ENHANCED BLACK HOLE DETECTION TECHNIQUE IN MOBILE ADHOC NETWORK

Dissertation submitted in fulfilment of the requirements for the Degree of

MASTER OF TECHNOLOGY

In

COMPUTER SCIENCE AND ENGINEERING

By

SHARANPREET SINGH

11408630

Supervisor

ROBIN PRAKASH MATHUR

School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

May 2017

TOPIC APPROVAL PERFORMA

School of Computer Science and Engineering

Program : 1702::M. Tech- CSE(Computer Science and Engineering)(FullTime)

COURSE CODE : CSE546 **REGULAR/BACKLOG :** Backlog **GROUP NUMBER :** CSEBGD0370

Supervisor Name : Robin Prakash Mathur **UID :** 14597 **Designation :** Assistant Professor

Qualification : _____ **Research Experience :** _____

SR.NO.	NAME OF STUDENT	REGISTRATION NO	BATCH	SECTION	CONTACT NUMBER
1	Sharanpreet Singh	11408630	2014	KN620	08968818166

SPECIALIZATION AREA : Database Systems **Supervisor Signature:** _____

PROPOSED TOPIC : Security issues in mobile adhoc network

Qualitative Assessment of Proposed Topic by PAC		
Sr.No.	**Parameter**	**Rating (out of 10)**
1	Project Novelty: Potential of the project to create new knowledge	6.33
2	Project Feasibility: Project can be timely carried out in-house with low-cost and available resources in the University by the students.	6.33
3	Project Academic Inputs: Project topic is relevant and makes extensive use of academic inputs in UG program and serves as a culminating effort for core study area of the degree program.	6.00
4	Project Supervision: Project supervisor's is technically competent to guide students, resolve any issues, and impart necessary skills.	7.33
5	Social Applicability: Project work intends to solve a practical problem.	6.33
6	Future Scope: Project has potential to become basis of future research work, publication or patent.	6.33

PAC Committee Members		
PAC Member 1 Name: Janpreet Singh	UID: 11266	Recommended (Y/N): Yes
PAC Member 2 Name: Harjeet Kaur	UID: 12427	Recommended (Y/N): Yes
PAC Member 3 Name: Sawal Tandon	UID: 14770	Recommended (Y/N): Yes
PAC Member 4 Name: Raj Karan Singh	UID: 14307	Recommended (Y/N): NA
DAA Nominee Name: Kanwar Preet Singh	UID: 15367	Recommended (Y/N): NA

Final Topic Approved by PAC: **Security issues in mobile adhoc network**

Overall Remarks: Approved

PAC CHAIRPERSON Name: 11011::Dr. Rajeev Sobti **Approval Date:** 03 Nov 2015

ABSTRACT

MANET is a most promising and rapidly growing field for research and development of wireless networks based on a self-organizing and rapidly deploying network. As the mobile devices and the wireless networks are significantly becoming more popular and increased over the past few year, it has now become one of the most active and vibrant field of communication in networks.

In this report we have focused on how a network with mobile nodes is attacked by the attackers with an overview of different types of attacks and primarily focusing on a particular type of attack that is Black Hole attack and we have provided a new approach to overcome this problem.

A black hole attack is one in which one node claims to be having the shortest path from the source to the destination by replying to the route request packet of the sender node. This node is named as a malicious node or attacker, which after gaining the trust of the sender receives all the data packets and then instead of forwarding, it starts dropping them in such a way that the packets can never be recovered. That is why it is called Blackhole node.

The main aim of this research is to provide an effective mechanism to detect suck kind of attacks and help the other nodes by preventing them not forwarding data packets to such nodes in the network. In this report we have discussed about detecting the malicious node with the help of distance-time value which is compared with certain parameters and then the malicious node is isolated with the help of clustering.

DECLARATION STATEMENT

I hereby declare that the research work reported in the dissertation entitled "ENHANCED BLACK HOLE DETECTION TECHNIQUE IN MOBILE ADHOC NETWORK" in partial fulfilment of the requirement for the award of Degree for Master of Technology in Computer Science and Engineering at Lovely Professional University, Phagwara, Punjab is an authentic work carried out under supervision of my research supervisor Mr. Robin Prakash Mathur. I have not submitted this work elsewhere for any degree or diploma.

I understand that the work presented herewith is in direct compliance with Lovely Professional University's Policy on plagiarism, intellectual property rights, and highest standards of moral and ethical conduct. Therefore, to the best of my knowledge, the content of this dissertation represents authentic and honest research effort conducted, in its entirety, by me. I am fully responsible for the contents of my dissertation work.

Signature of Candidate

Sharanpreet Singh

Reg.No: 11408630

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M.Tech Dissertation entitled **"ENHANCED BLACK HOLE DETECTION TECHNIQUE IN MOBILE ADHOC NETWORK"**, submitted by **Sharanpreet Singh** at **Lovely Professional University, Phagwara, India** is a bonafide record of his original work carried out under my supervision. This work has not been submitted elsewhere for any other degree.

Signature of Supervisor

Robin Prakash Mathur

Date:

Counter Signed by:

1) **HoD's Signature:** _____

   HoD Name: _____

   Date: _____

2) **Neutral Examiners:**

   - **Examiner 1**

     Signature: _____

     Name: _____

     Date: _____

   - **Examiner 2**

     Signature: _____

     Name: _____

     Date: _____

ACKNOWLEDGEMENT

I owe a debt of deepest gratitude to my dissertation supervisor **Mr. Robin Prakash Mathur**, Assistant Professor, School of Computer Science And Engineering, for his guidance, support, motivation and encouragement throughout the period within which this work has been 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 the Department, School of Computer Science and 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.

Last but not the least I am very lucky for having wonderful support of my friends and family members especially my parents. Thanks to almighty for providing me such invaluable gifts, support, enthusiasm and courage.

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Mobile Adhoc Network (MANET)

A mobile ad hoc network is a decentralized autonomous system of the mobile nodes which are connected to each other via wireless links and all nodes co-operate with each other by transferring data packets to each other in the network. It is a simple network with limited number of nodes which act as both hosts as well as the routers although a mobile ad hoc network do not require any type of base station or an access point or routers to deploy which is the key feature of MANET. It is not necessary that the source and the destination nodes are always in a direct connection with each other so they need the help of the other nodes within the same network, to make the communication possible.

There is no central control device which can control the data transfer and processing of the different nodes in MANET so it provides less security and leads to more chances of data loss within the network. But also on the other side it provides facilities like ease of deployment and faster speed of deployment.

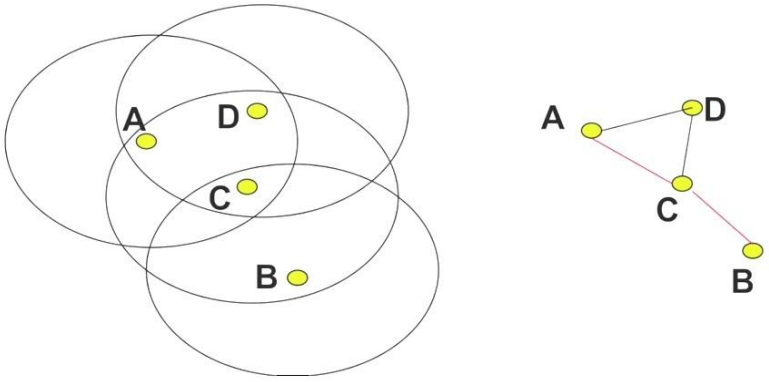


Figure 1.1: A simple mobile ad hoc network

Due to the nature of trusting the other nodes for communication within the network the mobile ad hoc networks are highly vulnerable to various attacks which give us a vast area to research on. Not just that, there are several other issues as well which are discussed further.

1.2 Advantages of MANET

- **Ease of deployment**: The mobile ad hoc networks are very easy to deploy in any situation like natural hazards, disaster prone areas, military areas, etc. It does not require any expertise to install. It is an automatic wireless sensible network that connects different nodes with each other when they come inside the range of the other node or device.
- **Speed of deployment:** As the devices come in the range of other devices it is just a matter of seconds that the device's details are shared among each other and is shown in the routing table of each other. It is a very fast process about few milliseconds of time to connect, that helps a lot in handling over the control from one node to another for a successful delivery of packets to the destination. Although the speed is sometimes dependant on the type of device connected to the network but in most cases it is fast.
- **Mobility:** In mobile ad hoc networks the nodes are able to move freely to any other location within or outside the network and are still able to communicate with the other nodes. Mobility leads to change in the topology of the network but we always have the option of choosing an alternate path. Mobility helps in transmission of data while moving.
- **Low Cost:** The deployment cost of the mobile ad hoc networks is relatively very low as compare to the other wireless or wired networks because of the fact that MANET do not need any central device, router, hub or access point to connect to different nodes and devices. The energy used to transfer the data is obtained from the devices itself.
- **Decentralized and robust**: One of the most useful advantage of the adhoc networks is that these networks do not have any centralized control device or management system such as a server computer that holds the data of all the other nodes. Due to this property, if one of the nodes loses its connectivity either it was an important node or not, the network still keeps on transferring the data via some other route (change of topology). We can manage to send the data packets over the network as long as there is at least one path available to the destination node. All the nodes can act as a server node by keeping the record of the neighbouring nodes and providing secure data transfer to the others.

1.3 Disadvantages of MANET

- **Lack of centralized management:** Due to lack of central management in the adhoc networks, it's easier for the attacking nodes to intercept into the network. As the nodes in the network are not aware of the all the nodes currently present, any malicious node can claim to be a trustworthy node and can disturb the network's performance.
- **No pre-defined boundary:** In mobile ad hoc networks, the boundary of the network isn't fixed. Any node can join and leave the network at any time. The nodes work in an open environment where they do not need any authentication before connecting the network. This property makes the network vulnerable and easy to break security.
- **Cooperativeness:** In the routing algorithms for MANETs it is usually pre-assumed that nodes in the network are cooperative and non-malicious. As a result the attacker node can easily break into the system as an important node in the path and then disrupt the network operations.
- **Limited power supply:** The nodes in the MANET have limited power supply, which causes several problems. The route is damaged if any of the intermediate nodes is gone out of power. A node can behave a little selfish in mobile ad hoc network when they get to know that there is only limited supply of power.
- **Adversary inside the network:** The nodes within the network may also behave maliciously due to any reason like hardware failure, virus problem, damage due to age of the system, etc. This is hard to figure out the behaviour of the nodes that it is malicious or not. Thus such types of attacks are more dangerous as compared to external attack.

1.4 Applications of MANET

- Communication in military operations.
- Automated battlefields.
- To provide services during emergencies.
- Operations like Search and rescue for military and police as well.
- Paying bills anytime from anywhere (E-commerce).
- Access of dynamic databases and mobile offices.

- Personal area networks.
- Networking at sites going through construction.
- Virtual classrooms in the university.
- Ad hoc communications during meetings and lectures.
- Multi-user gaming.
- Wireless peer-to-peer networking and access of internet while being outside.

1.5 MANET Issues and challenges

- **Dynamic Topology:** The nodes of a mobile ad hoc network tend to change their location which leads to change in the topology of the network. If it keeps on changing then it will ultimately affects the routing and packet delivery time will get extended. It is one of the major issue and challenge to mobile ad hoc networks.
- **Limited Bandwidth**: Wireless links tends to have capacity lower than the wired or infrastructure based networks. Due to limited capacity it is necessary to save the bandwidth for the nodes to use for data transmission instead of wasting it on the use of multiple control messages or unwanted data packet transmissions.
- **Routing overhead:** In wireless ad hoc networks, the updation of the routing tables is done after some time interval in table driven algorithms and during route finding process in demand driven algorithms so there are some stale routes that are left inside the routing tables of the nodes which are not updated yet, results in unnecessary overhead. Overhead leads to time consumption, slow data transfer, wastage of bandwidth and energy.
- **Hidden Terminal problem:** The hidden terminal problem occurs when multiple nodes send some data packet to a same third party node without knowing to the fact that both are sending data at the same time or the node is busy. This result in collision of the data packets cause the sender nodes are actually hidden from each other.
- **Battery constraints:** Different nodes or devices have different battery power limitations so in a particular ad hoc network the portability, size and weight of the devices are manipulated in terms of power.

- **Scalability:** The mobile ad hoc networks do not have any limitation on the total nodes to have in a particular network. With increase in the nodes the overall quality of the network decreases.
- **Security:** In mobile ad hoc network, when distant nodes want to communicate they have no choice but to trust the other intermediate nodes for a successful data transmission. Because the nodes are mobile in nature it may happen that some malicious nodes come inside the route or path and then drop or modify the data packets. Hence security is a major issue in MANET.
- **Multicasting:** Due the dynamic nature of the nodes, it makes it difficult for a node to multicast some information in a mobile ad hoc network. There are solutions to this problem like clustering of the nodes but the nodes do not stay forever in the same cluster hence leads to problems like multicasting.

1.6 MANET security goals

- **Availability:** Availability means that the resources or the nodes are available at the time of their need. Data and services both are important assets in terms of availability. In case of attack, when the network's performance is down, availability plays important role. The dynamic nature of the nodes does not keep them available all the time.
- **Confidentiality:** To keep the data private and accessible to the authorized nodes only is confidentiality. In simple term, the data of one node should not be exposed to the other nodes. It is very important if some nodes are sharing financial information or data that can adversely affect the node or the network.
- **Integrity:** The data is said to be integrated if it is same on both the sender and the receiver side. It means the data packets are not altered or dropped on the way towards destination. Integrity ensures that the message contains no corrupted data while transferring it towards destination.
- **Authentication:** Authentication ensures that the nodes in the communication are authenticated nodes, not fake or virtual nodes. The resources and services of a network should be used by the authenticated users only.
- **Authorization:** Authorization is basically providing different access rights to the different nodes. In a mobile ad hoc network, the sender and the receiver

nodes are authorized to view the data inside a packet. The other nodes that read the data are none other than the malicious nodes or unauthorized nodes.

- **Packet Delivery Ratio (PDR):** The packet delivery ratio can be defined as the number of data packets arrived at the destination over the number of data packets actually transmitted by the source node. Higher the PDR ratio shows higher protocol performance.
- **End- to-End delay:** It is the average time calculated by a particular data packet to travel towards destination from the source node.
- **Throughput:** It is the total number of data bits successfully transferred in a particular time interval. In other words, the total number of data packets arrived at the destination node from the source node over time. Its unit of measure is bits per second (bps).
- **Routing overhead:** It is the ratio of the amount of routing related control packets transmissions to the amount of data transmissions

1.7 Attacks on MANET

MANET Security Layer	Attacks
Multi-layer attacks	Denial of Service
	Impersonation
	Replay
	Man in the Middle
Application layer	Repudiation
	Data corruption
Transport layer	Session Hijacking
	SYN Flooding
Network layer	Black hole attack
	Grey hole attack

	Worm hole attack
	Byzantine attack
	Sybil attack
	Flooding
	Rushing
	Spoofing
Data link layer	Traffic monitoring and analysis
Physical layer	Jamming
	Interception
	Eavesdropping

Table 1: Attacks on MANET

CHAPTER 2

LITERATURE SURVEY

In a network, there are several layers at both ends of a transmission that helps in data transfer from source to destination. Each layer has its own functions, jobs, features and properties. The attackers always attack on the nodes aiming at a particular layer or sometimes multiple layers. With different features of each layer there are different types of attacks in a MANET that are exclusively made for particular layer in the network. As we have already discussed an overview about these layers and type of attacks on these particular layers, in this chapter we are going for a deeper study about some of these attacks.

In MANET, there are different types of routing protocols that are used to transfer data packets in the network. These routing protocols are described below.

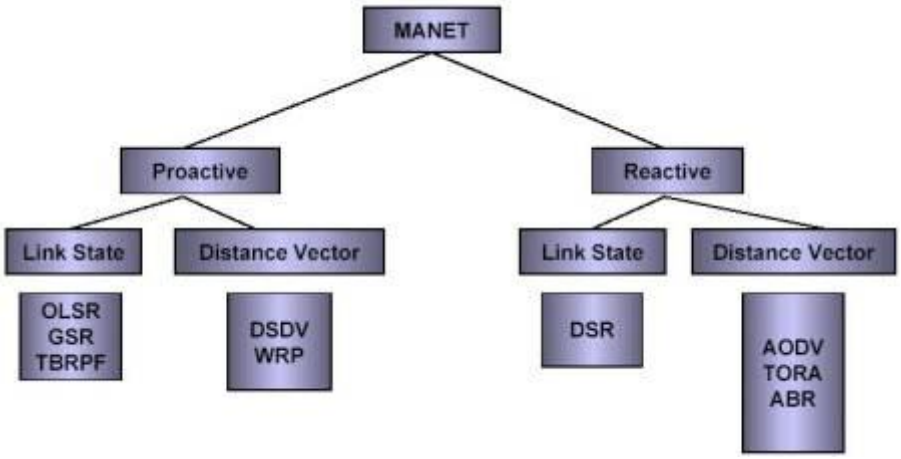


Figure 2.1: MANET routing protocols

2.1 MANET routing protocols

Link-State routing protocol

A link state routing protocol works on the basis of Dijkstra's algorithm. In this a node simply manages local link information from itself to all its neighbours in the term of hop counts. In this, the shortest path is chosen on the basis of the strength of each link between the nodes. Even if the hop count is more, if the data transfer rate between two

nodes is high then the path is selected as the shortest path. It is based on the speed of the data transfer.

Distance vector routing protocol

In this the speed or the strength of the link does not matter. The shortest path is chosen on the basis of hop count from the source to the destination. The less number of hops results in more chances for the path to get selected as the shortest path even if the distance in reality is more. In this, all the nodes in the network manages to maintain an overview of the network with an information about the total distance from to all the nodes from a single node within the network in the terms of hop count which is stored in the routing information of each node. By this way, each node can check the hop count to select the shortest path. Also on the other hand, it helps in removing the problem of count to infinity.

Proactive routing protocol

The proactive routing protocols are the one which keeps an update of all the nodes that are present in the network. These updates are done periodically after time to time to keep up to date fresh information about all the nodes in a network and also differentiating the stale routes. The update system of these protocols become a waste of energy and bandwidth as even if there is no need to transfer data, the nodes still keep updating each other and as a result lots of network resources get used for nothing.

Reactive routing protocol

The reactive routing protocols are the one which only activates when there is a need for transmission of the data packets in the network. On the meantime, the network does nothing, no updates of routes, no extra resource wastage. The routing protocol that is used in this research work belongs to this category i.e. AODV (Adhoc On-Demand Distance Vector).

Adhoc On-Demand Distance Vector routing protocol (AODV)

In this routing protocol, when the source node needs to transfer data packets towards the destination node, it needs the path to transfer data packets so first of all a Route Request Packet (RREQ) is generated by the source and it is broadcasted in the

network. This RREQ packet is received by all the intermediate nodes and the one who knows the path to the destination or if it is the destination node itself then it generates a Route Reply Packet (RREP) and sends to the same path back to the source. On the way back, when the RREP packet traverse back, it keeps on telling all the intermediate nodes about the path and the destination and this information is stored in the routing table of each intermediate node. When the data transmission starts, each node knows where to send the packets and this way data transmission is done.

There is a possibility that the source node may get multiple route replies from the intermediate nodes so in such cases the RREP packet which was received first is selected because the faster RREP can only be received from the node which is having less number of hops from source to itself. These RREP packets can only be generated by the destination or the neighbours of the destination only. So we have another possible factor which can be used to select the RREP i.e. Sequence number.

A sequence number is a number which is assigned to a node when it enters a network. The higher the sequence number is, the older and trustworthy the node is.

2.2Research papers and literature review

Blackhole detection with a new control packet [1]

It is a survey paper that contains the details about variety of attacks that may occur inside a mobile ad hoc network. A number of attacks are explained and among them one of the most devastating attacks was a Blackhole attack.

A black hole attack is a denial of service type attack that stops the data transmission by dropping packets. In [1] this approach, the modification in the route detection mechanism is done. The source node sends RREQ packet along with another CREQ i.e. Confirmation Route Request packet towards the next hop to the node which generates a RREP message. The next hop node then receives a CREQ packet and replies to the source with the conformation that does the destination's path is in its routing table or not and reply with a CREP i.e. Conformation Route Reply Packet. The validation is done with the help of the next node. In case if the next hop is also malicious then the source waits for more than one route reply packets and then check for a common node's presence in the two paths and rely on the path if it is there. The other drawback of this approach was that it consumes more time because it waits for multiple RREP packets to arrive.

Study of different attacks and performance parameters [2]

Manet is that type of network which allows different nodes to join the network and trust that node for data transmission without any verification because of lack of central management. Due to this property, Manet is vulnerable to many types of attacks which are explained in this [2] paper, such as Blackhole attack, Jellyfish attack, Neighbor attack. The first two attacks are common in nature except that Blackhole drops the packets and Jellyfish delays the packets and in the Neighbor attack the AODV protocol is modified as no node will be sharing their ID in the route detection so that the malicious node can make the others believe that it is directly connected to the destination. On the other hand some performance evaluation parameters are explained in the paper [2]. These parameters are:

- **Packet Delivery Ratio**

The packet delivery ratio can be defined as the total data packets arrived at the destination node over the total data packets actually transmitted by the source node. Higher PDR ratio shows better performance of the protocol. Average PDR is the average of all the PDR values received at all the receivers in the network.

- **End-to-End Delay**

It is the average time taken by a particular data packet to travel towards the destination from source. Average EED is the average value of all the EED values taken at all the receivers in the network.

- **Throughput**

The Throughput is defined as the total data bits received divided by per unit time. This time could be in seconds or minutes or any other time unit. Average throughput is the mean value of all the received throughput values in the network.

- **Delay Jitter**

Delay Jitter is the difference between the times of two consecutive data packets arrived. The average delay jitter is calculated by taking average of all the values at all the receivers in the network.

Architecture of MANET [3]

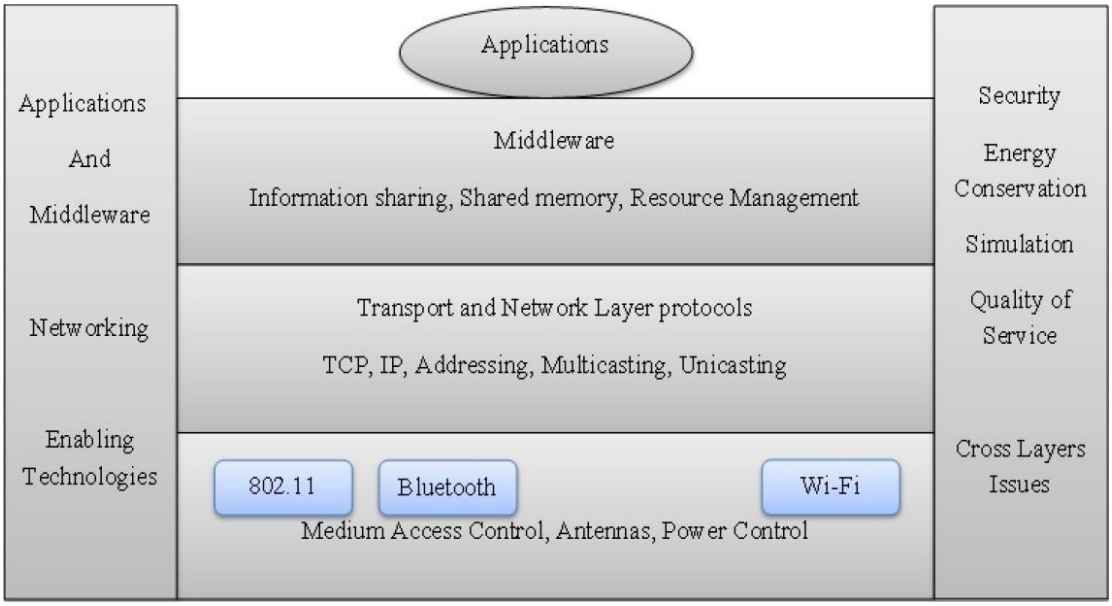


Figure 2.2: Architecture of MANET

Above is the architecture of the Manet. The base layer contains the technologies used in the Manet. The data packets pass through the network layer after going through the transport layer and reach the application layer. The transport layer provides an end-to-end data transmission with the facilities like TCP and UDP. The network layer helps forwarding data packets with the help of unicasting or multicasting. The middleware help the nodes by sharing the information and memory and providing resources to them.

Blackhole detection on the basis of intrusion detection system [4]

As we all know that an intrusion detection system is the one which detects the behaviour of a network or a scenario and compares it with the normal behaviour which is supposed to be happening in the system. If the behaviour is found to be different or uneven then alarm is sounded to notify others in the system. This intrusion detection system is implemented in the MANET in this paper [4] with some modification like a counter is set on the RREQ packet and instead of unicasting the RREP is broadcasted with a counter on it to notify the sender. The neighbouring nodes keep on checking the behaviour of the other nodes in their range for anomaly detection. An IDS agent in order to keep track of the network keeps an audit data collection. We also have the previously stored information about the network and

previously detected anomalies. The limitation of this approach is that it is time consuming.

Secure AODV Blackhole prevention [5]

In this paper, a new approach is provided in order to prevent the blackhole node by simply ignoring the first route reply packet that is received by the sender and selecting the next RREP packet received for data transmission. It may have increased the time taken for the data transmission but on the other hand the Blackhole prevention is done at a high success rate at a very little cost.

Assessment based detection of Blackhole attack [6]

In this paper the detection of the Blackhole node is done on the basis of time value. This time value is calculated on the basis of connection establishment and breakage. As we know all the nodes in the MANET are mobile in nature, when a new node come inside the range of the source node its time of joining is taken and as soon as the node leaves the range of the source node, again its time is taken and after getting these two time values their difference is taken. This difference is called the hint value and this hint value is further compared with the threshold value which was set earlier. If the hint value is less than the threshold value then the particular node is considered as the Blackhole node else it is a trustworthy node. The performance parameters are there with an improved packet delivery ratio and throughput.

A timer based approach for blackhole detection [7]

In this approach, a max_trust value is assigned to all the nodes in the network at the time of their joining. The nodes will not do any data transmission with the nodes which have trust value less than min_trust value. These trust values are dependent on the performance of the nodes in the process of data transmission. When source node starts forwarding the data packets after the route discovery, it provides a unique additional number to the nodes. When the node N starts forwarding the packets it starts a time to live value and adds it to each packet. When this TTL value expires, the node N enters the promiscuous mode and sees if the next node has received the packet or not. If the packet is not there then the node (N) decreases the trust value of that node and if the next node keeps on dropping packets like that then the trust value also kept decreasing and once the trust value is less than min_trust value then all the other nodes put this node into their blacklist table.

A new approach for blackhole detection "BRAVO" [8]

In this approach, two additional fields are added to the routing table which are credit and counter. The credit value is an integer value that indicates the level of trust. Its value is initialized with a formula i.e. K*Hop Count where K is constant. A counter is added to the table initially with value 0. As the data packets are transmitted, its value kept increasing and once the value reaches to a certain value, the credit value is decreased by 1 and the counter is again set to 0. On receiving the packets from the previous node S, the next node R checks whether the next node to the source is S or not and this way it comes to know if the node S is trustworthy or not.

A cooperative bait detection approach to detect collaborative blackhole attacks in Manet [9]

In this approach, the source node uses one of its neighboring nodes as a bait to entice the blackhole nodes. The basic working is that, the source node asks for the path to the network about the destination which is a node from its neighborhood at a one hop distance. The system is triggered only when there is an alarm about something malicious is happening in the network. It means when the source node gets multiple RREP packets from the paths other than the path of the bait node then it is definitely coming from a malicious node. Now a reverse tracing program is triggered in which the path from source to the destination is divided into two paths i.e. temporary trusted path and the non-trusted path. These paths are calculated from the next node to the node which is sending the RREP packet. In reverse tracing, the source node sends a test packet and a recheck packet and goes to the promiscuous mode to listen to the network for the detection of the malicious node. This paper is also taken as the base paper for this research work. As the main drawback of this approach was that, it consumes lots of time and resources and also it has to discard the bait path permanently means we cannot send any data packet to the direction of the bait node because this side is not verified as the bait is chosen randomly.

Detection of cooperative blackhole attack using RIT table [10]

The routing information table is another approach which is very helpful in the detection of the cooperative blackhole attack. In this table, there are 3 columns named as From Node, Through Node and Through Any Trustful node. In the columns there are integer values where 1 stands for True and 0 stands for False. This table is created at each node having information of these three columns about each node in the

network presently available. The 1st column indicates whether the node has transmitted data from this other node previously or not. The 2nd column indicates whether the node has received data from this other node previously or not. The 3rd node indicates whether this other node has been used for data transmission by other trustful node or not previously. On the bases of these values the source node selects the other node for data transmission.

Detection of cooperative blackhole attack using DRI table [11]

In this paper, a Data Routing Information table is used which is stored at each node containing value to the columns From, Through and Check Bit. These columns are filled with values either 0 or 1 where 0 means false and 1 means True. The check bit column is filled with the help of sending a probe packet to a particular node and check if the node receives the packet or not and on the basis of this process the third value is given to the table.

Detection of cooperative blackhole attack using GAODV [12]

Gratuitous AODV is new approach to detect blackhole node. In this approach, the source node and the destination nodes use some control packets to detect the blackhole node as the RREP is generated by the intermediate node (IN), the IN not only send the RREP to the source but also generates a CONFIRM packet and send it towards the destination. When the destination receives the CONFIRM packet from the IN, it then waits for the CHCKCNFRM packet from the source. After receiving these two packets, the destination replies to the source by unicasting a REPLY CONFIRM packet. Now all these new control packets carry some important information. Since, the blackhole node does not know the actual location of the destination, it cannot send a CONFIRM packet towards destination and when the destination receive only CHCKCNFRM packet from the source and do not get any packet from the IN it do not forward the REPLYCONFIRM packet to the source and that is how the blackhole node is detected. Now these new control packets store the information regarding the source address and the id of the IN. These addresses are used to detect malicious nodes in the network.

Detection of cooperative blackhole attack using Clock Synchronization and Relative Velocity Distance [13]

For the detection of cooperative blackhole nodes, broadcast synchronization method is used in this paper. Basically, all the clocks are synchronized with each other. The internal clock time of the network is compared with the external time clock and both the times are compared with the standard threshold time clock given that the clock time of a node is always greater than the threshold time during initialization. There are three new control packets are used, packet time clock source, packet time clock destination and standard threshold time for request and response. There is another method imposed for detection of blackhole nodes because sometimes the clock synchronization method fails when worms are present in the network. This new method is, calculating the relative distance from the source to the destination and making it the threshold distance and then comparing it with the actual distance from the source and the destination. Some normal cases and abnormal cases are explained as an example to explain these two methods for the detection of the cooperative blackhole nodes in the network.

A novel approach for blackhole node detection using MDE [14]

In (MDE) Malicious node Detection and Elimination technique, when for the first time the node is receiving beacon, it compares it with the other beacon signals received from all the neighbours and check if the destination address is changed or not. If the destination address is changed then the last address of the node from the beacon is changed to malicious and all the other nodes are notified. After the updation, a new MN address (non-mutable) field is added to the beacon with the property that the data in this field can only be updated and can never be altered. Based on this property the changed destination addresses of the nodes are analysed for detection and removal of the blackhole nodes from the network. For authentication purpose, the concept of public key and private key is used.

A new approach for blackhole detection [15]

In this paper, the concept of the data routing information table is used for the detection and prevention of the blackhole node. The final step of the process is modified from the former approach. When a node sends a RREP packet back to the sender, it adds two extra addresses i.e. Next Hop Node (NHN) and Previous Hop Node (PHN) along with the packet with their DRI values inside the packet. These DRI values are checked for the value to be 1 in at least Through part of the routing

table column and if it is 0 then there must a 1 value in the From part of the routing table column. If any of the values are 0 then the RREP generator node has to send a data packet to the NHN or PHN based on their value to convert it into 1 means YES means the communication did takes place. When both the values are 1 only then the RREP node sends the information back to the sender for data route creation.

Detection of cooperative blackhole attack using cross checking with true link [16]

It is another data routing information table based approach with a slightly changed crosschecking mechanism. In this approach, using rendezvous phase a nonce key is shared i.e. two random numbers are shared among nodes where RREP packet is generated. Based on the time constraint, the neighbouring nodes enters the values in the DRI table which haven't received the acknowledgment 0 or 1. After getting entries in the DRI table by the adjacent nodes, these values are verified using link verification method i.e. by sending ECC signature and two-nonce. The timing constraints of the rendezvous phase make the true link immune for capturing of the cooperative blackhole attacks.

A behavioural approach to detect malicious nodes in MANET [17]

It is a support vector machine (SVM) based approach where SVM receives set of input data and the behaviour of the nodes is observed. Terminologies used are packet delivery ratio (PDER), packet modification ratio (PMOR) and packet misroute rate (PMISR). For the detection of the malicious nodes, the system detects the behaviour of the nodes based on these mentioned values and with the help of SVM classifier the nature of the nodes is classified, integrating with the MANET. Firstly, collect all the metrics and save it as XML file. Then extracting the XML files using DOM (Dynamic Object Module) and uses these values as input for SVM. Now, if PDER>=0.3 AND PDER<=0.5 AND PMISR>=0.2 then the node is behaving abnormally. These are the threshold values that were calculated before.

Anomaly based intrusion detection of the blackhole node in MANET [18]

In this new approach, a monitoring node is used for the detection of the abnormalities in the network and detecting the malicious nodes based on the observations. There are some basic rules which are needed to be followed in order to execute this approach. Firstly, the monitoring node holds a unique ID so that it can easily be distinguished

from the other nodes in the network. It can cover all the nodes in the neighbour. It observes the behaviour of the neighbouring nodes at the network layer with the help of anomaly based intrusion detection. If the malicious node is encountered, it alarms the other nodes in the network. A monitoring node can never be malicious node, means sender can at least trust these nodes. The detection process of the malicious nodes is very simple. As the monitoring node has the power to monitor the whole topology of the network, it checks regularly whenever some data packets are travelling inside the network, the packet at each node before receiving and after forwarding is observed and compared. If the packet has a slightest change, the monitoring node intimate it to the sender and the packet is resend and that node is captured. If this step is successfully executed it means that the packet is safely reached at the destination.

Secure routing to prevent blackhole attack in MANET [19]

It is the one of the most easy to understand approach where a simple logic can help us to detect malicious node in a mobile adhoc network. The nodes are using the promiscuous mode to overhear the other nodes to check whether the packet is received or not. When a node replies to a route request packet then the node prior to the RREP node sends a plain data packet to the next to next hop of the RREP node and goes to the promiscuous mode to check whether the packet has been transferred to that node or not through the RREP generating node. If the plain data packet is not present at the next to next hop then the RREP generator node is malicious else the node is clean. The flow chart and the algorithm with graphical simulation of the output are given to make it clearer to understand.

Trust based security schemes a review [20]

In this paper several trust based research papers are collectively explained along with the details of how the trust is actually created among nodes in a mobile adhoc network and how this value is used for future data transmissions. Basically, the nodes have to trust the other nodes initially and then on the bases of their efficiency a trust value is given to the nodes for future use. As we go through this paper, we get to learn more about the authors that how they came up with the modifications in the traditional approaches.

Securing the data packets using asymmetric keys for data encryption and decryption [21]

In this paper, using the feature of clustering, each node generates its public and private keys and sends only public key to the cluster head. When the process of communication starts, the sender node first conveys the message to the cluster head and asks for the public key of the destination node. If the destination node is also in the same cluster then the work is easier else the cluster heads communicate with each other to get the public key of the destination node and sends it to the source node. The source node encrypts the data using this public key and send it to the cluster head on the other side, the destination node uses its own private key to decrypt the message and hence the data is secure.

Permutation based detection of blackhole node in MANET [22]

In this paper Adhoc on-demand multipath secure routing (AOMSR) method is introduced. It is based on permutation acknowledgement which helps to detect blackhole node in the network. There are several paths between the source node and the destination node which all are used in this approach to find out the malicious node path. Basically a data structure is added to the message header to send this message to a particular path which is one of the paths to the destination. The above approach is explained with the help of 3 alternative paths and choosing the best secure path among them. The data structure is, path number (PN), permutated acknowledgement number (PAckN), total number of paths (NP) and type of message (ToM). The sender sends each path a message with its PN and PAckN along with it. When the destination receives these messages, it stores all the relevant entries in the table and via pre-decided paths sends back the permutated acknowledgement. The sender node re-checks all the values to see if the values are received correctly. If it is true then there is no malicious node in the paths. But if there are some changes in the values then there must be a malicious node in the path which can be figured out with the help of PN number. The algorithm for the above approach is mentioned with the detailed description of its working explained.

Secure knowledge algorithm for black hole detection in MANET [23]

In this approach, every node in the network listens to the neighbouring nodes in the promiscuous mode. Each node observes the behaviour of the other nodes in order to see if the data packets are transferred in good health or not. The information is compared with the information stored in the knowledge table at each node. These two values must be same in order to confirm that the node is legitimate node. If the values are not same then the given node waits for a particular amount of time and tries to find out the reason of packet dropping. The reason can be figured out with the help of the algorithm given in the paper. The node is declared as malicious if the threshold is reached due to packet dropping. Also the node checks whether the next hop node is the destination node or not and TTL value is also checked in order to wait for the packet to arrive due to delay.

Securing network layer using C-Scan energy efficient protocol [24]

A previously introduced E2-SCAN scheme is modified into Conditional-SCAN with a new strategy for the token renewal. In this approach, promiscuous mode is used by all the nodes to hear the other nodes. Monitoring activities takes place among the nodes in the network. To gain the network access each node needs to have a token with a valid sign with the fields: OWNER ID, SIGNING TIME and EXPIRATION TIME. When a node wants to renew its token, it sends a token request (TREQ) packet containing old token ID and the current timestamp to the neighbouring nodes.

Detection of cooperative blackhole attack using MEDRI table [25]

Modified Extended Data Routing Information table, a modification in the DRI table is done in this paper in order to enhance the capability of the blackhole node detection and providing more promising security to the network. In this MEDRI table, we have eight fields with two older and six new fields. The third column is CTR means counter. The purpose of this column is to count how many times the node has behaved maliciously. The fourth column is BH that indicates the latest reaction of the node either malicious (1) or not (0). The fifth column is Timer, that will be used to consider a node malicious or not. The sixth and seventh columns are used for calculating the data packet size at the source and at the destination, respectively. The last or the eighth column, which is Result, uses a Boolean value (Yes/No) for the result of the comparison of the previous two fields. On the basis of these values a malicious node is detected in the network.

CHAPTER 3

PRESENT WORK

Present work provides an improvement in the detection of the malicious nodes by using a simpler method. The blackhole attack does a serious damage to the network as the data packets are lost forever they cannot be revived. To avoid such problems and also keeping the overhead low we have provided another approach to detect and prevent blackhole node attack in mobile adhoc networks.

3.1 Problem Formulation

There are lots of new approaches and terminologies to detect blackhole node in a Manet. Most of these approaches include delay in terms of route discovery and more overhead due to increase in the control packets used for the detection of the blackhole node. While some approaches provide less utilization of resources but their improvement in the detection of the malicious node is not up to the mark.

In a CBDS approach [9], the source node uses one of its neighbouring nodes as the bait to entice the malicious nodes. As the bait is used as the destination address and the source broadcasts its ID to get RREP from the other nodes. As we already know which nodes can send the reply to the RREQ the other nodes which reply to this packet comes under the surveillance. Now the detection of such nodes is done with the help of the reverse tracing technique. The drawback of this approach was that it totally negates a particular path for the data transmission for the future use from which it selects the bait node as this area of the network is not validated by the source node. The other drawback of this approach was that it do provides a better result as compared to a normal scenario but it also increase the overhead a little bit.

3.2 Objectives of the Study

After considering the whole scenario, our main aim is to develop an enhanced methodology for the detection of the malicious nodes with the help of less control packets to reduce the overhead from the network and having more suitable environment for the legitimate nodes. Our research is focused on following objectives.

- To analyse the existing algorithm for drawbacks and limitations and providing solution.

- To develop the enhance technology for black hole detection to detect malicious nodes with the help of threshold values with less overhead.

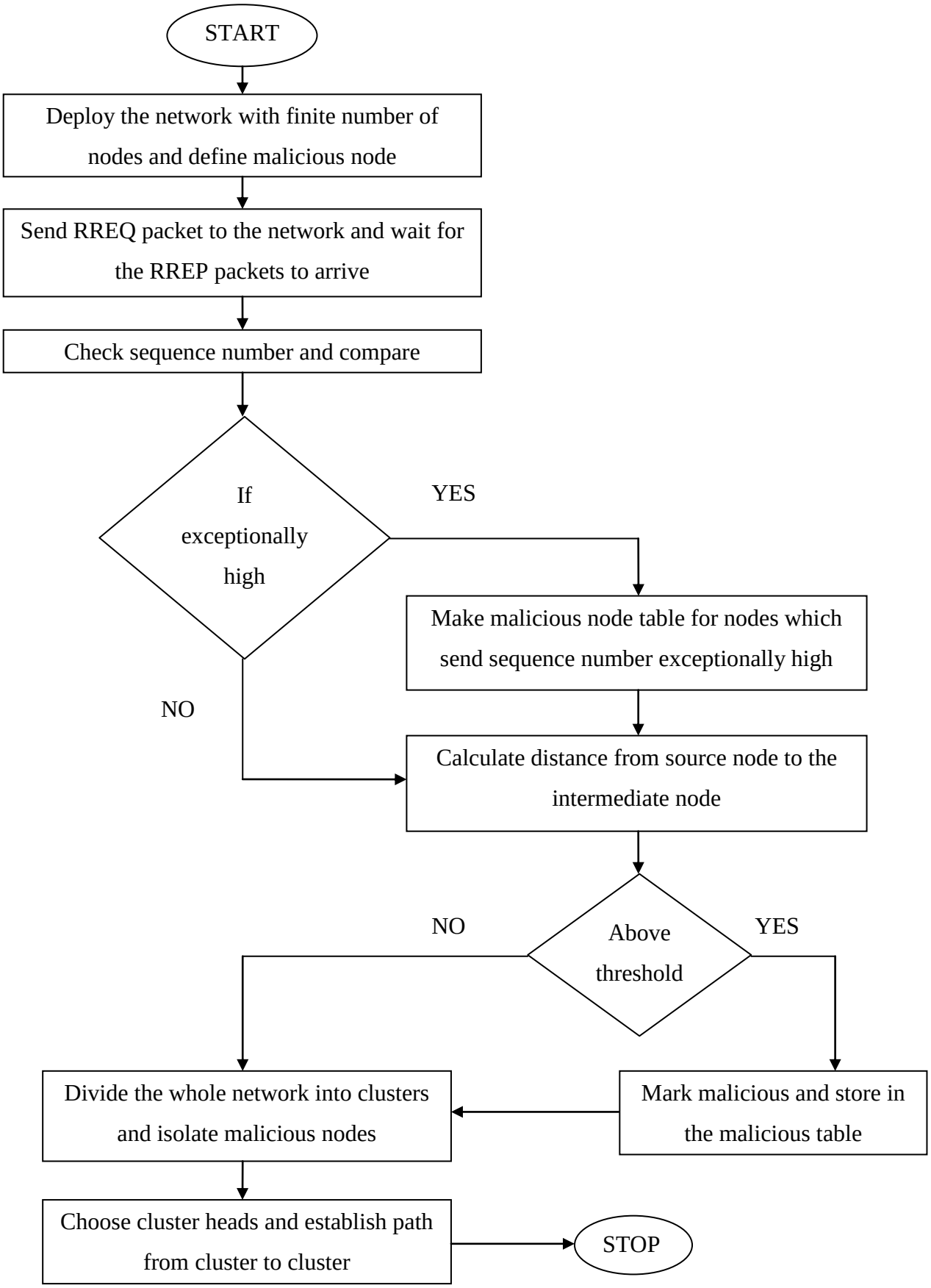
3.3 Research Methodology

As we know that a blackhole node always give fake shortest path towards the destination by replying a less hop count and maximum random sequence number so that it gets shortlisted for route discovery process and as the nature of the AODV protocol is that it always prefers the route which is having less hop counts and highest sequence number and this comparison is made only with the first two or three RREP packets arrived. So the blackhole node in order to get selected for the packet transfer sends a very high sequence number to the source. This sequence number is exceptionally high and we set a threshold value and compare the sequence number of the node with the threshold value. If the value increases the threshold then the node is listed as the blackhole node and is stored in the malicious table.

The next step is to check whether the node is closer to the source node or not. As we know that there are only two types of nodes which can send a RREP packet. It is either the destination node itself or a node which is at a one hop distance from the destination or the neighbouring nodes. As the whole simulation is done under certain limited area we can easily find the coordinates of the nodes in the network and we can check the distance of the IN with respect to the source node and with the help of Euclidean Distance Formula, the distance is calculated and compared with the threshold value which is calculated earlier. If the distance is less or if the IN is closer to the source node then the node is listed as the blackhole node and stored in the malicious table.

The third step is to divide the network into clusters and do not let the any of the node present in the malicious table to be the cluster head. As we know that the data transmission in clustered network is only done with the help of the cluster heads so the isolation process is done by not allowing the malicious nodes to become the cluster head of any cluster.

3.4 Flow Chart



CHAPTER 4

RESULTS AND DISCUSSIONS

Here is a normal scenario where the source and the destination nodes are defined and they start the data transmission by sending route request packet. We are using network simulator 2 as a tool for the simulation of the proposed algorithm. A network animator is used to graphically show how the nodes actually move and fall inside the range of the other nodes and starts sharing data packets by requesting and accepting the route request. The route request is shown with circles that tend to expand up to their limit i.e. the range of a node and neighbouring nodes are identified.

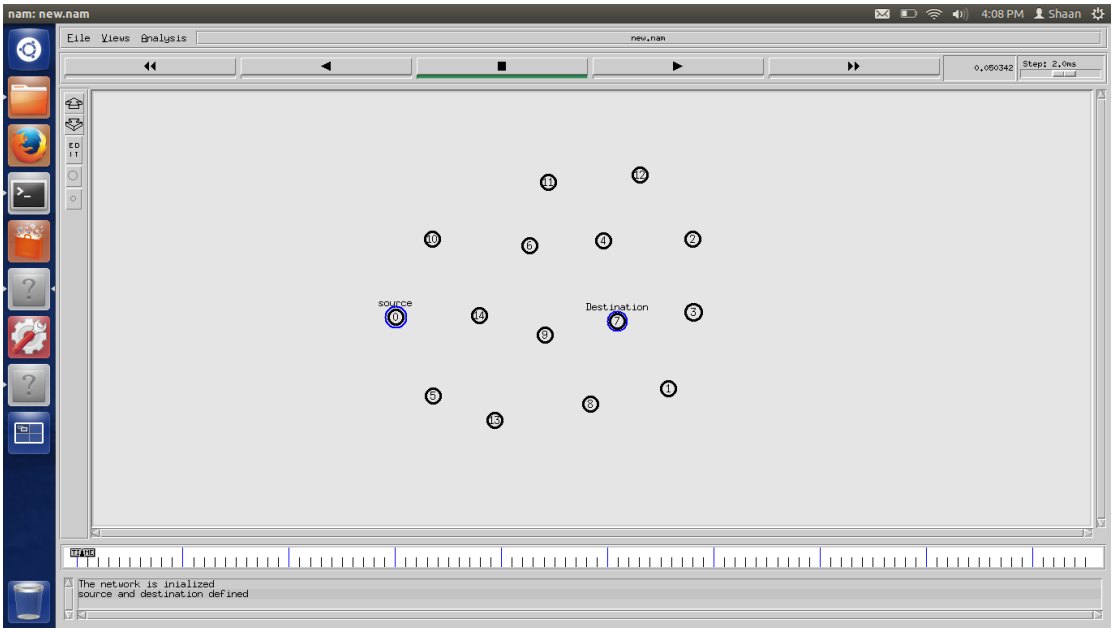


Figure 4.1: Network overview

The malicious nodes are defined in the network and it is observed that they are dropping the data packets and not forwarding them to the next node. With the help of our algorithm the nodes are detected and once the malicious nodes are detected they got isolated from the network, means the other nodes stop the communication with these nodes as shown below. The malicious nodes are highlighted with orange squares boundary line around them and an alert has been generated to notify other nodes to stop communicate with the malicious node.

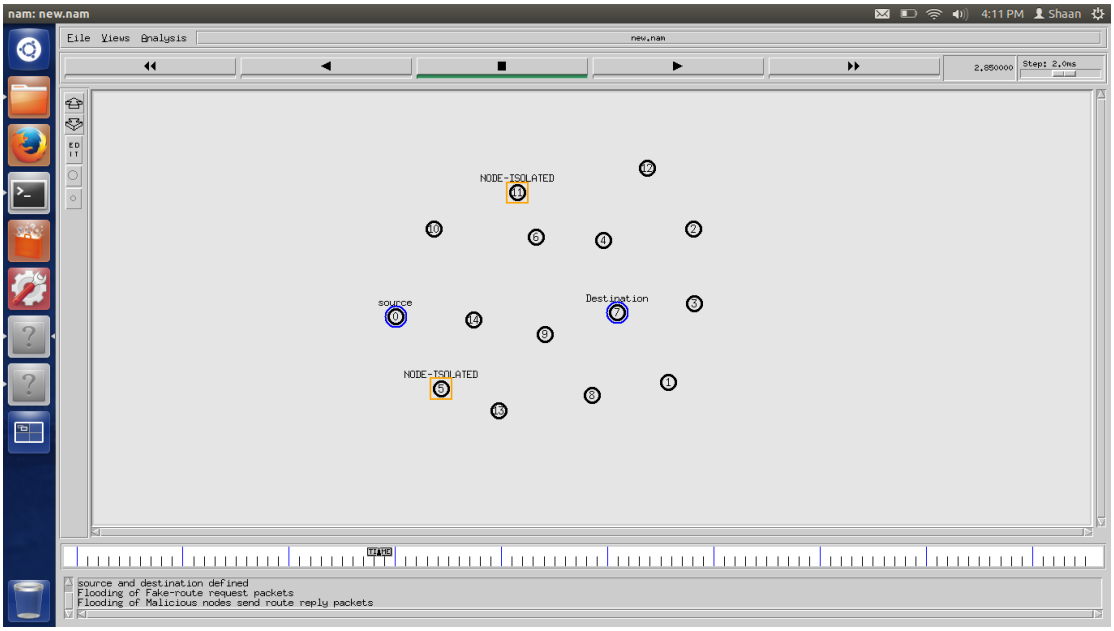


Figure 4.2: Isolation of malicious nodes

After the malicious nodes are being isolated, the clustering of the network is done in order to keep the malicious nodes isolated from the network. The large black circles indicate the range of the nodes which expands to their limit. The different colours are used to indicate different type or the category of nodes.

The little dots in the figure below are the data packets that actually carry the data and travels through the network. We can determine their direction of moving by simply reducing the simulation speed of the network which is given at the top right corner of the network animator (NAM).

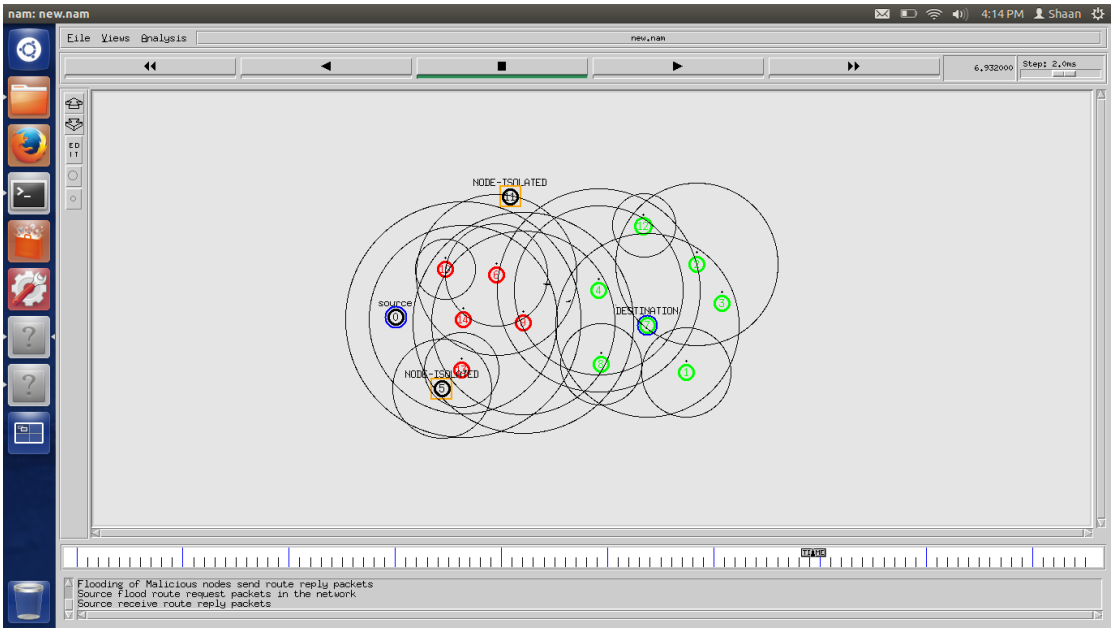


Figure 4.3: Clustering of the network

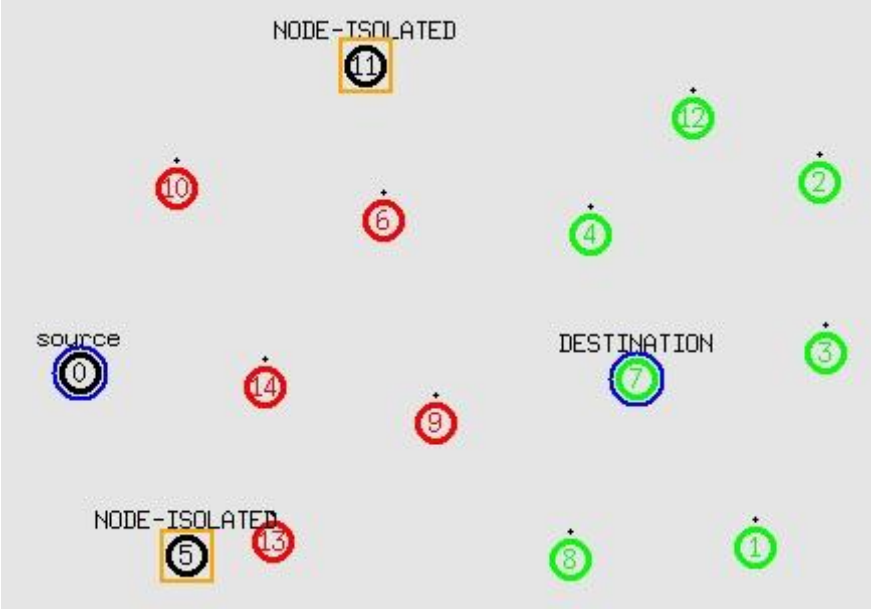


Figure 4.4: End of Simulation

As we can see clearly there are two clusters red and green, the source node belongs to the red cluster and destination node belongs to the green cluster. The isolated nodes are moved away from the cluster, even if they move inside they will still not be used as a path for data transmission.

4.1 Comparison with Existing System

The comparison between the two systems can be made graphically. There are some performances parameters on the basis of which we can decide whether the proposed approach is better or not. So we have compared the results of the two scenarios in the terms of all the performance parameters.

4.1.1 Packet Loss

The PDR is defined as the ratio of the total data packets arrived at the receiver divided by total number of data packets actually sent by the sender. Average PDR is the average of all the PDR values received at all the receivers in the network.

Here the packet loss value is observed instead of packet delivery ratio as both these values are used to find out how many data packets are actually received and how many data packets are lost during data transmission. The packet loss value is nothing but the opposite value of the packet delivery ratio or vice-versa.

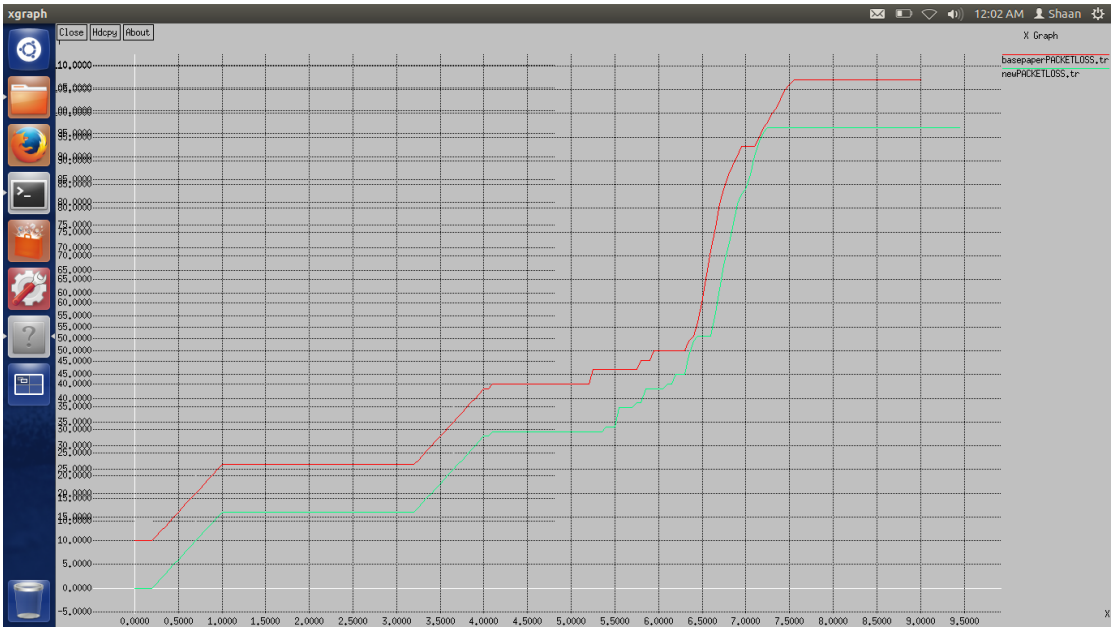


Figure 4.5: Graphical comparison of packet loss

As we can see above, the packet loss as compared to the CBDS approach is less in our approach. More packets arrive at the destination means more is the packet delivery ratio of the network. Red line indicates the CBDS and Cyan line indicates our approach.

4.1.2 Delay

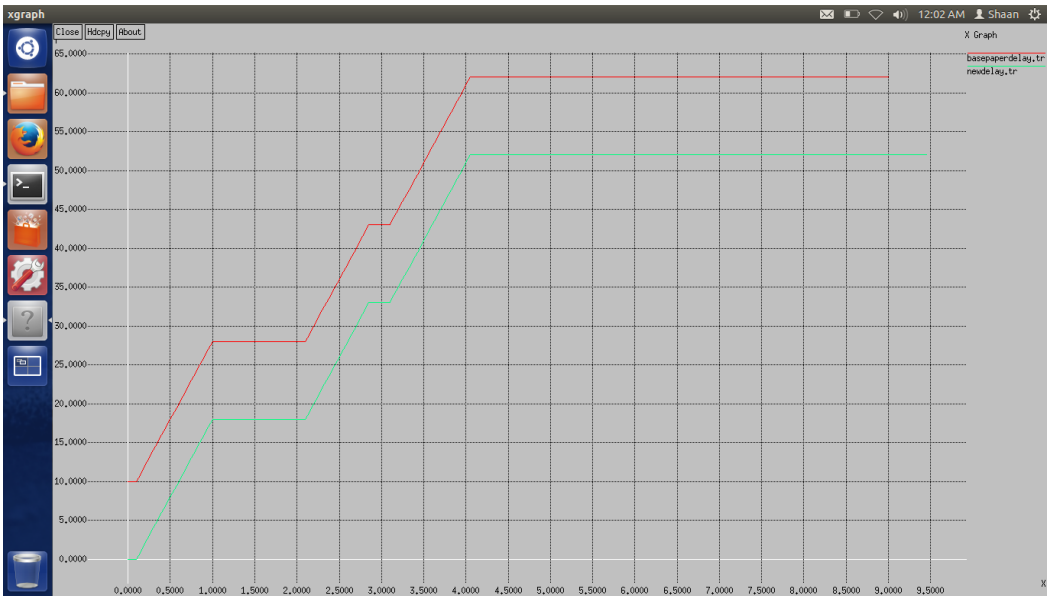


Figure 4.6: Graphical comparison of delay

The delay of the data packets in terms of time is less in this methodology as compared to the CBDS approach. Red line indicates the CBDS and Cyan line indicates our approach.

4.1.3 Throughput

The Throughput is the total number of data bits received divided by per unit time. The time could be in seconds or minutes or any other time unit. Average throughput is the average of all the received throughputs in the network.

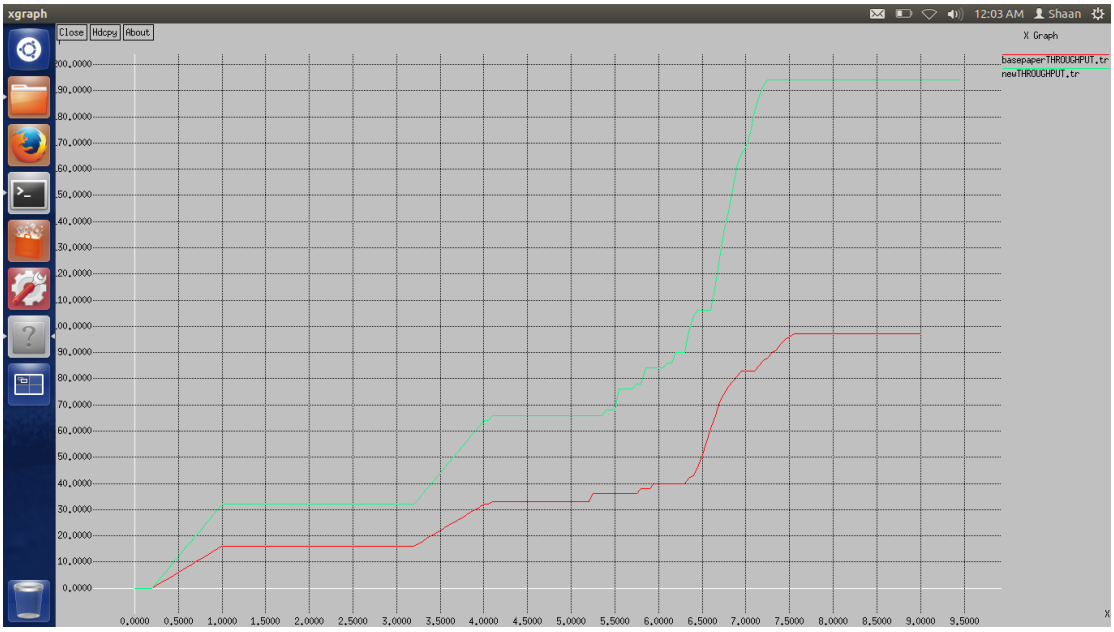


Figure 4.7: Graphical comparison of throughput

As we can see clearly the throughput of the network is increased as compared to the old scenario. Red line indicates the CBDS and Cyan line indicates our approach.

CHAPTER 5
CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

Our new approach is better than any other approach which is based on the threshold value detection of the malicious nodes in the mobile adhoc networks. For a successful implementation of the approach we need to install NS2 in any version of ubuntu or linux environment or we can also use some software that can virtually install the linux in our windows e.g. VMware. There is no need to use extra resources in the network.

The conclusion is that, this approach provides an efficient way to detect malicious nodes in a network at a very less cost. We can secure our systems from the attackers and it is very easy to implement.

5.2 Future Scope

For future, we can modify the clusters for better selection criteria of the cluster heads while here it is chosen randomly by isolating the malicious nodes. The future scope of this project is simple, this approach has very less complexity so it is very to understand and it do not require the use of additional control packets as compared to other approaches.

REFERENCES

[1] BOUNPADITH KANNHAVONG, HIDEHISA NAKAYAMA, YOSHIAKI NEMOTO, and NEI KATO, "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS," 2007.

[2] Hoang Lan Nguyen and Uyen Trang Nguyen, "A STUDY OF DIFFERENT TYPES OF ATTACKS IN MOBILE AD HOC NETWORKS," *25th Canadian Conference on Electrical and Computer Engineering (CCECE)*, p. 6, 2012.

[3] Rakesh Ranjan, Nirnemesh Kumar Singh, and Ajay Singh, "Security Issues of Black Hole Attacks in MANET," *International Conference on Computing, Communication and Automation (ICCCA2015)*, 2015.

[4] Kriti Patidar and Vandana Dubey, "Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks," 2014.

[5] Ashish Kumar Jain and Vrinda Tokekar, "Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in Mobile Ad Hoc Networks," *2015 International Conference on Pervasive Computing (ICPC)*, p. 6, 2015.

[6] Pooja and R. K. Chauhan, "AN ASSESSMENT BASED APPROACH TO DETECT BLACK HOLE ATTACK IN MANET," *International Conference on Computing, Communication and Automation (ICCCA2015)*, p. 6, 2015.

[7] Nidhi Choudhary and Dr. Lokesh Tharani, "Preventing Black Hole Attack in AODV using Timer-Based Detection Mechanism," *SPACES-2015, Dept of ECE, K L UNIVERSITY*, p. 4, 2015.

[8] Ermanno Guardo, Giacomo Morabito, Girolamo Catania, Agatino Mursia, and Ferdinando Battiati, "BRAVO: A Black-hole Resilient Ad-hoc on demand distance Vector rOuting for tactical communications," *2014 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, p. 2, 2014.

[9] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious Nodes in

MANETs: A Cooperative Bait Detection Approach," *IEEE SYSTEMS JOURNAL*, vol. 9, p. 11, March 2015.

[10] Ms. Gayatri Wahane and Ms. Savita Lonare, "Technique for Detection of Cooperative Black Hole Attack in MANET," *IEEE - 31661*, p. 8, July 2013.

[11] Ankur mishra, Ranjeet Jaiswal, and Sanjay Sharma, "A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network," p. 6, 2012.

[12] Sanjay K. Dhurandher, Isaac Woungang, Raveena Mathur, and Prashant Khurana, "GAODV: A Modified AODV against single and collaborative Black Hole attacks in MANETs," *2013 27th International Conference on Advanced Information Networking and Applications Workshops*, p. 6, 2013.

[13] Harsh Pratap Singh and Rashmi Singh, "A Mechanism for Discovery and Prevention of Coopeartive Black hole attack in Mobile Ad hoc Network Using AODV Protocol," p. 8, 2014.

[14] Vaithiyanathan , Gracelin Sheeba. R, Edna Elizabeth. N, and Dr. S. Radha, "A Novel method for Detection and Elimination of Modification Attack and TTL attack in NTP based routing algorithm," *2010 International Conference on Recent Trends in Information, Telecommunication and Computing*, p. 5, 2010.

[15] Ali Dorri and Hamed Nikdel, "A New Approach for Detecting and Eliminating Cooperative Black hole Nodes in MANET," *IKT2015 7th International Conference on Information and Knowledge Technology*, p. 6, 2015.

[16] Gayatri Wahane, Ashok M. Kanthe, and Dina Simunic, "Detection of Cooperative Black Hole Attack using Crosschecking with TrueLink in MANET," p. 6, 2014.

[17] Meenakshi Patel and Sanjay Sharma, "Detection of Malicious Attack in MANET A Behavioral Approach," p. 6, 2012.

[18] Shivani Uyyala and Dinesh Naik, "Anomaly based Intrusion detection of Packet

Dropping Attacks in Mobile Ad-hoc Networks," *2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, p. 4, 2014.

[19] Ashutosh Bhardwaj, "Secure Routing in DSR to Mitigate Black Hole Attack," *2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)*, p. 5, 2014.

[20] S. Sivagurunathan and K. Prathapchandran, "Trust based Security schemes in Mobile Ad Hoc Networks – A Review," *2014 International Conference on Intelligent Computing Applications*, p. 5, 2013.

[21] Adel ECHCHAACHOUI, Ali CHOUKRI, Ahmed HABBANI, and Mohamed ELKOUTBI, "Asymmetric and Dynamic Encryption for Routing Security in MANETs," p. 6, 2014.

[22] Dhaval Dave and Pranav Dave, "An Effective Black Hole Attack Detection Mechanism using Permutation Based Acknowledgement in MANET," p. 7, 2014.

[23] Ayesha Siddiqua, Kotari Sridevi, and Arshad Ahmad Khan Mohammed, "Preventing Black Hole Attacks in MANETs Using Secure Knowledge Algorithm," *SPACES-2015, Dept of ECE, K L UNIVERSITY*, p. 5, 2015.

[24] Sanjay K. Dhurandher, Isaac Woungang, and Issa Traore, "C-SCAN: An Energy-Efficient Network Layer Security Protocol for Mobile Ad Hoc Networks," *2014 28th International Conference on Advanced Information Networking and Applications Workshops*, p. 6, 2014.

[25] Vani A. Hiremani and Manisha Madhukar Jadhao, "Eliminating Co-operative Blackhole and Grayhole Attacks Using Modified EDRI Table in MANET," p. 5, 2013.