Defending Wormhole Attack in Wireless Ad-hoc Network

Nisha S.Raote

Student M.E. IV Semester [Wireless Communication & Computing]
n.raote@yahoomail.com,

Department of Computer Science & Engineering, G.H.Raisoni College of Engineering, Nagpur, India

ABSTRACT

The ad-hoc networks are the temporarily established wireless networks which does not require fixed infrastructure it is also called as infrastructure less network. Because of some flaws of adhoc network such as shared wireless medium and lack of any central coordination makes them more prone to attacks in comparison with the wired network. Among all the attacks wormhole attack is the most severe attack. In this attack an attacker capture the packets at one location in the network and send it two another attacker at a distant location through tunnels which is established through different ways like packet encapsulation, using high power transmission or by using direct antennas. This tunnel between two colluding attackers is virtual and it is called as a wormhole. The wormhole attack is possible even if the attacker has not comprised any hosts, and all communication provides authenticity and confidentiality. By using the various approaches for finding the solution over wormhole attack, the dynamic information of the packets could still be modified. So in order to give more robust protection in some special scenario like battlefields, which requires highly secured information, there is need of developing some secured mechanism for wormhole detection and prevention. Taking into consideration this problem the proposed scheme is developed. This paper discusses proposed works on wormhole attack along with its available counter measures in ad-hoc wireless network.

KEYWORDS

Ad Hoc Networks, comprised nodes, attacks, Wormhole attack, Wormhole attack modes.

1. INTRODUCTION

Ad-hoc wireless networks are an excellent choice for emergency operations, short-live networks and vehicular communication. The major security challenges in the adhoc wireless networks are the lack of a central control and the fact that each node has to forward the packets of other nodes. In order to avoid this, the adhoc network must deal with threats from external agents and comprised internal nodes (A node that perform internal attacks are comprised node, it can act as an informer by deliberate disclosure of confidential information to unauthorized nodes.).

The adhoc network has the features of shared broadcast radio channel, insecure operating environment, absence of infrastructure, lack of central authority, lack of association, limited resource availability dynamically changing network topology, resource constrains and lack of clear line of defence, make them vulnerable to a wide range of security attacks. There are two types of attacks namely, passive and active attack. In passive attack the adversary snoop the data exchanged in the network without altering it whereas the active attack tries to alter or destroy the data being exchanged in the network. These attacks could involve eavesdropping, message tampering, or identity spoofing. For an attacker to be able to launch damaging data attacks, one option is to have a large number of powerful adversary nodes distributed over the network and possessing cryptographic keys. It is possible for an attacker to achieve this attack by targeting specific control traffic in the network. Some examples of control traffic are topology discovery, distributed location determination, routing and monitoring liveness of a node. A particularly severe control attack on the routing functionality of wireless networks, called the *wormhole attack* [1] [2] [3], has been introduced in the context of ad hoc networks. In wormhole attack

DOI : 10.5121/ijcses.2011.2311

malicious node captures packets from one location in the network, and “tunnels” them to another malicious node at a far. The tunnel is established through different ways like packet encapsulation, using high power transmission or by using direct antennas it makes the tunnelled packet arrive either earlier or with number of hops lesser compared to the packets transmitted over normal multihop routes. This creates the illusion that these two nodes provide the shortest path through them. A wormhole tunnel can actually be useful if used for forwarding all the packets, it puts the attacker in powerful position compared to other nodes in the network, which the attacker could use in a manner that could compromise the security of the network.

In wormhole attack the two remote regions are directly connected through nodes (malicious) that appear to be neighbours but are actually distant from one another as shown in the figure1. Such wormhole attack results in the false route. So the wormhole attack is one of the most severe threats to ad-hoc networks, as it can do harm to both sender and receiver by performing packet dropping or alteration.

This paper is organized as follows. Section 2 lists the wormhole attack modes in section 3, we discuss the solutions that have been proposed in the literature as a countermeasure for this attack. Finally in section 4 proposed approach for mitigating wormhole and conclusion.

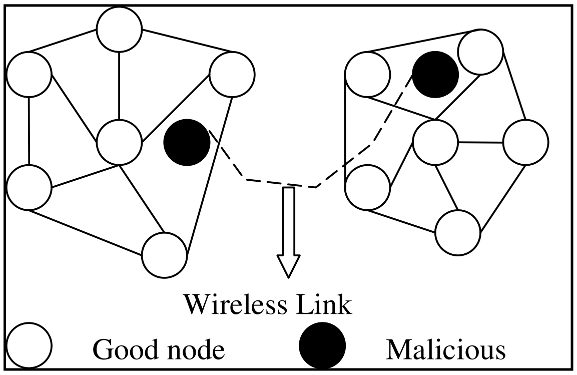

Figure 1 wormhole attack

2. WORMHOLE ATTACK

In this section mentions the wormhole attack modes [6], [13] which are classified based on the techniques used for launching the wormhole attack.

A. Wormhole Attack Modes

Wormhole attacks can be launched using several modes, among these modes, we mention the following:

- Wormhole using Encapsulation.
- Wormhole using Out-of-Band Channel.
- Wormhole with High Power Transmission.
- Wormhole using Packet Relay.
- Wormhole using Protocol Deviations.

B. Wormhole Attack Threats

We can consider wormhole attack as a two phase process [16][17]launched by one or several malicious nodes. The various threats cause by the wormhole attack are selective dropping or modification of data packets, switching off the wormhole link periodically in order to generate unnecessary routing activities, they also tries to disrupt the data flow. It is also possible for the attacker to simply record the traffic for later analysis.

3. RELATED WORK

This section summarizes the related works in the literature for wormhole attack detection & prevention as shown in the table 1 below.

Sr. No.	Wormhole recovery methods		
	Method	Requirement	Commentary
1	Packet leashes, geographical	GPS coordinates of Every node; Loosely synchronizedclocks (ms)	Robust, straightforward solution; inherits general limitations of GPS technology
2	Packet leashes, temporal	Tightly synchronized clocks (ns)	**Impractical**; required time synchronization level not currently achievable in to sensor networks
3	Packet leashes, end-to-end	GPS coordinates; Loosely synchronized clocks (ms)	Inherits limitations of GPS technology
4	Time of flight	Hardware enabling one-bit message and immediate replies without CPU involvement	**Impractical**; likely to require MAC-layer modifications
5	Directional Antennas	Directional antennas on all nodes or several nodes with both GPS and directional antennas	Good solutions for networks relying on directional antennas, but not directly applicable to other networks
6	Network visualization Not readily applicable to mobile networks.	Centralized controller	Seems promising; Works best on dense networks; Mobility not studied; Varied terrains not studied
7	Localization	Location-aware 'guard' Nodes	Good solution for sensor networks
8	LiteWorp	none	Applicable only to static stationary networks; **Impractical**
9	Statistical analysis	no requirements	Works only with multi-path on demand protocols;

10.	MGM	Light weight local monitoring	For necessary condition, the heavy weight RV protocol is triggered. it is more resource efficient and powerful

Table 1.Summary of various defences mechanisms for Wormhole attack

4. PROPOSED APPROACH

In order to give more robust protection in some special scenario like battlefields, where highly secured information is required there is a need of developing some secured mechanism for wormhole detection and prevention. So our aim is to build a robust and secure mechanism for preventing the devastating effects caused by the wormhole attack. The main objectives of this approach are as follows

- To prevent eavesdropping
- To avoid packet modification
- To provide authentication & confidentiality.
- To reduce the packet overhead.
- To minimize computation

This Scheme consists of four parts:

- Route Discovery
- Detection of Malicious Nodes
- Secure data transmission
- Route maintenance

In [4] the author makes use of hop count analysis that method first examine the hop count values of all the routes for data transmission .Finally we randomly transmit packets through safe routes. By using this approach the rate of using the route path through the wormhole can be minimized. In the proposed approach we are using this hop count analysis also we are using cryptographic approach for providing secured data transmission. In this approach we are using AODV routing protocol.

The AODV defines three types of messages such as Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) .These messages are processed as shown in the flow chart below;

This method uses the smart agent which is attached with all the authorized nodes and the nodes start communication after verifying the necessary details contain by the smart agent .The smart agent contains the cryptic data for checking the authenticity of the node. This method uses the RSA algorithm for providing secure communication. The packet is divided into n number of parts and these parts are encrypted using RSA and is decrypted at the receiver side.

5. CONCLUSION

In this paper, we proposed a solution that treats Wormhole attack problem by using cryptographic approach i.e. RSA and Multipath Routing concept. Our proposal will improve data security robustly .This approach in wireless Ad hoc Networks, increasing the transmission speed in security environment. Because, dividing the initial message and exploiting the characteristic of existence of multiple paths between nodes in an Ad hoc network and also increase the robustness of confidentiality.

REFERENCES

[1] Mariane A. Azer,Sherif M. El-Kassas, “An Innovative Approach for the Wormhole Attack Detection and Prevention in Wireless Ad-hoc Network”2010.

[2] Matthew Tan Creti,Matthew Beaman,Saurabh Bagchi,Zhiyuan Li,Yung-Hsiang Lu, “Multigrade Security Monitoring for Ad-hoc Wireless Networks” ,2009IEEE.

[3] Bhargava, B.de Oliveira, R. Yu Zhang Idika, “Addressing Collaborative Attacks and Defense in Ad Hoc Wireless Networks” 29th IEEE International Conference on Distributed Computing Systems, 2009

[4] Shang-Ming Jen, Chi-sung Laith & Wen-Chung Kuo, “A Hop Count scheme for avoiding wormhole attack in MANET,” Journal on Open access sensors, 2009.

[5] Khabbazian, M.;Mercier,H.;Bhargava, V.K. Severity Analysis and countermeasures for the Wormhole Attack in Wireless Ad Hoc Networks. IEEE Trans. Wireless Commun.2009, 8,736-745.

[6] Marianne Azer, Sherif Ei-Kassas Magdy El-Soudani, “A Full image of the Wormhole Attack towards introducing Complex wormhole attacks in wireless Ad-hoc networks”, in (IJCSIS) International Journal of Computer Science and Information Security, Vol. 1, No. 1, May 2009.

[7] F.Nait-Abdesselam,B.Bensaou,and T. Taleb, “Detecting and avoiding Wormhole attacks in Wireless Ad-hoc Networks”, in IEEE Communication Magazine.vol.46,April 2008,pp.127-133.

[8] G. Lee, D. k. Kim, J. Seo, “An Approach to Mitigate Wormhole Attack in Wireless Ad Hoc Networks*,”* IEEE International Conference on Information Security and Assurance, pp. 220-225, 2008.

[9] Naït-Abdesselam, F.; Bensaou, B.; Yoo, J. Detecting and Avoiding Wormhole Attacks in Optimized Link State Routing Protocol. In *IEEE WCNC*, Hong Kong, 2007; pp. 3119–3124.

[10] Ren, K.; Lou, W.; Zeng, K.,Moran, P.J. On Broadcast Authentication in Wireless Sensor Networks. *IEEE Trans. Wireless Commun*. 2007, *6*, 11–23

[11] Lazos, L.; Poovendran, R.; Meadows, C.; Syverson, P.; Chang, L.W. Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach. In *IEEE WCNC 2005*,

[12] Maheshwari, R.; Gao, J.; Das, S.R. Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information. In *IEEE INFOCOM*, Anchorage, AK, USA, 2007; pp. 107–115.

[13] Lazos, L.; Poovendran, R. SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks. In *ACM WiSE’04*, New York, NY, USA, October 2004; pp. 73–100.

[14] Khabbazian, M.; Mercier, H.; Bhargava, V.K. Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks. *IEEE Trans. Wireless Commun.* **2009**, *8*, 736-745.

[15] Perrig, A.; Canetti, R.; Tygar, D.; Song, D. Efficient Authentication and Signature of Multicast Streams over Lossy Channels. In *Proc. IEEE Symp. Res. Security and Privacy*, Oakland, CA, USA, May 2000; pp. 56–73.

[16] Khalil, I.; Bagchi, S.; Shroff, N.B. LITEWORP: A Lightweight Countermeasure for the Wormhole Attack sin Multihop Wireless Networks. In *IEEE DSN’05*, Yokohama, Japan, June 28-July 1, 2005; pp. 1–10.

[17] Qian. L.; Song, N.; Li, X. Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path. In *IEEE WCNC 2005*, New Orleans, LA, USA, March 13-17, pp. 2106–2111,2005.

[18] Lazos,L.;Poovendran,R.SeRLo;Secure Range-independent Localization for wireless Sensor Networks.In ACM WiSE'04,New York,NY,USA,October2004;pp.73-100.Lee, S.hyun. & Kim Mi Na, (2008) "This is my paper", ABC *Transactions on ECE*, Vol. 10, No. 5, pp120-122.

Authors

Biography

Ms. N.S.Raote is pursuing IV Semester M.E. in Wireless Communication and Computing from G.H.Raisoni College of Engineering, Nagpur, India, under R.T.M. Nagpur University. She is B.E.(I.T.) from K.D.K. College of Engineering ,Nagpur, India. Her areas of interest are, security in ad-hoc wireless network, and signal processing.