Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2014, Article ID 910242, 10 pages
http://dx.doi.org/10.1155/2014/910242

Research Article

Mobile Beacon Based Wormhole Attackers Detection and Positioning in Wireless Sensor Networks

Honglong Chen,[1,2,3] Wendong Chen,[4] Zhibo Wang,[5] Zhi Wang,[6] and Yanjun Li[7]

[1] *College of Information and Control Engineering, China University of Petroleum, Qingdao 266580, China*
[2] *The Hong Kong Polytechnic University and Shenzhen Research Institute, Shenzhen 518057, China*
[3] *Department of Computing, The Hong Kong Polytechnic University, Kowloon 999077, Hong Kong*
[4] *School of Electrical and Electronic Engineering, East China Jiaotong University, Nanchang 330013, China*
[5] *Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37934, USA*
[6] *State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China*
[7] *College of Computer Science and Technology, Zhejiang University of Technology, Hangzhou 310014, China*

Correspondence should be addressed to Honglong Chen; honglongchen1984@gmail.com

Received 13 February 2014; Accepted 24 February 2014; Published 30 March 2014

Academic Editor: Zhongwen Guo

Wormhole attack is a severe attack that can be easily launched by a pair of external attackers in hostile wireless sensor networks. In the wormhole attack, an attacker sniffs packets at one point in the network, and tunnels them through the wormhole link to the other attacker at another point of the network, which broadcasts them to its neighbors. Such kind of procedure can easily deteriorate the normal functionality of the networks. In this paper, we propose a novel wormhole attackers detection and positioning scheme based on mobile beacon, which can not only detect the existence of wormhole attacks, but also accurately localize the attackers for the system to eliminate them out of the network. The main idea is to detect whether the communication between the mobile beacon and each of the static beacons violates the communication properties and then the attacker can be estimated as the center of its communication area by determining the intersection point of the chords' perpendicular bisector. The simulation results illustrate that our proposed scheme can obtain a high wormhole attack detection probability as well as a high attackers positioning accuracy.

1. Introduction

Wireless Sensor Networks (WSNs) have been applied in more and more applications, such as the emergency response systems, military field operations, and environment monitoring systems, due to the development of the low-cost, low-power, and multifunctional sensor nodes. In normal WSN applications, the sensor nodes are organized to accomplish some kind of tasks, such as event detection or data gathering. However, since WSNs are usually deployed in hostile environments, which may be attacked by some malicious attacks, the functionality of networks may be interrupted. Therefore, security is a necessary characteristic of WSNs applications.

Attackers in WSNs can be classified into two categories, *external* attackers and *internal* attackers [1]. External attackers, such as the wormhole attack, can disrupt the network functionality without passing the system's authorization, while internal attackers, such as the compromise attack, are authenticated ones which can act as inner-network nodes to break the system's security.

Generally, the wormhole attack is launched by two colluding external attackers, which can disrupt or even collapse the functionality of the WSNs. In the wormhole attack, an attacker sniffs packets at one point in the network and tunnels them through the wormhole link to another attacker at the other point of the network, which broadcasts the packets to its neighboring nodes. Such a simple operation can severely affect the localization and routing procedures. For example, as shown in Figure 1, two kinds of nodes, that is, beacons and sensors, are deployed in the network, which is attacked by a wormhole attack lunched by A_1 and A_2. Due to the existence of the wormhole attack, two nonneighboring nodes S_1 and S_7 will consider each other as its neighbor. Moreover, S_6 will get

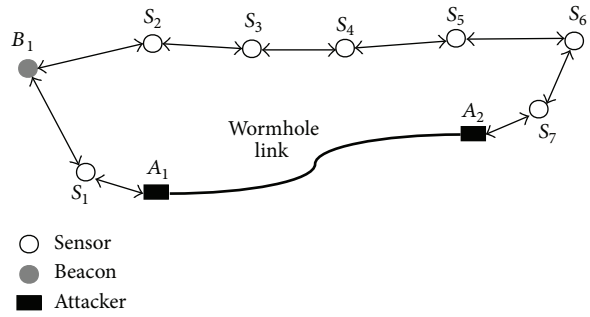

Figure 1: The impacts of the wormhole attack on a WSN.

a hop count 3 to B_1 via the path $S_6 \rightarrow S_7 \xrightarrow{\rightarrow A_2 \rightarrow A_1 \rightarrow} S_1 \rightarrow B_1$ since the relay behaviors of A_1 and A_2 are invisible to S_1, while the actual hop count should be 5 ($S_6 \rightarrow S_5 \rightarrow S_4 \rightarrow S_3 \rightarrow S_2 \rightarrow B_1$). Thus, the wormhole attack in Figure 1 can severely affect the self-localization of S_6 when the DV-Hop localization scheme [2] is adopted.

The above severe effects of the wormhole attack on WSN applications motivate us to propose an efficient scheme to defend against the wormhole attacks. In this paper, we first propose a novel wormhole attackers detection scheme which can detect the existence of the wormhole attacks with a high probability. Then we propose a basic positioning scheme to further localize the wormhole attackers. We also propose an enhanced positioning scheme to decrease the power consumption during the attackers positioning procedure. The main idea is to detect whether the communication between the mobile beacon and each of the static beacons violates the communication properties. The mobile beacon can localize the attacker as the center of its communication area which can be estimated by determining the intersection point of the chords' perpendicular bisector. Also, the localization accuracy of our proposed scheme is independent of the density of beacon nodes. The main contributions of this paper can be summarized as follows.

(i) We propose a novel wormhole attacker detection scheme based on the mobile beacon and the successful detection probability is also theoretically analyzed.

(ii) We propose a basic positioning scheme to accurately localize the wormhole attacker by estimating the center of the attacker's communication area.

(iii) We further propose an enhanced positioning scheme for the attackers positioning to decrease the power consumption.

(iv) We conduct simulations to illustrate the effectiveness of the proposed wormhole attackers detection and positioning schemes.

The rest of this paper is organized as follows. In Section 2, we discuss the existing wormhole attack detection and secure localization schemes. Section 3 presents the system model, including the network model and attack model. In Section 4, we propose the wormhole attacker detection and positioning schemes. The performance evaluation is conducted in Section 5. Section 6 concludes this paper.

2. Related Work

Wormhole attack detection has been a hot research topic during the last decade and lots of schemes have been proposed. In [3], the "packet leashes" mechanism is proposed to use geographical and temporal leashes to detect whether or not the packets are attacked by wormhole attacks. The wormhole detection approach in [4] is based on the end-to-end location information. Another set of wormhole attack preventing techniques [5–7] use the round-trip time of packets as a measurement to detect whether a packet travels via the wormhole link or not. In [8], a "diameter" feature based on the local map is used to detect abnormalities caused by wormholes. LiteWorp [9] makes use of two-hop neighborhood information of the stationary network to reject the packets relayed by the wormhole attacks. MobiWorp [10] uses a secure central authority to isolate the attackers globally after they are detected.

As the wormhole attack dramatically changes the network topology, the network topology information can be used to detect the existence of the wormhole attacks. Wang et al. [11] propose to detect wormhole attacks by visualizing the entire network topology with some anomalies, which is caused by the wormhole attacks. The scheme in [12] uses the network connectivity information to detect wormhole attacks based on the observation that the number of independent neighbors of two nonneighboring nodes is upper bounded. Another connectivity-based wormhole detection approach is proposed in [13] which is robust to different communication models and energy efficient. A topological approach is proposed in [14] to detect the wormhole attacks. In [15], a localized algorithm that detects the wormhole attacks directly using the connectivity information implied by the underlying communication graph is designed, and it requires no specialized hardware, which makes it practical in the real-world scenarios. By detecting whether the communication violates the properties, some novel wormhole detection schemes are proposed in [2, 16, 17].

However, all the above wormhole attack detection schemes cannot localize the attackers, which motivate us to propose the wormhole attackers detection and positioning scheme in this paper. Our proposed scheme can achieve a higher detection probability with a satisfied attackers positioning accuracy.

3. System Model

3.1. Network Model. In this paper, we consider a WSN consisting of three types of nodes: mobile beacon, static beacons, and sensors. The mobile beacon is a node with a GPS device which moves around the network to conduct some special tasks, such as detecting the wormhole attacks. The static beacons are the nodes with fixed locations which can obtain their coordinates in advance by manual deployment

or via GPS devices. The sensors are stationary nodes in the network that initially do not know their locations. All the nodes in the network have the same transmission range, denoted as R, and we assume that there is no packet loss during the communication between any two neighboring nodes. Note that our proposed scheme can be extended to the general scenario where packet loss exists. Each of the nodes has a unique ID in the network and all of them can cooperate with each other to realize WSNs applications, such as self-localization, target tracking, and data gathering.

3.2. Attack Model. A hostile environment is considered, in which the deployed WSN will be attacked by the *wormhole attacks*. A wormhole attack is typically launched by two external attackers, which collude with each other to disrupt the network's functionality. In the wormhole attack, one attacker sniffs packets at one point in the network and forwards these packets to the other attacker via a *wormhole link*, which will immediately broadcast them to its neighboring nodes. The communication range between the attackers and the nodes is also assumed to be R. However, the communication between two colluding attackers is considered to be symmetrical and not limited to the transmission range R since the wormhole link may be based on some certain communication technique, such as the wired communication. For simplicity, we assume that the distance between each pair of wormhole attackers is larger than $2R$; that is, each pair of wormhole attackers has no communication overlapping with each other. And also, each node in the network is assumed to be covered by at most one attacker.

We denote the mobile beacon, static beacons, sensors, and attackers as MB, B, S, and A, respectively. We also denote a disk centered at u with radius R as $D_R(u)$. For example, $D_R(B_1)$ indicates the communication area of static beacon B_1.

4. Wormhole Attacker Detection and Positioning

In this section, we will first propose the wormhole attacker detection scheme based on the mobile beacon, the detection probability of which will be theoretically analyzed. After that we will propose the wormhole attacker positioning schemes including the basic scheme and enhanced scheme, which can accurately localize the wormhole attackers.

4.1. Wormhole Attacker Detection Scheme

4.1.1. Communication Properties. Before proposing the wormhole attacker detection scheme, we firstly introduce two communication properties, which were proposed in [2] and will be the basis of the detection scheme in this paper.

Packet Uniqueness Property. A node normally cannot receive more than one copy of the same message from any of its neighbors.

Transmission Constraint Property. A node normally cannot communicate with nodes outside its transmission range.

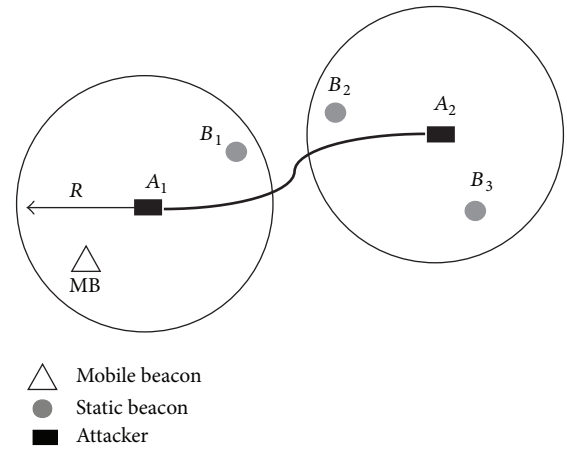

Figure 2: Communication procedure among the nodes under the wormhole attack.

In WSNs, the nodes may need to communicate with its neighbors to accomplish some tasks, and the communication in which should follow the above properties. For example, when a node sends a request message to one of its neighbors to get some information, such as the sensed temperature, it is considered to be normal that this neighbor sends a reply message to the sender for only once if there is no necessity of retransmission. Also, if two nodes are out of the transmission range of each other, it is considered to be normal that the packets from one of them cannot be directly received by the other.

4.1.2. Wormhole Attacker Detection Procedure. If a wormhole attack exists to disrupt the network's functionality, the packet uniqueness property and transmission constraint property may be violated by the nodes' communication. As shown in Figure 2, there are several nodes covered by the wormhole attack; that is, $MB, B_1 \in D_R(A_1)$ and $B_2, B_3 \in D_R(A_2)$. The distance between B_1 and B_2 is shorter than R and the distance between B_1 and B_3 is longer than R. When B_1 sends a request message to its neighbors, every node which receives the request message will send a reply message to B_1. The reply message from B_2 will arrive at B_1 twice, one directly from B_2 to B_1 since their distance is shorter than R and the other via the path $B_2 \rightarrow A_2 \rightarrow A_1 \rightarrow B_1$. Thus, it violates the packet uniqueness property. Although B_3 is out of the transmission range of B_1, it can also receive the request message via the path $B_1 \rightarrow A_1 \rightarrow A_2 \rightarrow B_3$. Similarly, the reply message from B_3 can also be received by B_1. Since the distance between B_1 and B_3 is longer than R, their communication violates the transmission constraint property.

To detect the wormhole attackers in the network, we can use a mobile beacon to detect whether the communication between itself and each of its neighboring static beacons violates the above communication properties. The wormhole attackers detection procedure is as follows.

(i) The mobile beacon moves in the network with some direction and step length and then stops to get its current location using GPS. The details of the

mobile beacon's mobility model including the moving direction and step length will be discussed in the wormhole attackers positioning scheme.

(ii) At each stopping location, the mobile beacon broadcasts a request message Req to its neighboring static beacons. Each static beacon who receives the request message will immediately reply a Rep message, including its ID and coordinate, to the mobile beacon.

(iii) When receiving the Rep message from the static beacon, the mobile beacon will check the receiving times of the Rep from each of the static beacons. If it receives a Rep message from a static beacon more than once, it can determine that there is a wormhole attacker within its transmission range.

(iv) If the mobile beacon receives the Rep message from each of the static beacons only once, it can then calculate the Euclidean distance between itself and each of them since the received Rep message includes the replier's coordinates. If the transmission constraint property is violated, it can determine that there is a wormhole attacker within its transmission range.

(v) If nothing abnormal is detected, the mobile beacon will move to next location and perform the above wormhole attacker detection scheme until it finishes the detection of the whole network.

4.1.3. Analysis of Wormhole Attacker Detection Probability. By carefully designing the mobility model of the mobile beacon, we can guarantee that the mobile beacon will move across the communication area of each attacker. Then we can get the following theorem.

Theorem 1. *The mobile beacon can detect the existence of the wormhole attack if at least one static beacon lies in the transmission range of either of the two attackers.*

Proof. Without loss of generality, we assume that there is only a static beacon B_1 in the transmission range of attacker A_1, that is, $B_1 \in D_R(A_1)$, and no static beacon exists in the transmission range of A_2. When the mobile beacon moves inside $D_R(A_2)$ and broadcasts a Req message, it can receive a Rep message from B_1 via the wormhole link. If the distance between the mobile beacon and B_1 is longer than R, it can determine that their communication procedure violates the transmission constraint property. Otherwise, if their distance is shorter than R, the mobile beacon will receive the Rep message from B_1 twice, one directly from B_1 to itself and the other via the wormhole link. Thus, it can determine that their communication procedure violates the packet uniqueness property. Therefore, the mobile beacon can detect the wormhole attack. Similarly, if there is only a static beacon B_1 in the transmission range of A_2 and no static beacon exists in the transmission range of A_1, the mobile beacon can also detect the wormhole attack when it moves inside $D_R(A_1)$. □

Based on Theorem 1, we can easily analyze the wormhole attacker detection probability of our proposed scheme. We first consider the scenario with single wormhole attack. The probability that at least one static beacon lies in $D_R(A_1)$ (or $D_R(A_2)$) is denoted as $\Pr(A_1)$ (or $\Pr(A_2)$). Then, the probability that the mobile beacon can successfully detect the wormhole attack, denoted as Ps, can be calculated as

$$\mathrm{Ps} = 1 - \overline{\Pr(A_1)} \cdot \overline{\Pr(A_2)}. \tag{1}$$

Assume that the deployment of static beacons follows the Poisson distribution with the density ρ_B. That is, the probability of k static beacons in an area D can be obtained as $\Pr(N_B = k) = ((D\rho_B)^k/k!)e^{-D\rho_B}$. Thus, we can get $\Pr(A_1) = \Pr(A_2) = 1 - e^{-\pi R^2 \rho_B}$. So the probability that the mobile beacon can successfully detect the wormhole attack is

$$\mathrm{Ps} = 1 - e^{-\pi R^2 \rho_B} \cdot e^{-\pi R^2 \rho_B} = 1 - e^{-2\pi R^2 \rho_B}. \tag{2}$$

For the scenario with multiple wormhole attacks, we consider the detection to be successful only if the mobile beacon can detect all of the wormhole attacks. Since we consider the case that a static beacon can be attacked by at most one attacker, the detection of one of the multiple wormhole attacks is independent of that of other wormhole attacks. Thus, the detection probability that all the wormhole attacks can be successfully detected can be easily obtained as

$$\mathrm{Ps} = \left(1 - e^{-2\pi R^2 \rho_B}\right)^n, \tag{3}$$

where n represents the number of wormhole attacks in the network. Note that a wormhole attack is composed of a pair of attackers.

4.2. Wormhole Attackers Positioning Schemes. Based on the above wormhole detection scheme, the mobile beacon can easily detect the wormhole attacks in the network. However, it is not enough to secure a WSN application. Thus, the mobile beacon has to further localize the attackers and then report to the system to eliminate them. In this section, we will first propose a basic positioning scheme which can localize the wormhole attackers accurately. To further reduce the power consumption during the positioning procedure, we will then propose an enhanced positioning scheme.

4.2.1. Basic Positioning Scheme. For ease of description, we assume that the WSN is deployed in a rectangular area of $d_x \times d_y\, m^2$ and the origin of the coordinate plane locates at the left bottom of the area. As shown in Figure 3(a), the mobile beacon can horizontally move from the origin of the coordinate plane towards the right boundary of the area with a constant moving step length ΔL_H. It will conduct the wormhole attacker detection scheme each time it moves for a distance of ΔL_H. When the mobile beacon arrives at the right boundary, it can move up for a distance of ΔL_P and then move horizontally towards the left boundary with a step length of ΔL_H. Similarly, when the mobile beacon arrives at the left boundary, it will move up for a distance of ΔL_P and then move horizontally towards the right boundary of the area with a step length of ΔL_H. Such operations will be conducted until the whole area is completely scanned by the mobile beacon.

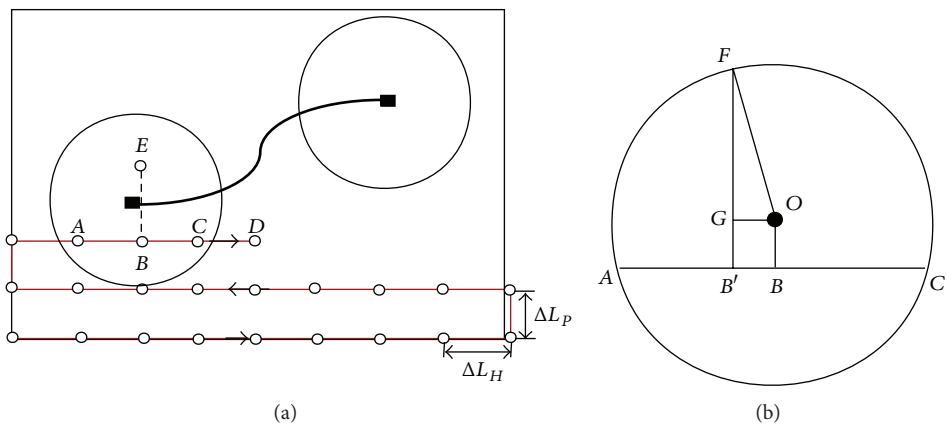

FIGURE 3: Attackers positioning of the basic scheme: (a) the attackers positioning procedure; (b) determination of ΔL_P.

When the mobile beacon enters the communication area of an attacker, such as A in Figure 3(a), it can detect the existence of the wormhole attack. Then it can save its current location as $v_f = (x_A, y_A)$. After that it continues to move towards the right boundary and can detect the wormhole attack at B and C. When the mobile beacon arrives at D, it cannot detect the wormhole attack anymore, and then it can save its previous location (C in Figure 3(a)) as $v_l = (x_C, y_C)$. After that the mobile beacon can estimate the line AC as the chord of the attacker's communication area and the attacker should lie on the perpendicular bisector of AC; that is, the location of the attacker should be $((x_A + x_C)/2, (y_A + y_C)/2 - \sqrt{R^2 - (x_A - x_C)^2/4})$ or $((x_A + x_C)/2, (y_A + y_C)/2 + \sqrt{R^2 - (x_A - x_C)^2/4})$. To further determine the actual location of the attacker, it can then move to $((x_A + x_C)/2, (y_A + y_C)/2 + R)$ (E in Figure 3(a)) and check whether it can detect the wormhole attack. If yes, it indicates that the attacker lies above line AC, and the mobile beacon will estimate the attacker's location as $((x_A + x_C)/2, (y_A + y_C)/2 + \sqrt{R^2 - (x_A - x_C)^2/4})$; otherwise, the attacker's location is $((x_A + x_C)/2, (y_A + y_C)/2 - \sqrt{R^2 - (x_A - x_C)^2/4})$.

Note that the mobile beacon only conducts the wormhole attack detection scheme every step of ΔL_H, and it cannot exactly determine the intersection points between the chord and the attacker's communication circle. As shown in Figure 3(a), A and C are not exactly on the attacker's communication circle. Thus, we need to carefully design ΔL_H and ΔL_P to make the proposed basic attacker positioning scheme feasible. As the value of ΔL_H determines the localization accuracy of the basic scheme, we can firstly set it as $\Delta L_H = \alpha R$, where $0 < \alpha < 1$. Then we have to determine the value of ΔL_P. As shown in Figure 3(b), when mobile beacon moves from A to C, it will estimate the location of the chord AC's midpoint with a maximum error of $\Delta L_H/2$. Assume that the mobile beacon estimates it as B', and then $BB' \leq \Delta L_H/2$. To guarantee that the mobile beacon can still detect the wormhole attack when it moves to $((x_A + x_C)/2, (y_A + y_C)/2 + R)$, it must be satisfied that $B'F \geq R$. As $BB' \leq \Delta L_H/2$, we can get

$$B'F = GF + B'G \geq \sqrt{R^2 - \frac{\Delta L_H^2}{4}} + B'G. \tag{4}$$

Then to guarantee that $B'F \geq R$, we can make $\sqrt{R^2 - \Delta L_H^2/4} + B'G \geq R$. Finally, we can get $B'G \geq R - \sqrt{R^2 - \Delta L_H^2/4}$. Also, to guarantee that the mobile beacon can conduct the wormhole attack for at least once on line AC, it must satisfy that $AC \geq \Delta L_H$. So $B'G = OB \leq \sqrt{R^2 - \Delta L_H^2/4}$. Thus, to guarantee that the mobile beacon can correctly localize the attacker when it moves along AC, it must satisfy that

$$R - \sqrt{R^2 - \frac{\Delta L_H^2}{4}} \leq B'G \leq \sqrt{R^2 - \frac{\Delta L_H^2}{4}}. \tag{5}$$

To guarantee that the mobile beacon can move across the attacker's communication range with the condition that $B'G \in [R - \sqrt{R^2 - \Delta L_H^2/4}, \sqrt{R^2 - \Delta L_H^2/4}]$, it must satisfy that $\Delta L_P \leq \sqrt{R^2 - \Delta L_H^2/4} - (R - \sqrt{R^2 - \Delta L_H^2/4})$. That is,

$$\Delta L_P \leq 2\sqrt{R^2 - \frac{\Delta L_H^2}{4}} - R. \tag{6}$$

The previous scheme can localize the attackers accurately when there exists only one wormhole attack. However, if multiple wormhole attacks exist and the attackers are close enough to each other, there may be some problem. For example, as shown in Figure 4, when the mobile beacon node moves from C to D, although it is out of transmission range of attacker A_3, it can still detect the wormhole attack since the communication between itself and B_1 violates the communication property. Thus, using the previous scheme, the mobile beacon node will incorrectly estimate the midpoint of the chord of $D_R(A_3)$, leading to inaccurate attackers positioning.

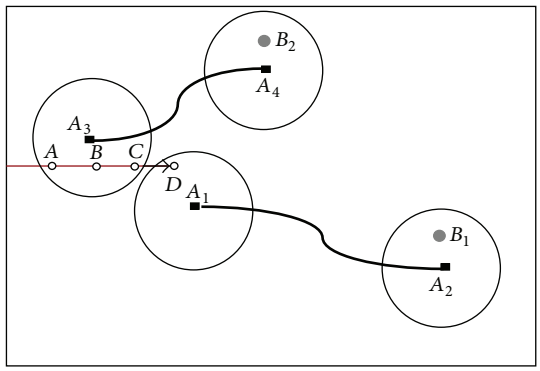

Figure 4: Attackers positioning of multiple wormhole attacks using conflicting set.

To solve this problem, we can use the concept of *conflicting nodes*, which we borrow from our previous work [18].

In this paper, we define the conflicting nodes of the mobile beacon node as the beacon nodes, and the communication between which and the mobile beacon node violates the packet uniqueness property or the transmission constraint property. That is to say, the conflicting nodes of the mobile beacon node are the beacon nodes which communicate with itself via the wormhole link. For example, as shown in Figure 4, when the mobile beacon node arrives at A, it can detect the wormhole attack as it can check that the communication between itself and B_2 violates the communication property; thus it will consider B_2 as its conflicting node. While it moves to D, it cannot communicate with B_2, but it can still check that the communication between itself and B_1 violates the communication property, so it will then consider B_1 as its conflicting node.

Thus, when the mobile beacon node enters the communication range of an attacker, we can get the following theorem.

Theorem 2. *When the mobile beacon node enters the area of $D_R(A_1)$, its conflicting nodes are all the beacon nodes inside $D_R(A_2)$, where A_1 and A_2 are a pair of wormhole attackers.*

Proof. All the beacon nodes inside $D_R(A_2)$ can be classified into two sets according to the distance between each of them and the mobile beacon node. For the beacon nodes, the distance between each of which and the mobile beacon node is not larger than R, and the communication between them and the mobile beacon node violates the packet uniqueness property. Thus, the mobile beacon node will consider them as its conflicting nodes. While, for the beacon nodes, the distance between each of which and the mobile beacon node is larger than R, the communication between them and the mobile beacon node violates the transmission constraint property since they can communicate with each other via the wormhole link. Thus, the mobile beacon node will also consider these nodes as its conflicting nodes. While for other beacon nodes outside $D_R(A_2)$, since they cannot communicate with the mobile beacon node via the wormhole link, they will not be considered as the mobile beacon node's conflicting nodes. □

Based on Theorem 2, we can get the following corollary.

Corollary 3. *If the mobile beacon node has the same conflicting nodes at two locations, then it is within the communication range of the same attacker.*

According to Corollary 3, the mobile beacon node can identify different wormhole attackers easily. For example, as shown in Figure 4, when the mobile beacon node moves to A, it will detect the wormhole attack. Furthermore, it will consider B_2 as its conflicting node. Then when it moves to B, it can still detect the wormhole attack and B_2 is also considered as its conflicting node. Thus the mobile beacon node continues to move to C and conducts the corresponding detection. When it moves to D, although it can detect the wormhole attack, it will find that its current conflicting node is different from the previous point; thus it can determine that it moves out the transmission range of the last attacker, that is, A_3. After that it can estimate the line AC as the chord of $D_R(A_3)$ and A_3 should lie on the perpendicular bisector of AC; that is, the location of A_3 should be $((x_A + x_C)/2, (y_A + y_C)/2 - \sqrt{R^2 - (x_A - x_C)^2/4})$ or $((x_A + x_C)/2, (y_A + y_C)/2 + \sqrt{R^2 - (x_A - x_C)^2/4})$. Then the mobile beacon node can first move to $((x_A + x_C)/2, (y_A + y_C)/2 - \sqrt{R^2 - (x_A - x_C)^2/4})$ to check whether it can detect the wormhole attack and also whether the conflicting node is still B_2; if yes, it can determine that the location of A_3 is $((x_A + x_C)/2, (y_A + y_C)/2 - \sqrt{R^2 - (x_A - x_C)^2/4})$. Otherwise, the location of A_3 is $((x_A + x_C)/2, (y_A + y_C)/2 + \sqrt{R^2 - (x_A - x_C)^2/4})$.

4.2.2. Enhanced Positioning Scheme. In the basic positioning scheme, when the mobile beacon node moves forward a step, it will conduct the wormhole attack detection, in which it broadcasts a Req message to its neighboring beacon nodes and then waits for the Rep messages from them. Such kind of procedure involves the message exchange between the mobile beacon node and its neighboring beacon nodes, which is energy consuming. In this section, we will propose an enhanced positioning scheme, which can reduce the energy consumption of the positioning procedure.

Since the mobile beacon node moves across the network, it may enter the transmission range of an attacker for more than once. As shown in Figure 5, when the mobile beacon node moves from A to C, it can detect the existence of the wormhole attack after which it can determine the location of the attacker as $((x_A + x_C)/2, (y_A + y_C)/2 + \sqrt{R^2 - (x_A - x_C)^2/4})$. Then it can save the currently estimated location of the attacker into the set X_A. When the mobile beacon node moves out of the transmission range of the current attacker, it will first check whether the next location lies in the transmission range of any of the attackers in X_A. If yes, it can ignore this location and check next location until the one which is outside the transmission range

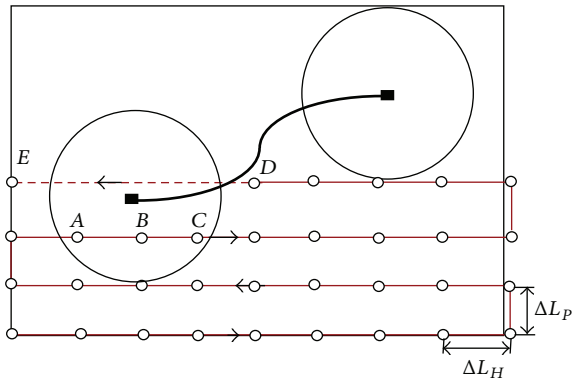

FIGURE 5: The procedure of the enhanced attackers positioning scheme.

of each of the attackers in X_A, and then it can move to that location and conduct the wormhole attack detection. Note that the attackers in X_A have already been positioned by the mobile beacon node; thus it will not affect the attacker positioning by ignoring the detection procedures at such locations. For example, as shown in Figure 5, when the mobile beacon node moves to D, it detects that there is no wormhole attack, and then it decides to move to next location, which is $(x_D + \Delta L_H, y_D)$. However, it can detect that the distance between next location and $((x_A + x_C)/2, (y_A + y_C)/2 + \sqrt{R^2 - (x_A - x_C)^2/4})$, which is estimated as the location of an attacker and is saved in X_A, is shorter than R, and then it will not conduct wormhole attack detection at this location. Similarly, the mobile beacon node will check the next several locations and find that E is not within the transmission range of each of the attackers in X_A. Thus it will directly move to E and conduct the wormhole attack detection there. By using such strategy, some unnecessary locations can be found, at which the energy-consuming wormhole attack detection procedure will not be conducted. Moreover, the enhanced positioning scheme will not degrade the attackers positioning performance.

5. Performance Evaluation

In this section, we present the simulation results to demonstrate the effectiveness of the proposed wormhole attackers detection and positioning scheme. We compare the proposed scheme with the label-based scheme proposed in [2] as the detection scheme of the label-based scheme is similar to our proposed scheme and it can also estimate the locations of the wormhole attackers. In the simulation, a WSN is randomly deployed in a $1 \times 1\,\text{km}^2$ region and the transmission range of each node is set as 150 m.

Figure 6 illustrates the comparison of the wormhole attack detection probability of our proposed scheme between the simulation and the theoretical model under single wormhole attack. We vary the number of beacon nodes from 10 to 30; that is, the density of the beacon nodes varies from 10^{-5} to 3×10^{-5}. The results show that the theoretical model matches the simulation quite well, which validates the correctness of

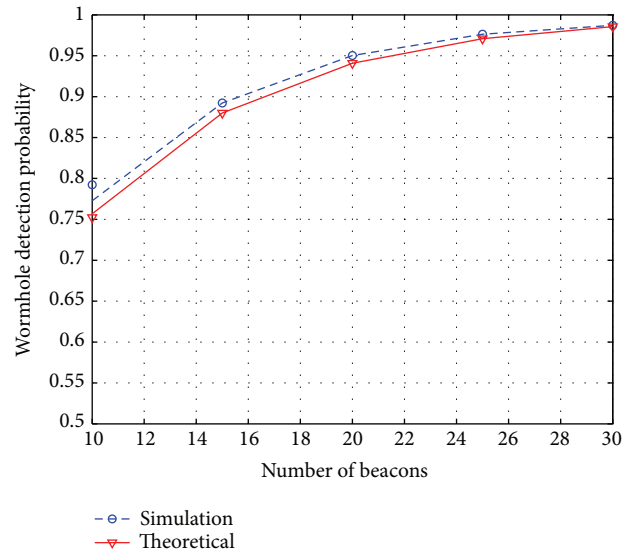

FIGURE 6: Wormhole attack detection probability: simulation versus theoretical model.

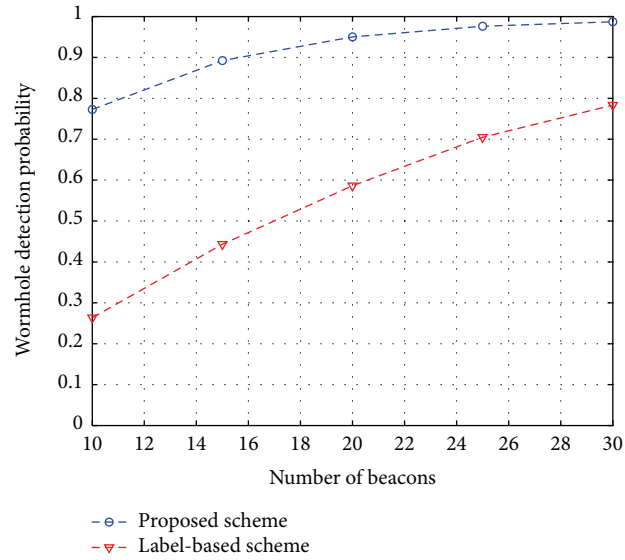

FIGURE 7: Wormhole detection probability of the proposed scheme and the label-based scheme with only single wormhole attack.

the theoretical analysis on the wormhole attack detection probability.

Figure 7 illustrates the wormhole detection probability of the proposed scheme and the label-based scheme when there is only a wormhole attack in the network. In the label-based scheme, the wormhole attack can be detected by checking whether the communications between the beacon nodes violate the properties and the precondition is that there exists at least one beacon node within the communication range of each of the attackers. In our proposed scheme, we select $\Delta L_H = 0.1R = 15\,\text{m}$, and ΔL_P is set as the maximum value corresponding to the selected ΔL_H; that is,

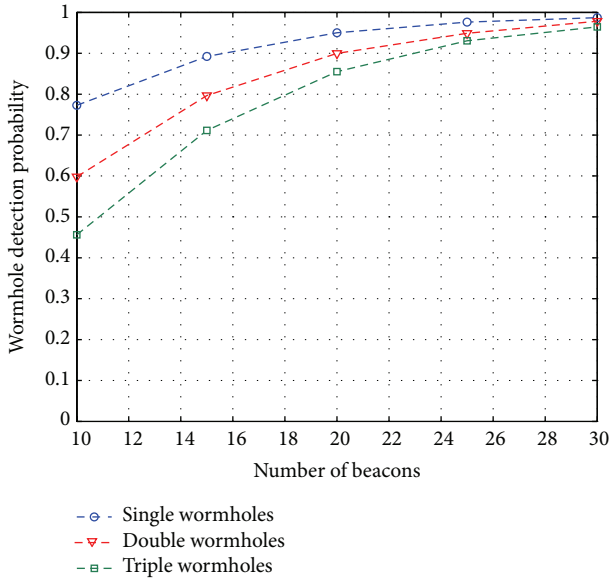

Figure 8: The effects of the number of wormholes on the detection probability.

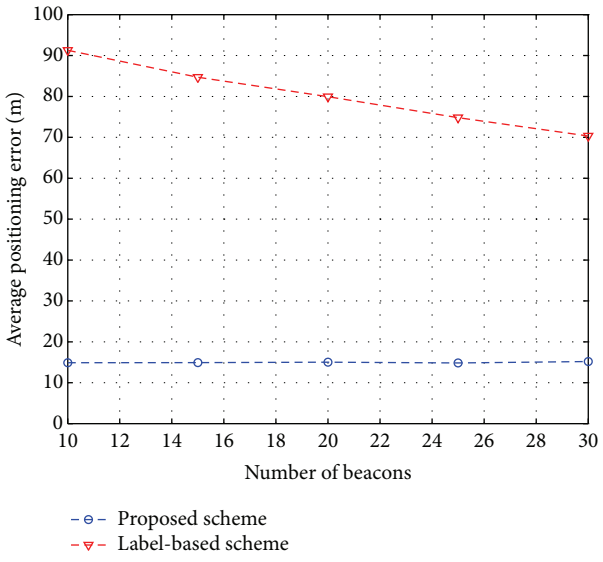

Figure 9: The average positioning error of our proposed scheme and the label-based scheme.

$\Delta L_P = 2\sqrt{R^2 - \Delta L_H^2/4} - R = 149.6$ m, which can minimize the power consumption introduced by the mobile beacon. It shows that our proposed scheme can achieve a much higher detection probability than the label-based scheme. And when the number of beacon nodes equals 20, that is, there are 1.4 beacons in the transmission range of the attacker in average, the detection probability of our proposed scheme is larger than 95%. Overall, our proposed scheme outperforms the label-based scheme.

Figure 8 illustrates the wormhole detection probability of our proposed scheme with different number of wormhole attacks in which the settings of ΔL_H and ΔL_P are the same

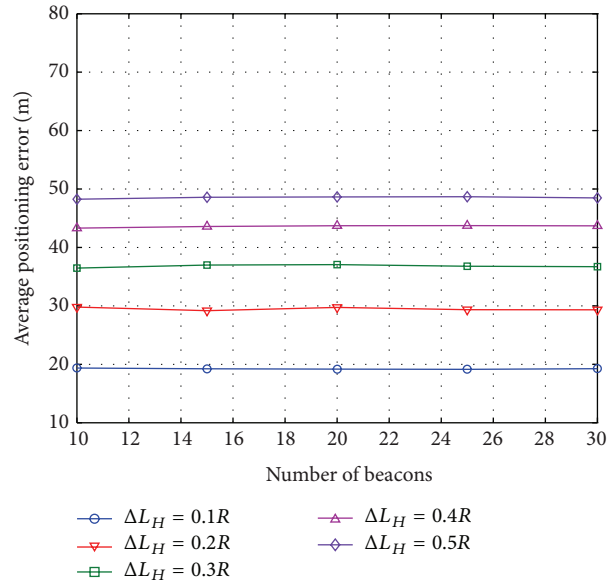

Figure 10: The effects of mobile beacon node's moving step length on the attacker positioning accuracy.

with that in Figure 7. It shows that when the number of wormhole attacks increases, the detection probability will decrease, which is consistent with (3). However, the detection probability is relatively high when the number of beacons is larger than 20.

Figure 9 illustrates the wormhole attacker positioning error of our proposed scheme and the label-based scheme in which the settings of ΔL_H and ΔL_P are the same with that in Figure 7. In the label-based scheme, the attacker will be estimated as the centrality of all the beacons within its transmission range. Note that the attackers positioning performance of the basic scheme and the enhanced scheme is the same; here we do not differentiate between them. It shows that our proposed scheme can achieve a much higher positioning accuracy than the label-based scheme. Furthermore, the positioning accuracy of the label-based scheme depends on the number of beacons, while our proposed scheme obtains a stable positioning accuracy with different number of beacons.

Figure 10 illustrates the effects of the moving step lengths ΔL_H and ΔL_P on the attacker positioning accuracy of our proposed scheme (here we also do not differentiate between the basic scheme and the enhanced scheme since their positioning performance is the same). We vary the value of ΔL_H from $0.1R$ to $0.5R$ with an increment of $0.1R$. And similarly, to minimize the power consumption introduced by the mobile beacon node, ΔL_P is set as the maximum value corresponding to each ΔL_H; that is, $\Delta L_P = 2\sqrt{R^2 - \Delta L_H^2/4} - R$. It shows that the increase of moving step length will degrade the attacker positioning accuracy. Furthermore, even when $\Delta L_P = 0.5R$, the attacker positioning error of our proposed scheme is still less than the label-based scheme.

Figure 11 illustrates the comparison of the detection times between the basic scheme and the enhanced scheme under

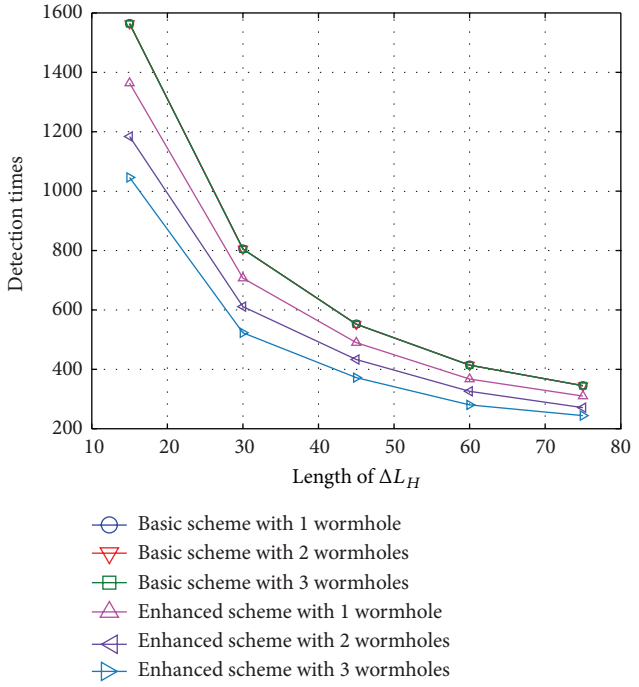

Figure 11: The comparison of the detection times between the basic scheme and the enhanced scheme.

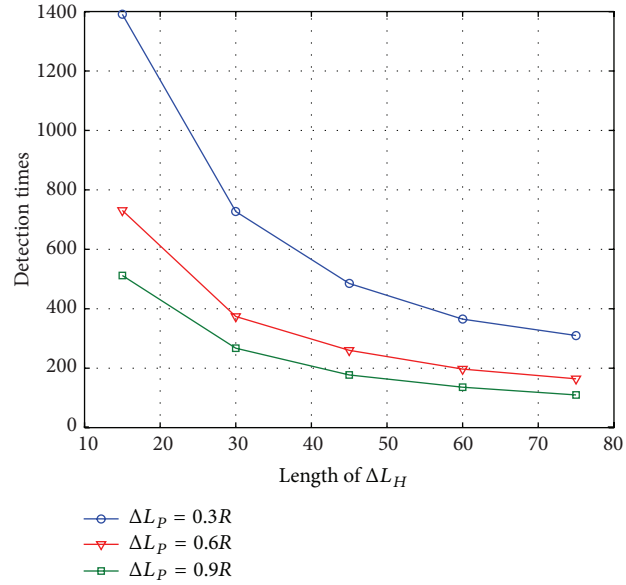

Figure 12: The effects of mobile beacon node's moving step length on the detection times of the proposed enhanced scheme.

different number of wormholes. The detection times here mean the total times that the mobile beacon node stop to conduct the wormhole attack detection in the whole network. Since the energy consumption in the proposed scheme mainly occurs during the wormhole attack detection, which requires the nodes to exchange messages, we can analyze the energy consumption of the scheme by directly evaluating the detection times. We adopt $\Delta L_P = 0.3R$ in Figure 11. We can observe that the number of wormholes does not affect the detection times of the basic scheme, while the increase of the number of wormholes will reduce the detection times of the enhanced scheme. Also, it shows that the proposed enhanced scheme has fewer detection times than the basic scheme, which indicates that it consumes less power than the basic scheme.

The effects of the moving step length ΔL_H and ΔL_P on the detection times of the proposed enhanced scheme are illustrated in Figure 12. The curves in Figure 12 show that the increase of moving step length, including ΔL_H and ΔL_P, can reduce the detection times; that is, it can reduce the introduced energy consumption. As the increase of the moving step length can also reduce the attackers positioning accuracy as shown in Figure 10, a tradeoff between the positioning accuracy and the energy consumption should be well balanced.

6. Conclusions

In this paper, we proposed a novel wormhole attackers detection and positioning scheme, which can not only detect the existence of wormhole attacks, but also localize the attackers with a high accuracy for the system to eliminate them out of the network. The main idea is to detect whether the communication between the mobile beacon and the static beacons violates the communication properties and then the attacker can be localized as the center of its communication disk by finding the intersection point of the chords' perpendicular bisector. The simulation results illustrated that our proposed scheme can obtain a high wormhole attack detection probability together with a high accuracy for localizing the attackers.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported in part by NSFC Grants no. 61309023, no. 61273079, and no. 61272463, Shandong Provincial Natural Science Foundation, China (no. ZR2013FQ032), the Fundamental Research Funds for the Central Universities (no. 13CX02100A), Open Project in Zhejiang Provincial Key Lab of Intelligent Processing Research of Visual Media (no. 2012008), State Key Laboratory of Industrial Control Technology under Grants no. ICT1206 and no. ICT1207, Hong Kong GRF Grants (PolyU-524308, PolyU-521312), and HKPU Grants (A-PL16, A-PL84).

References

[1] S. Čapkun, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, 2006.

[2] J. Wu, H. Chen, W. Lou, Z. Wang, and Z. Waang, "Label-based DV-Hop localization againstwormhole attacks in wireless sensor networks," in *Proceedings of the 5th IEEE International Conference on Networking, Architecture and Storage (NAS '10)*, pp. 79–88, July 2010.

[3] Y. C. Hu, A. Perrig, and D. B. Johnson, "Wormhole attacks in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 370–379, 2006.

[4] W. Wang, B. Bhargava, Y. Lu, and X. Wu, "Defending against wormhole attacks in mobile ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 6, no. 4, pp. 483–503, 2006.

[5] S. Čapkun, L. Buttyán, and J. Hubaux, "SECTOR: secure tracking of node encounters in multi-hop wireless networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor networks (in association with 10th ACM Conference on Computer and Communications Security)*, pp. 21–32, October 2003.

[6] Y. C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless Ad Hoc network routing protocols," in *Proceedings of the 2003 ACM Workshop on Wireless Security (WiSec '03)*, pp. 30–40, September 2003.

[7] J. Eriksson, S. V. Krishnamurthy, and M. Faloutsos, "TrueLink: a practical countermeasure to the wormhole attack in wireless networks," in *Proceedings of the 14th IEEE International Conference on Network Protocols (ICNP '06)*, pp. 75–84, November 2006.

[8] Y. Xu, G. Chen, J. Ford, and F. Makedon, "Detecting wormhole attacks in wireless sensor networks," *IFIP International Federation for Information Processing*, vol. 253, pp. 267–279, 2007.

[9] I. Khalil, S. Bagchi, and N. B. Shroff, "LITE WORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks," in *Proceedings of the International Conference on Dependable Systems and Networks (DSN '05)*, pp. 612–621, July 2005.

[10] I. Khalil, S. Bagchi, and N. B. Shroff, "MOBIWORP: mitigation of the wormhole attack in mobile multihop wireless networks," in *Proceedings of the Securecomm and Workshops*, September 2006.

[11] W. Wang, J. Kong, B. Bhargava, and M. Gerla, "Visualisation of Wormholes in underwater sensor networks: a distributed approach," *International Journal of Security and Networks*, vol. 3, no. 1, pp. 10–23, 2008.

[12] R. Maheshwari, J. Gao, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in *Proceedings of the 26th IEEE International Conference on Computer Communications (IEEE INFOCOM '07)*, pp. 107–115, May 2007.

[13] X. Ban, R. Sarkar, and J. Gao, "Local connectivity tests to identify wormholes in wireless networks," in *Proceedings of the 12th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc '11)*, May 2011.

[14] D. Dong, M. Li, Y. Liu, X. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," *IEEE/ACM Transactions on Networking*, vol. 19, no. 6, pp. 1787–1796, 2011.

[15] T. Dimitriou and A. Giannetsos, "Wormholes no more? Localized Wormhole detection and prevention in wireless networks," in *Proceedings of the IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS '10)*, 2010.

[16] H. Chen, W. Lou, and Z. Wang, "Secure localization against wormhole attacks using conflicting sets," in *Proceedings of the IEEE 29th International Performance Computing and Communications Conference (IPCCC '10)*, pp. 25–33, December 2010.

[17] H. Chen, W. Lou, J. Wu, Z. Wang, Z. Wang, and A. Xia, "Securing DV-Hop localization against Wormhole attacks in wireless sensor networks," *Pervasive and Mobile Computing*, 2014.

[18] H. Chen, W. Lou, and Z. Wang, "On providing Wormhole attack resistant localization using conflicting sets," *Wireless Communications and Mobile Computing*, 2014.