IMPACT OF BLACK HOLE ATTACK ON AODV ROUTING PROTOCOL

Ei Ei Khin[1] and Thandar Phyu[2]

[1]Faculty of Information and Communication Technology, University of Technology (Yatanarpon Cyber City), Pyin Oo Lwin, Myanmar
[2]Department of Advanced Science and Technology, Ministry of Science and Technology, Nay Pyi Taw, Myanmar

ABSTRACT

A mobile ad-hoc network (MANET) is a collection of wireless mobile nodes that dynamically self-organize to form an arbitrary and temporary network. The mobile nodes can communicate with each other without any fixed infrastructure. MANET can be set up quickly to facilitate communication in a hostile environment such as battlefield or emergency situation. The various severe security threats are increasing on the MANET. One of these security threats is black hole attack which drops all received data packets intended for forwarding. In this paper, we are simulating and analyzing the impact of black hole attack on Ad Hoc On-Demand Distance Vector (AODV) protocol. The simulation is carried on NS-2 and the simulation results are analyzed on various network performance metrics such as packet delivery ratio, normalized routing overhead and average end-to-end delay.

Keywords

MANET, AODV, Black Hole Attack, NS-2, Performance Parameters.

1. INTRODUCTION

A mobile ad-hoc network (MANET) [6] is a collection of mobile devices that used wireless communications capability without any central network authority or infrastructure. The mobile devices can easily communicate with another device by forwarding packets over themselves. MANETs are flexible networks that the mobile device or node can easily join and leave to the network. The connectivity of mobile nodes via wireless channel is used hop by hop routing. The nodes may be a host or router to discover a route and to forward the packets to the other nodes in the network [1].

MANETs have some special characteristic such as open medium, dynamic topology, lack of central monitoring and management, cooperative algorithms, no clear defence 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. Then, it absorbs all data packets that intended to forward to the destination. In this way, all data packets in the network are dropped. Hence, the network becomes data lost and affects the performance.

In this paper, we focus on the effect of Black Hole attack in MANET using AODV routing protocol. The rest of the paper is structured as follows. In Section 2, we describe an overview of

DOI : 10.5121/ijitmc.2014.2202

AODV routing protocol. In Section 3, we discuss about the black hole attack. In Section 4, we present the simulation results and performance analysis of black hole attacks in AODV protocol. Finally, we conclude this paper in Section 5.

2. OVERVIEW OF AODV ROUTING PROTOCOL

The AODV protocol is the most widely adopted and well known reactive routing protocol that the routes are created only when they are needed [7]. The mobile devices or nodes in the network exchange the routing packets between them when they want to communicate with each other and maintain only these established routes. The AODV routing protocol is one that adaptive the DSDV (Destination-Sequenced Distance Vector) protocol to get dynamic link conditions [3][8].

Whenever a node wants to send the data packet to another node, it checks its routing table. If it has a fresh route to the destination node, it uses that route to send the data packet. If it does not have a route or it is not fresh enough route, then the node starts the route discovery process. So, it broadcasts Route Request message (RREQ) to its neighbours. The intermediate nodes check whether it is the destination node or it has a fresh route to go to the destination node. If it is available, the intermediate node sends back Route Reply message (RREP) to the source node. Otherwise, it forwards the RREQ message to its neighbours by using flooding approach. This process is continued until whether the destination node is found or the node that has a fresh enough route to the destination is found. After finishing the route discovery process, the source node and the destination node can be communicate and send the packets between them.

When any node knows a link break or failure, Route Error (RERR) message is send to all other nodes for notifying the lost of link. Hello message is used for detecting and monitoring links to neighbours [10].

3. BLACK HOLE ATTACK

Black hole attack [4][5][2] is a kind of Denial of Service (DoS) attacks [7] in MANET. In this attack, a malicious node advertises that it has the best path to the destination node during the route discovery process. Whenever it receives the RREQ message, it immediately sends out a fake RREP to the source node. The source node first receives the RREP from the malicious node ahead of other RREPs. However, when the source node starts sending the data packet to the destination by using this route, the malicious node drops all packets instead of forwarding.

For example, let's consider the scenario in Figure 1. In this scenario, the node 'S' is the source node, 'D' is the destination node and 'M' is assumed the malicious node. When 'S' want to send the data packets to 'D', it starts the route discovery process by broadcasting RREQ message to the neighbouring nodes. So, the node 'C', 'E' and 'F' receive this message. Since M is a malicious node, it immediately sends out a RREP message to 'S' with high sequence number. 'S' assumes that it is the freshest route, ignores all other RREPs and sends any packets to the destination over it. However, the node 'M' drops all data packets instead of sending to intended destination.

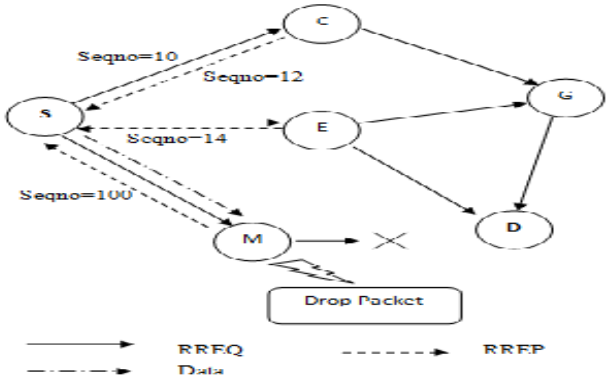

Figure 1. Black hole attack

4. SIMULATION ENVIRONMENT

In this simulation, we have implemented the black hole attack based on the AODV routing protocol using NS-2.34 [9]. For our simulation, we use the IEEE 802.11 Mac at the physical and data link layer. 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. The overall simulation parameters are presented in Table 1. We have evaluated the performance of the AODV protocol with the black hole attack or not. The following metrics are used to evaluate the performance.

Packet Delivery Ratio: The ratio between the number of CBR packets sent by the source and the number of packets received by the destination.
Average End-to-End Delay: The average delay between the sending of the data packet by the source and the receiving it by the destination. It is measured in milliseconds (ms).
Routing Overhead: The ratio of number of control packet generated to the data packets transmitted.

Table 1. Simulation parameters

Parameter	**Value**
Simulator	NS-2.34
Area	750m x 750m
Routing Protocol	AODV
Simulation time	300s
Application Traffic	CBR
Number of Nodes	20
Malicious Node	1 - 5
Pause time	4 s to 40s
Packet Size	512 bytes
Transmission rate	2 packets/s
Maximum speed	10 m/s to 80m/s
No of Connections	1 to 7
Movement Model	Random Waypoint

4.1 Effect of Malicious Nodes on Performance

We have simulated the black hole attack in AODV protocol using the parameters in Table 1. The packet delivery ratio (PDR) of AODV protocol in the context of variation in malicious nodes is shown in Figure 2. When the PDR of normal AODV protocol is 97.99%, the PDR of AODV with one black hole node is 69.03%. It can be seen that the PDR of AODV is dramatically decreased when there is an increase number of malicious nodes in the network. The impact of malicious nodes to the average end-to-end delay and the routing overhead on AODV protocol are shown in Figure 3 and Figure 4. It can be observed that there are raising delay and overhead when the number of malicious nodes is increased.

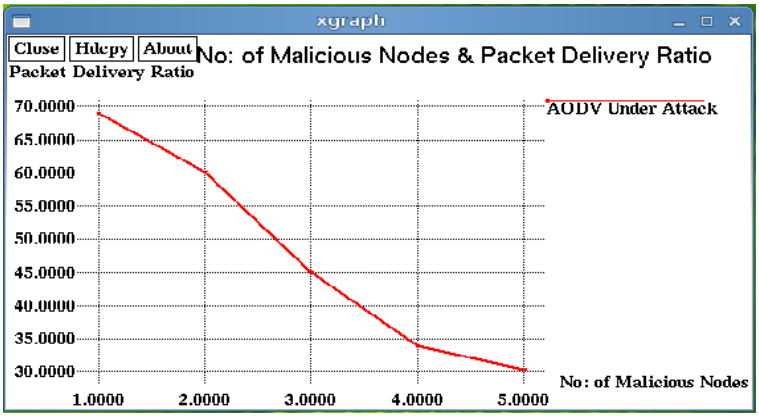

Figure 2. Effect of malicious nodes on packet delivery ratio

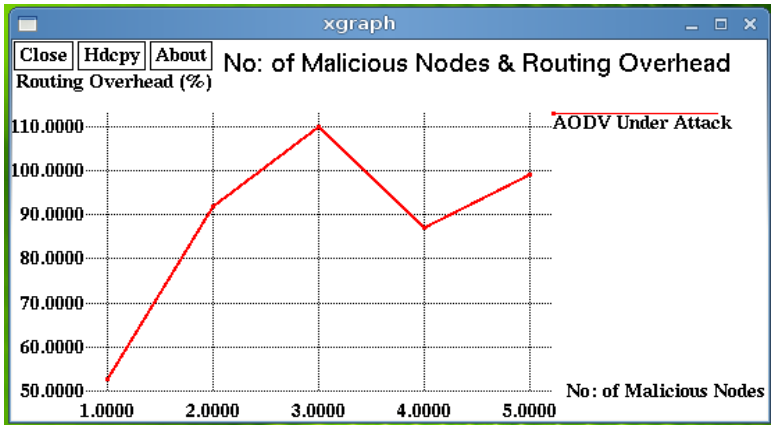

Figure 3. Effect of malicious nodes on overhead

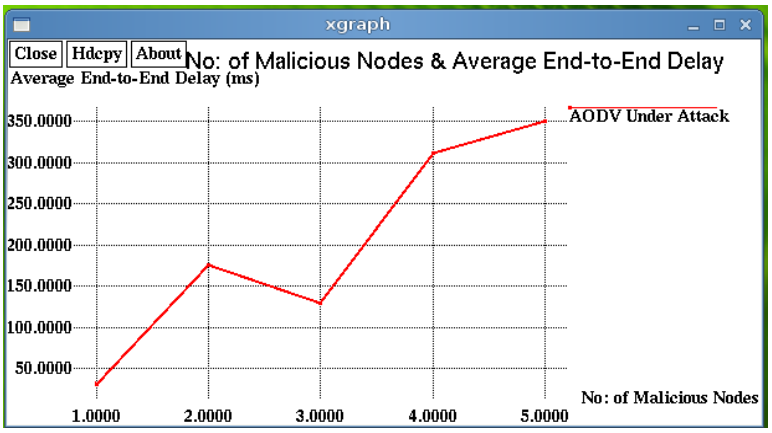

Figure 4. Effect of malicious nodes on delay

4.2 Effect of Pause Time on Performance

To evaluate the impact of pause time on the performance of AODV protocol, simulation is done with the parameters of Table 1and one malicious node. Although all PDR of AODV without attack is over 90%, the PDR of AODV with attack is 59.66% at 30s pause time in Figure 5. In Figure 6, there is a significant increase in the routing overhead. When the overhead of AODV is 50.63 at 40s pause time, the overhead of AODV with attack is 229.62. Figure 7shows that there is a slight increase in the average delay of AODV in 5s pause time since the black hole attack send the immediate reply without checking its table.

Figure 5. Effect of pause time on packet delivery ratio

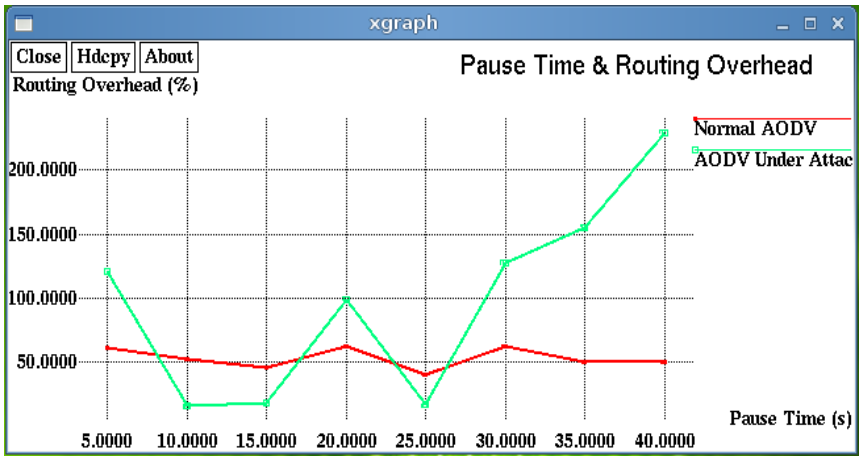

Figure 6. Effect of pause time on overhead

Figure 7. Effect of pause time on delay

4.3 Effect of Transactions on Performance

The performances of normal AODV and AODV under attack with the variation of transactions are evaluated as shown in Figure 8, Figure 9 and Figure 10.The number of transaction indicates the number of connection from source to destination. In Figure 8, the PDR of AODV with attack decreases about 20% than in normal AODV at 2 transactions. In Figure 9, there is a slight increase in the overhead of normal AODV at 2 transactions. It can be observed that, there is a significant increase in the average end-to-end delay with the effect of black hole, as compared to the normal AODV protocol at 3 transactions in Figure 10.

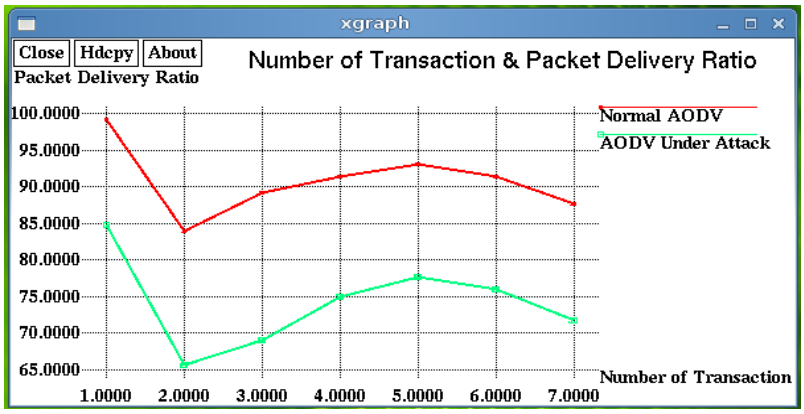

Figure 8. Effect of transactions on packet delivery ratio

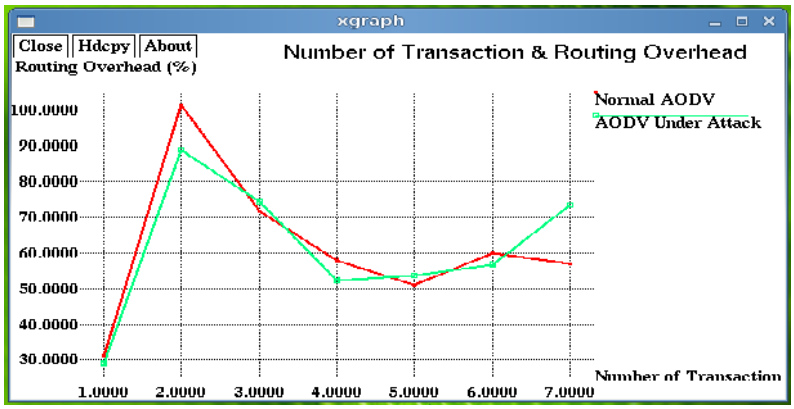

Figure 9. Effect of transactions on overhead

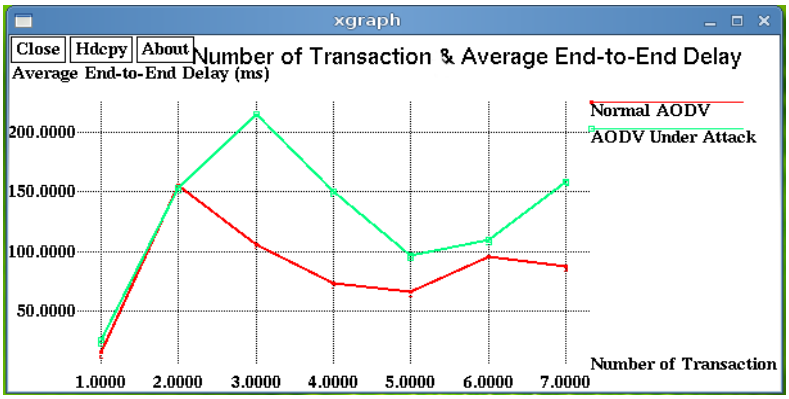

Figure 10. Effect of transactions on delay

4.4 Effect of Mobility on Performance

To evaluate the impact of mobility speed on the performance of AODV protocol, the simulation is done with the parameters in Table 1 and one black hole node. In Figure 11, the PDR of AODV without attack is 97.99% when the nodes move at the speed 10m/s. However, when there exists black hole attack, the PDR decreases to 69.03%. In Figure 12, there is a slight increase in the

overhead of AODV when the nodes move with 40m/s. The comparison of delay between AODV and AODV under attack is shown in Figure 13.

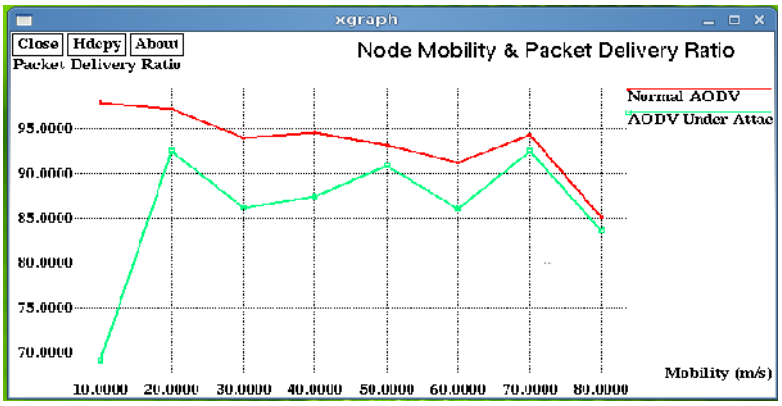

Figure11. Effect of node mobility on packet delivery ratio

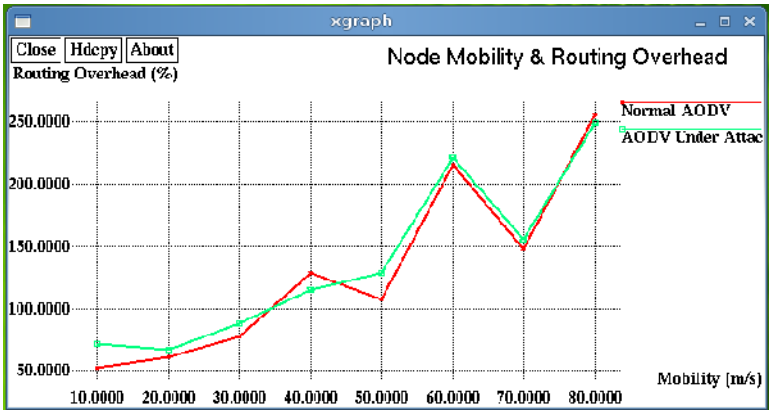

Figure 12. Effect of node mobility on overhead

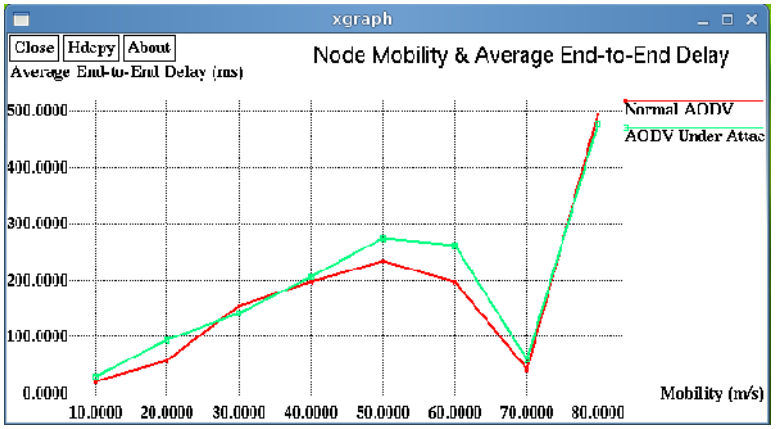

Figure 13. Effect of node mobility on delay

5. CONCLUSIONS AND FUTURE WORK

In this paper, we have analyzed the effect of black hole attack in the performance of AODV protocol. The simulation has been done using the network simulator (NS-2.34). The performance metrics like average end to end delay, packet delivery ratio and routing overhead has been detected and analyzed with the variable node mobility, pause time and number of transactions as shown in Figure 2-13. The simulation results show that when the black hole node exists in the network, it can be affected and decreased the performance of AODV routing protocol. So, the detection and prevention of black hole attack in the network exists as a challenging task. As future work, we intend to simulate and analyze the effect of the black hole attack in other routing protocols and we intend to perform the solution for the black hole attack and compare its performance with the AODV protocol.

REFERENCES

[1] Ranjeet Suryawanshi & Sunil Tamhankar., (2012) "Performance analysis and minimization of black hole attack in MANET", International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622, Vol. 2, Issue 4, pp.1430-1437.

[2] Mohammad Al-Shurman & Seong-Moo Yoo, Seungjin Park, (2004) "Black hole attack in mobile ad hoc networks", Proceedings of the 42nd annual Southeast regional conference ACM-SE 42, pp. 96-97.

[3] Charles E. Perkins & Elizabeth M. Belding-Royer, Samir R. Das (2003) Mobile Ad Hoc Networking Working Group, Internet Draft.

[4] Gaurav Sandhu & Moitreyee Dasgupta, (2010) "Impact of blackhole attack in MANET", International Journal of Recent Trends in Engineering and Technology, Vol. 3, No. 2.

[5] Hongmei Deng & Wei Li, Dharma P. Agarwal (2002) "Routing security in wireless ad hoc networks", University of Cincinnati, IEEE Communications magazine, Vol. 40, No. 10.

[6] Charles E. Perkins, (2001) Ad Hoc Networking, Addison-Wesley, Pearson edu.

[7] Ochola EO & Eloff MM, "A review of black hole attack on AODV routing in MANET".

[8] C. E. Perkins & Belding-Royer, S. Das (2003) "Ad-hoc on demand distance vector (AODV) routing", IETF RFC 3561.

[9] Kevin Fall, Kannan Varadhan, The NS Manual, Available: http://www.isi.edu/nsnam/ns/doc/index.html.

[10] Akanksha Nigam*, (2011) "A study of ad hoc on demand distance vector routing protocol", International Journal of Research in IT& Management (IJRIM), Vol. 1, Issue 2.