ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 8, Issue 3, March 2020

An Impact of Black Hole Attack on AODV Routing Protocol in MANETS Using NS2 Tool

Manasa K Chigateri[1], Md.M. Zakirulla[2], Khaja Moinuddin[3], Gavisiddesha P[4]

Assistant Professor, Department of Electronic & Communication Engineering, RYMEC, Ballari, Karnataka, India[1]

Assistant Professor, Department of Electronic & Communication Engineering, RYMEC, Ballari, Karnataka, India [2]

Assistant Professor, Department of Electronic & Communication Engineering, RYMEC, Ballari, Karnataka, India[3]

Assistant Professor, Department of Mechanical Engineering, BITM, Ballari, Karnataka, India[4]

ABSTRACT: Data communication refers to the transmission of digital data between two or more computers and a computer network or data network is a telecommunication network that allows computers to exchange data. The physical connection between networked computing devices is established using either cable media or wireless media. As the world of electronic communication has evolved from the transmission of analog signals to the transmission of digital bits and at the same time computer technology has continued to evolve at an astonishing rate, the desire to transmit more bits per second over a telecommunication link has grown. Thus, wireless communication is used. Advanced technologies of the 20th century, such as the internet and mobile communication, have made human lives easier.

KEYWORDS: WSN, AODV, MANETS, DES.

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) consists of a collection of mobile nodes which are not bounded in any infrastructure. Nodes in MANET can communicate with each other and can move anywhere without restriction. This non-restricted mobility and easy deployment characteristics of MANETs make them very popular and highly suitable for emergencies, natural disaster and military operations. Wireless networking is a method by which homes, telecommunication networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as connection between various equipment locations. The wireless network can be categorized based on their system architecture into two basic versions. The one is Infrastructure based network and the other is ad-hoc network. The biggest difference between them is, the infrastructure network consists of access point and nodes, meanwhile the ad-hoc network are independent from access point. In infrastructure based networking, a terminal cannot communicate directly with other terminals in the same cell and other cell. An access point here performs control messaging. Messages are sent to the access point and then the access point distributes the messages to the desired terminal. If a terminal wants to communicate with a terminal which is located in other cell, the access point will relay the message to other access point which has control over desired cell. The access points are normally wired connected. The problem in infrastructure based network is, if an access point in the network defects, all terminals in this cell cannot perform any communication.

Wireless ad hoc network is collection of wireless nodes that communicate directly over a common wireless channel. The nodes are equipped with wireless transceiver. They don’t need any additional infrastructure, such as base station or wired access point, etc. Therefore, each node does not only plays the role of an end system, but also acts as a router, which sends packets to desired nodes. The nodes in an ad-hoc network can be mobile, which is called as mobile ad-hoc network (MANETs). MANETs have some special characteristic such as open medium, dynamic topology, no clear defense mechanism and so on. In open and hostile environment, they are exposed to various types of attacks. One of these security attacks is the black hole attack. In this attack, the malicious node sends the fake reply to the destination node without checking its routing table and it absorbs all data packets that intended to forward to the destination. In this way, all data packets in the network are consumed. Hence, data loss occurs in the network and affects the performance.

II. Related work

ImrichChlamtac ,et al[1] describes that historically, mobile ad hoc networks have primarily been used fortactical network related applications to improve battlefield communications/survivability. The dynamic nature of military operations means that military cannot rely on access to a fixed pre-placed communication infrastructure in battlefield. Pure wireless communication also has limitation in that radio signals are subject to interference and radio frequency higher than 100MHz rarely propagate beyond line of sight (LOS). Mobile ad hoc network creates a suitable framework to address these issues by providing a multi-hop wireless network without pre-placed infrastructure and connectivity beyond LOS. Saleh Ali K. Al-Omari, Putra Sumari[2] All nodes in a wireless ad-hoc network act as a router and host as well as the network topology is dynamic because the connectivity between the nodes may vary with time.The special features of Mobile Ad Hoc Network (MANET) bring this technology great opportunity together with severe challenges. It implies that maintenance, routing and management, etc. have to be done between all the nodes. This case Called Peer level Multi Hopping and that is the main building block for Mobile Ad Hoc Network.GoitomAbrehaley et al[3] An ad hoc routing protocol is a standard for controlling node decisions when routing packets traverse a MANET between devices. A node in the network, or one trying to join, does not know about the topology of the network. It discovers the topology by announcing its presence and listening to broadcasts from other nodes (neighbors) in the network. The process of route discovery is performed differently depending on the routing protocol implemented in a network.
C. Perkins , E. Belding-Royer and , S. Das , et al[4] describes that ,the Ad hoc On-Demand Distance Vector (AODV) routing protocol is intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization**.** One distinguishing feature of AODV is its use of a destination sequence number for each route entry. The destination sequence number is created by the destination to be included along with anyroute information it sends to requesting nodes. Using destinationsequence numbers ensures loop freedom and is simple to program.Kulbir Kaur Waraich, et al[5] discusses that in AODV the communication among nodes take place only when required. It is a combination of on demand and distance vector. It includes two main functions route discovery and route maintenance.

It first discovers the route by sending route requests RREQ to each and every node in the network and then route maintenance takes place. Every RREQ contains source identity, destination identity, source sequence number, destination sequence number, time to live etc. Every time a node increases a sequence number and notices change in the neighborhood topology.Ali Dorri.et al[6] tells thatbecause of MANETs special characteristics like dynamic topology, hop-by-hop communications and easy and quick setup, MANETs faced lots of challenges allegorically routing, security and clustering. The security challenges arise due to MANETs self-configuration and self-maintenance capabilities.

PuneetKansal, et al[7] discusses about blackhole stating that the black hole attack in wireless ad- Hoc traffic between victim node and the malicious node, then network is major issue that needs efficient solutions. In black hole attack more than one node can be malicious. Most of the time black hole attack occurs in large Ad Hoc networks. Black holes refer to places in the network where incoming traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipients. Black Hole attacks effects the packet delivery and to reduce the routing information available to the other nodes causes: (i) It down grade the communication, (ii) effects of making the destination node reachable. Annapurna P Pati. et al[8] describes that energy is a scarce resource in ad hoc wireless networks .Each node has the functionality of acting as a router along with being a source or destination. Thus the failure of some nodes operation can greatly impede performance of the network and even affect the basic availability of the network, i.e., routing, availability, etc. Thus it is of paramount importance to use energy efficiently when establishing communication patterns. Kulbir Kaur Waraich. et al[9] discusses about performance metrics of AODV under attack and describes that AODV routing protocol is vulnerable to malicious behaviour. When a node sends packets to the destination without any failure then it acts as a genuine node. During malicious attack, a node starts behaving as malicious by keeping all packets with itself and not forwarding to the destination node. After receiving all the packets, malicious node starts dropping all these packets which affects whole network by degrading the performance of network

III. PROBLEM STATEMENT

MANETs set new challenges for network security and the need of an hour is to pay more attention to the security threats posed on the network. As nodes themselves are participating in relaying of messages, any malicious node in the network can easily misuse the message traffic either by dropping messages or by generating false messages etc.

Due to the limitation of network resources in mobile ad-hoc networks, the various cryptographic solutions applicable to wired networks are not directly applicable. The failure of some nodes operation can greatly impede performance of the network. Therefore there is a need for new security solutions which can find their application in this challenging domain. Hence there is a need to conserve the available resources.

IV. PROPOSED ALGORITHM

Several studies have proposed several solutions to support performancemetrics in the dynamic MANET environment &about the provisioning of security requirements in hand held devices where the resources are scare. The security provision will cost more resources and minimize the network life, it may adversely affect the performance metrics. Thus it isnecessary to consider both provisioning of security and minimizing the energy consumption to provide network life in an integrated manner. To evaluate the performance metrics, we need to choosethe most suitable evaluation methodology. Three evaluation methodologies,

- Simulation
- Experimental and
- Mathematical

4.1 Simulation Environment

In this simulation, the black hole attack based on the AODV routing protocol is implemented using NS-2.35. For this simulation, the IEEE 802.11 Mac at the physical and data link layer are used. The channel is Wireless Channel based on Two Ray Ground radio propagation model. AODV is used at the network layer as the routing protocol and UDP is used at the transport layer. Two scenarios were simulated, the first scenario consists of a Dumb led topology having, total of 50 nodes which are configured as per requirements, and given mobility. The performance metrics are evaluated for AODV protocol.

Second scenario illustrates that out of same 50 nodes one black hole is injected into the network. Analysis is done based on metrics and is compared with that of first scenario without black hole attack. The overall simulation parameters are presented in Table 4.1

Parameters	Values
Simulator	NS2 (2.35 Ver)
Routing Protocol	AODV
Number of Nodes	50
Simulation Time	10 seconds
Malicious node	1
Packet Size	1000 bytes
Traffic Type	CBR
Transmission Rate	0.1 Mbps
MAC Type	802.11

Table 4.1: Simulation Parameters

DOI: 10.15680/IJIRCCE.2020. 0803025

4.2 Performance Evaluationusing NS2

- Choosing and generating a wireless network topology to be used throughout the simulation.
- Once the topology has been generated traffic source and destination are fixed. Assign suitable traffic sources to the source node and traffic sinks to the destination nodes.
- Simulate and analyze the scenario.

The below Figure 4.1 illustrates the Network Animator Window (NAM) consisting of 50 mobile nodes where in node 6 is transmitter and node 32 is receiver. The figure shows route discovery process in which the RREQ control packets originated by the transmitter or source node is broadcasted over the network. Once the receiver receives the RREQ packets it in turn replies with RREP control packets (small packets in below figure).

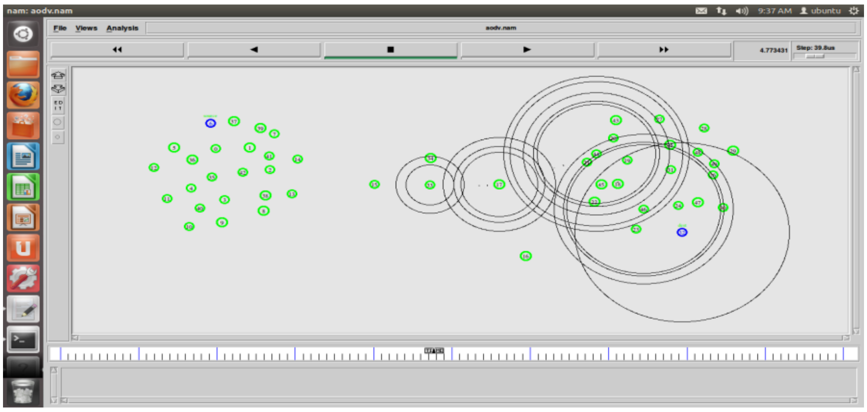


Figure 4.1: Route Discovery process in AODV for 50 nodes

Figure 4.2 illustrates the general scenario of AODV routing protocol, once the route has been established the source node starts sending the CBR data packets to the destination via the intermediate routers.

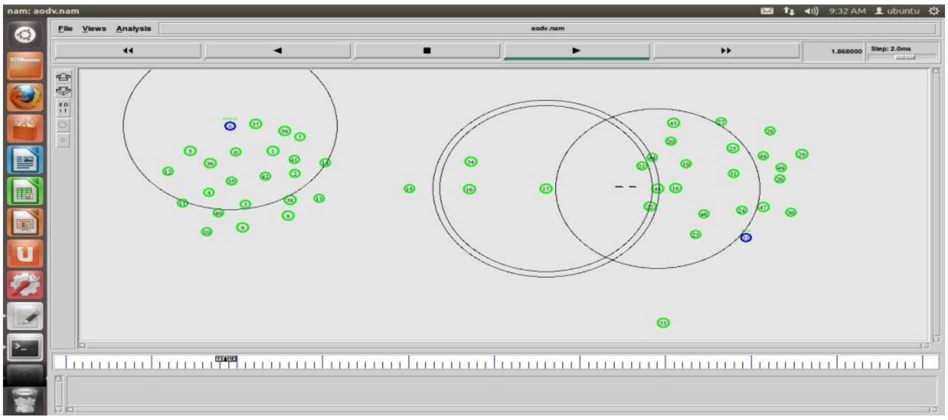


Figure 4.2: General AODV scenario

After simulating and analysing AODV routing protocol black hole attack was implemented as shown inFigure4.3. Here node 33 acts as black hole node which sends a false reply to the source during the route discovery process and consumes all the data packets sent by the source without forwarding it to the destination.

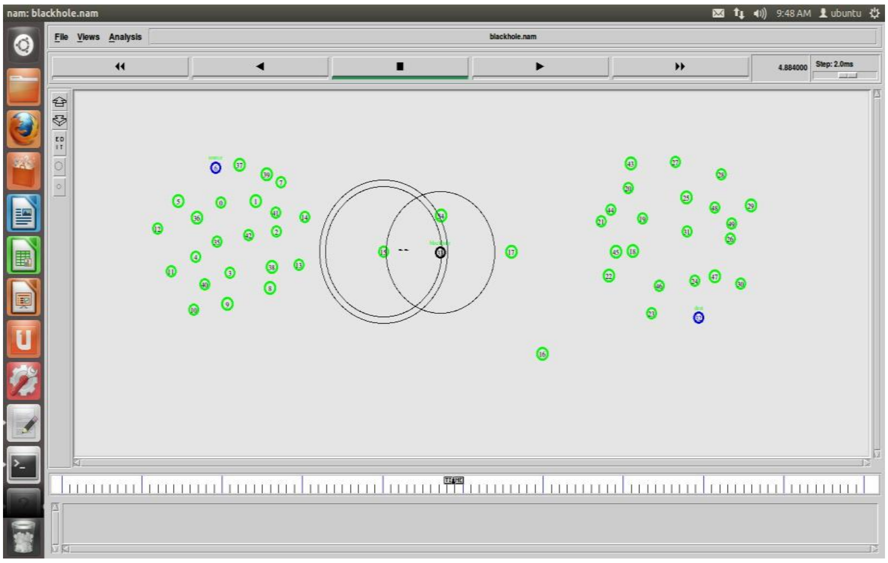


Figure 4.3: AODV under Black hole attack

4.3 Performance Metrics

Before proceeding with performance evaluation, one must choose the different metrics that would help in making comparisons. There could be different metrics to determine the performance like throughput, delay, packet delivery, jitter, packet loss, end to end delay, etc. The choice of metric would depend upon the purpose the network has been setup for.

The following metrics are used to evaluate the performance of black hole scenario.

Packet Delivery Ratio: The ratio between the number of CBR packets sent by the source and the number of packets received by the destination.

PDR = Total Received Packets/Total Sent Packets

Packet Loss Ratio: The ratio of number of dropped packets to the number of packets sent by source node.

Packet Loss Ratio = (Sent Packets-Received Packets)/ Sent Packets

Average End-to-End Delay: This is the average time involved in delivery of data packets from the source node to the destination node. To compute the average end-to-end delay, add every delay for each successful data packet delivery and divide that sum by the number of successfully received data packets. It is measured in milliseconds (ms).

Average End To End Delay= End To End Delay/ Received Packets

Energy Consumption: Energy consumption is an important metric for evaluating the performance of wireless network protocols .This study has added energy breakdown in each state in the traces to support detailed energy analysis. In addition to the total energy, now users will be able to see the energy consumption in different states at a given time. Following is an example from a trace file on energy.

[energy 979.917000ei 20.074 es 0.000 et 0.003 er 0.006]

The meaning of each item is as follows:

energy: total remaining energy
ei: energy consumption in IDLE state
es: energy consumption in SLEEP state
et: energy consumed in transmitting packets
er: energy consumed in receiving packets

4.4 Simulation Flow Diagram

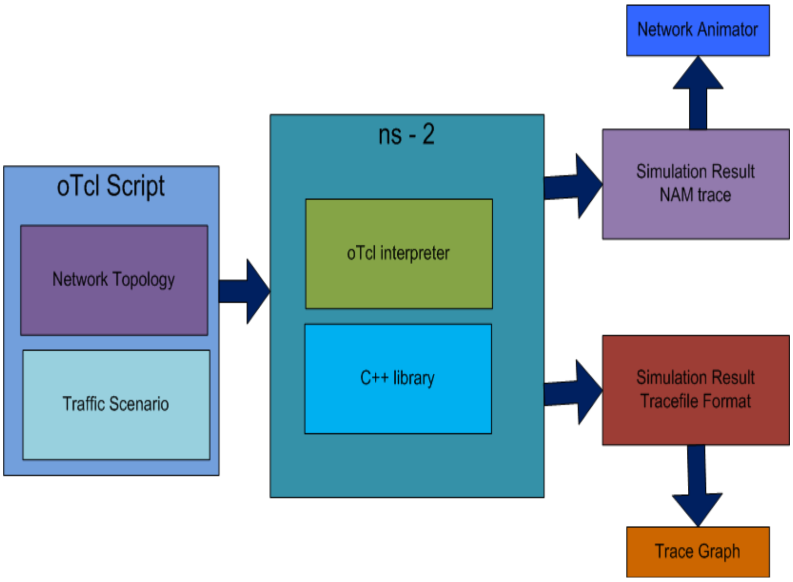


Figure 4.4: Simulation Flow Diagram in NS-2

V. SIMULATION RESULTS

From the experimental results of performance metrics - packet delivery ratio,packet lossratio, average end-to-end delay and energy consumption by the source node under black hole attack the following are observed.

5.1 Packet Delivery Ratio: From the graphs (Figure 5.1 & 5.2) below it is observed that packet delivery ratio is decreased when black hole node is introduced in the network i.e., PDR for general AODV scenario is 95.32% and for black hole scenario is 34.57%. Xgraph is plotted by extracting data from .tr file of .tcl using AWK scripts with time as X axis and PDR as Y axis.

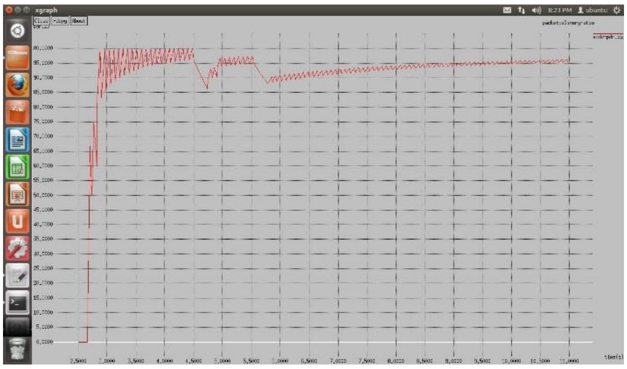


Figure 5.1: Graph for time v/s PDR for AODV

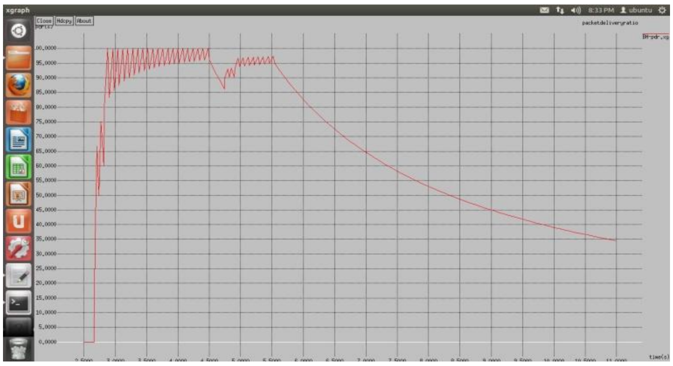
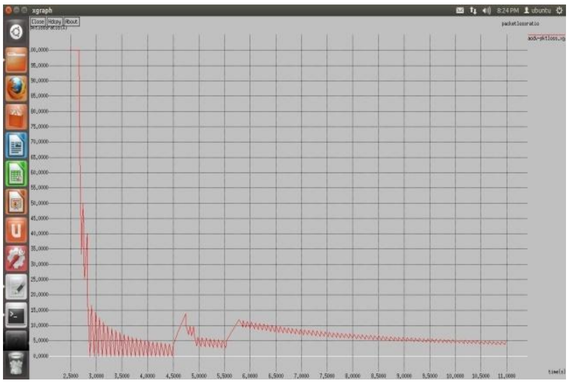


Figure 5.2: Graph for time v/s PDR for AODV under black hole attack



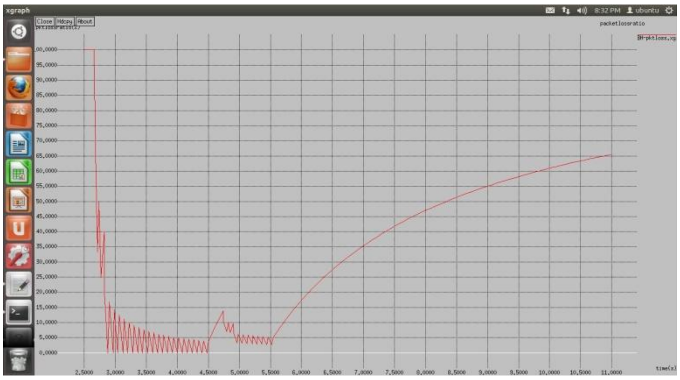
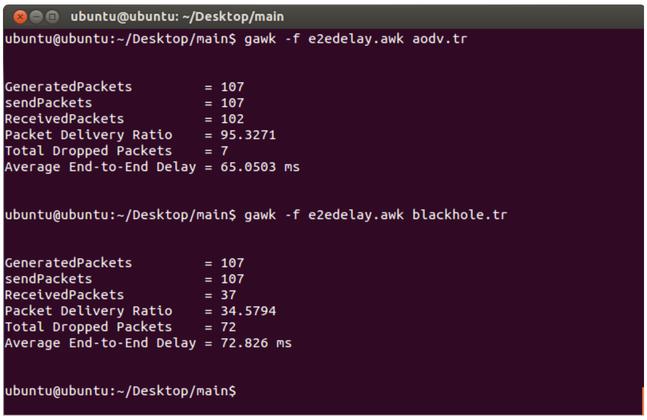


Figure 5.3: Graph for time v/s PLR for AODV **Figure 5.4: Graph for time v/s PLR for AODV under black hole attack**

5.3 Average End to End Delay

The average end to end delay for AODV and for black hole attack on AODV is 65.05 ms and 72.82 ms respectively as shown in the terminal (Figure 5.5)



```
ubuntu@ubuntu:~/Desktop/main$ gawk -f e2edelay.awk aodv.tr


GeneratedPackets         = 107
sendPackets              = 107
ReceivedPackets          = 102
Packet Delivery Ratio    = 95.3271
Total Dropped Packets    = 7
Average End-to-End Delay = 65.0503 ms


ubuntu@ubuntu:~/Desktop/main$ gawk -f e2edelay.awk blackhole.tr


GeneratedPackets         = 107
sendPackets              = 107
ReceivedPackets          = 37
Packet Delivery Ratio    = 34.5794
Total Dropped Packets    = 72
Average End-to-End Delay = 72.826 ms


ubuntu@ubuntu:~/Desktop/main$
```

Figure 5.5: Average end to end delay for AODV and Black hole

The above figure clearly shows that the average end to end delay for black hole is exceeded by 7.77 ms from that of AODV.

5.4Energy Consumption: Devices in a mobile network may rely on batteries or other exhaustible means as their power source. For these nodes, the conservation and efficient use of energy may be the most important system design criteria.Evaluation of energy consumed by the source node is carried out when there is a black hole attack in the network and the following graph (Figure 5.6) shows the result.

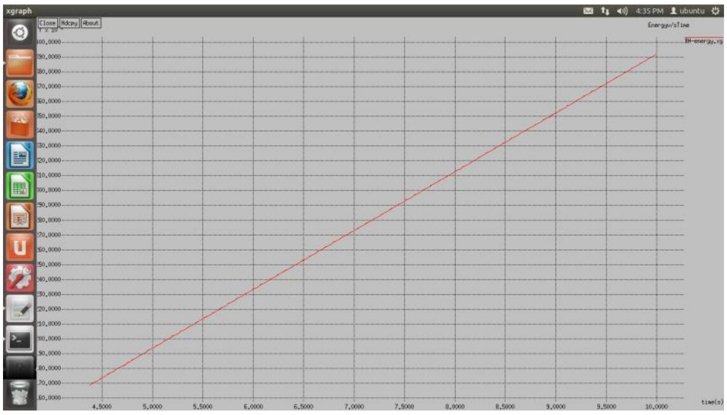


Figure 5.6: Graph for time v/s energy

It can be analyzed that after black hole attack the source node consumes 0.224163 joules of energy, which means 0.224163joules of energy goes in vain as the packets doesn't reach the destination, hence wastage of energy and failure in network.

VI. Conclusion and Future Work

This study analyses the effect of black hole attack on AODV performance. The simulation has been done using the network simulator (NS-2.35). The performance metrics like average end to end delay, packet delivery ratio, packet loss ratio and energy consumption by the source node under black hole attack has been evaluated and analysed. The simulation results show that when the black hole node exists in the network, it will affect and decrease the performance of AODV routing protocol.

The detection and prevention of black hole attack in the network exists as a challenging task. As future work, the study can be extended to

- Simulate and analyze the effect of the black hole attack in other routing protocols and intended to provide the solution for the black hole attack and compare its performance with the AODV protocol.
- Perform extensive simulation tests on mitigation of black hole attack for AODV and other routing protocols.

REFERENCES

1. ImrichChlamtacA, Marco ContiJennifer J.-N. Liu,**Mobile ad hoc networking: imperatives and challenges,**School of Engineering, University of Texas at Dallas, Dallas, TX, USAIstituto IIT, ConsiglioNazionaledelleRicerche, Pisa, ItalyDepartment of Computer Science, University of Texas at Dallas, Dallas, TX, USA

2. Saleh Ali K.Al-Omari, Putra Sumari, **An Overview Of Mobile Ad-Hoc Networks For The Existing Protocols And Applications,** School of Computer Science, Universiti Sains Malaysia, 11800 Penang, Malaysia,

3. GoitomAbrehaley, **Simulation-based Performance Evaluation of Selected Routing Protocols in Mobile Ad hoc Networks,** International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 04 – Issue 04, July 2015

4. C. PerkinsNokia Research Center, E. Belding-RoyerUniversity of California, Santa Barbara,S. DasUniversity of Cincinnati, **Ad hoc On-Demand Distance Vector (AODV) Routing,**RFC 3561, July 2003.

5. Kulbir Kaur Waraich and Barinderpal Singh, **Performance Analysis of AODV Routing Protocol with and without Malicious Attack in Mobile Ad-hoc Networks**, Research Scholar CSE Department, DAV University Jalandhar Punjab Research Scholar CSE Department, DAV University Jalandhar Punjab, International Journal of Advanced Science and Technology Vol.82 (2015), pp.63-70

6. Ali Dorri and Seyed Reza KamelandEsmailkheyrkhah, **Security Challenges in Mobile Ad-Hoc Networks: A Survey,** Department of Computer Engineering, Mashhad branch, Islamic Azad University, Mashhad, Iran, International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.1, February 2015.

7. PuneetKansalNishantPrabhat, Amit Rathee, **Black hole attack in Manet,** Department of ComputrerSc.&EnggPIET KurukshetraUniversty, International Journal of Advanced Research in Computer Science and Software Engineering .

8. Annapurna P Patil, Dr K Rajanikanth , BatheySharanya, M P Dinesh Kumar, Malavika J, **Design of an Energy Efficient Routing Protocol for MANETs based on AODV,** International Journal of Computer Science Issues, Vol. 8, Issue 4, No 1, July 2011.

9.Kulbir Kaur Waraich and Barinderpal Singh, **Performance Analysis of AODV Routing Protocol with and without Malicious Attack in Mobile Ad-hoc Networks**, Research Scholar CSE Department, DAV University Jalandhar Punjab Research Scholar CSE Department, DAV University Jalandhar Punjab.
10. Vinita Mishra1, Smita Jangale2, **Analysis and comparison of different network simulators,** International Journal of Application or Innovation in Engineering & Management (IJAIEM).
11.TeerawatIssariyakul • Ekram Hossain, **Introduction to NetworkSimulator NS2,** Department of Electrical & Computer Engineering University of Manitoba 75A Chancellor's Circle Winnipeg MB R3T 5V6.
12. J. Postel, User Datagram Protocol, RFC 768 ISI 28 August 1980
13.Navreet Kaur M.Tech CSE Student,SandhyaUmrao Research Scholar CSE Dept,Rajneesh Kumar GujralPh.D, **Simulation based Analysis of TCP Variants over MANET**
Routing Protocols using NS2, International Journal of Computer Applications (0975 – 8887)
Volume 99– No.16, August 2014
14.AmmarOdeh, EmanAbdelFattah and MuneerAlshowkan, **Performance Evaluation OfAodv And Dsr Routing**
Protocols InManet Networks, Department of Computer Science & Engineering, University of Bridgeport. International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012
15.N. Venkatadri , K. Ramesh Reddy , **Performance Metrics Comparison for On-demand Routing Protocols using NS2**, International Journal of Advanced Research in Computer Science and Software Engineering.
16.KamarularifinAbd. Jalil, Zaid Ahmad, Jamalul-LailAbManan, **Mitigation of Black Hole Attacks for AODV Routing Protocol,** International Journal on New Computer Architecture and Their Applications (IJNCAA) I(2): 336-343
17.PriyankaSonal Sao, JageshwerShriwas, RohitMiri, **Performance Evaluation of Black Hole Attack and Prevention Using AODV on MANET,** International Research Journal of Engineering and Technology (IRJET).
18.Madhav Sharma Prof. RajeshwarLalDua, **Evaluation of Different Performance Metrics of Wireless Sensor Networks in Different Topologies Using DSR Routing Protocol in NS-2 Simulator,** International Journal of Advanced Research in Computer Science and Software Engineering.
19. Ravi Kumar, Prabhat Singh, **Performance analysis of AODV, TORA, OLSR and DSDV Routing Protocols using NS2 Simulation,** International Journal of Innovative Research in Science, Engineering and Technology.
20. Marc Greis, **Tutorial for Network Simulator "ns",** expanded byVINT group**.**
21.Eitan Altman and Tania, **NS Simulator for Beginners,** Univ. d Los Andes, France.