LOVELY PROFESSIONAL UNIVERSITY

Detection of DDoS attack in VANET using LPN (Local Protection Node)

A Dissertation submitted

By

Pooja Bansal

Regd No. 11311343

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 & Engineering

Under the guidance of

Miss Shabnam Sharma

(Asst. Professor)

May 2015

INDIA'S LARGEST UNIVERSITY

LOVELY
PROFESSIONAL
UNIVERSITY

Transforming Education, Transforming India

School of: COMPUTER SCIENCE & ENGINEERING

DISSERTATION TOPIC APPROVAL PERFORMA

Name of the Student: POOJA BANSAL Registration No: 11311343

Batch: 2013-2015 Roll No. 68

Session: 2014-2015 Parent Section: K2307

Details of Supervisor: Designation: AP

Name SHABNAM SHARMA Qualification: M Tech

U.ID 14593 Research Experience: 0.1

SPECIALIZATION AREA: Neworks And Security (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. ~~DDOS~~ Attacks in VANET and its possible solution.
2. Security aspects in adhoc network.
3. Authentication scheme in VANET.

Shabnam
Signature of Supervisor 14593

PAC Remarks: Student will focus on authentication & solution on particular type of attack & I am expecting fruitful outcome & will be presented in the form of Research Paper.

11/10/14

APPROVAL OF PAC CHAIRPERSON: Signature: 11/10/14 Date:

*Supervisor should finally encircle one topic out of three proposed topics and put up for 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.

CERTIFICATE

This is to certify that **Pooja Bansal** has completed M.Tech dissertation titled "**Detection of DDoS attack in VANET using LPN (Local Protection Node)"** under my guidance and supervision. To the best of my knowledge, the present work is the result of his 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 in Computer Science and Engineering.

Date:

Signature of Advisor

Name:

UID:

DECLARATION

I hereby declare that the dissertation entitled, "**Detection of DDoS attack in VANET using LPN (Local Protection Node)**" 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

Regn. No.

ACKNOWLEDGEMENT

I feel great pleasure in submitting this report as the culmination of my guide's efforts. This required a very hard work, sincerity and devotion that I tried my best to put in my work and in turn gained a lot of knowledge and confidence from this analysis

I am deeply grateful to my mentor respected **Miss Shabnam Sharma, Assistant Professor, CSE/IT, LPU** who has helped me in each and every step till the begin till now. She has been a constant guiding force and source of illumination for me. It entirely goes to her credit that this work has attained its final shape. I would like to thank her for her valuable advice and guidance. I would also like to thank all my friends who were always there to motivate me in every step. They helped me a lot, also thanks to all those persons who are directly or indirectly involved in completing my work.

Pooja Bansal

ABSTRACT

Vehicular ad hoc Networks (VANET) provides consistent communication to the vehicles without prefixed infrastructure with road safety related applications. VANET is an ad hoc network so it also have the properties of self-organize, adaptive and temporary network. In VANET nodes are basically vehicles they itself act as a source, destination and router to forward the data packet from source to destination. The open architecture of VANET creates problems regarding the security aspects. There will be greater chances of occurrence of attack due to its mobile nature. One kind of attack is DDoS in which there are multiple attackers that can attack the victim at different time and at different place. In our detection scheme, a LPN node based strategy is used which easily detect the attacker and consumes less time.

.

Table of Contents

List of Figures

List of Tables

CHAPTER 1
INTRODUCTION

Wireless ad hoc Network (WANET) is a kind of wireless network. Network is ad hoc as it relies on infrastructure-less network such as no access points etc. WANET consist of wireless mesh networks, MANETs, Wireless sensor networks. VANET is subpart of MANET.

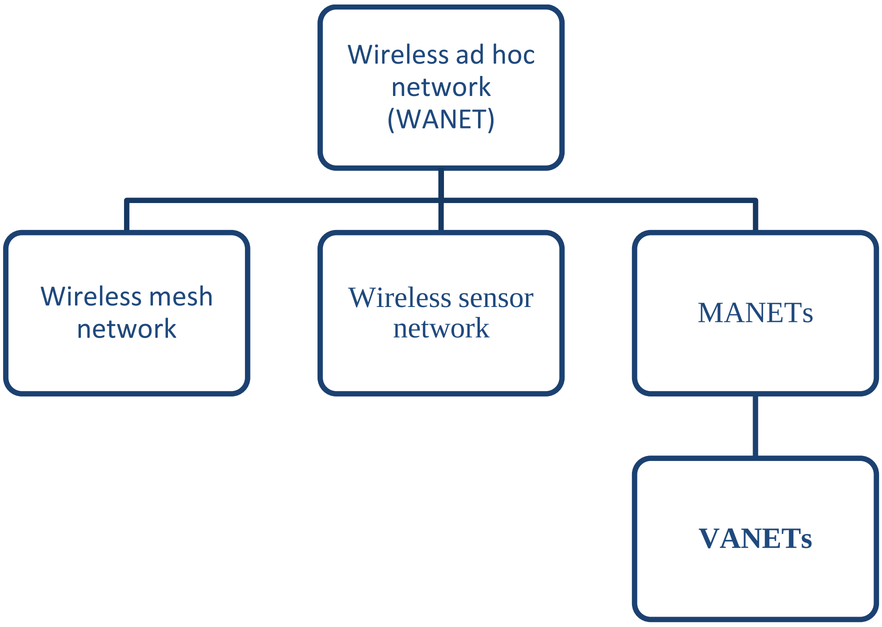


Fig 1.1 Types of Wireless Network

Ad Hoc Network: It is also known as infrastructure free network. In this no fixed infrastructure is available means no access points are used for communication. It is self-organized, no central administration is required to control and manage it. It is a kind temporary network which is mostly deployed in emergency situations. It is further divided into following parts as shown in fig 1.1:

- Wireless sensor network
- Wireless mesh network
- MANET

Wireless Sensor Network: WSN is networks in which collection of hundred to thousand sensor nodes are communicate with each other using wireless medium. Size of sensor nodes can be varying. It can be like a dust particle which we cannot able to see with naked eye or it can be large. Transmission range of nodes is limited that why it require intermediate nodes to transfer data from source to destination node. In this, sensor nodes collect the information and then forward that information to particular node which is known as sink node. Nodes can be homogenous or heterogeneous. Example: to detect the earthquake, this type of sensor network is used.

Wireless Mesh Network: In this mesh topology is used. Various elements are used in this gateways, mesh router and mesh client.

MANET: MANET is stand for mobile ad hoc network. In this, mobile nodes are communicating with each other without any fixed infrastructure. In this, nodes that are in range of each other will communicate directly, and other uses the intermediate nodes for communication. In Fig 1.2, A node want to communicate with B, both are in direct range, so they communicate directly. In fig 1.3, A node wants to communicate with D node but D node is not in range of A node so it uses node B and C as intermediate node to send data to D node. It is self-organized, adaptive and infrastructure less network and in this nodes are able to detect the presences of other nodes.

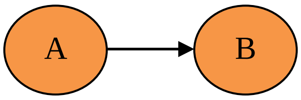


Fig 1.2 Direct communication between nodes

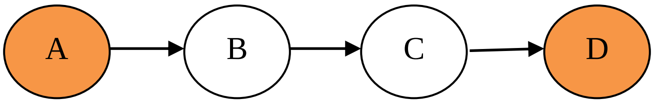


Fig 1.3 Communication by using intermediate nodes

VANET (Vehicular Ad hoc Network) uses vehicles as mobile nodes for the communication purpose and for data sharing. VANET is an ad hoc network so it also have the properties of self-organize, adaptive and temporary network. In VANET nodes are basically vehicles they itself act as a source, destination and router to forward the data packet from source to destination. In VANET network it converts every participating vehicle into a wireless router or node. The range of that particular network is in between 100 to 300 meters. As the car comes into the network then all the vehicles participated in that network are able to share information among others. But as they falls out of that network range then are no more able to communicate with the vehicles. VANET connects vehicles into a large mobile ad hoc network to share information at large scale. The first system that makes use of these networks is the police and fire vehicles to communicate with each other for the safety purpose.

Communication facilities in VANET can be configured in three ways viz. inter-vehicular communication, vehicle-to-roadside communication and routing based communication. Inter-vehicular communication facilitates communication one vehicle with another. Vehicle-to-roadside unit communication facilitates communication of vehicles and the infrastructure that are installed along the road in regular intervals. Routing-based communicates transmits messages from one vehicle to another till the message is received by the vehicle that the sender wants to send the message. Communication facilities are provided with the aid of roadside unit, on-board unit and a trusted third party.

1.1 VANET consists of three types of communication:

- Vehicle to Vehicular (V to V) or Inter-Vehicular Communication.
- Vehicular to Infrastructure or Vehicle to Roadside Communication.
- Routing Based Communication.

- **Vehicle to Vehicle Communication:** The communication takes place between one vehicle to another vehicle. The inter-vehicle communication configuration uses multi-hop multicast to transmit traffic information over multiple hops to a group of receivers.

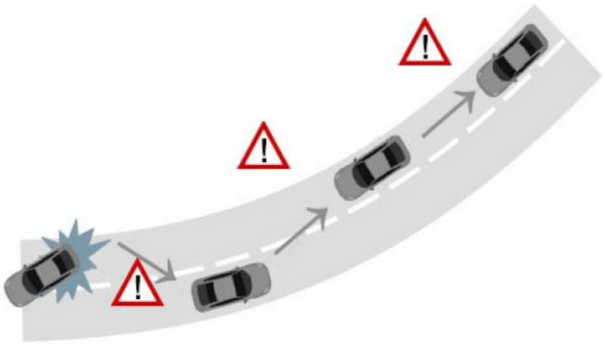


Fig 1.4: V-V Communication

- **Vehicular to Infrastructure:** In Vehicular to Roadside communication vehicles communicate with each other through Roadside units (RSUs). The vehicle-to-roadside communication configuration represents a single hop broadcast where the roadside unit sends a broadcast message to all equipped vehicles in the network.

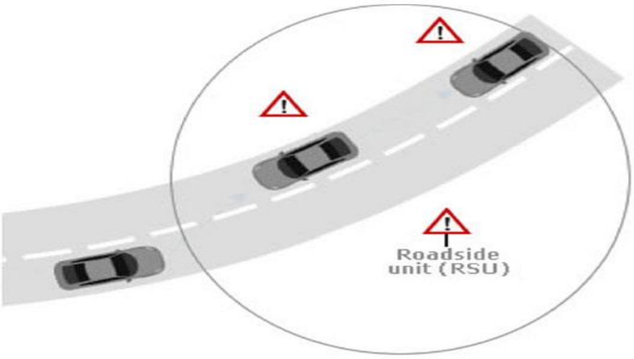


Fig 1.5: V-I Communication

- **Routing Based Communication:** This is a multi-hop unicast where a message is forwarded in a multi-hop fashion until the vehicle carrying the desired data is reached. When vehicle having the desired data receives the message, it immediately sends a unicast message containing the desired data to the vehicle from which it has received the message, which is then charged with the task of forwarding the data to the vehicle that had generated the message.

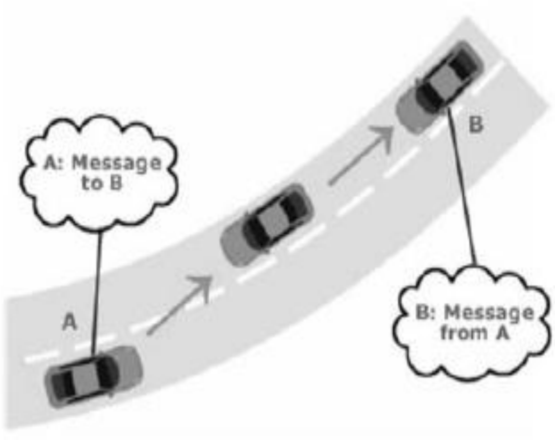


Fig 1.6: Routing Based Communication

1.2 Characteristics of VANET

- *High mobility:* Mobility in VANET is very high. Vehicles moves on road with high speed due to which link duration between vehicles will be very less. Because of this more reliable and stable routing is required to give efficient and long duration link.
- *Multi hop routing:* Multi-hop concept is when intermediate nodes are used to communicate. If two nodes want to communicate and they are in direct range then no need of multiple hop in between. But if two nodes are not in direct range then by using intermediate nodes communication is possible.
- *Predictable mobility:* In MANET mobility and topology is unpredictable, nodes can move in random direction. But in case of VANET vehicles moves on roads that are predefined, signs are used, traffic lights are used and also speed limits on road. So in this mobility and topology can be predictable.
- *Unlimited power and storage capacity:* In MANET power and storage capacity is limited but in case of VANET power is unlimited it also deal with storage capacity.
- *Delay sensitive:* VANET provide safety based services on road which are very delay sensitive like warning message at intersection point delay in that type of message can danger someone life.
- *Dynamic topology:* Vehicles travel on roads with very high speed due to which link between then will break very frequently and topology also change which is challenging to predict during routing.
- *Localization:* Location of nods can be accurately identified by using GPS which can be used during routing.

1.3 Security in VANET:

Due to mobile nature of the network the main issue arises is of security. As Security plays important role in the network for secure communication. It includes the threats to Availability, Authentication and Confidentiality.

- ➢ Threats to Availability
    - Denial of services (DOS) attack.
    - Broadcast Tampering.
    - Malware.
    - Black Hole Attack.
- ➢ Threats to Authentication
    - Masquerading.

    - Replay Attack.
    - Position Faking.
    - Sybil Attack.
- Threats to Confidentiality
    - Confidentiality of message exchanged between the nodes of a vehicular network. It considers gathering of Location information available through the transmission of broadcasted message. Location Privacy is the main issue for the vehicle users.

1.4 Architecture of VANET

A VANET uses cars as mobile nodes in a MANET to create a mobile network. All the participating cars are turn into a wireless router or node, allowing cars in the range of approximately 100 to 500 meters of each other to connect and, in turn, create a network with a wide range. The cars are moving in high speeds. As cars fall out of the signal range and drop out of the network, other cars coming inside the specified range can join in, connecting vehicles to one another so that a mobile vehicular network is created. The vehicles are equipped with advanced wireless communication devices without any base stations. In VANET each vehicle takes on the role of sender, receiver, and router to broadcast information to the vehicular network or transportation agency, which then uses the information to ensure safe, free-flow of traffic.

The main components of VANET:

On Board Units (OBUs): These are the communication devices mounted on vehicles to facilitate communication with other vehicles and roadside units. They enable short-range wireless ad hoc networks to be formed.

Roadside Units (RSUs): These are the communication units located aside the road that connects with the application server and the trust authority. They facilitate communication. The number and distribution of RSUs depends on the communication protocol to be used. Some protocols requires RSUs to be distributed evenly throughout the whole road network, some requires RSUs only at intersections, while others require RSUs only at region borders.

Trusted Authority (TA): They are third party entrusted with the job of certificate generation, distribution and revocation.

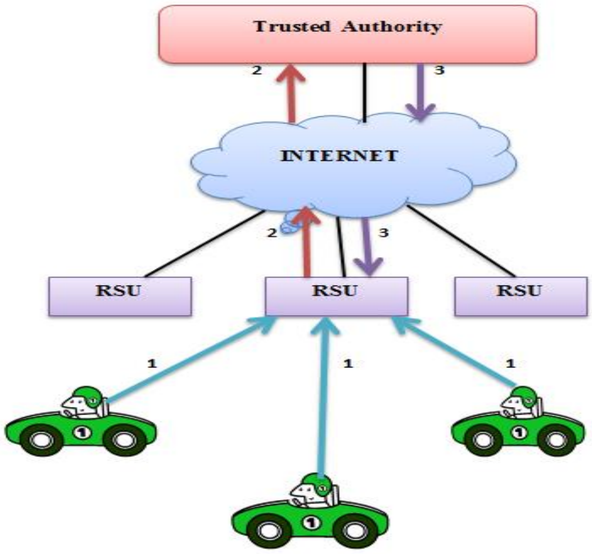


Fig 1.7: VANETs Architecture

1. Vehicle request RSU to issue certificate.
2. RSU forward to TA.
3. TA sends certificate to RSU.

VANETs Principle:

(i) A router called as Road Side Unit (RSU), where it connects the vehicular on the road with other network devices (base station).

(ii) Each vehicle has On Board Unit (OBU), where it connects the vehicle with RSU via DSRC radio.

(iii) Each vehicle has Temper Proof Devices (TPD), where it holds vehicle secrets such as driver's identity, speed, acceleration, route etc.

1.5 Standards for wireless access in VANETs

Standards that have been specified for implementing VANET in a reliable way are DSRC and WAVE. These standards range from protocols that apply to Transponder equipment and communication protocols through security specification, routing, addressing services, and interoperability protocols.

1.5.1 Dedicated Short Range Communication (DSRC):

DSRC is a one way or two ways short-range to medium-range wireless communication service that was developed to support IVC and VRC. DSRC was specially design for automotive use with an objective of providing high data transfers and low communication latency. In 1999, the United States Federal Communication Commission (FCC) allocated 75 MHz of spectrum at 5.9 MHz to be used by DSRC. In 2003, The American Society for Testing and Materials (ASTM) approved the ASTM-DSRC standard which was based n the IEEE 802.11a physical layer and 802.11 MAC layer. The DSRC spectrum is organized into 7 channels each of 10 MHz wide. One of the channels is restricted for safety communications only. Two channels are reserved for special purposes. The remaining 4 channels are service channel which can be utilized for safety and non-safety applications. Safety applications have higher priority over non-safety applications.

1.5.2 IEEE 1609-standards for wireless access in vehicular environments (WAVE) (IEEE 802.11p):

This is an enhancement to IEEE 802.11 to support intelligent transportation system application. WAVE defines two types of devices used in VANET viz. RSUs and OBUs. RSUs stationary devices while OBUs are mobile devices. Both RSU and OBU can be either a provider or a user of services and can switch between such nodes. In general RSU host an application that provides a service and the OBU hosts a peer application that uses this service.

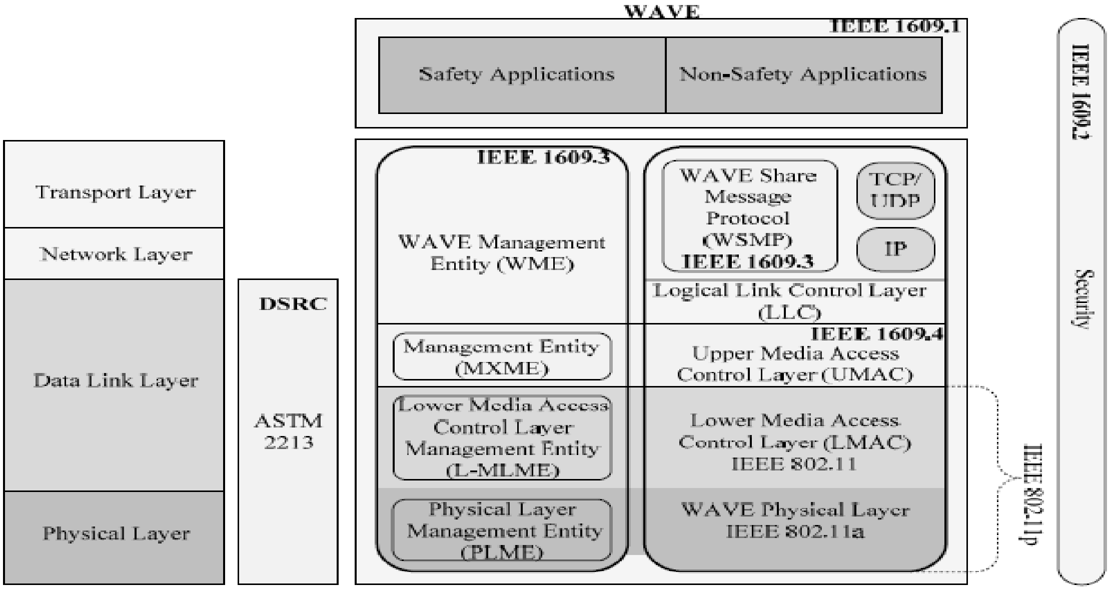

WAVE
IEEE 1609.1
Safety Applications
Non-Safety Applications
IEEE 1609.2
Security
Transport Layer
Network Layer
Data Link Layer
Physical Layer
DSRC
ASTM 2213
IEEE 1609.3
WAVE Management Entity (WME)
WAVE Share Message Protocol (WSMP) IEEE 1609.3
TCP/UDP
IP
Logical Link Control Layer (LLC)
IEEE 1609.4
Management Entity (MXME)
Upper Media Access Control Layer (UMAC)
Lower Media Access Control Layer Management Entity (L-MLME)
Lower Media Access Control Layer (LMAC) IEEE 802.11
Physical Layer Management Entity (PLME)
WAVE Physical Layer IEEE 802.11a
IEEE 802.11p

Fig 1.8: Wireless access in vehicular environments (WAVE) IEEE 1609, IEEE 802.11p and the OSI reference model

1.6 Applications of VANET

For describing VANET there are some common applications of VANET that benefits from them. Two applications categories where VANET plays crucial role are:

➢ Safety Related Application

Safety related applications as the name suggests are used to provide safety on the road. These applications are further divided into parts.

- ***Collision Avoidance:*** More than 60% of accidents on the road will be avoided if they get warning message before they collide with each other. If the car or vehicle driver gets warning at right time then the collision can be avoided.
- ***Cooperative driving:*** Drivers get messages for traffic related warnings such as lane changing or curve speed warning etc. With the help of these signals it co-operates the driver for the safe driving.

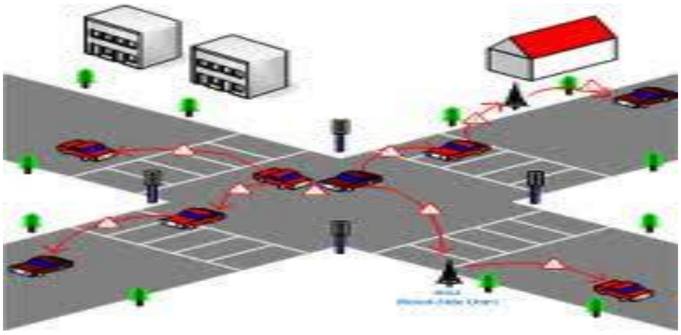


Fig 1.9: Cooperative Driving

- ***Traffic Optimization:*** Traffic can be coordinated and controlled by sending signals like jamming, accidents etc. to the vehicles so that they can choose another path to save their time.

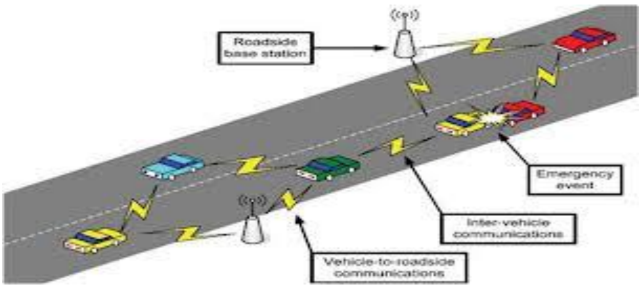

Roadside base station
Emergency event
Inter-vehicle communications
Vehicle-to-roadside communications

Fig 1.10: Traffic Optimization

- **User Based Application:** These kinds of applications provide comfort to the users apart from safety. Further these can be classified into the following:
  - ***Peer to peer application:*** In peer to peer application it provides the facilities like sharing music and movies among the vehicles in the network. Vehicles can share information related their entertainment also such as videos, audios etc.

5
Detect, Verify and Respond
Transguide Operations Center (TOC)
Typical Ramp Variable Message Sign (VMS)
2 Min. or Less
15 Seconds or Less
Loop Detectors
Access Road
Traffic Slows
1
Incident Occurs
2
Traffic Surveillance Camera
Typical Freeway Variable Message Sign & Lane Control Signals (LCS)
4
Traffic Warned to Route Around Incident

Fig 1.11: Peer to Peer Communication

  - ***Internet Connectivity:*** Now a day's people always want to connect to internet all the time. Hence VANET provides internet connectivity constantly without any interruption to the users.

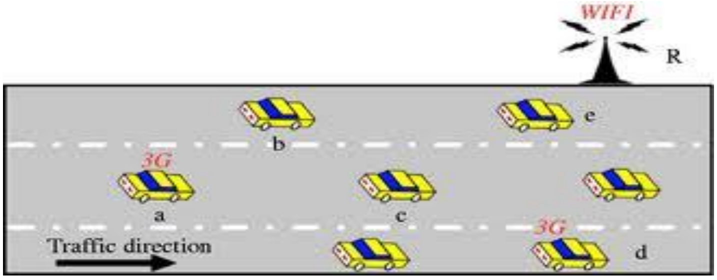


Fig 1.12: Internet Facility

  - ***Other Services:*** VANET provides number of uses/applications to its vehicles within the network. Other services it provides are like payment services to collect all taxes, locate vehicles to fuel station, restaurant or police station or to the fire station.

1.7 Difference between MANET and VANET

VANET and MANET share some common characteristics like: both can deploy without infrastructure, no central administration for controlling, nodes act as source, destination and intermediate nodes act as router to forward the data packet. But there are some differences in both networks.

- Topology in VANET is predictable as compare to MANET. Because in MANET mobile nodes move in random direction but in VANET vehicles are move on roads which are predefine.
- In MANET limited battery power and storage capacity, that limitations are not present VANET. In VANET sufficient battery power and storage capacity.
- In VANET mobility is high as compare to MANET. Vehicles move in faster speed as compare to mobile nodes. Due to which link failure is more in VANET.

1.8 DOS and DDOS Attacks in VANET

❖ **DOS Attack:** DOS (Denial of Service) attack is used to prevent the legitimate user to access resources provided in the network. This kind of attack occurs by jamming the channel so no authenticate user will access it. So the vehicle affected from that attack will be no more able to communicate with the other vehicles in the network. There are two alternative ways by which attacker do this attack:

i. It makes the node so busy or overwhelms the node so that it is not able to do anything else. As the node does not perform other necessary tasks as it is affected so the node becomes continuously busy. This is the basic level.

ii. In the extended level it does the channel jamming by generating high frequency as a result of it vehicle cannot communicate with each other.

- ***DOS Attack in V-V Communication:*** As in vehicle to vehicle communication there is only one attacker who is performing attack on the victim. It is the basic level in which it overwhelms the node or the vehicle such that it is not able to perform other necessary tasks as it becomes busy.

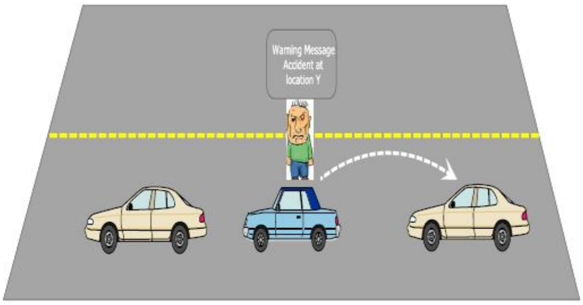


Fig 1.13: DOS attack in V-V [7]

- ***DOS Attack in V-I Communication:*** In vehicular to infrastructure the communication is done via RSU. The attacker continuously sends messages to RSU as a result of it RSU overloaded and it cannot provide services to the vehicles also called channel jamming.

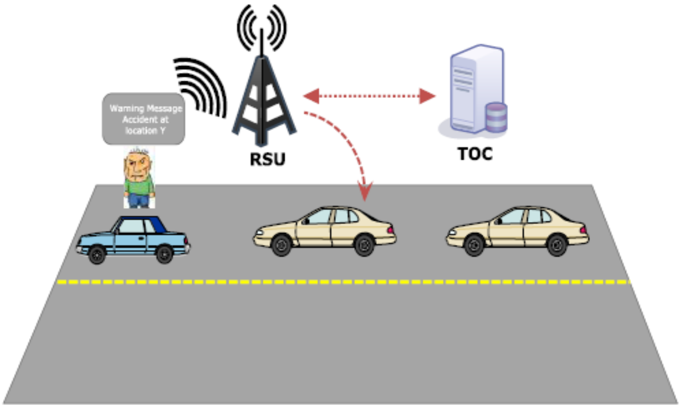


Fig 1.14: DOS attack in V-I [7]

❖ DDOS Attack in VANET

DOS attack causes DDOS (Distributed Denial of Services Attack). This attack takes place in distributed manner. There are number of attackers in the network that attacks from different locations with different timing slots. It is dangerous than the dos attack as in the dos there is only one attacker which can be easily identified but in DDOS attack there are number of attacker in the network.

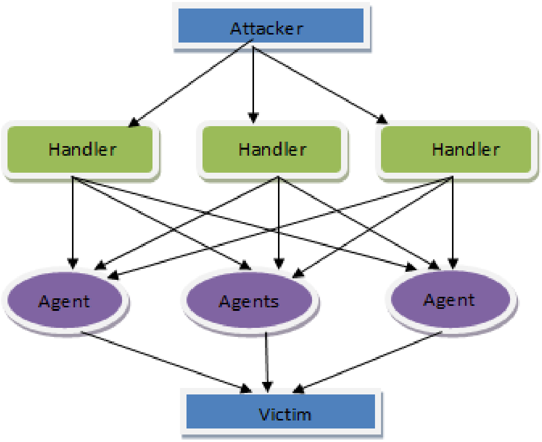


Fig 1.15: DDOS Attack Architecture

- ***DDOS Attack in V-V Communication:*** This kind of attack launches from different locations and at different time. These vary from node to node of the attacker. The main aim of the attacker is to provide inaccessibility to the users. In the figure number of attackers sends messages to the victim and it becomes busy and not able to communicate with others.

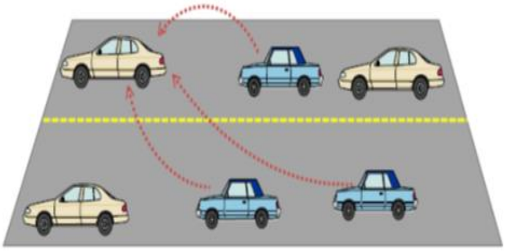


Fig 1.16: DDOS in V-V [7]

- ***DDOS Attack in V-I communication:*** In the vehicular to infrastructure n number of attackers sends false messages to the RSU (Road Side Units) from different locations such that the RSU becomes overloaded and the other vehicles that want service from RSU are not able to access it as it is overloaded.

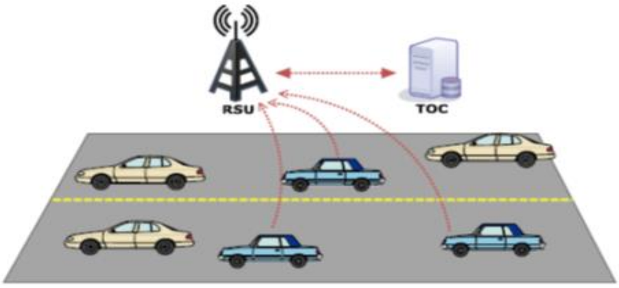


Fig 1.17: DDOS in V-I [7]

CHAPTER 2
REVIEW OF LITERATURE

(Minda Xiang, 2011) Proposed method of protection nodes to remove the effect of DOS or DDOS attacks in Mobile ad hoc network. They describe the strategy of protection nodes to protect the network from DDOS attack. Hierarchical network architecture is adopted to divide the nodes into multiple levels. Low level nodes used to protect the higher level nodes and lower level nodes are protected by the same level neighbor nodes. The node they chose to protect the high level node is Local Protection Node (LPN). When an attack route is built by the attacker, the very first hop or node from the source is selected as the protection node sometimes called as Remote Protection Node (RPN). RPN filters the false or rough packets at the source side coming from the source node and a message called ANM (Attack Notification Message) is broadcasted into the network to inform all other nodes about the malicious node. Thus every node in the network drops the packet coming from the malicious node. So this technique efficiently reduces the effect of DDOS attack from the network.

(A.Anna lakshmi, 2012) Discuss various techniques to defend against DDOS attack in MANTEs. Statistical filtering defense mechanism, it uses the hierarchical based filtering for the grouping of clusters. A cluster head is selected for each cluster to check filtering and routing. The other method they have described is flow monitoring table (FMT), which consist of flow id, source id and destination id. With each flow updated FMT is sent to destination node, if any variation is noticed in FMT, ECN (explicit congestion notification) bit is sent to the sender. Other method they have defined is protection node based strategy. By using hierarchical network architecture they divide the node into multiple levels. Lower level nodes used to protect higher level nodes. LPN (local protection node) is used to detect attack in the network. Other approach they have used is of AODV protocol. Mostly detection and protection from any attack is done by using this protocol.

(Al-Kahtani, 2012) Describes the security mechanisms to authenticate and validate message transmission and approaches to defend against the attacks occurred in the network. This paper gives a number of security and privacy schemes. Few of them are the Public Key Approach

(PKI), Symmetric and Hybrid Approaches. For the Prevention of DDOS attack it has defined a Certificate Revocation Technique (CRT). One part of PKI approach is CRT. Certified Revocation is done by the CA (Certified Authority) by two ways: Centralized and Decentralized. RSU sends the CRL (Certificate Revocation List) to the OBU (On Board Unit) .When the certificate is detected as invalid, CA sends messages to RSU which sends messages to all vehicles to revoke that particular certificate and stop the communication with it.

(V.Priyadharshini, 2012) Introduces a new cracking algorithm preventing DDOs attack in the network. Technology used for it is MAC. It maintains a status table that keeps the IP address of the users and their status. The algorithm consists of three parts: (i) Packet Filter: It works by inspecting the packets which transfers between computers on the internet. (ii) MAC Generator: It distinguishes the packet that contains the genuine source IP address from those who contains fake address. (iii) IP Handler: When the attacker uses genuine address the proxy server uses the deflect Round robin technique to collect the address from the client side. It also takes in account that if the user is sign in address for the first time then it is genuine user. If it is for two or more times than it is considered as normal user. If the user signed in for five or more than five times then it is considered as Attacker.

(Aditya Sinha P. K., 2013) This paper mainly stressed on the part of availability. Availability of the network is must needed when the nodes have to sends any information to other nodes. It is expected that security attacks will be increased in future because of more and more wireless application being developed. So in this regard, availability of network is exposed to many types of attack. It has defines DOS and DDOS attacks in the consideration of availability if network and also defines the possible solutions to overcome from these attacks. In DOS attack usually the attacker attacks the communication medium to cause the channel jamming and overwhelming of the network. There is only one attacker and one victim. The models they have defined depend on the OBU (On Board Unit) that is installed on each vehicle for making decision to block DOS attack. It has suggested the Switching technology, channel or to use frequency hopping technique. In DDOS attack: These types of attacks are very dangerous in the vehicular environment because the attacker attacks the victim in a distributed fashion. The attacker takes control over the other nodes in the network and launches the attack from different locations and in different timing slots. Suggested solution is the EDCA (Enhanced Distributed Channel Access) mechanism such as randomizing the RSU schedule, increasing the Contention Window and Randomization with Increasing the Contention Window.

(Ayonija Pathre, 2013) Defines the novel traffic congestion detection and removal scheme for DDOS attack. It defines the misbehavior of DDOS attack and the RSU mechanism for detection and removal purpose. The number of vehicles that receives the false packet is affected from the attack called as abstract node. The main aim of DDOS attack is to prevent legitimate access to any resource. So it provides RSU mechanism for prevention from this type of attack. RSU monitors the communication between the vehicles. It identifies the vehicle or the attacker vehicle that injects the false information packet into the network and then it blocks the activity of the attacker node and manages the traffic schedule affected by the attacker.

(TamilSelvan, 2013) As VANET is the class of MANET which uses cars as mobile nodes within the network. Applications like geographical location determination and online payment services etc. in VANET improves the driving safety, comfort to the passenger and attract more attention in your life. Security is the main issue in VANET. Various vulnerable attacks are DDOS attack, ID disclosure, Warm hole attack, Sinkhole attack etc. The existing solution to these types of attacks is that security should be provided only to the unauthorized users only not to authorized users. In this paper it has proposed a light weight holistic protocol to secure VANET from insider and outsider attack. The main problems in their existing detection mechanism are as it uses heavy weight protocol, time consumption will be more, If more users will connected to RSU at the same time then the overload will be more. When it uses the holistic protocol for secure data transmission in VANET then the advantages of using this are it uses light weight protocol, time consumption will be less.

(Ram Shringar Raw, 2013) It describes the security challenges with their possible solutions. In this paper replay attack, DOS attack, Routing attack etc. are defined along with their solutions. SEAD is used to remove the effect of DOS attack using one way Hash function which covers the security requirement of availability and authentication. Other approach they have defines is ARIADNE used to prevent DDOS attack using the symmetric cryptography technology. It also removes the effect of routing attack.

(Subir Biswas, 2013) It uses EDCA and DSRC mechanism. As DSRC consist of seven channels one is CCH (Control Channel) and six SCH (Secure Channel). CCH is used for transmitting short, system control and safety applications messages. SCH is usually picked for ordinary data communications. In the EDCA mechanism, it checks when the medium is idle, before transmitting the data frame, a station waits for AIFSk (Arbitration Inter-Frame Space where AIFSk is determined by the priority class k. If the medium is busy during AIFSk period, the sender needs to wait for the end of busy period. When there is a frame to broadcast then the sender selects a random number between 0 and CWmin and count downs every time slot while medium is idle. This paper also describes the attack model in which it calculates the jitter by using some mathematical concept.

(P., 2013) They describe the defense mechanisms against the various types of attacks and the radio DSRC (Dedicated short range communication) for the communication purpose. A secure authentication method is uses a unique identification for vehicles concatenated with some large random value to prevent Brute force attack and Hash algorithm is proposed to it. To deal with the Traffic analysis attack VIPER (Vehicle to infrastructure communication privacy enforcement protocol) is proposed. A novel solution is introduced to detect Sybil attack. DOS attack solution is based on the use of On Board Unit (OBU) which is installed in the vehicles. It defines the frequency hopping technique or switch channel technology by using OBU. Position attacks can be prevented by the Autonomous Position Verification method.

(**Shweta Tripathi, 2013**) Proposed a solution technique for prevention against DDOS attack. As Hadoop is an apache software foundation open source. It provides tools for processing vast amount of data using Map Reduce framework and implements the hadoop distributed file system. It gives two methods: (i) counter based method. It consists of three key parameters. Time interval which is the duration during which packets are to be analyzed. Threshold indicates the frequency of request. Unbalance ratio denotes the anomaly ratio of response per page request between client and server. (ii) Access Pattern Based Method: It differentiates the normal traffic from DDOS traffic. It consist of two Map Reduce jobs: 1st job get access sequence to web page between client and a web server and also computes the spending time and the bytes count for each request. 2nd job finds out the injected hosts by comparing the access sequence and the spending time among clients trying to access same server.

(C Balarengadural, 2013) FDPS based detection and prediction system), this technique is used to detect DDOS attack. Detection of this kind of attack is done on the basis of abnormal energy consumption by the sensor nodes. If any node is find out consuming abnormal energy then that node is considered as malicious one. An input is given to FLS (Fuzzy Logic System), after processing the input the LOA (Level of Acceptance) is derived as output. Prediction of DDOS attack is done by energy dissipation in which they have divided the operation into five states. By sensing all the five operating states of the sensor node they predict the attack by using chapman-Kolmogorov equation. A PAN coordinator is used to observe its neighboring sensor nodes in the network.

(Aditya Sinha P. S., 2014) Work done in this paper is about QLA (queue limiting algorithm) for protection of VANET from DOS attack. For the protection purpose they have assigned a queue to each node. This purpose provides a limit to each node of receiving packets from other node and also the messages is divided by using DSRC (dedicated short range communication). If any node is sending large number of packets to the victim node them the queue will accept the limited number of messages only and other will be discarded.

CHAPTER 3
PRESENT WORK

3.1. Problem Formulation

VANET is a kind of network that provides consistent communication to the vehicles in some described range. The communication can be compromised. The adaptable nature of network brings problems related to traffic safety and security. In VANET, there are number of vehicles communicating with each other. Multiple vehicles known as attackers create attack on the victim from different location and at different time and the victim cannot access the resources in the network. So these kinds of attacks known as DDoS attack are harder to detect. This study focuses on studying and analyzing various detection schemes in VANET. A methodology is introduced for detection purpose that detects the evil nodes in the network responsible for the occurrence of DDoS attack. When DDoS attack triggered into the network usually PDR (Packet delivery ratio) reduces. After that LPN node will be selected that sends monitoring message to its adjacent vehicles. After monitoring the nearest vehicles the LPN node identifies the attacker. This study aims to analyze the performance of detection scheme for DDoS attack in VANET.

3.2 Objectives

1. To trigger DDOS attack in VANET.
2. Detection of DDOS attack in Vehicular ad hoc Networks.
3. Implementation of proposed algorithm.

3.3 Methodology

The first step consists of studying VANET, its applications and architecture. The next step defines the study of security in VANET. After getting brief introduction about DDOS attacks in VANET, next step discuss about the prevention of DDOS attack. After studying number of algorithms defending DDOS attack we draw the comparison chart of the all algorithms we studied. The main motive is to detect the DDOS attack in the network and also prevent it.

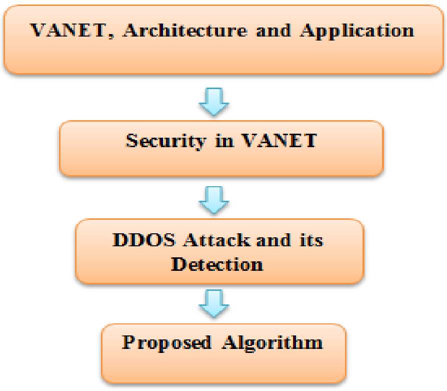

VANET, Architecture and Application
Security in VANET
DDOS Attack and its Detection
Proposed Algorithm

Fig 3.1: Research Methodology

Whenever the DDoS is triggered into the network; the PDR (Packet Delivery ratio) value is reduced. When the PDR value starts reducing, LPN node sends MM (monitor mode) message to all the adjacent vehicles in the network. The vehicles which receives MM message will start sensing their adjacent vehicles. The malicious vehicle which is flooding the network with rough packets will be detected.

Proposed Algorithm

The proposed algorithm is used to eliminate the effect of DDOS attack from the network. This algorithm uses the concept of protection node and further these nodes are divided into multiple levels according to their importance using hierarchical architecture. Whenever DDOS attack will be triggered by the malicious vehicle into the network, packet delivery ratio will be reduced.

Detection Algorithm:

```
Select LPN
  Vehicles send messages, compute PDR;
   When PDR decreases
     {
         LPN sends MM message to the vehicles, go to step 4
      }
    Else
     {
         Ignore
     }
   Vehicles receives MM message,
   Vehicle senses its adj V,
    If adj V flooding the rough packets into the network
     {
        Then it is malicious, go to step 7
     }
     Else
     {
         Ignore
      }
   Vehicle forward FPN to LPN.
   After receiving FPN, LPN filters all the malicious packet at source side and drop the drops the packet.
```

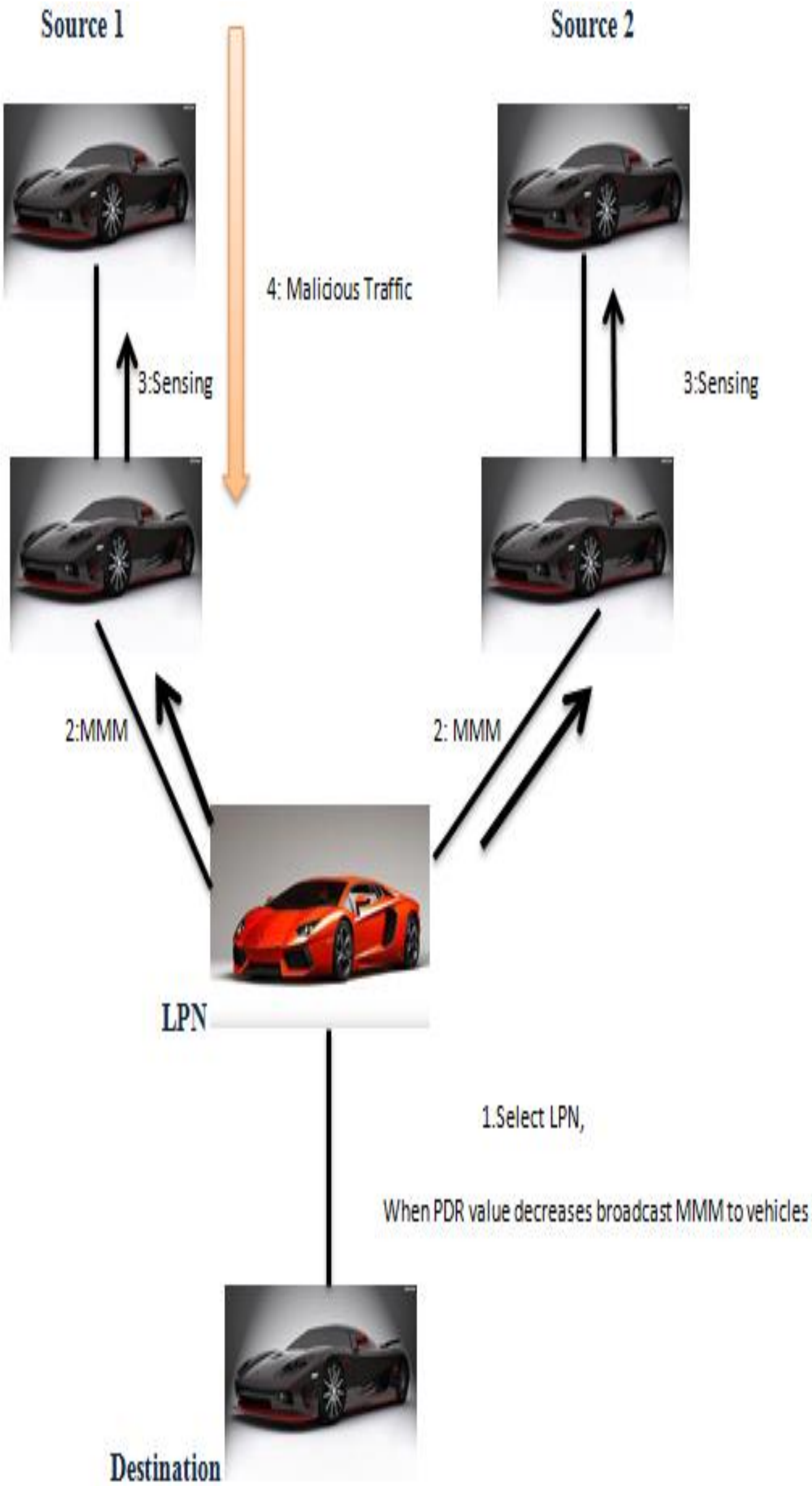
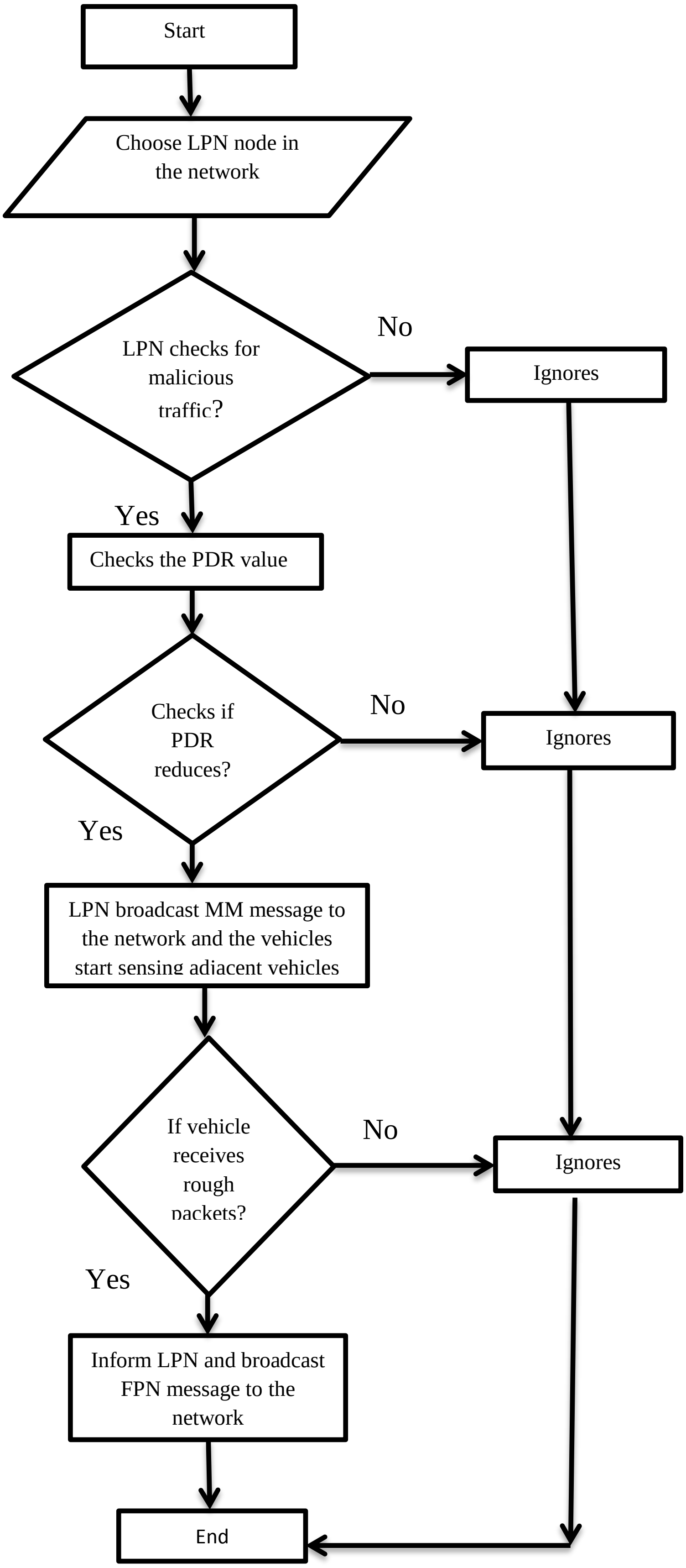


Fig 3.2: Process of defending DDoS Attack

3.4 The proposed algorithm basic functions as follows:



Start
Choose LPN node in the network
LPN checks for malicious traffic?
No
Ignores
Yes
Checks the PDR value
Checks if PDR reduces?
No
Ignores
Yes
LPN broadcast MM message to the network and the vehicles start sensing adiacent vehicles
If vehicle receives rough packets?
No
Ignores
Yes
Inform LPN and broadcast FPN message to the network
End

Fig 3.3: Flow Chart

3.5 TIMELINE

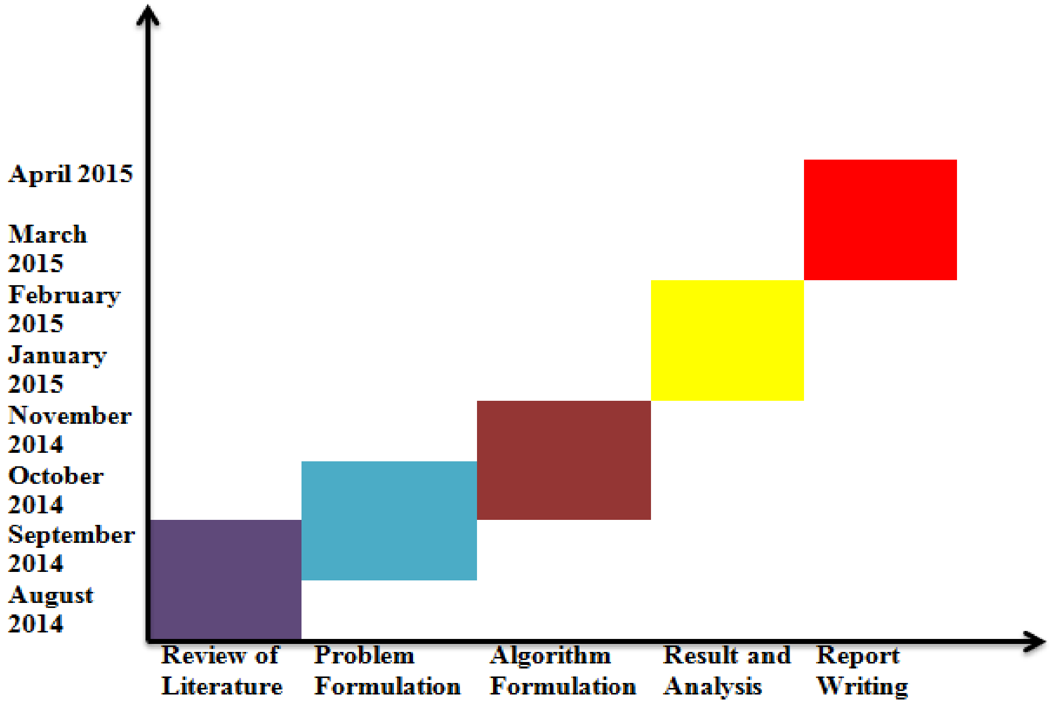


Fig 3.4: Timeline Graph

CHAPTER 4
RESULTS AND DISCUSSIONS

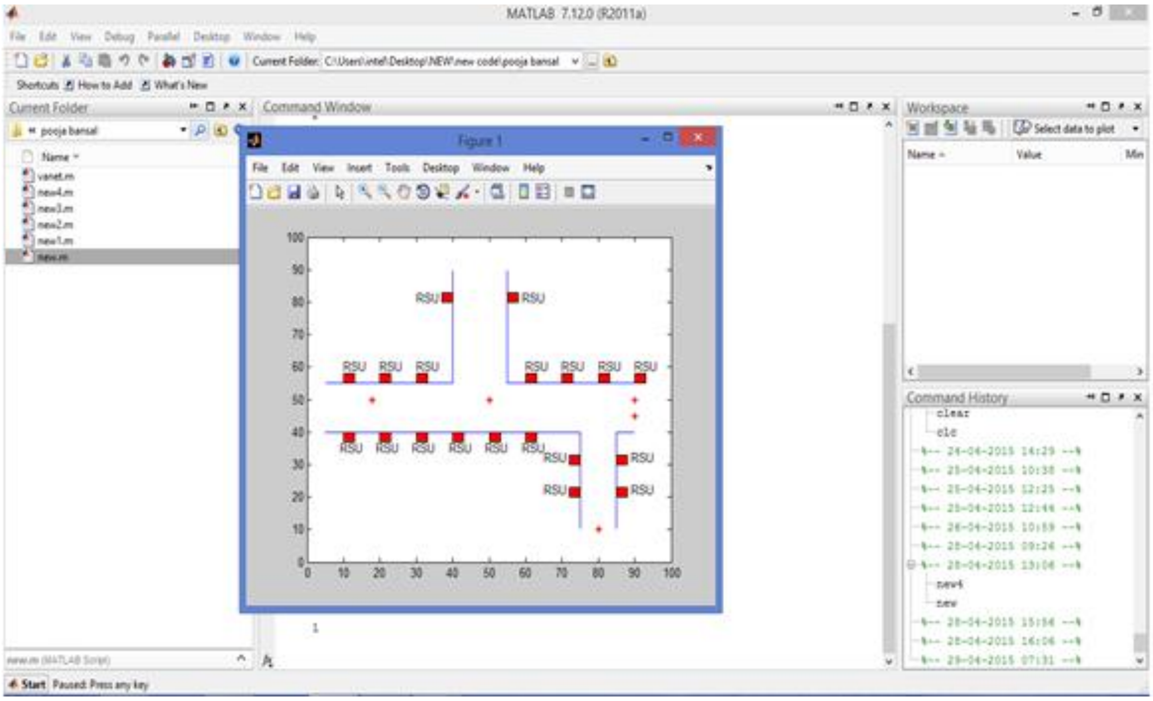
4.1 TOOL USED:

MATLAB

MATLAB (Matrix Laboratory), a tool used for matrix manipulations and also for plotting of data and functions. This tool is useful in implementation of algorithms. It is a 4th generation high level programming language developed by Math Works. It provides an interactive environment for numerical computation, visualization, iterative exploration, programming, application development, design and problem solving. MATLAB has a wide range of pre-defined library functions that help us to implement complex problem in simple way. It provides built in tools and graphics that help in creation of custom plots and visualization of data. Applications with graphical user interfaces can be built with the aid of various tools available in MATLAB. The programming interface of MATLAB provides development tools which improves code quality and performance. Algorithms implemented using MATLAB can be easily integrated with other external applications and languages such as C, JAVA etc. In the current scenario MATLAB has become one of the most used computational tools in science and engineering. MATLAB has a wide range of application such as implementing image and video processing, neural network, computational biology, mathematical computation, control system, vehicular network etc. MATLAB will be an ideal tool for implementing the proposed scheme.

4.2 Trigger DDoS attack into the Vehicular ad hoc Network (VANET)

(i) Vehicles enter into the network.



MATLAB 7.12.0 (R2011a)
File Edit View Debug Parallel Desktop Window Help
Shortcuts How to Add What's New
Current Folder
Command Window
Workspace
Select data to plot
Name Value Min
Command History
Figure 1
File Edit View Insert Tools Desktop Window Help
RSU
0 10 20 30 40 50 60 70 80 90 100
Start Paused: Press any key

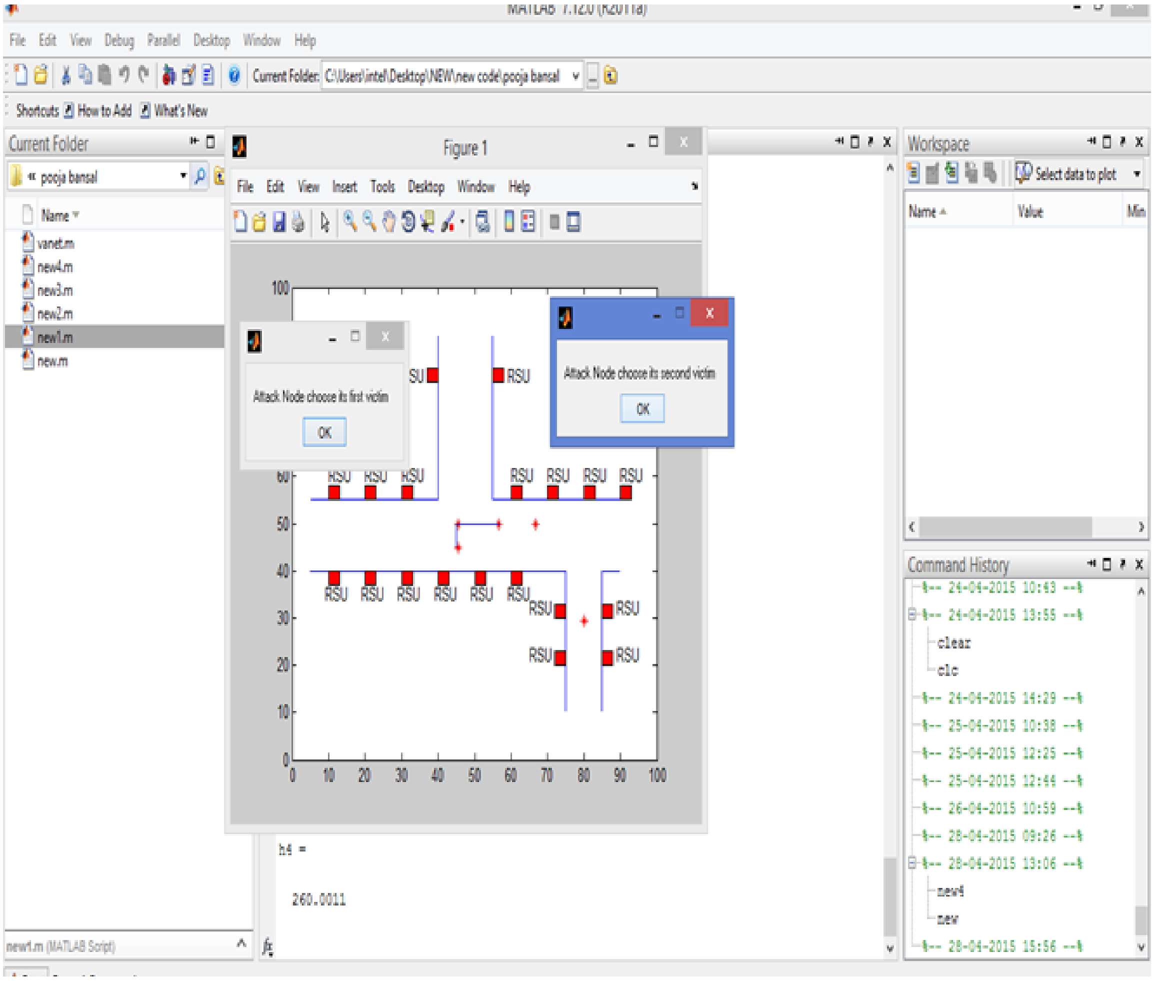
Current Folder: C:\Users\intel\Desktop\NEW\new code\pooja bansal

```
pooja bansal
Name
vanet.m
new4.m
new3.m
new2.m
new1.m
new.m
new.m (MATLAB Script)
```

```
clear
clc
%-- 24-04-2015 14:29 --%
%-- 25-04-2015 10:38 --%
%-- 25-04-2015 12:25 --%
%-- 25-04-2015 12:44 --%
%-- 26-04-2015 10:59 --%
%-- 28-04-2015 09:26 --%
%-- 28-04-2015 13:06 --%
new4
new
%-- 28-04-2015 15:54 --%
%-- 28-04-2015 16:06 --%
%-- 29-04-2015 07:31 --%
```

Fig 4.1: Initialization of Vehicles

(ii) Attacker chooses victims to trigger attack on the legitimate node.



Attack Node choose its first victim

OK

Attack Node choose its second victim

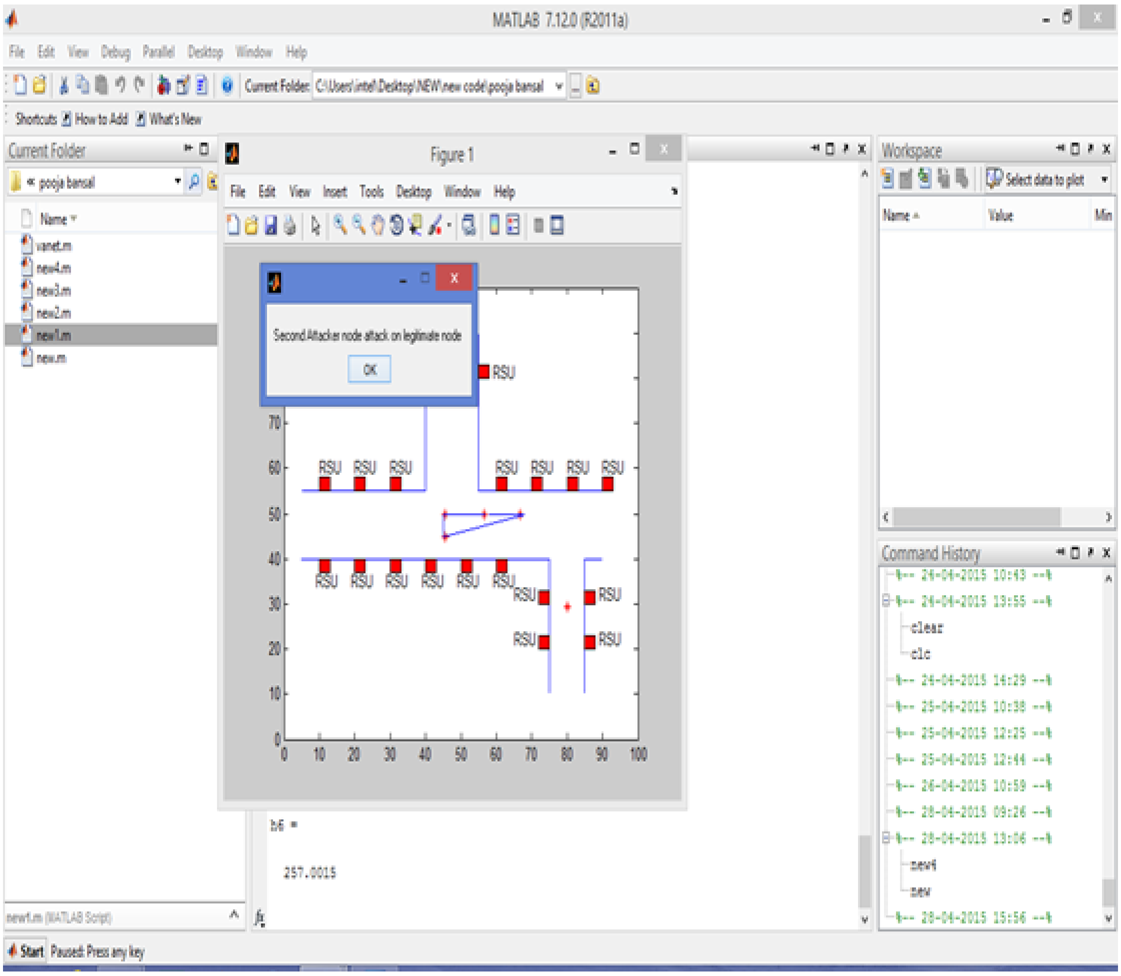
OK

```
h4 =

   260.0011
```

```
%-- 24-04-2015 10:43 --%
%-- 24-04-2015 13:55 --%
  clear
  clc
%-- 24-04-2015 14:29 --%
%-- 25-04-2015 10:38 --%
%-- 25-04-2015 12:25 --%
%-- 25-04-2015 12:44 --%
%-- 26-04-2015 10:59 --%
%-- 28-04-2015 09:26 --%
%-- 28-04-2015 13:06 --%
  new4
  new
%-- 28-04-2015 15:56 --%
```

Fig 4.2: Compromised Victims

(iii) Both the compromised vehicles start attacking the legitimate node.



Second Attacker node attack on legitimate node

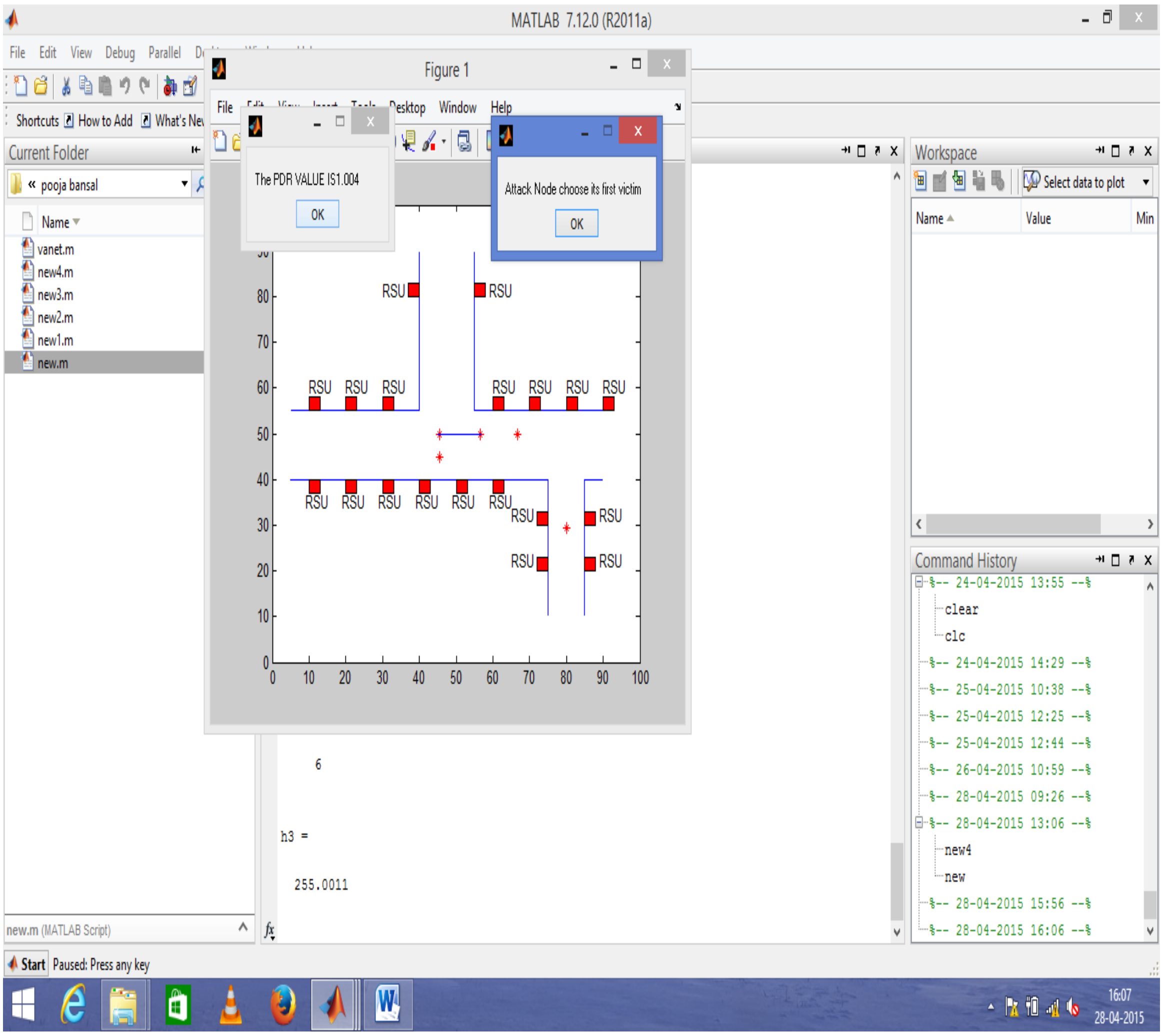
```
b6 =

  257.0015
```

```
%-- 24-04-2015 10:43 --%
%-- 24-04-2015 13:55 --%
  clear
  clc
%-- 24-04-2015 14:29 --%
%-- 25-04-2015 10:38 --%
%-- 25-04-2015 12:25 --%
%-- 25-04-2015 12:44 --%
%-- 26-04-2015 10:59 --%
%-- 28-04-2015 09:26 --%
%-- 28-04-2015 13:06 --%
  new4
  new
%-- 28-04-2015 15:56 --%
```

Fig 4.1: Both compromised nodes attacks the legitimate node

Here mainly the attacker is not doing anything. Attacker compromises the vehicle for attack purpose and then the compromised vehicles attack the legitimate node. In DDoS attack, there is one attacker and compromised nodes called agents. These agents are mainly responsible for the attack not the attacker.

(iv) When DDoS triggered into the network the PDR value reduces.



The PDR VALUE IS1.004

Attack Node choose its first victim

```
 6

h3 =

 255.0011
```

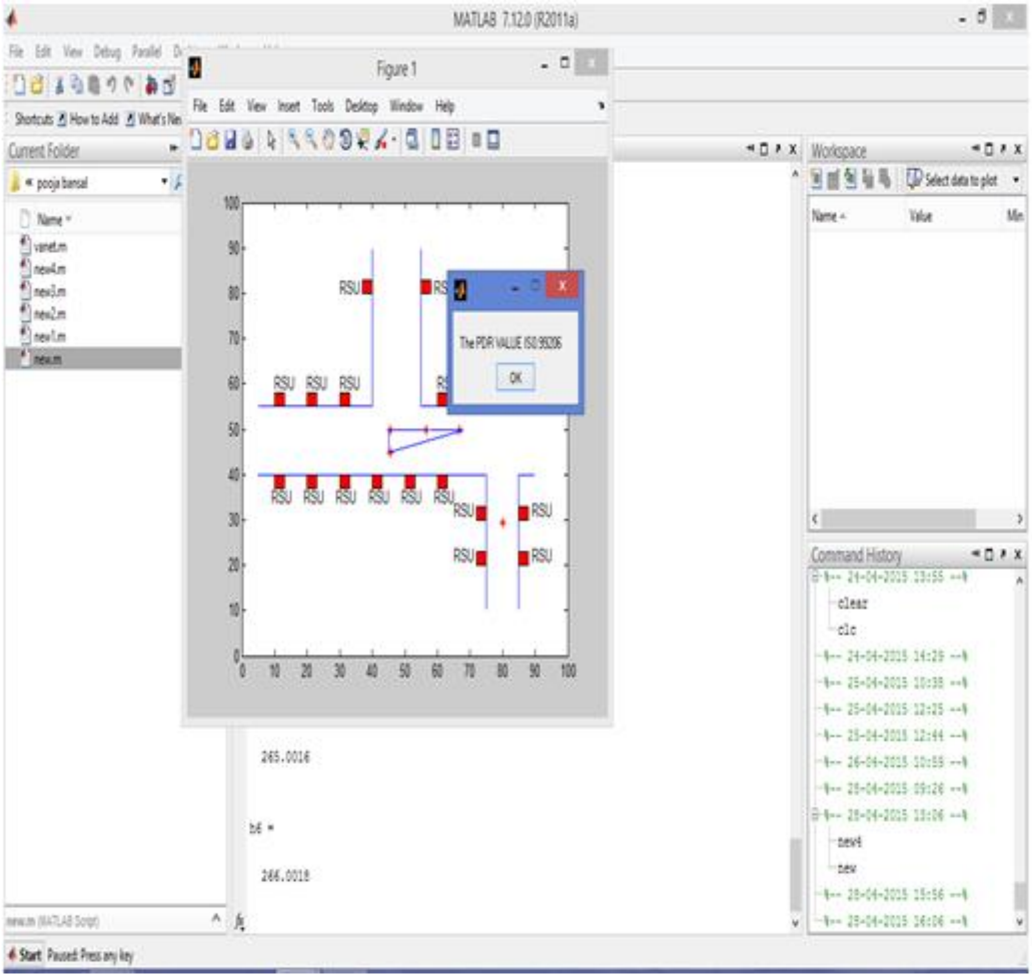
```
%-- 24-04-2015 13:55 --%
  clear
  clc
%-- 24-04-2015 14:29 --%
%-- 25-04-2015 10:38 --%
%-- 25-04-2015 12:25 --%
%-- 25-04-2015 12:44 --%
%-- 26-04-2015 10:59 --%
%-- 28-04-2015 09:26 --%
%-- 28-04-2015 13:06 --%
  new4
  new
%-- 28-04-2015 15:56 --%
%-- 28-04-2015 16:06 --%
```

Fig 4.4: Calculates PDR

In fig 4.2.3, when the attacker chooses its first victim the PDR (Packet Delivery Ratio) value is used to be calculated between these two vehicles. PDR value will be calculated by using this formula:

PDR= Number of messages received/ number of messages sent.

(v) When both the vehicles attack the legitimate node



The PDR VALUE IS0.99206

```
  245.0016

b6 =

  246.0018
```

```
%-- 24-04-2015 13:55 --%
  clear
  clc
%-- 24-04-2015 14:29 --%
%-- 25-04-2015 10:38 --%
%-- 25-04-2015 12:25 --%
%-- 25-04-2015 12:44 --%
%-- 26-04-2015 10:55 --%
%-- 28-04-2015 09:26 --%
%-- 28-04-2015 13:06 --%
  new4
  new
%-- 28-04-2015 15:56 --%
%-- 28-04-2015 16:06 --%
```

Fig 4.5: PDR reduces

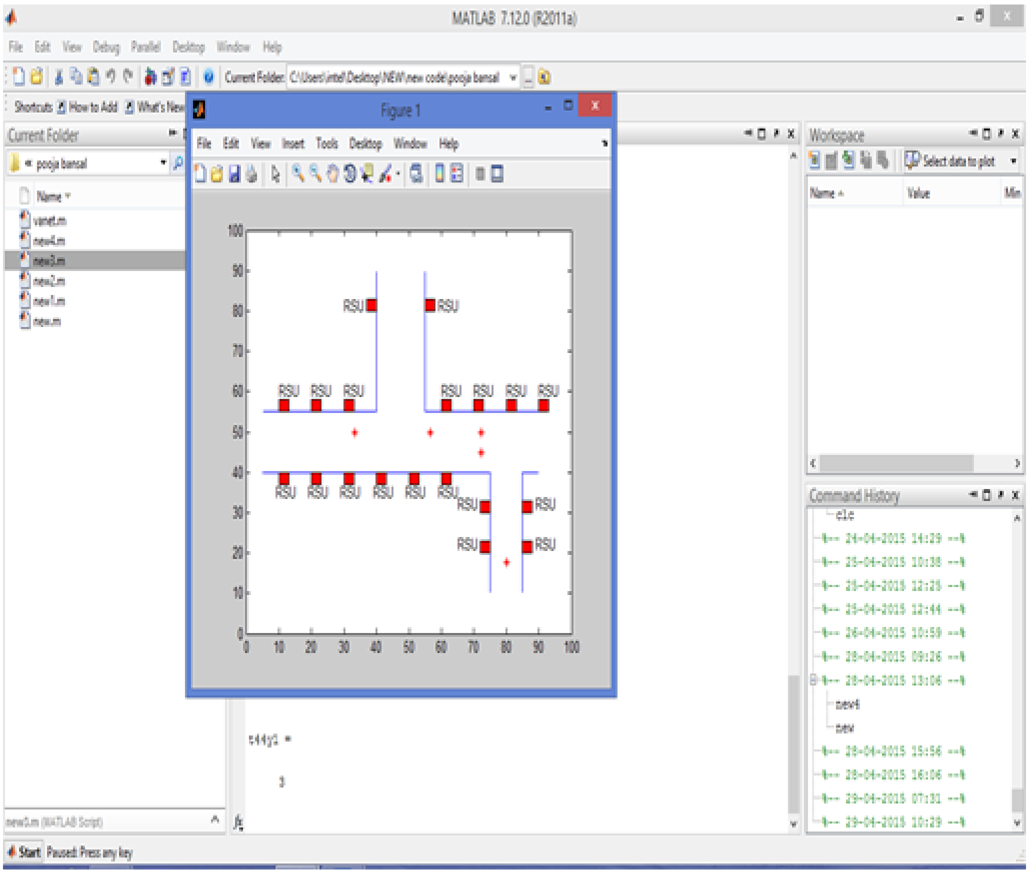
In this fig. When legitimate node gets affected by the attack i.e. it does not able to access the resources of the network the PDR value reduces which shows that DDoS attack is successfully taken place into the network.

Once the DDoS attack triggered into the network, the next step is to detect the kind of attack that has occurred into the network.

4.3 Detection Process

In the detection process first we choose a LPN (local protection node) then LPN calculates nearest neighbor using Euclidean distance and send monitor mode message to its neighbor. After receiving message the vehicle starts sensing its adjacent vehicles. If the packets send are greater than 5 then it is identified as attacker otherwise not.

In MATLAB the Detection process works as follows:

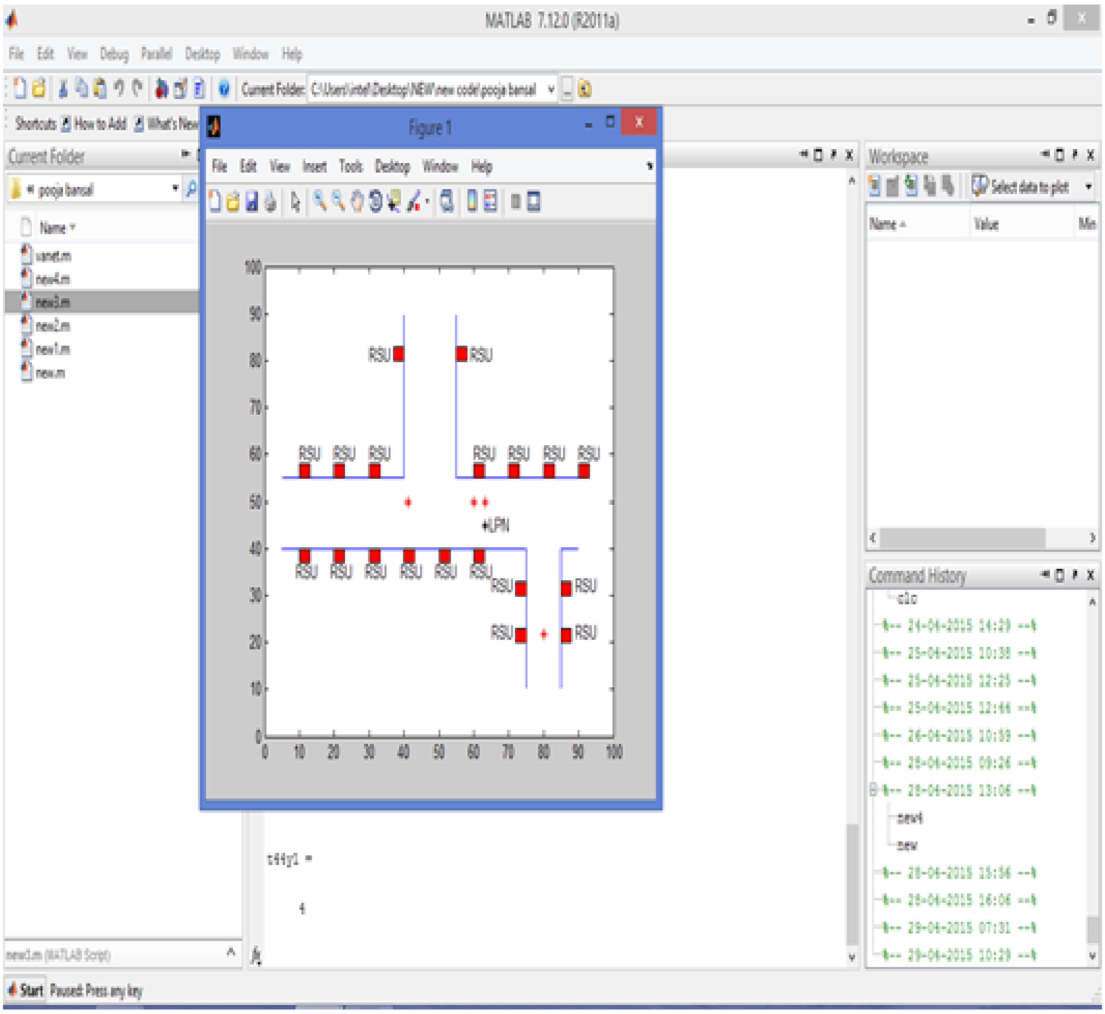


```
t44y1 =

     3
```

```
clc
%-- 24-04-2015 14:29 --%
%-- 25-04-2015 10:38 --%
%-- 25-04-2015 12:25 --%
%-- 25-04-2015 12:44 --%
%-- 26-04-2015 10:59 --%
%-- 28-04-2015 09:26 --%
%-- 28-04-2015 13:06 --%
new4
new
%-- 28-04-2015 15:56 --%
%-- 28-04-2015 16:06 --%
%-- 29-04-2015 07:31 --%
%-- 29-04-2015 10:29 --%
```

Fig. 4.7: Vehicles Initialization

Selection of LPN

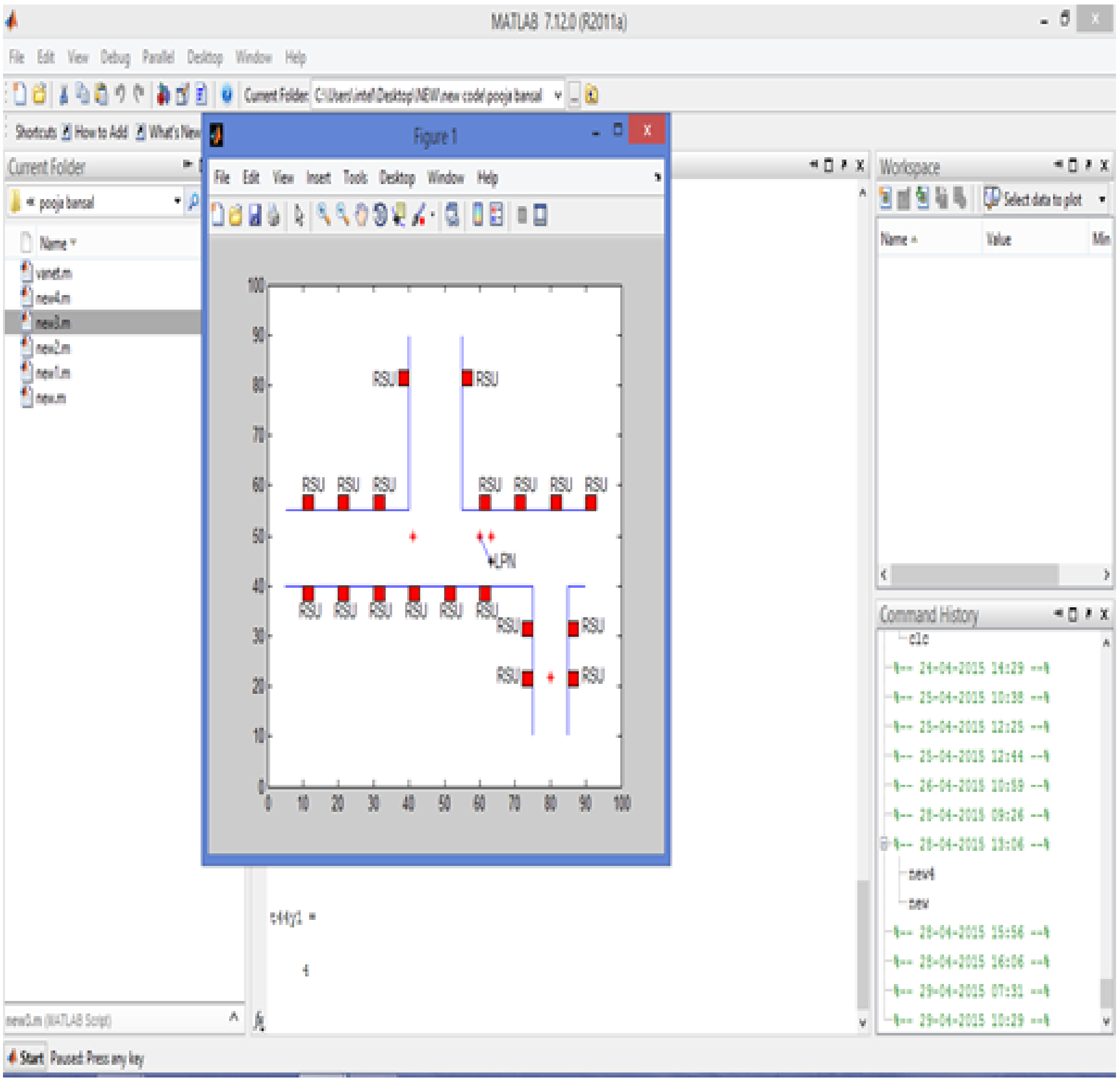


```
t44y1 =

     4
```

```
clc
%-- 24-04-2015 14:29 --%
%-- 25-04-2015 10:38 --%
%-- 25-04-2015 12:25 --%
%-- 25-04-2015 12:44 --%
%-- 26-04-2015 10:59 --%
%-- 28-04-2015 09:26 --%
%-- 28-04-2015 13:06 --%
new4
new
%-- 28-04-2015 15:56 --%
%-- 28-04-2015 16:06 --%
%-- 29-04-2015 07:31 --%
%-- 29-04-2015 10:29 --%
```

Fig. 4.8: LPN Selection

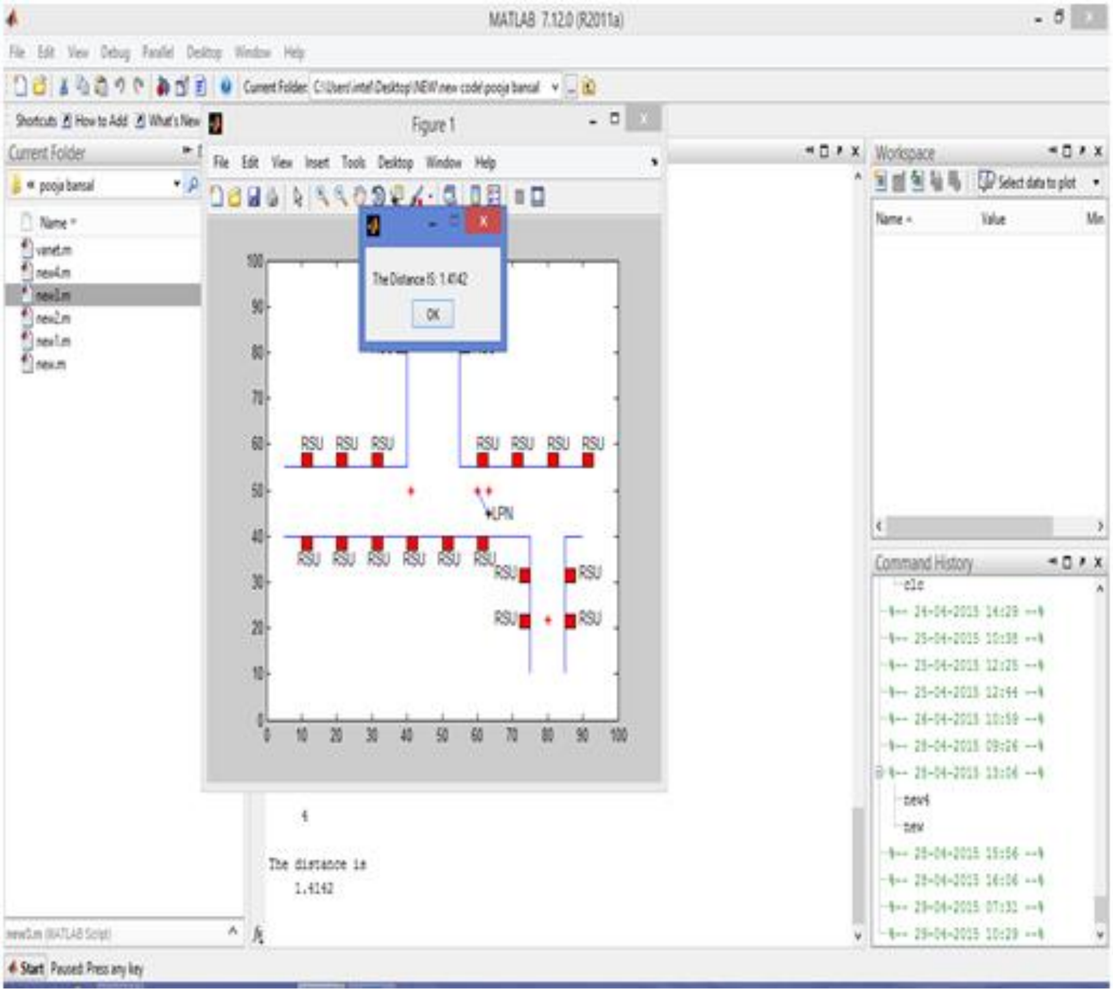
Choosing nearest neighbor using Euclidean distance



```
[illegible] =

     4
```

```
clc
%-- 24-04-2015 14:29 --%
%-- 25-04-2015 10:38 --%
%-- 25-04-2015 12:25 --%
%-- 25-04-2015 12:44 --%
%-- 26-04-2015 10:59 --%
%-- 28-04-2015 09:26 --%
%-- 28-04-2015 13:06 --%
new4
new
%-- 28-04-2015 15:56 --%
%-- 28-04-2015 16:06 --%
%-- 29-04-2015 07:31 --%
%-- 29-04-2015 10:29 --%
```

Fig. 4.9: Selection of nearest node



The Distance IS: 1.4142

```
     4

The distance is
    1.4142
```

```
clc
%-- 24-04-2015 14:29 --%
%-- 25-04-2015 10:38 --%
%-- 25-04-2015 12:25 --%
%-- 25-04-2015 12:44 --%
%-- 26-04-2015 10:59 --%
%-- 28-04-2015 09:26 --%
%-- 28-04-2015 13:04 --%
new4
new
%-- 28-04-2015 15:56 --%
%-- 28-04-2015 16:06 --%
%-- 29-04-2015 07:31 --%
%-- 29-04-2015 10:29 --%
```

Fig 4.10: Distance Calculation

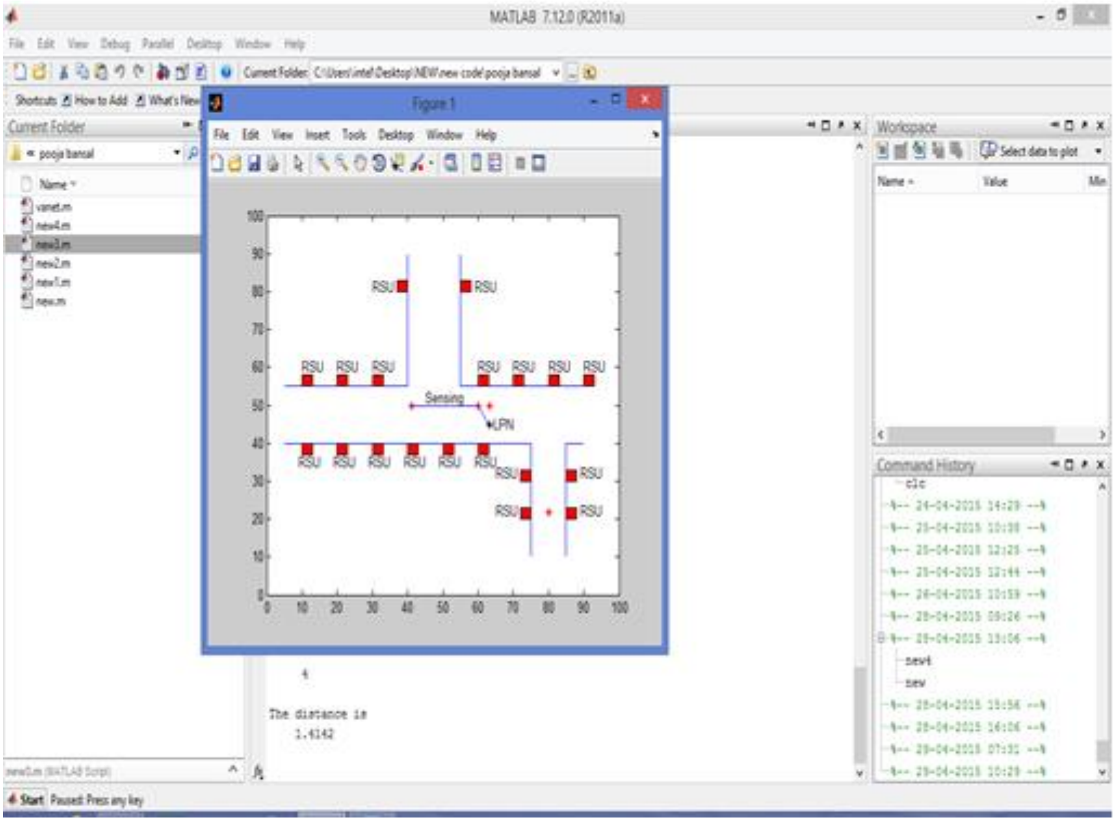
Euclidean distance formula is used to calculate the distance between two objects or two points.

P(X,Y) where X= x1,x2,x3...xn

Y= y1,y2,y3....yn

ED= sqrt((x1-y1)^2+ (x2-y2)^2+.....+(xn-yn)^2).

Attacker identification


MATLAB 7.12.0 (R2011a)
File Edit View Debug Parallel Desktop Window Help
Current Folder: C:\Users\intel\Desktop\NEW\new code\pooja bansal
Shortcuts How to Add What's New
Current Folder
pooja bansal
Name
vanet.m
new4.m
new3.m
new2.m
new1.m
new.m
new3.m (MATLAB Script)
Start Paused: Press any key
Figure 1
File Edit View Insert Tools Desktop Window Help
RSU
Sensing
LPN
0
10
20
30
40
50
60
70
80
90
100
Workspace
Select data to plot
Name
Value
Min
Command History

```
4

The distance is
   1.4142
```

```
clc
%-- 24-04-2015 14:29 --%
%-- 25-04-2015 10:38 --%
%-- 25-04-2015 12:25 --%
%-- 25-04-2015 12:44 --%
%-- 26-04-2015 10:59 --%
%-- 28-04-2015 09:26 --%
%-- 28-04-2015 13:06 --%
  newt
  new
%-- 28-04-2015 15:56 --%
%-- 28-04-2015 16:06 --%
%-- 29-04-2015 07:31 --%
%-- 29-04-2015 10:29 --%
```

Fig 4.11: Attacker Identification

The identification of attacker is based on sensing. When the nearest neighbor is selected it starts sensing its adjacent vehicles. Sensing is done on the basis of the following:

```
If rough packets >5
{
    Attacker identified.
}
Else
{
    Attacker not identified.
}
```

3.4 PERFORAMANCE EVALUATION

Table4.1: PDR variation

Scenario	Normal	Attack	Detection
PDR Value	1.004	0.9906	1.012

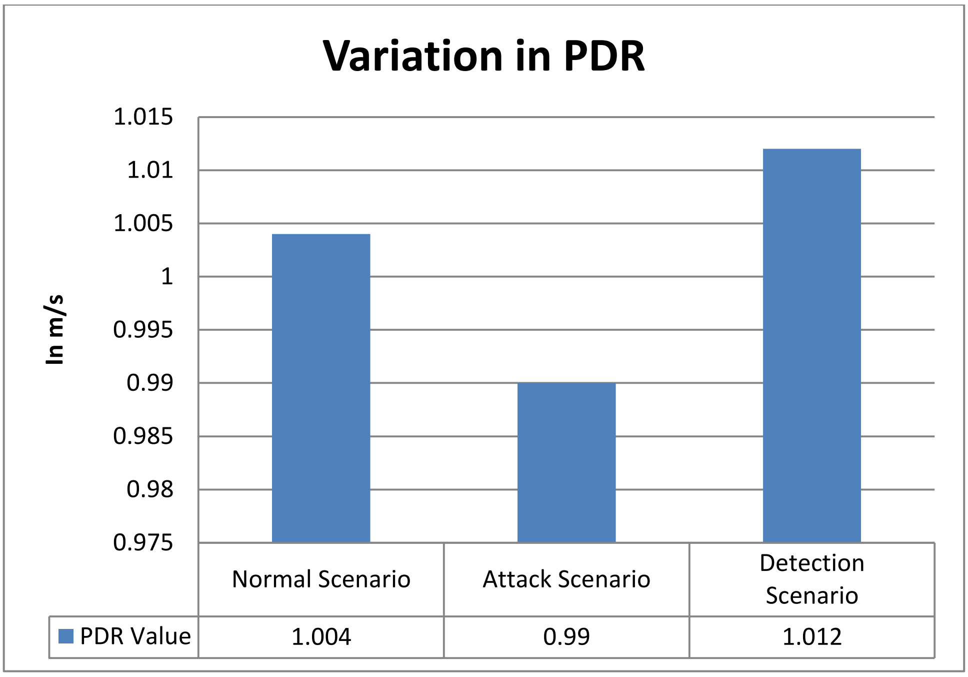


Fig 4.12: PDR Variation

In the given graph, it represents the variation in the PDR value. In the normal scenario when vehicles communicate with each other the value is normal but when the attack triggered into the network it affects the PDR value i.e. PDR reduces. After that when the detection scheme is applied PDR again increases.

.

Table 4.2: Delay variation

	Number of Nodes	Time in ms
Attack Scenario	4	0.265
	6	0.274
	9	0.283
Detection Scenario	**Number of Nodes**	**Time in ms**
	4	0.232
	6	0.225
	9	0.231

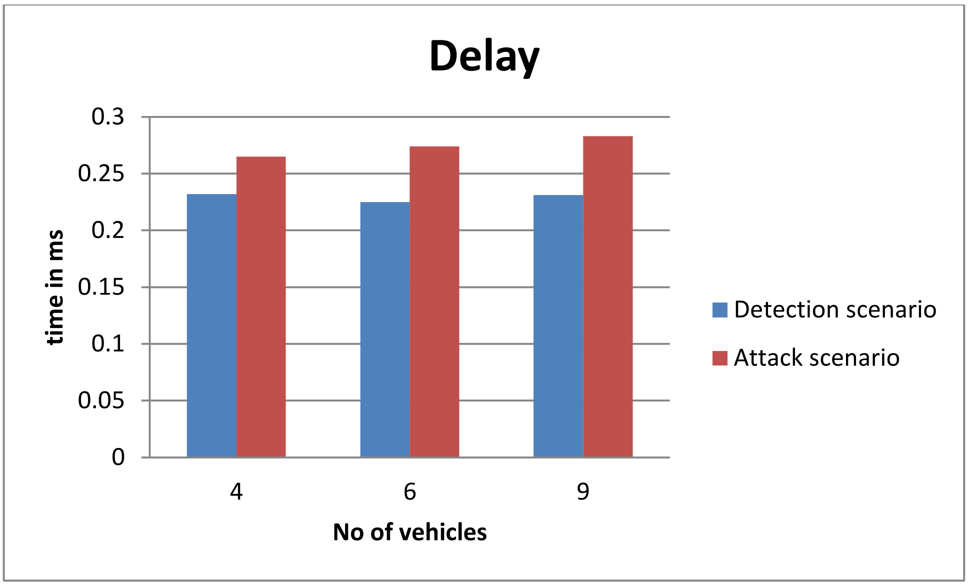


Fig 4.13: Delay Graph

The delay graph shows how much time each vehicle consumes while communication. In the attack scenario the vehicles communicates and thus their PDR value calculates. In the detection scenario it takes less time as Euclidean distance is applied to select nearest node. So the delay decreases.

.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

VANET (Vehicular Ad hoc Network) uses vehicles as mobile nodes for the communication purpose and for data sharing. In VANET network it converts every participating vehicle into a wireless router or node.VANET offers a wide range of applications that can come handy in our day to day life. Some application involves providing safety related information and sometimes critical information related to life and death. So the main issues in real time implementation of VANET is to provide secure communication channel between the users. Much kind of attacks are coming up into the network so it is necessary to get a solution to these. The proposed methodology focuses on the DDOS (detection of distributed denial of services) attack and thus provides protection to the network. MATLAB tool was used for the implementation of proposed algorithm. It provides an interactive environment for numerical computation, visualization, iterative exploration, and programming. The results were recorded and analyzed on the basis of PDR variation and delay and according to them graphs were plotted. In future we may focus on prevention of DDoS attack. As detection part is completed but there is no prevention mechanism applied for the DDoS attack.

CHAPTER 6
REFERENCES

A.Anna lakshmi, D. V. (2012). A Survey of Algorithms for Defending MANETs against the DDoS attack. *International Journal of Advanced Research in Computer Science and Software Engineering*, 155-163.

Aditya Sinha, P. K. (2013). Preventing VANET from DOS and DDOS Attack. *International Journal of Engineering Trends and Technology*, 4373-4376.

Aditya Sinha, P. S. (2014). QLA (Queue Limiting Algorithm) for protecting VANET from DOS(Denial of Service). *International journal of Computer Application* , 14-17.

Al-Kahtani, M. S. (2012). Survey on Security Attacks in Vehicular Ad hoc Networks(VANETs). *IEEE.*

Ayonija Pathre, C. A. (2013). A Novel defence Scheme against DDOS Attack in VANET. *IEEE.*

C Balarengadural, D. S. (2013). Fuzzy Based Detection and predction of DDOS attack in IEEE 802.15.4 low rate WPAN. *International Journal of Computer Science Issues*, 293-301.

Ch. Sudersan Raju, D. M. (July 2013). Adaptability of MANET Routing Protocols for VANETS. *International Journal of Advanced Research in Computer and Communication Engineering*, 7.

Chan-Ki Park, K.-H. C.-W.-H. (2013). Measuring the Performance of Packet size and Data rate for Vehicular Ad Hoc Networks. *IEEE*, 2.

Chetan aggarwal, A. J. (2013). Identification of malicious vehicle in VANET from DDOS attack. *Journal of Global Research in Computer Science*, 30-34.

M. Shahid Anwer, C. G. (September 2014). A Survey of VANET Technologies. *Journal of Emerging Trends in Computing and Information Sciences*, 11.

M.Raya. (2007). Securing Vehicular ad hoc networks. *Journal of Computer Security*, 39-68.

Minda Xiang, Y. C.-S. (2011). Mitigating DDoS Attacks using Protection Nodes in Mobile Ad Hoc Networks. *IEEE Global Communications Conference*, (pp. 1-6).

P., M. E. (2013). Threat Analysis and Defence Mechanism in VANET . *International Journal of Advances research in Computer Science and Software Engineering*, 47-53.

Ram Shringar Raw, M. K. (2013). Security Challenges, Issues and Their Solutions for VANET. *International Journal of Network Security and Its Applications*, 95-105.

Sherali Zeadally, R. H.-S. (2010). Vehicular ad hoc networks (VANETS): status,results, and challenges. *Springer*.

Shweta Tripathi, B. G. (2013). Hadoop Based Defence solution to handle DDOS Attacks. *Journal of Information Security*.

Subir Biswas, J. M. (2013). DDOS Attack on WAVE-enabled VANET through Synchronization. *IEEE.*

TamilSelvan, K. S. (2013). A Holistic Protocol for Secure Data Transmission in VANET. *International Journal of Advanced Research in Computer and Communication Engineering*, 4840-4846.

V.Priyadharshini, D. (2012). Prevention of DDOS Attacks using New Cracking Algorithm. *International Journal of Engineering Research And Applications*, 2263-2267.

YASSER TOOR AND PAUL MÜHLETHALER, I. A. (2008). VEHICLE AD HOC NETWORKS: APPLICATIONS AND RELATED TECHNICAL ISSUES. *IEEE*, 15.

Yeongkwun Kim, I. K. (2013). Security Issues in Vehicular Networks. *IEEE*, 5.

PUBLICATION

Paper presented in “FOURTH INTERNATIONAL CONFERENCE OF WIRELESS NETWORKS AND EMBEDDED SYSTEMS WECON-2015”.

CHAPTER 7

APPENDIX

List of Abbreviation

VANET	Vehicular Ad-Hoc Network
MANET	Mobile Ad-Hoc Network
OBU	On-Board Unit
RSU	Road-Side Unit
TA	Trusted Authority
TPD	Tamper Proof Device
DSRC	Dedicated Short Range Communication
LPN	Local Protection Node
RPN	Remote protection Node
MMM	Monitor Mode Message
FPN	Fake Packet Notification
DOS	Denial of Services
DDOS	Distributed Denial of Services
TV	Threshold Value
Adj v	Adjacent Vehicle
PDR	Packet Delivery Ratio

Glossary of Term

1. **PDR (packet delivery ratio):** It is the ratio of number of packets received to the number of number of packets sent.

PDR= no. of packets received/ no. of packets sent

2. **Euclidean distance:** This formula is used to calculate the distance between two objects or two points.

P(X,Y) where X= x1,x2,x3...xn

Y= y1,y2,y3....yn

ED= sqrt((x1-y1)^2+ (x2-y2)^2+.....+(xn-yn)^2).

3. **DOS:** DOS (Denial of Service) attack is used to prevent the legitimate user to access resources provided in the network. This kind of attack occurs by jamming the channel so no authenticate user will access it. So the vehicle affected from that attack will be no more able to communicate with the other vehicles in the network.

4. **DDOS:** DOS attack causes DDOS (Distributed Denial of Services Attack). This attack takes place in distributed manner. There are number of attackers in the network that attacks from different locations with different timing slots.

5. VANET: VANET (Vehicular Ad hoc Network) uses vehicles as mobile nodes for the communication purpose and for data sharing.

6. **On Board Units (OBUs):** These are the communication devices mounted on vehicles to facilitate communication with other vehicles and roadside units.

7. **Roadside Units (RSUs):** These are the communication units located aside the road that connects with the application server and the trust authority.

8. **Trusted Authority (TA):** They are third party entrusted with the job of certificate generation, distribution and revocation.