ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Analysis of AODV and OLSR Routing Protocol Under Wormhole Attack

Er. Neeraj Sharma
Student M.TECH(CBS),CST
Central University of Punjab,
Bhatinda (PB.), India

Abstract:A Mobile Ad Hoc Network (MANET) is a self organizing, infrastructure less, multi-hop network Mobile Ad hoc Networks (MANETs) work without any fixed infrastructure and each node in the network behaves as a router in order to transmit data towards the destination. The characteristics of MANET are both challenges and opportunities in achieving security models, such as confidentiality, integrity, authentication, availability, non repudiation and access control. Wormhole attack is one of the most severe routing attacks, which is easy to implement but hard to detect.In this. Paper we study the effects of Wormhole attack on MANET using both OLSR and AODV. The Mobility Models used are Random Waypoint mobility model and Gauss Markov mobility Model. The purpose of this study is to find which protocol is more vulnerable to the wormhole attack. The NS2 simulation results show the throughput, packet delivery ratio, AVG. End to End Delay, Packet loss received with and without Wormhole Attack.

Keywords:Wormhole, Tunnel, AODV, OLSR, MANETs

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is formed by some wireless nodes communicating each other without having any central coordinator to control their function. In MANET, as the nodes are utilizing open air medium to communicate, they face acute security problems compared to the wired medium. One such critical problem is wormhole attack[1]. Under this attack, two malicious nodes can collude together using either wired link or directional antenna, to give an impression that they are only one hop away. Wormhole attack can be launched in hidden or in participation mode. Wormholes can either be used to analyze the traffic through the network or to drop packets selectively or completely to affect the flow of information. The security mechanisms used for wired network such as authentication and encryption are futile under hidden mode wormhole attack, as the nodes only forward the packets and do not modify their headers.

II. ROUTING PROTOCOLS AND WORMHOLE ATTACK

Many routing protocols are available for MANET[2]. In this paper, we use AODV and OLSR routing protocol because these protocols are vulnerable to the wormhole attack. So we have simulated the behavior ofwormhole attack onAODV and OLSR in MANET.

A. AODV (Ad-hoc On-demand Distance Vector)

It is a pure on-demand routing protocol. For sending messages to destination, it broadcasts RREQ messages to its immediate neighbors. These neighbors in turn rebroadcast them to their neighbors. This process continues unless the RREQ message reaches the destination. Upon receiving the first RREQ message from the source node, it sends a RREP to the source node following the same reverse path. All the intermediate nodes also set up forward route entries in their table. Upon detecting error in any link to a node, the neighboring nodes forward route error message to all its neighbors using link. These again initiate a route discovery process to replace the broken link. The AODV routing protocol is vulnerable to wormhole[3] attack. Since the colluding nodes involved in wormhole attack uses a high speed channel to send messages, it is possible that the RREQ packet through them reaches the destination faster compared to usual path. According to this protocol, the destination discards all the later RREQ packets received, even though they are from authenticated node. The destination therefore chooses the false path through wormhole for RREP.

B. OLSR (Optimized Link State Routing)

OLSR is a proactive routing protocol. Topology information is exchanged periodically. Hello messages are broadcast to discover single hop neighbors. To distribute signaling traffic, flooding mechanism is used where every node forwards a flooded message not forwarded by it earlier. Topology messages containing the information about link states are then sent to all other nodes. From this information, each node computes the shortest path using symmetric links to form a partial topology graph. It is open to wormhole attack[4]. Remote nodes may send hello and topology control messages available at its colluding nodes to its own neighbors for dissemination as false information into the network. This will make two faraway nodes to wrongly consider themselves as neighbors, leading to failure of routing protocol.

OLSR optimize a link state protocol andcompress the information size of a send messages, and decrease the retransmission packets. It provides optimal based on number of hops. OLSR has a property of having the routes immediately available when needed; it is because of its proactive nature. In a link state protocol, all the links are declared to neighbor nodes and flooded in the network. OLSR is an optimization of link state protocol for MANET.[4]

III. WORMHOLE ATTCK IN AODV AND OLSR

Wormhole attack is a dangerous attack for MANETs. As soon as receiving a malicious node packet in this attack from one location in the network, it connects to other locations in the network, and as a matter of fact, these packets are sent into the network repetitively.[2]. This connection acts as a wormhole for the tunnel link two attackers. In this attack the attacker

create a wormhole depending on the kind of network connection (Wired or Wireless) even for packets without any addresses to itself because of the broadcast nature of these two kinds of networks. According to[3] Wormhole attacks can be arranged easily. For creating a wormhole attack, at least two transceivers are set at different locations on a wireless network by attacker.

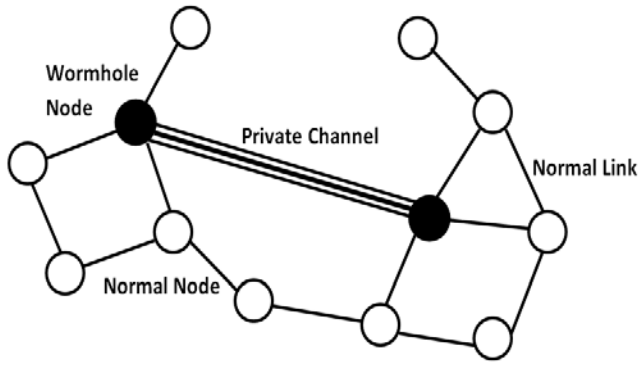

Figure 1.Wormhole Attack in AODV Protocol

According to [5] wormhole attack is an active attack. Wormhole attacker affects the original functionality of MANET routing protocols such as AODV and OLSR etc, but this research work emphasizes on wormhole attack in AODV and OLSR routing protocol.

Suppose a source wants to talk with destination.And this communication is possible through shortest path provided by AODV protocol (called normal route)[6]. But if two malicious nodes are kept at two different locations in the network and a malicious node accepts the traffic at one location, tunnels them through wormhole link to another malicious node, then replays packets into the network at that location, then this is called wormhole route [7]. Hence, the functioning of AODV protocol is completely disrupted by this attack. It affects various parameters such as delay, throughput, and packet delivery ratio.etc[8][9].

IV. SIMULATION SETUP &METHODOLOGY

To construct a real distributed testing environment, the cost and complexity is very high. So simulation is widely used in network research. Simulation is the manipulation of the model of a system that is used to observe the behavior of a particular system in a setup similar to real-life[10]. NS2 simulator is used in this research work and it is the most widely used simulator. This study was performed on Intel Core i3computer system using Ubuntu Linux 12.04 OperatingSystem.

A. Simulation Methodology

This work has been divided into following steps:

Step 1:Simulation of the on demand-oriented routing protocol AODV under two mobility models: RWP(Random Way Point) and GMM(Gauss Markov Mobility Model) by varying 10,20,30,40[9]. Number of nodes with Attack or Without Attack under MANETs.

Step 2:Simulation of OLSR under wormhole attack using two mobility models: RWP (Random Way Point) and GMM (Gauss Markov Mobility Model) by varying 10,20,30,40[9]. Numbers of nodes with Attack or without Attack under MANETs.

Step 3:Comparison of both routing Protocol under wormhole attack using two mobility models: RWP (Random Way Point) and GMM (Gauss Markov Mobility Model) by varying 10,20,30,40[9]. Numbers of nodes with Attack or without Attack under MANETs.

Table *1.* Summary of Parameters Used for Simulation

Area	*600m X 800m*
Simulation Time	100s
Number of Nodes	15,20,25,30,40
Routing Protocol	AODV,OLSR
Traffic Model	CBR
Pause Time	1s
Minimum Node Speed(m/s)	0
Maximum Node Speed	15,20,25,30,40
Transmission Power(mW)	0.6
Residual Power(mW)	0.3
Packet Size	512 bytes
Mobility Models	Random Way Point, Gauss Markov Model
Number of wormhole Nodes	2
Examined Approaches	With Attack , Without Attack
Parameter	End to End Delay ,Throughput, Packet Delivery Ratio,Packet loss
Channel	Wireless Channel.

Using AWK scripts, various performance metrics such as PDR, average throughput, and average end to end delay[9][11][12] have been analyzed graphically.

To analyze malicious nodes, an implementation hasbeen done at NS2 link layer. Required coding has beendone in ll.cc and ll.h files at link level. Firstly, in ll.cc and ll.h files[12], parameters such as size of wormhole peerlist (tunnel) and properties of nodes are defined and then in Tcl file, the definition of nodes is configured.

The movement scenarios of nodes for both mobilitymodels are generated through Bonn motion tool.[12]

V. ATTACK SIMULATIONS AND RESULTS ANALYSIS

In this section, we discuss experimental setup, followed byperformance evaluation metrics and also simulation results andanalysis.

A. Experimental Setup

The simulations are carried out using NS-2.35 network simulator to evaluate the effect of worm hole on AODV and OLSR routing protocol in MANET[2][9]. We userandom waypoint model as the mobility model and set thetraffic source to Constant Bit Rate (CBR); nodes move withinan area;. Therefore, we have used the scenario parameters aslisted in table 1 for each of the cases, varying the number ofnodes,

mobility, connections and attackers with successive. Simulations.

B. Performance Evaluation Metrics

The following performance metrics are considered forevaluation of malicious behavior of AODV and OLSR routing protocol Under Wormhole.

- ***Packet delivery ratio(PDR):****It* is the ratio between thetotal number of packets received by destination nodes and the total number of packets generated by the source nodes. Hence,the packet delivery ratio shows the total number of the data packets that reach destination successfully[9]. Higher packetdelivery ratio shows higher protocol performance.

$$PDR = \frac{\sum Number\ \ of\ packet\ \ recieve}{\sum Num\,ber\ \ of\ \ packet\ \ send} \qquad (1)$$

Figure 2 show conclude that the Packet Delivery Ratio with Attack will be less as compare to Figure 3 in without Attack under both the cases but The AODV have better performance as compared to OLSR.

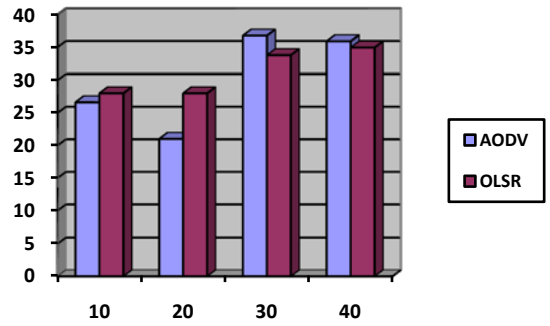

Figure 2. PDR of AODV and OLSR with Attack

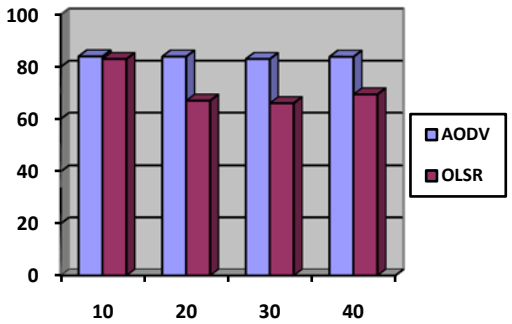

Figure 3.PDR of AODV and OLSR without Attack

- ***End to end delay:*** End to End of data packet is the time consumed by data packets to reach to respective destinations. It includes all the delay taken by router to seek the path in network: buffering, transmission, propagation, and re-transmission[11]. The average end to end delay for a packet which was sent by thenode, as a source node and received successfully at destination node is:

$$\text{End to end delay} = \frac{\text{Arrival time} - \text{send time}}{\text{Number of connections}} \qquad \textbf{(2)}$$

Where Arrive time is the time when the packet is received Successfully at destination node, and Send time is the timewhen sending of packet by node. The lower average end to end delay is the better.

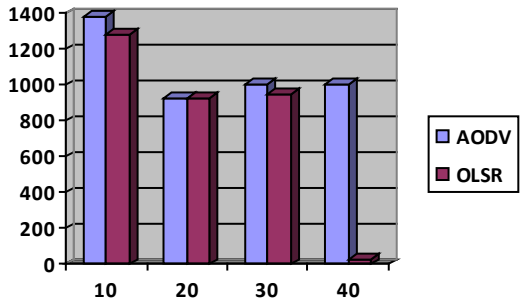

Figure 4. *AVG. End to End Delay of AODV and OLSR* with Attack

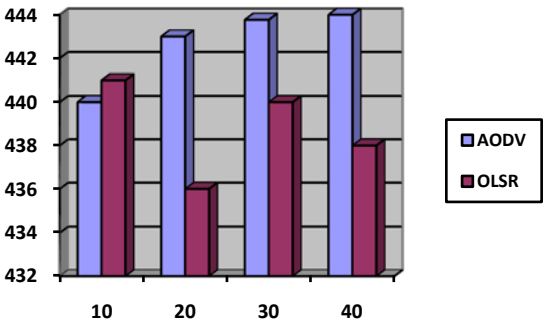

Figure 5. *AVG. End to End Delay of AODV and OLSR* without Attack

- ***Throughput:*** It can be defined as the number of successful bits per unit of time forwarded by the network from a source toa destination. Throughput is represented in bits/bytes persecond. A higher throughput is most essential factor in anynetwork[11].

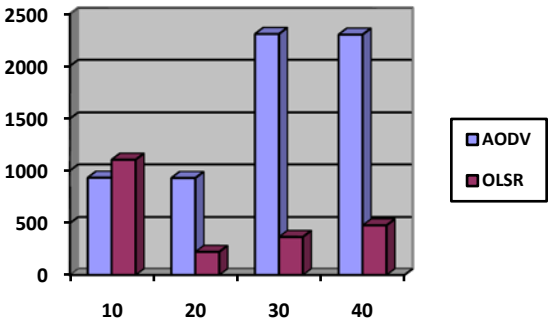

Figure 6.*Throughput of AODV and OLSR*with Attack

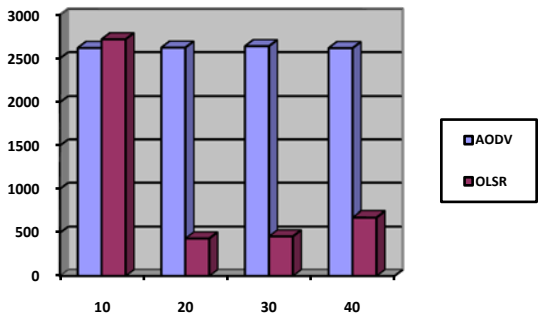

Figure 7.*Throughput of AODV and OLSR*without Attack

Figure 6 shows the throughput under attack in both the protocols is less but have different results.
Figure 7 shows the result of throughput in without case which is high as compare to with attack

- ***Packet loss:*** It is the difference between the total numberof data packets sent by the source node and received by the destination node.[9]

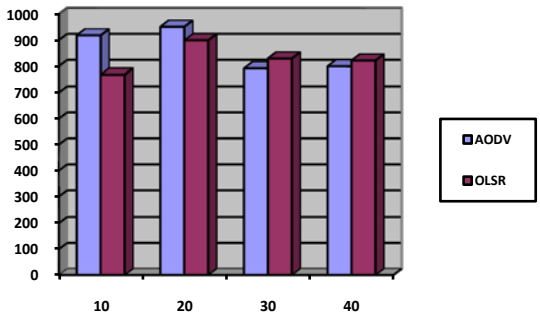

Figure 8.*Packet Loss of AODV and OLSR* with Attack

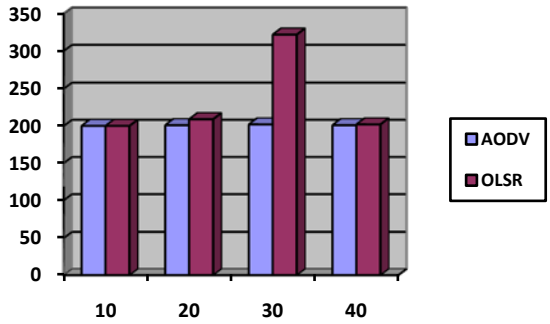

Figure 9. *Packet Loss of AODV and OLSR*without Attack

VI. CONCLUSION

In this Research Work, an exhaustive simulation for MANET is done using AODV and OLSR routing protocols[4] and the effect of the presence of wormhole is also simulated. Significant parameters such as throughput, end to end delay, packet delivery ratio and packet loss have been considered. The study focuses on how it is affected under wormhole attack in a network. These attacks have been implemented in NS-2 based on AODV and OLSR routing protocol. Then, I have compared the performance of AODV under attacks with OLSR in terms of Random Waypoint mobility model[12] and Gauss Markov mobility Model. From the simulations, Therefore, the Packet Delivery Ratio decreases in the network with a worm hole node. In addition, it is observed that the End-to-end Delay is higher in the wormhole attack. The throughput of the network is decreased with the wormhole attack. Consequently, the wormhole attack has a higher significant effect on the network performance. AODV is more vulnerable to wormhole attack in mobility domain, whereas OLSR is least vulnerable in non-mobile Domain[4]. Packet delivery ratio is overall low for AODV in Mobility domain.

VII. REFERENCES

[1] M. Enshaei and Z. B. Hanapi, “A review on wormhole attacks in manet,” *J. Theor. Appl. Inf. Technol.*, vol. 79, no. 1, pp. 7–21, 2015.

[2] P. North, M. Arena, and P. Area, “Advanced AODV Approach For Efficient Detection And Mitigation Of WORMHOLE Attack IN MANET,” 2016, pp. 1–6.

[3] G. Garg, S. Kaushal, and A. Sharma, “Reactive protocols analysis with wormhole attack in ad-hoc networks,” in *5th International Conference on Computing Communication and Networking Technologies, ICCCNT 2014*, 2014, pp. 7–13.

[4] P. Nagrath and B. Gupta, “Wormhole attacks in wireless adhoc networks and their counter measurements: A survey,” *ICECT 2011 - 2011 3rd Int. Conf. Electron. Comput. Technol.*, vol. 6, pp. 245–250, 2011.

[5] Z. Tun and A. H. Maw, “Wormhole Attack Detection in Wireless Sensor Networks,” 2008, pp. 545–550.

[6] M. Su, “WARP A wormhole -avoidance routing protocol by anomaly detection in mobile ad hoc networks,” *Comput. Secur.*, vol. 29, no. 2, pp. 208–224, 2010.

[7] C. Gupta and P. Pathak, “Movement based or neighbor based tehnique for preventing wormhole attack in MANET,” *2016 Symp. Colossal Data Anal. Networking, CDAN 2016*, pp. 1–5, 2016.

[8] M. Salehi, A. Boukerche, and A. Darehshoorzadeh, “Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks,” *Ad Hoc Networks*, vol. 50, pp. 88–101, 2016.

[9] H. Moudni, M. Er-Rouidi, H. Mouncif, and B. El Hadadi, “Performance analysis of AODV routing protocol in MANET under the influence of routing attacks,” in *Proceedings of 2016 International Conference on Electrical and Information Technologies, ICEIT 2016*, 2016, pp. 536–542.

[10] M. Sharma, A. Jain, and S. Shah, “Wormhole attack in mobile ad-hoc networks,” *2016 Symp. Colossal Data Anal. Networking, CDAN 2016*, pp. 1–4, 2016.

[11] M. Sadeghi and S. Yahya, “Analysis of Wormhole attack on MANETs using different MANET routing protocols,” *ICUFN 2012 - 4th Int. Conf. Ubiquitous Futur. Networks, Final Progr.*, pp. 301–305, 2012.

[12] G. Kaur and A. Kaur, “Performance Analysis of AODV for Wormhole Attack Using Different Mobility Models,” 2014, pp. 69–72.