A SECURITY FRAMEWORK FOR PREVENTING ATTACKER NODE USING WATCHDOG AND BAYESIAN THEORY

Dissertation submitted in fulfillment of the requirements for the degree of

MASTER OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

By

SHACHI SWAMI

11510269

Supervisor

Mr. HARJIT SINGH

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

June, 2017

PAC FORM

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : P172::M. Tech. (Computer Science and Engineering) [Full Time]

COURSE CODE : CSE545 **REGULAR/BACKLOG :** Regular **GROUP NUMBER :** CSERGD0300

Supervisor Name : Harjit Singh **UID :** 14952 **Designation :** Assistant Professor

Qualification : _____ **Research Experience :** _____

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Shachi Swami	11510269	2015	K1519	9530193884

SPECIALIZATION AREA : Database Systems **Supervisor Signature:** _____

PROPOSED TOPIC : A Security Framework for preventing attacker node using WATCHDOG and BAYESIAN theory

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	6.33
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	6.67
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	6.67
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.50
5	Social Applicability: Project work intends to solve a practical problem.	6.33
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	6.67

PAC Committee Members		
PAC Member 1 Name: Janpreet Singh	UID: 11266	Recommended (Y/N): Yes
PAC Member 2 Name: Harjeet Kaur	UID: 12427	Recommended (Y/N): Yes
PAC Member 3 Name: Sawal Tandon	UID: 14770	Recommended (Y/N): Yes
PAC Member 4 Name: Vikas Verma	UID: 11361	Recommended (Y/N): Yes
PAC Member 5 Name: Dr. Ramandeep Singh	UID: 14105	Recommended (Y/N): Yes
DAA Nominee Name: Kanwar Preet Singh	UID: 15367	Recommended (Y/N): Yes

Final Topic Approved by PAC: **A Security Framework for preventing attacker node using WATCHDOG and BAYESIAN theory**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11011::Dr. Rajeev Sobti **Approval Date:** 26 Oct 2016

ABSTRACT

The VANET is decentralized network in which communication takes places through moving or mobile nodes. The vehicle nodes are highly mobile nodes which can change its location at the steady rate. Malicious node becomes the part of network because of self configuring nature due to which various attacks like active and passive are triggered on network. The DDOS is a type of active attack because of which a malicious node selects and transfers control packet to other node which is being controlled by malicious node easily. The selected nodes are responsible to flood the victim node with the rough data packets. In this work, threshold based technique is been proposed in which network which is sending data above the threshold value will be responsible to trigger DDOS attack in the network.

Vehicular Ad-Hoc Networks (VANETs), an emerging profile for the improvement of road safety that has to be implemented all across the globe in coming years. Since the communication is carried out along an open wireless medium this makes the network more vulnerable to attacks. Vulnerability of the network can either be transmission of false information or vehicles assigned with fake identity, and they can possess inter-vehicle as well as vehicle-to-road side unit communication The proposed technique is been implemented in NS2 and it is been analyzed that proposed technique is performed well in terms of throughput, delay and packet loss.

DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation entitled "**A SECURITY FRAMEWORK FOR PREVENTING ATTACKER NODE USING WATCHDOG AND BAYESIAN FILTER"** 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.

Signature of Candidate

SHACHI SWAMI

11510269

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation entitled "**A SECURITY FRAMEWORK FOR PREVENTING ATTACKER NODE USING WATCHDOG AND BAYESIAN FILTER"**, submitted by **Shachi Swami** 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 de

Signature of Supervisor

Harjit Singh

Date:

Counter Signed by:

1) Concerned HOD:

HOD Signature: _____

HOD Name: _____

Date: _____

2) Neutral Examiners:

External Examiner

Signature: _____

Name: _____

Affiliation: _____

Date: _____

Internal Examiner

Signature: _____

Name: _____

Date: _____

ACKNOWLEDGEMENT

No research can be done in an isolated environment and this, certainly was not an exception. It was a concerted effort of all my friends, family and above all me. I would like to thank everyone from core of my heart.

I would like to express the deepest appreciation to my mentor, **Mr. HARJIT SINGH**, who has the attitude and the substance of a genius. He always helped to clear all doubts generated during different parts of this literature review and formulation of statement for my research work. His guidance is also a motivation for me to do work on time. His guidance was crucial for formulation of problem statement and carry forward approach.

TABLE OF CONTENTS

CONTENTS **PAGE NUMBER**

CONTENT **PAGE NUMBER**

LIST OF FIGURES

SUPERVISOR'S CHECKLIST

Name: **UID:** **Domain:**

Registration No.: **Name of student:**

Title of Dissertation:

☐ Front pages are as per the format.

☐ Topic on the PAC form and title page are same.

☐ Front page numbers are in roman and for report; it is like 1, 2, 3…….

☐ TOC, List of Figures, etc. are matching with the actual page numbers in the report.

☐ Font, Font Size, Margins, line Spacing, Alignment, etc. are as per the guidelines.

☐ Color prints are used for images and implementation snapshots.

☐ Captions and citations are provided for all the figures, tables etc. and are numbered and center aligned.

☐ All the equations used in the report are numbered.

☐ Citations are provided for all the references.

☐ Objectives are clearly defined.

☐ Minimum total number of pages of report is 50.

☐ Minimum references in report are 30.

Here by, I declare that I have verified the above mentioned points in the final dissertation report.

Signature of Supervisor with UID

CHAPTER 1
INTRODUCTION

1.1 Introduction to VANETs

There is a need of introducing communication technology within the vehicle-specific applications lately, various projects have been evolving within the networks of ad-hoc . Wider aspect is the Intelligent Transport System (ITS). There are various applications of the ITS which are also related to the Vehicle Transportation. The computerized system comprises of various components such as computers, communications, and management technologies as well as the sensor and control innovations. The functioning of a transportation system can be improved here by integrating these functions. For the purpose of enhancing the safety and efficiency of ground transportation networks, real-time information is required which is provided by these functions. The warnings related to environmental hazards, traffic and road conditions, and transmitting local information amongst vehicles is provided using the Vehicular Ad-Hoc Networks. If there is any such condition present where possibility of occurring various road closure, traffic jams and many accident casualty. The information can be spread across the network which might help the driver in avoiding the specific route as well as saving the time. The vehicles spread the warnings across the other vehicles through proper communication [1].

In case of emergency situations, the VANETs have proved to be beneficial due to their easy configuration as well as quick deployment. For asking any kind of help from other vehicles, a vehicle can send messages to other vehicles and can also inform the concerned authorities regarding problems they are facing on that road. For offering convenience and providing road safety VANETs are used in almost all areas. It is however, to be made sure that there are no invalid messages being sent across the network and the network is not being utilized in a malicious way. There is a possible situation to be present within the network in which the vehicles with their permanent identity can even easily ask for others help and mainly travel with very less fuel reserve. Even though their identity is familiar to attacker, it can monitor communication and will also try to extract information from the vulnerable vehicle present. It will continuously go behind other vehicle till it goes out with fuel and then finally attack it to

steal important information. Further, without contacting the authorities, the vehicle could be used in wrong manner. There can be a solution to this in which the permanent identity of the vehicle can be known only to its authorized personnel and hidden from all other vehicles. Through this, only the concerned authority will respond to any kind of issues which will help in assisting it and solving the issue. The protective measures taken here make sure that the information about which vehicle has asked for help regarding fuel shortage is not disclosed. This helps in ensuring the protection of the vehicle and related occupants. The nodes which are responsible for sending malicious messages across the network can be detected if the other vehicles are registered with some central authority. This is clearly meant that the nodes are to be identifiable for the messages generated through them. This results is providing proper authenticate measures within the network. The major privacy issues within VANETs involve the information as well as the communication privacy. It is easy for the malicious node to eavesdrop on the traffic of network if the information of the vehicle's location is disclosed within the network. It can also trace the details of the other vehicles present within the same location. There are various privacy enhancement techniques proposed to solve such issues. The main objective of VANETs here is to establish the requirements of the user to the road side units and even ensure a secure journey.

The Vehicular ad-hoc network has some special characteristics as compared to the MANETs. These characteristics are listed below [2]:

a. The VANETs are large-scale networks in which thousands of vehicles are deployed. The numbers of nodes which are present in network are large in number such that each vehicle can be registered within the network.

b. The mobility of the vehicles can be affected by the configuration of the road, the traffic laws as well as the speed limits. The behavior as well as interaction amongst the drivers is the reasons which affect the mobility of the vehicle. It is very complex to provide simulation in the vehicle traffic. It is thus a very tough task to simulate the vehicle traffic and provides the study for applications in the transportation engineering.

c. As compared to the typical mobile devices which are involved in MANETs, more resources are to be accessed by vehicles in the case of VANETs. There are large batteries, antennas, as

well as the processing power provided here. So it is not necessary to provide resource conservations measures here.

There are vehicles as well as road-side infrastructure units (RSUs) present in the VANETs. The vehicles can easily with other vehicles present in network as well as with the RSUs using VANETs. The RSUs are referred to as the fixed entities as well as the mobile entities are the vehicles. There can be one-hop communication amongst vehicles in VANETs or multi-hop in which the vehicles can act as routers and retransmit the messages. So, here the vehicles which communicate with other vehicles in a very direct manner each other and can transfer messages among various vehicles present in the network. The nature of the message is an important factor which determines the type of communication. The one-hop communication can be provided if the vehicles wish to communicate on individual basis. If the vehicle requires a certificate authority (CA) to travel along with it, a message is broadcasted and [assed across the network. This stops once the RSU is reached and this type of communication is known as multi-hop type of communication [3].

1.1.1 VANET Architecture

There are 3 domains in which the architecture of VANET is divided. They are In Vehicle domain. And the other one is infrastructure domain. Within first domain (vehicle) various units like on board (OBU) as well as units like application (AU) are present .When interacting with the OBU, the AUs perform various functions as they are the user devices. The ad hoc network comprises of the OBU's which are present in the vehicles as well as the RSUs which are present along the roadside. When within a proper range, the various units like on board and road side units easily transfer information to one another in wireless medium. Domain of ad-hoc is formed as the vehicles are directly to attaches to various road side units in ad-hoc medium according to their requirements. There are RSUs and CA present within the Infrastructure Domain. There is a connection between the CA and the RSU. The RSU here acts as a proxy for the CA. When the packet is to be forwarded from one OBU to another.

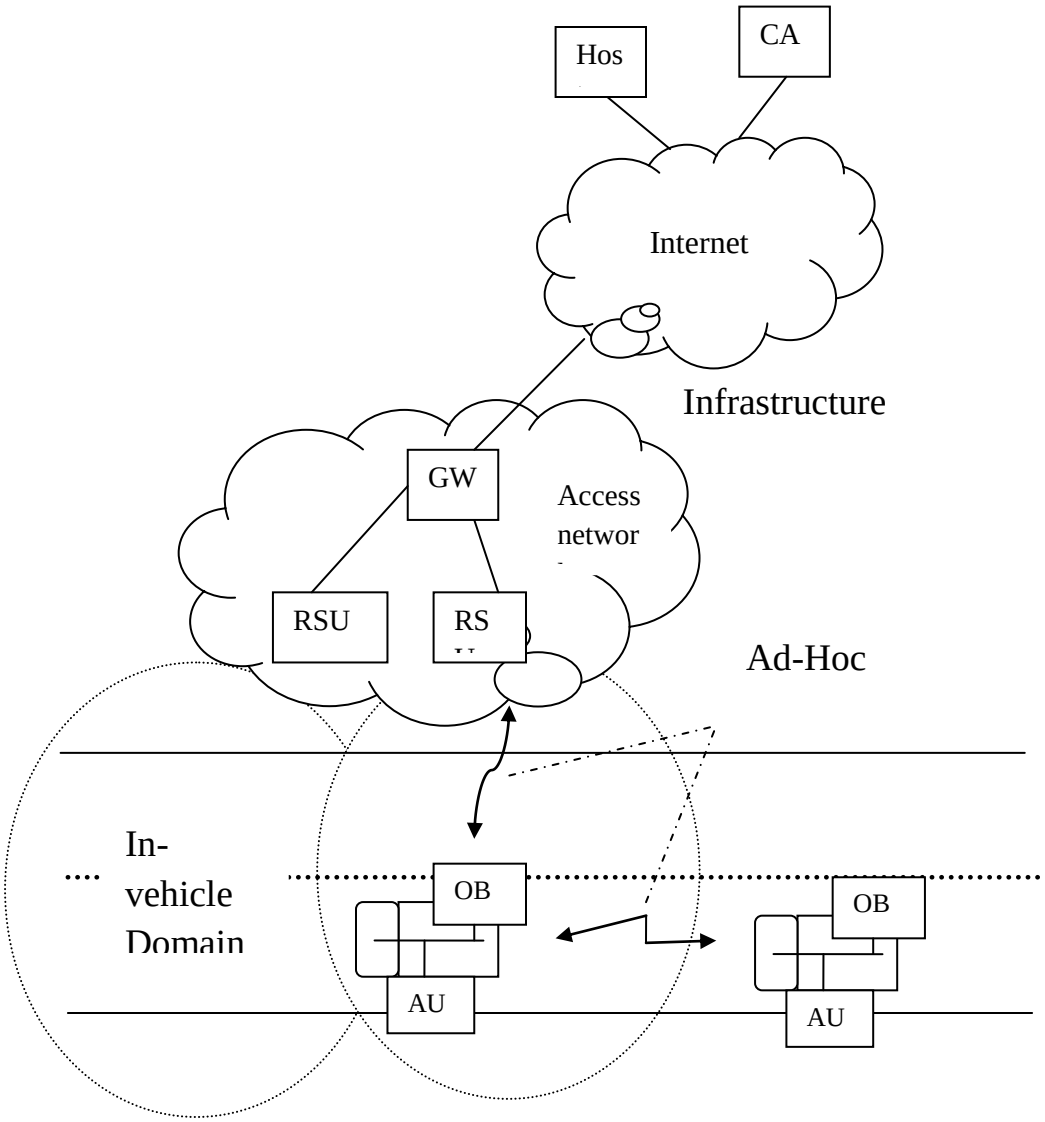

Figure 1: VANET system architecture

1.1.2 Applications of VANETs

For the purpose of enhancing the transportation safety as well as efficiency, the VANETs are proposed. An example of one such application is the cooperative collision avoiding. The speed of wireless communications is high due to which the drivers can receive alerts early due to which the accidents can be prevented. The driver stops the vehicle before the accident can occur. This

helps in providing safer transportation. The usage of VANETs for safety purposes is just one area which is explained below along with various other applications. They are as follows:

Safety Applications: For the purpose of reducing the delay in propagating emergency warnings, the VANETs can be utilized. The messages are exchanged amongst the vehicles for the purpose of notifying them in case of any possibility of danger. The neighboring vehicles are to be notified as soon as any vehicle recognizes certain situation. At any situation, the reaction or response is very quick. The information which is gathered by the sensors present in the vehicles such as the ABS, ESP, etc is sent through the warning messages to the other vehicles. The traffic congestion method also provides certain information which can also be utilized here. The Emergency Electronic Brake Light is the kind of warning message which is sent by the vehicles which allows the vehicles to provide a sudden braking in the forward path in which the hazard is possible. Here, the speed of the vehicles is reduced which helps them to prevent many vehicles and accidents. events or tasks such as deployment of airbags, loss of tyre traction or applying sudden brakes are also detected with the help of n-board sensors. The vehicular communication is utilized here mainly to gather the surrounding vehicle dynamics for warning the drivers in case of any possibility of collisions. A warning could be given to the rest of the vehicles in case any emergency vehicle such as a police car, fire engine or ambulance, is to be made to pass. The current position, time and destination of the emergency vehicle are provided such that the rest of the vehicles can stay away and provide a clear route for them. There is a reduction in the reaction time required at a certain incident of accident related to the emergency vehicles. The signal is given to the emergency vehicle which influences the infrastructure behavior and further results in reducing the response time of an emergency vehicle [5].

a. **Automated Highways:** For advancing the driving safety as well as enhancing the capacity of highways the automation of various driving functions is required. There are certain applications which are involved in the Vehicle-to-Roadside Units Communication. There is a proper assistance as well as warning given to the drivers when required during driving which helps in providing a safe driving scenario.
b. **Local Traffic Information Systems:** The distribution of information from RSU to vehicles can be done with the help of radio broadcasting. Without the involvement of RDS (Radio Data System) the traffic information can be distributed with the help of

onboard sensors, GPS and digital maps. This can help in creating powerful traffic information system. There can be a rapid as well as economic distribution of traffic information using the VANET communication. The drivers are mainly concerned with the traffic information related to the surroundings of the current location of the driver or the area it is destined or about to enter.

c. **IP based applications:** For the purpose of passenger's comfort and entertainment, the applications of VANETs are also required. For the purpose of accessing applications some traditional IP-based services are required. This requirement also needs the connectivity to Internet. The companies which try to sell product such as online games and promotional broadcasts are also an example of the applications. However, the VANET does not require any central access; this application contradicts the characteristics of VANETs. There might not be any connection with the Internet at various times. The main objective of VANET here is the safety improvement and the application contradicts it by not following the rule [6].

Convenient and safe driving is ensured with the help of VANETs. The safety of roads can automatically be improved when the ambulances are automatically identified or when the vehicles are notified if attacks are going to occur or not. A convenient information exchange is must of providing warnings on roads in order to provide communication with other vehicles.

1.1.3 VANET characteristics

There are various characteristics of VANETs. These characteristics create complications when the network is to be deployed. The various challenges are enlisted below:

a. **High Mobility:** There can be handshake based protocols within the network due to the fact that the vehicles are mobile and choose broadcast communications. Avoiding excess of exchange of information, the vehicles require authentication. If there is a chance of involving excess of exchange of information amongst the vehicles it can result in keeping the vehicles out of range before the authentication procedure ends. This is mainly because of highly mobile vehicles in network. There might be also problems such as providing paths with shorter lifetime amongst the nodes due to the high mobility. This might result in the partitioning of the network.

b. **Real time delivery of messages:** In the case of safety applications, the VANETs involve certain time constraints due to their involvement in emergency situations for alerting other vehicles for avoiding collisions, accidents or hazards. For this, there are certain deadlines which are very necessary to be met or the results might not be good. In case where an accident has occurred at an instant, the emergency authority must be made available at that current situation. If the help does not receive on time, it can result in loss of lives or traffic jams etc. There is no requirement of vehicles to communicate for a longer duration because of highly mobile vehicles in network. Also secure channel is established at higher speed. So, it can be said that the real time delivery of messages is very important .

c. **Location Awareness:** There is a GPS or certain location based tool involved in various location based applications. However, if any error occurs in these devices, the application involving VANET can directly be affected. For avoiding such situations, the installation and maintenance of these devices on regular basis is very important and must be performed. If there is any type of malfunctioning observed, the concerned authority must be informed immediately.

d. **Security:** There is no structured network involved in the VANETs. There is a chance that the untrustworthy nodes might enter the network for routing control and data messages. This makes the security of VANETs a much difficult task. The messages can possibly subject to corruption is there are such untrustworthy nodes involved in the routing of messages. For the purpose of maintaining the security, a secure routing, transport protocols as well as the identification of malicious user are very important. There are mainly four objectives which should be taken under consideration while maintaining the security of the network.

1.2 Routing in VANETs

The information related to link is used within the network for transferring the data packets from the source to the destination node in case of topology routing protocols. three broader classifications of these protocols [8]:

- Proactive

- Reactive
- Hybrid

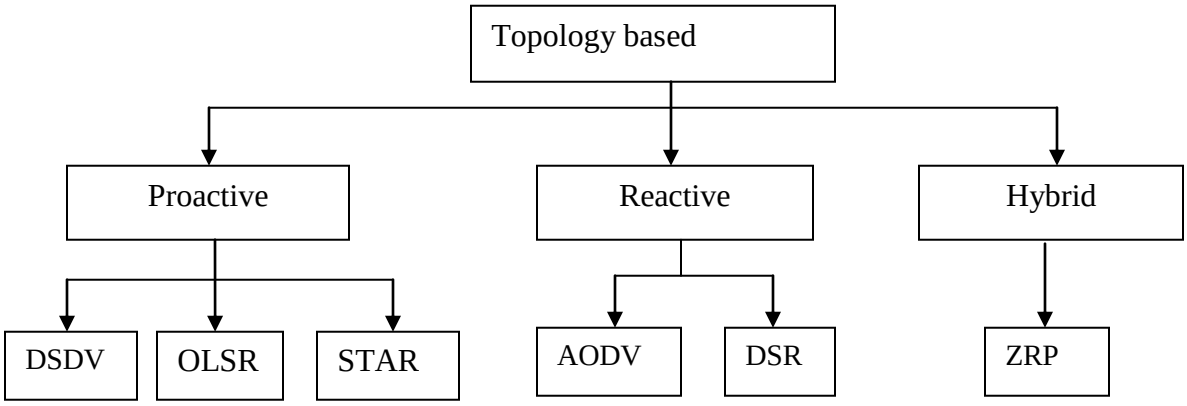

Figure 2: Topology based routing

a. Proactive protocol: basis of shortest path algorithms most of proactive protocols are built. The information gathered from various nodes are kept in tabular form and they are table depended. The table created is shared amongst the neighbors and in case any changes occur, each node updates its routing table as per those changes. There are various proactive methods such as link-state and the distance routing.

- Destination Sequence Distance Vector Routing (DSDV): loop free single path is provided towards the destination in this algorithm. There are two packets sent by the Instead of sending complete routing information, only the bandwidth utilization is reduced by sending the updates. However, the overhead in the network is still increased due to the incremental. This is due to the reason that the large scale networks are not able to adopt them due to such frequent incremental packets achieved.
- Optimized link state routing (OLSR): By sending link state information, the information maintained by this protocol. The updates are sent by each node to certain selective nodes once any change occurs within the network. Here, only once an update is received by the each node within the network. The updates cannot be retransmitted by the unselected packets. Only the updated information can be read here.
- Source-Tree Adaptive Routing (STAR): Within each router, the preferred routes are saved at each destination. By eliminating the periodic updates, the overhead in the

network is reduced. Unless any event occurs, there is no requirement of sending any kind of updates in the network. Although there is need of large memory as well as processing due to its need to maintain large trees for the complete network, this is used in these large scale networks.

As the distance vector routing requires higher bandwidth for sharing the information amongst the neighbors, the proactive based routing protocols might not be applicable in the case of high mobility nodes. In the case of large networks, the size of the table also increases. This might require huge memory and processing. The nodes have higher mobility in VANETs and so proactive routing protocols are not much beneficial .

b. Reactive Routing: The overhead which is made through the proactive r protocols can be overcome using the on-demand or reactive routing protocols. Only the routes which are currently active are maintained here using this type of protocol. The nodes which are currently being utilized for sending the packets from the source to destination are only highlighted here for route discovery and maintenance. By sending the RREQ (Route Request) from one node to establish the route for sending data at particular destination is done through route discovery. The node waits for RREP (Route Reply) once the RREQ is sent. If any RREP is not received within certain duration, it is assumed by the source node that the route is either unavailable or has expired. If the RREP is received at certain destination, the uncasing method is utilized for forwarding the information for ensuring that the route is present in communication. Mainly two categories classification of reactive protocols. The information is taken from the data packet and stored in the header by each node while forwarding them to other intermediate nodes within the network. Thus, for sending a packet to certain destination, there is no need to update the complete routing information by each intermediate node. This type of routing is not suitable for the large scale networks which include numerous nodes which have dynamic natures such as VANETs. There might be chances of route failure because of huge nodes present within network, might also be chances of network overhead and increment in the route information present in the header of each node due to the increment in the number of intermediate nodes. This is due the fact that there is a next hop and a destination address present for each data packet here. Thus, for sending the data packet to certain destination, the intermediate nodes involve the routing table information. In cases where sudden changes occur within the network, this methodology can

prove to be helpful. Fresh routing table information is received once the topology changes and new routes are selected as per the requirement. For the purpose of sending data packets towards the destination, the selected routes are thus utilized. The routing information as well as the carried knowledge related to each neighboring node is updates in these types of routing protocols. Therefore, in the case of highly mobile networks reactive routing can taken.

On Demand Distance Vector Routing in ad-hoc: It comes to category of reactive protocols. It involves the multi-hop type of reactive routing. As per the demand of the network, this protocol works and the demands are accomplished by utilizing the nodes within the network. Even when only two nodes require communicating amongst each other, the route discovery as well as maintenance is performed as per the demand. For remaining active at all instants and update the routing information at all durations, the need of nodes is not required here. So, only as per the requirements when the communication is performed, only then the maintenance and discovery of routes is to be made by AODV. The network load is reduced by broadcasting the route discovery mechanism with the help of AODV, present amongst intermediate nodes is utilized for maintaining the change in the topology as well as loop free routing. For this purpose the Destination Sequence Numbers of DSDV are utilized.

- Dynamic Source Routing DSR: This type of protocol is used in many multi-hop wireless networks. There are two operations performed here. The route discoveries as well as the routes maintenances are these two operations which make this protocol self-configuring and self-organizing. There is no need of any centralized administrator or infrastructure for managing the DSR routing protocol. The routes from the source to destination are required for discovering routes through this protocol.. At any instant in the network, the routing information for each source node can be changed. The updates are made by DSR once any change occurs. No routing information is required for routing the passing traffic by the intermediate nodes. However, the information is stored for future use. The overhead on the network is reduced using the DSR and also the self organizing and self configuring protocol is designed here .

c. Hybrid Routing: It has the features of both reactive and routing protocols. are combined in the case of hybrid routing protocols. This helps in providing more scalable and efficient routing protocols. The protocols involved in the hybrid category are mainly disadvantages observed in

the proactive and reactive routing protocols are removed here by proposing new hybrid protocols. For example, the issue of providing limited number of route searchers can be resolved here.

- Zone Routing Protocol (ZRP): The range of the proactive routing methods is limited up to the neighboring nodes locally using the ZRP. In case of reactive routing the ZRP searches the. The flexible route discovery and route maintenance can be provided using the "Intrazone" and "Interzone" through ZRP in the multiple networks. The reactive routing globally performs route discovery using the Interzone routing. The up-to-date route information is maintained locally as per its routing range in the case of intrazone routing based on proactive routing. The main aim of ZRP is to reduce the is reduced here. The route discovery performed is very efficient. The disadvantage of ZRP is that it. The disadvantage of ZRP is that in case where the behavior of nodes in highly dynamic and the topology changes are rapid, this cannot be used. The environment in which the nodes are not highly mobile and there are limited numbers of nodes, this routing protocol can be used .

1.3 Data Dissemination

There is a fixed mode of communication in vehicles and the road side units (RSUs). This problem can be solved using the data dissemination technique. Due to continuous topology changes as well as the limited range provided for wireless communication, on basis of global Channel State Information (CSI) there cannot be optimized scheduling decisions be provided by the distributed data dissemination techniques. This is due to the absence of the central controller in the architecture. As per the pre-determined rules the due to which fact that there is very little knowledge of the complete network. This will provide only certain level of local optimum within the network. Within the denser networks, there might be chances of collisions which will further result in causing delay in transmission of data. Due to this reason, the time cost for each data retransmission will increase for the complete network. The centralized scheduling systems result in providing increased throughput as well as reduction in the collision probabilities which is not provided by the distributed cooperative data dissemination techniques. The control server (CS) provides the decision-making for scheduling [14]. The vehicles which have highest utility as relay nodes are selected and the transmission frames are allocated to them as per the requirement.

In the case of earlier centralized scheduling techniques, CS need to gather the real time full CSI from the vehicles first, as it can only then make efficient scheduling decisions. The communication overhead increases here. Minimum of some milliseconds of CSI measurement collection is observed at the control server by the overall delay of CSI. Even if the measurement in correct, the full CSI will be outdated for scheduling here.

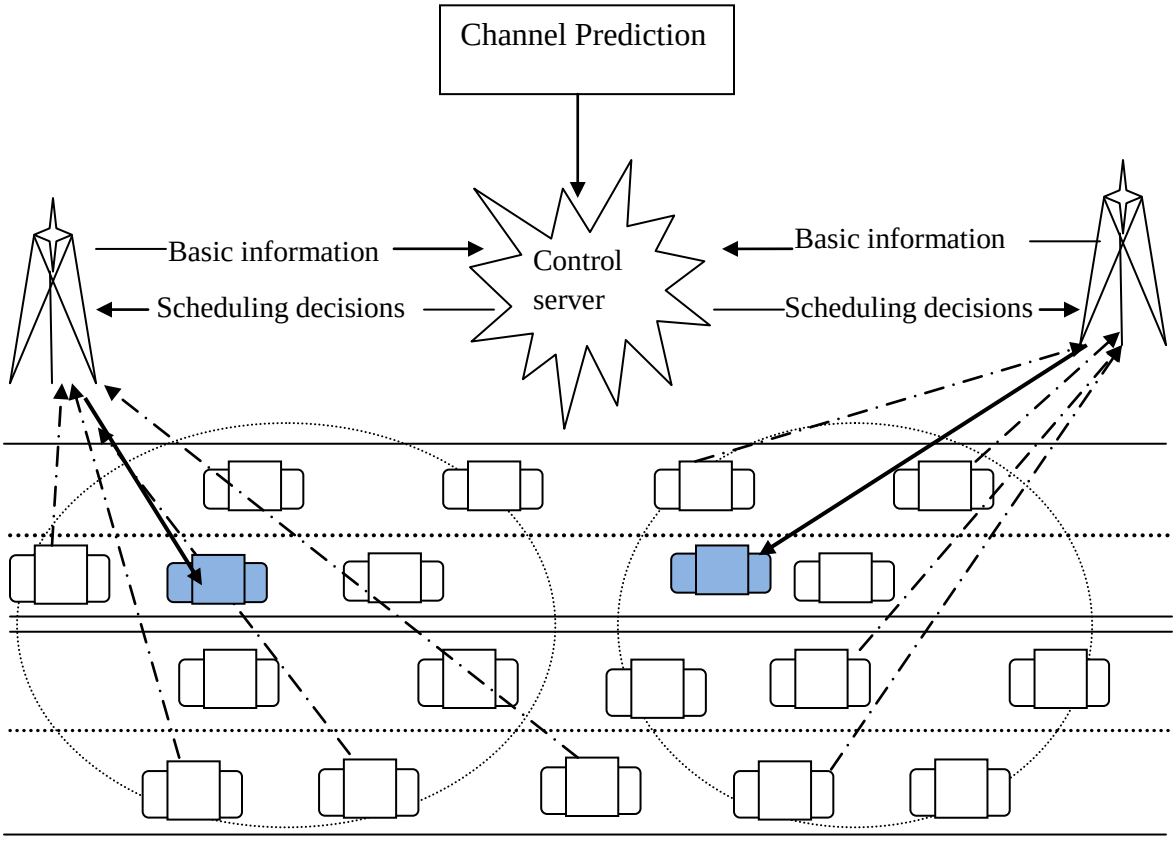

Figure 3: Cooperative data dissemination model with channel prediction

1.3.1 Challenges in Data Dissemination:

The process of spreading information across the distributed networks is known as data dissemination. The efficiency of traffic systems within the VANETs is enhanced through the involvement of data dissemination which further improves the quality of driving. Due to the fact that there are large numbers of vehicles available on the road, the communication amongst vehicles is not as easy as it seems to be. So, the transmission of data across the network is a very important issue. Various other challenging tasks observed here in the data dissemination techniques are described below:

i) High Mobility and Frequent Disconnections: The high mobility as well as the frequent disconnection of the topology at various regions in an area is the major challenge here. In the night as well as in the suburban areas, the traffic density is so low. However, in cities while their main hours of working, the network node density is extremely high. This might result in frequent network disconnection. There is no single solution for the disseminating the data to all there recipients available.

ii) Data Transmission in case of Disconnection: other major issue here is ensuring data transmission across the network which has less delay and before any disconnection occurs amongst the vehicles. The disconnection is not such a big issue when the target vehicles are in the closer range of the roadside unit within the dense network. In case where the vehicles are in the radio range and request for the similar data at same duration and are utilizing the wireless media the bandwidth utilization is the major concern. The data is transmitted to the highest throughput once the vehicle reaches at one-hop range of the RSUs. The connection time is most likely extended at the time when vehicles connect with each other as well as the RSU for spreading more data.

iii) Distribution of data over mesh nodes: A mesh like network is formed and data is disseminated to the vehicles when the roadside units are connected to each other for providing accurate data dissemination. This results in difficulty in distributing the data within the mesh network.

1.3.2 Types of Data Dissemination

With the help of data dissemination, the data is spread across the network while ensuring the optimum usage of network resources for fulfilling the requirements of users. Various data dissemination in vehicular ad-hoc network is:

i) Dissemination in V2I/I2V

ii) Dissemination in vehicle to vehicle (V2V)

iii) Dissemination in Opportunistic

iv) Dissemination in Peer-to-peer

v) Dissemination in Cluster

i) V2I/I2V Dissemination: There are two main mechanisms involved here which are, the push based as well as the pull based. Within the push data dissemination, the pouring of data as well as concept of buffering is involved. The road which has high mobile vehicles is selected within the data pouring method. The data broadcasted through data center to the different vehicle on the similar and crossing roads. The computer which uses wireless interface for gathering the data from surroundings and further delivers it to the vehicles is known as the data center. For the purpose of storing data the buffers are placed at the intersection points across the network. Further the data is transmitted to the mobile vehicles from these buffers. This concludes that the data is transferred from the mobile vehicles or RSUs to various vehicles in the case of push type data dissemination. Where vehicles wish to gather various packet information mainly through data centre or by using other vehicles, pull type data dissemination method is most commonly used. For purpose in making queries and receiving response this method is mostly utilized.

ii) V2V Dissemination: The flooding and relaying methods are utilized for vehicle to vehicle data dissemination. All of the nodes which are involved in data dissemination are used for broadcasting data in flooding which also involves the one to all communication. There is a selection of relay node or data is forwarded through the nodes towards next relay hop and the process continues, and the process is called relay type of data dissemination. This type of approach is mainly considered for congested networks.

iii) Opportunistic dissemination: The information is present in each intermediate node and also can transfer it to next coming node within opportunistic data dissemination networks. This continues until it reaches the destination node .

iv) Peer-to-Peer Dissemination: Here, the storage device is used to store data by the source node and the data is further sent across the network as per the requirement of other nodes.

v) Cluster Based Dissemination: There is a relay involving less number of intermediate node within network for reducing the broadcast storms and achieving better delivery ratio. To achieve this, the nodes kept in form of various clusters where nodes gather the data within the cluster thereafter forward to next set of present cluster.

1.4 Distributed Denial of Service Attack

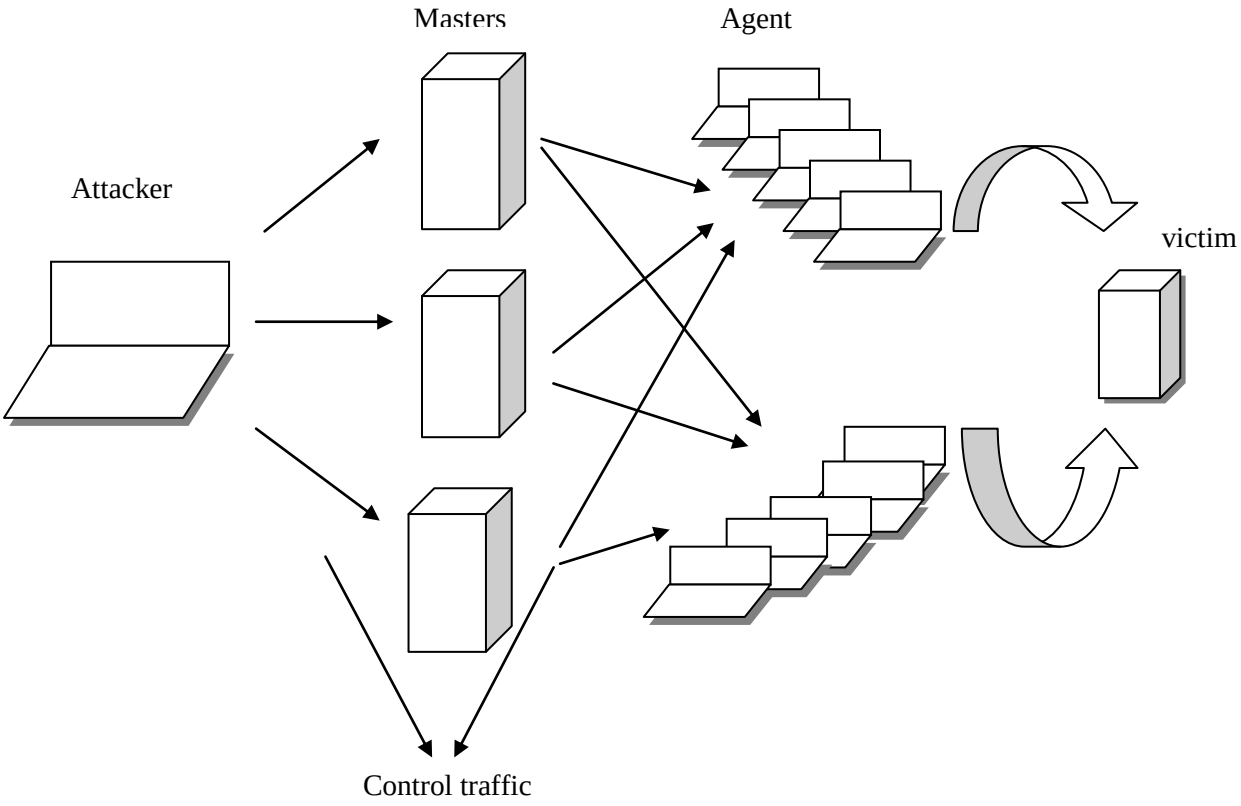

Figure 4: Distributed denial of service attack

"Typically" DoS attacks are being created by a single host (or minimal number of hosts at a comparative area). The principle genuine route for DoS assaults to force a genuine danger is to misuse some product or configuration imperfection. Such blemishes can fuse, for instance, wrong usage of the IP stack, which crash the whole host while getting a non-standard IP bundle (for instance ping-of-death). Such an assault would generally have bring down volumes of information. Unless a couple misuses exist at the casualty has, which have not been settled, a DoS assault should not to represent a genuine risk to top of the line benefits on today's Internet.

DDoS (Distributed Denial of Service) assaults would, generally, be produced by countless. These hosts might be amplifiers1 or reflectors2 or something like that, or even might be "zombies" (administrator program, which interfaces back to a pre-characterized ace hosts) who were planted on remote has and have been sitting tight for the charge to "assault" a casualty. It is very essential to see assaults created by several hosts, delivering many megabits consistently

surges. The essential instrument of DDoS is mass flooding, where an assailant or aggressors surge the casualty with the best number of parcels as they can remember the ultimate objective to overwhelm the casualty. The best approach to display what a DDoS assault does to a web server is to think on what may happen if all the number of inhabitants in a city chosen at a comparable minute to go and remain in the line of the neighborhood shop. These are all genuine solicitations for benefit – each one of the all-inclusive community came to purchase something, however there is zero possibility they would have the ability to get benefit, since they have a thousand different people remaining in line before them .

CHAPTER 2
LITERATUR REVIEW

Xia Shen, et.al," Distributed Congestion Control Methods for the IEEE 802.11p Vehicular Networks", 2013

A novel dispersed multi-need congestion control technique is proposed to expand the transmission open entryways for the most elevated need traffics while keeping the crash likelihood at a low level. Open issues for the future work on the blockage control approach configuration are attracted this paper. The rest of the difficulties in the studied clog control approaches are then finished up, which basically concentrate on the activity need and blockage estimation thought. Confronting these difficulties, a novel appropriated multi-need clog control approach is proposed for the IEEE 802.11p vehicular system. The recreation comes about have demonstrated that contrasted and the IEEE 802.11p convention, the proposed approach can ensure the fruitful transmission for the most elevated need movement and make the crash likelihood stay at a low level in the congested condition. This basic proposed approach moreover gets basic pick up in the framework throughput execution and can be adequately to be actualized in a pragmatic IEEE 802.11p MAC layer.

Dong Nguyen, et.al," Wireless Broadcast Based Network Coding", 2009

Conventional ways to deal with dependably transmit data over an error-prone system use either forward mistake redress (FEC) or retransmission procedures. In this paper, some system coding plans are proposed to decrease the quantity of communicate transmissions from one sender to various beneficiaries [22]. The standard thought is to enable the sender to consolidate and retransmit the lost parcels completely so that with one transmission, different collectors can recuperate their own specific lost bundles. For correlation, several hypothetical outcomes are gathered on the data transfer capacity effectiveness of the proposed arrange coding and customary programmed rehash ask for (ARQ) plans. Our proposed plans join particular lost parcels from different collectors to such an extent that various beneficiaries can recoup their lost bundles with one transmission by the sender. Some investigation is suited commonly upgrading system coding and channel coding strategies for given channel parameters, which can

furthermore enhance organize execution. Both reproductions and hypothetical examination affirm the upsides of the proposed arrange coding plans over the ARQ ones.

Alok Nandan, et.al," Co-operative Downloading in Vehicular Ad-hoc Wireless Networks", 2005

A typical thing in the Internet today is portrayed by sudden and unpredicted augmentation in omnipresence of on-line content. In this paper, we propose SPAWN, an agreeable technique for content conveyance and partaking in future vehicular systems. We think the issues required in using such a system from the viewpoint of Vehicular Ad-Hoc arranges. In particular, it is demonstrated that substance server and also remote get to organize stack lessening is basic [23]. A "correspondence effective" swarming convention is proposed which uses a chatter instrument that use the inalienable communicate nature of the remote medium, and a piece-choice technique that considers in choices to trade pieces. Through recreation it is seen that babble fuses area mindfulness into peer choice, while realizing low informing overhead, and thus upgrading the swarming convention execution. A diagnostic model is worked to depict the execution of SPAWN. It is seen that as more associates partake in the convention, the execution makes strides. Our convention uses a bit of the Bit Torrent-like impetuses in the convention, for instance, the one good turn deserves another approach and gagging calculations for empowering co-operation; however the high beat of hubs in vehicular systems make the strategies unnecessarily strict. A credit based framework that is accumulated transversely over different document scattering not just one record can be an approach that will energize co-specialist direct in vehicular systems.

Xiang Cheng, et.al," An Improved Parameter Computation Method for a MIMO V2V Rayleigh Fading Channel Simulator Under Non-Isotropic Scattering Environments", 2013

Simulations of various information numerous output (MIMO) vehicle-to-vehicle (V2V) Rayleigh blurring channels under more reasonable non-isotropic dispersing situations, we propose another parameter calculation strategy for the outline of aggregate of-sinusoids (SoS) reproduction models [24]. A key issue on the outline of deterministic reenactment models is the methods by which to legitimately plan exact and proficient parameter calculation techniques. The examination of V2V deterministic SoS channel test systems initially focused on the outline of

parameter calculation techniques under isotropic scrambling situations. Another parameter calculation strategy, named as IMMEA, for deterministic SoS reenactment models has been proposed under the state of non-isotropic disseminating MIMO V2V Rayleigh blurring channels. The proposed IMMEA is the primary parameter calculation technique that can meet the exactness productivity plan criteria for all non-isotropic dissipating MIMO V2V situations. Numerical outcomes have demonstrated that contrasted and existing MMEAs, the IMMEA gives a comparative proficiency, while it offers better approximations to the STCF of the reference show. Contrasted and the current significant techniques, the proposed strategy has comparable recreation effectiveness yet gives a better estimation than the coveted factual properties of the hypothetical reference display.

Christina Fragouli, et.al," Efficient Broadcasting Based Network Coding", 2008

The issue of broadcasting in a specially appointed remote system is considered, where all hubs of the system are sources that need to transmit data to each and every other hub. Our figure of authenticity is vitality productivity, a basic outline parameter for remote systems since it particularly impacts battery life and thusly arrange lifetime [25]. It is shown that applying thoughts from arrange coding permits recognizing basic advantages as far as vitality effectiveness for the issue of broadcasting, and proposing outstandingly basic calculations that permit understanding these advantages by and by. In particular, our hypothetical examination demonstrates that system coding enhances execution by a steady figure settled systems. This variable is computed exactly for some sanctioned designs. Advance it is demonstrated that in systems where the topology progressively changes, for example in view of portability, and where operations are confined to basic dispersed calculations, arrange coding can offer enhancements of an element of log n, where n is the quantity of hubs in the system. The bits of knowledge picked up are used from the hypothetical examination to propose low-unpredictability conveyed calculations for reasonable remote specially appointed situations, discuss various down to earth contemplations, and assess our calculations through package level reproduction.

Tracey Ho, et.al," A Random Linear Network Coding Approach through Multicast", 2006

A distributed arbitrary linear system coding approach is displayed for transmission and pressure of data when all is said in done multisource multicast systems. System hubs autonomously and

haphazardly select direct mappings from inputs onto yield interfaces over some field. It is demonstrated this achieves limit with likelihood exponentially moving toward 1 with the code length [26]. It is likewise shown that arbitrary direct coding performs pressure when key in a system, summing up mistake sorts for straight Slepian–Wolf coding really. Advantages of this approach are decentralized operation and heartiness to organize changes or association disappointments. It is demonstrated that this approach can misuse excess system limit with respect to enhanced achievement likelihood and strength. Some potential favorable circumstances of irregular direct system coding over steering are introduced in two cases of pragmatic situations: appropriated arrange operation and systems with progressively differing associations. Our deduction of these outcomes furthermore yields another bound on required field gauge for focused system coding on general multicast systems.

Kiattikun Kawila, et.al," Cobra-Q: A Cooperative-Bloom Filter-Assisted Query Protocol for Data Access in VANET", 2013

In vehicular networks, attempting to exchange a inquiry message for an asking for information productively when the objective hub is out of transmission extend from the requestor hub. This is because of many steering calculations experiencing perpetual way breaks when the vehicles are moving. In this paper, we concentrate on correspondence between vehicles to roadside unit stations by asking for information only a solitary jump correspondence from the asking for hub and does not need to use any directing calculations to make information exchange way [27]. We present a novel question convention for information access in VANET called COBRA-Q. The COBRA-Q can deal with moving vehicles and achieves to exchange the demand information inside one-jump correspondence. The COBRA-Q uses sprout channel procedure to keep and pack auto voyaging history records. We assess the execution of our proposed convention by reenactment in ns-3 with urban and parkway circumstance. The reenactment comes about demonstrate that the COBRA-Q can successfully get to information as far as rate of achievement rate and overhead of using question message. COBRA-Q bolsters moving hub issue and discontinuous network.

Xiaoqing Li, et.al," A survey based data dissemination in VANETs", 2014

Vehicular ad hoc networks (VANETs) aims to get the clever correspondence for vehicular systems, they can particularly enhance the security and proficiency issues of street activity. Information dispersal is the base of correspondence, it goes about as a basic part in VANETs framework. In this paper, the principal aftereffects of information scattering in vehicle to vehicle (V2V) correspondences are studied, and explain this survey on three sections: steering conventions, versatility model and security, all of which significantly impact the transmission execution in VANETs [28]. The standard agent look into procedures and accomplishments are introduced in each class, lastly, also close the examination patterns and difficulties for information scattering in VANETs. In case of mobility model, the selecting of vehicle mobility model has vital effect on the accurate analysis of the communication protocol performance in VANETs, e.g. throughput, transmission delay and route validity. So it would be an issue that designing a model which is more suitable for the genuine movement of versatile vehicles, based on the results of small scale and macro analysis. Additionally, the usage of far reaching security and protection, the arrangements may require the support of the significant number of layers in the convention stack rather than from single layer bolster. This policy of security in VANETs is missing in the existing works, and could be an issue for further research. Other related topics for security additionally are the QoS problems in secure routing.

Surya Nepal, et.al," Anitya: An Ephemeral Data Management Service and Secure Data Access Protocols for Dynamic Collaborations", 2007

Dynamic coordinated efforts are simply the strategies by which a gathering of self-representing components (maybe battling) team up to finish a commonplace focus by sharing resources that may be claimed and administered both secretly and together. Our focus in this paper is on controlling together possessed shared information that is naturally transient, as it doesn't exist outside the time of the joint effort [29]. This paper researches the utilization of the Ephemerizer idea as an approach to control the entrance to shared joint effort information. Towards this, we initially characterize an administration situated design Anitya1 that engages the improvement of an outsider administration for overseeing fleeting information in component joint efforts. Advance the consolidate savvy secure correspondence convention used as a piece of the Ephemerizer is augmented and three differing multiparty secure gathering correspondence

conventions are proposed for sharing coordinated effort information under the characterized design. The paper in like manner talks about the plan, usage, and assessment of the design and conventions. As the quantity of capacity hubs and information builds, how proportional the key administration benefit in overseeing expanded workload and how to make the key administration solid in case of potential framework disappointments ought to be considered.

Hoang D. T. Nguyen, et.al," On Transmission Efficiency for Wireless Broadcast Based Network Coding and Fountain Codes", 2011

This paper investigates the benefits of applying wellspring codes (FCs) in upgrading the transmission effectiveness in communicating frameworks. Particularly, a right articulation of the transmission productivity for remote communicate using FCs is resolved. This deduction licenses us to analyze the transmission productivity of the wellspring code approach (FCA) and system coding approach (NCA) in remote communicate [30]. NC-based retransmission methodology is up 'til now in view of programmed rehash ask for (ARQ). In all actuality, clients situated at the intensely shadowed territories or cell-edge areas generally speaking don't get adequate flag essentialness, and thusly many got groups are mistaken. This outcomes in an expansion in the overhead, and thusly diminishing the framework throughput, especially with a creating number of clients. The numerical outcomes exhibit that FCA achieves preferred execution over NCA when the quantity of clients is tremendous and the other way around when the quantity of clients is pretty much nothing. This paper plans the transmission productivity of FCA for remote communicate and contrasts and that of NCA. All in all, FCA achieves higher transmission productivity than NCA for countless and the other way around for couple of clients.

Xia Shen, et.sl," Data Dissemination in VANETs: A Scheduling Approach", 2014

Information dispersal is a promising application for the vehicular system. Existing information dispersal plans are overall in view of some arbitrary get to convention, which brings about the unavoidable impact issue. To address this issue, in this paper we plan a novel information spread technique from the booking perspective. An information scattering planning system is then proposed. In the proposed system, the essential test is the way by which best to allot the transmission chance to hubs with greatest scattering utility and to dodge the impact issue [31]. A novel is proposed and realistic transfer decision system and receive the space–time organize

coding (STNC) with low recognition many-sided quality and space–time differing qualities pick up to enhance the dispersal productivity. Contrasted and the arbitrary get to spread, for instance, Code On-Basic and the non-supportive transmission, our proposed information scattering procedure performs better the extent that the dispersal delay. Also, the proposed system works by a wide margin unrivaled in the thick system than the inadequate circumstance, profiting from the space–time differences pick up of STNC and no-impact transmissions. This is in sharp in opposition to the Code On-Basic strategy.

Subir Biswas, et.al," DDoS Attack on WAVE-enabled VANET Using Synchronization", 2012

A VANET that usages IEEE 802.11p EDCA system is powerless to a synchronization-based DDoS assault in view of periodicity of transmissions and little conflict window sizes. To aggravate the circumstance, neither the sender nor recipients of intermittent communicates will think about the assault since communicate correspondences in VANET don't have confirmations. In this paper, we break down the possibility of a synchronization construct DDoS assaults with respect to vehicular interchanges and propose alleviation strategies to avoid such an assault [32]. This paper tended to a security shortcoming of VANETs where a gathering of noxious elements can dispatch a DDoS assault misusing the IEEE 802.11p's EDCA vulnerabilities in view of little conflict window, nonappearance of attestations in communicate correspondences, and periodicity of administration reference points. An astute aggressor can without a lot of an extend synchronize to any intermittent transmission in the system. It is broke down that the possibility of propelling such an assault, and besides proposed unmistakable mitigating procedures including bigger EDCA parameters for VANET elements. Our assault show and the arrangements have been all around upheld by numerical examination, and also multiplication comes about.

Li He et.al," Mitigating DoS Attacks over Signature-Based Authentication in VANETs", 2012

In VANET, a vehicle communicates secure messages to its neighbors. Since hones in light of secure messages could be life-basic, confirmation of these messages must be guaranteed. Various mark based plans have been proposed for verification in VANETs, however few of them have

tended to the issue of refusal of administration (DoS) assaults against signature-based validation [33]. In such a DoS assault, aggressors can communicate manufactured messages with invalid marks to constrain the getting vehicles to perform clusters of pointless mark checks, and in like manner the kind vehicles can't confirm the messages from other honest to goodness vehicles. Our plan includes a pre-validation prepare before signature checking procedure to manage this kind of DoS assault. The pre-verification prepare abuses the confined hash chain and a gathering rekeying plan. Assessments demonstrate that the proposed conspire mitigates such DoS assaults effectively.

Mohamed Nidhal Mejrit, et.al," A New Security Games depended Reaction Algorithm Over DOS Attacks in VANETs", 2016

To adjust to, response techniques against these attacks exist. Toward this way, diversion hypothesis associated with the security of remote systems (generally called security amusements) can be a better than average technique for demonstrating. In this paper we propose a response strategy against DOS assaults in VANET. In this technique we have the decision between two proposed response recreations [34]. Diagram system and characterized measurements are motivated from diversion hypothesis models. To the best of our understanding, no equivalent recreations have been proposed some time as of late. Our commitments are: First, the paper has given another security diversions formalism for Denial of administration assaults in VANETs. Second, the paper has composed two possible recreations circumstance: (i) vital frame diversion and (ii) broad shape amusement. Third, it is concentrated the DOS assault under sensible suppositions, for instance, the use of genuine portability models in light of practical guide. Finally, the proposed recreations are assessed by propagations. It is believed these commitments to be to a great degree supportive for taking care of the DOS assault response issue in VANETs. The entertainments demonstrated the adequacy of our recommendation measured by the execution of the obtained comes about.

Ayonija Pathre, et.al," A Novel Defense Method against DDOS Attack in VANET", 2013

In this paper the novel movement detection of congestion and expulsion plot is proposed against DDOS assault. Here the aggressor direct is communicate the immense quantities of false data parcels in organize i.e. the false data about the activity. The quantity of hubs or vehicles that gets

the false parcel data is influenced from assault are called Abstract Node [35]. By and by if the movement is stuck or clog happening and their data goes to Roadside Unit (RSU) at that point RSU must be distinguished and prohibited for all time from the system in the wake of applying proposed effective approach. Proposed plot against DDOS assault intends to recognize and bar assailants from the system. Within the sight of escaping hand in organize the false data is moved in the system by that the vehicles are doing the steering as shown by false data. Proposed security conspire recuperates control data and enhances the execution of VANET within the sight of an aggressor.

Pooja. B, et.al," Mitigation of the Insider and Outsider DoS attack against the Signature Based Authentication in VANETs", 2014

Validation is an essential structure for ensured and secure correspondence of messages in VANETs. For validating messages the IEEE 1609.2 standard uses ECDSA as the standard computerized signature estimation. Regardless, the check time for an ECDSA mark is high. In like manner an inside or an outside aggressor could use a small amount of data transfer capacity and surge the system with invalid marks achieving Denial of Service (DoS) assault. Thusly in this work a two stage conspire is proposed to moderate inside and outside DoS assailants in VANETs [36]. In the vital stage HMAC marks figured from private and open key match are used for validating the conveying element. As simply legitimate clients can figure the HMAC signature, DoS assault due to outside assailants is moderated. If the substance is bona fide and subjects other vehicle to DoS assault, the second stage is intended to identify the insider aggressors. In this stage in light of the quantity of invalid marks overflowed by the assailant, it is contrasted against a limit an incentive with recognize within aggressor. In this manner DoS assault is relieved due to inside and furthermore outside aggressors. Test outcomes demonstrate that the proposed conspire mitigates DoS assault and also performs better with insignificant computational overhead.

Munazza Shabbir, et.al," Detection, Prevention of Distributed Denial of Service Attacks in VANETs", 2016

Vehicular ad-hoc systems are transforming into a standard and promising innovation in the current smart transportation world. As indicated by the security uses of VANETs any data

flowing through the system can be life critical. So the genuineness of the data is a basic need. The portability of the hubs and the erratic method for the relationship in the system has made VANET powerless against various security dangers [37]. One of the huge assault that debilitates the system by misguidedly using most of its benefits is DDOS assault. In this kind of assault an aggressor fakes distinctive personalities of hubs i-e uses mock IP locations to deplete the system by circling counterfeit messages and making it deny to oblige honest to goodness sales for administrations. So before the correct sending of this system for all intents and purposes its security needs ought to be met. In this paper a DDOS assault discovery and after that aversion conspire is proposed. The fundamental standard is keeping a mind the quantity of bundles being infused into the system. The proposed structure of this plan causes no Burdon on the system assets.

CHAPTER 3

PRESENT WORK

3.1 Problem Formulation

Vehicular ad-hoc network has the property of self configuring and a decentralized architecture. Vehicle to vehicle, vehicle to infrastructure are two basic mode of communication in vehicular ad-hoc network. Because of decentralized nature of ad-hoc network many nodes like malicious becomes the part of communicating network and causes the attacks like active and passive in network. And those malicious nodes which becomes the part of network causes DDOS attack which in turn reduces the performance of communicating channel or network. The malicious nodes triggers the DDOS attack by choosing some of victim nodes from the network and those victim node attack on other single node. The signature verification technique which is being described in base paper can be used for the detection of malicious nodes in network. This used technique is comparatively complex and also reduces the performance of network. In our present work some novel techniques are used which can detect malicious nodes easily and are light weight in nature that is doesn't reduce the efficiency of the network.

3.2 Objectives of Research

Following are various objectives for research:

a. Studying and analyzing different security vulnerabilities for vehicular ad-hoc networks

b. To propose technique for detection of malicious node in the network that is main cause for occurrence of various attacks in network like DDOS.

c. Currently used techniques uses the concept of mutual authentication and some other techniques for traffic monitoring algorithm in networks

d. The currently used schemes are compared on the basis of many commonly used terms like delay, throughput, packet loss etc.

3.3 Research Methodology

The current work is mainly based on to detect the malicious node present in the network which causes DDOS attack in network. DDOS is the distributed denial of service attack in which malicious node choose the legitimate node which will trigger some direct attack on chosen victim node in the network. In the DDOS attacks some of the malicious node will send the control packets to the legitimate nodes and legitimate nodes can easily transmit rouge packets directly to victim and trigger attack. In the current work the used techniques can easily detect if any malicious node present in the network thereafter to detect malicious nodes following are the steps which are followed:-

1. In the first step, the network is taken with the limited number of vehicle node. And fixed bandwidth is allocated to each vehicle node in the network

2. The road side units start analyzing the bandwidth consumption of each vehicle node and node which is using the bandwidth above allocated value will be the malicious nodes

3. In the third step, the road side units check the type of packets which node is sending which is using the bandwidth above the allocated value. When the node is sending the information to some of the victim node in form of data packets, it may be malicious node.

4 In the last step the node which is sending the rouge data packets , if that node will receive control packets from any node then that node will be detected as the malicious node that is main cause for the occurring of DDOS attack in the network.

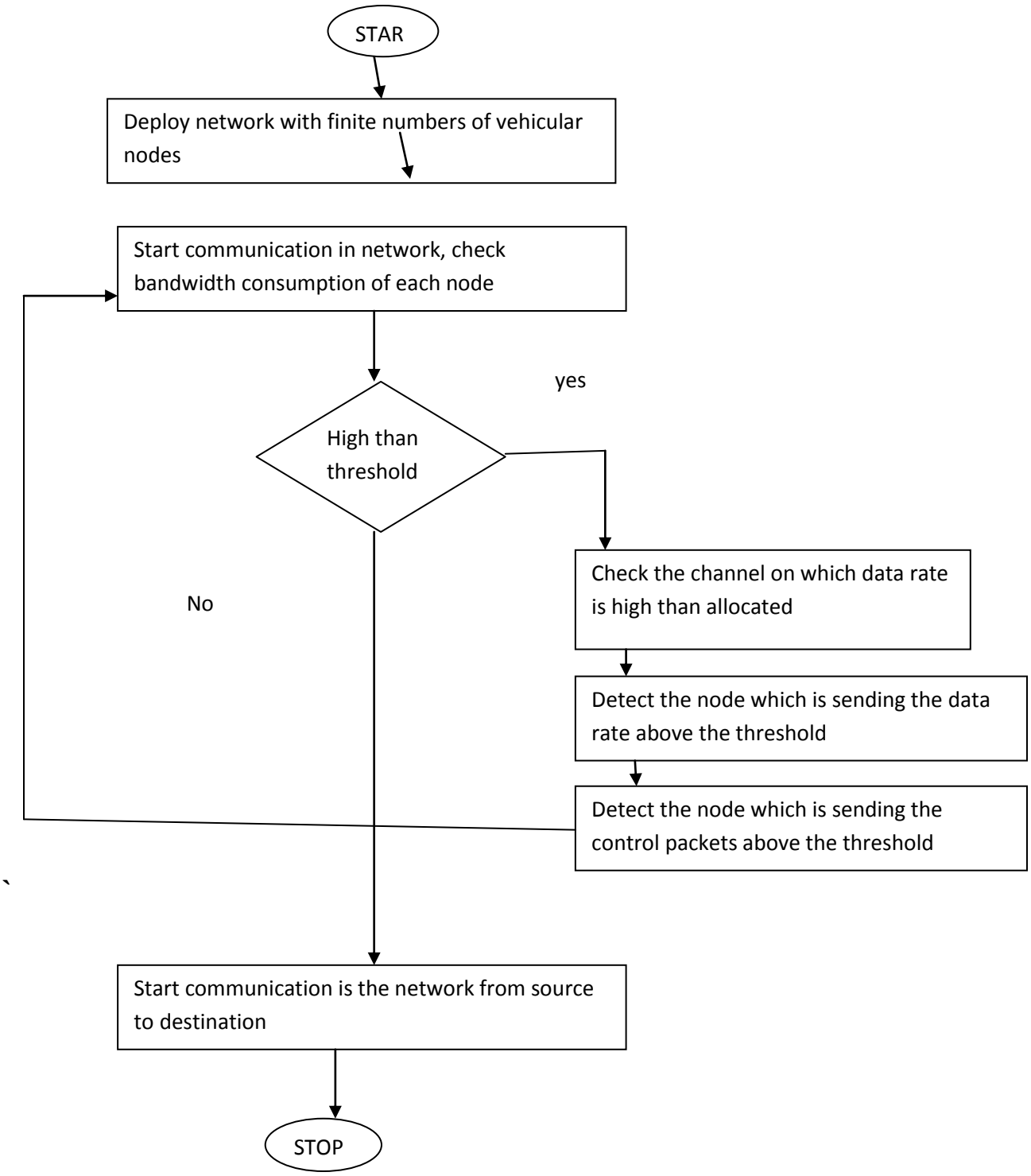

Figure 5: Threshold flowchart

Threshold based Algorithm

Input: Number of vehicle nodes

Output: Detection of malicious

1. Assign bandwidth the data rate to each node in the network

2. The source node start sending data to destination node

3. if (bandwidth consumption >threshold)

4. check channel on which data rate is high than threshold

5. check the node which is sending data packets on the node

6. If (node ==detected)

7. check the node which is sending control packets

8. isolate detected node

9. else

10. no malicious node

11. end

12. end

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Experimental Results

Tool: **NS2** works basically on operating system like UNIX and a simulation tool which is open source in nature. NS2 is an event simulator used in various research areas of networking. It also provides support in process of simulation of various protocols such as IP and routing multicast like TCP,UDP as compared with wireless and wired network . This tool has various advantages like it can easily detect network traffic graphically and also multiple protocols. It also provides facilities for various algorithms like queuing, routing. Various routing algorithms includes broadcast as well as local area network routing. Whereas queuing algorithm has less support for round robin and it comprises of fair queuing as well as FIFO. It is a real time network simulator which is being used and was initiated in 1989. In various packet switched networks this simulator is used for the study of congestion control.

Network simulator is mainly a separate tool for network; Virtual Internetwork Test-bed (VINT) started this programming simulator tool. NS is separate simulator for events in network. NS2 provides simulation facilities to various transport level protocols such as TCP, UDP. And also for many protocols of MAC layer it provides multicast as well as routing protocols over networks such as wireless or wired. Based on what user is demanding simulations are firstly stored in trace files that can be further provided as the input for various analysis purposes on varying components.

Network animator creates the required simulated environment and for this NAM (.nam) trace file is used.

X graph is used to give various graphical results and are stored with the file name trace file (.tr).

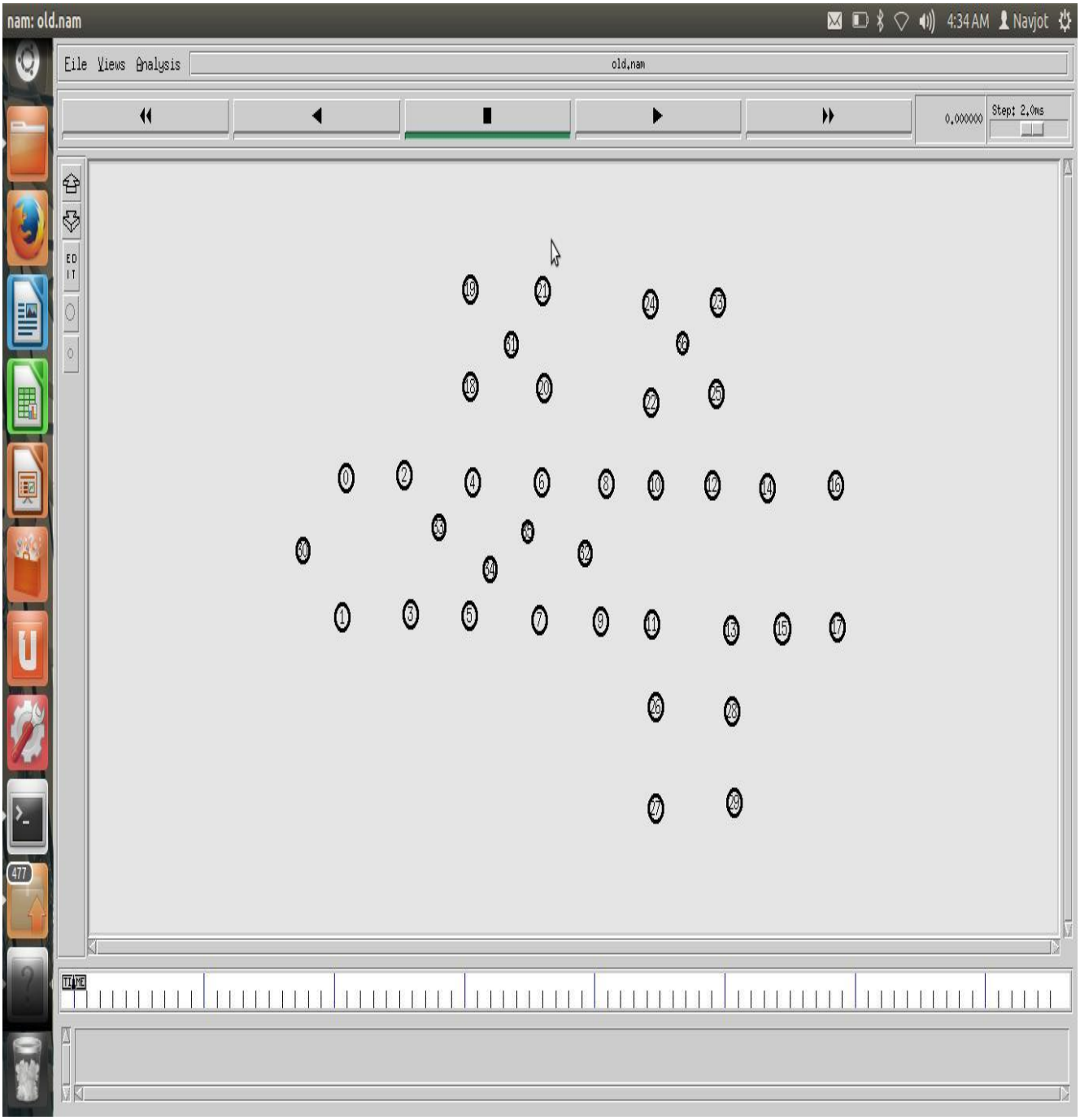

Figure 6: Deploy of network

As given in figure, vehicular ad-hoc network has the fixed number of communicating nodes or vehicle nodes. Network comprises of road side units are deployed which will pass the sensed information to the vehicle nodes

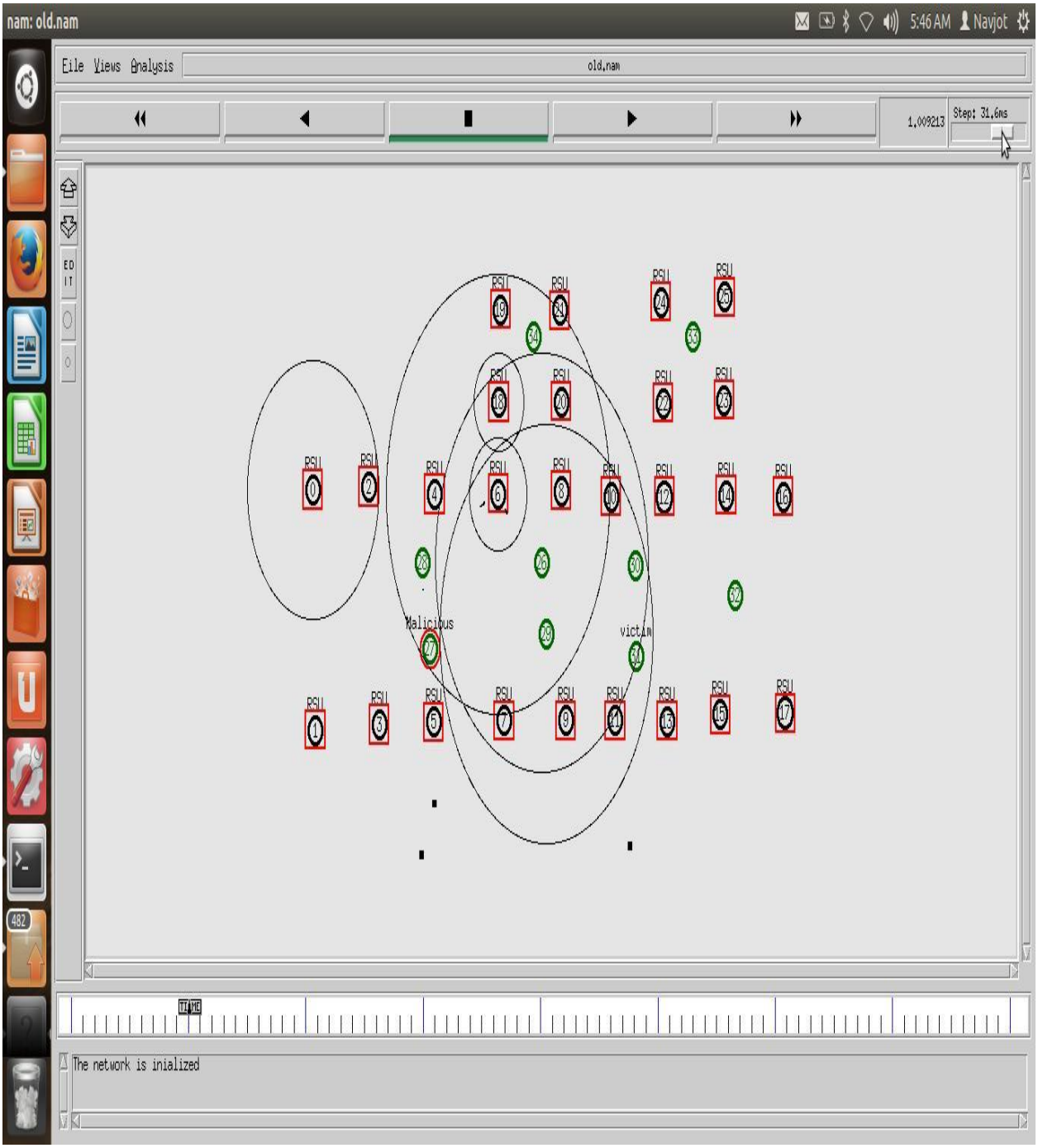

Figure 7: Communication in the network

As given in the figure, network is deployed and the nodes present in network can transfer packet to one another. Malicious node selects its victim nodes which trigger attack on the legitimate node

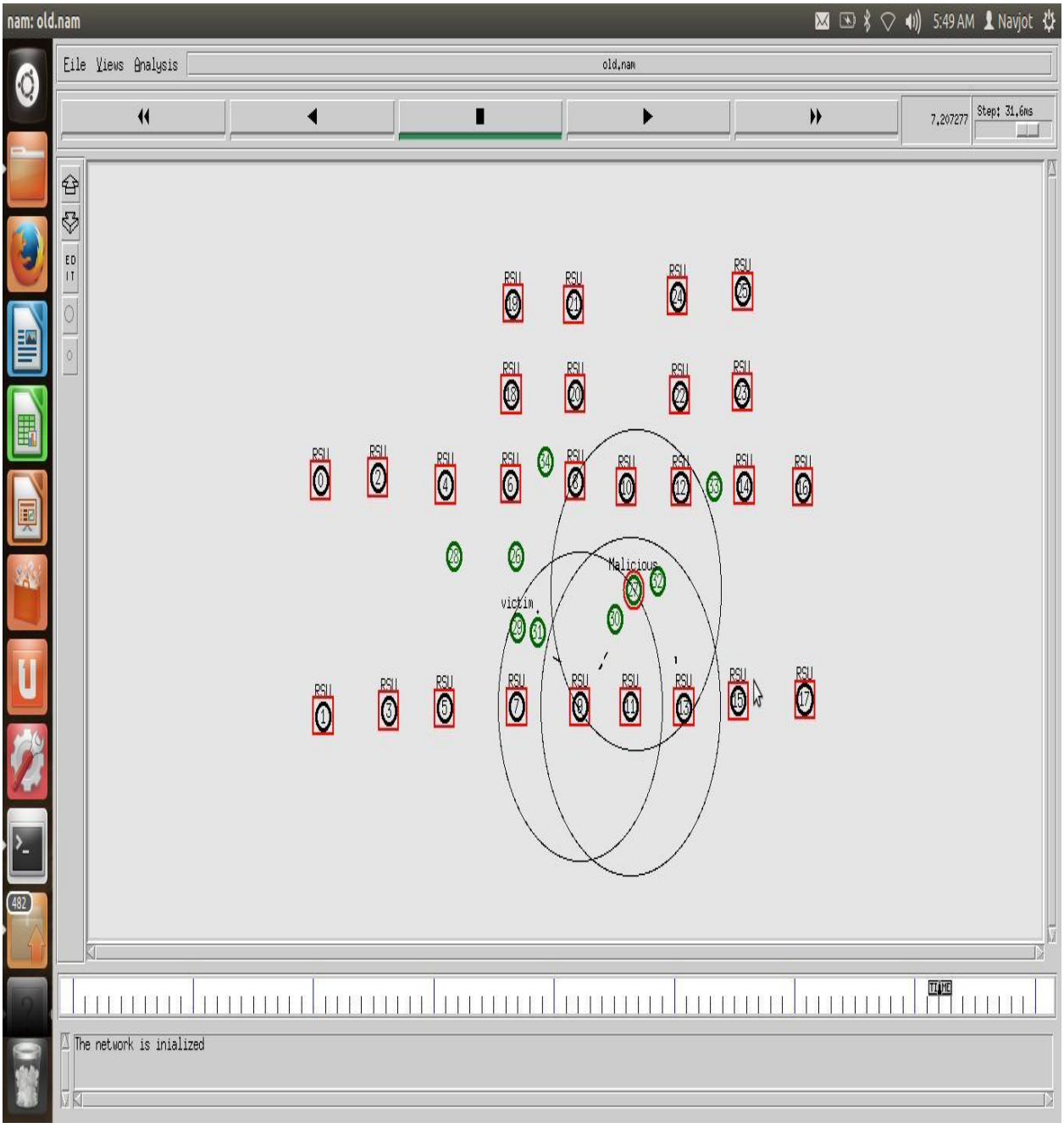

Figure 8: Trigger of attack

As shown in figure, the malicious node selects its victim node which trigger attack on the victim node. This leads to reduction in network throughput, increase delay and packet loss.

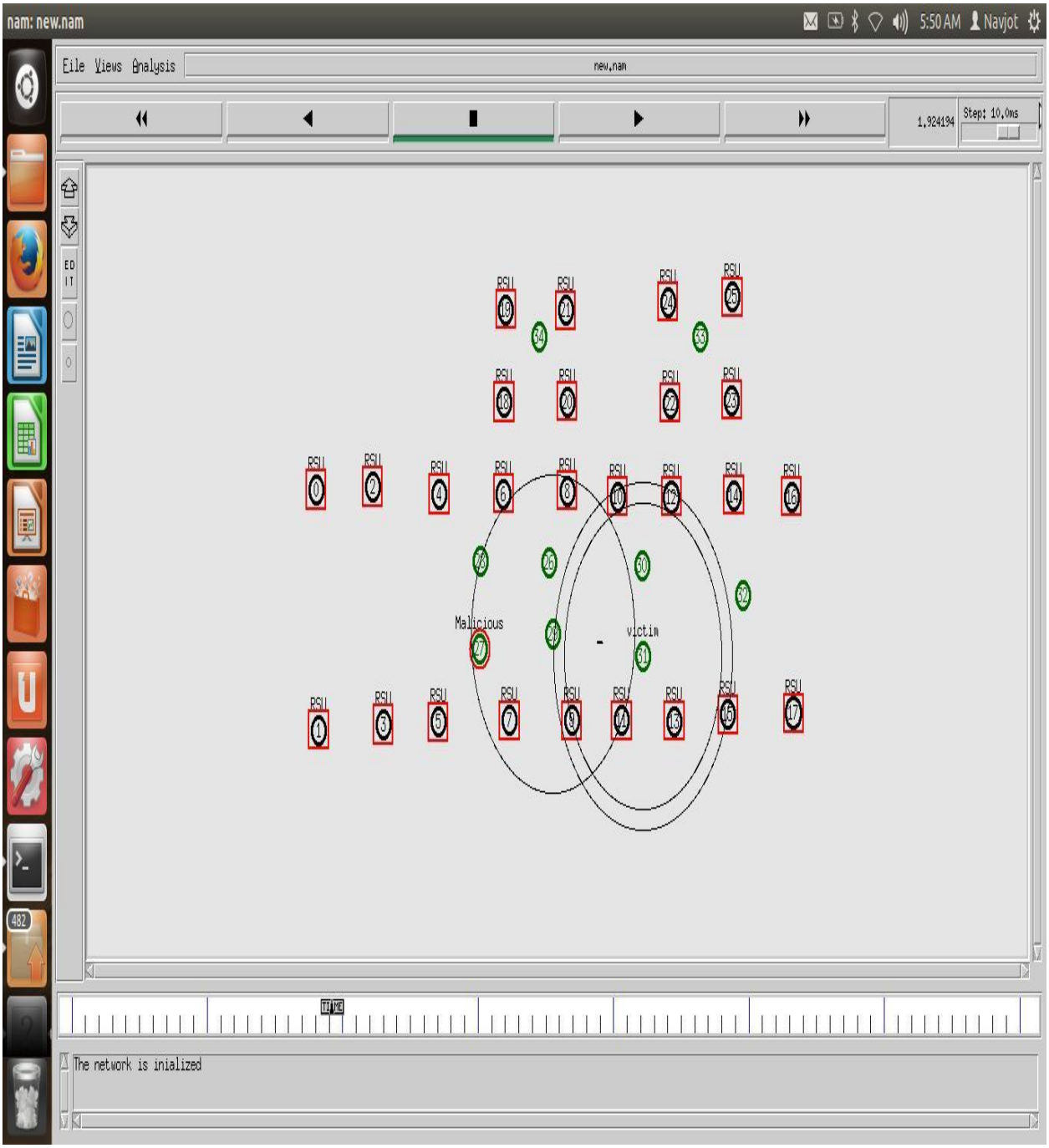

Figure 9: Detection of malicious node

As given in figure 5, malicious node chooses some of the victim node which will flood the network with the rouge data packets. The bandwidth is allocated to each node and node which is using above allocated bandwidth will may be the malicious node

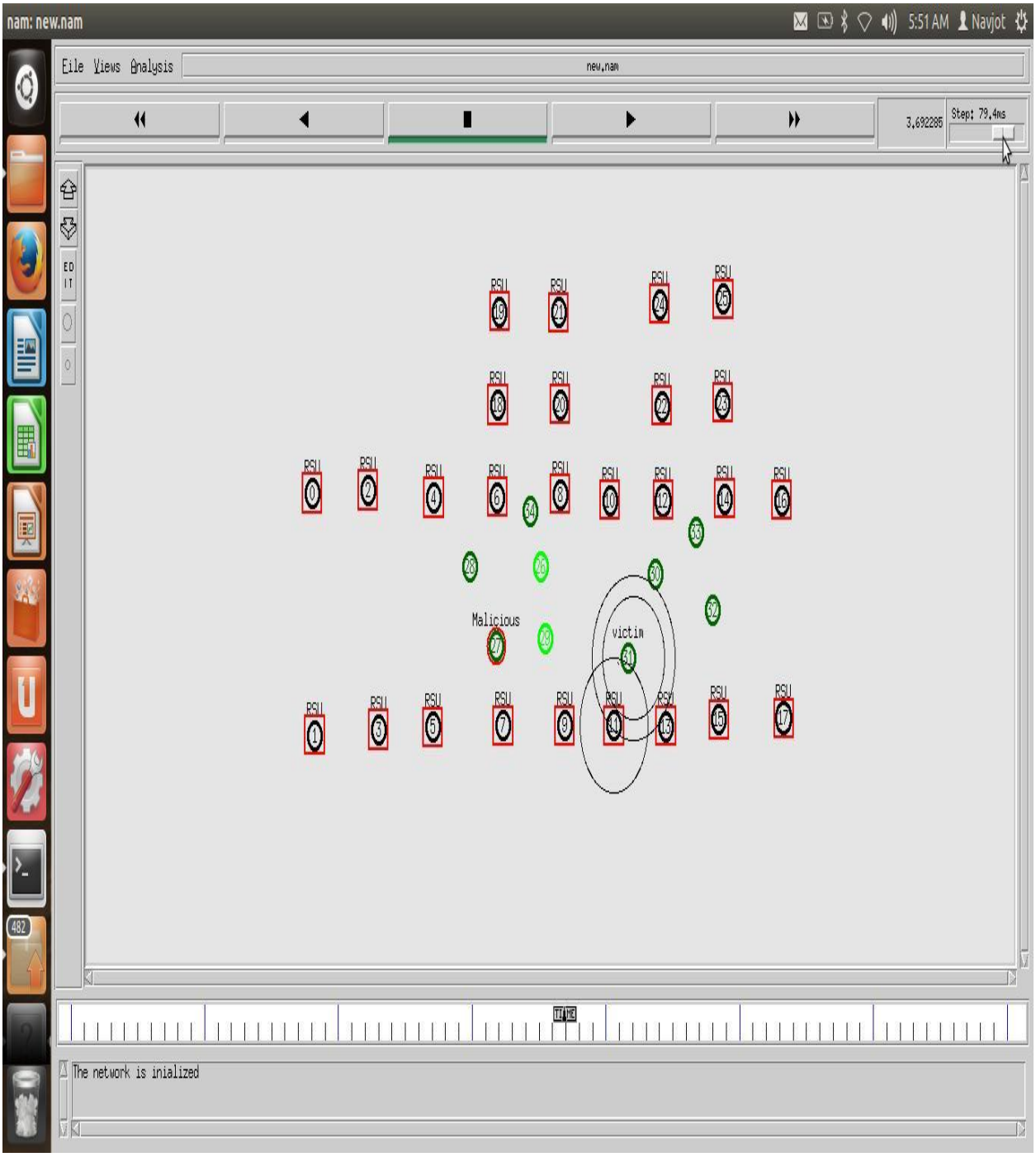

Figure 9.1: Detection of malicious node

As given in figure, node which is sending some of data packets above the threshold values will be the malicious node. In this figure the node is detected which send data packets.

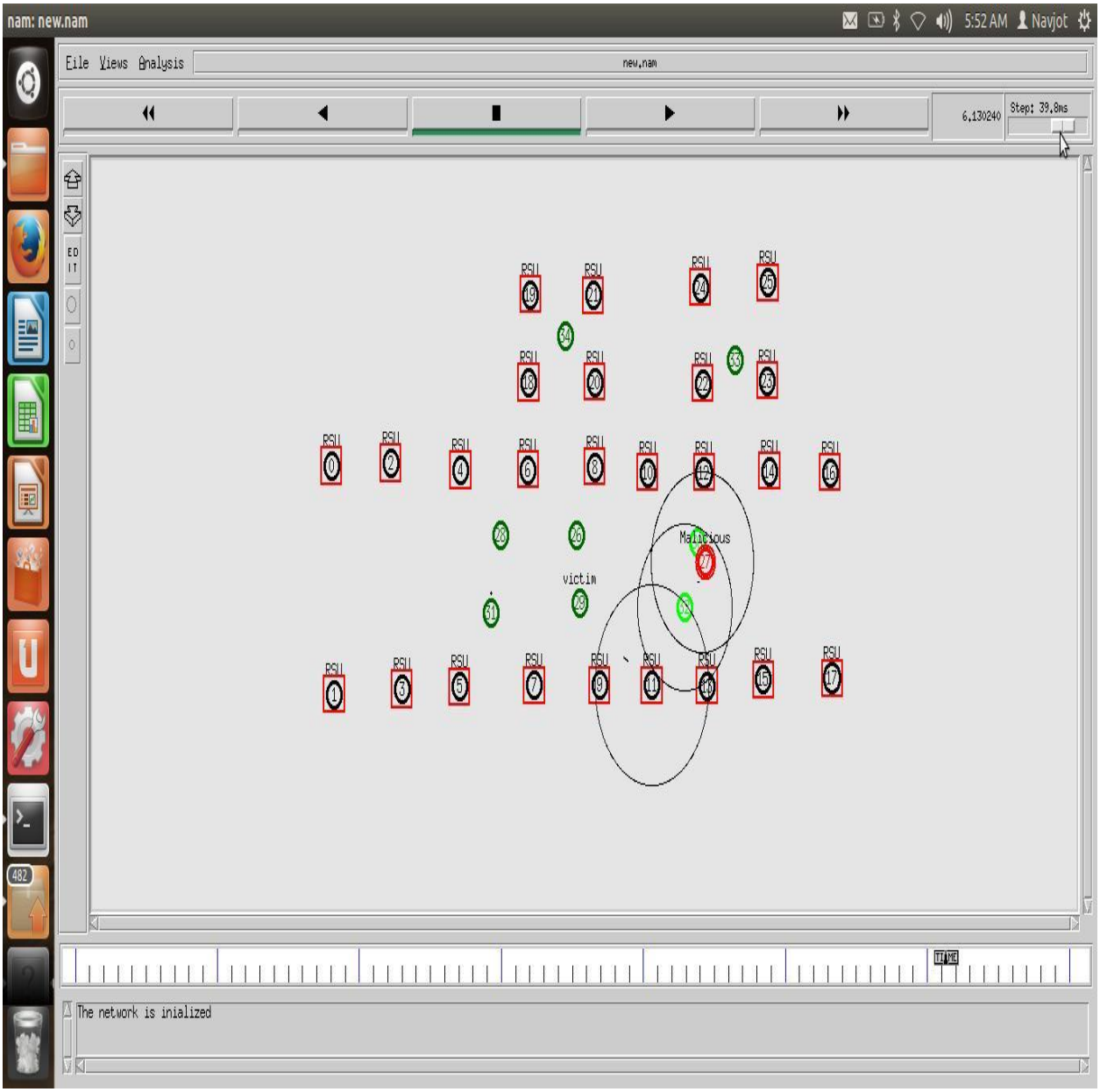

Figure 9.2: Detection of malicious node

As shown in figure, the node which is sending the data above the threshold value will be detected as the malicious node.

4.2 Comparison with existing technique

Figure 10: Delay Comparison

As shown in figure, the delay of the proposed and existing technique is compared, it is been analyzed that delay of proposed technique is less as compared as existing technique

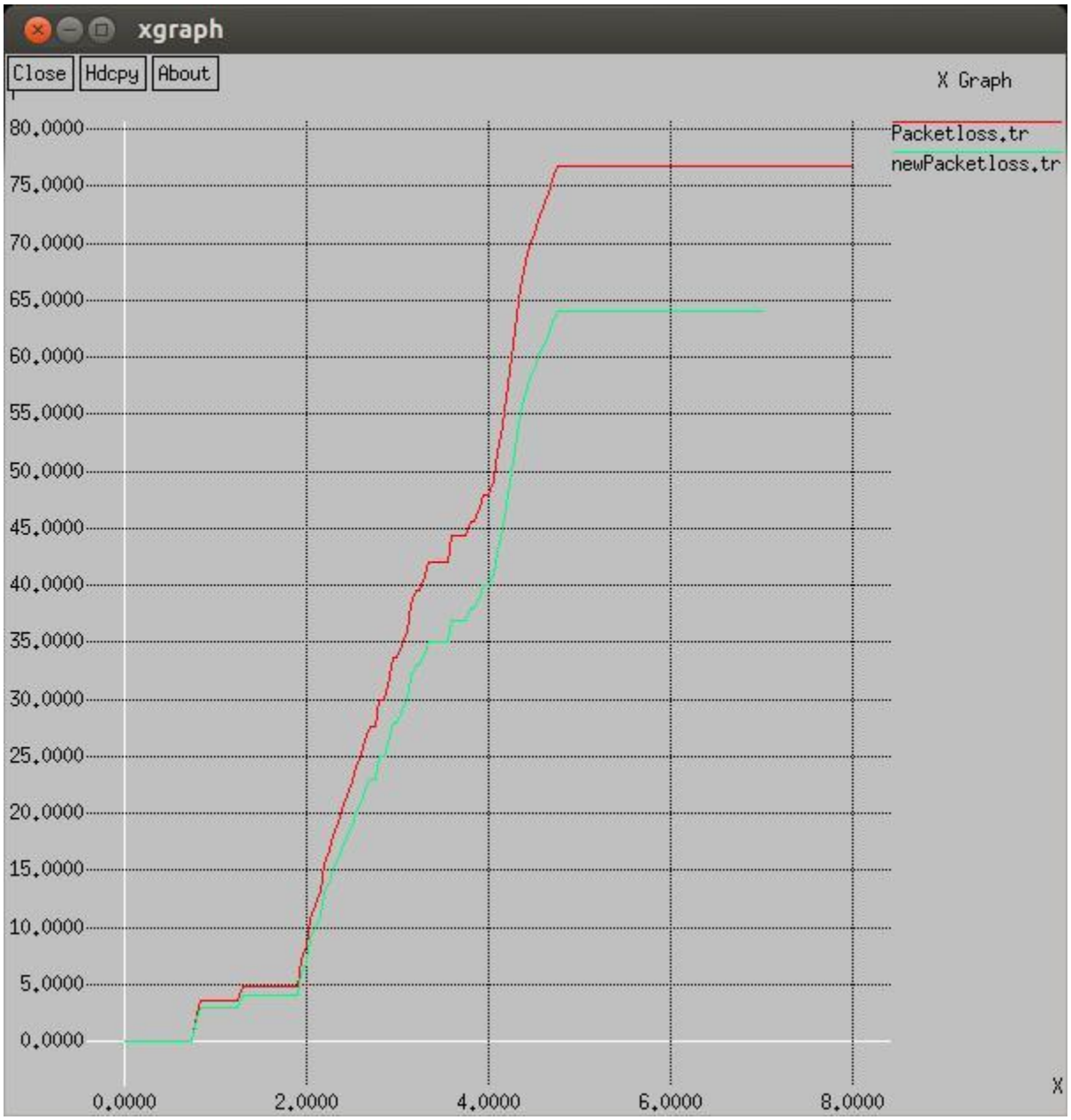

Figure 11: Packet loss comparison

As shown in figure, the packet loss of the proposed, existing and attack scenario is compared and it is been analyzed that packet loss of the proposed technique is minimum as compared to other scenarios

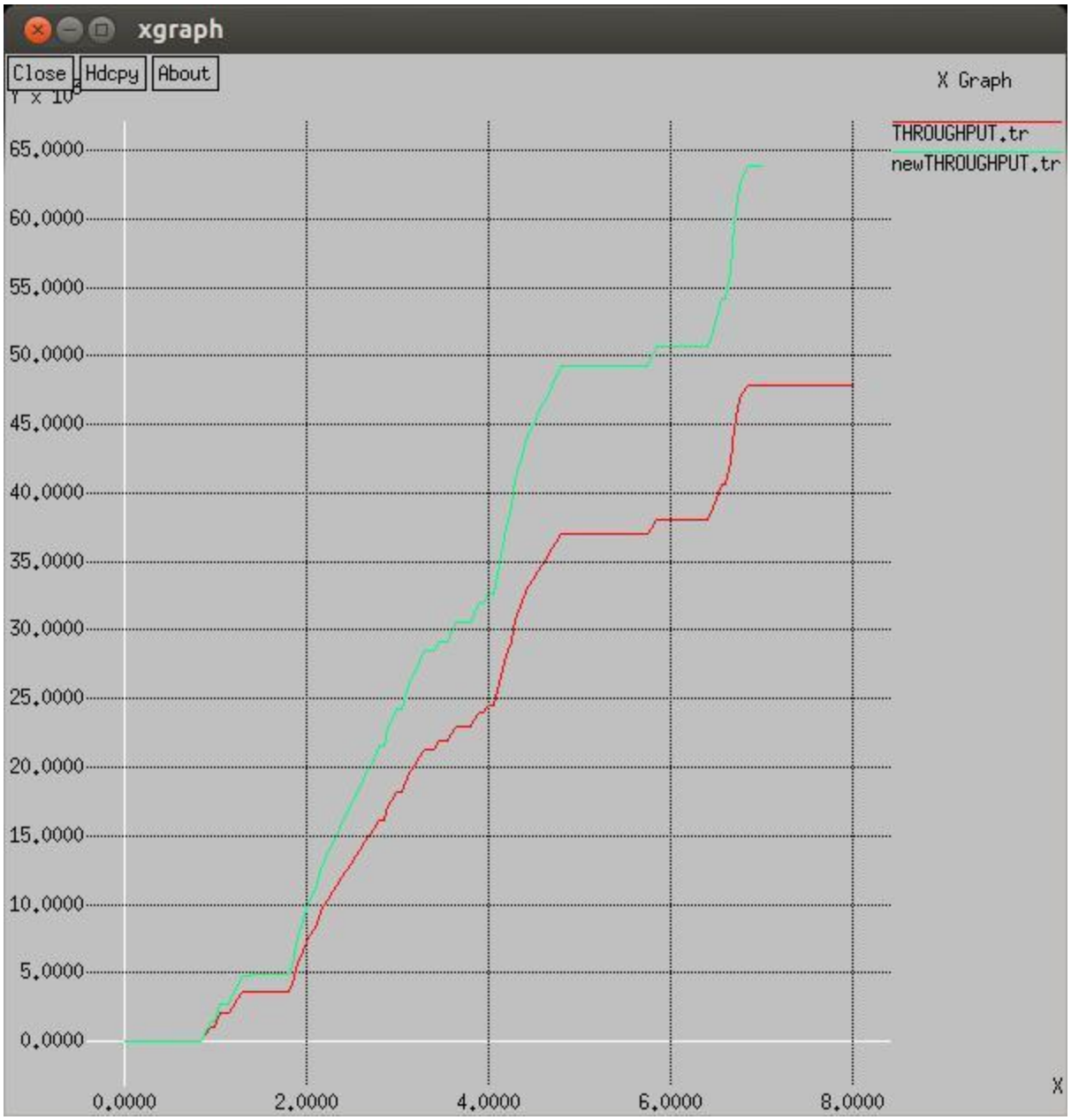

Figure 12: Throughput comparison

As shown in figure 10, The throughput of the proposed, existing and base paper technique and it is been analyzed that network throughput of proposed technique is maximum due to isolation of DDOS attack

CHAPTER 5
CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

In this work, it is been concluded that DDOS attack is the kind of active attack comprises of various malicious nodes flood the victim node with the rough data packets. The malicious node join the network because the ad-hoc network is the type of decentralized network.. In this work, threshold based technique is proposed in which node which is sending data above the assigned value will be marked as malicious which is sending rough data packets. The node which is sending the control packets above the assigned value will be detected as malicious nodes. The proposed technique performs well in terms of various parameters

5.2 Future Scope

Following are the future prospective of the research work

1. The proposed technique can be compared with other DDOS detection technique to check the reliability of the algorithm

2. In future the technique authentication will be proposed which leads to increase network security

REFERENCES

[1] A. Nandan, S. Das, G. Pau, M. Gerla, and M. Y. Sanadidi, "Co-operative downloading in vehicular ad-hoc wireless networks," 2005, IEEE WONS 2005, pp. 32–41, St. Moritz, Switzerland

[2] M. Li, Z. Yang and W. Lou, "CodeOn: Cooperative Popular Content Distribution for Vehicular Networks using Symbol Level Network Coding," 2011, IEEE J. Sel. Areas Commun., vol. 29, no. 1, pp. 223-235

[3] A. Duel-Hallen, "Fading Channel Prediction for Mobile Radio Adaptive Transmission Systems," 2007, IEEE, vol. 95, no. 12, pp. 2299-2313

[4] S. Haykin and B. Widrow, "Parameter estimation methods," 2003, Adaptive and Learning Systems for Signal Processing Communications and Control, Hoboken, NJ: Wiley

[5] Hayes, Monson H," Statistical Digital Signal Processing and Modeling", 1996, Hoboken, NJ: Wiley, pp. 541-550

[6] W. P. Siriwongpairat, T. Himsoon, W. Su, and J. R. K. Liu, "Optimum threshold-selection relaying for decode-and-forward cooperation protocol," 2006, Proc. IEEE WCNC pp. 1015–1020

[7] W Shangguang, F Cunqun, H Ching-Hsien, S Qibo, Y Fangchun," A Vertical Handoff Method via Self-selection Decision Tree for Internet of Vehicles," 2014, IEEE System Journal, doi: 10.1109/JSYST.2014.2306210

[8] S Michael, M Imad," Spatial distribution and channel quality adaptive protocol for multihop wireless broadcast routing in VANET", 2013, IEEE Trans Mobile Comput 12(4), 722–734

[9] SY Ni, YC Tseng, YS Chen, JP Sheu," The Broadcast Storm Problem in a Mobile Ad Hoc Network. Wireless Networks", 2002, 8, 153–167

[10] S Pani\chpapiboon, W Pattara-atikom," A Review of Information Dissemination Protocols for Vehicular Ad Hoc Networks", 2011, Communications Surveys & Tutorials IEEE 99, 1–15

[11] Korkmaz, G., Ekici, E., Ozguner, F., and Ozguner, U.," Urban Multi-hop Broadcast Protocol for Inter-vehicle Communication Systems", 2004, ACM International Workshop on Vehicular Ad Hoc Networks, (VANET'04), Philadelphia, USA, pp. 76–85

[12] Korkmaz, G., Ekici, E., and Ozguner, F.," An Efficient Fully Ad-hoc Multi-hop Broadcast Protocol for Inter-vehicular Communication Systems", 2006, IEEE International Conference on Communications, (ICC'06), Istanbul, Turkey, pp. 423-428

[13] L Wischof, A Ebner, H Rohling," Information Dissemination in Self Organizing Inter vehicle Networks", Intelligent Transportation Systems, 2005, IEEE Transactions on 6, 90–101

[14] L Uichin, M Eugenio, G Mario, B Paolo, L Pietro, L Kang-Won," Bio-inspired multi-agent data harvesting in a proactive urban monitoring environment", 2009, Ad Hoc Networks 7(4), 725–741

[15] Karp, B., and Kung, H.T.," GPSR: Greedy Perimeter Stateless Routing for Wireless Networks", 2000, Proceedings of the Annual International Conference on Mobile Computing and Networking (MobiCom'00), Boston, USA, pp. 243–254

[16] Hill, J., Szewczyk, R., Woo, A., Hollar, S., Culler, D., and Pister, K.," System Architecture Directions for Networked Sensors", 2000, International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), New York, NY, USA, pp. 93–104

[17] L Daoquan, L Haiyan, C Qiguang, W Huaicai," New routing algorithm based on geographical location", 2009, GPSR-AD. J Comput Appl 29(12), 3215–3217

[18] Candido Caballero-Gi," Light Weight Authentication for RFID used in VANETs," 2011, Conference, SPAIN

[19] Andres Ortiz," A Scaled Test Bench for Vanets with RFID Signalling", 2009, Springer

[20] Shivani," Route Planning in VANET by Comparitive study of Algorithms", 2013, Amritsar, Vol 3, Issue 7

[21] Xia Shen, Xiang Cheng, Rongqing Zhang, and Bingli Jiao," Distributed Congestion Control Approaches for the IEEE 802.11p Vehicular Networks", 2013, IEEE Intelligent transportation systems magazine

[22] Dong Nguyen, Tuan Tran, Thinh Nguyen, and Bella Bose," Wireless Broadcast Using Network Coding", 2009, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, Vol. 58, No. 2

[23] Alok Nandan, Shirshanka Das, Giovanni Pau, Mario Gerla and M.Y. Sanadidi," Co-operative Downloading in Vehicular Ad-hocWireless Networks", 2005, IEEE

[24] Xiang Cheng, Qi Yao, Cheng-Xiang Wang, Bo Ai, Gordon L. St¨uber, Dongfeng Yuan, and Bing-Li Jiao," An Improved Parameter Computation Method for a MIMO V2V Rayleigh Fading Channel Simulator Under Non-Isotropic Scattering Environments", 2013, IEEE COMMUNICATIONS LETTERS, Vol. 17, No. 2

[25] Christina Fragouli, Jörg Widmer, and Jean-Yves Le Boudec," Efficient Broadcasting Using Network Coding", 2008, IEEE/ACM TRANSACTIONS ON NETWORKING, Vol. 16, No. 2

[26] Tracey Ho, Muriel Médard, Ralf Koetter, David R. Karger, Michelle Effros, Jun Shi, and Ben Leong," A Random Linear Network Coding Approach to Multicast", 2006, IEEE TRANSACTIONS ON INFORMATION THEORY, Vol. 52, No. 10

[27] Kiattikun Kawila, Tanapoom Danmanee, Kultida Rojviboonchai," Cobra-Q: A Cooperative-Bloom Filter-Assisted Query Protocol for Data Access in VANET", 2013, Proceedings of ICCT

[28] Xiaoqing Li, Hui Li," A survey on data dissemination in VANETs", 2014, Chin. Sci. Bull., 59(32):4190–4200

[29] Surya Nepal, Julian Jang, John Zic," Anitya: An Ephemeral Data Management Service and Secure Data Access Protocols for Dynamic Collaborations", 2007, IEEE

[30] Hoang D. T. Nguyen, Le-Nam Tran, and Een-Kee Hong," On Transmission Efficiency for Wireless Broadcast Using Network Coding and Fountain Codes", 2011, IEEE COMMUNICATIONS LETTERS, Vol. 15, No. 5

[31] Xia Shen, Xiang Cheng, Liuqing Yang, Rongqing Zhang, and Bingli Jiao," Data Dissemination in VANETs: A Scheduling Approach", 2014, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, Vol. 15, No. 5

[32] Subir Biswas, Jelena Misic, Vojislav Misic," DDoS Attack on WAVE-enabled VANET Through Synchronization", 2012, IEEE

[33] Li He and Wen Tao Zhu," Mitigating DoS Attacks against Signature-Based Authentication in VANETs", 2012, IEEE

[34] Mohamed Nidhal Mejrit, Nadjib Achir and Mohamed Hamdi," A New Security Games Based Reaction Algorithm Against DOS Attacks in VANETs", 2016, IEEE

[35] Ayonija Pathre, Chetan Agrawal, Anurag Jain," A Novel Defense Scheme against DDOS Attack in VANET", 2013, IEEE

[36] Pooja. B, Manohara Pai M.M, Radhika M Pai, Nabil Ajam, Joseph Mouzna," Mitigation of the Insider and Outsider DoS attack against the Signature Based Authentication in VANETs", 2014, IEEE

[37] Munazza Shabbir, Muazzam A. Khan, Umair Shafiq Khan, Nazar A. Saqib," Detection and Prevention of Distributed Denial of Service Attacks in VANETs", 2016, IEEE