assigned)
{
Communication starts between cars
Road side units start gathering information about neighbours
If (Neighbour information on each road side units == same)
{
No malicious node exits in the network;
Else
{
Road side units flood ICMP messages in the network
Monitoring process= true
If (malicious car== detected)
{
Isolate malicious car with identification number
Else
Repeat process of monitoring
}

End

3.3.1 Flow Chart:

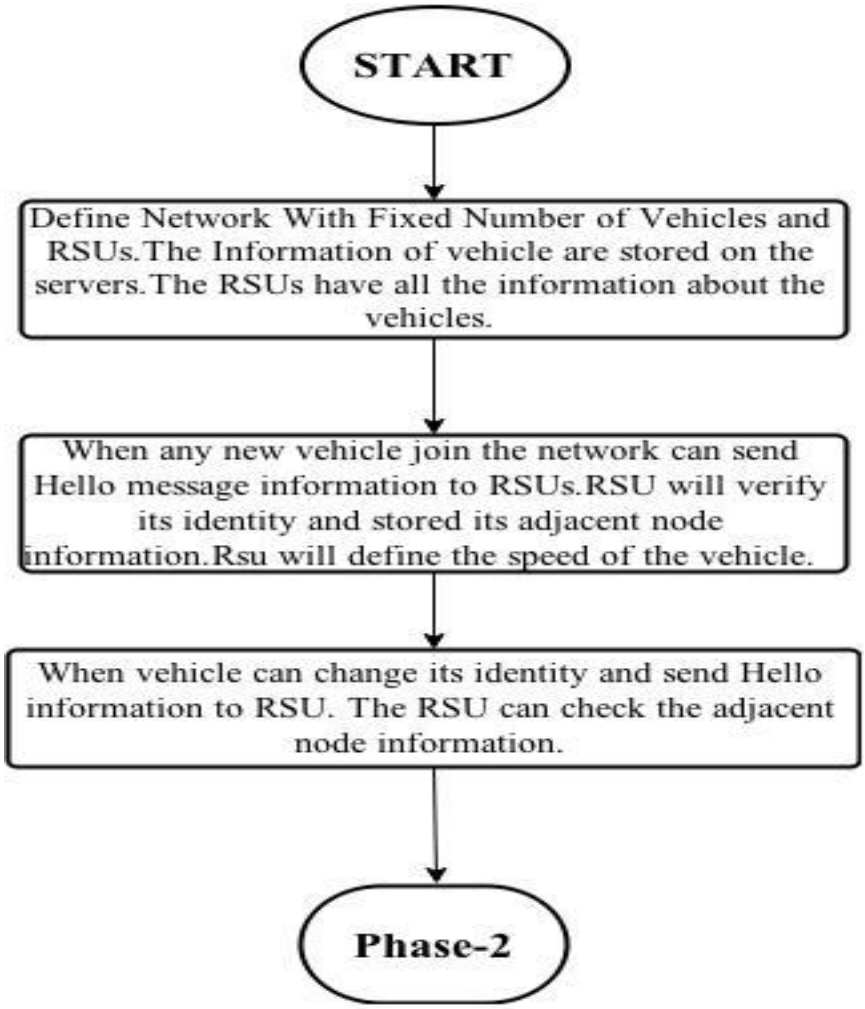


Figure 13 : Phase 1

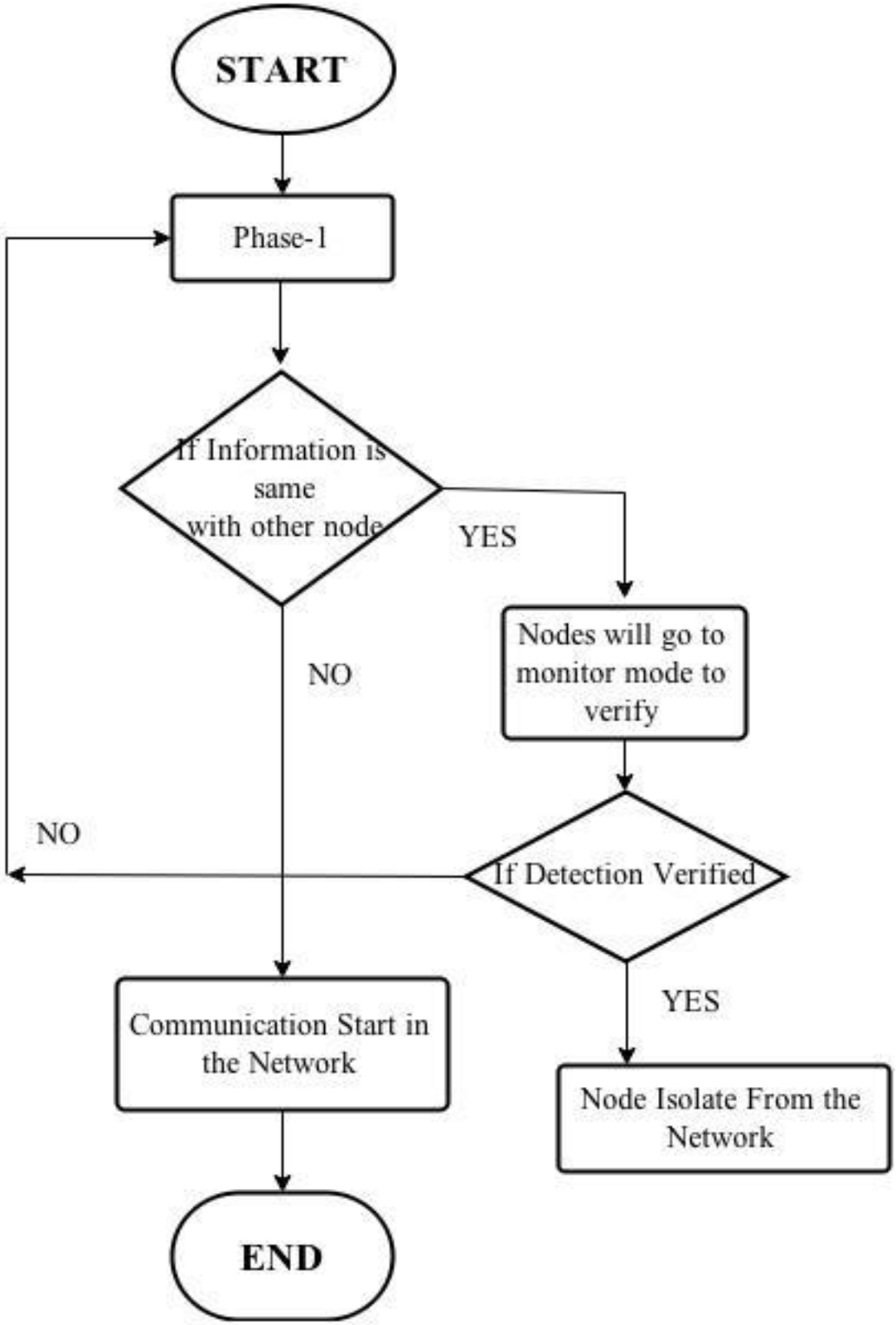


Figure 14 : Phase 2

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Simulation Environment

NS2 Overview: NS-2 is an open-source simulation tool running on Unix-like operating systems. It is a discreet event simulator targeted at networking research and provides substantial support for simulation of routing, multicast protocols and IP protocols, such as UDP, TCP, RTP and SRM over wired, wireless and satellite networks. It has many advantages that make it a useful tool, such as support for multiple protocols and the capability of graphically detailing network traffic. Additionally, NS-2 supports several algorithms in routing and queuing. LAN routing and broadcasts are part of routing algorithms. Queuing algorithm includes fair queuing, deficit round robin and FIFO. NS-2 started as a variant of the REAL network simulator in 1989. REAL is a network simulator originally intended for studying the dynamic behaviour of flow and congestion control schemes in packet-switched data networks. In 1995 ns development was supported by Defence Advanced Research Projects Agency DARPA through the VINT project at LBL, Xerox PARC, UCB, and USC/ISI. The wireless codes from the UCB Daedalus and CMU Monarch projects and Sun Microsystems have added the wireless capabilities to ns-2.

Depending on user's requirement the simulation are stored in trace files, which can be fed as input for analysis by different component:

- A NAM trace file (.nam) is used for the ns animator to produce the simulated environment.
- A trace file (.tr) is used to generate the graphical results with the help of a component called X Graph.

- **Number of nodes:** This parameter in the above table is used to represent number of nodes that are used for conducting the simulation.
- **Pause time**: this parameter represents the time interval for which the nodes can be paused in the network during simulation.

- **Traffic type:** Network traffic can be of two types viz. Variable Bit Rate (VBR) and Constant Bit Rate (CBR). The CBR traffic can suffer a maximum delay of T.
- **Simulation time**: Simulation time is the duration of time for which the simulation is carried out.

Table 1 : Simulation Parameter

Parameter	Value
Terrain Area	800 m x 800 m
Simulation Time	50 s
MAC Type	802.11
Application Traffic	CBR
Routing Protocol	AODV
Data Payload	512 Bytes/Packet
Pause Time	2.0 s
Number of Nodes	32
Number of Sources	1
No. of Adversaries	1

4.1.1 NS2

The network simulator NS is a discrete event network simulator developed at UC Berkeley that focuses on the simulation of IP networks on the packet level.

The NS project (the project that drives the development of NS) is now part of the Virtual InterNetwork Testbed (VINT) project that develops tools for network simulation research.

Researchers have used NS to develop and investigate protocols such as TCP and UDP, router queuing policies (RED, ECN, CBQ), Multicast transport, Multimedia and more.

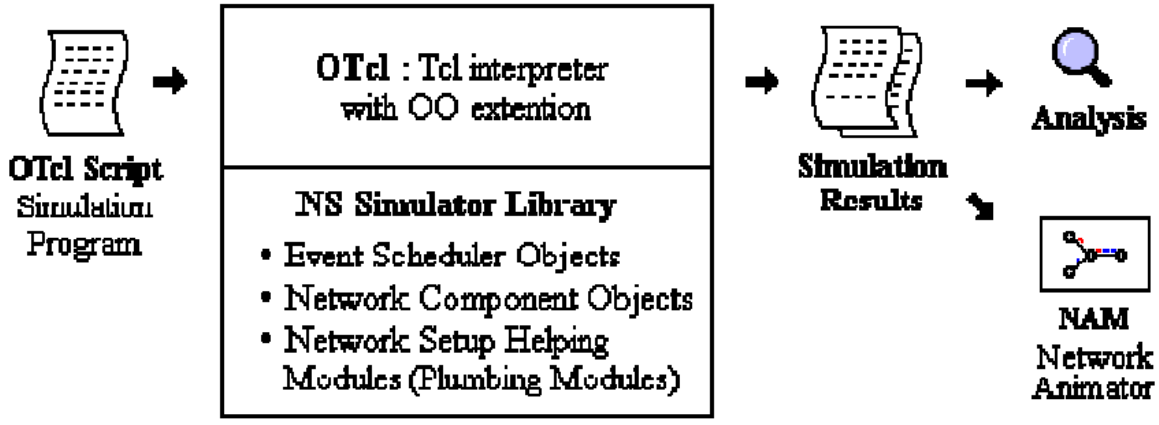


Figure 15 : Simplified user view of NS

NS is basically an Object-oriented Tcl (Otcl) script interpreter with network simulation object libraries. NS has a simulation event scheduler, network component object libraries and network setup (plumbing) module libraries (Fig 15).To use NS for setting up and running a network simulation, a user writes a simulation program in Otcl script language. Such an OTcl script initiates an event scheduler, sets up the network topology and tells traffic sources when to start and stop transmitting packets through the event scheduler.

The NS-2 architecture is composed of five parts:

- Event scheduler
- Network components
- Tclcl
- OTcl library
- Tcl 8.0 script language

Figure 16 shows a graphical overview of the NS-2 architecture. According to [3] “a user can be thought of standing at the left bottom corner, designing and running simulations in Tcl using the simulator objects in the OTcl library.” The event schedulers and most of the network components are implemented in C++ because of efficiency reasons. These are available to OTcl through an OTcl linkage that is implemented using tclcl. These five

components together make up NS, which is an object-oriented extended Tcl interpreter with network simulator libraries.

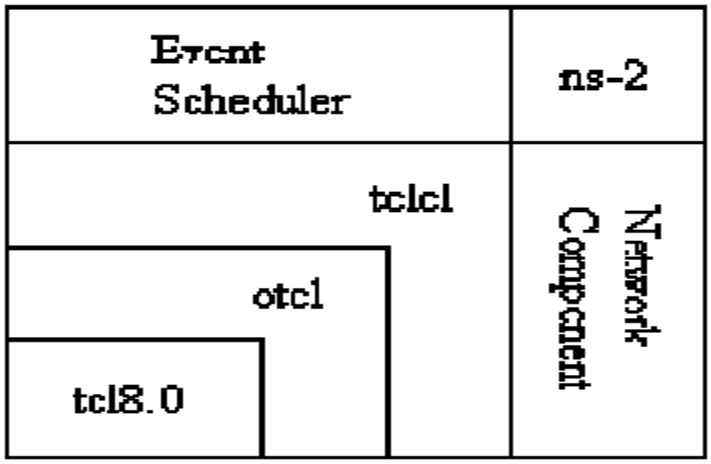


Figure 16 : Architectural view of NS2

4.1.2 Network Animation (NAM) Trace

NAM trace records simulation detail in a text file and uses the text file to play back the simulation using animation. NAM trace is activated by the command "$nsnamtrace-all $file," where "ns" is the Simulator handle and "file" is a handle associated with the file (e.g., "out.nam" which we create in any prog.) which stores the NAM trace information. After obtaining a NAM trace file, the animation can be initiated directly at the command prompt through the following command:

>> nam filename.nam >> nam filename.nam

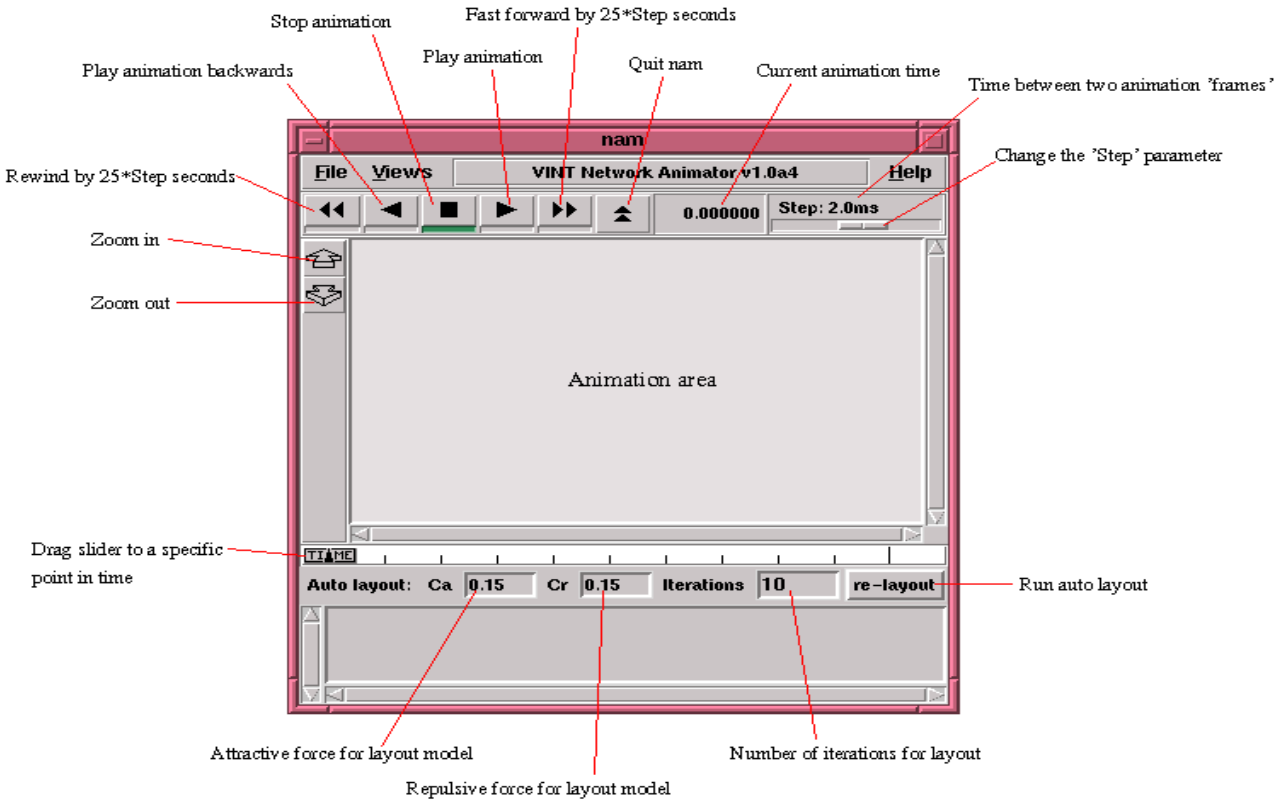
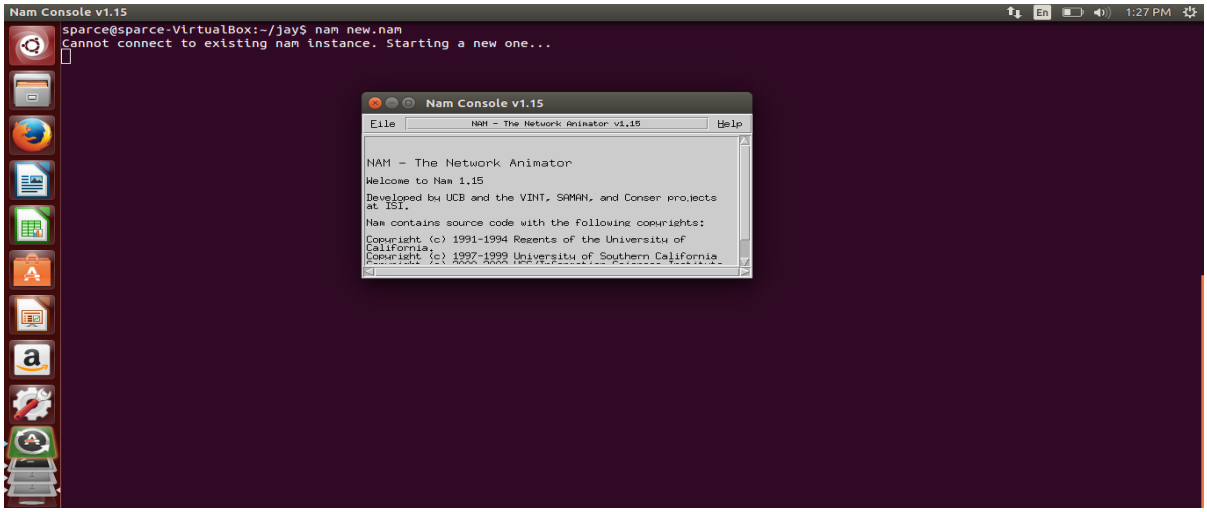


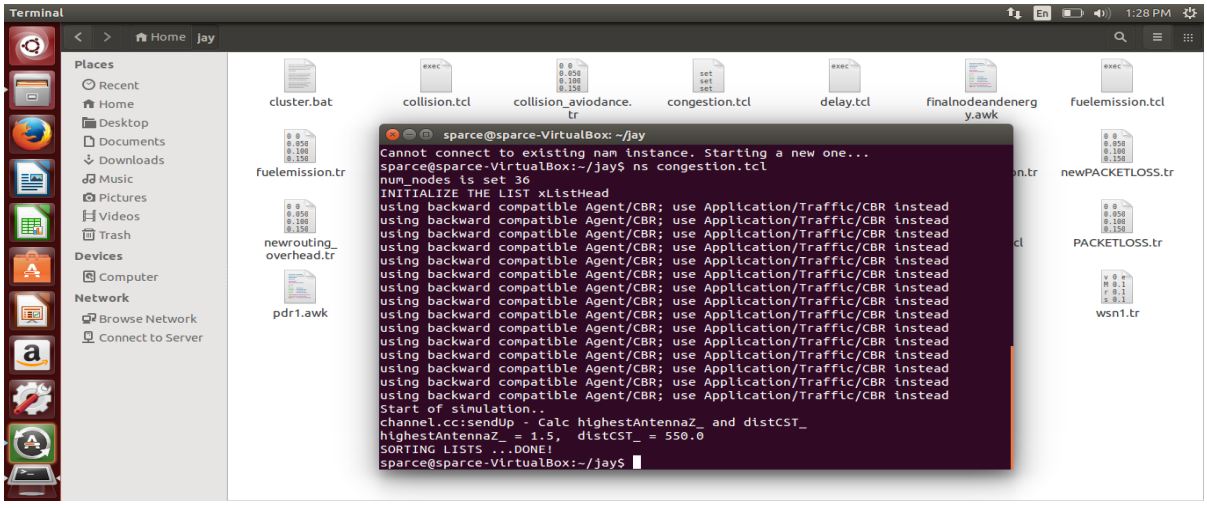
Figure 17 : NAM Space

4.2 Initialization of Network Deployment

The simulation for the projected method has been carried using network animator and the operating system used is Ubuntu.our Simulation is conducted within the network Simulator(NS) 2.35 environment on platform with GCC 4.3.4 and Ubuntu 14.04.1 shows in fig: 24. In NS 2.35. We make configuration with 32 nodes and flat grid size of 800x800m.Simulation is made with use of AODV routing. We generate the result in NS-2 with use of reference node technique.



(A)



(B)

Figure 18 : (A) Calling to Nam Space (B) Execution Tcl Script

As shown in Figure 18, Which normally run the nam for ns2 interface and another which show the execution of tcl file.

4.2.1 AODV Routing with Sybil Attack

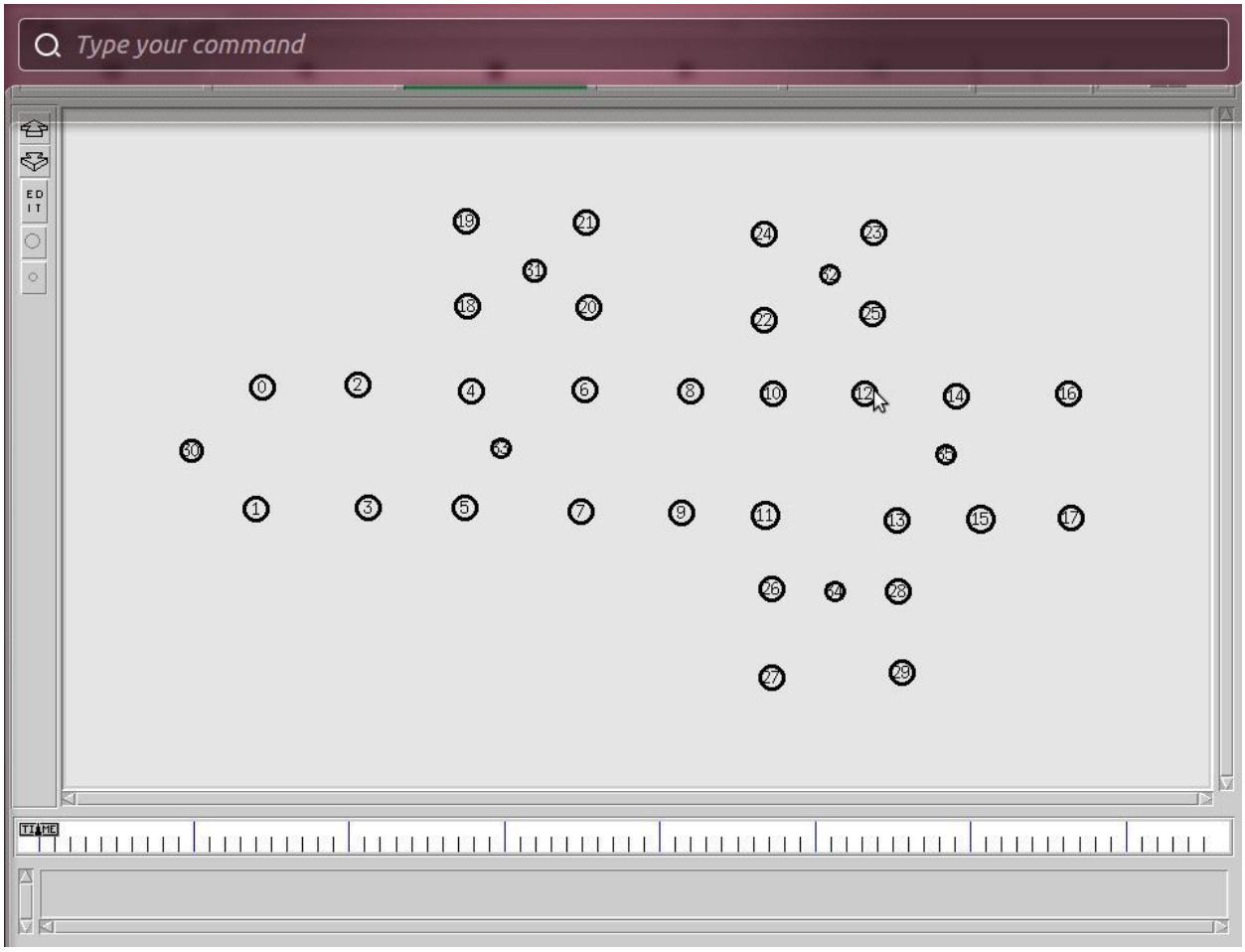


Figure 19 : Network deployment

As illustrated in figure 19, the vehicular adhoc network is deployed with fixed number of road side sensor nodes and fixed number of vehicles which moves freely on the roads .The communication done using AODV routing protocol.

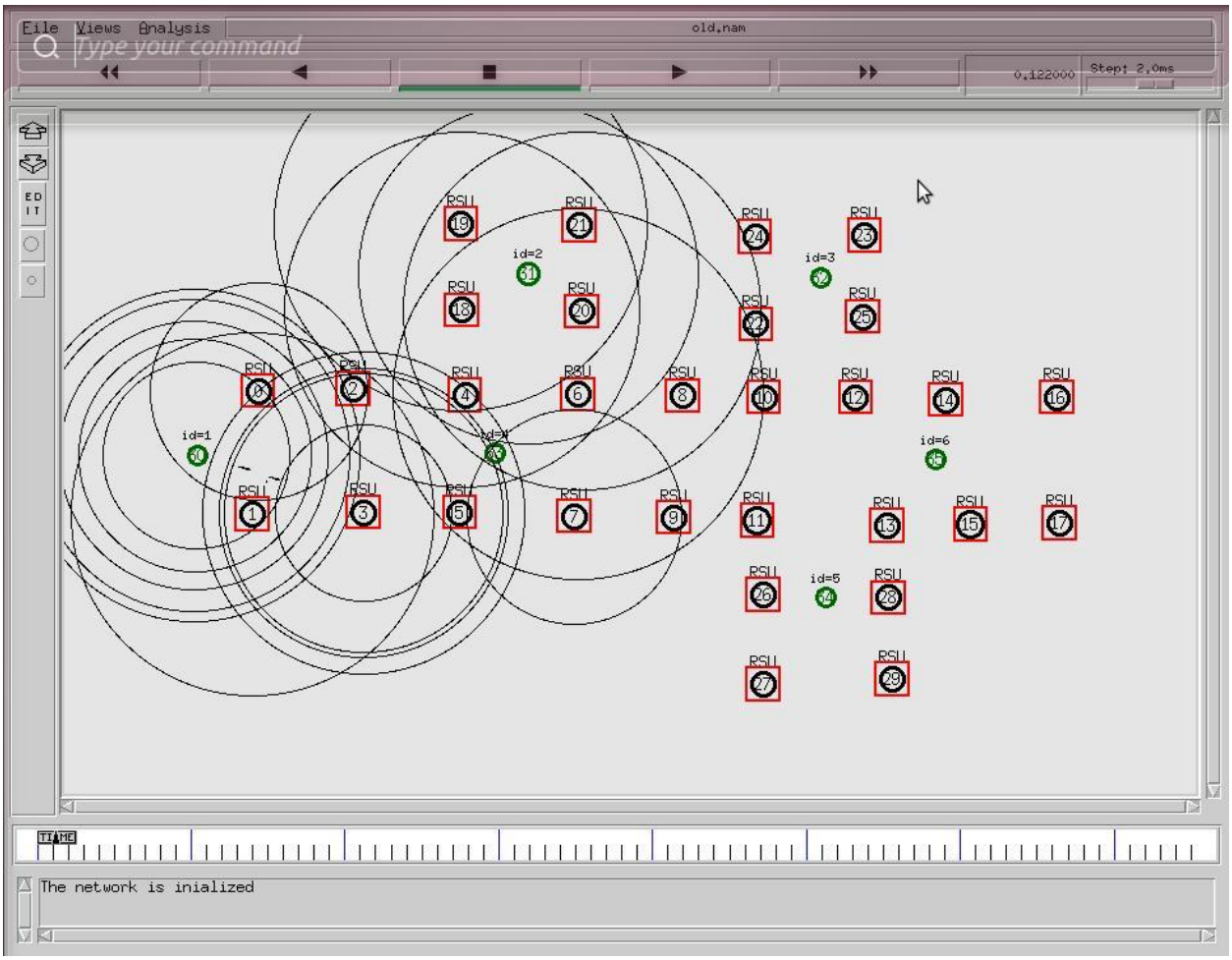


Figure 20 : Communication between cars

As shown in figure 19, the network is deployed with the finite number of road side sensor and smart cars, the smart cars are moving on the roads. To move freely on the roads the each smart car had identification number which it gets at the time of registration .After this identification number is used for further communication.

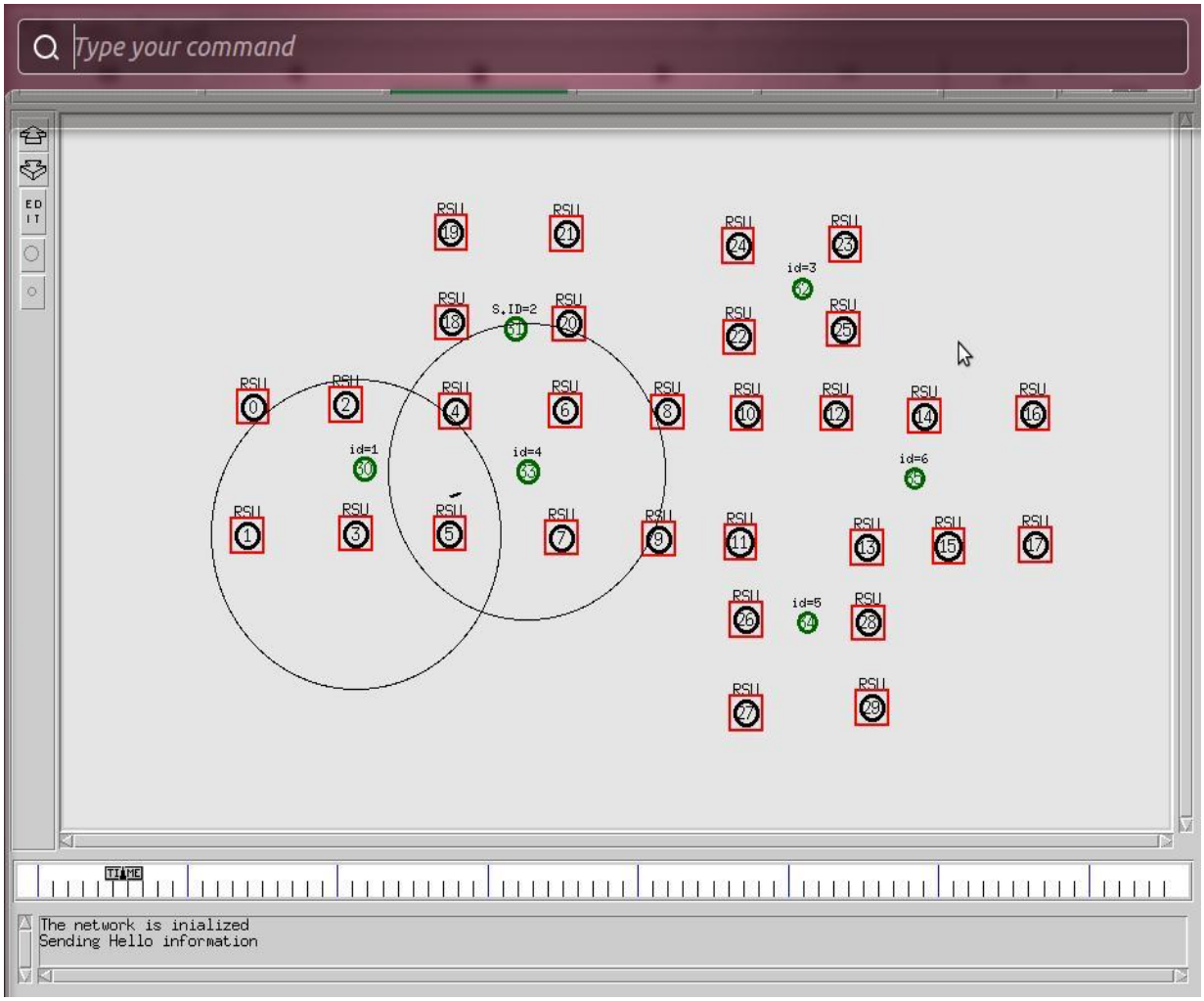


Figure 21 : Registration process of new car

As illustrated in figure 20, the cars are communicating with each other like the car with identification number of 1 is communicating with car with registration number of 4. The new car is entering in the network and sending registration request to new road side units for registration.

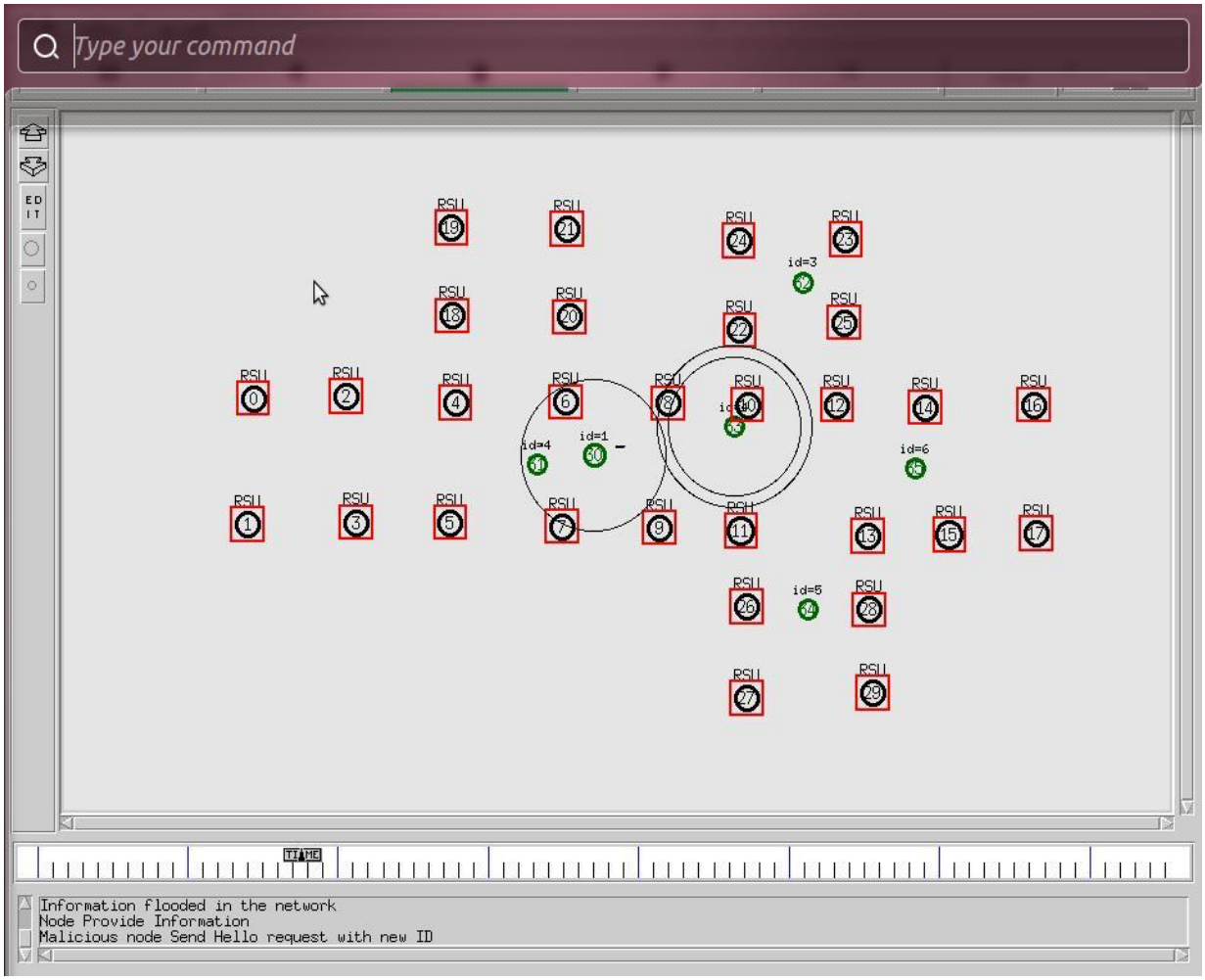


Figure 22 : Allocation of new identification

As shown in figure 21, the car which is entering in the network and it need to register with the road side unit to get its registration number. The new car get its registration identify of 4 which after can communicate with any vehicle or RSU unit using AODV protocol.

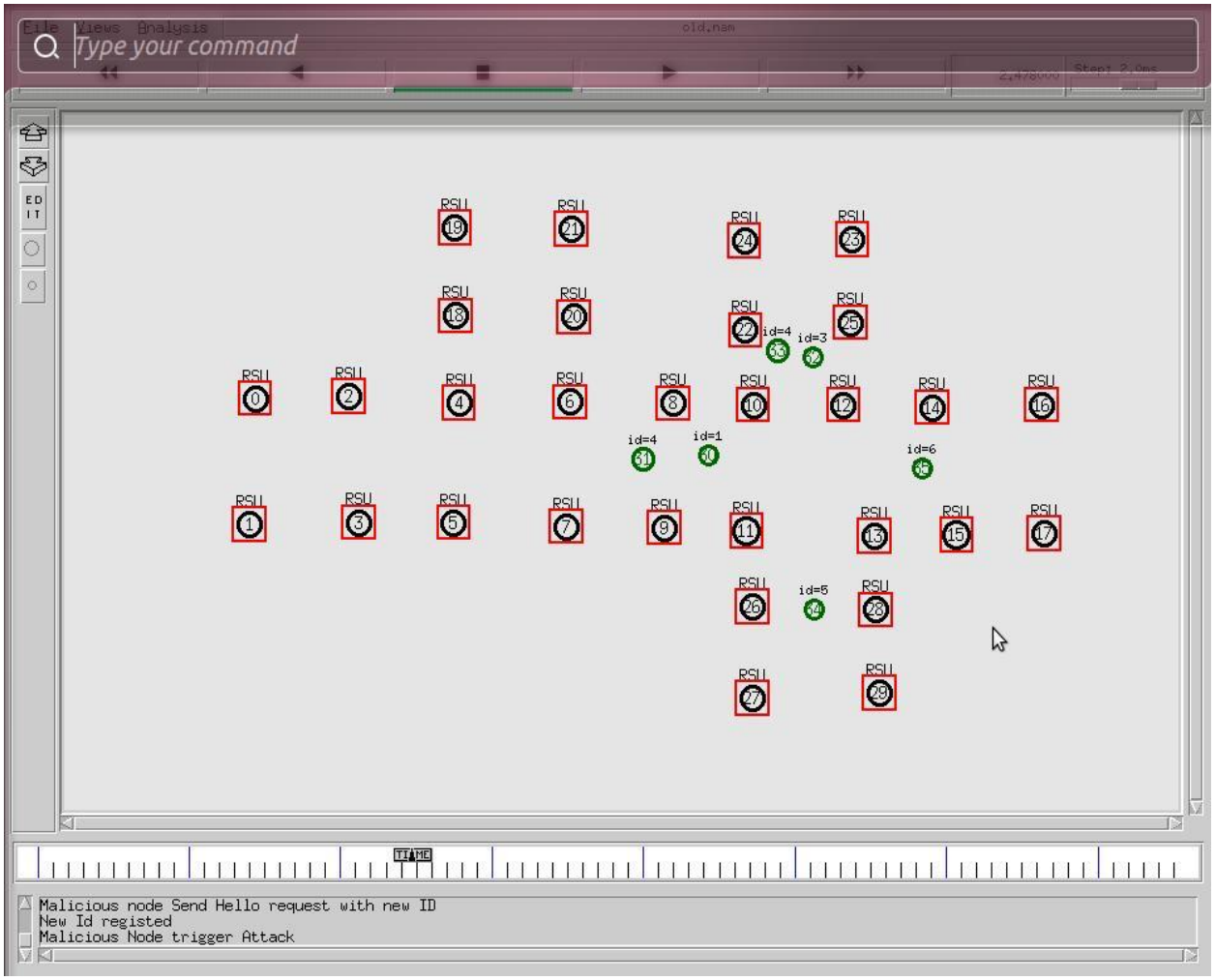


Figure 23 : Communication between cars

As illustrated in the figure22, the car with identification number of 1 is communication with the car of registration number of 4. The malicious node changes its identification from identification number of 2 to identification 4 and node 4 is called as Sybil node. The malicious node can now send request to communicate with id of Sybil node.

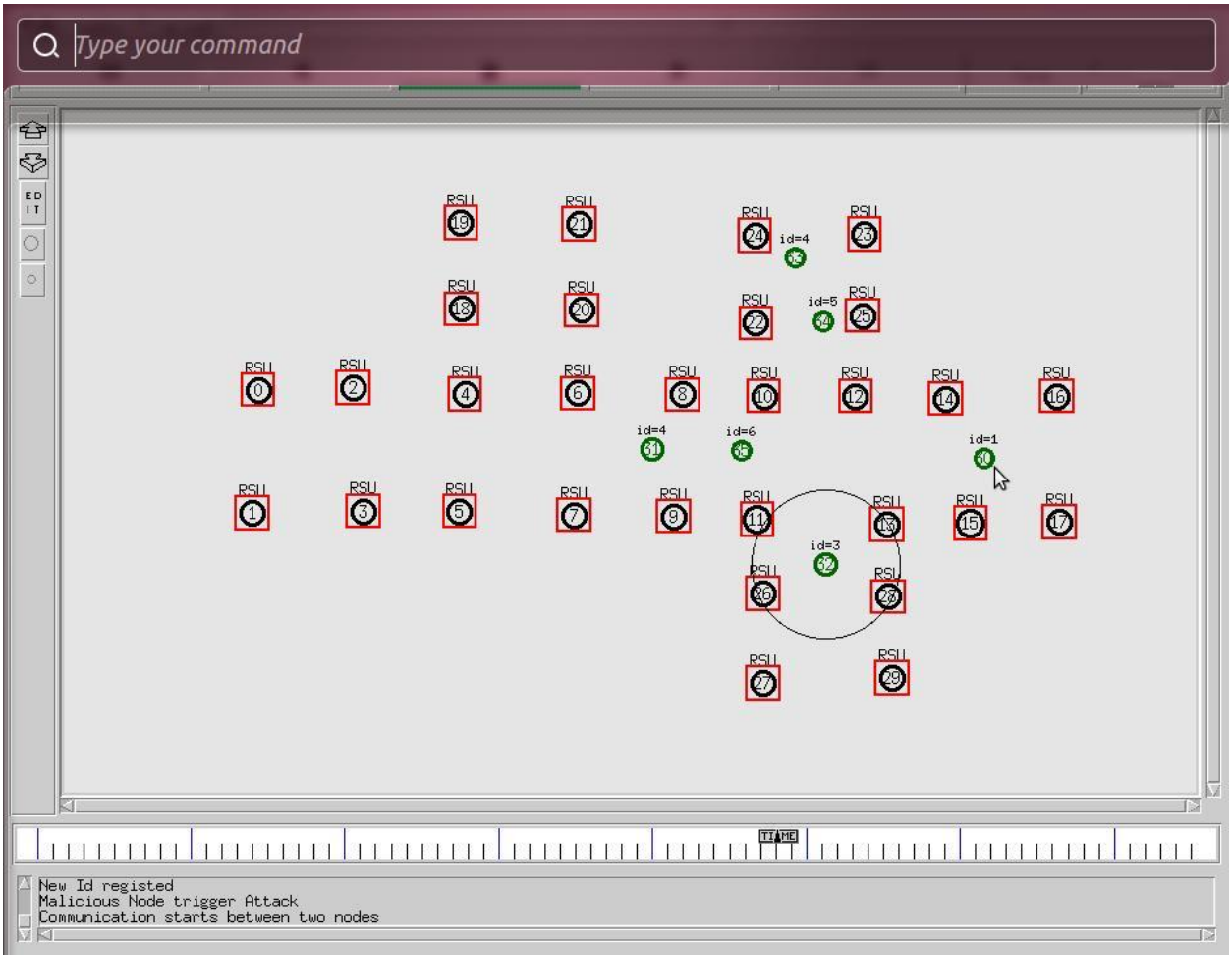


Figure 24 : Attack Triggered

As shown in figure 23, the malicious node changes its identification from 2 to 4. The malicious nodes had less distance from the legitimate node. The source node start sending data to malicious nodes and Sybil attack had been triggered in the network .And this way malicious node change identity and trigger the attack in the network.

4.2.2 Proposed Technique with Detect and Isolate Sybil Attack

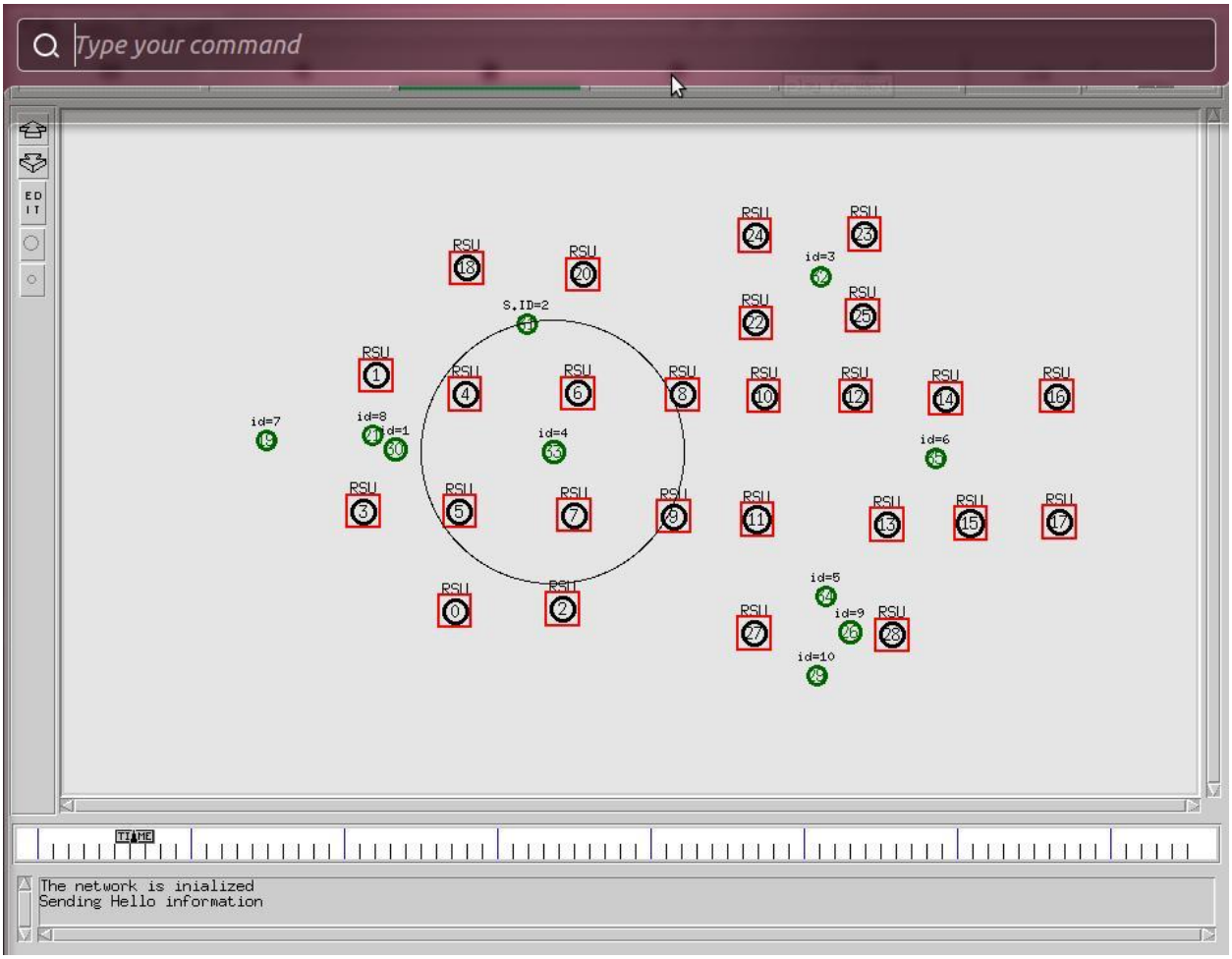


Figure 25 : Network Deployment

As illustrated in the figure 24, the network is deployment with the finite number of sensor nodes and finite number of smart cars. The smart cars can freely move on the roads and vehicle to vehicle communication and vehicle to road side communication is available.

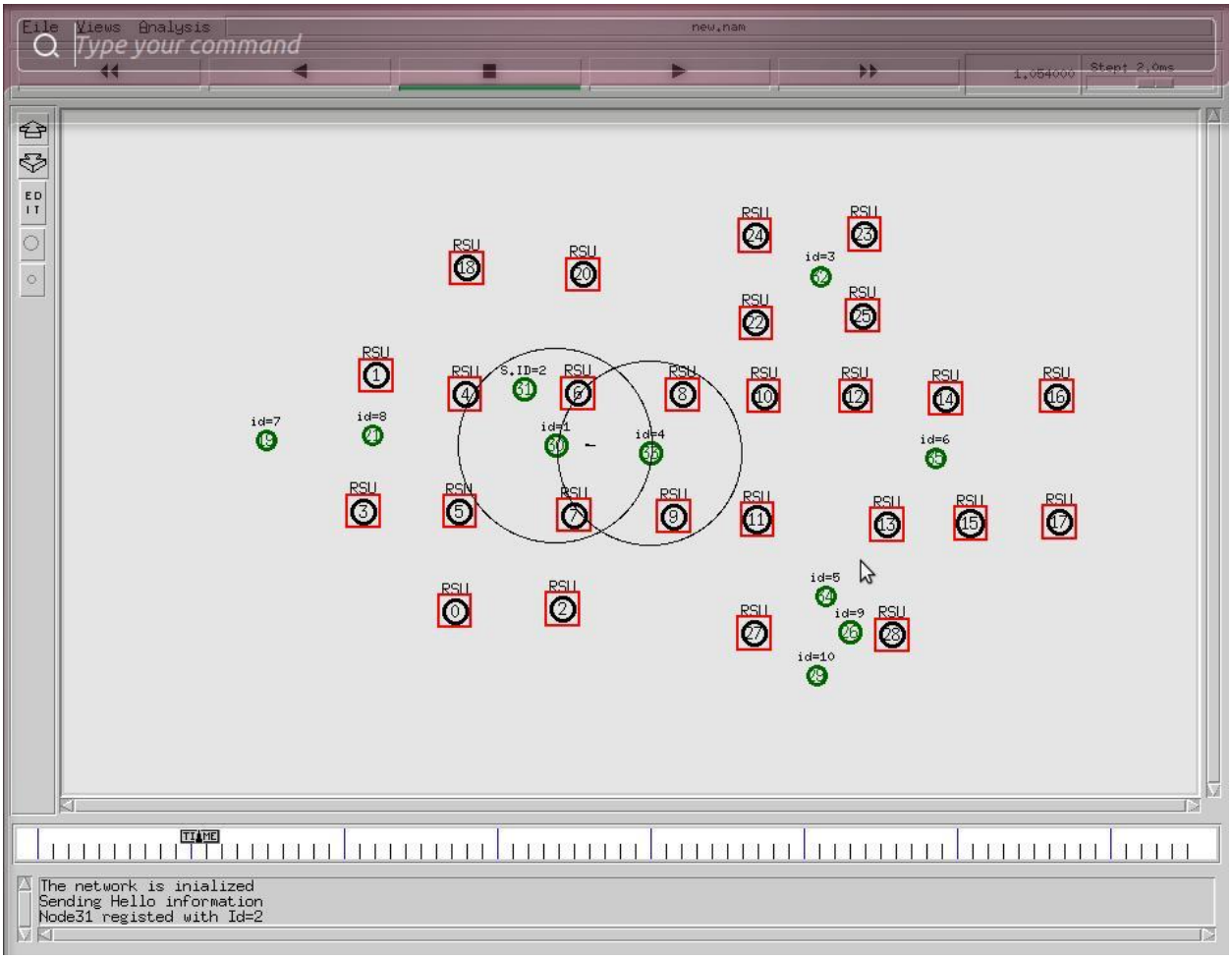


Figure 26 : Communication starts

As illustrated in the figure 25, The network is deployment and in the network vehicle to vehicle is possible. In the figure cars with the identification number of 1 start communicating with identification number of 4 using AODV protocol.

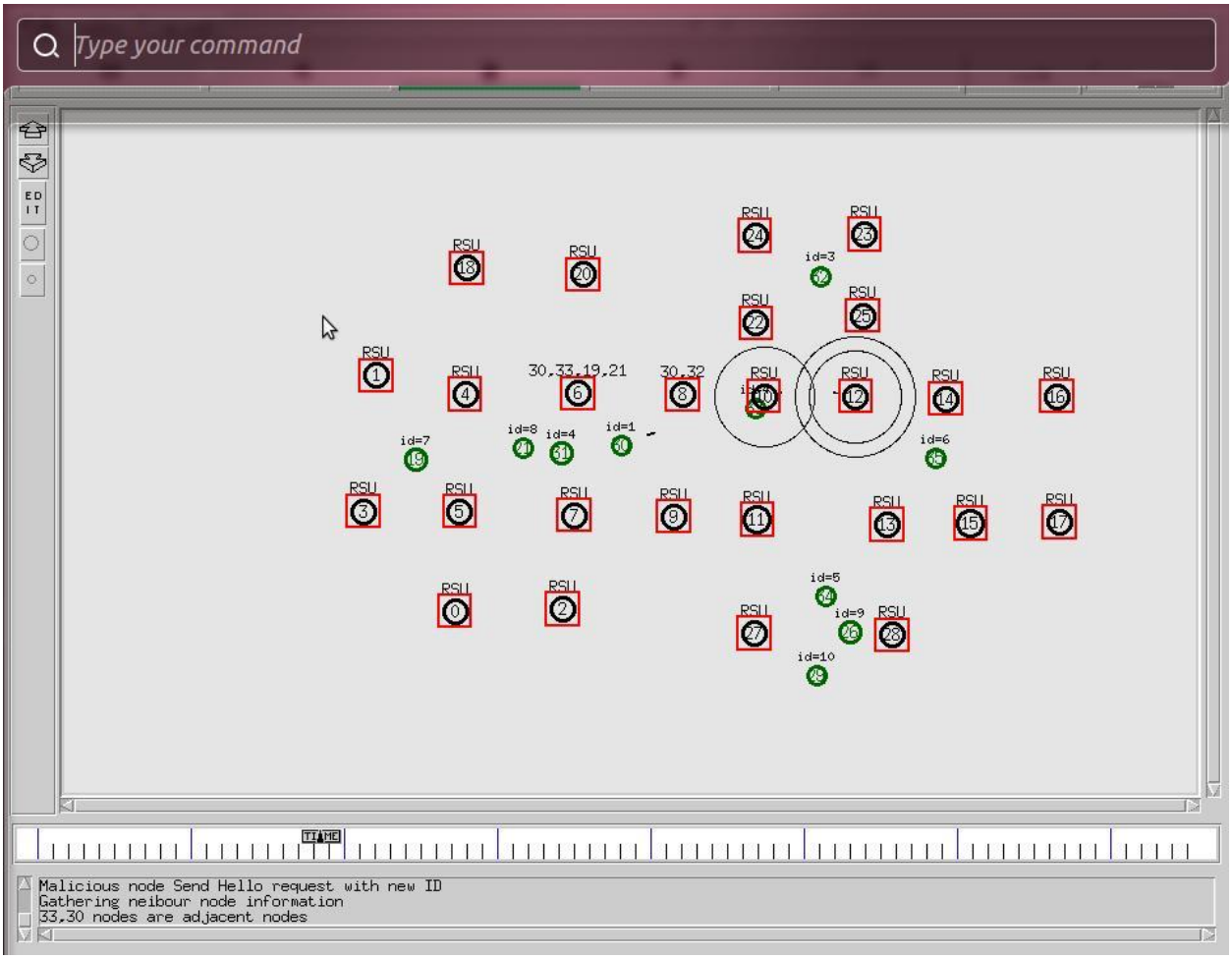


Figure 27 : Getting neighbour information

As shown in the figure 26, the malicious node can change its identification number and register with the identification number 4. The two legitimate cars are communicating with each other like car 1 and car 4. The road side unit's cars gathering the information of neighbours of each car. As in the network two cars of id 4 exits, the neighbours of are different. It means that some malicious nodes can exist in the network.

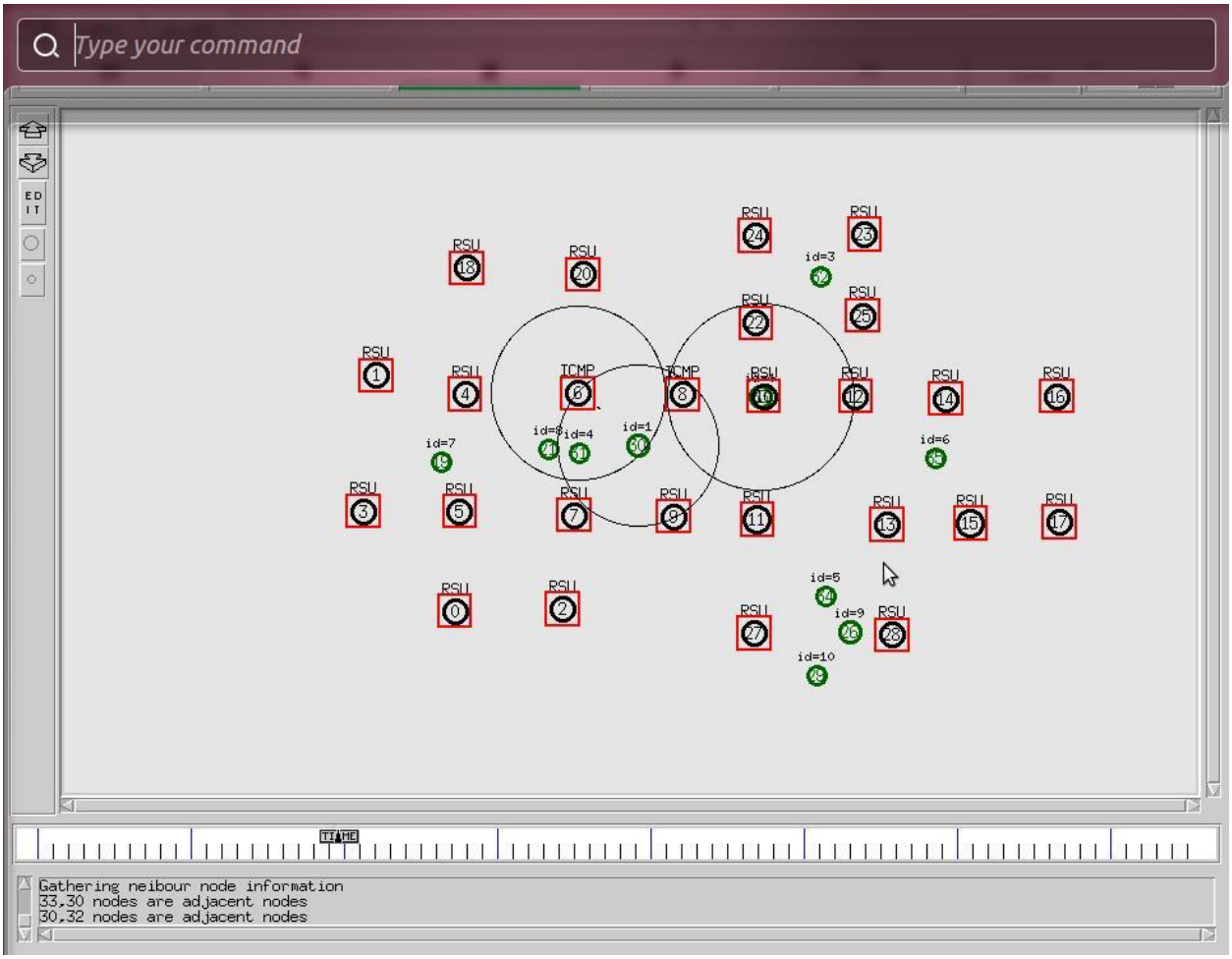


Figure 28 : Flooding of ICMP packets

As illustrated in the figure 27, the neighbours of car with identification number 4, is different. To detect the malicious cars from the network, the road side units start flooding the ICMP messages. When the cars receive ICMP messages, it will start monitoring its adjacent nodes.

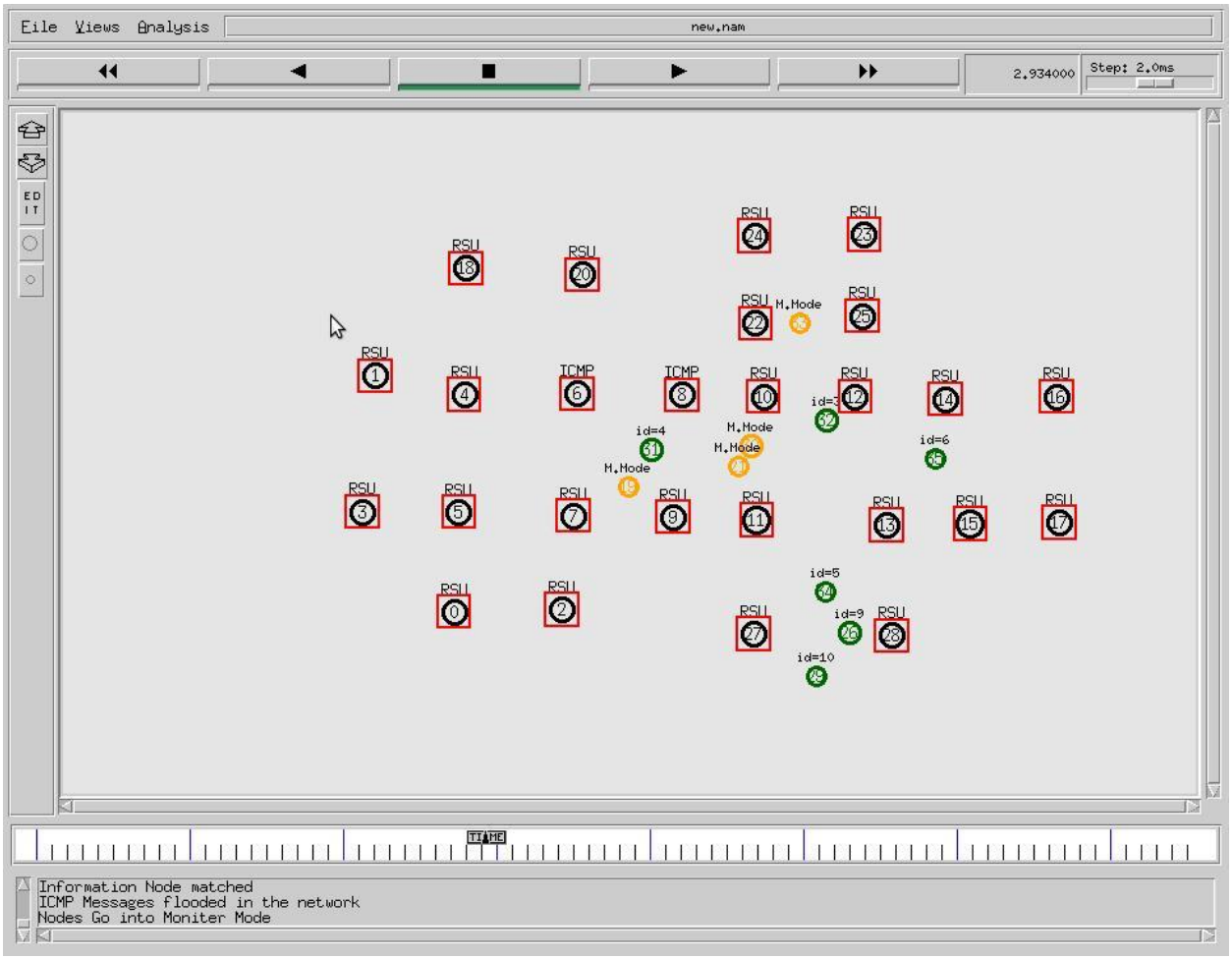


Figure 29 : The monitoring of adjacent nodes

As shown in the figure 28, The road side units start flooding the ICMP messages in the networks. The nodes when receive ICMP messages, it will start monitoring its adjacent nodes as shown in above figure with yellow colour.

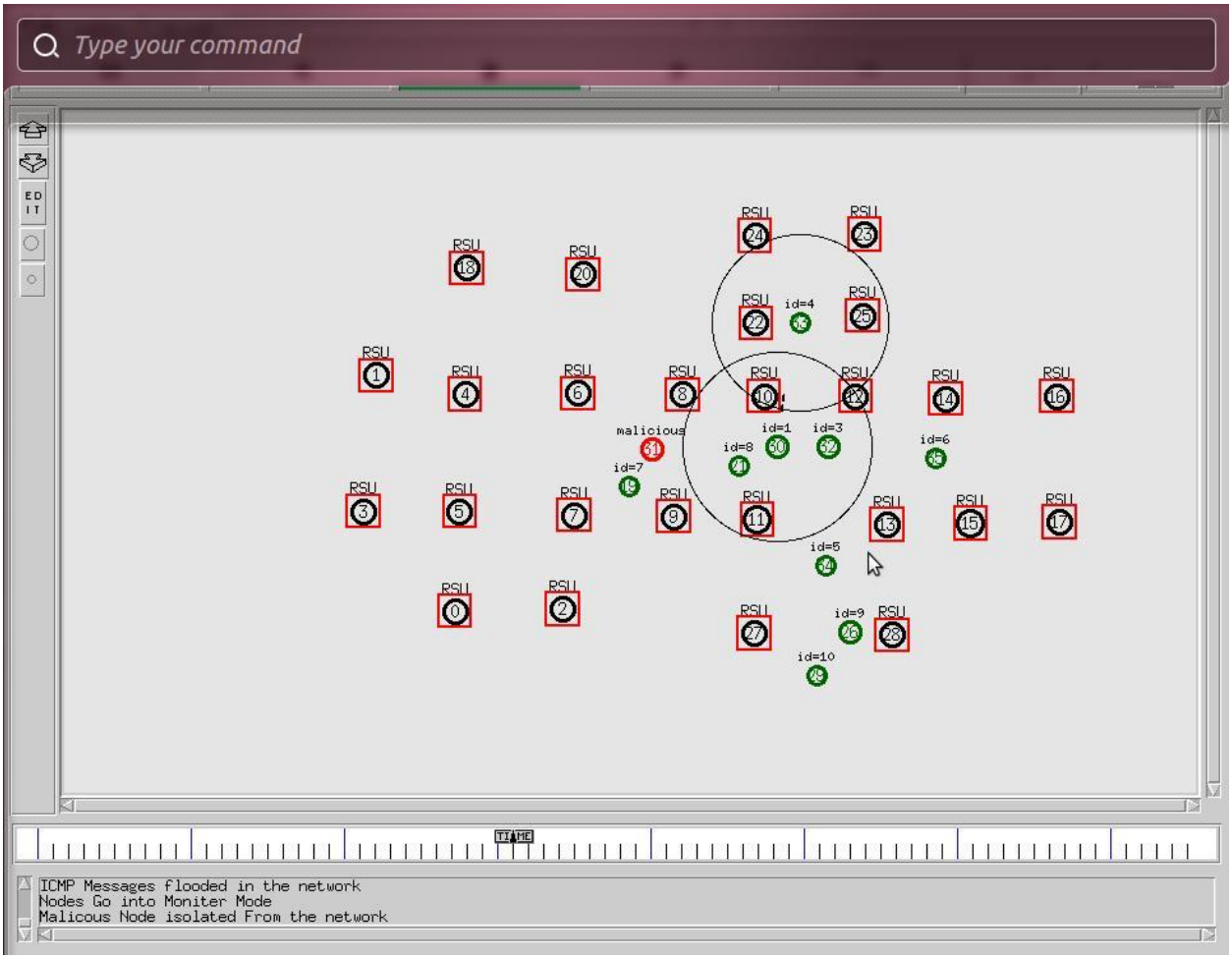


Figure 30 : Detection of malicious nodes

As shown in the figure 28, When the road side units came to know that some malicious nodes exits in the network, the road side units flood ICMP messages in the network. The cars in the network receive ICMP messages and start monitoring its adjacent nodes. From the monitoring, the malicious nodes are detected in the network and its isolate from network.

4.3 GRAPHS

The graphs are used to signify the variation in throughput and delay using the proposed method. Green line characterizes the change in case of the new scenario and red colour represents the conventional method. These two parameters are a widely used for validating the confirming the use of particular methods. Throughput can be defined as the number of packet data received per unit time whereas end-to-end delay defined as the time taken between sending of a packet and its receiving on the destination.

4.3.1 End-to-End Delay

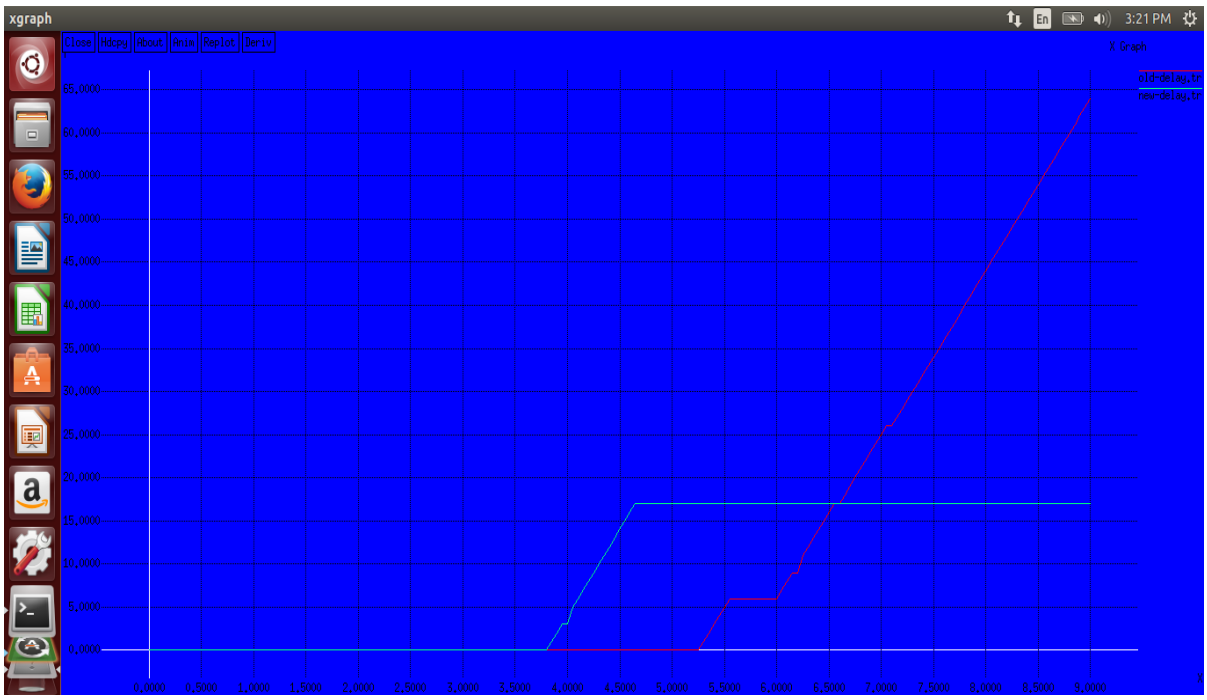


Figure 31 : End-to-End Delay

X-axis = Simulation Time Y-axis = delay in time

Figure shows the delay after deployment of the proposed method. It shows that our proposed method schema reduce delay while packet is going to transmit from source to destination. IN the previous schema, the delay starts linearly increasing when there is presence of malicious node in the path mark as red line whereas in absence of malicious node delay first decrease but the new path deploy because of malicious activity it will be not as much shortest the

previous so at some point of time the peak of the graph increase and decrease because of delay which mark as green line in graph.

4.3.2 Throughput

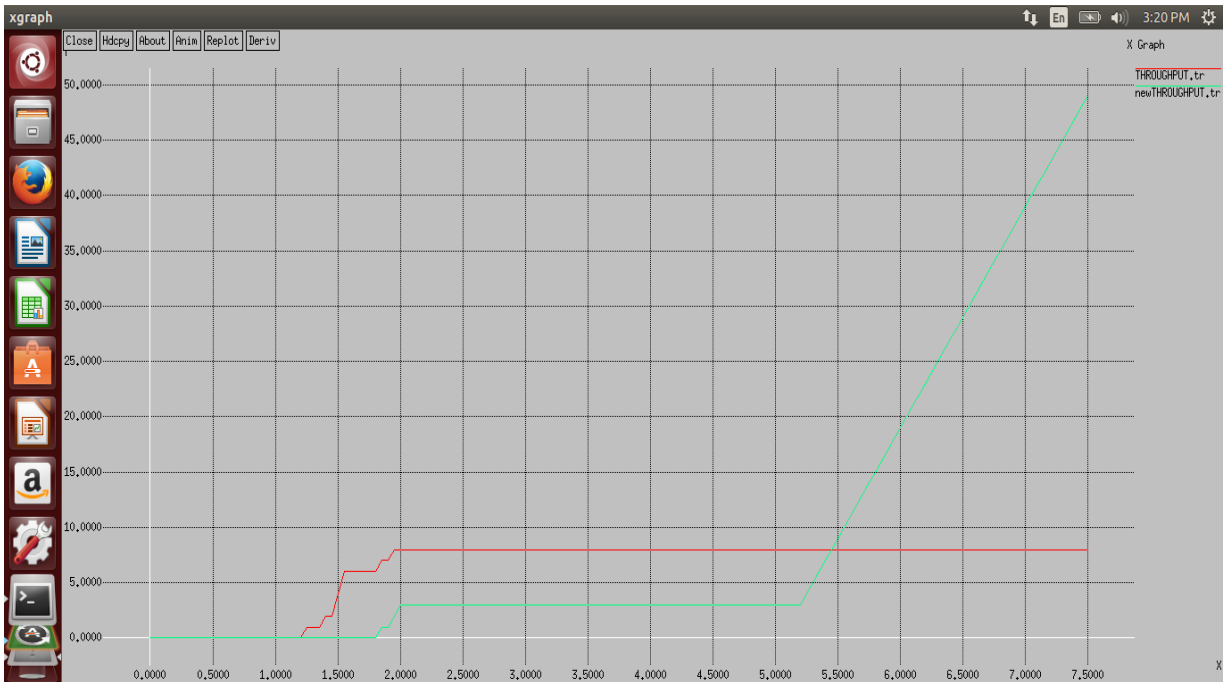


Figure 32 : Throughput

X-axis = Simulation Time

Y-axis = Number of packets received at destination

Figure 30 represents the average throughput after applying proposed method. As the delay in the network is minimum because of isolation of malicious node, so throughput of the network is linearly increase after some point of time. From graph we can see that when number of packet increase throughput is gradually increase with time in our proposed schema shown by green line. While red line represents previous schema when the malicious node present in the network at that time packet continuous drop so the line is constant for some period of time.

Calculating the Throughput of the system, we have used the following formula:

Throughput = Packet received * 8/ Amount of packet forwarded (over some point of time).

4.3.3 Routing Overhead

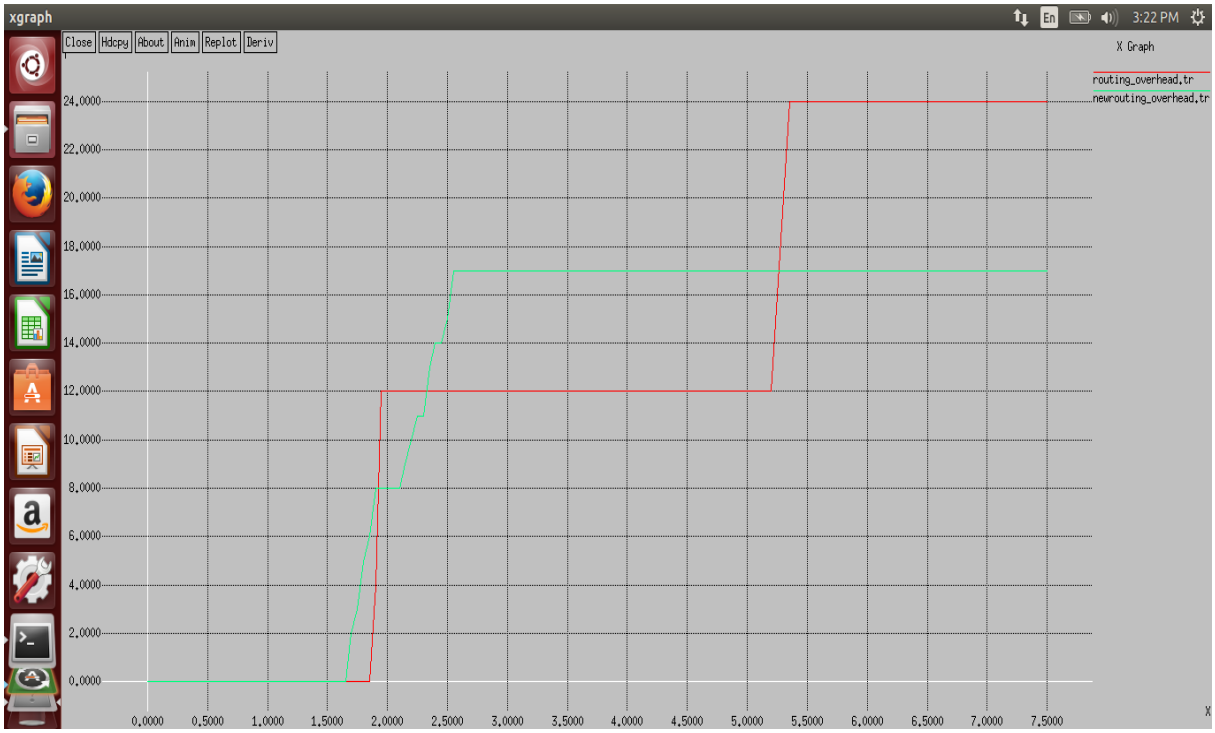


Figure 33 : Routing Overhead

X-axis = Simulation Time

Y-axis = Routing Overhead

In the network nodes often change their location within network. so, some stale routes are generated in the routing table which leads to unnecessary routing overhead. The malicious nodes can routing with Sybil node so routing overhead increase as shown in figure with red line. After detecting malicious node routing overhead decrease as shown in figure with green line.

4.3.4 Packet Loss

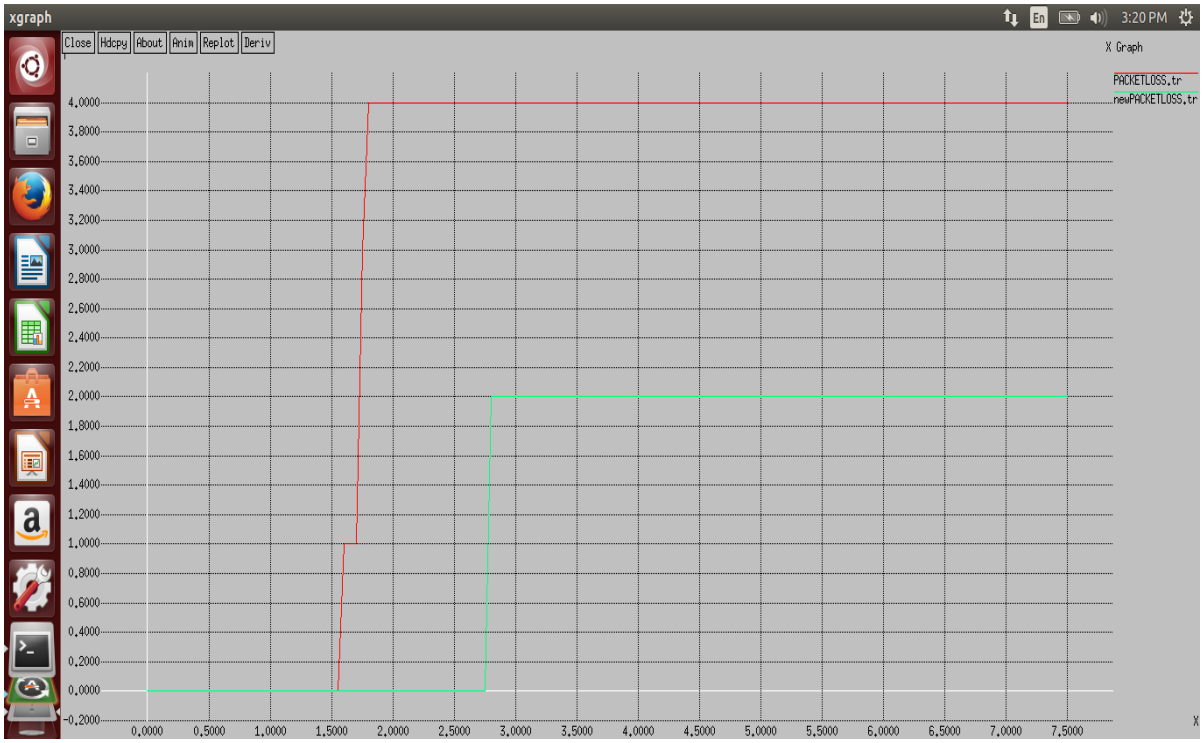


Figure 34 : Packet loss

X-axis = Simulation Time

Y-axis = Packets lost

As we have applied the ICMP and monitoring node for setting up to detect malicious node in the network. So after detect the malicious node packet loss is less as compared to the previous scenario. We make the channel secure so final result comes is maximization of throughput and minimization of packet loss. In figure 32, we see that the red line is continuously increase because of dropping of the packet and green line constant after some time because of securing of channel.

4.3.5 Fuel Emission

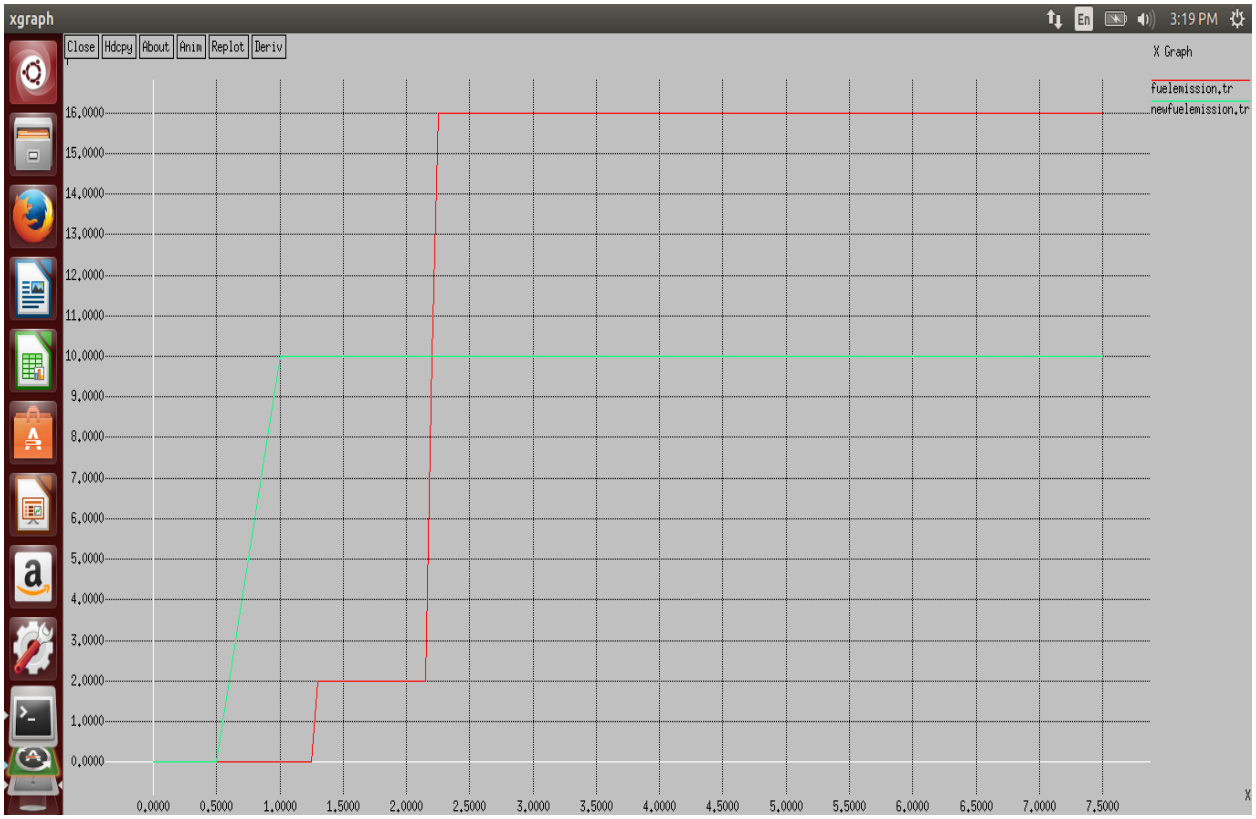


Figure 35 : Fuel Emission

X-axis = Simulation Time

Y-axis = Fuel Emission

Fuel emission basically how much fuel are emitted or use in vehicle. As shown above figure when malicious vehicle is present that time fuel emission are more because of every time changing id and send for communication which shown by red line. After Detect malicious vehicle using proposed method fuel emission are decrease as shown with green line.

CHAPTER 5

CONCLUSION AND FUTURE WORK

Vehicular ad-hoc network have been wast area of research work from past few years because it's widely used application in battlefield and business purpose. Due to openness and dynamic topology network is vulnerable from attacker. In this paper we have discuss VANET protocol, its characteristics and attack which trigger on it. We have discussed various techniques to isolate and detect Sybil attack which degrade the system performance by decreasing throughput, increasing latency and delay. In our feature work we proposed new algorithm based on monitor node technique to which improves network efficiency. The proposed technique increases the throughput, fuel emission and delay which based on monitoring method with ICMP message. Simulation show that monitor node technique easily detecting the misbehaving node and increasing the throughput.

In future work will work with more parameter and cooperative detection of node and add the more encryption schema to make channel secure. Even we will detect malicious node in the time of registration.

REFERENCES

[1] Hugo Conceicao (2008) “Large-Scale Simulation of V2V Environments", SAC’08 March 16-20,Fortaleza, Cear´ a, Brazil, pp 28-33.

[2] Stephan Olariu (2009) "An Architecture for Traffic Incident Detection ", MoMM, Kuala Lumpur, Malaysia, December 14–16.

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

[4] Maxim and jean-Pierre Hubaux (2005) “The security of vehicular ad hoc networks”,ACM,pp 11-21.

[5] Sumaiya Iqbal (2009) "Vehicular Communication: Protocol Design, Testbed Implementation and Performance Analysis", IWCMC’09, Leipzig, Germany, June 21-24, pp 410-415.

[6] A. AHMAD (2010) "Hybrid Multi-Channel Multi-hop MAC in VANETs ", MoMM2010, 8–10 November, Paris, France, pp 353-357.

[7] Rakesh Kumar, Mayank India (2012) “ A Comparative Study of Various Routing Protocols in VANET”,IJCA Journal, pp 1-12.

[8] Josiane Nzouonta et al (2008) “ Routing on City Roads using Real-Time Vehicular Traffic information “, p-18.

[9] Salim M.Zaki, M.A.ngadi,Maznah Kamat (2009),” A location based routing prediction service protocol for vanet environment”, IEEE, pp 15-23.

[10] Reena Didcach (2012)“ Mobility simulation of Reactive protocol for Vanet”, IEEE, pp 124-130.

[11] Rajesh Rajamani et al (2000) “On spacing policies for highway vehicle automation”, American control conference chicago, Illinois June.

[12] Gang Liu and Han Guo (2009), " Some aspects of road sweeping vehicle automation", IEEE lasme international conference on advanced intelligent mechatronics,pp 23-29.

[13] Kung et.al (2002)"A survey of mobility models for ad hoc network research", wireless communication & mobile computing (WCMC): special issue on mobile ad hoc networking: research, trends and applications, vol. 2, pp. 483-502.

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

[15] Su-Jin Kwag (2006) "Performance Evaluation of IEEE 802.11 Ad-hoc Network in Vehicle to Vehicle Communication ",Mobility '06 Proceedings of the 3rd international conference on Mobile technology, applications & systems, 1-59593-519-3.

[16] Michel Hugo (2010) "Self-Organized Traffic Control", VANET '10 Proceedings of the seventh ACM international workshop on VehiculAr InterNETworking, September 24, pp 85-90.

[17] Reena Dadhich (2011) "Mobility Simulation of Reactive Routing Protocols for VA Vehicular Ad-hoc Networks",IJCA .

[18] Jason J. Haas and Yih-Chun Hu University of Illinois at Urbana-Champaign Urbana, Illinois, U.S.A," Real-World VANET Security Protocol Performance" (2007) p1-7.

[19] Josiane Nzouonta, Neeraj Rajgure, Guiling Wang, Member(2008) ," VANET Routing on City Roads using Real-Time Vehicular Traffic Information", IEEE, and Cristian Borcea, Member IEEE , p1-18.

[20] Raya M. and Hubaux J. (2005) presented at the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, Alex-andria.

[21] Isaac J.T., Zeadally S., Camara J.S. (2010) IET communica-tionvol. 4,Iss 7, pp.894-903.

[22] 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.

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

[24] M. Raya, J. Pierre, Hubaux(2007),"Securing vehicular ad hoc Networks" Journal of Computer Security,vol.15, pp: 39-68.

[25] Bilal Mustafa (2010)," Issues of Routing in VANET", Umar Waqas Raja School of Computing Blekinge Institute of Technology.

[26] Vasundhara Uchhula Dharamsinh Desai (2006)" Comparison of different Ant Colony Based Routing Algorithms", University Nadiad, Gujarat, India, p1-5.

[27] Caelos de morais cordeiro and dharma p.agrawal,(2009)" mobile ad-hoc networking" , IJESE, Vol. 3, issue 2,pp 61-63.

[28] Muddassar Farooq and Gianni A. Di Caro (2008) ," Routing Protocols for Next Generation Networks Inspired by Collective Behaviors of Insect Societies: An Overview", Next Generation Intelligent Networks Research Center National University of Computer and Emerging Sciences (NUCES) Islamabad, Pakistan , p1-60.

APPENDIX

LAN :	Local Area Network
WAN :	Wide Area Network
MANET :	Mobile Ad-Hoc Network
VANET:	Vehicular Ad-Hoc Network
AS :	Autonomous System
DSN :	Destination Sequence Number
AODV :	Ad-Hoc On-Demand Distance Vector
RREQ :	Route Request
RREP :	Route Replay
RERR :	Route Error
CORE :	Common Open Research Emulator
PKI :	Public Key Interchange
NS :	Network Simulation
V2V :	Vehicle to Vehicle