Journal of The Gujarat Research Society

ISSN: 0374-8588

Volume 21 Issue 3, October 2019

RECOGNITION OF BLACK HOLE ATTACKS IN MANET USING EFFICIENT AD-HOC ON-DEMAND DISTANCE VECTOR (E-AODV) PROTOCOL

Kavita Arora[1], Dr. Kavita[2], Dr. Vishal Jain[3]

[1]Research Scholar, Department of Computer Science and Engineering, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan, India
Assistant Professor, Faculty of Computer Applications, Manav Rachna International Institute of Research and Studies

[2]Associate Professor, Department of Computer Science and Engineering, Jayoti Vidyapeeth Women's University, Jaipur, Rajasthan, India

[3]Associate Professor, Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University, Greater Noida, U.P., India

Abstract - MANET is a dynamic network consisting of mobile nodes and is easy to set up anywhere without using a fixed network infrastructure such as a base station. Due to this dynamic nature, MANET becomes vulnerable to security attacks. One of the major attacks that occur in MANET is black hole attack. Black hole attack causes the data packets around the attacker's node to be lost and ultimately the network suffers from data loss. Selection of the right routing protocol is one effort to minimize the impact of black hole attacks. This research was made to enhance the efficiency of AODV routing protocol to diagnose the impact of black hole attacks. The results of this study indicate that several QoS values such as throughput,delayand packet loss. However, while evaluating the results in the scheme the test results can be seen when the simulation with a black hole detection mechanism makes the packet loss value smaller than when there is no detection mechanism. The packet loss value in the random walk movement decreased from 76.17% in a black hole condition to 41.24% as the nodes

increase from 20 numbers to 30 numbers respectively in a black hole detection mechanism.

Keywords: MANET, Routing protocol, Black hole attack, QoS.

INTRODUCTION

Mobile Ad-hoc Network (MANET) is a temporary network which embodies ad hoc nodes. The mobile devices in this network can enter as well as exit any moment of time. This dynamic nature of each node makes it easy to obtain information. Each node can also behave abnormally such as carrying out black hole attacks which can disrupt the routing process. Black hole attack works by proclaiming to have the shortest path from the sender terminal to the goal node so as to force the sender node to transfer the data packets through this node only. Then the black hole node discards the packet it receives. This will be very dangerous if the packet sent is containing substantialdetails.So, MANET have to havesuch a security contrivance which can spot and reduce the impact of black hole attacks.

Previous research entitled "Mitigating the Effects of Black hole Attacks on AODV Routing Protocol in MANETs" has explained that black hole node will send RREP messages as soon as it receives Route Request messages through sender device without forwarding Route Request message to next node. Route Reply messages from malicious nodearrives at source node faster than RREP messages from other nodes. To overcome this, this study provides a solution by ignoring the RREP message that first reaches the source node [1].

Another study entitled "Implementing and improving the performance of AODV by receiving the reply method and securing it from Black hole attack" explains that the routing protocol AODV will automatically choose the first-coming RREP to select the path. In this study, all RREP messages will be stored in advance for a certain period of time after receiving the first RREP. Black hole identification is differentiated based on the value of delay and the largest sequence number of the collected routing information[2].

Based on the above problems, the authors made the scheme entitled "Recognition of Black Hole Attacks in MANET using Efficient Ad-hoc On-Demand Distance Vector (E-AODV) Protocol". In this scheme, the detection of black holes on MANET is done by forwarding a fake Route Request message. The destination address for spoofed RREQ message is converted to an address that does not exist on the network. When a black hole receives a fake RREQ message, it will immediately reply with an RREP message citing the highest sequence number and lowest hop count. In this case, detection node can make out that if this reply is a fake RREQ message, then the node is a black hole node. Consequently, parameters like End-to-End delay, PDR and through put are to be evaluated for performance analysis.

LITERATURE REVIEW

MANET: Mobile Ad-hoc Network (MANET) is a wireless network independent od any fixed infrastructure. It comprises of a set of ad-hoc nodes that can act as routers and hosts. Network configuration on MANET is carried out by nodes independently without using infrastructure [3]. MANET nodes are dynamic so that the formation of a network topology is dynamic. MANET nodes have several roles, such as ordinary nodes, forwarding packets, and nodes can act as routers [4].

MANET networks are formed in a dynamic way from several nodes over a wireless network that does not use a fixed infrastructure and centralized administration. Each node on the MANET network can move freely which makes the topology on the MANET network can change rapidly at any time. In general, routes between nodes in a MANET network can include multi-hops [5].

AODV: The AODV protocol is an example of a reactive protocol based on a divergentmethod from the proactive protocol. The weakness of the proactive protocol is the overhead that comes from the route maintenance process at each node is carried out every time. Reactive protocol does not do route

maintenance all the time; on the contrary it maintains the routing table when it is needed only. As and whenthesender node requires a route for sending data to a goal node, the routing table is checked for the same. If no route is found, a route discovery process will be carried out to discover a path to the destination node. Reactive protocols have advantage of reduced overhead compared to proactive protocols, especially in networks with low to moderate traffic [6]. However, the Ad-hoc On-Demand Distance Vector protocol performs mechanisms including route search (Route Discovery) and a Route Maintenance. Messages format of AODV protocol includes Route Request (RREQ), Route Reply (RREP) and Route Error (RERR). and these three make most of AODV protocol. Functions performed by these messages is to find a route to a certain node, notification of network topology changes and to maintain continuity of network connections respectively. AODV protocol has an active participation in the process of communication in an ad-hoc network. If desired path is available and valid, the process of using the AODV protocol is not executed. Such a mechanism is very advantageous to reduce energy use and data traffic in the network. Route searching is done when a node needs a next-hop that goes to its destination, which is done by transmitting RREQ messages to every other node in reach. The node that receives the RREQ will check whether it has route information to the intended node, in case the intermediate node does not possess route information to be sent togoal node, then will forward Route Request via intermediate node to the destination node. When an intermediate node passes Route Request, it repudiates next-hop to sender node, which is useful when sending a reply message. Then the goal node in return forwards a route reply message as a reply to RREQ. RREP contains sequencenumber and hop-count. The RREP message will be sent in a unicast manner to source node along the reverse-hop created by the intermediate node while forwarding the RREQmessage. Intermediate node receiving the RREPmessage will forward it to source node and will increment hop-count

value. As source node encounters many RREPs then one with the smallest hop-count value will be selected. [7-10]

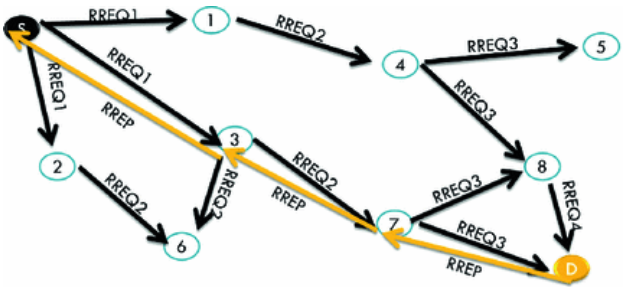

Figure 1: Routing using AODV Protocol in MANET

PARAMETERS AFFECTING ROUTING PROTOCOL PERFORMANCE: Network performance is measured by the Quality of Service (QoS) parameter. Performance network can show consistency, data transmission success rate, and others [11-15]. There are several parameters that can be used to measure performance networks include:

- **Throughput:** Throughput is the actual data rate per unit time. It is administered by the availability of bandwidth. It's measurement unit is Bps (Bits per second).
- **Packet Loss:** Loss of packetshappens when data packets in transit fail to reach destination. According to researchers [11-15] packet loss distinguished as one of the three types of errors encountered in communication digital, the other two are bit error and packet imitation by because of noise.
- **Packet Delivery Ratio:** PDR is the ratio of number of data packets generated by source node and delivered to intended recipient node.
- **End to End Delay:** End to end delay is the average time duration in between generation of packets at the end of source node and successful delivery of those data packets at destination including all possible delays due to buffering during route discovery latency, and queues at interfaces.

Black Hole: A black hole attack is an attack that discards the packet (drop packet) it receives. This attack works by giving a reply to every path request (RREQ message) it receives. The black hole node declares itself to have the route and immediately responds with an RREP message. The details in the RREP black hole message communicate that the presence of shortest route to the destination node by changing the hop count value to a minimum and a larger sequence number value. Black hole attacks can work with a single number and with many nodes or are called collaborative black hole attacks [17-19]. Black hole attack can be seen in Figure2. For example in Figure 2 N1 will forward a data packet to N6 and sender node starts the route discovery process. Assume node N2 to be an attack node without a route to N6 in its routing table. Node 2 declares itself to have a direct route to the goal node after receiving an RREQ from source node and replies by sending an RREP message to the source node. When the source node sends a message via N2, attacker node can easily drop data [19].

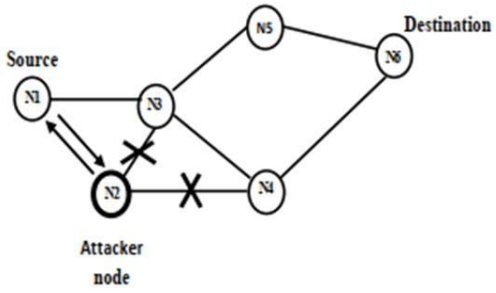

Figure 2: Black Hole Attack Process

METHODOLOGY

This section will explain the steps that will be carried out in the research. This research is a development of previous research and is an implementation of further development. The steps in this research include literature study, needs analysis, system design, system implementation, testing and analysis as well as conclusions and suggestions. The research methodology is shown in Figure 3.

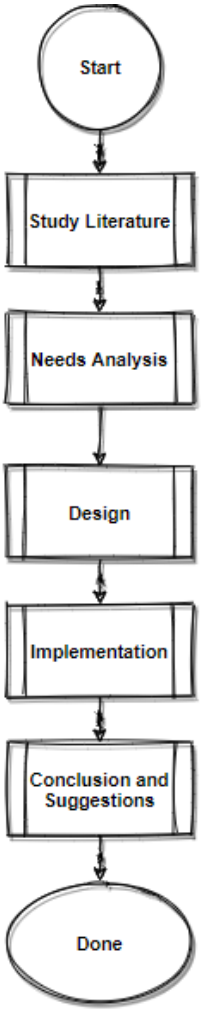

Figure 3: Flow of research methodology

- **General Description of the System**

The handling mechanism followed for black hole attacks comprises of exploring black holes and finding routes that do not pass through the black hole. the process of looking for black holes is done by sending an RREQ message with a false purpose. Furthermore, the process of finding a path to the destination. Data transmission is done by selecting the path contained in the routing table and avoiding black holes.

The following is a detection path that can be seen in Figure 4.1 black holes used in this study:

1. The addition of the Is Detect Black hole attribute is written to simulate, so the node that activates this attribute will act as a black hole node detector.
2. Checks whether there are malicious nodes. The check is carried out by the source node by sending a RREQ message with a fake destination address. If the Is Detact Blackhole attribute is active, send Request method will be modified by adding a fake RREQ message sending script.
3. Added a function in Recv Reply () to notify users the existence of a malevolent nodein the network. When the source node receives a fake RREQ reply message, the system will notify that the sender of the RREP is a black hole.
4. Flags black hole nodes that reply to false RREQ messages.
5. The process of finding a route by sending the original RREQ message. The source node broadcasts RREQ to find a route to the destination node.
6. Source node receives all RREP messages from the destination node and neighboring nodes that have route information.
7. Node sources can send messages through known paths and avoid black hole paths.

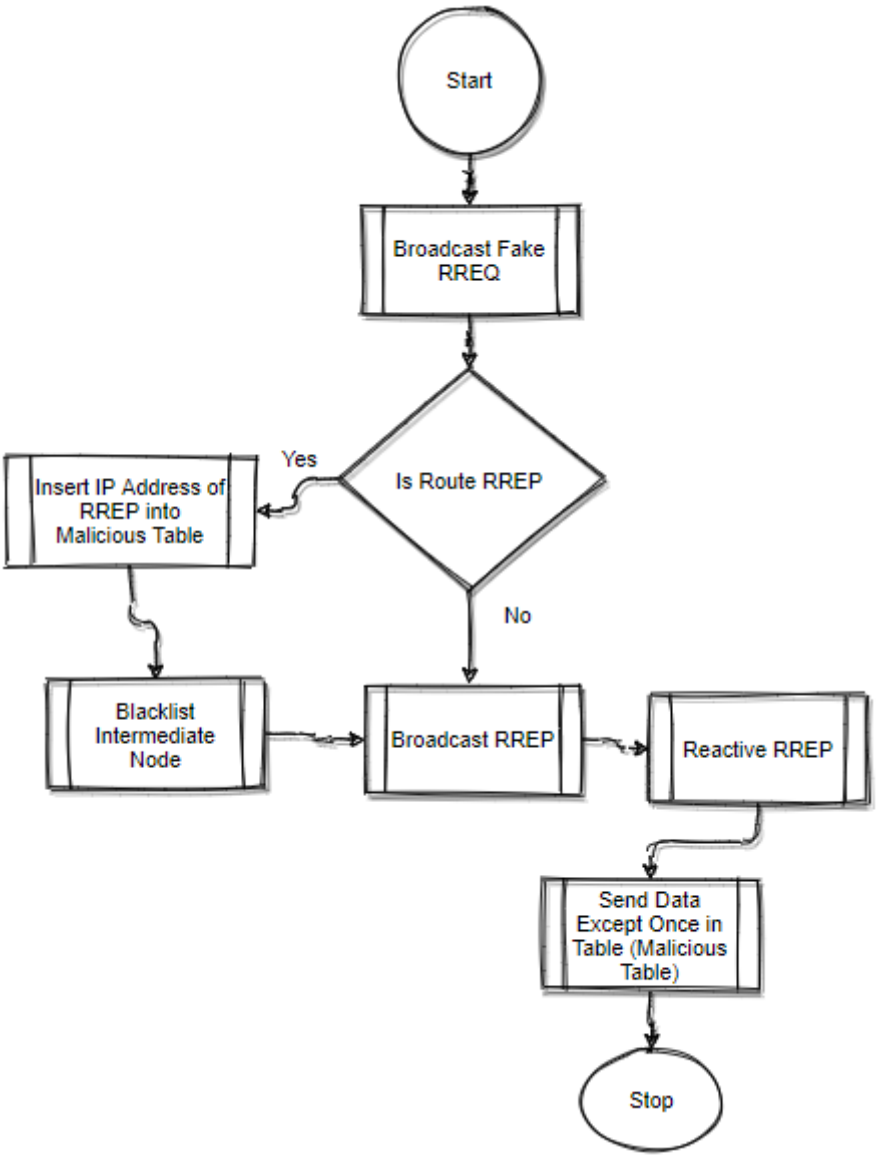

Figure 4: Black Hole Detection using AODV

DESIGN

The system design is done to provide an overview of the implementation of the AODV protocol on the MANET network and see the performance of the protocol in normal conditions. The configuration specified in this design uses the AODV routing protocol. The numbers of nodes made are 20, 25 and 30. The placement of nodes is done randomly using the random waypoint mobility type. All nodes will be randomly distributed over an area of 1000 meters x 1000 meters. The nodes move freely at speeds between 1 to 10m / s. in sending data between nodes using UDP connection with packet

typeCBR. The size of the packet sent is 512 bytes from source node (1) to node (16) assuming no black hole attacks. The configuration of the system implementation using the AODV protocol can be seen in table1, 2, 3 .

S.No	Parameter	Information
1	Routing Protocol	AODV
2	Total Nodes	20,25 and 30
3	Connection Type	UDP
4	Type of Packets	CBR
5	Size of Packets	512 Bytes
6	Packets CBR Rate	1000 KB
7	Area	1000 Meters * 1000 Meters
8	Simulation Time	1000 Seconds
9	Mobility Type	Random Waypoint
10	Node Speed	1 to 100 m/s

Table1: System configuration

The design of the test scenario is carried out to see and evaluate performance of protocol against the scenario of the black hole node position, movement type, and the number of nodes. From the test scenario data will be obtained to analyze the protocol. The design can be seen at as under:-

S.No	Parameter	Information
1	Routing Protocol	AODV
2	Nos. of Nodes	20,25 and 30
3	Nos. Blackhole Nodes	2 to 3
4	Connection Type	UDP
5	Type of Packets	CBR
6	Size of Packets	512 Bytes
7	Packets CBR Rate	1000 KB
8	Area	1000 Meters * 1000 Meters
9	Simulation Time	1000 Seconds
10	Mobility Type	Constant
11	Node Speed	1 to 100 m/s

Table2: Configuration of black hole position variations

S. No	Parameter	Information
1	Routing Protocol	AODV
2	Nos. of Nodes	20,25 and 30
3	Nos. Blackhole Nodes	2 to 3
4	Connection Type	UDP
5	Type of Packets	CBR
6	Size of Packets	512 Bytes
7	Packets CBR Rate	1000 kbps
8	Area	600 Meter * 600 Meter
9	Simulation Time	1000 Seconds
10	Mobility Type	Random Waypoint Movement, Random Walk Movement and Movement of Random Direction
11	Node Speed	1 to 100 m/s

Table 3: Configuration of Movement Type Variations

SIMULATION AND RESULTS

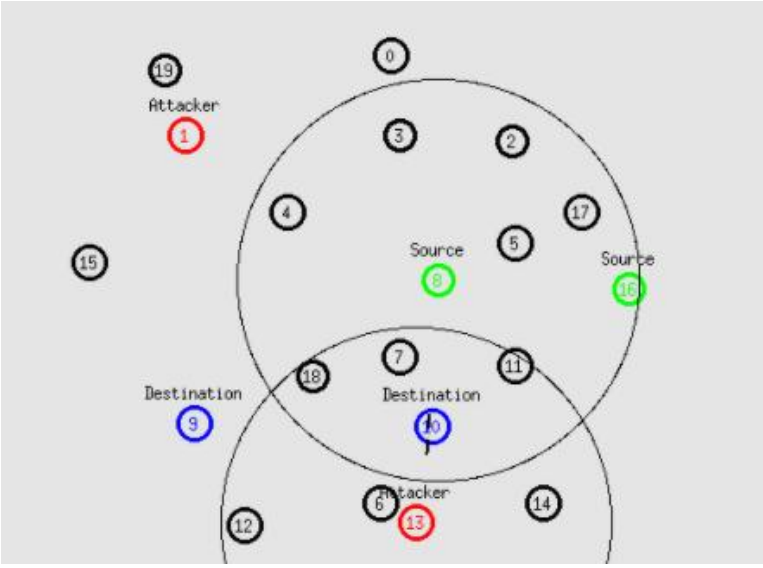

Figure 5: Animation displaying 20 nodes when there is black hole detection

Figure 5displays MANET network simulation under normal conditions in the NS2 Network Animation application. The simulation uses the AODV protocol with a number of nodes20. The position of each node has been determined over an area of 600 meters by 600 meters and uses the constant mobility type.

```
s 1.009088414 _7_ MAC  --- 0 ARP 80 [13a d 7 806] ------- [REPLY 7/7 13/13]
s 1.009352046 _8_ RTR  --- 0 AODV 48 [0 ffffffff 10 800] ------- [8:255 -1:255 29 0] [0x2 2 1 [10 0] [16 4]] (REQUEST)
s 1.009468495 _6_ RTR  --- 0 AODV 48 [0 ffffffff 7 800] ------- [6:255 -1:255 28 0] [0x2 3 1 [10 0] [16 4]] (REQUEST)
s 1.009525492 _14_ RTR  --- 0 AODV 48 [0 ffffffff 10 800] ------- [14:255 -1:255 29 0] [0x2 2 1 [10 0] [16 4]]
(REQUEST)
r 1.009728943 _13_ MAC  --- 0 ARP 28 [13a d 7 806] ------- [REPLY 7/7 13/13]
s 1.009738943 _13_ MAC  --- 0 ACK 38 [0 7 0 0]
r 1.010043472 _7_ MAC  --- 0 ACK 38 [0 7 0 0]
s 1.010113518 _11_ MAC  --- 0 AODV 100 [0 ffffffff b 800] ------- [11:255 -1:255 29 0] [0x2 2 1 [10 0] [16 4]]
(REQUEST)

Packet Delivery Ratio
-------------------------
Packet Sent:491 - Packet Received:117
[ Packet Delivery Ratio:23.83 ]
Average End-to-End Delay = 9.63162 ms
Average Throughput[kbps] = 25.21 [StartTime=1.00⟶StopTime=20.01]
```

Figure 6: Results of the NS2 20 node conditions where there is black hole detection

Figure 6 is a display on the Linux terminal simulation results of the MANET network in a condition where there is black hole detection on network using the NS2 application. The simulation is carried out with a different black hole position scenario. MANET network scenario in a condition where there is black hole detection in Figure 8 shows the results with a packet loss value of 76.17%, a packet delivery ratio of 23.83%, average delay of 9.63162 ms with average throughput of 25.21 in 20 Seconds which is calculated from the data flow between the source node (8 and 16) and the destination node (9 and 10) during the simulation process.

Journal of The Gujarat Research Society

ISSN: 0374-8588

Volume 21 Issue 3, October 2019

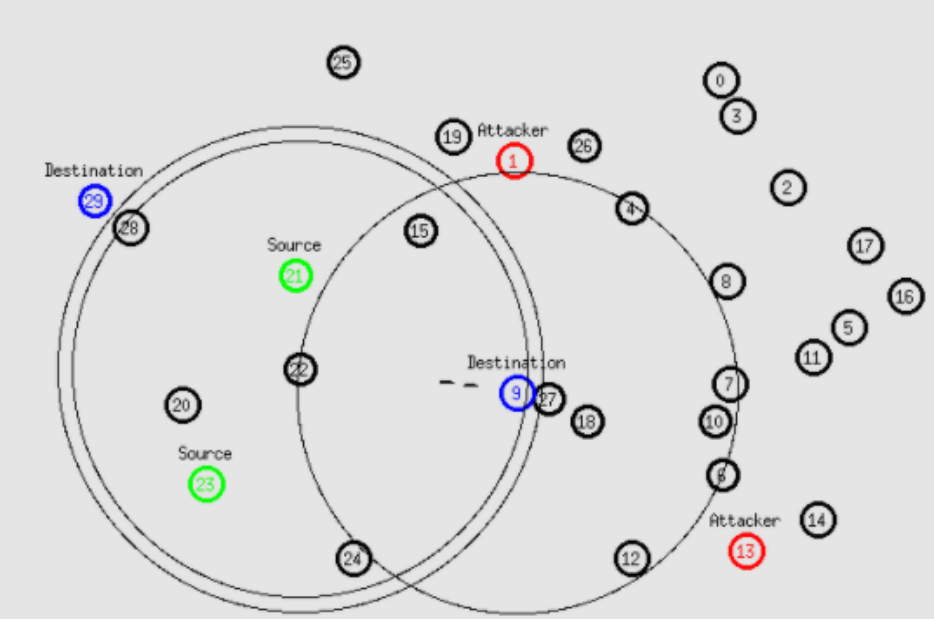

Figure 7: Network Animation display of 30 nodes when there is black hole detection

```
s 1.000535000 _16_ MAC  --- 0 AODV 100 [0 ffffffff 10 800] ------- [16:255 -1:255 30 0] [0x2 1 1 [10 0] [16 4]]
(REQUEST)
r 1.001335294 _17_ MAC  --- 0 AODV 48 [0 ffffffff 10 800] ------- [16:255 -1:255 30 0] [0x2 1 1 [10 0] [16 4]]
(REQUEST)
r 1.001335456 _5_ MAC  --- 0 AODV 48 [0 ffffffff 10 800] ------- [16:255 -1:255 30 0] [0x2 1 1 [10 0] [16 4]] (REQUEST)
r 1.001335460 _11_ MAC  --- 0 AODV 48 [0 ffffffff 10 800] ------- [16:255 -1:255 30 0] [0x2 1 1 [10 0] [16 4]]
(REQUEST)
r 1.001335491 _8_ MAC  --- 0 AODV 48 [0 ffffffff 10 800] ------- [16:255 -1:255 30 0] [0x2 1 1 [10 0] [16 4]] (REQUEST)
r 1.001335627 _2_ MAC  --- 0 AODV 48 [0 ffffffff 10 800] ------- [16:255 -1:255 30 0] [0x2 1 1 [10 0] [16 4]] (REQUEST)
r 1.001335732 _14_ MAC  --- 0 AODV 48 [0 ffffffff 10 800] ------- [16:255 -1:255 30 0] [0x2 1 1 [10 0] [16 4]]
(REQUEST)
r 1.001335772 _10_ MAC  --- 0 AODV 48 [0 ffffffff 10 800] ------- [16:255 -1:255 30 0] [0x2 1 1 [10 0] [16 4]]

Packet Delivery Ratio
------------------------
Packet Sent:491 Packet Received:288
[ Packet Delivery Ratio:58.66 ]
Average End-to-End Delay = 20.3629 ms
Average Throughput[kbps] = 30.29⟶[ StartTime=1.00⟶StopTime=39.94 ]
```

Figure 8: Results of the NS230 node conditions where there is black hole detection

Figure 7 and figure 8 is a display on the Linux terminal simulation results of the MANET network in a condition where there is black hole detection on the network using the NS2 application. Simulation performed under different types of mobility scenarios. MANET network scenario in a condition where there is black hole detection in Figure

10 shows the results with a packet loss value of 41.34%, a packet delivery ratio of 58.66%, and aaverage delay of 20.3629ms and thereafter average throughput of 30.29 in 40 second approx. which is calculated from the data flow between the source node (21 and 23) and the destination node (9 and 29) during the simulation process.

However, the simulation was carried out in 3 different conditions. Normal conditions when there are no black holes in the MANET network simulation. Black hole condition when there is a black hole node in the MANET network simulation. Detection conditions when there are black holes and black hole detection mechanisms in the MANET network. The test scenario is carried out by changing the position of the black hole node and varying the type of movement in each simulation.

Nodes	Nos. of Black Hole	Packet Delivery Ratio	End to End Delay	Average Throughput	Packet Loss
20 Nodes	2	23.83	9.63	25.21	76.17
25 Nodes	2	39.71	43.23	20.51	60.29
30 Nodes	2	55.66	20.36	30.29	41.24

Table 4: Parameter Results with Different Node Sets with 2 Black Holes

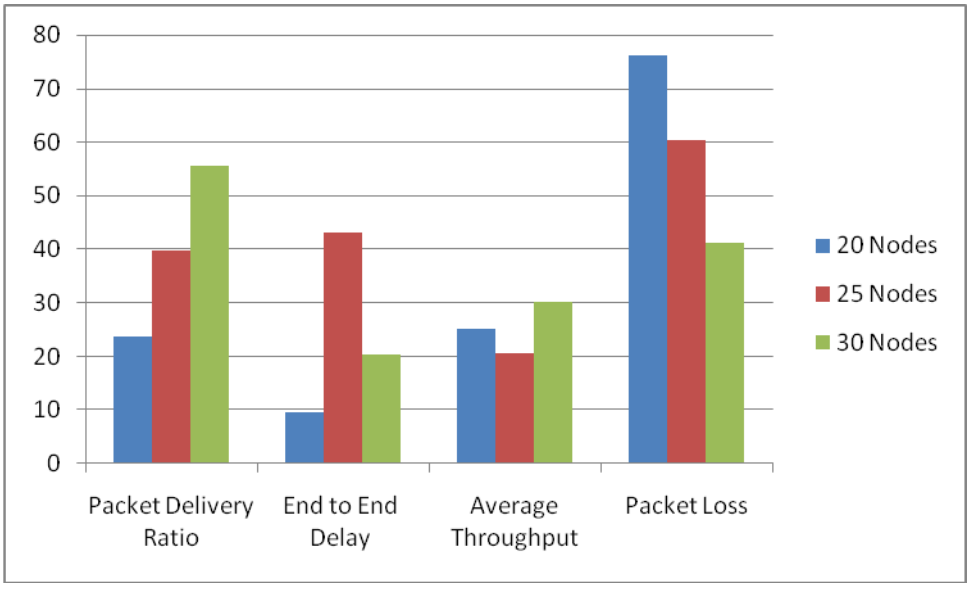

Figure 9: Bar Chart Depiction of Table 4.

CONCLUSION AND SUGGESTION

- **CONCLUSION**

From the results of the tests that have been carried out, the following conclusions can be drawn:

1. MANET network implementation with a black hole can be implemented. The black hole manages to discard all packets that have been passed on to him, so that the data sent cannot be sent to the destination. In the test results, the three scenarios can be seen when the MANET network simulation with a black hole can affect the packet loss value to be larger than the simulation under normal conditions.
2. MANET network implementation with a condition where a black hole detection mechanism can be run. The black hole detection mechanism can find out the position of the black hole and avoid the black hole route in sending data, so that the data sent can be sent to the destination. In the test results of the three scenarios, it can be seen when the MANET network simulation with black hole detection conditions can affect the value of the packet delivery ratio to be greater than the simulation with simulations in conditions where there are black holes.
3. The test results can be seen when the simulation with a black hole detection mechanism makes the packet loss value smaller than when there is no detection mechanism. The packet loss value in the random walk movement decreased from 76.17% in a black hole condition to 41.24% as the nodes increases from 20 numbers to 30 numbers respectively in a black hole detection mechanism.
4. 4.. From test results, it is visible that if simulation has a black hole detection mechanism, the delay value in the black hole position scenario is greater than the simulation without the detection mechanism. The delay value increases because additional time is needed to find the position of the black hole and find another route to avoid black holes. The amount of data sent in the black hole position

scenario has the same amount in each simulation. The value of delay in the movement type scenario and the number of nodes is smaller than the simulation without detection mechanism. The value of delay has decreased because the amount of data sent in each simulation has a different amount.

- **SUGGESTION**

From the results of the tests that have been carried out, several suggestions can be taken as follows:

1. Future research can be developed using other mechanisms to avoid or isolate the nodes that act as black holes from the MANET network

The next research can be developed with routing protocols and other attacks onthe MANET network

REFERENCES

1. K. Jain and V. Tokekar, "Mitigating the effects of Black hole attacks on AODV routing protocol in mobile ad hoc networks", 2015 International Conference on Pervasive Computing (ICPC), Pune, 2015, pp. 1-6.
2. Debarati Roy Choudhury, Leena Ragha, Nilesh Marathe, "Implementing and Improving the Performance of AODV by Receive Reply Method and Securing it from Black Hole Attack", Procedia Computer Science, Volume 45, 2015, Pages 564-570, ISSN 1877-0509.
3. Elahe Fazeldehkordi, Oluwatobi Ayodeji Akanbi, in "A Study of Black Hole Attack Solutions", eBook ISBN: 9780128053799 Imprint: Syngress Published Date: 3rd November 2015
4. Debarati Roy Choudhury, Leena Ragha, Nilesh Marathe," Implementing and Improving the Performance of AODV by Receive Reply Method and Securing it from Black Hole Attack", Procedia Computer Science, Volume 45, 2015, pp 564-570.
5. S, RAJASEKAR & A, SUBRAMANI. (2016),"A REVIEW ON ROUTING PROTOCOLS FOR MOBILE ADHOC NETWORKS",i-manager's Journal on Mobile Applications and Technologies.
6. Anggoro, Radityo & Suadi, Wahyu & Shiddiqi, Ary & Ijtihadie, Royyana& Lili, Suhadi & Pamungkas, Dimas. (2020)." The Development of Blackhole Attack In AODV Routing Protocol". 309-314.

7. Pal, Purba & Sarkar, Priya & Deb, Sonali& Bhattacharya, Gourab. (2019). “Analysis of AODV Protocol in MANET”. International Journal of Computer Applications. Vol. 177,pp 1-6.
8. Singh, Alok & Sharma, Saurabh & Srivastava, Rajneesh. (2020). “Investigation of random waypoint and steady state random waypoint mobility models in NS-3 using AODV”. Journal of High Speed Networks. 26. 1-8. 10.3233/JHS-200643.
9. Sanket Gulhane, “Modified AODV Routing Protocol For Ad hoc Network”, June 2013, ISBN-10 : 3659411426
10. Muhammad Idrees, “Enhancement of Throughput in AODV Using Relative Mobility of Nodes: The Case of Mobile Adhoc Networks (MANET)”,October 2011, ISBN:978-3-8465-3147-1
11. Karthikeyan, N. Kanimozhi and S. H. Ganesh, "Analysis of Reactive AODV Routing Protocol for MANET," 2014 World Congress on Computing and Communication Technologies, Trichirappalli, 2014, pp. 264-267.
12. A.A. Chavan, D.S. Kurule, P.U. Dere, “Performance Analysis of AODV and DSDV Routing Protocol in MANET and Modifications in AODV against Black Hole Attack”, Procedia Computer Science, Volume 79, 2016, Pages 835-844,ISSN 1877-0509.
13. Shrivastava, Madhup&Sahu, Monika & Rizvi, Murtaza & Ahmad, Khaleel. (2018). “IAODV: AN IMPROVED AODV ROUTING PROTOCOL FOR MANET”. International Journal of Advanced Research in Computer Science.
14. Meena Rao, Neeta Singh, “An Improved Routing Protocol (AODV nthBR) for Efficient Routing in MANETsAdvanced Computing, Networking and Informatics”- Volume 2, 2014, Volume 28 ISBN : 978-3-319-07349-1
15. Abdulaleem Ali Almazroi, Ma Ngadi,”Review on MANET: Characteristics, Challenges, Imperatives and Routing Protocols”, International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 2, February 2014, pg.432 – 437
16. Kumar S, Mohan & Majumder, Darpan. (2020). “A Review of Black and Gray Hole Attacks in AODV”.
17. Yadav, Renu & Hans, Meenu& Bhateja, Neha. (2014). “A Review Paper on Black Hole Attack in MANET Using AODV”.
18. Poongodi, T., & Karthikeyan, M. (2016). “Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks”. Springer Wireless Pers Commun.
19. Majumder, Darpan & Kumar S, Mohan. (2020),” A Review of Black and Gray Hole Attacks in AODV”.
20. Ning, P., & Sun, K. (2004). “How to misuse AODV: a case study of insider attacks against mobile adhoc routing protocols. Adhoc Network”, vol. 3, pp 795–819.(2004).