A Novel Approach to Defend Black Hole Attack in MANETs to Increase the Network Performance

[1]Mr. N Harsha, [2]Mrs. Anupama K C, [3]Dr. R Nagaraja

[1]Student, [2]Assistant Professor, [3]Professor & PG Coordinator
Department of ISE
BIT, Bengaluru

***Abstract*: Threat of attacks on mobile nodes is increasing because of infrastructure less network in Mobile Ad Hoc Networks (MANETs). Black hole attack is a threat where malicious node fallaciously advertises or broadcasts the good path to the node falsely during the route-establishment process to the destination node. When a request is received by the attacker to the destination node for a route it creates a reply for the short route and enters into the passageway to do something with the packets passing between them. If the Black Hole Node is present in the network, it will reduce the network performance along with the depletion of the energy in the network. The source node sends the data packet to the destination, the malicious node drops all packets intended for forwarding. The Ad-Hoc On Demand Distance Vector (AODV) routing protocol is used in the existing system to detect black hole attack. If a path identifies that it has a malicious node then the data packets are forwarded in the next best shortest path. Although it chooses the alternative path the data packets will be transferred with the constant bit rate which leads to delay in the network there by decreasing the performance.**

A Novel Approach to defend Black Hole attack in Mobile Ad-Hoc Networks (MANETs) to increase the network performance is proposed. When the black hole attack occurs, the MAC Protocol 802.11 b, g, will be tuned up by using the Adaptive algorithm which maximizes the Contention Window (CW) so that the data packets can be sent at higher speeds by which the delay in the network will be minimized. Due to this the proposed system is very advantageous in increasing the performance parameters like throughput, Packet Delivery Ratio (PDR).

***Keywords*: Contention Window (CW), Ad-Hoc on Demand Distance Vector (AODV), Mobile Ad-Hoc Networks (MANETs), Packet Delivery Ratio (PDR).**

CHAPTER 1

INTRODUCTION

The brief introduction of MANETs, architectural Model of MANETs, AODV routing protocol, Black-Hole attack, MAC protocol 802.11, existing and proposed system architecture including the limitation and advantages is discussed. The chapter also gives short description of organization of the report.

1.1 MOBILE AD-HOC NETWORKS (MANETs)

MANET is an ad hoc network which does not require any communication support for carrying data packets between two nodes in a network. MANET is an ad hoc network for mobile or also simply called as mobile ad hoc network which is a constant self-efficient, infrastructure-less network of mobile devices connected wirelessly. Mobile ad hoc networks acquire a flat network infrastructure. It has a mutual medium which is highly demandable for radio communication. In MANET architecture every computer or node indicates any device is a router as well as end host. The nodes or devices in the MANET architecture are in general independent. MANET has a dynamic topology structural design which highly promotes mobility. In the MANET architecture, each and every node works as a router since they route packets for other nodes [1].

1.2 AD HOC ON-DEMAND DISTANCE VECTOR

An Ad Hoc On-Demand Distance Vector is a routing protocol designed for wireless and mobile ad hoc networks. Unicast and multicast routing is supported by this protocol and also path is established to destination on demand. When source node requests, AODV protocol creates path between nodes. The path from source to the destination is maintained as long as it is required by the source. To connect multicast group members trees are created. To check route freshness sequence numbers are used by AODV. To find path to the destination AODV uses control messages. The types of control messages in AODV are discussed below.

1.3 BLACK HOLE ATTACK

In black hole attack routing protocol's liability is used by malevolent node and router drops the packets instead of receiving the packets. In AODV based network, RREP packet with high sequence number is generated by malevolent node as a response to RREQ packets. Source node chooses new route with malevolent node. Based on the number of malevolent nodes joining in network, there are three types they are: Single, Cooperative and Distributed black hole.

1.4 IEEE 802.11

IEEE is known has the Institute of Electrical and Electronics Engineers. The standard for wireless local area networks is IEEE 802.11 is a, which is followed by many vendors of WLAN products. The first digital wireless data transmitting standard, which deals with the physical and MAC layers in WLANs is the IEEE 802.11 [2].

1.5 EXISTING SYSTEM ARCHITECTURE

The architecture diagram of the Existing system is shown in Figure 1.4 where the nodes are represented along with its source, destination and its attacker's node.

While attacks, the attackers will launch Black-hole attack to compromise the authentic node. Source node is represented by node1 and the destination node is represented by node6 respectively as shown in Figure 1.4. Though node3 is a malicious

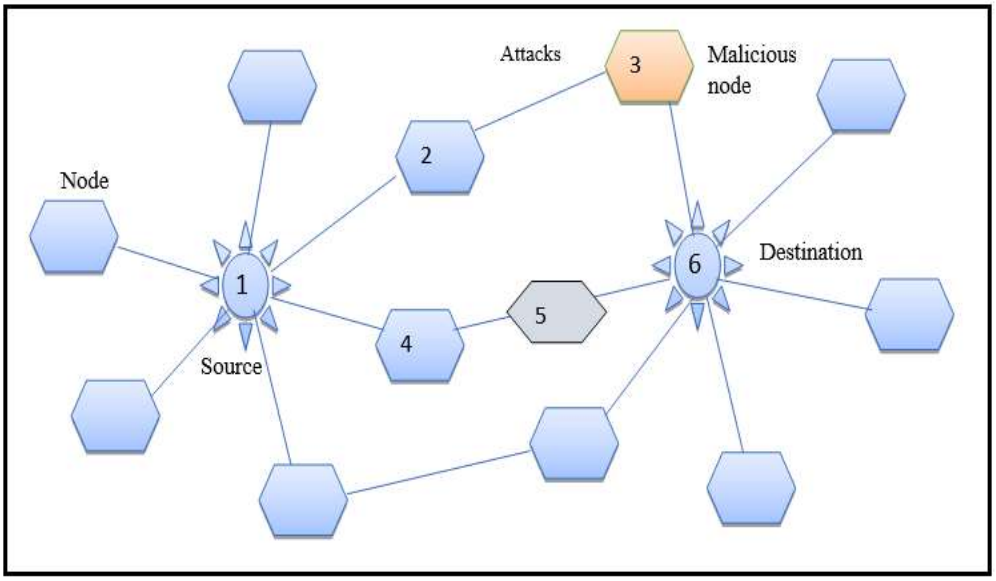

Figure 1.4: Existing Architecture Diagram

It quickly responds to RREQ and advertises to have the new and shortest route to destination. After receiving this malevolent RREP, node1 delivers data packets through the path claimed by the RREP. Then, node3 drops all the packets. Once the path through malicious node is selected by the source node which is spurious, without forwarding them to the next node in the network it absorbs data packets. Thus creating a black hole in the network where data packets sent to it are drained. Due to this effect network performance gets down drastically. In order to transmit data to destination when the attack occurs the AODV protocol chooses the next shortest path by sending the RREQ and RREP in the network. The data is transmitted at the nominal speeds due to which the delivery of the message is delayed and this leads to network performance degradation.

Limitation of the Existing System:

i. Network performance is degraded
ii. Increased Delay
iii. Reduced Packet delivery ratio
iv. Consumption of energy is more

1.6 PROPOSED SYSTEM ARCHITECTURE DIAGRAM

The project revolves around the concept of detecting and eliminating the black hole attacks over the network during data transmission. The AODV protocol is used to detect the misbehaviour node.

AODV helps in increasing the network performance and by eliminating the misbehaviour node in the network. After, eliminating the path containing the misbehaviour node, the packet is transmitted over the next path with shortest distance. The AODV routing protocol is used to determine the shortest distance to transmit the data. When the attack occurs in the network the MAC protocol 802.11b,g will be tuned up i.e, the Contention Window (Cmin & Cmax) to the maximum level using the Adaptive algorithm to speed up the process of data transmission. By this the total sum of the overall UTC[universal time] of the forwarders and therefore the total obstruction time of the obstruction host are going to be reduced ,and therefore by taking the neighbour data of the forwarders into consideration and can properly alter the data rates of the forwarders.

Advantages of the proposed system

i. Not only detects the attacked node but also eliminates that path and provides alternate shortest distance path to reach destination.
ii. Every node is related to a routing table that include all the information of routing of all the nodes. It will be considerably useful, in selecting the alternate nearest path.
iii. Network performance is improved.
iv. Reduced Delay & Increased packet delivery ratio.
v. Less consumption of energy.

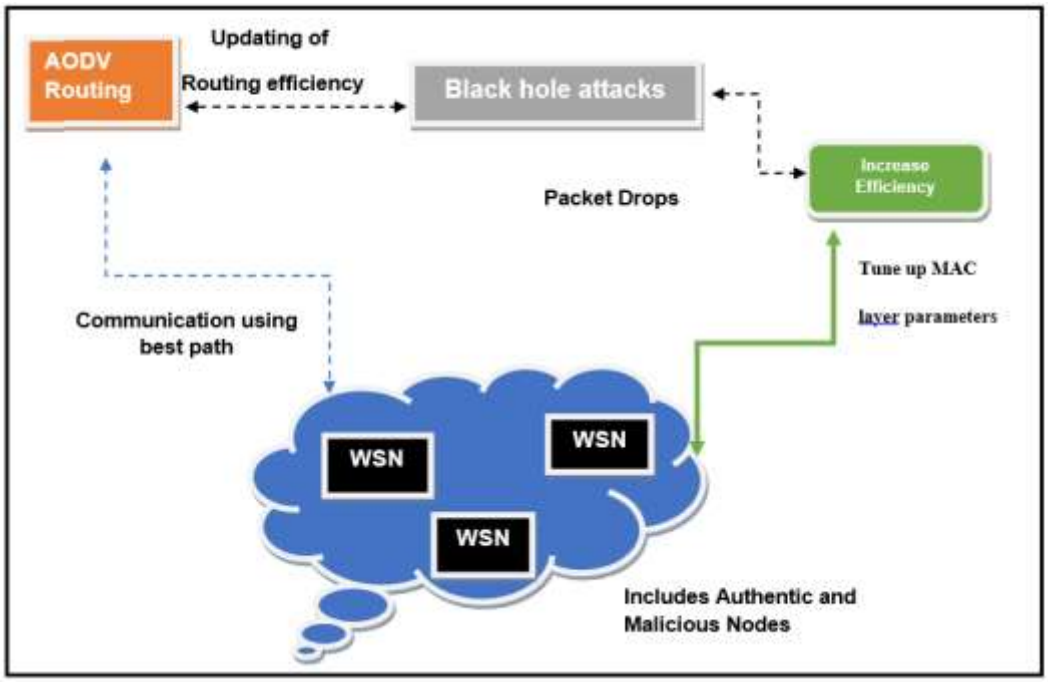

Figure 1.5: Proposed Architecture Diagram using AODV and MAC

CHAPTER 2

MOTIVATION AND PROBLEM STATEMENT

The ideas that motivates for this project and also the problem statement which includes malicious nodes which affects network performance like packet drops, delay, link break, deny message, fake routing, bandwidth consumption, message tampering, unavailability of nodes is discussed in this chapter.

2.1 MOTIVATION

Mobile ad-hoc networks are most useful in current environments. It requires high performance, network load and Throughput. In MANETs routing is the hot topic for the research. To increase the network performance of the MANETs while communicating with authentic nodes and to defend against the attackers, mutual coordination between the nodes which are participating in routing is required for correct operation of MANET. Network performance gets reduced because of participation of malicious nodes in routing. To conserve energy malicious nodes drops the packets received from neighboring nodes. Detection and isolation of malicious nodes need to be done to avert the delinquency. So Ad-Hoc On-Demand Distance Vector (AODV) routing protocol with adaptive algorithm is used to detect and isolate the malicious nodes and prevents malicious nodes from participating in the routing operation. Destination node sends alarm to source node to trigger the detection mechanism again when packet delivery ratio drops.

2.2 PROBLEM STATEMENT

The execution and utilization of wireless advances has expanded colossally, opening up roads for application in the less investigated territories. MANET is one vital field of worry, in which the portable nodes sort out themselves in a system without the assistance of any predefined foundation. MANET is utilized in basic applications where information and correspondence honesty is vital. MANETs are vulnerable to attack and detecting malicious nodes is difficult due to lack of centralized monitoring and infrastructure. Most of the existing systems have proposed on defending the single type of attack which reduces the efficiency of the network. The network gets more degraded when there are multiple attackers launching collaboratively which refers to more energy consumption of the nodes and increase in delay. Adhoc On-demand Distance Vector.

Malicious node behavior: The nodes which have predefined behaviors are called as normal nodes and the nodes who behaves unexpectedly or different kind of behavior such as packet dropping, injecting false information in messages are called as malicious nodes. Find that there is any malicious behavior than it is easy to detect malicious node. If a packet is send by the source node to the destination after a specific time and if any intermediate node response improperly, the source node continues the process again. Each nodes in this range maintains a list of sent and dropped packets and when number of dropped packets by a particular node exceeds from a certain threshold T max (maximum threshold value), the monitoring node in that range declares that node as misbehaving node since a malicious activity have already been observed in the network When a node fails to follow the security principles then it is considered as node is under attack. Such node exhibits the following behavior:

CHAPTER 3

LITERATURE SURVEY

Literature survey is one of the most efficient way of gathering the previous opinions and ideas which is related to the past studies and this is discussed in this chapter.

Rashmi et al. [1], proposed an Approach for Preventing Black-Hole Attack in MANETs a black-hole attack in the Mobile Ad-hoc network (MANET) is an attack occurs due to malicious nodes, which attracts the data packets by falsely advertising a fresh route to the destination. They have proposed a clustering approach in Ad-hoc On-demand Distance Vector (AODV) routing protocol for the detection and prevention of black-hole attack in MANETs

Neeraj Kumar et al. [2], proposed data dissemination protocol which is secure and energy efficient for WSN. From the available routes the best route is selected by defining the routing metric. Metric selects the route which consumes less energy which are very useful for increasing the performance of the network.

Shaiffu and Amandeep Kaur Virk [3], used IP backtracking in wireless sensor networks to identify and prevent black hole attack. Authentication of sender IP address of a packet is not done because IP is of trustworthy in nature.

Yu-Hsun Chen et al. [4], proposed delay sensitive protocol for network capacity enhancement in multirate MANETs, for the significant advances in wireless modulation technology. Some MAC standard such as 802.11a, 802.11b, and 802.11g can function with multiple data rates for QoS-constrained multimedia communication to utilize the limited resources of MANETs more efficiently.

Neelesh Gupta [5], proposed routing protocols for mobile ad hoc networks (MANETs) which have been explored widely. The work is targeted at finding a feasible route from a source to a destination without considering current network traffic or application requirements. Therefore, the network may easily become overloaded with too much traffic and the application has no way to improve its performance under a given network traffic condition. While it may be acceptable for data transfer, many real-time applications require quality-of-service (QoS) support from the network.

Dr. G. Padmavathi et al. [6] talked about the wide assortment of security assaults in remote sensor systems and the security instruments to deal with themselves from the assaults. Security objectives are classification, time synchronization, trustworthiness, secure limitation, validation, accessibility.

Zeng Yingpei et al. [7] recommend that Wireless sensor systems (WSNs) sent in unfriendly conditions is defenseless against clone assaults. In such assault, an enemy bargains two or three nodes, imitates them, and additions subjective number of reproductions into the system. In this way, the enemy can finish numerous inner assaults. Past arrangements on distinguishing clone assaults have a couple of downsides. At first, some of them require a focal control, which presents a couple of natural points of confinement. Second, some of them are deterministic and helpless against straightforward observer trading off assaults. Third, in a couple of arrangements the foe can without quite a bit of a stretch take in the basic observer hubs to begin brilliant assaults and shield copies from being distinguished.

CHAPTER 4

METHODOLOGY

The methods that are handling the system performance in a network are discussed in methodology chapter. To eliminate the attacks in the network and to increase the system performance different scenarios with the data flow diagram are explained. There are five modules they area topology module, node deployment algorithm, flow chart for the routing table formation, adaptive algorithm for the performance and attack module.

4.1 TOPOLOGY MODULE

The topology module involves in building wireless network topology which consists of mobile nodes, where every node operates with various channels.

The topology module has the five phases:

i. **Set up Wireless Network Topology:** The module consist of node configuration of each node, and topology creations of each topology.
ii. **Bandwidth and threshold:** Bandwidth will be assigned to every node in the network topology.
iii. **Identifying neighbours:** Euclidian distance concept is used to identify the neighbours for a particular node.
iv. **Specify the data packets, source, and destination:** Here the specification like the node which has to send the data and which node should receive the data will be done. And a node how much data it has to send along with the time will be specified
v. **Setting the start and end time of the simulator:** Here the Network simulator 2 start and end time will be specified. In Network simulator 2 the entire process takes place within the seconds. This process can be viewed with the help of NAM window at any time.

4.2 NODE DEPLOYMENT ALGORITHM

An algorithm of node deployment is used to randomly deploy the nodes in the network. The algorithmic flowchart used is shown in the Figure 4.2 which shows the work flow of the node deployment algorithm. Where the number of nodes and distance between nodes is the input to the algorithm once the input is given the next step is to check for the condition if the condition is no the process will stop if the condition is yes then the node will in the zero position and the process goes on and next the node id will be generated as i this process is continued until the condition is true. Finally a map will be created with the node id and position of the node, and the next step the increment process is called to continue this until a specific condition is met. The output will be node ID and node position.

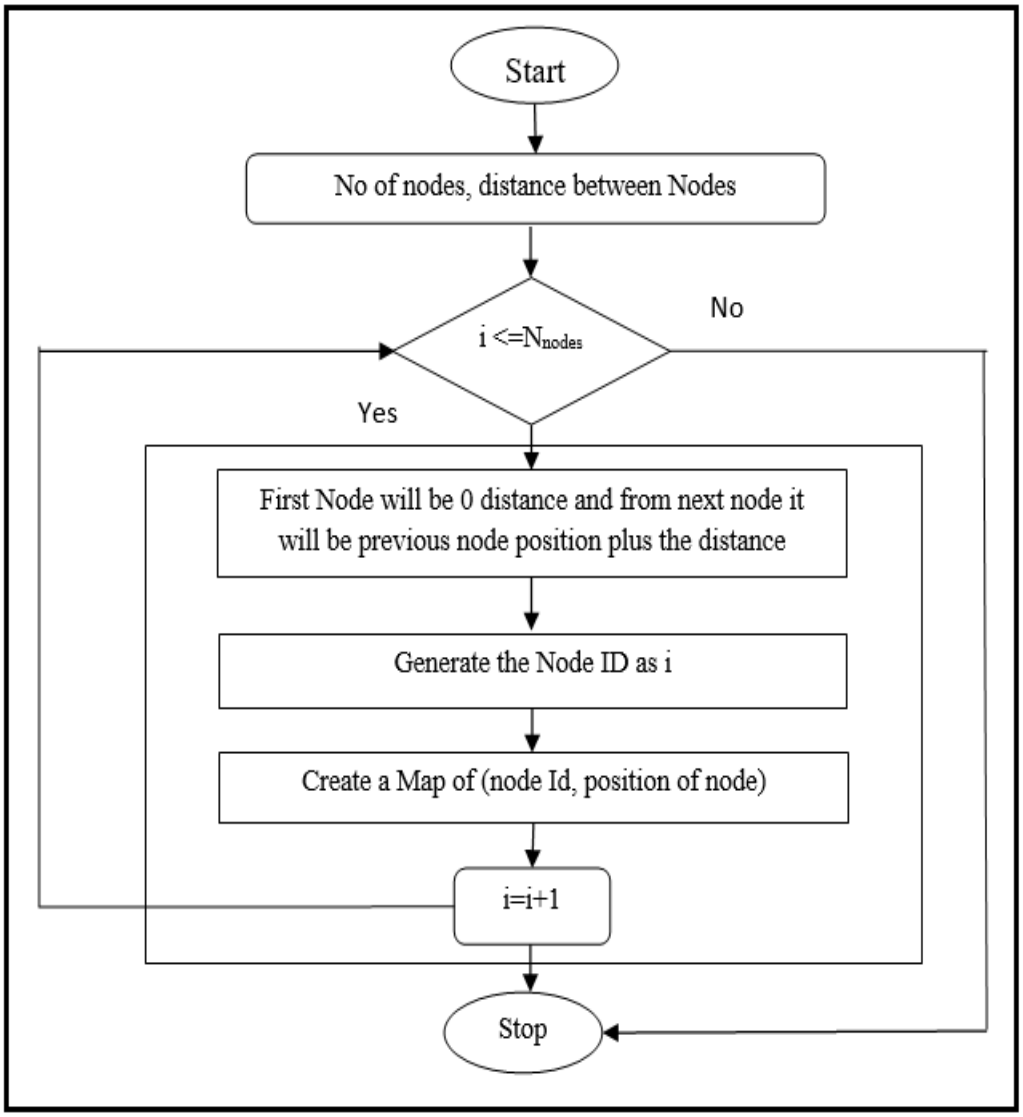

Figure 4.1: Nodes Deployment flowchart

4.3 FLOW CHART FOR THE ROUTING TABLE FORMATION

For the nodes to form the routing table where the routing table must contain the node id, distance, and flags. The routing table formation flowchart is shown in Figure 4.4. The first step is to start and the next step the input will be the node ids and the positions of the nodes and in the next step the condition will be checked if the condition is false the whole process will be stopped if the condition is true the routing table will be formed and the distances will be calculated between the nodes and these process is continues until a specific condition is met. To form a routing table in the manet the following steps should be followed.

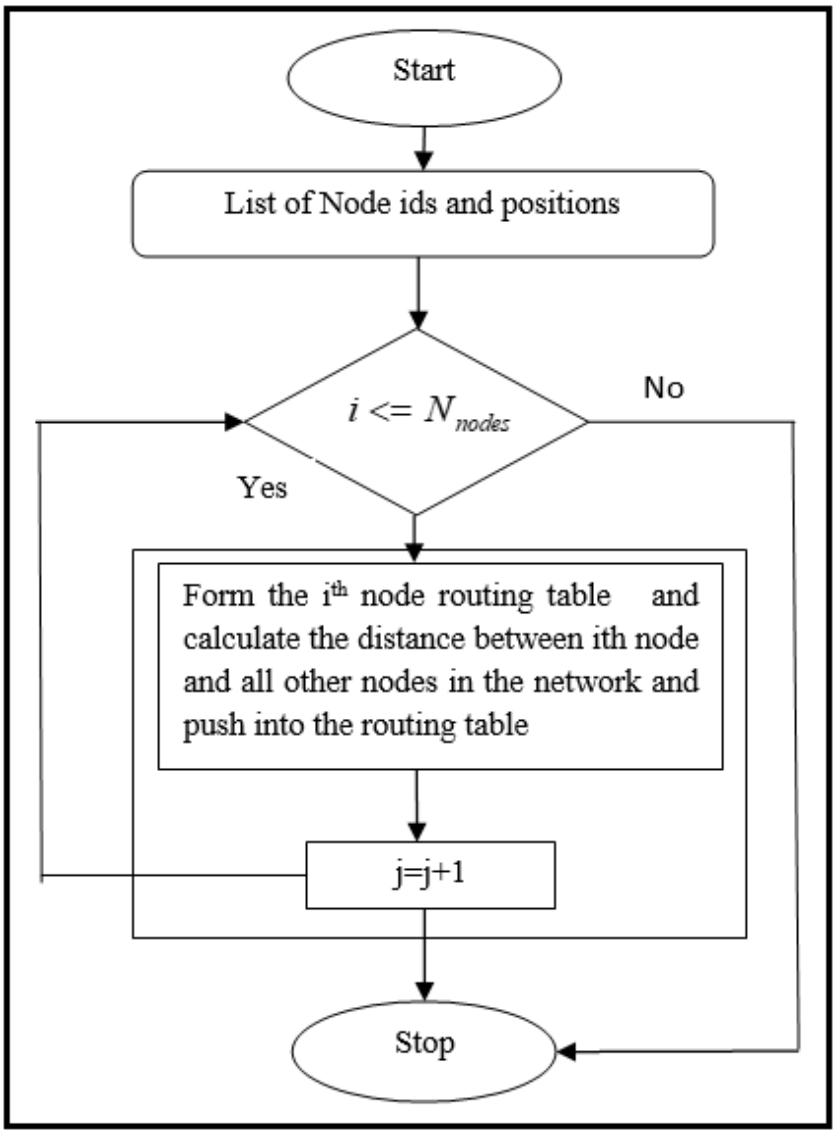

Figure 4.2: Routing Table formation flowchart

CHAPTER 5

IMPLEMENTATION

The procedure of how the proposed methodology is implemented in the network simulator is discussed in this chapter, and the software, tools required for the proposed system is discussed.

5.1 NODE DEPLOYMENT MODULE

The section contains functionality and explanation of the scripts which are being used in making topology. It includes creating Wireless Network topology, topology of nodes, here each node can work with different channels.

For the node creation a NodeClass is declared as a static and also it has the sub class TclClass as the public as shown in the Figure 5.1. The NodeClass() function is created as public so that it should be accessible for all the sub classes. For Tclclass the parameter "Node" is passed so that when ever in the code TclClass("Node") is called a new node will be created. In the TclClass("Node") Tclobjects are created with the int and const char, and in the end used return(new Node) to return the class. The tcl object is created to initialize for the tcl script and the const variable will be created with the integer datatype and the character datatype for the tcl script.

```
static class NodeClass : public TclClass
{
public:
        NodeClass() : TclClass("Node") {}
        TclObject* create(int, const char*const*)
        {
                return (new Node);
        }
} class_node;
```

Figure 5.1: Node deployment code snippet

5.2 ENERGY MODULE

The energy module is used to detect the node energy and the Figure 5.4 shows the energy module configuration code snippet where EnergyModelClass is declared as static class with the sub class TclClass as the public class. The EnergyModelClass () function is created as public so that it should be accessible for all the subclasses. For Tclclass the parameter "EnergyModel" is passed so that whenever in the code. TclClass the nodes energy will be calculated and shown for the argc the default value 8 is assigned for the mobile node class the n as an object is created, and when the argv value will be 4 the return function will be executed, i.e: the nodes energy will be recalculated.

```
static class EnergyModelClass : public TclClass
{
public:
        EnergyModelClass () : TclClass ("EnergyModel") {}
        TclObject *create (int argc, const char *const *argv) {
                if (argc == 8) {
                        MobileNode *n = (MobileNode*)TclObject :: lookup(argv[4]);
                        return (new EnergyModel(n, atof(argv[5]),
                                                atof(argv[6]), atof(argv[7])));
                }
                else {
                        Tcl :: instance().add_error("wrong arguments to errorModel");
                        return 0;
                }
        }
} class_energy_model;
```

Figure 5.2: Energy module configuration code snippet

5.3 ATTACK AND DEFEND MODULE

This module shows the code snippet of the how the attack is occurred and how it is defended.

```
void
AODV::rt_resolve(Packet *p) {
struct hdr_cmn *ch = HDR_CMN(p);
struct hdr_ip *ih = HDR_IP(p);
aodv_rt_entry *rt;
if(malicious==true)
{
drop(p, DROP_RTR_ROUTE_LOOP);
}
}
```

Figure 5.3: Attack code snippet

The attack module implementation code snippet is shown in the Figure 5.7. The void function is created with the AODV class, and the function rt_resolve(packet *p) is declared. If the *ch=HDR_CMN and the ih=HDR_IP the aodv_rt_entry will be called. And if (malicious==true) it executes the drop (p, DROP_RTR_ROUTE_LOOP); is executed which drops all the packets for the attacked node and the packets will be looped.

```
void
aodv_rtable::rt_delete(nsaddr_t id)
{
aodv_rt_entry *rt = rt_lookup(id);
 if(rt) {
    LIST_REMOVE(rt, rt_link);
    delete rt;
}
```

Figure 5.4: Defend code snippet

The defend module implementation is show in the Figure 5.8. The function is created as aodv_rtable class with the rt_delete(nsaddr_t id) this function will delete the route which contains the malicious node. And it will remove it by the function LIST_REMOVE (rt, rt_link) delete rt.

5.4 PERFORMANCE MODULE

The adaptive code to increase the performance is shown in the Figure 5.9. Where the MAC/802_11 is tuned up using the adaptive algorithm and its parameters CWMIN_15 is the contention window minimum size and it is set for 15. The CWMAX_1023 is the contention window maximum size and it is set for 1023. MaxPropagationDelay is set to 0.5 ms, the Data Rate is set for the 6Mbps as default. And also the slot time is defined.
The aodv_rtable class has the route delete function which deletes the route which is attacked and also LIST_REMOVE is also used to do same function.

```
Mac/802_11 set CWMin_ 15 ;
Mac/802_11 set CWMax_ 1023 ;
Mac/802_11 set SlotTime_ 0.000009 ;
Mac/802_11 set CCATime_ 0.000003 ;
Mac/802_11 set RxTxTurnaroundTime_ 0.000002 ;
Mac/802_11 set PLCPHeaderLength_ 40 ;
Mac/802_11 set PLCPDataRate_ 6.0e6 ;
Mac/802_11 set MaxPropagationDelay_ 0.0000005 ;
```

Figure 5.5: Performance module code snippet

5.5 HARDWARE AND SOFTWARE REQUIREMENTS

The various software environments and coding languages are used to set up the network, then data transmission or packet transmission, storing of network information, for the implementation platform independent languages is used, which are object oriented simple program algorithm implementation and network simulation are done by using the UBUNTU 11.10 software and the tool used is NS-2.35.

For the implementation platform independent languages is used, which are object oriented simple program, robust program, interactive program, easy to learn, dynamic and extensible.

5.5.1 Usage of C++ Language

The C++ language is used to write the functions and the classes for the project where the Node creation class is written and the object is created, energy class, encryption and decryption class and objects are created using the c++ language.

5.5.2 OTcl Script

OTcl (Object oriented Tool command language) is a part of tool language. It refers to object oriented extension of Tcl and it is a scripting language. OTcl is used to combine the TCL script and the c++ programs.

5.5.3 AWK Script – Reading trace file

AWK scripts are used to determine the performance of the network, the throughput.awk, E2E.awk, energy.awk are written in AWK script. The AWK scripts are used to search files for lines that consists specified patterns. Refer Annexure A 1.

5.5.4 Hardware Requirements:

Hardware requirements for the implementation of the project are. Any Processor with speed above 400 MHz, RAM: 2GB Min, Hard Disk: 20 GB.

CHAPTER 6

RESULTS AND DISCUSSION

The Results along with the graphs obtained from the proposed system which is implemented using the steps as mentioned in the methodology chapter is discussed in this chapter.

6.1 SNAPSHOTS

The hello packets transmission to the neighboring nodes is shown in the Figure 6.1 the Node 0 starts to send Hello packets and this process goes on till the node 38. This process is done to recognize all the nodes in the network.

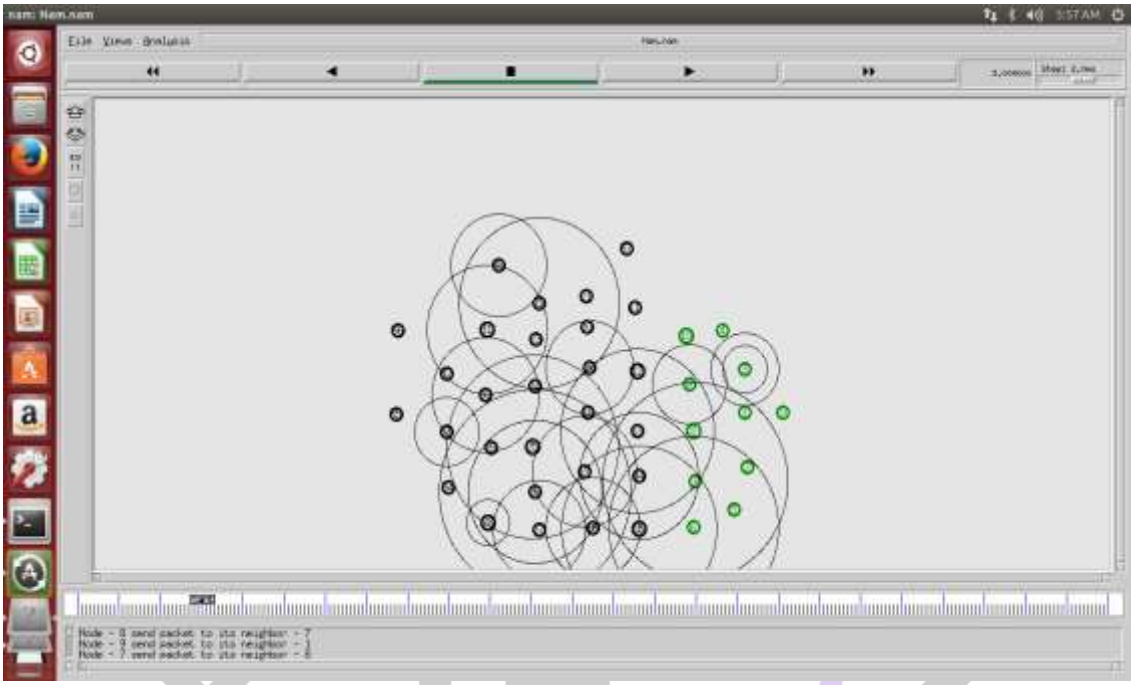

Figure 6.1: Hello packets transmission to the neighboring nodes

The route selection in the network is shown in the Figure 6.2. Once the source and destination node is selected in the network, the source i.e: the node 0 will start to send the route request to the destination, and from the destination end the route reply will be received then the AODV selects the shortest route i.e in the figure above the nodes with purple color indicates the route for data transmission.

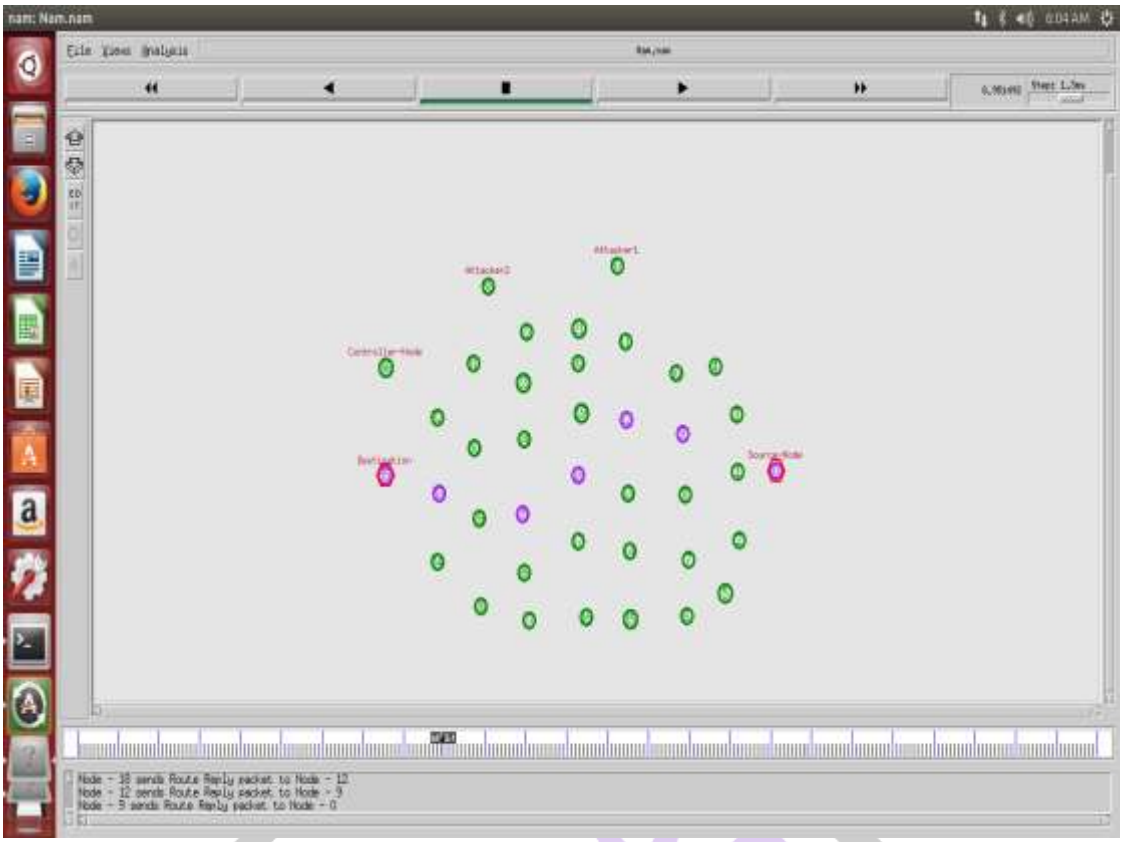

Figure 6.2: Identifying the first route

How the nodes are attacked and the packets are dropped is shown in the Figure 6.3 when the transmission starts the attacker node i.e., node 37 launches the black hole attack to the node12 and the node12 starts dropping all the data packets which it receives.

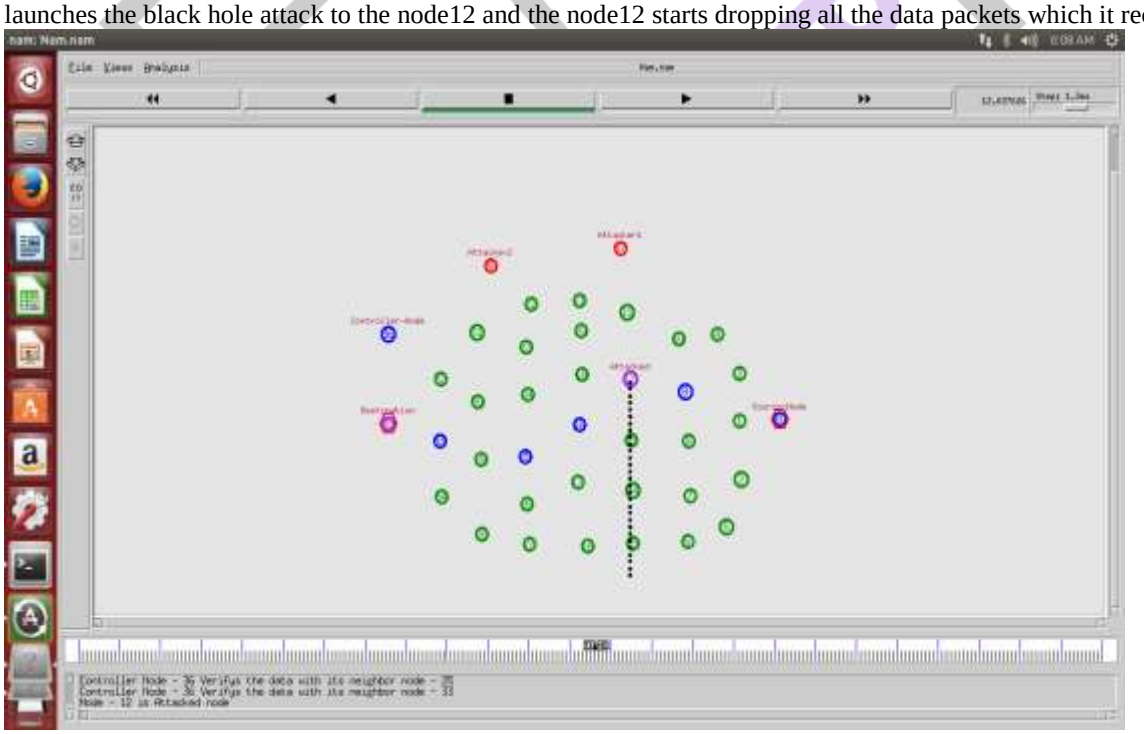

Figure 6.3: Nodes are attacked and the packets are dropped

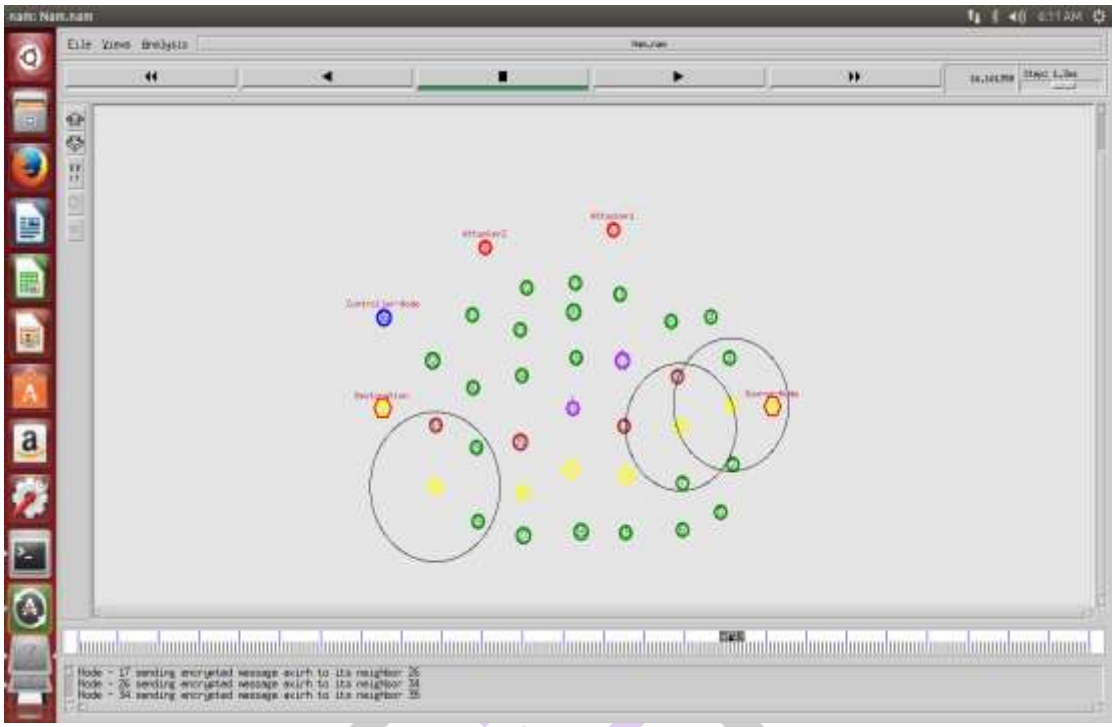

Figure 6.4: Forming the second route in the network

6.2 PACKET DELIVERY FRACTION (PDF)

The difference between the data packets accepted at the destination and the data packets generated at the CBR sources is called PDF. The PDF is calculated using the equation 6.1.

$$PDF = \frac{1}{n}\sum_{A=0}^{n}\frac{(Pr * 100)}{Ps} \quad \text{----------(6.1)}$$

where:
Pr: Destination end packets.
A: Application ID
Ps: Packets sent from source end
n: application

The PDF comparison of the present and the proposed system is shown in the Figure 6.5. In the below graph the Dotted line denotes the proposed system where as the Black line indicates the Present system. Here the PDF for the Existing system is 63% and the proposed system is 65%. This graph results proves that the proposed system PDF is comparatively improved than the present system, Refer Annexure A 8.

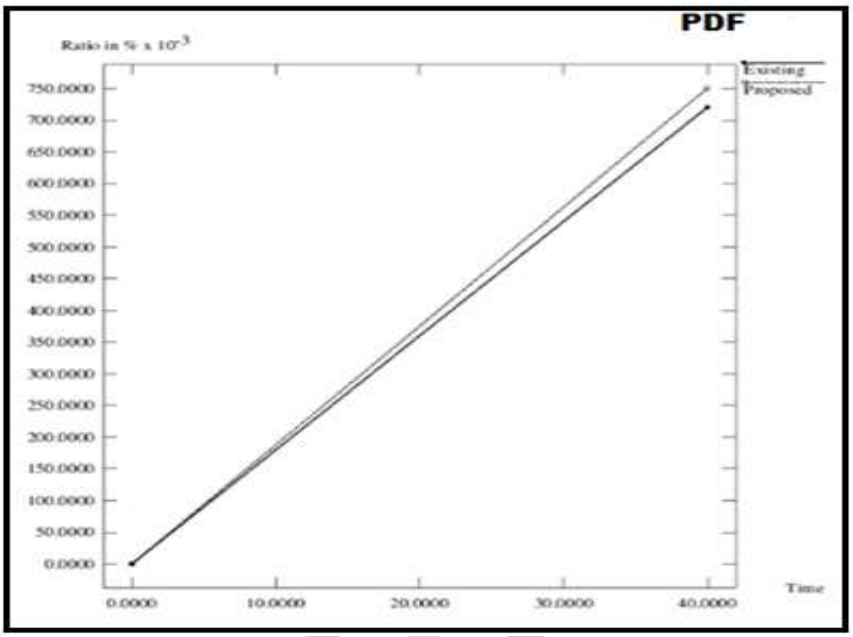

Figure 6.5: Packet Delivery Fraction graph

6.3 CALCULATING END-TO-END DELAY

The comparison of transfer time of the data packet at receiver node to the time it was transferred by the sender node. The equation 6.2 is used for calculating the average value.

$$E = \frac{1}{n}\sum_{A=0}^{n}(tr - ts) \quad \text{----------(6.2)}$$

where:
tr: First packet received time at receiver end.
ts: First packet received time at sender end .
A: application

The E2E Delay comparison of the present and the proposed system is shown in the Figure 6.6. In the graph the Dotted line indicates the proposed system where as the Black line indicates the Present system. Here the Xaxis denotes the Time, and the Yaxis denotes the delay in mili-seconds. Here the E2E Delay for the Existing system is 2.9 ms and the proposed system is 3.5 ms, the graph results says that the proposed system E2E delay is comparatively better than the existing system, Refer Annexure A 6.

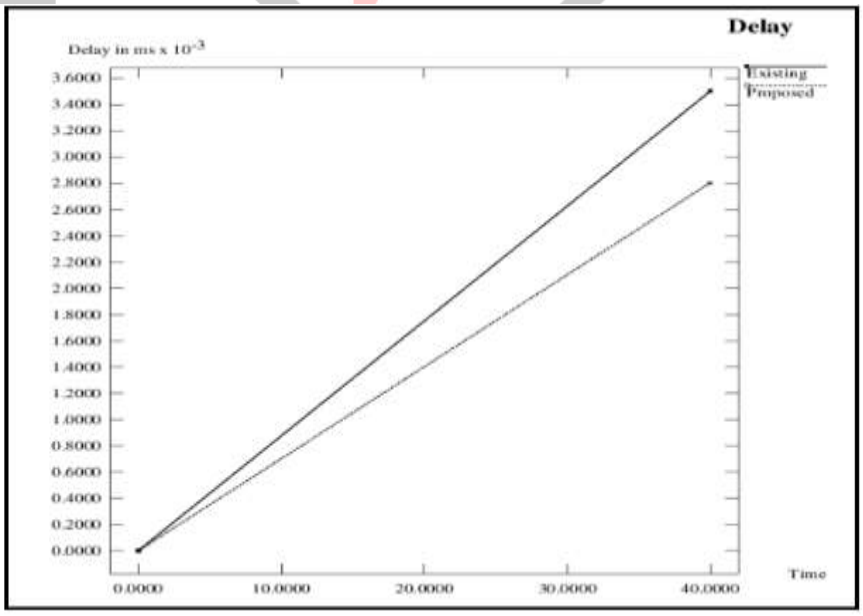

Figure 6.6: End-to-End Delay Comparison

CHAPTER 7

CONCLUSION AND FUTURE ENHANCEMENT

In Manet's always there is a growing threat of attacks on the Mobile nodes. Black hole attack is one of most important issues in Manet's due to which performance of the network drops. Which includes the parameters such as Packet Delivery Fraction, Throughput, and End-to-End delay. The proposed method detects the black hole attacks in MANET and also improves the performance of the network by tuning up the MAC protocol by using the Adaptive algorithm. The simulation analysis and results shows that the proposed algorithm achieves a very good rise in Packet Delivery Fraction, Throughput and minimal end-to-end delay. The proposed method is an effective solution for detection of the black hole attacks in the network.

The proposed methodology is implemented and simulated for the AODV routing algorithm it can also be further extended for use by any other routing protocols, and also the energy consumption can be minimized.

REFERENCES

[1] Rashmi, Ameeta Seehra, "A Novel Approach for Preventing Black-Hole Attack in MANETs", International Journal of Ambient Systems and Applications (IJASA) Vol.2, No.3, September 2014

[2] Neeraj Kumar "A Secure and Energy Efficient Data Dissemination Protocol for Wireless Sensor Networks International Journal of Network Security", Vol.15, No.6, PP.490–500, Nov. 2013

[3] Shaiffu and Amandeep Kaur Virk, "Greyhole and Blackhole Attack Identification and Prevention using IP Backtracking" International Journal of Computer Applications Volume 169, July 2017.

[4] Yu-Hsun Chen, Chia-Cheng Hu, Eric Hsiao-Kuang, "A Delay-Sensitive Multicast Protocol for Network Capacity Enhancement in Multirate MANETs" IEEE journal 1937-9234 2017.

[5] Neelesh Gupta Roopam Gupta "Routing protocols in Mobile Ad-Hoc Networks" IEEE INTERACT.2010.5706220, 31 January 2011

[6] Dr. G. Padmavathi, Mrs. D. Shanmugapriya Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks, International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2017.

[7] Zeng Yingpei, Cao Jiannong, Zhang Shigeng, Guo Shanqing and Xie Li "Random-walk based approach to detect clone attacks in wireless sensor networks IEEE Journal, vol.28, no.5, pp.973-691,June 2010.