International Journal of Computer Networks and Communications Security

VOL. 1, NO. 1, JUNE 2013, 1–6
Available online at: www.ijcncs.org
ISSN 2308-9830

Performance Evaluation of Routing Protocol on AODV and DSR under Wormhole Attack

Mojtaba GhanaatPisheh Sanaei[1], Ismail Fauzi Isnin[2], Majid Bakhtiari[3]

[123]Faculty of Computer Science and Information system
Universiti Teknologi Malaysia (UTM)
Johor 81310, Malaysia

E-mail: [1]ghanaatpisheh.m@gmail.com, [2]ismailfauzi@utm.my, [3]bakhtiari.majid@gmail.com

ABSTRACT

Today's Mobile Ad hoc Networks (MANETs) became a popular issue for scientists, and diverse studies have been made to increase the performance of ad hoc networks. In MANET nodes compromise to forward packets for each other communicate beyond their transmission range. The mobile nodes communicate with each other without any infrastructure. As wireless ad-hoc networks lack an infrastructure, they are exposed to a lot of attacks [1]. One of these attacks called Wormhole Attack that two adversary node collaborate together to transmit the packets in out of band channel. In this paper, performance of Ad hoc on-Demand Distance Vector (AODV) Protocol and Dynamic Source Routing (DSR) protocol are evaluated in presence of wormhole attack and without wormhole attack with Constant Bit Rate (CBR) traffic under dissimilar scalable network mobility. Also we evaluate effect and compare it with standard protocol in term of Packet Delivery Ratio, throughput and End to End Delay via simulation, using Network Simulation2 (NS2) for our research.

Keywords: *Mobile Ad-Hoc Network, Wormhole Attack, Ad hoc on-Demand Distance Vector, Dynamic Source Routing, Constant Bit Rate.*

1 INTRODUCTION

As mentioned before an ad hoc network is a wireless network, which do not have a fixed and centralized infrastructure. MANET is a kind of ad hoc network, which can alter location and self-configure on the sky [2]. MANET can be a standard Wi-Fi connection, like a cellular or satellite broadcast and sometimes they are limited to a local area of wireless system, such as a group of laptops. A Vehicular Ad Hoc Networks (VANETs) is a kind of MANET that permits vehicles to connect with wayside equipment [3]. When vehicles may not have a direct Internet connection or link, the wireless wayside equipment can be connected to the Internet, permit the vehicles to send data over the Internet. The vehicle data can be used for measure traffic or keep track of trucking navies. Because of the nature of mobile ad hoc network, usually not very secure, so it is essential to be precaution what data is sent over MANET. The mobile nodes have senders and receivers with smart antennas, which permit the mobile nodes to communicate with each other's. Figure 1 shows a simple mobile ad hoc network.

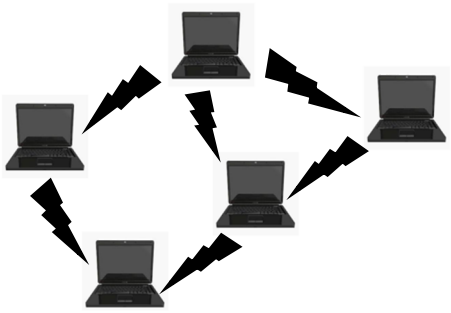

Fig. 1. A mobile ad hoc network

The topology of network changes periodically by getting in and out of the nodes on the network. The first goal of invention of MANET was for militarily

and healthy purposes, but now it's used in many area. Such as data collection in some zone, disaster hit regions and in salvation missions [4].

Many security methods were introduced by researchers in MANET, because the existence of critical and important issues in this type of network. Nodes in MANETS lose much energy like battery power by attaching in and out with junction to wireless network [5]. The main goal of developing the ad-hoc routing protocols is to confronting with the dynamic nature of MANET. The efficiency of routing protocol can be specified by the energy consumption. Battery power is used during routing traffic and joining a node in a network as well.

Basically routing protocols are categorized to three types, reactive, proactive and hybrid routing protocol. Proactive routing protocol is table-driven verses reactive routing protocol is on-demand protocol [6]. DSR and AODV both are reactive routing protocol, but they have differences with each other. In AODV routing a source node initiate routing protocol but in DSR routing a route cache is kept, and due to this over head of memory increases. In AODV routing protocol every node maintain the routing table and each routing table involve of next node information for a route to the sink. The intermediate nodes between the sender and receiver are responsible for discovering a nearest and fresh route to the destination in route detection process. In routing attack, malicious node immediately replies to these path discovery processes giving incorrect Information of having a nearest path to destination. Source node supposes that sending data packets through legitimate route; In fact packets forwarding via two malicious node that collaborate together to send data packet to destination through out-of-band channel [7].

2 OVERVIEW ON AODV AND DSR ROUTING PROTOCOL

In this section we are going to explain two popular reactive protocols on mobile ad hoc network [8].

2.1 Ad hoc on-Demand Distance Vector (AODV) Protocol

AODV routing is a routing protocol for mobile ad hoc network (MANETs) and other wireless ad-hoc network. It is a reactive routing protocol, meaning that it establishes a route to a destination node only on demand [9]. For sending the packet to destination, it broadcast request packet to neighbors, also this neighbors re-broadcast that packet to their neighbors. This possess will continues until the packet reached to the destination. Upon the destination received the first request packet from the source node, it send a reply packet to source node following the reverse path [10]. Also all intermediate nodes set up forward path entries in their table. When the fault happened in any link to a node, the neighboring nodes forward path fault to all neighbors that utilizing the link. This is a gol of the discovery packet to find the broken link. The weakens of AODV is vulnerable to worm hole attack [7]. It is possible the request packet forwarded to destination nod faster as other path, when two colluding nodes using high speed channel to send the packet. Base on this routing protocol, the destination node drop all later request packets received, even they are received from trusted node. Therefore the destination selects the false path through wormhole for replay packet. In contrast, the most common routing protocols of the Internet are proactive, meaning they find routing paths independently of the usage of the paths like DSR.

2.2 Dynamic Source Routing (DSR) protocol

DSR is a reactive routing protocol as send the packet to destination to discover address of route. This routing needs source route maintenance, while the use of route, it is needed to monitor the process of the route and notify the sender of any mistake [11]. It is weak against wormhole attack and DoS attack could be occurred at the destination. This routing protocol needs to forwarding of only the first RREQ packets received by it and will drop other RREQ packets for the same route. This RREQ packet includes some information about intermediate nodes and the hop count. The route used to send data packet, when the route discovered. According to wormhole attack, that uses fast channel for forwarding the message, the RREQ packet through them will receive to destination faster than other paths. This result will be from a wormhole route to be discovered as the route to destination nod. The packet may be selectively or fully dropped by the wormhole attacker resulting permanent DoS attack at the destination node.

3 WORMHOLE ATTACK ON MANET

The mobile ad hoc networks faced to many securities threats [12]. These threats can destroy or interrupt the normal performance of the networks. Wormhole attack is one of these threats that happen by two or more malisons node. This kind of attack done by two malicious nodes in which the first malicious node eavesdrop or listen in packets at one area and then send them by tunnel to second

malicious node in other area [13]. Forwarding data packet between this two or more adversary node occurred via directional wireless connection or direct wired connection.

For example in Figure 2, the source node (S) sends packets to destination node (D) through two routes. In first route the packet is sent to destination by five nodes that we call normal path (A-B-C-D) and the second route is wormhole path, which packet are sent to destination by three nodes (W1-W2-D). When the packets transmit through node W1, the data eavesdropped by the adversary, it means nodes W1 and W2 can catch data packet and tunneled the data to node (D) very fast, before other rote deliver their packet to node D, therefor the packets from legitimate routes dropped and wormhole path chosen for transferring data packet between source and destination.

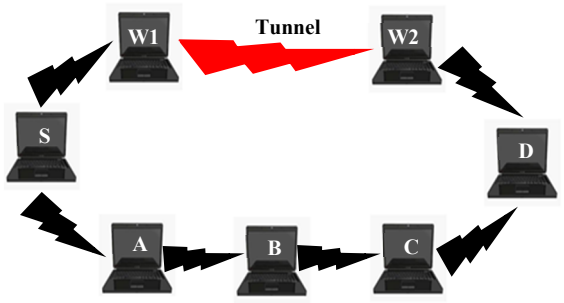

Fig. 2. A simple wormhole attack

4 SIMULATION PARAMETERS

The simulation implemented by Network Simulation 2 (NS2) [14], to simulate mobile ad hoc network circumference. We accomplish the random waypoint motion model for our simulation, in which the node starts at accidental position, waits for the pause time, and then goes to another accidental position with the 0 m/s to the maximum simulation speed. The size of each packet is 512 bytes and a forwarding rate of 3 packets per sec [15]. The simulation parameters are shown in Table 1.

Table 1: Simulation Parameter Value

Simulation Parameters	***Value***
Routing Protocol	AODV, DSR
Application traffic	CBR
Number of Nodes	30
Transmission range	200 m
Transmission rate	3 packets/sec
Packet Size(bytes)	512
Number of malicious nodes	2
Pause time	10 s
Simulation Time	1000 s
Simulation area(m2)	500*500
Type of Attack	Wormhole

5 RESULTS AND DISCUSSIONS

We have used three parameters for assessing the execution of two on demand reactive, AODV and DSR, routing protocols.

5.1 Evaluation without attack

According to mobility of nodes and the size of network, the overall performance of the protocols can be compared in conditions of three parameters:

5.1.1 Packet Delivery Ratio (PDR)

The PDR can be estimated as the ratio of the number of delivered data packet to the destination and the number of data packets that are sent by the source. Figure 3 shows as the count of node increase it gets better because contingency of route breakage decrease. For calculating the PDR the following formula can be used:

$$PRD = \frac{\sum \text{Count of packet receive}}{\sum \text{Count of packet send}} \quad (1)$$

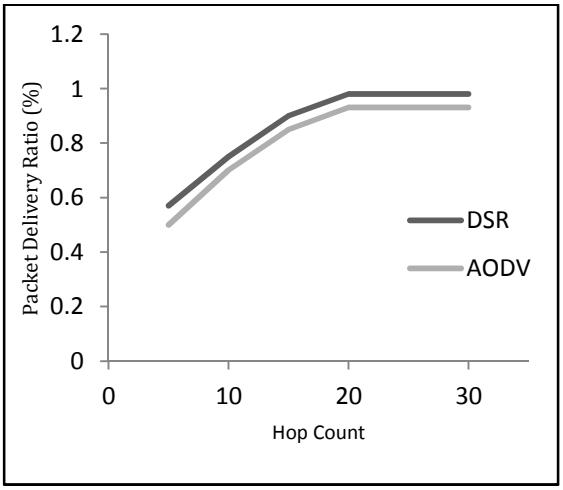

Fig. 3. Packet Delivery Ratio

5.1.2 End to End Delay of data packets (E2ED)

E2ED is the average time that taken by a data packet to arrive in the sink. It contains the queue in data packet forwarding and the delay caused by path discovery process. Only the data packets are counted that successfully received by destination.

To calculate the E2ED, we need the time difference between the packets were sent and received, and then we should divided them to the total time difference over the total count of packets. For estimating the E2ED the following formula can be used:

$$E2ED = \frac{\sum \text{Arrive time} - \text{Send time}}{\sum \text{Count of connections}} \quad (2)$$

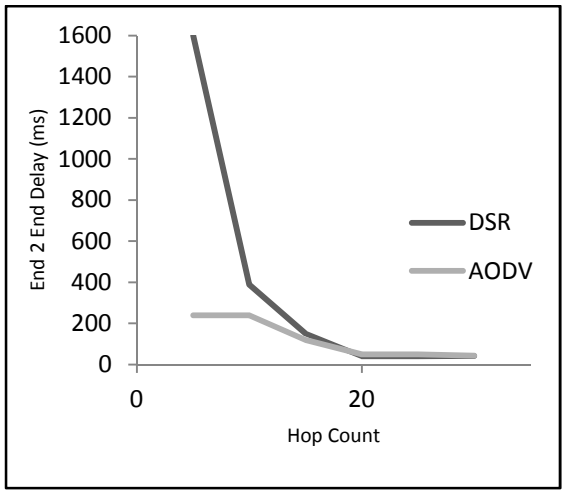

Fig. 4. End 2 End Delay

5.1.3 Throughput

The average rate of successful packet delivery over a communication channel called throughput. The throughput is usually measured in bit/s or data packets/sec. From below graph we can analyze as count of node growth in network throughput gets better.

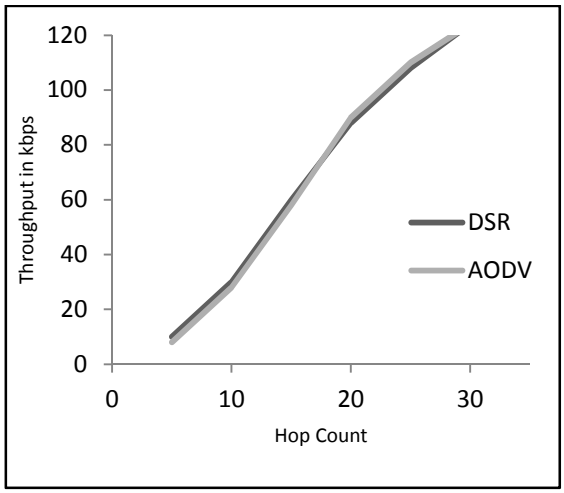

Fig. 5. Throughput

5.2 Evaluation without attack

And now, performance of the protocols in terms of three parameters with attack:

5.2.1 Packet Delivery Ratio (PDR)

In low traffic mode AODV protocol delivers approximately 90 percent of data packets, but the packet loss begins when the number of nodes goes up. DSR routing show short efficiently than AODV when count of nodes are low, but when network load increment PDR of DSR degraded faster compared with AODV.

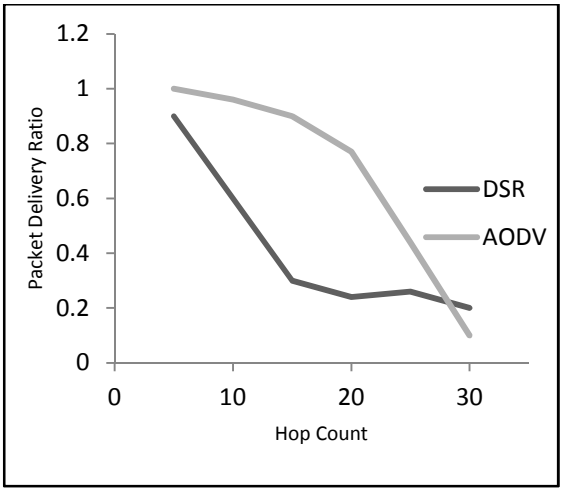

Fig. 6. Packet Delivery Ratio

5.2.2 End to End Delay of data packets (E2ED)

In Figure 7 the average of E2ED is low. Base on AODV protocol, only one route that is shortest route for transfer data packet, but DSR use more than one route which makes more delay as it is not always using shortest path for to delivery packet from sender node to sink node due to this reason average E2ED for AODV is low compared with DSR.

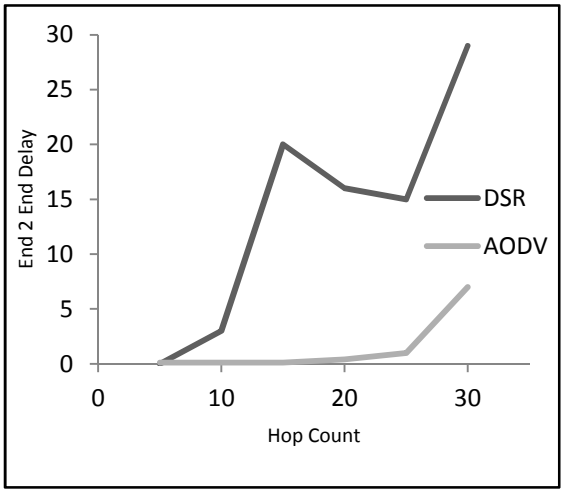

Fig. 7. Average End 2 End Delay

5.2.3 Throughput

According to AODV routing, it uses only one path to transfer packet as long as path fails. After failure, it starts again for finding a new path between source and destination by discovery process. Utilizing only one path for sending packets from source to destination makes short change in delay which will with lead to short throughput. Figure 8 show that Throughput is always high in DSR, because of using more than one path to delivery packets from source to destination, unlike AODV protocol. These different paths make change in delay to forwarding the packet, due to this issue gain considerable throughput in case of DSR. For AODV and DSR protocols throughput increases when count of node increases.

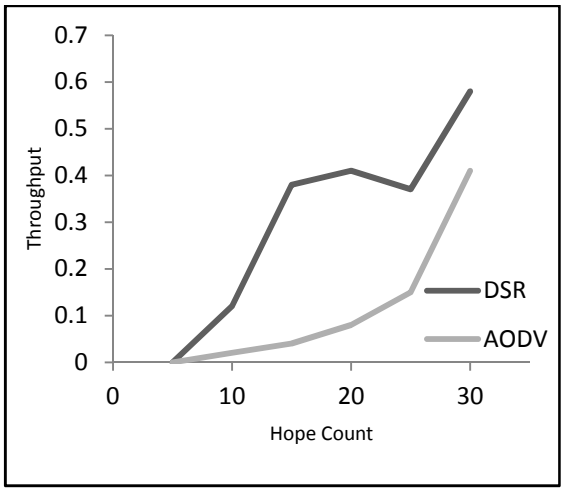

Fig. 8. Throughput

6 CONCLUSION

In this research paper we generally analysis the perform-ance of two On-Demand routing protocols DSR and AODV on the basis of average End 2 End delay, Packet Delivery Ratio and throughput. We have simulated our work with malicious node and without malicious node on ad hoc network. Also we used CBR for our traffic para-meters. Du mobility of nodes we chose random way point model with CBR traffic sources. AODV is gives better performance than DSR for Average End 2 End delay and when node density is low. Based on our analysis and research, the DSR routing is vulnerable to wormhole attack than AODV.

7 REFERENCES

[1] Sanaei, Mojtaba GhanaatPisheh, Babak Emami Abarghouei, Hadi Zamani, Miranda Dabiranzohouri. "An Overview on Wormhole Attack Detection in Ad-hoc Networks." Journal of Theoretical and Applied Information Technology. 52, no. 2, June 2013.

[2] Sanaei, Mojtaba GhanaatPisheh, Babak Emami Abarghouei, and Hadi Zamani. "Performance Analysis of SRTLD and BIOSARP Protocols in Wireless Sensor Networks." International Journal 3, no. 4 (2013).

[3] Hartenstein, Hannes, and Kenneth P. Laberteaux. "A tutorial survey on vehicular ad hoc networks." Communications Magazine, IEEE 46.6 (2008): 164-171.

[4] Sweta, Soni, Arun Nahar, and Sanjeev Sharma. "Performance Evaluation of Efficient MAC in Mobile Ad Hoc Wireless Networks." International Journal of Computer Science 8.

[5] Mishra, Manoj Kumar, et al. "Measure of Impact of Node Misbehavior in Ad Hoc Routing: A Comparative Approach." IJCSI (2010): 10.

[6] Singh, Smita, et al. "Comparison and Study of AOMDV and DSDV Routing Protocols in MANET Using NS-2." International Journal (2012).

[7] Narmada, Mrs A., and P. Sudhakara Rao. "Performance Comparison Of Routing Protocols For Zigbee Wpan."

[8] Karimi, Ramin, Mahboobeh Haghparast, and Ismail Fauzi ISnin. "Secure Geographic Routing Protocols: Issues and Approaches." arXiv preprint arXiv:1111.6539 (2011).

[9] Soni, Santosh Kumar. "Performance simulation of MANET protocols with the combination of horizontal and vertical topology using NS2." Wireless and Optical Communications Networks (WOCN), 2012 Ninth International Conference on. IEEE, 2012.

[10] Sheu, Jang-Ping, et al. "Virtual landmarks assisted routing protocol in Vehicular Ad hoc Networks." Personal, Indoor and Mobile Radio Communications, 2009 IEEE 20th International Symposium on. IEEE, 2009.

[11] Hassnawi, L. A., et al. "Measurement study on the end-to-end data transmission in motorways surveillance system using Wireless Ad Hoc Camera Networks (WAHCN)." Engineering and Industries (ICEI), 2011 International Conference on. IEEE, 2011.

[12] Maroofi, Rehan, Vilas Nitnaware, and Shyam Limaye. "Area Efficient Design of Routing Node for Network-on-Chip." International Journal of Computer Science Issues (IJCSI) 8.4.

[13] Sookhak, M., et al. "Detecting wormhole attack in wireless Ad-hoc network." International Journal of Computer Science and Telecommunications 2.7 (2011): 28-34.

[14] Shah, Samyak, et al. "Performance Evaluation of Ad Hoc Routing Protocols Using NS2 Simulation." Conf. of Mobile and Pervasive Computing. 2008.

[15] Bhalaji, N., and A. Shanmugam. "Reliable Routing against selective packet drop attack in DSR based MANET." Journal of Software 4.6 (2009): 536-543.