

WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks

Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung
Division of Electrical and Computer Engineering, Hanyang University
17 Haengdang-dong, Sungdong-gu, Seoul, 133-791, Korea
{sun0467,dykim,dohyeon,}@mnlab.hanyang.ac.kr, jijung@hanyang.ac.kr

Abstract

In wireless ad hoc networks, nodes compromise to forward packets for each other to communicate beyond their transmission range. Therefore, networks are vulnerable to wormhole attacks launched through compromised nodes because malicious nodes can easily participate in the networks. In wormhole attacks, one malicious node tunnels packets from its location to the other malicious node. Such wormhole attacks result in a false route with fewer. If source node chooses this fake route, malicious nodes have the option of delivering the packets or dropping them. It is difficult to detect wormhole attacks because malicious nodes impersonate legitimate nodes. Previous algorithms detecting a wormhole require special hardware or tight time synchronization. In this paper, we develop an effective method called Wormhole Attack Prevention (WAP) without using specialized hardware. The WAP not only detects the fake route but also adopts preventive measures against action wormhole nodes from reappearing during the route discovery phase. Simulation results show that wormholes can be detected and isolated within the route discovery phase.

1. Introduction

A Mobile Ad-hoc NETWORK (MANET) comprises nodes that are organized and maintained in a distributed manner without a fixed infrastructure. These nodes, such as laptop computers, PDAs and wireless phones, have a limited transmission range. Hence, each node has the ability to communicate directly with another node and forward messages to neighbors until the messages arrive at the destination nodes. Since the transmission between two nodes has to rely on relay nodes, many routing protocols [11, 12, 13, 14] have been proposed for ad hoc networks. However, most of them assume that other nodes are trustable and hence they do not consider the security and attack issues. This provides many opportunities for attackers to break the network. Moreover, the open nature of wireless communication channels,

the lack of infrastructure, rapid deployment practices, and the hostile environments in which they may be deployed, make them vulnerable to a wide range of security attacks described in [1, 2, 3, 4, 5, 6]. However the attacks are performed by a single malicious node. Many solutions proposed in order to solve single node attacks in [10, 15, 16] cannot defend attacks that are executed by colluding malicious node, such as wormhole attack, which damage is extensive than single node attacks.

In this paper, we focus on an attack launched by a pair of colluding attackers: wormhole attack. Two malicious nodes that are separated by a large distance of several hops build a direct link called a tunnel and communicate with each other through the tunnel. The tunnel can be established in many different ways, for example, through an out-of-band channel, packet encapsulation, and high-powered transmission. This route via the wormhole tunnel is attractive to the legitimate nodes because it generally provides less number of hops and less latency than normal multi-hop routes. The attackers can also launch attacks without revealing their identities. The wormhole attack is still possible even if the adversary does not access the contents of the packet. Therefore, it can be difficult to detect wormhole attacks since the contents of the packets are not modified.

In order to detect these attacks, some mechanisms have been proposed [3, 4, 7, 8, 9]. However, most of these mechanisms require specialized devices that can provide the location of the nodes or tight time synchronization. Moreover, they focus only on the method of detection of the wormhole route. In this paper, we propose an efficient algorithm based on Dynamic Source Routing (DSR) protocol [12, 13]. The advantage of this algorithm is that it does not require the location information of time synchronization.

This paper is organized as follows. Section 2 presents related works on the detection of wormhole attacks. In Section 3, we describe wormhole detection and the prevention algorithm in detail. Simulation results and analysis are presented in Section 4. Finally, the conclusion is provided in Section 5.

2. Related Works

Packet Leash [4] is an approach in which some information is added to restrict the maximum transmission distance of packet. There are two types of packet leashes: geographic leash and temporal leash. In geographic leash, when a node A sends a packet to another node B, the node must include its location information and sending time into the packet. B can estimate the distance between them. The geographic leash computes an upper bound on the distance, whereas the temporal leash ensures that a packet has an upper bound on its lifetime. In temporal leashes, all nodes must have tight time synchronization. The maximum difference between any two nodes' clocks is bounded by Δ , and this value should be known to all the nodes. By using metrics mentioned above, each node checks the expiration time in the packet and determine whether or not wormhole attacks have occurred. If a packet receiving time exceed the expiration time, the packet is discarded.

Unlike Packet Leash, Capkun et al. [7] presented SECTOR, which does not require any clock synchronization and location information, by using Mutual Authentication with Distance-Bounding (MAD). Node A estimates the distance to another node B in its transmission range by sending it a one-bit challenge, which A responds to instantaneously. By using the time of flight, A detects whether or not B is a neighbor or not. However, this approach uses special hardware that can respond to a one-bit challenge without any delay as Packet leash is.

In order to avoid the problem of using special hardware, a Round Trip Time (RTT) mechanism [5] is proposed by Jane Zhen and Sampalli. The RTT is the time that extends from the Route Request (RREQ) message sending time of a node A to Route Reply (RREP) message receiving time from a node B. A will calculate the RTT between A and all its neighbors. Because the RTT between two fake neighbors is higher than between two real neighbors, node A can identify both the fake and real neighbors. In this mechanism, each node calculates the RTT between itself and all its neighbors. This mechanism does not require any special hardware and it is easy to implement; however it can not detect exposed attacks because fake neighbors are created in exposed attacks.

The Delay per Hop Indicator (DelPHI) [13] proposed by Hon Sun Chiu and King-Shan Lui, can detect both hidden and exposed wormhole attacks. In DelPHI, attempts are made to find every available disjoint route between a sender and a receiver. Then, the delay time and length of each route are calculated and the average delay time per hop along each route is computed. These values are used to identify wormhole. The route containing a wormhole link will have a greater Delay per Hop (DPH) value. This mechanism can detect both types of wormhole attack; however, it

cannot pinpoint the location of a wormhole. Moreover, because the lengths of the routes are changed by every node, including wormhole nodes, wormhole nodes can change the route length in a certain manner so that they cannot be detected.

3. WAP (Wormhole Attack Prevention)

In this section, we describe a method for preventing wormhole attack called as Wormhole Attack Prevention (WAP). All nodes monitor its neighbors behavior when they send RREQ messages to the destination by using a special list called Neighbor List. When a source node receives some RREP messages, it can detect a route under wormhole attack among the routes. Once wormhole node is detected, source node records them in the Wormhole Node List. Even though malicious nodes have been excluded from routing in the past, the nodes have a chance of attack once more. Therefore, we store the information of wormhole nodes at the source node to prevent them taking part in routing again. Moreover, the WAP has the ability of detecting both the hidden and exposed attacks without special hardware.

3.1. Assumption

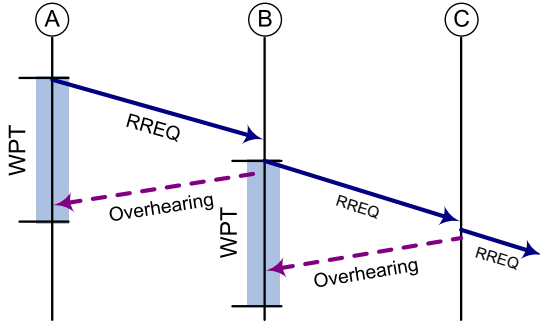
At the link layer, it assumes that a node can always monitor ongoing transmissions even if the node itself is not the intended receiver. This typically requires the network interface stay in the promiscuous reception mode during all transmissions, which is less energy efficient than listening only to packets directed to oneself. We also assume that radio links are bi-directional; that is, if a node A is in transmission range of some node B, then B is in transmission range of A. We further assume that the transmission range of a wormhole node is similar to a normal node because more powerful transceiver is easy to detect.

3.2. Neighbor Node Monitoring

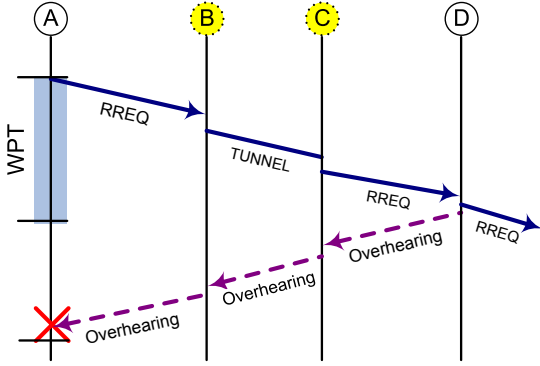
Neighbor Node Monitoring is used to detect neighbors that are not within the maximum transmission range but pretend to be neighbors. In order to reduce network overheads by additional packets, this mechanism is achieved during the route discovery process. Originally, the intermediate node which has a route to destination can send a RREP to source. However, our mechanism does not support the DSR optimization because it performs end-to-end signature authentication of routing packet and verification of whether a node is authorized to send a RREP packet. Therefore, an intermediate node cannot reply from its cache.

Figure 1 shows an example of the secure neighbor monitoring. Node A sends a RREQ, which starts a wormhole prevention timer (WPT). When node B receives the RREQ,

B must broadcast to its neighbors because B is not a destination. A can check whether the RREQ arrives within the timer. If A receives the message after the timer expires, it suspects B or one of B's next nodes to be wormhole nodes.



(a) Neighbor node monitoring of legitimate nodes



(b) Neighbor node monitoring of wormhole nodes

Figure 1. Example of Neighbor Node Monitoring

Once a malicious node overhears a RREQ, the node can claim to be another wormhole node that is actually not within the transmission range of a neighbor node. For this reason, two nodes may believe that the other is its neighbor which does not want to expose itself. In order to prevent this problem, nodes monitor the malicious behavior of neighbors and record it in the own neighbor node table.

3.2.1 Neighbor Node Table

Each node maintains a Neighbor node table that contain a RREQ sequence number, neighbor node ID, sending time and receiving time of the RREQ and count. By using this table, all nodes monitor the activities of neighbors in its table and check for malicious behavior of the neighbors. All the fields of neighbor node table set to zero. Table 1 shows an example of the neighbor node table.

If any node sends a RREQ, it records the RREQ sequence number and sending time of the RREQ. Then, on overhearing a RREQ from any node, it records the address of the neighbor node and the time when it receives the packet. If the node receives the RREQ after the timer count, called as WPT, it considers the neighbor node sending the RREQ as a node affected by wormhole nodes. The count value in its table will be increased by 1. It must be noted that the count value does not exceed the previously configured threshold. If the count value exceeds the threshold, the node cannot engage in the network. This method ensures that wormholes nodes are avoided in all the future data connections.

Table 1. Neighbor Node Table

RREQ seq #	Neighbor Node ID	Sending Time	Receiving Time	Count

3.2.2 Wormhole Prevention Timer

We detect wormholes by using a special timer. For using this timer, all the nodes do not require clock synchronization, except the source node. As soon as a node sends a RREQ packet, it must set the WPT and wait after sending the RREQ packet until it overhears its neighbor's retransmission. The WPT consider the maximum amount of time required for a packet to travels from a node to a neighbor node and back to the node. If WPT is too small, the legitimate nodes can be excluded. On the other hand, if it is too large, it is difficult to detect wormhole attacks.

Two formulas are considered to determine whether or not the nodes have a mobility. If the nodes are fixed like sensor node, the WPT is estimated by

$$WPT = \frac{2 \times \text{Transmission Range}(TR)}{V_p} \quad (1)$$

Here, TR denotes a distance that a packet can travel and V_p denotes the propagation speed of a packet. It is assumed that the maximum propagation speed of the radio signal is the speed of light and the delay from sending and receiving packets is negligible.

On the other hand, if the nodes have a mobility with an average velocity of V_n , the distance that packet can travel may be different. The maximum transmission distance of a packet is calculated by

$$\text{Radius} = V_n \times \frac{2 \times TR}{V_p} = \frac{2 \times V_n \times TR}{V_p} \quad (2)$$

Consequently, when network are formed in the mobile environment, the WPT of nodes is given by

$$WPT = \frac{2 \times V_n \times TR}{(V_p)^2} \quad (3)$$

By using the formulas 1, 3, when a node overhears its neighbor node's re-transmission, it checks whether the packet has arrived before the WPT expired. If a hidden wormhole attack is launched, the packet transmission time between two fake neighbor nodes may be longer than the normal transmission time of one hop. Therefore, we can detect a route through a wormhole tunnel.

3.3. Wormhole Route Detection

We detect exposed wormhole node when a source node selects one route among all the routes collected from the RREP packets within the RREP waiting timer. In the DSR protocol, the route selection without any wormhole attack is simple. The source node selects the smallest hop_count route among all the received routes.

Unfortunately, the smallest hop_count route may contain wormhole nodes. Hidden attacks can be detected by neighbor node monitoring. However, if wormhole nodes are exposed and act like a legitimate node, it is difficult to detect a wormhole route by using only the neighbor node monitoring mechanism.

Therefore, nodes must check a RREP packet on receiving it from neighbor nodes. When a wormhole node sends a RREP to indicate that a colluding node is its neighbor, normal neighbor nodes of the wormhole node examine whether they have corresponding RREQ packet previously received from the node in their table. For example, in figure 2, suppose a source node S broadcasts RREQ at time T_a , and then receives a RREP at time T_b ; the source node can calculate the time delay per hop in the route by using hop_count field in the RREP. The formula is given by

$$Delay \text{ per hop} = \frac{T_b - T_a}{Hop \text{ count}} \leq WPT \quad (4)$$

As specified in above, the maximum amount of time required for a packet to travel one-hop distance is $WPT / 2$. Therefore, the delay per hop value must not exceed the estimated WPT.

In normal situation such as Figure 2(b), a smaller hop_count provides a smaller time delay. This can be explained by the fact that a shorter route should have a smaller round trip time. Hence, the delay per hop_count value of the normal route should have similar values.

3.3.1 Wormhole Node List

When a node detects exposed wormhole nodes during route discovery, it must keep a wormhole node list, which is in-

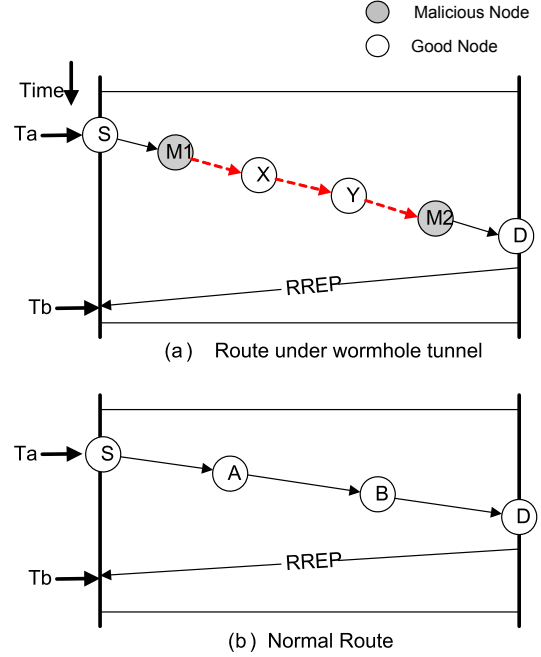


Figure 2. Time Delay of Route Discovery

dexed by wormhole node and colluding node. For example, if a node overhearing a RREP discovers that the previous node is wormhole node, it places previous node and next node from the RREP packet in the node's blacklist. A node must broadcast information of the wormhole nodes in the blacklist. Each time nodes receive the messages, the node should set the wormhole node list and record the information. After the wormhole nodes is specified in the list, any packet from the nodes in the wormhole list.

4. Simulation

4.1. Simulation Environment

We have implemented wormhole attack and our proposed algorithms in a Qualnet [17]. For our simulations, we use CBR (Constant Bit Rate) application, UDP/IP, IEEE 802.11b MAC and physical channel based on statistical propagation model. The simulated network consists of 50 randomly allocated wireless nodes in a 1500 by 1500 square meter flat space. The node transmission range is 250 meter power range. Random waypoint model [18] is used for scenarios with node mobility. The minimum speed for the simulations is 0 m/s while the maximum speed is 10 m/s. The selected pause time is 30 seconds. A traffic generator was developed to simulate constant bit rate sources. The

size of data payload is 512 bytes. Five data sessions with randomly selected sources and destinations are simulated. Each source transmits data packets at the rate of 4 packets/s. Duration of the simulations is 900 seconds.

4.2. Simulation Results

The network throughput is measured for the basic DSR routing protocol and DSR with the WAP method. The speed of nodes is varied to compare the results. Figure 3 shows the results of the network throughput of both techniques for different node speeds. Even if there are no wormhole nodes, the network throughput diminishes in the environment of both DSR and WAP method as the node speed increases because the network generally becomes more fragile as the node speed increases. However, the network throughput of the basic DSR protocol dramatically decreases when there are wormhole nodes in the networks. For example, the throughput value is 74.7% when the basic DSR is used and when the nodes are moving with a speed of 10 m/s. However, the throughput value is 88.9% when the WAP is used under a wormhole attack. This proves that the network throughput of the WAP algorithm exceeds that of the basic DSR protocol.

We experiment on the capability of wormhole detection and isolation with WAP method. Generally, in the basic DSR protocol, each node does not check a RREQ packet overheard from its neighbor nodes. Therefore, the fraction of packets sent through the wormhole tunnel is high. In contrast, each node that uses the neighbor node table and wormhole node list take into account the information of the subsequent node before forwarding a packet. Therefore, the packets sent through a wormhole tunnel are mostly dropped to prevent the packets from arriving at the destination. Figure 4 provides the fraction of packets sent over wormhole routes in the basic DSR and modified DSR with the WAP algorithm at varying speeds.

5. Conclusion

With development in computing environments, the services based on ad hoc networks have been increased. However, 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.

The detection of wormholes in ad hoc networks is still considered to be a challenging task. In order to protect networks from wormholes, previous solutions require specialized hardware. Thus, in this paper, we propose an algorithm to detect wormholes without any special hardware.

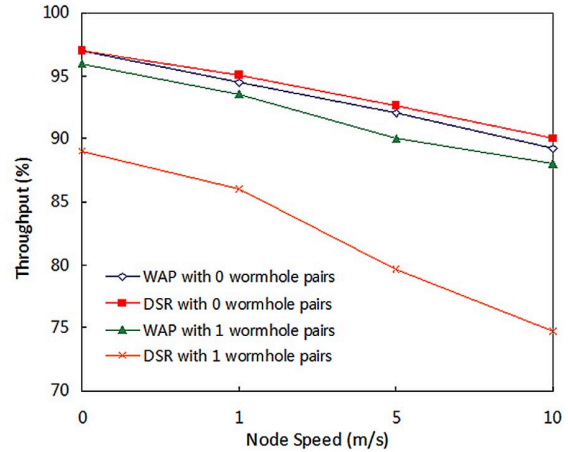


Figure 3. Effect of Wormhole Attack on Network Throughput

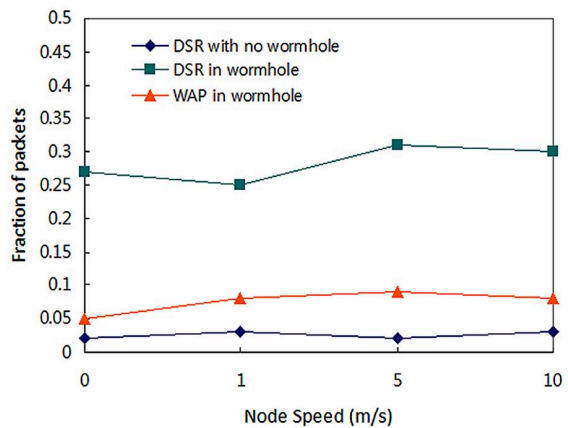


Figure 4. Fraction of Packets Sent Through Wormhole

We achieve this through the use of the neighbor node monitoring method of each node and wormhole route detection method of the source node on the selected route. Our mechanism is implemented based on the DSR protocol and is proven to be capable through simulation results. In future studies, we plan to study false positive problems with regard to the detection of wormholes and a mechanism to solve such problems. Moreover, we plan to apply the WAP algorithm to other on-demand routing protocols.

Acknowledgement

This research was supported by the Ministry of Knowledge Economy, Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Advancement) (IITA-2008-C1090-0801-0016)

References

- [1] L. Buttyán and J.-P. Hubaux. Report on a working session on security in wireless ad hoc networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, 7(1):74–94, Jan 2003.
- [2] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang. Security in mobile ad hoc networks: challenges and solutions. *IEEE Wireless Communications*, 11(1):38–47, Feb 2004.
- [3] L. Hu and D. Evans. Using directional antennas to prevent wormhole attacks. In *Network and Distributed System Security Symposium (NDSS)*. The Internet Society, Feb 2004.
- [4] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. *IEEE INFOCOM*, Mar 2003.
- [5] J. Zhen and S. Srinivas. Preventing replay attacks for secure routing in ad hoc networks. In *ADHOC-NOW*, LNCS 2865, pages 140–150, 2003.
- [6] Y.-C. Hu, A. Perrig, and D. B. Johnson. Rushing attacks and defense in wireless ad hoc network routing protocols. In W. D. Maughan and A. Perrig, editors, *ACM Workshop on Wireless Security (WiSe)*, pages 30–40, Sep 2003.
- [7] S. Capkun, L. Buttyán, and J.-P. Hubaux. SECTOR: secure tracking of node encounters in multi-hop wireless networks. In *ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, pages 21–32, Oct 2003.
- [8] I. Khalil, S. Bagchi, and N. B. Shroff. LITEWOP: A lightweight countermeasure for the wormhole attack in multihop wireless networks. In *Dependable Systems and Networks (DSN)*, pages 612–621, Jun 2005.
- [9] I. Khalil, S. Bagchi, and N. B. Shroff. MOBIWOP: Mitigation of the wormhole attack in mobile multihop wireless networks. *Securecomm and Workshops 2006*, pages 1–12, Aug 2006.
- [10] L. Tamilselvan and D. V. Sankaranarayanan. Prevention of impersonation attack in wireless mobile ad hoc networks. *International Journal of Computer Science and Network Security (IJCSNS)*, 7(3):118–123, Mar 2007.
- [11] C. E. Perkins, E. M. Belding-Royer, and S. R. Das. Ad hoc on-demand distance vector (AODV) routing. RFC 3561, The Internet Engineering Task Force, Network Working Group, Jul 2003. <http://www.ietf.org/rfc/rfc3561.txt>.
- [12] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. In Imielinski and Korth, editors, *Mobile Computing*, volume 353, pages 153–181. Kluwer Academic Publishers, 1996.
- [13] D. A. Maltz and D. B. Johnson and Y. Hu. The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. RFC 4728, The Internet Engineering Task Force, Network Working Group, Feb 2007. <http://www.ietf.org/rfc/rfc4728.txt>.
- [14] R. V. Boppana and S. P. Konduru. An adaptive distance vector routing algorithm for mobile, ad hoc networks. In *IEEE Computer and Communications Societies (INFOCOM 2001)*, pages 1753–1762, 2001.
- [15] P. Papadimitratos and Z. J. Haas. Secure routing for mobile ad hoc networks. In *Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, Jan 2002.
- [16] Y.-C. Hu, D. B. 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 (WMCSA)*, pages 3–13. IEEE Computer Society, Dec 2002.
- [17] Scalable Network Technologies (SNT). *QualNet*. <http://www.qualnet.com/>.
- [18] J. Broch, D. A. Maltz, D. B. Johnson, Y.-C. Hu, and J. G. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM)*, pages 85–97, Oct 1998.