AN EFFICIENT SECURITY PROTOCOL FOR PREVENTION OF SYBIL ATTACK IN VANET

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

By

GURPREET KAUR

11203048

Supervisor

HARJIT SINGH

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

April, 2017

ABSTRACT

The vehicular adhoc network is the self-configuring network in which two types of communication are possible i.e. vehicle to vehicle and vehicle to infrastructure. The basic application of VANET is road safety and driver comfort. Vehicular extremely established network is inherits from mobile improvised network which is basically for the careful transport system. VANET is independent and self-organized network where each node acts as a server or client to communicate with other vehicles and provide information to them. Due to its decentralized nature, security is the main concern of this network. The Sybil attack is highlighted which reduce network performance. It consists of sending several messages from one vehicle to multiple other nodes. When any node creates several fake identities then confusion occurs in the network. In our research, we mainly focused onto detect malicious node from the network.

DECLARATION

I hereby declare that the research work reported in the dissertation II entitled "**AN EFFICIENT SECURITY PROTOCOL FOR PREVENTION OF SYBIL ATTACK IN VANET**” in partial fulfillment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. Harjit Singh. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University’s Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Gurpreet kaur

11203048

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation II entitled "**AN EFFICIENT SECURITY PROTOCOL FOR PREVENTION OF SYBIL ATTACK IN VANET"**, submitted by **Gurpreet kaur** at **Lovely Professional University, Phagwara, India** is a bonafide record of her original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Harjit Singh

Date: 29/04/17

Counter Signed by:

1) **Concerned HOD:**

   HoD's Signature: ________________

   HoD Name: ____________________

   Date: ___________________

2) **Neutral Examiners:**

   External Examiner

   Signature: _______________

   Name: __________________

   Affiliation: ______________

   Date: ___________________

   Internal Examiner

   Signature: _______________

   Name: __________________

   Date: ___________________

ACKNOWLEDGEMENT

I Gurpreet kaur, Student of B.Tech-M.Tech CSE has successfully done my dissertation II entitled “**AN EFFICIENT SECURITY PROTOCOL FOR PREVENTION OF SYBIL ATTACK IN VANET**” under the guidance of Mr. Harjit Singh. I thank all the teachers, people and my classmates who helped a lot while doing my dissertation II works.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

VANET is a part of the mobile ad hoc networks. The example of a vehicular ad hoc network can be taken as a Bus System which is followed in universities. The buses have the facility of picking as well as dropping the students from different areas in a region. These buses however, are connected to each other also. This forms an ad hoc network.

The Vehicular ad hoc networks are the most prominent research area for the research purposes due to their increase in demand of usage. The vehicles and the elements that are present at the roadside are connected to each other for the purpose of communication and this network is self-configuring in nature. They do not require any fixed infrastructure for them. The transferring and receiving of the information back and forth holds the current traffic conditions of the network. Wi-Fi is the new latest technology used for the purpose of initiating the implementation of vehicular ad hoc networks.

For the purpose of communication in VANETs the new Dedicated Short-Range Communication (DSRC) method is proposed. The low latency and high data rate is ensured with the usage of this technique as it provides the short and medium range communications within it. The organizations which are build up in a certain building with less distances, the communication channels are changed more recently, and also the time provided to connect to the vehicles is less use this kind of techniques. With the absence of an automatic intelligent design for building an efficient protocol configuration in VANETs is not possible. It is due to the fact that there are many problems (NP-problems) arising with it. The areas where highly dynamic topologies and less coverage areas are to be considered, there are various design issues which need to be taken care of [2].

A network in which all the vehicles are represented as the nodes of the network is known as the vehicular ad hoc network. These network communications are built to ensure the network safety and comfort for the driver. An intelligent transport system is provided for the purpose of establishing a vehicular ad hoc network which is anyhow a subset of the mobile ad hoc networks. The vehicles find it very beneficial and so for the purpose of ensuring safety all the vehicles must be provided with this facility. The vehicles and the elements present on the roadside are provided with a wireless communication network. The properties of this network also involve its autonomous nature as well as the self-organizing wireless communication network. For the purpose of exchanging or sharing the information, the nodes present in the VANET act as servers or clients on their own. There are three different categories of the VANET architecture which are pure cellular, pure ad hoc and hybrid. The VANETs have various applications some of which are enlisted below:

- **Safety applications:** for the purpose if reducing accidents and avoid any loss of lives using the vehicles, the safety applications are very beneficial. As a result of collision in vehicles, many accidents and losses have been seen. This technique provides active road safety which helps on avoiding collisions by providing a proper guidance to the drivers with exact required information.
- **Car speed warning:** Protocols are used for the purpose of providing a combined GPS and digital maps facility to the users which will decrease the treat level for a driver which is arriving at speed.
- **Traffic signal violation warning:** if there is any driver which causes a threat of running over the traffic signal, there will be a warning imposed to the user. A message will be sent once the decision is made by keeping in consideration the traffic signal status, the position of the vehicle and its approaching speed.
- **Collision risk warning:** The possibilities of collision are detected by the vehicles and the RSU amongst various numbers of vehicles which are unable to communicate with each other. The information about the vehicles that are approaching toward the opposite direction as well as the ones reaching the destination.
- **Lane change warning:** Within a roadway lane the positioning of the vehicle is checked and monitored, if at any instance it is not safe to change the lanes, the driver is notified regarding that.

1.1 V2V Communication: Along with the advancements in the heterogeneous communication technologies and the deployment architectures, the vehicular ad hoc networks have two broader categorizations: car-to-car (C2C) communication and car-to-infrastructure (C2I) communication [5].

There are numerous types of deployment options for the various types of communication configurations. There can also be an integration of the vehicular network deployments into specific wireless hot spots along the road. The operating services of such hot spots can be done from homes, at offices, by the wireless internet service providers or even by the integrated operators. Within the existing cellular systems also the vehicular ad hoc network deployment can be involved [5].

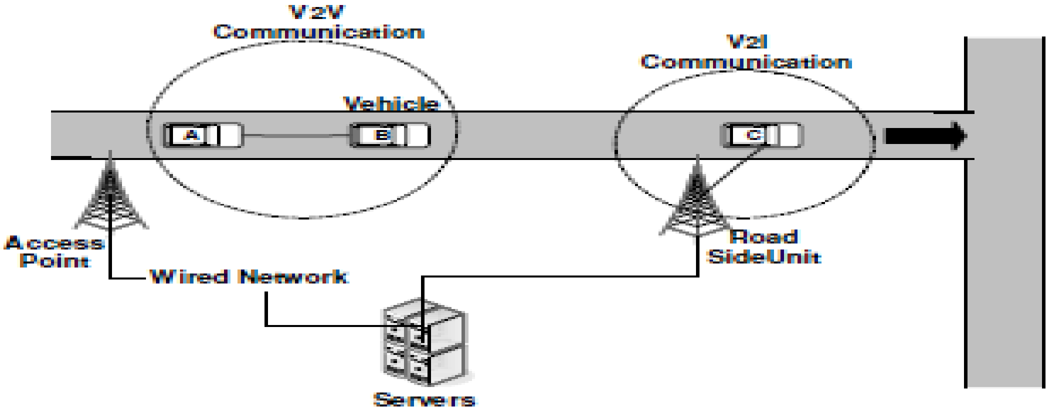


Fig 1: communication architecture [4]

There can be a communication between two vehicles without the presence of any infrastructure network. There can be a proper co-operation and transferring of required communication within the vehicles for their own as well as others benefits [5].

There can be a proper categorization of the networks on the basis of some certain characteristics [5]:

1. In-vehicle communication

2. Vehicle-to-roadside/vehicle-to-infrastructure communication

3. Inter-vehicle communication (single- and multi-hop)

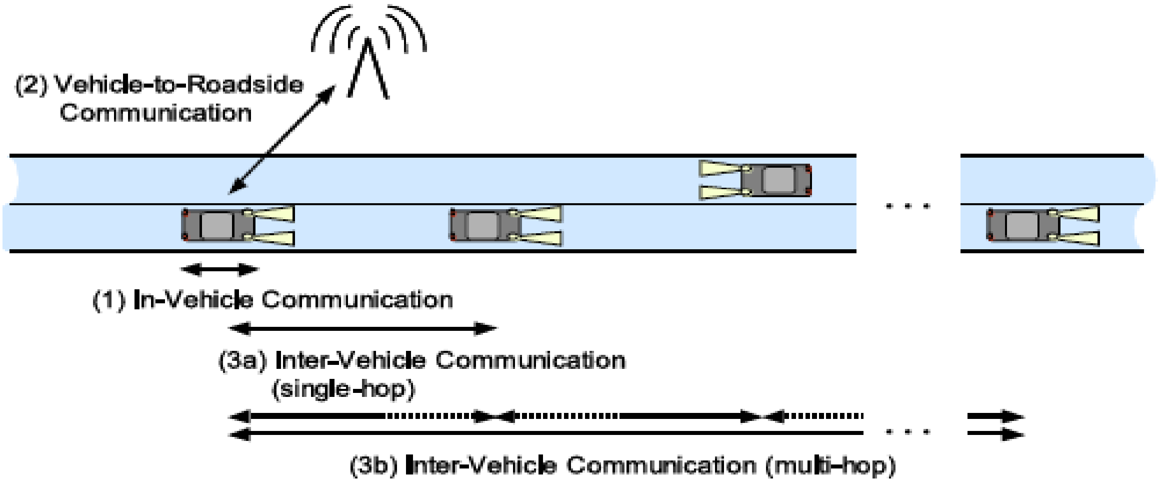

(2) Vehicle-to-Roadside Communication
(1) In-Vehicle Communication
(3a) Inter-Vehicle Communication (single-hop)
(3b) Inter-Vehicle Communication (multi-hop)

Fig 2**:** Domains of vehicular communication

- **In-Vehicle Communication (In VC):** There is an exchange of information in between the various components inside a vehicle. Almost all of the modern day cars involve such type of communication [5].
- **Vehicle-to-Roadside Communication (VRC):** Another name for it is the vehicle to infrastructure communication. There can be present any type of communication such as the vehicle to fixed infrastructure or otherwise. The communication here could be both unidirectional or bidirectional [5]. The In-vehicle to road side communication has another name for it which is the vehicle to infrastructure communication. From the broadcast station to the vehicle the communication of information is possible for the broadcast system support in a unidirectional manner. There is a point to point communication with the base station or the access point in the entire vehicle of the system. The physical synchronization and the medium access are used to provide communication to the base station. The excess load is balanced and the access control is provided in the appropriate channel. There are further classifications of the bidirectional technologies which are the cellular mobile phone systems and the small range systems. The infrastructure which is required for information is to be always available and this is to be ensured by the existing cellular infrastructures. Higher data rates can be available at less cost through the small local areas. The range of VRC changes from tens of meters to hundreds of kilometers in the wireless local area technologies for the public radio systems.

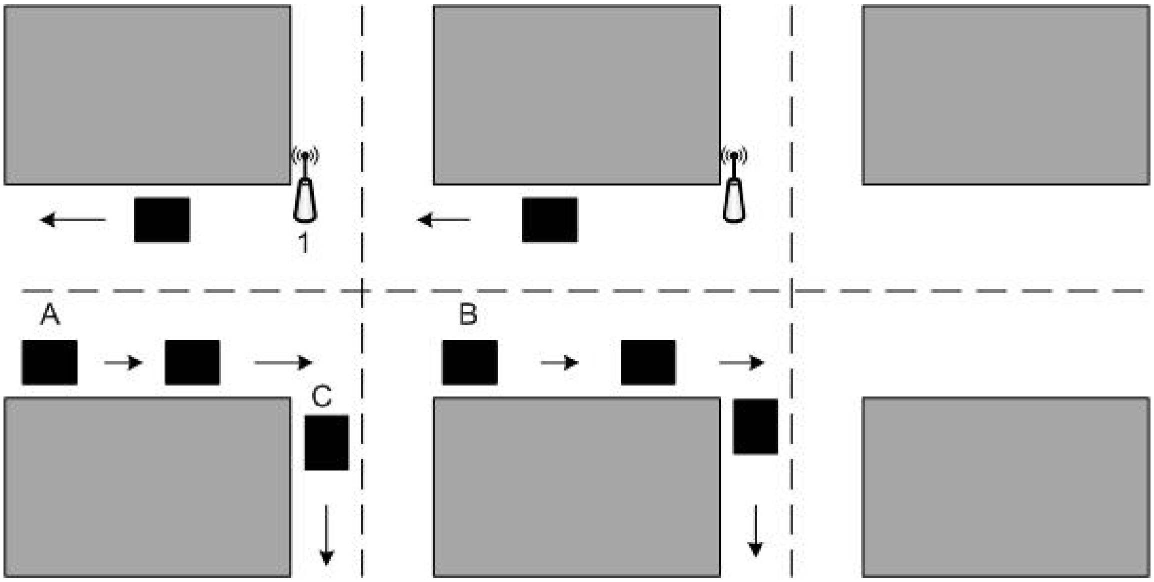


Fig 3**:** Infrastructure of VANET

1.2 Major Issues in VANET: The major issues which occur in VANET are enlisted below:

1. **High Mobility:** In accordance with the learn based schemes, there is a proper learning of the behaviours of each node. It is not possible for the nodes to interact when the nodes are highly mobile.

2. **Real-time Guarantee:** For the purpose of proper message delivery, there are some strict guidelines which are to be followed. They can then be used in applications such as hazard warning, collision avoidance, and accident warning information.

3. **Privacy and Authentication:** The personal identification of each user can be exposed by others. To avoid this, there is need to identify the vehicles through the messages which can be sent only to the authenticated users through the message transmissions. A new system is set which helps in hiding the information of vehicles from the common nodes. The central authorities are however to be notified in the case of accidents or emergencies.

4. **Location Awareness**: The GPS facility is used for the purpose of handling the vehicular network's applications. There is a chance of delay to occur in situations where there is no proper system placed.

5. **Delay in VANET**: For the purpose of path identification, there should be less delay issue in the vehicular networks. The probability of collision between the various vehicles is to be monitored by the system vehicle and the RSU. The vehicles that are approaching in the opposite direction and the ones that are going to the destination are to be informed to the other users. For this reason, the data of all such vehicles is gathered. In VANET there are many security challenges which are to be handled through these security applications. There are many hazardous outcomes of these accidents which can lead to loss of lives or jam problems. These are to be minimized with the help of preventive measures.

1.2.1 Steps taken to reduce delay problem in VANET: When the topology of the network is changed or there are highly moving nodes or vehicles present in the system, the routing mechanism in VANET is very difficult to perform. A greedy position based routing approach known as the Edge Node Based Greedy Routing (EBGR) is used for the purpose of forwarding the packets to the nodes. These nodes are available in the edge of the transmission range of the source or the forwarding node [7]. On the basis of the potential score of the nearest node, the most appropriate next hop is appointed. There is a minimization of the end to end delay of the packet transmission in the results when compared to the current routing protocols of the VANET.

The effect of the traffic lights is measured with the help of the delay-bounded routing protocol. During the crossing of a vehicle through an intersection, the information about the traffic lights is gathered, Along with this, the information related to the traffic load of the road present in the next section is provided. This helps in providing a more accurate assumption regarding the vehicles and the message deliverance in a strategic manner. There is a better usage of the time and a reduction in use of the radio resources which are needed to deliver the message within the time according to the simulation results achieved. For the purpose of assuming the available time and the distance travelled, the linear regression technique is used by the protocol. At a certain moment, there can be switching provided to the delivery strategy which will help in reducing the number of relays by radio [8]. There are two schemes of this protocols used. One is the greedy strategy and the other is the centralized scheme. The calculation of the available time for sampling of current data and decision making regarding delivery strategy is done with the help of sampling the current data through the greedy scheme. The minimum cost path is selected with the help of global statistical information using the centralized scheme. The efficiency of the protocol is handled by the simulation results.

A handoff procedure in between the V2V and V2I in the technique is represented by vehicle-to-X. It is to be made sure that the vehicles are connected irrespective of the mobility issues or the traffic conditions [9]. For the purpose of protocol switching, the time delay and the time propagation rates are the performance metrics. The vehicles transmit warning messages through the V2V or V2I communications. It is seen through the simulation outcomes that there is a decrease in the delays when the already existing network communications are combined with the inter-vehicular communications. However, there is an increase in the transmission time delays of the network of the traditional opportunistic vehicular communications. In order to enhance the QoS which is the delay in terms of the path selection across the network, there is a new algorithm which uses ant colony optimization along with the vehicle routing. The DYMO algorithm is combined with the ant colony optimization for providing enhancements in it and there are also chances of determining a new path which will help in preventing congestion in the network. The delay is minimized once the problem of congestion is eliminated from the network [10].

1.2.2 Characteristics of vehicular network: There are different behaviours and characteristic properties of VANETs which help them be different from the other networks. The unique features of VANETs are described below:

- **Unlimited transmission power:** The main aspect in the ad hoc devices is the power issue. In the VANETs however, continuous power is supplied to the computing and communication devices.
- **Computational capacity very high:** The sensing capabilities, communication, as well as the computing can be affordable by the operating vehicles on their own.

- **Predictable mobility:** The prediction of the vehicle mobility is very difficult in the case of mobile ad hoc networks. The roadway movements of the vehicles are the only ones which are easy to be predicted. This can be done through the positioning systems and the GPS technologies which are map based. The parameters such as average speed, the current speed and the trajectory which help in identifying the future position of the vehicle are determined.
- **High mobility:** The configurations of VANETs are different and they are highly dynamic in nature. For instance, on a highway the relative speed of a vehicle could be up to 300 km/h and the density of the vehicles is 1 km. Also the relative speed could be up to 60 km/h and the density of the nodes is extremely high on the rushing hours.
- **Partitioned network:** There will be much frequent partitions in the vehicular ad hoc network. The traffic could be of dynamic nature which might result in the huge inter-vehicular gaps in areas which are less populated in various isolated clusters of the nodes.
- **Network topology and connectivity:** The scenarios of the vehicular ad hoc networks change from location to location as per the movement of the vehicle in the dynamic scenarios. When there is a connection and disconnection between the links of the nodes, the network topology also changes accordingly. The network extremely depends on the two factors namely the range of the wireless links and the fraction of participant vehicles. Here, only a part of the vehicles on the road would be equipped which the wireless interfaces [8].

1.3 VANETs applications benefits: The learning as well as the designing phases of VANETs is a very tough task. For the ease of understanding them, classifications are done into various classes and the set of protocols are assigned accordingly for each class. The benefits for the classifications are enlisted below:

- Application models are developed for the purpose of representing large number of applications which have similar properties and are put into the same class for the purpose of validations and simulation.
- According to the identified application class, the key performance metrics which are relevant to it are placed as benchmarks. This is done to evaluate the performance such that it can meet the requirements of the application class.

- A networking protocol stack is created for every individual class of applications. The reusability of the class can be improved with the help of this mechanistic modules or networking protocols.

1.4 Attacks in VANET: VANETs security is violated by various types of attacks. Some of these attacks are enlisted below:

1.4.1 Sybil Attack in VANET:

The attack occurs when a single node keeps sending multiple messages to other nodes which are pretended to be from different identities. In most of the cases, Sybil attack is possible. It can only be exempted from the extreme conditions and assumptions of chances of resource parity and coordination amongst the entities. A type of confusion occurs in the whole network when a single node starts sending multiple copies of it selves. There is a chance that all the illegal, fake ID's and the authority are claimed [21]. The collision within the network starts beginning which results in causing Sybil attack in the network. Both internal and external attacks can be triggered in this type of attack. However, the external attacks can be avoided by providing authenticities measures. This is not possible with the internal attacks. The identity and entity within a network have one to one mapping.

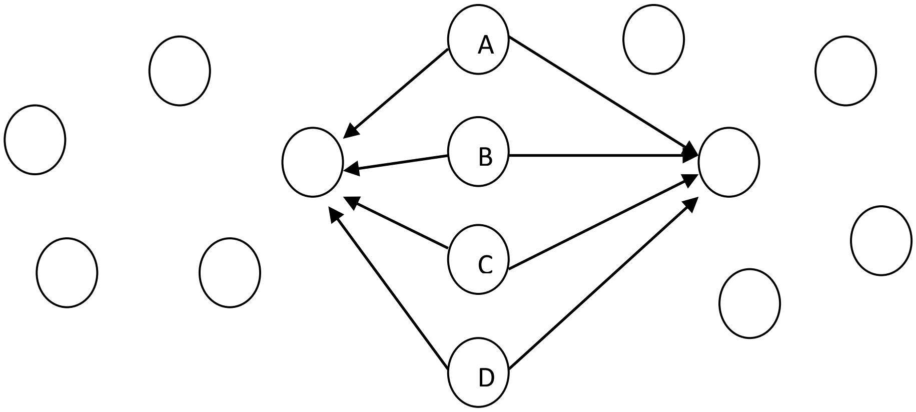


Fig 4: Sybil Attack

A fake identity within the network is created by the Sybil nodes which are represented in the figure as A, B, C, D nodes. Sybil attack is such a critical attack where the multiple messages are created by the attacker and are sent to other vehicles with different Ids each time. This makes the other nodes get confused such that the nodes assume the messages are arriving from other nodes.

Due to this a jam occurs within the network. This forces the vehicle to choose another path and leave the road which is a benefit for the attacker. The figure 1.6 shows that the red color cars have similar Ids which are marked as A. This is responsible for triggering Sybil attack in the network. There are two types of Sybil attacks namely, sensitive and throughput sensitive attacks.

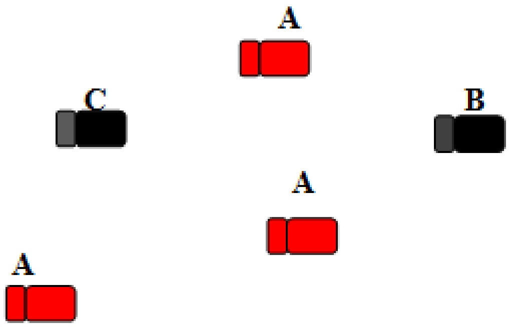


Fig 5: Sybil attack in the network

1.4.2 Denial of Service Attack:

The main aim of the DOS attack is the prevention of a legitimate user from using the resources as well as the services. The whole channel as well as the network can be jammed in this attack. This results in an inability of not being able to access the network by the authorized vehicles. Here, there is no communication possible in between the users due to the occurrence of attack. The node is made to be busy by the attacker such that the nodes are not able to perform the necessary tasks. This results in packet dropping [22].

1.4.3 Distributed Denial of Service Attack:

Due to its distributive nature, the DDOS attack is more harmful than the DOS attack. For the purpose of launching the attack, various types of locations are used. Various time slots can be used for the purpose of sending the messages where the natures of the message as well as the time slot are different for each vehicle. V2V and V2I can both have DDOS attack within them.

The aim of this attack remains to slow the network down which might also result in jamming the complete network [22].

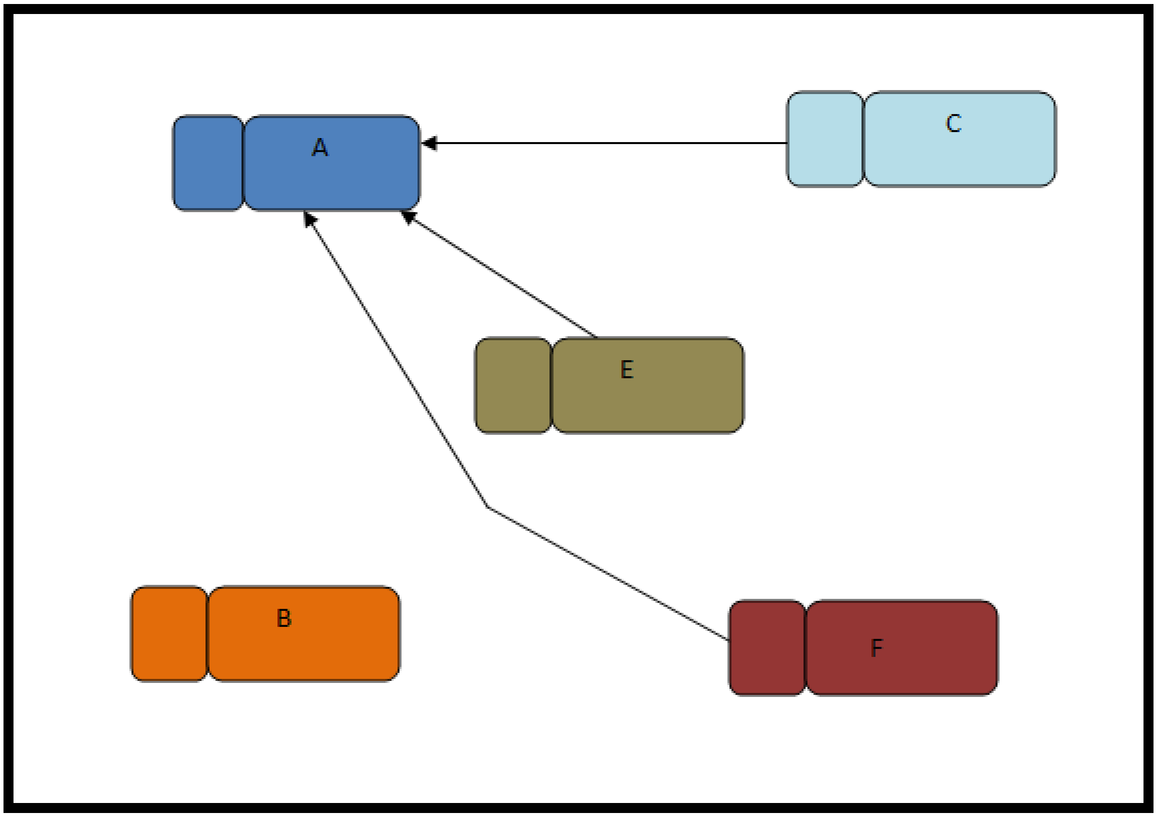


Fig 6: DDOS attack

1.4.4 Spamming:

Various messages present in the network are spammed by the attacker in this type of attack. This results in using more bandwidth which further results in increasing the latency of the network. The group's user is sent numerous messages by the attacker which has no relation with their work and just help in increasing the load of the network [23].

1.4.5 Black hole Attack:

For the routers which are present in the flooding based protocol, the requests which are to be received here are sent to the attacker directly. A reply for the short node to the destination of a route is created by the attacker once it receives a message. The reply enters the gateway for performing some actions on the packets passing in between them [10].

1.4.6 Wormhole Attack

In this type of attack, a packet is received by the malicious node in the network at a point which is tunneled back to another point at another location where rests of the packets are present within the network. The disruptions are caused once the controlled messages are routing. This is known as a network layer attack. When there two colliding attackers tunnel in between them, the attack caused is known as the wormhole attack [8].

1.4.7 Node Impersonation Attack:

The vehicles that are present in the VANET are identified with the help of their Ids. A unique ID is given to each of the vehicle which helps them in communicating with each other easily. For the purpose of identifying the reason for accidents, ID can be used more prominently. With the help of node impersonation attack, it is possible for the attacker to change or hide an original id of the node and a different id is provided instead. The node acts as if it is the original originator of the message. According to its own benefits the content of the network can be changes. It is very easy to send messages to any of the vehicles once this attack occurs in the network [23].

1.4.8 Replay attack:

The unauthorized users use the reply attack which helps them to be a legitimate user or the road side unit. The replaying of already generated frames is done to the new connection by the attacker here. The generated frames are captured by the attacker and used as a part of frame. False information is provided by the attacker which is related to the identity of the vehicle which is responsible for the accident [24].

1.4.9 GPS Spoofing:

For the purpose of updating all the information, the table is maintained in the network. The vehicle is identified in the network and along with it its geographic location in also identified. For fooling the network the GPS satellite signal is generated which is more effective than the original signals.

1.4.10 Timing Attack:

For reducing the delay in the application, the time accuracy needs to be maintained in the network which will also help in improving its performance. In the ITS safety application, the major issue is the timing attack. Instead of modifying the data, in this attack, additional content is added to the original data. More time than the given time is consumed by the messages to reach to the destination after this attack. The ITS application is time dependent and needs the transmission of data within the given time. If this requirement is not fulfilled there are chances of serious accidents [22].

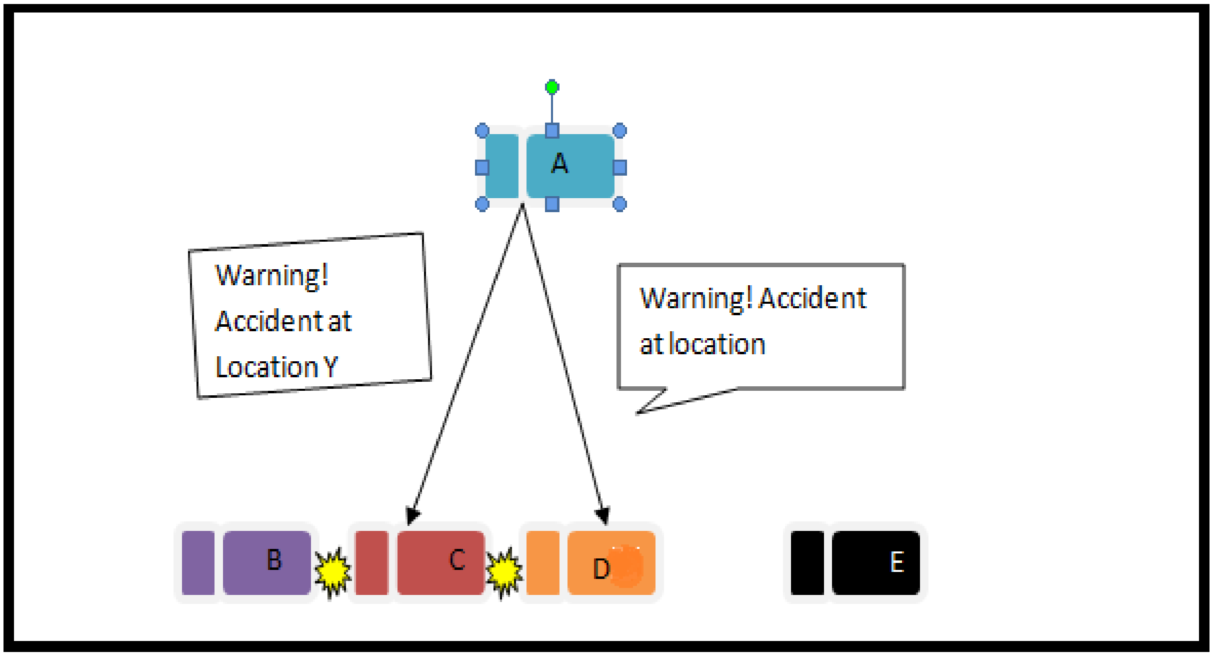

A
Warning! Accident at Location Y
Warning! Accident at location
B
C
D
E

Fig 7: Timing Attack

1.4.11 Social Attack:

The victim is confused in this attack by the attacker. For the purpose of disturbing the driver, the attacker sends unnecessary, non-informative, unmoral messages to the driver. Due to this reason the driver gets disturbed. The main objective of the attack which is to disturb the driver is achieved by these messages as the driver gets irritated and losses his concentration. The distribution within the network is caused due to such attack.

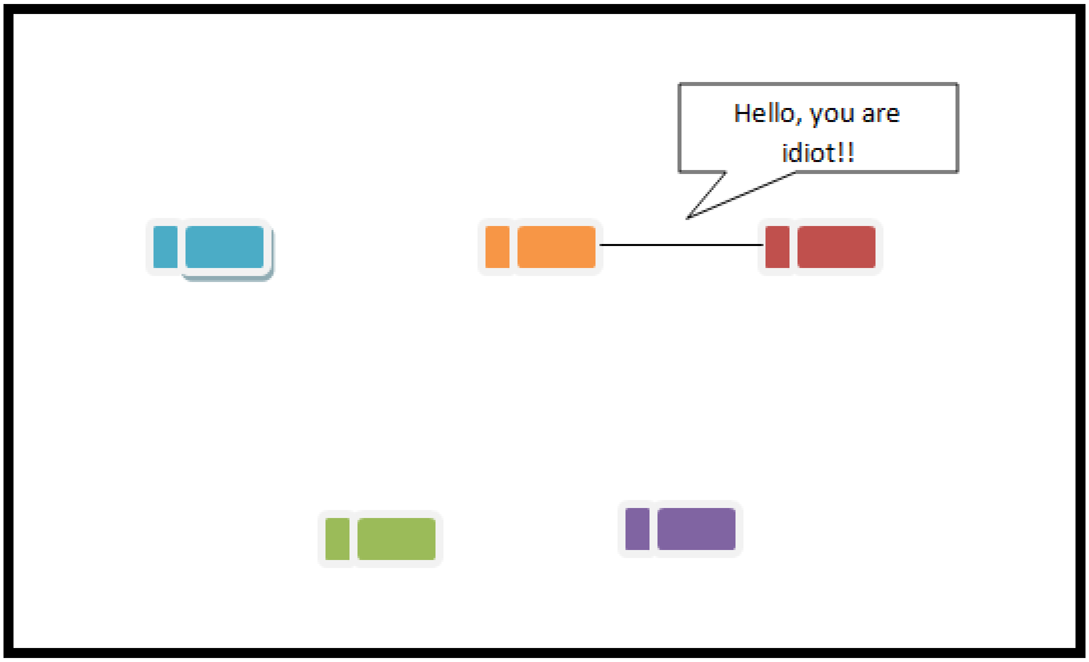


Fig 8: Social Attack

1.5 Routing Protocols in VANET

There are various routing protocols in VANET which are enlisted as follows [25]:

1.5.1 LAR Protocol:

The vehicular communications are made to be more challenging due to the fact that there are various characteristics of the location based routing protocols. The networks are divided into three broad categories which are cellular, ad hoc and hybrid. Infotainment which includes latest new, or the information of the locality, is supported by the cellular network. The vehicle to infrastructure model is the basis of this category. A wide range of vehicular applications are supported by the present infrastructure. There is however, still a need of a fixed infrastructure deployment due eliminate the drawbacks found. The ad hoc networks which do not require any prior infrastructure help in reducing the drawbacks identified. This is more prominent in the vehicle to vehicle communication. However, due to the network partitioning, routing link failures as well as the rapid topology changes, the network faces many challenges. The access points are deployed along the road in the network as a solution to the problems notified. In networks where there is no issue regarding the energy consumption also, this solution is opted. In the case of hybrid communication, there is a centralized architecture based cellular network in which the traffic information is gathered from the road with the help of access points. The acquired information is processed by the access points and is used by the drivers as per the requirement. In the traditional routing protocols, the performance of the network is degraded by the dynamic nature of the vehicular communication, the high speed of the vehicles as well as their mobility. The issues of the mobile ad hoc network are highlighted by the traditional ad hoc routing protocols [25], [26], [27], [28]. These are applicable for the MANETs due to the fact that they lack the high mobility and dynamic nature which is present in vehicular communication. The position-based routing protocols have proved to be more prominent for the highly dynamic and mobile networks. The forwarding strategies are enlisted below:

- Greedy forwarding: As shown in the scenario in the figure 1, if one uses the greedy forwarding technique, the packets from the source node are forwarded to the node closes to the destination 'D'. Here, the S send packet to A.
- Improved greedy forwarding: The neighbouring table in this case is first consulted by the source node and further, new predicted position of all its neighbours is computed. This is done on the basis of the direction and velocity. The node which is closest to the destination is selected. The new predicted position of its neighbour is predicted by S. Let us assume that at time t2 the vehicle B overtakes the vehicle A. The B is selected here as the next hop instead of A by the S.
- Directional greedy forwarding: The only nodes which move towards the destination are considered in the directional greedy approach. The node which moves towards the goal and is nearest to the goal is chosen. The vehicle B is along these lines chosen as a next bounce.
- Predictive directional greedy forwarding: The data of their 2-bounce neighbours is kept up by the sending hub here. The sending hub before sending the parcel, counsels its neighbouring table. It figures the anticipated position of the considerable number of neighbours (one-bounce and 2-jump neighbours). The hub which has one-jump neighbour moving towards the goal and is nearest to it is chosen. Here as appeared, vehicle is chosen by S because of its one jump neighbour C which moves towards goal D.

1.5.2 DGR (Directional Greedy Routing): Here the bounce number is decreased by choosing the hub which moves towards the goal. The Predictive Directional Greedy Routing (PDGr) improves the Directional Greedy Routing convention which predicts the portability of the vehicle. The versatility data is accomplished from the activity design and in addition the road format [25].

1.5.3 GSR (Geographic Source Routing): Here, the Dijkstra's shortest path algorithm is used by the GPS system on the map. This strategy aide is figuring the most limited way on every intersection. The covetous sending procedure is utilized along the way of the following intersection. This is utilized until the goal is come to in the system. There is no utilization of the ongoing activity data with the end goal of way determination of the following hub. Another vehicle which is present outside the network is selected for the purpose of recovery. This is done with the help of greedy forwarding technique. The technology known as GSR is the result of combination of the position based and topology based routing. It is a reactive location service. As a result of using the beacons, there is a high overhead on the network. However, it is more scalable and suitable for sparse networks [26].

1.5.4 A-STAR: It stands for Anchor-based-street and traffic aware routing. It is a position based routing mechanism which uses city bus routes for the purpose of identifying an anchor path for packet delivery along with the high connectivity. The traffic awareness is provided with the help of considering number of bus lines present on the road. A better decision making is done on the selected path according to the reduction of vehicle density which further reduces the chance of local maximum condition. The road is market out of service when the local maximum takes place. This results in recalculation of the path [25] [26].

1.5.5 GyTAR (Greedy Traffic Aware Routing): The proposed technique is used in city environments where the intersection is kept as the base. The geographical routing protocol is used for this technique. The junction selection and the data forwarding between the two junctions are the two parts of the network. The positions of the junctions are recognized by the digital maps. The digital maps are also used for distinguishing the shortest path towards the destination. This is done with the help of Dijkstra's shortest path algorithm [27].

1.5.6 EGySTAR: This is the modified version of GySTAR routing protocol. The junction is selected dynamically because it is based on vehicular traffic density. The direction of the destination is considered and the curvature distance towards the destination is also noticed. The drawbacks of GySTAR are eliminated when the directions of the vehicles are considered before the next junctions are selected. Each junction is assigned the score accordingly and the junction which has the highest score is selected. The next destination junction has higher vehicular traffic which is moved towards the destination [28].

1.7 AODV: The AODV is an on-demand routing protocol, which is described as a reactive routing protocol. When in a network, there is a need for the source node to route to particular destination the routing establishment is initialized by the route discovery process. All the neighbors forward the RREQ packet to the neighbors of the source node on its own. The forwarding of packets to their neighbors and further to the next neighbors keeps going until the destination is reached. The process can also stop on an intermediate node which has a fresh route to the required destination.

CHAPTER 2

REVIEW OF LITERATURE

[Xiao, B., Yu, B., & Gao, C. (2006) In this paper, for the purpose of detecting and localizing the Sybil nodes in VANETs, a new security method is proposed. This method is based on the statistical analysis of the signal strength distribution. Through this method, each vehicle present on the road is able to detect the Sybil vehicles closer to them with the help of this distributed and localized mechanism. This is done through verification of the claimed positions. A basic signal strength based position verification scheme is first introduced. Here, the traffic patterns as well as the assistance from the roadside base stations are used up to their benefits. Here, two statistical algorithms are used for enhancing the accuracy of the positional verification. The verification error rate is lowered with the help of the statistic nature of these algorithms. For the detection of Sybil nodes in GPS as well as RSSI, the signal measurements are used. The reported positions of the vehicles are confirmed with the help of Vehicle-to-Vehicles communication used within this scheme. The RSSI measurements are used for reference purposes. The parameters such as vehicle mobility, traffic patterns and supports from the roadside are used for correcting the errors identified in the RSSSI measurements [3].

Hao, Y., Tang, J., & Cheng, Y.(2011) A security protocol is proposed in this paper, which identifies the Sybil attack in case of position based applications. The privacy of the VANETs is the main concern here. The Sybil attacks are identified locally by the vehicles in a cooperative manner. This is done through proper examination of the rationality of positions of vehicles according to their neighbors. The communicational characteristics as well as the GPS positioning of the vehicles are used to detect the attack. The required information is present in the periodically broadcasted safety related messages. There is no need of any extra hardware and the communication required here is also less. The overhead computation will also be involved in the vehicles in this system. The protocol used here is very lightweight and is perfect for utilizations are real applications; a scenario is considered where the malicious vehicle adjusts its communication range so that it is not detected. It is known as the smart attacker scenario. These scenarios included with the malicious vehicles' scenario are also taken under consideration in this method. The performance of the proposed protocol is shown using simulation based results which are performed in NS2 [4].

Chang, S., Qi, Y., Zhu, H., Zhao, J., & Shen, X. (2011) In this paper, a novel approach is proposed for the purpose of Sybil attack detection. The technique known as Footprint is used along with the trajectories of the vehicles in order to identify the Sybil attack. This mechanism however, preserves the location privacy of the vehicle. Whenever a vehicle comes towards the Road-Side Unit (RSU), the authorized message from the RSU is asked as a proof for the appearance time at RSU. A location hidden authorized message is created in this scheme. It has two aims. The first aim holds to imply RSU signatures on the messages which are ambiguous such that the RSU location information is not disclosed from the authorized message. The second aim is to assign two authorized messages using similar RSU in the same instant of period. These can further be used for identification purposes. A location hidden trajectory is generated in the vehicles. It is used for the location-privacy-preserved identification. This is done by gathering consecutive series of the authorized messages. The communities of Sybil trajectories can be recognized as well as dismissed by the Footprint with the help of social relationships with accordance with the similarity definition of two trajectories used [5].

Tong Zhou, Romit Roy Choudhury, Peng Ning, and Krishnendu Chakrabarty (2011) In this paper a Privacy Preserving Detection of Abuses of Pseudonyms protocol is used. This is used for the detection of Sybil attacks in VANETs. Here, a malicious user is detected which pretends to be multiple vehicles. A distributive approach is used with the help of passive overhearing of set of fixed nodes which are known as road-side boxes (RSBs). There is no vehicle in this network for disclosing the identity to detect the Sybil attack here. This results in preserving the privacy of this node at all instants. The inherent trade-off of the securities is quantified according to the results of this proposed scheme. The parameters which make sure about this are the detection latency and the privacy of the vehicles. This proposed scheme is able to detect the Sybil attacks at low overhead and delay along with the privacy preservation of the vehicles. The numerous vehicles that are affected by the malicious user are also highlighted by using this approach. A passive listener is used in the distributive manner which sets the fixed nodes which are also known as the road side boxes. There is no need to distinguish the identity of any vehicle which helps in preserving the privacy of the network at all times and is of great helps [6].

Lee, B., Jeong, E., & Jung, I (2013) in this paper, a Detection Technique is proposed for the Sybil Attack which is the DTSA protocol. The session key based certificate (SKC) is used for validations of the inter-vehicle Ids in vehicular ad hoc networks. The Ids of the vehicles are verified by the SKC and the generation of anonymous ID of the vehicle is also done here. The creation of a session key, the expiration date as well as the local server certification is also done for identifying the Sybil attack along with the verification time of the ID. The detection time of the Sybil attack is reduced with the help of this method. The reduction of verification time is also done here using the hash function and the XOR operation. The anonymous ID can be used for the purpose of protecting the privacy of the driver. The drivers can thus drive safely and reliable information can be provided for VANETs and this can result in reducing the traffic accidents [7].

Li, M., Xiong, Y., Wu, X., Zhou, X., Sun, Y., Chen, S., & Zhu (2013) in this paper, the detection of replicated attacks in wireless sensor networks (WSNs) is studied. The variants of replication attacks are spawned. One of them is the Sybil attack. A regional statistics detection scheme (RSDS) is proposed in this paper. This scheme provides solutions to three main problems. The first is the addressing of the Sybil attack by the RSSI-based distributed detection mechanism. The second is the prevention of the network with the help of the protocol from various node failures caused due to the Sybil attacks. Third is, the verification of the RSDs which can maintain the high detection probability along with low system overhead using the imposed experiments. At the final stage, the protocol is run in a prototype detection system along with the 32 nodes. The results show that the experiment conducted here has high efficiency [8].

Gañán, C., Muñoz, J. L., Esparza, O., Mata-Díaz, J., & Alins, J (2014) in this paper, a critical security issue of VANETs is discussed which is the cause of malicious vehicles. The potentially sensitive information can be leaked by the system. The vehicles that need any kind of information can be provided by the Road Side Units (RSUs) which receive the authorized status queries. There is a loss of privacy results by the RSUs which holds the checking vehicles with the query’s target. A Privacy Preserving Revocation Mechanism (PPREM) is proposed in this paper. This scheme is based on the universal one-way accumulator and provides explicit, concise, authentication and unforgettable information regarding the revocation status of each certificate. Along with all this, the privacy of the user is ensured throughout. The service status checking process is replaced by the time-consuming CRL. A one way accumulator is applied here which holds a fast revocation checking process. The security and privacy of the VANETs are ensured by the PPREM. It also ensures the reduction of revocation cost [9].

Balamahalakshmi D., & Shankar M. K. V.(2014) In this paper a compromised RSU detection mechanism is proposed for the purpose of detecting the Sybil attack. The trajectory information is used in this method which generates multiple RSUs. However, the location of the vehicle is hidden and not exposed. The location as well as the timing information will be generated by the RSU for the vehicle. This is done when the vehicle passes through the RSU. The verification is done through this message. For the purpose of reducing the size of the message, the number of adjacent RSUs is eliminated. The length of the trajectory information is reduced and there is no loss of information. Through the method, the bandwidth overhead of the network is also reduced [10].

Rajesh Rajamani (2000) in this paper the spacing policies are proposed which help in the highway vehicle automation. Here, a dispersing approach which is a nonlinear capacity of speed is examined. When contrasted with the standard time-crevice controller, the string security, movement stream solidness and in addition the higher activity stream limit is given. The autonomously present information is utilized by the spacing policy. The guarantee of proving string stability by the spacing policy is seen after the analytical calculations are seen. Also it ensures the traffic flow stability by maintaining smaller steady state spacing. Larger traffic flow capacities which are in the range of 20-65 m/h are provided through this mechanism. The ACC vehicles present on the highways of today can readily use the spacing policy [11].

Gang Liu and Han Guo (2001) in this paper a design framework of intelligent transport systems which is related to the aspects of road sweeping vehicle automation. The exchange of information from the within, from car to car as well as from car to road is the main aim for the road condition information transferring module. The security issues of VANETs are to be discussed and there solutions are to be derived. This is to be made sure that there solutions can be implemented under certain security patterns [12].

Kung (2002) in this paper a survey of mobility models for ad hoc network research is proposed. In this paper the specialists proposed security engineering for vehicular correspondence. The primary point of the proposed engineering holds the administration of characters. Further there should be the involvement of cryptographic keys which ensure the security of communications and integrate the privacy enhancement technologies. The components which could be upgraded such as to provide enhanced security and privacy protection for future are aimed to be achieved by the system proposed [13].

Hao Wu (2011) in this paper a new technology which was proposed for the communications being held at vehicles present within shorter range was proposed. Both the V2V and V2I communications are proposed under the highway scenario. This work discusses the network characteristics of the driving network environment through this paper [14].

Su-Jin Kwag The performance evaluation of the IEEE 802.11 ad hoc networks is proposed in this paper. This evaluation in performed in the vehicle to vehicle communication for analyzing the performance of IEEE 802.11 ad hoc networks. The V2V communication which is done in a vehicular environment focuses on the justification which is important for the safety related services. The mobility effects are also considered here. The future work suggestions are also discussed in this paper [16].

Jason J. Haas and Yih-Chun Hu (2007) in this paper, the execution estimations of the reproductions of VANETs are proposed. The info hints of the vehicle developments that are made by the movement test systems depend on the activity show hypothesis. The work which depends on the extensive scale recordings of vehicle developments is talked about in this paper. There has been very less publication on the large scale recording vehicle movements. A new VANET simulator that handles the vehicles which are more in NS2 are developed for the purpose of enabling analysis on this scale. The results which provide simulation results statistically are present which provide cross validation between ns2 and the current simulator. The ECDSA signatures are used for proposing the authentication mechanism which helps in comparing it to broadcast authentication mechanism with the help of TESLA. The evaluations are performed in this paper with the help of real vehicle mobility. The strength and weakness of the authentication schemes is shown with the help of proper comparisons made within the various schemes in terms of the reception rates and the latency of the broadcasting packets [18].

Josiane Nzouonta, Neeraj Rajgure, Guiling Wang (2008) in this paper a RBVT named routing protocol is proposed which is a road based protocols. This protocol is proposed with the help of vehicular traffic information routing that is based on the already existing routing protocols within the VANETs. The geographical forwarding technique is used in this paper for sending the packets in between the intersection path for the reduction of sensitivity within the paths for individual node movements. Here, a reactive RBVT-R protocol as well as proactive RBVT-P protocol is proposed and further compared with the MANET protocols such as AODV, OLSR etc. The RBVT-R protocol is proven to the best protocol through the simulation results. The parameters developed after the results were the delivery rate and the average delay [19].

CHAPTER 3

PRESENT WORK

3.1 PROBLEM FORMULATION

The vehicular adhoc network is the network in which vehicles can communicate with each other and vehicle can communicate with the road side units. In vehicle to vehicle communication, two type of communication is possible which is single hop and multihop communication. In the multihop communication, various type of routing protocols are used which are reactive, proactive and hybrid protocols. In this work, AODV protocol is used for the path establishment which is the reactive routing protocol. Due to decentralized nature of the network, various types of active and passive attacks are possible which are triggered by the malicious nodes. These attacks reduce network performance in terms of various parameters. The Sybil attack is the active type of attack which is triggered by the malicious node. The Sybil attack drop some of the packets and some of the packets are forwarded to the destination. In this work, novel technique will be proposed which recognize malicious hubs from the system which are mindful to trigger Sybil attack in the network.

3.2 OBJECTIVES OF THE STUDY

1. To implement and evaluate the impact of Sybil attack in vehicular adhoc networks.
2. To propose improvement in AODV protocol for detection and isolation of Sybil attack in VANETs.
3. To implement proposed technique and compare with existing algorithm in terms of various parameters.

3.3 RESEARCH METHODOLOGY

The vehicular adhoc networks is the decentralized type of network in which no central controller is present and nodes can change its location any times. The vehicular adhoc network has three major issues which are security, routing and quality of service. Due to self-configuring nature of the network, malicious nodes join the network that triggers various types of active and passive attacks. The Sybil attack is the active type of attack in which malicious node spoof the identification of the legitimate node. The legitimate node is not able to get the required data which leads to reduction in network throughput. In this work, technique is been proposed which recognize malicious hubs from the system which are mindful to trigger Sybil attack in the network. The proposed techniques is based signal strength based technique and monitor mode techniques. In the proposed technique, the road side units flood the ICMP messages in the network. The vehicle nodes when receive the ICMP messages will start sending its signal strength value to its nearest road side units. The road side units will gather all the information and exchange the information with each other. The vehicle node which has multiple signal strength values will be detected as the node which may cause the intrusion in the networks. To confirm that which node is the malicious node, the road side units send the control packets in the network and vehicle nodes when receive the control packets will go to monitor mode and start watching its adjacent nodes. The node which is malicious is detected and technique is multiple path routing is applied which isolate malicious nodes from the network.

Proposed Algorithm:

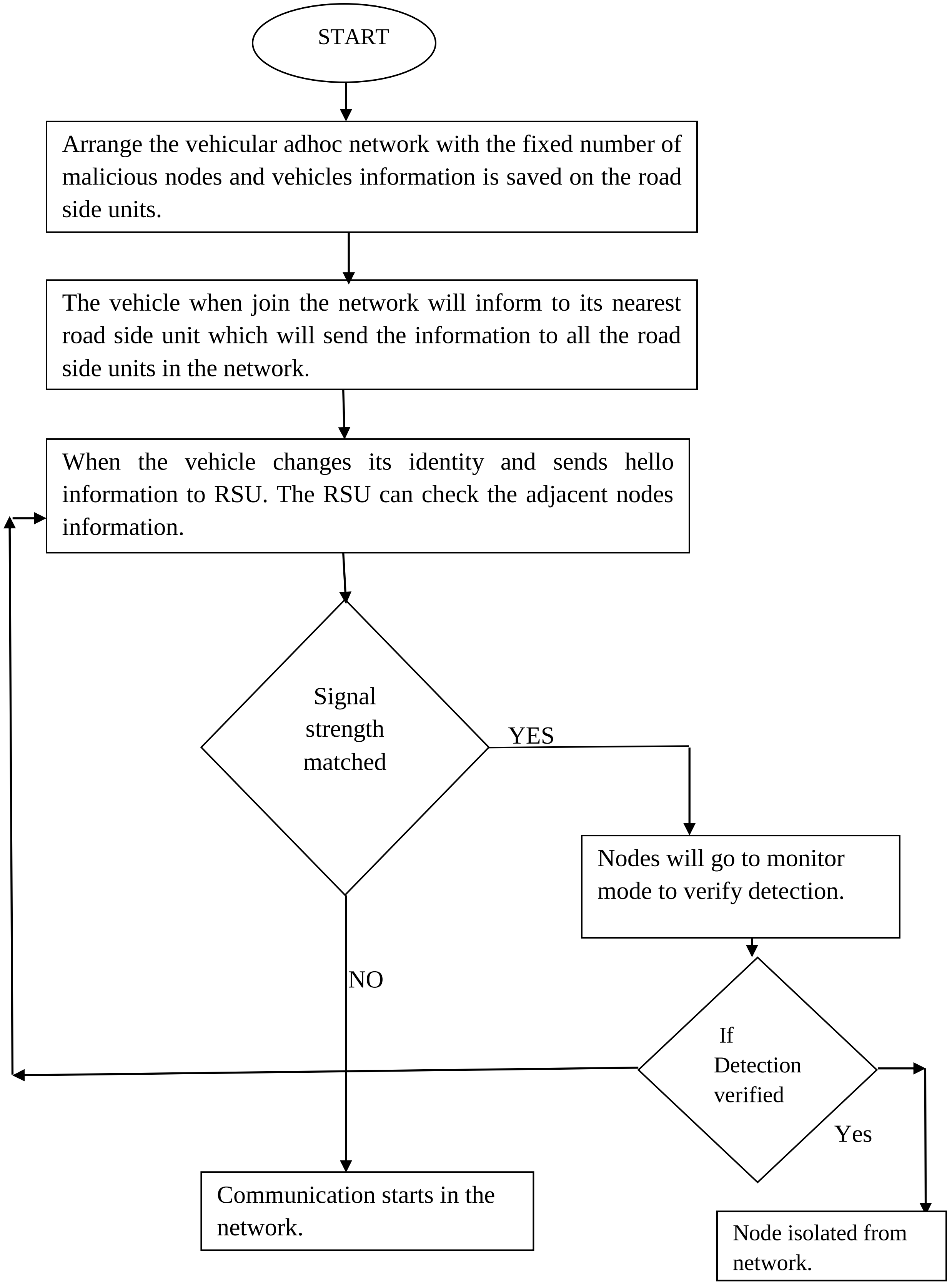
Input: vehicles, RSU, malicious vehicle

Output: Malicious vehicle

```
Apply information gathering process

{

    1. Node send its credentials to road side units
    2. If(Matched= true)
    3. Assign identification
    4. Else
    Send not verified message
    }
    }
If (signal strength ==not matched)
    Send ICMP messages in the network
    Node receive the message go to monitor node
    If(Node change id==true)
    Node ==Malicious node
    Else
    Node=Legitimate node
    }
    End
```


START
Arrange the vehicular adhoc network with the fixed number of malicious nodes and vehicles information is saved on the road side units.
The vehicle when join the network will inform to its nearest road side unit which will send the information to all the road side units in the network.
When the vehicle changes its identity and sends hello information to RSU. The RSU can check the adjacent nodes information.
Signal strength matched
YES
Nodes will go to monitor mode to verify detection.
NO
If Detection verified
Yes
Communication starts in the network.
Node isolated from network.

FLOWCHART

CHAPTER 4

RESULTS AND DISCUSSION

Tool: NS2 is an open-source re-enactment instrument running on Unix-like working frameworks. It is a prudent occasion test system focused at systems administration look into and gives generous support to re-enactment of steering, multicast conventions and IP conventions, for example, UDP, TCP, RTP and SRM over wired, remote and satellite systems. It has many points of interest that make it a valuable device, for example, bolster for numerous conventions and the capacity of graphically itemizing system movement. Furthermore, NS-2 underpins a few calculations in directing and lining. LAN steering and communicates are a piece of directing calculations. Lining calculation incorporates reasonable lining, shortage round robin and FIFO. NS-2 began as a variation of the REAL system test system in 1989. Genuine is a system test system initially proposed for concentrate the dynamic conduct of stream and clog control plots in bundle exchanged information systems?

The system test system (NS), which is a discrete occasion test system for systems, is a recreated program created by VINT (Virtual Internetwork Test-bed) extend gathering. It bolsters reproductions of TCP and UDP, some of MAC layer conventions, different steering and multicast conventions over both wired and remote system and so on. Contingent upon client's necessity the re-enactment are put away in follow records, which can be encouraged as contribution for investigation by various part:

- 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.

4.1 EXPERIMENTAL RESULTS

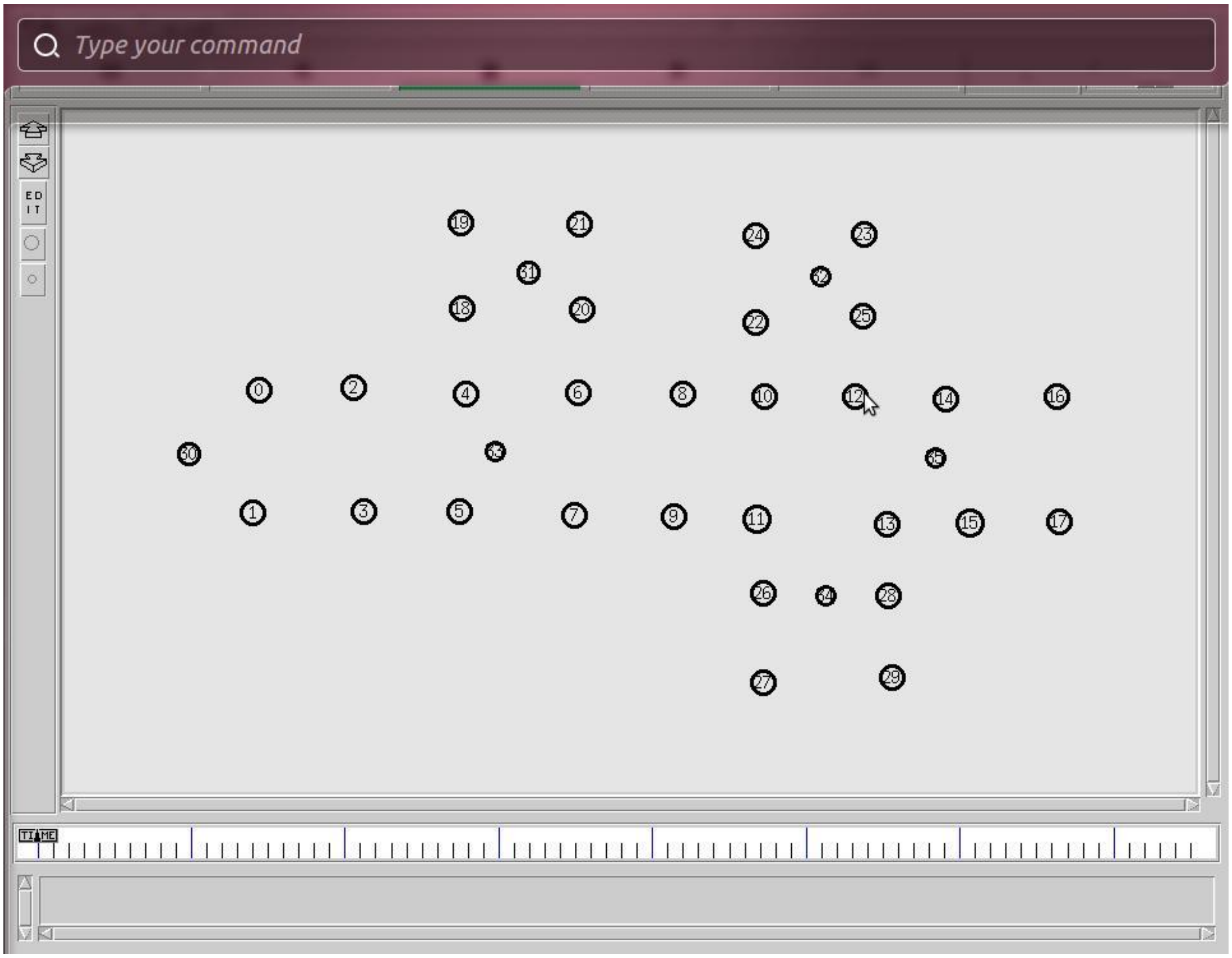
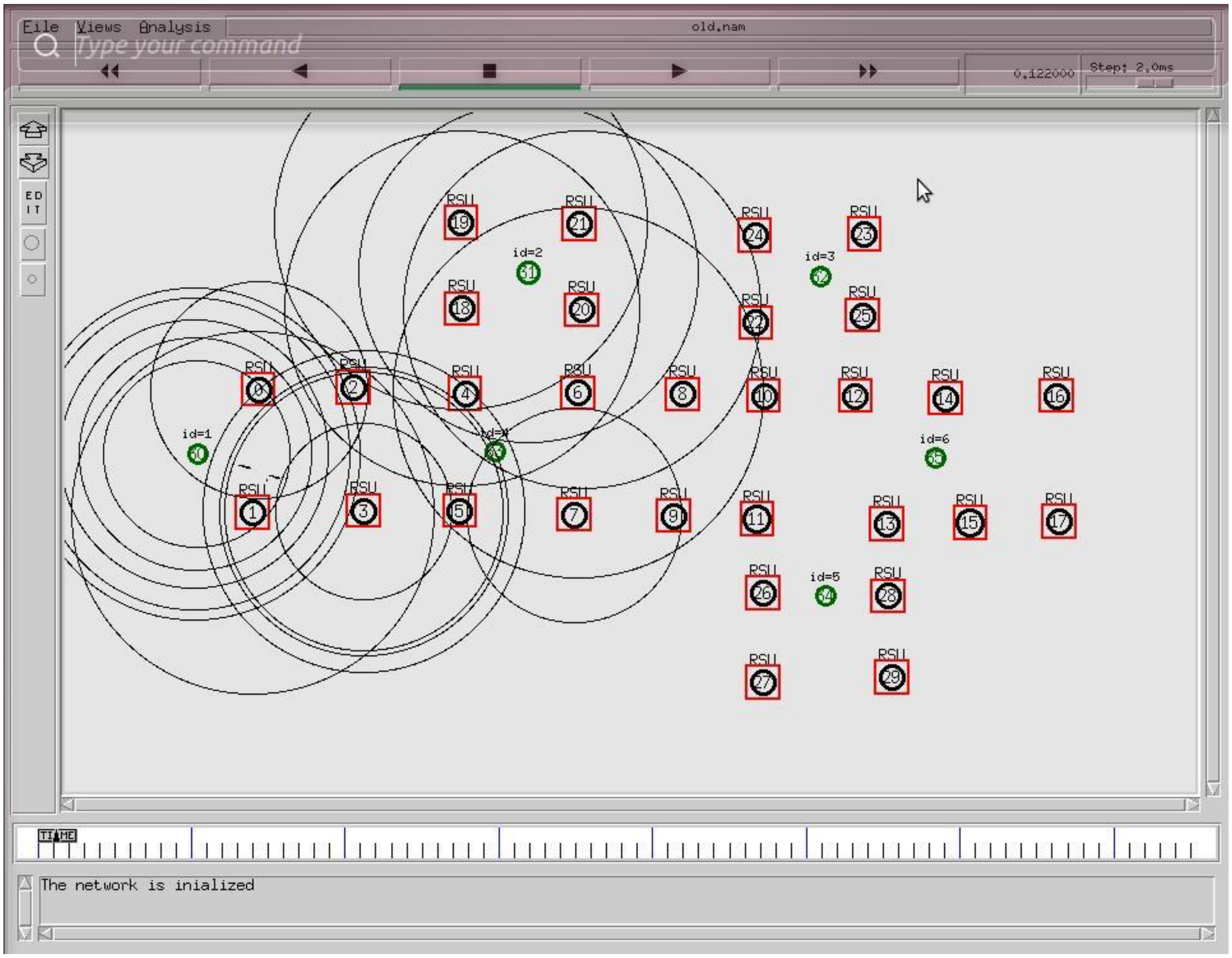


Fig 9: Network deployment

As illustrated in figure 1, the vehicular adhoc network is arranged in such a way that there are number of road side units which are fixed and there are number of vehicles which can move freely in the network.

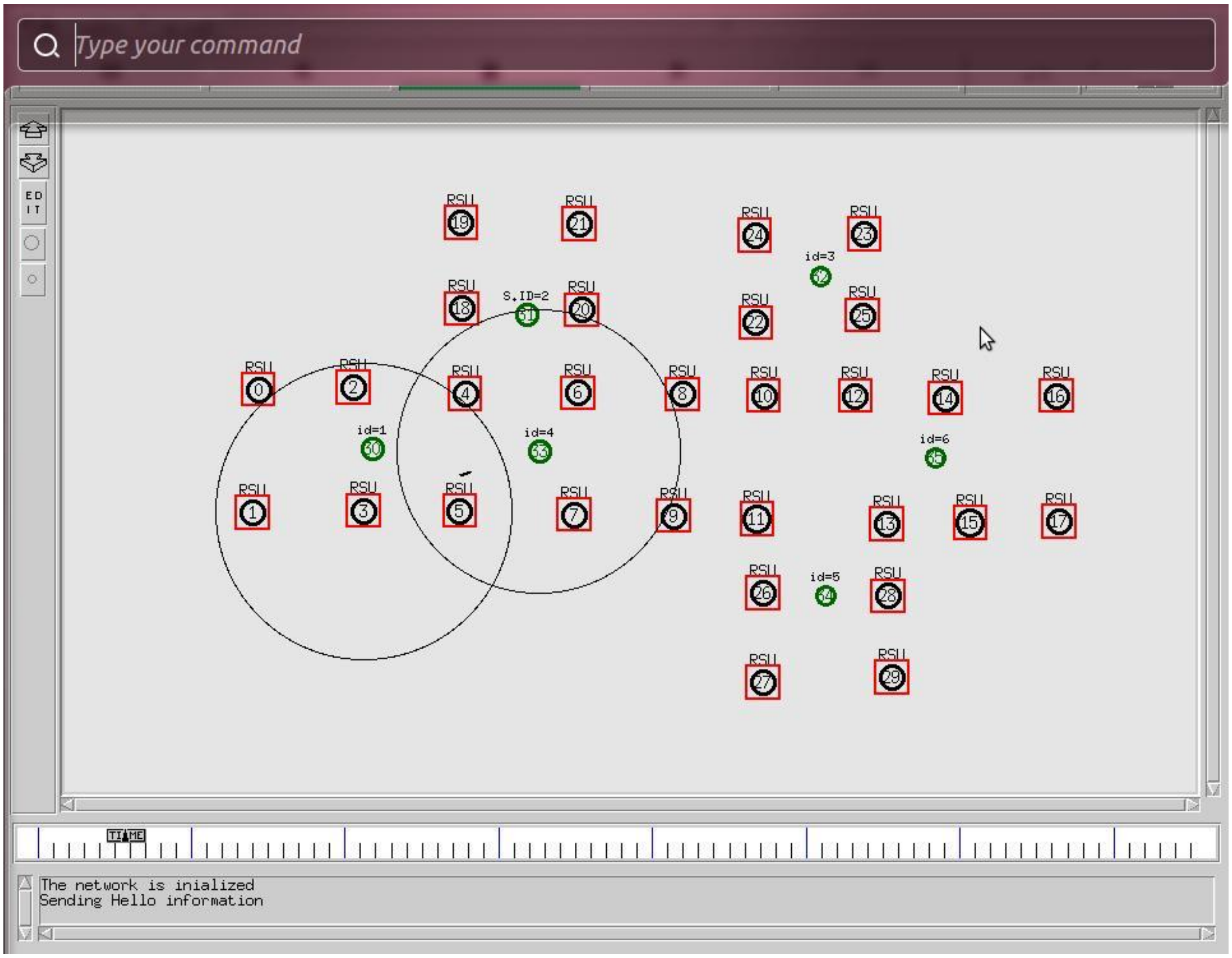


```
The network is inialized
```

Fig 10: Communication between cars

As shown in figure 2, the network is arranged with the fixed number of road side sensor and smart cars, the smart cars are moving on the roads. At the time of registration, each vehicle gets its identification number to move freely in the network.

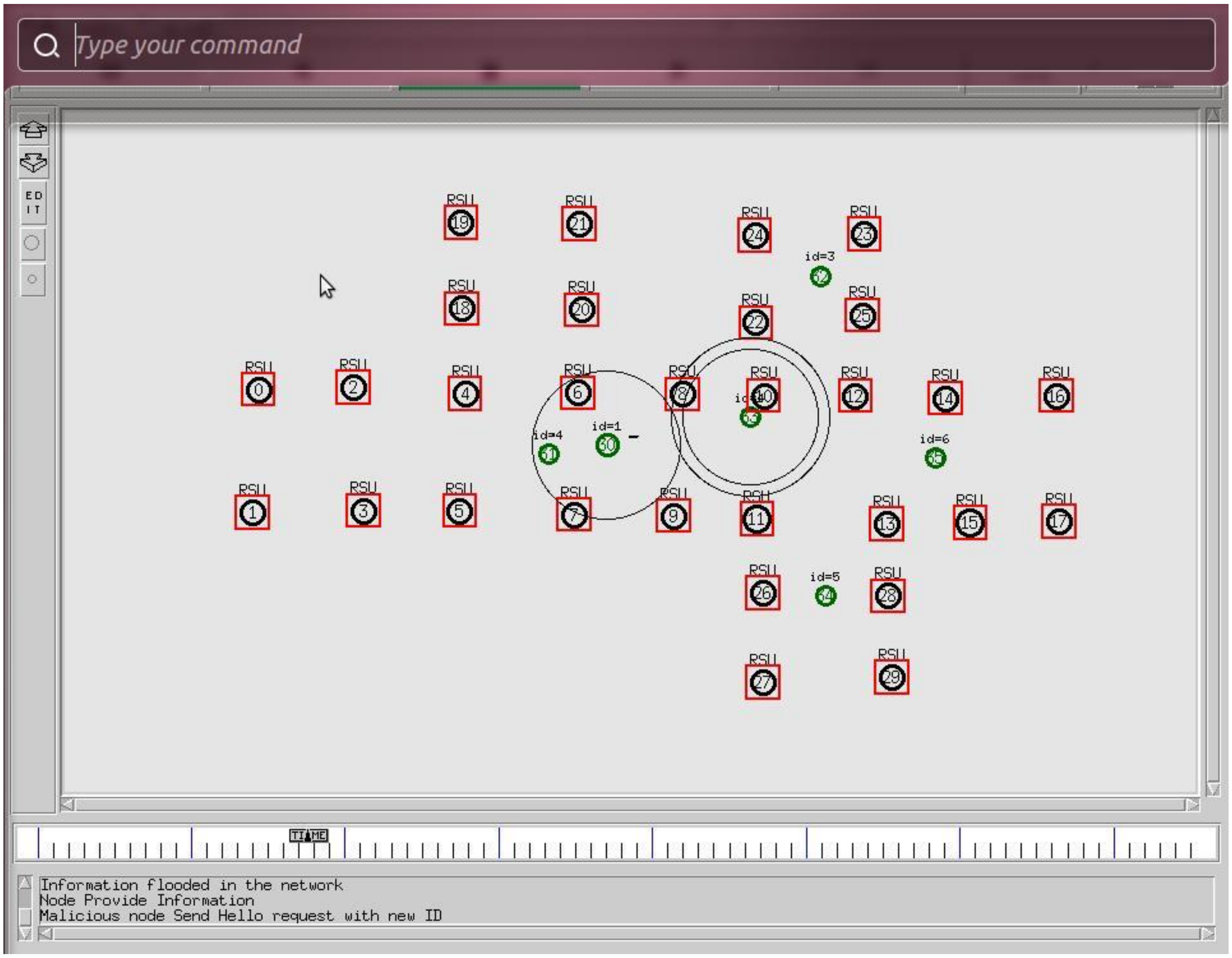
.



```
The network is inialized
Sending Hello information
```

Figure 11: Registration process of new car

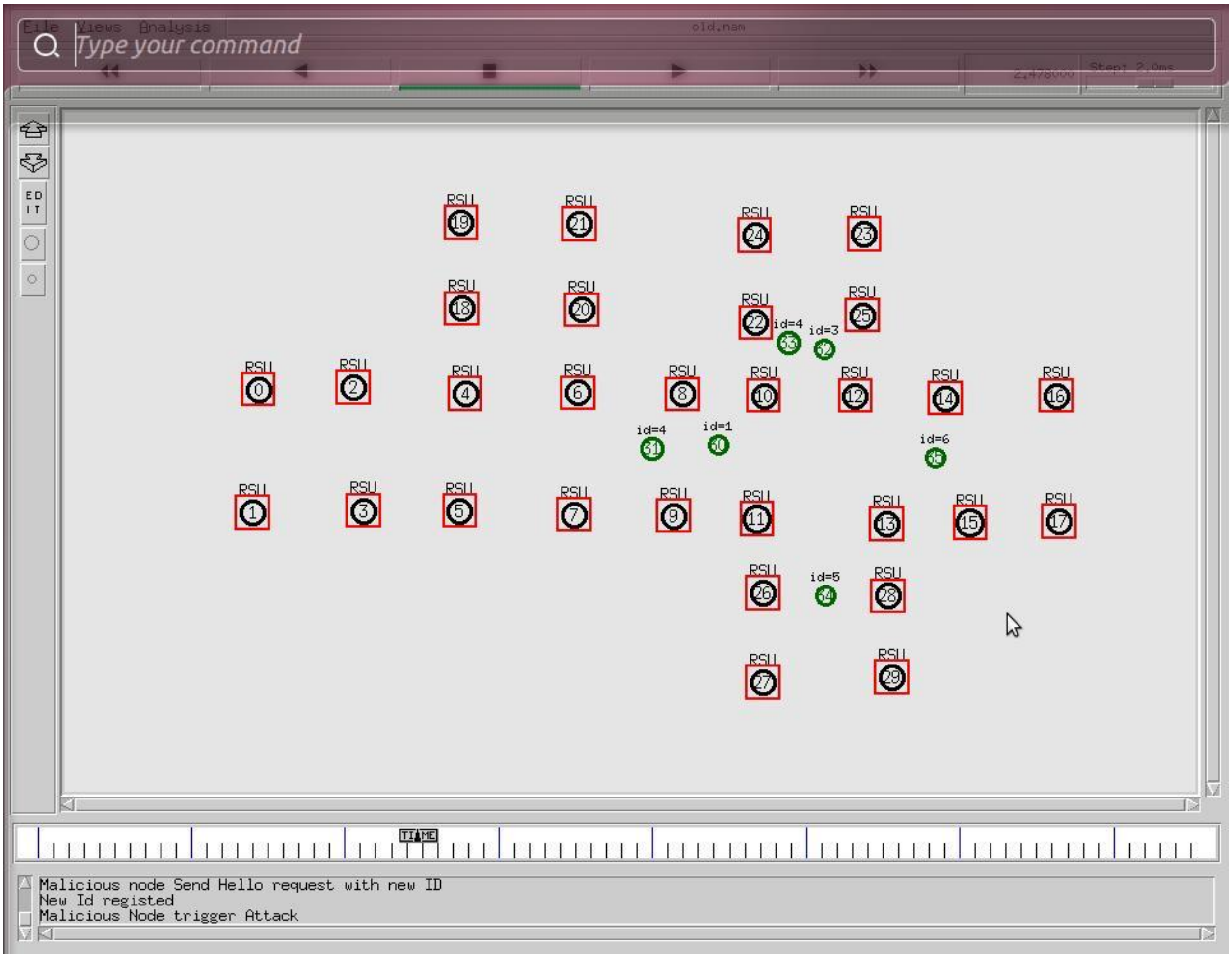
As illustrated in figure 3, the smart cars are communicating with each other like the car having identification number of 1 is communicating with car having registration number of 4. The new car is coming in the system and sending registration request to new road side units.



```
Information flooded in the network
Node Provide Information
Malicious node Send Hello request with new ID
```

Fig 12: Allocation of new identification

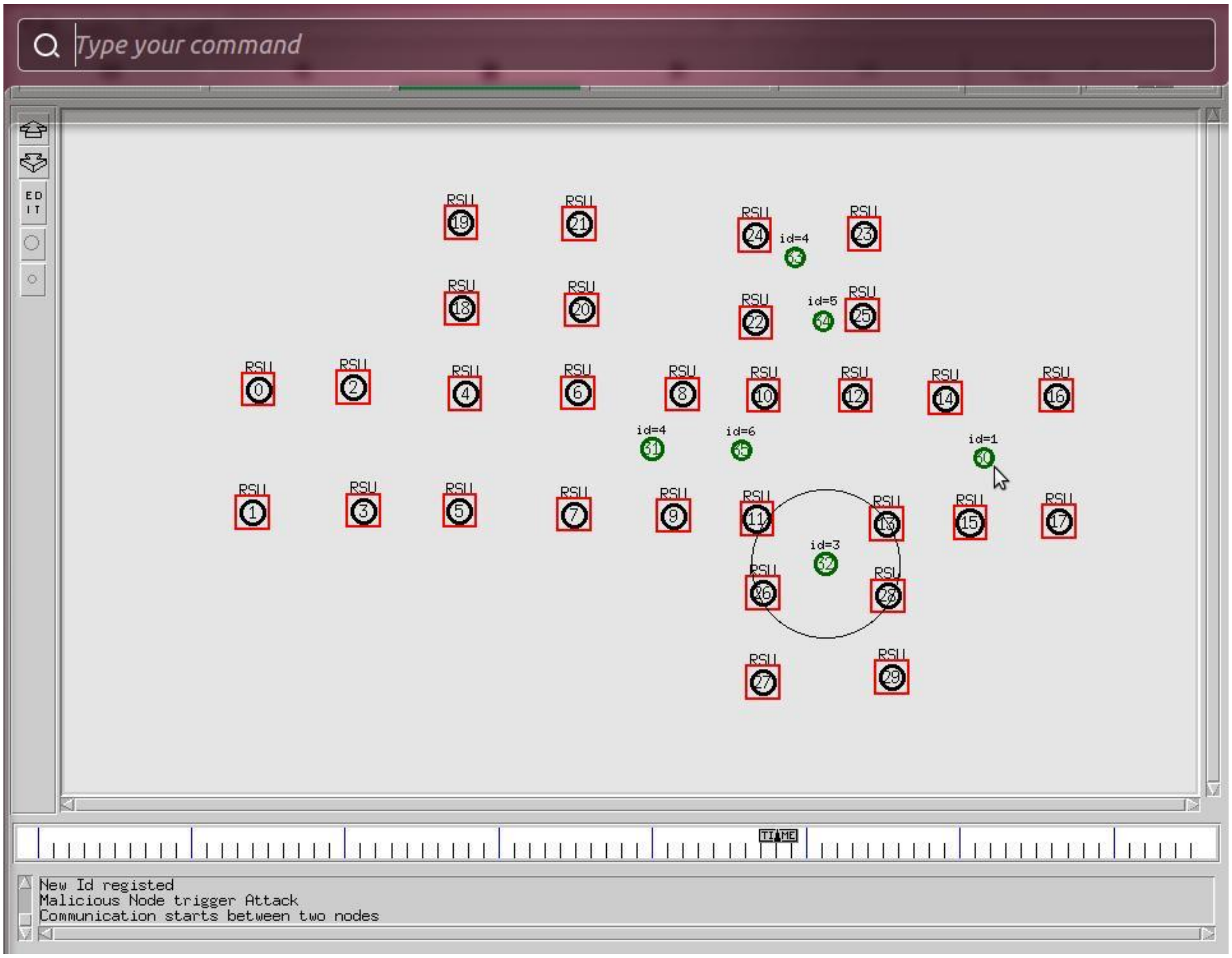
As shown in figure 4, the new car which just enters the network needs to register to gets its identification number. The road side unit provides it the identification number of 4.



```
Malicious node Send Hello request with new ID
New Id registed
Malicious Node trigger Attack
```

Fig 13: Communication between cars

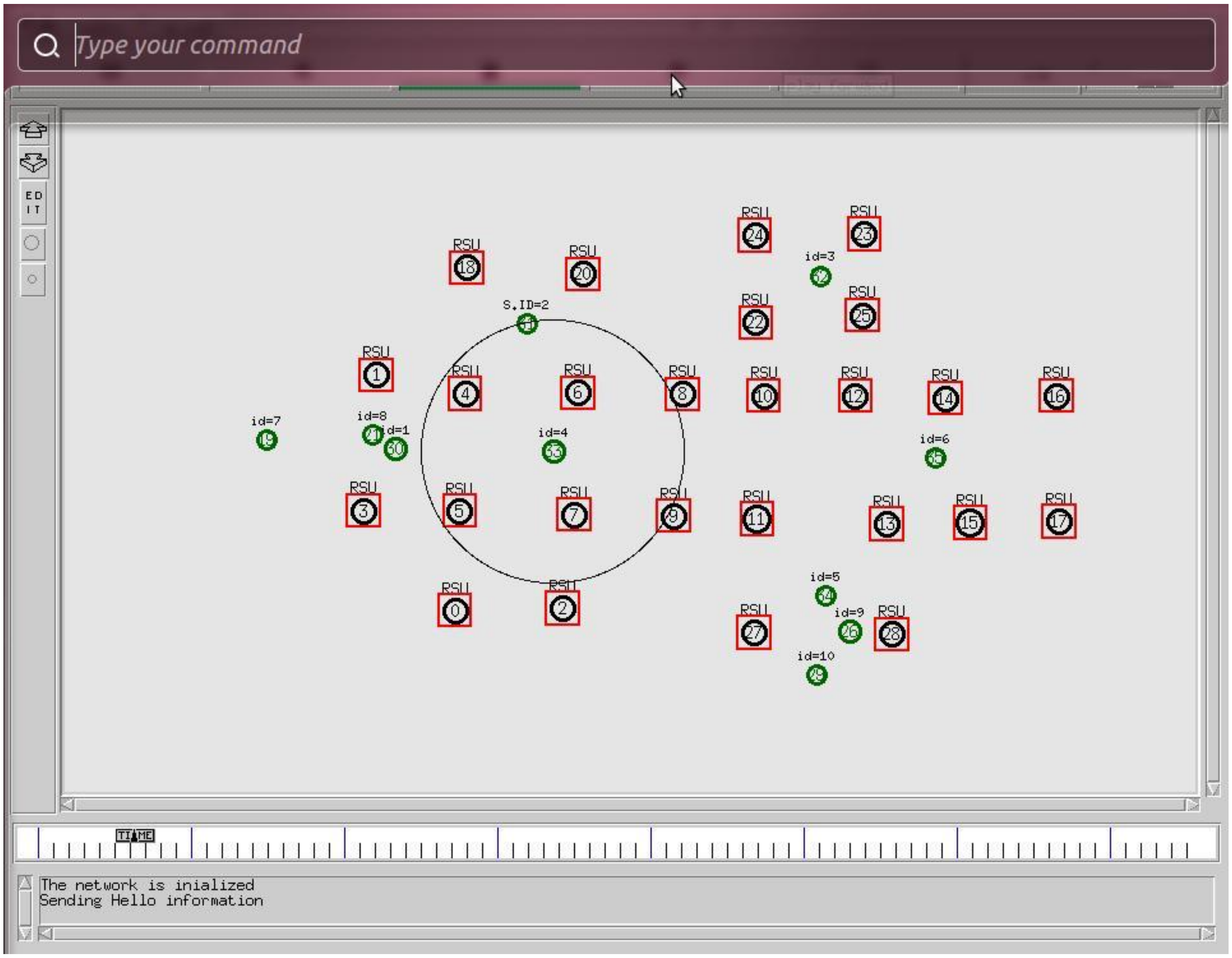
As illustrated in the figure5, the car having identification number 1 is communicating with the car having identification number 4 and then the malicious node is changing its identification number from 2 to identification 4.



```
New Id registed
Malicious Node trigger Attack
Communication starts between two nodes
```

Fig 14: Attack triggered

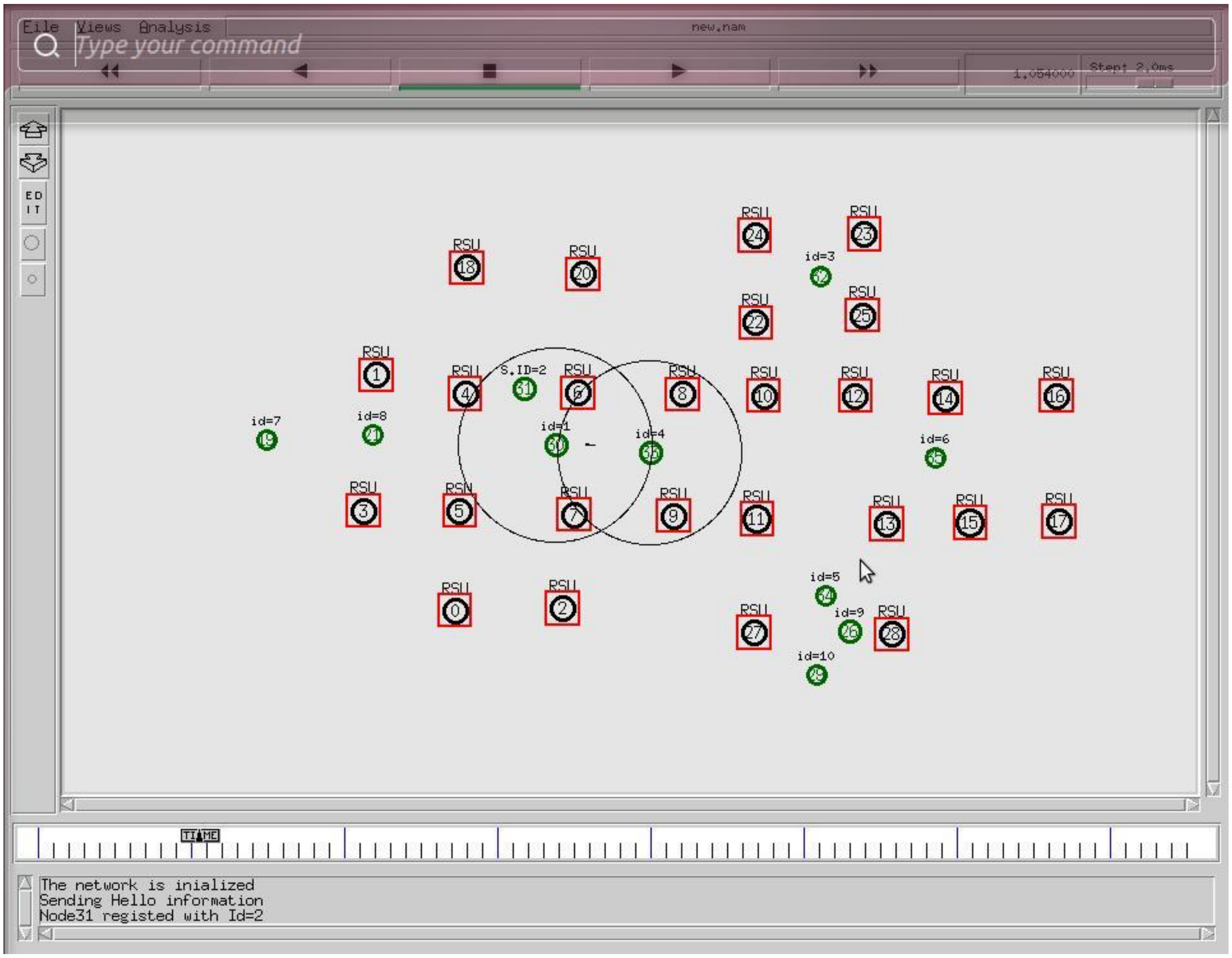
As shown in figure 6, the malicious node has changed its identification number from 2 to 4. The malicious node come closer to legitimate node. The source starts sending its data to the malicious node and Sybil attack has occurred in the network.



```
The network is inialized
Sending Hello information
```

Fig 15: Network Deployment

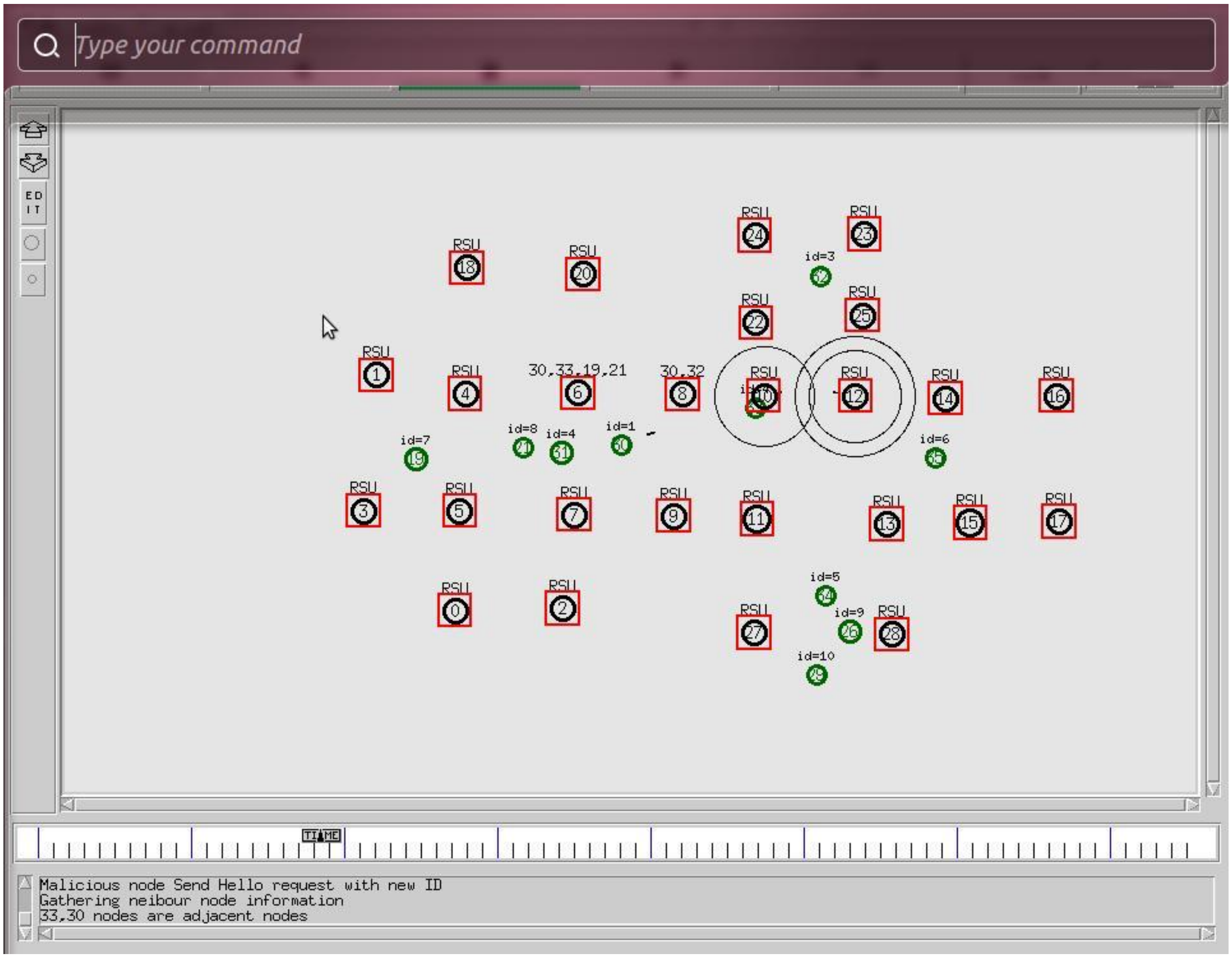
As illustrated in the figure 7, the vehicular adhoc network is arranged in such a way that there are number of road side units which are fixed and there are number of vehicles which can move freely in the network. They can communicate V2V and V2I.



```
The network is inialized
Sending Hello information
Node31 registed with Id=2
```

Fig 16: Communication starts

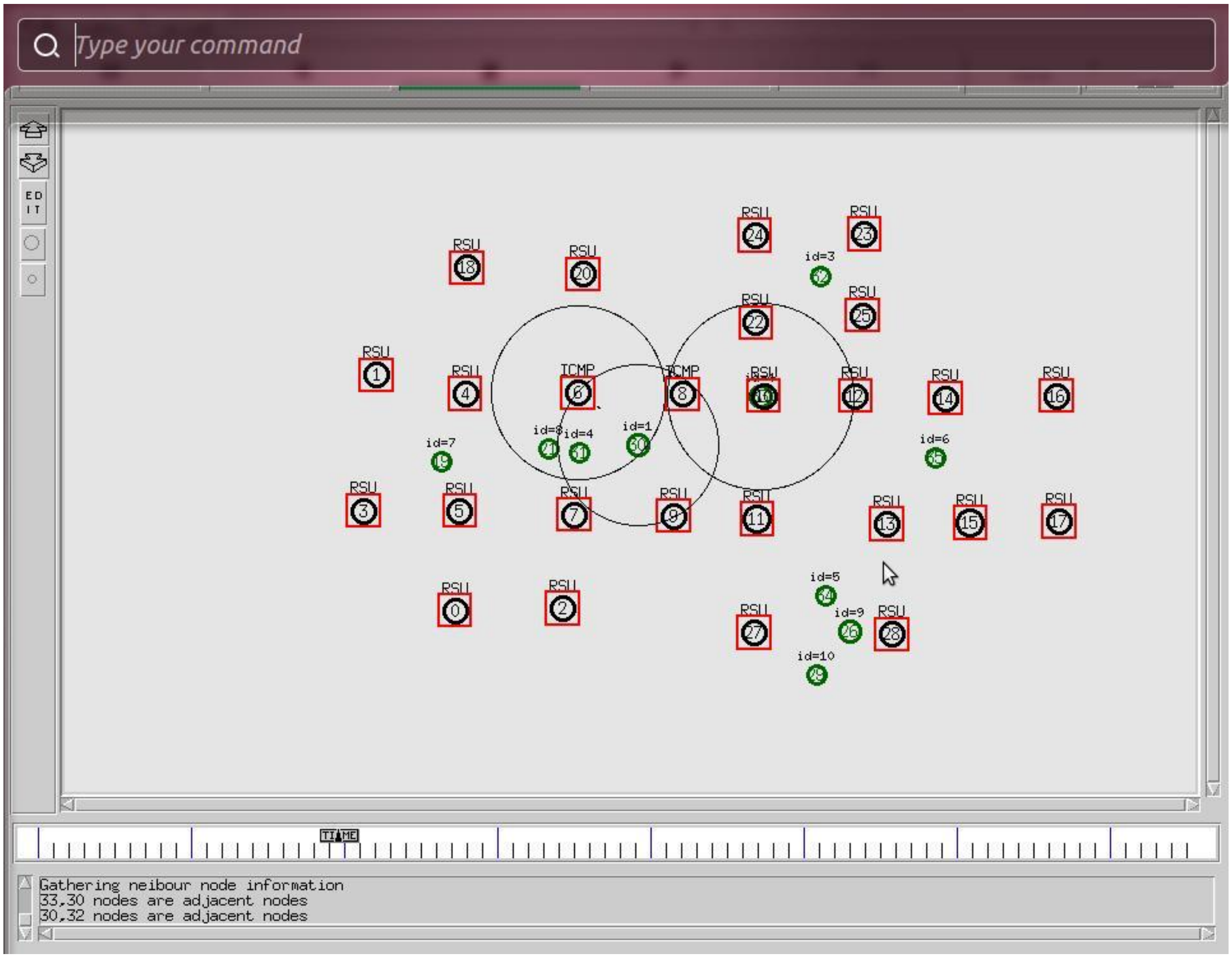
As illustrated in the figure 8, the network is arranged with the fixed number of road side sensor and smart cars, the smart cars are moving on the roads. At the time of registration, each vehicle gets its identification number to move freely in the network.



```
Malicious node Send Hello request with new ID
Gathering neibour node information
33,30 nodes are adjacent nodes
```

Fig 17: Getting signal strength information

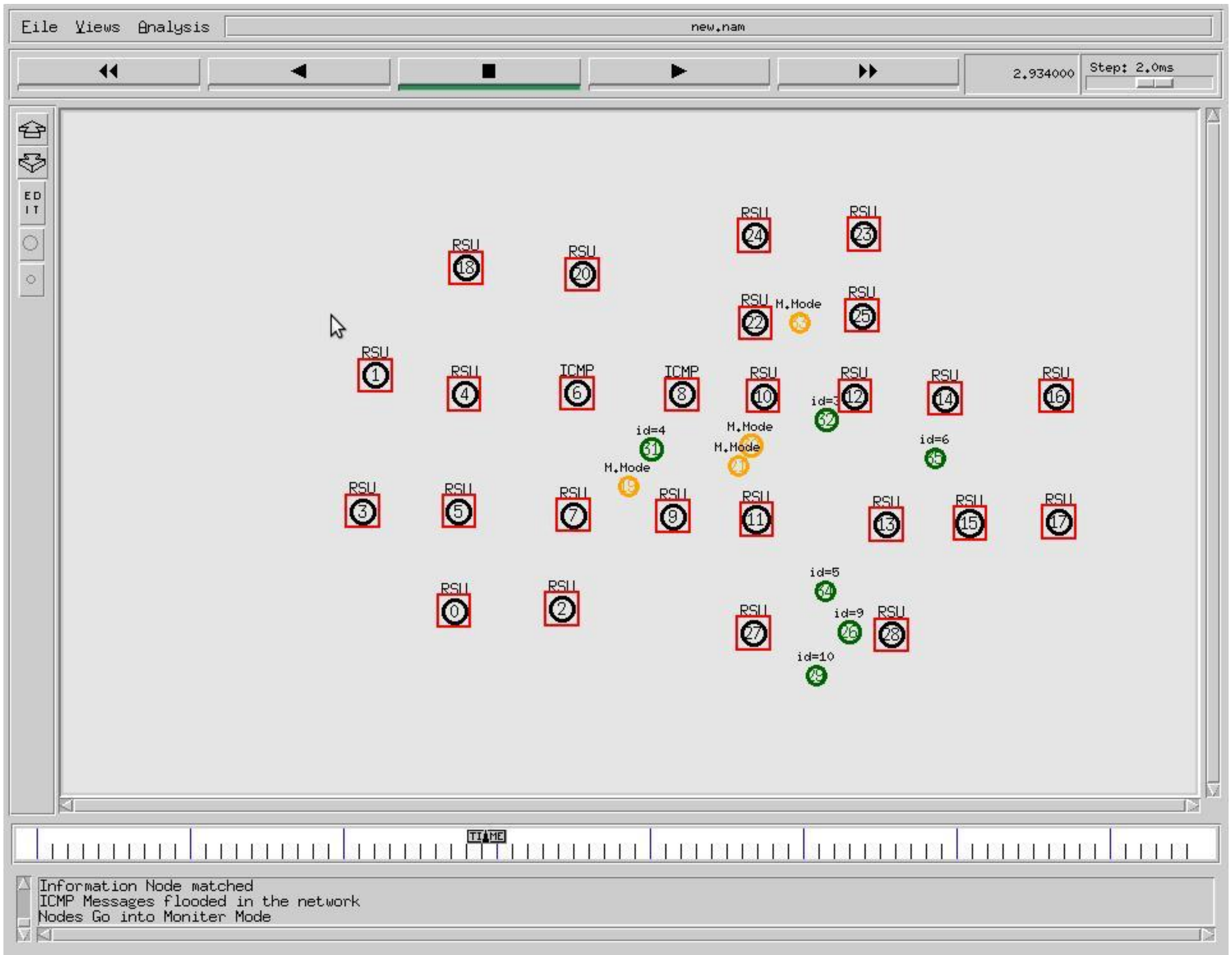
As shown in the figure 9, malicious node changes its identification and registers with the new id. The two legitimate cars i.e. car 2 and car 4 is communicating with each other. The road side units gather the signal strength of each car. As the two cars with same id are present in the network then the signal strength comes different. So the malicious node exists in the network.



```
Gathering neibour node information
33,30 nodes are adjacent nodes
30,32 nodes are adjacent nodes
```

Fig 18: Flooding of ICMP packets

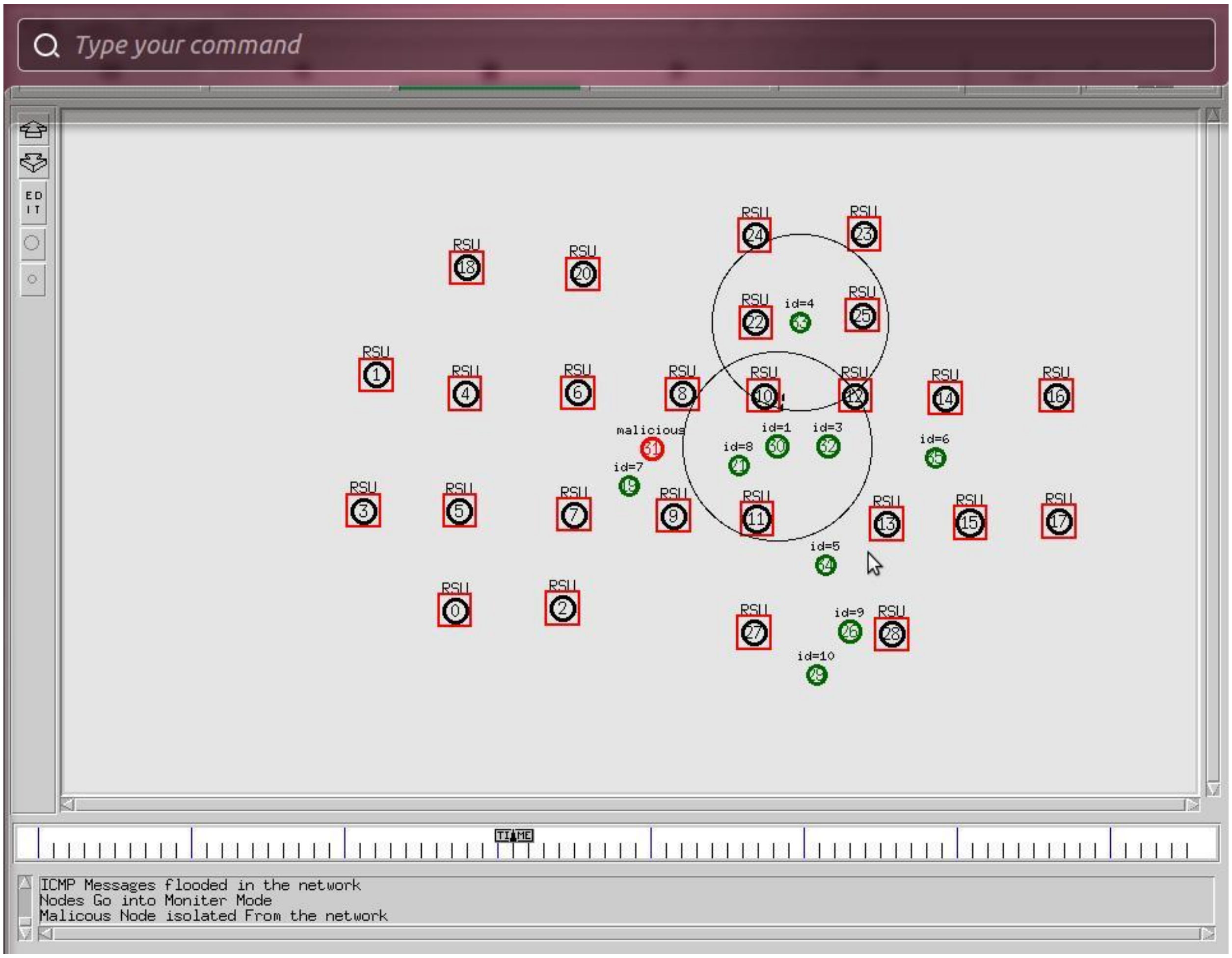
As illustrated in the figure 10, the neighbors of car having identification no 4 is different. The road side units start flooding the ICMP messages in the network to detect malicious node in the network. When cars receive ICMP messages, the nodes go to monitor mode.



```
Information Node matched
ICMP Messages flooded in the network
Nodes Go into Moniter Mode
```

Fig 19: The monitoring of adjacent nodes

As shown in the figure 11, 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.



```
ICMP Messages flooded in the network
Nodes Go into Moniter Mode
Malicous Node isolated From the network
```

Fig 20: Detection of malicious node

As shown in the figure 6, we have seen that malicious node has occurred in the network, the road side units start sending ICMP messages in the network. Upon receiving ICMP messages, the cars start to monitor the adjacent nodes. From the monitoring, the malicious nodes get detected.

4.2 COMPARISION WITH EXISTING TECHNIQUE

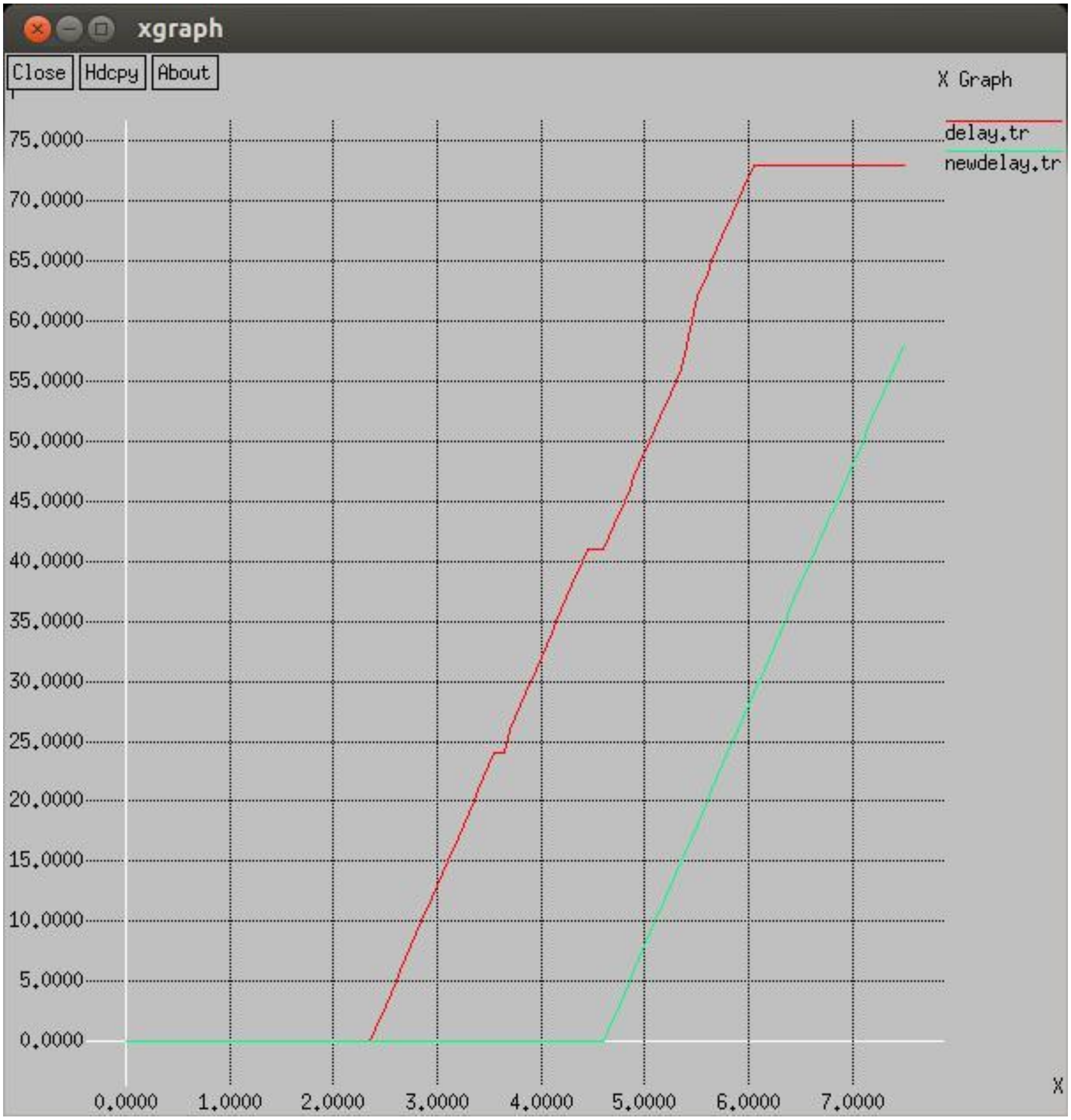


Fig 21: Delay Comparison

As shown in figure 13, the delay of the proposed and existing technique is compared and it is been analysed delay of the proposed technique is reduced isolation of Sybil attack in the network.

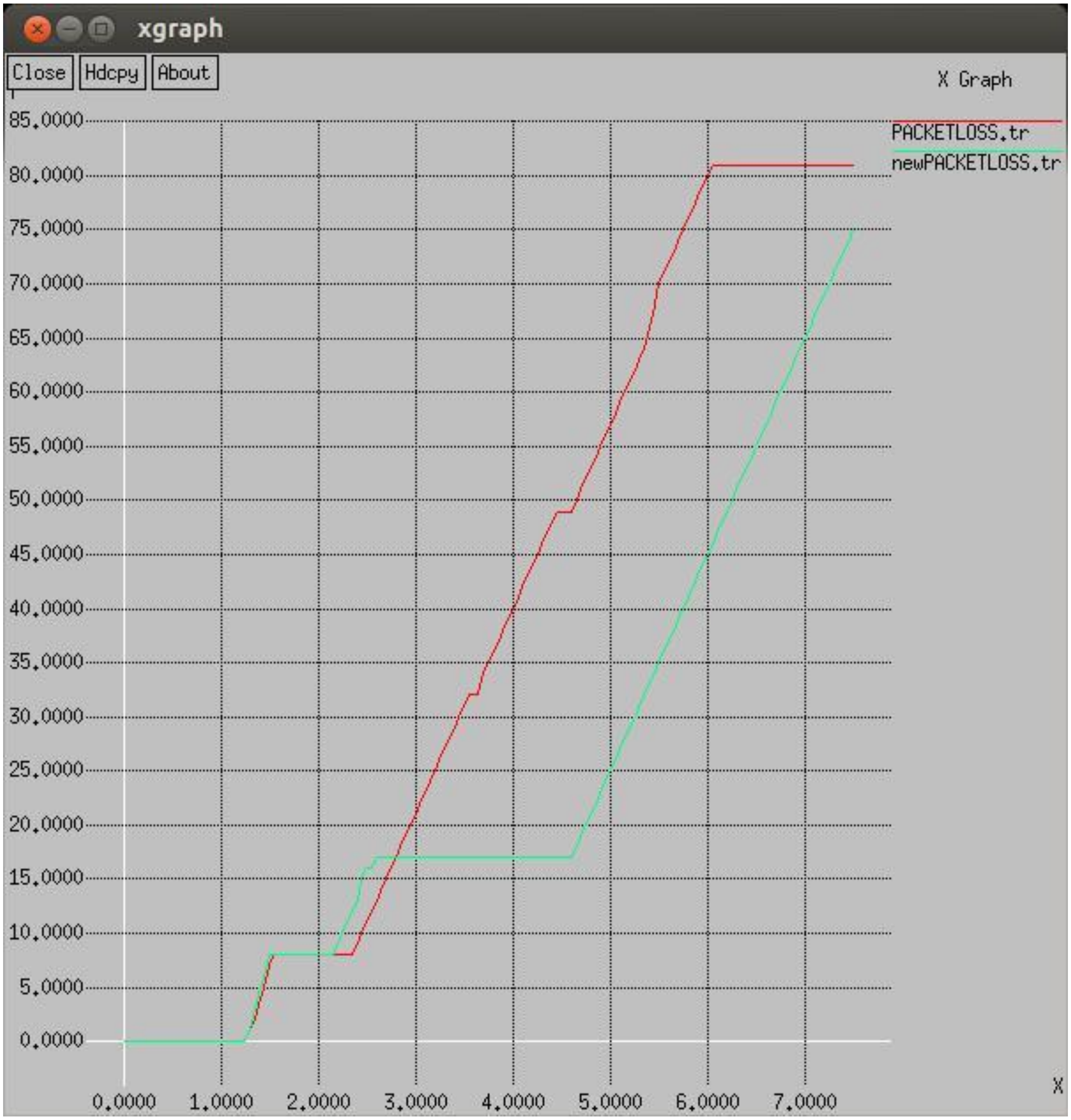


Fig 22: Packet loss comparison

As shown in figure 14, the packet loss of the proposed and existing technique is compared and it is been analysed that network packet loss is reduced when Sybil attack is isolated from the network.

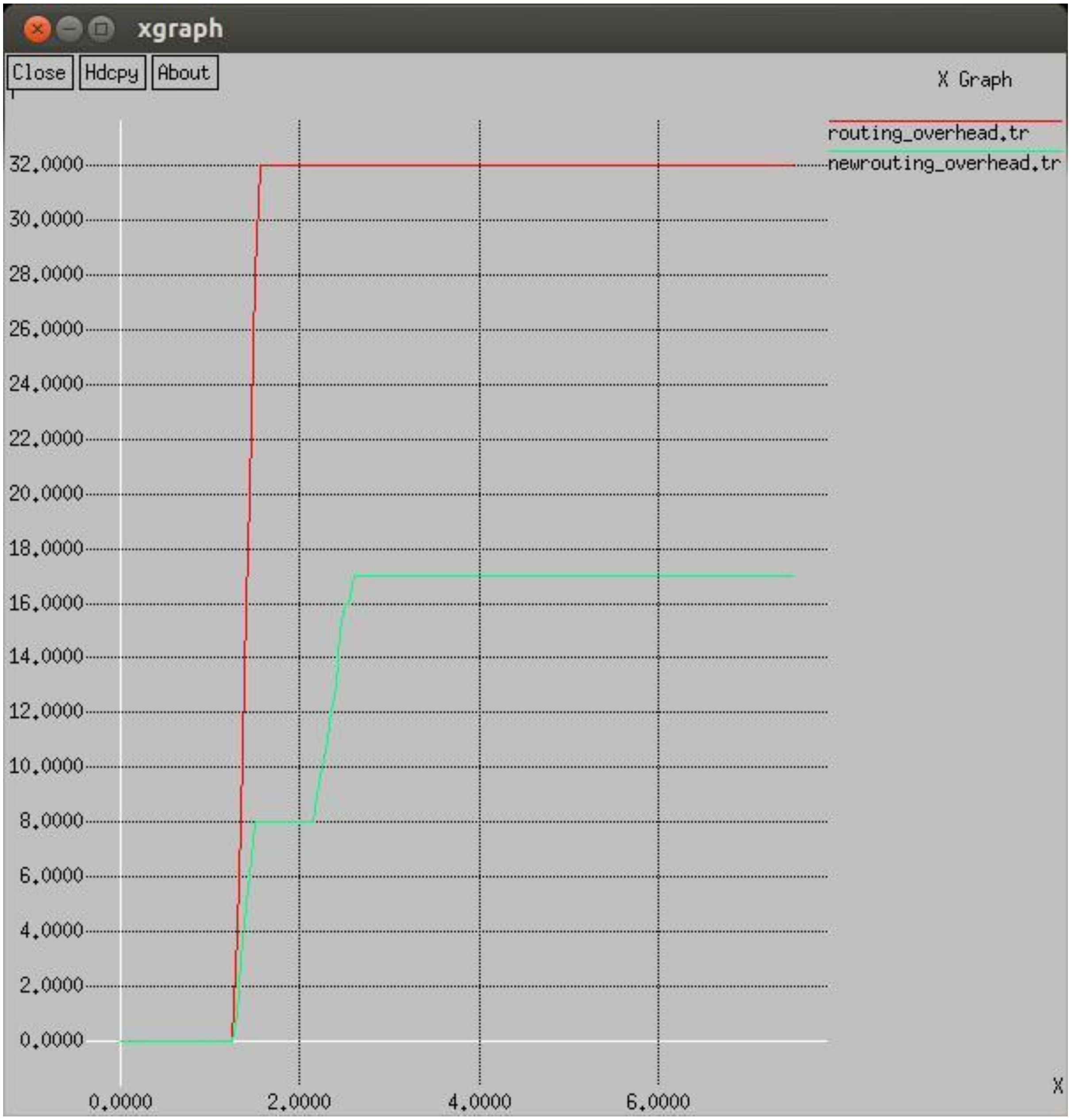


Fig 23: Routing overhead Comparison

As shown in figure 15, the routing overhead is the parameter which measures the extra number of packets which are transmitted in the network. The routing overhead in the network is reduced when attack is detected and isolated from the network.

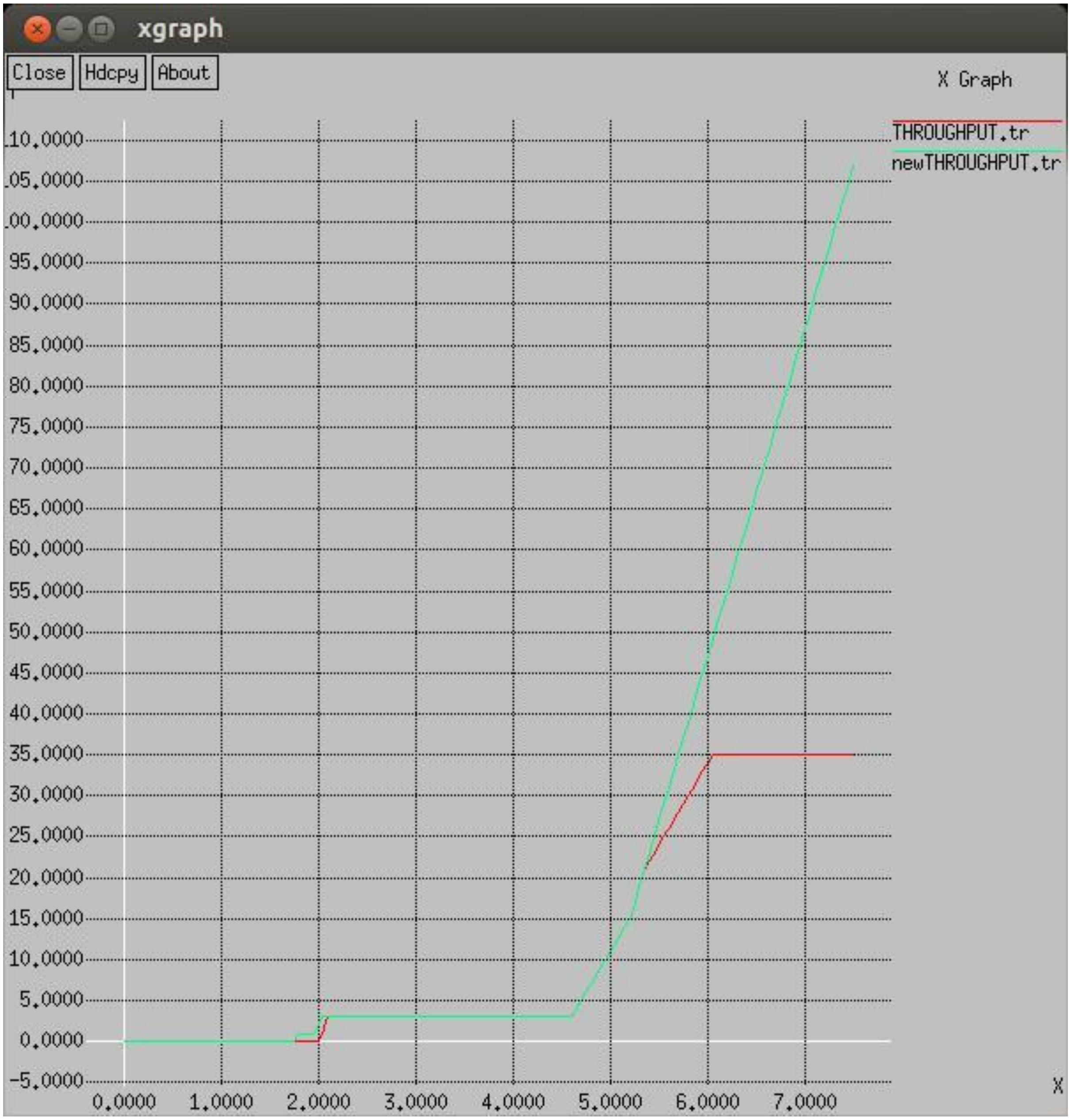


Fig 24: Throughput Comparison

As shown in figure 16, the throughput of the proposed and existing technique is compared and it is been analysed that after the malicious node isolation the network throughput is increased at steady rate.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 CONCLUSION

In this work, it is been concluded that broadcasting is the technique which is applied to select efficient path from source to destination. Due to decentralized nature of the network, sometime malicious nodes join the network which is responsible to trigger various types of active and passive attacks. This work depends on to detect malicious nodes from the network which are mindful to trigger Sybil assault in the network. The simulation of the proposed technique is been done in Ns2 and results shows that performance is increased in the network.

5.2 FUTURE SCOPE

Following are the various future prospective

1. The proposed technique can be applied to detect the sinkhole attack from the wireless sensor networks.
2. The proposed algorithm can be compared with the previously proposed algorithm to check authenticity of the technique.

REFERENCES

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

[2] Stephan Olariu"An Architecture for Traffic Incident Detection ", *MoMM2009, December 14–16, 2009, Kuala Lumpur, Malaysia.*

[3] Jeong-Ah Jang "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 "The security of vehicular ad hoc networks",ACM,2005

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

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

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

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

[9] Salim M.Zaki, M.A.ngadi,Maznah Kamat," A location based routing predicton service service protocol for vanet environment, IEEE, 2009

[10] Reena Didcach " Mobility simulation of Reactive protocol for Vanet", IEEE, 2012

[11] Rajesh Rajamani et al "On spacing policies for highway vehicle automation", *American control conference chicago, Illinois June 2000*

[12] Gang Liu and Han Guo, " Some aspects of road sweeping vehicle automation*", IEEE lasme international conference on advanced intelligent mechatronics,2001*

[13] Kung et.al “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, no. 5, pp. 483-502, 2002.*

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

[15] Su-Jin Kwag “Performance Evaluation of IEEE 802.11 Ad-hoc Network in Vehicle to Vehicle Communication ", *Mobility 06, 1-59593-519-3*

[16] Michel Hugo "Self-Organized Traffic Control", *VANET’10, September 24, o, Illinois,*

[17] Reena Dadhich Department of MCA, Govt. College of Engineering, Ajmer, India,” Mobility Simulation of Reactive Routing Protocols for Vehicular Ad-hoc Networks”(2011)

[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, IEEE, and Cristian Borcea, Member IEEE,” VANET Routing on City Roads using Real-Time Vehicular Traffic Information” (2008) 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, “Security Attack with an Effective Solution for DOS attack in VANET”, International Journal of Computer Applications (0975 – 8887) Volume 66– No.22, March 2013

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

[25] Bilal Mustafa Umar Waqas Raja School of Computing Blekinge Institute of Technology Box 520 SE – 372 25 Ronneby Sweden,” Issues of Routing in VANET”(2010)

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

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

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