Lai *EURASIP Journal on Wireless Communications and Networking* (2016) 2016:274
DOI 10.1186/s13638-016-0776-0

EURASIP Journal on Wireless Communications and Networking

RESEARCH Open Access

Detection of wormhole attacks on IPv6 mobility-based wireless sensor network

Gu-Hsin Lai

Abstract

New communication networks are composed of multiple heterogeneous types of networks including Internet, mobile networks, and sensor networks. Wireless sensor networks have been applied to various businesses and industries since the last decade. Most sensors have the ability of communication and the requirement of low power consumption. 6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks) plays an important role in this convergence of heterogeneous technologies, which allows sensors to transmit information using IPv6 stack. Sensors perform critical tasks and become targets of attacks.

Wormhole attack is one of the most common attacks to sensor networks, threatening the network availability by dropping data or disturbing routing paths. RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) is a standard routing protocol commonly used in sensor networks. This study proposes a RPL-based wormhole detection mechanism. The rank of a node-defined RPL is adopted to measure the distance. The proposed detection method discovers malicious wormhole nodes if unreasonable rank values are identified. The experimental results show that the proposed detection method can identify wormholes effectively under various wireless sensor networks.

Keywords: Wormhole attack, Sensor networks, IPv6, RPL, Mobility

1 Introduction

Wireless sensor networks with IoT (Internet of Things) have been applied to many applications such as ecosystem monitoring, disaster watch, building automation, health monitoring, object tracking, and plant control. The sensor data carry out important information such as vital signals or disaster alerts; transmission failure or error data might cause system malfunction or serious incidents. The existing Internet protocol IPv4 could only provide about 4 billion public IP addresses; the limited IP spaces constrain the growth of wireless sensor network applications.

IPv6 is the latest version of Internet Protocol, a communication protocol that provides an identification and location system for the network devices in the new type of communication networks. Many sensors and tiny devices facilitate IPv6 to provide connectivity.

In wireless sensor networks, the network topology could change due to a weak mobility (new nodes join the network or hardware failure of existing devices) or strong mobility (physical movement of nodes) [1]. However, wormhole attack could also make topology change in wireless sensor network. Therefore, building a security mobility management mechanism is very important for wireless sensor networks.

A typical architecture of wireless sensor networks is illustrated in Fig. 1, where all the sensors transmit data to the root. Wormhole attack is one of the most common attacks in sensor networks. Figure 2 illustrates an example of wormhole where the two malicious nodes, M1 and M2, form a wormhole tunnel T1 through which redirects the transmissions. Some routing paths going through the wormhole tunnel might be shorter than the normal multi-hop routes [2–4]. Therefore, wormhole attacks may change the original routing paths, and the wormhole nodes may eavesdrop or discards the data going through the wormhole tunnel. Furthermore, the two wormhole end nodes consume more power energy than others. Once their resources are exhausted, the sensor network might not operate properly. Wormhole attacks compromise the network availability and data privacy and may cause serious security problem in sensor networks.

According to the wireless sensor network architecture, each node usually is only aware of its neighbor nodes

Correspondence: Lgx4@ulive.pccu.edu.tw
Department of Information Management, Chinese Culture University, Taipei, Taiwan

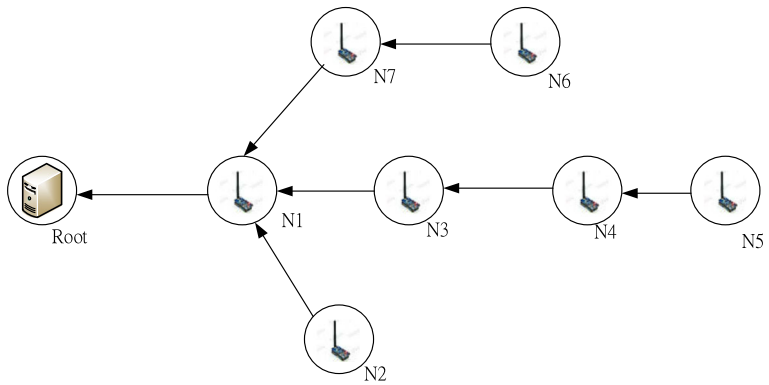

Fig. 1 An example of wireless sensor network topology

and possesses limited resources. Centralized and sophisticated detection methods might not be feasible because sensor nodes only have limited computing power. On the other hand, equipping with additional hardware for all sensor nodes is costly. Hence, detection systems requiring additional hardware might not be practical.

Based on the above constraints, this study proposes a distributed detection method by applying the standard routing protocol IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL), available in all the sensor nodes to identify wormhole attacks without additional hardware. RPL [5, 6] is a standard routing protocol for wireless sensor networks [7]. However, RPL is vulnerable to wormhole attacks [8]. The proposed detection method applies the rank information from RPL to estimate the relative distance to the root node; the rank value will be compared with that of the neighbors; if the discrepancy exceeds a threshold value, it signals an anomaly where a wormhole might exist.

The main contributions of this paper are as follows:

1. The proposed approach builds a security mobility management mechanism in wireless sensor network.
2. The proposed approach does not need any extra hardware or special powerful nodes which were required by the previous work [2, 9, 10].
3. The proposed mechanism is based on an existing protocol, the proposed mechanism. It could be implemented on existing wireless sensor network hardware.
4. The proposed mechanism is distributed; no centralized analysis is needed. It means no additional communication is needed.
5. The proposed system needs only few computing resource, the lifetime of battery of devices would not be affected.

2 Related work

In this paper, we propose a wormhole detection mechanism based on RPL routing protocol. In this section, prior works about detection of wormhole attack are reviewed in Section 2.1. In Section 2.2, we investigate the vulnerability

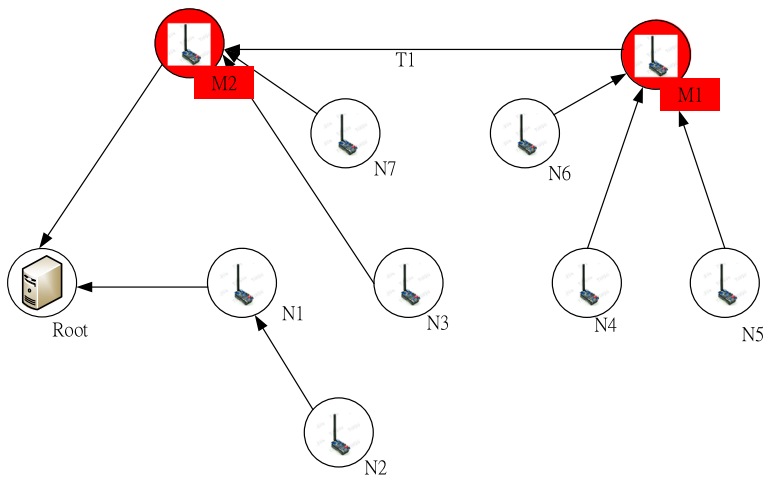

Fig. 2 An example of wormhole attack

of RPL routing protocol, and some RPL-based wormhole detection approaches are reviewed.

2.1 Prior work of detecting wormhole attacks

Wormhole attacks in wireless sensor networks were introduced by Sanzgiri [11], Papadimitratos [12], and Hu [2, 3, 8]. In a wormhole attack, a wormhole tunnel is constructed by two malicious nodes. Malicious nodes will "tunnel" their received routing information to another point in the network and then replay them. Once the wormhole tunnel is constructed, malicious nodes could eavesdrop on traffic from their neighbor nodes, drop packets or to perform man-in-the-middle attacks [4].

Hu et al. proposed two types of packet leashes: geographic leashes and temporal leashes to prevent wormhole attacks [4]. Leashes are designed to protect against wormholes over a single hop wireless transmission. Geographical leash will ignore any messages from unreasonable distance, and temporal leash will ignore any packets with unreasonable lifetime [4]. However, to construct packet leashes, all nodes must have synchronized clocks and their own position. It is impractical in most wireless sensor network environment.

A lightweight wormhole detection approach called LITEWORP was proposed by Khalil et al. [9]. In LITEWORP, each node builds its two-hop neighbor list. By monitoring all control traffic of neighbor, LITEWORP could identify and isolate malicious node. However, monitoring and extracting every neighbors' traffic result in extra overload. Moreover, it is not always possible to find guard node for particular link. The proposed system is not suitable for nodes with limited battery capacity. Khalil et al. also proposed a routing protocol called MobiWorp to detect and isolate wormhole attack [13]. MobiWorp rely on a secure central authority (CA) for global tracking of node positions. MobiWorp also deployed a special node called guard node to maintain a black list and monitor network traffic. However, CA and guard node are impractical in some wireless sensor network applications.

Choi et al. proposed a Wormhole Attack Prevention (WAP) algorithm which measured the round-trip time (RTTs) between neighbors, identifying that two neighbors which are not within each other's communication range are supposed to be suffering from wormhole attack [14]. But, WAP algorithm could only be suitable for wireless sensor network applications with a lot of nodes. WAP algorithm could not detect false positive alarm while affected nodes only have few neighbor nodes due to lack of enough neighbor nodes' information.

2.2 IPv6 Routing Protocol for Low-Power and Lossy Networks

The RPL became a standard routing protocol for wireless sensor networks [6]. RPL is primarily designed for 6LoWPAN (IPv6 over Low-powered Wireless Personal Area Networks). Because IPv6 provide almost unlimited IP space, it is suitable for wireless sensor network applications for point-to-point communication or point-to-multicast communication among tiny nodes. 6LoWPAN network is a wireless sensor network which supports IPv6. 6LoWPAN uses IPv6 as Internet layer and IEEE 802.15.4 as data link and physical layer [7]. Differ from typical stand-alone wireless sensor networks, devices of wireless sensor network applications only have limited resources, and these devices are accessible from anywhere. Hence, wireless sensor network applications are exposed to threats both from the Internet and from within the network. RPL protocol provides new ICMPv6 control messages to exchange routing graph information. RPL protocol uses DIO (DODAG Information Objects) messages to advertise information for building RPL DODAG, and DAO (Destination Advertisement Object) messages are used for supporting downward traffic toward leaf nodes. Nodes send DIO messages periodically, once nodes receive a DIO message, they might use the information to join a new network or update their routing table [6]. Now, the most popular wireless sensor network standard like ZigBee IP supports RPL [15, 16]. ZigBee is a low-cost, low-power, wireless sensor network standard which enable tiny and smart devices to work together for wireless sensor network applications [15]. Therefore, the proposed system will be based on RPL routing protocol. RPL is also vulnerable to wormhole attack. Attackers could send fake ICMPv6 routing packets to construct wormhole tunnel. Khan et al. proposed a Merkle-tree-based authentication to prevent wormhole attack [17]. An added authentication mechanism while maintaining parents within a DODAG can be used for avoiding promotion of routes encompassing malicious nodes sending replay attacks around the surrounding region. However, building Merkle tree needs additional communication and computation resources.

Sensor network applications make use of tiny devices which have limited resources and electricity power. Therefore, additional hardware requirement or complicated detection algorithm is not suitable for detecting wormhole attacks in such environments. In this article, the proposed system is based on RPL without extra hardware or complicated detection algorithm.

3 Proposed system

In this paper, an intrusion detection system to identify wormhole attacks is proposed. To avoid routing loops, RPL calculates the number of hops from a node to the root. "Rank" in RPL represents the position of a node; it increases when the node moves away from the root [5]. The geographic leashes [2] inspired us to use nodes' location to detect wormhole attacks. Rank is informative

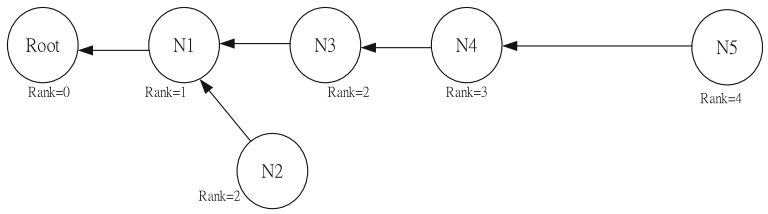

Fig. 3 An example of RPL network topology

to estimate the distance to root node. Therefore, the proposed system applies the rank value to identify suspicious rank values from DIO messages.

To illustrate the idea of the proposed detection method, Figs. 3 and 4 give an example of how rank values are changed before and after the wormhole tunnel is established. Figure 3 shows the rank value of each node defined by RPL. The root node has the rank of 0, and the rank values represent the number of hops to the root plus one. Figure 4 shows the change of the rank values after the malicious nodes, *M1* and *M2*, are deployed and form a wormhole tunnel. When the two nodes are inserted in the network, to update the routing table, the root node sends DIO message to node *N1* and *M1*; the rank of node *N1* and *M1* is 1. The DIO message will be transmitted accordingly to the following neighbor nodes to update the rank values. It can be seen that the rank value provided by RPL is informative for estimating the distance to the root.

The proposed detection method adopts the rank value to identify wormholes. Figure 5 illustrates the framework of proposed system. The RPL specification defines four types of control messages for topology maintenance and information exchange. In this paper, DIO messages are first collected by proposed system, and then rank value is extracted from DIO messages. Once DIO messages are extracted, the proposed system will detect if the DIO message is from malicious node or not.

The detection algorithm is outlined in Fig. 6. As this is a distributed algorithm, each node in the sensor networks examines the features extracted from the packet header to see if a wormhole exists in the network. To shorten the detection process, the malicious nodes are stored in a black list once they have been identified, which will not be examined by the detection system repeatedly. The rank value from the IPv6 header of an incoming traffic is inspected to see if the rank increases gradually or it is different from its neighbors significantly. If the ICMPv6 message is considered as benign, the receivers will update their neighbor table and routing table accordingly.

This study assumes that when a wireless sensor network exists, no malicious nodes when it is deployed in the beginning. The correct routing table of each node in the newly deployed network will be established before wormhole attack is issued. The proposed detection method defines the following two attributes to discover abnormal DIO messages: *Rank_Threshold* and *Rank_Diff*.

Rank_Threshold is defined as the difference of the rank values between its parent and the node itself as formulated in Eq. (1); the attribute value is obtained when the routing table is constructed or updated. For the example illustrated in Fig. 3, *Rank_Threshold* of node *N5* is 1 because its rank is 5; that of its parent *N4* is 4. Therefore, *Rank_Threshold* of node *N5* is $|3 - 4| = 1$.

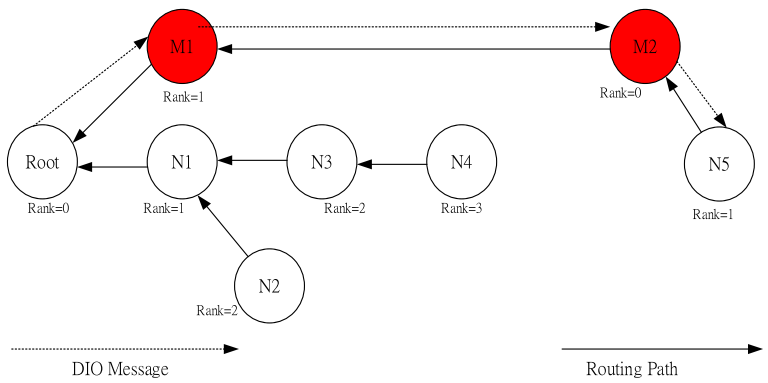

Fig. 4 An example of wormhole attack in RPL network

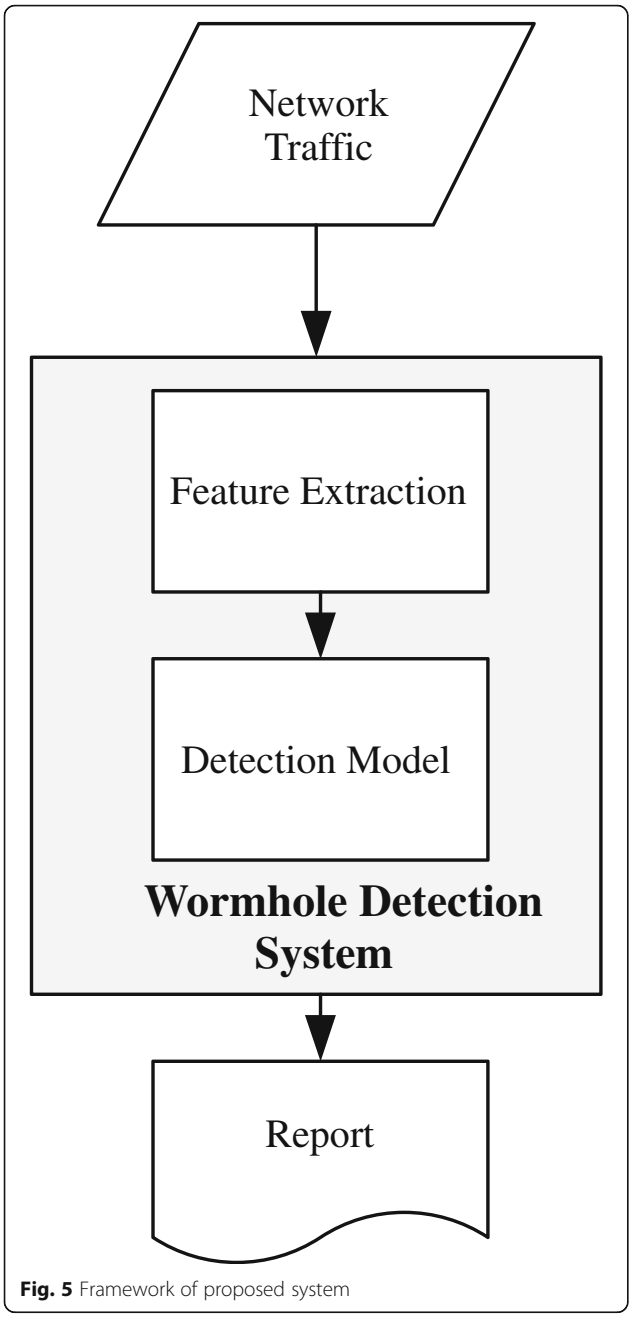

Fig. 5 Framework of proposed system

$$Rank\_Threshold = |(ParentRank) - (SelfRank)| \quad (1)$$

Rank_Diff is defined as the rank difference between the source node and the node itself as expressed in Eq. (2). For the example illustrated in Fig. 4, when node *N5* receives a new DIO message from malicious node M2, it would compute the *Rank_Diff*. The *Rank_Diff* is 4 because the rank value of *SourceRank* is 1, and rank of node *N5* is 5. Therefore, *Rank_Diff* of node *N5* in Fig. 4 is $|0 - 4| = 4$.

$$Rank\_Diff = |(SourceRank) - (SelfRank)| \quad (2)$$

The proposed system considers a DIO message as malicious when *Rank_Diff* > *Rank_Threshold*. In Fig. 4, the DIO message sent by node *M2* will be identified as malicious by node *N5* as *Rank_Diff* > *Rank_Threshold*. By applying the proposed system in every node, nodes will ignore any unreasonable DIO messages. Thus, wormhole attack will be prevented. The proposed system is easy to implement and does not need any additional hardware or complex computing.

4 Simulation and results

In this section, we present the simulation environment and results for the proposed approach. The goal of this simulation is to evaluate the performance of the proposed method. For wormhole detection, our system tries to detect malicious DIO messages correctly. Confusion matrix is used as measurements and in shown in Table 1. In this section, six different experiments are conducted to evaluate the performance of proposed system in different parameters.

This study uses the following performance measurements to evaluate the proposed approach: precision (SP), recall (SR) and accuracy (A). The formulas are expressed as below.

$$SP = \frac{TP}{TP + FP} \quad (3)$$

$$SR = \frac{TP}{TP + FN} \quad (4)$$

$$A = \frac{TN + TP}{TP + FN + FP + TN} \quad (5)$$

4.1 Experiment 1

Experiment 1 is used to validate the correctness of proposed approach, and it also describes how all experiments in this research are conducted. In this section, all nodes are deployed by random, the first deployed node is root node. Malicious nodes are deployed after deploying all benign nodes. Table 2 illustrates the parameters of this example, and Table 3 shows the location (coordinates) of each node.

After all nodes are deployed, the routing path will be established based on RPL protocol. Figure 7 illustrates the topology before wormhole attack of experiment 1.

Figure 7 shows number of nodes, routing path, and rank value of each node. For example, 9(15) means the ninth node in this experiment and its rank value is 15. After routing path of each node is established, the malicious node 52 and 51 start to spread fake routing message. Figure 8 shows the changes of topology after wormhole attack.

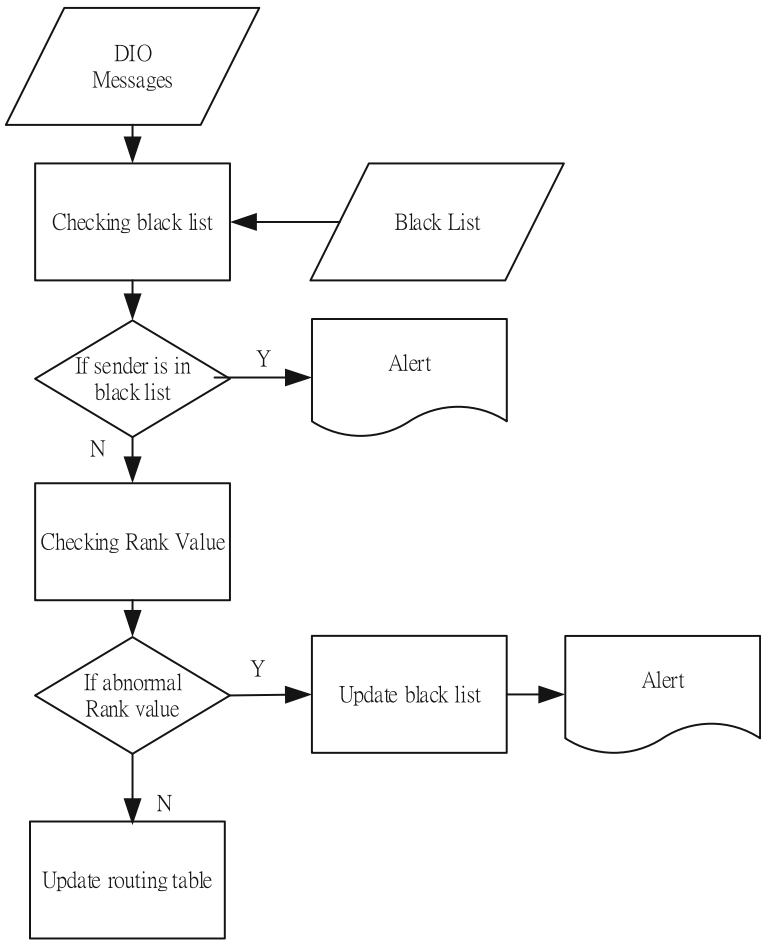

Fig. 6 Process of wormhole detection model

Node 51 and node 52 first build their wormhole tunnel, and then node 52 replays the router advertisement message from node 52's parent node (node 29) to its neighbor nodes. Neighbor nodes of node 52 will change their routing path. In this experiment, nodes 3, 7, 9, 11, 14, 15, 18, 31, and 43 change their routing path. The proposed approach could 100% identify the affected and malicious nodes. For example, before wormhole attack, the rank value of node 31 and its parent node (node 14) is 10 and 9, respectively. Therefore, the *Rank_Threshold* of node 31 is $|9 - 10| = 1$. After malicious nodes launch wormhole attack, node 31 receives the advertisement message from node 52. The rank value of advertisement message is 6. Therefore, the *Rank_Diff* of node 31 is $|6 - 10| = 4$. According to the proposed detection mechanism, if *Rank_Diff* > *Rank_Threshold,* the node which sends abnormal advertisement message is malicious. Table 4 illustrates the result of experiment 1. True positive (TP) is 9 because all affected nodes could be detected (This also means the proposed system could detect malicious nodes.). True negative (TN) is 41 because there is not any unaffected node to be identified as affected node (This also means there is not any benign node to be identified as malicious node.). Experiment 1 shows that the proposed system could detect malicious nodes and affected nodes without any false negative.

Experiment 1 already shows that the proposed system could detect malicious wormhole tunnel. However,

Table 1 Confusion matrix

	Identified as affected	Identified as unaffected
Affected nodes	True positive (TP)	False positive (FP)
Unaffected nodes	False negative (FN)	True negative (TN)

Table 2 Parameters of experiment 1

Map size	500×500
Number of benign node	50
Communication ranges of benign nodes	100
Weight of rain fade	1.0
Length of wormhole tunnel	300

Table 3 The location of each node in experiment 1

	MAC address	Coordinates
Root node 1	Mac addr:11:11:11:11:11:1	(10,100)
Node 2	Mac addr:11:11:11:11:11:2	(350,320)
Node 3	Mac addr:11:11:11:11:11:3	(439,99)
Node 4	Mac addr:11:11:11:11:11:4	(33,139)
Node 5	Mac addr:11:11:11:11:11:5	(418,384)
Node 6	Mac addr:11:11:11:11:11:6	(467,302)
Node 7	Mac addr:11:11:11:11:11:7	(382,41)
Node 8	Mac addr:11:11:11:11:11:8	(280,323)
Node 9	Mac addr:11:11:11:11:11:9	(427,71)
Node 10	Mac addr:11:11:11:11:11:10	(17,117)
Node 11	Mac addr:11:11:11:11:11:11	(354,123)
Node 12	Mac addr:11:11:11:11:11:12	(478,281)
Node 13	Mac addr:11:11:11:11:11:13	(208,174)
Node 14	Mac addr:11:11:11:11:11:14	(280,115)
Node 15	Mac addr:11:11:11:11:11:15	(278,72)
Node 16	Mac addr:11:11:11:11:11:16	(169,274)
Node 17	Mac addr:11:11:11:11:11:17	(144,376)
Node 18	Mac addr:11:11:11:11:11:18	(402,138)
Node 19	Mac addr:11:11:11:11:11:19	(75,457)
Node 20	Mac addr:11:11:11:11:11:20	(315,420)
Node 21	Mac addr:11:11:11:11:11:21	(79,158)
Node 22	Mac addr:11:11:11:11:11:22	(14,13)
Node 23	Mac addr:11:11:11:11:11:23	(183,170)
Node 24	Mac addr:11:11:11:11:11:24	(456,268)
Node 25	Mac addr:11:11:11:11:11:25	(26,384)
Node 26	Mac addr:11:11:11:11:11:26	(24,199)
Node 27	Mac addr:11:11:11:11:11:27	(162,72)
Node 28	Mac addr:11:11:11:11:11:28	(94,40)
Node 29	Mac addr:11:11:11:11:11:29	(22,225)
Node 30	Mac addr:11:11:11:11:11:30	(440,178)
Node 31	Mac addr:11:11:11:11:11:31	(296,161)
Node 32	Mac addr:11:11:11:11:11:32	(222,214)
Node 33	Mac addr:11:11:11:11:11:33	(114,326)
Node 34	Mac addr:11:11:11:11:11:34	(247,275)
Node 35	Mac addr:11:11:11:11:11:35	(230,260)
Node 36	Mac addr:11:11:11:11:11:36	(65,181)
Node 37	Mac addr:11:11:11:11:11:37	(61,284)
Node 38	Mac addr:11:11:11:11:11:38	(448,267)
Node 39	Mac addr:11:11:11:11:11:39	(296,323)
Node 40	Mac addr:11:11:11:11:11:40	(237,401)
Node 41	Mac addr:11:11:11:11:11:41	(475,99)
Node 42	Mac addr:11:11:11:11:11:42	(23,207)
Node 43	Mac addr:11:11:11:11:11:43	(309,112)
Node 44	Mac addr:11:11:11:11:11:44	(106,50)
Node 45	Mac addr:11:11:11:11:11:45	(255,405)
Node 46	Mac addr:11:11:11:11:11:46	(195,61)
Node 47	Mac addr:11:11:11:11:11:47	(249,81)
Node 48	Mac addr:11:11:11:11:11:48	(324,323)
Node 49	Mac addr:11:11:11:11:11:49	(271,393)
Node 50	Mac addr:11:11:11:11:11:50	(489,356)
Malicious node 51	Mac addr:11:11:11:11:11:51	(69,216)
Malicious node 52	Mac addr:11:11:11:11:11:52	(345,99)

applications of wireless sensor networks could be applied to many areas. In this paper, experiments 2 to 5 are conducted to evaluate if the proposed system could detect wormhole attack in different environments and applications.

4.2 Experiment 2

Experiment 2 will evaluate if the proposed system could detect wormhole attack in different map sizes. Table 5 illustrates the parameters in experiment 2, and Table 6 shows the result of experiment 2.

The result of experiment 2 shows that the proposed system could detect wormhole attack perfectly in different map sizes without any false negative. This is a very important feature because nodes of wireless sensor network could be deployed in a small area like a house or be deployed in a large area like a farm. The proposed system is suitable for various wireless sensor network applications.

4.3 Experiment 3

Experiment 3 evaluates if the number of benign nodes affects the detection performance or not. Table 7 presents the parameters of experiment 3, and Table 8 shows the results.

The results of experiment 3 show that the number of benign nodes does not affect the detection performance. The number of nodes in a sensor network may vary in different applications and applied environments. Some applications such as smart homes need few nodes, and some networks such as VANETs (Vehicular Ad Hoc Networks) involve a lot of nodes. Detection mechanisms [14] relying on neighbor node information may not be able to detect wormholes if there are not enough nodes in the environment. The results show that the proposed system could detect wormholes in various network environments ranging from a small to large amount of nodes.

4.4 Experiment 4

Experiment 4 tests if communication range of nodes will affect the detection performance of proposed system.

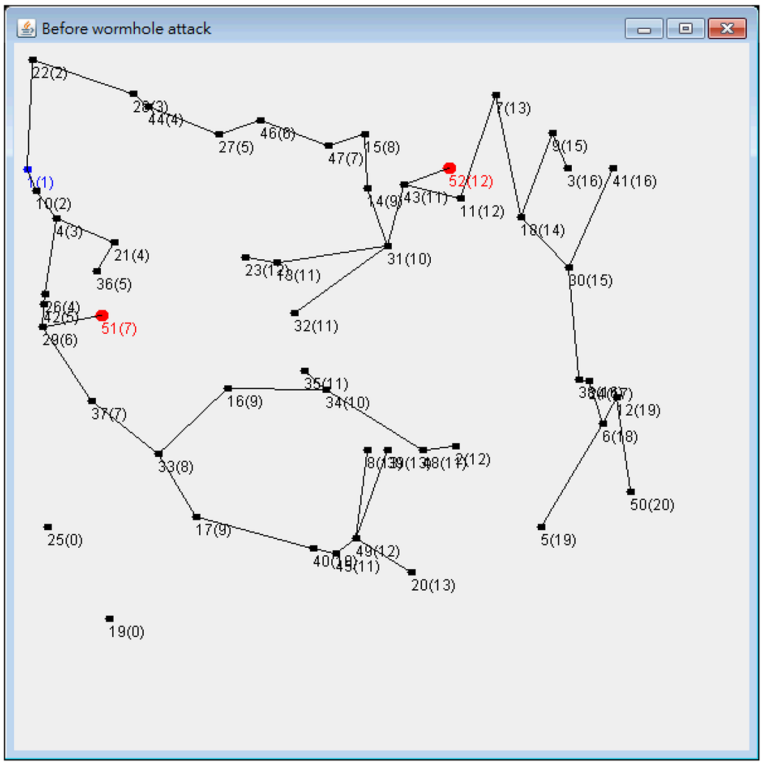

Fig. 7 Topology of experiment 1 before wormhole attack

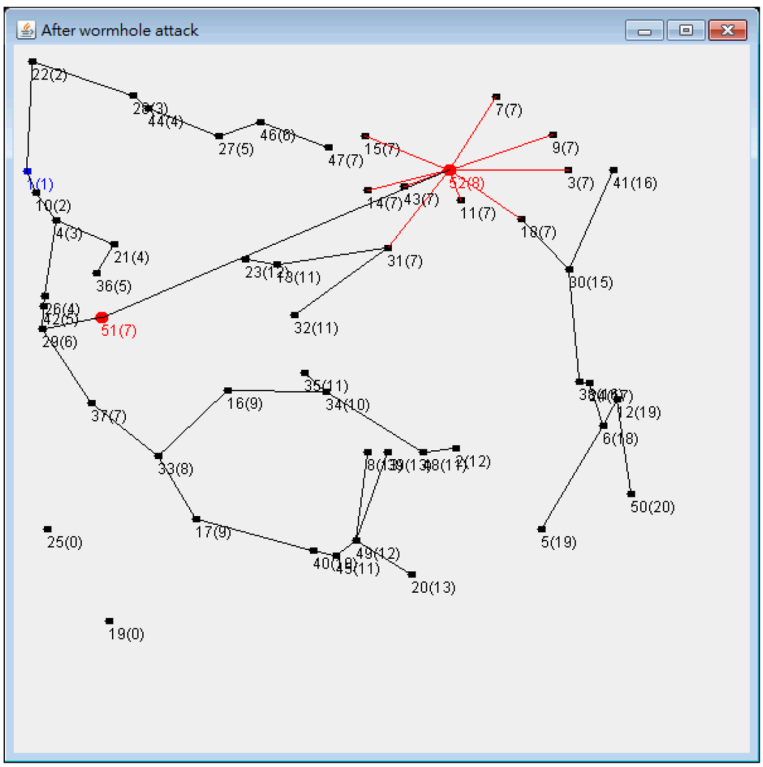

Fig. 8 Topology of experiment 1 after wormhole attack

Table 4 Result of experiment 1

TP	9
FN	0
TN	41
FP	0
Accuracy	100%
Precision	100%
Recall	100%

Nodes with longer communication range mean more neighbor nodes and complex routing tables. Different wireless sensor network applications need different communication ranges. In Zigbee's specification, communication range of Zigbee devices are from 50 to 300 m. Table 9 illustrates the parameters in experiment 4, and Table 10 shows the result of experiment 4.

The result of experiment 4 shows that communication range of benign nodes would not affect the detection performance of proposed system. Communication range of nodes varies with applications. Some applications like smart home need only shorter communication range, and some network like VANETs (Vehicular Ad Hoc Networks) need longer communication range (like 100 m or longer). The result shows that the proposed system could detect wormhole in different wireless sensor network applications.

4.5 Experiment 5

In experiment 5, we evaluate the relation between the distance of wormhole tunnel and the performance of our approach. Distance of wormhole tunnel always longer than communication range of benign nodes. If distance of wormhole tunnel is shorter than communication range of benign nodes, malicious nodes will never attract any traffic. However, some detection mechanisms use transmission time to estimate transmission distance nodes [4]. If the length of wormhole is short, such detection mechanism may not work. Table 11 illustrates the parameters in experiment 5, and Table 12 shows the result of experiment 5.

Table 5 Parameters of experiment 2

Map size	200 m×200 m, 300 m×300 m, 500 m×500 m, 800 m×800 m, 1000 m×1000 m
Number of benign node	100
Communication ranges of benign nodes	100 m
Weight of rain fade	1.0
Length of wormhole tunnel	300 m

Table 6 Result of experiment 2

	Map size				
	200×200	300×300	500×500	800×800	1000×1000
Accuracy (%)	100	100	100	100	100
Precision (%)	100	100	100	100	100
Recall (%)	100	100	100	100	100

The result indicates that the proposed system will detect wormhole attacks with different distances of wormhole tunnel.

The results of experiments 1 to 5 show that proposed system could detect wormhole attack well in different situations. The proposed system is a location-based detection system. Although each node could not know their exact location, the relative location will be get based on rank value in RPL routing protocol. Any malicious DIO messages will be ignored due to unreasonable rank value. The proposed approach does not need any additional devices like GPS or complex algorithm to compute location of nodes. Some approaches like temporal leashes which used transmission time to estimate transmission distance nodes [4]; Wired Equivalent Privacy (WEP) which monitor network traffic of neighbor nodes to detect wormhole [14]. In this paper, we implement temporal leashes and WEP as benchmark of proposed system. Experiment 6 evaluates the detection performance based on different rain fade. Table 13 illustrates the parameters in experiment 6, and Table 14 shows the result of experiment 6.

Result of experiment 5 shows that the proposed system and WEP could detect wormhole perfect in different rain fade levels. Detection accuracy of packet leashes will vary by rain fade because some benign nodes are identified as malicious due to Network latency. Packet leashes approach used transmission time to estimate transmission distance. But packet leashes did not consider that network latency could result in longer transmission time. Once Network transmission is unstable, benign nodes would be identified as malicious nodes.

Number of benign nodes is also a very important parameter to evaluate a detection mechanism of wormhole. Some detection approaches need neighbor nodes' information to detect wormhole attack. Table 15 illustrates the parameters in experiment 7, and Table 16 shows the result of experiment 7.

Table 7 Parameters of experiment 3

Map size	500 m×500 m
Number of benign nodes	10, 30, 50, 100, 200
Communication range of benign nodes	100 m
Weight of rain fade	1.0
Length of wormhole tunnel	300 m

Table 8 Result of experiment 3

	Number of benign nodes				
	10	30	50	100	200
Accuracy (%)	100	100	100	100	100
Precision (%)	100	100	100	100	100
Recall (%)	100	100	100	100	100

Table 9 Parameters of experiment 4

Map size	500 m×500 m
Number of benign node	100
Communication ranges of benign nodes (m)	50, 75, 100, 150, 200
Weight of rain fade	1.0
Length of wormhole tunnel	300 m

Table 10 Result of experiment 4

	Communication range of benign nodes				
	10	30	50	100	200
Accuracy (%)	100	100	100	100	100
Precision (%)	100	100	100	100	100
Recall (%)	100	100	100	100	100

Table 11 Parameters of experiment 5

Map size	500 m×500 m
Number of benign node	100
Communication range of benign nodes	100 m
Weight of rain fade	1.0
Distance of wormhole tunnel (m)	150, 200, 300, 400, 500

Table 12 Result of experiment 5

	Distance of wormhole tunnel				
	150 m	200 m	300 m	400 m	500 m
Accuracy (%)	100	100	100	100	100
Precision (%)	100	100	100	100	100
Recall (%)	100	100	100	100	100

Table 13 Parameters of experiment 6

Map size	500 m×500 m
Number of benign node	100
Communication range of benign nodes	100 m
Weight of rain fade	1.0, 1.2, 1.5, 1.8, 2.0
Distance of wormhole tunnel	300 m

Table 14 Result of experiment 6

	Rain fade				
	1.0	1.2	1.5	1.8	2.0
Accuracy of proposed system (%)	100	100	100	100	100
Accuracy of packet leashes (%) [4]	99	79	64	54	49
Accuracy of WAP (%) [14]	100	100	100	100	100

Table 15 Parameters of experiment 7

Map size	500 m×500 m
Weight of rain fade	1.0
Communication range of benign nodes	100 m
Number of benign nodes	10, 30, 50, 100, 200
Distance of wormhole tunnel	300 m

Table 16 Result of experiment 7

	Number of benign nodes				
	10	30	50	100	200
Accuracy of proposed system (%)	100	100	100	100	100
Accuracy of packet leashes (%) [4]	100	99	99	99	99
Accuracy of WAP (%) [14]	71	95	100	100	100

The result of experiment 7 indicates that WAP will have low accuracy when few nodes are deployed. WAP analyzed neighbor nodes' traffic, if there are enough neighbor nodes, WAP could not get enough information to detect wormhole well. According to experiments 6 and 7, the results show the proposed system outperform WAP and packet leashes. Our system could apply to most wireless sensor network applications without additional hardware. The results of experiments 1 to 7 show that the proposed system could 100% detect wormhole. Compared with traditional wormhole detection approach, the proposed system has higher accuracy rate. Moreover, the proposed system does not need any additional hardware or special nodes. The experiments show the proposed system is a good security mobility management mechanism for wireless sensor network.

5 Conclusions

Wireless sensor network or IoT will be the trend, and more and more wireless sensor network applications have been developed in the world. Due to the nature of wireless sensor network, the devices have only limited computing and electricity capability. Thus, wormhole detection in wireless sensor networks becomes a challenge. This study proposes a wormhole detection mechanism based on RPL routing protocol without additional hardware requirement. The simulation results show the proposed system could detect wormhole correctly. The proposed detection system focuses on the availability of IPv6 wireless sensor network. However, confidentiality is also important for the application of wireless sensor network. Malicious nodes can make fake DIO messages to evade detection. Wireless sensor network applications might apply IPSec technology like IPsec-for-6LoWPAN to ensure the confidentiality and integrity of wireless sensor network applications. The proposed detection system could be a good security mobility management mechanism for wireless sensor network because (1) the proposed system has 100% accuracy; (2) the proposed system does not need any special hardware or special nodes; (3) the proposed system could be applied in any environment; the proposed system needs only few computing resources.

Acknowledgments

This work is supported in part by the Ministry of Science and Technology, Taiwan, Republic of China, under Grants MOST 105-2221-E-034 -011 -MY2.

Competing interests

The author declares that he/she has no competing interests.

Received: 6 March 2016 Accepted: 15 November 2016
Published online: 29 November 2016

References

1. M Ali, T Suleman, ZA Uzmi. "MMAC: A mobility-adaptive, collision-free mac protocol for wireless sensor networks," *in Performance, Computing, and Communications Conference, 2005. IPCCC 2005. (24th IEEE International*, Phoenix, 2005), pp. 401-407
2. L Hu, D Evans. "Using Directional Antennas to Prevent Wormhole Attacks," in *NDSS*, (San Diego, 2004)
3. Y-C Hu, A Perrig, DB Johnson. "Packet leashes: a defense against wormhole attacks in wireless networks," *in INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications.* (IEEE Societies, San Francisco, 2003), pp. 1976-1986
4. Y-C Hu, A Perrig, DB Johnson, "Wormhole attacks in wireless networks," *Selected Areas in Communications*. IEEE J **24**, 370–380 (2006)
5. T Tsvetkov, RPL: IPv6 routing protocol for low power and lossy networks. Sens Nodes Oper Netw Appl **59**, 2 (2011)
6. T Winter, *"RPL: IPv6 routing protocol for low-power and lossy networks"*. 2012
7. L Wallgren, S Raza, T Voigt. "Routing Attacks and Countermeasures in the RPL-based Internet of Things," *International Journal of Distributed Sensor Networks*, vol. 2013, 2013. http://dsn.sagepub.com/content/9/8/794326.full
8. O Garcia-Morchon, S Kumar, R Struik, S Keoh, R Hummen, *Security Considerations in the IP-based Internet of Things*, 2013
9. I Khalil, S Bagchi, NB Shroff, MOBIWORP: mitigation of the wormhole attack in mobile multihop wireless networks. Ad Hoc Netw **6**, 344–362 (2008)
10. R Poovendran, L Lazos, A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks. Wireless Netw **13**, 27–59 (2007)
11. K Sanzgiri, B Dahill, BN Levine, C Shields, EMB Royer. "A secure routing protocol for ad hoc networks," in *Network Protocols, 2002. Proceedings. 10th IEEE International Conference on*, Paris, 2002, pp. 78-87
12. P Papadimitratos, ZJ Haas, *Secure Routing for Mobile Ad Hoc Networks* (the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, 2002), pp. 193–204
13. I Khalil, S Bagchi, NB Shroff. "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks," in *Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on*, Yokohama, 2005, pp. 612-621
14. S Choi, D-y Kim, D-h Lee, J-i Jung. "WAP: Wormhole attack prevention algorithm in mobile ad hoc networks," in Sensor Networks, *Ubiquitous and Trustworthy Computing, 2008. SUTC'08.* (IEEE International Conference, Taichung, 2008), pp. 343-348
15. Wikipedia contributors. (3 February 2016 16:09 UTC). *ZigBee*. Available: https://en.wikipedia.org/w/index.php?title=ZigBee&oldid=702729380. Accessed 23 Feb 2016
16. ZigBee. (2015). *The ZigBee Alliance*. Available: http://www.zigbee.org/. Accessed 23 Feb 2016
17. FI Khan, T Shon, T Lee, K Kim. "Wormhole attack prevention mechanism for RPL based LLN network," in *Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on,* Da Nang, 2013, pp. 149-154