ENERGY CONSUMPTION ANALYSIS OF ANTI-BLACK HOLE ATTACK MECHANISM FOR AODV ROUTING PROTOCOL IN MANET

[1]Fawaz Mahiuob, Mohammed Mokbal, [2]Khalid Saeed

[1] Computer Science/IT Department IBMS, The University of Agriculture Peshawar, Pakistan

[2] Computer Science/IT Department IBMS, The University of Agriculture Peshawar, Pakistan

Corresponding author: Email: khalidsaeed@aup.edu.pk

ABSTRACT*: Mobile Ad-hoc Networks (MANETs) are a set of nodes which can move freely and are connected by means of wireless medium, in which the nodes have limited energy, limited memory, and limited processing capabilities, as well as speed and data transfer rate are limited. MANETs are vulnerable to different attacks because communication can be done among nodes via a wireless communication links, and nodes are free to join and leave the network. Routing protocols require energy to perform routine tasks and transfer data packets. Therefore, these protocols need to be protected against attacks and at the same time they should be able to keep the energy of the node. There are many routing protocols strategies to maintain energy, but these strategies lacks in protection from attacks. We developed an Anti-Black Hole attack mechanism for AODV routing protocol (ABHMAODV) which can detect and eliminate black hole attach completely. This research is based on energy consumption analysis of Anti Black Hole Attach Mechanism for AODV Routing Protocol. For extensive simulations, eight ABHMAODV and eight AODV scenarios have been considered. The proposed and existing protocols are tested in both under attack and without attack scenarios in which the number of mobile nodes, Black Hole nodes and connection link number are different. The simulation is done using Network Simulator (NS2.35). Simulation results proved that the proposed ABHMAODV protocol can be adopted for any routing strategy, in order to increase the efficiency of the network in different aspects and scenario. At the same time the proposed approach provides protection from the black hole attack up to 100%.*

Keywords: MANET; AODV; Anti Black Hole Attack Mechanism for AODV; Energy Consumption Analysis; NS2.35.

1. INTRODUCTION

A set of wireless nodes makes mobile ad hoc network (MANET) which can be set up dynamically anywhere and anytime without the need of earlier established network infrastructure. It is called an autonomous system because mobile nodes are free to move randomly and communication can be done among them via a wireless communication links. The node sometimes acts as a host and sometimes act as a router [1],[2]. Moreover, the network topology also frequently changes. These nodes cooperate with each other in order to do routine tasks in the network [1]. It is called infrastructure-less networks because it is temporary and has a short-range [3].

Since the communication among two nodes in the network consumes energy and energy is associated with cost, therefore, it is necessary to reduce the cost of energy which is required for communications, for the purpose of improving the life of nodes in the network.

This research has compared the energy consumption of AODV and ABHMAODV using the network simulator NS2 [4] with an increased density nodes, increased communication links and increased number of the attack nodes. The tcl scripting language has been used for configuring the scenarios [5].

There is a need of protocols in order to pass the packets in the network. There are several routing protocols in MANETs which lies under different categories such as proactive, reactive and hybrid routing protocols. This research is based on Anti-Black Hole attack mechanism for Ad-hoc On-demand Distance Vector (AODV) Routing Protocol which is a reactive routing protocol.

This research paper is summarized as: section 2 consist of basic operation of AODV Routing Protocol, section 3 contains the relevant work done, section 4 includes details about simulation, section 5 consists of details about results and discussion, section 6 include brief conclusion and future work.

2. AODV ROUTING PROTOCOL

The Ad hoc On-Demand Distance Vector (AODV) is a reactive routing protocol, which offers rapid acclimation to dynamic link situation, less processing use, reduces the overhead of memory, less network bandwidth use, and set unilateral path to targets inside the ad hoc network. The AODV protocol uses a table of routes, which keeps information on recent routes which has been used by the recent node. In other words, AODV maintains routes only between nodes which need to communicate with each other. Each mobile node keeps a routing table which maintains information about next-hop of a path towards the target node. The protocol uses two functions such as route discovery and route maintenance [6].

In AODV routing protocol operation when the source node needs to communicate with the target node and does not have a fresh-route or does not have known route, than the source node broadcast RREQ message to its neighbour nodes. Moreover, the process will continue till finding an intermediary node, which has a fresh-enough-route to the target node or to find the same target node. In order to avoid the same RREQ message forwarded from different neighbours, the node handling route request RREQ will accept the first one received, and ignore the other copies. When the route request reaches to the neighbour node and it does not have a fresh enough route and valid route to the target node specified in the RREQ, than the neighbour node forwards the request to the rest of its neighbour nodes through re-broadcast RREQ message. In addition, it establishes the opposite route and records it in the routing table [6].

3. RELATED WORK

Margi and Obraczka [8] suggested instrumentation energy model for the sake of allowing them to sufficiently and strictly account for the energy consumed by ad hoc network protocols' communication-related tasks completed by clearly accounting for all potential airing states, i.e, receiving, transmitting, overhearing, idle, sleeping, sensing, and seeing the diverse energy charges associated with each one of them.

Kanakaris et al. [9] conducted a study to evaluate the efficiency of four protocols for some energy metrics which are used in ad hoc networks, taking into consideration mobility. Overall results showed that in small networks there is no significant difference in terms of energy consumption and throughput. As for medium and large size ad hoc networks, it has been proved that, the TORA protocol performance is not effective. However, the results showed a good performance for AODV and DSR protocols with the medium and large size networks, and the performance of AODV protocol in terms of throughput was well in all the scenarios that have been evaluated.

Gouda et al. [10] compared DSDV and AODV routing protocols in MANETs relying on the energy aware performance metrics, the comparison outcomes proved that the AODV was able to adapt for any routing strategy in terms of increasing the network lifetime and is better than DSDV.

Karadge and Sankpal [11] suggested a routing scheme to enhance packet delivery ratio and network lifetime for AODV named as maximum energy level AODV (Mel-AODV). The proposed mechanism compiles the gross node energy on the connection as path selection metric. The proposed routing scheme lengthens the system lifetime and enhance the packet delivery ratio.

Krishnamoorthy and Arivazhagan [12] suggested an energy efficiency method in routing protocols for Mobile Ad-hoc network. In this approach, the remaining energy and hop count are used as variables during route selection. The route choice depends on the largest minimum remaining energy and the shortest hop count. A range of the neighbour's node is used to control transmission power of node.

4. SIMULATION ENVIRONMENT

This research is based on analysing the energy consumption of our earlier proposed mechanism for AODV protocol such as anti-black hole attack mechanism for AODV routing protocol which was proposed and published by us [7] to detect black hole attack while using AODV routing protocol and eliminating the attack completely, moreover the mechanism maintains the performance of the AODV protocol while eliminating black hole attacks. The mechanism consists of:

- Detection method.
- Blacklist entry-using functions.
- Implementation of the protection system through an integrated algorithm.

The proposed mechanism requires a simple modification in the algorithm to eliminate the black hole attack without compromising the efficiency of the basic protocol. Since this research is based on the analysis of energy consumption of our earlier proposed mechanism which was published [7] therefore the algorithm is reproduced for the purpose of understanding.

4.1 Algorithm

A simple amendment in the protocol algorithm has been done to eliminate the black hole attack [7].

The algorithm is as follows:

a. If (am source node) {
   1. Get the des_Sq#_rt from my own routing table;
   2. Get the des_Sq#_pck from header packet of RREP;
   3. // call detection method
   4. If ((node which sent RREP not in black-list) and (des_Sq#_pck> des_Sq#_rt+gap)) {
   5. Attack= true;
   6. Call black-list
   7. Insert this node into black-list;
   8. Do not update my routing table;
   9. Drop route; Packet free; Return; }
   10. Else If (node sent RREP is in black-list) {
   11. Attack= true;
   12. Update time for this node in black-list;
   13. Do not update my routing table;
   14. Drop route; Packet free; Return; }
   15. If ((node sent RREP is not in black-list) or (des_Sq#_pck < des_Sq#_rt+gap)) {
   16. Attack= false;
   17. Update my routing table; Return; } }

b. If (am not source node "intermediate") {
   1. Get the des_Sq#_rt from my own routing table;
   2. Get the des_Sq#_pck from header packet of RREP;
   3. // detection method
   4. If ((node sent RREP is not in black-list) and (des_Sq#_pck > des_Sq#_rt+gap)) {
   5. Attack= true;
   6. Do not forward this packet;
   7. Do not update my routing table; }
   8. Else If (node sent RREP is in black-list) {
   9. Attack= true;
   10. Do not forward this packet;
   11. Do not update my routing table; }
   12. Else {
   13. Attack= false;
   14. Forward this packet;
   15. Update my routing table; }

4.2 Energy Model

The energy model used in this research is shown in Table1, which is used to measure the power consumed in each state (i.e. Transmission (Tx), Reception (Rx), Idle, Sleep, transitionPower and transitionTime states). The transmission mode is equal to the energy consumed (Watt) for transferring each packet, reception mode is equal to the energy consumed (Watt) for receiving each packet, idle mode is equal to the energy consumed (Watt) when the node is in idle mode, sleep mode is equal to the energy consumed (Watt) when the node is in sleep mode, transitionPower is equal to the energy consumed (Watt) in state transition from sleep to idle and

transitionTime is the time (second) which is used in state transition from sleep to idle.
Worth mentioning that ad hoc nodes have never been put into power saving mode.

4.3 Simulation Methodology

This research work has been divided into groups based on the number of nodes, which are total four groups, each group containing two scenarios such as normal and under attack.
The first group contains 10 nodes and 1 communication link in normal operation such as without attack, and 1 black hole node while under attack.
The second group contains 20 nodes and 2 communication links in normal operation such as without attack, and 2 black hole nodes while under attack.
The third group contains 30 nodes and 3 communication links in normal operation such as without attack, and 3 black hole nodes while under attack.
The fourth group contains 40 nodes and 4 communication links in normal operation such as without attack, and 4 black hole nodes while under attack.
This research consists of a total 16 scenarios. The scenarios are simulated separately by using the parameters in table 1.

Table 1: **Simulation Parameters.**

Parameters	Values
Operating System	Linux Mint Release 17.2
Network Simulator	NS2.35
Type of Channel	Wireless Channel
Radio Propagation Model	Two Ray Ground
Type of Antenna	Omni Antenna
Type of Interface queue	DropTail/PriQueue
Max Packet in Ifqueue	50
Type of Network Interface	Phy/WirelessPhy
Type of MAC layer	Mac/802.11
Simulation Area	1000m x 1000m
Initial Energy	100 Joule
Transmission Power	2.0 W
Reception Power	1.0 W
Idle Power	0.010 W
Sleep Power	0.001 W
Transition Power	0.2 W
Transition Time	0.005 S
Routing Protocols	AODV, ABHMAODV, with AODVblackhole
Type of Attack	Black Hole attack
Mobility Model	Random Waypoint
Simulation Time	300 seconds
Number of Scenarios	16 (4x4)
Number of Nodes	10,20,30,40
Node Speed	20m/s

4.4 Performance Parameters

i. Total Energy consumed: The overall energy consumed as a whole by the nodes in the network.
ii. Average Energy Consumed by each node: The overall energy consumed as a whole by the nodes vs the number of nodes in the network
iii. Average residual energy for each node: Total energy remaining for all nodes after transmission divided by the number of nodes in the network
iv. Packet Sent: Total number of data packets sent by the source nodes within simulation time.
v. Packet Received: Total number of data packets received by the target node within simulation time.
vi. Drop Rate: Total data packets dropped vs all data packets sent.
vii. Throughput Rate [bps]: Throughput is the number of packets successfully reached at target per unit time (total size of packets received vs total time taken for transmission).
viii. Packet Delivery Ratio: total packets received by target vs total packets sent by the source.
ix. End-To-End delay Rate: End-To-End delay is equal to the time(s) at moment the data packet have received from the target node minus time (s) at moment the data packet have sent from the source node. The average delay = Total delay/received packet.
x. Normalized Routing Load: total routing packets transmitted at network layer vs total data packets received at the application layer.
xi. Routing overhead: whole routing packets transmitted including the packets which are forwarded at network layer.

5. RESULTS AND DISCUSSION

Table 2 to 9 shows the energy consumption analysis of AODV and ABHMAODV for different scenarios, which are under attack and normal operation without attack.
Table 2 and 3 shows the results of energy consumption analysis of normal AODV without attack for four scenarios such as 10, 20, 30 and 40 nodes by using AWK scripting language for analysing the trace files.

Table 2: **Energy Consumption Analysis of Normal AODV**

No. of Nodes	Packet Sent	Packet Received	Packet Dropped	Total Energy Consumed by All Nodes	Average Energy Consumed by each Node	Average Residual Energy for each Node
10	1196	1196	0	252.381	25.2381	74.7619
20	2392	2392	0	626.748	31.3374	68.6626
30	3588	3586	2	1764.69	58.823	41.177
40	4784	4596	188	2304.42	57.6105	42.3895

Table 3: Energy Consumption Analysis of Normal AODV

No. of Nodes	PDR%	Average Throughput(bps)	Average Throughput[kbps]	End-To-End Delay(s)	Routing Loud	Normalized Routing Loud
10	100	612352	16.40	0.0262611	24	0.020
20	100	1224704	32.79	0.0501415	44	0.018
30	99.9443	1837056	49.19	0.0348781	95	0.026
40	96.0702	2353152	63.00	0.143690	566	0.123

Table 4 and 5 shows the results of energy consumption analysis of AODV under attack for four scenarios such as 10, 20, 30 and 40 nodes. The results show that the black hole attack was able to manipulate in determining the route in order to be through itself, and then dropping all packets that were supposed to pass through it. The target node did not receive any packet, therefore, the PDR and throughput becomes zero, moreover, the end-to-end delay and normalized routing load becomes infinite due to the division of result value by zero.

Table 4: Energy Consumption Analysis of AODV under Attack

No. of Nodes	Packet Sent	Packet Received	Packet Dropped	Total Energy Consumed by All Nodes	Average Energy Consumed by each Node	Average Residual Energy for each Node
10	1196	0	1196	104.203	10.4203	89.5797
20	2392	0	2392	343.934	17.1967	82.8033
30	3588	0	3588	929.759	30.992	69.008
40	4784	0	4784	1231.72	30.793	69.207

Table 5: Energy Consumption Analysis of AODV under Attack

No. of Nodes	PDR%	Average Throughput(bps)	Average Throughput[kbps]	End-To-End Delay(s)	Routing Loud	Normalized Routing Loud
10	0	0	0	N/A	12	N/A
20	0	0	0	N/A	44	N/A
30	0	0	0	N/A	102	N/A
40	0	0	0	N/A	172	N/A

Table 6 and 7 show the result of energy consumption analysis of normal ABHMAODV for four scenarios such as: 10, 20, 30 and 40 nodes. Results show that the performance of ABHMAODV and AODV without attack are close to each other with the slight better results produced by ABHMAODV.

Table 8 and 9 show the result of energy consumption analysis parameters of ABHMAODV under attack for four scenarios: such as 10, 20, 30 and 40 nodes. The result shows that the black hole attack was eliminated completely, and the effect that was emerged in the AODV under attack condition has completely finished in the ABHMAODV under attack scenario. Moreover the network functionality becomes normal even under attack.

Table 6: Energy Consumption Analysis of Normal ABHMAODV

No. of Nodes	Packet Sent	Packet Received	Packet Dropped	Total Energy Consumed by All Nodes	Average Energy Consumed by each Node	Average Residual Energy for each Node
10	1196	1196	0	252.489	25.2489	74.7511
20	2392	2392	0	626.653	31.3327	68.6673
30	3588	3587	1	1556.77	51.8925	48.1075
40	4784	4710	74	2586.55	64.6638	35.3362

Table 7: Energy Consumption Analysis of Normal ABHMAODV

No. of Nodes	PDR%	Average Throughput(bps)	Average Throughput[kbps]	End-To-End Delay(s)	Routing Loud	Normalized Routing Loud
10	100	612352	16.40	0.02627	24	0.020
20	100	1224704	32.79	0.0501	44	0.018
30	99.9721	1837056	49.19	0.03445	123	0.034
40	98.4532	2411520	64.56	0.15649	407	0.086

Table 8: Energy Consumption Analysis of ABHMAODV under Attack

No. of Nodes	Packet Sent	Packet Received	Packet Dropped	Total Energy Consumed by All Nodes	Average Energy Consumed by each Node	Average Residual Energy for each Node
10	1196	1196	0	252.304	25.2304	74.7696
20	2392	2392	0	626.897	31.3449	68.6551
30	3588	3586	2	1560.24	52.0078	47.9922
40	4784	4710	74	2336.67	58.4167	41.5833

Table 9: Energy Consumption Analysis of ABHMAODV under Attack

No. of Nodes	PDR%	Average Throughput(bps)	Average Throughput[kbps]	End-To-End Delay(s)	Routing Loud	Normalized Routing Loud
10	100	612352	16.40	0.01794	12	0.010
20	100	1224704	32.79	0.05022	44	0.018
30	99.9443	1836032	49.16	0.05721	217	0.061
40	98.4532	2411520	64.57	0.16255	568	0.121

The figures 1, 2, and 3 show the total energy consumed by all nodes for all scenarios, average energy consumed by each node and average residual energy for each node in each scenario. The results show that the original AODV has consumed more energy as compared to normal ABHMAODV and ABHMAODV under attack in 30 nodes scenario, although the percentage of PDR is 99.9443%, while ABHMAODV and ABHMAODV under attack have PDR values of 99.9721% and 99.9443% respectively. In 40 nodes scenario, normal ABHMAODV has more energy than original AODV but this is due to its PDR is high as compared to AODV. The AODV under attack consumed less power, due to the absence of any transfer of packets between the source and target, moreover PDR and throughput is equal to 0%.

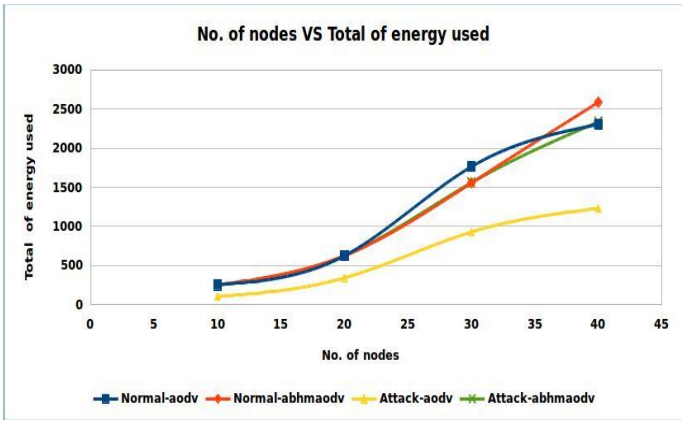

Figure 1: **Total Energy Consumed by All Nodes**

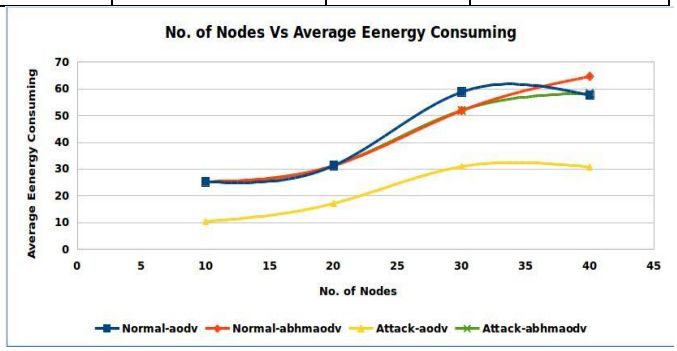

Figure 2: **Average Energy Consumption**

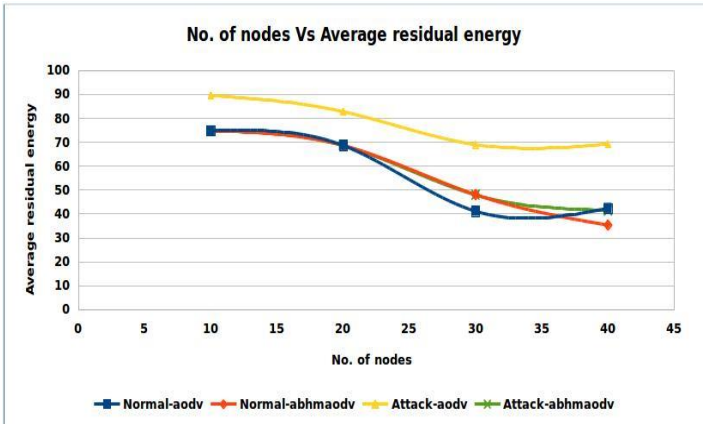

Figure 3: **Average Residual Energy**

The figures 4 and 5 show the packets sent, and packets received for each scenario. The result shows that both protocols sent equal packets but with a slight difference in the received packets, which appeared clearly in the scenario having 40 nodes, which demonstrate that the normal ABHMAODV has received more packets as compared to normal AODV. Moreover, in case of attack, ABHMAODV under attack sent and received packets successfully, which shows that it has successfully eliminated black hole attack.

While in the scenario of AODV under attack, no packet has been received due to the black hole attack.

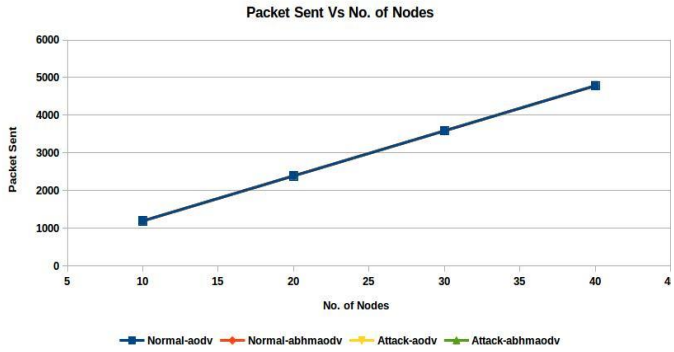

Figure 4: **Packets Sent.**

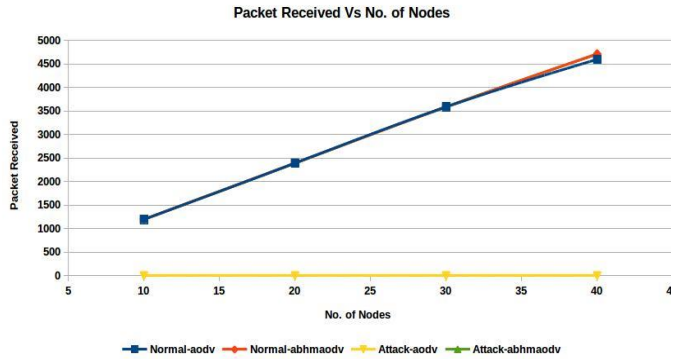

Figure 5: **Packets Received.**

The figure 6 shows the average packets dropped in each scenario. The result shows that ABHMAODV without attack or under attack works better as compared to AODV in some scenarios, and work equally in the other scenarios. In the scenario of AODV under attack all packets have been dropped.

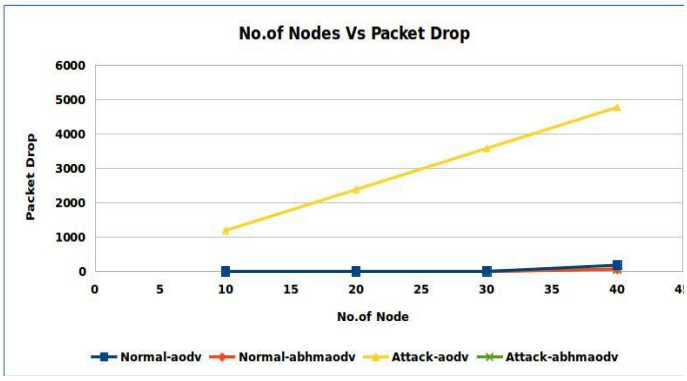

Figure 6: **Packet Dropped**

Figure 7 and 8 show the average throughput and average packet delivery ratio of each scenario. The result shows that ABHMAODV without attack or under attack works better than AODV in some scenarios, and work equally in the others. Whereas average throughput and average packet delivery ratio in the scenario of AODV under attack is equal to 0%.

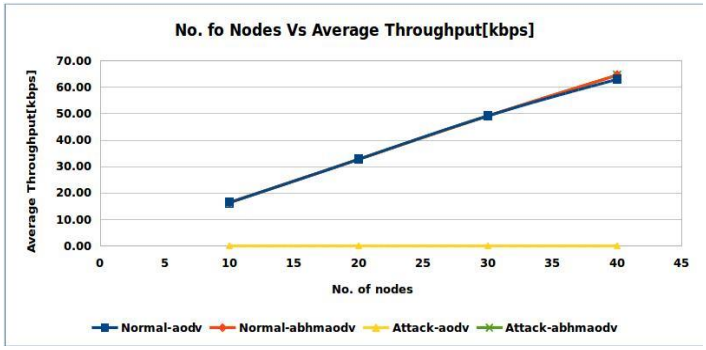

Figure 7. Average Throughput (Kbps)

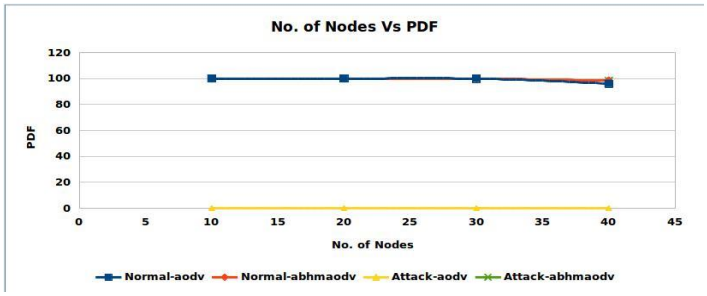

Figure 8: Average Packet Delivery Ratio

Figures 9 and 10 show the average delay and normalized routing load of each scenario. The result shows that ABHMAODV and AODV without attack produced almost same results. In the scenario of ABHMAODV under attack there are variations in the delay because when the nodes were less, the delay was also less as compared to normal AODV, while in the scenario of 20 the results equal, and in the scenario of 30 and 40 nodes it increased slightly. While in the scenario of AODV under attack, the values are not known due to the absence of any packets received.

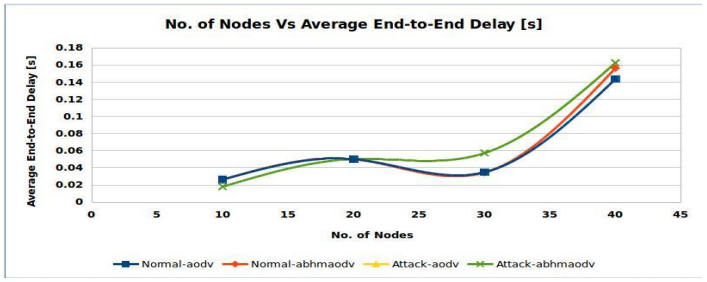

Figure 9: Average Delay

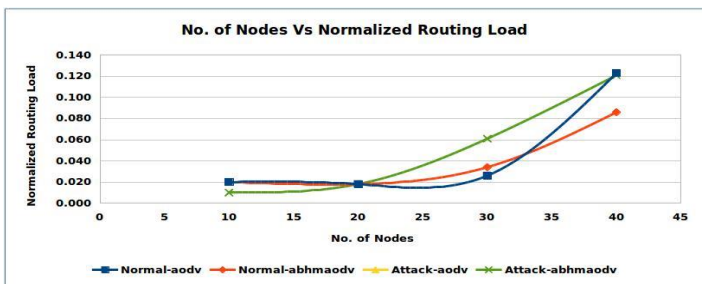

Figure 10: Normalized Routing Load

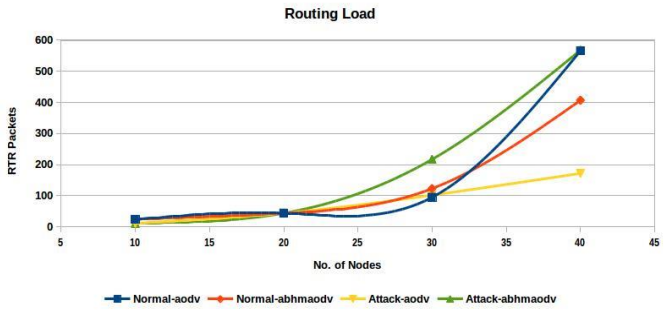

Figure 11: Routing load

Figure 12, 13, 14, and 15 show energy consumption at each node for each scenario. The results show that ABHMAODV without attack or ABHMAODV under attack are almost same to AODV without attack in most scenarios. In the scenario of AODV under attack, the energy consumption is much lower as compared to the normal case, which shows that the network is not working properly.

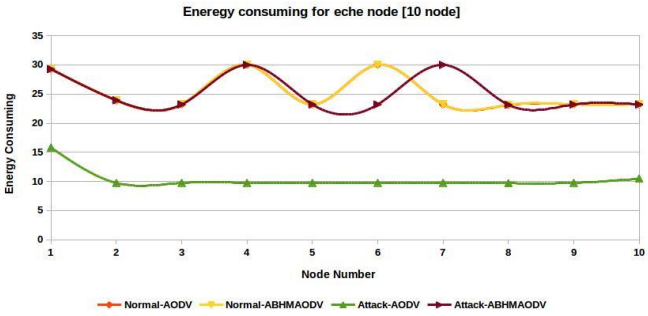

Figure 12: **Energy Consumption at Each Node (Scenario 10 Nodes)**

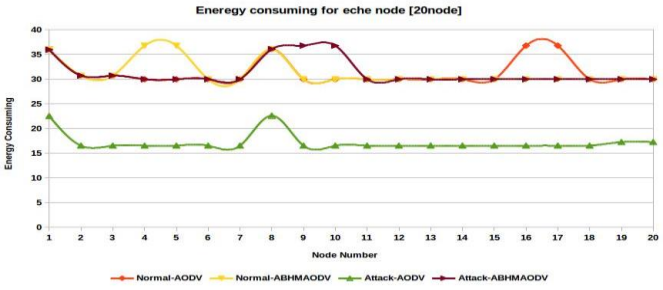

Figure 13: Energy Consumption at Each Node (Scenario 20 Nodes)

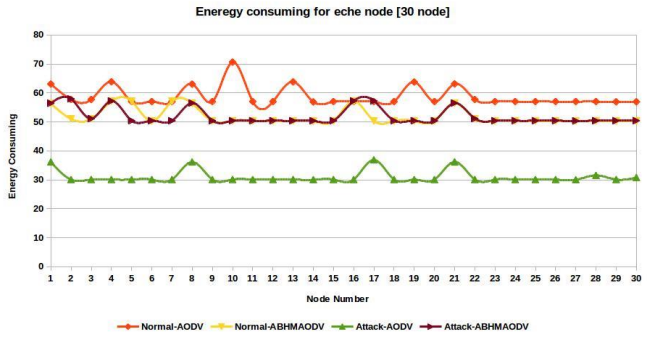

Figure 14: Energy Consumption at Each Node (Scenario 30 Nodes)

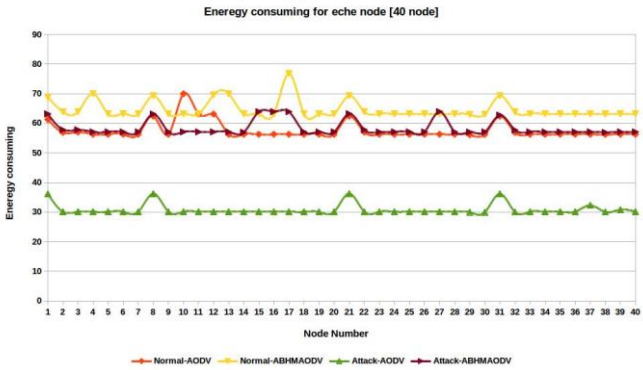

Figure 15: Energy Consumption at Each Node (Scenario 40 Nodes)

6. CONCLUSION AND FUTURE WORK

Conclusions

The analysis of energy consumption of AODV and ABHMAODV under black hole attack and without black hole attack is done in NS2.35 by increasing the number of nodes, number of connection link and the number of black hole attack nodes. It is concluded that ABHMAODV in both without attack scenario and under attack scenario performs well in terms of packet delivery ratio PDR and throughput as compared to AODV protocol. The energy consumption of ABHMAODV in without attack scenario and under attack scenario is less as compared to AODV except for a very few situations. Moreover, it has been concluded that the network while using ABHMAODV is considered fully protected from the black hole attack.

Future work

This research has analysed AODV and ABHMAODV protocols regarding their energy consumption, whereas in future this mechanism (ABHMAODV) can be improved in order to protect against other types of attacks and at the same time maintaining performance.

REFERENCES

[1] Corson, S., and J. Macker. "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501." (1999).

[2] Chlamtac, Imrich, Marco Conti, and Jennifer J-N. Liu. "Mobile ad hoc networking: imperatives and challenges." *Ad hoc networks* 1.1 (2003): 13-64.

[3] Sreenath, N., A. Amuthan, and P. Selvigirija. "Countermeasures against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol in MANETs." *Computer Communication and Informatics (ICCCI), 2012 International Conference on*. IEEE, 2012.

[4] Issariyakul, Teerawat, and Ekram Hossain. *Introduction to network simulator NS2*. Springer Science & Business Media, 2011.

[5] Ousterhout, John K. "TCL and the TK Toolkit." *Computer Science Division, Department of*

Electrical Engineering and Computer Science, University of California, Berkeley (1993).

[6] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das. *Ad hoc on-demand distance vector (AODV) routing*. No. RFC 3561. 2003.

[7] Mahiuob, Fawaz, and Khalid Saeed. "Anti-Black Hole Attack Mechanism for Ad Hoc On-Demand Distance Vector (AODV) Routing Protocol in Manets."*International Journal of Computer Applications* 135.11 (2016): 37-45.

[8] Margi, Cintia B., and Katia Obraczka. "Instrumenting network simulators for evaluating energy consumption in power-aware ad-hoc network protocols."*Modeling, Analysis, and Simulation of Computer and Telecommunications Systems, 2004.(MASCOTS 2004). Proceedings. The IEEE Computer Society's 12th Annual International Symposium on*. IEEE, 2004.

[9]Kanakaris, Venetis, David Ndzi, and Djamel Azzi. "Ad-hoc networks energy consumption: a review of the ad-hoc routing protocols." *Journal of Engineering Science and Technology Review (JESTR)* 3.1 (2010): 162-167.

[10] Gouda, Bhabani Sankar, Arkaprava Bhaduri Mandai, and K. Lakxmi Narayana. "Simulation and comparative analysis of energy conservation performance metric for ERAODV, AODV and DSDV routing protocols in MANET." *Information and Communication Technologies (WICT), 2012 World Congress on*. IEEE, 2012.

[11] Karadge, P. S., and Dr SV Sankpal. "A performance comparison of energy efficient AODV protocols in mobile ad hoc networks." *International Journal of Advanced Research in Computer and Communication Engineering* 2.1 (2013).

[12] Krishnamoorthy, Thamizhmaran, and Akshaya Devi Arivazhagan. "Energy efficient routing protocol with ad hoc on-demand distance vector for MANET." *Intelligent Systems and Control (ISCO), 2015 IEEE 9th International Conference on*. IEEE, 2015.