Detection and Prevention of Distributed Denial of Service Attacks In VANETs

Author

MUNAZZA SHABBIR

NUST201362459MCEME35213F

Supervisor

Dr. MUAZZAM A. KHAN

DEPARTMENT OF MECHANICAL ENGINEERING

COLLEGE OF ELECTRICAL & MECHANICAL ENGINEERING

NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY

ISLAMABAD

MAY, 2013

Detection and Prevention of Distributed Denial of Service Attacks In VANETs

Author

MUNAZZA SHABBIR

NUST201362459MCEME35213F

A thesis submitted in partial fulfillment of the requirements for the degree of

MS Computer Engineering

Thesis Supervisor:

Dr. MUAZZAM A. KHAN

Thesis Supervisor's

Signature:____

DEPARTMENT OF MECHANICAL ENGINEERING

COLLEGE OF ELECTRICAL & MECHANICAL ENGINEERING

NATIONAL UNIVERSITY OF SCIENCES AND TECHNOLOGY,

ISLAMABAD

MAY, 2013

Declaration

I certify that this research work titled "*Detection and Prevention of Distributed Denial of Service Attacks In VANETs"* is my own work. The work has not been presented elsewhere for assessment. The material that has been used from other sources it has been properly acknowledged / referred.

Signature of Student

MUNAZZA SHABBIR

NUST201362459MCEME35213F

Language Correctness Certificate

This thesis has been read by an English expert and is free of typing, syntax, semantic, grammatical and spelling mistakes. Thesis is also according to the format given by the university.

Signature of Student

MUNAZZA SHABBIR

NUST201362459MCEME35213F

Signature of Supervisor

Copyright Statement

Acknowledgements

I am thankful to my Creator Allah Subhana-Watala to have guided me throughout this work at every step and for every new thought which You setup in my mind to improve it. Indeed I could have done nothing without Your priceless help and guidance. Whosoever helped me throughout the course of my thesis, whether my parents or any other individual was Your will, so indeed none be worthy of praise but You.

I am profusely thankful to my beloved parents who raised me when I was not capable of walking and continued to support me throughout in every department of my life.

I would also like to express special thanks to my supervisor Dr. Muazzam A.Khan for his help throughout my thesis and also for Networking courses which he has taught me. I can safely say that I haven't learned any other engineering subject in such depth than the ones which he has taught. I am also grateful to my thesis committee members Dr. Saad Rehman, Dr. Arsalan Shaukat and Dr. Shehzad Khalid for their valuable feedback in this research work.

I am also thankful to my husband Danish Faraz for showing endless faith in me and encouraging me at every point when I felt discouraged.

I would also like to thank my friends Ms. Khushnaseeb Fatima and Ms. Muntaha Sakeena for their support and help throughout the course of the study.

Finally, I would like to express my gratitude to Mr. Umair Shafiq Khan who rendered valuable assistance to my study.

Dedicated to my parents

Table of Contents

List of figures

Abstract

Current crowded fashion of traffic and increasing count of mobiles on roads, undoubtedly demand for an Intelligent Transportation System. Vehicular ad-hoc networks commonly known as VANETs is becoming a popular technology in the modern transportation world. The idea of VANET is similar to MANETs except from the fact that here vehicles represent the mobile nodes of the wireless network. As per the basic applications of VANETs any information circulating through the network can be life crucial. So the integrity of the information is a critical need. The mobility of the nodes and the nature of the connections in the network have made VANET vulnerable to many security threats. One of the major and notorious attacks that exhaust the network by illegitimately using all of its resources is DDOS attack. In this type of attack an attacker fakes multiple identities of nodes I-e uses spoofed IP addresses to harm the network by making it deny to cater to legitimate requests for services hence jeopardizing the availability of network. In this thesis a review is made of the already proposed defense mechanisms and a novel detection and prevention scheme is proposed.

In the presented solution the simplest fact about DDOS attacks is manipulated I-e flooding or abnormal number of packets sent by a potential attacker. By keeping a check on this number an attack can be detected relatively earlier and can be prevented by abandoning the sender node.

Ns2 simulator is used to implement and analyze the mechanism and to show the results.

CHAPTER 1: INTRODUCTION

1.1 Overview

Every year, as the architectural infrastructure is getting more sophisticated yet crowded and with growing number of vehicles on the road the need to make driving a more organized act is becoming important. For an organized traffic flow vehicles need to have a constant information supply about locations, surrounding traffic scenarios, routes etc.

There can be many categories of information that can be helpful to organize the traffic in a better way e.g. info to assist driver and about the safety of both the driver and the car, traffic jam warning, news about an accident, message from the preceding vehicles about brakes, road maintenance, distance between two adjacent vehicles and many other messages that can prevent an accident or harm [1]. Keeping these needs in regard the concept of Intelligent Transportation System ITS emerged. Its main aim is to make driving and safety conditions better and also provide on the go infotainment. For this, information between the vehicles and some control units was necessary to share, and to do this sharing an Ad Hoc vehicular network is created [2].

The idea of vehicular ad hoc networks is based upon manets given that in VANET vehicles serve as mobile nodes. The basic characteristics of these types of networks are that nodes can freely move into any direction and in and out of a network's range. But still they can connect with each other either in a single hop or via multihop link. In VANET vehicles can communicate with each other and also with RSUs which are road side units wirelessly. These communications are referred to as V2V and V2I respectively [3] [4]. The presence of RSUs (road side units) not only increase the scalability of network but further link these vehicles to an infrastructure. An infrastructure or a back bone network can monitor and control the network traffic and can make decisions regarding its security and other matters.

1.2 Problem Statement and Motivation:

Security challenges and threats are a major concern as far as deploying VANETs commercially or practically is concerned. Networks like VANETs in which nodes are connecting and communicating wirelessly are more likely to be exposed to attackers, because the lack of a wired central infrastructure makes it very difficult to monitor the activities of a network. Three major factors affected by attacks are integrity, confidentiality and availability. As apparent from name DOS attacks harm the availability of network and its services. DOS is the most common, notorious yet easy to launch attack type but its impact is massive and deteriorating. Catering to the requests of users is top most priority of any network and damaging its availability means making network useless. Distributed denial of service attacks are even worst where multiple perpetrators target a common victim, flooding it with abnormally large number of bogus messages, stripping it of all of its resources such that it’s no longer able to deal with legitimate requests of actual packets.

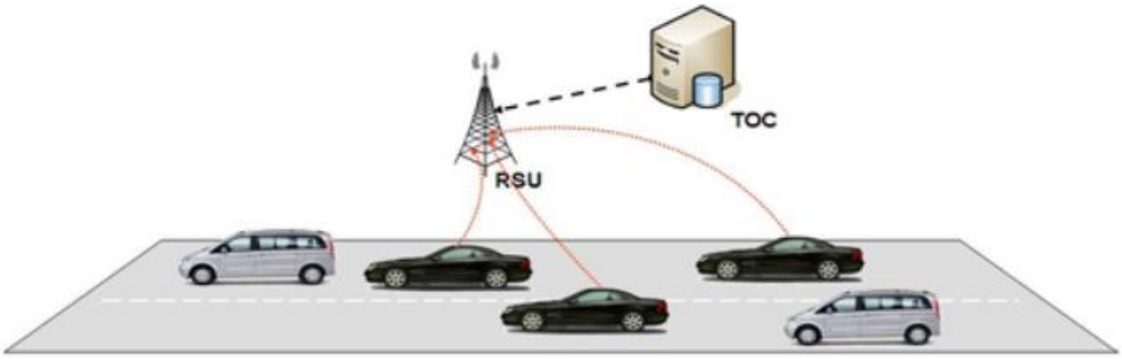


Figure 1.1: DDOS attack launched on RSU by attackers [4]

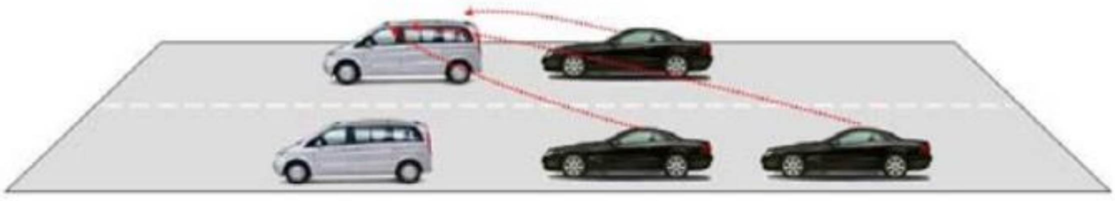


Figure 1.2: DDOS attack launched on a victim vehicle [4]

Every layer of a network in communication model of a network is prone to DDOS attacks, likewise at every layer the ways to perform this attack is different. The layer considered in our case is transport. At transport layer the DDOS has the form of sync attack or smurf attack. As TCP is used for connection establishment at transport layer so exploiting this fact an attacker sends maliciously large number of connection establishment request packets. The victim tries to respond to all these request by sending acknowledgements back to these requests but the sender (attacker) is usually a spoofed id does not respond back to these acknowledgements leaving a numerous number of half opened connections at receiver (victim's) part. This exhausts the victim and makes it unable to respond to actual requests.

Moreover, its difficult to trace back the attacker as the attacker usually uses a spoofed id.

1.3 Thesis Objective:

As discussed earlier the structure and working of VANET is so that DDOS attacks are inevitable. The objective of our work in this thesis work is to come up with a defense mechanism which detects the attack at an early stage so that very limited damage is caused, takes advantage of the available resources such as battery power of vehicle and presence of infrastructure and above all is simple. The proposed scheme is designed to full fill the above mentioned criterions.

1.4 Structure of Thesis:

This thesis work is divided into 7 chapters.

First chapter is about the introduction to the work done, the problem statement, objective of thesis and how we plan to tackle the problem is mentioned in this chapter.

Second chapter covers the details of underlying network in focus i-e VANET, its introduction, technology used, applications and working.

Third chapter is about the security challenges VANET faces, different types of attackers, attacks and vulnerabilities of network.

Fourth chapter researches on the already done work in this domain, different categories of solutions provided, and work done by researchers.

Fifth chapter introduces readers to the platform which is used to implement the algorithm. It covers NS2, it structure and working, and AWK scripting also.

Sixth chapter shows our proposed methodology, its working, components, result plotting, simulation and results.

Final chapter 7 gives conclusion and future work to be done.

CHAPTER 2: VANET

2.1 VANET Architectural Model:

The basic VANET architecture can be divided into two parts as per the nature of entities and their communication with each other present in the network.

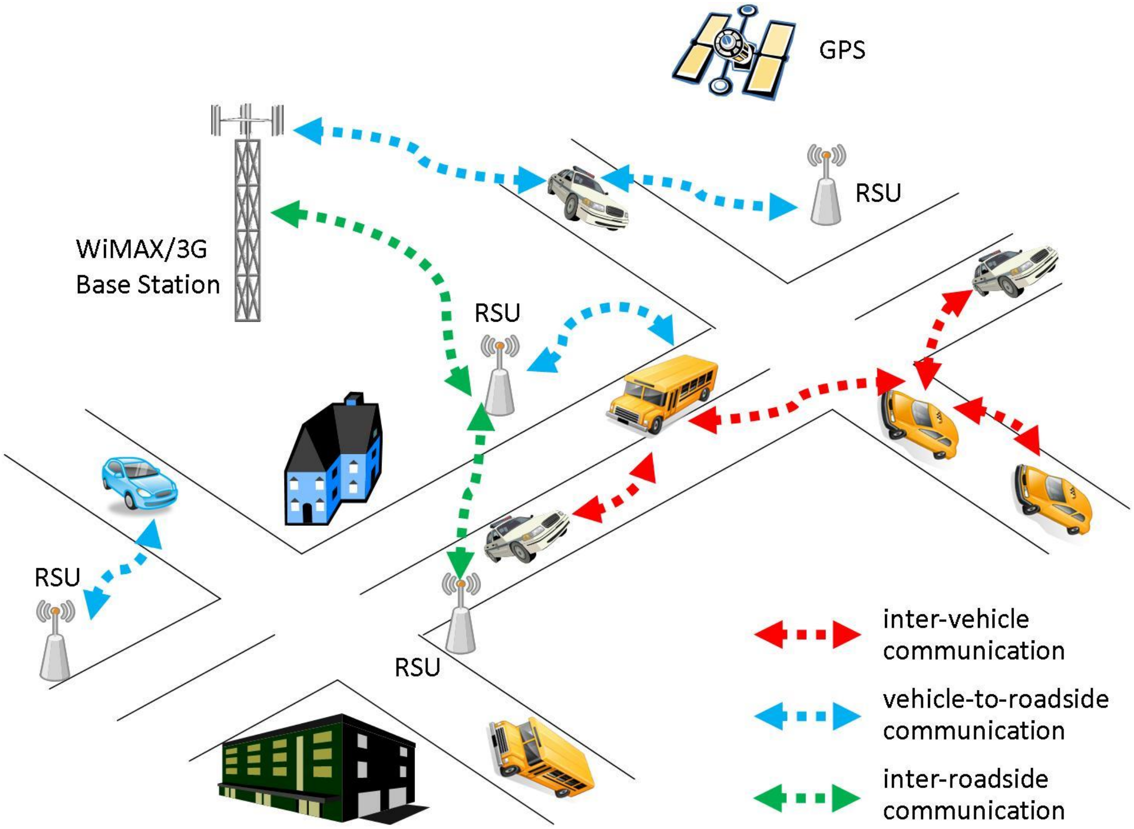


Figure 2.1: VANET architecture [17]

2.1.1 Infrastructural model:

This part of the network generally consists of four types of participants; **manufacturers, legal authority, trusted third party ,** three of these are considered to come under the same umbrella , and **service providers.** As they are the part of infrastructural environment so they are connected permanently. Generally their job is to control and manage the traffic flow or provide additional services.

Manufacturers may or may not be the part of this model but as manufacturers their job is to individually classify each automotive. The task for legal authority is to register each vehicle in the network and issue a license plate as its unique identity. It also manages other legal matters regarding transportation such as penalties, offences etc. trusted third parties or TTPs are responsible for management of credentials and time stamping, these services are important for both legal authorities and manufacturers. Service providers give access to those services to the entities in network which are provided in VANET e.g. location based services and digital video broadcasting [3].

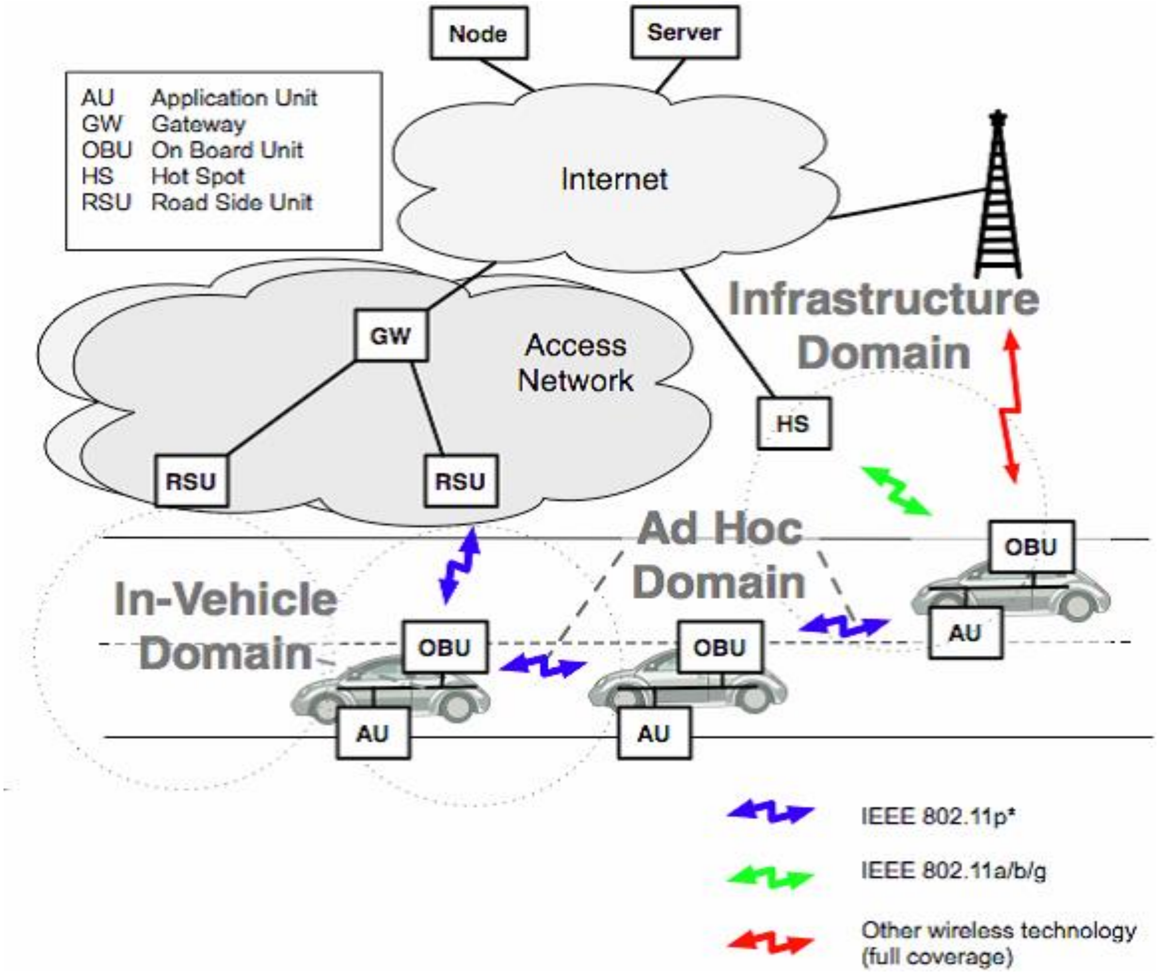


Figure 2.2: VANET model domains [9]

2.1.2 Ad Hoc model:

This part of the network works similar to MANETs where vehicles serve as mobile nodes and connect with each other on ad hoc bases. These connections are between vehicles and between vehicles and RSUs. To serve the purpose each vehicle is equipped with on board unit OBU. OBU provides interface to user in a vehicle at a passenger device called application unit. OBU runs necessary algorithms and communication protocols and hence enables the V2V and V2I communication. They might also consist of sensors to keep a check on vehicles own status and immediate environment [3].
RSUs are the gateways between infrastructural and ad hoc model.

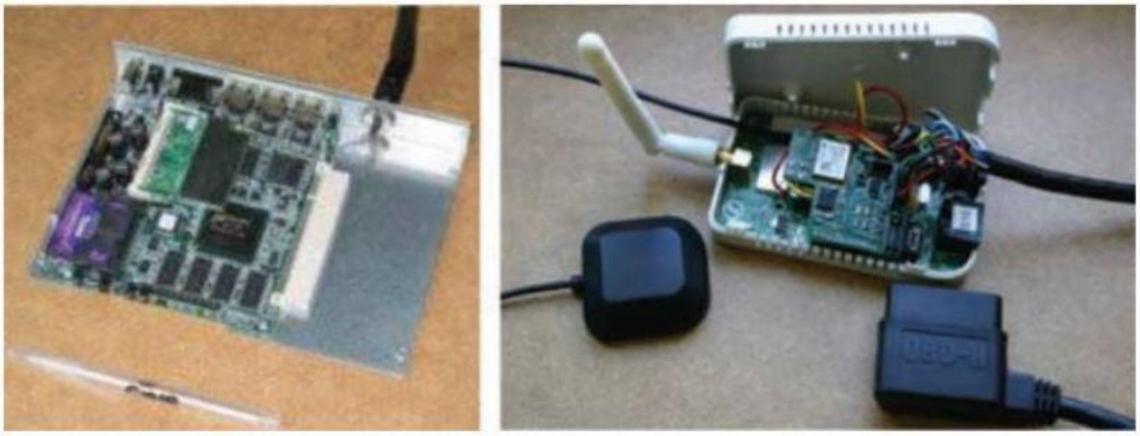


Figure 2.3: MIT developed test OBUs [11]

2.2 Characteristics of VANET:

Though the foundation of VANET is based upon MANET but as it is particularly designed for transportation assistance purposes so it is, in many ways different than MANET. The distinct features of VANET are as follows:

• High Mobility: The hubs in VANETs typically are moving at rapid. So its hard to foresee a hub's position whenever.

• Rapidly changing system topology: Due to high hub versatility and irregular rate of vehicles, the position of hub changes as often as possible. As a consequence of this, system topology in VANETs tends to change often.

• Unbounded system size: VANET can be actualized for one city, a few urban communities or for nations. This implies system size in VANET is topographically unbounded. Also exceptionally versatile hubs enter and leave the system as often as possible so the extent of system is not determined at any given time.

• Frequent trade of data: The specially appointed nature of VANET spurs the hubs to assemble data from alternate vehicles and street side units. Henceforth the data trade among hub gets to be successive.

• Wireless Communication: VANET is intended for the remote environment. Hubs are associated and trade their data remotely. Along these lines some security measure must be considered in correspondence.

• Time Critical: The data in VANET must be conveyed to the hubs with in time constrain so that a choice can be made by the hub and perform activity as needs be.

• Sufficient Energy: The VANET hubs have no issue of vitality and calculation assets. This permits VANET utilization of requesting systems, for example, RSA, ECDSA usage furthermore gives boundless transmission power.

• Better Physical Protection: The VANET hubs are physically better ensured. Hence, VANET hubs are harder to trade off physically and lessen the impact of foundation assault [6].

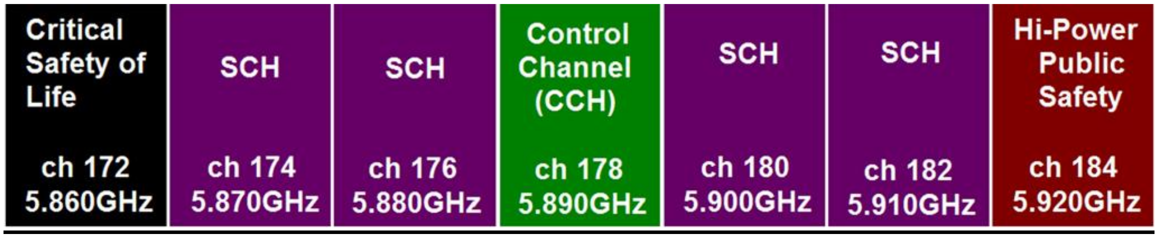
2.3 VANET Standards:

For convenience in interoperability and implementations of new technologies in new fields of communications and information technology, defining standards is a must.

When its about VANETs, all the functionalities of physical layer to application layer are specified after standardization. Usually in literature the complete protocol stack of VANETs is designated by DSRC, WAVE etc. which are explained as follows;

2.3.1 DSRC:

VANET is a unique network hence its requirements are different from other networks. The network can is expected to be enormous as the number of vehicles i-e nodes can range upto 70 million or more as per recent traffic scenarios. With such a huge number of vehicles moving at such a high speed, some separate utilities were required to be designated to this sort of network. A specific communication standard, called Dedicated Short Range Communications (DSRC) has been developed to deal with such requirements (Armstrong Consulting Inc.). Dedicated Short Range Communications (DSRC) is a dedicated communication channel for short and medium ranges, thereby it supports vehicle to vehicle and vehicle to road side communications in VANET. Such communications cover a wide range of applications, including vehicle-to-vehicle safety messages, traffic information, toll collection, drive-through payment, and several others. DSRC is aimed at providing high data transfers and low communication latency in small communication zones. Each vehicle can communicate with other vehicles using short radio signals DSRC (5.9 GHz), for range that can reach 1 KM. DSRC uses 802.11 access methods. . The DSRC spectrum is organized into 7 channels each of which is 10 MHz wide. One channel is restricted for safety communications only while two other channels are reserved for special purposes (such as critical safety of life and high power public safety). All the remaining channels are service channels which can be used for either safety or non-safety applications. Safety applications are given higher priority over non-safety applications to avoid their possible performance degradations and at the same time save lives by warning drivers of imminent dangers or events to enable timely corrective actions to be taken [5]. For a more in-depth discussion of DSRC, the reader is referred to [8, 11]

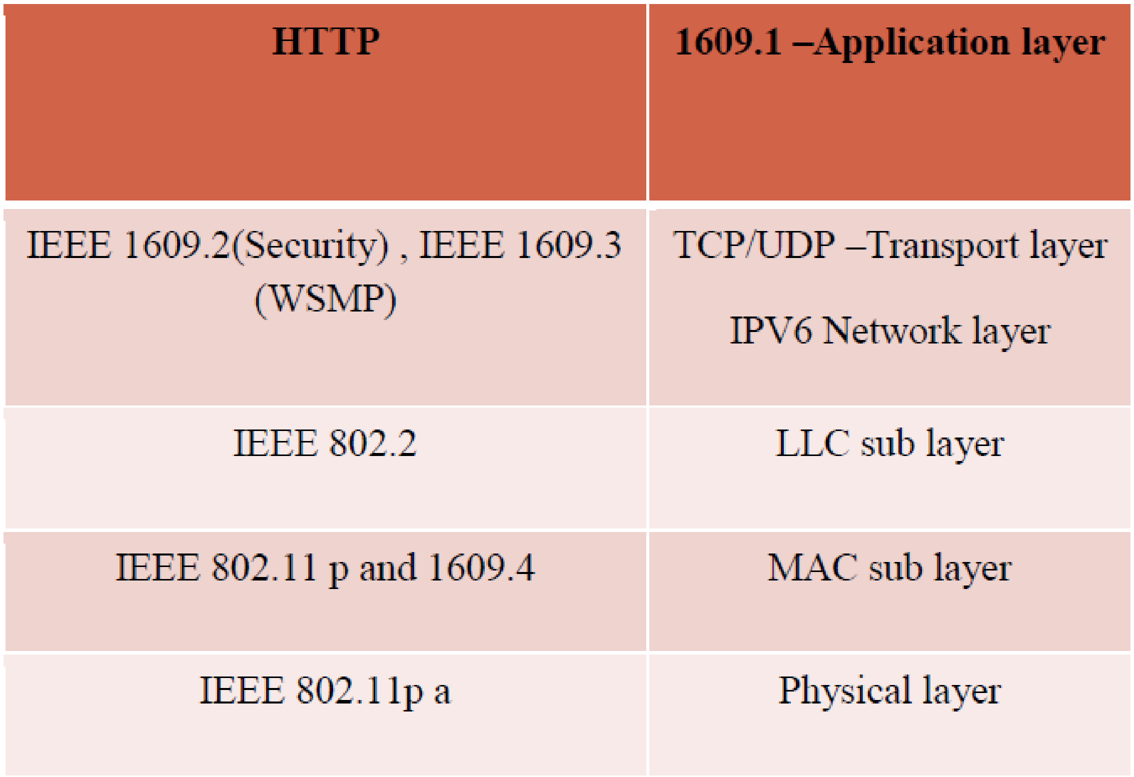


Critical Safety of Life	SCH	SCH	Control Channel (CCH)	SCH	SCH	Hi-Power Public Safety
ch 172 5.860GHz	ch 174 5.870GHz	ch 176 5.880GHz	ch 178 5.890GHz	ch 180 5.900GHz	ch 182 5.910GHz	ch 184 5.920GHz

Figure 2.4: DSRC channels [25]

2.3.2 Wave:

WAVE stands for wireless access in vehicular environments. Wave IEEE 1609 is a standard. This standard provides all the standards and details on the basis of which VANET is established and operates.



HTTP	1609.1 –Application layer
IEEE 1609.2(Security) , IEEE 1609.3 (WSMP)	TCP/UDP –Transport layer IPV6 Network layer
IEEE 802.2	LLC sub layer
IEEE 802.11 p and 1609.4	MAC sub layer
IEEE 802.11p a	Physical layer

Figure 2.5: WAVE protocol stack [25]

These standards are provided by IEEE. Architectural framework of VANET, communication protocols, services and interfaces are defined in these standards so that in any VANET environment vehicle to vehicle and vehicle to infrastructure communications are made following these standards. WAVE provides implementation foundation for messages security and applications offered by VANET e.g. safety, automatic toll payment, traffic management etc.

2.4 Routing Protocols in VANETs:

Routing protocols in VANET should be able to do two things aptly; selecting the best possible route for packets and assigning a unique address to each vehicle in the network. Traditional adhoc based routing protocols cannot cater to the unique needs of VANET due to high mobility of nodes in the network, changing topology, changing densities of vehicles in the network at different times of the day, transmission ranges etc. But still with some modifications and optimizations any MANET protocol can be used for inter vehicular communication. Routing protocols for VANETs can be grouped into six categories which are explained as follows [1][5];

1. Topology based routing protocols
a. Proactive routing protocol
b. Reactive/on-demand routing protocols
2. Position based routing protocols
3. Cluster based routing protocols
4. Broadcast routing protocols
5. Geocast Routing Protocols
6. Infrastructure based routing protocols

2.5 VANET Applications:

ITS applications include basically applications for coordination of driving systems, cooperation for collision avoidance, and notifications danger of the road. Comfort applications for travelers are also an innovative ITS applications category, they include the provision of mobile internet access, a variety of on-board services. VANET applications can be classified into several family of classifications. These classifications range from two to several categories according to the degree of accuracy. In [51], they classify applications into only two categories: Safety and Infotainment [1].

According to author's research in [7] the applications of VANETs are classified on the basis of types of data exchange taking place in VANET i-e vehicle to vehicle communication and vehicle to infrastructure's communication. The classification of application hence done is as follows;

1) Safety applications:

2) Commercial applications

3) Convenience oriented applications

4) Productive Applications

2.5.1 Safety Applications:

The main objective of development of VANET was to bring more and more safety on the roads. This objective can be achieved by constant transfer of information messages between the cars and between the vehicles and road side units. RSU can store the information sent by different nodes that can be used by vehicles at any time. Information such as neighborhood vehicles, their speed etc., road condition, and road curves etc. safety applications can further be classified into;

Real-time traffic: RSUs keep all the updated information about the network entities and surroundings and this info can be made available to the vehicles at any time needed. With the help of such real time information availability on immediate basis traffic jams, congestions and potential accidents can be avoided.

Co-operative Message Transfer: Between vehicles message transfer just to pre assist each other to avoid inconvenience is also of great benefit e.g. if a vehicle is halted or is quite slow it can inform other following vehicles so they can apply emergency brakes and hence can prevent collision. Authentication of these messages is a concern but still it's an advantageous application with proper authentication schemes.

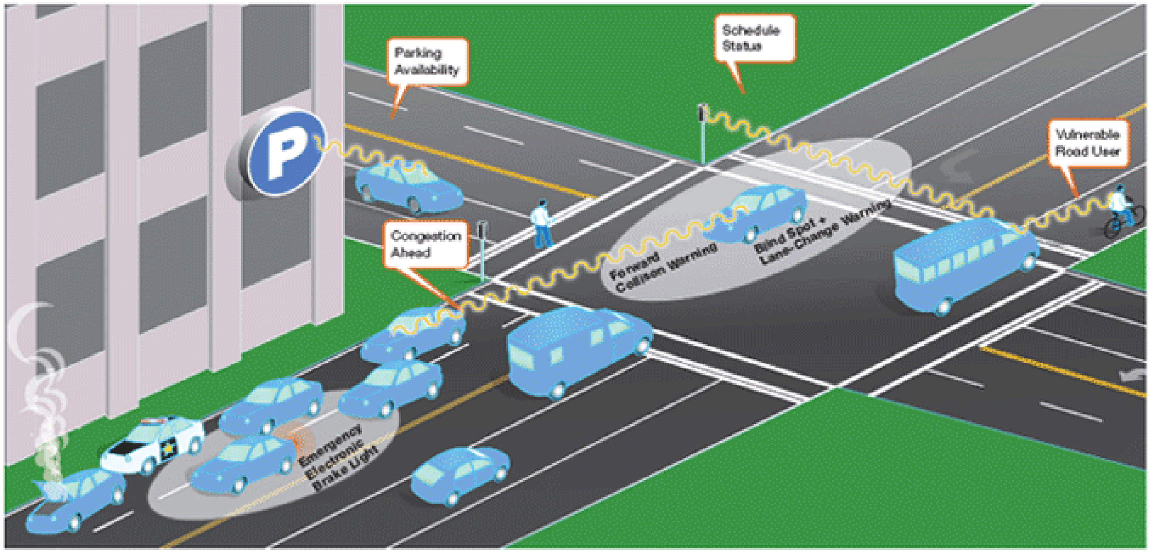

Parking Availability
Schedule Status
Vulnerable Road User
Congestion Ahead
Forward Collision Warning
Blind Spot + Lane-Change Warning
Emergency Electronic Brake Light

Figure 3.16: Scenario Depicting the Situational Awareness Concept

Figure 2.6: Safety and other messages exchanged in network [13]

Post-Crash Notification: After any vehicle has been in an accident it will spread a need for help or warning message in its approachable surroundings.

Road Hazard Control Notification: so that the following vehicles won't suffer any inconvenience, a vehicle will inform them about any road hazards or meteorological issues ahead e.g. land sliding, fog, downhill etc.

Traffic Vigilance: The cameras can be installed at the RSU that can work as input and act as the latest tool in low or zero tolerance campaign against driving offenses

2.5.2 Commercial Applications:

Commercial applications come under the category of info-tainment. Via these application passenger or driver can have a quick access to internet to get both information and stay entertained. There are different types of commercial application;

Remote Vehicle Personalization/ Diagnostics: It helps in downloading of personalized vehicle settings or uploading of vehicle diagnostics from/to infrastructure.

On the go access to internet: as mentioned earlier RSUs are gateways between vehicles and infrastructure, so if routing is done by RSU to and from vehicles and infrastructure, drivers can access internet for info-tainment purposes.

Value-added advertisement: different type of commercial advertisements such as road side motels, restaurants, fuel pumps, workshops etc. are aired through the vehicles in communication range to get the attention of travelers.

2.5.3 Convenience oriented Applications:

Driving experience can be made convenient if the traffic management is enhanced. For driver's convenience following applications can be designed:

Route diversion: in case of heavy traffic or road congestion or blockage if drivers are informed earlier they can take an alternative route.

CHAPTER 3: SECURITY CHALLENGES IN VANETS

“A wireless network of intelligent vehicles can make a highway travel safer and faster. But can hackers use the system to cause accidents?” Authors Jeremy Blum and Azim Eskandarian raised this question in “Threat of Intelligent Collisions” [10]. This simple question puts many question marks on the credibility of the data exchanged between vehicles in VANET that might lead to the harm of vehicles instead of their safety. Given the nature of VANET the integrity of data going viral is a major concern, an attacker can modify, and remove or misuse the information being sent hence jeopardizing many lives or degradation of the network. Due to the mutual cooperation among vehicles about sharing the communication channel [10], volatile connection among vehicles, vehicles entering and leaving a network shortly and the size of the network, the implementation of a proper security scheme is a very difficult task [1]. On the other hand VANET has an advantage over other MANETs in terms of battery life. As afore mentioned, VANET has no constraints over battery life due to which heavy computational algorithms are possible to run on OBUs for security purposes [5].

3.1 Types of Attackers:

Before designing any security scheme for VANET against attacks, identification of type an attacker is must. Each type of an attacker has different roles and powers. They are classified as:

1. Insider vs. Outsider: The insider is one of the authenticated nodes of the network that might have been tampered by the manipulator. Being a trusted member of the network it has many authorities that can be used against the network. While the outsider is an attacker that is regarded as an intruder by network entities and has very less impact over the network.

2. Malicious vs. Rational: A malignant aggressor looks for no personal advantages from the assaults and plans to hurt the individuals or the usefulness of the system. Subsequently, he may utilize any methods dismissing resulting expenses and results. Despite what might be expected, a rational assailant looks for individual benefit and consequently is more unsurprising regarding the assault means and the assault target.

3. Active vs. Passive: An active aggressor can create messages, while a passive assailant delights himself with illegitimately listening the data exchange between entities and further misusing it [11].

3.2 Classification of VANET Attacks:

Given the diversity of VANETs possible threats and attacks, and in the interests of clarity and simplification, it is necessary to classify them.

Attacks on availability: Availability is a very important factor for VANETs. It guarantees that the network is functional, and useful information is avail- able at any

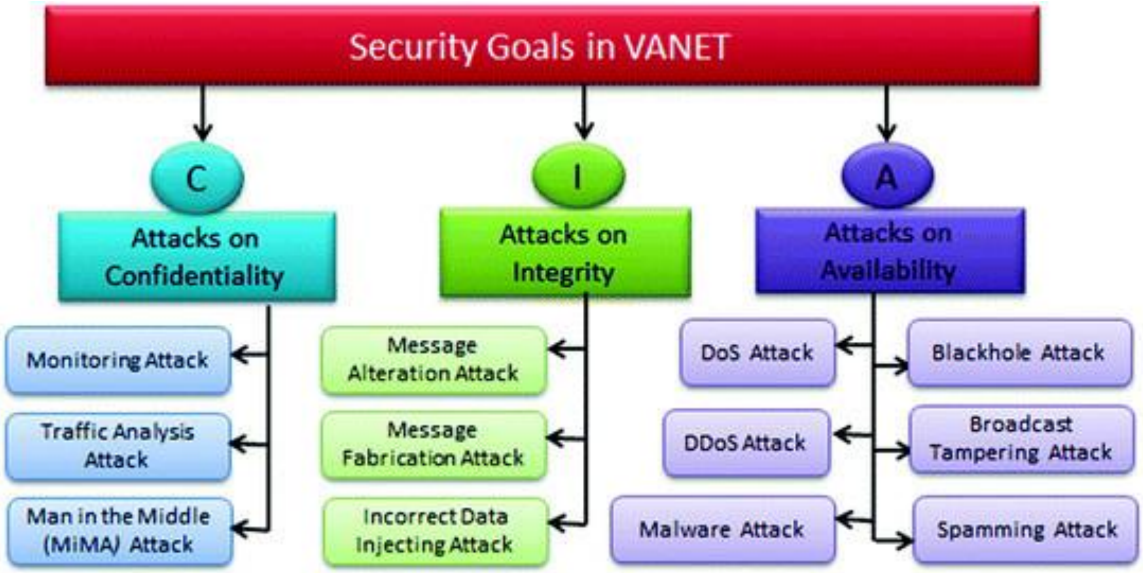


Figure 3.1: Security goals in VANET [6]

Availability is a vital component for VANETs. It promises that the system is practical, and helpful data is profit capable at any working time. This basic security necessity for VANETs, which primary reason for existing is to guarantee the clients' lives, is an important focus for a large portion of the assailants. A few assaults are in this classification, the most renowned are the Denial of Service assaults (DoS).

Attacks on authenticity and identification: Authenticity is a major challenge of VANETs security. All existing stations in the network must authenticate before accessing available services. Any violation or attack involving the process of identification or authentication exposes all the network to a serious consequences. Ensure authenticity in a vehicular network is to protect the authentic nodes from outside or inside attackers infil-trating the network using a falsified identity. The importance of identification–authentication process comes from the fact that it is frequently used whenever a vehicle needs to join the network or a service. There are several types of attacks in this category.

Attacks on confidentiality: Confidentiality is an important security requirement for VANETs communications, it ensures that data are only read by authorized parties. In the absence of a mechanism to ensure the confidentiality of the exchanged data between nodes in a vehicular network, exchanged messages are particularly vulnerable to attacks such as the improper collection of clear information. In these cases, the attacker can gather information on the location of the vehicle and its routes, on users’ privacy, etc. The information collected in the absence of a confidentiality mechanism may affect the privacy of individuals, knowing that it is difficult to detect this kind of attack, since it is virtually passive and user currently is not aware of the collection. However, in the case where the exchanged messages do not contain any sensitive information confidentiality is not necessary.

Attacks on integrity and data trust: The integrity of exchanged data in a system is to ensure that these data have not been altered in transit. Integrity mechanisms help therefore to protect information against modification, deletion or addition attacks. In the case of VANETs, this category targets mainly V2V communications compared to V2I communications be- cause of their fragility. One of the possible techniques which facilitate this kind of attacks is the manipulation of in-vehicle sensors.

Attacks on non-repudiation/accountability: Non-repudiation in computer security means the ability to ver- ify that the sender and the receiver are the entities who claim to have respectively sent or received the message. Otherwise, the non-repudiation of data origin proves that data has been sent, non-repudiation of arrival proves that they were received. In a VANET context and since the manipulated data related to the safety and privacy of the users, it should be always possible to verify all hard- ware and software changes of security settings and applications (update, modification, addition, etc.).

3.3 Attacks on availability:

Denial of Service attacks: The Denial of Service (DoS) attacks ac-tually include a family of attacks targeting the availability of network services, which can have serious consequences especially for VANETs applications. Because of their impacts, DOS attacks are classified as a dangerous class of attacks. They can be performed by internal or external malicious nodes to the network. In these attacks, the attacker tries to block the principal means of communication and aims to interrupt ser- vices, so they will not be available to legitimate users. As an example, flooding the control channel with high volumes of messages generated by intentionally manufacturing .The network nodes (OBU and RSU) will not be able to handle the huge amount of received data. DDoS attack (Distributed Denial of Service) is a variant of DOS attacks, it is a distributed attack ordered by a main attacker who plays the role of “attack manager” with other agents who may be also victims unknowingly. The action methods of DDoS attacks are in most cases flooding the network and the results are always disastrous. Jamming, greedy behavior, blackhole attack, are examples of DOS attacks.

Jamming attack: The jamming attack, is a physical level of De-nial of Service attack. Jamming in its basic definition is the transmission of a signal to disrupt the communications chan- nel, it is usually intentional. This lowers the signal to noise ratio (SNR: Signal to Noise Ratio) for the receiver. Unin- tentional interference is called “interference” and occurs when a transmission is made in a frequency band that is already in use and operational. For a successful adaptive jamming attack, the jammer must act at the same time that the activity of the useful signal to jam. It must also choose the most effective signal transmission model that merges the best the receiver. In a VANET network, jamming once successful, can have inevitable consequences. Some research works have looked for some techniques to reduce the effect of jamming for mobile ad hoc networks.

Greedy behavior attack: The Greedy attack is an attack on the functionality of the MAC layer according to the architecture of the OSI model. The greedy node does not respect the channel access method and always tries to connect to the media. The main purpose is to prohibit other nodes to use the sup-port and services. According to, a greedy behavior node tries also to minimize its waiting time for faster access to the channel and penalize other non-compromised nodes. Greedy behavior causes overload and collision problems on the trans- mission medium, which produces delays in authorized users services. Greedy behavior is independent and hidden to upper layers, then it cannot be detected by mechanism designed for those layers.

Blackhole attack: The Blackhole attack is a conventional attack against the availability in ad hoc networks, it exists also for VANETs. In Blackhole attack, the malicious node receives pack- ets from the network, but it refuses to participate in the op-erations of routing data. This disrupts the routing tables and prevents the arrival of vital data to recipients mainly because the malicious node always declares being part of the network and able to participate, which is not the case practically . The effect of this type of attacks is more dangerous for VANETs than other mobile networks. A Blackhole node can e.g. redirect the traffic that receives to a specific node which does not exist in fact and this causes data loss. Blackhole attack can also be used as a first phase of a man in the middle attack that we detailed later.

Grayhole attack: This attack consists in removing only the data packets of certain applications that are vulnerable to packets loss. GrayHole is considered as a Blackhole attack variant.

Sinkhole attack: This attack consists that the malicious node attracts neighboring nodes so their packets go through it, this helps to eliminate or modify the received packets before re- transmitting them eventually. The Sinkhole attack can be used to mount other attacks as Grayhole and Blackhole.

Wormhole attack: Wormhole is a denial of service attack, it requires the participation of at least two nodes. It simply consists that an attacker *A* sends a message to an attacker *B* geographically far from him, that *B* broadcasts completely. This message suggests to neighboring nodes of *B*, that *A* is their neighbor. This attack allows two or more legitimate nodes and non-neighbors (their radio transmission areas do not over- lap) to exchange control packets between them, to create non-existent roads.

Malware attack: Given the existence of a software components to operate the OBU and RSU, the possibility of infiltration of malware (malicious software) is possible in the network dur- ing the software update of VANET units. The effect of a malware is similar to the effect of viruses and worms in an ordinary computer network, except that in a VANET network, disruption of normal functionality is always followed by serious consequences.

Broadcast tampering attack: In this type of attack, the attacker tries to make and inject fake security alert messages in the network. This may hide the true safety messages to legiti-mate users, it can cause also accidents and seriously affect the overall network security. In general this type of attack is possible for a legitimate node.

Spamming attack: As in a web environment, the spam messages such as advertisements e.g. have no utility for users. In a VANET network which is a mobile radio environment, this type of attack aims to consume bandwidth and cause voluntary collisions. Given the lack of a centralized management of the transmission medium, this makes more difficult the control of such attacks.

3.4 TCP DDOS/SYN Flooding Attack:

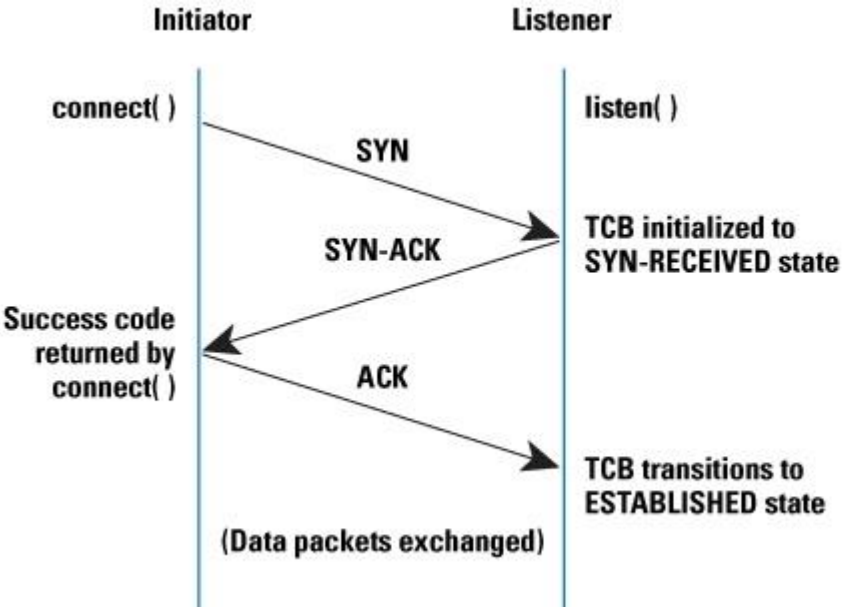


Figure 3.2 : TCP 3 way handshake [10]

As transmission control protocol is used at transport layer foe connection establishment with other nodes. The type of DDOS attack which misuses TCP features to launch an attack is called SYN flooding attack. In our thesis we have covered this type of attack n has proposed a solution against it. According to the TCP protocol, to establish a connection between any two nodes a three way handshake is required. A three way handshake is a three step method. The node which desires to communicate sends a SYN packet to the receiver. Every node has a data structure to save all the incoming SYN packets, in normal communication a node sends SYN requests no more than maximum limit of a reciever’s data structure. Till this point connection is said to be half-opened. When so ever a receiver receives a SYN packet it dispatches a SYN-ACK to sender in response to which sender sends back an ACK and connection is confirmed.

In a SYN flood attack, an attacker and its bots start flooding the victim with SYN. Upon receiving such an enormous number of SYN requests, victim’s data structure is over filled with these flooded requests and no more space is left to store and entertain a legitimate request SYN. Moreover victim starts sending SYN-ACK back to attackers but upon receiving no response a large number of half opened connections are left at victim’s part stripping it off of all its resources.

CHAPTER 4: LITERATURE REVIEW

DDoS (Distributed Denial of Service) assault is one of the fundamental dangers that the Internet is confronting. The guard of DDoS assaults has turned into a hot exploration subject. The DDoS assault makes utilization of a wide range of sources to send a great deal of futile parcels to the objective in a brief span, which will devour the objective's asset and make the objective's administration occupied. Among all the system assaults, the DDoS assault is less demanding to do, more hurtful, difficult to be followed, and hard to anticipate, so its danger is more serious.The detection,n of assaults is a vital part of resistance of DDoS assault, and the discovery results can influence the general execution of assault safeguard. As of late, the DDoS assaults are tending to utilize genuine source IP location to play out an assault, so it has turned out to be more hard to recognize the ordinary system stream and the assault stream, which makes an early and exact identification more troublesome [13]. Distinctive scientists and creators have proposed their answers against various sorts of DDOS assaults. On a broader level all of these solutions can be categorized in three classes, briefly described below.

4.1 Channel Switching:

As mentioned earlier, communication channel reserved for VANET has multiple channels each of bandwidth of 10 MHz and a maximum data transfer ratio of 27Mbps. While the communication is continued only one of the channel is used while the rest are usually inactive. So in the case of DDOS attack when the channel is being invaded by attackers, the legitimate traffic can be directed to an alternative channel.

4.2 Frequency Hopping Spread Spectrum:

By using this technology signals are sent over a different frequency band by increasing the signal bandwidth via adding keys. In this way when so ever an attack is detected the legitimate traffic of packets is shifted to a different frequency range.

4.3 Technology Switching:

According to the infrastructure of VANET there are two sorts of communications taking place i-e between vehicles V2V and between vehicle and RSU, so when ever an attack is launched, one way to dodge is to switch the communication path e.g if possible than fo V2V to V2I and from there to vehicle.

In [17] a method to detect ddos is presented by analyzing traffic flow in the network. This method uses: the Traffic Analyzer, the Fuzzification, the Fuzzy Inference Engine, the Knowledge Base, and Forensic Analyzer. Traffic patterns are read from a trace file and log files are created. Then by using fuzzy algorithm analysis is carried out. The analysis is the crunch of this whole process, it provides information like where why, when and by whom an incident took place in network and then draw conclusion about the happening of an attack.

In [18] a filtering based methodology is proposed to detect DDOS attacks. This scheme works against the IP spoofing phenomenon which is the basis of DDOS attack. The algorithm of detection works at victim's side independently and collects the source data of its clients, e.g source IP addresses, how many hops is the server away in no attack instances. So when an attack is detected, on the basis of already collected data of actual packets, legitimate and malicious packets can be filtered out. In the scheme the source address is classified into different fields making the information extraction fast and easy. In [19] the concept of clustering the nodes into groups on the basis of specific parameters is used for scalable communication within a cluster and between clusters a RSUs. The parameters used to form clusters are battery power, connectivity, memory and distances between nodes. The most feasible node from a group of nodes is made a cluster head. The responsibilities of cluster head includes collecting the information of group members such as ids, max flooding n max packet drop, as well to communicate with RSU on behalf of all the nodes in a cluster. To communicate with RSU a cluster head locates nearest RSU and sends a message n required info , on the basis of info received RSU passes a conclusion about any node being malicious or not and then informs cluster head to terminate that nodes connection.

In [20] once again traffic pattern is scrutinized to look up for any anomalies leading to ddos attack. According to author in a normal scenario the abrupt disruptions in traffic flow is monitored on the basis of two statistical parameters i-e volume and flow of data packets in bytes transmitted in network.

In [21] a cryptographic defense mechanism is used for classification and filtering of attacks packets. If a packet is identified as a malicious packet, it is blocked at the external boarder line router of network and the victim is saved at an initial stage. Before initiating the communication both the participating entities must identify and authenticate themselves to avoid IP spoofing. And for the authentication of the packets being transmitted hash based cryptography is used.

In [23] the spoofed ips of attacker ids are identified by comparing them with the already existing data base of existing ip addresses. Within the network at regular basis, announcing packets are transmitted by each vehicle in the network to all the neighboring vehicles to inform them about their presence and stay updated about theirs and to gain information about next node. In this scenario each node in the network has an updated database about its surroundings. In the case of presence of an attacker a node will find a duplicate ip address in their data log and such identical addresses will be considered as attackers.

[24] uses an attacked packet detection algorithm through which vehicles communicate with RSU. This mechanism gains information about the communicating vehicles exact location. After that details about the packets broadcasted via that vehicles are collected; mainly the frequency and velocity of packets. Depending on these variables values decision is made that it's an attacking vehicle or safe one.

In our base paper[27] the idea which is exploited is about the average time of a communication session between two nodes is short, while an attacker node will keep on transmitting packets to the victim node for an extended period and will flood it. So according to the proposed algorithm the average time of communication between two normal nodes is computed and stored as max threshold value. For all the future communication sessions their time interval is compared with threshold value. If the input value increases the max value, the sender node will be considered as malicious and is terminated.

CHAPTER 5: NETWORK SIMULATOR & AWK LANGUAGE

5.1 NS 2.35:

NS is an event simulator which simulates events packets by packets. In this simulator many protocols, network components, types of networks and models of traffic are implemented. On this platform, network responses and behavioral changes are simulated and examined. Different levels of network topologies can be implemented from small scale to extensive ones, different experimental events are carried out on them and results are checked for multiple traffic loads.

NS is friendly with many operating systems such as

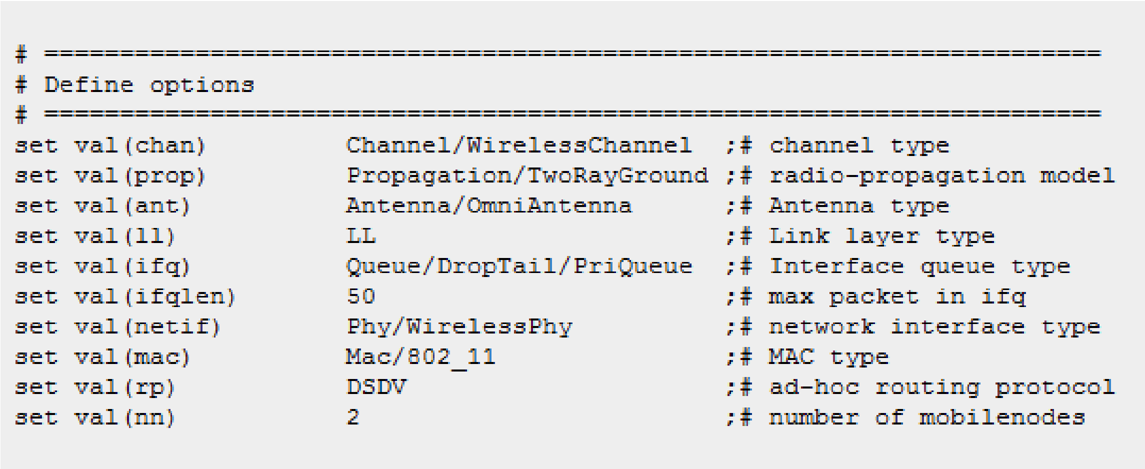
- Unix
- Linux
- Free BSD
- SunOS/Solaris
- Windows 95/98/NT/2000/XP

5.1.1 Backend Environment of Network Simulator:

NS is implemented with the help of two languages, on the back end C++ is used while at front end OTcl is used for different scripting by user. Usage of C++ makes the simulation effective and makes processing faster. While OTcl helps create diverse network topology, its flexible and simple to use.

5.1.2 Defining nodes and topology:

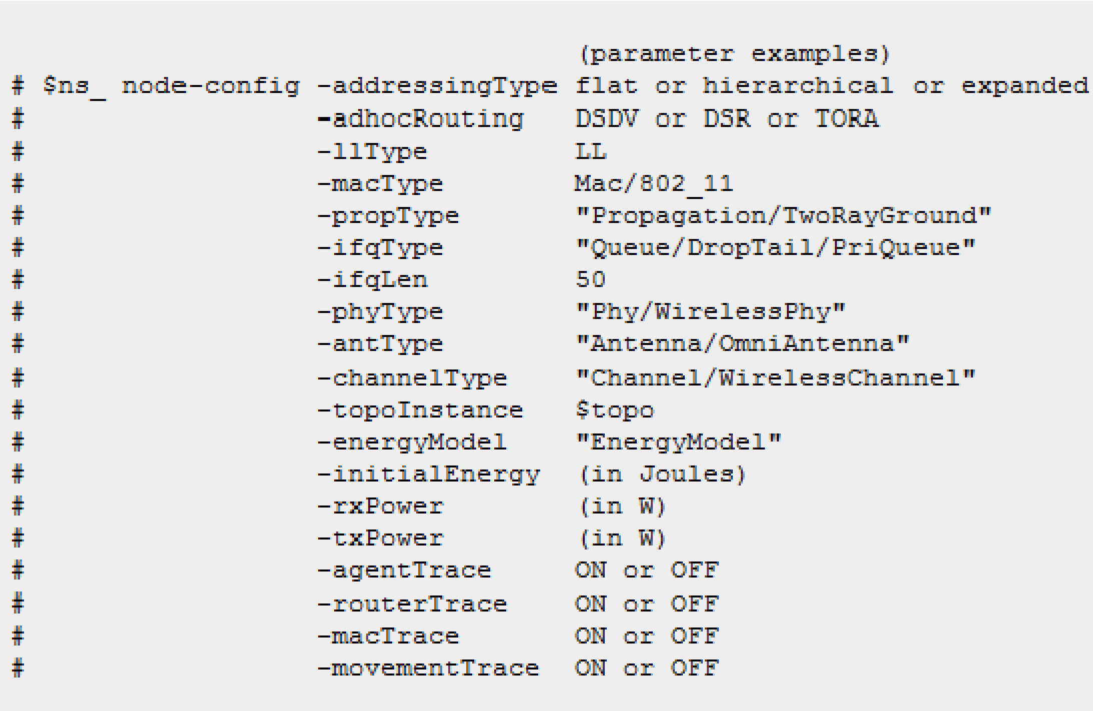
In figure 5.1 a general form of network topology options is given. To create a network, shown parameters must be configured such as channel type, antenna type, queue type, routing protocol and extent of a network



```
# ======================================================================
# Define options
# ======================================================================
set val(chan)         Channel/WirelessChannel  ;# channel type
set val(prop)         Propagation/TwoRayGround ;# radio-propagation model
set val(ant)          Antenna/OmniAntenna      ;# Antenna type
set val(ll)           LL                       ;# Link layer type
set val(ifq)          Queue/DropTail/PriQueue  ;# Interface queue type
set val(ifqlen)       50                       ;# max packet in ifq
set val(netif)        Phy/WirelessPhy          ;# network interface type
set val(mac)          Mac/802_11               ;# MAC type
set val(rp)           DSDV                     ;# ad-hoc routing protocol
set val(nn)           2                        ;# number of mobilenodes
```

Figure 5.1: Network topology configuration [22]

.

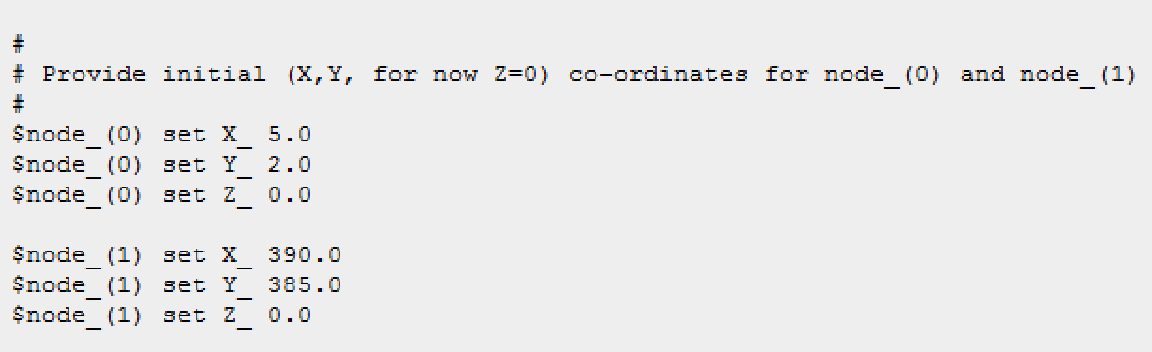


```
                                     (parameter examples)
# $ns_ node-config -addressingType flat or hierarchical or expanded
#                  -adhocRouting   DSDV or DSR or TORA
#                  -llType         LL
#                  -macType        Mac/802_11
#                  -propType       "Propagation/TwoRayGround"
#                  -ifqType        "Queue/DropTail/PriQueue"
#                  -ifqLen         50
#                  -phyType        "Phy/WirelessPhy"
#                  -antType        "Antenna/OmniAntenna"
#                  -channelType    "Channel/WirelessChannel"
#                  -topoInstance   $topo
#                  -energyModel    "EnergyModel"
#                  -initialEnergy  (in Joules)
#                  -rxPower        (in W)
#                  -txPower        (in W)
#                  -agentTrace     ON or OFF
#                  -routerTrace    ON or OFF
#                  -macTrace       ON or OFF
#                  -movementTrace  ON or OFF
```

Figure 5.2: Node configuration [22]

After establishing a network one has to configure the wireless nodes. For node configuration the parameters mentioned in above figure should be set.

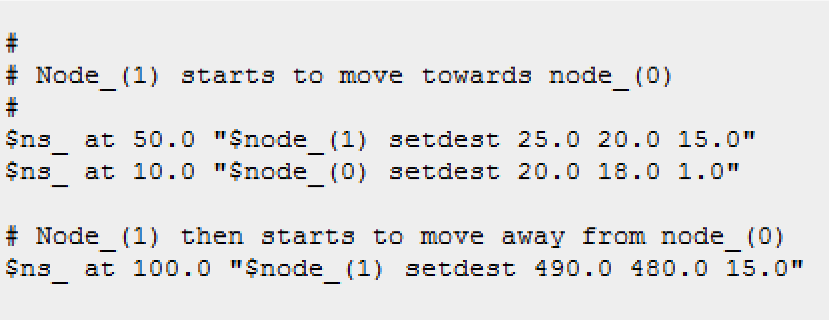
Once the nodes are configured initial position of nodes is set in following format.



```
#
# Provide initial (X,Y, for now Z=0) co-ordinates for node_(0) and node_(1)
#
$node_(0) set X_ 5.0
$node_(0) set Y_ 2.0
$node_(0) set Z_ 0.0

$node_(1) set X_ 390.0
$node_(1) set Y_ 385.0
$node_(1) set Z_ 0.0
```

Figure 5.3: Positioning nodes [22]

For wireless adhoc mobile network nodes are always moving so for node movement following script is used.



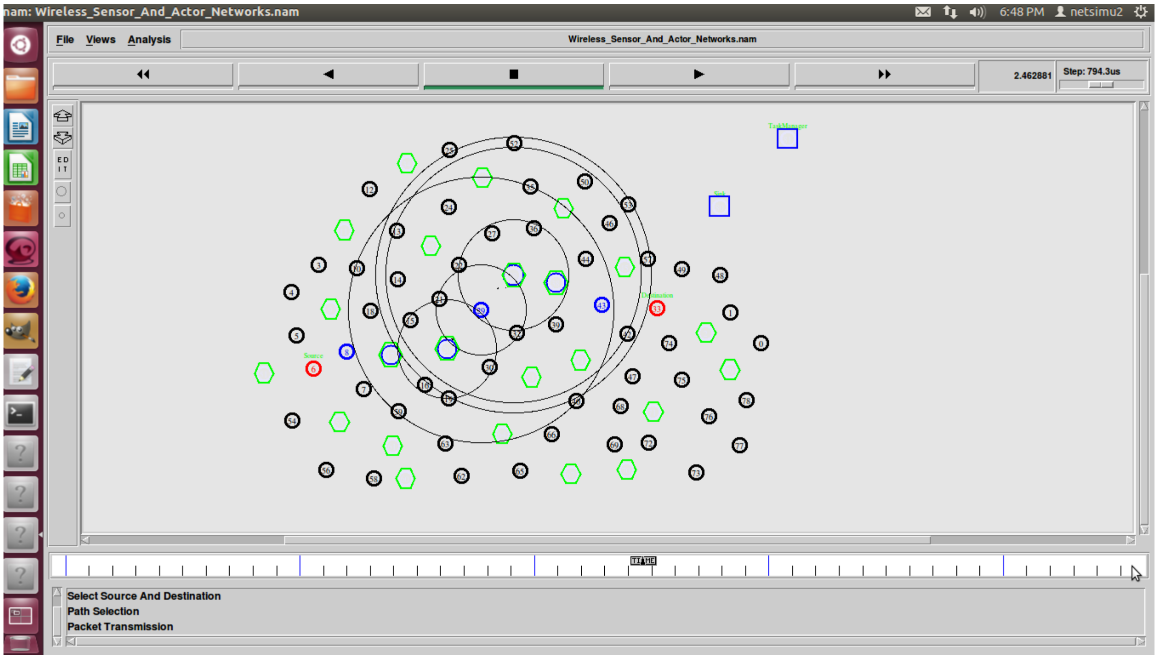
```
#
# Node_(1) starts to move towards node_(0)
#
$ns_ at 50.0 "$node_(1) setdest 25.0 20.0 15.0"
$ns_ at 10.0 "$node_(0) setdest 20.0 18.0 1.0"

# Node_(1) then starts to move away from node_(0)
$ns_ at 100.0 "$node_(1) setdest 490.0 480.0 15.0"
```

Figure 5.4: Node movement [22]

After setting up the network and nodes the communication between the nodes is created as per the type of network either wired or wireless.

5.1.3 Network Animator (NAM):

Network animation is a graphical tool which is used to animate the simulated tcl files in NS2. NAM provides and supports animation of different phenomenons and events of network like placing of nodes, their movement, packet transfer happening between nodes, packet loss, routing etc. the input to NAM is usually the parameter and data provided in a tcl file.


nam: Wireless_Sensor_And_Actor_Networks.nam
6:48 PM
netsimu2
File
Views
Analysis
Wireless_Sensor_And_Actor_Networks.nam
2.462881
Step: 794.3us

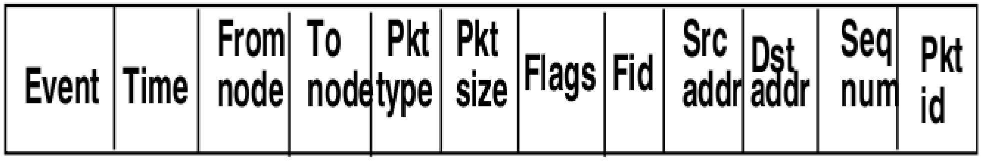
Select Source And Destination
Path Selection
Packet Transmission

Figure 5.5: NAM example [5]

5.2 Tracing

5.2.1 Tracing Objects

When a tcl file is simulated, a trace file is generated. Trace file contains all the information about the packets traversed in the network, when packets are received, types of packets, addresses of sender and receiver, packet id etc. Trace files are helpful in extracting useful information like count of packets, packet drop ratio, packet delivery ratio etc. trace files are in the form of lines. Each line represents an individual packet and each column gives away some unique information about the packet. The format of a trce file line is shown and explained below.



Event	Time	From node	To node	Pkt type	Pkt size	Flags	Fid	Src addr	Dst addr	Seq num	Pkt id

Figure 5.6: Trace file format [17]

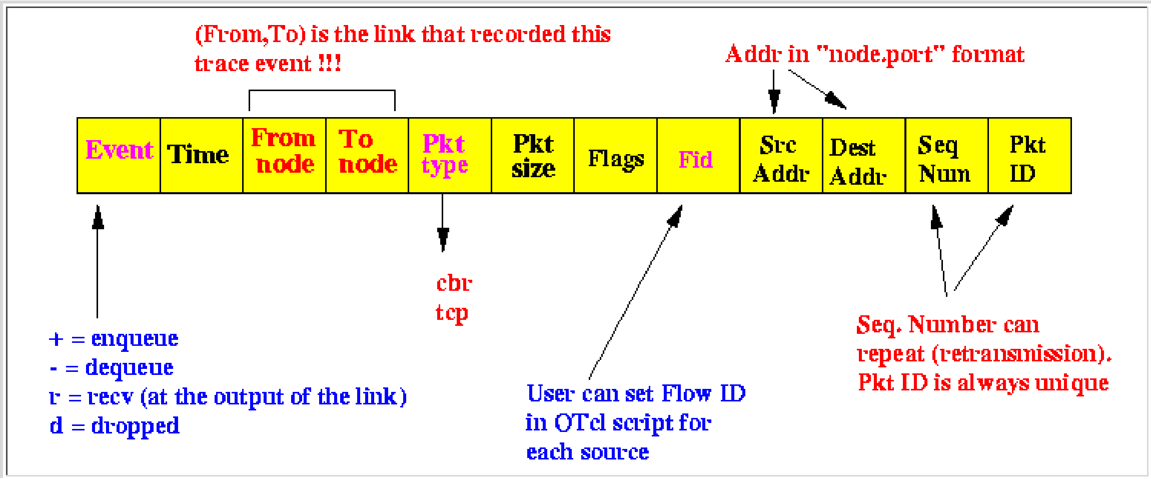
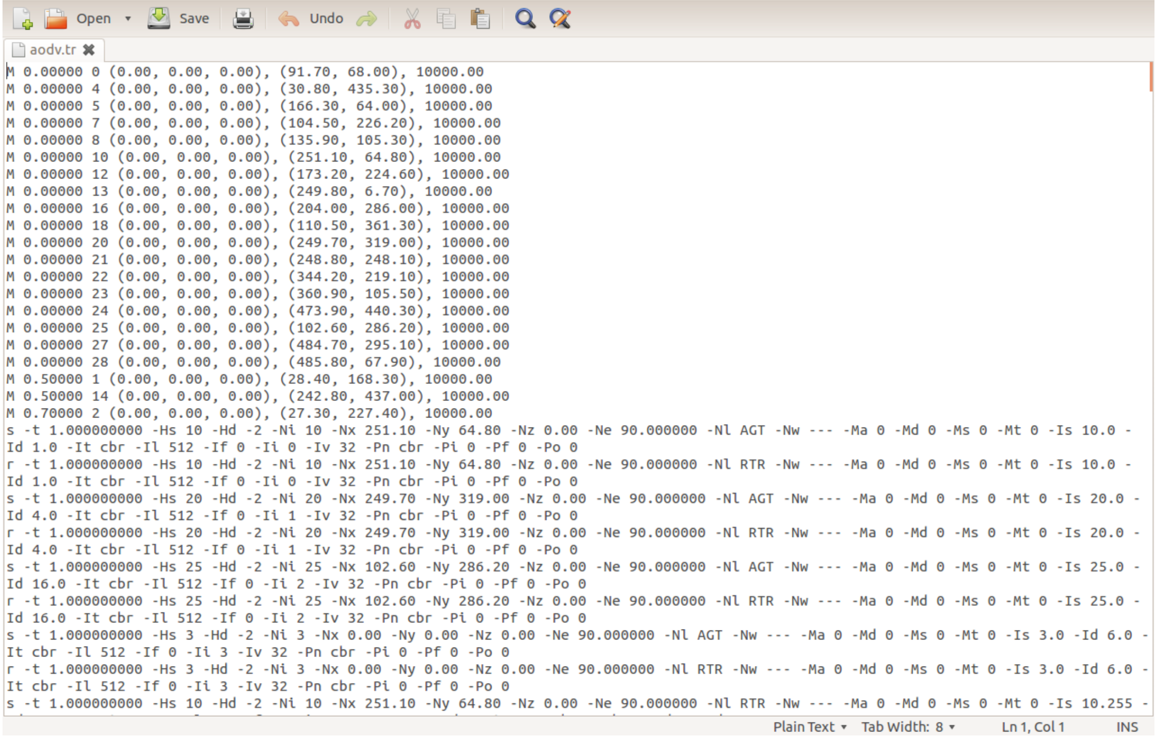

(From,To) is the link that recorded this trace event !!!
Addr in "node.port" format
Event
Time
From node
To node
Pkt type
Pkt size
Flags
Fid
Src Addr
Dest Addr
Seq Num
Pkt ID
cbr
tcp
+ = enqueue
- = dequeue
r = recv (at the output of the link)
d = dropped
User can set Flow ID in OTcl script for each source
Seq. Number can repeat (retransmission).
Pkt ID is always unique

Figure 5.7: Trace file format explained [17]

5.2.2 Structure of Trace files:



```
M 0.00000 0 (0.00, 0.00, 0.00), (91.70, 68.00), 10000.00
M 0.00000 4 (0.00, 0.00, 0.00), (30.80, 435.30), 10000.00
M 0.00000 5 (0.00, 0.00, 0.00), (166.30, 64.00), 10000.00
M 0.00000 7 (0.00, 0.00, 0.00), (104.50, 226.20), 10000.00
M 0.00000 8 (0.00, 0.00, 0.00), (135.90, 105.30), 10000.00
M 0.00000 10 (0.00, 0.00, 0.00), (251.10, 64.80), 10000.00
M 0.00000 12 (0.00, 0.00, 0.00), (173.20, 224.60), 10000.00
M 0.00000 13 (0.00, 0.00, 0.00), (249.80, 6.70), 10000.00
M 0.00000 16 (0.00, 0.00, 0.00), (204.00, 286.00), 10000.00
M 0.00000 18 (0.00, 0.00, 0.00), (110.50, 361.30), 10000.00
M 0.00000 20 (0.00, 0.00, 0.00), (249.70, 319.00), 10000.00
M 0.00000 21 (0.00, 0.00, 0.00), (248.80, 248.10), 10000.00
M 0.00000 22 (0.00, 0.00, 0.00), (344.20, 219.10), 10000.00
M 0.00000 23 (0.00, 0.00, 0.00), (360.90, 105.50), 10000.00
M 0.00000 24 (0.00, 0.00, 0.00), (473.90, 440.30), 10000.00
M 0.00000 25 (0.00, 0.00, 0.00), (102.60, 286.20), 10000.00
M 0.00000 27 (0.00, 0.00, 0.00), (484.70, 295.10), 10000.00
M 0.00000 28 (0.00, 0.00, 0.00), (485.80, 67.90), 10000.00
M 0.50000 1 (0.00, 0.00, 0.00), (28.40, 168.30), 10000.00
M 0.50000 14 (0.00, 0.00, 0.00), (242.80, 437.00), 10000.00
M 0.70000 2 (0.00, 0.00, 0.00), (27.30, 227.40), 10000.00
s -t 1.000000000 -Hs 10 -Hd -2 -Ni 10 -Nx 251.10 -Ny 64.80 -Nz 0.00 -Ne 90.000000 -Nl AGT -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 10.0 -
Id 1.0 -It cbr -Il 512 -If 0 -Ii 0 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
r -t 1.000000000 -Hs 10 -Hd -2 -Ni 10 -Nx 251.10 -Ny 64.80 -Nz 0.00 -Ne 90.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 10.0 -
Id 1.0 -It cbr -Il 512 -If 0 -Ii 0 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
s -t 1.000000000 -Hs 20 -Hd -2 -Ni 20 -Nx 249.70 -Ny 319.00 -Nz 0.00 -Ne 90.000000 -Nl AGT -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 20.0 -
Id 4.0 -It cbr -Il 512 -If 0 -Ii 1 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
r -t 1.000000000 -Hs 20 -Hd -2 -Ni 20 -Nx 249.70 -Ny 319.00 -Nz 0.00 -Ne 90.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 20.0 -
Id 4.0 -It cbr -Il 512 -If 0 -Ii 1 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
s -t 1.000000000 -Hs 25 -Hd -2 -Ni 25 -Nx 102.60 -Ny 286.20 -Nz 0.00 -Ne 90.000000 -Nl AGT -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 25.0 -
Id 16.0 -It cbr -Il 512 -If 0 -Ii 2 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
r -t 1.000000000 -Hs 25 -Hd -2 -Ni 25 -Nx 102.60 -Ny 286.20 -Nz 0.00 -Ne 90.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 25.0 -
Id 16.0 -It cbr -Il 512 -If 0 -Ii 2 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
s -t 1.000000000 -Hs 3 -Hd -2 -Ni 3 -Nx 0.00 -Ny 0.00 -Nz 0.00 -Ne 90.000000 -Nl AGT -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 3.0 -Id 6.0 -
It cbr -Il 512 -If 0 -Ii 3 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
r -t 1.000000000 -Hs 3 -Hd -2 -Ni 3 -Nx 0.00 -Ny 0.00 -Nz 0.00 -Ne 90.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 3.0 -Id 6.0 -
It cbr -Il 512 -If 0 -Ii 3 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
s -t 1.000000000 -Hs 10 -Hd -2 -Ni 10 -Nx 251.10 -Ny 64.80 -Nz 0.00 -Ne 90.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 10.255 -
```

Figure 5.8: Trace file sample [17]

1. The principal field is event.It gives you four conceivable images "+" '- " "r" 'd'.These four images compare separately to enqueued, dequeued, got and dropped.

2. The second field gives the time at which the occasion happens

3. The third field gives you the info hub of the connection at which the occasion happens

4. The fourth field gives you the yield hub at which the occasion happens

5. The fifth field demonstrates the data about the parcel type.i.e whether the bundle is UDP or TCP

6. The 6th field gives the parcel size

7. The seventh field give data about a few banners

8. The eight field is the stream id(fid) for IPv6 that a client can set for every stream in a tcl script.It is additionally utilized for determining the shade of stream in NAM show

9. The ninth field is the source address

10. The tenth field is the destination address

11. The eleventh field is the system layer convention's parcel arrangement number

12. The last field demonstrates the remarkable id of bundle

5.3 AWK:

The fundamental capacity of awk is to look documents for lines (or different units of content) that contain certain examples. At the point when a line matches one of the examples, awk performs indicated activities on that line. awk keeps on preparing information lines along these lines until it achieves the end of the info documents. An arrangement of moves to be made against floods of printed information for removing particular information containing aspecific design.

5.3.1 Structure of AWK projects

"AWK is a dialect for preparing content documents. A document is dealt with as an arrangement of records, and of course every line is a record. Every line is separated into a grouping of fields, so we can think about the principal word in a line as the primary field, the second word as the second field, et cetera. An AWK system is a grouping of example activity articulations. AWK peruses the info a line at once. A line is checked for every example in the system, and for every example that matches, the related activity is executed." - Alfred V. Aho[8] The info is part into records, where of course records are isolated by newline characters so that the information is part into lines. The project tests every record against each of the conditions thus, and executes the activity for every expression that is valid.

AWK Scripts are great in preparing the information from the log (follow records) which we get from NS2.

CHAPTER 6: PROPOSED METHODOLOGY

Defense methodologies in networking are based upon three stages, prevention, detection and mitigation. The basic focus of any defense mechanism should be to come up with a solution which is effective, fast and poses minimal overhead on network and resources. While researching the previously used techniques it was noticed that all of them were complex and time consuming, while we wanted to focus on a simple technique exploiting simple facts about network and taking advantage of the knowledge that every vehicle has sufficient supply of battery power of its own which can be used to run necessary algorithm.

6.1 Main Idea:

As it is explained, DDoS attacks are all about flooding malicious packets to a victim by multiple attackers. Every node in the network has a specific capacity to receive the incoming packets and store them in its buffer to deal with the. In normal traffic scenarios the packets received by a node never cross the receiver's buffer and hence a node is able to deal with all the incoming legitimate requests conveniently. In DDOS attack a group of attackers will target a common victim and will start sending dummy messages to it on a large scale. these messages are requests to initiate a connection with victim but as the attacker doesn't wish to initiate a proper connection with victim, so all these requests are kept pending without any further response from attackers while victim is still waiting for it and during this wait, is unable to entertain upcoming legitimate request packets.

As the main point here is that abnormaly large number of packets are the distinctive feature between an attacker and a normal node so why not identify the attacker by keeping a check on the number of packets sent by a node, or a potential attacker?.

In our proposed scheme we are simply counting the number of packets sent by any node in the network to judge that whether its a malicious node or a normal one.

Here we are cosidering the advantage of better battery power resource as the nodes in this case are vehicles. So we can use an algorithm which can run on the OBU of every vehicle continously to detect an attacker. The sufficient battery power of vehicles make it praticaly possible to run algorithms on board with minimum or no overhead on network.

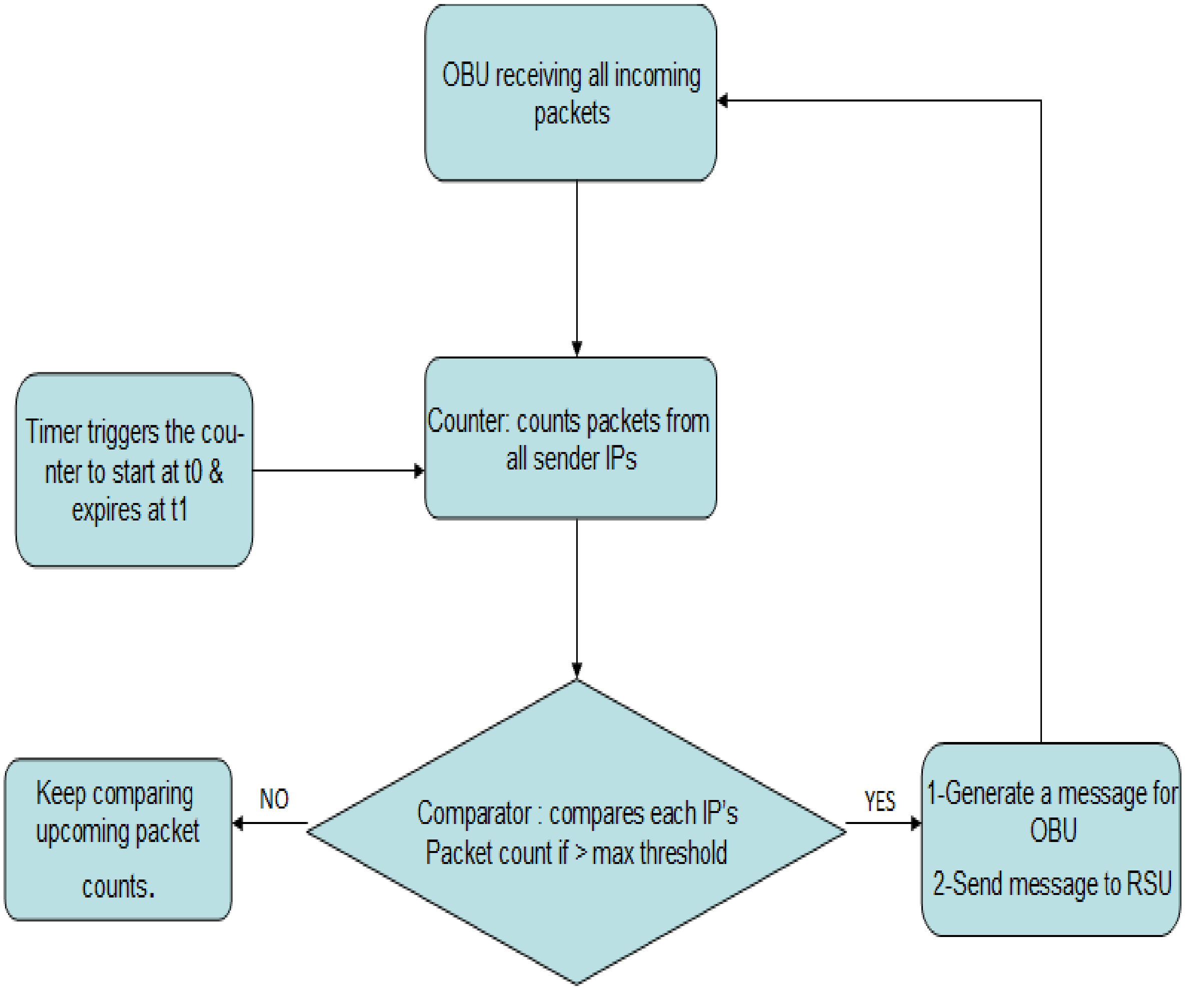

OBU receiving all incoming packets
Timer triggers the cou-nter to start at t0 & expires at t1
Counter: counts packets from all sender IPs
Keep comparing upcoming packet counts.
NO
Comparator : compares each IP's Packet count if > max threshold
YES
1-Generate a message for OBU
2-Send message to RSU

Figure 6.1 : Flow chart of proposed methodology

Lets consider a random vehicle ‘x’ in VANET, the OBU on x is recieving request messages from multiple Ips (other vehicles) in the network at the same time. The buffer of x will recieve these request messages and will process them and will take required action against them.

6.2 Designed Methodology:

Now as per the designed scheme each OBU on vehicles is modified to have some additional components and features. A counter and timer is integrated with OBU.

This counter takes input from a timer, that triggers the counter to start counting at time t0 and then stops/restarts when a particular time interval is over, in our case this time interval is of 10 seconds.

Now when an OBU recieves packets from any neighbouring node, timer will trigger the counter to start and in these 10 seconds counter will count the packets sent by every sender to that particular vehicle and forwards that packet count of each IP to the comparator. Note that OBU holds information that which packets are coming from which IP. After counting packets for 10 seconds the counter will restart to count the upcoming packets. The comparator's job is to compare the packet count sent in that time period, of each sender IP with a max threshold value. This max threshold value is obtained from normal traffic scenario.

On comparison with the threshold value if comparartor finds that the count of packets from any IP esxceeds the threshold value it will pass that sender's id to the "alarm message module". This module is required to do two tasks, it will send a message to vehicle's OBU to immediately terminate any sort of communication with that malicious IP and also sends a message to RSU to alarm it about the attacker node so that the RSU sends a message to all the vehicles in the netwok in advance, to not to initiate communication with attacker IP.

So in every adjacent 10 seconds this check is made and communication with malicious nodes is terminated.

6.3 Implementation:

The platform used to implement this technique is NS2.35. Given below is the TCL file of the main code that comprises of network establishment, DDOS attack, defense technique and results representations.

```
#
======================================================================
=======
# Define options
#
======================================================================
=======
set val(chan)       Channel/WirelessChannel  ;# channel type
set val(prop)       Propagation/TwoRayGround ;# radio-propagation model
set val(ant)        Antenna/OmniAntenna      ;# Antenna type
set val(ll)         LL                       ;# Link layer type
set val(ifq)        Queue/DropTail/PriQueue  ;# Interface queue type
set val(ifqlen)     50                       ;# max packet in ifq
set val(netif)      Phy/WirelessPhy          ;# network interface type
set val(mac)        Mac/802_11               ;# MAC type
set val(rp)         AODV                     ;# ad-hoc routing protocol
set val(nn)         30                       ;# number of mobilenodes
set val(x)                1400                         ;#X dimension to topography
set val(y)                1600                 ;#X dimension to topography
set val(stop)             10
#-------Event scheduler object creation--------#

set ns [new Simulator]
# Creating trace file and nam file

set tracefd [open wireless1.tr w]
set namtrace [open wireless1.nam w]


$ns trace-all $tracefd
$ns namtrace-all-wireless $namtrace $val(x) $val(y)

# set up topography object
set topo [new Topography]
$topo load_flatgrid $val(x) $val(y)

set god_ [create-god $val(nn)]



# configure the nodes
        $ns node-config -adhocRouting $val(rp) \
                   -llType $val(ll) \
                   -macType $val(mac) \
                   -ifqType $val(ifq) \
                   -ifqLen $val(ifqlen) \
                   -antType $val(ant) \
                   -propType $val(prop) \
                   -phyType $val(netif) \
                   -channelType $val(chan) \
                   -topoInstance $topo \
                   -agentTrace ON \
                   -routerTrace ON \
                   -macTrace OFF \
                   -movementTrace ON

## Creating node objects...
for {set i 0} {$i < $val(nn) } { incr i } {
          set node_($i) [$ns node]
     }
     for {set i 0} {$i < $val(nn)  } {incr i } {
          $node_($i) color black
          $ns at 0.0 "$node_($i) color black"
     }

# Provide initial location of mobile nodes
$node_(0) set X_ 550.0
$node_(0) set Y_ 150.0
$node_(0) set Z_ 0.0

$node_(1) set X_ 550.0
$node_(1) set Y_ 300.0
$node_(1) set Z_ 0.0

$node_(2) set X_ 550.0
$node_(2) set Y_ 400.0
$node_(2) set Z_ 0.0

$node_(3) set X_ 550.0
$node_(3) set Y_ 550.0
$node_(3) set Z_ 0.0

$node_(4) set X_ 450.0
$node_(4) set Y_ 650.0
$node_(4) set Z_ 0.0

$node_(5) set X_ 300.0
$node_(5) set Y_ 650.0
$node_(5) set Z_ 0.0
.
.
.
```

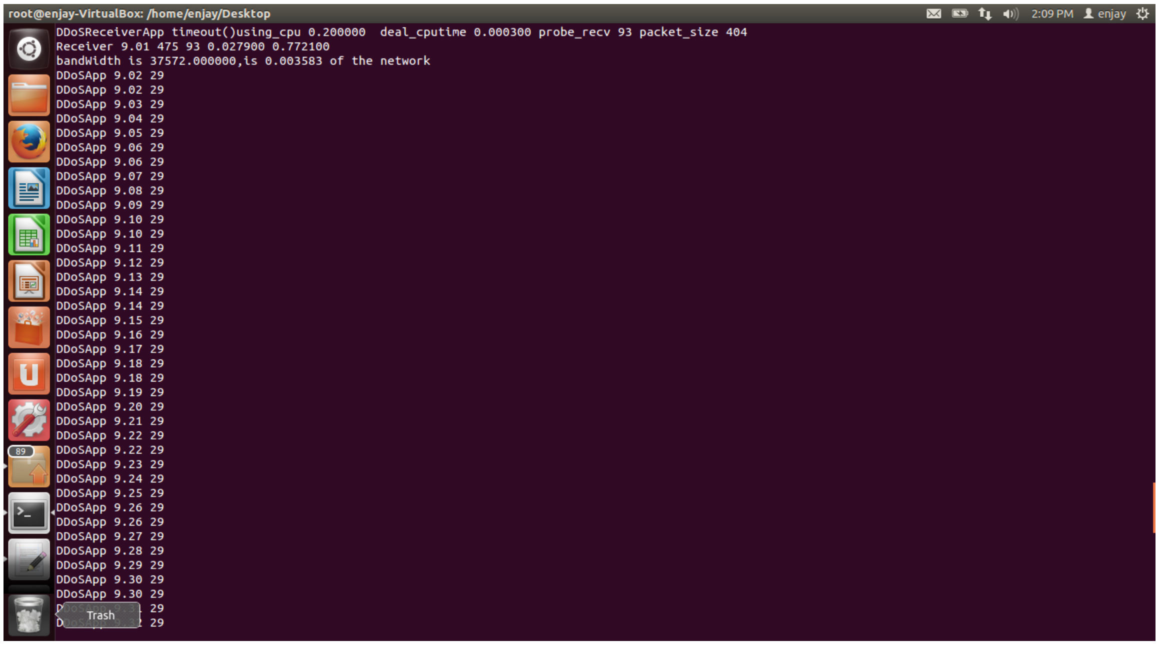
```
.
.
.
.
.
.
.
$node_(26) set X_ 50.0 #vehicle
$node_(26) set Y_ 800.0
$node_(26) set Z_ 0.0


$node_(27) set X_ 50.0 #vehicle
$node_(27) set Y_ 750.0
$node_(27) set Z_ 0.0


$node_(28) set X_ 1350.0 #vehicle
$node_(28) set Y_ 800.0
$node_(28) set Z_ 0.0


$node_(29) set X_ 700.0 #vehicle
$node_(29) set Y_ 1600.0
$node_(29) set Z_ 0.0
$node_(29) color red




# node movement
$node_(25) color blue
$ns at 0.0 "$node_(25) color blue"
$ns at 0.5 "$node_(25) setdest 700.0 850.0 400.0"
$ns at 2.0 "$node_(25) setdest 700.0 1500.0 400.0"

$node_(26) color blue
$ns at 0.0 "$node_(26) color blue"
$ns at    0.5 "$node_(26) setdest 700.0 800.0 300.0"
$ns at 2.0 "$node_(26) setdest 1350.0 800.0 400.0"

$node_(27) color blue
$ns at 0.0 "$node_(27) color blue"
$ns at 0.5 "$node_(27) setdest 700.0 750.0 450.0"
$ns at 2.0 "$node_(27) setdest 700.0 100.0 400.0"
```

```
$node_(28) color blue
$ns at 0.0 "$node_(28) color blue"
$ns at 0.5 "$node_(28) setdest 700.0 800.0 300.0"
$ns at 2.6 "$node_(28) setdest 700.0 50.0 400.0"

$node_(29) color blue
$ns at 0.0 "$node_(29) color blue"
$ns at 0.5 "$node_(29) setdest 700.0 50.0 500.0"

#===================================DOS
Portion=================================
set an_id [expr $val(nn) - 3]
set ad [expr $val(nn) - 1]
set p_size 404
set probing_port 80
set thr 1
set sendTime 1

#1st sender node number 28
set i 28

   set a1 [new Agent/MessagePassing]
   $node_($i) attach $a1 $probing_port
   set w($i) [new Application/DDoS/Sender]
   $w($i) re-addr $an_id 80
   $w($i) re-addr $ad 80
   $w($i) scan-arg $sendTime $p_size
   $w($i) threads $thr
   $w($i) time-step 0.008
   $w($i) attach-agent $a1
   $ns at 4.0 "$w($i) start"
   $ns at 1.5 "$w($i) stop"
#2nd sender node number 29
 set j 29

   set a2 [new Agent/MessagePassing]
   $node_($j) attach $a2 $probing_port
   set w($j) [new Application/DDoS/Sender]
   $w($j) re-addr $an_id 80
   $w($j) re-addr $ad 80
   $w($j) scan-arg $sendTime $p_size
   $w($j) threads $thr
   $w($j) time-step 0.008
   $w($j) attach-agent $a2
   $ns at 4.0 "$w($j) start"
   $ns at 1.5 "$w($j) stop"
```

```
set dealTime 0.0003
set CPU 0.8

#Receiver Node 27
set a3 [new Agent/MessagePassing]
$node_($an_id) attach $a3 $probing_port
set w($an_id) [new Application/DDoS/Receiver]
$w($an_id) attach-agent $a3
$w($an_id) cpu $dealTime $CPU
$w($an_id) bandwidth 10485760
$w($an_id) port $probing_port
$w($an_id) down-time 60
$w($an_id) p-size 404
$w($an_id) time-step 1
$w($an_id) times 1

 # Define node initial position in nam
for {set i 0} {$i < $val(nn)} { incr i } {
$ns initial_node_pos $node_($i) 30
}

# Telling nodes when the simulation ends
for {set i 0} {$i < $val(nn) } { incr i } {
    $ns at $val(stop) "$node_($i) reset";
}

# Ending nam and the simulation
$ns at $val(stop) "$ns nam-end-wireless $val(stop)"
$ns at $val(stop) "stop"
$ns at 10.1 "puts \"end simulation\"; $ns halt"
#==============================Xgraph=========================
==============
#set f0 [open out0.tr w]

#stop procedure:
proc stop {} {
    global ns tracefd namtrace f0
    $ns flush-trace
    close $tracefd
    close $namtrace

 #close $f0
#       close $f1
 #      close $f2
```

```
        #Call xgraph to display the results
            exec awk -f 1.awk wireless1.tr > out.tr
            exec awk -f 2.awk out.tr > final.tr
        exec xgraph final.tr -geometry 800x400 &
exec nam wireless1.nam &
}

$ns run
```

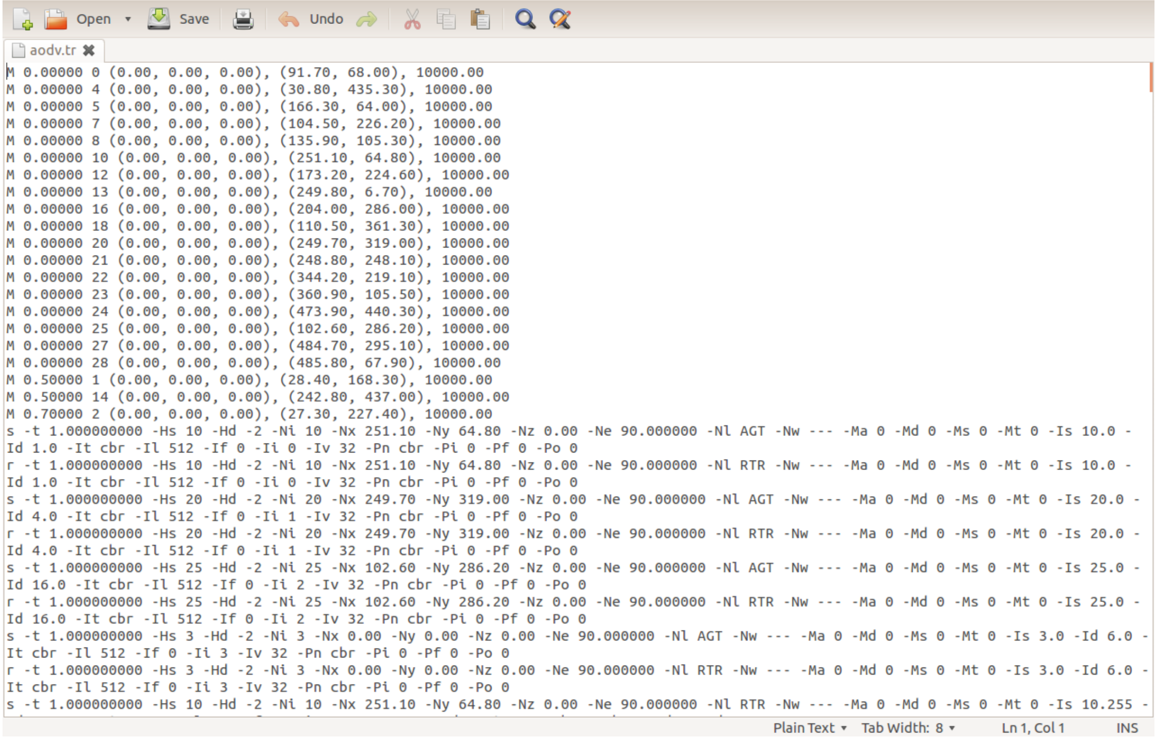
6.4 Results:



```
root@enjay-VirtualBox: /home/enjay/Desktop
DDoSReceiverApp timeout()using_cpu 0.200000  deal_cputime 0.000300 probe_recv 93 packet_size 404
Receiver 9.01 475 93 0.027900 0.772100
bandWidth is 37572.000000,is 0.003583 of the network
DDoSApp 9.02 29
DDoSApp 9.02 29
DDoSApp 9.03 29
DDoSApp 9.04 29
DDoSApp 9.05 29
DDoSApp 9.06 29
DDoSApp 9.06 29
DDoSApp 9.07 29
DDoSApp 9.08 29
DDoSApp 9.09 29
DDoSApp 9.10 29
DDoSApp 9.10 29
DDoSApp 9.11 29
DDoSApp 9.12 29
DDoSApp 9.13 29
DDoSApp 9.14 29
DDoSApp 9.14 29
DDoSApp 9.15 29
DDoSApp 9.16 29
DDoSApp 9.17 29
DDoSApp 9.18 29
DDoSApp 9.18 29
DDoSApp 9.19 29
DDoSApp 9.20 29
DDoSApp 9.21 29
DDoSApp 9.22 29
DDoSApp 9.22 29
DDoSApp 9.23 29
DDoSApp 9.24 29
DDoSApp 9.25 29
DDoSApp 9.26 29
DDoSApp 9.26 29
DDoSApp 9.27 29
DDoSApp 9.28 29
DDoSApp 9.29 29
DDoSApp 9.30 29
DDoSApp 9.30 29
DDoSApp 9.31 29
DDoSApp 9.32 29
```

Figure 6.2: Results

Above shown is the screenshot of the terminal window showing the results obtained when the code was run. In the screenshot we can see DDOS attack being launched.



```
M 0.00000 0 (0.00, 0.00, 0.00), (91.70, 68.00), 10000.00
M 0.00000 4 (0.00, 0.00, 0.00), (30.80, 435.30), 10000.00
M 0.00000 5 (0.00, 0.00, 0.00), (166.30, 64.00), 10000.00
M 0.00000 7 (0.00, 0.00, 0.00), (104.50, 226.20), 10000.00
M 0.00000 8 (0.00, 0.00, 0.00), (135.90, 105.30), 10000.00
M 0.00000 10 (0.00, 0.00, 0.00), (251.10, 64.80), 10000.00
M 0.00000 12 (0.00, 0.00, 0.00), (173.20, 224.60), 10000.00
M 0.00000 13 (0.00, 0.00, 0.00), (249.80, 6.70), 10000.00
M 0.00000 16 (0.00, 0.00, 0.00), (204.00, 286.00), 10000.00
M 0.00000 18 (0.00, 0.00, 0.00), (110.50, 361.30), 10000.00
M 0.00000 20 (0.00, 0.00, 0.00), (249.70, 319.00), 10000.00
M 0.00000 21 (0.00, 0.00, 0.00), (248.80, 248.10), 10000.00
M 0.00000 22 (0.00, 0.00, 0.00), (344.20, 219.10), 10000.00
M 0.00000 23 (0.00, 0.00, 0.00), (360.90, 105.50), 10000.00
M 0.00000 24 (0.00, 0.00, 0.00), (473.90, 440.30), 10000.00
M 0.00000 25 (0.00, 0.00, 0.00), (102.60, 286.20), 10000.00
M 0.00000 27 (0.00, 0.00, 0.00), (484.70, 295.10), 10000.00
M 0.00000 28 (0.00, 0.00, 0.00), (485.80, 67.90), 10000.00
M 0.50000 1 (0.00, 0.00, 0.00), (28.40, 168.30), 10000.00
M 0.50000 14 (0.00, 0.00, 0.00), (242.80, 437.00), 10000.00
M 0.70000 2 (0.00, 0.00, 0.00), (27.30, 227.40), 10000.00
s -t 1.000000000 -Hs 10 -Hd -2 -Ni 10 -Nx 251.10 -Ny 64.80 -Nz 0.00 -Ne 90.000000 -Nl AGT -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 10.0 -
Id 1.0 -It cbr -Il 512 -If 0 -Ii 0 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
r -t 1.000000000 -Hs 10 -Hd -2 -Ni 10 -Nx 251.10 -Ny 64.80 -Nz 0.00 -Ne 90.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 10.0 -
Id 1.0 -It cbr -Il 512 -If 0 -Ii 0 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
s -t 1.000000000 -Hs 20 -Hd -2 -Ni 20 -Nx 249.70 -Ny 319.00 -Nz 0.00 -Ne 90.000000 -Nl AGT -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 20.0 -
Id 4.0 -It cbr -Il 512 -If 0 -Ii 1 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
r -t 1.000000000 -Hs 20 -Hd -2 -Ni 20 -Nx 249.70 -Ny 319.00 -Nz 0.00 -Ne 90.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 20.0 -
Id 4.0 -It cbr -Il 512 -If 0 -Ii 1 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
s -t 1.000000000 -Hs 25 -Hd -2 -Ni 25 -Nx 102.60 -Ny 286.20 -Nz 0.00 -Ne 90.000000 -Nl AGT -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 25.0 -
Id 16.0 -It cbr -Il 512 -If 0 -Ii 2 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
r -t 1.000000000 -Hs 25 -Hd -2 -Ni 25 -Nx 102.60 -Ny 286.20 -Nz 0.00 -Ne 90.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 25.0 -
Id 16.0 -It cbr -Il 512 -If 0 -Ii 2 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
s -t 1.000000000 -Hs 3 -Hd -2 -Ni 3 -Nx 0.00 -Ny 0.00 -Nz 0.00 -Ne 90.000000 -Nl AGT -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 3.0 -Id 6.0 -
It cbr -Il 512 -If 0 -Ii 3 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
r -t 1.000000000 -Hs 3 -Hd -2 -Ni 3 -Nx 0.00 -Ny 0.00 -Nz 0.00 -Ne 90.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 3.0 -Id 6.0 -
It cbr -Il 512 -If 0 -Ii 3 -Iv 32 -Pn cbr -Pi 0 -Pf 0 -Po 0
s -t 1.000000000 -Hs 10 -Hd -2 -Ni 10 -Nx 251.10 -Ny 64.80 -Nz 0.00 -Ne 90.000000 -Nl RTR -Nw --- -Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 10.255 -
```

Figure 6.3 : Resulting tracefile

A screenshot of trace file generated is shown above. This trace file gives away complete information about packets being traversed in the network, both malicious and normal ones.

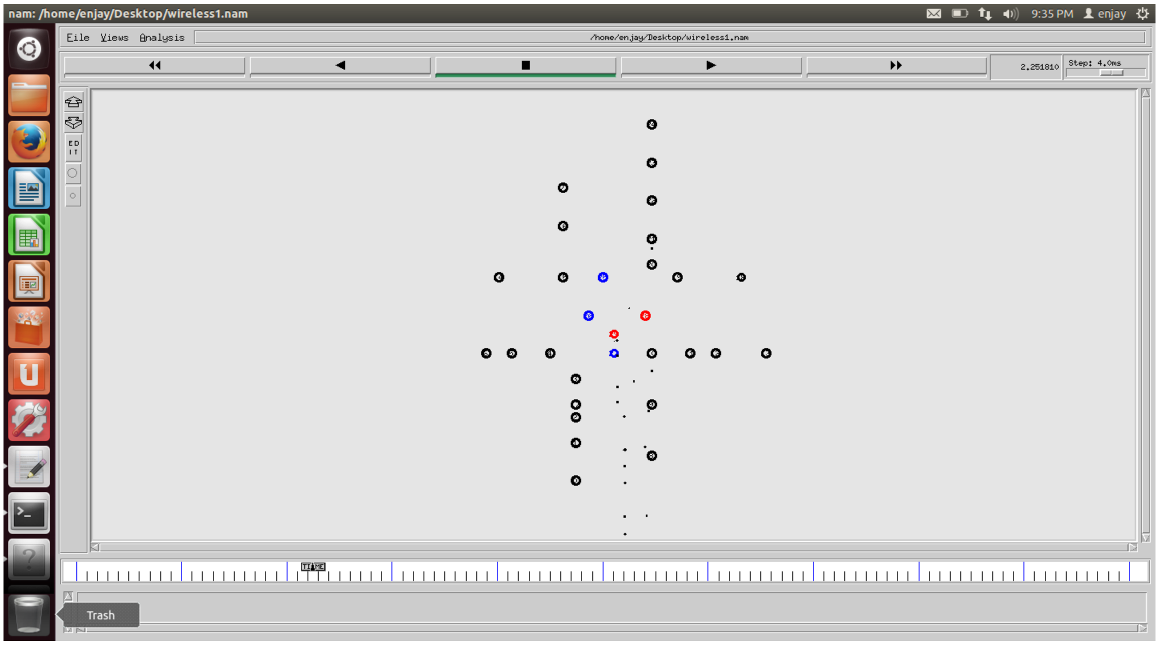
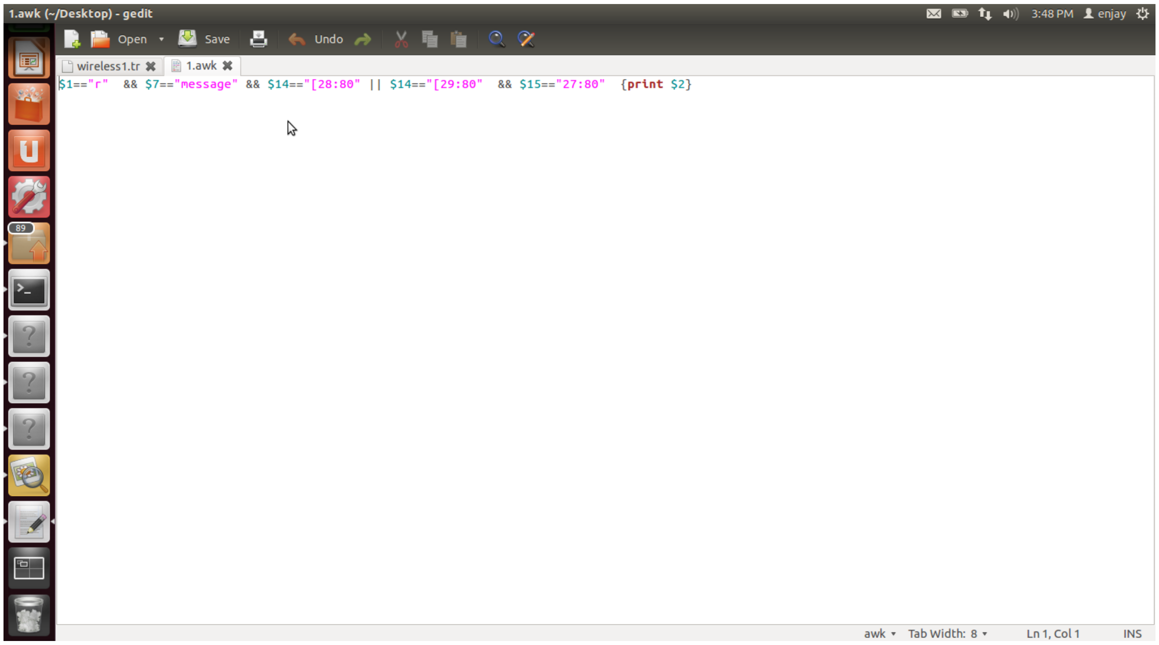

nam: /home/enjay/Desktop/wireless1.nam
9:35 PM
enjay
File
Views
Analysis
/home/enjay/Desktop/wireless1.nam
2.251810
Step: 4.0ms
Trash

Figure 6.4 : Resulting NAM file

In figure animation of the simulated tcl code is shown. We can see from the graphical presentation that there are 25 vehicles configured as RSUs, in black color and 5 as vehicles. The blue nodes represent non malicious nodes and red ones are attacker vehicles.

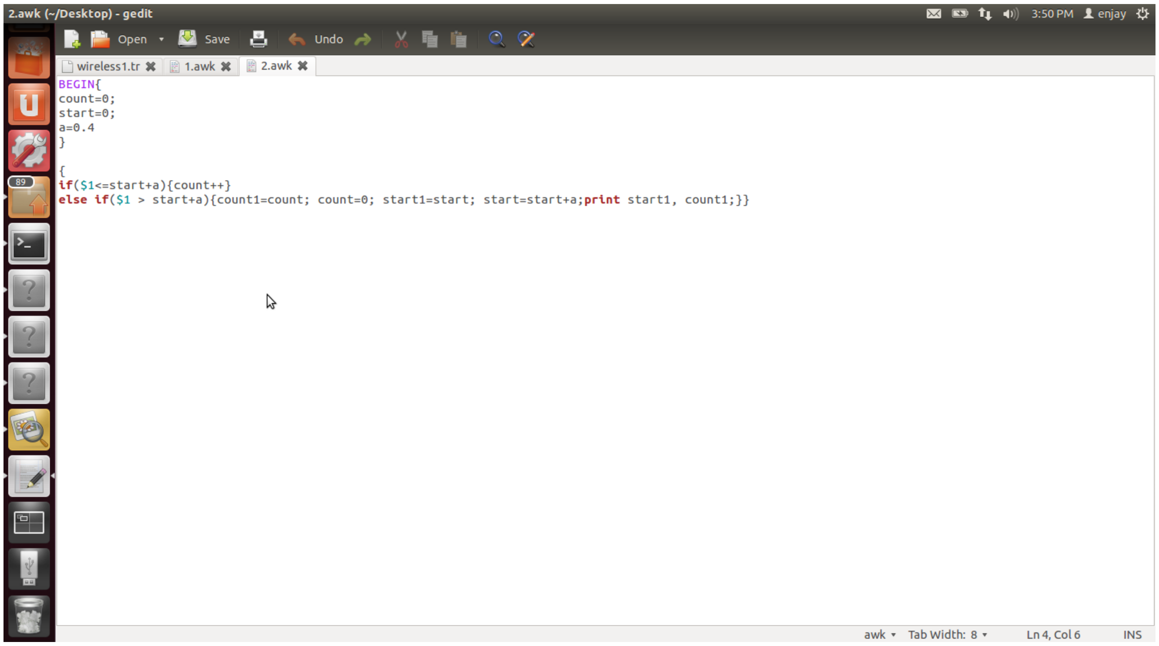
After the simulation of the proposed algorithm in the network, awk scripts are applied on resulting trace files to extract the desired information from the network i-e the number of packets traversing in the network prior to, during and after attack, packet delivery ratio etc.

Following are the screenshots of the actual awk scripts used to extract and count the number of packets received at victim node sent by attacking nodes and normal nodes.



```
$1=="r"  && $7=="message" && $14=="[28:80" || $14=="[29:80"  && $15=="27:80"  {print $2}
```

Figure 6.5 : awk 1



```
BEGIN{
count=0;
start=0;
a=0.4
}

{
if($1<=start+a){count++}
else if($1 > start+a){count1=count; count=0; start1=start; start=start+a;print start1, count1;}}
```

Figure 6.6 : awk 2

Using the information given by trace files following results are obtained which show the efficiency of defense algorithm.

In figure 6.7 it is evident that with the increasing number of attackers the number of flooding increases but the proposed method is capable of minimizing the flooding more efficiently than the base paper's defense mechanism..

In figure 6.8 the count of packets in the network is given vs the simulation time. It can be seen that before the attack was launched at t=4 sec the number of packets in the network was according to the normal communication between the nodes. At t=4 when the attack is launched we can see a sudden and a huge increase in traffic resulting in a sharp peak but within few seconds the packet count was reduced back to a reasonable number as the proposed algorithm defended the attack

6.5 Simulation Results:

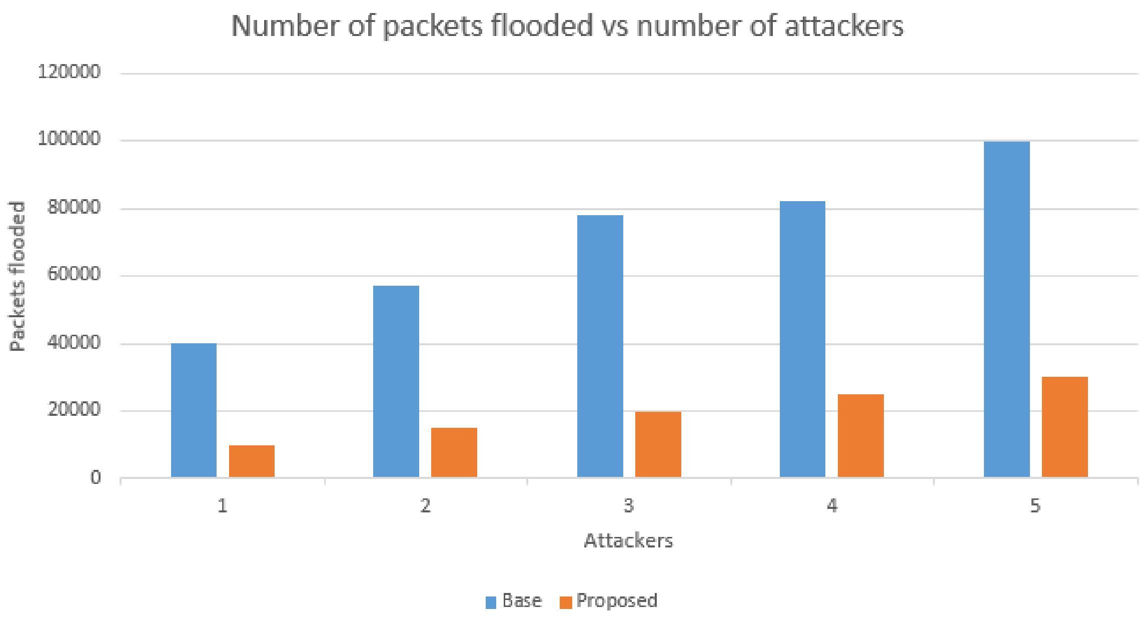


Figure 6.7: Comparison between base & proposed method’s efficiency.

.

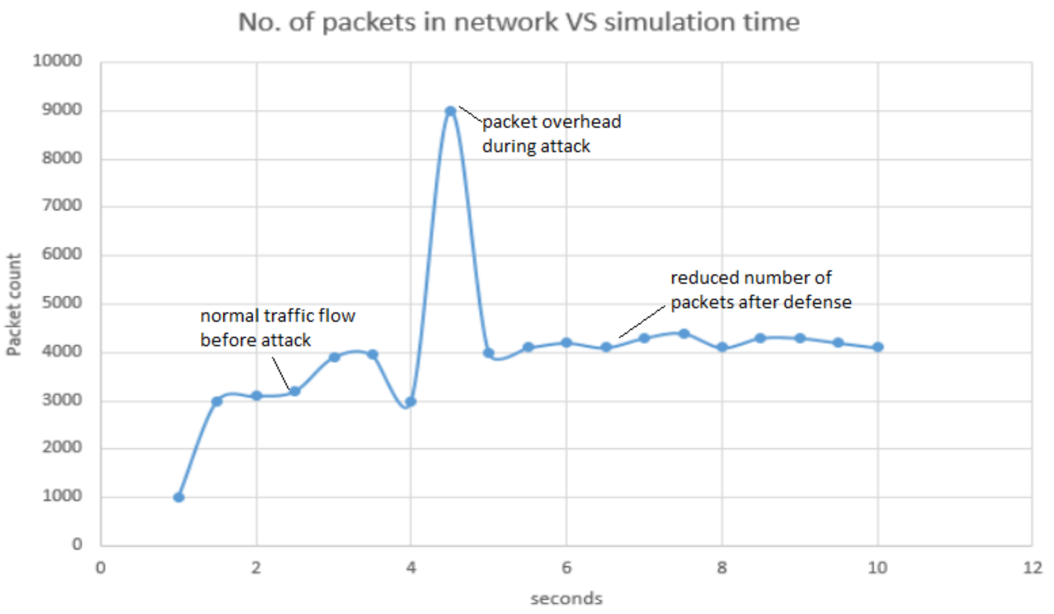


Figure 6.8 : Approx. number of packets in the network during the simulation time.

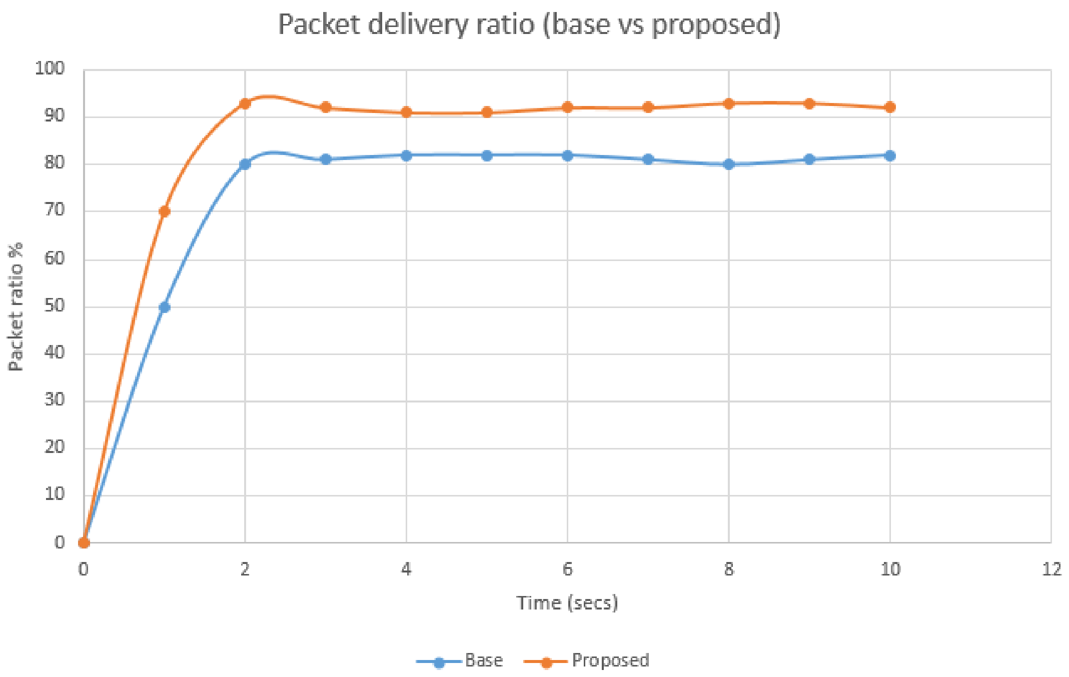


Figure 6.9 : Comparison between packet delivery ratio of proposed and existing defense mechanisms.

In figure 6.9 the packet delivery ratio is shown. It can be noticed that the packet delivery ratio of proposed algorithm is better than the existing algorithm.

CHAPTER 7: CONCLUSION AND FUTURE WORK

7.1 Conclusion:

Though VANET will proved to be a promising technology in the domain of intelligent transportation systems but its unfortunate that not much work has been done on its security issue. Though many solutions have been already proposed but almost none of them was taken seriously enough to be worked upon extensively and hence all of them lie in the research phase yet. As mentioned earlier that researchers have a huge advantage regarding power restraints in VANET as vehicles have their own independent battery power making it possible for on board computations, be it about security algorithms or else.

There are many aspects of VANET nature which make it difficult to apply conventional security techniques. Specially the fact that still flooding is the most common way to broadcast messages between nodes hop makes it a hard task to differentiate between legitimate or malicious traffic.

Our target while working on this thesis was to propose a solution which focuses on the advantages that we have in VANET and utilize them. Moreover to come up with a solution which is as simple as it can get. Our proposed solution poses minimal overhead on network. As our methodology exploits a very basic fact about DDOS attack i-e flooding so complication are reduced on contarary to techniques like cryptography etc.

Our methodology is a ground level idea, if proper work is done on it, it can prove to be an actual defense mechanism in practical security scenarios.

7.2 Future Work:

In future VANET are expected to be a major phenomenon in intelligent transportation and will be integrated to modern automobile industry. The need of security mechanisms will grow likewise. The scope of advancement in our proposed methodology is high. It needs to be scaled and checked on a large network. In coming days as VANET will mature and new modifications are made in it, new ways will be opened for security mechanism. We plan to make our algo more efficient and scalable to a large network.

BIBLIOGRAPHY

[1]. Mohamed Nidhal Mari, Jalel Ben-Othman and Mohamed Hamdi , “Survey on VANET security challenges and possible cryptographic solutions”, Vehicular communications: Elsevier, 2014.

[2]. Rainer Bauman, “Vehicular Adhoc network (VANET)”, Master’s thesis, 2004.

[3]. Jose Maria de Fuentis, Ana Isabel Gonzalez-Tablas and Arturo Ribagorda, “Overview of security issues in Vehicular Adhoc networks”, publishes in Handbook of research on mobility and computing, 2010.

[4]. Ghassan Samara, Wafaa A.H. Al-Salihy and R.Sures, “Security analysis of Vehicular Adhoc networks (VANET)”, in Second international conference on network application, protocol and services, 2010.

[5]. Sherali Zeadally et al., “Vehicular Adhoc networks (VANETs); status, results and challenges”, Springer Science and Buisness Media, 2010.

[6]. Ram Shringar Raw, Manish Kumar and Nanhay Singh, “Security challenges, issues and their solutions for VANET”, International Journal of network security and its application (IJNSA), Vol. 5, Sept 2013.

[7]. Vishal Kumar, Shailendra Mishra and Narottam Chand, “Applications of VANETs: Present and future”, Scientific research, communication and network, Feb 2013.

[8]. Jagadeesh Kakarla, S Siva Sathya, B Govinda Laxmi and Ramesh Babu B, “A survey on routing protocols and its issues in VANET”, International journal of computer applications, Vol. 28-No. 4, August 2011.

[9]. Pino Caballero-Gil (2011). Security Issues in Vehicular Ad Hoc Networks, Mobile Ad-Hoc Networks: Applications, Prof. Xin Wang (Ed.), ISBN: 978-953-307-416-0, InTech, http://www.intechopen.com/books/mobile-ad-hoc-networks-applications/security-issues-in-vehicular-ad-hocnetworks

[10]. Jeremy Blum and Azim Eskandarian, “The threat of intelligent collisions”, IEEE computer society, 2004.

[11]. Maxim Raya and Jean-Pierre Hubaux, “The security of Vehicular adhoc networks”, SASN’05, 2005, USA.

[12]. Ghassan Samara, Wafaa A.H. Al-Salihy and R.Sures, “ Security issues and challenges of vehicular adhoc networks (VANET)”, IEEE Xplore, 2010.

[13]. Subir Biswas, Jelena Misic and Vojislav Misic, “DDOS attack on WAVE-enabled VANET through synchronization”, 2012.

[14]. Priyanka Sirola, Amit Joshi and Kamela C.Purohit, “ An analytical study of routing attacks in VANETs”, International journal of computer science engineering (IJCSE), Vol. 3, July 2014.

[15]. Abdulmotaleb El Saddik et al., “ Detecting and preventing IP spoofed distributed DoS attacks”, International journal of network security, 2008.

[16]. Aditya Sinha and Prof. Santosh K.Mishra, “ Preventing VANET from DOS and DDOS attack”, International journal of engineering trends and technology (IJETT), Vol. 4, 2013.

[17]. Komal B. Sahare, DR. L G.Malik, “ An approach for detection of attack in VANET”, International journal of engineering research `and application (IJERA) and International conference on industrial automation and computing (ICIAC), 2014.

[18]. Fasheng Yi et al., “ Source based filtering scheme against DDOS attacks”, International journal of database theory and application.

[19]. Vikash Porwal, Rajeev Patel and Dr. R.K. Kapoor, “An investigation of DoS flooding attack in VANET”, International journal of advance foundation and research in computing (IJAFRC), Vol. 1, Dec 2014.

[20]. B.B.Gupta, R.C. Joshi and Manoj Misra, “An efficient analytical solution tothwart DDOS attacks in public domain”, International conference on advances in computing, communication and control, 2009.

[21]. Archana S. Pimpalkar and A. R. Bhagat Patil, “Defense against DDOS attacks using IP address spoofing”, International journal of

innovative research in computer and communication engineering, Vol. 3, issue 3, March 2015.

[22]. Kamlesh Namdev and Prashant Singh, “Efficient and secure communication in vehicular adhoc network”, International journal of computer application, Volume 127, October 2015.

[23]. Karan Verma, Halabi Hasbullah and Ashok Kumar, “Prevention of DOS attacks in VANET”, Published in Wireless personal communication, November 2013.

[24]. S. Roselin Mary, M. Maheshwari and M.Thamaraiselvan, “Early detection of DOS attacks in VANET using attacked packet detection algorithm (APDA)”,2013.

[25]. Jieren Cheng et al., “DDOS attack detection algorithm using IP address features”, Springer-Verlog, Berlin Heidelberg, 2009.

[26]. Adil Mudassir Malla and Ravi Kant Sahu, “Security attacks with an effective solution for DDOS attacks in VANET”, International journal of computer application, Vol. 66, March 2013.

[27]. Er. Pallavi Bansal and Er. Lokesh Pawar, “Reducing impact of flooding in VANET due to distributed Denial of service attacks”. IJESC, 2015.

[28]. Pranav Kumar Singh, Kapang Lego and Dr. Themrichon Tuithung, “Simulation based analysis of Adhoc routing protocol in urban and highway scenario of VANET”, International journal of computer application, Vol. 121, January 2011.