A

Dissertation II Report

On

SECURITY MECHANISM FOR MITIGATION OF FLOODING AND BLACKHOLE ATTACKS USING AODV PROTOCOL IN MANET

A Dissertation report submitted in partial fulfillment of the requirements for theaward of the degree of

Masters of Technology

by

Kashif Kawsar Qadri

UNDER THE GUIDENCE

OF

Assistant Professor

Vishali Sharma

Project Supervisor

Lovely Professional University GT Road (Nh-1),Phagwara, Punjab, 144402, India

May, 2015

CANDIDATES DECLARATION

I hereby certify that the work, which is being presented in the Dissertation report entitled as **"Security Mechanism For MitigationOf Flooding And Black hole attack using AODV ProtocolIn MANET"** in the domain of Networking, in partial fulfillment of the requirement for the award of the Degree of Master of Technology submitted to the institution is an authentic record of my own work carried out during the period - August 2014 to May 2015under the supervision of **Vishali Sharma**. Ialso cited the reference about the text(s)/figure(s)/table(s) from where they have been taken.

.

Date: Signature of the Candidate

This is to certify that the above statement made by the candidate are correctand to the best of my knowledge.

Date: Signature Supervisor

CERTIFICATE

This is to certify that the declaration statement made by this student is correct to the best of my knowledge and belief. The Dissertation II proposal based on the Network Simulator tool learnt is fit for the submission and partial fulfillment of the conditions for the award of M.Tech in Electronics and Communication from Lovely Professional University, Phagwara.

Name:

U.ID:

Designation:

Signature ofFaculty Mentor

ACKNOWLEDGEMENT

The real spirit of achieving is through the way of excellence of austere discipline, without which I would never have succeeded in finishing it without the co-operation, encouragement and help provided to me by various personalities. With this deep felt consent and pleasure, I would like to express my heartfelt gratitude to all those who helped me in preparation of this training report.

It gives us immense pleasure in expressing my deepest and sincerest gratitude towards myProject guide**AssistantProfessor Vishali Sharma** for her considerate help,inspiring guidance throughout this work.

Also, I am thankful to all those, particularly the ***Lovely Professional University*** that has been instrumental in creating proper, healthy and conductive environment.

I would be defying if I do not mention my constant source of inspiration and vitality, that is, my parents who invested their present for my future, for their co-operation, support and encouragement.

ABSTRACT

Mobile Ad-hoc network (MANET) is collection of infrastructure less, decentralized self-directed nodes which form the dynamically a temporary network for transmitting data. These nodes are basically the systems or devices which can act simultaneously as host and router. These nodes have self alignment ability thus can be positioned instantly without any need of infrastructure. Because of the dynamic nature of the MANETs they are more prone to the attacks.Out of these attacks FLOODINGattackand BLACKHOLEattack are some of them. There are many routing protocols which have been developed for the MANETs out of these protocols Ad hoc on demand distance vector protocol (AODV) is one of them.Flooding is a kind of Denial of Service (DoS) attack in MANET. This type of attack exhausts battery power, storage space and bandwidth. Flooding the extreme number of packets may vitiate the performance of theparticular network. This study cogitateshelloflooding attack. As the RREQ packets are uninterruptedly flooded by the malicious node. In this report my main concernis detection of flooding attack on the AODV protocol is being presented using group mobility model. This is the simulation based study in which throughput, Packet delivery ratio (PDR), and overhead has been simulated and studied. It was observed that the value of throughput and PDR increased up to 73.20 and 0.9948 respectively while as the value of overhead decreased to 1.4139.In Black hole attack a kind of malicious node whose job is to drop the data packets in a given network. This attack is usually done during route discovery process. After receiving RREQ, the back hole authenticates its route and sends fake RREP. With the result source node send the data packets after receiving the fake RREP with which data is been dropped by the blackhole. And my main concern is to detect and prevent the Blackhole attacks in MANET using AODV protocol and based on the limitations of the previous methodology, a new techniques that is Intrusion Detection system has been implemented for better results.The simulation tool used for the study was NS-2.

Keywords: MANET, Flooding Attack, AODV, PDR, Blackhole attack,RREQ,RREP,

TABLE OF CONTENTS

Title **Page No.**

List of Tables……..x

List of Figures……xi

Abbreviations…….....xiii

CHAPTER 1 INTRODUCTION

1.1 Basic idea about Wireless Ad hoc Network……..….1

1.2 Introduction to Mobile Ad hoc Network (MANET)…….....2

1.3 Comparison of Infrastructure and Adhoc Network…….… ..3

1.4 Routing in MANET's…….. ..4

1.4.1 Table Driven Routing Protocols…….…… …5

1.4.2 On-Demand Routing Protocols…….... 6

1.5Problem Declaration……...…….. …..6

1.6 Motivation…… ….7

1.7 Objective of the Project…… ….8

CHAPTER 2 LITERATURE SURVEY

2.1 Literature Review……..… …….9

CHAPTER 3 MANET PROTOCOLS

3.1 Introduction to AODV protocol…..…….. 17

3.1.1 Route Discovery Mechanism in AODV…… ……...17

3.1.2 Route Maintain Mechanism in AODV…… …….…18

3.1.3 Advantages and Disadvantages of AODV protocol…… …….....18

3.2 Introduction to DSDV protocol…… ….…...19

3.2.1 Disadvantages…… ….…...20

3.3 Introduction to DSR protocol…… ……...20

3.3.1 Advantages and Disadvantages…… …....21

3.4 Comparison of AODV, DSDV and DSR protocols…… ….....22

CHAPTER 4 SECURITY IN MANET

4.1 Security threats in MANET……..... ...23

4.2 Attack Types

4.2.1 Passive Snooping……..…24
4.2.2 Selective existence (Selfish Node)…….....24
4.2.3 Gray Hole Attack……...……..25
4.2.4 Impersonation…….....25
4.2.5 Modification Attack…….....26
4.2.6Attack Against Routing Tables…….…....27
4.2.7 Sleep Deprivation Torture Attack……....27
4.2.8 Black Hole Attack…….....28
4.2.8.1 Black Hole Attack In AODV Protocol…….…....28
4.2.9 Sequence Number……..…...30
4.2.10 Flooding Attacks……....30
4.2.11 Introduction to Malicious Node…….....31
CHAPTER 5 RESEARCH METHODLOGY
5.1 Research Methodologies……..……...33
5.2 Simulation Tool…….....33
5.3 Introduction to Network Simulator……34
5.4 Simulation Set up…….....35
5.5 Propose Methodology To Detect Flooding Attacks In Manet……36
5.5.1 Algorithm For Detection Of Malicious Node In Manet…….…….....37
5.5.2 Overview OfNormal And Malicious Behaviour Of A Node……..,,,.39
5.6 Implementing A New Routing Protocol In NS 2.5…….41
5.7 Intrusion Detection System……..……...42
CHAPTER 6 SIMULATION AND RESULTS
6.1Simulation of various Topologies……..……..…44
6.2 Comparative Analysis using tables…….……47
6.3 Evaluation of various parameters through graphs…….……..…50
CHAPTER 7 CONCLUSION AND FUTURE WORK
7.1 Conclusion…….……64
7.2 Future work……..……..…65
7.3 List of Publication…….…….66
REFRENCES……...67

LIST OF TABLES

Table No.	Title	Page No.
1.1	Classification of MANET routing protocols.	5
3.1	Routing table of X.	20
5.1	NS 2.5 Simulation Setup.	35
6.1	Results of comparison of AODV, DSDV and DSR protocols.	47
6.2	Results of comparison of AODV And Black Hole AODV Protocol	48
6.3	Results of comparison of Black Hole AODV And IDS AODV .	48
6.4	Comparison b/w Before And After Detection Of Malicious Node.	49

LIST OF FIGURES

Figure No.	Title	Page No.
1.1	Chain structure of routing protocol.	4
3.1	AODV route discovery.	17
3.2	Route error Message in AODV.	18
3.3	Connection of nodes in DSDV.	19
4.1	Black hole node scenario.	29
4.2	The ad hoc flooding attack.	31
5.1	Network simulator 2 representation.	34
5.2	Flow Chart For Detection Of Malicious Node.	38
5.3	Normal BehaviourPaket transfer.	39
5.4	Defined Algorithm For Usual And Malicious Nodes.	42
6.1	40 Node Topology Of AODV.	44
6.2	40 Node Topology Of DSDV.	44
6.3	40 Node Topology Of DSR.	45
6.4	40 Node Topology Of Black Hole AODV.	45
6.5	40 Node Topology Of idsAODV.	46
6.6	40 Node Topology Showing Flooding Attacks.	46
6.7	40 Node Topology For Detection Of Malicious Node.	47
6.8	Throughput Analysis Of AODV,DSDV And DSR.	50
6.9	Throughput Analysis Of AODV And Black Hole AODV.	51
6.10	Throughput Analysis Of idsAODV And Black Hole AODV.	52
6.11	Throughput Parameter v/s Simulation Time At Flooding Attack.	53
6.12	Throughput Parameter v/s Simulation Time After Detection Of Malicious Node .	54
6.13	Overhead v/s Simulation Time In Presence Of Flooding Attack.	55
6.14	Overhead v/s Simulation Time After Detection Of Malicious .Node.	55
6.15	NRL Analysis Of AODV,DSDV And DSR.	56
6.16	NRL Analysis Of AODV And Black Hole AODV.	57

6.17	NRL Analysis Of idsAODV And Black Hole AODV.	58
6.18	PDR Analysis Of AODV,DSDV And DSR.	59
6.19	PDR Analysis Of AODV And Black Hole AODV.	60
6.20	PDR Analysis OfidsAODV And Black Hole AODV.	61
6.21	PDR v/s Simulation Time In Presence Of Flooding Attack.	61
6.22	PDR v/s Simulation Time After Detection Of Flooding Attack.	63

LIST OF ABBREVIATIONS

MANET	Mobile Adhoc Networks
AODV	Adhoc On-Demand Distance Vector
ABR	Associativity Based Routing Protocol
CGSR	Clusterhead Gateway Switch Routing Protocol
CBRP	Cluster Based Routing Protocol
DSR	Dynamic Source Routing
DSDV	Destination Sequenced Distance Vector
DOS	Denial of Service
FSR	Fisheye State Routing
GSR	Global State Routing
HSR	Hierarchical State Routing
iMANETs	Internet Based Mobile Ad hoc Networks
inVANETs	Intelligent Vehicular Ad hoc Networks
IDS	Intrusion Detection System
NS2	Network Simulator 2
NAM	Network Administrator
OTcl	Object Oriented Tool Command Language
RREQ	Route Request
RREP	Route Reply
RERRs	Route Errors
SSR	Signal Stability Routing
TORA	Temporally Ordered Routing Protocol
TTP	Trusted Third Party
VANETs	Vehicular Ad hoc Networks
WRP	Wireless Routing Protocol
ZHLS	Zone based Hierarchical Link State Routing Protocol

CHAPTER 1
INTRODUCTION

1.1 BASIC IDEA ABOUT WIRELESS AD-HOC NETWORKS

These types of networks can be defined as the collection of self-directed nodes which are self-achieved without having any kind of self-governing infrastructure or substructure. Therefore it exhibits the property of self-mobility phenomenon or topology, and these nodes can effortlessly links the escape from the network at any instant of time. Ad-hoc networks are very significant chiefly in the fields of defense or military, it can be utilized for rescue operations, it can be used to locate the victim or target combat field scenarios, it can also be used in earthquake damaged areas and flood effected areas. In short these kind of networks are established in those areas where there is least possibility to set up stabilized network [3]. As it is very different for centralized networks, in Ad-hoc networks there is no kind of centrally located hub. In this type of networks nodes interact with one another of their own without having any sort of hub, nodes sends the HELLO packets in order to establish links in between them, for this purpose different types of routing protocols are been used such as *AODV (Ad-hoc On-Demand Distance Vector),DSDV (Destination-Sequenced Distance-Vector), DSR (Dynamic source routing),SSR(Signal Stability Routing) and TORA(Temporally Ordered Routing Protocol)*[4]. In this kind of networks each node act as router. Each node is in search of truthful node in order to send data packet. Because of decentralized nature of Ad-hoc wireless networks these kind of networks are more susceptible to numerous amounts of attacks, in which of them are Blackhole attack and Flooding attacks. In blackhole attack the malevolent node engrosses whole network packets, it works analogous to actual blackhole of universe, while as in flooding attack network is flooded with the control packets such as RREQ, RREP packets in the particular network during route discovery process of on demand protocol, like AODV protocol , intermediary nodes are answerable to find a renewedalleyway to the destination, directingfinding packets to the nodes which comes in near regions or we can say neighboring nodes. Malevolent nodes do not use this procedure and instead, they nippilyanswer to the source node with incorrectdata as though it has renewedabundantroute to the destination. Therefore source node directs its data packets via

the malevolent node to the destination foretelling it is theright path. Blackhole attack may possiblyensue due to a malevolent node which is eloquentlydisobeying, as well as a spoiled node interface. In any case, nodes in the network will frequentlyattempt to discover a path for the destination, which makes the node ingest its battery in toting to droppingdata packets.

1.2 INTRODUCTION TO MOBILE ADHOC NETWORKS (MANET)

As MANET can be defined by its name also these are the mobile ad-hoc networks, in these networks the nodes are movable and can move in any direction, these networks are self-configuring they do not have well organized structure or infrastructure. Basically word Ad-hoc has been derived from the Latin word which means "for this purpose" [2]. In this kind of network each and every node performs like a router, the main purpose of MANET is to circulate data from source node to destination node for which different types of routing protocol are used which are earlier mentioned. From mid-1990's MANET's have proper attention in the field of research [6]. The chief aim of MANET's is to join with world's largest network known as internet. Numerousspeculative papers appraise protocols and their capabilities, superciliousfluctuatingnotches of suppleness and mobilityinside a demarcated space, frequently with wholly nodes within a limited hops of all other. Numerous protocols are formerlyappraisedfounded on events such as the packet drop rate, the overhead trade in by the routing protocol, network throughput,end-to-end packet delays etc.

There are different types of MANET's

- *Vehicular Ad hoc networks (VANET's)* these types of Ad hoc networksare capable for interaction or helps to communicate among the vehicles and automobiles with the wayside apparatuses..

- *Internet based mobile ad hoc networks(iMANET's)*in this type of ad hoc networks different movable associated nodes are linked with static Internet-gateway nodes [4]. Mostly in this kind of ad-hoc networks commonly used routing protocols are not applicable, hence modification is needed in this kind of ad-hoc networks.

- *Intelligent vehicular ad hoc networks (InVANET's)*in this type of ad hoc networks concept of artificial intelligence has been implemented [4]. It helps to reduce accidents and

mishaps because it works efficiently during these kinds of situations, these networks are intelligently manufacture to prevent such kind of mishaps.

- Each and every mobile ad-hoc network is a kind of ad-hoc networks but every ad-hoc network is not a MANET because generally in ad-hoc networks nodes are not movable while as in MANET every node is movable [3].

1.3 COMPARISON OF INFRASTRUCTURE AND WIRELESS ADHOC NETWORK.

Infrastructure networks are those networks which are self-organized structural network architecture; positions are desirable which comes under exposure area of access points. Hence, agility and mobility is obtained through the distance among the access points and positions, while as in ad-hoc there is complete opposite scenario, in this kind of network a node or station can transfer the informational data towards the new station or node only in presence of third node or station which might shield both the nodes jointly. Confidential informational data is furthered through intermediary stations or nodes with the help of the network routing protocols like AODV, DSDV, and DSR etc. This methodis used for maintenances ofgranderoperationalzoneon the other hand physical layer complicationupsurges [5]. Nodes or Stations mighthunt upon the objective station which is out of assortment by flooding the network with newscasts that are send off byevery station, while as in infrastructural networks or an organized network, the access points have potential to conceal battery optimization for its nodes or stations. Although stations exhibits the power redeemable mode and access point have potentialbulwark frames for stations. On the other hand in an ad-hoc network there is much huge amount of power consumption, meanwhile there is transference of frames by stations which are not certainly apprehended by themselves. After there is transferring of packets over the movable or mobile nodes there is alteration of hop count in mobile adhoc networks on the other hand in organized WLANs, the communication criterion for two hops, It is a prospectto embracespeedilyaltering, arbitrary, multi-hop in MANET of theirtopologies in particular routing functions[2].

1.4 ROUTING IN MANET

There are three different types of routing protocol divided according to their uses and functions are mentioned below.

1. Proactive protocols.
2. Reactive protocols.
3. Hybrid protocols.

Chain of routing protocols are given below in figure 1.1

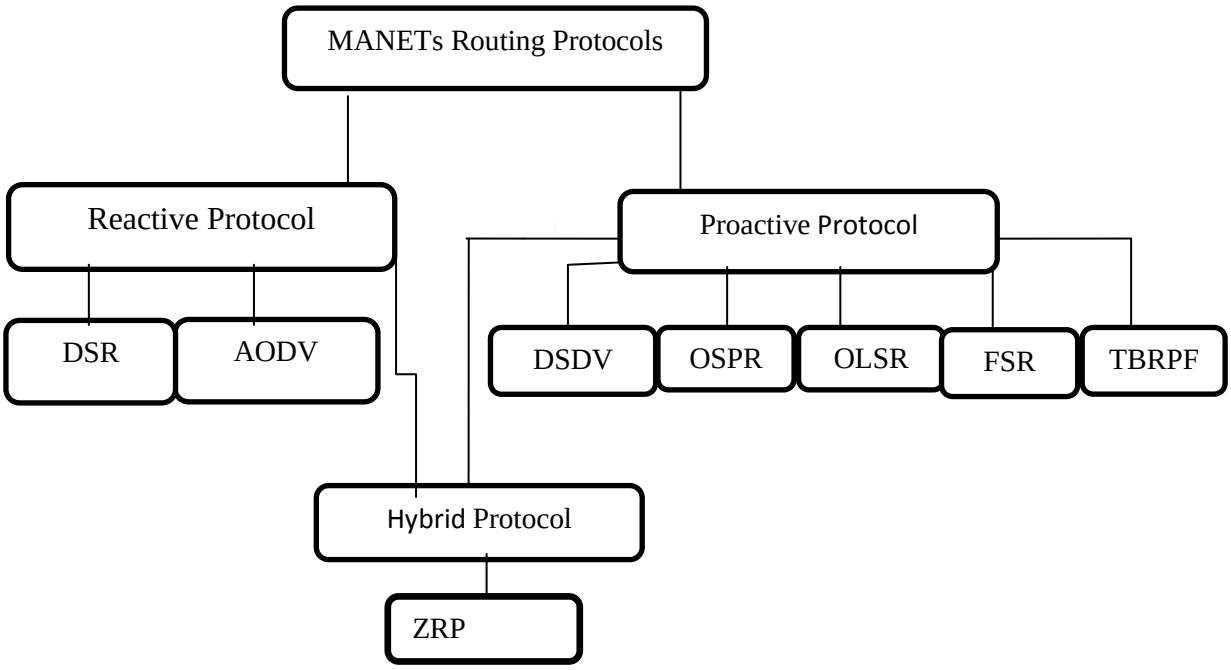

Figure1.1 Chain structure of routing protocols

As mobile ad hoc networks have distinctive downsides and characteristics such as power is restricted, bandwidth is also restricted, topology is highly self-motivated and dynamic and there is exponential error rate etc.Furthermore in contrast to infrastructural or self-organized existing networks, the mobile ad hoc networks have every movable node and are associated in arbitrary manner [7]. Each and every node of mobile ad hoc networks is acting like router and yields part in finding and up observance in edict to create a trustworthy route of each other with which it is not possible to use same routing protocols of wired networks in wireless networks and adequately the protocols have been established for mobile ad hoc

networks [6]. Thereforethere is a classification of routing protocols on the bases of running of routing tables. There are two groups of routing Protocols thatare Table Driven Routing Protocols and On-Demand Routing Protocols which are explained below.

Table 1.1: Classification of MANET routing protocols

MANET ROUTING PROTOCOLS	
On-Demand Routing Protocols	**Table Driven Routing Protocols**
Ad-Hoc On-Demand Distance Vector Routing (AODV)	Destination-Sequenced Distance Vector Routing Protocol (DSDV)
Cluster based Routing Protocols (CBRP)	Wireless Routing Protocol (WRP)
Dynamic Source Routing Protocol (DSRP)	Zone-based Hierarchical Link State Routing Protocol (ZHLS)
Temporally Ordered Routing Algorithm (TORA)	Global State Routing (GSR)
Associativity Based Routing (ABR)	Clusterhead Gateway Switch Routing Protocol (CGSR)
Signal Stability Routing (SSR)	Fisheye State Routing (FSR)
	Hierarchical State Routing (HSR)

1.4.1 TABLE DRIVEN ROUTING PROTOCOL

In this type of routing protocol, each and every node maintains updating of its routing table, in order to uphold the trustworthiness in a routing tables, themultiple updated messages are proliferated by each and every single node to the network [6]. In case there is change in network topology, each and every node updates itself with the new entries, Table Driven Routing Protocols extantnumeroustechnical hitches.

- There is extension in bandwidth overhead because of sporadically updating the network topology.
- There is promptly drain of battery and node remain wakeful because of sporadicallychanging or updating route table entries.
- Numerouslaid off route entries to the explicit destination pointlessly take place in the routing tables.

Destination-Sequenced Distance Vector Routing Protocol(DSDV),Cluster head Gateway Switch Routing Protocol(CGSR),Fisheye State Routing(FSR),Hierarchical State Routing (HSR),Zone-Based Hierarchical Link State Routing Protocol(ZHLS)Wireless Routing Protocol(WRP) and Global State Routing (GSR)are Table Driven Routing Protocols [8].

1.4.2 ON-DEMAND ROUTING PROTOCOL

In contrast to table driven routing protocol, on-demand routing protocol is very much different, as on-demand are not periodically updated,its only upgraded when it is desirable. Original source node proliferates the route request packets in order to locate to link up with thee destination node, which is done when intermediary nodes receives the broadcasted RREQ (Route Request packets) it further in order to locate path towards the destination node. Subsequently, the destination node n return propels the route reply packets through the shortest lived route to establish the secure connection towards the source node. The route rests in the route tables of the nodes over and done with shortest route until the route is no longer compulsory.The different On-demand routing protocols are : Temporally Ordered Routing Algorithm(TORA),Ad-hoc On-Demand Distance Vector(AODV), Dynamic Source Routing Protocol(DSRP),Associativity Based Routing(ABR),Cluster Based Routing Protocol(CBRP)and Signal Stability Routing (SSR) [5] .

1.5 PROBLEM DECLARATION

In previous researches, the work were prepared on many security disputes like Gray hole attacks, wormhole attack , various Denial of services and Black hole attacks convoluted in MANETS using various proactive routing Protocols like Destination Sequenced Distance vector (DSDV) and Optimized Link State Routing Protocol (OLSR) etc.In this report i have explained Black Hole attack and Flooding attack studied under the AODV routing protocol and its effects are elaborated by stating how this attack upset the performance of MANET. Very slight attention has been given to the point to study the impact of Black Hole attack in MANET using both Reactive and Proactive protocols and to compare the weakness of both these protocols against the attack. There is a requirement to address both these types of protocols as well as the influences of the attacks on the MANETs.

1.6 MOTIVATION

As security is an important apprehension in Mobile Ad hoc networks in current era. Network should be accessible to important services, integrity and Privacy, secrecy and Concealment of informational data, it can only be attained by guaranteeing the security concerns. Asmobile ad-hoc networks are the open medium and topologies are dynamic in nature, absence of central hub and there is not any definite safeguard mechanism with which it is more susceptible to various attacks. Due to these reasons there is an alteration in Battle field conditions for mobile ad-hoc networks against the security disputes.

1.7 THE OBJECTIVES OF THESIS

The main goal ofthis thesis is:

1) Comparing the distinct parameters on NS2 simulations by doing literature survey of AODV protocols.

2) Forming topology of 20, 30 and 40 nodes using AODV, DSDV and DSR routing protocols in NS2.

3)Comparison on the bases of different parameters like throughput, packet delivery ratio(PDR) and Normalized routing Load (NRL) of above mentioned simulation of three different routing protocols.

4)Table formation on the basis of simulations and results obtained for different protocols.

5)Inducing a Blackhole attack on 20, 30,40 nodes topology by using AODV routingprotocol.

6)Adding Blackhole AODV file in NS-2 and converting one of the nodes as attacker node.

7)Introducing IDS (Intrusion Detection System) to prevent blackhole attack in node topology in NS2.

8) Addition of malicious node to initiate Flooding attack in 40 node topology on the based of AODV protocol in NS-2.

9) Detection of malicious node in Flooding attack of 40 node topology on the based of AODV routing protocol in NS-2.

10) Comparing the performance parameters of all the scenarios and assessing the results working on those parameters

CHAPTER 2
LITERATURE SURVEY

2.1 LITERATURE REVIEW

[1] JaydipSen et.al "A Mechanism for Detection of Cooperative Blackhole Attack in Mobile Ad Hoc Networks" 2011 Second International Conference on Intelligent Systems, Modeling and Simulation, page no 338-343. In this paper two concepts has been implemented ,that is concept of DRI table and concept of Cross checking which helped to anticipate the numerous blackhole attacks , there has been adequate amount of increase in the packet delivery ration i.e. 60% which is very good amount for the overall efficiency of particular network.

[2] Jaspal Kumar et.al "Effect of Blackhole Attack on MANET Routing Protocols" I.J. Computer Network and Information Security, 2013, 5, Published Online April 2013 in MECS, page no 64-72 .In this paper concept of new protocol i.e. IAODV(Improved Ad-hoc On demand Distance Vector) has been implemented which works on two principles i.e. Multipath and Path Accumulation concepts. As per analyses that under blackhole attack there has been cumulative increasing in packet delivery ratio of IAODV which is far efficient than normal value of PDR in Ad hoc on demand distance vector but the value of other parameters like end-to-end delay is almost the same , while as there is smaller amount rise in the routing load overhead .

[3] Yaserkhamayseh et.al "A New Protocol for Detecting Blackhole Nodes in Ad Hoc Networks," International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011, page no 36-47. In this paper there is a concept of trust table were given, with which the three comes some modifications in the original ad hoc on demand routing protocol, each and every node has its own table in order to store the path addresses of trustworthy nodes, higher the value stored in table more is the possibility that the node will be genuine. If node broadcasts the RREQ and the value in a table remains zero it means there is possibility the particular node will be black hole. Value of truth table of particular node will be 2 only and only when replying node is a destination node. After source node receive the route reply packets,then it decides for some time whether to send the

informational data or may delay for another desirable route. It improves the parameters of network like throughput, PDR, and decreases overhead and end-to-end delay. The main aim was to make the protocol compatible with a technique to eradicate the malicious node from a particular network,and protocol should be supportive in order to eradicate the malicious node when working jointly.

[4] Ketan S. Chavda et.al " Removal Of Blackhole Attack In AODV Routing Protocol Of MANET", 4th ICCCNT – 2013 July 4 -6, 2013, Tiruchengode, India, In this paper new method has been explain in order to thwart Blackhole attacks . Simple methods has been implemented which do not alter normal functioning of intermediate node and destination node.This approach do not alter the normal functioning of ad hoc on demand routing protocol. This purely works on destination sequence number, the node having high sequence number is consider genuine node, by condition if there is differencenot relatively high in two numbers then Route reply having remarkably high destination sequence number is having supplementary probability to be a malevolent node and an AWARE message having the node credentials number isgenerally formed which is broadcasted to near neighbor nodes so that any message or notice receive from that kind of malicious node is rejected. List of those malicious nodes can be maintained by the nodes taking part in communication network which can be helpful to prevent blackhole attack.Throughput is decreased by 93% when normal AODV protocol is used in blackhole attack while using novel approach throughput is increased by 20% in blackhole. PDR is also increased by 40% than previous used normal AODV protocol in blackhole attack.

[5] P. Manickam1 et.al "Performance Comparisons Of Routing Protocols In Mobile Ad-Hoc Networks", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 1, February 2011, page no 98-106, In this paper comparison between the main three routing protocols that is Destination sequenced distance vector, Dynamic source routing and Ad hoc on demand distance vector by using Network simulator version 2. Different parameters like, Average end-to-end delay, Throughput and packet delivery ratio.. As Destination sequenced distance vectorDSDV is a proactive routing protocol and are effectual for fewer number of nodes which are less movable sincethe stowing of routing data in the routing table at each

and every node,by Assessment of with DSDV, AODVand DSR protocol, in each and every packet the overhead byte will go on increasing when topology of network will change as DSR protocol is using route cache and source routing that's why DSR is more preferred for moderate traffic with moderate mobility, while as in Ad hoc on demand routing protocol there is an increase in end-to-end delay and destination sequence distance vector is having low end-to-end delay ,AODV has very better results in packet delivery ratio. By concluding every point, DSR shows better results than AODV in terms of overhead.

[6] KaminiMaheshwar et.al " Blackhole Effect Analysis and Prevention through IDS in MANET Environment",European Journal of Applied Engineering and Scientific Research, 2012, 1 (4):84-90, In this paper blackhole is been detected by checking behavior activity and malicious activity through the behavior analysis basis known as data filtering method and also having safe guard through attack of blackhole activity with the help of intrusion prevention system in AODV protocol which is been discussed already. The proposed algorithm takes performance by applying it in the network simulator-2 and the fallouts explain the well effect of the IDS based AODV.

[7] VipinKhandelwal IC et.al "Blackhole Attack and Detection Method for AODV Routing Protocol in MANETs", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, April 2013 page no 1555-1559, In this paper new method known as Dynamic Learning have been enlightened, which helps to understand that malevolent node reduces the overall performance of network. As ad hoc on demand distance vector are more susceptible to different vulnerable attacks because sequence number is used for node assortment, therefore malevolent takes benefit , by changing its own sequence number, and effects badly on network parameters like throughput, PDR, overhead etc..

[8] ShekharTandan et.al " A PDRR based detection technique for blackhole attack in MANET", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1513-1516.In this paper work intends a procedure is applied onpacket drop fraction in which it has been appraised and certified . New technique that is

detection of threshold has been explained, with which the premeditated packet drop fraction in contradiction of a value of threshold. The value of threshold is a supreme packet drop fractional assessment deprived of malevolentnodeattack. Packet drop fraction is having very less value during normal operation of network i.e. in absence of malevolent node, while as under vulnerable attack by malevolent node the value of packet deliver fraction increases abundantly above the value of threshold. Hence the proposed scheme evaluates associateswith packet drop fraction to pre stated value of threshold.

[9] Harsh PratapSingh et.al"Guard against cooperative blackhole attack in Mobile Ad-Hoc Network", International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 7 July 2011, In this paper RBS (Reference Broadcast Synchronization) is method used for clock synchronization process in MANET, now this paper used same technique in order to remove the cooperative blackhole attacks by relative velocity reference distance method for the finding of Blackhole node. These approaches are very effective for the practice of exploring a Blackhole in a MANET. This offered procedure is replicated in NS2 network simulator and very good results Have been obtained in associates of winding technique in its place of these properties it has some drawback e.g. They have find a mistaken reference distance of the reference node now all the node found as a Blackhole node. Now in future they have lessened the method of exploring precise method for relative reference distance.

[10] Mehdi Baratiet.al"Performance Evaluation of Energy Consumption for AODV and DSR Routing Protocols in MANET"- . In this paper two routing protocols have been compared i.e. ad hoc on demand distance vector and dynamic source routing on the bases of consumption of energy and consumption of routing energy. Then different parameters of networks have been estimated on the bases of different consumption of power and by using different types of mobility traffic models.

[11] TaranpreetKaur et.al " Defending MANETs against Flooding Attacks for Military Applications under Group Mobility" Proceedings of 2014 RAECS VIET Punjab University Chandigarh, 06 - 08 March, 2014.In this paper To vitiate the performance of MANET, the Denial of Service (DOS) Attacks, like Route Request Flooding Attack comes under

Distributed Denial of service attacks are foremost danger. A new slant is proposed which will competently defend from RREQ Flooding Attack in Military battlefield circumstances. Following are the main points taken into attention: The optimal value of k varies from situation to situation. For Clustering situations the best value of k is 2, in relations of PDR, Delay, Overhead, and Throughput. The location of attacking nodes also plays vital role on values of various metrics. If all malicious nodes are existing in unique cluster the performance ruin is more, as clustering overhead increases.

[12] Ping Yi et.al "A New Routing Attack in Mobile Ad Hoc Networks" International Journal of Information Technology Vol. 11 No. 2. In this paper, the Flooding Attackhas been described, a novel and dominant attack against on demand ad-hoc routing protocols. This attack permits attacker to stand a denial of service attack against all on-demand routing protocols for mobile ad hoc networks, even secure on-demand routing protocols. Here the report of Flooding Attack Prevention (FAP) to resisting this attack is given. The results of this implementation show the Flooding Attack Prevention efficiently shield the Ad Hoc Flooding Attack with little overload. The method of neighbor suppression which are characteristics of mobile ad-hoc network. The chief idea of neighbor suppression is that each neighbor determines the rate of RREQ initiated by intruder. If the rate surpasses some threshold, all neighbors will not receive and forward packets from intruder. Here are two tables in every node: Rate_RREQ and Blacklist. The table of Rate_RREQ records the rate of RREQ which every neighbor node initiates, and does not record times of forwarded RREQ. The Rate_RREQ has two columns: Node_ID and RREQ_time. Node_ID includes all neighbor node ID. RREQ_time records times which neighbor node originates RREQ.

[13] Nitiket N Mhala et.al "An Implementation Possibilities for AODV routing protocol in real world" In this paper the main focus is on functioning implementation of AODV routing protocol by means of certain design potentials and possible opportunities for finding needed AODV events. And the socket based mechanism particularly when AODV routing daemon connects changes to the IP route table. The paper suggests the need of implementation of Generic Netlink Family.

[14] SudhirAgrawal et.al "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks" Journal Ofcomputing, volume 3, issue 1, January 2011, ISSN 2151-9617. In this paper due to absence of a distinct central authority, securitizing the routing process becomes a perplexing taskthereby leaving MANETs susceptible to attacks, which results in worsening in the performance characteristics as well as rises aserious interrogatory mark about the consistency and reliability of such networks. Efforts have been made to current an outline of the routing protocols, the known routing attacks and the suggested countermeasures to these attacks in several mechanisms.

[15] Abhijeetkumar et.al"Mitigation of flooding Attack in MANET using NS-3" International Journal for research in applied scienceand engineering technology (IJRASET)Vol. 2 Issue IV, April 2014 ISSN: 2321-9653. In this paper DoS attack was instigated on account of RREQ Flooding. Then with the assistance of projected scheme, detection of the DoS attack because of RREQ flooding is done.Then detecting the malicious nodes and blacklisted. In this process none of the sincere nodes which may be mistakenlyaccused of being ill-behaved were not malicious. The routine of the network was improved in the existence of conceded nodes and creating the limit-parameters adaptive in nature.This can be done by making calculations centered on parameters like memory, processing capability, battery power, and average number of requests per second in the network and so on. Further, the protocol can be made protected against other types of possible DoS attacks that loom it. Mobile computing contains mobile communication. The concerns related to this network are ad-hoc and infrastructure networks as well as communication properties, protocols and the like. Thus the scope of enrichment and improvements in Wireless Networks, preferably Mobile Ad Hoc Networks is huge.

[16] MeghnaChhabra et.al " A Novel Solution to Handle DDOS Attack in MANET" Journal of Information Security, 2013, 4, 165-179 .In this paper as MANET's are more susceptible in comparison to wired networks due the deficiency of a trustworthy centralized authority and limited resources. There is a vital need to cultivate a system to handle DDoS attack in mobile ad hoc network. The numerous attack mechanisms and problems due to DDoS attack has been enlightened and also how MANET can be affected by these attacks . In addition to this,

a novel solution is anticipated to grip DDoS attacks in mobile ad hoc networks. Novel approach has been enlightened as the monitoring node will propel a “Hello” packet to its next neighborhood node that is the monitored node and will pause for its reply. If it does not get reply within the fixed interval then the node being scrutinized is flooded node that is the victim node. Later, the id of this node will be restricted and the entry of victim node will be canceled from the routing tables of entirely nodes. After discovery of the nodes, the path is located in which attack is being accomplished and figure out the broadcast ids whose effect will be quashed. Code for the technique has been employed in neighbor management function, To Get Broadcast ID function and conclude function of aodv.pc file.

[17]AlokparnaBandyopadhyay et.al“A Simulation Analysis of Flooding Attack inMANET using NS-3”, 978-1-4577-0787-2/11/$26.00 ©2011 IEEE.In this paper, the security of AODV routing protocol in MANET was examined by recognizing the influence of flooding attack on it. The flooding attack in AODV protocol was simulated by means of the NS-3 network simulator. Though, analogous results can also be found when using the DSR routing protocol. It was perceived that the occurrence of malicious flooding nodes in MANET can affect the performance of the general wireless network and can act as one of the chief security threats. By the simulation, it can be resolved that due to the widespread flooding in the network, average proportion of packet loss, average routing overhead and average bandwidth requirement all upturns, therefore lessening the overall network throughput. A robust monitoring appliance must be implemented in the mobile nodes of MANET for the documentation and isolation of the conceded flooding nodes from the network. Selected sort of enticement mechanism may also be unified in the network to apply cooperation among all the nodes in MANET to mend the overall network performance.

[18] BounpadithKannhavong et.al“A Survey of Routing Attacks in Mobile Ad- Hoc Networks” IEEE Wireless Communications” October 2007 1536-1284/07/$20.00 © 2007 IEEE page no 85-91. In this paper the existing state of the knack of routing attacks and countermeasures in a MANET has been revised. For countermeasures, there has been acknowledged their benefits as well as their weaknesses. It exhibited that while many resolutions have been anticipated, they still are not flawless in terms of trade-offs among use

and efficiency. For example certain solutions that depend on cryptography and key management seem promising, but they are too affluent for resource inhibited MANETs. Although some resolutions work fine in the company of one malicious node, they might not be applicable in the presence of numerous plotting attackers. Some resolutions may entail distinct hardware such as a GPS or an amendment to the existing protocol.

CHAPTER 3

MANET PROTOCOLS

3.1 INTRODUCTION TO AODVPROTOCOL

Ad hoc On-Demand Distance Vector (AODV) Routing is a kind of routing protocol implemented in mobile ad hoc networks (MANETS) and various other wireless ad hoc networks.

3.12 Route Discovery Mechanism in AODV

When a joining is required in AODV, the network is muted up. Around that moment the network node that is required for the connection announces a signal for bonding. A message is frontward by AODV and records the node that they perceived it from, crafting a detonation of inadequate routes back to the penurious or needy node. A node directs a message in inverse through an impermanent path to the entreating node when the node acquires such type of message and by this moment has a pathway to the anticipated node [8]. The route that has the smallest sum of hops is used by the indigent or needy node to instigate. Aftersome time, unfilled entries in the routing

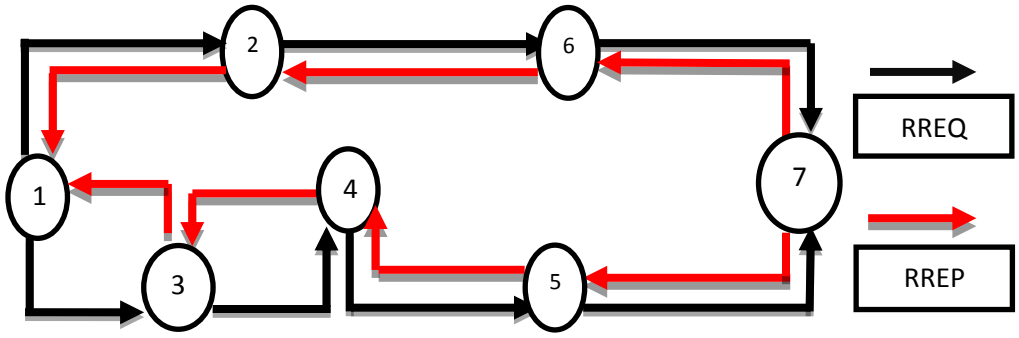

Fig. 3.1 AODV Route Discovery

Figure 3.1 represents route Discovery process of AODV routing protocol, there are seven nodes present In the network Black arrows represents the path through which route requests

has been send in forward direction while as red arrow represent the path through which route reply has been send by nodes in backward direction after receiving the route requests.

3.13 Route Maintain Mechanism in AODV: A routing error is distributed back to a transmitting node and the procedure replays when alinkage miscarries. The lowest number of messages to jam the space network is much of the complication of the protocol. Every request for a route has a sequence number such as [4]. For the disappearance of route requests that the nodes have formerly conceded on, they make use of sequence numbers. To restrict how many times a route can be redirected, the routes use one extra feature of "time to live" number. When failure of route request occurs, many more route request might not be directed until twice as much time has taken place as the timeout of the former route request [4]. This is another such feature.

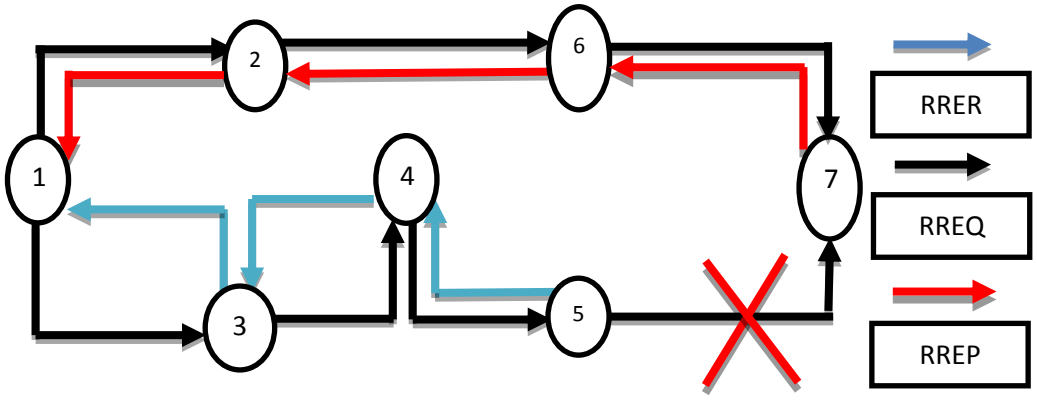

Fig. 3.2 Route Error Message in AODV3.14

ADVANTAGES AND DISADVANTAGES OF AODV PROTOCOL

- Devising routes reorganized on demand and that destination numbers are functional to discover the immediate prior route to the destination is the chief benefit of this protocol.
- For communication along the prevailing links, AODV crafts no additional traffic.
- AODV doesn't has a perquisite for memory or calculation and creates a distance vector routing much guidelines [3]. Delay is considerably less in the joining setup.

- The intermediary nodes have a larger but not the newest destination sequence number and these nodes can lead to unreliable routes if the source sequence number is much timeworn, thereby having out of date entries. This is the chief drawback of this protocol.
- In reply to a solo Route Request packet can lead to hefty control overhead when there are multiple Route Reply packets. Superfluous bandwidth consumption due
  To infrequent beaconing is another disadvantage of AODV [3].

3.2 INTRODUCTION TO DSDV PROTOCOL

Destination-Sequenced Distance-Vector Routing (DSDV) is used for ad hoc mobile networks upended on the Bellman-Ford algorithm and is a table-driven arrangement. P. Bhagwat and C. Perkins advanced it in 1994 [8]. Algorithm resolved the routing loop difficulty which was its chief advancement. A sequence number is included in all the record of routing table. If the connection exists the sequence number is commonly even else, an odd number is used. The emitter requires to send out the next update with this number and the number is produced by the destination. By directing full dumps not often and minor incremental updates more frequently routing information is scattered among the nodes.

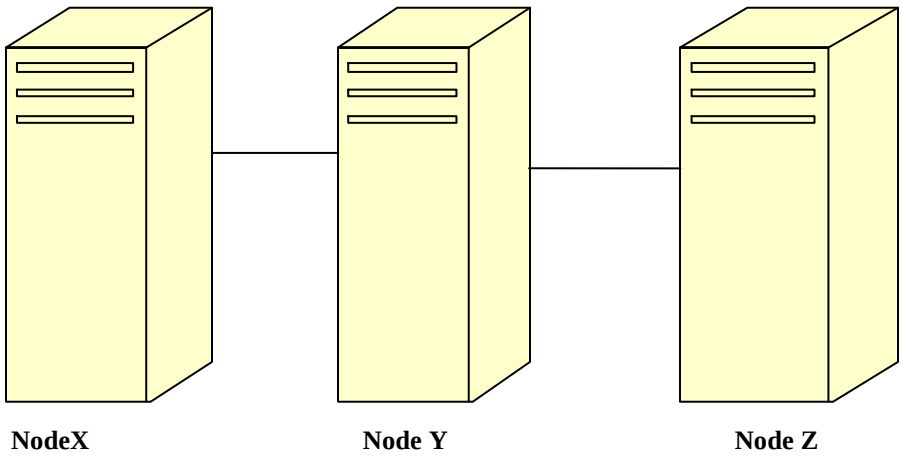

Fig. 3.3 connection of nodes in DSDV

Also the routing table of Node x in this network is:

Table 3.1: Routing table of X

Destination	Next Hop	Number of Hops	Sequence Number	Install Time
X	X	0	A 48	001100
Y	Y	1	B 38	001300
Z	Y	2	C 29	001600

Selection of Route-A router uses the newest sequence number if it accepts up-to-date information data. Superior metric is used for the path if the sequence number is same as the one earlier in the table. In while [5] stale entries are the records that haven't been updated. As the next node hops, it is detached and these entries as well the paths.

3.2.1 DISADVATAGES

It utilizes bandwidth even when the network is not in use and DSDV requires a continual update of its routing tables, with which the battery power is more utilized and very less quantity of bandwidth is present. A new sequence number is vital before the network re-converges when each and every time the topology of the network shifts; thus, DSDV is not fit for topmost dynamic and vibrant networks [2]. This does not agitate traffic in regions of network that are not fretful by the topology shift as in all distance-vector protocols.

3.3 INTRODUCTION TO DSR

Dynamic Source Routing (DSR) is used for wireless mesh networks as a routing protocol. It forms a route according to the demand if the transmitting computer requires one in that respects it is similar to AODV [2]. As an alternative to relying on the routing table at all the intermediate device it uses source routing. Assembling the address of all the devices between source and destination during the route discovery is required for obtaining the source routes. Nodes processing the route discovery packets acquire the collected path information. Route packets get damaged learned paths. The routed packets have the address of all the devices the

packet will travel to so that source routing is achieved. DSR alternatively calculates a flow id option that permits packets to be send on a hop-by-hop basis to avoid using source routing. All the routing information is managed (repeatedly updated) at mobile nodes so that the protocol relies exactly on source routing. Route Discovery and Route Maintenance are its two essential stages. If, the message has traversed to the desired destination node (Route Request would be would be inserted into the route reply which actually resides in the route record), Route Reply would be generated [2].

The destination node must have a route to the source node to direct back the Route Reply. The route will function if the route is contained resides in the cache of the Destination Node. Alternatively, by checking the route record in the route request message header (all the links should be symmetric) the route will be inverted. The beginning of the Route Maintenance Phase is completed where the Route Error packets are created at a node if the transmission takes place. From the route cache of the node the hop with error will be discarded [1]. At the mark all routes consisting of the hop are curtailed. To create the most possible route, the beginning of the Route Discovery Phase is brought into progress.

An on-demand protocol which restrains the bandwidth used by control packets in ad -hoc wireless networks is called Dynamic source routing protocol and is implemented by discarding the periodic table update messages used in table-driven approach. In the above protocols, the former is beacon-less and thus, does not need periodic transmissions of the hello packets which a node consumes to ensure its neighbors of its residing and this is the main difference between these protocols. Around the time when the route construction phase as Route Request packets are flooded in the network, a route is the basic approach of this protocol. The Destination node replies by frontward a Route Reply packet back to the source which transfers the information of the route carried by the route request packet on getting a route request packet [4].

3.3.1 ADVANTAGES AND DISADVANTAGES

The requirement to flood the network in a periodic manner with a table update messages which are consumed in a table driven approach is not essential in the reactive approach of this protocol. Setting up of a route is completed only when needed and thus, the requirement to locate the routes to all other nodes in the network as needed by the table driven approach is

eliminated in a reactive on-demand approach. The consumption of the route cache information faultlessly to reduce the control overhead is done by the intermediate nodes [4]. The busted link is not locally mended by the route maintenance mechanism which is the shortcoming of this protocol. Because of the stale route cache information during the route reconstruction phase irregularities could take place. In this approach the connection setup delay is more than in the other approach. Although, the protocol does well in static and low-mobility environments, the efficiency reduces with mobility reaching higher values [4]. Because of the source routing mechanism used in DSR a major routing overhead is knotted due to routing protocol. Path length directly depends on this routing overhead.

3.4 COMPARISON OF AODV, DSDV, DSR PROTOCOLS

- ***Throughput-*** It can be defined as the rate of unbeaten message past a path channel. This information can traverse over a physical link or logical link or sent through a known network node. Throughput is continuously calculated in bits per second (bit/s or bps), and often in information packets per second or data packets per time slot. The total of data rates that are send to all the terminals in the network is the system throughput or aggregate throughput. Digital bandwidth use is similar to the throughput.
- ***Packet Delivery ratio-*** It is defined as the number of delivered data packets to the destination. Delivered data to the destination is depicted by it.Summation of number of packets received/ Summation of number of packets
  Sent.

For the better working of the protocol, the value of the packet delivery ratio should be higher. .

- ***Normalized Routing Load-*** The sum of number of the routing packets transmitted per data packet is known as Normalized Routing Load. The ratio of the sum of number of routing packets transmitted (also consists of forward routing packets) to the sum of number of data packets received gives us the value of the Normalized Routing Load.

CHAPTER 4

SECURITY IN MANET

4.1 SECURITY THREATS IN MANET

Some features donot pose a safety concern for ad hoc networks like weakness of operating systems and higher layer applications that fit into the manager programs like databases, browsers or client server. In opposite to the routing layer of ad hoc networks; like physical, MAC and network layer which is the most important task of wireless ad hoc network for the routing contrivance, keeping the packets sequentially a route discovery process, wide-ranging attack forms are dangerous. Application safety, network security, database security which are calculated in changed workings which are not expounded thoroughly at this moment are the additional limitations [14]. Not accelerating packets or totaling and changing some considerations of routing messages; like sequence number and ip address are the two solutions to the ripples in a wireless ad hoc network. Ad hoc networks are detailed in segments. Authentication and cryptography or mutually in a network serves as an anticipatory approach and can be used instead of attackers and thus proves as a critical contrivance. Malevolent 'insiders' which practice one of the critical solutions can also can also impend safety, though these contrivances protect the network counter to attacks that come from the exterior. E.g. recipes are saved by terror resilient hardware which are used in the Lorries in the network, it is hard to say that these Lorries show similar comportment if the enemy invades them [14]. On the other hand, a node may incidentally not respond as if it is damaged. Attack is a node with an impaired battery which is incomplete to accomplish network tasks which may be professed as an attack. Self-centeredness is alternative cruel activities of the nodes. By not taking part in network processes selfish nodes restrain from draining its capital. Thus, defamed and selfish nodes also break the network enactment as they donot probably route network packets, like in routing appliance. We should therefore safeguard that the complete thing is appropriately in the network to backing general security and differentiate how an invader is able to impair the ad hoc wireless network. Intrusion detection system are used to protect wireless ad hoc networks to detain the workings of assailants and can form a resolution contrary to these breaks.

4.2 Attack Types

4.2.1 Passive Snooping

To detect what is going on in the network an invader can pay attention to many wireless network. Firstly concentrate to control messages to guess the network topology to know in what sense nodes are placed or are sociable with changes. Around the network afore invading can collect brainy evidence [14]. By means of encryption while it should be faithful be in the appropriate place to raise layer applications and thus can know the evidence that is communicated by means of encryption. Hearing is also a frightening to place alone. By knowing radio signals an unauthentic node can poster a wireless network. Traffic engineering skills have been set to counteract this.

4.2.2 Selective Existence (Selfish Nodes)

It is a type of attack in which the malicious node also called selfish node and which is not contributing in the network for its benefit to boost efficiency and preserve its important possessions like power. Selfish node sets forward its actually each time peculiar cost is intricate to attain this. Selective existence attacks are recognized as selfish code conducts. For example, as long as it does not twitch the broadcast, selfish nodes do not even direct any HELLO messages and descent all packets even if they are directed to itself [15]. Selfish node accomplishes a route discovery and that propels the compulsory packets when a selfish node desires to twitch a linking with alternative node. A silent node is yielded when the node no more desires to practice the network. Adjoining nodes nullify their peculiar route accesses to this node and selfish node grows into indistinguishable on the network after a while. The objectives of the confronting node are actually the sinking packets may be alienated into two groupings. Because of the supplementary nodes that it will attack far ahead the attacker may famine to descent the packets of the single supplementary node. To realize whether it derives of commencing this node it is requisite to guise the packet. Attacker fills the CPU supply and indeed the battery life if it guises at the contented wholly packets accumulating from the network [15]. As the selfish node expends the battery life this is not an excepted behavior. If its object is not to ingest its own possessions attackers are not attentive in the pleased of the packets. Selfish node comportment is the first kind of dipping packets that cannot be

engaged. Selfish node comportment does not include selectively dropping messages. Nodes just do not take part in the network and they do not amend the gratified of packets because selective existence is a form of passive attack.

4.2.3 Gray Hole Attack (Routing Troublesomeness)

Dipping of messages is a result of gray holes attacks is an active attack variety. Flops are do so and firstly the node acts decorously. Acting decorously node replys valid RREP messages to nodes that pledges RREQ message. It grosses over the directive packets in this way. Denial of service attack (DoS) is presented when the node just dribs the packets. Adjoining nodes may need to discover a route another time if the adjoining nodes attempt to direct the packets over destructive nodes. RREP messages is a route inaugurated by attacking node [14]. Until malicious node prospers its aim the procedure goes on (like network source consumption, battery consumption). Routing misbehavior defines this attack. One of the comportments of botched or overloading nodes is the plummeting of packets. Selection existence, gray or black hole attack should not weigh every plummeting packet action. To distinguish most of the data packets have been advanced, DSR being the only exception most of the protocols have no machinery.

4.2.4 Impersonation

Only MAC or IP addresses uniquely identify hosts due to lack of validation in ad hoc networks. To validate the sender node these validations are not sufficient. Ad hoc network protocols are not provided with non-repudiation. The modest methods to make-believe as an additional node are MAC and IP hoaxing. By altering the source IP address in the control message, malicious nodes attain impersonation. To encourage nodes to change their routing tables make believe to be pleasant node such as attacks counter to routing table is the additional purpose to impersonation. Man-in-the-middle attack is one of the fascinating impersonations. By uniting plummeting and hoaxing attacks, malicious node makes this attack. We should stop it from accepting any supplementary route information data to the destination so that it must be the only node in range of the destination. Using attacks counter to the routing table the malicious node may also alter the routing tables of dupe node. Malicious node pauses at this moment for an RREQ message to the destination node from

source node. Malicious node drips the RREQ and returns to a hoaxed RREP message to source node as if the approaching from the destination node when source node sends an RREQ message [14]. Malicious node achieves to create a route both to the source and the destination node and attacker controls the communication among the source and the destination by undertaking this. Malicious node can easily get the up layer communication if the communication is encrypted and involves a validation to MAC or IP address [14].

4.2.5 Modification Attack

To begin the direct and true path control messages are used. Amending content of the control messages (e.g. RREQ, RREP, RRER etc.) is done by malicious nodes to route packets to the way they need. If the message does not cast out its usual tasks it is called as modification. Hop counter, sequence number, life time etc. are concede along with control messages as route information data. For creating a true route this information has an immense role [14]. Malicious node can achieve its own attacks amending these fields in the control messages. To make believe as an additional node in the network impersonation is only achieved by the amending source. To misinform the dupe or the intermediary node and this amendment is counter to the replay messages for altering route informational data in the control messages. Malicious node needs to alter the route information of the dupe node for instance by altering the hop counter or the sequence number in the RREP messages. Firstly, malicious node seizes the RREP message and finally directing it to the demanded node in this type of attack. It picks up the inflated route in the network when the dupe node obtains this false message. To affect the net performance or its intention must be self-interested, it does not death to route the packet when the malicious node aims for it. By telling a number of fundamental nodes and reducing hop count field of the RREP messages to accomplish this attack. Detour attack is the other name for this attack. By altering the destination IP field in any control message another attack is accomplished. The communication is broken and thus, messages are not furthered to significant role. To perform the denial of service (DoS) attack or to additional malicious node to gather the total network dump, malicious node may do the directing [14]. More than one malicious node should be placed in the network and one of them should be positioned in the network to gather messages to perform the last one. Collective malicious nodes can attain all informational data about the network by this way.

4.2.6 Attack againstthe Routing Tables

To find supplementary nodes simply in the network every single node has its identification routing table. This routing table pulls the network topology for each node of the epoch (max. 3 seconds, duration of the ACTIVE_ROUTE_TIMEOUT perpetual value of AODV protocol) it's the equivalent time. Attacked nodes do not discover any route to supplementary node whom it wants to join if the malicious node attacks counter to this table [15]. By producing a new control message this attack is continuously performed. Fabricating attack is the other term for it. Counter to the routing tables there are several attacks. By fabricating false control messages every single one is ended. To endeavor a black hole attack, malicious node first conquers into the routing table of the dupe, directing false RREP message to endeavor a black hole attack. The legal network working links are noticeable as broken because malicious node also suppers deceitful RRER messages to the network. Using RREQ messages, additional attack type counter to the routing table is to try to generate loads of route entries for non-existent nodes. Routing table of the attacked node is occupied and does not have plentiful entry to form a new one as the end result. In contrast to the routing tables, attacks touch the network integrity, changing the network topology customary in the routing tables. Due to route discovery process and the network integrity in a wide area incorrect control messages are dispersed swiftly in the network. Network Integrity Attacks are recognized attacks counter to the routing table.

4.2.7 Sleep Deprivation Torture Attack (Battery Exhaustion)

To make the most of the battery life and mobile nodes choose to stop at the sleep mode when they are not used. One of the severe types of Denial Of Service Attacks is the Sleep Deprivation Torture which touches only nodes specially handled devices that has restricted resources [15].Attacker can proliferate some control messagesthrough the network in which other nodes are concerned in a period time. Rest of the nodes start processing these avoidable packets until their batteries wholly run out and permit to the operation mode from the sleep mode.

4.2.8 Black Hole Attack

Malicious nodes never ever refer true control messages primarily because of the dissimilarities of Black Hole Attacks associated to Gray Hole Attacks. Malicious node waits for the adjoining nodes to send the RREQ messages to bring out the black hole attack. Malicious node deprived of examining its routing table instantaneously sends a RREQ messages to bring out a black hole attack [3]. Deprived of examining its routing table malicious node instantaneously sends a false RREP message giving a way to destination over itself ,allocating a high sequence number to resolve in the routing table of the target node before supplementary nodes send a right one when the malicious node obtains a right message. When initiating to direct packets over malicious node entreating nodes take off for granted that route discovery method is accomplished and snub other RREP messages. Malicious node attacks takes over wholly routes and attacks all RREQ messages. When they are not furthering any place all packets are directed to a point. Gulping of all activities and stock is called black hole parallel. Malicious node should be should be situated at the epicenter of the wireless network to thrive a black hole attack. Every message will be accelerated to the prey node if malicious node cover ups false RREP messages as if it rises from an alternative prey node as a substitute for itself. Prey node will have to process all arriving messages and is imperiled to a sleep deprivation attack by doing this. Black hole attack affects the complete network while gray hole attacks in contrast to one or two nodes in the network to segregate them [5]. Malicious node does not direct false messages and thus, it stabs gray hole attacks which cannot be alleged simply. Due to plummeting of the messages, comportment of botched or encumbered nodes may appear like selfish node attacks. Botched nodes cannot customize a black hole attack even though they will drop the message afterwards since, botched nodes cannot formulate a new control message. AODV Routing Protocol and this attack type will be illustrated.

4.2.8.1 BLACKHOLE ATTACK IN AODV PROTOCOL

In an ad-hoc network that uses the AODV protocol, a Blackhole node swallows the network traffic and drops all packets. To explain the Blackhole Attack i added a malicious node that displaysBlackhole behavior in the scenario of the figures 4.1 in below.

Assuming that Node 3 is the malicious node. When Node 1 broadcasts the RREQ message for Node 4, Node 3 instantly responds to Node 1 with an RREP message that includes the maximum sequence number of Node 4, as if it is coming from Node 4. Node 1 assumes that Node 4 is behind Node 3 with 1 hop and rejects the newly received RREP packet come from Node 2.

Afterwards Node 1 starts to send out its data packet to the node 3 trusting that these packets will influence Node 4 but Node 3 will drop all data packets. In a Blackhole Attack, after a while, the sending node understands that there is a link error because the receiving node does not send TCP ACK packets [13]. If it sends out new TCP data packets and discovers a new route for the destination, the malicious node still operates to deceive the sending node. If the sending node sends out UDP data packets the problem is not identified because the UDP data connections do not wait for the ACK packets [13].

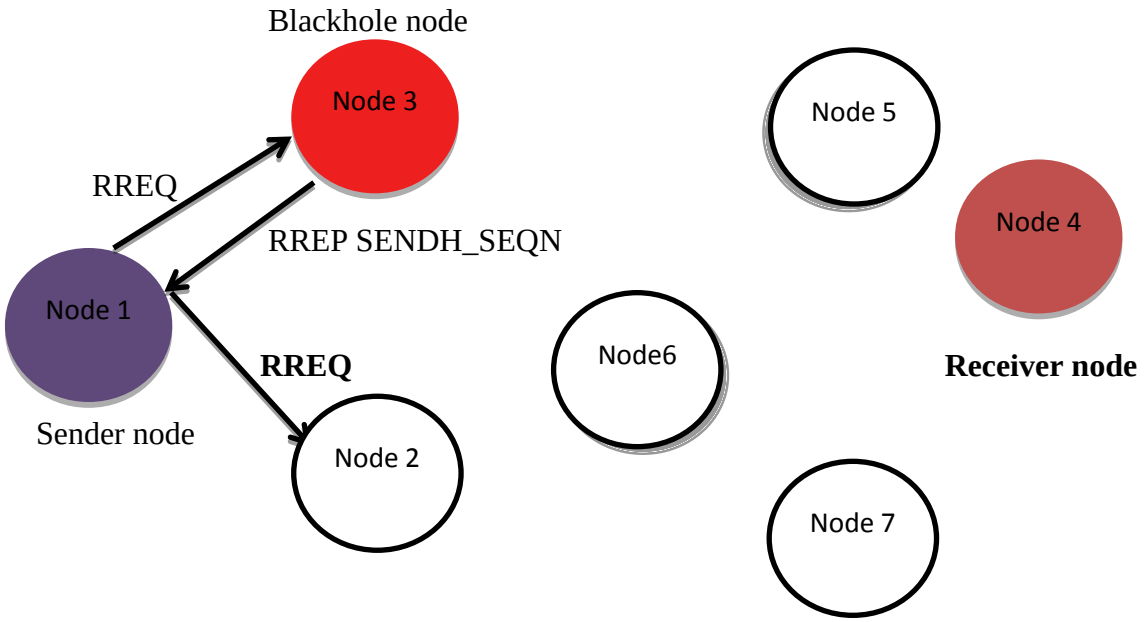

Figure4.1: Blackhole node scenario

4.2.9 SEQUENCE NUMBERS

Sequence Numbers serve as time stamps and grant the nodes to compare how fresh their information on the other node is. However when a node sends any type of routing control message, RREQ, RREP, RERR etc., it raises its own sequence number. Higher sequence number is more accurate information and whichever node sends the highest sequence number, its information is perceived and route is established over this node by the others.

The sequence number is a 32-bit unsigned integer value (i.e., 4294967295). If the sequence number of the node reaches the highest possible sequence number, 4294967295, then it will be reset to zero (0). If the results of subtraction of the modern stored sequence number in a node and the sequence number of incoming AODV route control message is below zero, the stored sequence number is modified with the sequence number of the incoming control message [5].

While Node 2 forwards the RREP message coming from Node 3, it matches its own last stored sequence number with that of Node 3. If it notices that the sequence number is newer than its own, then it changes its route table entry as required.

4.2.10Flooding Attacks

The flooding attack is tranquil to apply but causing the utmost damage. This type of attack can be attained either by using RREQ or Data flooding [16]. In RREQ flooding the attacker overflows the RREQ in the entire network which grosses a lot of the network assets. This can be attained by the attacker node by choosing kind of I.P addresses that do not occur in the network. By exploit so no node is capable to response RREP packets to these flooded RREQ. In data flooding the attacker grows into the network and fixed up paths between all the nodes in the network. Once the paths are recognized the attacker inoculates an enormous volume of useless data packets into the network which is focused to all the other nodes in the network [16]. These enormous uninvited data packets in the network obstruct the network. Any node that assists as destination node will be demanding all the time by reception of useless and unsolicited data all the stint.

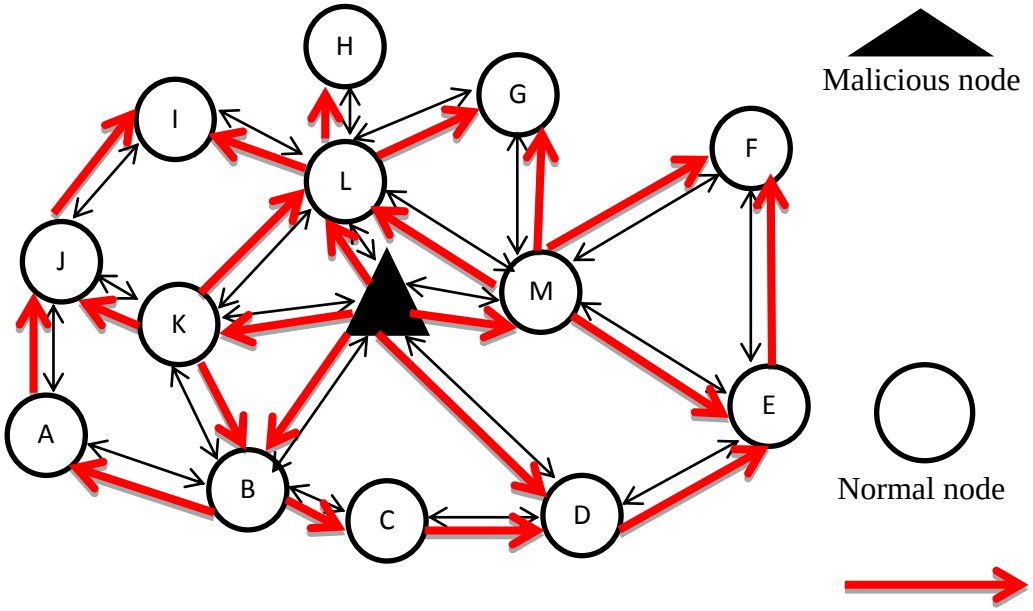

Fig.1 The Ad Hoc Flooding Attack

4.2.11 Introduction to Malicious node

Any node under attack in ad hoc network displays an anomalous behaviour called the malicious behaviour. In this situation, the entire operation of a network gets disturbed and to prevent such malicious behaviour several security solutions have been utilized. There are some nodes whose main purpose is to cause harm and disorder to the network. These type of nodes, referred as *malicious* nodes, do not show their identities while disrupting network services [16]. The objective of the malicious nodes is to maximize the damage before they are detected and removed. They are also rational, and their payoff is determined by the amount of damage they cause due to their disturbing nature.In order to minimize the impact of the malicious nodes, detection mechanism needs to be worked out. Thus, a regular node should be used to look into its surroundings and differentiate a malicious node from a regular one. However, the detection process has is not easily incorporated. First, monitoring is very costly. To identify the malice, a regular node has to listen to the channel and/or process the information sent by the nodes being monitored. The listening and processing take down the resources of a regular node. Hence, an “always on” monitoring scheme is not efficient even if it could prevent the damages. Second, the malicious node can disguise itself. To reduce the

chances of being detected, a malicious can behave like a regular node and work its way in longer intervals to attack the network. Third, the randomness and unreliability of the wireless channel bring more limitations to the monitoring and detection process[16].

Not only, is identifying the malicious nodes the end of the story. In most of the cases, a malicious node is eradicated as soon as it is detected, there might be situations where malicious nodes can be kept and purposely used. The most straightforward reason for the coexistence is that a malicious node has no idea whether it has been tracked or not, and it will continue to operate like a regular node to prevent from being detected. During this course, i.e., when the malicious node cooperates in disguise, it can be feated for normal network operations. This "involuntary" help from the malicious node may be important, especially when the network resource is limited. As a matter of fact, from the perspective of the malicious nodes, coexistence gives them a longer lifetime in the network [16].

CHAPTER 5

RESEARCH METHODLOGY

5.1 RESEARCH METHODOLOGIES

Major Data and Ancillary Data-The main content of data for learning the particular tool i.e. Network Simulation version 2 has been collected from the book "Introduction to Network Simulator" by springer and I got help from the internet where many lectures and many websites are accessible which provided help for implementation and execution of the project in Network Simulation version 2.35.

Software used for Research:

- *VMware version 8.0*- It is a software which helps in virtualization and clouding of the software. There are different operating system with which it is compatible like Microsoft windows, Linux, Mac OS X and many other operating systems also.
- *Ubuntu version 12.04*- It is a different kind of operating system which is known as Linux operating system, its desktop is unity by default, in past the desktop environ was different, where GNOME were used. These are available free of cost.
- *Network Simulator version 2.35*- I have executed and implemented my project on the Network Simulator version 2.35. It is based on Linux software, to install this particular software VMware 8.0 in collaboration with Ubuntu 12.04 is used.

5.2SIMULATION TOOL

There are different simulation tool available in market but for MANET researcher community prefer Discrete Event scenario. This software is highly compatible with different tangible environs models to grasp outcome, due to which the Network Simulation version 2.35 is the primary choice for researchers and in addition the Network Simulator versions 2.35 is an open source.

5.3INTRODUCTION TO NETWORK SIMULATOR

Network Simulator program concept was developed by University of California Berkley, which is an event driven network simulation code, it contain different high level network objects like protocols, energy models, pattern of traffic foundations. Network Simulator is a fragment of VINT project which is endorsed by DARPA since 1995.

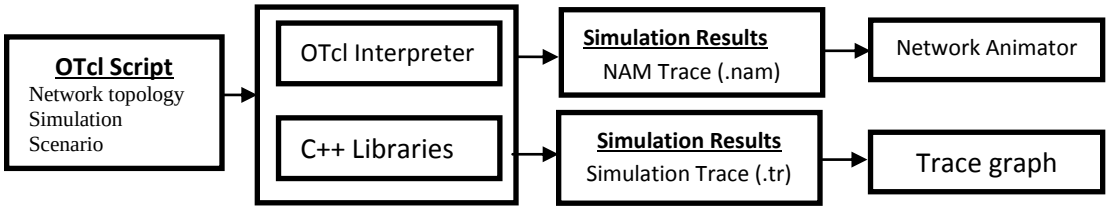

Figure 5.1: Network Simulator version 2 representation

Programing language used in network simulator is "Object Oriented Tool command Language" to decode the user written program code. OTcl is an object oriented language. Tcl scripts written by users are interpreted by Network simulator. Tcl scripts are combination of C++ program codes. Figure 4.1 explains there are two imperative study, one is Network Animation, which represents the pictorial animatronics of program code simulation. Another one is trace file which is used for the study of comportment of all objects in a simulation. NAM software uses ".nam" file while as trace software uses ".tr" file which contains all traces of simulation.

NS project is usually disseminated lengthways with diverse sets (nam, otcl, ns,tcl, etc.) termed as "compact set", although it can be downloaded one by one also. In my thesis I have implemented my program code on NS 2.35 (Network Simulator version 2.35). I have inscribed ".tcl" files in the text editor, and have examined the results with the help of ".tr" file in collaboration with **"awk", "wc", "cat"** commands of Unix operating system. Implementation of Blackhole comportment to AODV protocol is done in C++.

5.4 SIMULATION SETUP

Parameters	Value
Routing Protocol	AODV
Simulation Time	20 s
No. of Mobile Nodes	40
Transmission Area	1300*1300
Mobility Model	Group Mobility Model
Type of Traffic	UDP
Data Packet Size	1024
Rate	5 mb/s
Speed Of a node	15 m/s
Proposed RREQ Rate Limit	10

Table 5.1: NS-2.5 Simulation Setup

This table explains different parameters and their values in a simulation used to implement the particular program code, Ad hoc on demand distance vector is used as routing protocol. Simulation time used is 20 seconds. No of movable nodes are 40. Transmission area used is 1300*1300 meters. Mobility model used is group model, in nodes moves in uniform speed in one particular direction. User datagram protocol is used as traffic agent. Packet size is 1024 bits taken into account. Rate at which date is transferred from one node to another is 5mb/s. Speed at which nodes move with the Transmission area is 15 m/sec. Route Request broadcast limit is 10 packets per second.

5.5 PROPOSED METHODOLOGY TO DETECT FLOODING ATTACKS IN MANET

In this proposed work following are the methods which were being implemented:

A) Neighbour Selection:

Source node selects its neighbour nodes within the range of 250 meters then divides nodes which comes within 200 meters where cluster of nodes is formed and nodes which come within 50 meters of range. Nodes present in the range of 200 meters broadcasts route request packet to nodes which come within the range 50 meters, these nodes are considered to be monitoring nodes. These monitoring nodes will check the RREQ_ Broadcast rate for every selected nodes which comes within 200 meters of range from source node.

B) Updating Routing Table:

Monitoring node will send route reply packets back to the source node about the collecting information from selected node which are within the range of 200 meters from source node. Then source node will check its routing table entries if RREQ_Broadcast rate of selected nodes rate is greater than RREQ accept limit rate, then node is considered to be a malicious else if RREQ_Broadcast rate of selected node is smaller than RREQ accept limit rate then node is considered to be genuine node.

C) Cluster Head Formation:

After source node making changes in routing table entries will select a genuine node which will be closer to destination node is selected as cluster head and malicious node will be isolated from other intermediate node. In similar way other cluster of nodes will be formed with their respective cluster heads which will be close to destination, after which data is send from source to destination via different intermediate cluster heads.

5.5.1 ALGORITHM FOR DETECTION OF MALICIOUS NODE UNDER FLOODING ATTACK IN MANET

Route Request -> RREQ

Value of Threshold Limit -> VTL

Broadcast Limit for RREQ -> BLR

Testing Nodes -> TN

Nodes within the Radial range of Source node ->NRS

- STATE :: Begin
- CHECK (NRS) {
- If
- CONDITION ::NRS =200 meters
- Close neighbours.
- CALL PROCESS_RREQ
- Else
- CONDITION : : 200m< NRS <=250m
- Monitoring nodes
- CALL PROCESS_RREQ }
- CHECK NODE (BLR,VTL)
- { IfCONDITION : : BLR < VTL
- STATE : : Acceptance
- Process as normal.
- Else ifCONDITION : : BLR >= VTL
- STATE : : Malicious node
- Add to Black list
- Else
- STATE : Termination }
- Stop.

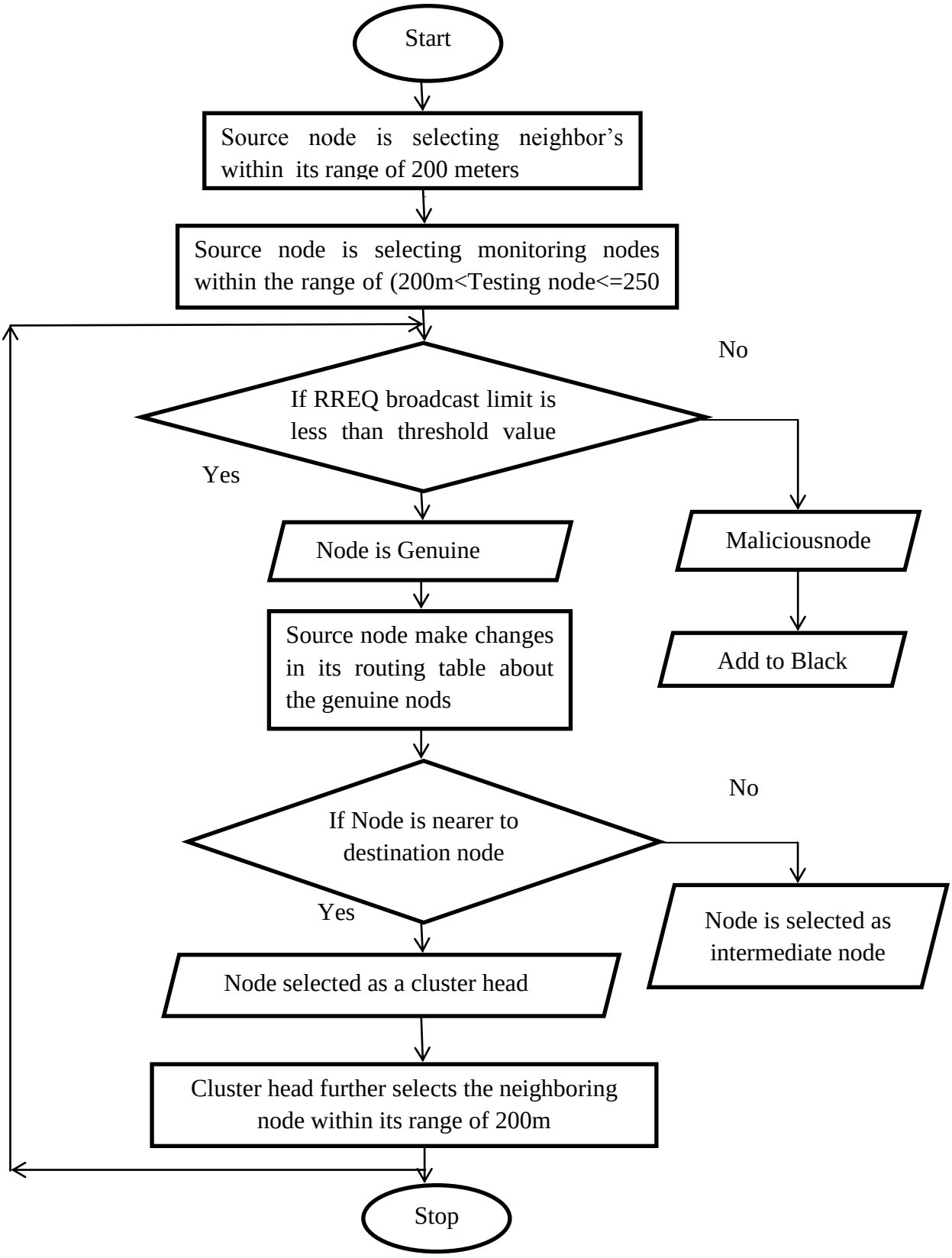

Figure 5.2 Representsdetection of malicious node in MANET under attack

5.5.2 OVERVIEW OF USUAL AND MALEVOLENT BEHAVIOUR OF A NODE

This unit explains the usual and malevolent characteristics of a node in MANET's. Firstly the usual behaviour of node has been explained and then its malicious behaviour has been explained.

(i) Usual Behaviour **–** During the transferring of data packets from source node to destination nodein an ad hoc network, security principals like (Authenticity (Au), Non-Repudiation (NR),Availability (Av),Confidentiality(C), and Integrity (I)), have to keepmaintained, therefore it is called as usual behaviour of a node.

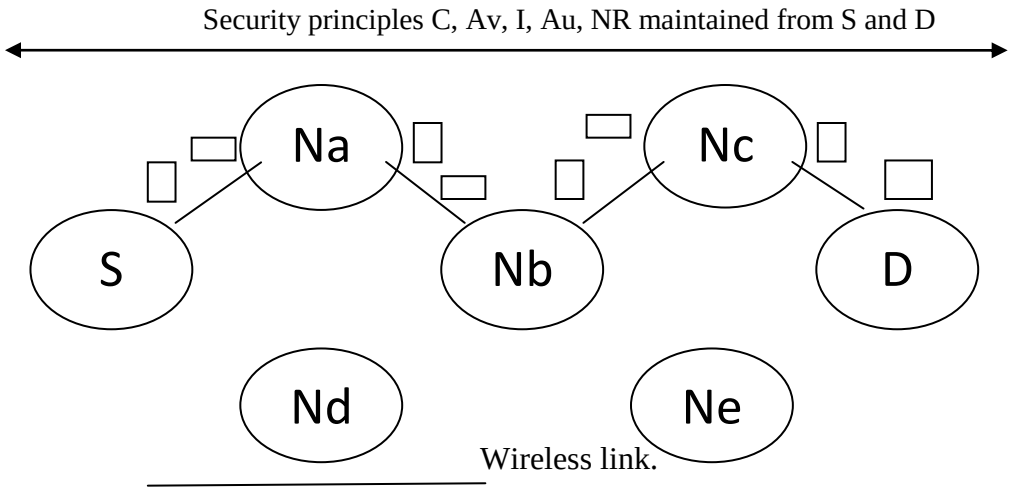

Figure 5.3 Normal behaviour of packet transfer

Figure 5.3 explains the usual mechanism of packet transference from source to destination node, in which Na, Nb, Nc, Nd and Nf are the intermediary nodes.

(ii) Malicious Behaviour-When there is a security breach in particular by any node that node is known as malicious node, and shows the following behaviour.

A. Dropping packets-When packets start falling and do not reach to its destination.

B. Exhausting Battery power– There is unwanted battery consumption till its end by malicious node on needless procedures.

C. Overflow of buffer- There are false updates filled in buffer so that authentic node won't get chance to store its updates, so there is preoccupation of memory.

D. High Bandwidth Intake -There is a high intake of bandwidth by malevolent node,
So that other genuine node won't get chance to use it. .

E. Incoming of Malicious Node - A malevolent node can work autonomously irrespective of its certification.

F. Injecting Fusty Packets -Malevolent node injects unwanted packets generate turmoil in a network

G. Delay- There is deliberate delay in advancing of packet because of malevolent node.

H. Link Breakdown-Malevolent node create link breakdown during the transference of data between two genuine nodes.

I. Altering in Message- A malevolent node can alter the insides of the packets.

J. Disagreeing from Directing Data Packets- Malevolent node can disagree from sending data to other authentic nodes.

K. Bogus Routing-Malevolent node have capability to crafting a false route in order to grasp the confidential information.

L. Unavailability of Node -A malevolent node detach the node so that it won't take part in task in order to generate delay.

M. Pilfering Information-A malevolent node can take confidential data, content, whereaboutsand sequencenumber for future attacks.

N. Capturing of Session –A malevolent node can capture the session between two authentic nodes in order to collect some confidential information.

O. Others- There are other methods also through which a node behaves in a malicious manner.

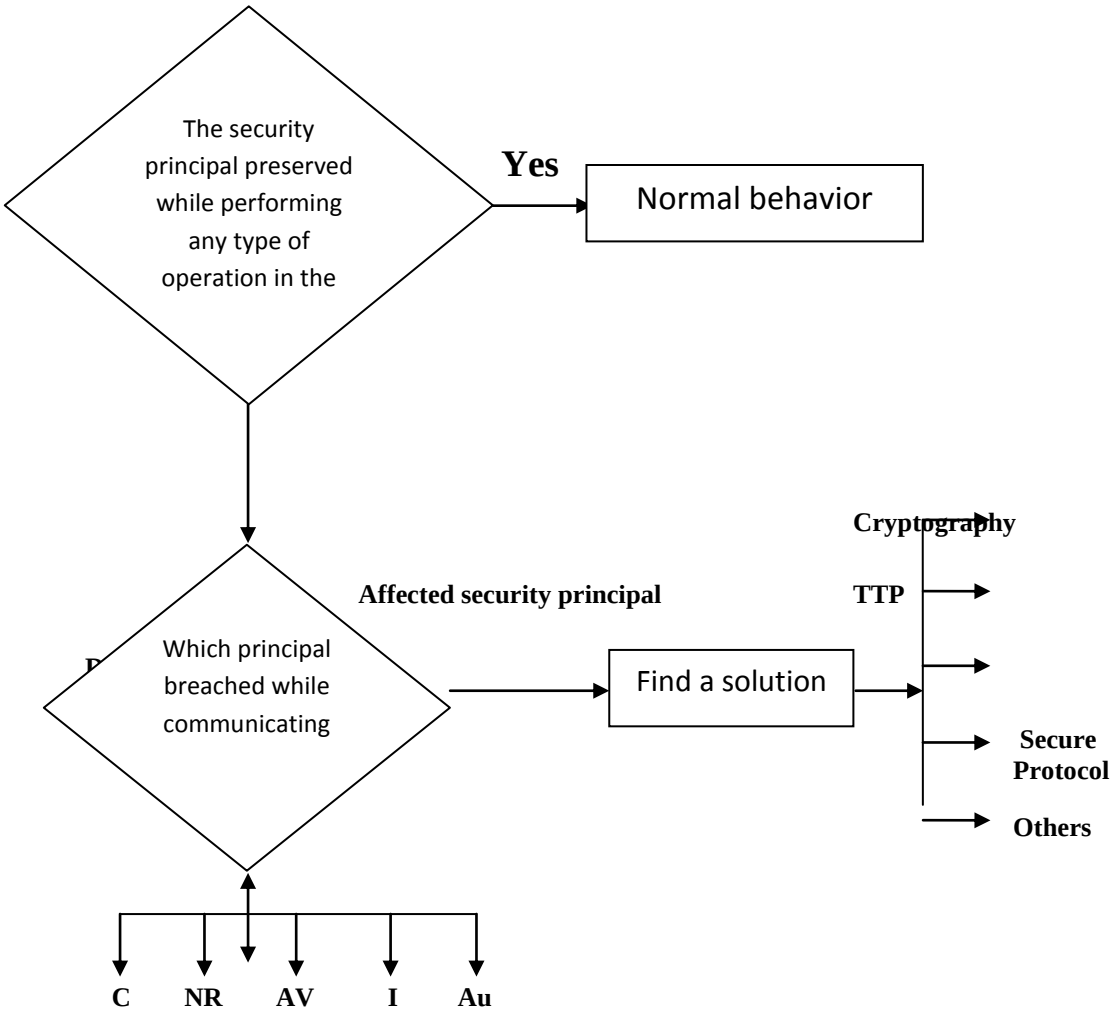

Fig.5.4 Defined Algorithm for usual& Malevolent Behaviour of a Node

The normal and the malicious behaviour of a node described above can be easily figured by the algorithm shown in Fig 5.4.

5.6 IMPLEMENTINGANEWROUTINGPROTOCOLIN NS2.5 TO SIMULATE BLACKHOLE BEHAVIOR

In order to implement the Black hole node in a MANET using NS-2, some modifications are required to show the packet dropping character of node. Every routing protocols are installed in core directory of NS-2.35. Firstly AODV protocol is replicated in the main directory, the name of directory is been changed to **"blackholeaodv"**.

File with name of AODV is been changed to **"blackholeaodv"** like blacholeaodv.cc, blackhole.h, blackhole.tcl,etc except "aodv_packet.h". The interesting is that AODV and "**blackholeaodv"** will transfer the same data packet as that of AODV packets. Every is changed like function, classes, structs, constants and variable names excluding struct names of AODV packet.h program code. Both the two protocols are same basically, in order to integrate Blackhole aodv with NS-2 some more changes are required.The first file modified is "*tcl**lib*\ *ns-lib.tcl*",Second file which is worked out is "*makefile*" in the root directory of the "**ns-2.35**".After these changes, there is need of inserting the blackhole characteristic in a program code which is done with the alteration in the blackhole.cc file.

5.7 INTRUSION DETECTION SYSTEM

An intrusion is technically defined as "an attempt by an unauthorized body to compromise the authenticity, integrity, and confidentiality of a resource." The role of an intrusion detection system (IDS) is to try to trap a hacker's presence on a compromised network, to flush out any malfeasance because of the hacker's presence, and to catalogue the activities so that similar attack scan be bypassed in the future. Intrusions consists of the following type of attacks:

(i) Malign sensitive information on internal networks.

(ii) Appropriate confidential and proprietary information.

(iii) Dampen functionalities and resources provided to possible legitimate users.

IDSs are needed to prevent problems arising due to an attack. Correction of the damage wrought by an attacker and the subsequent legal issues can be much costly and time consuming than detecting the attacker's presence and eradicating him at an earlier stage. IDSs give a better logged account of the means and modalities used by the notorious attackers, which can be used to prevent and circumvent possible attacks in the future. Therefore, present day intrusion detection capabilities provide organization with a good source for overall security analysis. The question as to what kind of intrusion detection system to deploy is proportional on the size and scale of the organizations internal networks, the total amount of confidential information maintained on the network, and so on. From time to time, attackers will manage to comprehend other security measures, such as cryptography, firewalls, and so on. It is crucial that information regarding these compromises

immediately flow to the administrators. Such tasks can be accomplished by using intrusion detection systems. Negligence of administrators is a limitation in network security. With the help of intrusion detection systems, it can help administrators in finding out any remaining vulnerability or exploits that a potential attacker could use.

CHAPTER 6

SIMULATION AND RESULTS

6.1 SIMULATION OF VARIOUS TOPOLOGIES

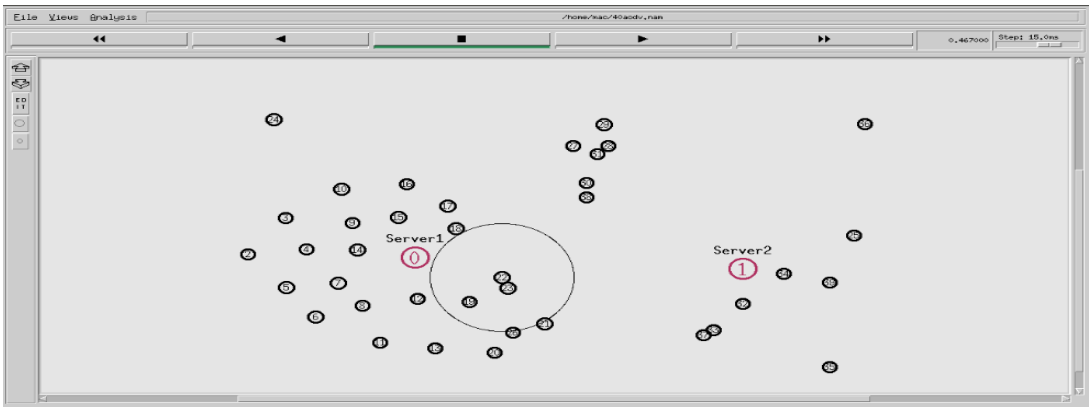

Figure 6.1: 40 node topology of AODV

In figure 6.1 server 1 acts as source node and server 2 acts as destination node for AODV protocol. Using NS-2.

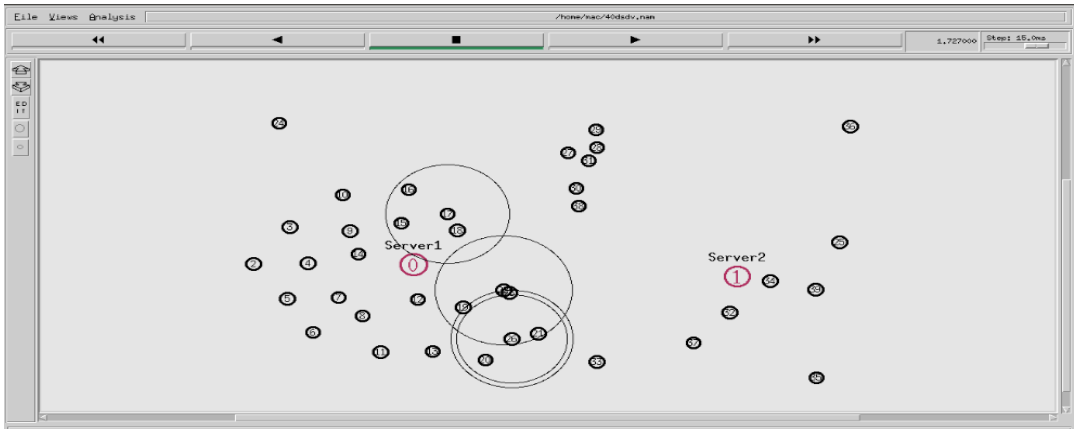

Figure 6.2: 40 node topology of DSDV

In figure 6.2 server 1 acts as source node and server 2 acts as destination node for DSDV protocol using NS-2.

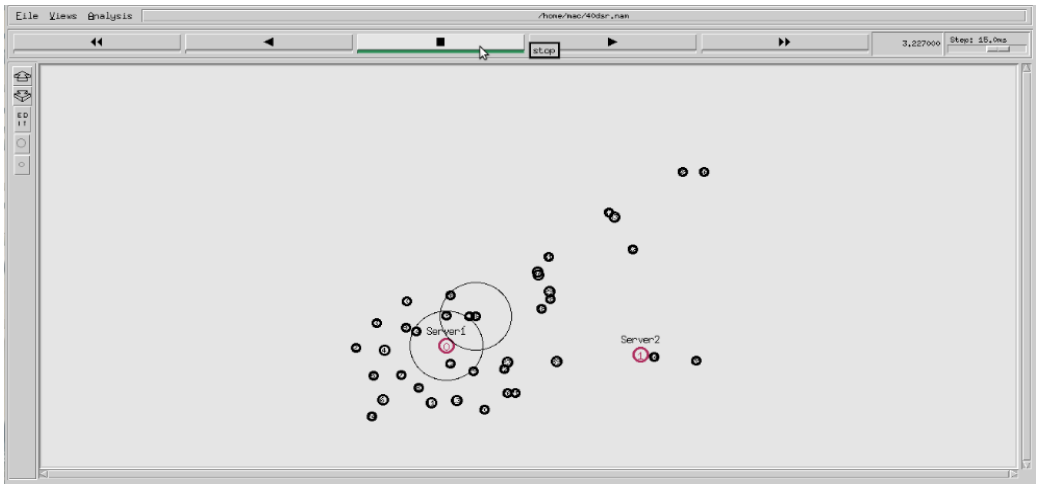

Figure 6.3: 40 node topology of DSR

In figure 6.3 server 1 acts as source node and server 2 acts as destination node for DSR protocol using NS-2.

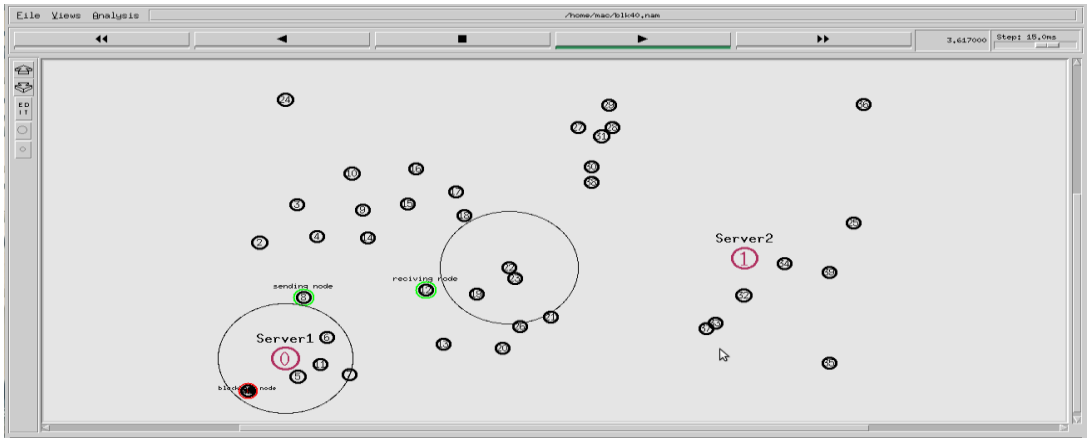

Figure 6.4: 40 node topology of blackholeAODV

In figure 6.4 node 24 has been detected as black hole while node 8 acts as source node and node 8 is acting as destination node,AODV has been used as routing protocol using NS-2

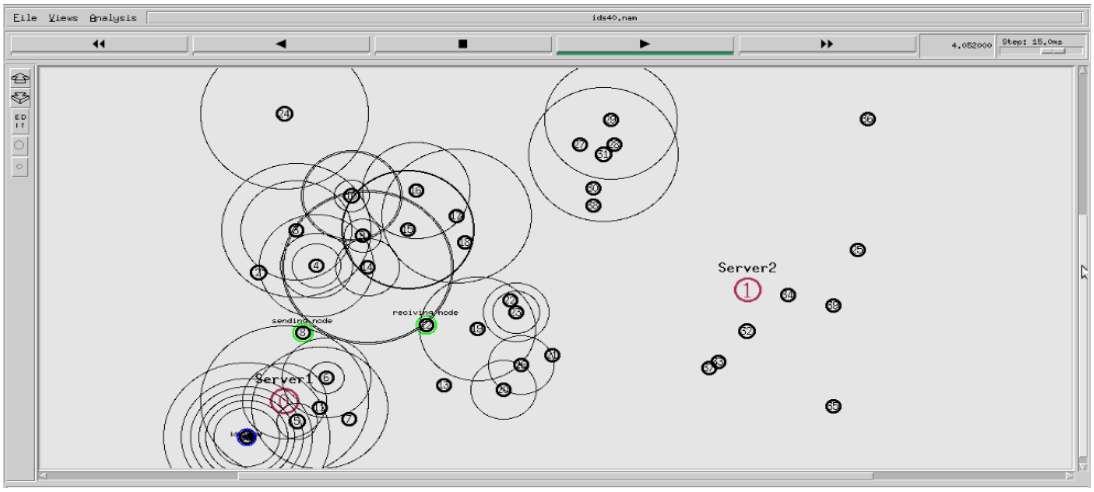

Figure 6.5: 40 node topology of idsAODV

In figure 6.5Intrusion detection systemtechnique has been implemented on AODV protocol in order to mitigate black hole attack. Here node 8 acts as source node and node 12 acts as destination node.

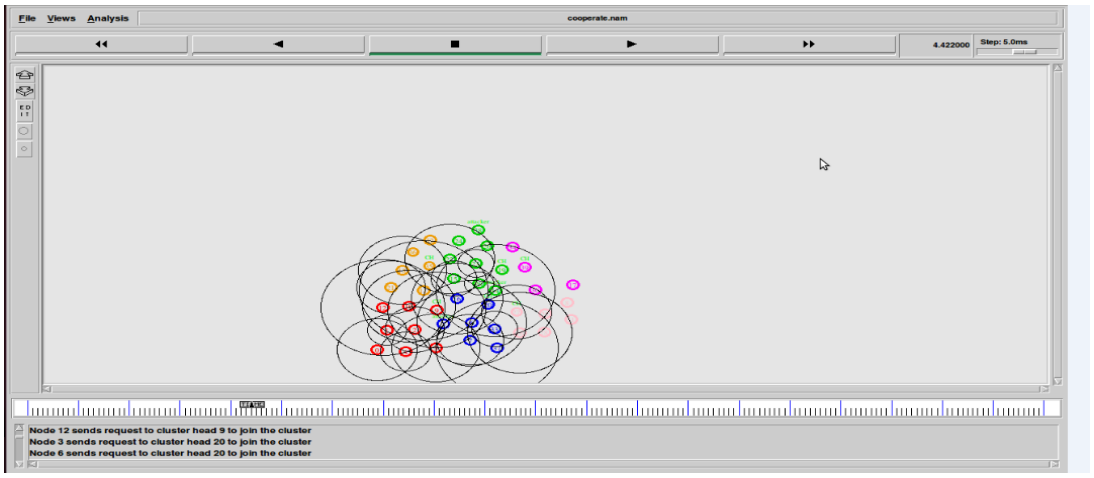

Figure 6.6: 40 node topology showing flooding attack.

In figure 6.6 nodes 35,19,27,39and 9 acts as cluster heads, nodes 9 and 14 act as malacious nodes. Node 0 act as source node and node 39 act as destination node.

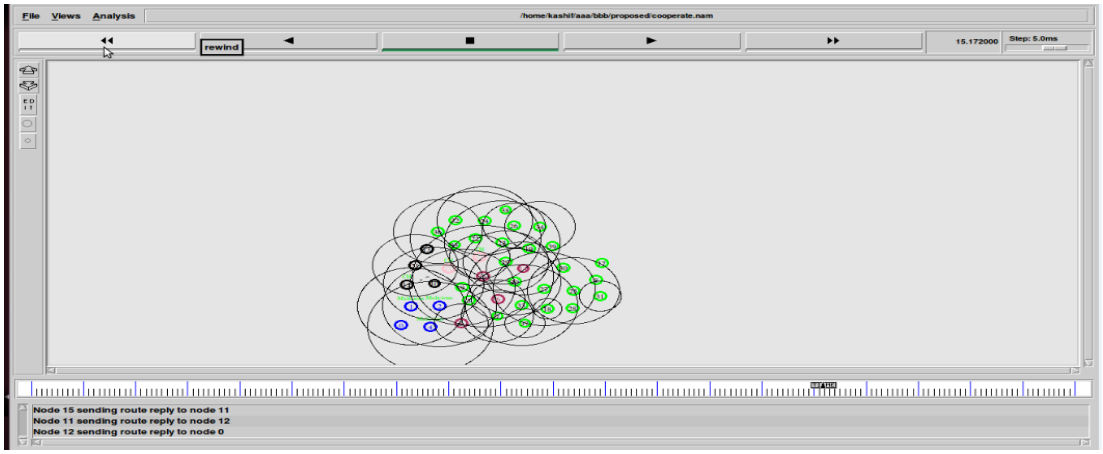

Figure 6.7: 40 node topology showing detection and prevention of flooding attack

In figure 6.7 nodes 12, 11 and 15act as cluster heads. Nodes 1, 2 and 4 act as malicious node. Node 0 is source node and node 39 is a destination node.

6.2 COMPARITIVE ANALYSIS USING TABLES

Table 6.1 Tabulated Results of Comparison of AODV, DSDV and DSR protocols

Protocol	AODV	DSDV	DSR
Total Nodes	20	20	20
Throughput	114.71	59.49	146.941
Normalized Routing Load	5.714	1.407	0.166
Packet Delivery Ratio	100	67.04	81.62

Protocol	AODV	DSDV	DSR
Total Nodes	30	30	30
Throughput	53.68	127.91	140.14
Normalized Routing Load	3.783	1.0	0.827
Packet Delivery Ratio	**98.70**	**70.14**	**69.72**

Protocol	AODV	DSDV	DSR
Total Nodes	40	40	40
Throughput	62.48	109.92	132.35
Normalized Routing Load	5.032	1.587	2.216
Packet Delivery Ratio	100	56.18	64.62

Table 6.2 Tabulated results of comparison between AODV and blackhole AODV protocol

Protocol	AODV	AODV	AODV
Total Nodes	20	30	40
Throughput	114.71	53.68	101.37
Normalized Routing Load	5.714	3.783	4.642
Packet Delivery Ratio	100	98.70	98.051

Protocol	blackholeAODV	blackholeAODV	blackholeAODV
Total Nodes	20	30	40
Throughput	2.02	22.11	19.60
Normalized Routing Load	329.80	51.242	87.51
PDR	3.246	21.428	20.129

Table 6.3 Tabulated results of comparison between blackholeAODV and idsAODV

Protocol	idsAODV	idsAODV	idsAODV
Total Nodes	20	30	40
Throughput	114.49	53.58	14.19
Normalized Routing Load	2.444	7.296	22.727
PDR	100	98.70	71.771

Protocol	blackholeAODV	blackholeAODV	blackholeAODV
Total Nodes	20	30	40
Throughput	3.65	9.21	13.53
Normalized Routing Load	128.778	47.886	67.353
Packet Delivery Ratio	5.844	22.72	22.077

Table 6.4 Tabulated results of comparison between before detection of malicious node which cause flooding and after the detection of malicious node .

Protocol	Total Nodes	Throughput	PDR	Overhead
AODV	40	20.42	.98825	1.426

Protocol	Total Nodes	Throughput	PDR	Overhead
AODV	40	73.20	.9948	1.4139

6.3 EVALUATION OF VARIOUS PARAMETERS THROUGH GRAPHS

A.Throughput-

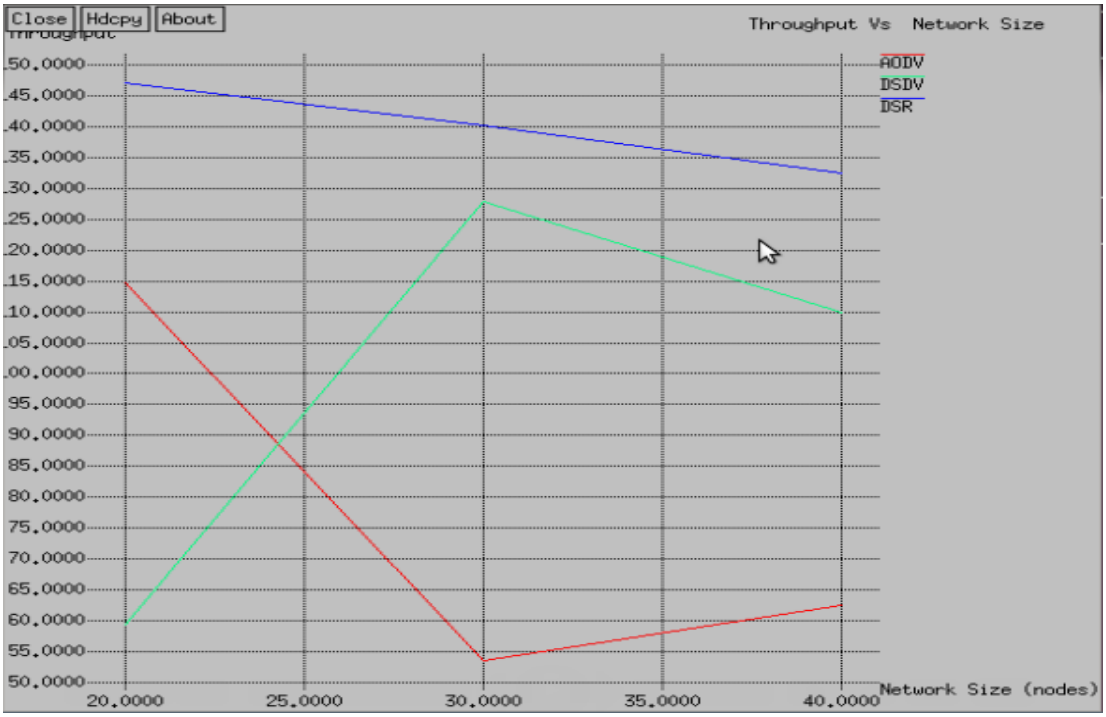

Figure 6.8 Throughputanalysis of AODV, DSDV and DSR

Figure 6.8 shows Throughput the analysis of AODV,DSDV and DSR protocols. Red line represents the throughput analysis of AODV protocol for 20,30 and 40 nodes.Green line represents the throughput of DSDV protocol for 20,30 and 40 nodes.Purple line represents the throughput analysis of DSR protocol.As in this figure throughput decreases while increasing the number of node in DSR protocol.Throughput for 20 nodes in AODV protocol is high and least for 30 nodes in AODV protocol.Throughput for 20 nodes is least in DSDV protocol while highest for 30 nodes in DSDV protocol. And this figure explains that DSR performs well for throughput while as DSDV performs normal for throughput and AODV perform low for throughput.

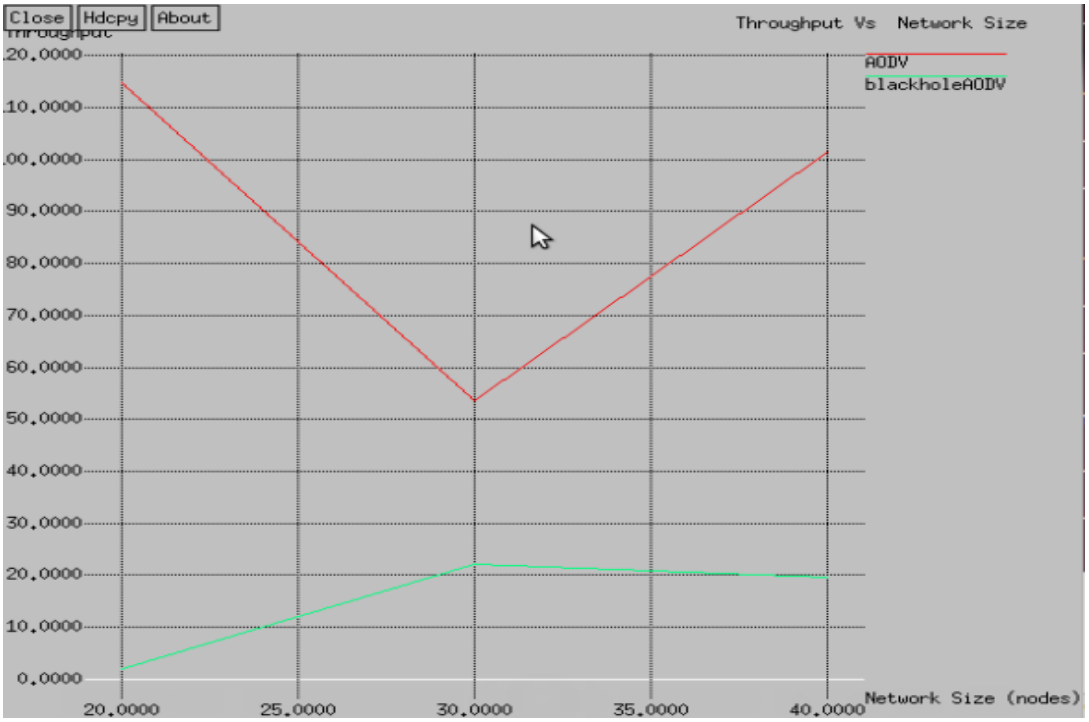

Figure 6.9 Throughputanalysis of AODV and blackholeAODV

Figure 6.9 shows Throughput the analysis of AODV, blackhole AODVprotocols. Red line represents the throughput analysis for AODV protocol for 20,30 and 40 nodes.Green line represents the throughput for blackhole AODV for 20, 30 and 40 nodes.As in this figure throughput for normal AODV protocol is high while as by inducing blackhole in the same network throughput will be decreasedwhich means by 20 node topology using AODV protocol is having throughput equal to 115 kbps approximately and lowest at 30 node topology which is equal to 55 kbps approximately while as throughput for 20 node topology in modified AODV protocol that is blackhole AODV is having lowest throughput equal to 3 kbps and highest for 30 node topology using blackhole AODV protocol equal to 22kbps approximately.

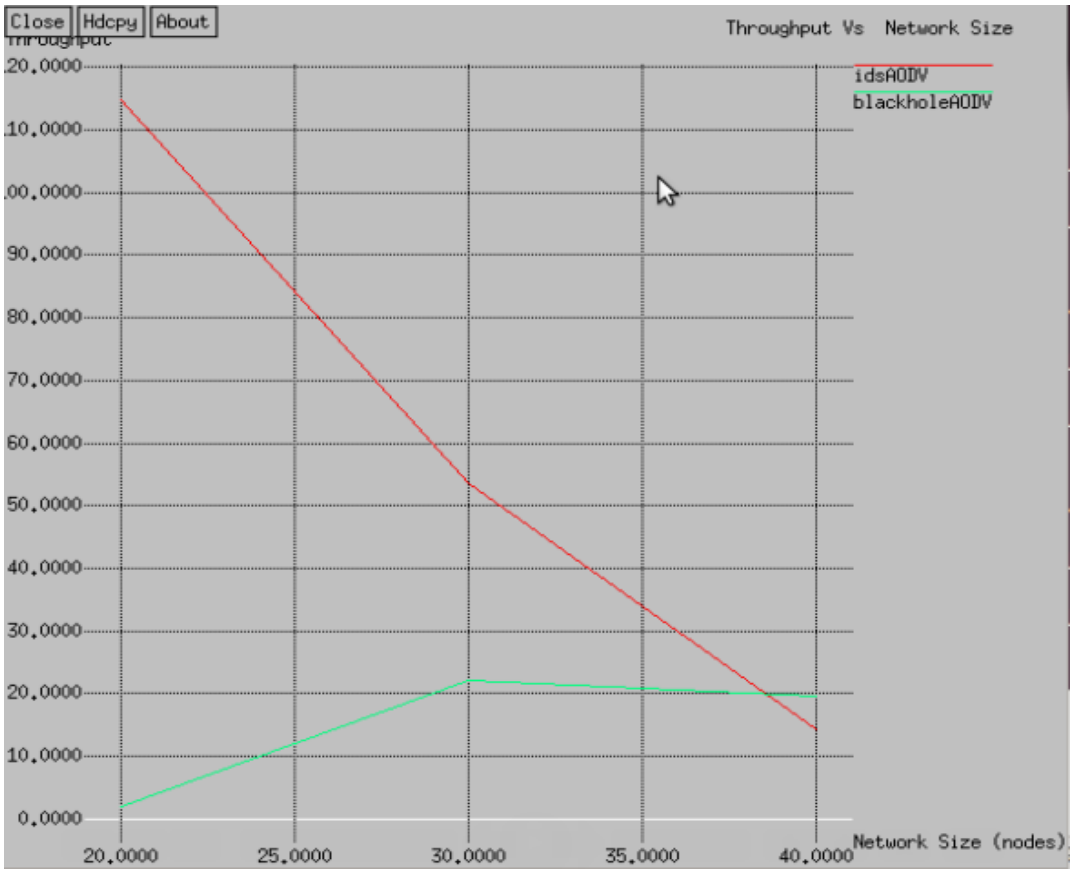

Figure 6.10 Throughput analysis of idsAODV and blackholeAODV

In figure 6.10 red line represents the modified AODV that is IDS AODV which means Intrusion Detection System has been implemented in AODV protocol which helps to provide security against different attacks in particular network.Green line represents the blackhole AODV protocol which means blackhole node has been induced in an AODV routing algorithm. In case of 20 nodes topology using IDS AODV routingprotocol,throughputis equal to 115kbps approximately and for 40 nodes topology throughput is equal to 15kbps approximately. While as in 20 nodes topology using blackhole AODV,throughputis approximate equal to 4 kbps and for 40 nodes topology throughput is approximately 20kbps.Which means this figure shows that IDS-AODV performs well in case of throughput and blackhole AODV performs low in case of throughput.

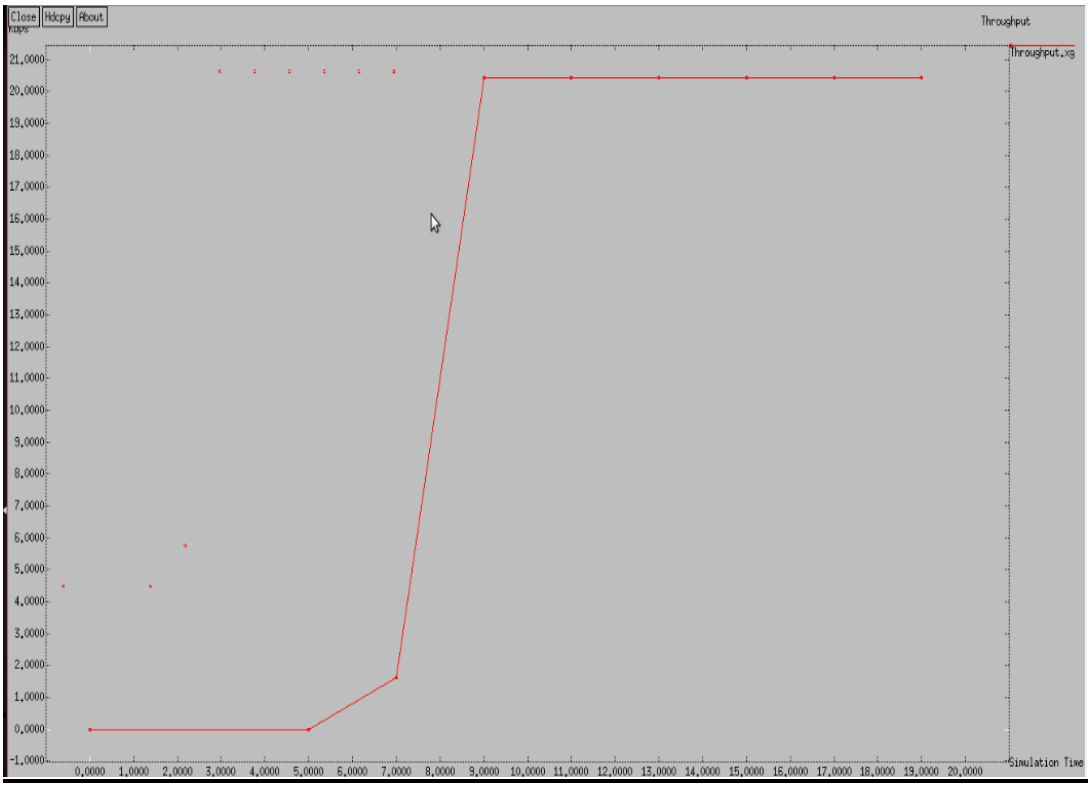

Figure 6.11: Throughput parameter vs. Simulation Time during flooding attack

Figure 6.11 shows at simulation time 0, 1,2,3,4 and 5 seconds the value of throughput corresponds to zero and from 5 seconds to 7 seconds of simulation time throughput increases to 2 kilo bytes per second.Then after 7 seconds throughput abruptly increases to 20 kilo bytes per second Upto 20 seconds simulation time It indicates that after completion of 8 seconds deployment of nodes at their respective positions takes place and every node starts communicating with their respective cluster heads, therefore the throughput of a particular network increases to 20 kilobytes per second.

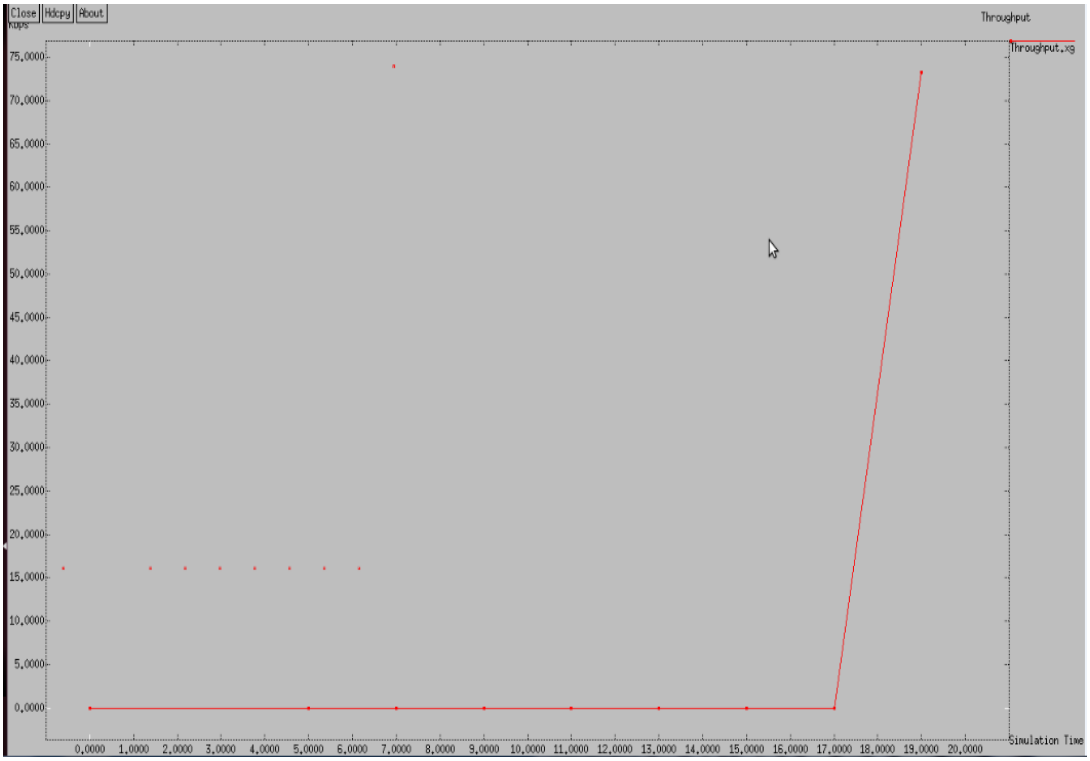

Figure: 6.12Throughput parameter vs Simulation Time

Figure 6.12 shows at simulation time 0, 5, 7, 9, 11, 13, 15 and 17 seconds the value of throughput corresponds to zero and at 19 second of simulation time throughput abruptly increases to 73.20 bits per second. It indicates that after completion of 19 seconds deployment of nodes at their respective positions takes place and every node starts communicating with their respective cluster heads, therefore the throughput of a particular network increases to 73.20 bits per second.

B. Overhead-

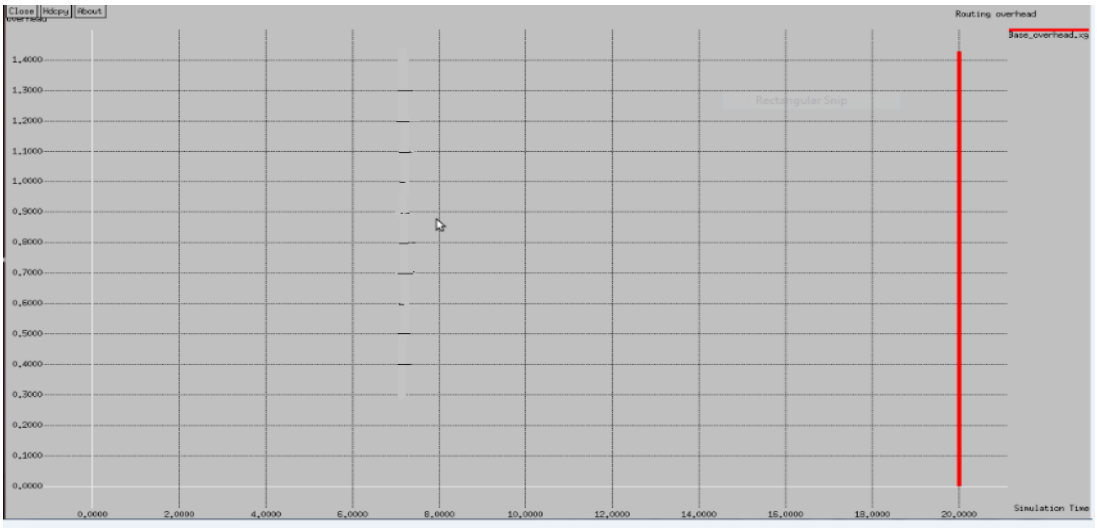

Figure 6.13:Overhead vs Simulation Time in presence of flooding attack

Figure 6.13shows the overhead parameter of the simulated network. At simulation time of 20 seconds the overhead value attained was 1.4139 in presence of flooding attack.

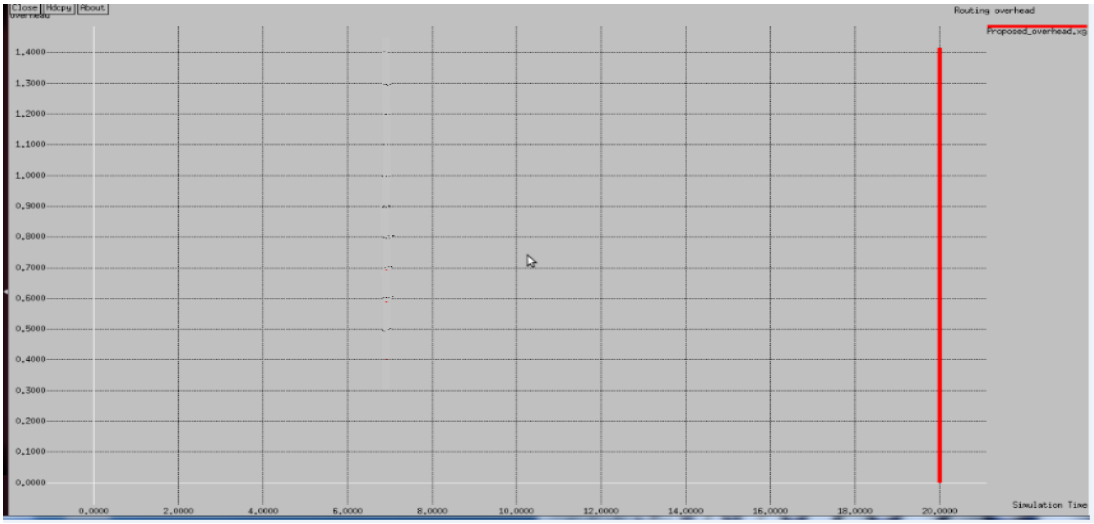

Figure 6.14:Overhead vs Simulation Time after detection of malicious node

Figure 6.14 shows the overhead parameter of the simulated network. At simulation time of 20 seconds the overhead value attained was 1.4139 in presence of flooding attack.

C. *Normalized Routing Load (NRL)*

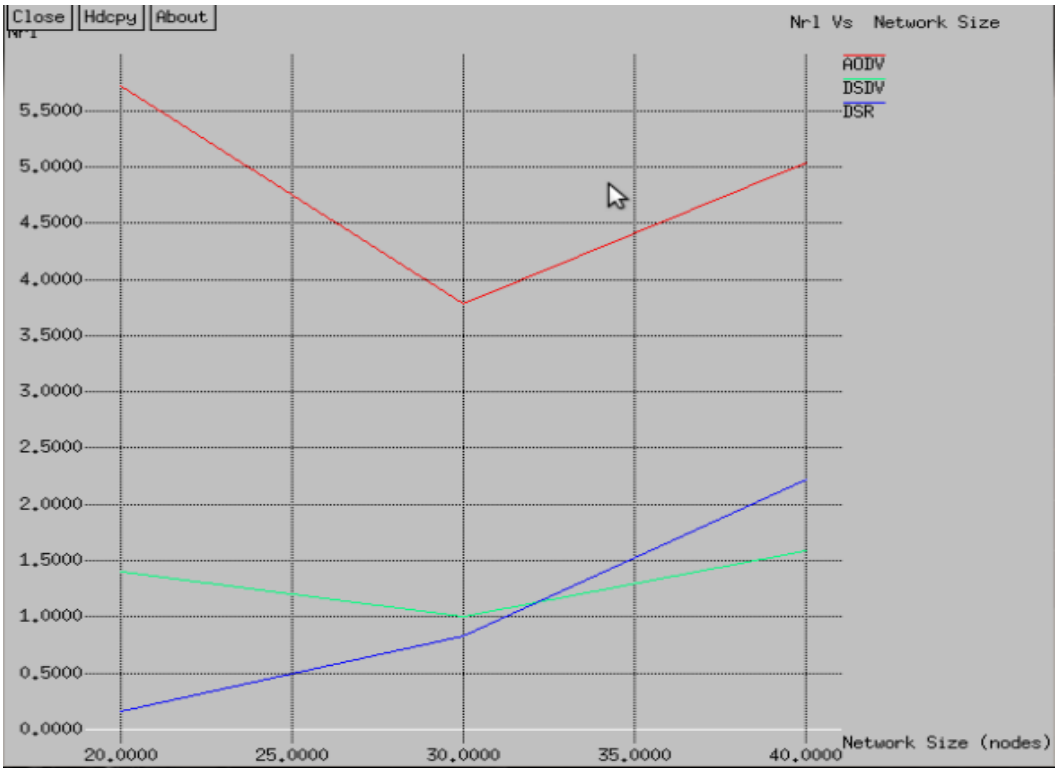

Figure6.15:NRL analysis of AODV, DSDV and DSR

Figure 6.15 shows NRL the analysis of AODV,DSDV and DSR protocols.Red line represents the NRL analysis of AODV protocol for 20,30 and 40 nodes.Green line represents the NRL of DSDV protocol for 20,30and 40 nodes .Purple line represents the NRL analysis of DSR protocol.This figure shows 20 nodes of AODV are having highest NRL and 30 nodes are having least NRL.40 nodes of DSDV is having higher NRL and 30 nodes are having least NRL.20 nodes of DSR are having least NRL and 40 nodes of DSR is having highest number of NRL.

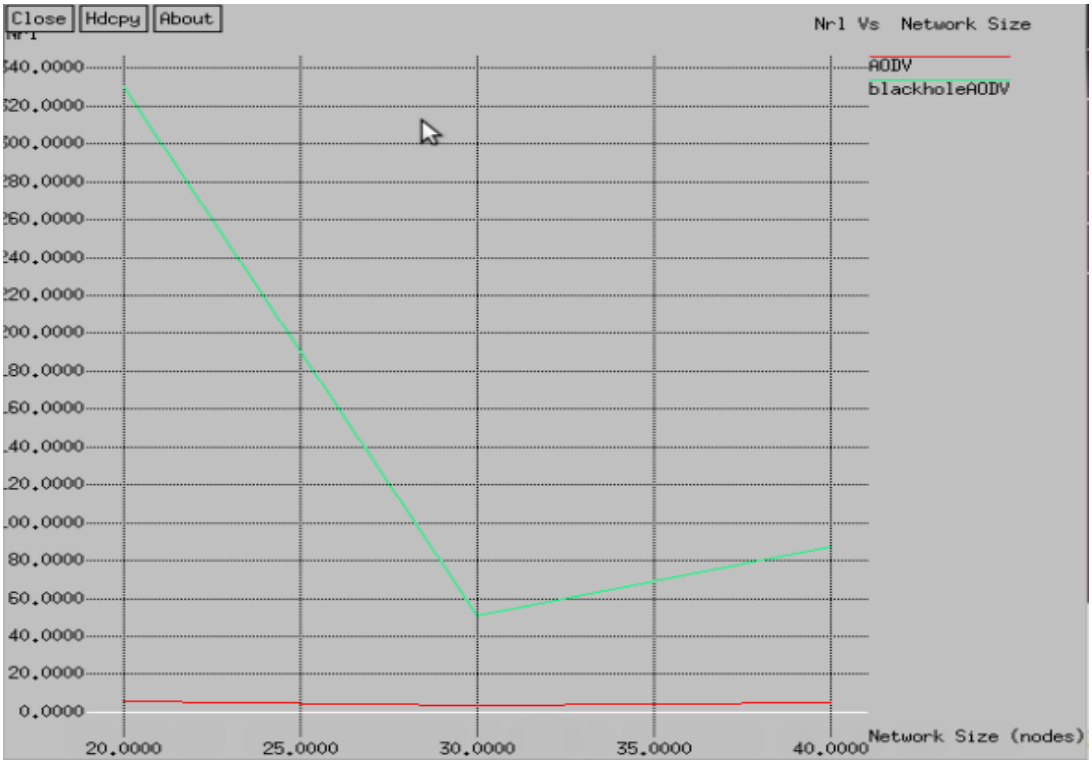

Figure 6.16: NRL analysis of AODV and blackholeAODV

Figure 6.16 shows NRL the analysis of AODV and blackhole AODV protocols.Red line represents the NRL analysis of AODV protocol for 20, 30 and 40 nodes.Green line represents the NRL of blackhole AODV protocol for 20,30and 40 nodes. This figure shows blackhole AODV are having high NRL than normal AODV, which means by inducing the blackhole node in the normal network it increases the normalized load of a network which resuls in congestion of network.

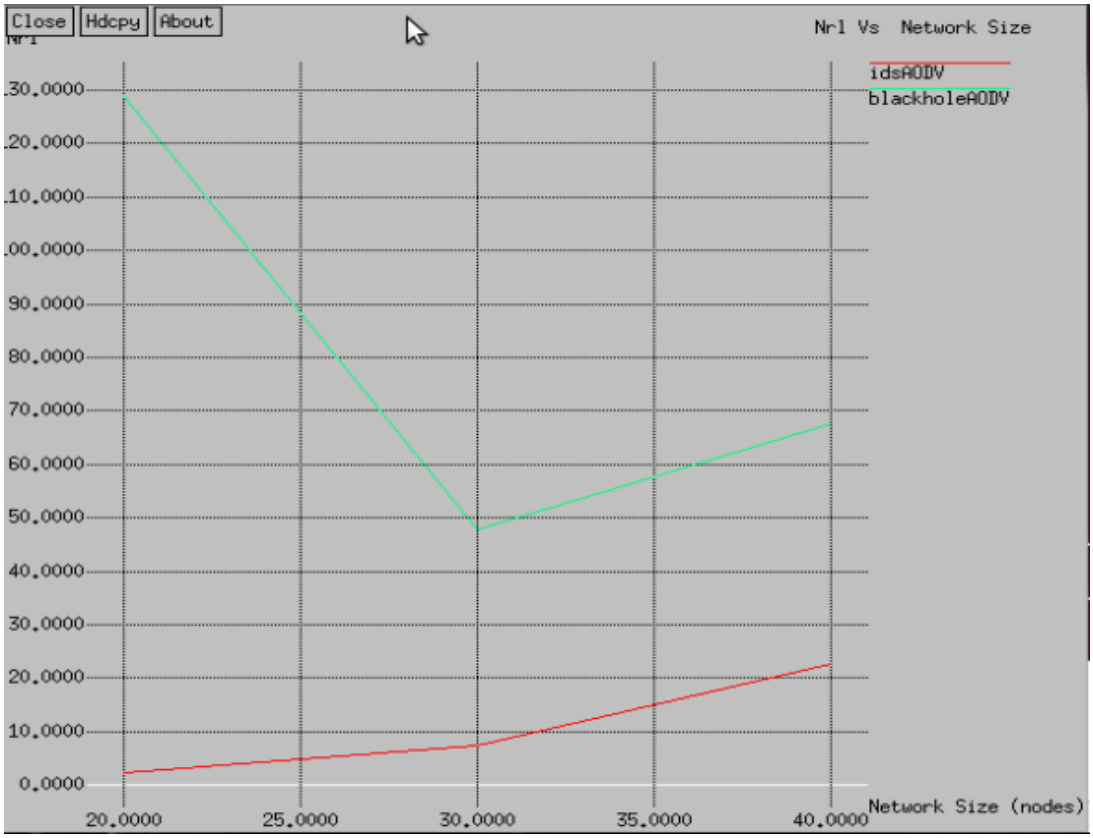

Figure 6.17: NRL analysis of idsAODV and blackholeAODV

Figure 6.17 shows NRL the analysis of AODV and IDS-AODV protocols.Red line represents the NRL analysis of IDS-AODV protocol for 20,30 and 40 nodes.Green line represents the NRL of blackhole AODV protocol for 20,30and 40 nodes . This figure shows IDS-AODV are having low NRL than blackhole AODV, for 20 node topology using IDS-AODV protocol the NRL is equal to 3 approximately and for 40 nodes topology the value of NRL is equal to 22 while as for 20 node topology using blackhole AODV protocol vale of NRL is equal to 30 and for 30 nodes topology vale of NRL is equal to 48 which means by inducing the blackhole node in the normal network it increases the normalized load of a network which results in congestion of network.

D. Packet Delivery Ratio (PDR)-

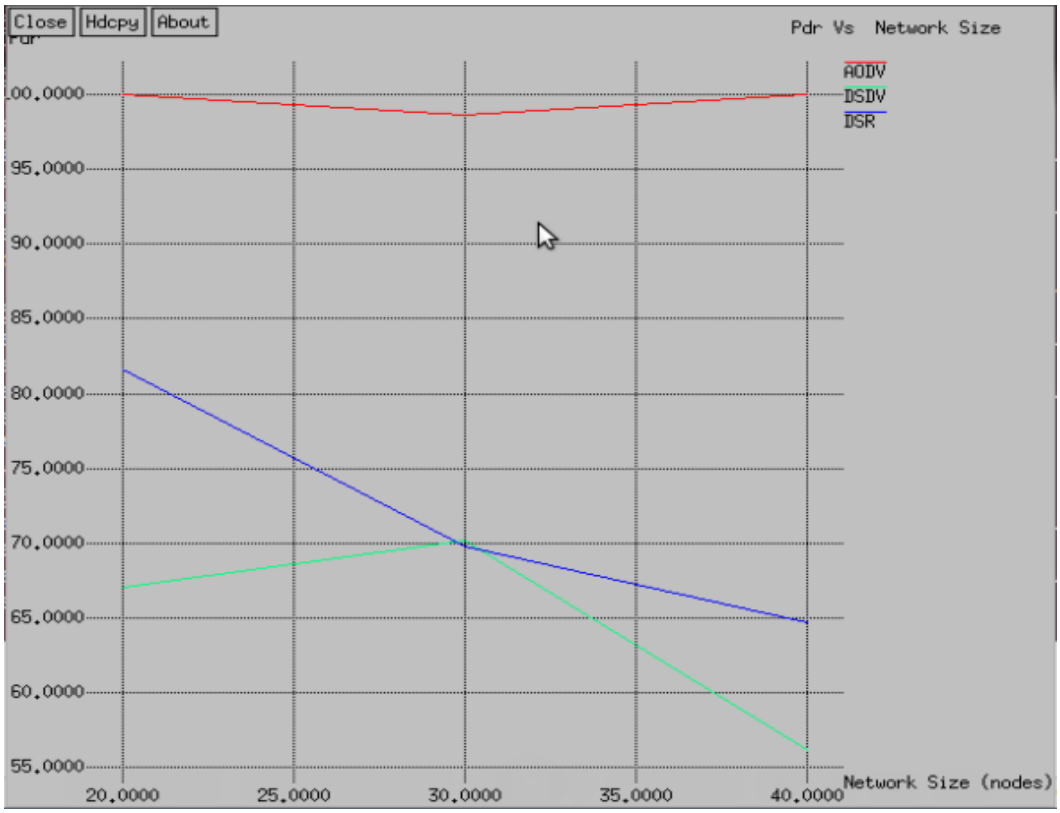

Figure 6.18: PDR analysis of AODV, DSDV and DSR

Figure 6.18 shows PDR the analysis of AODV,DSDV and DSR protocols.Red line represents the PDR analysis of AODV protocol for 20,30 and 40 nodes.Green line represents the PDR of DSDV protocol for 20,30,and 40 nodes .Purple line represents the PDR analysis of DSR protocol.20 and 40 nodes of AODV are having highest number of PDR and 30 nodes of AODV are having least PDR.30 nodes of DSDV is having highest PDR and 40 nodes of DSDV are having least PDR.20 nodes of DSR is having highest PDR and 40 nodes of DSR is having least PDR.

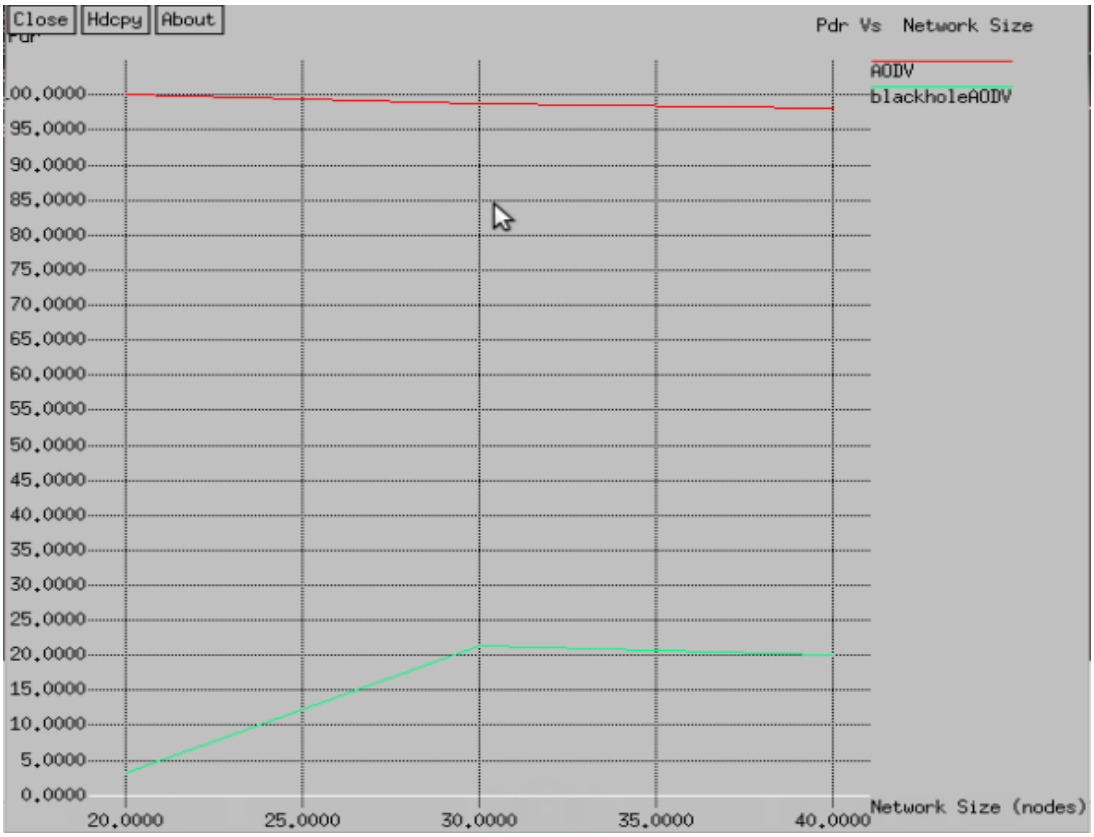

Figure 6.19: PDR analysis of AODV and blackholeAODV

Figure 6.19 shows PDR the analysis of AODV and blackhole AODV routing protocols.Red line represents the PDR analysis of AODV protocol for 20,30 and 40 nodes.Green line represents the PDR of blackhole AODV protocol for 20,30 and 40 nodes. For 20 nodes topology using AODV routing protocol the value of PDR is equal to 100 approximately and for 40 nodes topology its vale is equal to 98 approximately while as for 20 nodes topology in presence of blackhole the value of PDR is equal to approximately 3 and for 40 nodes topology the value of PDR is equal to 20. Hence it can be clearly observed that particular network performs well for PDR using AODV routing protocol while as value of PDR is degraded when black hole node is present in a particular network.

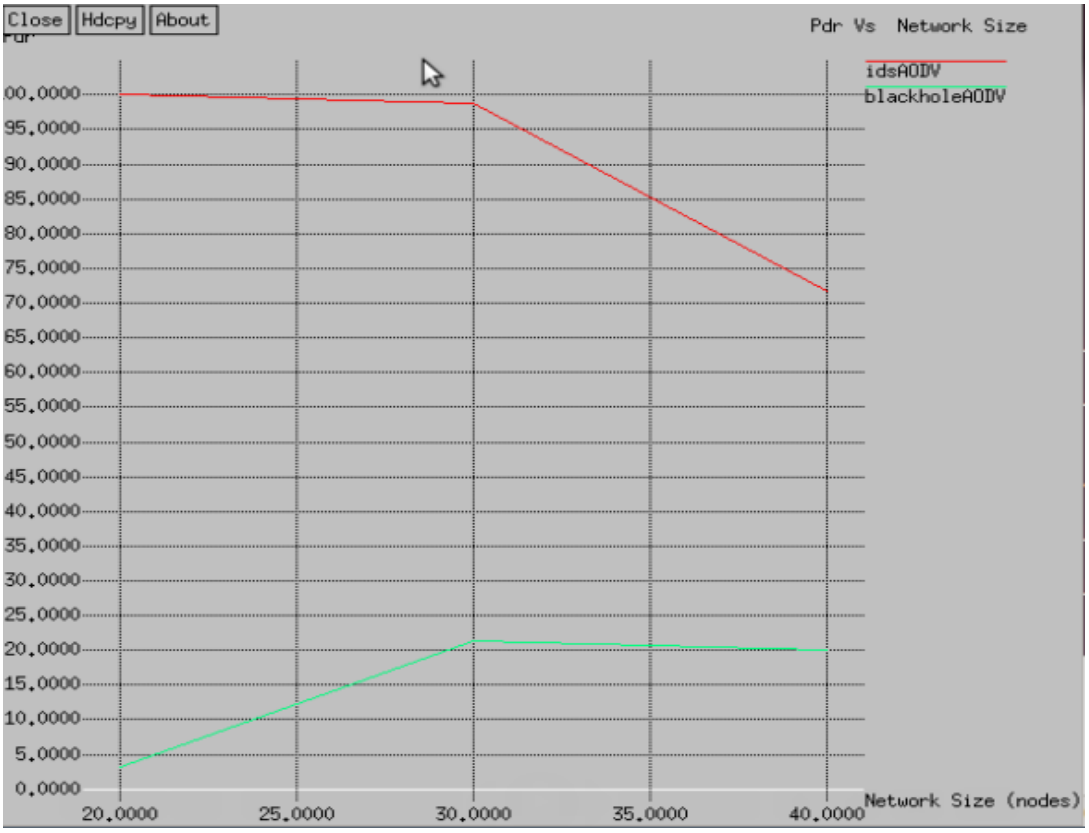

Figure 6.20: PDR analysis of idsAODV and blackholeAODV

Figure 6.20 shows PDR the analysis of IDS(Intrusion Detection System)-AODV and blackhole AODV routing protocols. Red line represents the PDR analysis of IDS-AODV protocol for 20, 30 and 40 nodes. Green line represents the PDR of blackhole AODV protocol for 20, 30 and 40 nodes. For 20 nodes topology using IDS-AODV routing protocol the value of PDR is equal to 100 approximately and for 40 nodes topology its vale is equal to 73 approximately while as for 20 nodes topology in presence of blackhole the value of PDR is equal to approximately 3 and for 40 nodes topology the value of PDR is equal to 20. Hence it can be clearly observed that particular network performs well for PDR using Intrusion Detection Systemin AODV routing protocol in presence of Black hole while as value of PDR is degraded when black hole node is present in a particular network.

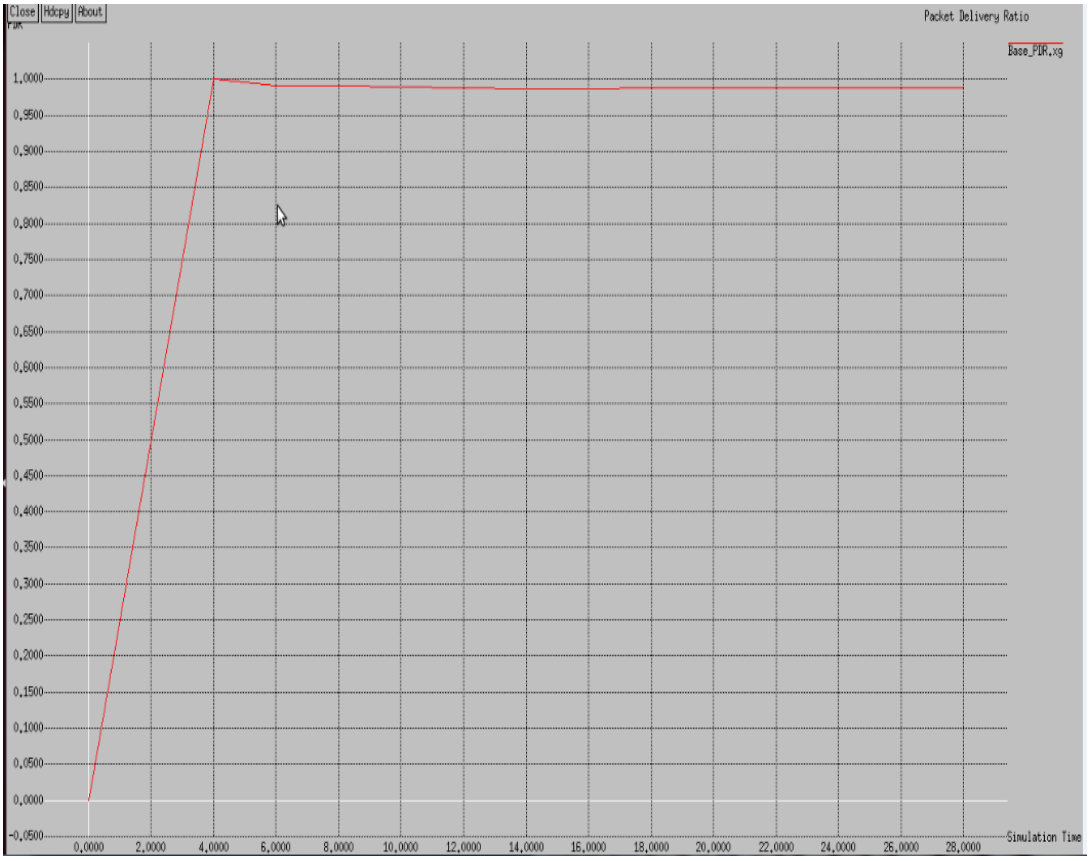

Figure 6.21:PDR vs Simulation Time in presence of flooding attack

Figure 6.21 shows the PDR analysis40 nodes topology using AODV routing protocol. As it can be clearly observed that from simulation time 0 second to 4 seconds it has been abruptly increased to .988 approximately then after 4 seconds value of PDR has been fluctuated in between 4 seconds upto 20 seconds of simulation time the values varies from (.977 to .988) in presence of malicious node.

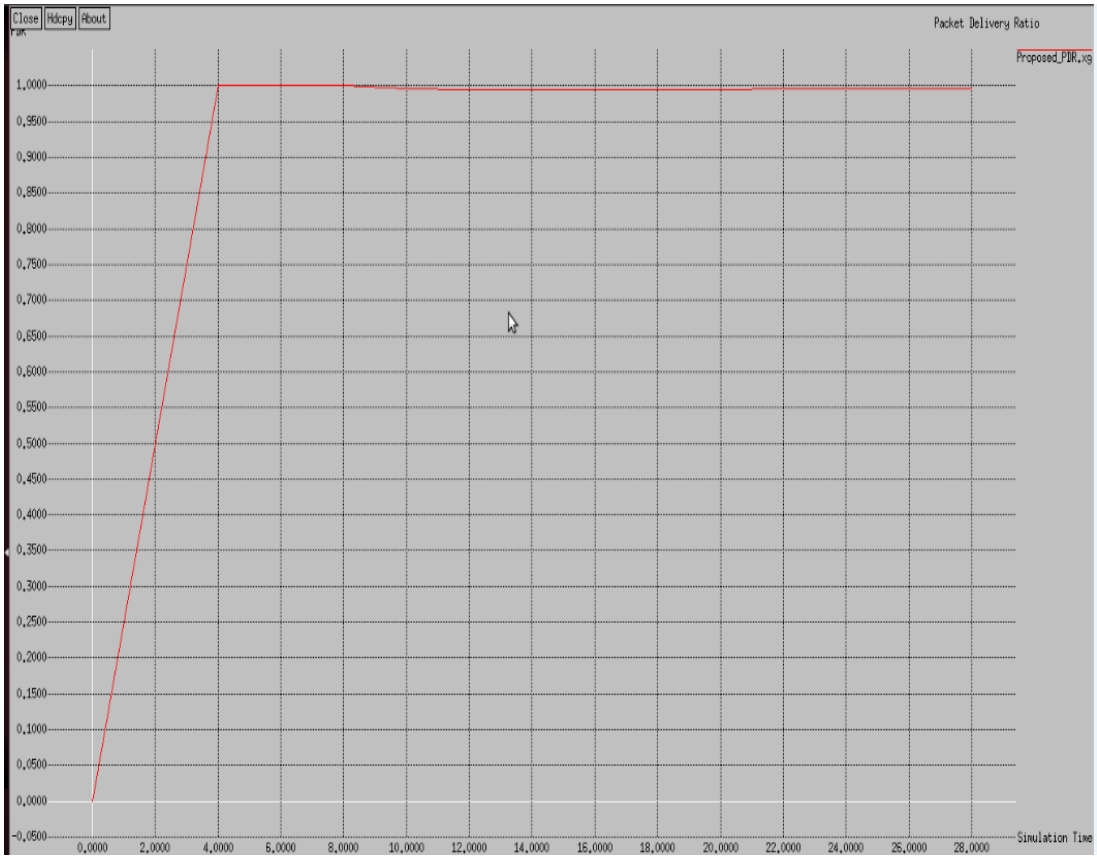

Figure 6.22:PDR vs Simulation Time after detection of flooding attack

Figure 6.22 shows the PDR analysis 40 nodes topology using AODV routing protocol. As it can be clearly observed that from simulation time 0 second to 4 seconds it has been abruptly increased to 1 approximately then after 4 seconds value of PDR has been fluctuated in between 4 seconds upto 20 seconds of simulation time the values varies from (.98 to .999) after detection of malicious node.

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1CONCLUSION

The area of ad-hoc networking has been gettingcumulativedevotion among scientists in latest years, as the obtainable wireless networking and mobile computing hardware roots are now adept of assisting the potential of this technology. Over the bygone few years, a assortment of newfangled routing protocols beleaguered specially at the ad-hoc networking situation have been proposed, but little enactment information on each protocol and node tailed performance assessment between the protocols has formerly been presented. This project has offered a paralleling performance of protocols for routing packets between wireless mobile hosts in an ad-hoc network AODV, DSR and DSDV with scenario consist of dynamic network size which used an AODV and DSR from On-Demand protocols compared with DSDV from proactive table-driven routing protocols. There is no clear winner among the protocols in our case, since different parameters seem to give different performance rankings of the protocols.It is always difficult to draw a conclusion that amongst these protocols which one is the best in all respects. There is always a trade-off between one and the other parameters. Every protocol has its own significance and depending on the type of application they are implemented on it is the user who decides which one would suite best.

And two attacks have been implemented while using AODV routing protocols that is **blackhole attack and flooding attack** Through the analysis and comparison of network simulation results, i can conclude that when the numberof nodes are varied, AODV has the highest Packet Delivery Ratio, Throughput and Normalized Routing- Load while in presence of blackhole node all the network parameters are degraded.

And in presence of malicious node which causes flooding also effects network parameters very badly. Both the attacks causes'plentiful degradation to network parameters but after comparing all the network parameters I observed that black hole attack causes more damage in comparison to flooding attack.

The general observation from my simulation:

- AODV Based on normal Distance Vector Algorithm, so that nodes keep up route cache and uses destination sequence number for each route entry, Route Discovery Mechanism is started when a route to new destination is desired by broadcasting a Route Request Packet (RREQ). And Route Error Packets (RERR) are used to remove broken links.
- DSDV is a proactive table driven routing protocol i.e. it keep up a table of every nodes in topology. Route Discovery Mechanism is started when the topology is established, when data is to be transmitted a nodes checks its table for the route of that particular node
- DSR has two main mechanisms: Route Discovery is like to the one in AODV but with source routing in its place and Route Maintenance is proficient through route caches each entries in route caches are updated as nodes learn new routes, several routes can be stored.

Besides that I also described myalterations to the *ns* network simulator in order to attack the nodes in topology for that I add new protocols like blackholeAODV and Malicious node and I also have taken measures to prevent these attacks using protocol idsAODV compared their performance with other protocols. Through the analysis and comparison of network simulation results, I can conclude that Throughput and Packet Delivery ratio are affected to a large extent when blackhole node is added in a topology while in case of malicious node causing flooding attack Throughput and Normalized Routing Load are affected to a large extent. When idsAODV is compared with blackholeAODV the Packet Deliver Ratio increases significantly.

7.2 FUTURE WORK

Wireless Ad-Hoc networks are widely used networks due to their malleable nature i.e. easy to arrange regardless of geographic limitations. These networks are open to both external and internal attacks as there is not centralized security mechanism. A lot of research work is still need in this area. I tried to determine and analyze the impact of Blackhole attack and Flooding attack in MANETs using AODV protocol. There is a need to analyze Blackhole attack in other MANETs routing protocols such as DSR and DSDV. Other types of attacks such as Wormhole, Jellyfish and Sybil attacks are needed to be studied in comparison with Blackhole attack and Flooding attack. They can be classified on the basis of how much they

affect the performance of the network. Blackhole attack can also attack the other way around i.e. as Sleep Deprivation attack. The detection of this behavior of Blackhole attack as well as the abolition strategy for such behavior has to be carried out for further research. In my project, I tried to eliminate the Blackhole effect in the network. But detectionof the Blackhole Node is another future work. In my project, I assume the blackhole node is detected and tried to eliminate its effects. There are many IntrusionDetection Systems (IDS) for ad-hoc networks. These IDSs could be tested todetermine which one is the best to detect the Blackhole. Additionally, I used UDP connection to be able to count the packets atsending and receiving nodes. If I had used the TCP connection between nodes, thesending node would be the end of the connection, since ACK packets do not reachthe sending node. This would be another solution for finding the Blackhole Node.This takes place after the route determination mechanism of the ADOV protocol andfinds the route in a much longer period. My solution finds the path in the AODVlevel. Finding the blackhole node with connection oriented protocols could beanother work as a future study.

And as I have used cluster head mechanism to detect the malicious node which causes Flooding attack in a network other different routing protocols other than AODV protocol and different mechanisms can also be used to detect the malicious nodes.

7.3 LIST OF PUBLICATIONS

KashifKawsarQadri, Vishali Sharma"Security Mechanism For Mitigation Of Flooding And Black hole attack using AODV Protocol In MANET"paper accepted in IJAER SCOPUSindexed.

References

[1]JaydipSen, SripadKoilakonda, ArijitUkil, “A Mechanism for Detection of Cooperative Black Hole Attack in Mobile Ad Hoc Networks” 2011 Second International Conference on Intelligent Systems..

[2] Jaspal Kumar, M. Kulkarni, Daya Gupta “Effect of Black Hole Attack on MANET Routing Protocols” I.J. Computer Network and Information Security, 2013, 5, 64-72 Published Online April 2013 in MECS.

[3] Yaserkhamayseh, Abdulraheem Bader, Wail Mardini, and MuneerBaniYasein,”A New Protocol for Detecting Black HoleNodes in Ad Hoc Networks,” International Journal of Communication Networks and Information Security (IJCNIS) Vol. 3, No. 1, April 2011.

[4Ketan S. Chavda, AshishV.NimavatPG Student, Master of Computer Engineering,C.U. Shah College of Engineering and Technology,”Removal Of Black Hole Attack In AODV Routing Protocol Of MANET”, 4th ICCCNT – 2013 July 4 -6, 2013, Tiruchengode, India,

[5] P. Manickam1, T. GuruBaskar , M.Girija , Dr.D.Manimegalai ,” Performance Comparisons Of Routing Protocols In Mobile Ad-Hoc Networks”, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 1, February 2011.

[6]KaminiMaheshwar; Divakar Singh,” Black Hole Effect Analysis and Prevention through IDS in MANET Environment”,European Journal of Applied Engineering and Scientific Research, 2012, 1 (4):84-90,

[7] VipinKhandelwal IC, Dinesh Goyal,”Black Hole Attack and Detection Method for AODV Routing Protocol in MANETs”, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 4, April 2013 1555.

[8]ShekharTandan and PraneetSaurabh,” A PDRR based detection technique for blackhole attack in MANET”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4), 2011, 1513-1516

[9] Harsh Pratap Singh, Sanjeev Sharma,” Guard against cooperative black hole attack in Mobile Ad-Hoc Network”, International Journal of Engineering Science and Technology (IJEST) Vol. 3 No. 7 July 2011.

[10]Mehdi Barati I, Kayvan, AtefiFarshad, YasharAzab, Daftari- “Performance Evaluation of Energy Consumption for AODV andDSR Routing Protocols in MANET”.

[11] TaranpreetKaur, Amanjot Singh Toor ,Krishan Kumar Saluja" Defending MANETs against Flooding Attacks for Military Applications under Group Mobility" Proceedings of 2014 RAECS VIET Panjab University Chandigarh, 06 - 08 March, 2014.

[12] Ping Yi, Zhoulin Dai, Shiyong Zhang, YipingZhong." A New Routing Attack in Mobile Ad Hoc Networks" International Journal of Information Technology Vol. 11 No. 2.

[13] Nitiket N Mhala1 and N K Choudhari "An Implementation Possiblities for AODV routing protocol in real world"

[14] SudhirAgrawal, Sanjeev Jain, Sanjeev Sharma "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks" Journal Ofcomputing, volume 3, issue 1, january 2011, ISSN 2151-9617.

[15] Abhijeetkumar, ArchanaBharti"Mitigation of flooding Attack in MANET using NS-3" International Journal for research in applied scienceand engineering technology (IJRASET)Vol. 2 Issue IV, April 2014 ISSN: 2321-9653.

[16] Meghna Chhabra1, Brij Gupta1, AmmarAlmomani"A Novel Solution to Handle DDOS Attack in MANET" Journal of Information Security, 2013, 4, page no.165-179.

[17]AlokparnaBandyopadhyay, SatyanarayanaVuppala,PrasenjitChoudhurya Simulation Analysis of Flooding Attack inMANET using NS-3978-1-4577-0787-2/11/$26.00 ©2011 IEEE.

[18] BounpadithKannhavong,Hidehisa Nakayama, YoshiakiNemotoandNei Kato, "A Survey of Routing Attacks in Mobile Ad- Hoc Networks" IEEE Wireless Communications" October 2007 1536-1284/07/$20.00 © 2007 IEEE page no 85-91.

BOOKS

[1]C.K. Toh, *Ad Hoc Mobile Wireless Networks: Protocol and System* "Adhoc Routing Protocols", Pearson Education, 2002

[2] C. Shiva Ram Murthy and B.S. Manoj, *Ad Hoc wireless Networks: Architecture and Protocols,* "On-demand Routing Protocols", Pearson Education, Inc., 2004