Watch-Nodes-Based Wormhole Attacks Detection in Wireless Mesh Networks

Liang-yu Luan [1]
[1] *College of Applied Science, Beijing University of Technology, Beijing 100124, China*

Ying-fang Fu [2*]
[2*] *Fantai Lingshi Technology (Beijing) Limited, Beijing 100044, China*

Peng Xiao [3]
[3] *College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China*

Ling-xi Peng[4]
[4]*Department of Computer and Education Software, Guangzhou Univ., Guangzhou 510006, China*

Received 30 November 2011
Accepted 15 June 2012

Abstract

Wormhole attacks, as a devastating type of threats in wireless mesh networks, have received much attention in recent years. This paper proposes a type of wormhole attack model and its corresponding detection scheme. In this scheme, the combination of a number of techniques, such as distributed voting, watch-nodes-based detection and identity-based cryptosystem are used. The simulation results and qualitative analysis demonstrate the performance and cost of the proposed scheme are more advantageous over the some of the previous schemes.

Key words: Wormhole Attack, Routing Protocol, Wireless Mesh Network, Distributed Voting, Identity-based Cryptosystem.

1. Introduction

A wireless mesh network (WMN) is a dynamically self-organizable and self-configurable network in which all the nodes can work together to automatically form a multi-hop ad hoc network to maintain network connectivity [1]. A WMN is a natural solution to the deployment of large-scale wireless networks[2.] Thus, maintaining the security of communication among mobile nodes in a WMN is critical for the routing protocols designed for such multi-hop networks. However, since there is a lack of fixed infrastructure and the network is mostly operated over the open media, any malicious attacks could easily disrupt normal operations in such a network. A particularly devastating attack to the normal routing functionality in a WMN is the so-called wormhole attacks in which a malicious node could capture packets at one location and send them through a "tunnel" to another cooperating malicious node at a distant location that could relay the received packets locally. Such a "tunnel" can be established in many different ways, such as using an out-of-band hidden channel (e.g., a wired link) or some other high speed transmission media, or through packet encapsulation, etc. The tunnel can make tunneled packets arrive at a sooner or via a fewer number of hops to those transmitted over other normal multi-hop routes, which makes it appear that the two end points of the tunnel are very close to each other[3-4]. As a result, the route involving the two cooperating malicious nodes through the tunnel could be selected as the route of choice for packet transmission and subsequent attacks could be launched to the packets by the malicious nodes. Prior research on wireless multi-hop networks, especially on ad hoc networks, has produced some solutions for the detection of wormhole attacks. However, since most of the solutions require the use of specialized hardware to match senders and receivers

[*] Corresponding author, E-mail: fuyingfang@bjut.edu.cn

Published by Atlantis Press

through directional antennas or ultrasonic signals, they are not practical for general wireless mesh networks.

In this paper, we propose a new scheme for the detection of wormhole attacks in which we employ a number of techniques, such as distributed voting, watch nodes-based detection and identity-based cryptosystem. We perform a thorough analysis of our proposed scheme through simulation on some important aspects of wormhole attack detection in a mesh network such as detection success rate, detection delay and average detection delay and share our observation based on the simulation results.

This paper is organized as follows. In the next section, we review some related work in wormhole attack detection in multi-hop wireless networks. In Section 3, we describe a common type of wormhole attack. In Section 4, we present a new wormhole attack detection scheme that based on the watch nodes. In Section 5, we perform a thorough analysis of our scheme and present our simulation results. Finally, we conclude this paper in Section 6 in which we also discuss our future work.

2. Related Work

Wormhole attacks in wireless networks were first noted by B. Dahill et al.[5] and two approaches were proposed to fight against such attacks. In the first approach, i.e., RF watermarking, radio waves would be modulated in a specific pattern and any changes to the pattern would be used as a trigger for the detection of such an attack. In the second approach, using a similar principle, neighboring nodes would communicate with each other using special types of signals. However, the first approach would not be effective if the carrier wave can be accurately replicated at the transmitting end and captured at the receiving end of the wormhole. The second approach is not practical because it is impossible to require all users in a WMN to use special types of signals for communication.

L. Hu and D. Evens proposed a scheme in which directional antennas are used to prevent wormhole attacks [6]. In the scheme, every node shares a secret key with every other node and maintains an updated list of its neighbors. Neighbor lists are built in a secured manner by using the direction in which a signal is heard from a neighboring node with the assumption that the antennas on all the nodes are aligned. Although the scheme can help to mitigate wormhole attacks, it has the following obvious shortcomings. First, since neighboring nodes use a symmetric secret key to authenticate each other, it would be difficult to defend man-in-the-middle attacks for the malicious nodes could capture the symmetric secret key. Second, since a node determines if another node is a neighbor based on whether the directions of their antennas are aligned with each other, it is not always reliable.

Y. Hu, A. Perrig and D. Johnson presented two packet leash approaches to defend against wormhole attacks[7-8]. The first approach is based on geographical leashes to ensure that the recipient of a packet is within a certain distance from the sender, and the other approach is based on temporal leashes to ensure that a packet has an upper bound on its lifetime. The two approaches would restrict the maximum distance that a packet can travel. Both the geographical and the temporal leashes would need to be protected using TIK authentication protocol. Every node has its own public key in the TIK authentication protocol, and each node must issue its public key to the others nodes, which increases the storage space of every node and the network bandwidth.

All the wormhole attack detection methods mentioned before requires the employment of specialized hardware devices, directional antennas or time synchronization, thus limits their applicability. Afterward, some wormhole attack detection methods those don’t need any requirements were proposed. Such as, H. S. Chiu and K. S. Lui proposed a scheme that relies on the delay/hop (DPH) value to detect wormhole attacks in a routing path [9]. X. Wang and J. Wong proposed a scheme based on end-to-end detection of wormhole attacks (EDWA) [10]. L. Lazos et al. proposed a graph-based framework to tackle wormholes[11]. M. Khabbazian et al proposed a timing-based solution[12]. D.Done et al. proposed a topological detection-based method to detect wormhole attacks [13]. S.Gupta et al. proposed a wormhole attack detection protocol using hound packet. Those schemes don’t require synchronized clocks or any special hardware. However, those schemes have some limitations that prevented the applicability of them. For example，document 9 only detects the existing of wormhole attacks but which mobile nodes launched the wormhole attacks can not be detected. Besides, when mobile nodes move around, the DPH values also change accordingly. Therefore, this scheme is not very scalable. Document [10] is effective only when the source and the destination nodes are not too far from each other. As the distance between the source and the destination nodes becomes longer, the scheme will become less effective because an accurate estimation of the hop count value would become more difficult. Therefore, this scheme has the scalability problem. Document [11] assumed the existence of guard nodes have extraordinary communication range. Document [12] assumed the network is static. Documents [13] and [14] would increase the wormhole attack detection spending for using topological detection (the topology in WMN change continually) and hound packet (increase the spending of hound packet transmitting) respectively.

3. Wormhole attacks through out-of-band channel

Wormhole attacks could be particularly effective in wireless multi-hop network routing that the two mesh routing protocols MR-LQSR (Multi-Radio Link-Quality Source Routing) [15] and HRPU (Hybrid Routing with Periodic Updates) [16], and the sensor TinyOS beaconing routing protocol [17]. We now use the MR-LQSR protocol as an example to illustrate how wormhole attacks can be launched against such routing protocols.

In the MR-LQSR protocol, the way in which neighboring nodes are discovered and propagated to other nodes in the network is similar to that in the DSR protocol. In the protocol, if a source node, say S, needs to discover a route to a destination node, say D, node S would flood the network with a route request packet. Any node that hears the request packet will process the packet, add its own identity to the source route, and rebroadcast the packet. To limit the amount of flooding traffic in the network, each node would broadcast only the first route request packet that it receives and drop all future copies of the same request packet. For each route request packet that node D receives, it would generate a route reply packet and send the packet to node S. The source node would finally select the best route from all the route reply packets it receives based on the *WCETT* (weighted cumulative expected transmission time) and the route with the smallest *WCETT* will be selected as the best route. Eq. (1) is the formula for calculating the WCETT [18]:

$$WCETT = (1-\beta) * \sum_{i=1}^{n} ETT_i + \beta * \max_{1 \le j \le k} X_j \cdot \qquad (1)$$

$$X_j = \sum_{\substack{\text{Hop i is} \\ \text{on channel j}}} ETT_i \quad , \left(1 \le \mathrm{j} \le \mathrm{k}\right) \cdot \qquad (2)$$

In the above equations, n is the total number of links in a route, k is the total number of channels in the system, ETT_i is the expected transmission time of a packet over link i, X_j is the transmission time through the hops over channel j, and β is a tunable parameter such that $0 \le \beta \le 1$ .Wormhole attacks through out-of-band channel can be established, for instance, by using a long-range directional wireless link or a direct wired link. Let's now consider the scenario depicted in Fig.1, in which a source node, say S, tries to find a route to a destination node, say D, by broadcasting a route request packet. When node Q receives the request packet, it would forward the packet to node X because it is not the destination node specified in the packet. If the two malicious nodes X and Y maintain an out-of-band channel between them, node X can then tunnel the route request packet to node Y that is a legitimate neighbor of node D. Malicious node Y will rebroadcast the request packet to its neighbors including node D. Node D eventually gets two request packets through the two routes S–Q-X–Y–D and S–E–F–G–H–D. Since the WCETT value for the first route is smaller than that for the second one, the first route S–Q-X–Y–D will be selected as the best route path. Afterwards, the two malicious nodes X and Y can launch various attacks to received data packets including dropping or modifying packets, forwarding only some of the received packets, etc. To fight against the wormhole attacks just described, we present in the next section a new wormhole attack detection scheme by considering the characteristics of wireless mesh networks as well as those of the wormhole attacks.

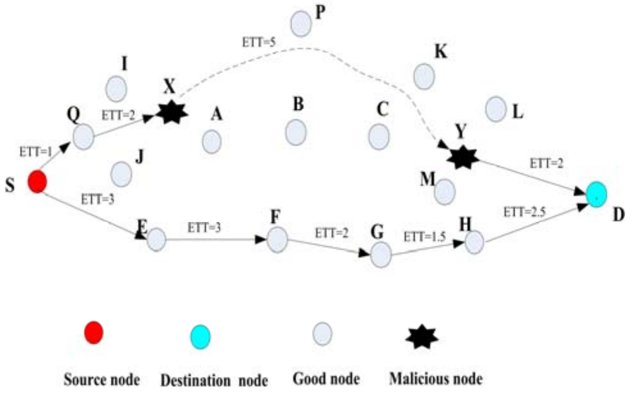
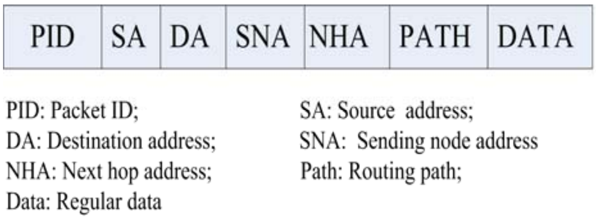


Fig.1. Wormhole Attacks Using Out-of-Band Channel

4. Wormhole Attacks Detection Scheme

4.1. *The packet format*



PID	SA	DA	SNA	NHA	PATH	DATA

PID: Packet ID; SA: Source address;
DA: Destination address; SNA: Sending node address
NHA: Next hop address; Path: Routing path;
Data: Regular data

Fig.2. Packet Format

The packets used in our detection scheme contain seven fields as shown in Fig.2. In any packet, PID denotes the ID of the packet. SA, DA, SPA and DHA denote the addresses of the source node, the destination node, the sending node and the next hop node, respectively. PATH records the IDs of all the nodes along the path and DATA contains the data to be transmitted. Before adding the PATH into the corresponding field, the sending node would encrypt them with the identity of the destination node.

4.2. *Watch nodes-based detection scheme*

The watch nodes-based detection scheme proposed here is intended to be used for the detection of wormhole attacks that use out-of-band channels as illustrated in Fig.1. We can see in the figure that source node S has just found the best route S-Q-X-Y-D to destination node D. Then, node S would send all data packets to node D through this route. Nodes I and J are the watch nodes of the link Q-X and nodes P and B are the watch nodes of the link X-Y. When node S sends a data packet to node D, it would include in the packet fields the packet ID (PID), the source node address (SA), the destination address (DA), the next hop address (NHA), and any data that is encrypted with the identity based private key of the node D along with the public key of the zone to which node D belongs (identity based private key may be attainted in document [19].When node Q hears the data packet, it checks to see if it is the destination node. Since it is not, it would replace the corresponding addresses in SNA and NHA with its own address and its next hop address, respectively, and then forward the packet to node X. Nodes X and Y will do the same as what node Q did. In the process of sending out the data packet, we use the watch node detection method described following to monitor all the outgoing links. If a sending node i sends x number of packets to a receiving node j and the receiving node j only forwards y number of packets, The packet drop ratio γ of the link i-j can be expressed using Eq.(3).

$$\gamma = (x - y / x) \times 100\ \% \ . \qquad (3)$$

If a watch node of the link i-j discovers that $\gamma > \tau$ where τ is the threshold of γ , or the sending packet is not in its watch buffer, it would send the detection information to an administrator to inform the router of the existence of a wormhole link. When the administrator receives the detection information, it would initiate the voting scheme in which the administrator would send the detection information to all the watch nodes of the suspected wormhole link. Every watch node would eventually send its voting decision to the router based on the packet drop ratio of the link that it watches or monitors. The administrator would aggregate all the voting results from all the watch nodes to determine if the link is indeed a wormhole link. If a majority of the watch nodes indicate that the link is indeed a wormhole link, the administrator would decommission the two attacking nodes i and j from the network following the key update and revocation scheme described in document [20].

5. Simulation Results and Analysis

5.1. *Simulation of the received packet ratio*

We use OPNET 10.5 in our study to simulate and analyze the performance of the proposed wormhole attack detection scheme in a wireless mesh network.

In the simulation of the received packet ratio, we distribute a number of nodes randomly over a square area of 100×100m2 as illustrated in Fig.3 with the various parameters as follows: the channel transmission rate of the wireless receiver is set at 11Mbps; the power is fixed at 1W; the interval for sending out packets is 0.01 second; the normal received packet ratio is 99.9%; the simulation time runs for 20 seconds; and the threshold τ of packet dropt ratio γ is 10%. The parameter τ is defined as the highest average packet dropt ratio that the system runs normally in different periods. The meaning of parameter γ is that when a watch node notices that the packet dropt ratio γ of a link exceeds 10%, the watch node would send detection information to a zone router.

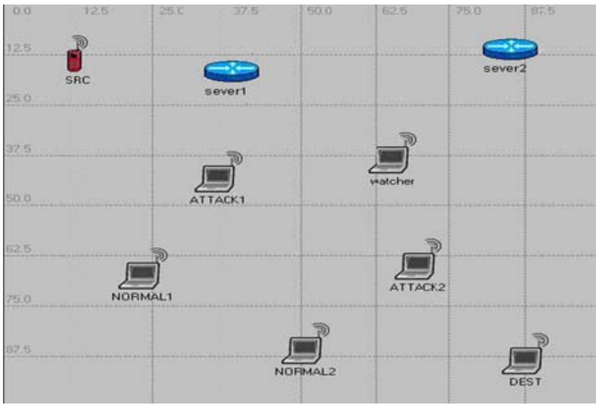


Fig.3. Simulation Scenario for the Received Packet Ratio

In the beginning of the simulation, source node SRC sends out packets to destination node DEST through route SRC-ATTACK1-ATTACK2-DEST during the first two seconds. Then attacking nodes ATTACK1 and ATTACK2 randomly drop 20% of the packets over the link ATTACK1-ATTACK2. When watch node WATCHER notices that the packet drop ratio of the link ATTACK1-ATTACK2 exceeds 10%, it sends detection information to its zone router. Eventually, the zone router would decommission the two collusive wormhole attack nodes ATTACK1 and ATTACK2. Afterwards, source node SRC will send all packets to destination node DEST through the other route SRC-NORMAL1-NORMAL2-DEST. The results for the received packet ratio are shown in Fig.4, in which the ratio is 100% during the first two seconds and then decreases rapidly after the two attack nodes launch the wormhole attack by dropping packets. After the zone router receives the detection information from the watch node, it would decommission the two attack nodes. The received packet ratio starts to go up again 3.41 seconds later and reaches 98.2% when the simulation ends at the 20th second.

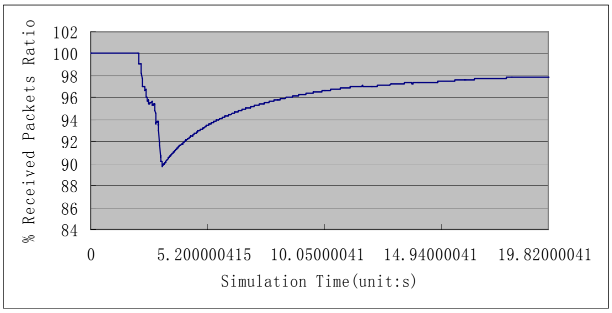


Fig.4. Results of the Received Packets Ratio

5. 2. *Simulation of the detection delay*

In the simulation, we randomly distribute twenty five source nodes labeled as SRC_0, …, SRC_24, five watch nodes labeled as watcher_0, …, watcher_4, one destination node DEST, twenty five pairs of nodes labeled as ATT_0-ATT2_0, ATT_1-ATT2_1, …, ATT0_24-ATT2_24, and two zone routers over a square area of $500 \times 500\text{m}^2$ as shown in Fig.5. The longest transmission time between any two nodes is 0.267μs and the transmission time between all watch nodes and the routers is less than 0.267μs. The twenty five pairs of nodes may be normal nodes or collusive wormhole attackers. The interval of sending out packet follows a uniform distribution with the range (0, 0.03). In the simulation, if three out of the five watch nodes determine that one pair of nodes are collusive attackers, following the majority voting rule, the pair would be considered as collusive attackers and the zone router would decommission the pair out of future communication. If not specified, all the other parameters are the same as they are in the previous simulation scenario. Our goal here is to simulate the detection delay, the average detection delay and the detection success rate for different scales of collusive wormhole attackers with the number being between 1 and 25 pairs. We also consider the following two different cases with the first one being that the router would actively ask for the voting results from all the watch nodes and the second one being that the router would only passively wait for the voting results from all the watch nodes.

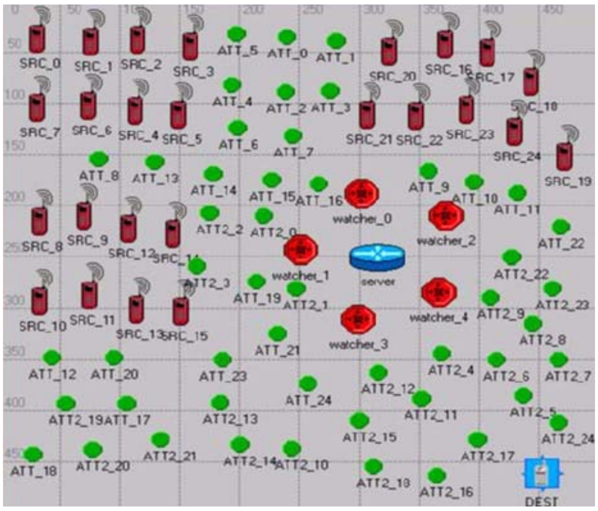


Fig.5. Simulation Scenario of Detection Delay and Average Detection Delay

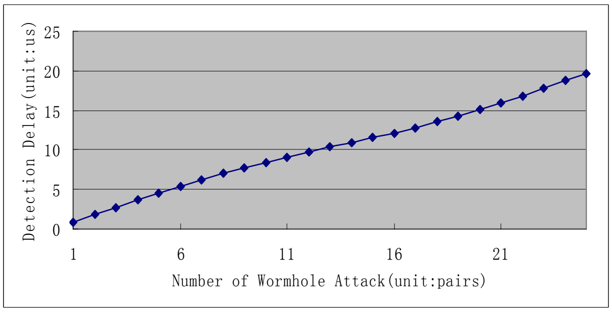


Fig.6. Detection Delay

In the first case, the detection delay would increase along with the increase in the number of collusive wormhole attackers as shown in Fig.6. At one extreme, the time delay to detect one pair of collusive wormhole attackers is 0.916µs. At the other extreme, the time delay to detect all the 25 pairs of collusive wormhole attackers is 19.735µs. The detection success rate, on the other hand, always remains at 100% as shown in Fig.7, in which the horizontal axis is the number of attacking nodes in pairs. Fig.8 shows the average detection delay in the first case in which we can see that when the number of pairs of collusive wormhole attackers increases from 1 to 19, the average detection delay would decrease with the increase in the number of collusive wormhole attackers. When the number of pairs of collusive wormhole attackers increases from 19 to 25, however, the average detection delay increases with the increase in the number of collusive wormhole attackers. The average detection delay with the presence of 19 pairs of collusive wormhole attackers is 0.749µs and that with 25 pairs of collusive wormhole attackers would increase to 0.789µs.

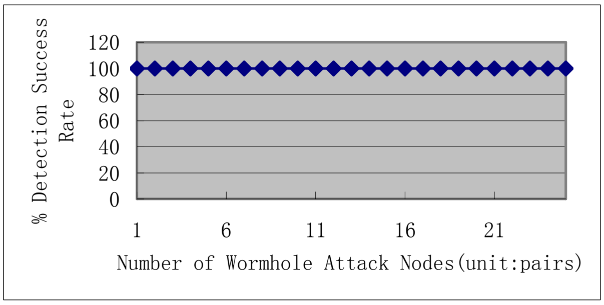


Fig.7. Detection Rate

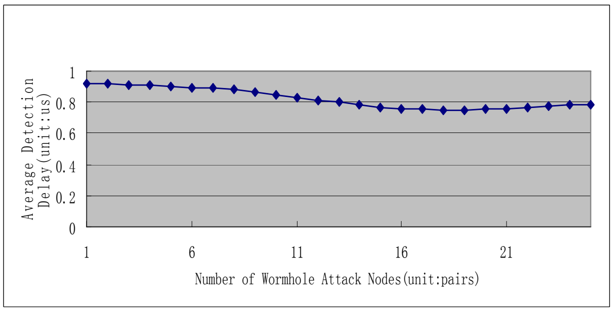


Fig.8. Average Detection Delay

To explain the inconsistency that the simulation results show in the first case, we should notice that nodes in a wireless network send out packets with a broadcast manner. Consequently, there are at least two types of conflicts in transmitting signals. The first type of conflicts occurs between the communication among normal and abnormal nodes and that among watch nodes and the routers while the second type occurs between the watch nodes and the routers, and the two types of conflicts exist in the system at the same time. When the number of collusive wormhole attackers is less than a certain value, the major factor that impacts the detection delay and the average detection delay is the first type of conflicts. When the number of collusive wormhole attackers exceeds a certain value, the major factor that impacts the detection delay and the average detection delay is the second type of conflicts. Therefore, although the detection delay increases with the increase in the number of wormhole attackers, the average detection delay would decrease. For example, communication among the 25 pairs of nodes will conflict with communication between the router and the five watch nodes. When one pair of collusive wormhole attackers is detected and subsequently decommissioned by the router, there remain only 24 pairs of nodes in the system. Therefore, the conflict ratio between the 25 pairs of nodes and the router and the five watch nodes is lower than that between the 24 pairs of node and the router and the five watch nodes. On the other hand, with a large number of wormhole attackers, a large amount of detection information would be sent to the router from the watch nodes, which would result in an increase in the conflict ratio. Therefore, the detection delay and the average detection delay increase accordingly.

In the second case, we simulate the detection delay, the average delay and the detection success rate for different numbers of wormhole attackers as well as for different wait times. The wait time is the length of time that a router waits for the voting results from the watch nodes after it receives the first result. In our simulation, we use seven different values for the wait time set between 0.20μs and 0.26μs with an interval of 0.01μs.

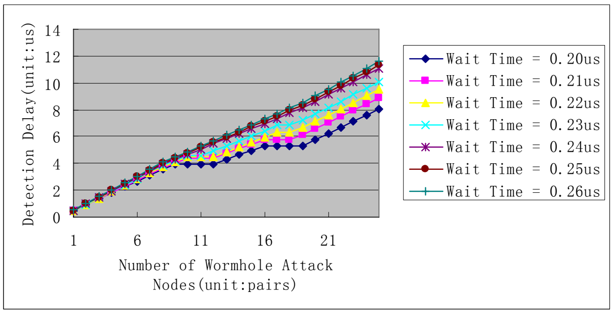


Fig.9. Detection Delay for Different Wait Times

As shown in Fig.9, in which the horizontal axis is the scale of attacking nodes in pairs and the vertical axis is the detection delay, when the wait time changes from 0.24μs to 0.26μs, the detection delay increases with the increase in the number of wormhole attackers while, when the wait time changes from 0.20μs to 0.23μs, the detection delay still increases although not consistently with the increase in the number of wormhole attackers. With the same number of wormhole attackers, the shorter the wait time is, the shorter the detection delay will be. The fact that the differences in detection delay from 1 to 9 pairs of wormhole attackers are less than those from 9 to 25 pairs of wormhole attackers shows that the wait time has less impact on detection delay for smaller numbers of wormhole attackers. However, the wait time would have higher impact on detection delay for larger numbers of wormhole attackers.

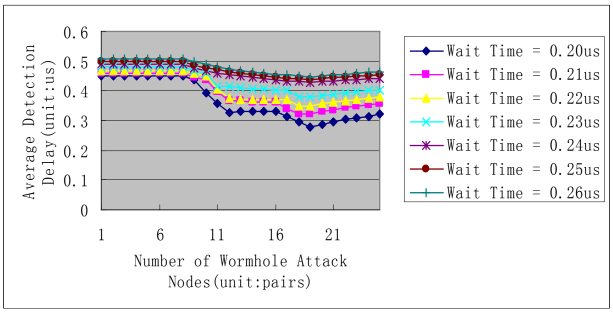


Fig.10. Average Detection Delay for Different Wait Times

Fig.10 shows the average detection delay for different numbers of wormhole attackers as well as for different wait times in which the horizontal axis is the scale of attacking nodes in pairs and the vertical axis is the average detection delay. We can see that when the number of wormhole attackers remains the same, the shorter the wait time is, the shorter the average detection delay will be. When the wait time is set the same, the average detection delays for one to eight pairs of wormhole attackers are the same. However, when the wait time increases from 0.24μs to 0.26μs, the average detection delay would decrease continuously as the number of pairs of wormhole attackers increases from 8 to 19. When the wait time decreases from 0.23μs to 0.20μs, the average detection delay would also decrease as the number of pairs of wormhole attackers increases from 8 to 19 although not uniformly. The average detection delay starts to increase when the number of pairs of wormhole attackers reaches 19. As can be seen in Fig.9, smaller numbers of wormhole attackers would have little impact on the average detection delay for a fixed wait time. Also, from Fig.10, we can see that, when the number of wormhole attackers changes within a certain range, the average detection delay actually decreases with an increase in the number of wormhole attackers. However, when the number of wormhole attackers exceeds a certain value, the average detection delay will increase accordingly. As shown in Fig.11, in which the horizontal axis is the scale of attacking nodes in unit of pairs and the vertical axis is the detection success rate, when the wait time changes from 0.24μs to 0.26μs, the detection success rate remains at 100%. When the wait time increases from 0.20μs to 0.23μs, the detection success rate is 100% when the number of pairs of wormhole attackers is between 1 and 9. Afterwards, the ratio would zigzag when the number of pairs of wormhole changes between 9 and 25 pairs. The lowest such ratio occurs when the wait time is 0.20μs and there are 16 pairs of wormhole attackers.

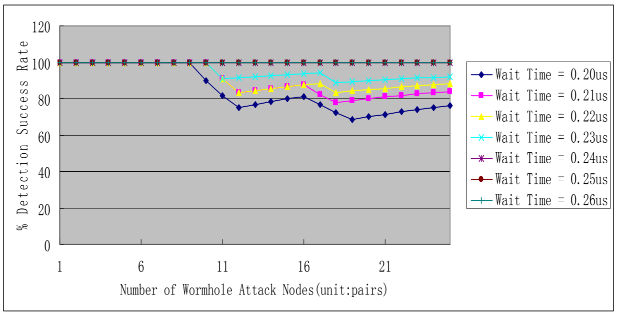


Fig.11. Detection Success Rate for Different Wait Times

Based on our simulation study on the detection delay, the average detection delay and the detection success rate, we can conclude that, in general, the shorter the wait time is, the shorter the detection delay and the average detection delay will be. However, the lower the ratio between the wait time and the communication time between the two nodes with the longest distance in the network and the more the number of wormhole attackers, the lower the detection success rate. Therefore, the wait time is a very important parameter to get the best detection success rate, detection delay and average detection delay. If the detection success rate is the primary goal, our simulation shows that the best result can be achieved when the wait time is set at 0.23μs because, in this case, the detection success rate is 100% and both the detection delay and the average detection delay are close to the best result of all. Other criteria may also be used to choose the best detection results.

6. Conclusion and Future Work

In this paper, we proposed a watch-nodes-based wormhole attack detection scheme. By comparing our scheme with some existing wormhole attack detection approaches through analysis and simulation, we show that our scheme can effectively detect wormhole attacks in wireless mesh networks with the following advantages:

(a) The use of distributed voting scheme to determine wormhole attackers would improve the robustness of wormhole attack detection.

(b) Compared with the schemes in [4-8], our detection scheme doesn't need the special signals required in [4], directional antennas required in [5], loosely or tightly synchronized clocks required in [6-7], and the special equipment to detect and send the ultrasonic frequency required in [8].

(c) Compared with the schemes in [11-12], our scheme doesn't make any assumptions.

(d) In contrast to the scheme in [9-10, 13-14], the detection success rate and detection spending of wormhole attack detection are all improved through theory analysis.

Therefore, our scheme is more practical than previous schemes. Although we have shown qualitatively through analysis and simulation that the wormhole attack detection scheme that we proposed in this paper are more advantageous over the some of the previous schemes in terms of performance and cost, as the future work towards achieving our eventual goal, we plan to run more elaborate experiments to compare the performance of our detection scheme with that of those methods that use special hardware or make some assumption.

Acknowledgements

This work was supported by the National Natural Science Foundation of China under Grant No. 61100150, Natural Science Foundation of Guangdong Province of China under Grant No. S2011040004528 and S2011040003843.

References

1. I.F. Akyildiz and X. Wang, A survey on wireless mesh networks, *IEEE Comm*. Mag. **43**(9) (2005) S23-S30.
2. X. Wang, S. Choi and J.P. Hubaux, Wireless mesh networking: theories, protocols, and systems, *IEEE Wireless Comm.* **13**(2) (2006) 8-9.
3. I. Khalil, S. Bagchi and N.B. Shroff, MOBIWORP: Mitigation of the wormhole attack in mobile multi-hop wireless networks, *Ad Hoc Networks*. **6**(2008)344-362.
4. P. Nagrath, and B. Gupta, Wormhole Attacks in Wireless Ad hoc Networks and their Counter Measurements: A Survey, in *Proc. 3rd Int. Conf. Electronics on Computer Technology*(Kanyakumari, India, 2011), pp.245-250.
5. K. Sanzgiri, B. Dahill, B.N. Levine and C. Shields, etc, A secure routing protocol for ad hoc networks, in *Proc. 10th Int. Conf. IEEE Network Protocols*(Paris, France, 2002), pp.78-87.
6. L.X. Hu and D. Evans, Using directional antennas to prevent wormhole attacks, *(pdf from isoc.org*).
7. Y.C. Hu, A. Perrig and D.B. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, in *Proc. 22nd INFOCOM*(San Francisco, USA, 2003), pp. 1976-1986.
8. Y.C. Hu, A. Perrig and D.B. Johnson, Rushing attacks and defense in wireless ad hoc network routing protocols, in *Proc. ACM Workshop on Wireless. Security*(San Diego, CA, United States, 2003), pp.30-40.
9. H. S. Chiu and K. S. Lui, DelPHI: wormhole detection mechanism for ad hoc wireless networks, in *Proc. Wireless Pervasive Computing*(Phuket, Thailand , 2006), pp.1-6
10. X. Wang and J. Wong, An end-to-end detection of wormhole attack in wireless ad hoc networks, in *Proc. 31st Ann. Int. Conf. Computer Software and Application* (Beijing, China,2007), pp.34-41.
11. L. Lazos, R. Poovendran and C. Meadows, et al, Preventing Wormhole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach, in *Proc. int. Conf. IEEE wireless communications and networking*(New Orleans, LA, United states, 2005), pp.1193-1199.

12. M. Khabbazian, H. Mercier, and V.K.Bhargava, Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks, *IEEE T. on Wireless Comm.* **8**(2)(2009) 736-745.
13. D.ezun Dong, M.IEEE and M.Li, et al, Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks, *IEEE T. Networking.* (2011)1-9.
14. S. Gupta, S.Kar and S Dharmaraja, WHOP: Wormhole Attack Detection Protocol using Hound Packet, in *Proc. Int. Conf. Innovations in Information Technology*(Abu Dhabi, United Arab Emirates, 2011), pp.226-231.
15. C.E. Perkins and E.M. Royer, Ad hoc on-demand distance vector routing, in *Proc. 2nd IEEE Workshop on Mobile Computing Systems and Applications* (New Orleans, US 1990), pp. 90-100.
16. R. Draves, J. Padhye and B. Zill, Routing in multi-radio, multi-hop wireless mesh networks, in *Proc. ACM Ann. Int. Conf. Mobile Computing and Networking*(Philadelphia, PA, United states, 2004), pp.114-128.
17. A. Damle, D. Rajan and S.M. Faccin. Hybrid routing with periodic updates (HRPU) in wireless mesh networks, in *Proc. Wireless Communications and Networking Conference*(San Diego, CA, United States, 2006), pp. 318-324.
18. A. Khalili, J. Katz and W.A. Arbaugh, Toward secure key distribution in truly ad-hoc networks, in *Proc. Symposium on Applications and the Internet* (Orlando, FL, USA 2003), pp. 342-346.
19. Y. Fu, J. He and G. Li, A zone-based distributed key management scheme for wireless mesh networks, in *Proc. 32nd Ann. Int. Conf. Computer Software and Application* (Turku, Finland , 2008), pp. 68-71.
20. Y. Fu, J. He, R. Wang and G. Li, Mutual authentication in wireless mesh networks, in *Proc. 43rd IEEE Int. Conf. on Communications*(Beijing, China, 2008), pp. 2606-2610