International Journal of Engineering & Technology, *7 (4.34) (2018) 358-363*

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Comparative Performance AODV-ANT and AOMDV-ANT in BlackHole

Ajeng Mayang*, Savitri Galih

Faculty of Engineering, Widyatama University, Indonesia
**Corresponding author E-mail: ajeng.mayang@widyatama.ac.id*

Abstract

In this paper, we simulate the black hole attack to compare performance AODV-ANT and AOMDV-ANT to support the advance of the node communications to deliver a good management. In our simulation, the result shows AODV-ANT has decrease packets receive in Blackhole attack comparing without black hole until 0.03%, and while in AOMDV-ANT decrease until 0.47%. But, in throughput, AOMDV-ANT is better than AODV-ANT. The result is AOMDV-ANT has decrease throughput in Blackhole attack comparing without black hole until 0.93%, and while in AODV-ANT decrease until 1.85%. Then, in packet delivery ratio (PDR), AODV-ANT has decrease PDR in Blackhole attack comparing without black hole until 10.357%, and while in AOMDV-ANT decrease until 13.57%. In simulation performed, the impact of the black hole can be seen in the PDR. This occurs because of the random node mobility. For our simulations using NS-2:35 as a tool.

Keywords: *MANET, AODV, AOMDV, Ant-Net, Black Hole Attack.*

1. Introduction

A mobile ad hoc network (MANET) communication is where all nodes are mobile and communicate each other via wireless connections [4]. Ad-hoc network is characterized by dynamic topology, self-configuration, self-organization, restricted power, temporary network and lack of infrastructure [8]. In this way, ad-hoc networks has a dynamic topology such as nodes can easily join or leave the network at any time. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks [2]. These include passive eavesdropping, active interfering, impersonation, and denial-of-service Blackhole attack is one of many possible attacks in MANET [9].

The paper study about performance routing algorithm for packet routing in MANETs based on observed AODV-ANT algorithm comparing to AOMDV-ANT algorithm in black hole attack. ACO is a learning algorithm, and improving performance as time passes [12]. ACO stores information regarding past links and their worthiness, and uses that information to find an optimal route. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks. One of these attacks is the Black Hole attack. In the Black Hole attack, a malicious node absorbs all data packets in itself, similar to a hole which sucks in everything in. In this way, all packets in the network are dropped. In any case, nodes in the network will constantly try to find a route for the destination which makes the node consume its battery in addition to lose packets [2].

Efficient routing in Ad-hoc network should have the routing protocols limit the number of nodes when be informed of topology change. Routing protocol in routing network in real is not ideal, we have some attack like malicious in black hole in network. In the research work we argue that the two key objective are to comparing between two algorithms in black hole case.

1. The protocols must involve multiple path between source and destination. The protocols is used AODV and AOMDV with ANT algorithm to optimize and expected can be handling when a route is failure.
2. We compare the AODV-ANT algorithm and AOMDV-ANT algorithm without black hole attacks and with black hole attacks. The aim of present research work is to provide a comprehensive analysis comparing AODV-ANT and AOMDV-ANT in black hole.

In our study, we simulate the Black Hole attack in wireless ad-hoc networks and evaluate its damage in the network [2]. We make our simulations using NS-2 (Network Simulator version 2.35).

2. Related Work

Wireless networks are network which are used to communicate between computers and their devices by using radio frequency. These networks must be in their range and have equal status for communication between nodes otherwise the nodes cannot be communicated. The wireless network can be classified into two types: Infrastructure or Infrastructure less network. Infrastructure networks the nodes are mobile but base stations are fixed. But in Infrastructure less networks the nodes can move but base stations are also not fixed [10].

2.1. Ad-Hoc On-Demand Distance Vector Routing (AODV) Routing Protocols in Black Hole

The AODV routing protocol is an adaptation of the DSDV protocol for dynamic link conditions. Every node in an ad hoc network maintains a routing table, which contains information about the route to a particular destination. Whenever a packet is to be sent by a node, it first checks with its routing table to determine whether a route to the destination is already available. If so, it uses that route to send the packets to the destination. If a route is not available or the previously entered route is inactivated, then the node initiates a route discovery process. A RREQ (Route REQuest) packet is broadcasted by the node. Every node that receives the RREQ packet first checks if it is the destination for that packet and if so, it sends back an RREP (Route Reply) packet. If it is not the destination, then it checks with its routing table to determine if it has got a route to the destination. If not, it relays the RREQ packet by broadcasting it to its neighbors. If its routing table does contain an entry to the destination, then the next step is the comparison of the 'Destination Sequence' number in its routing table to that present in the RREQ packet. This destination sequence number is the sequence number of the last sent packet from the destination to the source. If the destination sequence number present in the routing table is lesser than or equal to the one contained in the RREQ packet, then the node relays the request further to its neighbors. If the number in the routing table is higher than the number in the packet, it denotes that the route is a 'fresh route' and packets can be sent through this route. This intermediate node then sends a RREP packet to the node through which it received the RREQ packet. The RREP packet gets relayed back to the source through the reverse route. The source node then updates its routing table and sends its packet through this route. During the operation, if any node identifies a link failure it sends a RERR (Route ERRor) packet to all other nodes that uses this link for their communication to other nodes. This is illustrated in Fig. 1a and b. Since AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node M can carry out many attacks against AODV. This paper provides routing security to the AODV routing protocol by eliminating the threat of 'BlackHole' attacks [7].

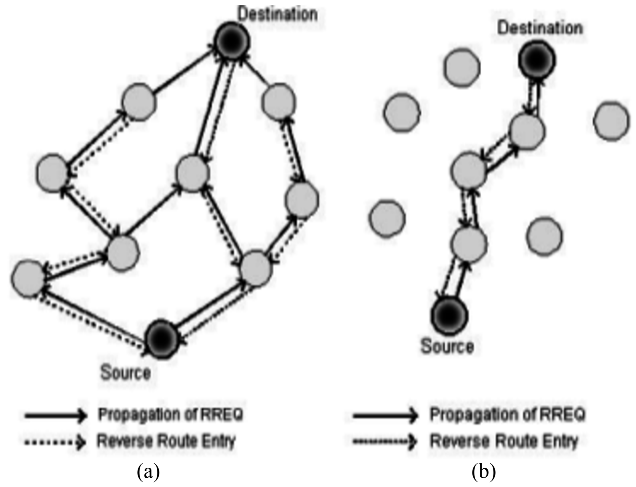


Fig. 1: Propagation of (a) RREQ (b) RREP [7]

2.2. Ad-Hoc on-Demand Multipath Distance Vector Routing (AOMDV) Routing Protocols in Black Hole

Ad hoc On-Demand Multipath Distance Vector (AOMDV) shares numerous characteristics with AODV. It is based on the distance vector routing and uses hop-by-hop routing approach. Furthermore, AOMDV also finds routes on demand using a procedure of route discovery. The main difference is in the number of routes found in each route discovery. In AOMDV, route request (RREQ) transmission from the source towards the destination establishes multiple reverse paths both at intermediate nodes as well as the destination. Multiple route reply (RREPs) traverse these reverse paths back to form multiple forward paths to the destination at the source and intermediate nodes. Note that AOMDV also provides intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency. AOMDV relies on the routing information already available in the underlying AODV algorithm, thereby limiting the overhead incurred in discovering multiple paths. It does not employ any special control packets. In reality, extra RREPs and RERRs for multipath discovery and maintenance along with a few extra fields in routing control packets (i.e., RREQs, RREPs, and RERRs) constitute the only additional overhead in AOMDV relative to AODV [7].

2.3. Ant Colony Optimization

It is one of most successful and distributed algorithm of swarm intelligent. It is meta-heuristic algorithm for solving combinatorial problems. It uses the principle searching behavior of real ants. These ants do not communicate directly, but communicate through a chemical substance called pheromone. The ants deposit it when they are going from nest to that food source. This chemical substance makes the path for other ants. The ant walks toward food source and follow the path where pheromone substance value is maximum. The other ants find that substance through their smell. These agents (ants) moving around in the network from one node to the other, updating routing tables (called pheromone table) of the nodes that they visit with what they have learned in their traversal so far. The path is chosen according to amount of pheromone. The ant follows that path also add their pheromone and increases the amount and mostly shorter path have more concentration of pheromone. The longer path has less than shorter. This substance fades (decreases) their concentration if that path is not in use for long time then it disappears [10].

2.4. Blackhole Attack and Classification

In Blackhole attack, all network traffics are redirected to a specific node which does not exist at all. Because traffics disappear into the special node as the matter disappears into Blackhole in universe. So, the specific node is named as a Blackhole. A Blackhole has two properties. First, the node exploits the ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets. Second, the node consumes the intercepted packets. Blackhole attacks in AODV protocol routing level can be classified into two categories: RREQ Blackhole attack and RREP Blackhole attack [7].

3. Simulation Design

3.1. Working of ANT-AGENTS WITH Ad-Hoc on-Demand Distance Vector Routing (AODV)

Ant Colony Based Routing Algorithm (ANT-AGENTS WITH AODV) which reduces overhead, because routing tables are not interchanged among nodes. It consists of three phases namely Route Discovery phase, Route Maintenance and Route Failure Handling. The Route Discovery phase consist of two mobile agents that is Forward Ant (FANT) for route request and other agent is Backward Ant (BANT) for route reply to create new routes. FANT packets have unique sequence number and source address is broadcasted by the sender and will be passing on by the neighbors of the sender. Node receiving the FANT for the first time generates a record with entries of destination address (Source address of FANT), next hop (address of previous node), and pheromone value (number of hops the FANT needed to reach this node). The destination node extracts information of FANT, destroys it and creates BANT which establish pheromone track to destination node [10].

In Route Maintenance phase, DUPLICATE ERROR flag is set for duplicate packets to prevent from looping problems. It also allows for the evaporation of pheromone by decrementing factor in route table. In Route Failure Handling phase, node deactivates the path by reducing pheromone value to 0 in corresponding route table entry and go to the Route Discovery phase for selecting path and sending packets to the destination over that path [10]. Figure 2 shown ANT agent with AODV algorithm working.

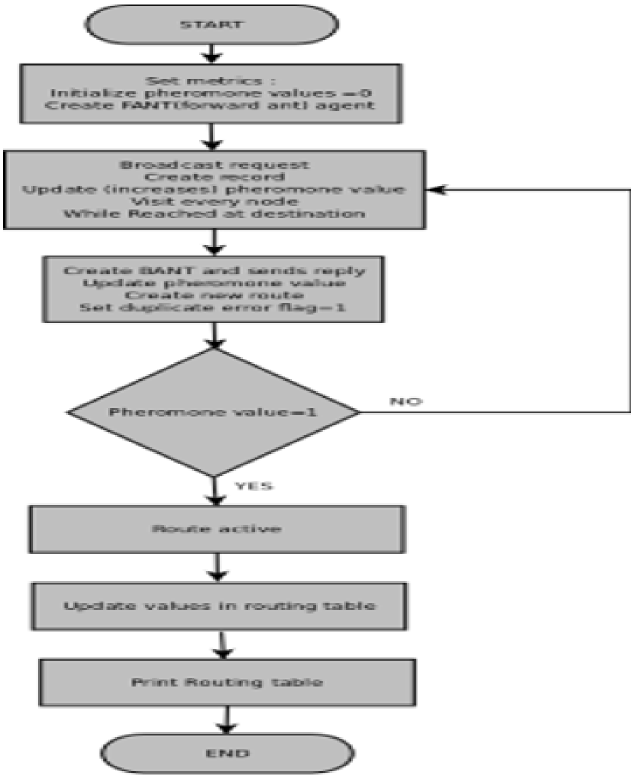

START
Set metrics :
Initialize pheromone values =0
Create FANT(forward ant) agent
Broadcast request
Create record
Update (increases) pheromone value
Visit every node
While Reached at destination
Create BANT and sends reply
Update pheromone value
Create new route
Set duplicate error flag=1
Pheromone value=1
NO
YES
Route active
Update values in routing table
Print Routing table
END

Fig. 2: Ant-Agents with AODV algorithm [10]

3.2. AOMDV-ANT Algorithm Designed

In AOMDV-ANT design is not difference much from AODV-ANT. The difference AOMDV-ANT and AODV-ANT lies on it is multi path of AOMDV, and AODV is on single path.

3.3. Black Hole Attack

In an Ad-Hoc Network that uses the AODV-ANT and AOMDV-ANT protocols, a black hole node absorbs the network traffic and drop all packets [2].

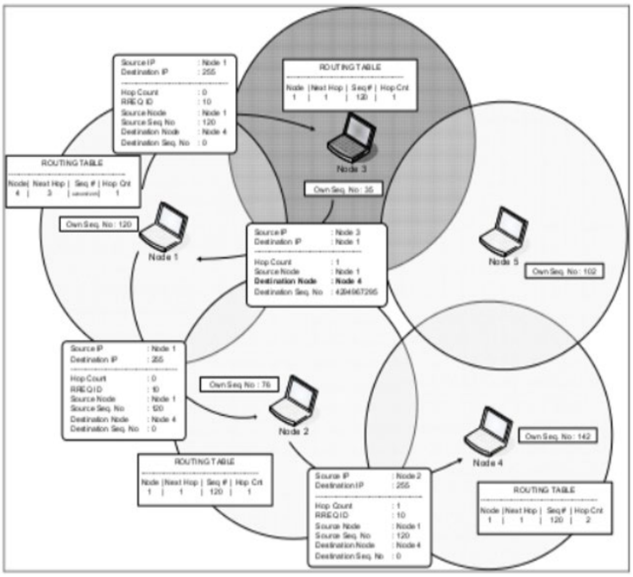


Fig. 3: Illustration of Black Hole Attack [2]

In this scenario shown in Figure 3, we assume that Node 3 is the malicious node. When Node 1 broadcasts the RREQ message for Node 4, Node 3 immediately responds to Node 1 with an RREP message that includes the highest sequence number of Node 4, as if it is coming from Node 4. Node 1 assumes that Node 4 is behind Node 3 with 1 hop and discards the newly received RREP packet come from Node 2. Afterwards Node 1 starts to send out its data packet to the node 3 trusting that these packets will reach Node 4 but Node 3 will drop all data packets [2].

In a Black Hole Attack, after a while, the sending node understands that there is a link error because the receiving node does not send TCP ACK packets. If it sends out new TCP data packets and discovers a new route for the destination, the malicious node still manages to deceive the sending node. If the sending node sends out UDP data packets the problem is not detected because the UDP data connections do not wait for the ACK packets [2].

3.4. Design System Overview

This research generally discusses the analysis of comparing AODV-ANT and AOMDV-ANT, without black hole and with black hole. Figure 4 shows about modelling system in this research.

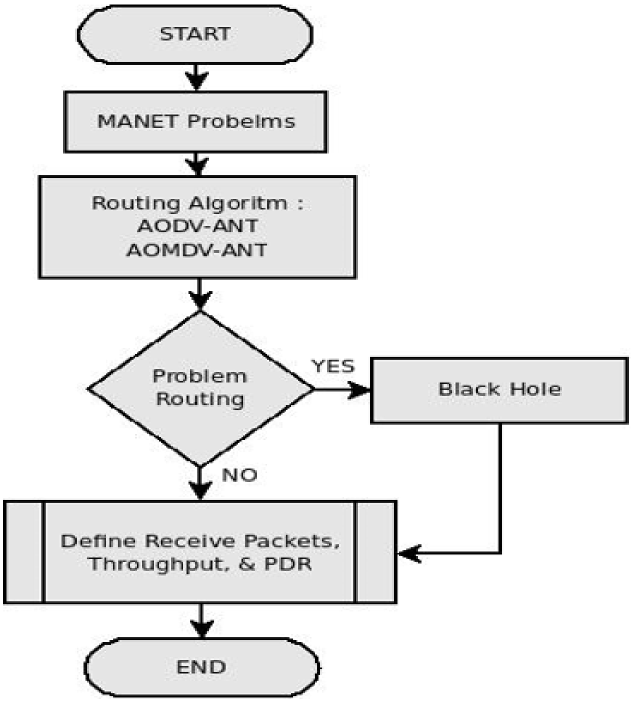


Fig. 4: Research Design System

In our simulation in black hole, we calculate all packets received in destination, because the black hole does not drop all packet from the source. The black hole in our case like man in the middle attack, the black hole intercepts the packets and deliver wrong packets to the destination.

4. Performance Evaluation

This Chapter describes the performance evaluation of the AODV-ANT and AOMDV-ANT algorithm with Black Hole and without Black Hole, using various performance metrics and simulation settings.

4.1. Simulations Parameters

The implementation of simulation is used NS-Allinone 2.35. Simulation environment is as follows in Table 1.

Table 1: Environment variables and its associated values used in simulations

No.	Parameter Variables	Associated Values	Associated Values
1	Simulation Tool	Ns-Allinone- 2.35	Ns-Allinone- 2.35
2	Radio-propagation model	Two Ray Ground	Two Ray Ground
3	MAC type	Mac/802_11	Mac/802_11
4	Interface queue type	Queue/Drop Tail/Pri Queue	Queue/Drop Tail/Pri Queue
5	Antenna model	Omni Antenna	Omni Antenna
6	Max packet in ifq	50	50
7	Number of mobile nodes	10 - 100	10 - 100
8	Protocol type	AODV	AOMDV
9	Optimization Algorithm	AntHoc Net	AntHocNet
10	X dimension of topography	500 m	500 m
11	Y dimension of topography	500 m	500 m
12	Simulation Time	150 second	150 second

4.2. Simulation Results and Analysis

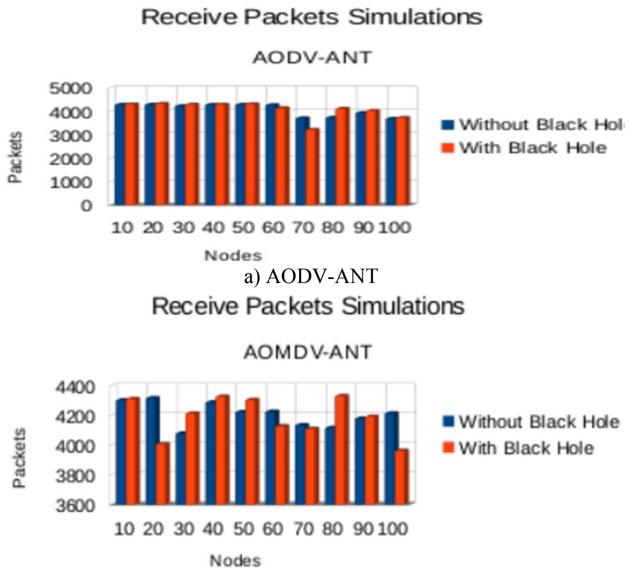
In scenario we analyze the receive packets, throughput, packet delivery ratio, and residual energy. The result and analysis as below.

4.2.1. Receive Packet Results and Analysis

In this simulation we analyze the received packet in AODV-ANT and AOMDV-ANT when without black hole and with black hole attack. The result is captured in Table 2 and as shown in Figure 5.

Table 2: Receive Packets simulations

Node	Without Black Hole		With Black Hole	
	AODV-ANT	AOMDV-ANT	AODV-ANT	AOMDV-ANT
10	4299	4305	4311	4313
20	4305	4319	4335	4010
30	4242	4082	4303	4216
40	4294	4291	4300	4329
50	4300	4226	4322	4307
60	4281	4228	4146	4130
70	3725	4138	3225	4112
80	3747	4119	4126	4333
90	3951	4182	4031	4194
100	3703	4217	3736	3965



a) AODV-ANT

b) AOMDV-ANT

Fig. 5: Receive Packets: (a) AODV-ANT; (b) AOMDV-ANT

From Figure 5 (a), we know that the AODV-ANT with black hole has small average than without black hole. In AODV-ANT without black hole we have 4084.7 packet and in AODV-ANT with black hole we have 4083.5. We can assume that in AODV-ANT with black hole performance is decrease 0.03% comparing to AODV-ANT without black hole.

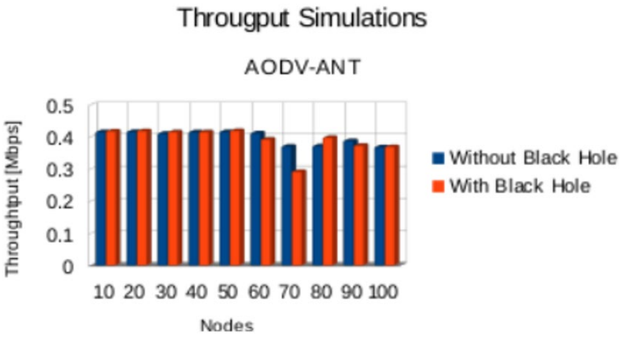
Then, in Figure 5 (b), we know that the AOMDV-ANT with black hole has small average than without black hole. In AOMDV- ANT without black hole we have 4210.7 packet and in AOMDV-ANT with black hole we have 4190.9. We can assume that in AOMDV-ANT with black hole performance is decrease 0.47% comparing to AOMDV-ANT without black hole.

4.2.2. Throughput Result and Analysis

Now, we examine throughput in AODV-ANT and AOMDV-ANT when without black hole and with black hole attack. The results are captured in Table 3 and as shown in Figure 6.

Table 3: Throughput simulations

Node	Without Black Hole		With Black Hole	
	AODV-ANT	AOMDV-ANT	AODV-ANT	AOMDV-ANT
10	0.417 Mbps	0.418 Mbps	0.418 Mbps	0.417 Mbps
20	0.417 Mbps	0.419 Mbps	0.419 Mbps	0.385 Mbps
30	0.411 Mbps	0.399 Mbps	0.416 Mbps	0.404 Mbps
40	0.416 Mbps	0.416 Mbps	0.416 Mbps	0.419 Mbps
50	0.417 Mbps	0.409 Mbps	0.42 Mbps	0.418 Mbps
60	0.413 Mbps	0.411 Mbps	0.399 Mbps	0.394 Mbps
70	0.372 Mbps	0.398 Mbps	0.293 Mbps	0.403 Mbps
80	0.373 Mbps	0.401 Mbps	0.399 Mbps	0.419 Mbps
90	0.389 Mbps	0.408 Mbps	0.374 Mbps	0.408 Mbps
100	0.369 Mbps	0.409 Mbps	0.37 Mbps	0.385 Mbps



a) AODV-ANT

b) AOMDV-ANT

Fig. 6: Throughput simulations: (a) AODV-ANT; (b) AOMDV-ANT

From Figure 6 (a), we know that the AODV-ANT with black hole has small average than without black hole. In AODV-ANT without black hole we have 0.3994 Mbps and in AODV-ANT with black hole we have 0.3920 Mbps We can assume that in AODV-ANT with black hole performance is decrease 1.85% comparing to AODV-ANT without black hole.

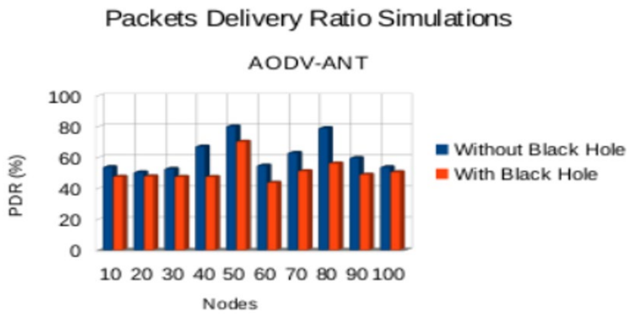
Then, in Figure 6 (b), we know that the AOMDV-ANT with black hole has small average than without black hole. In AOMDV-ANT without black hole we have 0.4092 Mbps and in AOMDV-ANT with black hole we have 0.4054 Mbps. We can assume that in AOMDV-ANT with black hole performance is decrease 0.93% comparing to AOMDV-ANT without black hole.

4.2.3. Packets Delivery Ratio Result and Analysis

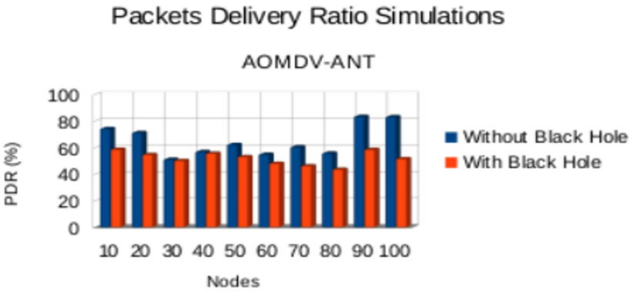
Then, we examine packet delivery ratio (PDR) in AODV-ANT and AOMDV-ANT when the packets are without black hole and with black hole attack. The results are captured in Table 4 and as shown in Figure 6.

Table 4: Packets Delivery Ratio Simulations

Node	Without Black Hole		With Black Hole	
	AODV-ANT	AOMDV-ANT	AODV-ANT	AOMDV-ANT
10	54.18%	74.41%	47.90%	58.76%
20	50.77%	71.34%	48.17%	54.78%
30	53.02%	51.28%	47.81%	50.32%
40	67.52%	57.06%	47.78%	55.78%
50	80.52%	62.38%	70.62%	53.17%
60	55.17%	55.05%	44.01%	48.22%
70	63.31%	60.64%	51.53%	46.31%
80	79.38%	55.96%	56.52%	43.69%
90	60.06%	83.55%	49.28%	58.68%
100	54.13%	83.34%	50.87%	51.73%



a) AODV-ANT



b) AOMDV-ANT

Fig. 6: PDR: (a) AODV-ANT; (b) AOMDV-ANT

From Figure 6 (a), we know that the AODV-ANT with black hole has small average than without black hole. In AODV-ANT without black hole we have 61.806 % and in AODV-ANT with black hole we have 51.449 %. We can assume that in AODV-ANT with black hole performance is decrease 10.357% comparing to AODV-ANT without black hole.

Then, in Figure 6 (b), we know that the AOMDV-ANT with black hole has small average than without black hole. In AOMDV-ANT without black hole we have 65.501% and in AOMDV-ANT with black hole we have 52.144 %. We can assume in AOMDV-ANT with black hole performance is decrease 13.357% comparing to AOMDV-ANT without black hole.

In the results of simulations, we conducted that the black hole effect is visible in the PDR. From the simulations results it can be counted the differences between PDR on AODV-ANT and AOMDV-ANT in the black hole and without black holes, as shown in the Table 5 and Figure 7.

Table 5: Packets Delivery Ratio Differences without Black Hole and with Black Hole

Node	AODV-ANT	AOMDV-ANT
10	6.28%	15.65%
20	2.60%	16.56%
30	5.21%	0.96%
40	19.74%	1.28%
50	9.89%	9.21%
60	11.16%	6.83%
70	11.78%	14.33%
80	22.86%	12.27%
90	10.78%	24.87%
100	3.26%	31.61%

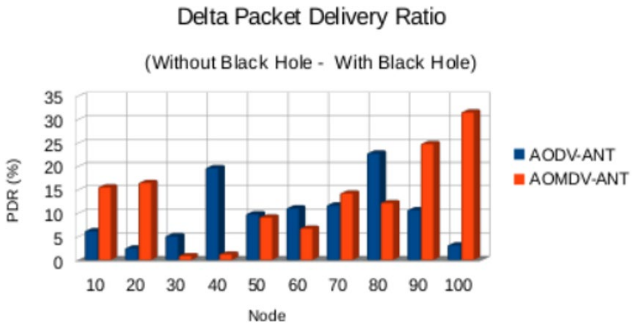


Fig. 7: PDR Differences without Black Hole and with Black Hole

From Table 5 and Figure 7, it can be seen that the results vary. It can be occurred for their mobile node. The differences between the nodes with black hole and without black holes in Figure 5, for the example AODV-ANT at node 40, the results differ quite considerably. It can occur because in the time without a black hole, nodes movement quite tenuous, whereas when with a black hole, nodes movement closer to each other, thus causing the value of PDR is high (picture in attachment). It is consistence with the nature of black holes that absorb energy so that node will send packet from source to the destination, it will always pass through the nodes of infected black hole first.

5. Conclusion

MANETs is highly dynamic and distributed in nature [8]. This thesis tried to evaluate the performances between AODV-ANT algorithm and AOMDV-ANT algorithm in Black Hole attack using NS 2.35. The comparisons are based receive packets, throughput, and packet delivery ratio.

In the results of the simulation is that the influence of the black hole can be seen in the PDR. From the comparison PDR without black holes and with black holes, it obtained varying results, it because in the time without a black hole, nodes movement quite tenuous, whereas when with a black hole, the nodes movement closer to each other, thus causing the value of PDR is high. This is consistence with the nature of black holes that absorb energy, so that the node will send packet from source to the destination, it will always pass through the nodes of infected black hole first.

The future work of research can be considered in the following research. In order to observe the performance AOMDV-ANT for energy aware in each node in the network.

References

[1] Dokurer, S., Erten, Y. M., & Acar, C. E. (2007). Performance analysis of ad-hoc networks under black hole attacks. Proceedings of the IEEE Southeast Conference, pp. 148-153.

[2] Dokurer, S. (2006). Simulation of Black hole attack in wireless Ad-hoc networks. Master thesis, Atılım University.

[3] Bhattercharjee, A., & Paul, S. (2014). A review on some aspects of black hole attack in MANET. International Journal of Engineering Trends and Technology, 10(8), 396-401.

[4] Ducatelle, F., Di Caro, G., & Gambardella, L. M. (2005). Using ant agents to combine reactive and proactive strategies for routing in mobile ad-hoc networks. International Journal of Computational Intelligence and Applications, 5(2), 169-184.

[5] Misra, S., Dhurandher, S. K., Obaidat, M. S., Gupta, P., Verma, K., & Narula, P. (2010). An ant swarm-inspired energy-aware routing protocol for wireless ad-hoc networks. Journal of Systems and Software, 83(11), 2188-2199.

[6] Kanani, C., & Sinhal, A. (2013). Ant colony optimization based modified AOMDV for multipath routing in MANET. International Journal of Computer Applications, 82(10), 14-19.

[7] Sharma, S., & Gupta, R. (2009). Simulation study of blackhole attack in the mobile ad hoc networks. Journal of Engineering Science and Technology, 4(2), 243-250.

[8] Esmaili, H. A., & Shoja, M. R. (2011). Performance analysis of AODV under black hole attack through use of OPNET simulator. World of Computer Science and Information Technology Journal, 1(2), 49-52.

[9] Ghonge, M., & Nimbhorkar, S. U. (2012). Simulation of AODV under blackhole attack in MANET. International Journal of Advanced Research in Computer Science and Software Engineering, 2(2), 1-5.

[10] Bansal, E., & Verma, A. K. G. (2013). Improving performance of AODV using ant agents. Master thesis, Thapar University.

[11] Singh, G., Kumar, N., & Verma, A. K. (2014). Antalg: An innovative ACO based routing algorithm for MANETs. Journal of Network and Computer Applications, 45, 151-167.

[12] Woungang, I., Obaidat, M. S., Dhurandher, S. K., Ferworn, A., & Shah, W. (2013, June). An ant-swarm inspired energy-efficient ad hoc on-demand routing protocol for mobile ad hoc networks. Proceedings of the IEEE International Conference on Communications pp. 3645-3649.

[13] Singh, G., Kumar, N. G., & Verma, A. K. (2014). Design and development of ACO routing protocol for MANETs. PhD thesis, Thapar University.

[14] Misra, P. (1999). Routing protocols for ad hoc mobile wireless networks. http://suraj.lums.edu.pk/~cs678/papers/17_routing_for_ad_hoc.pdf.

[15] Royer, E. M., & Toh, C. K. (1999). A review of current routing protocols for ad hoc mobile wireless networks. IEEE Personal Communications, 6(2), 46-55.