Computer Science and Information Systems 11(3):1127–1141 DOI: 10.2298/CSIS130921068W

An Efficient Wormhole Attack Detection Method in Wireless Sensor Networks

Guowei Wu[1], Xiaojie Chen[1], Lin Yao[1], Youngjun Lee[2], and Kangbin Yim[2]

[1] School of Software, Dalian University of Technology,
Dalian, 116620 China
wgwdut@dlut.edu.cn, 747070908@qq.com, yaolin_yl@hotmail.com
[2] Dept. of Information Security Engineering, Soonchunhyang University,
Asan, 336-745 Korea
dog3hk@gmail.com, yim@sch.ac.kr

Abstract. Wireless sensor networks are now widely used in many areas, such as military, environmental, health and commercial applications. In these environments, security issues are extremely important since a successful attack can cause great damage, even threatening human life. However, due to the open nature of wireless communication, WSNs are liable to be threatened by various attacks, especially destructive wormhole attack, in which the network topology is completely destroyed. Existing some solutions to detect wormhole attacks require special hardware or strict synchronized clocks or long processing time. Moreover, some solutions cannot even locate the wormhole. In this paper, a wormhole attack detection method is proposed based on the transmission range that exploits the local neighborhood information check without using extra hardware or clock synchronizations. Extensive simulations are conducted under different mobility models. Simulation results indicate that the proposed method can detect wormhole attacks effectively and efficiently in WSNs.

Keywords: wormhole attacks, wireless sensor network, local neighborhood, network topology.

1. Introduction

Wireless sensor networks (WSNs) consist of a large number of low-cost and resource constraint sensor nodes to perform distributed sensing tasks. Sensor nodes in WSNs collaborate with each other to transmit messages in a multi-hop manner. WSNs are used for various tasks such as surveillance, widespread environmental sampling, security, and health monitoring [23][2]. WSNs are characterized by their infrastructure-less nature, ease of deployment and independence to any pre-existing architecture [24]. Since the open nature of wireless communication, WSNs are prone to be attacked in various ways, such as Denial of Service (DOS) attack, the wormhole attack, the Sybil attack, selective forwarding attack, etc. [22].

In this paper, the wormhole attack [1][5][10] is taken into consideration. The wormhole attack is a kind of tunneling attack, which is very dangerous and damaging to defend against even though the routing information is confidential, authenticated or encrypted [9]. The adversary doesn't need to have knowledge about the routing protocols or compromise the sensor nodes. In wormhole attack, two malicious nodes are connected through a low-latency link, namely wormhole link. A low latency can be realized through a network cable, other kind of wired link technology or just a long-range out-of-band wireless transmission [20]. Once the wormhole link is established, the adversary eavesdrops on packets at one end of the link, tunnels them through the wormhole link and replays the packets at the other end of the link. This makes the sensor nodes around the two ends of the wormhole link seem like neighbor nodes as though they are multi-hops away from each other actually.

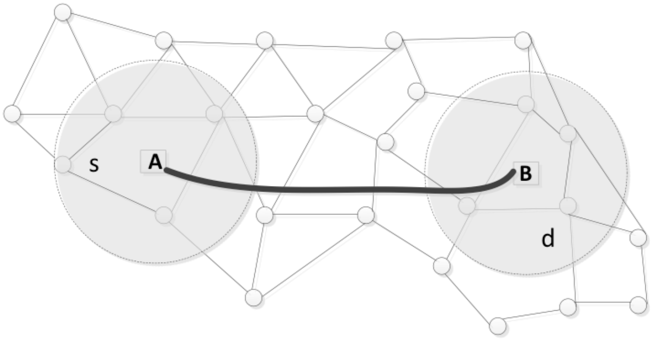

Fig. 1. The Minimum Key Set Route

An example of wormhole attack is given in Fig.1. Node A and B are two malicious nodes placed by the adversary connected via a network cable. So node A and B are the two end points of the wormhole link. Node A receives packets, tunnels them through the wormhole link and replays the packets at node B and vice versa. As a result, nodes in the neighborhood of node A will assume that all nodes in the neighborhood of node B are their neighbors and vice versa. For example, source node s can take a one-hop path to send packets to destination node d via the wormhole link instead of a multi-hop path.

A number of protocols have been proposed to defend against wormhole attacks in wireless networks by adopting synchronized clocks, positioning devices, or directional antennas [19]. In this paper, we introduce novel approaches for detecting wormhole attacks and propose an efficient wormhole detection algorithm, which is named Transmission Range based Method (TRM). With the existence of wormhole, the network topology is destructed and normal routes are misled. Unlike many existing techniques, it does not use any specialized hardware, making it extremely useful for real-world scenarios. Most importantly, however, the algorithm can always prevent wormholes, irrespective of the large transmission range, by checking the local neighborhood information to decide whether the network topology is true or faked, while its efficiency is not affected even by the dynamic topology. We also provide an analytical evaluation of the algorithm's correctness through simulation experiments that demonstrates its efficiency in terms of computation complexity and processing delay. The remainder of this paper is organized as follows. In Section 2, related works are discussed. The wormhole attack detection method is presented in Section 3. The performance of our method is evaluated through simulation experiments in Section 4. At last, we conclude our work in Section 5.

2. Related Works

Wormhole attack is very destructive since the neighborhood information is confused. Any routing protocol relying on network topology information can't work normally. Periodic protocols like Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [6] will malfunction because the routing table information is different from the real network topology due to the wormhole. On-demand protocols like Dynamic Source Routing protocol (DSR) [11] will have false route establishment because the route quest and route reply message in the route discovery stage will contain the wormhole link. So all the routes established by these network routing protocols are attracted to the wormhole and the adversary can launch further attack like selective forwarding attack, black hole attack and etc. What is worse, the wormhole attack is easily deployed to some extent. The adversary has no need to compromise any node in the network and don't need to deal with the cryptographic keys. The integrity, authenticity and confidentiality are still reserved in the existence of wormhole. All the adversary has to do is to place two malicious nodes in good positions in the network and make them receive and send packets.

Because of the reason, the detection of wormhole attack has become an essential issue and various methods have been proposed to detect the wormhole. In [7], Hu et al. introduce the general mechanism of packet leashes to detect wormhole attacks. Two types of leashes are used: geographic leashes and temporal leashes. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. However, to form a leash, each node must know its own location and have synchronized clocks. In [8], the End-to-end Detection of Wormhole Attack (EDWA) is proposed in wireless ad-hoc networks. The source node estimates the minimum hop count to the destination and compares the hop count value received from the reply packet to detect the wormhole. Obviously, each node should measure its geographical location through a GPS. There are some solutions based on the discovery and maintenance of node neighborhood. For instance, LITEWORP [12] uses secure two-hop neighbor discovery and local monitoring of control traffic to detect nodes involved in the wormhole attack. It provides a countermeasure technique that isolates the malicious nodes from the network thereby removing their ability to cause future damage. MobiWorp [13] is further proposed to complement LITEWORP by introducing some location-aware mobile nodes.

Most existing solutions are based on the network topology. Lazos et al. [14] present a graph-based framework to tackle wormhole attacks. Making use of geometric random graphs induced by the communication range constraint of the nodes, the authors present the necessary and sufficient conditions for detecting and defending against wormholes. In [16], the authors propose a wormhole detection approach with only local connectivity information. The algorithm uses only connectivity information to look for forbidden substructures in the connectivity graph. In [4] a distributed connectivity-based wormhole detection method is proposed. Each node collects its k-hop neighborhood and checks whether the boundary of its k-hop neighborhood sub-graph has one or two circles. Its basic idea is based on the observation that the neighborhood that encloses a wormhole link will have two cycles and single cycle otherwise. In [3], authors develop a simple distributed algorithm for wormhole detection in wireless ad hoc and sensor networks, using only the communication graph, and not making unrealistic assumptions. Their algorithm works well in relatively dense and regular networks but results in many false positives in sparse or random networks. In [15], each node locally collects its neighborhood information and reconstructs the neighborhood sub-graph by Multi-Dimensional Scaling (MDS). Potential wormhole nodes are detected by validating the legality of the reconstruction. Then, a refinement process is introduced to filter the suspect nodes and to remove false positives. In the paper [21], wormhole attack detection is proposed based on Round-Trip Time (RTT) between successive nodes and congestion detection mechanism. If the RTT between two successive nodes is higher than the threshold value, a wormhole attack is suspected. If a wormhole is suspected, node's transitory buffer is probed to determine whether the long delay between the nodes is due to wormhole or not, as delays can be caused due to congestion or by queuing delays.

3. Proposed wormhole detection method

Detecting wormholes in WSNs is essential since they can make the routing protocols malfunction. In this paper, a highly efficient wormhole detection method named TRM is developed, which uses the local neighborhood information to calculate the transmission range.

3.1. Network model

In order to prepare for the discussion of the wormhole detection, the network model is presented first. In the network model, a WSN with N sensor nodes is considered, which can be denoted by a directed graph $G = (V, E)$. In this graph, V is the set of vertices indicating the sensor nodes and E is the set of direct edges indicating the wireless links in the graph. The graph takes a Unit Disk Graph (UDG) [17] as its connectivity model. In UDG, each node is modeled as a disk of unit radius in the plane, which indicates the transmission range of a single node. Each node is a neighbor of all nodes located in its disk. Nodes are randomly distributed in the specified area. Two types of nodes are considered in the network: normal nodes and malicious nodes placed by the adversary. Malicious nodes differ from normal nodes in their transmission range, power and calculation capability.

3.2. Adversary model

As described in Section 1, one end of the wormhole eavesdrops on packets, tunnels them through the wormhole and replays them at the other end of the wormhole. The adversary can place many pairs of malicious nodes to deploy wormholes across the whole network. The adversary's goal is to attract as more routes through the wormhole link as possible. And as long as the wormholes are placed carefully, the majority of the network routes can be attracted to the wormhole link. To introduce our wormhole detection method, some assumptions must be made first. These three assumptions following lay a foundation for our wormhole detection method.

1. The wormhole link is long enough so the regions of the two end points don't overlap with each other [17]. For example, A and B in Fig.1 are well separated from each other, i.e., they are multi-hops away.

2. There is some time t when the wormhole is absent, so the sensor nodes have enough time to establish their neighbors.

3. The wormhole is closed [25]. The wormhole attacks are divided into three groups (closed, half open, and open) according to the format of the tunnel and attacker's capability. In this paper, we focus on the closed wormhole attack.

3.3. Principle and analysis

In order to explain our wormhole detection method, its principle analysis is presented first. In the network, each node pair can establish a link because their distance is less than or equal to the transmission range r. For any node m, the neighbor set of m is denoted by $N(m)$. For example, if a node B can receive packets from node A with one hop, node B is a neighbor of node A and meets $B \in N(A)$. The principle is to check the neighbor topology by using the geometric relationship of nodes' locations under the constraint of the communication range of the two involved sensor nodes.

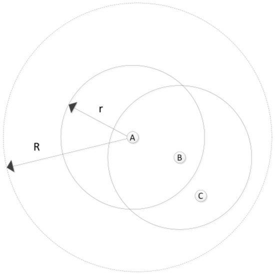

Fig. 2. Neighbor Nodes without Wormhole

The principle is illustrated in Fig.2 by studying the geometric relationship among nodes in the network without wormholes. Node A and B are two neighbor nodes to be checked. Node C meets $C \in N(B)$ but $C \notin N(A)$. The transmission range of node A, B and C is r. When node A adjusts its transmission range to $R = 2r$ in Fig.2, all the neighbors of node C become neighbors of node A. So it meets that $C \in N(A)$ and $N(B)$ $\subseteq N(A)$.

The geometric relationship among nodes in the network under wormhole attack is totally different as shown in Fig.3. Node A and B are two neighbor nodes which are connected via the wormhole link. Node C and D both meet that C, $D \in N(B)$. Node A, B and D are mutually neighbors due to the wormhole link as described in Section 1.

Node B and D lay in node A's neighbor list due to the wormhole link. Node C is far from the wormhole end point and thus free from wormhole attack. The transmission range of these four nodes is r at first. Then the transmission range of node A is expanded to $R = 2r$. Node D is node A's neighbor connected by the wormhole link. However, since node A and B are multi-hops away from each other, node C is still not a neighbor of node A even though the radius of node A is doubled. After increasing the radius of

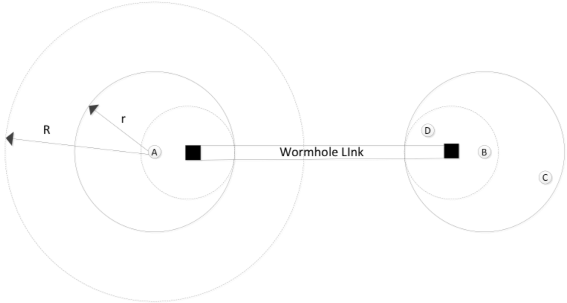

Fig. 3. Neighbor Nodes with Wormhole

node A, one of node B's neighbors is still not a neighbor of node A. So it meets that $D \in N(A)$ and $C \notin N(A)$. As a result, not all the neighbors of node B turn into neighbors of node A, which meets that $N(B) \not\subset N(A)$. And this can be used to check whether there exists a wormhole between two sensor nodes.

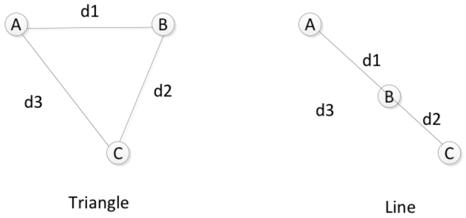

Fig. 4. Neighbor Nodes with Wormhole

Then we make some calculations to prove that the above principle is feasible. As shown in Fig.4, the distance between A and B is denoted by $d1$; the distance between B and C is denoted by $d2$, the distance between A and C is denoted by $d3$. There are two cases of node-relative position: triangle and line. According to the neighbor relationship described above and their transmission range r, it is obvious that $d1 \leq r$ and $d2 \leq r$. In the triangle case, it can be seen that $d3 < d1 + d2 \leq 2r$. In the line case, it can be seen that $d3 = d1 + d2 \leq 2r$. So we can get $d3 \leq 2r$. Since the radius of node A is $R = 2r$, node C is within node A's transmission range. And it meets that $d3 \leq 2r$ for $\forall C \in N(B)$. Therefore, we can get the formula $N(B) \subseteq N(A)$. When the network is under the wormhole attack, the actual distance of the two neighbor nodes A and B may be very far away. It may meet that $d3 > 2r$ for $\forall C \in N(B)$. Node C is still not a neighbor of node A after expanding its radius to $2r$. But due to the wormhole, some node like D in Fig.3 may still be a neighbor of node A, which means that $C \notin N(A)$, $\exists C \in N(B)$. Therefore, we can get $N(B) \not\subset N(A)$. Now we can get the conclusion that:

1. When there is a wormhole and the transmission range of node A is R, there must exist a node $C \in N(B)$ but $C \notin N(A)$.

2. When there is no wormhole and the transmission range of node A is R, all nodes $C \in N(B)$ meet $C \in N(A)$.

3.4. Detection procedure

Based on the principle of detecting wormholes, detailed detection procedure will be presented in this section. Two neighbor nodes such as node A and B are to be checked which has its neighbor list $N(A)$ and $N(B)$ separately. The neighbor list information can be exchanged between neighbors through periodic beacon messages. After nodes A and B exchange the neighbor list information, the detection procedure will begin. Node A notifies all its neighbors in $N(A)$ through its beacon messages that will increase its transmission radius. The neighbor nodes receiving this notification will not change their transmission radius in the next beacon time. Then node A increases its transmission range to $2r$ and updates its neighbor list $N(A)$. Finally, node A compares $N(A)$ and $N(B)$:

1. If the neighbor lists $N(A)$ and $N(B)$ satisfy $N(B) \subseteq N(A)$, then there is no wormhole link between node A and B.
2. If the neighbor lists $N(A)$ and $N(B)$ satisfy $N(B) \not\subset N(A)$, then there is a wormhole link between node A and B.

The node A and B in Fig.4 is used as two tested nodes to describe the main wormhole detection procedure of TRM algorithm. The flow of wormhole detection is shown in the Fig.5. In our model, every node has a current list of its neighbors. Moreover, the neighbor list is regularly updated. Each node can request its neighbors to get their neighbor lists by transmitting a beacon message to its neighbors. Finally, each node can know one-hop neighbor information and two-hop neighbors as well. After a node starts the wormhole detection process, the node first broadcasts a beacon message including a packet to notify its neighbors, which will increase the transmission range. All nodes receiving this notification will not change their transmission range in the next beacon period. After sending the message, the transmission range of node A is increased to $2r$. If the neighbors of node B are still neighbors of node A, node A will search from the neighbor list in the next beacon period. If B's one neighbor, node C, is still not a neighbor of A, a wormhole will be detected. From Fig.5, we can see that communication links between nodes are required to establish in the primary stage. Then a node adopts the neighbor discovery mechanism to establish the link with other node. During the discovery stage, every node will send its own neighbor list to its neighbors by sending beacon frames. By this way, each node can get its neighbor information within two hops. Finally, the network topology will be established. The beacon information will be transmitted at regular intervals. After changing the radius, a test node will update its neighbor node list in the next beacon time. By comparing its current neighbor list with the previous list, a test node can find the existence of false topology that does not exist in a normal network. Then the wormhole is detected.

In some wormhole detection methods based on statistical analysis, the algorithm calculates the link frequency statistics for some time to determine the presence of a wormhole. This method must work after the routes are established and transmission is observed for some time. TRM algorithm can begin execution before the route establishment phase causing a large number of packets to be transmitted to the base station. In this way, wormholes can be detected before the network traffic to be sent. Then the administrator of the network can eliminate the bad effects of wormholes. The description of the algorithm is shown in Table 1.

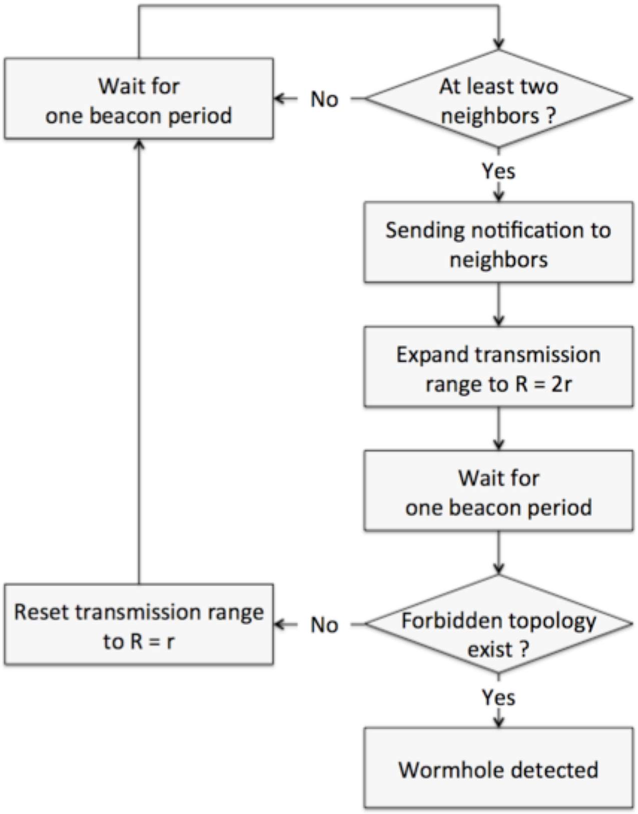

Fig. 5. Wormhole Detection Process

3.5. Complexity and feasibility analysis

In order to demonstrate that our algorithm is a lightweight one, the complexity of the wormhole detection is analyzed from the aspects of time complexity and space complexity. The time complexity is the time consumed by executing the algorithm. In order to obtain the time complexity, the consumption time of detecting a pair of wormhole nodes is calculated firstly. Suppose there is a wormhole between node A and node B. The algorithm needs to find a node in $N(B)$ but not in the neighbor list of node A. Since the number of neighbors is a constant c, the time complexity of wormhole detection is $O(C)$, i.e., $O(1)$. Secondly, the consumption time of detecting all pairs of wormhole nodes is calculated. At this time, every node and its neighbors should be checked. When the num-

Table 1. Transmission Range based Method to Detect Wormholes

```
Line  Description
1     Given: Network $N$ with node radius $r$, wormhole number $c = 0$
2     While check every node $m$ in $N$ do
3         Expand radius of $m$ to $R$ = $2r$
4         For each node $n$ in $N(m)$ do
5             If there exists once $d \in N(n)$ and $d \notin N(m)$
6             then $c + 1$
7         end for
8     end while
```

ber of nodes is limited such as n and the number of its neighbors is c, the time complexity of TRM is $O(cn)$, i.e., $O(n)$.

The space complexity is defined as the storage space. In the TRM, the space complexity is influenced by the number of nodes in the network. According to our algorithm, except the neighbor list, no extra data structures are required to store in TRM. Suppose there is a wormhole between node A and node B. Because only neighbor information is stored, the space complexity is obviously $O(1)$. When all the n nodes in the network are checked, the space complexity is $O(n)$. The feasibility of the algorithm is that every node must have its neighbor nodes. Suppose n nodes are distributed in a square region with the side length d and the transmission radius r. According to TRM algorithm, the number of nodes in each row is $\sqrt{n}$ lying on a line of length d. The distance between two neighbor nodes is $\frac{d}{\sqrt{n}-1}$. Every node can communicate with each other as long as the distance between neighbor nodes is less than the node's transmission radius. So it should be met $\frac{d}{\sqrt{n}-1} \leq r$, which is easy to implement. However, there may be some particularly isolated nodes, which doesn't make sense for the wormhole attacker. In summary, the feasibility of the proposed algorithm has been verified.

4. Simulation analysis

In order to verify the performance of our wormhole detection method, various experiments have been carried out. In the simulated system scenario, the wireless sensor network consists of 100 sensor nodes. First, we show the great damage of wormhole attack to the network. Among the entire nodes, ten source nodes and ten destination nodes are selected randomly. Then routes are established between those source and destination nodes. The routes are set up using the basic Shortest Path Algorithm for simplicity. Then it can be seen in the simulation as shown in Fig.5 that the routes are badly corrupted due to the existence of wormhole. The routes are broken since the routes cross the wormhole end points. In this way, the traffic can be attracted to the wormhole link and the adversary can mount further attack like sinkhole attack or just eavesdrop on the information:

In the experiments, the nodes are distributed randomly in 5x5, 10x10, 15x15, and 20x20 square separately. The node transmission range is 2 meters and nodes are distributed randomly, which forms a unit disk graph for universality. The wormholes are also placed in a random way.

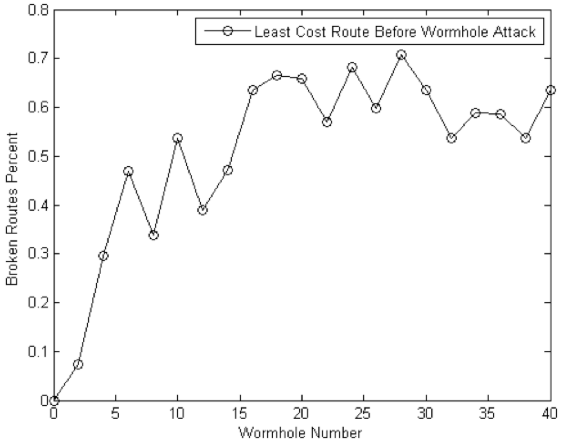

Fig. 6. The Broken Routes Percent by Wormholes

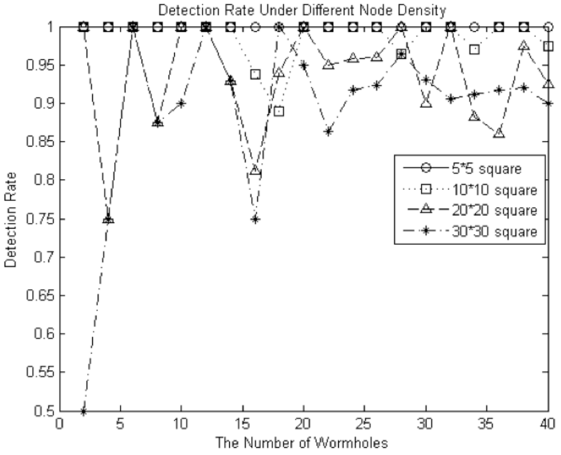

Fig. 7. Simulation Results of Wormhole Detection Rate

In Fig.7, the wormhole detection rate is calculated as the number of wormholes increases from 2 to 40. The detection rate is also compared under different system scenario in which the networks with the same number of wormholes have different node densities. Network distribution area 5x5 corresponds to the greatest node density. And the node density decreases as the network distribution area increases to 10x10, 20x20, and 30x30. It can be seen from Fig.6 that the bigger the node density, the higher the detection rate. The detection rate is perfectly 100% when the side length of the network is square since it's easy to detect wormholes when a node has many neighbors. A node's detection failure can be complemented by another neighbor node. The detection rate is not 100% because some neighbor nodes around the wormhole can't detect the wormhole link. The detection may fail because the node has nearly no neighbor to check the local neighborhood information using our method. This situation, which is of low probability in practical application, happens in very spare network or some isolated sensor nodes. Moreover, there is no worth for the adversary to attack such isolated sensor nodes because little traffic will be caused to use by the attack.

To compare the performance of TRM with other wormhole detection method, two other kinds of detection methods are simulated in the experiments. The Transmission Time based Mechanism (TTM) [13] detects wormhole attacks during the route setup procedure by computing transmission time between every two successive nodes along the established path. The Four Way Handshaking algorithm (FWH) [18] uses a simple four-way handshaking messages to exchange. It can be seen from Fig.8 when the wormhole length is smaller than 10, our method can achieve the highest detection rate. When the wormhole length is 2, the transmission time of two neighbor nodes created by wormhole link is not too long to be detected. The FWH algorithm is also affected by the time. Our TRM has nothing to do with the time and detect the wormholes according to the geometric relationship of nodes as described in section 3. So our TRM can have high detection rate all the time in different network scenarios.

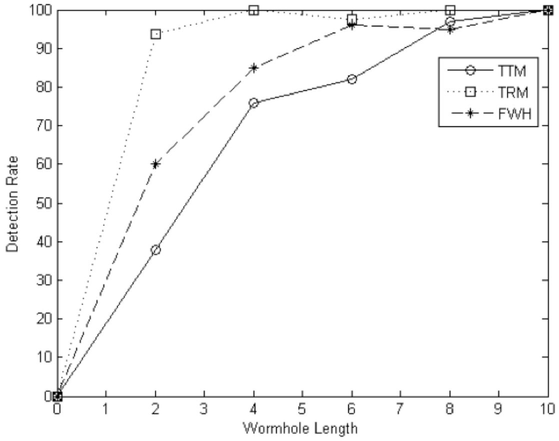

Fig. 8. Detection Rate of Different Detection Methods

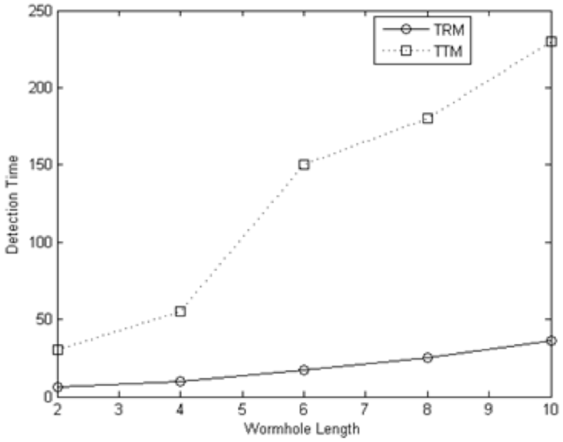

Fig. 9. Detection Time Comparison

In Fig.9, the detection time of TRM and TTM algorithm is compared. The actual average transmission time between one-hop nodes is ten milliseconds. However in TTM, the RTT between two nodes connected through the wormhole link is calculated since the two endpoints of wormholes are far away. In TTM, the detection result is obtained through calculating transmission time. So the detection time is longer when the wormholes are far away. It can be seen in Fig.9 that the detection time increases greatly as the length between wormholes increases. In TRM, however, the wormholes are detected by checking the false neighbor topology. The wormholes can be found out by calculating the geometrical relationship between nodes. In this way, the computation is of low complexity and more quick. At the same time, since the node's neighbor list has nothing to do with the length of wormholes, the wormhole length doesn't affect the detection time. So the detection time doesn't increase greatly as the length of wormhole increases.

5. Conclusions

Wormhole attack in WSNs has been drawing more and more attention since it can disrupt normal network routing protocols. However, in previous work of wormhole detection, most of them need either extra hardware or clock synchronizations and suffer from high complexity. In this paper, an efficient wormhole detection method is proposed, which is based only on local neighborhood information. Through judging the node's position, we can determine whether the node is in the local network topology affected by the wormhole link.

In the detection procedure, the neighborhood information of each node is updated and exchanged periodically between neighbors along with the increment of the transmission range. A local topology that has a wormhole link finally reports a mismatch of the neighborhood information between nodes. According to the analysis, the algorithm gives $O(n)$ for both of the time complexity and the space complexity.

The simulation results also demonstrate that our wormhole detection method can achieve a high wormhole detection rate. For the simulation, we organized a wireless sensor network with 100 sensor nodes and deployed up to 40 wormholes in it with different density. In case of a denser network with more wormholes, the detection rate was getting higher. In the performance comparison with other detection methods, the proposed TRM gave much bigger detection rate for wormholes with shorter lengths.

In the future, the proposed algorithm is required to enhance the performance for coarse networks and consider the separated nodes as well as optimizing the procedure even for dense networks. Performance of the proposed TRM algorithm also should be evaluated for various network conditions such as the case that the network has frequent link breaks between nodes as a common problem in a practical environment.

Acknowledgments. This research was sponsored in part by the Fundamental Research Funds for the Central Universities (No. DUT13JS10). This work was also supported in part by the Soonchunhyang University Research Fund.

References

1. Agrawal, S., Jain, S., Sharma, S.: A survey of routing attacks and security measures in mobile ad-hoc networks. Journal of Computing 03(01), 41–48 (2011)
2. Akyildiz, W., Sankarasubramaniam, Y., Cayirci, E.: Wireless sensor networks: a survey. Computer Networks 38(04), 393–422 (2002)
3. Ban, X., Sarkar, R., Gao, J.: Local connectivity tests to identify wormholes in wireless networks. In: Proceedings of the 12th ACM International Symposium on Mobile Ad Hoc Networking and Computing. pp. 65–78 (2011)
4. Dong, D., Li, M., Liu, Y., Liao, X.: Wormcircle: connectivity-based wormhole detection in wireless ad hoc and sensor networks. In: Proceedings of the 15th International Conference on Parallel and Distributed Systems. pp. 72–79 (2009)
5. Hu, Y.: Wormhole attacks in wireless networks. IEEE Journal on Selected Areas in Communications 24(02), 370–380 (2006)
6. Hu, Y., Johnson, D., Perrig, A.: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks 01(01), 175–192 (2003)
7. Hu, Y., Perrig, A., Johnson, D.: Packet leashes: A defense against wormhole attacks in wireless networks. In: Proceedings of 22nd Annual Joint Conference of the IEEE Computer and Communications. pp. 1976–1986 (2003)
8. Hu, Y., Perrig, A., Johnson, D.: An end-to-end detection of wormhole attack in wireless ad-hoc networks. In: Proceedings of 31st Annual International Computer Software and Applications Conference. pp. 39–48 (2007)
9. Jhaveri, R., Patel, D., Jatin, D., Parmar, D., Shah, B.: Manet routing protocols and wormhole attack against aodv. International Journal of Computer Science and Network Security 10(04), 12–18 (2010)
10. Jhaveri, R., Patel, S., Jinwala, D.: Dos attacks in mobile ad hoc networks: A survey. In: Proceedings of Advanced Computing & Communication Technologies. pp. 535–541 (2012)
11. Johnson, D., Maltz, D., Broch, J.: Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks. In: Perkins, C. (ed.) Ad Hoc Networks, pp. 139–172. Addison-Wesley Longman Publishing Co., Inc. Boston, MA, USA (2001)
12. Khalil, I., Bagchi, S., Shroff, N.: Liteworp: a lightweight countermeasure for the wormhole attack in multihop wireless networks. In: Proceedings of the International Conference on Dependable Systems and Networks. pp. 612–621 (2005)
13. Khalil, I., Bagchi, S., Shroff, N.: Mobiworp: mitigation of the wormhole attack in mobile multihop wireless networks. Ad Hoc Networks 06(03), 344–362 (2008)

14. Lazos, L., Poovendran, R., Meadows, C., C., S., L., C.: Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach. In: Proceedings of the IEEE Wireless Communications and Networking Conference, Broadband Wirelss for the MassesReady for Take-off. pp. 1193–1199 (2005)
15. Lu, X., Dong, D., Liao, X.: Mds-detection using local topology in wireless sensor networks. International Journal of Distributed Sensor Networks 2012, 1–9 (2012)
16. Maheshwari, R., Gao, J., Das, S.: Detecting wormhole attacks in wireless networks using connectivity information. In: Proceedings of the 26th IEEE International Conference on Computer Communications. pp. 107–115 (2007)
17. Maheshwari, R., Gao, J., Das, S.: Detecting wormhole attacks in wireless networks using connectivity information. In: Proceedings of 26th IEEE International Conference on Computer Communications. pp. 107–115 (2007)
18. Nat-Abdesselam, F., Bensaou, B., Yoo, J.: Detecting and avoiding wormhole attacks in optimized link state routing protocol. In: Proceedings of IEEE Wireless Communications and Networking Conference. pp. 3117–3122 (2007)
19. Patel, K., Manoranjitham, T.: Detection of wormhole attack in wireless sensor network. International Journal of Engineering Research & Technology 02(05), 366–369 (2013)
20. Poovendran, R., Lazos, L.: A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. Wireless Networks 13(01), 27–59 (2007)
21. Sebastian, M., Kumar, A.: A novel solution for discriminating wormhole attacks in manets from congested traffic using rtt and transitory buffer. I. J. Computer Network and Information Security 05(08), 28–38 (2013)
22. Sharma, K., Ghose, M.: Wireless sensor networks: an overview on its security threats. IJCA, Special Issue on Mobile Ad-hoc Networks pp. 42–45 (2010)
23. Sohrabi, K., Gao, J., Ailawadhi, V., Pottie, G.: Protocols for self-organization of a wireless sensor network. IEEE Personal Communications 07(05), 16–27 (2000)
24. Triki, B., Rekhis, S., Boudriga, A.: A novel secure and multipath routing algorithm in wireless sensor networks. In: Proceedings of 2010 International Conference on Data Communication Networking. pp. 1–10 (2010)
25. Wang, W., Bhargava, B., Lu, Y., Wu, X.: Defending against wormhole attacks in mobile ad hoc networks. Wireless Communications and Mobile Computing 06(04), 483–503 (2006)

Guowei Wu received B.E. and Ph.D. degrees from Harbin Engineering University, China, in 1996 and 2003, respectively. He was a Research Fellow at INSA of Lyon, France, from September 2008 to March 2010. He has been an Associate Professor in School of Software, Dalian University of Technology (DUT), China, since 2003. Dr. WU has authored three books and over 20 scientific papers. His research interests include embedded real-time system, cyber-physical systems (CPS), and wireless sensor networks.

Xiaojie Chen received B.E. and Master degrees from Dalian University of Technology, China, in 2010 and 2013, respectively. He is an engineer in China Unicom. His research interests include embedded real-time system, cyber-physical systems (CPS), and wireless sensor networks.

Yao Lin received B.E. and Master degrees from Harbin Engineering University, China, in 1998 and 2001, respectively, and received Ph.D. degree from Dalian University of Technology, China in 2011. She has been a lecturer in School of Software, Dalian University of

Technology (DUT), China, since 2004. She has co-authored one book and over ten scientific papers. Her research interests include pervasive computing, cyber-physical systems (CPS), and wireless sensor networks.

Youngjun Lee received B.E. degree from Dept. of Information Security Engineering, Soonchunhyang University, Korea, in 2013. He is currently pursuing his Master degree. His research interests include malware analysis, secure hardware design, and CPS security and testing.

Kangbin Yim received his B.S., M.S., and Ph.D. from Ajou University, Korea in 1992, 1994 and 2001, respectively. He is currently a Full Professor in the Department of Information Security Engineering and the founding director of the R&BD Center for Security and Safety Industries (SSI) in Soonchunhyang University. He has served as the executive board member of Korea Institute of Information Security and Cryptology, Korean Society for Internet Information and The Institute of Electronics Engineers of Korea. He also has served as editor of the journals such as JIT, MIS, IJCM, JCPS, JISIS and JoWUA. His research interests include vulnerability assessment, malware analysis, embedded systems security, and software-hardware co-design and evaluation. Related to these topics, he has worked on more than fifty research projects and published more than a hundred research papers.

Received: September 21, 2013; Accepted: February 27, 2014.