



L OVELY
P ROFESSIONAL
U NIVERSITY

**DETECTION OF BLACK HOLE ATTACK WITH
IMPROVED AODV PROTOCOL IN MANET**

A Dissertation Proposal

Submitted

By

Lalita

(11303509)

To

Department of Computer Science & Engineering

In partial fulfillment of the requirement for the

Award of the degree of

Master of Technology in Computer Science

Under the guidance of

Mr. Anurag Singh Tomar

(May 2015)

School of: Computer Engineering

DISSERTATION TOPIC APPROVAL PERFORMANCE

Name of the Student: LALITA Registration No.: 11303509 (11303509)
 Batch: 2013 Roll No. B55
 Session: 2nd Semester Parent Section: RK2306
 Details of Supervisor: Designation: Asst. Prof.
 Name: Anurag Qualification: M. Tech
 U.I.D.: 15812 Research Experience: 3 years

SPECIALIZATION AREA: _____ (pick from list of provided specialization areas by DAA)

PROPOSED TOPICS

1. Wireless Network (MANET)
2. Cloud Computing (Security Issue)
3. Image Processing (Segmentation of Image)

Anurag
 Signature of Supervisor

PAC Remarks: Student will focus on Algorithm to prevent from Black hole attacks. I am expecting to Publish Research Paper in this topic

APPROVAL OF PAC CHAIRPERSON:

11/10/14
 Signature: [Signature]

Date:

*Supervisor should finally encircle one topic out of three proposed topics and put up for approval before Project Approval Committee (PAC)

*Original copy of this format after PAC approval will be retained by the student and must be attached in the Project/Dissertation final report.

*One copy to be submitted to Supervisor.

ABSTRACT

Mobile Ad-Hoc network is widely used in our society in forms of mobiles, laptops, tablets and palmtops and etc. We are not stable at one place and always moving from place to another place. Ad-hoc network is a way to make our communication effectively and easily. Ad-hoc network is a collection of dynamic nodes it means any node can join the network and leave the network any time. Ad-hoc network creates a network connection between two entities in a single session for communication. In ad-hoc network does not use any router or wireless base station. For example two friends are there and one friend want send a file to his mobile to his friend's laptop. Such type of communication is possible to use the ad-hoc network communication in a form of Bluetooth. The communication of Bluetooth acts as an ad-hoc and does not required any wireless base station or router. In ad-hoc network the bandwidth capacity is very much limited and network is to be optimized maximum efficiency with in limited bandwidth. Wireless communication is less secure than wired communication and that's why it is the vulnerability of mobile ad-hoc network and any threat can easily affect the communication. Many types of attacks are developed today which badly crash the network and make the communication performance degrade. These attacks are worm hole attack, black hole attack, sink whole attack, Sybil attack, flooding attack and man in middle attack and many more. We propose the technique on security of mobile ad-hoc network. To provide the security of mobile ad-hoc network we generate new techniques for detection of black hole attack. Black hole attack is type of malicious node who drops the packet instead to send that packet to their destination. For the security of the network propose new algorithm that increase packet delivery rate and increase the throughput as well as reduce the delay of packet delivery. In this propose algorithm try to check the black hole node by route request packets and implement the prime number concept for detect the black hole node. It will improve the performance of the networks.

CERTIFICATE

This is to certify that **LALITA** has completed M.Tech dissertation proposal titled **Detection of black hole attack with improved AODV protocol in MANET** under my guidance and supervision. To the best of my knowledge, the present work is the result of her original investigation and study. No part of the dissertation proposal has ever been submitted for any other degree or diploma.

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

Date:

Signature of Advisor

Name: Anurag Singh Tomar

UID: 15812

ACKNOWLEDGEMENT

I owe a debt of deepest gratitude to my thesis supervisor, **Mr. Anurag Singh Tomar**, Department of Computer Science & Engineering, for his guidance, support, motivation and encouragement throughout the period this work was carried out. His readiness for consultation at all times, his educative comments, his concern and assistance even with practical things have been invaluable.

I am grateful to **Mr. Dalwinder Singh**, Head of department Computer Science & Engineering for providing me the necessary opportunities for the completion of my work. I also thank the other faculty and staff members of my department for their invaluable help and guidance.

DECLARATION

I hereby declare that the dissertation proposal entitled, “Detection of Black Hole Attack with improved AODV protocol in MANET” submitted for the M.Tech Degree is entirely my original work and all ideas and references have been duly acknowledged. It does not contain any work for the award of any other degree or diploma.

Date:

Lalita

Registration no: 11303509

TABLE OF CONTENTS

Abstract.....	i
Certificate.....	ii
Acknowledgement.....	iii
Declaration	iv
Table of Contents.....	v
List of Figures	vi
List of Tables.....	vii
Chapter 1 Introduction.....	1
1.1 Mobile Adhoc Networks.....	2
1.2 Types of Adhoc Networks.....	3
1.3 Types of Routing Protocols.....	4
1.4 Features of manet.....	7
1.5 Applications of Manet.....	8
1.6 Challenges of Manet.....	9
1.7 Black hole attack.....	10
Chapter 2 Review of Literature.....	12
Chapter 3 Present Work.....	28
3.1 Problem Formulation.....	29
3.2 Objectives of the study.....	30
3.3 Proposed Algorithms	29
Chapter 4 Results and Discussions.....	36
Chapter 5 Conclusion & Future scope.....	43
Chapter 6 References.....	44
Chapter 7 Appendix.....	50

LIST OF FIGURES

S.NO	LIST OF FIGURES	PAGE NO.
1.1	Wireless networks and its types	2
1.2	Mobile ad-hoc networks	3
1.3	Types of Routing Protocols	4
1.4	Black hole	11
2.1	Trust based model ET-AODV	18
3.1	Flow chart of proposed methodology	31
3.2	Packet delivery ratio	32
3.3	Probability check of two assumptions	33
3.4	Ratio of check forward request	34
4.1	Comparison of end to end delay graph	37
4.2	Comparison of throughput graph	38
4.3	Throughput awk script	39
4.4	Delay awk script	39
4.5	Screenshot of SAODV protocol	40
4.6	Screenshot of testcode.tcl	40
4.7	Nam file screenshot 1	41
4.8	Nam file of screenshot 2	41
4.9	Nam file of screen shot 3	42

LIST OF TABLES

4.10 simulation parameters

43

CHAPTER 1

INTRODUCTION

In today's world the Wireless network is very much use and use wireless data connection for connecting the network nodes. The wireless network generally uses the radio communication for connecting the networks. A wireless network generally use the radio communication for connect the devices like laptops, mobiles and etc. Wireless network generally have two types-

- Infrastructure network-These types of network are those network where already an infrastructure build for manage the network or coordinate the network. Infrastructure network is physically connected to its devices like routers, switch, hubs and etc. These types of networks are using the access points between devices and the base stations for communication to each other.
- Infrastructure less network-These types of networks are totally opposite to infrastructure network. These types of networks are not using any physical device for communication like as the infrastructure networks. In these types of networks not use any access point between devices and base stations. In these types of network not any coordinator or manger so it is called as infrastructure less because lack of predefined network structure.

In this following Figure no.1.1 describe the wireless network types, the wireless network are infrastructure and infrastructure less as explain above. The infrastructure network further divides as –

- Cellular network-Cellular Network is a type of wireless network and it distributed over particular land areas and each area has one particular transceiver and these are called as cells.
- Wireless LAN-Wireless LAN is a type of computer network that use to connect two or more devices together with the help of distribution method in a limited area. This gives user ability to move around within a local coverage area for their communication.

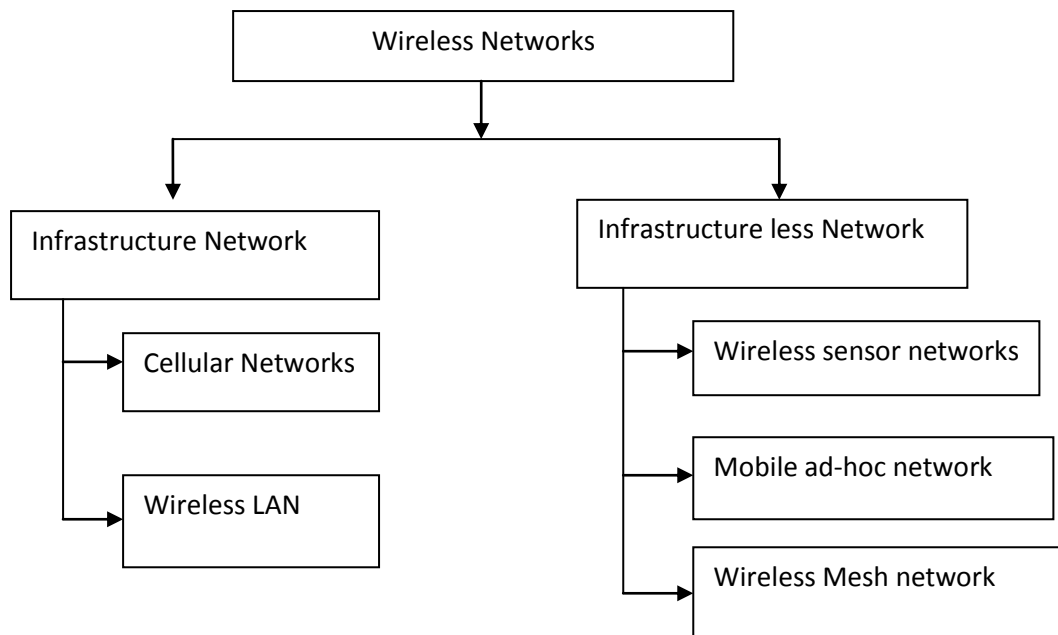


Figure 1.1 wireless network and its types

So, all these are the all parts of the wireless network, which divides the network in two different parts. One part is for wired network and the other part is the part is for the wireless network or we can say that the ad-hoc mobile network or peer to peer network.

1.1 Mobile Ad-Hoc Network

Now we will discuss the mobile ad-hoc network, Mobile ad-hoc network is a collection of dynamic nodes, it means in MANET any node can enter the network any time and join the network any time. There is no effect if any node can automatically leave the network. For example, If there any three friends communicate with each and one friend using laptop and others two using mobiles and one friend that using laptop send some files to his friends mobiles via Bluetooth and between two friends who using mobiles off his Bluetooth during transfer the file time, then it no effect on other friend who also using mobile and he will receive the file successfully to his friend's laptop. We can say that it is a form of wireless network. Because it is ad-hoc means temporary nodes stable in network. In MANET there is no access points and infrastructure. There is no coordinator who coordinates the system.

In this Figure-1.2 shows the mobile ad-hoc networks that all systems or devices are connected to each other directly without base station and access points.

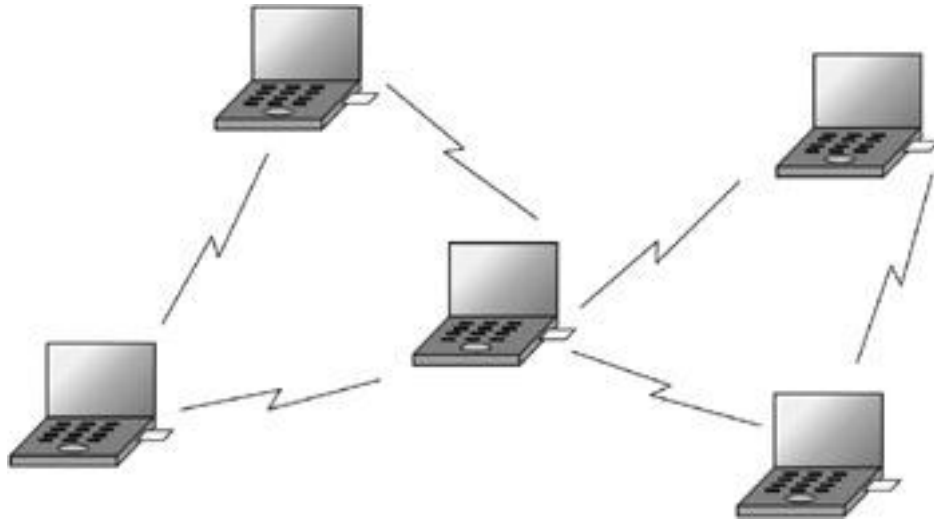


Figure 1.2 Mobile ad-hoc networks

All devices are connected to each other without base station and access points.

1.2 Types of Mobile Ad-Hoc Network

a) **WIRELESS SENSOR NETWORK-** A sensor network is an infrastructure comprising of sensing, computing and communication elements to monitor physical or environmental conditions like temperature, sound, etc. Nowadays mobile phones are also equipped with sensors like proximity sensors, light sensors. Other types of sensors are biosensors, chemical sensors, etc.

The main basic component of wireless sensor network are-

- Microcontroller
- Transceiver
- External memory Power source

b) **WIRELESS MESH NETWORK-** Wireless mesh network are depend of radio nodes and organized in mesh topology. Mesh network combinations of mesh clients, mesh routers and gateways. The mesh clients can often laptops, cell phones and other connecting devices and mesh routers are often forward traffic to and from the gateway networks.

1.3 Types of Routing Protocols

Now we will discuss about types of routing protocols which use in mobile ad-hoc networks. In Ad-hoc types of routing protocols are divided in three parts namely-

- Proactive routing protocol
- Reactive routing protocol
- Hybrid routing protocol

These 3 again comprise of the other protocols that are clearly mentioned and represented diagrammatically below:

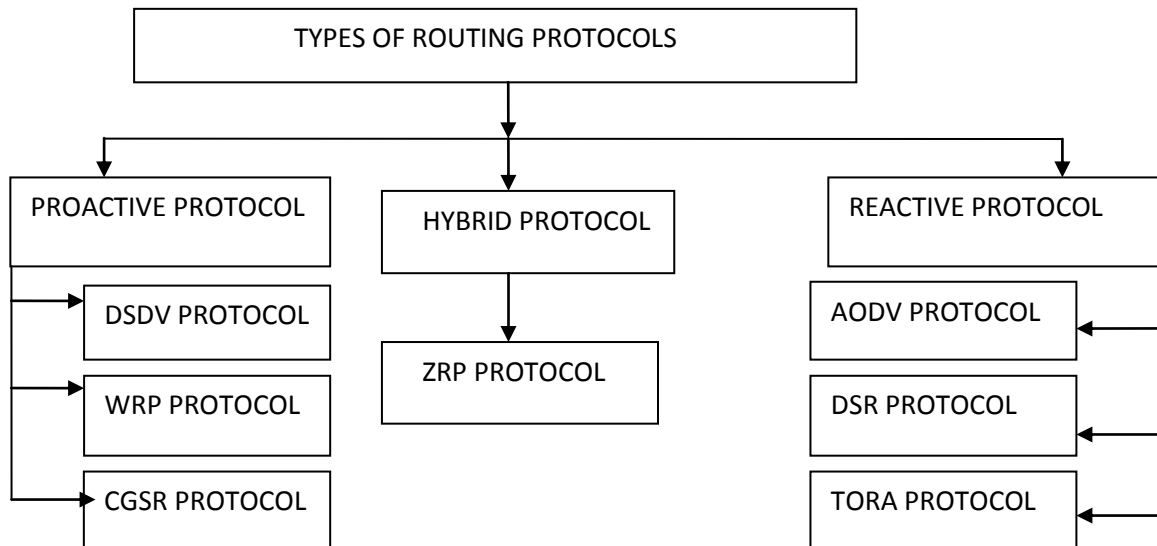


Figure 1.3 Types of routing protocol

- **PROACTIVE OR TABLE –DRIVEN ROUTING PROTOCOLS**-Table driven or proactive protocols are that protocols where tables are already maintain for send the plackets source to destination. In this routing protocol every node maintains one or more tables through to this representing the entire topology of the network. The table is updated after a time interval regularly due to maintain the table up-to-date to each node with every other node. To maintain the table up to date the topology exchanges the table information regularly. That's the reason this routing protocol is called as the table driven protocols. The table driven protocols are as follows-
 - a) **DESTINATION SEQUENCE DISTANCE VECTOR ROUTING PROTOCOL**-This protocol called as (DSDV) PROTOCOL. This protocol is based on bell-men ford

algorithm. This protocol is mainly use the problem of the routing loops problem. The best feature of this protocol is the on every entry of the routing table contains a sequence number. If the link is present in the network than use the even numbers otherwise use the odd number sequence order.

b) **WIRELESS ROUTING PROTOCOL**-Wireless routing protocol is a name of WRP protocol and it is also the part of the table driven routing protocol. WRP PROTOCOL is the enhance version of the DSDV protocol that use the concept of bell-men ford algorithm. With this algorithm calculates the path from source to destination. Like DSDV protocol the WRP also keep the up to date tables for route maintenance. But the basic difference both of them is the DSDV protocol use only one topology table for route maintains but the WRP protocol use the set of tables for route maintains. The table that maintained by node is the-

- Distance table (DT)
- Routing table (RT)
- Link cost table (LCT)
- Message retransmission list (MRL)

CLUSTER GATEWAY SWITCH ROUTING PROTOCOL-CGSR protocol use the hierarchical network topology. CGSR make nodes into the cluster and these clusters members choose their cluster head. The cluster head is elect dynamically and use the least cluster change (LCC) algorithm. According to this cluster head election the cluster head becomes that node which comes under the range of another cluster head. The benefit of CGSR protocol is that it allocates the bandwidth and provides better bandwidth utilization.

- **REACTIVE OR ON DEMAND ROUTING PROTOCOL**-ON Demand or reactive protocols are that protocols where tables are not already maintained. This protocol performs the task of path finding. This protocol is work whenever source realizes that it may want to send the packet to destination so for find the accurate path the source node send the request to all connecting nodes.

a) **Ad-hoc On-demand Distance–vector routing protocol (AODV)**-It is on demand routing protocol and does not contain any table like as the proactive routing

protocols. In this protocol when source want to send the packet to destination than send the route request packet to all connecting nodes for send the data packet to destination. After than the all connecting nodes give that source node reply packet in respect to route request packets. AODV has three main phases-

- ROUTE REQUEST PHASE
 - ROUTE REPLY PHASE
 - ROUTE MAINTAINCE PHASE
- b) DYNAMIC SOURCE ROUTING PROTOCOL (DSR)-DSR routing protocols also the on-demand routing protocol. The main motive of this protocol is to restrict the bandwidth consumption by control packets. The main difference of this protocol and between other protocol is the for connection establishment it does not require send hello packets. The working is same as the AODV protocol but in this protocol use sequence no. with route request packet. The sequence no. in the packet avoids the problem of loop-formation and avoids multiple transmissions of same packets. The DSR protocol also use the route cache, this route cache is used by the intermediate nodes. The two main phases of DSR routing protocol-
- ROUTE DISCOVERY PHASE
 - ROUTE MAINTAINCE PHASE
- c) TEMPORALY ORDERED ROUTING ALGORITHM-This routing protocol is called as TORA. It is source initiated protocol and reduces the loop-formation problem. It is use the link reversal algorithm. In TORA each node keeps the one local hop information.
- **Hybrid Routing Protocol**-Hybrid protocol has contains the features of the proactive and reactive protocol information. Hybrid means combination of something.
- a) ZONE ROUTING PROTOCOL-Zone routing protocol is a hybrid protocol. Which protocol is using within an area that is called as the intra zone routing protocol and that protocol which using outside of area that is inter zone routing protocol.

1.4 Features of Mobile Ad-Hoc Networks-

1. Distributed environment-In mobile ad-hoc networks there is no central coordinators among the nodes so there is distributed environment and all the functions divides between the nodes.
2. Multi-Hop routing-Whenever any node try to communicates with another node but due to the networks problem or out of range the packet send by the intermediate routers.
3. Dynamic terminology- The nodes are free to move in the environment due to the dynamic feature, it means any node can join or leave the network any time.
4. Autonomous-The nodes are independent to move due to the absence of central coordinator so they can act as a host or router itself.
5. Light- weight- In Manet environment there is no constraint of power and storage because their light weight feature and use less CPU capability.
6. Shared Physical Medium-The medium of wireless communication can be accessible with any entity and device and there is no issue about this.
7. Scalability- in the Manet there is no issue of scalability and can add number of nodes for access the services.
8. Limited Bandwidth-There is bandwidth issue to nodes and network very much less and efficiency gains on the level of maximum.
9. Type of Routing- In mobile ad-hoc networks there is type of routing that depends on the network. The single-hop routing is simpler than multi-hop routings.
10. Manet Structure-The mobile ad-hoc structure is easier than wired networks. It is easy to understand and creates.
11. Ease of Deployment-The mobile ad-hoc networks is easy to deploy with number of nodes and scenarios.
12. Speed- The mobile ad-hoc networks gives the facility of speed. The data can be shared fast way from one device to another.
13. Topologies- Manet there is use two types of topologies that are used in network and that are the heterogeneous and homogenous topology. Heterogeneous means communication between different devices to each other and homogenous means communication of same devices.

1.5 Applications of Manet-

1. Rescue time- On the time of disasters when any type of communication not working on that type of environment than the Manet plays very important role.
2. Educations and conferences- The Manet plays role in the educational institutes on the time of conferences and seminars.
3. Military Sectors- The ad-hoc networks give the advantage to military persons to contact their vehicles and soldiers so they can handle the situation of battles.
4. Commercial Sectors- In the commercial sectors it is very helpful because due to this easy to create communication between ship to ship and ad-hoc mobile communications and etc.
5. Low level- In the low level environment like home networks where with the help of devices can exchange information like personal area networks.
6. Civilian Environments- It is very helpful in civilian environment like cabs, sports stadium, boats and small crafts.
7. Multi games-The mobile ad-hoc networks very important role in the multi door out games for small kids.
8. Music and Entertainments- The mobile ad-hoc networks today most use in entertainment purpose and shopping and music etc.
9. Replacement of fixed infrastructure- In case of the natural disasters the replacement of fixed infrastructure use the techniques of mobile ad-hoc networks.
10. Network and constructions sites- Mobile ad-hoc networks use in network and construction sites because their wired network is not work successfully.
11. E-commerce and business- The mobile ad-hoc networks very useful for e-commerce and business sites for electronic payments any times and anywhere. This use for dynamic database access and mobile offices.
12. Supporting doctors and nurses in hospitals- The mobile ad-hoc networks is very useful in hospitals for contacts to doctors and nurses in emergency situation.
13. Vehicular services-The mobile ad-hoc network is use in the vehicular area networks in case of road or accident guidance and transmission of road and weather condition.

1.6 Challenges in Manet-

1. Infrastructure less- The first challenge in Mobile ad-hoc networks is the infrastructure less environment so designing new network design is challenges.
2. Dynamic Environments- The other issue in the mobile ad-hoc networks is the dynamic environments means changing topology affect the communication of source to destination.
3. Power issue-The other issue in the Manet is the limited battery life and power so this reason it consumes lots of resources and increase the overhead.
4. Autonomous nature-Due to the absence of the admin there is no central coordinator to control the function of the mobile nodes due to this reasons the mobile nodes move in network and fails to configure that proper.
5. Device Discovery- When the new node comes in the network than this very important to update their existence to all nodes in the networks.
6. Scalability-Manet scalability is a big issue because it adds more nodes without any issue than it creates complexity and more over vulnerabilities.
7. Limited Physical Security- The next task is the limited physical security because it shared the wireless medium to both the legitimate users and malicious nodes.
8. Topology maintains- The topology maintains quality is very poor because updating dynamic information link is a challenge.
9. Network configuration- Due to the dynamic nature of nodes configures the dynamic nodes and their connections are the challenge in mobile ad-hoc networks.
10. Channel Quality- There is varying of channels and that's the reason the resource are not proper utilized.
11. Vulnerabilities- In Manet there is a big issue is the security because the mobility any node can leave and join the networks any time so any malicious node can also come there and crash the networks.
12. Limited wireless bandwidth-The bandwidth utilization is not good because dynamic nature of nodes.
13. Changing Network topology-The changing network topology is also a big issue in mobile ad-hoc networks and that's why the resources not utilized and use.

1.7 Black Hole Attack-

Black whole attack is a type of MANET attack which present in a network in true node but the true definition of black hole attack is a malicious node. Now it is important to know why we called this node as a malicious node.

Procedure of black hole attack- Black hole is a type of Malicious node act as false node in the network and show that he has best path for send the packet or says that it having fresh route to the destination. Source node broadcasts RREQ packet and further forwarded to intermediate nodes to search the best and short path. If the malicious is present in the network and if that node receive RREQ packet, it's immediately sends false RREP packet with high sequence number. In this the false node claims the he has the best path for send the packet .Thus the false node drops the packet and modifies the packet in network.

STEP 1:- There are lots of nodes in network but between all these nodes there is one source node and one destination node. we define the work of black hole on the basis of AODV protocol ,that is the reactive protocol and works and maintain table when the source node want to send any packet to destination node but lack the information about particular path or route .

STEP 2:- In step 2, the source node send the RREP packet to all other nodes and their intermediates for shortest and secure path. After receiving the RREP packet to source ,all nodes try to find the best path for packet sending .But on that time duration the malicious node which shows itself true node, that node immediate reply to source node for best path. After receiving RREP packet to malicious node first, the other nodes reply packet will discarded by source node.

STEP 3:- Now the source node send it packet to that malicious node for destination node. But the malicious node does not send this packet to destination and discards or transfer that packet from one network to another network.

In figure-1.4 explains, the source node is node 1 and destination node is 4 and 3 is a malicious node who act as an honest node. When source node send the request packets to all nodes than malicious node first of all give the reply and take the packet from source and drop the packet instead send that packet to destination node.

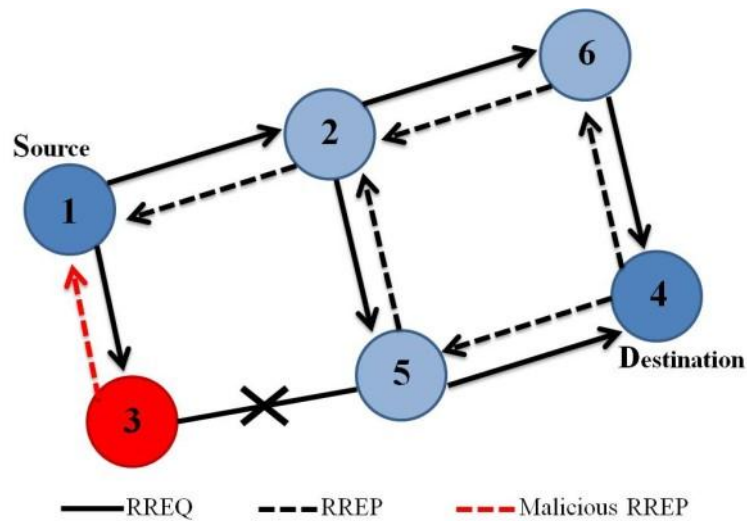


Figure 1.4 black hole attacks

The black hole attack is silent type of attack that is silently drop the packets in networks and very hard to find out this attack. In the network the black hole attack is also known as the packet drop attack and it is a type of denial of service attack. If we examining the traffic of the network and topology than the black hole them are invisible and detects by the packet loss or detected by the monitor of loss traffic. The simple form of black hole is the ip address with which a host is address that is actually not running or an address to which no host is assigned in the network.

The black hole specifically dropping the packet on routing level .The black hole attack is the two types –

- Single black hole attack
- Cooperative black hole attack

The single black hole attack as the name clear that only one node in the network is the malicious node that drop the packet and carry packet from source node but on the another side the cooperative black hole attack is the number of malicious node present in the network that make a group and know about each other and try to attack on the network by form of group so this is more difficult to find as compare to the single black hole attack.

CHAPTER 2

LITERATURE REVIEW

Detecting Black hole attack on AODV-based Mobile Ad hoc network by Dynamic learning method (Santoshi Kurosawa, Hidehisa Nemto, 2007) presented the method to detect the black hole attack by anomaly detection method with using the dynamic learning method which updated after a time interval.

A dynamic learning system against black hole attack in AODV based MANET (Payal. N. Raj and Prashant B. Swades,2009) says the method to detect the black hole method with comparing of intermediate sequence number and source sequence number and after check the threshold limit and check the black hole node and if node detect than reject and block that node with alarm message.

Preventing Black hole attack in mobile Ad-hoc network using anomaly detection (Y.F.Alem and Z.C.Xuan, 2010) explores technique to detect the single and multiple black hole attack through IDAD method. In this method first the all nodes activities are collected and save all these activities of nodes to IDAD mechanism. The IDAD performs the role of audit data which compare the every node activity with its store data base and if any node activity is out of data then the IDAD system isolate that node from the network.

Preventing AODV routing protocol from black hole attack (L.Himral, V.Vig, 2011) gives the idea to find the black hole node to safe the routing protocol by check the sequence number of source node or intermediate node those give the reply back or we can say that RREP packet send by those nodes. Now the malicious node give first of all reply with higher sequence number. Now this sequence number store in RR table and with this sequence number the source sequence will compare. If the number difference is more than that intermediate node will malicious node and this entry without delay will block.

An approach for detection and removal of black hole in MANETS (Herminder Singh, Shewta, 2011) describe the detection of black hole attack with the number of sent packets to node which will be equal to 0.After the malicious node detect we will be apply the feedback method to avoid the reacceptances of incoming packets at these black hole . The packets coming at the immediate previous nodes to black hole nodes are propagated back to the sender follow an alternative path to send the packets to destinations.

Trust Based Routing Mechanism in MANET Design and implementation (Taseem Eiza and Rashid Hafeez khoka, 2011) the method used for detect the malicious node by his two proposed algorithm. In this method they talk about the friendship AODV protocol because they make an assumption that all nodes which work in a network they work as a friends and all friends have friendship range and it is the identity of those nodes and these nodes are true nodes and the authors said that the true nodes range will always high and if any node has low sequence number than that is the malicious node. For the identification of true node they set a threshold limit like (1-100) and if any node has limit below 1 than that node will malicious node and they block that node. In their proposed solution they introduce the friendship AODV with two methods or two algorithms-

- Forward evaluate algorithm
- Reverse evaluate algorithm

Secure AODV against maliciously Packet dropping (Mohammad Taqi Soleimani, 2011) presented the purpose to stop the packet dropping and designed to detect the black hole attack through neighbor's information. When node receiving the RREP packet after that to check the validity of packet, the source node will broadcast the NREQ packets to all its two hops neighbors to check that is there any destination node or suspicious node? After that to check these neighbors' nodes further send this request to their neighbor's nodes after send the reply back to source node with RREP packet and with this packet contain the information of the neighbors list. In this if there any suspicious node found that alarm packet send to all nodes.

A Trust System in MANET with Secure Key Authentication Mechanism (S.Neelavathy Pari, Sabarish Jaypal and Sridharan Duraisamy, 2012) for the purpose of detect the malicious node .For this Multi Point Relay Based Recommendation Protocol(MPRRP) withsha-1 key encrypted authentication mechanism the author made a trust table that divide in three parts for check the validity of honest node. The Authentication Manager and Network Interface are directly connected with each other and the Network interface phase performs the task of key generation, key encryption and key decryption. The key is used for authentication of nodes in the network. The trust calculation part defines further defines two important phase Behavior plan and Recommendation plan. The authentication manager do original work for security and it uses secure hash algorithm for key encryption and decryption. When nodes enter into the network then they have encrypted key and after that that key is decrypted and enter into the network and made the

part of the network. This helps to prevent malicious nodes and impersonating node from entering into the network. Now the behavior manager check the behavior of the node and the recommendation manager give the task to that new node to send the packet to destination, if that particular node sent the packet to destination proper than it is genuine otherwise malicious node.

A New Black Hole Attack Prevention System In clustered Manet (Ira Nath and Dr. Rituparna Chakvati, 2012) Using the trust estimator between the cluster and the node. They check the trust value after t stamp of time .The friendship table is updated after t estimate of interval.

(H. Weerasinghe and H.Fu, 2012) presented the technique to detect the Black hole attack. He introduced the use of DRI (Data Routing Information) to keep the information of past mobile nodes of the network and these nodes crosschecking by source node.

PPN: Prime Product Number based Malicious Node Detection Scheme for MANET (Sapna Gambhir, Saurabh Sharma, 2012) shows the method to detect the malicious nodes with the help of prime product number and using the concept of AODV protocol and the cluster head. According to the researchers they can detect the malicious nodes with prime product number it means in the network every node has its prime identity and it cannot be modified. When any node send the route reply packets to the originator node or source node send the intermediate nodes send its own prime number and every node has the member of at least one cluster and the cluster head maintains and monitor the nodes . The identification of the nodes is their prime number that receives by the source node. The source node always selects that node which sequence number will higher and minimum hops counts. After the selection divide that prime number with source node. If that number divisible than it prove that node is honest node otherwise malicious node.

Detection of black hole attack in mobile ADHOC Networks (Shashi Gurung, Aditya Kumar and Dr.Krishan Kumar Saluja, 2013) reveals the method of detection of black hole attack using AODV protocol. Through to this technique the detection of black hole attack and easy to finding the secure path from source to destination. In this proposed methodology propose a solution to identify the black hole node, remove that node from routing table and finally added to the blacklist table. In this approach when sender broadcast the RREQ packet, it will wait for reply and following are two things that are required in each node.

- Reply Table
- Blacklist Table

In reply table the incoming replies are stored and the route is selected which has the highest destination sequence number. Once the route is selected the sender starts dummy packets to its intermediate nodes. If the intermediate node is normal node, it will forward the packet to destination or its next hop. After some time the source node send the confirmation acknowledgement request to destination via alternative optimal route for confirming whether it has received dummy packets or not. Now if the destination has received the dummy packets it will send confirmation acknowledgement reply in form 0 and 1.0 means destination did not received the dummy packets and 1 means the destination has received the dummy packets and source ignore the confirmation acknowledgement reply from that node to which dummy packet was sent. Based on the reply, the sender will come to know about reliability of that particular node whether it was malicious or not. Now the black list table, each node will check its table to identify whether this packet coming from malicious node. If this is prove than immediately discard the packet and record that node in blacklist table.

Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-Hoc Network (Romina Sharma and Rajesh Shrivastava, 2013) presented for detection of black hole attack with this method there is reduction in packet delivery ratio and throughput. In this method the author try to modify the working of AODV protocol by adding next hop information in the RREP message and two other control messages that is-

- Further route request
- Further route reply

Receiving the route reply message from nodes with next hop information than the source node again broadcast further route request to all next hop nodes to the received RREPs. The next hop nodes reply back with further RREP message to source node. A Black hole node never its next hop so it will not receive FRREQ and never send FRREP message to source node. Now the source node sends the data packets to the destination with shortest path.

(P.Raj and P.swades, April 2013) the new technique to detect the black hole attack is checking RREP messages from intermediate nodes for possible intrusion activities. The

technique is successful based on the cooperation of all nodes with each other. It means if any mobile nodes discover any attack by intruder, node notifies all other nodes by broadcasting alarm messages.

Modified DSR Protocol for Detection and Removal of Black Hole Attack in MANET (Mohanpriya and Llano Krishnamurthy, 2013) describe the detection of the black hole attack in Manet. In this proposed method used the Modify DSR protocol and the source node broad cast the route request packets to all nodes The requested destination or any intermediate node having the path can send back the reply to source node. The malicious node which performs itself as the honest node send the reply and try to receive the packet and when packet received drop the packet instead send the packet to its destination. For avoid this problem the author proposed the technique and check the packet drop ratio by packets received at the destination node and packets send by sender node.

Intrusion detection system based MANET security against selective black hole attack (K. Mahalaxmi & Dr. D. Sharmila, 2013) presented the method to detect the black hole attack by ids technique and this method will apply only selective black hole nodes .This method only apply when ids stand on sniff mode and moreover this not only detect the black hole nodes but also prevent the network with such type of attack. For detect the black hole node they introduced the method that is ABM, it means anti-black hole mechanism. With help of this the easily check the black hole node .Because they are set the value of threshold and whenever the threshold exceed, on that time the ids alarm a message and this message got by anti-black hole mechanism (ABM). So this technique helpful for secure transmission of packets and safe routing.

Dynamic Training Intrusion detection schemes for black hole attack in Manets (A.Naveen and K.Rama Linga Reddy, 2013) tell us the method to detect the black hole attack by ids techniques and apply here threshold limit. According to this technique the author presented the two concepts threshold limit and data limit. If the threshold limit is greater than the data limit than this would consider as the normal data but if it is not greater than data limit than it will consider as the abnormal data and detect the black hole attack.

Techniques for detection of cooperative black hole attack in MANET (Ms. Gayatri Wahane and Ms. Savita Lonare, 2013) use the technique to detection of black hole attack with the modification of source node, the intermediate node provide the information of next hop and save the entry of NHN.After receive the routing information the source node

checks the intermediate node whether it is trusted or not. The source node sends the packet through intermediate route and checks its trust value. If it send the data to its destination than it is reliable and trusted otherwise malicious node.

Efficient Malicious Detection for AODV in mobile ad-hoc networks (M.Amresh and G.Usha, 2013) reveals the ET-AODV techniques and it tells the main motive to increase the packet delivery ratio and reduce the packet drop rate in networks for secure communication. Here the main motive is the calculation of trusted path and it calculates to monitor the traffic of neighbors nodes using watch dog mechanism and trust based routing is done by parameters mechanisms. The node total energy and efficient energy is calculates to another node from initial and current node energy. To maintain the trust based method to keep the security of the confidentiality and authentication. In this mechanism there is four parts are divide and these are as-

- Route trust based estimation
- Trust value routing
- Secure transaction
- Malicious Detection

In this paper the author describes the four main parts of this model through to these to detect the black hole node. For the black hole detection approaches use the two concepts that are as follows-

- Computably limited
- Computationally Intensive

The Computationally intensive techniques are the mix-up of different methods like Fuzzy algorithms, Genetic algorithms. On the other hand we can see that the Computationally limited has simple parameters, manipulation of the networks and the message parameters like neighbors and trustiness between of the nodes. Complexity is another factor of the black hole attack. To neighbor and nodes trustiness are matter on the role their reputation ,it means if we want to calculates the trustiness of the nodes than we have to see the nodes that send the packet to its destination or not and give the acknowledgment of the packet to its source or not.

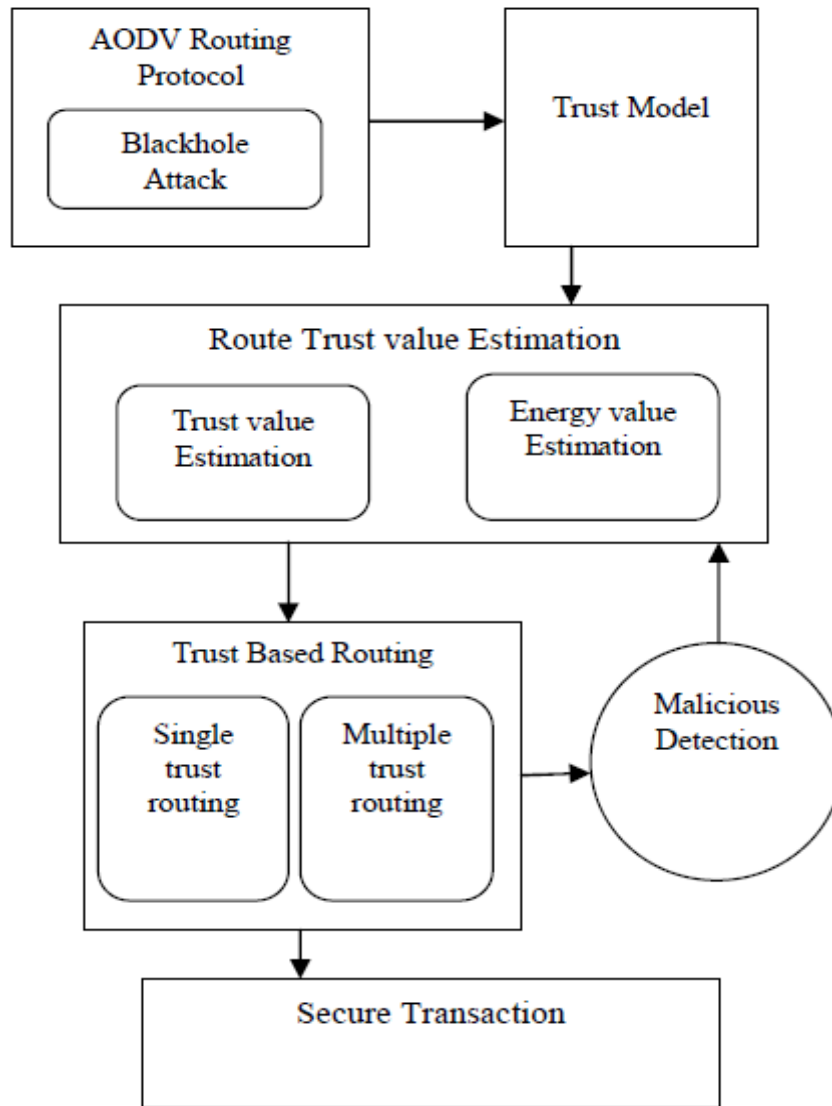


Figure 2.1 Trust based model and ET-aodv

The value of the trust model is based on the neighbor node. For the scalability the proposed model is based on the local information to calculate the trust value.

A novel taxonomy of black hole attack detection in mobile ad-hoc networks (Ahemed Sharif and Amin Shoukry, 2013) classifies the detection approaches accordingly the name of computation. The contextual fuzzy techniques rely on genetic algorithm, fuzzy logic and the clustering algorithms. Two types of approaches are used-

- Using neighbor and trustiness between nodes
- Using feed –back
- Using acknowledgement based
- Using Reputation

The acknowledgment and the reputation plays very great role because the nodes reputation based on the nodes reputation.

Hierarchical energy efficient intrusion detection systems for black hole attacks in WSNs (Samir Athmani and Azeddine Bilami, 2013) describes the detection of black hole attack in wireless sensor networks with the intrusion detection systems. The concept is based on the detection of black hole node with the communication of sensor node and base station. At the end of the transmission the sensor node sends the control packet's to the base station. The control packets have the information contains the number of packets and node identifier to the cluster head. The cluster head than allows to the base station for detect the black hole node in the networks. When the base station identifier the black hole node then beep the alarm in sensor networks and broadcast the message to all the nodes. When the black hole node detects then the base station contains all in the table at one place and try to detect the black hole and if any node detect genuine than make that cluster head for sensor network for control the packets. After then elect the senior cluster head between the groups of the cluster heads.

Secure route discovery for preventing black hole attacks on AODV based Manets (Seryvuth Tan and Keecheon Kim, 2013) tell the Manet AODV and it is called as the secure-AODV. The standard AODV protocol and the minimum and maximum values for the sequence number are based on 32-bit based arithmetic. The minimum sequence number represents the minimum sequence number and the maximum number represents the maximum sequence numbers. Here three threshold are classify-

- Small number of threshold
- Medium environment threshold
- Large environment threshold

A Reaction Based Approach to Detect Black Hole Attack Using Modified AODV Protocol(Geeta Pattun and V.Sireesha,2014) says in MANETS to detects the Black Hole Attack through this method can be implemented by including control packets to the existing AODV protocol. To detect the black hole attack the proposed method involves two control packets.

The control packets are-

- Reaction-to-discovery-packet
- Reaction-to-send-data-packet

After receiving the route reply packet to check the path for send the packet to destination. After this the next step check the originality of intermediates nodes send the reaction-to-discovery-packet .If the reaction-to-discovery-packet is much lesser than reaction-to-send-packet than it is very clear that the node is not honest node and it is malicious and the traffic is immediately divert to other route.

An efficient algorithm for detection of black hole attack in AODV based MANET (Neelam Khemariya, Ajay Khunteta, 2014) presents the detection of black hole attack with an algorithm which not only detects the single malicious node but also detect the group of black hole nodes. The best thing of this protocol is that it not only detects the black hole node when the node is not idle but also when the node is idles.

A secured data transmission method using enhance proactive secret sharing scheme to prevent black hole attacks in Manet (K. Selvavinayaki , Dr. E. Karthikeyan , 2014) presents the method to detect and prevent the black hole attack in Manet using proactive secret sharing scheme and according to this method used new enhance proactive secret sharing scheme (NPSSS) . It implemented over AOMDV protocol and this protocol is used for loop free path for route discovery. According to NEPSSS scheme the RREP and RREP packets are modified to hold the additional information. Like when source S wants to communicates with destination D and node A and node B are the intermediate nodes in the network between the S and D.

Here source S broadcasts the intermediate node that node give the route reply in the answer of route request and uses the private key to decrypt the message and get the flow id. After this with the help of flow id to update the table to designated the destination D. S receives the private key to decrypt the message and uses the public key of destination node to identify the destination. Than the source node sends the message with the flow id. The cluster head maintains the trust threshold value based on trust active and node information to detect the black hole node. If any node value have the below trust hold value than it will identify as the black hole node.

Detection and prevention of cooperative Black Hole attack (P.S.Hiremath and Anuradha T., 2014) gives the method to detect the cooperative black hole attack. In this algorithm there is the network where N number of the nodes and x is the number of the black hole nodes in the network and T is the threshold value or we can say the limit of RRep sequence number of responding nodes. On the starting point the black list is 0 and the S is the source node and randomly assigns the x nodes as the black hole nodes among n nodes.

The source node S starts to broadcast the route request packets to all corresponding node for the path. If the neighboring nodes have the path than they will send the route reply otherwise the neighboring nodes forward that request to their next till the destination is reached? The source nodes S receive the RREP packets from neighboring nodes on multiple paths. If the value of RREP sequence number $> T$, than that time node suspects as a black hole node and it added to the black list and the routing table make updated and the alarm will sound to all neighboring nodes to tell about that black hole node.

A weighted clustering algorithm for improving MANET security (Shirsty Chandel and Prof. Ashish Tiwari 2014) use technique device specific approach of for optimizing the detection and prevention of black hole attack and here follow three basic things like mobile nodes, cluster heads, monitoring server. The all these three performs different tasks where the mobile nodes performs the operations of send and receive the packets but it's also receive the service of its nearest cluster heads. The cluster heads are the service providers and these provide their participation in intra-cluster communication. The primary objective is to communicate with trusted nodes and new mobile node wants enter than cluster head the responsibility to monitors all these. The server calculates the trust value functions.

Optimized positioning of multiple base stations for black hole attacks (Anurag Singh Tomar and Gaurav Kumar Tak 2014) describe the approach to specify the prevention of black hole attack by deploying the multiple base stations. For this reason they use the concept of genetic algorithm and with the help of this easy find out the optimized position. For the prevention of the black hole attack they use the genetic algorithm in three phases. In the first phase they deploy the nodes in wireless sensor networks and create the black hole region. In the second part they set the BS with the genetic algorithm

and repositioned that and the last part they start routing of fifty nodes and start calculating results.

Enhanced multiple approaches for prevention and elimination of black hole attack in mobile ad-hoc networks considering the enhancement of network throughput (Maninder pal Singh, Man Mohan Sharma 2014) the technique to prevent the black hole attack with consider the network throughput and used the opnet simulator for the result. For this randomly generate a number in between 0 to maximum number of nodes and make the nodes as black hole attack is done by transmitter and receiver. Then generate the routes from selecting transmitted nodes to any destination node with specified average route length. After this it will send the packet to selected destination and stat timer and hops counts and delay. Now if the hop counts of particular route decrease compare than average hop count than we say that one is the attacker of that route. Now check the that route and confirm the attacker nodes the process again start and start check about that route and nodes by neighboring nodes and that neighboring nodes tells the history of that all nodes of particular route.

Prevention of black hole attack on AODV in MANET using hash function (Anand .A. Aware and Kiran Bhandari 2014) show the method to detect the black hole attack and prevent it with the help of hash function. The author tells us that how we can detect the black hole attack. According to this method when the initial point of communication the source node start communication with the destination node than for this reason send the route request packets to all nodes. Now the gray hole or black hole attacker which acts as the best route itself, they will send the route reply packets to source node and try to convenience the source node their self-best and shortest route for packet delivery. But now the source node after received the packet from malicious node which acts as a honest node till wait for second route reply packet. When the source nodes received the packet from second node than discards the first route reply packet from first node and send the packet through second route. Here the author present the another method which is hash function that only done by source and receiving node because there might be case that there will be several malicious nodes and the second reply send from any malicious node instead the genuine node. So the reason behind to generate the hash function is the data integrity. The hash value message on the source sha-1 and the destination side it will sha-2 and this hash function will apply on the second route reply packet and node. If the hash

value at the source node and destination side will same without error than the second route will optimal otherwise it suspect as black hole node.

Removal of selective black hole attack in Manet by aodv protocol (T.Manikandan, N.Kamaraj and C.Senthilkumar, 2014) presented IDS based communication and transmission range of nodes A and B.It means on the basis of physical characteristics the all nodes are within transmission range of each other. Also the solution assumes that all the nodes are authenticated and can participate in communication that all nodes are authorized node. Their use the multiple routes from source to destination. The source node has to cache the other routes to mitigate the overhead incurred during the process of the new routes and with the help of ids removes the promiscuous nodes.

Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in Manet (Suparna Bishwas, Tanmoy Nag and Sarmistha Neogy, 2014) tells us the mechanism to detect the black hole attack and how to prevent the network from its bad effect. It proposed the trust model and evaluates the strategy to build reliable and secure routing in the network. The main motive of the paper is to identify the black hole attack and prevent from the packet to intercept and secure routing transmission. The solution based on the multiple routes to communication for the source and the destination node. In the prevention of the black hole attack use the most suitable route for transmission of the packets. According to the technique each node in the network has assigns three parameters. These three parameters are-

- Rank
- Remaining battery power
- Stability Factor

The rank parameters are equals value as the fidelity level. Those nodes which are the part of the networks and participate here are the rank. The rank is based on the reliability it means 0 is considered as the malicious node or the black hole node. This node will than isolate the network when the alarm beeps and broadcast message send to all the nodes. If the source node send the request message to all node than set the timer and if the destination node also receive the request message than have to send the acknowledgement and if the acknowledgement not send than the timer expires and if send the timer

incremented. The batter constraint takes as the parameters of the node that check on the emergency time by the source node. Stability shows the higher and genuine the node.

Techniques of detection of cooperative black hole attack using true-link in mobile ad-hoc networks (Gayatri Wahane, Ashok .M. Kanthe and Dina Simunic, 2014) show the techniques to detection of cooperative black hole attack with the modification of the AODV protocol by the DRI data routing Information with trust link concept. In the concept of DRI the two malicious nodes called B1 and B2 are cooperative black hole attack and try to attract the intermediate nodes for shortest path for destination and drop the packets. For the identification of the nodes two bits of additional information are attached with source node .The first bit “from” stands the routing data packets from and the second bit “through” who send the data packets. In the DRI table 1 stands for true and 0 means false node. Cross checking true link is based on the timer based mechanisms. The black hole attack comes from mostly the network layers. This information works with the DRI and cross checking table for detect the malicious node. After this use the concept of the RTS and CTS which identify the malicious, if CTS not equals to nil than success and packet will forward.

Behavioral and node performance based gray whole attack detection and amputation in AODV protocol (Shristi Jain and Sandeep K Raghuwanshi, 2014) tells the method to detect the gray whole attack. Initially the source and destination node communicate to each other and a ids node set which act as a watch dog of whole network and when that ids watch to drop the packets than send the unicast message to sender for change the new route where the gray hole node not present and that after check the performance of every node. If the performance of the node is zero than the incoming packet not send for communicating further.

A review-Secure route discovery for preventing black hole attack on AODV based Manets (Hansraj Bhakte and Rahul Kulkarni, 2014) purpose the solution to detect the black hole attack in Manets. The solution is that the all intermediate nodes disable to given reply and only the destination side node would give reply so in this manner avoid the black hole to enter the networks with the help of SAODV protocol and the other solutions to use multiple paths to reduce the black hole attack .In this method when the intermediate node give reply than another path checks it either is true path or not. If that

intermediate node exist than that is trusted node and we include in the networks but if not than isolate from the network and alarm a message to all nodes about black hole.

A mechanism for discovery and prevention of cooperative black hole attack in mobile ad-hoc Networks using AODV protocol (Harsh partap Singh and Rashmi Singh, 2014) use the concept of BS means clock synchronization for removal of cooperative black hole attack .The first step is the internal clock synchronized with the external clock time sequence. The internal and the external clock when compared to the threshold limit than find out the great high mobile nodes.The malicious node act as the normal node. In this we just change the node mobility and set the parameter of pause time. The author takes the two cases .The first case is the normal and second is the abnormal case. In the abnormal case the clock synchronization totally fails and detects the black hole node.

Performance of ids in an Adhoc networks under black whole and gray whole attacks (Mozmin Ahemed and Mohammad Anwar Husain, 2014) gives the approach of detects the black hole attack and gray whole attack .The detection of black hole attacks the author reveals the information that black hole node is a silent type of attack that silently drop the packets in networks and the author detect it with AODV protocol with CBR traffic. The node ‘S’ keeps the counts of number of votes it receives from its neighboring nodes and it accepts only one vote to each neighbor. The time set for receiving the votes from the neighboring nodes and the votes only received within a fixed time. The neighboring nodes that receive the request of voting they attempt to join the voting process. If a node ‘2’ is a black hole node than this message forward to all the nodes.

A new intrusion detection Framework for Vehicular networks (Hichem Sedjelmaci and Sidi Mohammad Senouci, 2014) revels the information to calculate the trust level of vehicular. The author used the two terms that use in the trust level of vehicles and that are as –

- Local intrusion Detection Module running at cluster member level
- Global intrusion Detection Module running at cluster level

With this two approaches try to detect the malicious vehicles for accuracy of networks. Before the cluster formation the all nodes have work on the local intrusion detection level and when the node calculate or below the threshold limit than it switched to the global intrusion detection module. Local intrusion detection module activated at each cluster

member because the at each detection period here detect the neighboring nodes. With the detection of each vehicles storing their id and perform the different tasks like PDR, PSR, RSSI AND MDR. The local level of cluster has further two types-

- Rule base intrusion techniques
- Learning based Intrusion techniques

Global intrusion detection of cluster is an equipped with these two levels-

- Trust based techniques
- Malicious vehicle's evasion techniques

Black hole Tolerant protocol for Zigbee wireless networks (Hemant Sharma, Koushik Banerjee and Brijish Kumar Chursia, 2014) represents the techniques for detects the black hole attack with Zigbee wireless network with modification of AODV protocol. The Zigbee wireless techniques represents in three ways-

- Zigbee coordinator-

It is considered as the root of the networks or sometimes acts as the bridge of the networks. The Zigbee coordinator is most important for deployment the protocol for check the trust level.

- Zigbee router-

The Zigbee router acts an intermediate between the Zigbee end devices and the Zigbee coordinator.

- Zigbee end devices-

The Zigbee end devices have limited functionality and it creates a communication between the Zigbee coordinator and the Zigbee router.

Intrusion Detection using MLP for Manets (K.Pavani and Dr. A. Daodaran, 2014) gives us the idea to detect the normal and malicious behavior of the system and try to detect the black hole and gray whole attacks. So the author presents the idea to detect these attacks with ids and MLP in neural networks. Use the protocol ad hoc demand vector and creates algorithms, first simulate the black and gray hole and collect the data from the audit records than start the feature selection and MLP modeling and then performance analysis

Detection of black hole in wireless sensor based on data mining (Mandeep Singh and Gursheen Kaur, 2014) explores the information or technique to detect the black hole attack in wireless sensor networks. In this proposed algorithm use the two algorithms in detection of the black hole attack .The algorithms that use in this paper use by the author is-

- Clustering Algorithms
- K-Means Algorithms

This paper is based on two phases for the efficient performance of the network and detection of the black hole attack. The two stages are-

- The wireless sensor network created on ns2 simulator and it's analyze is done with the awk files and data log is extracted with the trace file.
- Than extracted to dataset in data mining process to further analyze the pattern and behavior of the nodes.

First deploy the nodes in network and implement black hole attack and then generate the trace files of both the networks. After this step obtain clusters in K-means algorithms. If PS means profile score greater than threshold than the data is non-malicious but if DS means Deviation score is greater than threshold than the data is malicious and generate the new alert.

Preventing black hole attack in AODV using Timer-Based Detection Mechanism (Nidhi Chodhary and Dr. Lokesh Tharani, 2015) tells us the preventing of black hole attack with the modification of AODV protocol. The AODV protocol initially works as the normal protocol and start to send route request message to all nodes and in the initial point of communication all nodes trust value maximum. The most important is the threshold limit it means that node whose trust value $< \text{min_value}$, so this condition they will not communicate further. When communication starts than on that time the source node assigns a unique sequence number to it every packet. When the node N start communication than it sets a timer of t seconds and listens wireless links .When the timer expires than the node N checks the packets weather it receives the data packets from its neighbors or not. If the node N does not hear the packet than it will reduce its trust value from its next hops neighbors.

CHAPTER 3

PRESENT WORK

Wireless network is a very big area and today the whole world using the wireless network in their daily life. The wireless network has very big role for communication. Today everyone want comfort and that's use the wireless network because today with the help of the wireless network the person can easy access the world information and wireless LAN is very big example of the wireless network. For example if we are using the Wi-Fi than it is not important you do your all work on one place but you can seat anywhere in the Wi-Fi range and do your work easily. The MANET is big enhancing version of the wireless network. MANET means MOBILE AD-HOC NETWORK. MANET is a collection of dynamic nodes and it does not have the access point like wired network. In MANET the node some time act as a router or some time host. In MANET the nodes can free to leave or join the network any time. Here the features of multi –hop routing, when the source and destination out of range and does not able to send the message to each other. The MANET has best features are use a lesser amount of power; less memory .In the MANET all nodes are cooperative. But with all these feature the MANET has some drawback or we can say some weakness which makes it more vulnerable compare than wired network. Due to the lack of centralized environment and without coordinator any node can leave the network and does not required permission for enter the network. The second problem is there is very much possibility of packet loss in a high range. With this reason the transmission range goes interrupted. Here limited bandwidth use and with this reason the overhead problem increase. Multiple types of attacks are attack on the network and try to access the information like black hole, wormhole, gray hole, Sybil, flooding; denial of attack and etc. The black hole attack is also the attack that drops the packet which sends by the sender. With my proposed methodology with use different parameters detect the Black hole attack and safe the network with that attack. Due to this sometime the network goes crash.

3.1 Problem Formulation-

A black hole is very senior type of attack that is very harmful for the network and sometimes it totally degrade the performance of the network. In black hole attack, when the source want to send the data packets to the destination node if the destination node is not directly available and no direct path is available than the source send the route request packet to all nodes for the shot and best path for send the data packet to the destination. Now the black hole which already include in that network act as self the honest node and receive the route request packet and first of all send the route reply packet to source node and tell that node about that path which is shortest and path for send the data packet. Now the source node believe it is the best path and after incoming route reply packets will discarded from source node and send that data packet through the malicious node which act as self is honest node. Now that malicious node after take the packet from source node drops the packets in way and not sends the packet to destination node

Sometimes the black hole nodes work as a group, this type of the attack is called as the co-operative black hole attack where multiple malicious nodes work in a group. This group of malicious nodes completely disruption of the routing and packet forwarding function of the network and crash the network

In study done by M. Mohanpriya, they have proposed a modified DSR routing protocol which defines a threshold value and compare the ratio of number of packets received at the destination to the number of packets sent by the destination.

If the number of packets received at the destination are less than 80 percent of the packets sent by the source it initiates the process to detect the malicious node. However this approach detects black hole node only after the attack has occurred. This approach may lead to loss of some useful information to the destination and loss the data packets. With this approach the data packet is very much loss and end to end delay is increase. The routing overhead is very much due to MDSR because in MDSR for transmission of QREQ, QREP, MNREQ and ALARM packets.

3.2 Objectives of the Study

We aim at reducing the loss of information which is useful in the network at the same time detecting the malicious node present in the network. Whenever the source node forwards the route request messages in the network to form a route to the destination node, the malicious node upon receiving the request message generates a route reply to the source claiming the shortest path to the destination. Whereas the legitimate node present in the network forwards the route request to its neighbour nodes. We aim at using the fact to detect the black hole node, that black hole never forwards the route request message in the network. We calculate the ratio of number of request packets forwarded by a particular node to the number of request packets received by it. For the black hole this ratio tends to be zero since it doesn't forwards the request packets. This will easily detect the black hole nodes in the network. As two step verification, after source node detects the malicious node by looking at the ratio value, the source node must look at the sequence number of the packets received by it from various paths. The sequence number generated by the black hole is always higher as compared to other nodes in the network. This will further lead to verification of the results obtained using the ratio method. These are the objectives of the proposed method which we will try to achieve-

- In recent years, the end to end delay was very high between sources to destination due to packet dropping in black hole attack. So, due to this network performance was degraded but now the end to end delay will be less with the proposed algorithm.
- The Proposed algorithm will detect the black hole attack very efficiently in terms of packet drop rate and bandwidth.

3.3 Algorithm of the Proposed Work

Now we will discuss the new methodology for detection of black hole attack. In this Figure 1.6 describes how the methodology works in step by step

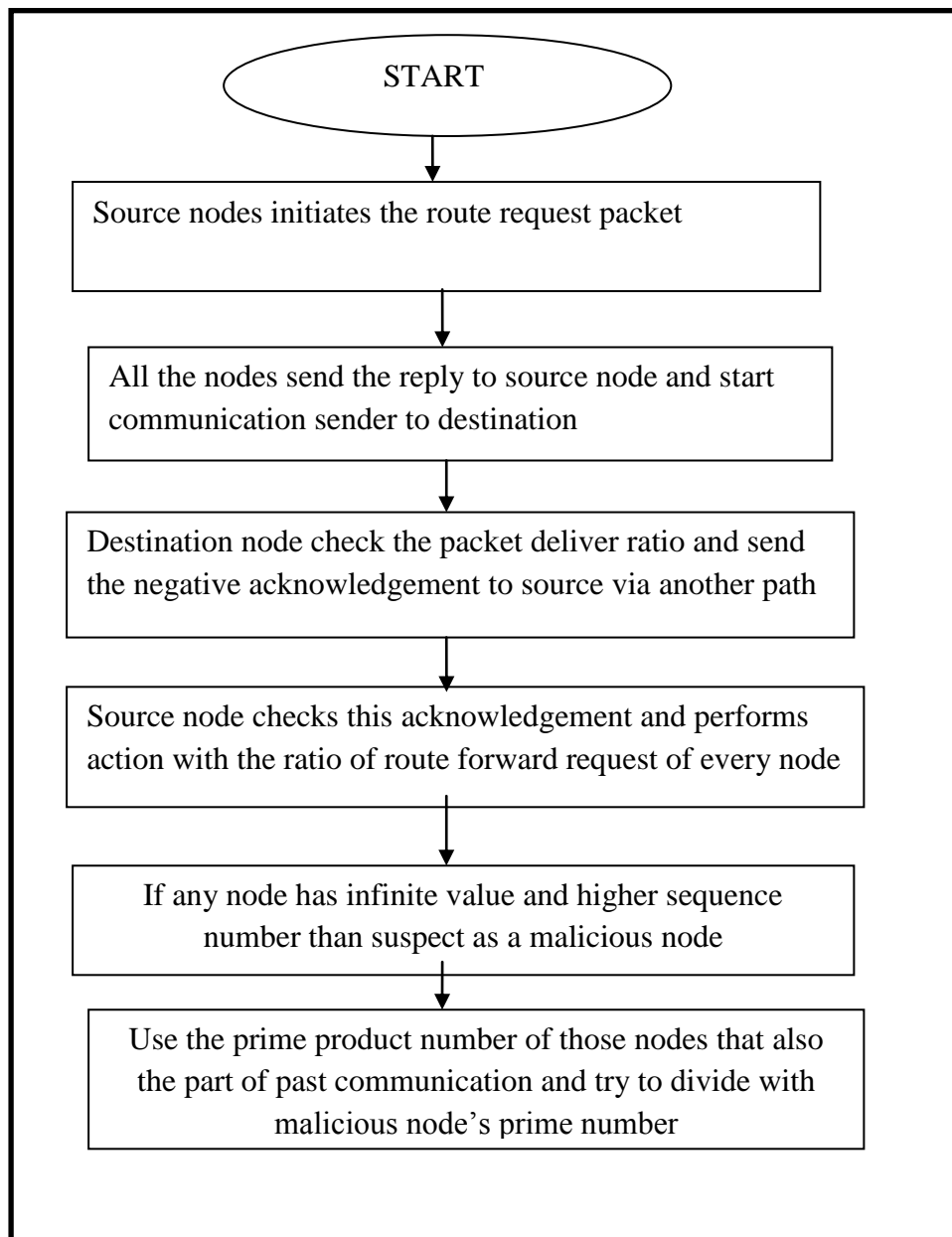


Figure 3.1 Flow chart of proposed methodology

In this above flow Chart all steps include of detection of the Black hole attack ,For the Detection of Black hole Attack using improved Ad hoc on demand routing Protocol and this protocol has main two phase –

- Route discovery Phase
- Route maintains Phase

The algorithm steps of the proposed work we will discuss now-

a) Packet delivery ratio check on destination node

1. First step first of all we will deploy the nodes in the network and make a network.
2. The source will start the communication and send the route request packets to all neighboring nodes.
3. The data packets send to the nodes and start the communication.
4. When destination node release that the packets comes from source node very less after communication.
5. Due to this reason check the threshold limit and according to this the threshold limit is below 10-20 packets.
6. The destination node check or we can say calculate the packet delivery ratio on the basis of this suspense and try to reach the final result.
7. This packet delivery ratio checks if the total packets counts less than 20 than the destination node check the packet delivery ratio.
8. We have formula to check the packet delivery ratio that destination node uses.

$\text{Packet delivery ratio} = \frac{\text{the ratio of the number of packets received at the destination}}{\text{The number of packets sends by the source}}$

Figure 3.2 packet delivery ratios on destination node

9. The correct counts of the packets the destination node uses the concept of the probability to check the malicious nodes and use the packet delivery ratio for check the correct packets count.
10. One thing is very clear that the destination node before use the technique of packet delivery ratio it is very important to know why that destination node uses two conditions of probability.

11. The reason behind this is the destination node analyze two time slot for detect the malicious node that t1 and t2.
12. On the time of t1 first destination node check how many packets are successfully received out of total packets.
13. Let's 2 out of 10 data packets are receive at time t1.The first condition of probability apply here.
14. The destination nodes have some doubts on that path and have suspected about the malicious node.
15. This doubt clearance the destination node waits for t2 time slot.
16. The time t2 again start to check the successful packets and behavior of malicious node. The time t2 the successful packets received 4 out of 10 packets but other packets are not receive to destination node.
17. These analyses confirm the destination node about the malicious node and apply the second conditions of probability here.
18. The task for packet deliver ratio performs on the basis of these probabilities.
19. We get two conditions of probabilities to check the malicious node :-
 - a) 20% chances are the node that is not a black hole node but 80% chances that is black hole node. Now we check the probability of 80% that is 80/100 means 0.8 chances that is black hole node.
 - b) 25% chances are the node that is not a black hole but 75% chances we are sure that this is black hole node. Now we check the probability of 75% that is 75/100 means 0.75 chances that is not a black hole node.
 - c) We combine both assumptions for check the total probability of malicious node for future predication and try to eliminate the black hole attack-

$$P=P1 \times P2 = (80 \times 75) = (0.8 \times 0.75) = 0.6$$

Figure 3.3 probability checks of two assumptions on destination node

20. We can see the result of total probability after this calculation.
21. There is 60% chances that node is the black hole and 40% chances that is not black hole.
22. We have suspected that the node is malicious. For confirm this we check the forwarding ratio of route request packets by source node.

23. Due to this reason the destination node send the acknowledgement to source node contains the information of packet delivery ratio by alternative path.
24. The source node tries to check this malicious node after receiving the acknowledgement from destination node.
25. The source node checks that route which is suspected by destination node.
26. The destination node sends the negative acknowledgement or dummy packet to source node via alternative path. The next task performs by the source node.

b) Detection Step by source node

1. The malicious node reply backs itself but in case of AODV protocol the other nodes reply come from the destination node.
2. This would mean that other nodes have forward the request packets, so for them forwarding ratio will not be infinite.
3. The ratio of checks the forward route request is the number of request packet forward by the neighbor node to the request packets received by the node by the source node.
4. The table for ratio of request messages for each node will be looked up. The node for which the ratio is infinite will be detected as malicious node.

Received Route Request Message

Forward Route Request Message

Figure 3.4 forward route requests Ratio check

5. The source node will contains this information of malicious node in the network keep secret until source node not confirms about the malicious node. This table and try to explore that malicious node
6. The time the source node not 100% sure about that malicious node the source node checks the packet sequence number for verification of malicious node again.
7. We assume that the malicious node's sequence always is high because malicious node wants show that path best and guarantee to deliver the packet.
8. The malicious node in the network or any genuine node performs this action due to path break or any other reason the source node confirms it with prime number technique.
9. The final confirmation of genuine node and malicious node the source node use the technique of the concept of prime number.

c) Confirms the Difference of genuine node and malicious node with prime number by source node-

1. The difference of genuine node and malicious node use the concept of prime number and this network every node has prime number.
2. The malicious node act as the genuine node and due to this reason that malicious node also use a prime number.
3. To avoid this problem and make the difference of honest and malicious node the source node broadcast fake packet and this packet contains the message that all nodes send their prime numbers for new network session.
4. The malicious node also the part of this network so that node receives this message and thinks this message not only for me but for all nodes which is the part of this network.
5. The source number use the primary product numbers of any two nodes that are also give participation in past communication.
6. The source node sends the dummy packet to all nodes which has the information is that the source node wants to create new session so send their prime number.
7. When the malicious node receives this packet and immediately attaches its prime number with that prime product number and send dummy packets to the source.
8. The prime number of that malicious node checks by the source node and try to divide that number to prime product number.
9. The number is not divisible to prime product number than this is confirm that node malicious node and the source node blocks that black hole node and update this to all nodes.

CHAPTER 4

RESULTS AND DISCUSSIONS

The black hole attack is very senior type of attack and it effects the communication between the source to destination and increase the end to end delay time. The black hole acts as the honest node in the network and when the source wants to send any data packet to destination, The source node send the route request packet to all nodes, on that time the black hole which acts as the honest node in the network also receives that route request packet and send the first reply to source node. When source node receive the route reply packet from black hole node .The source node hand over the packet to that black hole node and the black hole start to drop the packet instead send the packet to destination node. After this proposed methodology first of the packet loss will be reduced and malicious node will also be detected in advance, before starting of communication. Proposed methodology will reduce the end to end delay or can say negligible. After this methodology the performance of throughput will increase and bandwidth will be used in proper manner. The network performance will increase in positive side.

For the implementation of my proposed work, I use the tool of NS2 .NS2 is the open source simulator and that use for the virtual simulation in network. It provides substantial support for tcp, routing protocols and multicast routing. The main motive behind the NS2 tool for simulation and moreover with the help of with this tool we can create any complex scenario and testing.

When we talk about result in NS2 than the results can be obtained quickly and more ideas can be tested in smaller interface. The best thing is the easy to detect the bugs and remove this.

Now if we talk about NS2 protocols than we can run any protocol like tcp, udp, http and routing protocols and the mac protocols without this we can set the traffic model according to our requirement like cbr, vbr web and etc. In NS2 the unique feature is the NS2 we have the facility to check the nam and trace files for outputs. The ns2 creates the list of events that simulate one after the other for access the result.

The NS2 have the package of two types of end that use in simulation time. The first is the front end and the other is the back end. For the front end we have to use the tcl file, which

helps us to make animation or scenario. For the tcl file use the extension of the c++ files and easy to change and fast. The second part is the back end where we use the c++ or we can say the .cc files. In .cc files we have to deploy the protocol and make new protocols according to our research work. For the NS2 we use the structure of ns2 or we can say the flow control or steps. There are 6 steps in ns2 structure.

The 6 steps are- event scheduler turns on tracing files, create network topology and make connections and generate traffic and etc. So we can say that it is helpful for different types of scenarios and protocols suits.

My proposed work's results are as follows-

A) Comparison of end to end delay graph-

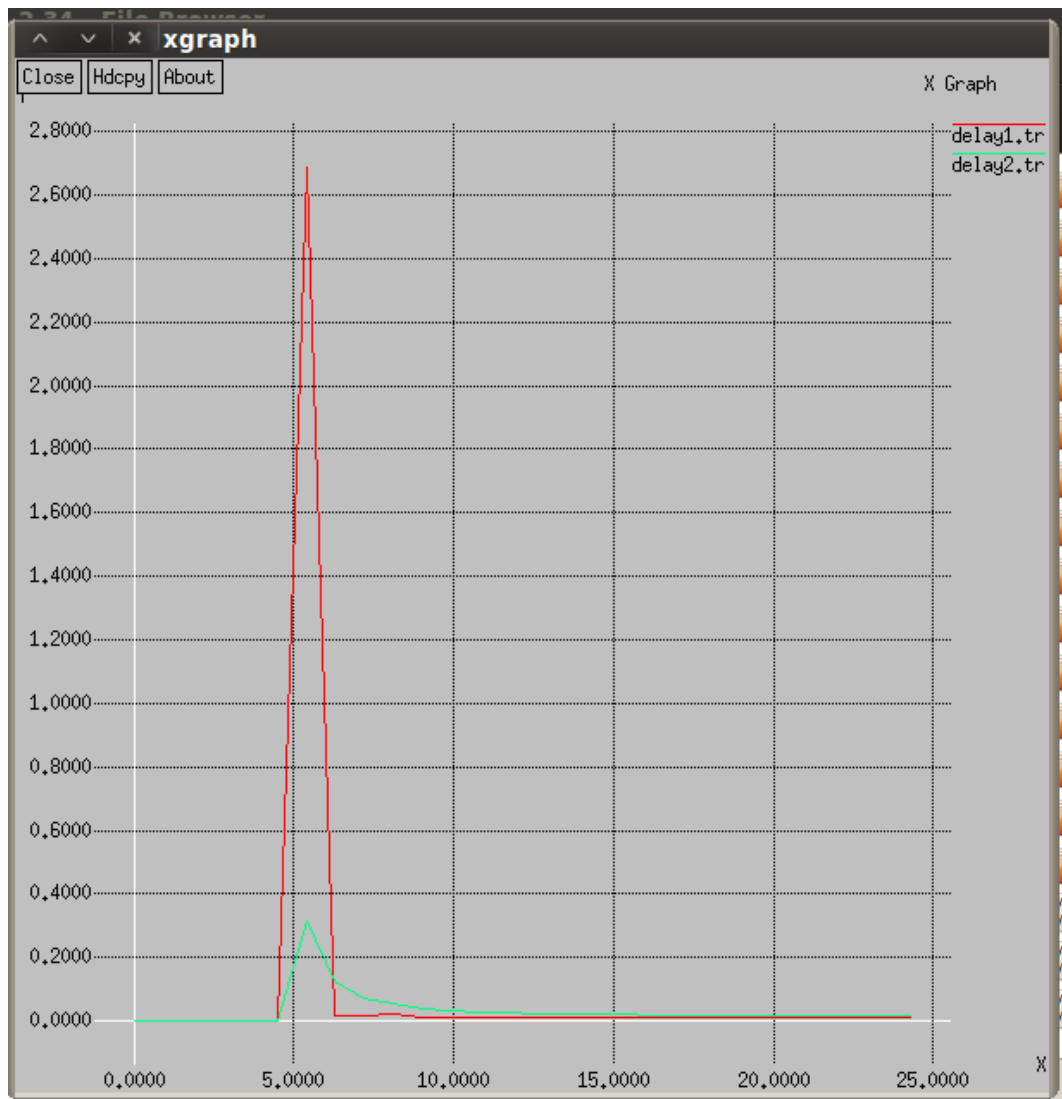


Figure 4.1- comparison of end to end delay graph

In the graph 4.1 the delay of end to end delays very much less as compare to the first delay. The first delay is shown through the red line and my delay is shown by green line.

B) Comparison of Throughput graph-

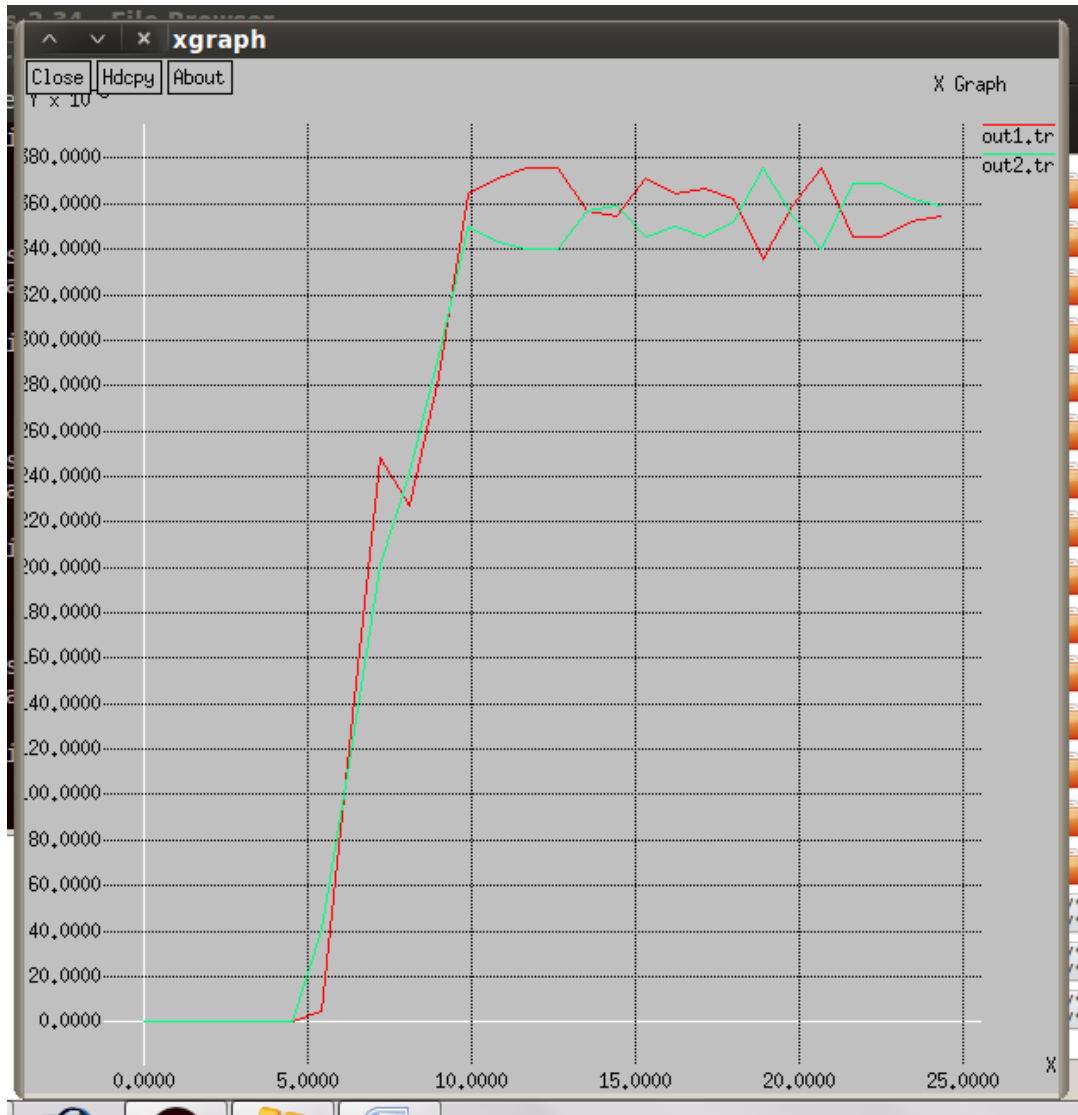
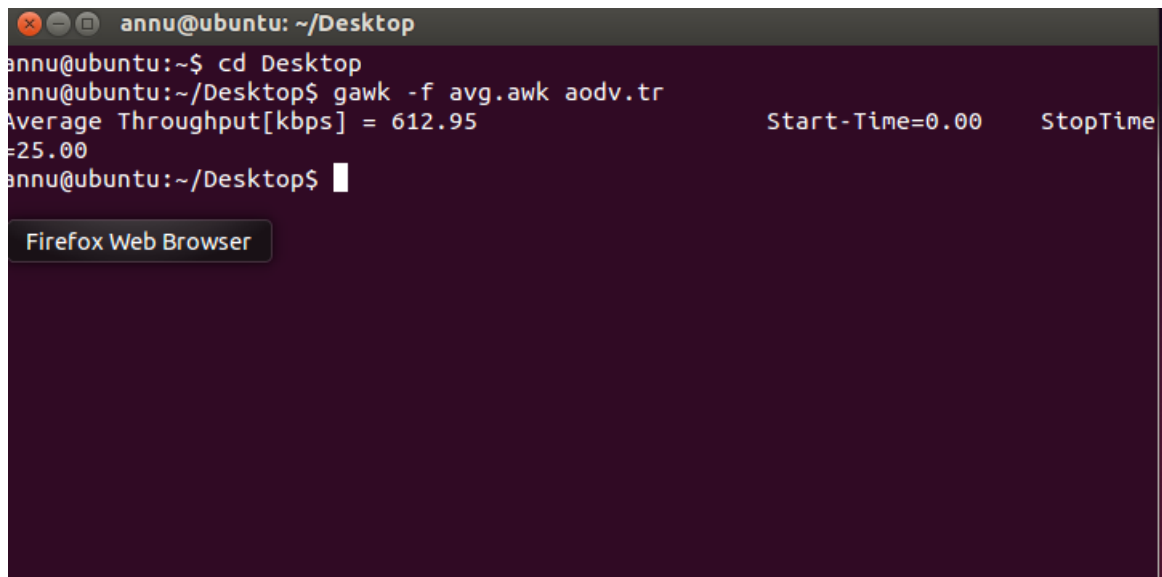


Figure 4.2 comparison of throughput graph

The graph 4.2 shows the throughput in this graph. The green line throughput is much better than the red one. Now we see the awk files that use in ns2 for scripting on the basis of trace files.

A) Throughput awk file-

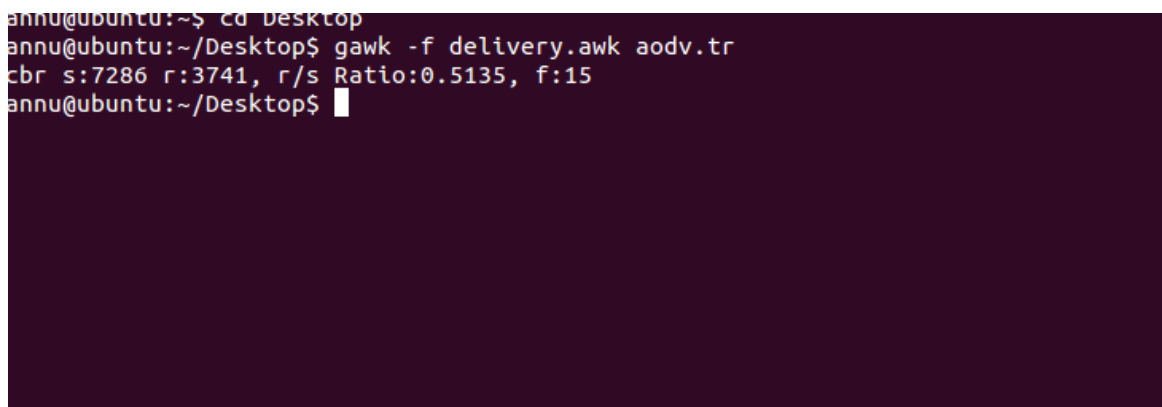


```
annu@ubuntu: ~/Desktop
annu@ubuntu:~$ cd Desktop
annu@ubuntu:~/Desktop$ gawk -f avg.awk aodv.tr
Average Throughput[kbps] = 612.95          Start-Time=0.00      StopTime
=25.00
annu@ubuntu:~/Desktop$
```

Figure 4.3 Throughput awk script

In the figure 4.3 throughput awk script the average throughput rate is 612.95 kbps shown in this script and with the help of this we can calculate the performance of network.

b) Awk script of packet delivery rate-



```
annu@ubuntu:~$ cd Desktop
annu@ubuntu:~/Desktop$ gawk -f delivery.awk aodv.tr
cbr s:7286 r:3741, r/s Ratio:0.5135, f:15
annu@ubuntu:~/Desktop$
```

Figure 4.4 awk script of packet delivery rate

In this figure 4.4 shows the script of packet delivery rate and there is use the constant bit rate and shows the sender and received packets. Now show the simulation of my thesis that is as follows-

a) SAODV protocol attached to ns2 file-

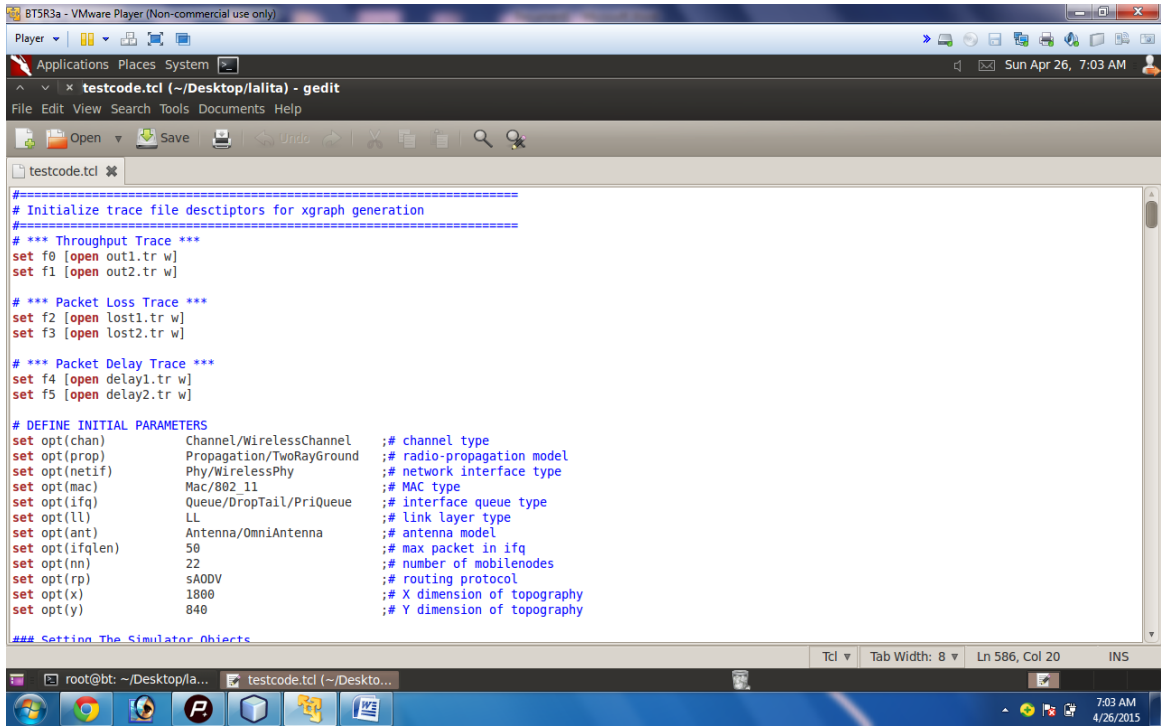


Figure 4.5 screen shot of sAODV protocol

In the figure 4.5 tcl codes show the all initial parameters and the all traces which I mentioned in my implementation.

b) Running the testcode.tcl file-

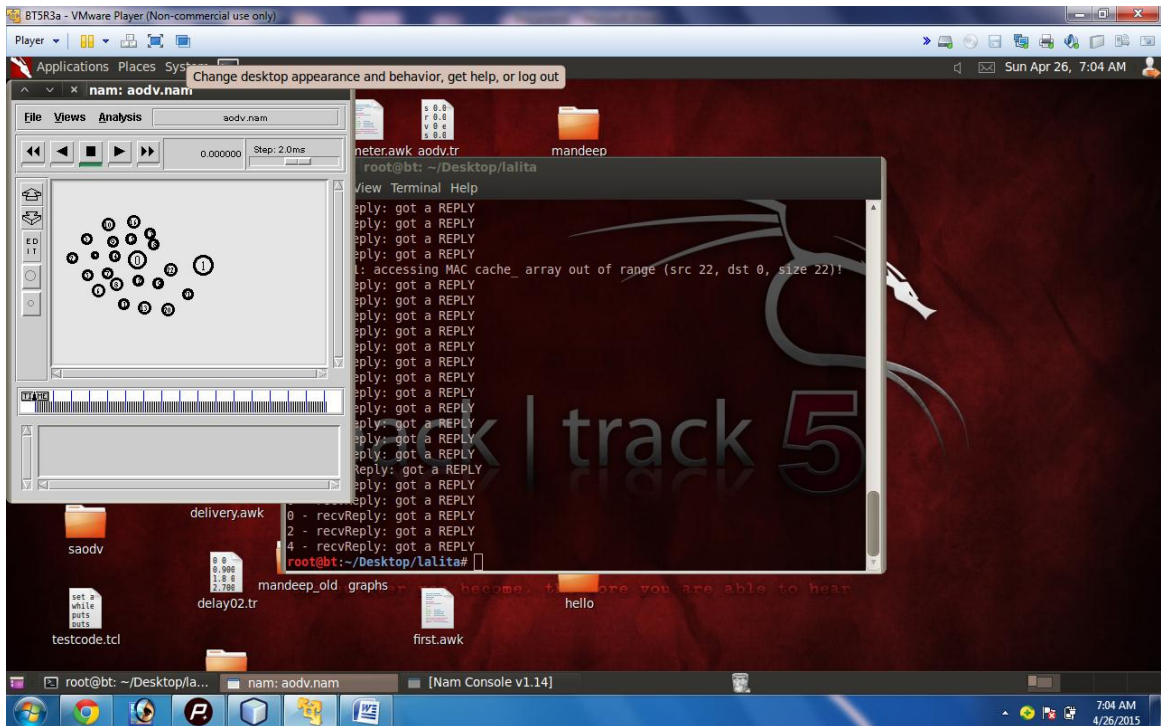


Figure 4.6 screen shot of testcode.tcl file

In the figure 4.6 show the start of nam file when we execute the tcl file in ns2. With the help of this we can show the simulation of implementation or front end.

c) Running nam file screenshot no 1-

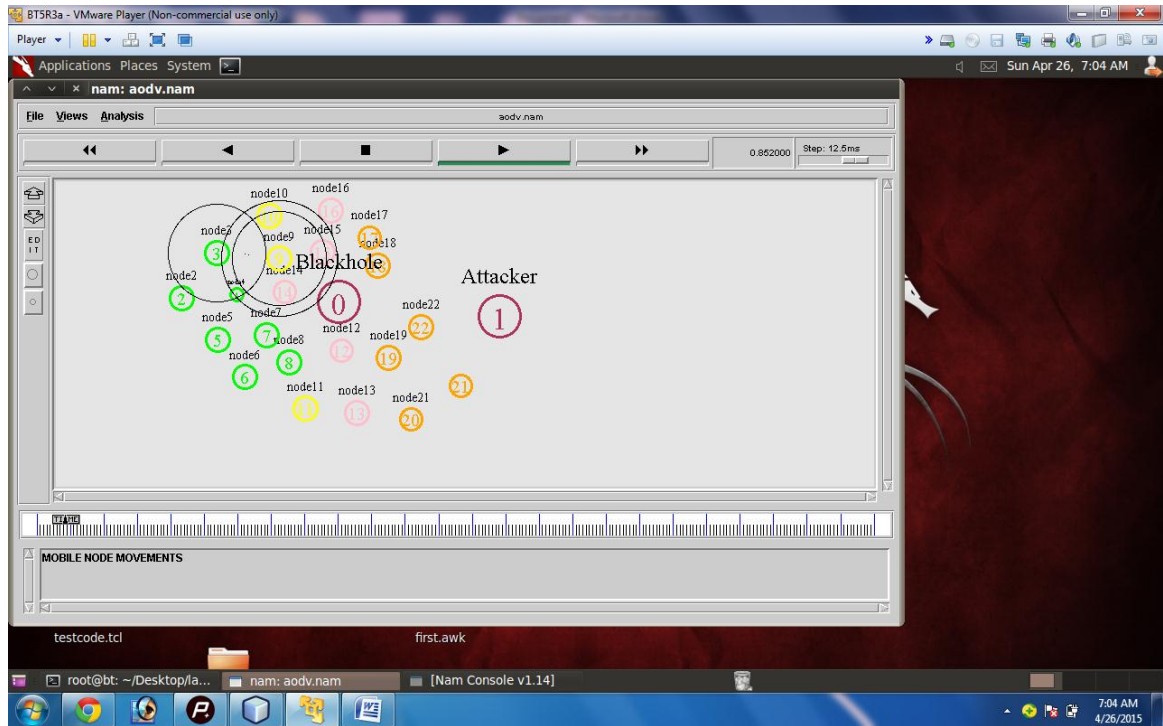


Figure 4.7 nam file screen shot 1

The figure 4.7 show the nam file when the tcl code start or execute successfully. In this figure the mobile nodes are move.

d) Running nam file Screenshot no 2-

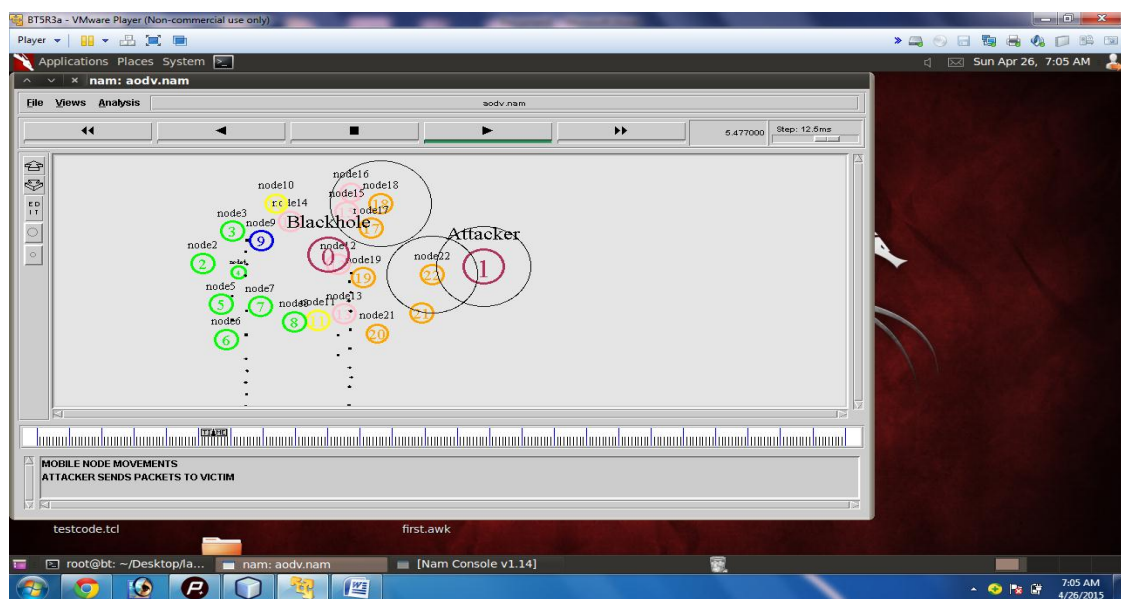


Figure 4.8 nam file screen shot 2

In figure 4.8 the attacker or the malicious node starts sending packets to the victim node.

e) Nam files screen shot-

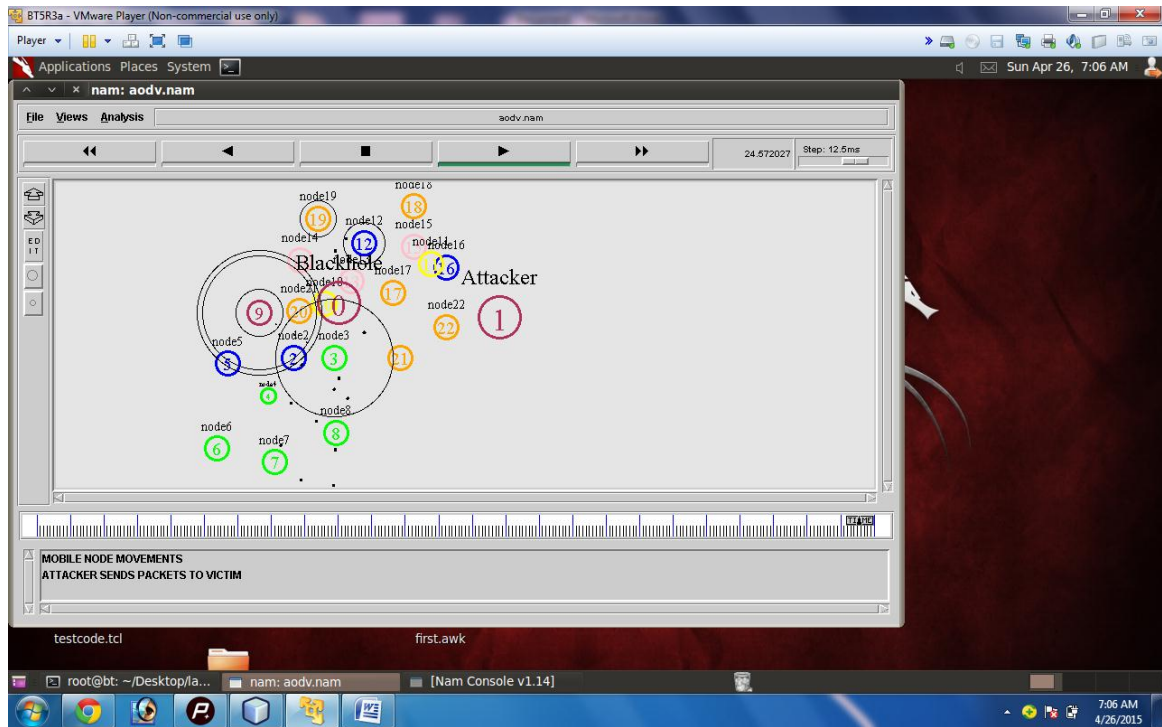


Figure 4.9 nam file screen shot 3

In figure 4.9 the nam file is working when black hole is detect by the source node.

f) Parameters-

S.No	Parameter	Value
1	Protocol	AODV
2	Transmission Range	250m
3	Wireless medium	IEEE 802.11
4	Simulation Time	100s
5	Grid Size	4X4

Table 4.10 parameters of simulations

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

The black hole attack is very senior type of attack and as compare to other types of attacks it degrades the performance of the network and sometime crash the network and stop communication between all nodes. To prevent from this type of attacks many researchers suggests their ideas for detects the black hole attack because it's works as a honest nodes in the network and when source start send the packet to destination ,it take the packets from that node and drop the packets in way and not send the packet to destination node. The route request and verification algorithm using the AODV protocol improves the quality of network and communication between source and destination node and no any malicious node can attack the network and drop the packet as well as cannot degrade the network performance. The best thing is the end to end delay between nodes becomes less. It also increases the security of network and packets. This detects the black hole attack before start communication through route request packets not with data packets.

In the future scopes we will use the best technique in prime number that will help in detect the malicious node and would consider on the selective black hole attack and improve the throughput much better and try to reduce the delay.

CHAPTER 6

REFERENCES

References to Books:

1. C. K. Toh (2002) Ad-Hoc Mobile Wireless Networks protocols and systems, Pearson's Publications, South Asia
2. C. Shiva Ram Murthy and B. S. Manoj (2004) Ad-Hoc Wireless Networks architectures and protocols, Pearson's Publications, South Asia.

References to Articles:

1. Anand A. Aware and Kiran Bhandari (2014) "Prevention of black hole attack on AODV in MANET using hash function", IEEE.
2. Ashutush Bhardwaz (2014) "Secure Routing in DSR to mitigate black hole attack", International conference on control, Instrumentation, Communication and Computational Technology.
3. A.Naveen & K.Rama Linga Reddy (2013) "Dynamic Training intrusion detection Scheme for black hole attacks in Manet", International Journal of computer science and network security, volume 13,no. 10,October 2013.
4. Ahemed Sharif and Amin Shoukry (2013) "A Novel taxonomy of black hole detection techniques in mobile ad-hoc networks," International conference on computational science and engineering.
5. Anamika Thakur "Review-Secure route discovery for preventing black hole attack on AODV based Manet", International Journal of science and research, ISSN-2319-7064.
6. Anurag Singh Tomar and Gaurav Kumar Tak (2014) "Optimized positioning of multiple base stations for black hole attack", International journal of advanced research in computer engineering and technology, volume3,issue 8,August 2014.

7. Ekta gupta and Akhilesh Tiwari (2014) “Approaches for detection and prevention of black hole attack in AODV: A Critical review”, International journal of commuting science and information technology, Volume 7.
8. Gayatri Wahane and Ashok .Kanthé (2014) “Techniques for detection cooperative black hole attack using true-link in mobile ad-hoc networks”, MIPRO.
9. Gursheen Kaur and Mandeep Singh (2014) “Detection of black hole in wireless sensor networks based on data mining”, IEEE.
10. Geeta Pattun &V.Sireesha (2014) “A Reaction Based Approach to Detect Black Hole Attack Using Modified AODV protocol in MANETS”, International Journals of Computer Networks and Wireless Communication, (FEBURAY 2014), ISSN: 2250-3501, Volume.
11. Gayatri Wahane and Savita Lonare (2013) “Techniques for detection of cooperative black hole attack in manet” IEEE, (July 2013), 4rth Iccent 2013.
12. Herminder Singh, Shewta (2011) “An approach for detection and removal of black hole in MANETS”, International Journal of Research in IT &Management (IJRIM), volume.1, issue 2.
13. Hichem Sedjelmaci and Sidi Mohammad Senouci (2014) “A New Intrusion Detection Framework for Vehicular Networks”, IEEE.
14. Harsh Partap Singh and Rashmi Singh (2014) “A mechanism for discovery and prevention of cooperative black hole attack in mobile ad hoc networks”, IEEE.
15. Ira Nath and Dr. Rituparna Chaki (2012) “A New black hole attack prevention system in clustered Manet”,International journal of Advance research in computer science and software engineering, volume 2,issue 8,august 2012.
16. K. Selvavinayaki, Dr. Karthikeyan (2014) “A secure data transmission method using enhance proactive secret sharing scheme to prevent black hole attacks in

- MANETS”, journal of theoretical and applied information technology, ISSN-1992-8645.
17. K.Pavani and Dr. A. Damodaram (2014) “Intrusion Detection Using MLP for Manet”, IEEE.
 18. K. Mahalaxmi & Dr .D .Sharmila (2013) “ Intrusion detection system on MANET security against selective black hole attack”, International journal of research in computer engineering and electronics, Volume 2, Issue 3,(June 2013),ISSN 2319-376X.
 19. L. Himral, V.Vig (2011) “Preventing AODV routing protocol from black hole attack”, International Journal of Engineering Science and Technology (IJEST), volume.3.
 20. Hemant Sharma and Koushik Banerjee (2014) “Black hole Tolerant protocol for Zigbee wireless networks”, International conference on computational Intelligence and communication networks.
 21. Mohammad Taqi Soleimani (2011) “Secure AODV against Malicious Packet Dropping “, Institutes of Electrical and Electronics Engineer-IEEE.
 22. Mozmin Ahemed and Mohammad Anwar Hussain (2014) “Performance of an IDS in an Adhoc Networks under Black hole and Gray hole attacks” ,IEEE.
 23. Mohanpriya & Lingo Krishnamurthy (2013) “Modified DSR Protocol for Detection and Removal of Selective Black hole Attack in MANET”, Computers and Electrical Engineering.
 24. M.Amresh and G.Usha (2013) “Efficient malicious detection for AODV mobile Ad-Hoc Networks”, International Conference on Recent Trends in Information technology.

25. Man Mohan Sharma and Maninder pal Singh (2014) “Enhanced multiple approaches for prevention and elimination of black hole attack in mobile ad-hoc networks considering the enhancement of network throughputs”, International journal of engineering science and research technology ,ISSN:2277-9655,may 2014.
26. Neelam Khemariya& Ajay Khunteta (2013) “An efficient algorithm for detection of black hole attack in AODV based Manets” International Journals of Computer Applications, (2013), Volume.66, Number.18.
27. Nidhi Chodhary and Dr. Lokesh Tharani (2015) “Preventing black hole attack in AODV using Timer based Detection Mechanism,IEEE,SPACES-2015.
28. Payal. N. Raj & Prashant B. Swades (2009) “A Dynamic learning system against black hole attack in AODV based MANET”, International Journal of Computer Science Issues, volume.2, p 54-59.
29. P.S.Hiremath, Anuradha .t. (2014)”Detection and prevention of cooperative black hole attacks in MANETS”, International journal of research in computer and communication technology (IJRCCT), ISSN-2278-5841.
30. Romina Sharma & Rajesh Shrivastava (2013) “Modified AODV Protocol to Prevent Black Hole Attack in Mobile Ad-hoc network”, International Journal of Innovative Research & Development (April 2013) ISSN: 2278-0211, Volume 2 issue 4.
31. Santoshi Kurosawa (2007) “Detecting black whole attack on AODV based Mobile Ad-hoc Networks by Dynamic learning method”, International Journal of Network Security, vol.5, no.3.
32. S.Neelavathy Pari, Sabarish Jaypal & Sridharan Duraisamy (2012) “A Trust System In Manet with Secure Key Authentication Mechanism”, Institutes of Electrical and Electronics Engineer-IEEE, (ICRTIT-2012), ISBN: 978-1-4673-1601.

33. Sapna Gambhir, Saurabh Sharma (2013) "PPN: Prime Number based Malicious Node Detection Scheme for MANET", IEEE international advance computing conference (IACC), 978-1-4673-4529/S 31.00.
34. Shashi Gurung, Aditya Kumar & Dr. Krishan Kumar Saluja (2013) "Detection of Black hole Attack in Mobile ADHOC Networks", UACEE International Journal in Advances in Computer Networks and its Security-IJCNS, (September 2013), ISSN 2250-3757.
35. Shristi Chandel and prof. Ashish Tiwari (2014) "A Weighted clustered algorithm for improving MANET security", International journal of computer science and information technology research, volume 2, issue 3.
36. Shristi Jain and Sandeep K Raghuvanshi (2014) "Behavioral and node performance based gray hole attack detection and amputation in AODV protocol", International conference on advances in engineering & Technology Research, ICATER-2014.
37. Suparna Bishwas and Tanmoy nag (2014) "Trust based energy efficient and avoidance of black hole attack to ensure secure routing in manet", Applications and innovations of mobile computing.
38. Seryvuth yen and Keecheon Kim (2014) "Secure route discovery for preventing black hole attacks on AODV-based Manets", IEEE.
39. Samir Athmani and Azeddine Bilami (2014) "Hierarchical Energy Efficient intrusion Detection system for black hole attacks in WSNs", IEEE.
40. Taseem Elisa, Shakur Abdul Razak, Rashid Hafeez Khokhar & Normalia Samian (2011) "Trust-Based Routing Mechanism in MANET: design and implementation", Springer Science + Business Media, LLC.

41. Y.F. Alem & Z.C. Xuan (2010) "Preventing Black hole attack in mobile ad-hoc network using anomaly detection", IEEE, ICFCC, 2nd international conference on, volume 3, pages V3-672.

ABBREVIATIONS

MANET	Mobile Ad-Hoc Network
DSDV	Distance Sequence Distance Vector
WRP	Wireless Routing Protocol
CGSR	Cluster Gateway Switch Routing Protocol
AODV	Ad-Hoc on Demand Distance vector
DSR	Dynamic Source Routing Protocol
TORA	Temporally Ordered Routing Protocol
ZRP	Zone Routing Protocol
RREQ	Route Request Query
RREP	Route Reply
DT	Distance table
RT	Routing Table
LCT	Link Cost Table
MRL	Message Transmission List
MDSR	Modify dynamic source routing protocol
NREQ	Neighbor route request query
NRREP	Neighbor route reply
MN	Malicious nodes
NRREP	Route reply from intermediate nodes
SAODV	Secure ad-hoc on demand vector