A Novel Paradigm: Detection & Prevention of Wormhole Attack in Mobile Ad Hoc Networks

Shilpa Jaiswal[#1], Sumeet Agrawal[*2],

[#] *Research Scholar, M.Tech, dept. of computer science & engineering AITR Indore, Rgpv Bhopal, India*

[*]*Research Scholar, M.Tech, dept. of electronics & Communication, AITR Indore, Rgpv Bhopal, India*

***Abstract*-This paper emphasized to propose and develop a scheme for the prevention of wormhole attack from intermediate and surrounding threads.**

In wireless ad hoc networks, it is difficult to detect wormhole attacks because malicious nodes impersonate legitimate nodes. Various issues including security, legitimacy and node concurrency still persist in mobile ad hoc networks among these, security being one of the major concerns. The wormhole attack is among the most threatening and dangerous attacks on these types of networks. During the attack a malicious node captures packets from one location in the network, and tunnels them to another distant malicious node, which replays them locally.

***Keywords*- wormhole, impersonation, legitimacy, security, concurrency.**

I. Introduction

Wireless ad-hoc network is promising to solve many challenging real-world problems, for example, communication in emergency response system, military field operation and oil drilling and mining Operation. The proliferation of wireless devices also stimulates the emergent Applications in wireless ad hoc network. However, the realization and wide deployment of such network faces many challenges. Security is one of the most challenging problems as the operation environment of such network is usually unpredictable and the existing mechanisms such as routing protocols assume a trusted environment. Hence any malicious behavior could disrupt the normal operation of the networks.

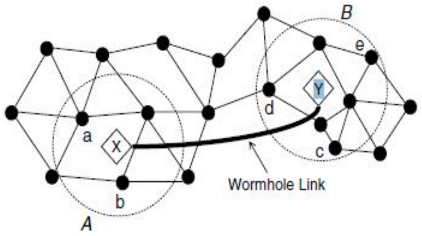

Figure1: Wormhole Attack Demonstration

Figure 1: A wormhole attack. X and Y denote the wormhole nodes connected through a long wormhole link. As a result of this attack, nodes in Area A consider nodes in Area B their neighbors and vice versa.

Wormhole attack [1][2][3][4] is a severe attack in wireless ad hoc network in which the adversary builds a tunnel between two end points which are usually multi-hops away. This tunnel between two malicious nodes is called wormhole. The message recorded at one end point is relayed to the other end and re-broadcasted into the network. The wormhole attack is particularly challenging to detect in that it can be mounted without compromising any nodes. Furthermore, the attackers Can mount the attack without revealing their identities. Earlier countermeasures to the wormhole attack have relied on specialized hardware which may not be feasible in wireless ad hoc network scenario. Moreover, most of the protocols prevent the wormhole attack by securing each link and no method has been proposed to identify the locations of the two end points of the wormhole.

II. SIGNIFICANCE OF WORMHOLE ATTACK

While wormhole could be a useful networking service as this simply presents a long network link to the link layer and up, the attacker may use this link to its advantage. After the attacker attracts a lot of data traffic through the wormhole, it can disrupt the data flow by selectively dropping or modifying data packets, generating unnecessary routing activities by turning off the wormhole link periodically, etc. The attacker can also simply record the traffic for later analysis. Using wormholes an attacker can also break any protocol that directly or indirectly relies on geographic proximity. For example, target tracking applications in sensor networks can be easily confused in the presence of wormholes. Similarly, wormholes will affect connectivity-based localization algorithms, as two neighboring nodes are localized nearby and the wormhole links essentially 'fold' the entire network. This can have a major impact as location is a useful service in many protocols and application, and often out-of-band location systems such as GPS are considered expensive or unusable because of the environment.

III. LITATURE SURVEY

With the rapid development in wireless technology, ad hoc networks have emerged in many forms. These networks operate in the license free frequency band and do not require any investment in infrastructure, making them attractive for military and selected commercial applications. The set of applications for ad hoc networks is diverse, ranging from small, static, to large-scale, mobile, highly dynamic networks. However, a vital problem concerning their security must be solved in order to make use of these applications. One of the most famous attacks on this type of networks is the wormhole attack. Wormhole attack can be schematized in two phase process launched by one or several malicious nodes. In the first phase, these malicious nodes, called wormhole nodes, try to lure legitimate nodes to send data to other nodes via them. In the second phase, wormhole nodes could exploit the data in variety of ways. The end to end detection of wormhole attacks have the glory of detection and suggest prevention of wormhole attacks in mobile ad hoc networks. The set of mechanisms in defending against wormhole attack is location-based end to end wormhole attack detection. The source node estimates the minimum hop count to the destination based on the geographic information of the two end hosts in which the receiver's location is piggy-backed (first come first served) by the route reply packet during the route discovery. For a received route, the source compares the hop count value received from the reply packet with its estimated value. If the received value is less than the estimation, the corresponding route is marked as if a wormhole is detected. Then, the source launches wormhole TRACING in which the two end points of the wormhole will be identified in a small area provided that there are multi-paths exist between the source and destination. Finally, a normal route is selected for the data communication. In extension to this following aspects [5] can be considered: (a): A hidden wormhole attack and exposed wormhole attack; (b): an end-to-end detection of hidden wormhole attack with geographic information at each node; and (c): to identify the location of the two end points of a hidden wormhole attack.

IV. RELATED WORK

In this chapter, we discuss some methods for exposed wormhole attack, hidden attack and many more methods for detecting & prevention f wormhole attack.

Exposed wormhole attack: Exposed wormhole attack is called byzantine attack [6] in which the two end points are two compromised hosts. Then the adversary builds a virtual tunnel between the two compromised nodes. To defend against exposed wormhole attacks, several secure routing protocols have been proposed Secure Routing Protocol [7], SEAD [8], and ARIADNE [9].

Survey of various secure routing protocols schematized the key ingredients for the purpose of studying attacks in mobile ad hoc networks [10]. In addition, some methods are dedicated to detecting exposed wormhole attacks. In [4], a multi-dimensional scaling visualization method is applied to visualize the anomaly introduced by the wormhole. A central controller uses the Dijkstra algorithm [11] to reconstruct the topology of the network. The wormhole can be located by detecting the bending features on the rebuilt network topology. A. Pirzada et. al. [12] derived a trust-based wormhole detection and evasion.

Hidden wormhole attack: To protect the network from hidden wormhole attack, a few methods have been studied which include packet leashes [15], SECTOR [16], and directional antennas methods which is described below in this chapter.

Hue et. al. [15] proposed to defend against wormhole attacks using packet leash which is to restrict a packet's maximum allowed transmission distance. Two packet leashes can be used: geographical leash or temporal leash depending on whether the distance or time is used to bound the transmission. Both methods require authentication of received packets. Geographical leash requires a loosely synchronized clocks and temporal leash demands a tightly synchronized clocks.

SECTOR (Secure Tracking Of node encounters) [16] prevents wormhole attack by bounding the maximum distance between two neighbor nodes through a series of fast one-bit exchange. These mechanisms use a special hardware to ensure accurate time measurement and fast processing between the sender and receiver.

Some another method for detecting & prevention of wormhole attack is explained in this paper.

LITEWORP [17] detects wormhole attack based on local traffic monitoring at some selected nodes. This detection method may introduce other attacks such as blackmail attack through impersonation [6].

Dynamic Source Routing [13] based upon their sincerity in execution of the routing protocol. This method is based on the observation that tunneling through a wormhole requires encapsulation that the end points of a wormhole has to change This method requires the wireless card can work promiscuous mode and sending mode back and forth. Intrusion detection or tamper-proof hardware has also addressed the issue of compromised nodes.

A TRUELINKS [6] scheme prevents wormhole attack using link verification at MAC layer between two neighbors. The protocol adapts MAC frames in 802.11 to verify and authenticate neighbors.

V. PROPOSED WORK

To overcome these loopholes the focus of work is to analyze and simulate all possibilities of wormhole attacks behaviors in respect of recent scenario that further needs to design an algorithm and protocol architecture for wormhole attack prevention. The objective of selecting this work is to have very vast opportunities to detect and prevent a wormhole attack and to predict all possible simulations. So, a Secure Protocol for indentifying an end to end connection among various nodes of ad hoc networks is to be proposed to eliminate possible hazards. The occurrence of misbehavior is so rapid and our protocol suggests a new hierarchy of wormhole attack prevention scheme.

VI. SCOPE OF WORK

The scope of this work is intended to reduce the possibilities of wormhole attacks in an ad hoc network. The protocol may assist to design new paradigm for secure routing protocols in better and faster way. The proposed work after simulations may give various results to actuate the problem of wormhole attacks and clear cut analysis of its occurrence and to motivate the existing protocols to update.

VII. CONCLUSION

In this work the technique of end to end detection of wormhole attacks emphasized. This proposal may change the revolutionary direction in secure routing protocols in wireless and cellular ad hoc networks. This challenging opportunity of studying and simulating wormhole attacks may give relevant outcomes and this simulation based on the wormhole detection and identification of the source node that may select a shortest route from a set of legitimate routes. This may eliminate the possibilities of wormhole and their occurrence in MANET.

REFERENCES

[1] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. In Proceedings of the Second Annual Conference of the IEEE Computer and Communication and Societies

[2] S. Capkun, L. Buttyan, and J. Hubaux. 'SECTOR: Secure tracking of node encounters in multi-hop wireless networks'. In the Proceedings of ACM Workshop on Security (Ad Hoc and Sensor Networks

[3] L. Hu and D. Evans 'Using directional antennas to prevent wormhole attacks' In Proceedings of the Network and Distributed Security Symposium (NIX'S).

[4] W. Wang and B. Bhargava, Visualization of wormholes in sensor networks. In Proceeding of the ACM Workshop on Wireless Security (WISE).

[5] Xia Wang, Johnny Wong, An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks, 31st Annual International Computer Software and Applications Conference

[6] J. Eriksson, S. Krishnamurthy, and M. Faloutsos. TRUELINK: A practical countermeasure to the wormhole attack. In The 14th IEEE International Conference on Network Protocols (ICNP)

[7] P. Papadimitratos and Z. Haas. Secure routing for mobile ad hoc networks. In SCS Communication Networks and Distributed Systems Modeling and Simulation Conference

[8] Y. Hu, D. Johnson, and A. Perrig. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. In IEEE Workshop on Mobile Computing Systems and Applications.

[9] Y. Hu, A. Perrig, and D. Johnson. ARIADNE: A secure on demand routing protocol for ad hoc networks. In ACM MobiCom 2008

[10] Y.-C. Hu and A. Perrig. A survey of secure wireless ad hoc routing. In IEEE Security and Privacy, Special issue on Making Wireless Work, May 2004

[11] E. W. dijkstra. A case study on two problems in connection with graph, Numerical Mathematics

[12] A. A. Pirzada and C. McDonald. Detecting and evading wormholes in mobile ad-hoc wireless networks. International Journal of Network Security,

[13] J. Broch, D. Johnson, and D. Maltz. The dynamic source routing protocol for mobile ad hoc networks, Dec. 1998

[14] L. Qian, N. Song, and X. Li., Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path routes. Wireless Communications and Networking Conference, Mar. 2005.

[15] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. In Proceedings of the llvenly-Second Annual .loin1 Conference of the IEEE Computer and Communication Societies, April 2007

[16] S. Capkun, L. Buttyan, and J. Hubaux. SECTOR: Secure tracking of node encounters in multi-hop wireless networks. In Proceedings of the ACM Workshop on Security in Ad Hoc and Sensor Networks.

[17] I. Khalil, S. Bagchi, and N. B. Shroff. LITEWORP: A lightweight countermeasure for the wormhole attack in multi hop wireless networks