A Project Report

On

PERFORMANCE EVALUATION AND PREVENTION OF BLACK HOLE ATTACK IN MANET

Submitted for partial fulfilment of the requirements for the award of the degree of

BACHELOR OF ENGINEERING
IN
COMPUTER SCIENCE AND ENGINEERING

BY

Paruchuri Sumanth
1601-14-733-115

Gundu Vamshi Krishna
1601-14-733-116

Under the guidance of

Ms P.Vimala Manohara Ruth
Asst. Professor
Department of CSE

Department of Computer Science and Engineering
Chaitanya Bharathi Institute of Technology(A)
Hyderabad - 500075
April, 2018

Chaitanya Bharathi Institute of Technology (Autonomous)
(Regd. No. 855/2009)
(Affiliated to O.U; All U.G and 5 P.G. Programmes (Civil, CSE, ECE, Mech. & EEE) Accredited by NBA; Accredited by NAAC (UGC); ISO Certified 9001 : 2008)
Chaitanya Bharathi P.O., CBIT Campus, Gandipet, Kokapet (V),
Gandipet Mandal, Ranga Reddy District, Hyderabad - 500 075, Telangana
e-mail : principal@cbit.ac.in; Website: www.cbit.ac.in ✆ : 040 - 24193276, 277, 280, Fax: 040 - 24193278

CERTIFICATE

This is to certify that the project work entitled "Performance Evaluation And Detection Of Black Hole Attack In MANET" submitted by Paruchuri Sumanth, 1601-14-733-115 and Gundu Vamshi Krishna, 1601-14-733-116 in partial fulfilment of requirements for the award of degree of Bachelor of Engineering in Computer Science and Engineering as specialization is a record of the bonafide work carried out under the supervision of Ms P.Vimala Manohara Ruth, Assistant Professor, Dept. of CSE and this has not been submitted to any other University or Institute for award of Degree or Diploma.

Project Guide

Ms P.Vimala Manohara Ruth
Assistant Professor
Department of CSE
CBIT,Hyderabad

Head of the Dept

Dr.M.Swamy Das
Professor and Head
Department of CSE
CBIT,Hyderabad

DECLARATION

We hereby declare that the research work entitled " Performance Evaluation and Prevention of Black Hole Attack in MANET " is original and bonafide work carried out by us as a part of fulfilment for Bachelor of Engineering in Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, Gandipet, Hyderabad, under the guidance of Ms P.Vimala Manohara Ruth Assistant Professor, Department of CSE, CBIT.

No part of the project work is copied from books/journals/internet and wherever the partition is taken, the same has been duly referred in the text. The report is based on the project work done entirely by us and not copied from any other source.

Paruchuri Sumanth

160114733115

Gundu vamshi Krishna

160114733116

ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without introducing the people who made it possible and whose constant guidance and encouragement crowns all efforts with success. They have been a guiding light and source of inspiration towards the completion of the project.

We would like to express our sincere gratitude and indebtedness to our project guide, Ms P.Vimala Manohara Ruth, Assistant Professor, Dept of CSE, who has supported us throughout our project with patience and knowledge.

We are also thankful to Head of the Department, Dr.M.Swamy Das, Professor and Head, Dept. of CSE for providing excellent infrastructure and a conducive atmosphere for completing this project successfully.

We are also extremely thankful to our Project Coordinator Dr.T.Sridevi, Associate Professor, Dept. of CSE, for her valuable suggestions and interest throughout the course of this project

We convey our heartfelt thanks to the lab staff for allowing us to use the required equipment whenever needed.

Finally, we would like to take this opportunity to thank our families for their support through the work. We sincerely acknowledge and thank all those who gave directly or indirectly their support in completion of this work.

Paruchuri Sumanth
160114733115

Gundu Vamshi Krishna
160114733116

ABSTRACT

A mobile ad hoc network MANET is a collection of mobile nodes in which the nodes can communicate without the need of any access point or infrastructure. The wireless nodes can dynamically form a network to exchange information among them without making use of any existing network infrastructure. The mobile hosts are free to move dynamically and act as routers.

Security is a highly challenging issue in ad hoc networks. Understanding possible forms of attacks is the first step towards developing good security solutions. The presence of malicious nodes will affect the performance and reliability of the network. In Black hole attack, nodes which are called malicious will drop the packet instead of forwarding towards destination. Thus, a Black hole attack degrades the performance of the network.

In this project, The performance metrics of a MANET such as Throughput, Packet delivery ratio, packet loss are evaluated when there is no malicious node, single malicious node which leads to a single black hole and multiple malicious nodes which leads to multiple black hole attacks, compare the metrics with no blackhole, single black hole and multiple blackholes and draw graphs for them, The moment of nodes of MANET in NAM, number of packets consumed by black holes is shown. And proposed a solution using Fake routing protocol to prevent black hole attacks imposed by both single and multiple black hole nodes. Simulation's results show that the proposed protocol provides better performance in terms of packet delivery, throughput, packet loss in presence of Black holes, and helps in prevention of Black hole attack.

List of Figures

Fig.No	Figure Name	Page No
2.1	RREQ from Source RREQ	9
2.2	RREP to Source RREP	9
2.3	Packet Drop by node 3	10
3.1	DFD level-0	20
3.2	DFD level-1	21
3.3	Usecase diagram	22
3.4	Activity diagram	23
3.5	Working of NS2	32
3.6	NAM	35
4.1	Malicious nodes X Packet loss	36
4.2	Malicious nodes X Throughput	37
4.3	Malicious nodes X Packet delivery ratio	38
4.4	Manet with 100 nodes	39
4.5	Manet with 50 nodes	40
4.6	Time X packets lost	41
4.7	Time X Throughput	42
4.8	Time X Delay	43

4.9	No. of malicious nodes X Throughput	44
4.10	No. of malicious nodes X Packet delivery ratio	45
4.11	No. of malicious nodes X Packet loss	46

List of Tables

Table.No	Table Name	Page No
4.1	PDR in the presence of one and two malicious nodes	36
4.2	Throughput in the presence of one and two malicious nodes	37
4.3	Packets dropped by one and two malicious nodes	38

TABLE OF CONTENTS

Certificate i

Declaration ii

Acknowledgement iii

Abstract iv

List of Figures v

List of Tables vii

Chapter I : Introduction

1.1 Objective 1

1.2 Problem Definition 2

1.3 Existing System 2

1.4 Proposed System 2

1.5 Organization of Report 3

Chapter II : Literature Survey

2.1 Security Threats in MANETs 6

2.1.1 Attacks using Modification 6

2.1.2 Attacks using Impersonation 7

2.1.3 Attacks using Fabrication 7

2.1.4 Gray hole attack 7

2.1.5 wormhole attacks 7

2.1.6 Lack of Cooperation 8

2.1.7 Blackhole attack 8

2.2 AODV Routing protocol 10

2.2.1 Modified AODV routing protocol 12

2.3 MANET 14

2.3.1 Characteristics of MANET 15

2.3.2 Challenges in MANET 16

Chapter III : Methodology

3.1 System Design 18

3.1.1 Proposed Algorithm 18

3.1.2 Diagrammatic Representation 19

3.1.2.1 Data flow diagrams 19
3.1.2.1.1 DFD level-0 19
3.1.2.1.2 DFD level-1 20
3.1.2.2 UML diagrams 21
3.1.2.2.1 Usecase Diagram 22
3.1.2.2.2 Activity Diagram 23
3.2 TCL scripting 24
3.3 System Requirements 30
3.3.1 Software requiremnts 30
3.3.2 Hardware Requirements 31
3.4 Implementation of proposed solution 30
3.5 Network Simulator-2 31
3.5.1 Structure of NS-2 32
3.5.2 Network components 33
3.5.2.1 Packet 33
3.5.2.2 Link 34
3.6 NAM 34
Chapter IV : Results and discussions
4.1 Performance Evaluation Results 36
4.2 Prevention Results 44
Chapter V : Conclusion and future work 47
References 48
Appendix 50

Chapter I
Introduction

Network security is a crucial issue in the present generation networks. Most network security solutions focus on vulnerabilities in the end systems, but not on vulnerabilities in the network devices. However , the Internet is growing in fast rate and simultaneously supports the increase in requirement of running dynamic, heterogenous applications. So, the technology used to build the networks has changed in recent years and new vulnerabilities are coming out. As a result, the focus of attacker has shifted to attacking the network infrastructure(e.g. router , awitch,etc) itself, as pointed out in. Until recently the packet forwarding functionality of most high-performance network routers is implemented using Application Specific Integrard Circuits(ASICs)[15]. ASICs are costly to develop and they could only achieve the performance that was needed for multi-Gigabet for second traffic forwarding, as discussed in.

The use of such high performance processor provides routers with much more flexibility to customize routers functionality after production. Therefore, industry is moving towards developing routers[15] using programmable packet processors rather than using AICs. Routers play the most vital role in data transport, But, customization od routers introduces increased vulnerabilities and attacks[7]. Also, many researches have found several security vulnerabilities allow a remote attacker to execute arbitrary commands with little effort and take full control of the router's configuration settings. The number of attacks that affect the network infrastructure has increased settings. The number of attacks that affect the network infrastructure has increased recently and this is a serious concern for the next generation networks.

Several Route replies come and selects the best one. In proactive routing protocols, such as the Optimized link State Routing (OLSR) protocol [9], nodes obtain routes by periodic exchange of topology information. For maintaining this information routing tables are using. Due to the lack of centralized administration most of these protocols are depending on each other to get updated. In such a network an attacker has more possibility to launch an attack by denying the services or changing the basic characteristics of the network and as a result disrupting the routing.

Many counter measures are developing for avoiding the attacking possibilities. Among them the first one is effective intrusion detection system such as watchdog, path rater[11] etc. There are many techniques for protecting the routing protocols in the network. They are key management, encryption techniques etc., which provides confidentiality, authentication and integrity. As a result it prevents the joining of unauthorized nodes into the network and protects it. The problem in key management is that it will cause heavy traffic by exchanging keys. And also for a bandwidth limited network such as MANET this exchanging of keys will result in high cost constraints[3]. Another preventive measure is the use of secure routing protocols such as authenticated routing for ad hoc networks (ARAN), Ariadne, secure AODV (SAODV), SEAD(Secure Efficient Adhoc Distance Vector) routing protocol[5]. In general, the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, absence of central authorities, distributed cooperation. The existing security solutions for wired networks cannot be applied directly in wireless MANETs.

MANET‟s are suitable for Military networking requirements, safety/rescue operations, wearable computing and communications, satellite-based information delivery and finally in scenarios requiring rapidly-deployable communications with survivable, dynamic networking mobile data exchange (RFC 2501). There are many issues in MANET such as Routing, Attack, Topology Management, Context awareness, Identity Management, Power Management, etc. (Abdullahi Arabo *et al* 2007). Due to the openness in network topology and the absence of centralized administration in management, MANETs are vulnerable to attacks from Black hole nodes. The packet loss due to the Black hole nodes has been detected and to be isolated from the mobile ad-hoc network to increase the reliability of the network.

The proposed work is to prevent attacks from Black hole nodes and improve the security performance of the whole network, especially in terms of packet delivery ratio, average end-to-end delay. To overcome this, a Dynamic trust prediction model is proposed .This model is used to calculate the trust value, which is based on the node‟s historical behavior as well as the future behavior. By using this one can kick out the untrustworthy nodes, obtain a reliable packet delivery route and alleviate the attacks from Black hole nodes, which is called as Trusted AODV (TAODV). TAODV provides a flexible and feasible approach to choose the shortest route that meets the security requirements of data packet Transmission.

1.1 Objective

Network Security is crucial while transferring data from one node to another node, The main objective is to protect the packets from threats such as blackhole attacks aiming to evaluate performance metrics when there is a blackhole attack in the network and to prevent the blackhole using fake routing protocol.

Mobile ad hoc network (MANET) is a self –organized system comprised of mobile nodes without any fixed infrastructure. MANET‟s are at more risk to attacks since it is dynamic in nature. Security is a decisive requisite in MANET‟s when assessed to wired networks. MANET‟s are more suspicious to security attacks due to the need of a reliable centralized cloud and inadequate resources. The scenario in which data messages are dropped while routing messages are forwarded is known as black hole attack. The proposed Trusted AODV (TAODV) routing protocol provides a solution for black hole attack by identifying the malicious nodes by using trust value of the node and identify trusted path free from malicious modes for reliable data delivery. Normally the packet drop may happen either due to congestion or due to malicious nodes present in the network. The main objective of this work is to speed up the process of identification of malicious node by using trust based approach. The results show that this protocol leads to a better packet delivery ratio with maximum throughput when compared to normal AODV protocol.

1.2. Problem Definition

The problem analyzed is evaluating the performance of the network when an attack performed by the attacker through misbehaving router.

Evaluating the performance of the network under blackhole attack and preventing the malicious nodes in the network and minimizing its impact on next generation networks.

Comparison of performance of the network under normal AODV and modified AODV(secure) under blackhole attack in MANET.

1.3. Existing System

In existing system the intermediate node behaves as blackhole which drops the packets in the network, so the throughput is decreased and affects network performance[9]. Due to the light weight detection mechanism, the blackhole node is not eliminated from routing and its presence degrades the network performance.

An ad-hoc network is a collection of wireless mobile nodes that performas a temporary network without any centralized administration. In such environment, it may be necessary for one node to enlist other hosts in forwarding a packet to its destination due to limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad-hoc routing protocol that allows it to discover multi job paths through the network to any other node. This idea of mobile ad-hoc network is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly.

1.4. Proposed System

In proposed system, The performance metrics of a MANET such as Throughput, Packet delivery ratio, packet loss[1] are evaluated when there is no malicious node, single malicious node which leads to a single blackhole[1] and multiple malicious nodes which leads to multiple blackhole attacks, compare the metrics with no blackhole, single blackhole and multiple blackholes and draw graphs for them, the moment of nodes in MANET is showed in NAM, show number of packets consumed by blackholes. A solution is proposed using Fake routing protocol to prevent blackhole attacks imposed by both single and multiple blackhole nodes. Simulation's results show that the proposed protocol provides better performance in terms of packet delivery, throughput, packet loss in presence of blackholes, and helps in detection of blackholes[2].

1.5. Organization of the report

This report is organized as follows:

- The first chapter deals with introduction of the project, its objective, motivation and proposed solution
- The second chapter gives an elaborated view of the literature survey of this project work
- The third chapter gives an insight of the overall architecture and UML diagrams,implementation of the proposed system and the software and hardware system requirements
- Fourth Chapter deals with results analysis
- Fifth Chapter has the conclusion and the future work

Chapter II
Literature Survey

Wireless Ad-hoc Networks are autonomously self-organized netwotks without infrastructure support. In a wireless ad-hoc betwork, nodes move arbitrarily; therefore the network may experience rapid and unpredictable topology changes. Because nodes in a wireless network have limited transmission ranges, some nodes cannot communicate directly with each other. Hence, routing paths in wireless ad-hoc networks potentially contain multiple hops, and every node in wireless ad-hoc networks has the responsibility to act as a router

Security is a major concern for protected communication between nodes in a hostile environment. In hostile environments adversaries can bunch active and passive attacks against intercept able routing in embed in routing message and data packets. Focus is on fundamental security attacks in wireless ad-hoc networks. Wireless network has no clear line of defence, so, it is accessible to both legitimate network users and malicious attackers.

2.1 Security Threats in MANETs

The current mobile ad-hoc networks allow for many different types of attacks. Although the analogous exploits also exits in wired networks but it is easy to fix by infrastructure in such a network. Active attack is attack when misbehaving node has to bear s ome energy costs in order to perform the threat. On the other hand, passive attacks are mainly due to lack of cooperation with the purpose of saving energy selfishly. In this the attacks are classified as modification, impersonation, fabrication, wormhole and lack of cooperation[13].

2.1.1 Attacks using Modification

Modification is a type of attack when an authorized party not only gains access to but tampers with an asset. For example a malicious node can redirect the network traffic and conduct

DOS attacks by modifying message fields or by forwarding routing message with false values.

2.1.2 Attacks using Impersonation

As there is no authentication of data packets in current ad-hoc network, a malicious node can launch many attacks in a network by masquerading[13] as another node i.ie. spoofing. Spoofing is occurred when a malicious node misrepresents its identity in the network(such as alerting its MAC orIP address in outgoing packets) and alters the target of the network topology that a benign node can either.

2.1.3 Attacks through Fabrication

Fabrication[7] is an attack in which an authorized party not only gains the access but also inserts counterfeit objects into the system. In MANET, fabrication is used to refer the attacks performed by generating false routing messages.

2.1.4 Grey hole attack

A malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability[14]. This attack is more difficult to defect than the blackhole attack where the malicious node drops the received data packets with certainly. A Grey hole[14] may exhibit its malicious behaviour in different ways. It may drops packet coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of grey hole node may behave maliciously for some time duration by dropping packets but may switch to normal behaviour which is a combination of two, thereby making its detection even more difficult.

2.1.5 Wormhole Attacks

Wormhole attack[3][8] is also known as tunneling attack. A tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing date routes. This exploit gives the oppurtunity vertex cut[10] in the network that is controlled by the two colluding attackers.

2.1.6 Lack of Cooperation

Mobile ad-hoc networks rely on the cooperation of all the participating nodes. The more nodes cooperate transfer traffic, the more powerful a MANET[6] gets. But one of the different kinds of misbehaviour a node may exhibit is selfishness. A selfishness node wants to preserve own resources while using the services of others and consuming their resources.

2.1.7 Blackhole attack

The black hole attack is one of the well-known major security threats in wireless mobile ad hoc networks. The intruders utilize the Black hole to carry out their malicious behaviors because the route discovery process is necessary and inevitable. Many researchers have conducted different detection techniques to propose different types of detection schemes. Trust relationship between the nodes play a significant role in isolating the malicious nodes that roots a black hole attack in the network. A malicious node (black hole node) may always respond positively to route requests even when it does not have proper routing information. The black hole node can drop all packets forwarded to it. In other words Black Hole attack is one of the attacks that advertise it for having the shortest path to destination node and drops the entire packet that is coming from source node.

An example is shown as Fig 2.1, node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehaviour node who replies the RREQ packet sent from source node as shown in Fig 2.2, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. As what mentioned above, a malicious node probably drops the packets as shown in Fig 2.3. This suspicious node can be regarded as a black hole problem in MANETs.

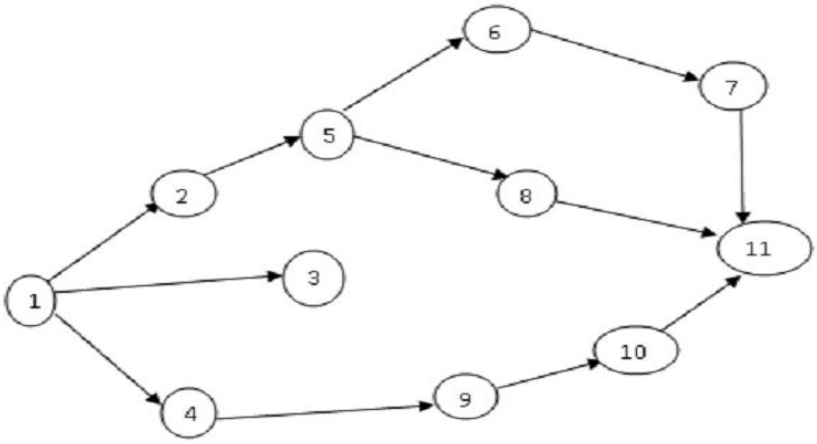

Fig 2.1 : RREQ from Source RREQ.

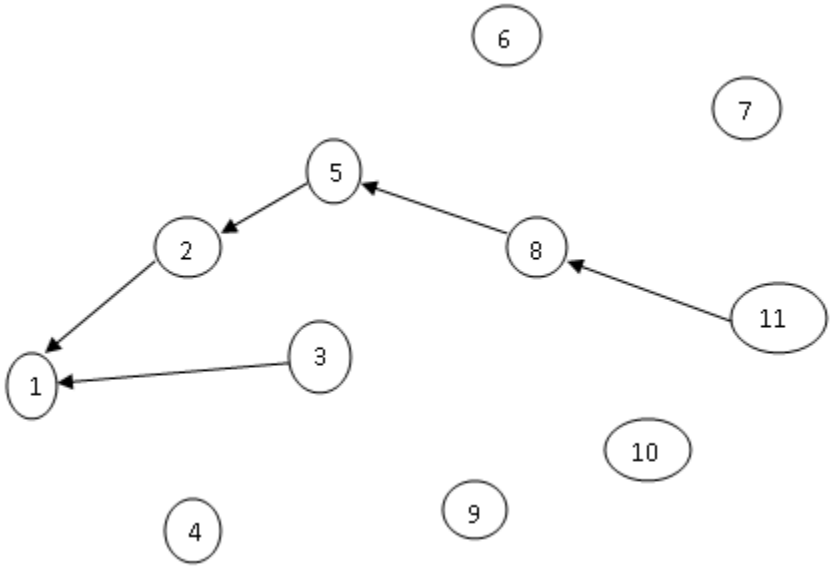

Fig 2.2 : RREP to Source RREP

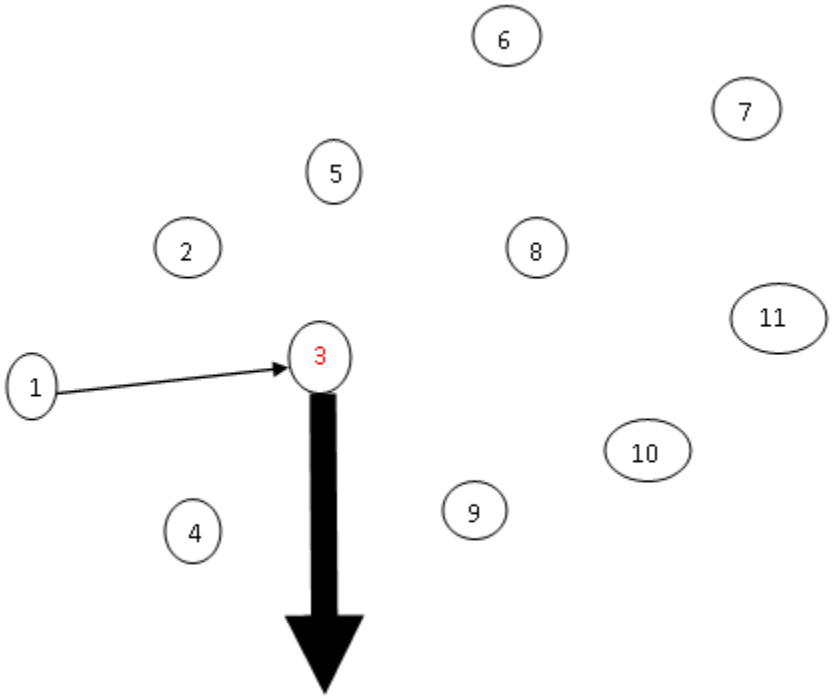

Fig 2.3 : Packet Drop by node 3.

2.2 AODV Routing protocol

AODV[1] is a Reactive routing protocol and one of the most considered on demand routing protocols because it routes between the nodes only as desired by the nodes in ad hoc networks. It is capable of both uni cast and multicast routing. The route discovery process in AODV is done through route request (RREQ)[1].

Whenever the source node wants to communicate with the destination node it will check the routing table for the existing route. If the route exists then it will start the communication, if not it broadcasts RREQ packet into the network. Nodes receiving the RREQ check for the destination address and update their information for the source and set up backward pointers to source in the routing tables. Along with source and destination address, RREQ also contains the most recent sequence number for the destination. The node that has received the request packet will reply if it is the destination or it has a

route towards the destination having higher sequence number. Otherwise, it rebroadcasts the RREQ to other nodes in the network.

Once the request reaches the destination, RREP is sent back to the source node, nodes set up forward pointers to the destination. The communication starts once the source node receives the reply packet. Sequence number plays a key role in AODV protocol. If source node receives a reply packet (RREP) that has highest sequence number with small hop count, it updates its routing information and starts using better route.

AODV is a routing protocol, hence that deals with routing table management. Routing table entry includes following fields:

-Destination IP Address

-Destination sequence number

-Next hop IP address

-Life time

-Hop count

Source node Broadcast RREQ messages to establish a route. These RREQ messages are received by the Intermediate nodes. If a route to the destination is available, start sending data. Else generate a RREQ packet and they update their routing table. It checks for the destination and then forward the RREQ if it is not the destination. It also maintains the back-pointer to the originator. At once the destination receives the RREQ message the Destination generates RREP message. RREP sent back to source using the reverse pointer set up by the intermediate nodes. RREP reaches source, the path is established and communication starts. At times, the intermediate node generate route reply, if a 'fresh enough' route is a valid route entry for the destination whose associated sequence number is at least as great as that contained in the RREQ. Change the sequence number of the destination node if stale, increment the hop count by 1 and forward.

Each originating node maintains a monotonically increasing sequence number. It is used by other nodes to determine the freshness of the information. Every node‟s routing table contains the latest information available about the sequence number for the IP address of the destination node for which the routing information is maintained. It is updated whenever a

node receives new information about the sequence number from RREQ, RREP, or RERR messages received related to that destination.

2.2.1 Modified AODV routing protocol

The path established previously in the routing protocol for packet delivery has to be recomputed since the trust value of the nodes participating in the routing process is less than the threshold value. The path must be recomputed based on the trust values. The trust value for each node is calculated using the following metrics. The above mentioned trust metrics are considered to re-compute the path in routing protocol which leads to a better packet delivery ratio and throughput. The node participating in the routing process in the TAODV protocol possess a maximum trust value. The nodes are subjected to continuous monitoring and evaluation to establish a best routing path for every instance of a connection establishment.

The Trusted AODV Protocol implemented for new route discovery and path re-computation in the existing MANET. This protocol completely isolates the misbehaving nodes based on the trust management. Hence the packet drop is only due to the effect of congestion in the network. This leads to a better packet delivery rate as no misbehaving nodes are participated in the routing process. The Comparison of Existing AODV and Trusted AODV (TAODV) based on packet drop ratio are implied. The result shows that the packet loss ratio is reduced to a large scale as only the trusted nodes are made to participate in the routing process. The results inferred prove that the reliability of the packet delivery in MANET is better than that of the Normal AODV routing process.

Steps for Path Recomputation in TAODV:

Step 1 : The source node S looks up for a route to destination node D in its local routing table. The available route should meet the requirements: trust and QoS constraints. If such routes are found, go to Step 3; if there is no such a route, the source node S initiates a route discovery procedure.

Step 2 : The source node S checks its neighbour nodes trust degree by judging with the trust threshold γ from its local trust record table. Then, node S broadcasts route request packets REQ to its neighbour nodes with their trust degree is greater than γ ;

Step 3 : When the intermediate neighbor node k of node j has an available route to the destination node D, and the routing cost metric is least, that is, the trust degree of all nodes in the available route is greater than γ , moreover, the QoS parameter of total link delay overhead is minimum, so node k can generate a route reply packet REP to node S;

Step 4 : When the intermediate neighbour node k of node j has an available route to the destination node D, and the routing cost metric is least, that is, the trust degree of all nodes in the available route is greater than γ , moreover, the QoS parameter of total link delay overhead is minimum, so node k can generate a route reply packet REP to node S;

Step 5 : Otherwise, the node k performs the route discovery procedure similar to Step 3. Under the requirements of trust and QoS constraints, node k continues broadcasting the updated REQ packet to its next neighbour nodes, until the REQ packet arrives the destination node D;

Step 6 : When the destination node D receives several REQ packets, it fetches their fields of trust values and decides to choose the optimal route which has the maximum trust value. Meanwhile, the node D generates a route reply packet REP and sends back to the source node S along the reverse direction of optimal route.

2.3 MANET

A Mobile Ad hoc Network, or MANET, consists of a group of cooperating wireless mobile hosts (nodes) that dynamically constructs a short lived and self-configuring network without the support of a centralized network infrastructure[6]. The mobile nodes can be cell-phones, PDAs and laptops and typically support several forms of wireless connectivity like 802.11, IrDA, Bluetooth, etc.

One advantage of wireless networks is the ability to transmit data among users in a common area while remaining mobile. However, the range of transmitters or their proximity to the wireless central points limits the distance between peers. Mobile Ad hoc networks mitigate this problem by allowing out of range nodes to route data through intermediate nodes, i.e., each send its own data as well as routes and forwards data on behalf of other nodes.

Initaining a table that stores entry <source, destination, sum, path>. Whatever the current node is, the source, the destination or the intermediate node, it inserts such an entry into the table when sending, forwarding or receiving packets for the first time. The value of each field is: Source: the address of source. Destination: the address of destination. sum: the total number of packets that the current node sends, forwards, or receives using the route path Path as source, intermediate node or destination respectively. path: the route that is used for the communication between

<source, destination>. The path is a list of nodes addresses or an path ID for simplicity.

The deployment of a MANETs is easy due to the absence of setting up any infrastructure for communication. Mostly such kind of networks are required in military application and emergency rescue operations. But slowly MANETs have entered with the areas of gaming, sensing, conferencing, collaborative and distributed computing . This dynamic network is yet to capture most of the commercial applications. Research is still going on in this direction so that the MANET can be deployed in any area where a faster and cheaper network can be setup instantly for data communication.

2.3.1 Characteristics of MANET:

Wireless medium: The wireless medium used by the nodes to communicate with each other has time-varying coverage and asymmetric propagation properties. It is less reliable and more prone to interference compared to a wired medium.

Dynamic Topologies: Nodes are free to move arbitrarily with different speeds; thus, the network topology may change randomly and at unpredictable times.

Infrastructureless Network: Network is not depending on any fix infrastructure for its operation.

Power Management: As the nodes are not fixed, they rely on batteries as their power source. Thus mechanisms and protocols devised for such networks need to keep the energy constraint in mind.

Peer-to-Peer nature: These are not fixed nodes with pre-defined roles. Thus, all protocols need to be designed for distributed environments composed of “peers" and need to be robust enough to handle these distributed dynamic topologies. These different characteristics of wireless ad hoc networks require different techniques than the wired networks, especially at the three lower-most layers, to effectively perform the network functions. The widely adopted standard for wireless networks, at the physical and data-link layer is IEEE 802.11
(for wireless local area networks).

Limited computing and energy resources: There are limited computing power, memory, and disk size due to the limited battery capacity, as well as limitation on device size, weight, and cost.

Limited service coverage: Due to device, distance between devices, network condition limitations, service implementation for wireless devices is more challenging as compared to the wired networks and their elements and at the same time MANETs faces many constraints.

Higher interference results in lower reliability: Infrared signals suffer interference from sunlight and heat sources, and can be shielded/absorbed by various objects and materials. Radio signals usually are less prone to being blocked; however, they can be interfered by other electrical devices. The broadcast nature of transmission means all devices are potentially interfering with one another. Self-interference also happens due to multipath.

Highly variable network conditions: Higher data loss rates due to interference. User movement causes frequent disconnection. Channel changes occur as users move around. Received power diminishes with distance.

Limited Bandwidth: Wireless links continue to have significantly lower capacity than infrastructure networks. In addition, the realized throughput of wireless communications - after accounting for the effects of multiple access, fading, noise, and interference conditions, etc., is often much less than a radio's maximum transmission rate.

2.3.2 Challenges in MANET:

Routing in Dynamic Topology: In MANET, the presence of node mobility changes the link of connectivity between the nodes very frequently. The existing conventional Bellman Ford routing algorithm or classic Link State algorithms are not applicable for such dynamic network where the topology changes with the free movement of the nodes.

Topology maintenance: Updating information of dynamic links among nodes in MANETs is a major challenge.

Lack of central Infrastructure: There exist several solutions in a cellular network to handle the mobility of the nodes while routing is the major concern. But, MANET doesn’t have a centralized monitoring authority and the lack of any central facility decreases the routing efficiency as well as the throughput.

Scalability: In MANETs, the nodes are constrained with the limited battery power, computation capability and storage capacity. As the network size increases, the number of packets forwarded by each node also increases. This drains the node resources fast, making it

dead in a short period. Similarly, topology maintenance overhead in a scalable dynamic network is another challenging issue. This ultimately affects the QoS of the network.

Cooperativeness: Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by violating the protocol specifications.

Energy Efficiency: Portable mobile devices are mostly operated by the batteries whose life span is very limited. Further, the nodes in the MANET have to perform the role of an end system (transmitter or receiver) as well as an intermediate system (forwarding packets of other nodes) which causes more battery drainage.

Security and Privacy: Mobility implies higher security risks such as peerto-peer network architecture or a shared wireless medium accessible to both legitimate users and malicious attackers.

Autonomous: No centralized administration entity is available to manage the operation of the different mobile nodes in MANETs.

Poor Transmission Quality: This is an inherent problem of wireless communication caused by several error sources that result in degradation of the received signal.

Chapter III
Methodology

3.1 System Design

The system architecture is a conceptual model that defines the structure, behavior, and views of a system. An architecture description is a formal description and representation of a system, organized in a way that supports reasoning about the structures and behaviors of the system.

System design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering.

Object-oriented analysis and design (OOAD) is a popular technical approach for analyzing, designing an application, system, or business by applying the object-oriented paradigm and visual modeling throughout the development life cycles to foster better stakeholder communication and product quality.

3.1.1. Proposed System

The steps involved in the proposed algorithm for performance evaluation are:

1. Create a MANET
2. Implement of AODV routing protocol[2][5]
3. Insert nodes into the network
4. Introduce malicious node into the network
5. Send packets from source to destination
6. Display moment of nodes and packets in NAM
7. Evaluate performance metrics
8. Generate graphs using Xgraph

The steps involved in proposed algorithm for blackhole prevention are:

1. Create MANET
2. Implement Fake routing protocol
3. Insert mobile nodes and malicious nodes into the network
4. source broadcasts RREQ(Route Request message) with its own ID(SSN(Source Sequence number))[4] in place of DSN(Destination Sequence Number)
5. Intermediate Nodes sends RREP(Route Reply message) packet having highest SSN
6. If (RREP(SSN)>RREQ(SSN))[4] is true then node is blacklisted and other nodes are notified
   Otherwise normal routing process of AODV is involved
7. Display results in NAM and terminal

3.1.2 Diagramatic Representation

3.1.2.1 Data flow diagrams

A data flow diagram (DFD) maps out the flow of information for any process or system. It uses defined symbols like rectangles, circles and arrows, plus short text labels, to show data inputs, outputs, storage points and the routes between each destination.

3.1.2.1.1 DFD level-0

Context level DFD, also known as level 0 DFD, sees the whole system as a single process and emphasis the interaction between the system and external entities.

Fig 3.1 DFD level-0

DFD-0 takes mobile nodes as input for analysis phase and gives results for given metrics as output, hence entire processing such as blackole attack and prevention goes on in analysis phase.

3.1.2.1.2DFD level-1

The next stage is to create the Level 1 Data Flow Diagram. This highlights the main functions carried out by the system. As a rule, level-1 describes the system using between two and seven functions - two being a simple system and seven being a complicated system. This enables us to keep the model manageable on screen or paper.

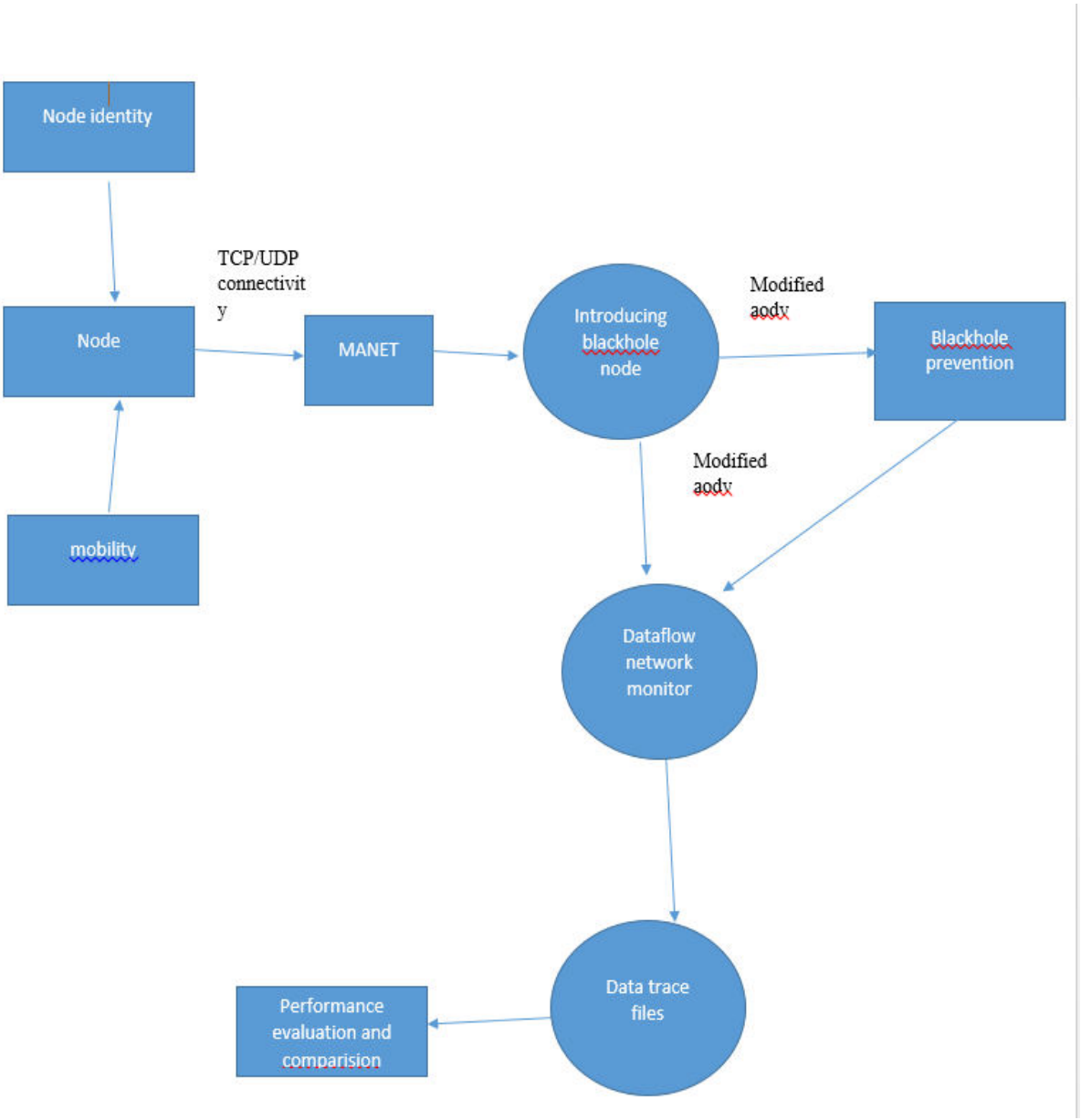

Fig 3.2 DFD level-1

The elaboration view of DFD-0 is DFD-1, in this level node is given an identity and mobility to move and to identify with unique number. Prevention is done using modified AODV routing protocol. Trace files are generated and graphs are drawn, performance evaluation under blackhole attack and prevention is shown at the end.

3.1.2.2 Uml Diagrams

UML (Unified Modeling Language) is a standard language for specifying, visualizing, constructing, and documenting the artifacts of software systems. UML is a way of visualizing a software program using a collection of diagrams.

3.1.2.2.1 Usecase Diagram

A use case diagram in the Unified Modelling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

A use case is a set of scenarios that describing an interaction between a user and a system. A use case diagram displays the relationship among actors and use cases. The two main components of a use case diagram are use cases and actors.

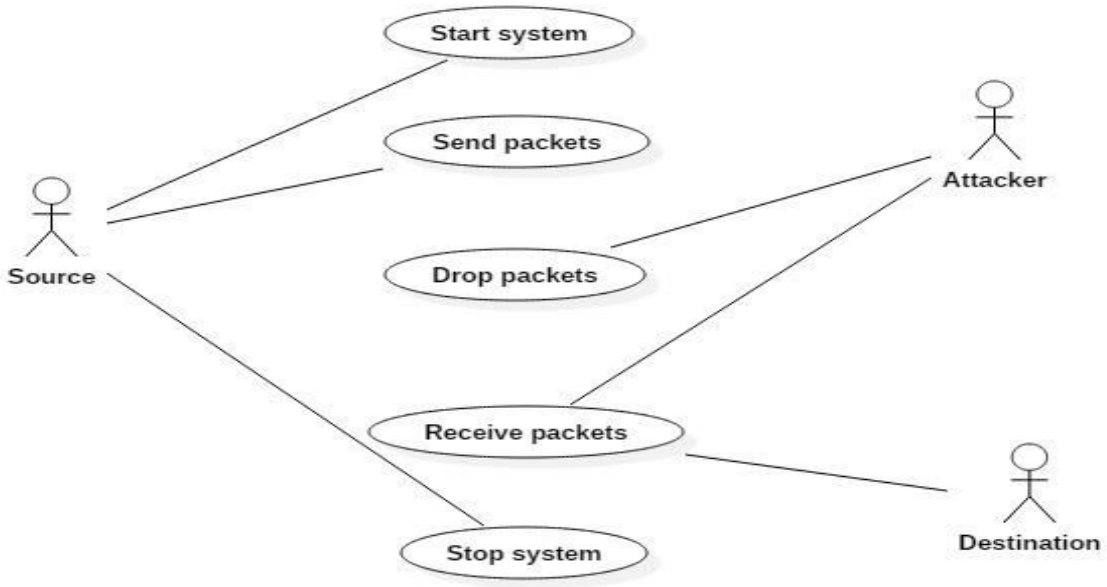

Fig 3.3 Usecase Diagram

In the above usecase diagram three actors namely source, destination and attacker are used. Source starts the system by sending RREQ packet to neighbouring nodes to find the shortest path to the destination, and sends packets to destination. At the end of communication it closes the communication channel using stop system. Attacker in this network is malicious node, which acts as if it is having the highest sequence number and less hopcount and source accepts its routereply message, then its starts dropping the packets and this scenario creates a blackhole attack.

3.1.2.2.2 Activity Diagram

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams are intended to model both computational and organizational processes (i.e. workflows). Activity diagrams show the overall flow of control.

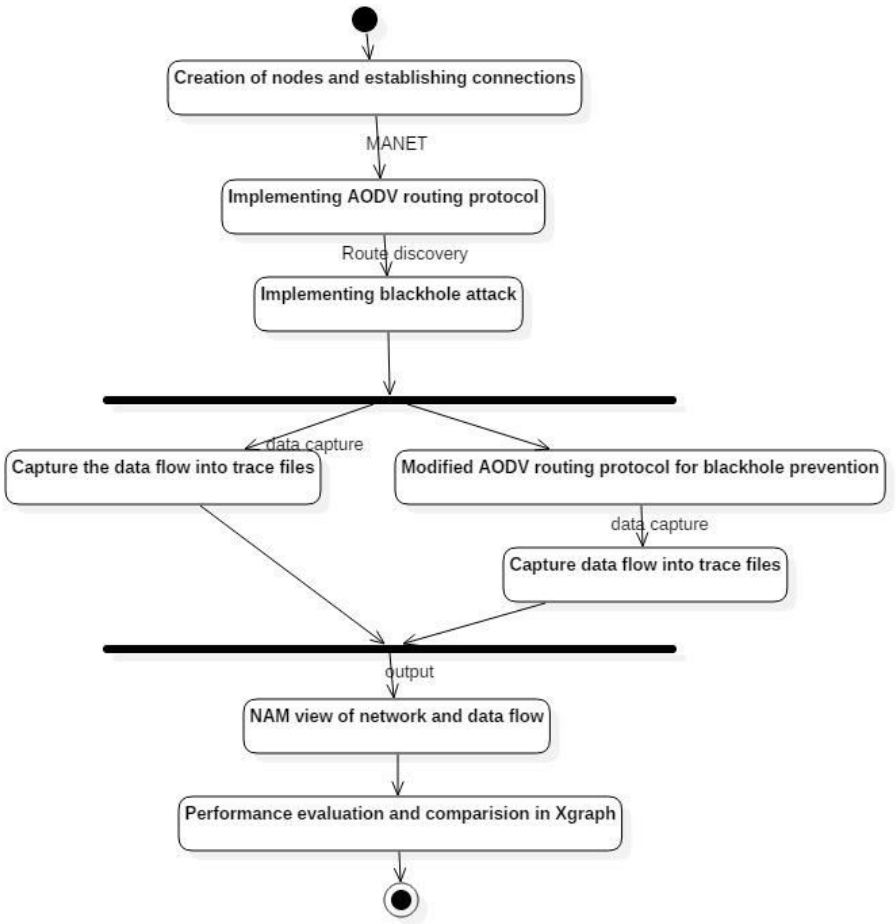

Fig 3.4 Activity Diagram

The above activity diagram tells start action is performed, then creation of nodes and connection is established between them, and AODV routing protocol is implemented and blackhole attack is performed and trace files are generated in one phase of a fork and blackhole is prevented using modifies AODV routing protocol and trace files are generated in another phase of the fork. At the end results are displayed in NAM and compared using graphs.

3.2 TCL Scripting

Variables in Tcl

```
set <variable_name> <variable_value>
```

Example:

```
set x 10
set name "john"
set price 12.2
```

```
set x  ;# this command will return value of x
```

Unset command

```
unset x
```

Print/Use variable's value

```
set y $x
```

put command :

```
puts "hello world"
  # Output: helloworld
```

If-else

TCL also has construct for if-else. Syntax for if-else is given below.

Syntax :

```
 if {condition} {
if-body
}
# Another syntax
 if [ expr condition] {
  if-body
}
```

Program :

```
set x 10
if { $x < 50 } {
puts "x is less than 50"
}


if [ expr $x == 20 ] {
puts "x is equal to 20"
} else {
puts " x is not equal to 20"
}
# Output:
```

```
14    x is less than 50

      x is not equal to 20
```

Loop

In TCL while loop has similar syntax as in c. Only different is in condition specification.

- **While Loop**

Syntax :

```
while {  condition } {
while-body
}
```

Example of printing event values form 0 to 100 :

```
1    set s 0
2    while { $s < 100 } {
3    puts $s
4    set s [expr $s+2]
5    }
```

For loop

For loop in tcl also has three parts initialisation, condition and increment or decrement.

Syntax :

```
for { initialisation} { condition} {increment/decrement} {
loop-body
}
```

Example:

```
for {set i 0} { $i < 10} { incr i} {
puts $i
}
# Output:
#0
#1
#2
#3
#4
#5
#6
#7
#8
#9
```

Procedure

Multiple commands can be combined to make a new command. This can be done by making a procedure. Procedure is similar to function in 'c'.

Syntax:

```
proc <procedure name> {  } {
procedure-body
}
```

Program :

```
# Program to make procedure for factorial
proc fact { a  } {
set fact 1
for {set i 1} {$i <= $a} {incr i} {
set fact [expr $fact * $i]
}
puts $fact
}
# Calling procedure
fact 5

#Output:
# 120
```

#Create a simulator object

set ns [new Simulator]

#Opening the nam trace file

set nf [open out.nam w]

$ns namtrace-all $nf

#Creating nodes

set n0 [$ns node]

#Creating a duplex link between the nodes

$ns duplex-link <$node0> <$node1> <bandwidth> <delay> <QueueUsed>

#Connect the traffic source with the traffic sink

$ns connect $udp0 $null0

#Call the finish procedure after 5 seconds of simulation time

$ns at 5.0 "finish"

#Run the simulation

$ns run

3.3 System Requirements

3.3.1 Software requirements

Operating system – UBUNTU

Simulation tool – NS-2

Other tools – NAM, Xgraph

3.3.2 Hardware requirements

CPU type - Intel Pentium 4

RAM size – 512MB

Hard disk capacity– 80GB

Clock speed – 3.0 GHz

3.4 Implementation of Proposed Solution

The source node broadcasts its own address and sequence number included into fake RREQ[11] packet instead of destination address and destination sequence number. As the source node's sequence number is the most recent and fresh sequence number. The other nodes do not have the latest or fresh sequence number of the source node. When the intermediate nodes receive the fake RREQ packet, If the intermediate nodes have the source sequence number greater than the one received in fake RREQ packet, it will reply with RREP packet. But in our case, the legitimate intermediate node will have the small source sequence number than described in fake RREQ packet because only source node will have its latest or fresh enough sequence number. But if there exist any blackhole nodes in the network, then they will reply with the RREP packet as it will advertise itself having the shortest path with the highest sequence number. So, the source node will detect the blackhole nodes and will

notify the other nodes about the blackhole nodes so that the rest of the legitimate nodes will not communicate with blackhole nodes. In existing system, the destination sequence number is used by the source node to compare the destination sequence number with the RREP packet's destination sequence number but in this case the source node may not have the fresh enough destination sequence number. As the source node had the old destination sequence number it used at the last time. In some techniques, the RREP destination sequence number is compared with some threshold value but not given on which basis threshold value is calculated. The parameters are not cleared while calculating the threshold value.

The proposed multiple blackhole nodes detection mechanism algorithm:

a) The source node broadcasts the fake RREQ packet with its own source sequence number and address in the destination sequence number and destination address in the RREQ packet fields respectively[11].

b) When legitimate nodes receive the fake RREQ packet, it will compare the source sequence number in fake RREQ packet it received with the sequence number of the source described in the table.

c) As the source node sends its own sequence number, it will be more obvious that it will be the latest or fresh one. The intermediate node will have the source sequence less than the described in fake RREQ packet. So it will not reply with RREP packet.

d) But, if there exist any blackhole node in the network then it will reply with the RREP packet and advertises itself as having the shortest path with highest source sequence number.

e) The source node will then detect the blackhole nodes exist in the network. And then send the ALARM[12] packet having the list of blackhole nodes to the rest of the nodes.

3.5 Network simulator-2

NS-2 is a packet –level simulator and essentially a centric discrete event scheduler to schedule the events such as packet and timer expiration. Centric event scheduler cannot accurately emulate "events handled at the same time" in real world, that is, events are handled one by one. This is not a serious problem in most networj simulations, because the events here are oftenl transitory. Beyond the event scheduler, ns-2 implemtns a variety of

network component and protocols. Notably, the wireless extension, derived from CMU Monarch Project, has 2 assumptions simplifying the phyical world: Nodes do not move significantly over the length of time they transmit or receive a packet.

This assumption holds only for mobile nodes of high-rate and low-speed. Consider a node with the sending rate of 10kbps and moving speed of 10m/s, during its significantly and cause reception failure. Node velocity is insignificant compared to the speed of light. In particular, none of the provided models include Doppler effects, although they could.

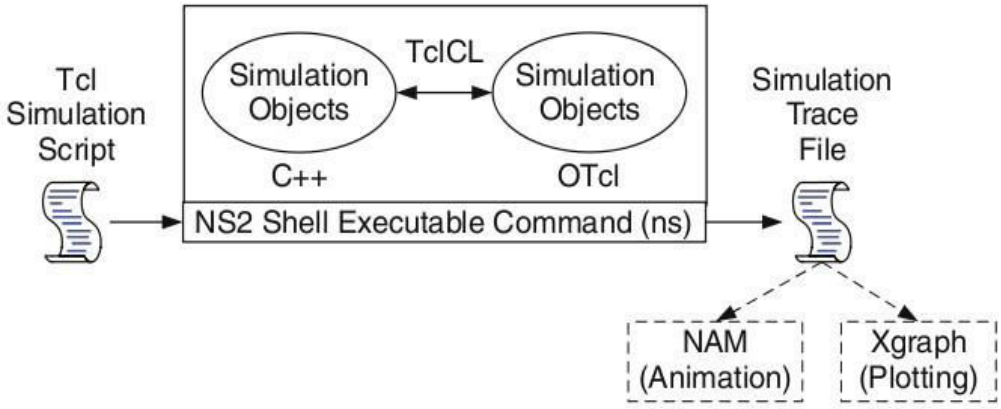

Fig 3.5 Working of NS2

3.5.1 Structure of NS-2

- Create the event scheduler
- Turn on tracing
- Create network
- Setup routing
- Insert errors
- Create transport connection
- Create traffic
- Transmit application-level data

Functionalities of NS-ALLINONE2.28:

C++/OTcl Linkage

Root os ns-2 object hierarchy

Bind(): link variable values between

TclObject

C++ andOTcl

Command(): link OTcl methods to C++ implementations

TclClass

Create an OTcl object, and create a linkage between the OTcl object and C++ Object

Tcl C++

Methods to access Tcl interpreter

TclCommand

Standalone global commands

EmbeddedTcl

Ns script initialization

3.5.2 Network components

The root of the hierarchy is the TclObject that is the superclass of all OTcl library objects(scheduler, network components, timers and other objects including NAM related ones). As an ancestor class of TclObject, NsObject class is the superclass of all basic network component objects that handle packets, which may compose compound network objects such as nodes and links. The basic network components are further divided into two subclasses, Connector and Classifier, based on the number of the possible output data paths. The basic network objects that have possible multiple output data paths are under the Classifier class.

3.5.2.1 Packet

A NS packet is composed of a stack of headers, and an optional data space. A packet header format is initialized when a simulator object is created, where a stacckof all registered headers, such as the common header that is commonly used by any objects as needed, IP header, TCP header, RTP header(UDP uses RTP header) and trace header, is defined, and the offset of each header in the stack is recorded. What this means is that whethte ot not a specific header is used, a stack composed of all registeref headers if created when a packet it processes using the corresponding offset value.

3.5.2.2 Link

A link is another major compund object in NS. When a user creates a link using a duplex-link member function of a simulator object, two simplex links in both directions are created. One thing to note is that an output queue of a node is actually implemented as a part of simplex link object. Packets dequeued from a queue are passed to the Delay object that simulates the link delay, and packets dropped at a queue are sent to a NULL Agent and are freed there. Finally, the TTL object calculates Time to live parameters for each packet received and updates the TTL field of the packet.

3.6 NAM

NAM provides a visual interpretation of the network topology created. The application was developed as part of the VINT project. Its features are as follows. Displays the NAM application and its components. Provides the visual interpretation of the network created. Can be executed directly from a tcl script. Controls include play, stop, ff, rw, pause, a display speed controller and a packet monitor facility.

It presents information such as throughput, number packets on each link. Provides a drag and drop interface for creating topologies.

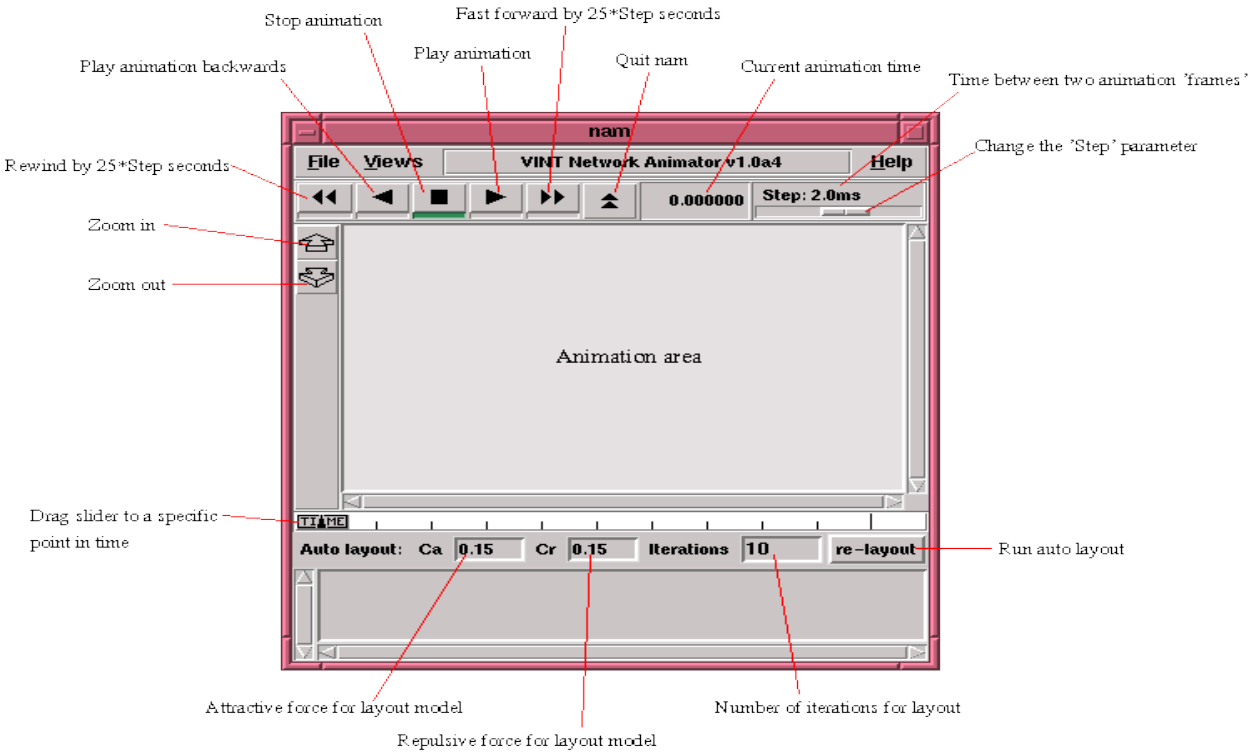

Figure 3.6 Nam

Chapter IV

Results and Discussions

4.1 Performance Evaluation Results:

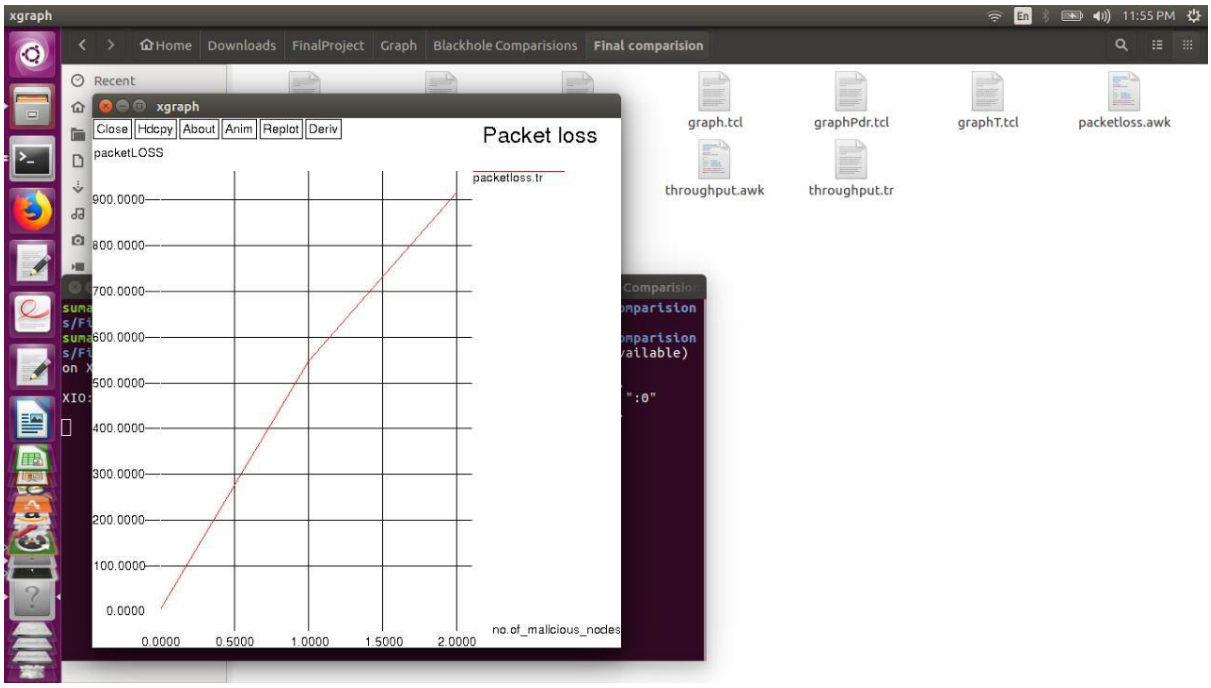

Fig 4.1 Malicious nodes X Packet loss

The above figure is a graph drawn between number of malicious nodes and packetloss, it is observed that as the number of malicious nodes in the network increases the packetloss increases. When there is no malicious node at all the packet loss is almost zero , when there is a single malicious node the loss gradually increased to around 500 packets, when there is another malicious node the packet loss increased very rapidly to 900.

Packet loss= No. of packets sent – No. of packets received

Table 4.1 packets dropped by one and two malicious nodes

No of nodes In the network	Packets dropped by 1 malicious node	Packets dropped by 2 malicious nodes
20	742	976
50	1187	1226
100	1094	1119

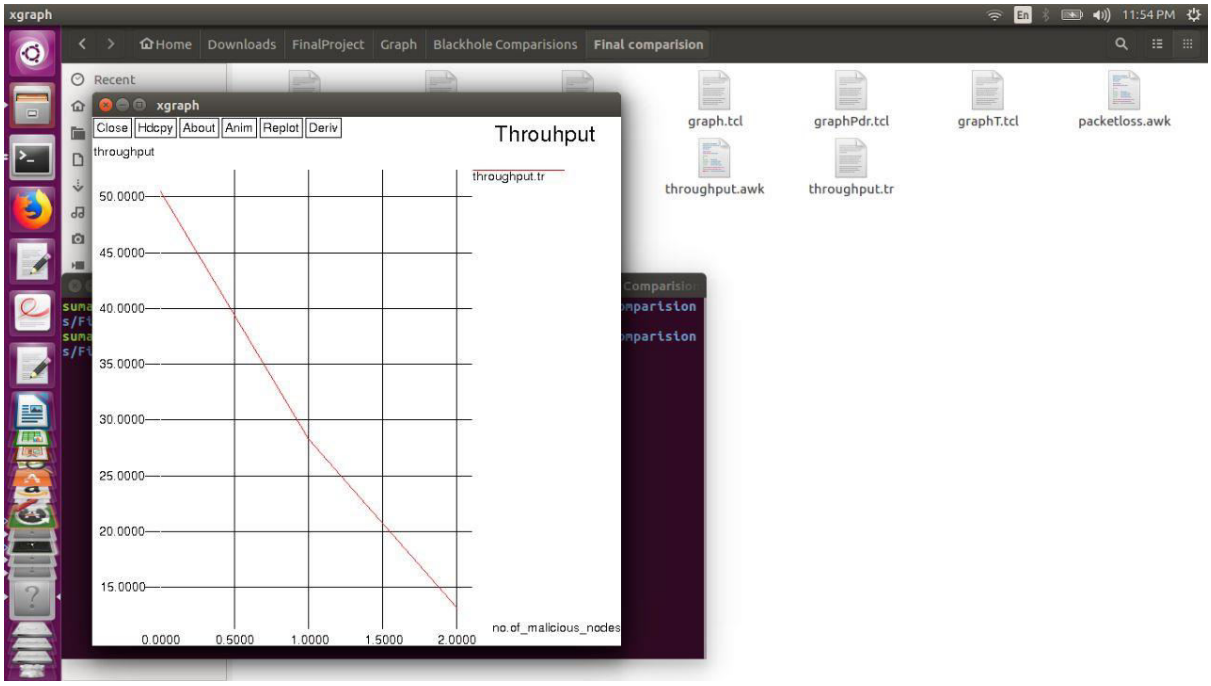

Fig 4.2 Malicious nodes X Throughput

Throughput = No. of packets received/Simulation time

Throughput is inversely proportional to time, so as the time taken to a packet to reach destination increases throughput decreases. When there is no malicious node the throughput is very high around 50, when there is a single malicious node throughput has decreased to 28. When there are two malicious nodes there is no enough throughput , it is decreased below 15.

Table 4.2 Throughput in the presence of one and two malicious nodes

No of nodes	Throughput for 1 malicious node	Throughput for 2 malicious node
20	1782	943
50	186.48	146.62
100	520	430

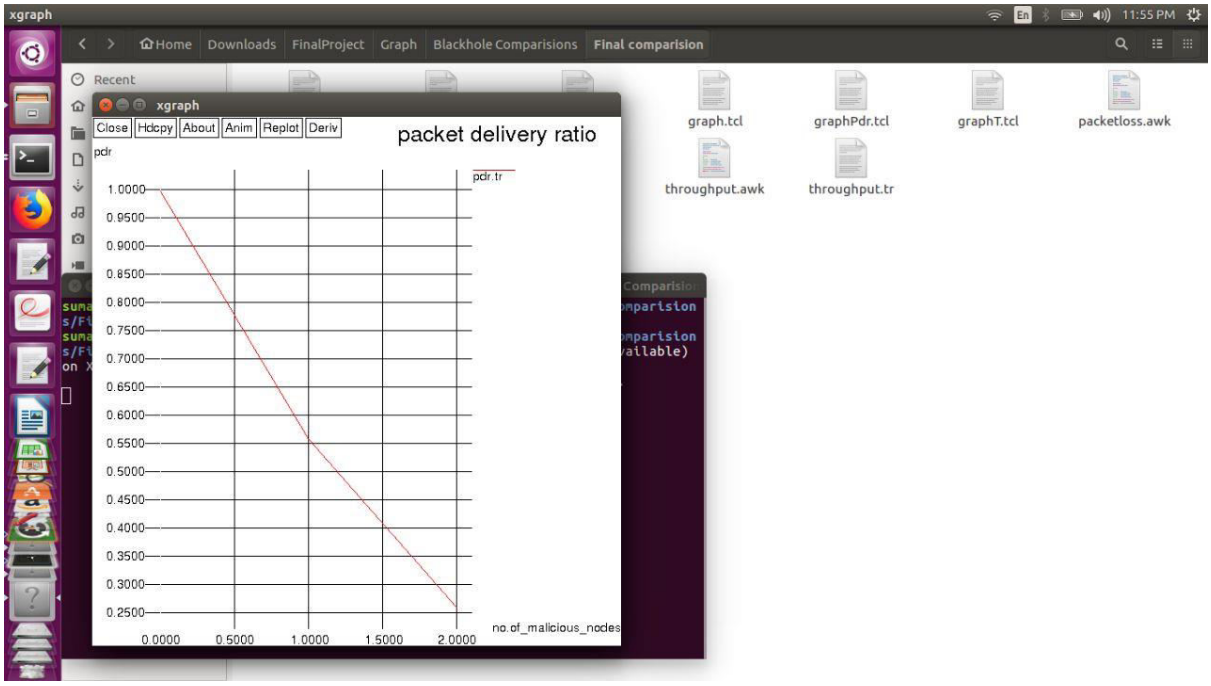

Fig. 4.3 malicious nodes X packetDeliveryRatio

Packet delivery ratio = number of packets received/number of packets sent

When every packet reaches the destination from source then the packet delivery ratio is one as number of packets sent is equal to number of packets received. It is observed from the graph that when there is no malicious node the packet delivery ratio is maximum to one, which means all the packets are reached from source to destination. As the malicious nodes in the network increased the packet delivery ratio gradually decreased, when there are two malicious nodes the delivery ratio is below 0.25.

Table 4.3 PDR in presence of one and two malicious nodes

No of nodes	PDR for single malicious node	PDR for two malicious node
20	40.02	21.2
50	4.19	1.04
100	11.70	9

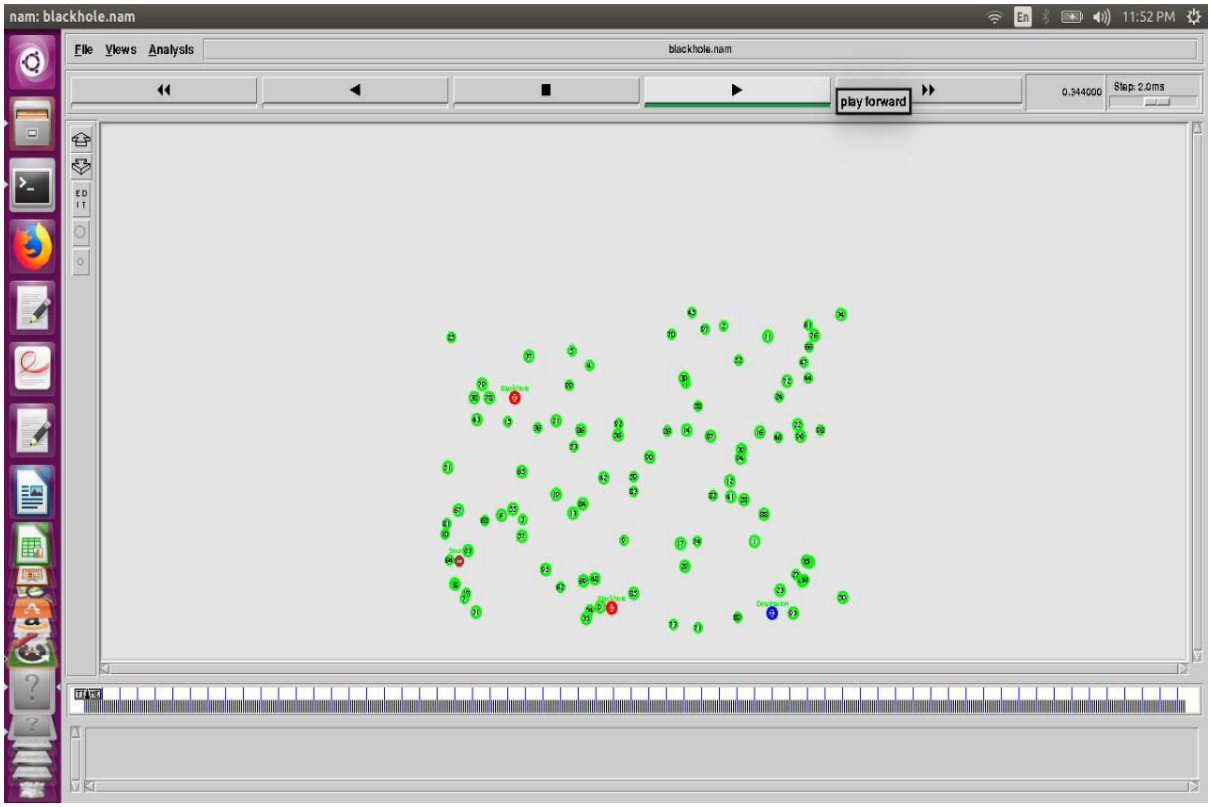

Fig. 4.4 MANET with 100 nodes

This is a screenshot of MANET with 100 mobile nodes, green color ones are normal nodes, red color ones are malicious nodes which leads to blackhole attack. Source node and destination nodes are colored with blue to distinguish from other nodes.

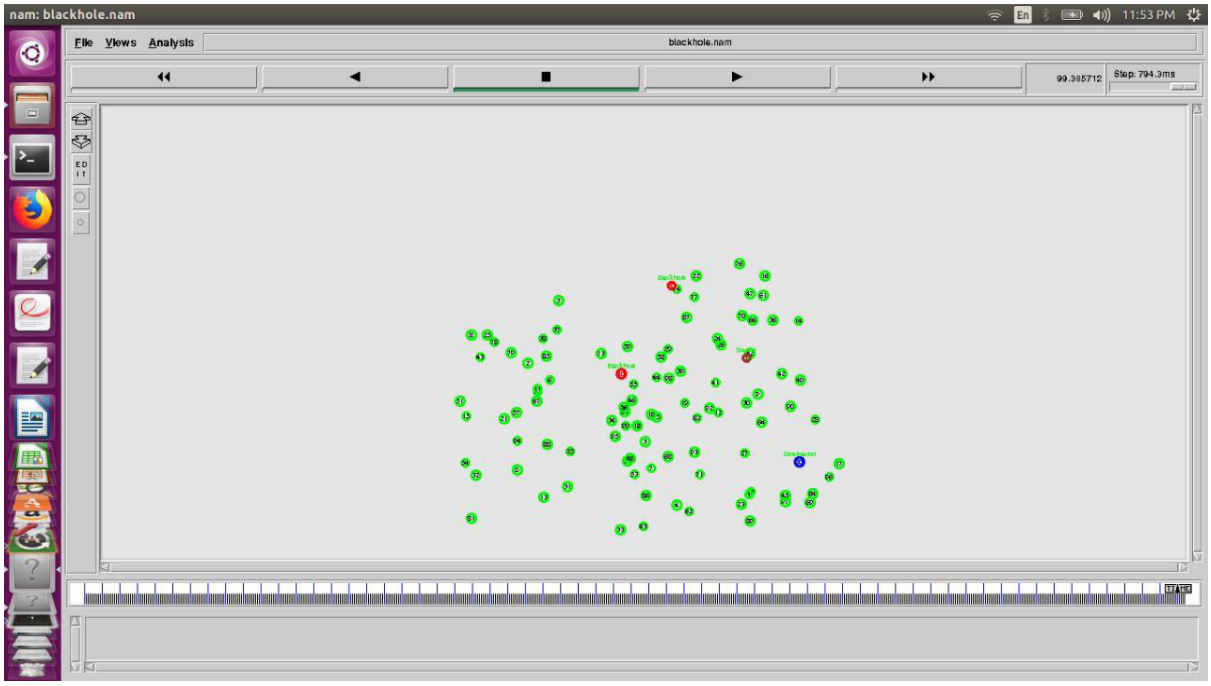

Fig 4.5 MANET with 50 nodes

This is a screenshot of MANET with 100 mobile nodes, green color ones are normal nodes, red color ones are malicious nodes which leads to blackhole attack. Source node and destination nodes are colored with blue to distinguish from other nodes.

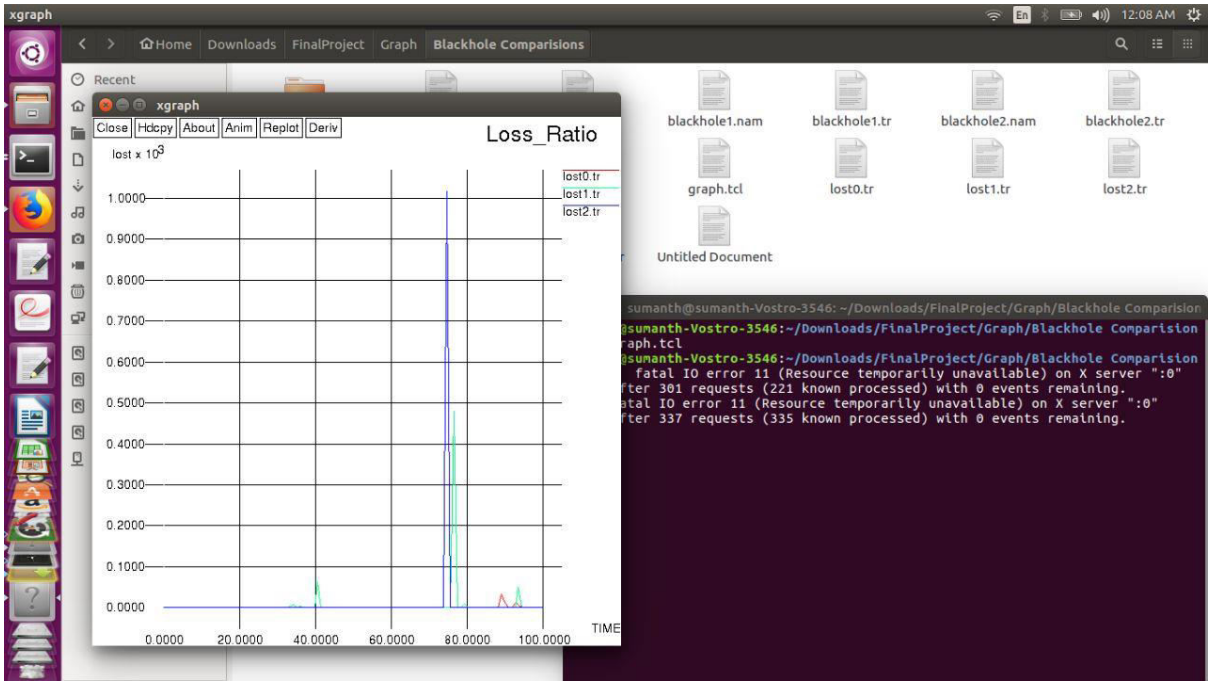

Fig 4.6 Time X lostx10^−3

This is packet loss ratio graph generated from a trace file. Red color graph shows lost ratio with respect to time when zero malicious nodes are in network. Green color graph shows lost ratio with respect to time when one malicious node is in network. Blue color graph shows lost ratio with respect to time when two malicious nodes are in network. It is observed that the loss ratio is very high for blue color graph which has two malicious nodes in network compared to green and red color graphs.

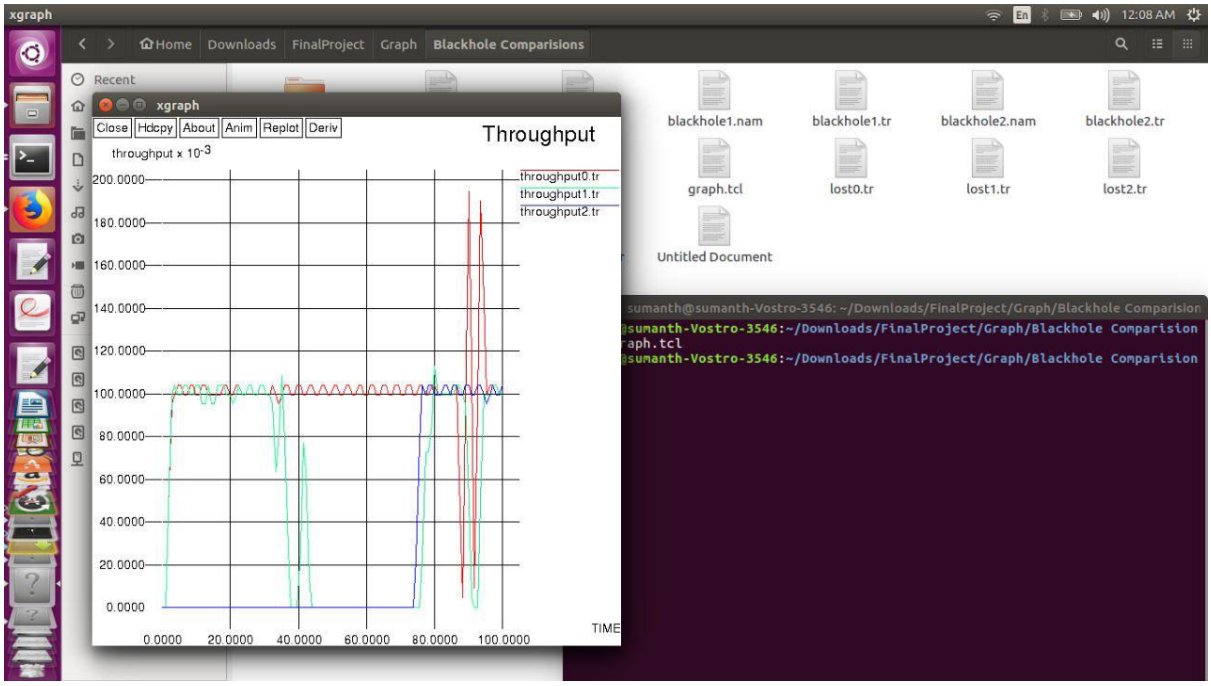

Fig 4.6 Time X Throughputx10^-3

As throughput is inversely proportion to time , which means there is high throughput if it takes less simulation time. Red color graph shows throughput with respect to time when zero malicious nodes are in network, Green color graph shows throughput with respect to time when there is one malicious node in network, Blue color graph shows throughput with respect to time when there are two malicious nodes in network.

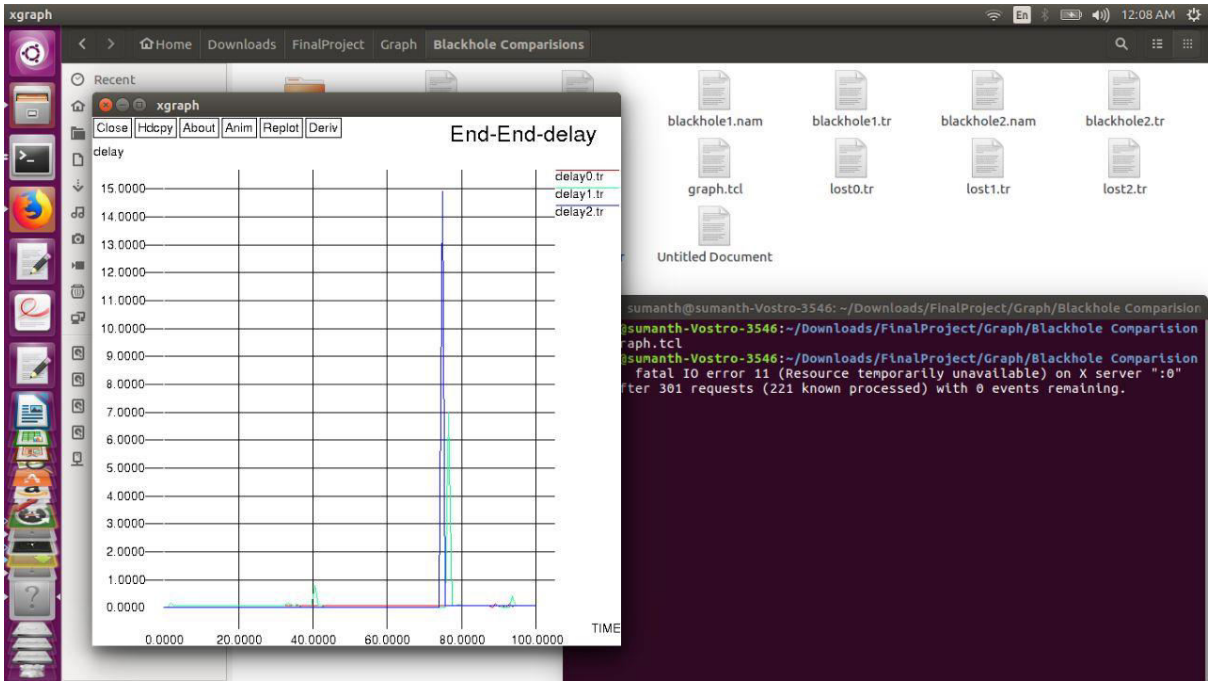

Fig 4.7 Time X delay

This graph shows the delay of messages in the network, if there is huge delay for a packet in the network it means it was lost to malicious node and that packet never reaches to the destination. Red color graph shows end-to-end delay with respect to time when zero malicious nodes are in network which shows very less delay from the graph. Green color graph shows delay with respect to time when one malicious node is in network , through which it is observed, some delay of packets in the network. Blue color graph shows delay with respect to time when two malicious nodes are in network, it is observed very high delay in the network.

4.2 Prevention Results

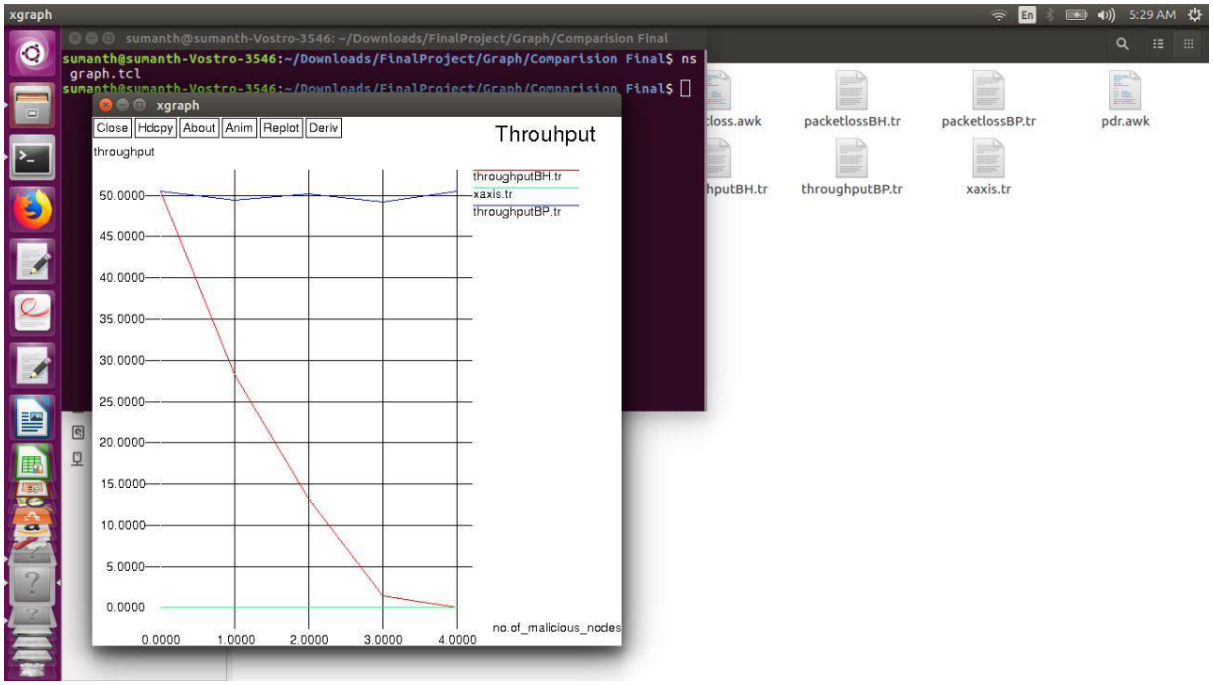

Fig 4.7 No. of malicious nodes X Throughput

From the above graph it is observed that the throughput is decreasing when there is a blackhole attack which is shown by red color line. When prevention is done throughput is good which is shown by a blue line.

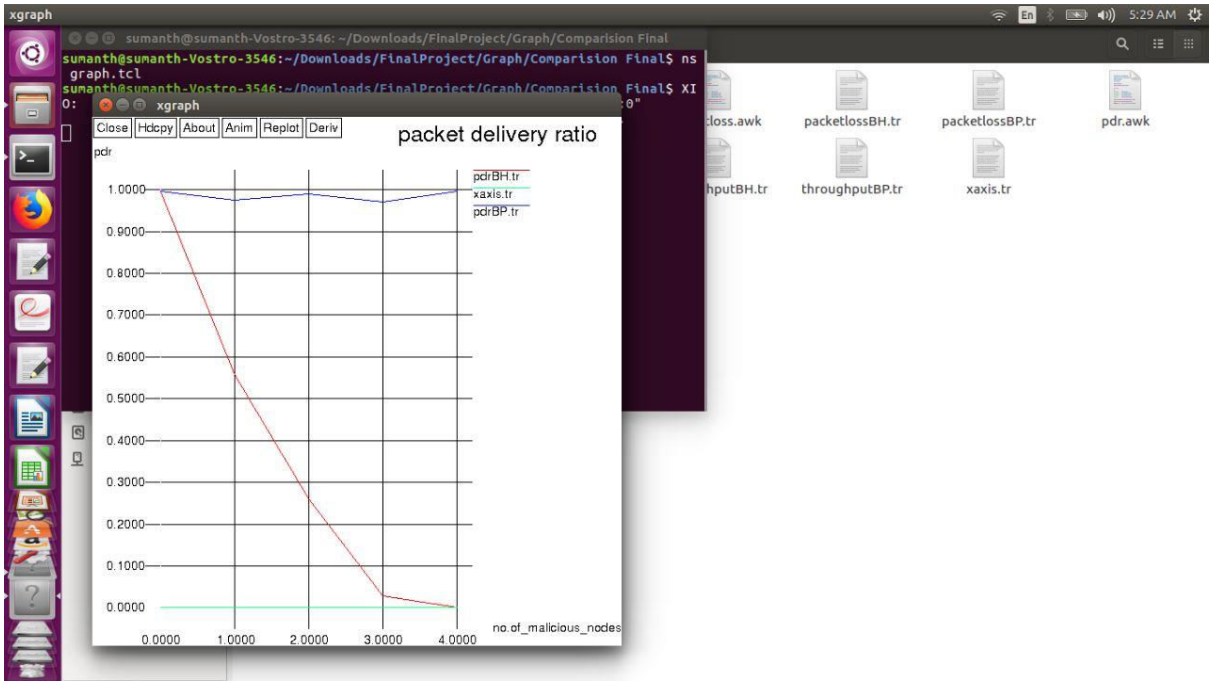

Fig 4.8 No. of malicious nodes X packet delivery ratio.

From the above graph it is observed that the packet dellivery ratio is decreasing when there is a blackhole attack which is shown by red color line. When prevention is done packet delivery ratio is good which is shown by a blue line.

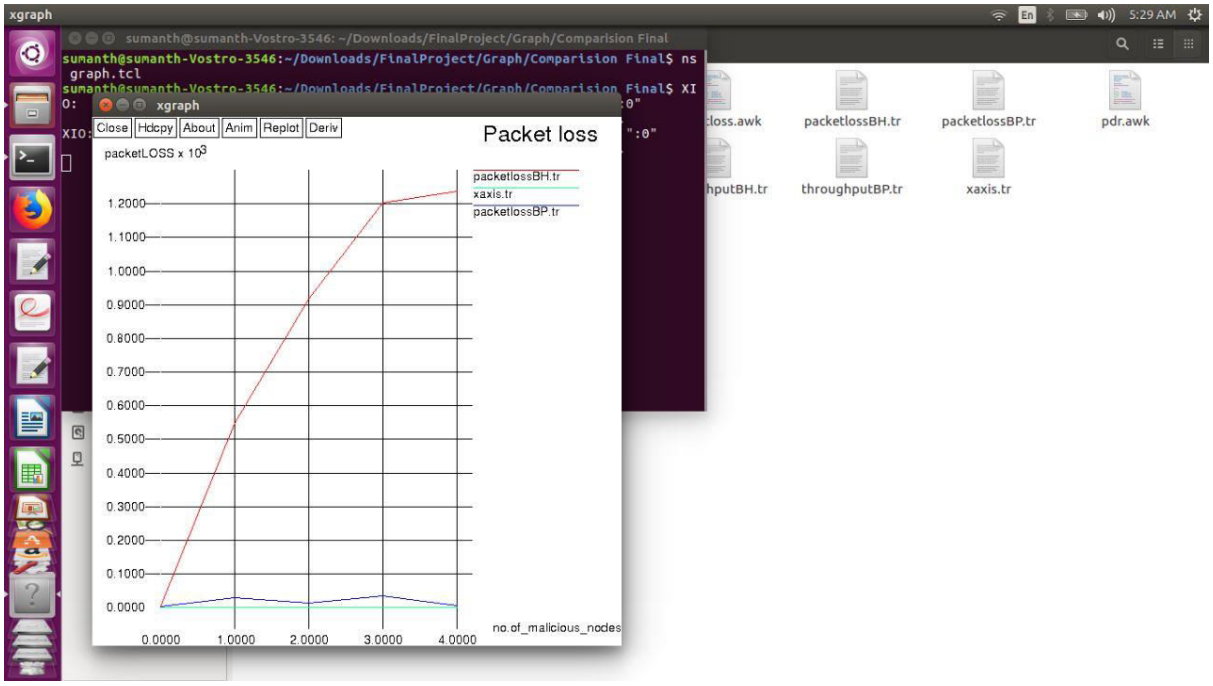

Fig 4.9 No. of malicious nodes X packet loss

From the above graph it is observed that the packet loss is increasing when there is a blackhole attack which is shown by red color line. When prevention is done packet loss is very less which is shown by a blue line.

Chapter V

Conclusion and Future Work

One type of attack is analyzed, that is blackhole attack in MANET using AODV routing protocol. The main criteria is analyzing the system performance with no blackhole, single blackhole and multiple blackholes and drawing graphs from the results, at the end preventing the blackhole attack from consuming the packets thereby increasing the performance of the network.

The following parameters were evaluated to measure the performance of the MANET:

(a) Throughput,
(b) Packet delivery ratio,
(c) Packet loss.

It is observed that the routing of data Packets in the mobile ad hoc network using AODV routing protocol is affected when there is a Blackhole attack due to which the efficiency of the network degrades.

In the prevention of blackholes this technique assumes that the source node is an intelligent node which uses the sequence number concept to detect the multiple blackhole nodes in MANET. This detection mechanism is effectively implemented using NS 2.35.

After the detection of blackhole nodes, the notification of black listed nodes to other nodes increases the network overhead which should be reduced in future. Also, in future a timer can be under which the detection will be done so that the delay of data packets can be decreased.

References

[1] K.Madhuri N.Kasi, Viswanath, P.Usha Gayatri "Performance Evaluation of AODV under Blackhole Attack in MANET using NS2", 2016

[2] Nishu Kalia, Harpreet Sharma, "Detection of Multiple Blackhole nodes attack in MANET by modifying AODV protocol", 2016

[3] K.Madhuri, N.Kasi Viswanath "Implementation of Position Based Technique to Prevent Worm Hole Attack in AODV Routing Protocol for Manet", Journal & Magazine of Engineering,Technology,Management and Research (IJMETMR)-Volume 5 ISSN No:2320 - 3706(Print) October 2016., Issue. 11.

[4] Umang, Dr. B V. R. Reddy, Dr. M .N. Hoda "MNI AODV Analytical model for Attack mitigation using AODV routing in ad hoc networks",.2014 International Conference on Computing for Sustainable Global Development (INDIACom).

[5] Uma Rathore Bhatt, Abhishek Dangarh, Akanksha Kashyap, Aishwarya Vyas "Performance analysis of AODV & DSR Routing protocols for MANET",.Fourth International Conference on Communication Systems and Network Technologies, 2014.

[6] Rakesh Kumar Singh, Rajesh Joshi and Mayank Singhal "Analysis of Security Threats and Vulnerabilities in Mobile Ad Hoc Network (MANET) International Journal of Computer Applications (0975 – 8887 Volume 68– No.4, April 2013.

[7] PriyankaGoyal, Vinti, Parmar, Rahul Rishi. MANET:Vulnerabilities, Challenges, Attacks, Application, IJCEM International Journal of Computational Engineering & Management, Vol.11, January 2011 ISSN (Online): 2230-7893 www.IJCEM.org,

[8] Anshika Garg, Shweta Sharma "A Study on Wormhole Attack in MANET".International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 3 Issue 2, May 2014.

[9] Fan-Hsun Tseng,Li-Der Chou and Han-Chieh Chao "A survey of blackhole attacks in wireless mobile ad hoc networks", HumancentricComputing and Information Sciences2011.

[10] Ankita M.Shendurkar, Prof. Nitin R.Chopde " A Review of Blackhole and Worm Hole Attack on AODV Routing Protocol in MANET" International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 8 - Mar 2014

[11] Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng (2007) "A Distributed and Cooperative Blackhole Node Detection and Elimination Mechanism for Ad Hoc Network". Paper presented at the PAKDD workshops, Nanjing, China, 22-25, pp. 538-549.

[12] E.A. Mary Anita, V. Vasudevan (2011), "Blackhole Prevention in Multicasting Routing Protocols for Mobile Ad hoc Networks using Certificate Chaining", International Journal of Computer Applications, Volume 1, pp. 21-28.

[13] Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao (2011), "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", Human-centric Computing and Information Sciences,Springer, New York, pp. 1-16.

[14] Gurdeep Singh Bindra, Ashish Kapoor, Ashish Narang, Arjun Agrawal (2012), " Detection and Removal of Co-operative Blackhole and Grey hole Attacks in MANETs", 2012 International Conference on System Engineering and Technology, Bandung, Indonesia, pp. 1-5.

[15] K.Madhuri Routing protocols in MANET, International Journal of Information and Communication Technology (IJICT).December 2011, ISSN NO. -1466- 6642.

Appendix

Wireless code

```
puts "Enter number of nodes (more than 10 nodes)"
set tnn [gets stdin]
#===================================
#     Simulation parameters setup
#===================================
set val(chan)   Channel/WirelessChannel    ;# channel type
set val(prop)   Propagation/TwoRayGround   ;# radio-propagation model
set val(netif)  Phy/WirelessPhy            ;# network interface type
set val(mac)    Mac/802_11                 ;# MAC type
set val(ifq)    Queue/DropTail/PriQueue    ;# interface queue type
set val(ll)     LL                         ;# link layer type
set val(ant)    Antenna/OmniAntenna        ;# antenna model
set val(ifqlen) 50                         ;# max packet in ifq
set val(nn)     $tnn                       ;# number of mobilenodes
set val(rp)     AODV                       ;# routing protocol
set val(x)      1500                       ;# X dimension of topography
set val(y)      1500                       ;# Y dimension of topography
set val(stop)   100.0                      ;# time of simulation end

#===================================
#        Initialization
#===================================

set f0 [open throughput.tr w]
set f1 [open lost.tr w]
set f2 [open delay.tr w]
#Create a ns simulator
set ns [new Simulator]

#Setup topography object
```

```
set topo       [new Topography]
$topo load_flatgrid $val(x) $val(y)
create-god $val(nn)

#Open the NS trace file
set tracefile [open blackhole.tr w]
$ns trace-all $tracefile

#Open the NAM trace file
set namfile [open blackhole.nam w]
$ns namtrace-all $namfile
$ns namtrace-all-wireless $namfile $val(x) $val(y)
set chan [new $val(chan)];#Create wireless channel


#=================================
#     Mobile node parameter setup
#=================================
$ns node-config -adhocRouting  $val(rp) \
                -llType        $val(ll) \
                -macType       $val(mac) \
                -ifqType       $val(ifq) \
                -ifqLen        $val(ifqlen) \
                -antType       $val(ant) \
                -propType      $val(prop) \
                -phyType       $val(netif) \
                -channel       $chan \
                      -energyModel EnergyModel \
                      -initialEnergy 100 \
                       -rxPower 0.3 \
                       -txPower 0.6 \
                -topoInstance  $topo \
                -agentTrace    ON \
                -routerTrace   ON \
```

```
            -macTrace      OFF \
            -movementTrace ON

#=================================
#        Nodes Definition
#=================================
for {set i 0} {$i < $val(nn) } {incr i} {
set n($i) [$ns node]

$n($i) set X_  [expr rand() * 1500]
$n($i) set Y_ [expr rand() * 1000]
$n($i) set Z_ 0.000000000000;
$ns initial_node_pos $n($i) 30

}

puts "Enter source node"
set source [gets stdin]
puts "Enter destination node"
set dest [gets stdin]

puts "Enter Total Number of Blackhole in the network:"
set twh [gets stdin]
puts "Enter Blackhole node ids:"
for {set i 0} {$i < $twh } {incr i} {
set whno [gets stdin]
set no($i) $whno
}
for {set i 0} {$i < $twh } {incr i} {
$n($no($i)) color red
$ns at 0.0 "$n($no($i)) color red"
$ns at 0.0 "$n($no($i)) label Blackhole"
$ns at 0.0 "[$n($no($i)) set ragent_] hacker"
}
```

```
$n($source) color green
$ns at 0.0 "$n($source) color brown"
$ns at 0.0 "$n($source) label Source"

$n($dest) color blue
$ns at 0.0 "$n($dest) color blue"
$ns at 0.0 "$n($dest) label Destination"

#for random motion
for {set i 0} {$i < $val(nn)} {incr i} {
    set xx_ [expr rand()*1500]
    set yy_ [expr rand()*1000]
    set rng_time [expr rand()*$val(stop)]
    $ns at $rng_time "$n($i) setdest $xx_ $yy_ 15.0"   ;# random movements


}


#=================================
#        Agents Definition
#=================================
#Setup a UDP connection
set udp0 [new Agent/UDP]
$ns attach-agent $n($source) $udp0
set null1 [new Agent/LossMonitor]
$ns attach-agent $n($dest) $null1
$ns connect $udp0 $null1
$udp0 set packetSize_ 1500

#=================================
#        Applications Definition
#=================================
```

```
#Setup a CBR Application over UDP connection
set cbr0 [new Application/Traffic/CBR]
$cbr0 attach-agent $udp0
$cbr0 set packetSize_ 1000
$cbr0 set rate_ 0.1Mb
$cbr0 set random_ null
$ns at 1.0 "$cbr0 start"
$ns at 100.0 "$cbr0 stop"

set holdtime 0
set holdseq 0

set holdrate1 0

proc record {} {
global null1  f0 f1 f2 holdtime holdseq holdrate1

set ns [Simulator instance]
set time 0.9 ;#Set Sampling Time to 0.9 Sec

set bw0 [$null1 set bytes_]
set bw1 [$null1 set nlost_]

set bw2 [$null1 set lastPktTime_]
set bw3 [$null1 set npkts_]

set now [$ns now]

      # Record Bit Rate in Trace Files
      puts $f0 "$now [expr (($bw0+$holdrate1)*8)/(2*$time*1000000)]"



      # Record Packet Loss Rate in File
      puts $f1 "$now [expr $bw1/$time]"
```

```
if { $bw3 > $holdseq } {
        puts $f2 "$now [expr ($bw2 - $holdtime)/($bw3 - $holdseq)]"
    } else {
        puts $f2 "$now [expr ($bw3 - $holdseq)]"
    }

$null1 set bytes_ 0
$null1 set nlost_ 0

set holdtime $bw2
set holdseq $bw3

set  holdrate1 $bw0
   $ns at [expr $now+$time] "record"   ;# Schedule Record after $time interval sec
}


# Start Recording at Time 0
$ns at 0.0 "record"


#===================================
#        Termination
#===================================
#Define a 'finish' procedure
proc finish {} {
   global ns tracefile namfile
   $ns flush-trace
   close $tracefile
   close $namfile
   exec nam blackhole.nam &
#exec xgraph throughput.tr -geometry -x time -y throughput -t Throughput 800x400 &
 #exec xgraph lost.tr  -geometry -x time -y lost -t Lost 800x400 &
```

```
 #exec xgraph delay.tr  -geometry -x time -y delay -t End_End_Delay 800x400 &
    exit 0
}
for {set i 0} {$i < $val(nn) } { incr i } {
    $ns at $val(stop) "\$n($i) reset"
}
$ns at $val(stop) "$ns nam-end-wireless $val(stop)"
$ns at $val(stop) "finish"
$ns at $val(stop) "puts \"done\" ; $ns halt"

$ns run
```

The above code takes the input as number of nodes in the MANET and takes source and destination ID's, then asks to enter the number of malicious nodes in the network with their respective ID's.

Throughput:

```
BEGIN {
        recvdSize = 0
        startTime = 400
        stopTime = 0
 }

 {
            event = $1
            time = $2
            node_id = $3
            pkt_size = $8
            level = $4

 # Store start time
 if (level == "AGT" && event == "s" && pkt_size >= 512) {
  if (time < startTime) {
            startTime = time
            }
      }

 # Update total received packets' size and store packets arrival time
 if (level == "AGT" && event == "r" && pkt_size >= 512) {
      if (time > stopTime) {
            stopTime = time
            }
      # Rip off the header
      hdr_size = pkt_size % 512
      pkt_size -= hdr_size
      # Store received packet's size
      recvdSize += pkt_size
      }
```

```
  }

  END {
      printf("Average Throughput[kbps] = %.2f\t\t
StartTime=%.2f\tStopTime=%.2f\n",(recvdSize/(stopTime-
startTime))*(8/1000),startTime,stopTime)
  }
```

The above code calculates the throughput.

PacketLoss:

```
BEGIN {
        sendLine = 0;
        recvLine = 0;
        fowardLine = 0;
}

$0 ~/^s.* AGT/ {
        sendLine ++ ;
}

$0 ~/^r.* AGT/ {
        recvLine ++ ;
}

$0 ~/^f.* RTR/ {
        fowardLine ++ ;
}

END {
        printf "cbr s:%d r:%d, r/s Ratio:%.4f, f:%d \n", sendLine, recvLine, (sendLine-
recvLine),fowardLine;
}
```

This above code calculates packetloss in the MANET.

PacketDeliveryRatio:

```
BEGIN {
        sendLine = 0;
        recvLine = 0;
        fowardLine = 0;
}

$0 ~/^s.* AGT/ {
        sendLine ++ ;
}

$0 ~/^r.* AGT/ {
        recvLine ++ ;
}

$0 ~/^f.* RTR/ {
        fowardLine ++ ;



}

END {
        printf "cbr s:%d r:%d, r/s Ratio:%.4f, f:%d \n", sendLine, recvLine,
(recvLine/sendLine),fowardLine;
}
```

This above code helps us in calculating packetdelivery ratio.