ZAMBIA INFORMATION COMMUNICATION TECHNOLOGY (ICT) JOURNAL

Volume 1 (Issue 1) (2017) Pages 47-50

Performance Analysis of AODV Routing Protocol Under Blackhole Attack With Sink Shifting

Marumo R. Okaile
University of Botswana
Computer Science
Department
Gaborone, Botswana

Sangodoyin O. Adedeji
University of Botswana
Computer Science
Department
Gaborone, Botswana

Ramajalwa P. Emma
University of Botswana
Computer Science
Department
Gaborone, Botswana

Moile Tshepo
University of Botswana
Computer Science
Department
Gaborone, Botswana

***Abstract*— Routing protocol selection are the primary ways to design any wireless network. In Mobile Ad-hoc Network (MANET), the chosen protocol ought to be the best in terms information delivery and data integrity. Hence, the performance analysis of the protocol is the major step before choosing a specific protocol. In this paper, the performance analysis is applied to *Ad-Hoc On-Demand Distance Vector* protocol using Network Simulator2. Packet delivery ratio and energy are the two common measures used for the comparison of the performance of above protocol.**

Keywords—AODV protocol, Performance Matrix, Blackhole Attck.

I. INTRODUCTION

Ali et al described a mobile Ad-hoc network (MANET) [1] as a collection of mobile devices that uses wireless communication capabilities with no central network authority or infrastructure. The mobile devices will simply communicate with another device by forwarding packets over themselves. MANETs are versatile networks in which the mobile devices or nodes will simply join and leave the network. The connectivity of mobile nodes via wireless channels are referred to as hop by hop routing. The nodes could also be a host or router to get a route and to forward the packets to the other nodes in the network [2].

MANETs have some special characteristic like: open medium, dynamic topology, cooperative algorithms and so on. In an open and hostile setting, they're exposed to various forms of attacks. One amongst these security attacks is the Blackhole attack, Vrai [3]. During this attack, the malicious node sends the faux reply to the destination node without checking its routing table. Then, it absorbs all data packets that is intended to be forwarded to the destination, Vrai [3]. At this point, all data packets within the network are dropped. Hence, data is lost and affects the performance.

In this paper, we focused on the result of Blackhole attack in MANET using the Ad hoc On-Demand Distance Vector (AODV) routing protocol. The rest of the paper is structured as follows. Literature review is presented in section 2, we briefly highlighted on the AODV routing protocol in section 3. In Section 4, we discussed about the Blackhole attack. In Section 5, we presented the simulation results and performance analysis of the Blackhole attack in the mentioned protocol. In section 6 we justified our reason for using the Network Simulator 2, and finally, we concluded this paper in Section 7.

II. LITERATURE REVIEW

According to Mohamed A.A and Peter J.B MANETS [10] inherit security attacks faced by both wired and wireless networks and other attacks unique to themselves due to their nature. Node mobility as one of the characteristics makes it difficult to distinguish between stale and fake routes. The paper analyses the impact of flooding, selfish, gray hole and blackhole attack on AODV routing protocol and their effects on the performance metrics. Blackhole is seen to have a dramatic impact on network performance because it introduces a fake Route Reply (RREP) which affects the network.

Houda M et al [11] evaluated and compared performance of AODV routing protocol under blackhole, flooding and rushing attacks. The performance metrics studied are Packet Delivery Ratio, Average End to End Delay and Average throughput. The attacks are implemented on Ns-2. The results of the simulation show AODV degrades under attacks with a blackhole attack having a significant effect on network performance.

According to Chaubey N et al [12], AODV is efficient and scalable but has no inherent security mechanisms, it has a lot of security vulnerabilities. The paper studied the impact of network size on performance of AODV and Trust Based Secure on Demand Routing Protocol 'TSDRP' under a blackhole attack. The performance metrics considered are Packet Delivery Ratio (PDF), Average End-to-End Delay (AED), Average Throughput (AT) and Normalized Routing Load (NRL). TDSRP routing protocol performs better than AODV in the presence of malicious node while increasing the network size.

III. MANET ROUTING PROTOCOLS

In this section, we will briefly describe the key features of the Ad-hoc On-Demand Distance Vector(AODV) protocol studied in our simulation. We will conjointly describe the actual parameters that we decided to use to implement on every protocol. However, the fundamental variations within this protocol are primarily based on classification which are reactive.

In Reactive or on-demand routing, routes are solely discovered when they are literally required. Hence, a node that wishes to send a packet to a different node, initializes the reactive protocols to search for the route in an on-demand basis and establishes a connection to transmit and receive a packet. The route discovery usually consists of a network wide flooding of requested messages. In distinction, this approach has some benefits as well as disadvantages and can be analyzed from its performance metrics as mentioned in next section.

A. Ad-Hoc On Demand Distance Vector

The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multihop routing between participating mobile nodes wishing to establish and maintain an Ad-hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. This protocol enables mobile nodes to respond to link breakages and changes in network topology in a timely manner. The operation of AODV is loop-free, and by avoiding the Bellman-Ford "counting to infinity" problem, it offers quick convergence when the ad hoc network topology changes (typically, when a node moves in the (network). When links break, AODV causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link.

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 any route information it sends to requesting nodes. Using destination sequence numbers ensures loop freedom and is simple to program. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest sequence number.

IV. BLACK HOLE ATTACK

Blackhole attack is described by Vrai [3], as a kind of Denial of Service (DoS) attack [4] in MANET. In this attack, a malicious node advertises that it's the most effective path to the destination node throughout the route discovery process. Whenever it receives the Route Requests (RREQ), it instantly sends out a fake Route Replies (RREP) to the source node. The source node first receives the Route Replies from the malicious node ahead of different RREPs, Ming-Yang Su [5]. However, once the source node starts sending the data packet to the destination by exploiting this route, the malicious node drops all packets rather than forwarding.

For example, let's think about the scenario in Figure 1. During this situation, the node '1' is the source node, '4' is the destination node and '3' is assumed the malicious node. '1' needs to send the data packets to '4', it starts the route discovery process by broadcasting RREQ message to the neighboring nodes. So, the node '2', '3' receive this message. Since 3 is a malicious node, it instantly sends out a RREP message to '1' with high sequence number. '1' assumes that it's the shortest route, ignores all different RREPs and sends any packets to the destination over it. However, the node '3' drops all data packets rather than sending to intended destination.

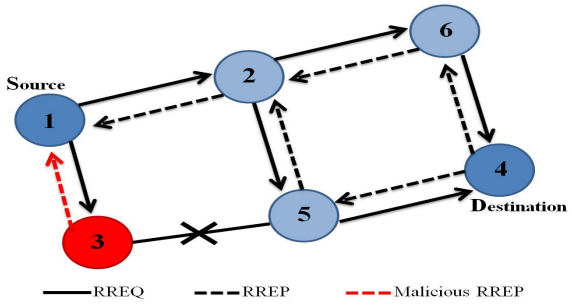

Figure 1: Black hole illustration

V. SIMULATION ENVIRONMENT

The simulation is carried out using Network Simulator 2 (NS-2). Sanzgiri et al [7] describes NS-2 is an open source environment which accommodates the possibility of new protocols and alterations to the existing protocols. The AODV protocol is implemented to the simulator, we also needed to create a header, aodv.cc file extension (for our C++ code) and a patch to integrate both files. The source code is modified to introduce the black hole attack to the network.

The simulations aim to show how AODV performs under the black hole attack, therefore two simulation scenarios were created; the first setup simulates the network under normal operation, and the second setup simulates the network with the Blackhole attack being active. The simulations are done on a square area of 500m X 500m. The number of nodes used during the simulation was: 20,30,40,50. The speed of the simulation was set at 20 m/s.

The model utilized as a wireless transmission channel at the physical layer is two ray ground propagation. The algorithm that is utilized at the data link layer is IEEE 802.11. AODV is used as a network layer routing protocol. The transport layer protocol that is employed is User Datagram Protocol (UDP) and the generated data packets are constant bit rate (CBR).

The size of the packets is 512 bytes. UDP is used because it is connectionless so the source node does not notice when there is no connection between itself and the destination node. It continues to send the packets even when there is a malicious node discarding them, so it is easy to accurately count the number of packets sent and received. If Transmission Control Protocol (TCP) was used, the source node would stop sending

the packets if it does not get acknowledgement packet from the destination node. Figure 3 below shows a snapshot of wireless network configuration parameters used.

Parameters	Value
Simulator	Ns 2.35
Protocol Studied	AODV
Simulation time	200 seconds
Simulation Area	500 X 500
Node Movement model	Random waypoint
Traffic Type	TCP (cbr)
Number of Nodes	20, 30, 40, 50
Performance Matrix	PDR, Energy

Table 1: Simulation set-up

VI. REASON FOR NETWORK SIMULATOR 2

NS2 is a global project development and have open source projects for students and clients. This offers students and research scholars to use the developer skills to develop an efficient project. Because it's open source, it provides a lot of support for various innovative ideas. Unlike OPNET, NS2 is a discrete event simulator targeted at networking research.

VII. RESULTS AND DISCUSSION

Two different scenarios have been considered during the simulation. In the first scenario, no attacker node is placed into the network whereas in the second one, there are a number of attacker nodes. In order to assess the effect of nodes mobility on the network i.e. moving further and close to the sink, the speed of nodes has been changed from 0 to 20 meters per second in each of the scenarios. Packet drop ratio, Energy have been regarded as network parameters.

A. Packet Delivery Ratio

Packet Delivery Ratio is the number of packets successfully received by the destined node divided by the number of packets generated by source node.

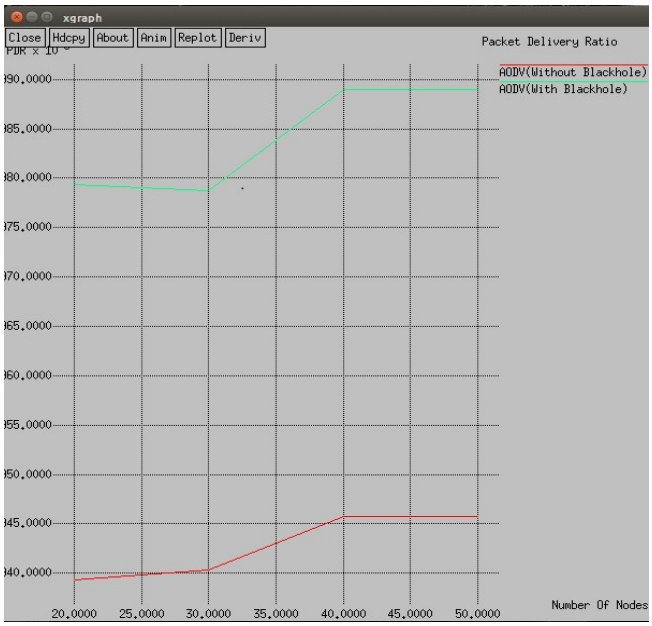

Figure 2: Number of nodes vs PDR

Number of Nodes	Packets Sent	Packets Delivered	Packet Delivery Ratio
20	1983	1942	0.9793
30	7220	6789	0.9403
40	6572	6215	0.9457
50	6572	6215	0.9457

Table 2: Packet Delivery Ratio for normal AODV

Number of Nodes	Packets Sent	Packets Delivered	Packet Delivery Ratio
20	3053	2849	0.9331
30	1067	9950	0.9787
40	9781	9673	0.9889
50	9781	9673	0.9889

Table 3: Packet Delivery Ratio for AODV under attack

Figure 2, table 2 and table 3 displays the results from the simulation. An attacked network, where the green line shows the results of attacked node, as the sink is being moved further away from the attacker node, will produce a greater distance and a higher failure rate.

B. Energy

Energy determines the life time of a network. The metric is adopted in this paper to determine the energy consumption rate in a normal network environment and an attacked network environment. The impact of the network activity, during the normal simulation without the Blackhole attack and with the Blackhole attack, determines the outcome of the total energy consumed by the nodes.

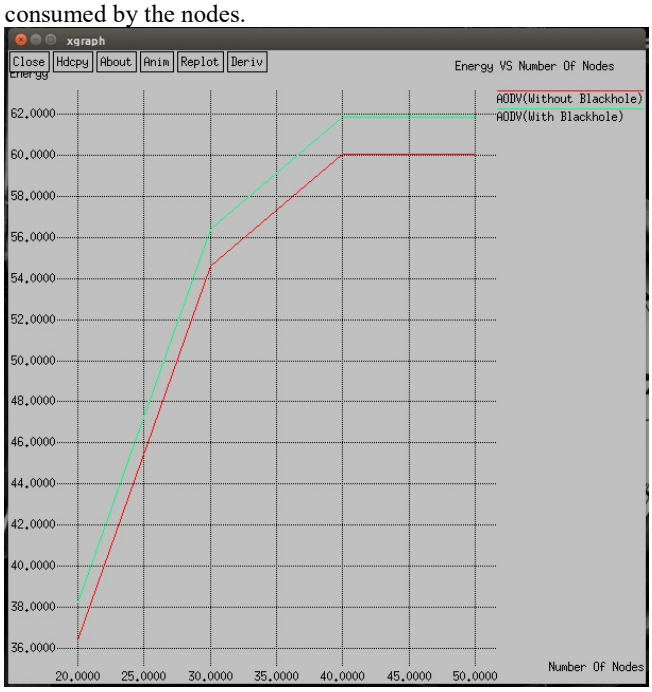

Figure 3: Number of nodes vs Energy

Number of Nodes	Normal AODV	AODV under black hole attack
20	36.4	38.2
30	54.6	56.4
40	60.06	61.86
50	60.06	61.86

Table 3: Average Energy Consumption

Figure 3 shows the energy consumption of the nodes as an attacker is introduced against the number of nodes with the sink shifting. Both the graphs reach a constant energy consumption rate as the sink moves further and it highlights that after some point the number of nodes does not have any effect, but as the sink shifts further away, the energy consumption rate increases. Therefore, a conclusion can be drawn here that the two scenarios have a directly proportional relationship.

VIII. CONCLUSION

The performance of AODV is affected when there is an attacker in the network, both metrices studied show a decline network performance with the introduction of an attacker node, therefore it can be concluded that the sudden spike on energy consumption can raise an alarm to check for network vulnerability.

During the simulation, we observed that there is a possibility of a successful communication between the nodes in a MANET network(AODV) whilst the Blackhole attack is active, provided there are “n” number of nodes.

The main aim of the paper was to see how a Blackhole attack does the proximity of the attached node to the sink shifting, thereby affecting both performance matrices. Finally, the result showed that the further the attacked node was from the sink the higher the energy consumption was, hence higher packet failure rate. The limitation on this experiment was the lack of computational power to run more simulations thus we plan to extend this experiment to a high-performance computing center which then we will include more performance Metrices like jitter, throughput etc.

References

[1] Ali A.S.Ihbeel, Hasein Issa Sigiuk and A.A.Alhnsh, ”Simulation Based

[2] Evaluation of MANET Routing Protocols for Static WSN,” the second international conference on innovative computing technology (in tech 2012), IEEE, Brasil 2012.

[3] V.Rai, ”Simulation of Ad-hoc Networks Using DSDV, AODV And DSR

[4] ProtocolsAnd Their Performance Comparison,” Proceedings of the 4th National Conference; INDIACom-2010.

[5] Ming-Yang Su*"WARP:A wormhole-avoidance routingprotocol by anomaly detection in mobile ad hoc networks" Journal Computers & Security 29(2010) 208-224.

[6] Hongmei Deng; Li, W.; Agrawal, D.P., "Routing security in wireless ad hoc networks," Communications Magazine, IEEE, vol.40, no.10, pp.70,75, October, 2002.

[7] Sanzgiri, K.; Dahill, B.; Levine, B.N.; Shields, C.; Belding-Royer, E.M., "A secure rout ing protocol for ad hoc networks," Network Protocols, 2002. vol., no., pp.78,87, Nov. 2002

[8] Y. Zhang, Lee W., “Intrusion detection in wireless ad hoc networks,”Proceeding of MOBICOM, Aug 2000.

[9] L. Zhou, Haas Z., “ Securing ad hoc networks,” IEEE Network Magazine, vol. 13, no.6, Nov/Dec 1999.

[10] P. J. Mohamed A.A, "Analysis of Security Attacks on AODV Routing," IEEE, pp. 290-295, 2013.

[11] M. E.-r. e. a. Houda M, "Performance Analysis of AODV Routing Protocol in," 2nd International Conference on Electrical and Information Technologies ICEIT, 2016.

[12] A. A. e. a. Nirbhay Chaubey, "Performance Analysis of TSDRP and AODV Routing Protocol under Black Hole Attacks in MANETs by Varying Network Size," International Conference on Advanced Computing & Communication Technologies, pp. 320-324, 2015.