International Journal of Scientific and Technical Advancements
ISSN: 2454-1532

A Review on Wormhole Attack in AODV for Mobile Ad-Hoc Networks

Priyanka Sharma[1], Sameru Sharma[2], Harinder Dhingra[3]
[1, 2, 3]Department of Electronics and Communication Engineering Govt.College of Engineering and Technology, Jammu
Email address: [1]priyankasharma1808@gmail.com, [2]sameru33@rediffmail.com, [3]dhingra_h@yahoo.com

***Abstract*—** One of the major issues in Mobile Ad-hoc Network (MANET) is security because of its inherent liabilities. Its infrastructure-less network with dynamic topology pose a number of challenges to security design and makes it vulnerable for different types of security attacks. Under wormhole attack a pair of colluding nodes makes a tunnel using a high speed network. These colluding nodes create an illusion that the two remote nodes of a MANET are directly connected through nodes that appear to be neighbours but are actually distant from one another.

***Keywords*—** MANET, RREQ, RREP.

I. INTRODUCTION

An Ad-Hoc network is an autonomous collection of mobile nodes and wireless communication network used to connect these mobile nodes. This type of network is known as Mobile Ad-Hoc Network (MANET). Each device in a MANET is free to move independently. MANET is an infrastructure less network with no fixed BS for communication. Intermediate mobile nodes act as router to deliver the packets between the two nodes. So, MANET is a highly dynamic network and hence more vulnerable to attack.

Nodes in Ad-hoc networks are computing and communication devices. Applications of Ad-hoc networks include military communication, emergency relief operations, commercial and educational use in remote areas, and in meetings and other situations where the networking is mission oriented and communication based.

II. SECURITY GOALS

Security services include the functionality required to provide a secure networking environment. The main security service can be summarized as follows:

- Authentication: This service verifies user's identity and assures the recipient that the message is from the source that it claims to be from. Firstly, at the time of communication initiation, the service assures that the two parties are authentic, that each entity is what it tells. And next, it must assure that the third party doesn't interfere by impersonating one of the two authentic parties for the purpose of authorized transmission and reception.
- Confidentiality: This service ensures that the data transmitted over the network is not disclosed to unauthorized users. Confidentiality can be achieved by using different encryption techniques.
- Access Control: This limits and controls the access of such a resource which can be an application or a host system.
- Integrity: The function of integrity control is to assure that the data is received in verbatim as sent by authorized user. The data received contains no modification, deletion or insertion.

III. WORMHOLE ATTACK

Wormhole attack is a severe threat against packet routing in sensor networks that is particularly challenging to prevent. In wormhole attack, an adversary receives packets at one location in the network and tunnels them to another location in network, where the packets are resent into the network to consume the bandwidth. The wormhole attack would involve two distant malicious nodes colluding to undertake their distance from each other by relaying the packets along an out-of-band channel which is available only to the attackers. Thus, a false route would be established by the attackers which would shorten the hop distance between any two non-malicious nodes.

Wormhole attacks can also cause Denial-of-service through unauthorized access, Data Traffic, and routing disruptions. The malicious node(s) can add itself in a route and then drop the data packets. Denial of service can prevent the discovery of legitimate routes and unauthorized access could allow access to wireless control systems that are based on physical proximity [1].

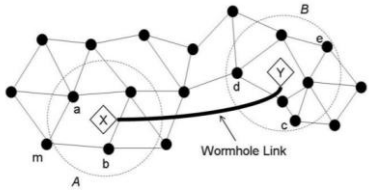

Fig. 1: Wormhole attack [1].

Figure 1.2 shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes A1 and A2 are two colluding attackers and that node S is the target to be attacked. During the attack, when source node S broadcasts an RREQ to find a route to a destination node D, its neighbors J and K for- ward the RREQ as usual. However, node A1, which received the RREQ forwarded by node J, records and tunnels the RREQ to its colluding partner A2. Then, node A2 rebroadcasts this RREQ

Priyanka Sharma, Sameru Sharma, and Harinder Dhingra, "A review on wormhole attack in AODV for mobile ad-hoc networks," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 199-200, 2016.

to its neighbor P. Since this RREQ passed through a high-speed channel, this RREQ will reach node D first. Therefore, node D will choose route D-P-J-S to unicast an RREP to the source node S and ignore the same RREQ that arrived later. As a result, S will select route S-J- P-D that indeed passed through A1 and A2 to send its data [11].

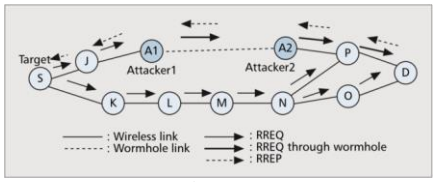

Fig. 2 Example of .wormhole attack [11].

IV. WORMHOLE ATTACK MODES

Wormhole attacks can be achieved using several modes as follows:

- Wormhole with high power transmission: In this mode, when a attacker node gets a RREQ, it broadcasts the RREQ at a high power level towards the destination. By this method, the malicious mode attracts the packets to follow path passing from it.
- Wormhole using encapsulation: When the source node broadcast the RREQ packet, a malicious node which is at one part of the network receives the RREQ packet. Then it tunnels that packet to a second malicious node via legitimate path only, it then rebroadcasts the RREQ. When the neighbors of the second colluding party receive the RREQ, it discards all of them and the result is that the routes between source and the destination go through the two malicious nodes that will be said to have formed a wormhole or the tunnel between them. This prevents the other nodes from discovering any other legitimate path that are more than two hops away.
- Wormhole using out of band channel: This mode for wormhole attack involves the use of an out of band channel. In this mode, an out-of-band high bandwidth channel is placed between two end points to create a wormhole link.
- Wormhole using Packet Relay: In this mode also, one malicious node replays packets between two far nodes and this way fake neighbours are created.

V. TYPES OF WORMHOLE ATTACK

Wormhole attacks are of different types namely, closed wormhole, half open wormhole and open wormhole. Figure 3 shows these different types of wormhole attack.

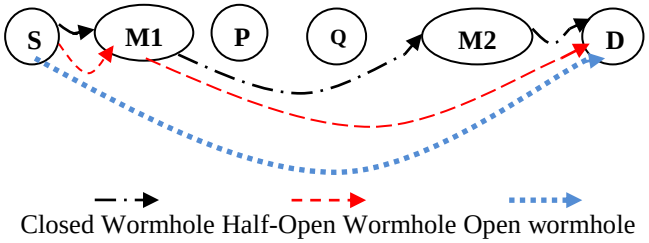

Fig. 3. Types of wormhole attack.

- Open wormhole attack: In the open wormhole attack, the attackers include themselves in the RREQ packet header in the route discovery stage. Other authentic nodes are aware that the two colluding parties lie on the path but they would think that they are direct neighbors.
- Half open wormhole attack: One side of the wormhole does not modify the packet and only another side modifies the packet, following the route discovery procedure. This leads to the path S-M 1-D for the packets sent by S for D.
- Closed wormhole attack: The attackers do not modify the content of the packet in a route discovery. Instead they simply tunnel the packet from one side of the wormhole to another side and it rebroadcasts the packet.

VI. CONCLUSION

In this paper a brief introduction of wormhole attack and its effect on MANET is discussed. Wireless ad hoc networks are vulnerable to various attacks due to the physical characteristic of both the environment and the nodes. A wormhole attack is such an attack, that is, it is executed by two malicious nodes causing serious damage to networks and nodes, relaying the packets along an out-of-band channel which is available only to the attackers. Thus, a false route would be established by the attackers which would shorten the hop distance between any two non-malicious nodes.

REFERENCES

[1] Pravin Khandare, Prof. N. P. Kulkarni, "Public Key Encryption and 2Ack Based Approach to Defend Wormhole Attack", *International Journal of Computer Trends and Technology*, volume4, Issue3- 2013.

[2] Anil Kumar Fatehpuria, Sandeep Raghuwanshi, "An Efficient Wormhole Prevention in MANET Through Digital Signature", *International Journal of Emerging Technology and Advanced Engineering*, Volume 3, Issue 3, 2013.

[3] L. Sudha Rani, R.Raja Sekhar (Ph.D), "Detection and prevention of wormhole attack in stateless multicasting", *International Journal of Scientific & Engineering Research*, Volume 3, Issue 3, March -2012.

[4] P. Niranjan, P. Srivastava, R. kumar Soni, R. Pratap, " Detection of wormhole attack using hop-count and time delay analysis", International *Journal of Scientific and Research Publications*, Volume 2, Issue 4, April 2012.

[5] P. Sharma, Prof. A. Trivedi, "An approach to defend against wormhole attack in adhoc network using digital signature", *IEEE* 2011.

[6] S. Gupta, S. Kar, S. Dharmaraja, "WHOP: Wormhole attack detection protocol using hound packet", *International Conference on Innovations in Information Technology*, 2011.

[7] Mariannne. A. Azer, "Wormhole attacks mitigation", *Sixth International Confernece on Availability, Reliability and Security*, 2011.

[8] R. H. Jhaveri, A. D. Patel, J. D. Parmar, B. I. Shah, " MANET routing protocols and wormhole attack against AODV", *IJCSNS International Journal of Computer Sciences and Network Security*, vol. 4, April 2010.

[9] M. Khabbazian, H. Mercier, and V. K. Bhargava, "Severity analysis and countermeasure for the wormhole attack in wireless adhoc networks", *IEEE Transaction on Wireless Communications*, vol. 8 (2), 2009.

[10] V. Mahajan, M. Natu, A. Sethi, "Analysis of wormhole intrusion attack in MANETs", *IEEE*, 2008.

[11] B. Kannhavong, H. Nakayama, Y. Nemoto, and N. Kato, "A survey of routing attacks in mobile ad hoc networks", *IEEE Wireless Communications*, 1536-1284/07/$20.00, pp. 85-91, October 2007.

[12] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L. W. Chang, "Preventing wormhole attack on wireless adhoc networks: A graph theoretic approach", *IEEE Communications Society IEEE*, 2005.

Priyanka Sharma, Sameru Sharma, and Harinder Dhingra, "A review on wormhole attack in AODV for mobile ad-hoc networks," *International Journal of Scientific and Technical Advancements*, Volume 2, Issue 4, pp. 199-200, 2016.