LOVELY PROFESSIONAL UNIVERSITY

Analysis of enhanced Request Response Detection Algorithm for Denial of Service Attack in VANET

A Dissertation submitted

By

Deepali

(11310836)

To

Department of Computer & Science Engineering

In partial fulfillment of the Requirement for the

Award of the Degree of

Master of Technology in Computer Science

Under the guidance of

Mrs. Isha

(May 2015)

INDIA'S LARGEST UNIVERSITY
LOVELY PROFESSIONAL UNIVERSITY
Transforming Education, Transforming India

School of:Computer Science and Engineering

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the student	:Deepali	Registration No	:11310836
Batch	:2013-2015	Roll No	:RK2307B62
Session	:2014-2015	Parent Section	:K2307

Details of Supervisor:

Name	:Isha	Designation	: Assistant Professor
UID	:17451	Qualification	: M.E
		Research Exp.	:4 years

Specialization Area: Networking

Proposed Topics:-

1. Analysis of enhanced protocol for detection of denial of service attack in VANET.
2. Analysis of prevention of denial of service attack in VANET.
3. Security issues in wireless sensor networks.

17451
Signature of supervisor

PAC Remarks:

Topic '1' is approved

'Publicatn is expected'

28/9

16/10/14

APPROVAL OF PAC CHAIRMAN   Signature: Date:

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

ABSTRACT

Vehicular ad hoc networks are likely to be deployed in coming years and become the most relevant form of MANET. It is the special class of MANET i.e mobile ad hoc networks .In recent years not much work has to be done on security. So VANET is used for life saving of passengers .An attacker can change the behavior of other vehicle or infrastructure in the network and also try to challenge the network with their malicious attacks. The main purpose of the VANET is to provide road safety and comfort to the passengers. VANET itself make and break the connection in a network. At the starting of the VANET most of the people focused on its friendly and cooperative environment and due to this way many different problems came in being. In VANET security is to be consider one of the primary concerns in order to provide secure communication between different nodes in a Vehicular ad hoc network environment. VANET has its own characteristics and due to its characteristics only vehicular ad hoc network security come in advanced or the popular research topic. In today's vehicular ad hoc network become one of the main topic in research studies. In this report Denial of service (DOS) attack on network availability is shown with its security level in VANETenvironment.DOS attacks are very dangerous in VANET because they affect the network. So in this report how to detect the DOS is shown.

ACKNOWLEGMENT

It is a pleasure of mine to find myself penning down these lines to express my sincere thanks to all my coordinators to give me this opportunity of preparing this project, to enhance my professional as well as my technical practice. I express my deep sense of gratitude to my DISSERTATION MENTOR Mrs. Isha to give me knowledge about the topic and the concept related to this research. Without this guidance I could not even imagine to complete my dissertation on time.

My deepest gratitude is to all my teachers for always boosting my moral and providing me encouraging environment. In the last, I would like to thank my parents, without whom nothing was possible.

Deepali

DECLARATION

I hereby declare that the dissertation proposal entitled, **Analysis of enhanced Request Response Detection Algorithm for Denial of Service Attack in VANET**, submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date-

Investigator-Deepali

Reg No-11310836

CERTIFICATE

This is to certify that **DEEPALI** has completed M.tech dissertation proposal titled **Analysis of enhanced Request Response Detection Algorithm for Denial of Service Attack in VANET,** under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

The dissertation proposal is fit for the submission and the partial fulfillment of the conditions for the award of M.tech Computer Science & Engg.

Date: **Signature of Advisor**

Name: Isha

UID: 17451

TABLE OF CONTENTS

Abstract……………………………………………………………………………i

Acknowledgement……………………………………………………………...ii

Declaration…….…………………………………………………………….iii

Certificate…………………………………………………………………….iv

Table of Contents……………………………………………………………v

List of Figures ……………………………………………………………..11

Chapter 1 Introduction………………………………………………….…..1-9

1.1 VANET……………………………………………………………………………………………………1

1.2 Various types of ad hoc network……………………………………………………………………2-3

1.3 Classes of Attack…………………………………………………………………………………………3-6

1.4 Denial of Service attack……………………………………………………………………………6-9

Chapter 2 Review of Literature……………………………………………..10-21

Chapter 3 Present Work……………………………………………………..22-24

3.1 Problem Formulation……………………………………………………..22

3.2 Objectives…………………………………………………………………23.

3.3 Research Methodology……………………………………………………24

Chapter 4 Results and Discussion…………………………………………..25-36

4.1 Introduction to NS2………………………………………………………25-26

4.2 Proposed Algorithm……………………………………………………….27

4.2 Simulation Parameters……………………………………………………27-29

4.3 Results……………………………………………………………………...29-36

Chapter 5 Conclusion and Future Scope……………………………………..37

Chapter 6 References…………………………………………………………38-39

Chapter 7 Appendix………………………………………………………………..40

LIST OF FIGURES

Figure1. VANET Architecture…………………………………………………………......1

Figure2. Classes of Attack……….……………………………………………………….3

Figure3. Taxonomy of Denial of service attack……………………………………………5

Figure4. Offender achieve DoS Attack…….………………………………………………7

Figure5. Channel Jamming...…………………………………………………………….8

Figure6. Network Loading……………………………………………………………...9

Figure7. Open command prompt………………………………………………………….27

Figure8. How to run TCL…….…………………………………………………….......28

CHAPTER 1

INTRODUCTION

Now a days vehicular ad hoc networks (VANET) are having more and more importance. It is used to enhance the protection of passengers and to reduce the occasion of traffic congestion. VANET is the class of MANET i.e mobile ad hoc networks. In this every node can move freely within the network and were stay connected, every node can communicate with other node. Now these days various accidents occur on the road, the estimated number of death is about 1.2 million in a year and various people are injured about 40 times of the number. So the aim of VANET is to provide safety. Its main potential is to improve vehicle and road safety, traffic efficiency and convergence as well as to provide comfort to both drivers and passengers. There are two types of nodes such as Road Side Units (RSUs) and On Board Units (OBUs). In case of road side unit there are fixed nodes along the routes where as on board unit refers to the mobile nodes which are equipped with radio interface that enables connecting to other nodes in wireless way. VANETs are dynamic in nature. Various numbers of nodes can communicate once as a group but they can change their own structure caused by leaving of member or joining with another node. Therefore it means nodes are "keeping in touch" with other nodes in a group to maintain the network.

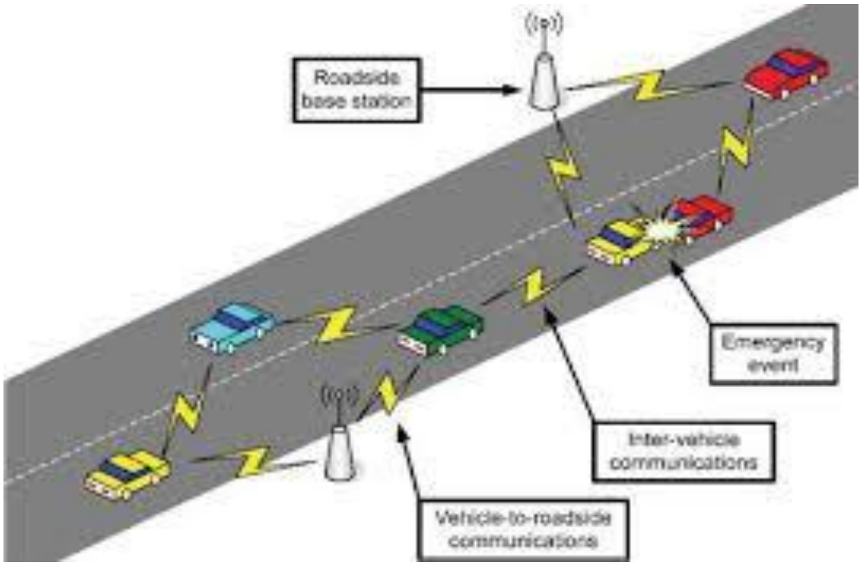

Roadside base station
Emergency event
Inter-vehicle communications
Vehicle-to-roadside communications

Figure 1: Vanet Architecture

1.1 Various types of Ad hoc Networks:

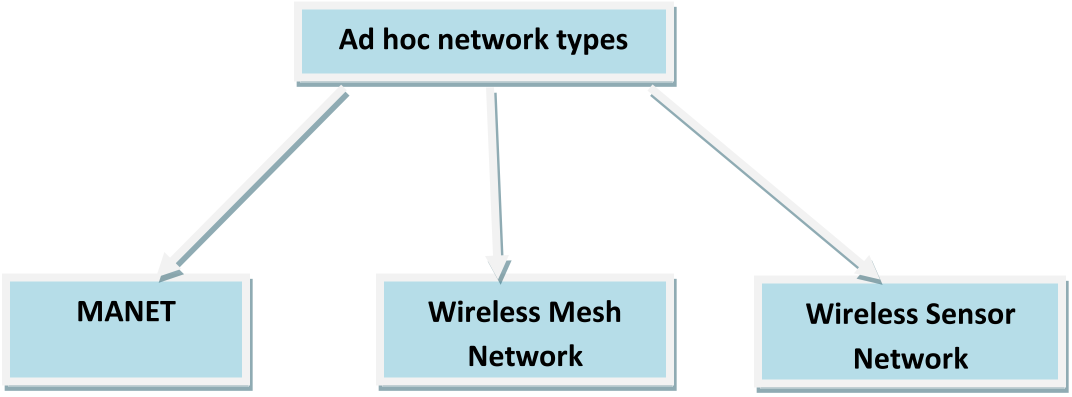


Figure 2: Types of Ad hoc network

MANET:

It stands for mobile ad hoc network which is infrastructure less in nature. In this wireless technique is used for connecting the nodes. To move a data from one point to other point controller is not required. Topology is maintained by all the nodes in network. In this nodes employed as router and host all nodes have ability to connect or depart the network in this inadequate bandwidth and node mobility are entailed. It issued different types of protocols and benefits in power battery consumption and routing traffic. The route is discovered with the help of routing protocols and changing topology causes link failure in network.

Wireless Mesh Network:

In this network mesh topology is used that interact with each other through radio nodes. The network employed mesh router, mesh clients and gateways for interaction purposes. For communication mesh clients used laptops, cell phones and wireless devices. The mesh router is not connected to internet but cover traffic in path to and from a gateway.

Wireless Sensor Network:

A wireless sensor network is a combination of small senor nodes that obtained energy from the batteries. A sensor node is made up of sensing unit, processor, transceiver and power source. The nodes are fewer in hardware and support software deployment. It is very useful for data gathering purposes like military, irrigation and underwater. The main problem in WSN is power efficiency that is attained by DPM or DVS.

1.2Various Classes of Attacks on VANET

Each class defines different types of attacks, their threat level and as well as attacks priority. The major aim of this model is to easily identify the attacks and their association to different class.

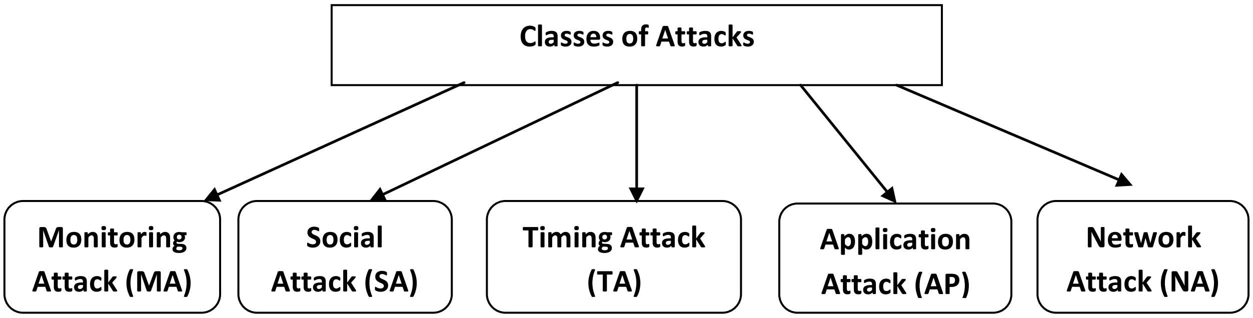


Figure 3: Classes of Attack

1).First Class: Network Attack: In this class attackers can affect directly other vehicles and infrastructure. These attacks are very dangerous because they affect the whole network. The main aim of these types of attacks is to create problem for legitimate users. In this class various attacks are come under like denial of service attack (DOS), Distributed denial of service attack (DDOS), Sybil attack, node impression attack.

2).Second Class: Application Attack: The main aim of this class is to change the content of the applications by attacker and he can use for their own benefits. In this the attacker can modify or change the actual message and send wrong messages or fake messages to other vehicles due to which various accidents occurs. For example Bogus information attack in which attacker send fake information to the network and these fake messages affects the behavior of users on the road.

3).Third Class: Timing Attack: In this case the main aim of attacker is to only add time slot in the original message due to which delay in the original message is to be created. It means the attacker does not disturb the other content of message , he just only creates the delay in message and the messages are received after it requires time.

4).Fourth Class: Social Attack: Its main aim is to indirectly create some problem in the network. The legitimate users show some angry behavior when they receive these types of messages. When the user heard some wrong message then he ultimately affects his driving behavior by increasing his speed of his vehicle. In this way the attack may occur.

5).Fifth Class: Monitoring Attack: The main aim of the attacker is to monitor the whole network and listen the communication between vehicle to vehicle and vehicle to infrastructure. Due to which if attacker find any related or useful information then he pass this information to the concern person.

1.3 Communication Types of VANET:

There are three communication types of VANET i.e vehicle to vehicle (V2V), vehicle to infrastructure (V2I) and vehicle to road side communication.

1).Vehicle to Vehicle Communication: This type of communication is for short type of communication. It is for short range networks it means it is very fast and efficient and also provides real time safety to vehicles.

2).Vehicle to Infrastructure Communication: This type of communication is for long range vehicular networks. It makes use of pre existing networks infrastructures such as wireless access points.

3).Vehicle to Road Side Communication: The communication between the vehicles and road side unit are supported by vehicle infrastructure protocol and vehicle to road side protocol.

1.4 Various Goals of VANET:

1).It improves the traffic safety and comfort to drivers.

2).There is proper information of traffic.

3).Local danger warning.

4).Reduces accidents, traffic intensity.

1.5 Various challenges of Ad hoc Network:

Vehicular ad hoc network are having various challenges which are as follows:

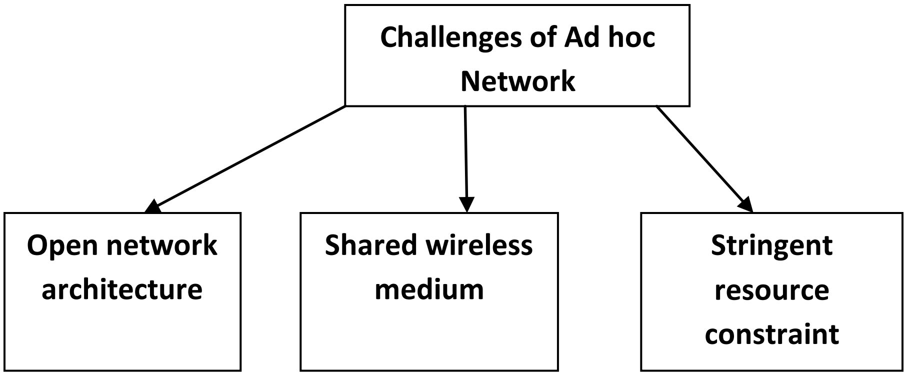

Challenges of Ad hoc Network
Open network architecture
Shared wireless medium
Stringent resource constraint

Figure 4: Various of Ad hoc network Challenges

Each person having knowledge that mainly the wired network do not work with vehicular ad hoc network domain.

While in case of wireless network every person know and it is also true that the security of VANET is current research topic among all other topics, but because of various other unique characteristics such as self configuring and self organizing of VANET there are various challenges. Most common challenges like shared highly dynamic network topology, wireless medium, stringent resource constraints and open network architecture. It is correct that the solution of wired network is not mostly directly applied on vehicular ad hoc network domain.

There are also various other challenges in Vehicular ad hoc network with respect to the wireless security because of some of following reasons which are as follows:

1. Mainly the wireless network is having various chances of attacks because of active eavesdropping to a large amount of interfering.
2. In this the trusted third party because of its lack or problem, it is very difficult to use or implement any security mechanisms.

3. Each and everyone knows that the Vehicular devices are having limited or having very less computation capability and power consumption functionalities which are mainly helpful and vulnerable for Denial of Service attacks. And it is impossible for human being to run large security algorithms which need high computations like public key algorithms etc.
4. Because of different properties of vehicular ad hoc network such as infrastructure less and self-organizing, there are many chances for trusted node to be compromised and to establish attacks on the networks.

And it is also very difficult to make a difference between the stale routing and faked routing information due to mobility of node mechanism. There are also other ways of attack in node mobility mechanism it is due to enforces frequent networking reconfiguration.

1.6 Various advantages of Vehicle Ad Hoc Network:

1. VANET favours the drivers in different ways like different types of warnings, related to bad weathers and also related to road conditions.
2. The drivers find the best route for reaching the destination with the help of VANET.
3. VANET also favor the driver to connect with an internet while during driving their cars or within the cars.
4. VANET also helps the car for establishing communication between themselves with the help of VANET infrastructure.
5. If any problem comes during driving the car, by using VANET-based network the driver can take help.

1.7 Denial of Service attack:

Denial of service is one of the serious level attacks in vehicular network. In Dos attack the attacker attacks the communication medium to cause the channel jam or to create some problems for the nodes from accessing the network .Its goal is to block the services and availability of network by sending a packet stream continuously thus overloading the on board radio trasnductor and road side radio transductor making unable to process further.

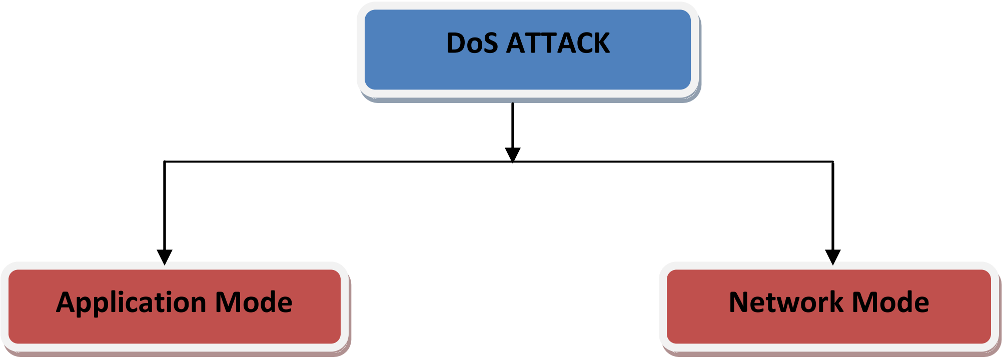


Figure 5: Taxonomy of Denial of Service Attack

Application Mode: In this type the application attack will broadcasts a wrong message to mobile vehicle drivers and then diverts them to another path.

Network Mode: This type of DoS attack creates a very serious problem in VANET. In this the bandwidth is blocked by an attacker.

1.6 There are three ways due to which the offender can achieve the denial of service attack:

1).Communication channel jamming

2).Overloading of network resource

3).Packet dropping

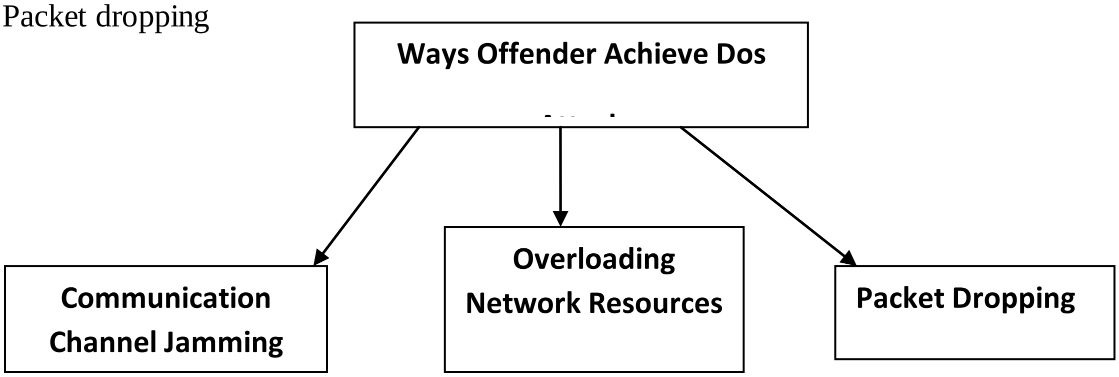

Ways Offender Achieve Dos
Communication Channel Jamming
Overloading Network Resources
Packet Dropping

Figure 6: Offender achieve Dos Attack

1).Communication Channel Jamming

In this type the attacker jams channel due to which users are not able to access or use the network. As its name indicate to jam the channel. In this a very high frequency are send the attacker and then jam the communication. Only when nodes leave the domain of attack it can able to send or receive message.

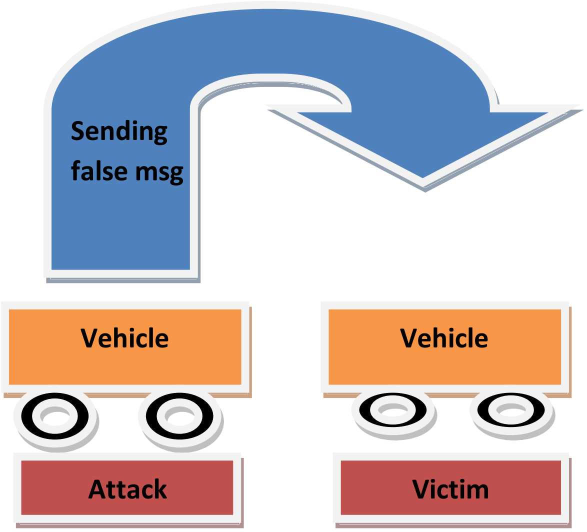


Figure 7: Channel Jamming

2). Overloading of Network resources

As its name indicates in this the attacker can overload the node resources so that nodes cannot perform or does other work or tasks. All node resources are busy in message verification which comes from attacker node. In this RSU is engaged to check messages thus road side unit is not able to response to any other nodes and in this way service is not present or unavailable.

DOS attack In Vehicle to Infrastructure communication

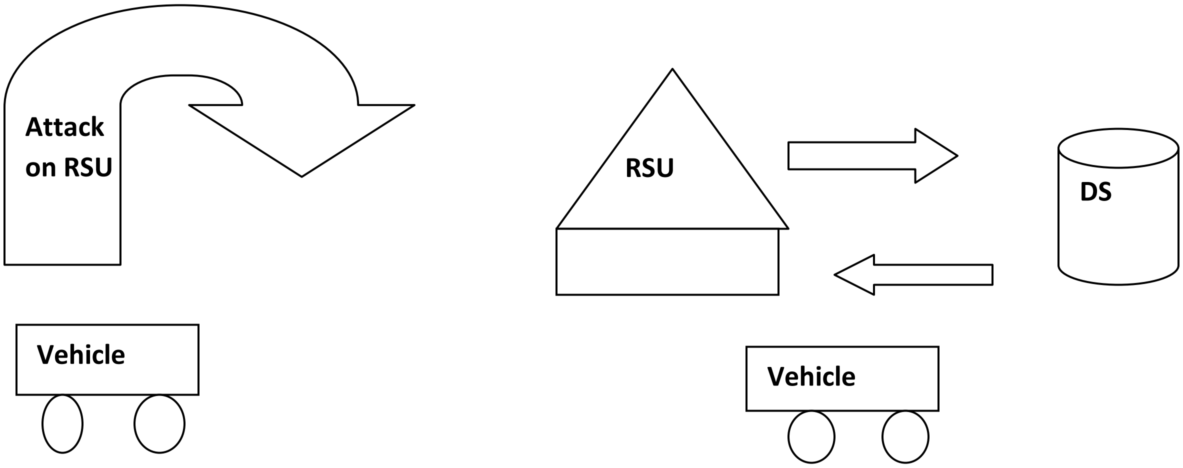


Figure 8: Network Overloading

3).Packet dropping: In this type the various packets are to be dropped among various vehicles .Each were having their own IP address. False information is to be given to every vehicle due to which various accidents may occur. So this is all about the packet dropping.

CHAPTER 2

REVIEW OF LITERATURE

Detection of various attacks that exists as threat to security are detected and studied in the. Literature survey**.**

Roselin et al. (1) proposed a model for detecting the dos attack by using attacked packet detection algorithm. The mechanism is attached to the road side unit (RSU).In this approach vehicle send various messages to the RSU by using APDA mechanism. It is used for detecting the position of vehicle. This ADPA algorithm is used before verification time. When the position is detected after that information is stored in the road side unit (RSU).The position or velocity of vehicle is identified by the on board unit. This algorithm is mainly used for detecting the vehicle’s position and also detects the packet send by vehicle. If the packet was not attacked by attacker then vehicle cannot be tracked.

This algorithm is used before verification time and also used for increasing security. Its main purpose is to avoid delay overhead.

Verma et al. (2) proposed a bloom filter based detection method which provide security service to the legitimate vehicles in VANET,this bloom filter method is used to detect the Denial of service attack.

A bloom filter based detection method is also used to defend against the IP spoofing of addresses in DOS attacks. It mainly focuses in increasing the systems connectivity as well as reliability.

In this paper two techniques are used for detecting the denial of service attack:

1).Traffic capacity based Dos detection scheme

2).IP-CHOCK (FILTERING) DETECTION ALGORITHM

1).Traffic capacity based Dos detection scheme: Now in first technique he generally shows that which flows are at victim attack and which are genuine. By using the packet detection mechanism various dos detection attacks are to be found. In this technique all packets are to be marked when the packet reaches its destination there should be a mark on packet by all of the RSU on the path that means the packet is traversed. It means the packet that traverse from that path are having same mark. So by using bloom filter packet it filter outs the packet. It means the packet which is having marked it means that packet is secure no attack on the packet.In this way by using this bloom filter based detection method author comes to know about the attacked packet.

2).IP-CHOCK (FILTERING) DETECTION ALGORITHM: In this algorithm three phases are to be there Detection Engine Phase 1, Detection Engine Phase 2,Bloom Filter Phase. The detection engine phase1 collects the data which is to be processed in the next phase. While in detection engine phase 2 only process the information which is to be collected by the phase 1.If phase 2 does not found any malicious node then the information is to be stored in the data base. In third phase active bloom filter with a hash function is to be used. If in the decision engine malicious node is to be finding then alarms are generated and sends a link to all other nodes or vehicles that there should be a malicious node. In this way denial of service attack is to be detected.

Lyman et al. (3) proposed real time detection of dos attack. In this paper author mainly focus on the "jamming" of periodic messages called beacons which are exchanged by vehicles in platoon. In a platoon truck or leading vehicle is driven by person. In this the detector first only detects the event happening after that he computes hoe explainable occurring of collision is. It detects by using unicast method which is based on linear regression. This paper is based on two techniques:

1).A simple real time detector method for detecting the dos attack.

2). The detector is validated in terms of detection and false alarm probabilities within the limited time for two types of jamming attacks.

Two models are to be assumed:

1).Random jamming

2).On-Off jamming

1).Random jamming: In case of random jamming every packet which is transmitted in the channel is corrupted independently.

2).On-Off Jamming: In the off state packet are safe means no packet is to be jammed, while in case of ON state beacons are to be destroyed.

Jamming detection method used in this paper:

It includes two phases installation phase and second phase is normal operation of detector.

1).Installation phase: The main aim of this is to divide the vehicles in to various groups in such a way that no other beacon can collide with other beacon. In this way the detector made some estimates for beacons generation moments.

2).Normal Operation of detector: In this the detector firstly listen the channel and then after that records the identifier of vehicles and in this way beacons are successfully received. The decision is to be made as follows:

1).Alarm: There is at least one group, which shows one beacon has not received.

2).No alarm: Otherwise

Dak et al. (4), presented literature survey on security challenges in VANETs. In this paper various security issues are shown confidentiality, integrity, authentication, availability and non repudiation which are aimed to secure the vehicle to vehicle (V2V) and vehicle to infrastructure (V2I).Various attacks are shown in this paper which are as follows:

1).Sybil attack: In case of Sybil attack multiple fake nodes are to be present who broadcast the wrong information. In this the on board units are attached to the vehicles through which multiple copies are to be send to the other vehicles and every node contains the different identity. The problem starts when the malicious node is able to act as multiple vehicles and provides false data.

2).Node Impression attack: It is defined as the attack in which modified message is to be send by the node and act like that the message is come from the originator for the unknown purpose. In this case two techniques are used to detect the attack i.e greedy algorithm which is used for detection of malicious vehicle and the other algorithm is outlier detection algorithm which has been proposed for overcome this problem.

3).Sending False Information: As its name indicates it is defined as the attack in which wrong or fake information is send between the nodes to create a chaos scenario. The fake information is send by the attackers to vehicles for their own reasons. A technique is used to detect this attack is group signature technique. This technique is relies on password access.

4).ID Disclosure: In this case the identity is disclosed by the node and node's location is to be tracked. In this the target node is to be observed by the observer and virus is sending to the neighbors nodes. In this way when the neighbors are attacked by the virus then location of nodes are to be identified.

Sinha et al. (5), proposed a technique to secure from denial of service attack and some solutions to overcome from attacks are also discussed in this paper.

In VANET various attacks occur in the communication medium due to which channel jam. So to prevent from these kinds of attack or to save the legitimate nodes some techniques are to be used.

1).Oppress the node resources: In case of denial of service attack the attacker aim is to overwhelm the node such that they can not perform any other tasks.

Case1: Vehicle to vehicle communication suffers by DOS attack; in this the attacker can send the wrong message to victim node that "Accident at location Z". Then after that this message is send again and again by attacker, to keep the victim node busy and he will properly deny to accessing the network.

Case2: In this vehicle to infrastructure communication suffers by DOS attack; whole attack is to be done on the road side unit (RSU), in this road side unit is engaged to check messages due to which RSU are unable to give response to other nodes and in this way service is unavailable.

Now solution for this kind of attack is that the node can protect itself from attack. Every vehicle should have on board unit (OBU) to take decisions to block the denial of service attack. If the attack occurs the processing unit will suggest to use switch technology or to use frequency hopping technique.

2).Physical Layer attack: Channel Jamming: As its name indicates the channel is jammed by the attacker due to which other users are unable to access the network.

There are two possible cases:

Case1: In this case the attacker can send high frequencies due to which communication is jammed between nodes .It means nodes are unable to send or receive messages. Only the nodes receive or send messages when node leaves the domain attack.

Case2: In this type of attack the communication is jammed between nodes and road side units. In this case near to RSU the attacker launch the attack to jam the channel which causes the network breakdown. This causes network unavailability.

Now solution for this kind of attack is that he made assumption that jammer only transmits when valid radio activity is signaled. Using this technique the attacker decreases the probability of detection.

3).Distributed Denial of Services (DDOS):It is very dangerous attack. In this the attacker attacks from different locations. The attacker might be use different time slots for sending messages. The goal of this attack is same to down the network.

Case1: The main purpose of attacker is to send messages to victim by using different locations or by using different time slots. The aim of attacker is to block the network or to breakdown the network.

Case2: In this case road side unit is attacked by the attacker or road side unit unable to respond which causes denial of service.

Sinha et al. (6), proposed the queue limiting algorithm which will help to prevent or protect from denial of service attack. In this paper firstly described the system model which shows that every vehicle is having on board unit and for communicating with other vehicles they use DSRC channels. In this access points are present, vehicles send information about collision, crash and then after that access points send information to go that place. If access points are not present then information are passed by the vehicles. But if attacker knows then the things will be uncontrolled. Various false messages are sending to the victim node. Al channels are filled with CLASS 1 in this way victim node is not able to communicate with other vehicles due to which accident occurs.

Now the prevention mechanism includes that attacker send various false safety messages to victim node by using DSRC channel. In this technique every vehicle are having some upper bar for receiving few number of safety messages. If node receives limited number of messages then it protects the node from denial of service attack. It means that when DOS attack occurs every internal queues of on board unit are to be filled and all are busy in processing of these messages. If few messages come from sender, the task performed by on board unit is easy. So this queue limiting algorithm is used for protecting from DOS attack.

Mohammed et al. (7), proposed techniques to detect and notify the attacks like “intrusion detection”. Various attacks occur on vehicular ad hoc network such as Dos attack, black hole attack, Sybil attack etc. There are various characteristics of networks like highly dynamic network topology, shared wireless medium. In simple language intrusion is defined as any set of actions that done to compromise confidentiality, integrity or available of resource. The main work or goal of intrusion is to protect the system because if intrusion is detected then the attacks can be controlled.

Intrusion detection is having three phases: the first phase includes data collection which is followed by analysis phase and then finally minimizes the impact of attack.

Intrusion detection system is categorized according to detection techniques which are as follows:

1).Signature based system: The collected data should be compared with the database behavior of certain attacks. If data coincide with malicious behavior then attack is detected.

2).Anomaly detection system: The IDS detects behavior which shows before prestablished behavior and gives the notification.

3).Specification based system: It is the process in which a set of conditions that a protocol must satisfy. When the protocol does not meet the conditions then it means attack occurs or attack is detected.

Then after that in this paper three intrusion detection architecture are shown:

1).Stand-alone IDS: In this process every node is having its own local resource to collect data on remote nodes and detects the intrusion. In this way no data is to be exchanged and there is no information about position of other nodes.

2).Cooperative and distributed IDS: As its name indicates there is a cooperation between neighboring nodes to detect the intrusion. This type of cooperation is to be done by exchanging information or alerts.

3).Hierarchical IDS:In this process various groups or set of clusters are to be made and having one cluster head which is determined by cooperative algorithm between nodes. It main function is to reduce the cooperation between nodes. The cooperation is done by elected cluster head and each of the members of same cluster.

Verma et al. (8), proposed Bloom filter based IPCHOCKREFERENCE detection method to prevent from denial of service attack. User Datagram Protocol (UDP) –based on flooding which is also common form of DOS attack. In this paper the author shows that various types of flooding attacks occur. Just only one algorithm is not sufficient to detect the attack. So there is need to combine the detection system which uses various methods for detecting the attack. In case of spoofing attacker generate 32 bit numbers which is used as request addresses for attacking message.

The three goals of this paper are as follows:

1).The message delivery ratio is to be increased, by increasing the stability of link route message and also overhead is to be decreased, by reducing retransmission of message caused by drops occurring.

2).Reliability and connectivity of vehicle is also increased, by decreasing link breakage between communicating nodes and up to date information is to be provided by forwarding vehicle.

3).The overhead is also reduced which results from sending beacon between nodes.

The CUSUM technique is used which is based on IPCHOCKREFERENCE method. CUSUM is applied to detect the changes in digested traffic.

Devi et al.(9),proposed Request Response Detection Algorithm after Attacked Packet Detection Algorithm which will be used for detecting the denial of service attack in VANET. In this vehicles are having on board radio transductor and on the road side there are road side transductor.

Early detection algorithm is used before the verification. For the detection of attacked packet this algorithm considers mainly frequency and velocity of vehicle. Firstly the road side radio transductor (RSRT) sets the range and decides the range can form network which mainly depends on the transmission range. After that the vehicles request the RSDT with the help of attacked packet detection technique. Then the vehicles are verified by RSDT and make the database. Whole timestamp, location are shown by attacked packet algorithm.

After using attacked packet detection the vehicles are verified buffered in to RSRT. The jamming due to denial of service attack can again reduced by using Request Response detection Algorithm. Now in case of RRDA the vehicle which want to enter that are enter by request RSRT. Then it updates the counter. After that it checks the hop count. In this way RRDA algorithm works. The RRDA is used for further new request which wants to engage the network.

R.Hunjet et al. (10) proposed the working of different relay nodes in the wireless sensor network. Where as in mobile ad hoc network there are a large of problem when some more node is added to the network. Now in ad hoc network the relay placement is continuously changed during the connectivity of the network, and also the calculation of various relay coordinates should take place by using non-global information due to various scalability issues. In this paper the author also introduces the method for performing distributed MANET that how mobile ad hoc network work with the relay placement within nodes n-hop neighborhoods. Networked Autonomous Vehicles (NAVs) must act as various mobile relays for placing themselves at their chosen locations. The various algorithms are used for maintain the connectivity in the network and also compared, but the most famous and efficient algorithm is bridge and articulation point detection (BAP) algorithm. In this thesis paper the author also explain the combined use of up to five additional relay nodes and due to which the algorithm may increase the average ground unit network connectivity up to 82% and also the size of the network’s largest segment up to 54% in mobile ad hoc networks of 10 to 25 nodes.

This whole work is used to show that MANETs is very useful for the NAVs. The average greatest size and ground unit connectivity of a network are improved by the addition of these nodes utilizing appropriate distributed movement algorithms.

T.Sandeep et al. (11), discuss about the various challenges of vehicular ad hoc network which is used by everyone today and as well as in future. Various issues in the vehicular ad hoc network are also present such as quality of service, rapid reaction with stringent timing constraint, frequent discontinuities, dynamic topology, congestion control during emergency, less bandwidth user authentication and data authentication, revenue generating user applications, balances in between privacy and liabilities, search and rescue operation zero visibility situations , etc these all are the different challenges that are faced while designing the VANET. In this paper, they also mentioned the VANET routing protocols which are having.

X.Rngyan et al. (12), Hybrid sensor network technology is a major component of future ITS applications. The author proposed a hybrid architecture which makes combination of VANETs and roadside WSNs for intelligent navigation. As different from traditional ITS application, Sensors in wireless sensor network and VANET are mainly used for perceive and exchange roadside and vehicular information for supporting the intelligent navigating decision process. In this the author firstly provides protocol architecture, and then they discuss about the various scenarios and use various cases of the system in intelligent navigation. After that, the author discuss about the software and hardware implementation of the prototype, analyze a simulation on the discussed scenarios, and present a full fledge data communication experimental result to prove the feasibility of the prototype.

In greedy forwarding technique immediate neighbors of destination node are used for forwarding the packets table is maintained which contains information of neighbors. In this beacon messages send to neighboring nodes in particular time period if forwarding node cannot obtained hello message from neighboring node then that node is deleted from table. The problem in greedy forwarding technique is local maxima problem in this if sender having the two neighbor nodes on same distance then sender will not decide to send the data packet to which neighboring node in greedy forwarding.

S.Farzad et al. (13), In this paper, the author tries to eliminate the security problem in vehicular ad hoc networks. As author said earlier also that Vehicular Ad hoc Network (VANET) is one of the new forms of Mobile Ad hoc Network (MANET), it is also one of the new form of simple ad hoc network also but it must be clear that simple ad hoc network is not a mobile network. In vehicular ad hoc network there is use of same functions like mobile connectivity protocols for communication or the data is transferred between the vehicles as well as also between the roadside equipments. In case of VANET, the devices such as Wireless device sends an information to the nearby vehicles, and by using this they may transmit the message from one vehicle to an another vehicle, due to which only VANET helps us in increasing road safety and traffic optimization. While different technologies there are some other important issues of VANET. In case of VANET the security is one of the most important problems. It is just because of an open network, which is easily accessible from everywhere in VANET radio range and it becomes very easiest target for the attackers and the malicious users.

The vehicular ad hoc network is also a combination of different other technologies such as communications and computing which gives the benefits for using various other types of its other technology. Due to which every person came to know that vehicular ad hoc network is a advance technology and it also became very easy for the attackers to ruin or to attack on the network. Then the defaulters or other the malicious users try to break or challenge the network for their own selfish behavior and for some other illegal use. The simple ad hoc protocols play an important role in vehicular ad hoc network but they are smaller than VANET because of its small size limit. Various characteristics of VANET are similar and taken by the Ad hoc network but it is very hard in implementing security capabilities and as well as the policies.

Paul et al. (14), discussed the various characteristics of VANET such as high dynamic topology, frequent disconnect network, mobility modeling, battery power and communication environment. In this paper they also discussed about various pros and cons of routing protocols. Various pros of topology based are route discovery is not required, low latency and flooding required when demanded some of cons are excessive flooding causes disruptions and unused paths occupy bandwidth. Various pros of position based are high mobility pattern and scalability some of cons are GPS does not works in tunnels.

P.Vineetha et al. (15), author proposed the Inter-vehicular communication of future having some authority for avoiding some of the problems of namely, road travel, collisions, traffic congestions, emissions, fuel consumption,. The largest implementation in the ad hoc network is vehicular ad hoc network. The main conclusion is that the security of VANETs is having a lot of importance, because many malicious attacks may destroy the human lives. This paper is mostly focused on enhancing the security of such networks by secure protocols designed for VANETs. The author also discuss the existing security protocols, the author mostly improve the intelligence of decision system for enhancing the security and data, with the help of the physics of vehicle dynamics and historical data, which may be taken from different sensors like In-Vehicle Systems (IVS), GPS, and On-Road Assistance systems (ORA).

Aggarwal et al. (16) discuss the various applications of VANETs such as intelligent transport applications, comfort applications, collision prevention, cooperative driving, traffic improvements and location-based services. These applications help the drivers, avoid congestion on road, and also help to maintain security. After that various pros and cons of routing protocols are also discussed in this paper.

T.Pratibha et al. (17), author proposed different vehicular ad hoc network routing protocols which exits. VANET is a fast combination technology with a simple ad hoc network and also with a cellular technology. All the technologies are mainly used for improving the road safety and efficiency and also to communicate different vehicle with other. In the vehicular ad hoc network there is no use of any infrastructure or no use of installing infrastructure other vehicles are try for exchanging information within the networks because of which the road safety must be improved.

In this the author also discussed that there is an ad hoc on demand distance vector which provides idea of mobile gateway and also won in improving the vehicle to vehicle connectivity on road. The main idea for implementing AODV is that it establishes and also disconnects the node because of involving of its dynamic nature earlier. GPSR that is position based protocol which helps in communication in the vehicular network. The main aim of GPSR protocol is that it gives a very large rate of successfully delivered packets on single hop or on many hops. Due to which GPSR is used which is position-based routing does not have to maintain other routes. While, it might be possible to simulate the topology-based routing.

S.Mohommad et al. (18), author mainly discuss about the worm hole attack This type of attack taken place in the presence of at least two or more other malicious nodes. In this type of attack the node establishes its own tunnel that is if a packet comes to any one of them, it may be induced to any other pair of these malicious nodes by this tunnel and that node may be broadcasts it into other network. This may gives a very small connection which is controlled with the help of these malicious nodes. So they make a control on all the Packets that come to them and also security of data within packets or delete them. So the wormhole work is a wrong understanding of the network topology. This type of attack may destroy the network operation, mainly in networks that may prefer on demand routing protocols such as DSR or AODV .So in this paper the author provides an efficient method for saving wormhole attack in vehicular ad hoc networks and also detects the attacker as soon as possible. In this paper, the author makes take help of packet leashes and the defined algo of authentication known as HEAP. The correction also takes place on the packet leashes algorithm. The author establishes this type of scheme so that no attack can enter in the network. The author tries to define that this technology is having a low overhead, increases security and performance takes place in an acceptable level of the network.

CHAPTER3

PRESENT WORK

3.1 Problem Formulation

Vehicular ad hoc networks are a special class of mobile ad hoc networks where the mobile nodes are the vehicles moving on the roads. Vehicles in the network exchange information between each other without the requirement of the infrastructure because of their ad hoc nature. Vehicles are equipped with on board units such as radio transductor and geographical positioning system (GPS) to provide for the location services. Since these vehicles communicate wirelessly, they are prone to several attacks such as Sybil attack, denial of service attack etc. Taking into account such attacks, security becomes important for the vehicles in order to ensure the safe communication between vehicles. All the vehicles need to be authenticated in order to take part in communication between the vehicles. In our work we will be focusing our attention on the denial of service attacks. In Dos attack the attacker attacks the communication medium to cause the channel jam or to create some problems for the nodes from accessing the network .Its goal is to block the services and availability of network by sending a packet stream continuously thus overloading the on board radio trasnductor and road side radio transductor making unable to process further. In our base paper two algorithms are to be used:

1).Attacked Packet detection algorithm (APDA)

2).Request Response detection algorithm (RRDA)

In case of APDA algorithm vehicles can be verified by using attacked packet detection algorithm (APDA) in which the vehicle has to be in the range of the RSU to join the network. The APDA compares the timestamps to accept or discard the packet. This algorithm detects the denial of service before the verification for a particular vehicle has been done. The APDA verifies the vehicles on the basis of velocity of the vehicles, however there may be emergency vehicle moving at higher speed , in that case the emergency vehicle will be marked as malicious and not allowed to join the network.

After initial verification the second algorithm i.e RRDA is to be used when a vehicle joins the network, the study considers request and response detection algorithm to verify the new requests. And the RRDA is also based on hop count comparison, as the vehicles move in and out of the transmission range of the RSRT, the hop count will change, as a result it will be difficult to detect the malicious vehicle on the basis of hop count.

3.2 Objectives

The main objectives of the study are as follow:

1. To detect the malicious vehicles by using the scheduling approach.

2. To compare the proposed protocol with existing RRDA algorithm for DoS detection.
3. To analyse the performance of enhanced protocol in terms of throughput and routing overhead.

3.3 Research Methodology

In vehicular ad hoc networks, nodes are the vehicles which move at higher speeds as compared to nodes in mobile ad hoc networks. Since vehicles communicate wirelessly, they are prone to various attacks. In our work, we will focus on the denial of service attacks in vehicular ad hoc networks. Vehicles communicate with road side units to have access to information. Initially all the vehicles need to be registered prior to take part in the communication. We will use detection of the malicious vehicle in the network during the verification phase. The vehicles before entering in the network must pass the verification test defined by attacked packet detection algorithm. The difference between time at which vehicle sends the request and receiver receives the request must be less than threshold value for the vehicle to pass the verification test. According to APDA, the road side unit sets a range, so all the vehicles in its range can communicate with it, however any malicious node lying outside the range of the RSU can send the verification request so for that vehicle the difference of the sending and receiving the request at the RSU will be more than threshold value so it can be detected. However, if any node manages to pass the verification test and becomes a part of the network then we can detect it by allocating them time slots. After the node has passed the verification test and it becomes the part of the network. Road side units will allocate the time slots to the vehicles for communication. Since the malicious vehicle will continuously flood the control messages, so the RSU can easily detect which vehicle is sending more than average number of requests received by it in particular time slots assigned to the respective vehicles.

1. Verify the vehicles using time stamp method defined by APDA2. Allocate the time slots to the vehicles by RSU
3. After verification, the vehicles will start communicating.
4. If particular vehicles tend to send the more number of requests as compared to other vehicles, then mark it as malicious.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction to NS2

NS2 is a network simulator whose main purpose is to provide network research. This tool is developed by UC Berkeley. It provides a collaborative environment. It includes NAM files i.e network animator. The programming is done or written in C++ language, where as simulation scripts are written in OTCL language. The main aim or goal of NS2 is as follows

1. To make protocol design and traffic studies.

2. Ns2 is used for comparing the protocols.

3. The new architecture design are also made.

NS2 also provides collaborative environment:

1. It is freely distributed and open source.

2. It also increases the confidence in various results.

The various NS2 models are as follows:

1. The first one is traffic model which includes web, telnet, FTP and constant bit rate (CBR).

2. The second model i.e transport protocols which includes Unicast: UDP multicast and TCP.

3. The third model is routing and queuing which includes Ad Hoc routing and wired routing.

4. Then the next model is queuing protocols which includes drop-tail and RED i.e Random Early drop.

Various researches based on NS2 are as follows:

1. Multicast: routing and reliable multicast

2. Transport: TCP congestion control

Now various components of NS2:

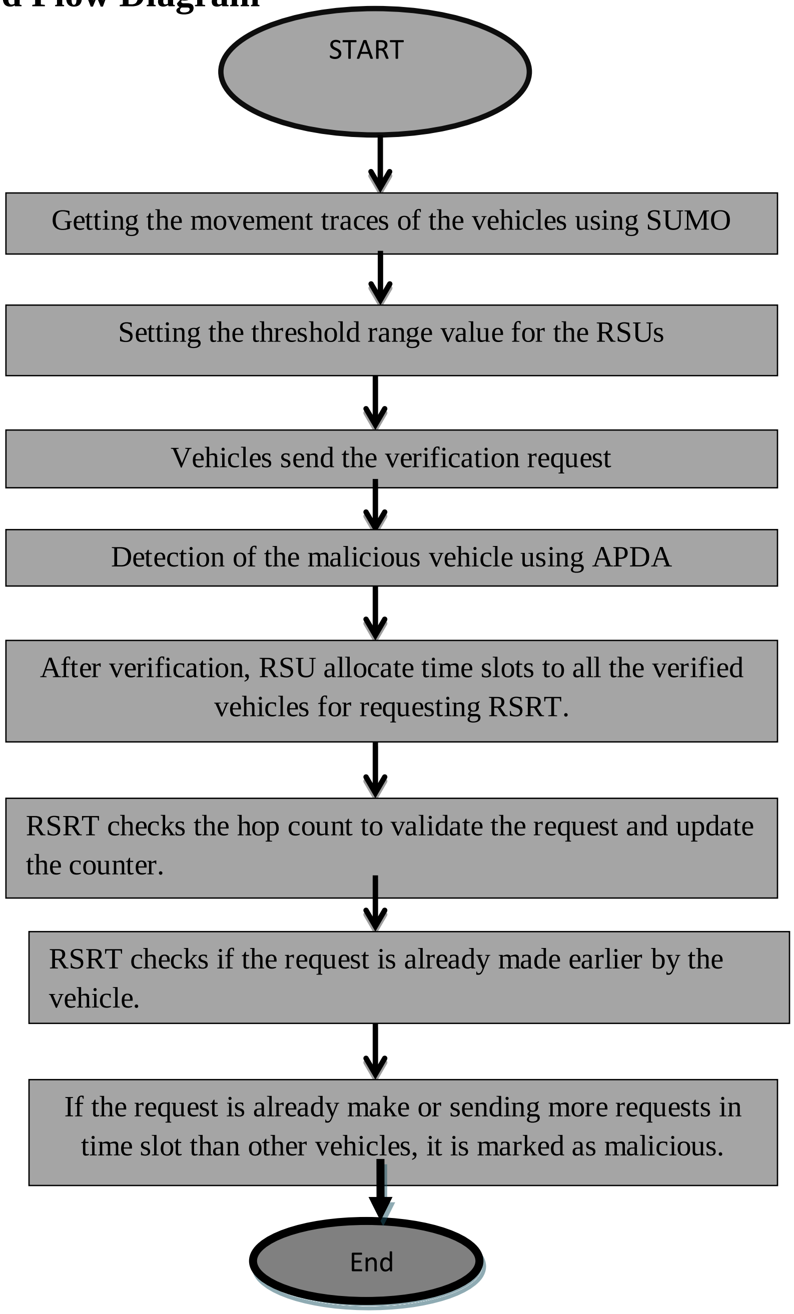
1. NS2 is the simulator itself.

2. NAM: It is a network animator. This animator is used to generate the ns scripts. This is used only for presentation it is not used for research tracing.

3. Pre-processing: It includes traffic and topology generators.

4. Post-processing: It includes simple trace analysis, mainly in awk or in TCL.

4.2 Proposed Flow Diagram


START
Getting the movement traces of the vehicles using SUMO
Setting the threshold range value for the RSUs
Vehicles send the verification request
Detection of the malicious vehicle using APDA
After verification, RSU allocate time slots to all the verified vehicles for requesting RSRT.
RSRT checks the hop count to validate the request and update the counter.
RSRT checks if the request is already made earlier by the vehicle.
If the request is already make or sending more requests in time slot than other vehicles, it is marked as malicious.
End

/

4.3 Proposed Algorithm:

1.Vehicular node sends request for communication to RSU form setting up a communication.

2.RSU verify the packet with timestamp given on request packet.

3.Check the request packet for sender ID if is blocked due to malicious activity.

4.Check the packet if already sent the request previously:

a. If request already done check the timestamp of requested packet.

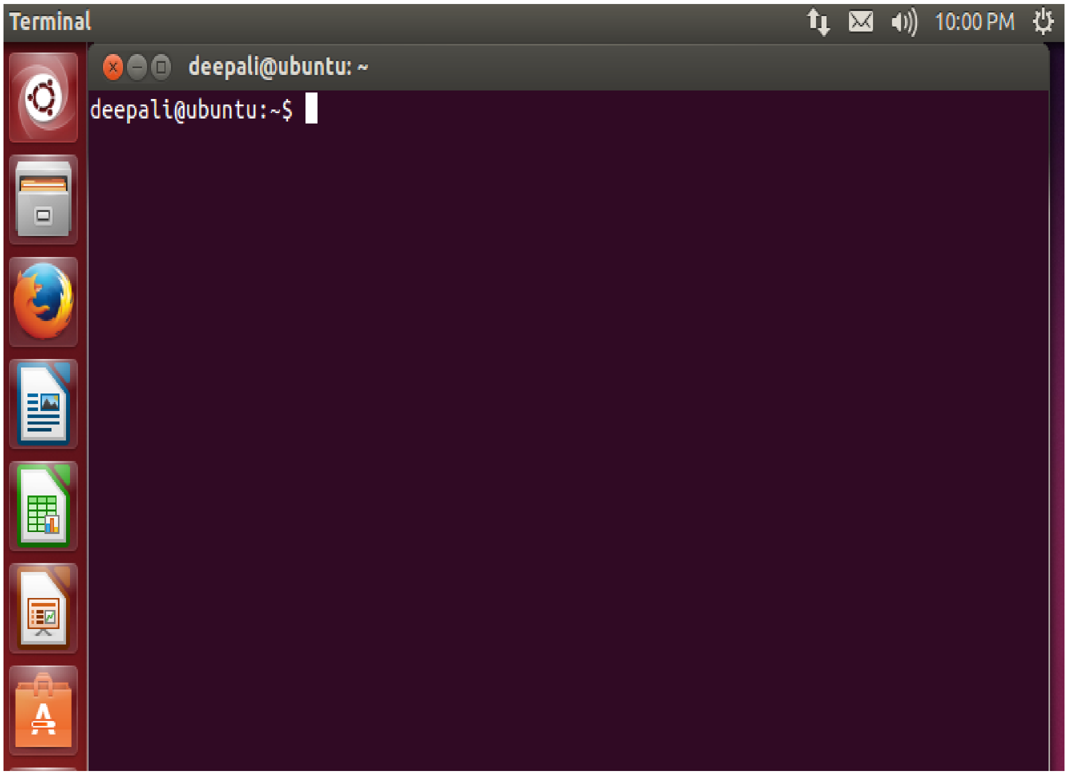
b. If timestamp difference is less than threshold then request get rejected.

c. And if difference is greater than the threshold value then request accepted and authorized to setup communication.

d. After authorization the communication starts within network and information is passed on next RSU unit.

4.4 Implementation

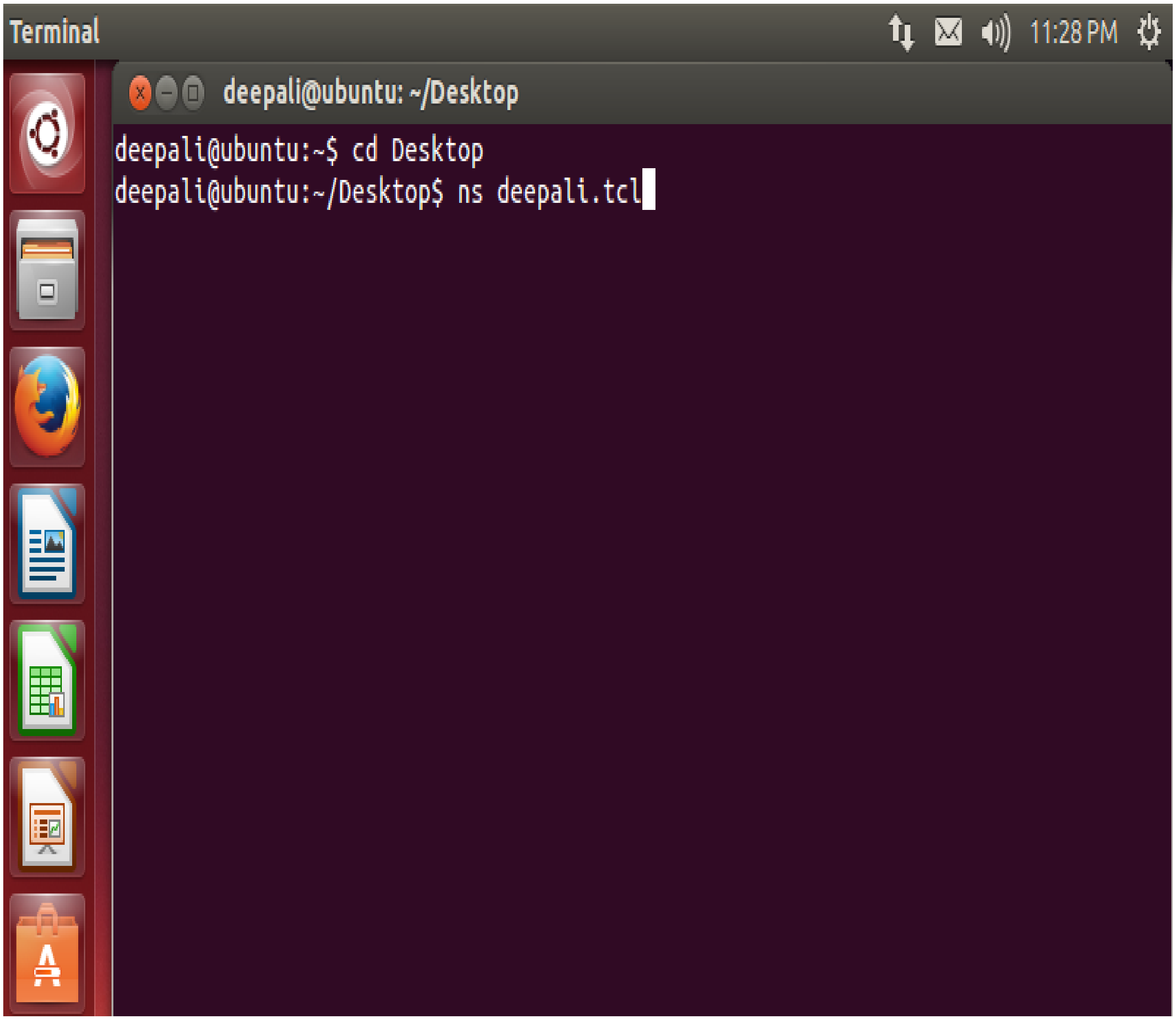
The figure shows the main front of NS2.In this page the various command are to be written.



```
deepali@ubuntu:~$ 
```

Figure 9: Open Command Prompt

For opening the tcl file firstly go to terminal then writ the command i.e. cd Desktop which shows that the file is placed in the desktop. Then write the command i.e. ns deepali.tcl by writing this command the tcl file is opened.



```
deepali@ubuntu:~$ cd Desktop
deepali@ubuntu:~/Desktop$ ns deepali.tcl
```

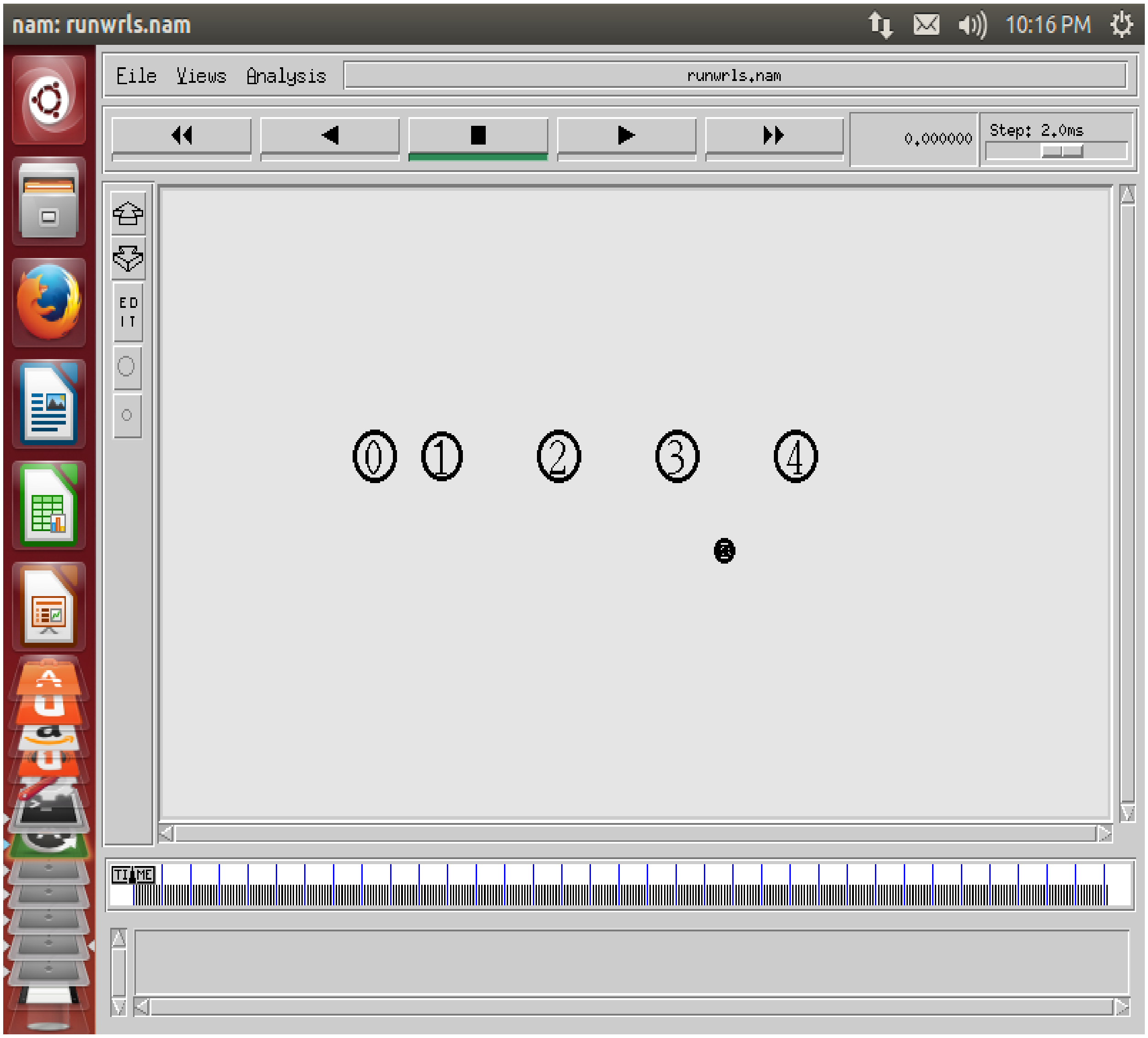
Figure 10: How to run tcl file

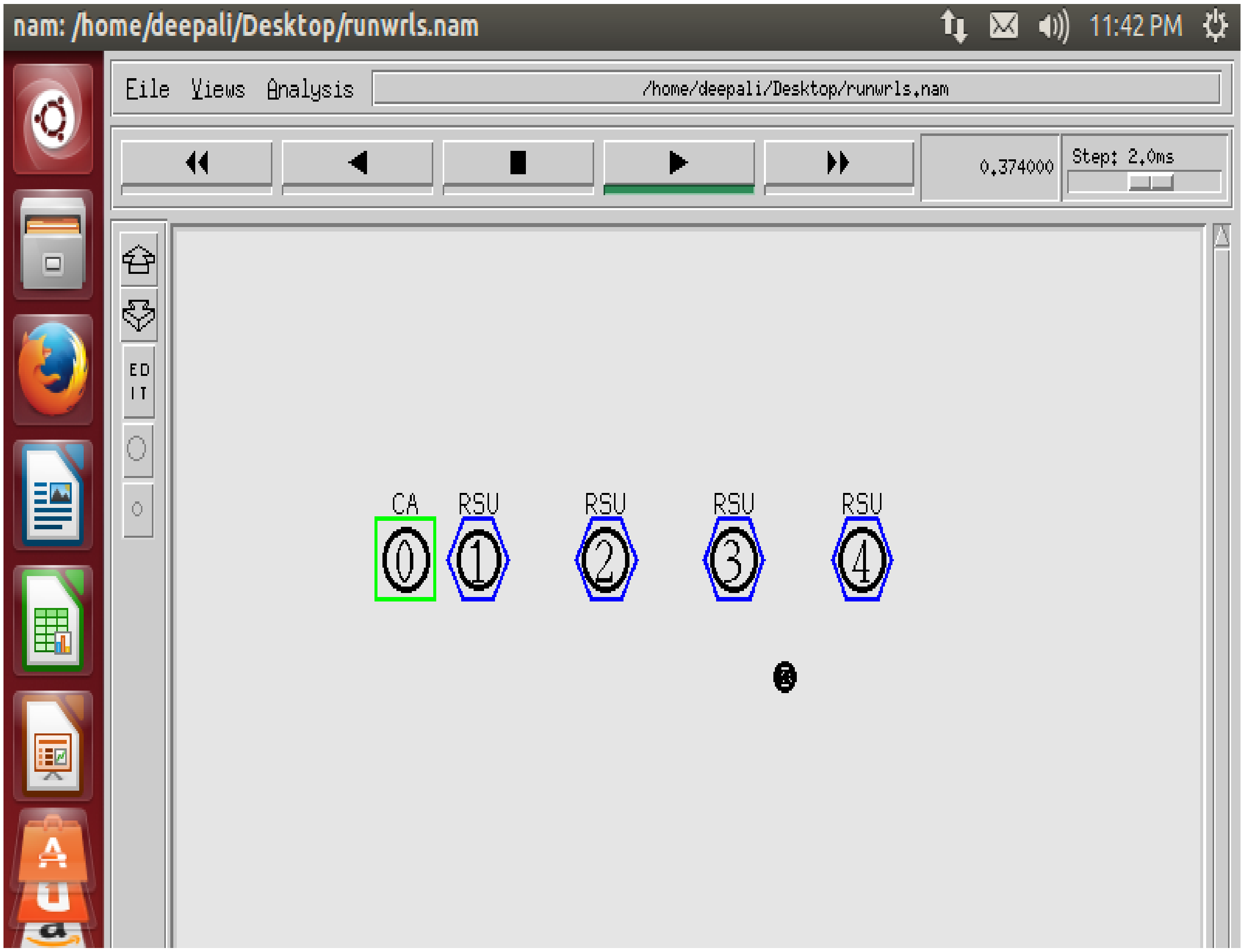
Here is the results of thesis The simulation parameters that have been taken are listed below.

S.NO.	Parameter	Value
1	Transmission Range	250m
2	Wireless medium	IEEE 802.11
3	Simulation Time	100s
4	No. of nodes	8

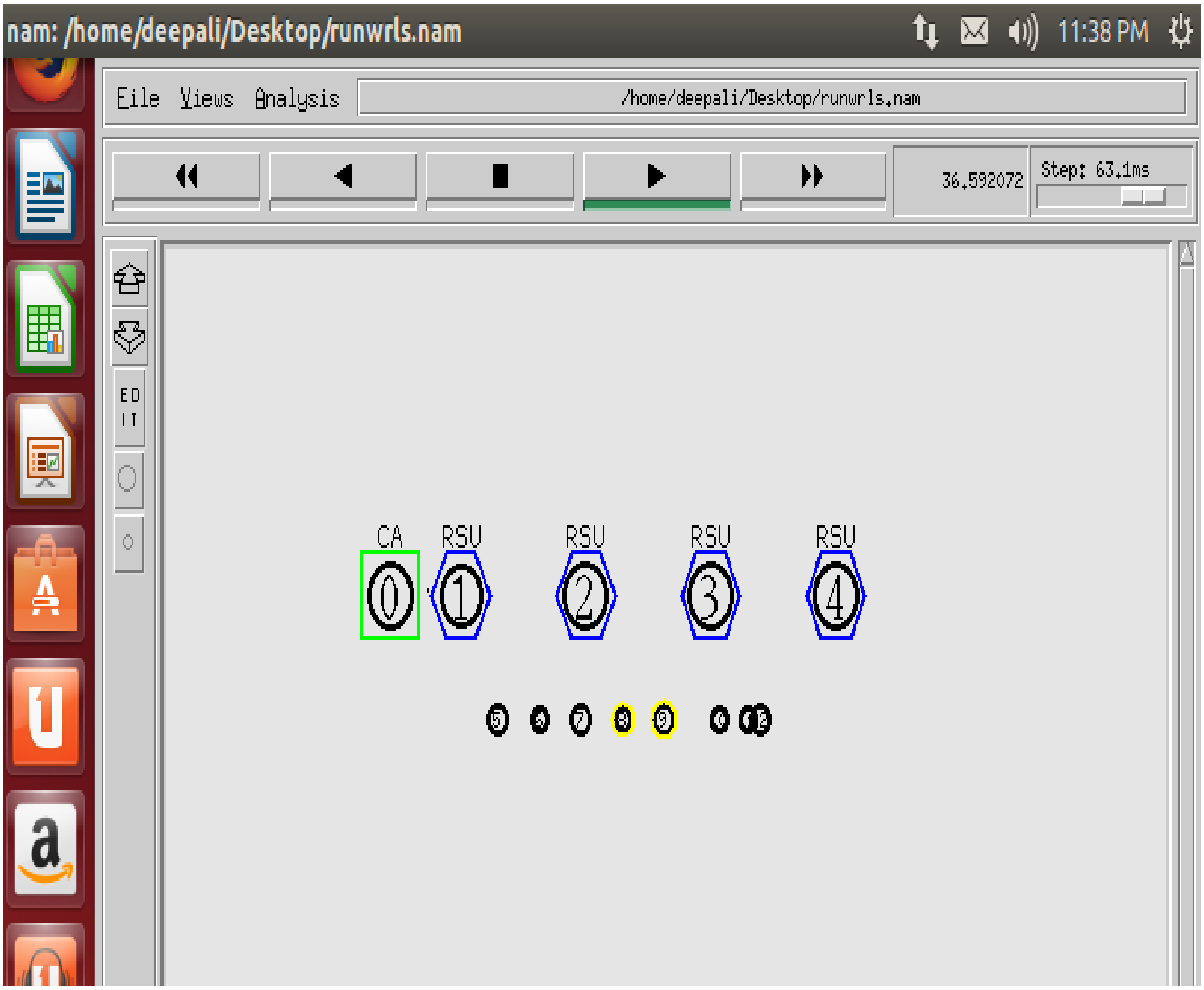
Figure 11: SIMULATION PARAMETERS

Then write the command i.e. deepali2.tcl.After writing this command the tcl file is to be opened.

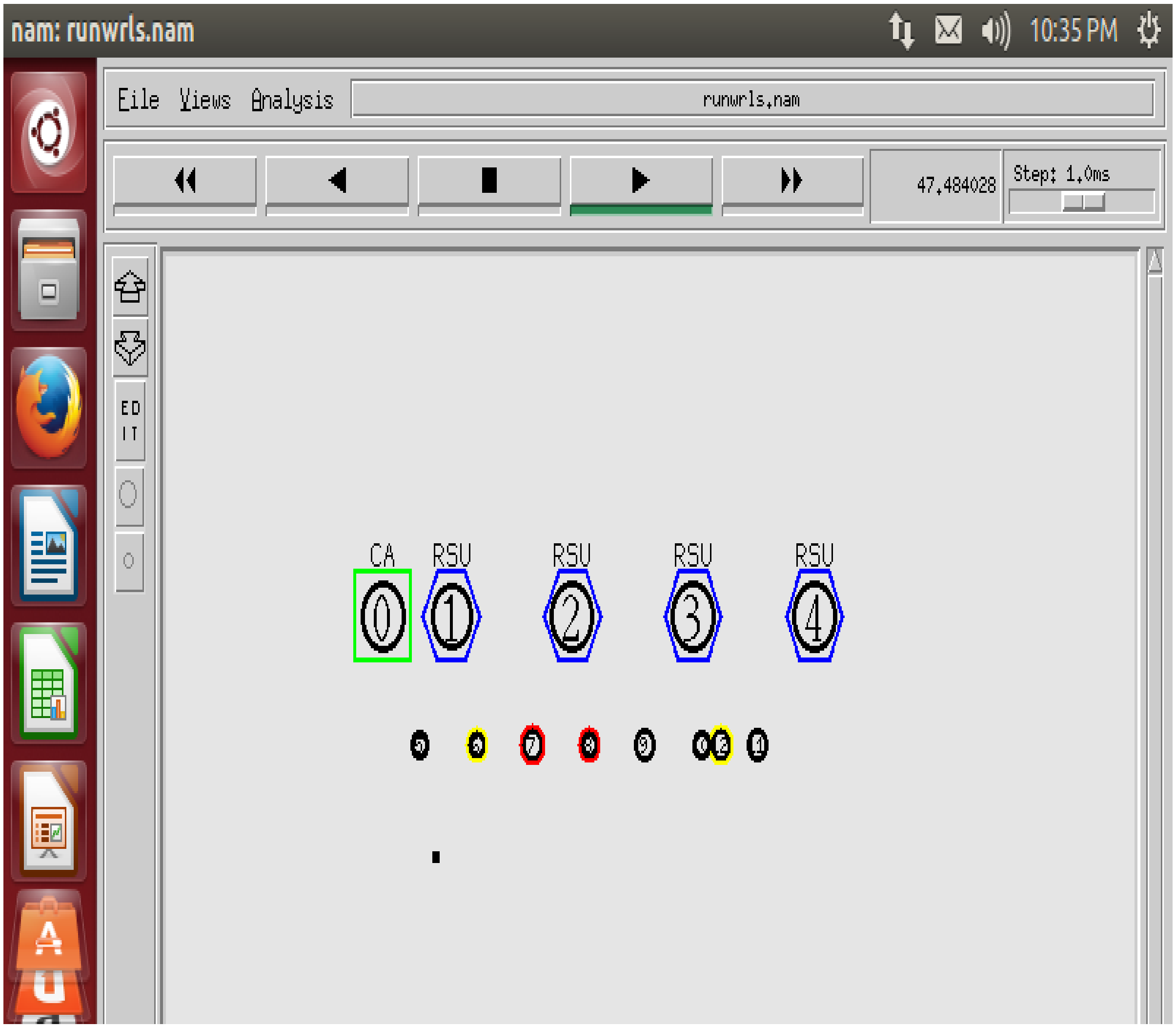



nam: /home/deepali/Desktop/runwrls.nam
11:42 PM
File
Views
Analysis
/home/deepali/Desktop/runwrls.nam
0.374000
Step: 2.0ms
EDIT
CA
RSU
RSU
RSU
RSU
0
1
2
3
4

After opening the ns deepali2.tcl there are four RSU i.e four road side units are present and there is one centralized authority and eights nodes i.e eights vehicles are to be shown.After that press the play button then all vehicles start moving from one position to another and they start communicating with other vehicles and with RSU’s.



This shows that the nodes with red circle is detected as malicious nodes.i.e on those nodes the attack is detected.While yellow nodes are suspicious nodes which shows that the are very close to attack but aatck is not done on yellow nodes.The centralized authority have an sender id it means if one time the node is detected that it is malicious then that node can not be again gone through that network.If the node is detected as malicious then it can’t be entered in to the network. The malicious node can be detected by using scheduling approach.



47.484028

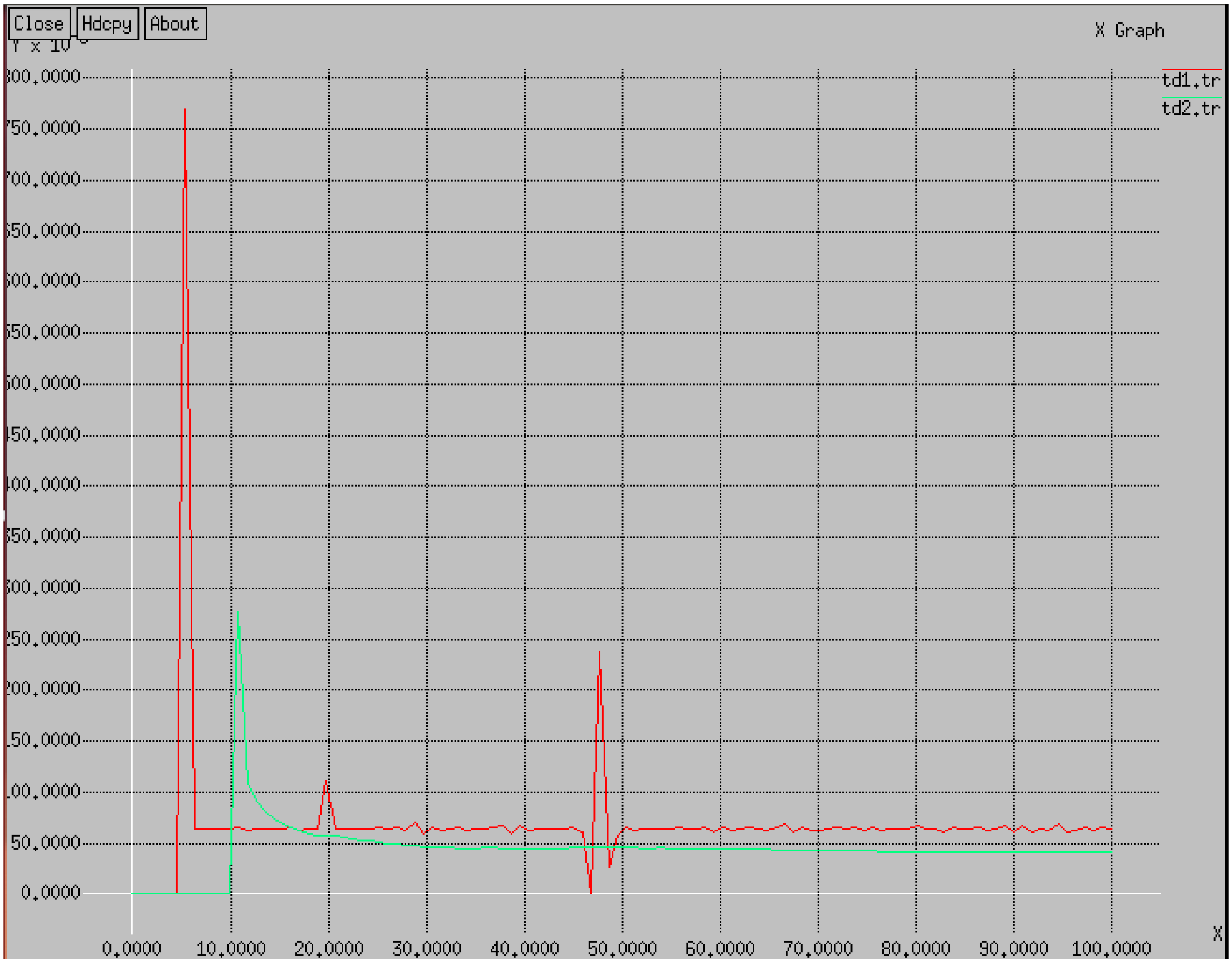
Step: 1.0ms

Some of the security issues which we take in our implementation and their results are show below. And the results are shown by using graphs using different parameters.

4.5 Comparison of Graphs

4.5.1 Delay Comparison

The Xgraph shows the performance of the enhanced protocol as compare to the previous one. Starting with the Graph 1 the delay2 is negligible as compared to delay1 which was the delay in RRDA Protocol.



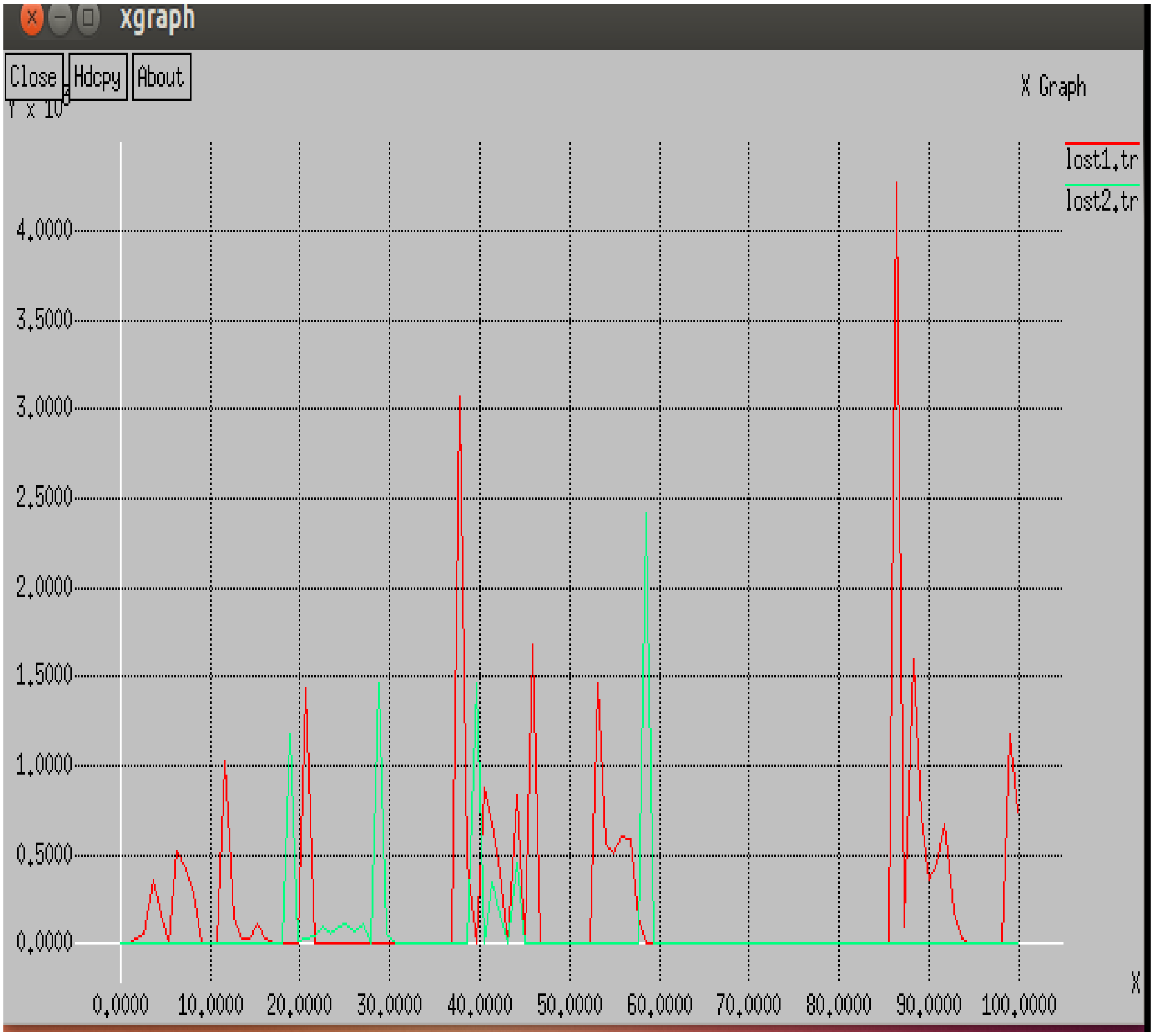
Graph 1: Delay

In this graph the red line represents the old delay while the green line represents the new delay.

The enhanced algorithm gives better result in terms of delay as compared to previous algorithm.

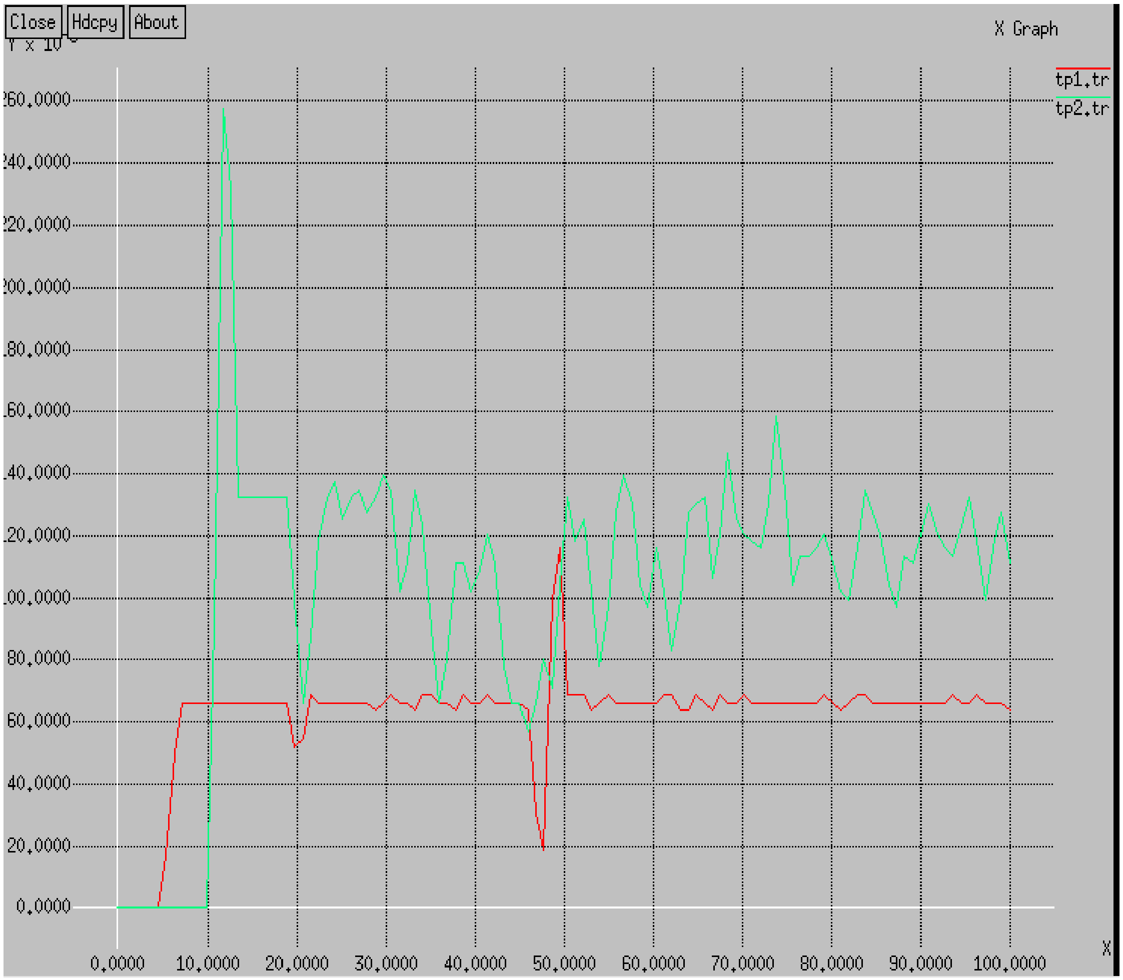
4.5.2 Packet Loss Comparison

This graph shows the packet loss which is again less because of single hop communication. So, the enhanced protocol gives better results as compared to old protocol.



Graph 2: Packet Loss

This graph shows the overall throughout which is more in case of enhanced RRDA protocol, thus making it better as compared to other protocols.



Graph 3: Throughput Comparison

CHAPTER 5
CONCLUSION AND FUTURE SCOPE

The detection of Denial of service attack is very essential in case of vehicular ad hoc network. Till date various researches has been carried out but still at present the vehicular ad hoc network are not secured because of attacks occurring on the network. The main purpose of this report is to detect the Denial of service attack, by increasing the throughput by applying scheduling process. So this study proposes a scheme for providing an efficient mechanism to detect the attacks and reduce the accidents to a great extent.

Future Scope:

In future we are going to apply this algorithm for multiple invalid request send from multiple vehicles at the same time and detect the attacks in the early manner. So that no that no attack occurs in the vehicular ad hoc network and the ad hoc network become more safe and more secure.

CHAPTER 6
REFERENCES

1. Roselin, M.,& Mahsehwari, M.,(2013).Early Detection of DOS Attacks in VANET Using Attacked Packet Detection Algorithm (APDA),.In *Engineering and Computational Sciences, 2013*. IEEE.

2. Verma, K. & Hasbullah, H., (2014).IP_CHOCK (filter)-Based Detection Scheme for Denial of Service (DOS) attacks in VANET,.In *Engineering and Computational Sciences, 2014*. IEEE.

3. Lyamin, N. & Vinel, A., (2014).Real-time detection of Denial-of-Service attacks *In802.11p vehicular networks, 2014.*IEEE.

4. Raw, R. &Kumar, M., (2013).Security Challenges, Issues and Their Solutions For VANET, *International Journal of Network Security,2013*.

5. Sinha, A. (2014) Technique to Secure DOS Attack, *International Journal on AdHoc Networking Systems,2014.*

6. Sinha, A. &Mishra, K,. (2014).Queue Limiting Algorithm (QLA) for Protecting VANET from Denial of Service (DOS) Attack,2014.

7. Ouahidi, EL., (2014). A Review and Classification of Various VANETIntrusion Detection Systems, *Journal of Engineering Science and Technology, 2014.*

[8]Verma, K. Hasbullah, H., (2012).An Efficient Defense method against UDP Spoofed flooding traffic of DOS Attack In VANET,.*Journal of Engineering Science and Technology, 2012.*

[9] Gandhi.U, (2014). Request Response detection algorithm for detecting DOS attack in VANET, *Journal of Engineering Science and Technology, 2014.*

[10] Sahibi.F, (2011). The Security of Vehicular Ad hoc Networks", 2011 Third International Conference on Computational Intelligence, Communication Systems and Networks, *Journal of Engineering Science and Technology, 2011.*

[11] Tomer.P,.(2010). An Application of Routing Protocols for Vehicular Ad-hoc Networks, *Journal of Engineering Science and Technology, 2010.*

[12] Li.Y,.(2012). Maintaining Connectivity in Mobile Ad hoc Networks Using Distributed Optimization *Journal of Engineering Science and Technology, 2012.*

[13] Tayal.S,.(2012). VANET-Challenges in selection of Vehicular Mobility Model *Journal of Engineering Science and Technology, 2012.*

[14] Li.Y,.(2014). Challenges of Intervehicle Ad Hoc Networks, *Journal of Engineering Science and Technology, 2014.*

[15] Singh, S., & Agrawal, S. (2014, March). VANET routing protocols: Issues and challenges. In *Engineering and Computational Sciences (RAECS), 2014 Recent Advances in* (pp. 1-5). IEEE.

[16] Paul, B., Ibrahim & Bikas (2011) VANET Routing Protocols: Pros and Cons. *International Journal of Computer Applications (0975 – 8887)Volume 20– No.3, April 2011.*

[17] S., & Agrawal, S. (2014, March). VANET routing protocols: Security challenges. In *Engineering and Computational Sciences (RAECS), 2014 Recent Advances in* (pp. 1-5). IEEE.

[18]Mohammad's., (2012).A Novel approach for avoiding wormhole hole attack in VANET,.*Journal of Engineering Science and Technology, 2012.*

CHAPTER 7

APPENDIX

ABBREVATIONS

MANET	Mobile Ad hoc Network
VANET	Vehicular Ad hoc Network
MA	Monitoring Attack
SA	Social Attack
TA	Timing Attack
AP	Application Attack
NA	Network Attack