Analysis of Worm-Hole Attack in MANET using AODV Routing Protocol

Ms Neha Choudhary, Dr Sudhir Agrawal
Truba College of Engineering & Technology, Indore, INDIA

***Abstract*—** MANET is an infrastructure less, dynamic, decentralized network. Any node can join the network and leave the network at any point of time. Due to dynamic infrastructure-less nature and lack of centralized monitoring points, the ad hoc networks are vulnerable to attacks. The network performance and reliability is break by attacks on ad hoc network routing protocols. AODV is a important on-demand reactive routing protocol for mobile ad hoc networks. There is no any security provision against a "Wormhole" attacks in existing AODV protocol The wormhole attack is also one of the severe attacks of MANET. The wormhole attack is basically launched by a pair of collaborating nodes. In wormhole attack two collaborating attacker nodes occupy strong strategic locations in two different parts of the network and advertise to have the shortest path for transmitting data and make wormhole tunnel.. This paper discusses some of the techniques put forwarded by researchers to detect and prevent worm hole attack in MANET using AODV protocol .

***Index Terms*—** MANET, AODV, adhoc, worm hole attack, Malicious Node.

I. Introduction

1.Introduction: Mobile Ad-hoc Network (MANET) is formed by some wireless nodes communicating each other without having any central coordinator to control their function. Such a network is helpful in creating communication between nodes that may not be in line-of-sight and outside wireless transmission range of each other. Similar wireless networks have important applications in a wide range of areas covering from health, environmental control to military systems. In MANET, as the nodes are utilizing open air medium to communicate, they face acute security problems compared to the wired medium. Under Wormhole attack, two faraway 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 [1].

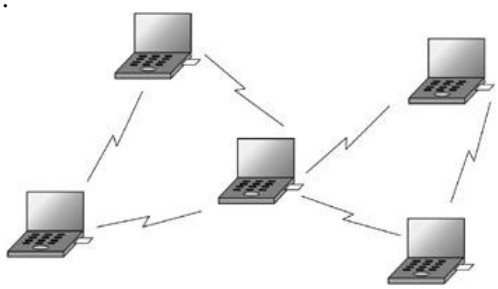

Figure1.1: Simple Mobile Ad-hoc etwork

II. Wormhole attack

2. Wormhole attack: The wormhole attack is one of the most severe attacks of MANET. Wormhole attack is a type of the Denial-of-Service attacks effective on the network layer. It affects network routing, and especially location based wireless security [2]. The wormhole attack is basically launched by a pair of collaborating nodes. In wormhole attack two collaborating attacker nodes occupy strong strategic locations in two different parts of the network. By occupying dominant positions in a network these two nodes can cover complete network and advertise to have the shortest path for transmitting data. The two attacker nodes are connected to each other using a link which is called wormhole tunnel. At one end of wormhole tunnel, one node overhears the packets in its local area and forwards them to the other node which replays them to its local area.

The wormhole tunnel can be established to obtain a direct low latency communication link between two distant nodes (attacker nodes) using private high speed network for example using an Ethernet cable or optical link. If these two nodes forward all the packets legitimately then in a way they are supporting the faster communication and routing within the network. However, this is not the case as these attacker nodes either drop or selectively

forwards the packets or alter them.

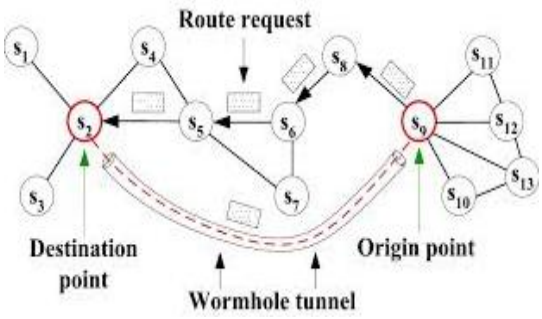

Figure 2.1: Wormhole Attack

Figure 2.1 shows the two attackers placed themselves in a strong strategic location in the network. Here the target node sends RREQ packets all over the network to find out the possible legitimate routes. As the attacker 1 receives the RREQ packet sent by the target node it forwards it to the attacker 2 over the wormhole link between them. As the colluding attacker 2 receives the RREQ packet, transmit it to the destination node. The destination node on its part sends a RREP packet back to the target node over the wormhole link between the colluding attackers. In order to present them as a legitimate route, the colluding attackers forward the RREP packet to the target node. After they are picked up by the target node for the transfer of the data as authentic users within MANET, the attackers can intercept the data flow, i.e. receive the information and does not forward it to the end user (destination node), or selectively forward data packages in order to not being caught.

2.1 Types of Wormhole Attack

Wormhole attack can be launched by using various techniques in wireless networks. These are as follows [2]:

2.1.1Wormhole using Out-of-Band Channel: In this type of wormhole attack is launched by using a dedicated out-of-band high bandwidth channel to connect two attacker nodes. The link connecting two end points to create a wormhole link is a low latency link. This channel can be achieved, for example, by using a long-range directional wireless link or a direct wired link using an Ethernet cable or high capacity optical link.

Figure 2.2 explains this type of wormhole attack. Node A sends a route request to node B. Nodes X and Y are malicious nodes connected through an out-of-band channel. Node X tunnels the route request to Y. Y is a legitimate neighbour of B. Node Y broadcasts the packet to its neighbours, including B. B receives two RREQ through two paths: A-X-Y-B and A-C-D-E-F-B. The route through wormhole tunnel X-Y is shorter and faster than the other route. Thus B selects path through wormhole tunnel to send RREP.

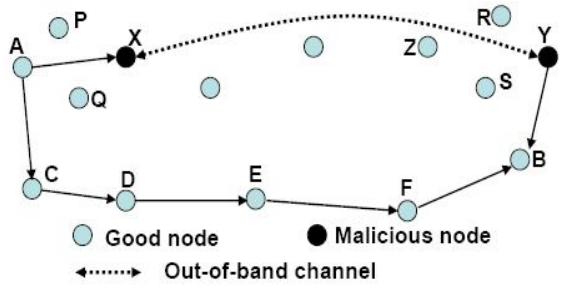

Figure2.2: Wormholes through out of band channels

2.1.2 Wormhole using Packet Encapsulation: When wormhole attack is launched using packet encapsulation, each packet is routed via the legitimate path only. However, when RREQ packet is sent, one node encapsulates the packet such that other nodes on the way are prevented from increasing the number of hop count. When this encapsulated packet is received by the other wormhole end, it is decapsulated to its original form and forwarded in its local area. Thus the destination or other nodes in local area of second colluding node considers the two colluding nodes as direct neighbours and the path through them as the shortest path. Routing protocols that use the shortest path as metric to choose the best route is vulnerable to this type of wormhole attack.

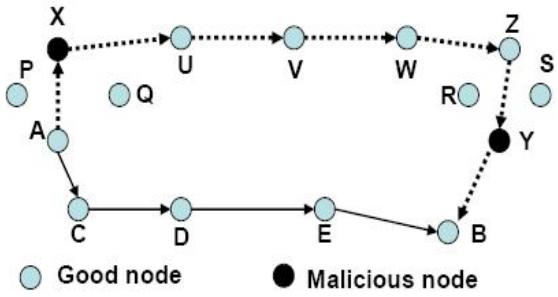

Figure 2.3: Wormhole Attack using packet encapsulation

In Figure 2.3 Node A broadcasts a route request (RREQ). X gets this RREQ and encapsulates it in a packet destined to Y. RREQ reaches Y using the path that exists between X and Y (U-V-W-Z). Node Y after receiving the packet, decapsulates it and rebroadcasts it again, which reaches B. Because of packet encapsulation done at one end, the hop count

does not increase during the traversal through U-V-W-Z. RREQ also travels from A to B through C-D-E. Node B thus receives RREQ from two different routes, the first is four hops long (A-C-D-E-B), and the second is apparently three hops long (A-X-Y-B). Node B will select the second route since it appears to be the shortest but in reality it is seven hops long.

2.1.3Wormhole using High Power Transmission: For launching wormhole attack using high power transmission, a malicious node when gets a RREQ, it broadcasts that request with high power. Another malicious node located in some other part of the network receives this RREQ and rebroadcasts it towards the destination. Using this high power transmission method, the malicious node increases its chance to be in the routes established between the source and the destination.

2.1.4 Wormhole using Packet Relay: Using packet relay wormhole attack can be launched by using only one malicious node also. In this technique the malicious node replays the packets between two distant nodes and convinces them that they are neighbours. In this way fake neighbours are created. Cooperation of a greater number of malicious nodes together makes condition even worse. Cooperating malicious nodes can serve to expand the fake neighbour list of a victim node to several hops. For example, in the figure assume that node A and node B are two non-neighbour nodes with a malicious neighbour node X. Node X can relay packets between nodes A and B to give them the illusion that they are neighbours.

Wormhole attack does not require MAC protocol information. Also wormhole attack can affect the network even without the knowledge of cryptographic techniques implemented [4]. This makes it very difficult to detect.

III. Proposed techniques

3.1 Hop Count Analysis Approach: This research work proposes an efficient technique to detect and prevent wormhole attack without the need for special hardware or strict location or synchronization requirements. The proposed technique makes use of variance in routing information between neighbors to detect wormholes. The detection technique uses an approach based on hop count. The wormhole affected routes are distinguished from legitimate routes by analysing the hop count value of all paths. The basic idea of the technique is to discover alternative routes to the destination. These alternative routes will be extensively dissimilar in length i.e. the lengths of the alternative paths are invariably greater than the path including wormhole tunnel.

3.1.1 Overview: The objective of this research was to detect and prevent wormhole attacks in AODV routing protocol which has been done in the proposed technique based on hop count analysis approach. The basic idea behind the proposed technique is using hop count as a parameter to distinguish paths containing wormhole tunnel.The basic idea of hop count analysis is illustrated in figure 3.1. Mostly the routes contain larger hop count value for example hop count value is 5 and 6 in the network shown in figure, to establish connection between source node and destination node. While the hop count value of the path going through wormhole tunnel will be much smaller, in this case the value of hop count is 2. It can be explained as, consider a source node which wants to communicate with a destination node. If source node communicates through the wormhole tunnel then it encounters only 2 hops. But the other possible alternative routes comprise 5 or 6 hops to transfer a packet from the same source to destination nodes. Thus it can be a basic approach that the route path having too small hop count value or the path having invariably smaller number of hops may be unsafe. So the proposed technique is that by avoiding the route paths having too short hop count value the wormhole tunnel can be kept away.

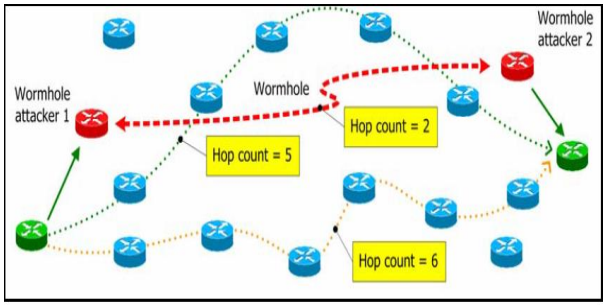

Figure:3.1 Compare hop count values of all available routes linking source node and destination node

In the proposed detection technique, hop count values of all the available route paths is calculated first. Source node then verifies the one hop neighbours and accordingly a threshold value is set, which is used for comparing the number of hops of the current route with the next available route. If the length of the new route differs extensively compared to the length of the preferred path followed by AODV then it can be concluded as a wormhole attack.

3.1.2 Algorithm of the proposed hop count based detection technique: In the proposed technique, any node not necessarily the source node, which is set in detect mode uses this hop count analysis approach to detect and prevent wormhole attack. Whenever any node sends the RREQ packets and in turn start receiving RREP packets, it follows the below mentioned algorithm using the checkpath( ) function module in AODV routing protocol implemented in ns-2. The algorithm is repeatedly executed in ns-2 in every 0.1 seconds. The purpose of repeatedly checking the routes is to ensure that the wormhole attacker nodes should not get included in the selected path for packet transmission from source to destination because of the RREP packet sent by the malicious nodes. This is possible because the malicious node sets the highest sequence number and lowest hop count which is one in the RREP packet.
Hop-count Analysis Algorithm:

1. To detect wormhole in AODV, all the available paths to the destination are checked one by one through routing table.
2. To check the paths, AODV determines number of hops and each one-hop neighbor is verified.
3. If there is one hop neighbour, it is legitimate and threshold is incremented by 1, otherwise it is decremented. This way a threshold value is set.
4. Then the next alternative path is checked in similar manner and number of hops is calculated which again defines a new threshold value.
5. Source node compares length of selected route with alternative path by comparing number of hops and threshold.
6. If the number of hops of the considered route is greater than the set threshold, it is concluded that wormhole exists.
7. On detecting malicious route, the corresponding next hop entry is deleted, so that now that suspected neighbor is not used for routing
8. Similarly other paths are examined using the step 5 – 10.

IV.Results for Comparison for Several Node

4.1 Packet Delivery Ratio Comparison: This subsection shows the packet delivery ratio of the three routing protocols, calculated for different number of nodes. The variation of packet delivery ratio with the number of nodes is shown in figure 4.1.

Table 4.1 PDR Comparison Chart of AODV, AODV under attack and modified AODV

No. of Nodes	AODV	AODV under wormhole attack	Modified AODV
5	99.4%	1.13%	76.8%
10	98.54%	1.46%	55.12%
15	98.66%	0.89%	47.32%
20	87.85%	0.81%	39.27%
25	86.97%	0.57%	42.21%

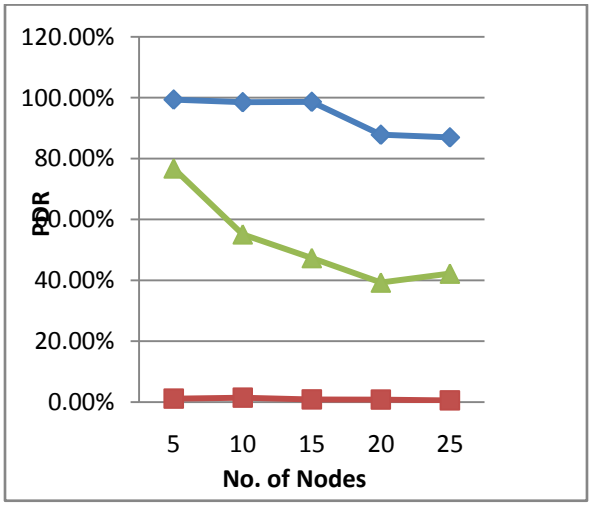

Figure 4.1: PDR Comparison of AODV, Wormhole AODV and Modified AODV

4.2 Average End-to-End Delay Comparison :End-to-end delay for all the received packets is calculated and averaged. In this subsection, average end-to-end delay for the three routing protocols is calculated for different number of nodes. Figure 4.2 shows the average delay for different number of nodes.

Table 4.2: Average end to end delay (in msec) Comparison Chart of AODV, AODV under attack and modified AODV

No. of Nodes	AODV	AODV under wormhole attack	Modified AODV
5	62.67	20.12	96.68
10	15.77	8.58	8.70
15	12.55	41.68	36.27
20	67.8	38.67	40.76
25	252.78	50.62	68.65

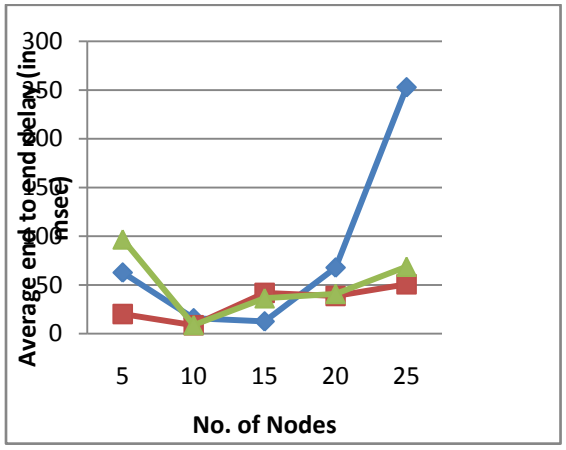

Figure 4.2: Average end to end delay Comparison for AODV, Wormhole AODV and Modified AODV

4.3 Throughput Comparison :The network throughput is calculated at all the destination nodes by including all the links. In this subsection, throughput for the three routing protocols is calculated for different number of nodes. Throughput for different number of nodes is shown in figure 4.3.

Table 4.3 Throughput (in kbps) Comparison Chart of AODV, AODV under attack and modified AODV

No. of Nodes	AODV	AODV under wormhole attack	Modified AODV
5	82.27	102.67	68.45
10	146.71	82.10	94.39
15	131.28	124.43	104.15
20	182.74	96.89	100.75
25	252.98	148.87	148.07

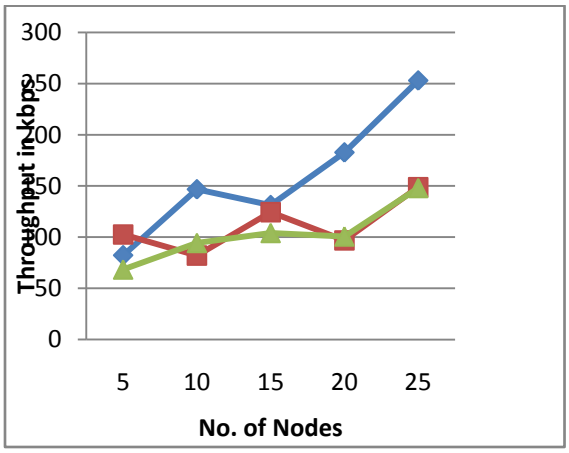

Figure 4.3: Throughput Comparison of AODV, Wormhole AODV and Modified AODV

V. Conclusion

This research work carried out the detailed study and analysis of AODV routing protocols and security issues and attacks in MANET theoretically and through simulation. This research work proposed technique namely hop-count analysis for detecting and preventing wormhole attack. To evaluate the performance of proposed techniques, simulation of wormhole attacks along with the simulation of proposed technique had been done.

VI. REFERENCES

[1]C. K. Toh, "Ad Hoc Wireless Networks"

[2] Z. Danailov, "Attacks on Mobile Ad hoc Netwoks", Seminar Report, Integrated Information Systems, Ruhr University, Bochum, Germany, 2012.

[3]M. Meghdadi, S. Ozdemir and I. Guler, "A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks", IETE Technical Review, Vol.28, Issue 2, pp 89-102, 2011.

[4] B. Wu, J. Chen, J. Wu and M. Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Springer, 2006.

[5]Xu Su Rajendra V. Boppana, "On Mitigating In-band Wormhole Attacks in Mobile Ad Hoc Networks", in proceedings of IEEE Communications Society, ICC 2007.

[6]A.VANI and D. S. Rao, "A Simple Algorithm for Detection and Removal of Wormhole Attacks for Secure Routing in Ad Hoc Wireless Networks", International Journal on Computer Science and Engineering (IJCSE) ISSN : 0975-3397 Vol. 3, No. 6, 2011.

[7] R. Maheshwari, J. Gao and S. R Das, "Detecting Wormhole Attacks in Wireless Networks using Connectivity Information",

[8] L. Hu and D. Evans "Using Directional Antennas to Prevent Wormhole Attacks" , In Network and Distributed System Security Symposium (NDSS 2004), San Diego, California, USA. February 2004.

[9] V. Kumar and A. Kush, "Worm Secure Protocol for Wormhole Protection in AODV Routing Protocol", International Journal of Computer Applications, Vol. 44, No.4, 2012.

[10] K. Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 24, 2008.

[11] Y. Xu, G. Chen, J. Ford and F. Makedon, "Detecting Wormhole Attacks in Wireless Sensor Networks"

[12] W. Ahad and M. Sharma, "Efficient Multipath Algorithm in MANETs to Prevent Wormhole Attack", CT International Journal of Information & Communication Technology, Vol. 1, Issue 1, pp 5-8, 2013.

[13] P. V. Tran, L. X. Hung, Y. K. Lee, S. Lee and H. Lee, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks", IEEE, pp 593-598, 2007.

[14] T. V. Phuong, N. T. Canh, Y.K. Lee, S. Lee, and H. Lee, "Transmission Time-based Mechanism to Detect Wormhole Attacks", IEEE Asia-Pacific Services Computing Conference, IEEE Computer Society, pp 172-178, 2007.

[15] X. Wang and J. Wong, "An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks"

[16] P. Sharma and A. Trivedi, "Prevention of Wormhole Attack in Ad-Hoc Network", Special Issue of International Journal of Computer Applications (0975 – 8887) on Electronics, Information and Communication Engineering - ICEICE No.5, 2011.