International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.1, Jan-Feb 2012 pp-230-234 ISSN: 2249-6645

Securing Layer-3 Wormhole Attacks in Ad-Hoc Networks

T. Krishna Rao[1]
[1]PG Scholar,
Department of IT,
Aurora Engineering College,
Bhongir, Nalgonda Dist,
Andhra Pradesh, India

Mayank Sharma[2]
[2]Associate Professor
Department of IT
Aurora Engineering College
Bhongir ,Nalgonda Dist,
Andhra Pradesh , India

Dr. M. V. Vijaya Saradhi[3]
[3]Professor, Head of the Department
Department of IT
Aurora Engineering College
Bhongir, Nalgonda Dist,
Andhra Pradesh,India

Abstract - In ad hoc networks, malicious nodes can carry wormhole attacks to fabricate a false scenario on neighbour relations among mobile nodes. The attacks threaten the safety of ad hoc routing protocols and some security enhancements. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. In this paper, we present a new approach for detecting wormhole attacks. The Witness Integration Multipath protocol is based on the Multipath DSR routing protocol and finds suspicious behavior related to wormhole attacks.

Keywords: - MANET, source routing, multipath, wormhole attacks

I. INTRODUCTION

Ad-hoc networks must deal with threats from external agents and compromised internal nodes. The lack of a central control and the fact that each node must forward packets of other nodes represent major security challenges. In such environments, it is difficult to assure the confidentiality and the integrity of the communications as well as the availability of the services. Mobile ad-hoc networks [1]have been an attractive field of research for many years now. Due to their characteristics, these networks are an excellent choice for emergency operations, vehicular communication and short-live networks.

In the Wormhole attack, an attacker records a packet or individual bits from a packet, at one location in the network, tunnels the packet (possibly selectively) to another location, and replays it there. It is simple for the attacker to make the tunnelled packet arrive with better metric than a normal multihop route. This can be done for tunnelled distances longer than the normal wireless transmission range of a single hop. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to it, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole.

The paper is organized as follows. Section 2 presents an Overview of Wormhole Attacks. Section 3 discusses the related works. Section 4 presents the approach. Section 5 gives an overview of implementation and results and Section 6 presents the conclusions.

II. OVERVIEW OF WORMHOLE ATTACKS

In a *wormhole attack*, an attacker receives packets at one point in the network, "tunnels" them to another point in the network, and then replays them into the network from that point. For tunnelled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunnelled packet arrive with better metric than a normal multihop route, for example through use of a single long-range directional wireless link or through a direct wired link to a colluding attacker. It is also possible for the attacker to forward each bit over the wormhole directly, without waiting for an entire packet to be received before beginning to tunnel the bits of the packet, in order to minimize delay introduced by the wormhole. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to it, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole[2].

If the attacker performs this tunnelling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. However, the wormhole puts the attacker in a very powerful position relative to other nodes in the network, and the attacker could exploit this position in a variety of ways. The attack can also still be performed even if the network communication provides confidentiality and authenticity, and even if the attacker has no cryptographic keys. Furthermore, the attacker is invisible at higher layers; unlike a malicious node in a routing protocol, which can often easily be named, the presence of the wormhole and the two colluding attackers at either endpoint of the wormhole are not visible in the route.

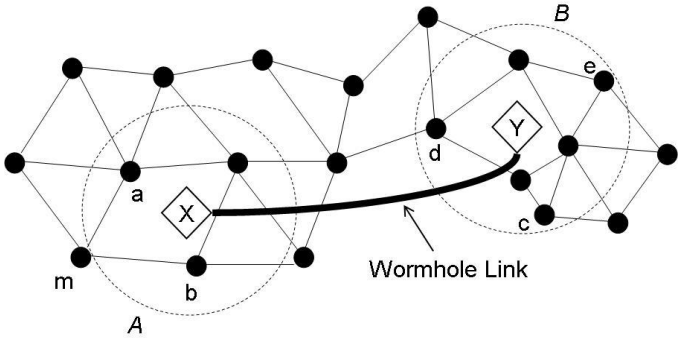

Figure 1: Wormhole Attack

An example of Wormhole attack is shown in the figure 1. Here X and Y are the two end-points of the wormhole link (called as wormholes)[4]. X replays in its neighborhood (in area A) everything that Y hears in its own neighborhood (area B) and vice versa. The net effect of such an attack is that all the nodes in area A assume that nodes in area B are their neighbors and vice versa. This, as a result, affects routing and other connectivity based protocols in the network. Once the new routes are established and the traffic in the network starts using the X-Y shortcut, the wormhole nodes can start dropping packets and cause network disruption. They can also spy on the packets going through and use the large amount of collected information to break any network security. The wormhole attack will also affect connectivity-based localization algorithms and protocols based on localization, like geographic routing, will find many inconsistencies resulting in further network disruption.

The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of (and thus a neighbour of) that node. For example, when used against an on-demand routing protocol such as DSR [16], [17] or AODV [27], a powerful application of the wormhole attack can be mounted by tunnelling each ROUTE REQUEST packet directly to the destination target node of the REQUEST. When the destination node's neighbours hear this REQUEST packet, they will follow normal routing protocol processing to rebroadcast that copy of the REQUEST and then discard without processing all other received ROUTE REQUEST packets originating from this same Route Discovery. This attack thus prevents any routes other than through the wormhole from being discovered, and if the attacker is near the initiator of the Route Discovery, this attack can even prevent routes more than two hops long from being discovered. Possible ways for the attacker to then exploit the wormhole include discarding rather than forwarding all data packets, thereby creating a permanent Denial-of-Service attack (no other route to the destination can be discovered as long as the attacker maintains the wormhole for ROUTE REQUEST packets), or selectively discarding or modifying certain data packets.

The neighbour discovery mechanisms of periodic (proactive) routing protocols such as DSDV [26], OLSR [33], and TBRPF [5] rely heavily on the reception of broadcast packets as a means for neighbour detection, and are also extremely vulnerable to this attack. For example, OLSR and TBRPF use HELLO packets for neighbour detection, so if an attacker tunnels through a wormhole to a colluding attacker near node B all HELLO packets transmitted by node A, and likewise tunnels back to the first attacker all HELLO packets transmitted by B, then A and B will believe that they are neighbours, which would cause the routing protocol to fail to find routes when they are not actually neighbours. For DSDV[3], if each routing advertisement sent by node A or node B were tunnelled through a wormhole between colluding attackers near these nodes, as described above, then A and B would believe that they were neighbours. If A and B, however, were not within wireless transmission range of each other, they would be unable to communicate. Furthermore, if the best existing route from A to B were at least 2n + 2 hops long, then any node within n hops of A would be unable to communicate with B, and any node within n hops of B would be unable to communicate with A. Otherwise, suppose C were within n hops of A, but had a valid route to B. Since A advertises a metric of 1 route to B, C would hear a metric n+1 route to B. C will use that route if it is not within n+1 hops of B, in which case there would be an n-hop route from A to C, and a route of length n+1 from C to B, contradicting the premise that the best real route from A to B is at least 2n + 2 hops long.

In each of these protocols, the wormhole can be used to attract ad hoc network traffic, and can use this position to eavesdrop on traffic, maliciously drop packets, or to perform man-in-the-middle attacks against protocols used in the network. The wormhole attack is also dangerous in other types of wireless networks and applications. One example is any wireless access control system that is based on physical proximity, such as wireless car keys, or proximity and token based access control systems for PCs [8], [20]. In such systems, an attacker could relay the authentication exchanges to gain unauthorized access.

III. RELATED WORKS

Due to the characteristics of the wormhole attacks, cryptographic solutions are not sufficient. Numerous physical approaches have been proposed to secure the neighbor discovery process. Most of the solutions presented so far require that the nodes handle information about self-location, perform clocks synchronization or rely on specialized antennas or on information such as trust relationship. Only few solutions have been proposed to secure the overall end-to-end route discovery process. Other approach contains timing and/or position information to packets. This restricts the maximum transmission distance permitted to a packet. They propose two kinds: geographical and temporal. To use geographical approach, each node must know its own location and all nodes must have loosely synchronized clocks. To use temporal approach, all nodes must have tightly synchronized clocks. Thus, if a receiving node determines that the neighbor discovery signal of a given node has traveled too far, the node should discard it. Another approach is to estimate the distance separating two nodes from the round-trip travel time taken by a message and its acknowledgement. This mechanism relies on a specialized hardware allowing the destination to send a response to a one bit challenge message as fast as possible.

Several approaches have been developed to prevent or to detect wormhole attacks. The first three solutions address mainly the closed wormhole attacks. They present how to protect the neighbour discovery process. Hu *et al.* [15] propose the addition of *leashes* containing timing and/or position information to packets. A leash restricts the maximum transmission distance permitted to a packet. They propose two kinds of leashes: geographical and temporal. To use geographical leashes, each node must know its own location (e.g. GPS) and all nodes must have loosely synchronized clocks. To use temporal leashes, all nodes must have tightly synchronized clocks. Thus, if a receiving node determines that the neighbour discovery beacon of a given node has travelled too far, the node should discard it.

C˘ apkun *et al.* [16] estimates the distance separating two nodes from the round-trip travel time taken by a message and its acknowledgement. This mechanism relies on a specialized hardware allowing the destination to send a response to a one bit challenge message as fast as possible. Hu and Evans [17] use directional antennas to detect wormhole attacks. If a node uses a specific sector to communicate with a neighbour, this neighbour should use its opposite sector. The existence of a wormhole would introduce inconsistencies in the network that could be detected by the other nodes simply by adding some sector information to the packets. The next solutions address the open wormhole attacks. They present how to prevent or detect malicious actions from compromised internal agents. Pirzada and McDonald [18] derive a trust relationship for neighbour nodes based upon their compliance to a routing protocol (DSR). The nodes' trust levels are then used to avoid communication through potential wormholes.

Khalil *et al.* [18] propose that the nodes in a static network obtain in a secure way the one-hop and two-hop topological information from their neighbours. Then, each node observes the behaviour of their neighbours searching for typical patterns related to wormhole attacks. The same authors also propose to support nodes mobility by adding a trusted central authority in charge of authorizing nodes to move and to create new neighbour associations [20]. Wang *et al.* [14] extend the geographical leashes and use them in an end-to-end verification process. This process determines whether all the supposedly neighbour pairs of a path are not too far apart. Finally, Qian *et al.* [21] present a different approach to detect wormhole attacks. The solution is based on statistical analysis of the information gathered during the multipath routing process (SMR). A link generating a wormhole attack should be used by the routing protocol with an unusually high frequency. Unfortunately, only uniform grid networks have been considered.

IV. APPROACH

The Dynamic Source Routing (DSR) protocol [22] is an on demand source routing protocol for mobile ad-hoc networks. When a source needs a path towards a destination, it broadcasts *Route Request* (RREQ) messages. As these messages are forwarded, they gather the intermediate nodes they go through. Then, the destination replies with unicast *Route Reply* (RREP) messages to the source. The source chooses its path based on the received RREP messages. To avoid too many RREQ packets in the network, the protocol uses two mechanisms: local cache and selective broadcasting for intermediate nodes. An intermediate node can respond if it has a valid path in its cache. Otherwise, it forwards the request message if it is a new one.

The DSR protocol has been adapted to discover disjoint multipath between a source and a destination. Using multiple paths can improve the quality of service as well as the fault resilience of a network. The routing protocol used in this paper is based on a modification of the Split Multipath Routing (SMR) protocol [23] proposed by Quian *et al.* [21]. The modified protocol allows intermediate nodes to forward repeated copies of a RREQ message, as long as their hop counts are not larger than the hop counts of already received copies. The destination should receive numerous copies of the RREQ message. Thus, the destination should be able to build a list of available paths from the source; this information gives a partial view of the network that would be used by the WIM-DSR protocol in the discovery of possible wormhole attacks.

The WIM-DSR final step is slightly different from the previous protocols. The main objective of WIM-DSR is to gather information during the route discovery phase and to find possible anomalies due to open wormhole attacks The

destination chooses a path and broadcasts it towards the source. The intermediate nodes should rebroadcast only one copy of a given RREQ message. This step should allow intermediate nodes to validate the information. WIM-DSR determines if the information gathered by the modified routing protocol during the route discovery shows the typical behaviour of wormhole attacks.

The aim of WIM-DSR is to find *fully witnessed* paths, i.e. paths with only witnessed edges between the source and the destination. Fully witnessed path should not contain any open wormhole. Strongly witnessed paths should be preferred. However, weakly witnessed paths should also be considered since the strongly witnessed condition is very restrictive and can generate numerous false positive alarms.

Once a fully witnessed path is found, the destination signs its RREP message and broadcasts it towards the source. For a strong witnessed path, the destination broadcasts a unique signed RREP message which is rebroadcast by all the nodes of the path. The other nodes simply overhear it. This allows each witness to receive the message from at least two nodes. For a path of length l, only $l - 1$ RREP messages are sent overall. For a weak witnessed path, the destination unicasts a signed RREP message along the path. Moreover, for each witness, the destination also unicasts a signed confirmation RREP message along a path going through that witness.

The real gain for the malicious nodes is the strong open wormhole attack. In such a case, they would be selected by any protocol selecting the shortest paths. Such a wormhole represents a shortcut in the network. The effectiveness of WIM-DSR to detect open wormhole attacks is proven in the following lemmas. They show that the path selection algorithms cannot find *false* witnesses for *strong open wormholes*.

V. EVALUATION

The objective is to determine how many pairs of source and destination nodes do not have fully witnessed paths in a given set of points. These pairs would represent the false positive alarms for the protocol. The network density is important for ad-hoc networks. For a given region, there are two ways to increase the density: (1) increase the number of nodes or (2) increase the transmission range of the nodes. Since the complexity of the simulation program depends on the number of nodes, the number of nodes is fixed and different range values are used. The concept of this paper is implemented and different results are shown below.

The proposed approach is implemented in Java and J2ME technology on a Pentium-III PC with 20 GB hard-disk and 256 MB RAM. The propose approach's concepts show efficient results of retrieving data from mobile nodes and has been efficiently tested on different systems.

Figure 2: Sending message

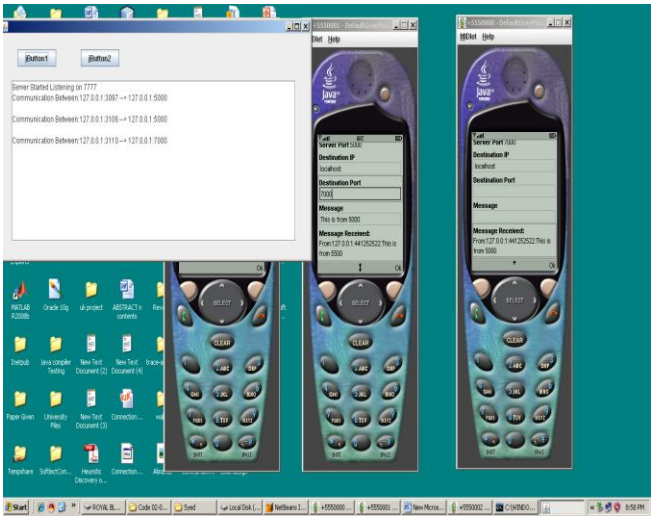

Figure 3: Edge Witnessing

Figure 4: Finding Witnessed paths and detecting attacks

VI. CONCLUSTIONS AND FUTURE ENHANCEMENTS

We introduce a new approach preventing strong open wormhole attacks. The WIM-DSR protocol uses the information collected by the destination node during the route discovery process of a multipath routing protocol to detect suspicious behaviour. The results obtained in this project show that the WIM-DSR protocol is able to detect all strong open wormhole attacks with a very low rate of false positive alarms. This solution does not require any cryptographic processing by the intermediate nodes, if no attack takes place.

Our implementation has shown that the prevention can be considered as reliable. The routing metric packet delivery is high mobility. Characteristics and results for this system were achieved after an extensive design part in our implementation. Design has been a key part to get reliable results. This study could be continued by, for instance, developing the multipath aspect of our protocol. It could be achieved by splitting data packets from the source to the destination; the whole message would not be transmitted by the same path or the same nodes all the time. Another solution could be to enforce reliability adding some redundancy code; in that case, it would allow not sending again packets in case one link breaks.

REFERENCES

[1] Y.-C. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 370 – 380, 2006.

[2] "Mobiworp: Mitigation of the wormhole attack in mobile multihop wireless networks," *Ad Hoc Networks*, vol. 6, pp. 344–362, 2008.

[3] D. Johnson and D. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks*. Kluwer Academic Publishers, ch. 5, pp. 153 – 181.

[4] S. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in *Proc. of the IEEE International Conference on Communications*, 2001, pp. 3201 – 3205.

[5] Y.-C. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wireless Networks*, vol. 11, pp. 21 – 38, 2005.

[6] David B. Johnson and David A. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. In *Mobile Computing*, edited by Tomasz Imielinski and Hank Korth, chapter 5, pages 153–181. Kluwer Academic Publishers, 1996.

[7] David B. Johnson, David A. Maltz, and Josh Broch. The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks. In *Ad Hoc Networking*, edited by Charles E. Perkins, chapter 5, pages 139– 172. Addison-Wesley, 2001.

[8] Adrian Perrig, Ran Canetti, Doug Tygar, and Dawn Song. Efficient Authentication and Signature of Multicast Streams over Lossy Channels. In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, pages 56–73, May 2000.

[9] Charles E. Perkins and Pravin Bhagwat. Highly Dynamic Destination- Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In *Proceedings of the SIGCOMM'94 Conference on Communications Architectures, Protocols and Applications*, pages 234–244, August 1994.

[10] Amir Qayyum, Laurent Viennot, and Anis Laouiti. Multipoint Relaying: An Efficient Technique for flooding in Mobile Wireless Networks. Technical Report Research Report RR-3898, Project HIPERCOM, INRIA, February 2000.

[11] Bhargav Bellur and Richard G. Ogier. A Reliable, Efficient Topology Broadcast Protocol for Dynamic Networks. In *Proceedings of the*

Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'99), pages 178–186, March 1999

[12] Mark Corner and Brian Noble. Zero-Interaction Authentication. In *Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002)*, pages 1–11, September 2002.

[13] Tim Kindberg, Kan Zhang, and Narendar Shankar. Context Authentication Using Constrained Channels. In *Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002)*, pages 14–21, June 2002.

[14] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 6, pp. 483 – 502, 2006.

[15] L. Butty´an and J.-P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge University Press, 2008.

[16] Y.-C. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 370 – 380, 2006.

[17] S. Capkun, L. Butty´an, and J.-P. Hubaux, "Sector: secure tracking of node encounters in multi-hop wireless networks," in *Proc. of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN)*, 2003, pp. 21 – 32.

[18] L. Hu and D. Evans, "Using directional antennas to prevent wormhole attacks," in *Proc. of the Network and Distributed System Security Symposium*, 2004.

[19] A. A. Pirzada and C. McDonald, "Detecting and evading wormholes in mobile ad-hoc wireless networks," *Int. Journal of Network Security*, vol. 3, pp. 191 – 202, 2006.

[20] I. Khalil, S. Bagchi, and N. B. Shroff, "Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks," *Computer Networks*, vol. 51, pp. 3750–3772, 2007.

[21]"Mobiworp: Mitigation of the wormhole attack in mobile multihop wireless networks," *Ad Hoc Networks*, vol. 6, pp. 344–362, 2008.

[22] L. Qian, N. Song, and X. Li, "Detection of wormhole attacks in multipath routed wireless ad hoc networks: a statistical analysis approach," *Journal of Network and Computer Applications*, vol. 30, pp. 308 – 330, 2007.

[23] D. Johnson and D. Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks*. Kluwer Academic Publishers, ch. 5, pp. 153 – 181.

[24] S. Lee and M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks," in *Proc. of the IEEE International Conference on Communications*, 2001, pp. 3201 – 3205.