Research Article

A Secure Localization Approach against Wormhole Attacks Using Distance Consistency

Honglong Chen,[1, 2] Wei Lou,[2] Xice Sun,[1, 2] and Zhi Wang[1]

[1] *State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou, Zhejiang 310027, China*
[2] *Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong*

Correspondence should be addressed to Zhi Wang, wangzhizju@gmail.com

Wormhole attacks can negatively affect the localization in wireless sensor networks. A typical wormhole attack can be launched by two colluding attackers, one of which sniffs packets at one point in the network and tunnels them through a wired or wireless link to another point, and the other relays them within its vicinity. In this paper, we investigate the impact of the wormhole attack on the localization and propose a novel distance-consistency-based secure localization scheme against wormhole attacks, which includes three phases of wormhole attack detection, valid locators identification and self-localization. The theoretical model is further formulated to analyze the proposed secure localization scheme. The simulation results validate the theoretical results and also demonstrate the effectiveness of our proposed scheme.

1. Introduction

Wireless sensor networks (WSNs) [1] consist of a large amount of sensor nodes which cooperate among themselves by wireless communications to solve problems in fields such as emergency response systems, military field operations, and environment monitoring systems. Nodal localization is one of the key techniques in WSNs. Most of current localization algorithms estimate the positions of location-unknown nodes based on the position information of a set of nodes (*locators*) and the internode measurements such as distance measurements or hop counts. Localization in WSNs has drawn growing attention from the researchers, and comprehensive approaches [2–6] are proposed. However, most of the localization systems are vulnerable under the hostile environment where malicious attacks, such as the *replay attack* or *compromise attack* [7], can disturb the localization procedure. Security, therefore, becomes a significant concern of the localization process in hostile environment.

The *wormhole attack* is a typical kind of secure attacks in WSNs. It is launched by two colluding *external attackers* [7] which do not authenticate themselves as legitimate nodes to the network. When starting a wormhole attack, one attacker overhears packets at one point in the network, tunnels these packets through the wormhole link to another point in the network, and the other attacker broadcasts the packets among its neighborhood nodes. This can cause severe malfunctions on the routing and localization procedures in WSNs. Khabbazian et al. [8] point out how the wormhole attack impacts on building the shortest path in routing protocols. For the localization procedure under wormhole attacks, some range-free approaches [9, 10] have been proposed. We will propose a range-based secure localization scheme under wormhole attacks in this paper.

To prevent the effect of wormhole attack on the range-based localization, we propose a distance-consistency-based secure localization scheme including three phases: wormhole attack detection, valid locators identification and self-localization. The wormhole attack detection is designed to detect different types of wormhole attacks. For the valid locators identification, different identification schemes are proposed under different wormhole attacks. Both basic approach and enhanced approach are devised using these identification schemes. We formulate the theoretical model to analyze the probability of detecting wormhole attacks and the probability of successfully identifying all valid locators.

Simulation results show the effectiveness of our proposed scheme and validate the theoretical results.

As a summary, this paper makes the following contributions:

(i) a novel wormhole attack detection scheme is proposed to detect the existence of a wormhole attack and to further determine the type of the wormhole attack;

(ii) a basic identification approach is designed to identify the valid locators for the sensor. Two independent algorithms are proposed to handle different wormhole attacks;

(iii) an enhanced identification approach is developed which achieves better performances than the basic approach;

(iv) theoretical analysis on the probability of detecting wormhole attacks and the probability of successfully identifying all valid locators are conducted and verified by simulations.

(v) simulations are conducted to further demonstrate the effectiveness of the proposed secure localization schemes.

The remainder of this paper is organized as follows. In Section 2, we discuss the related work on the secure localization. Section 3 describe the network model and the attack model of the system. The secure localization scheme is proposed in Section 4. Section 5 gives the theoretical analysis and Section 6 presents the simulation results. Section 7 concludes the paper and outlines our future work.

2. Related Work

The secure localization in hostile environment has been investigated for several years and many secure localization systems have been proposed [11, 12].

To resist the compromise attack, Liu et al. [13] propose the range-based and range-free secure localization schemes, respectively. For the range-based scheme, a Minimum Mean Square Estimation method is used to filter out inconsistent beacon signals. For the range-free scheme, the nodes adopt the voting-based location estimation which can ignore the minor votes imposed by the malicious nodes. SPINE [7] utilizes the verifiable multilateration and verification of positions of mobile devices into the secure localization in the hostile network. The mechanism in [14] introduces a set of covert base stations (CBS), whose positions are unknown to the attackers, to check the validity of the nodes. ROPE [15] is a robust positioning system with a location verification mechanism that verifies the location claims of the sensors before data collection. A suit of techniques in [16] are introduced to detect malicious beacons which can negatively affect the localization of nodes by providing incorrect information. TSCD [17] proposes a novel secure localization approach to defend against the distance-consistent spoofing attack using the consistency check on the distance measurements.

To detect the existence of wormhole attacks, researchers propose some wormhole attack detection approaches. In

[18], *packet leashes* based on the notions of geographical and temporal leashes are proposed to detect the wormhole attack. Wang and Bhargava [19] detect the wormhole attack by means of visualizing the anomalies introduced by incorrect distance measurements between two nodes caused by the wormhole attack. Reference [20] further extends the method in [19] for large scale network by selecting some feature points to reduce the overlapping issue and preserving the major topology features. In [21], a detection scheme is elaborated by checking whether the maximum number of independent neighbors of two nonneighbor nodes is larger than the threshold.

To achieve secure localization in a WSN suffered from wormhole attacks, SeRLoc [9] first detects the wormhole attack based on the *sector uniqueness* property and *communication range violation* property using directional antennas, then filters out the attacked locators. HiRLoc [10] further utilizes antenna rotations and multiple transmit power levels to improve the localization resolution. The schemes in [13] can also be applied into the localization against wormhole attacks. However, SeRLoc and HiRLoc need extra hardware such as directional antennae, and cannot obtain satisfied localization performance in that some attacked locators may still be undetected. Reference [13] requires a large amount of computation and possibly becomes incompetent when malicious locators are more than the legitimate ones. In [22], Chen et al. propose to make each locator build a conflicting-set and then the sensor can use all conflicting sets of its neighboring locators to filter out incorrect distance measurements of its neighboring locators. The limitation of the scheme is that it only works properly when the system has no packet loss. As the attackers may drop the packets purposely, the packet loss is inevitable when the system is under a wormhole attack. Compared to the scheme in [22], the distance-consistency-based secure localization scheme proposed in this paper can obtain high localization performance when the system has certain packet losses. Furthermore, it works well even when the malicious locators are more than the legitimate ones, which causes the malfunction of the scheme in [13].

3. Problem Formulation

In this section, we build the network model and the attack model, describe the related definitions, and analyze the effect of the wormhole attack on the range-based localization, after which we classify the locators into three categories.

3.1. Network Model. Three different types of nodes are deployed in the network, including locators, sensors, and attackers. The locators, with their own locations known in advance (by manual deployment or GPS devices), are deployed independently in the network with the probability of Poisson distribution. Each locator has a unique identification. The attackers collude in pairs to launch a wormhole attack to interfere with the self-localization of the sensors. All the nodes in the network are assumed to have the same transmission range R. However, the communication

range between two wormhole attackers can be larger than R, as they can communicate with each other using certain communication technique.

The sensors measure the distances to their neighboring locators using the Received Signal Strength Indicator (RSSI) method; the measurement error of the distance follows a normal distribution $N(\mu, \sigma)$, where the mean value $\mu = 0$ and the standard deviation σ is within a threshold. The sensors estimate their locations using the Maximum Likelihood Estimation (MLE) method [3]: Assume that the coordinates of the m neighboring locators of the sensor are $(x_1, y_1), (x_2, y_2), (x_3, y_3), \ldots, (x_m, y_m)$, respectively, and the distance measurements from the m locators to the sensor are $d_1, d_2, d_3, \ldots, d_m$, the location of the sensor (x, y) satisfies

$$
\begin{aligned}
(x - x_1)^2 + (y - y_1)^2 &= d_1^2 \\
(x - x_2)^2 + (y - y_2)^2 &= d_2^2 \\
&\vdots \\
(x - x_m)^2 + (y - y_m)^2 &= d_m^2.
\end{aligned}
\tag{1}
$$

By subtracting the last equation from each of the rest in (1), we can obtain the following equations represented as a linear equation $AX = b$, where

$$
A = \begin{bmatrix}
2(x_1 - x_m) & 2(y_1 - y_m) \\
2(x_2 - x_m) & 2(y_2 - y_m) \\
\vdots & \vdots \\
2(x_{m-1} - x_m) & 2(y_{m-1} - y_m)
\end{bmatrix}, \quad X = \begin{bmatrix} x \\ y \end{bmatrix},
$$

$$
b = \begin{bmatrix}
x_1^2 - x_m^2 + y_1^2 - y_m^2 - d_1^2 + d_m^2 \\
x_2^2 - x_m^2 + y_2^2 - y_m^2 - d_2^2 + d_m^2 \\
\vdots \\
x_{m-1}^2 - x_m^2 + y_{m-1}^2 - y_m^2 - d_{m-1}^2 + d_m^2
\end{bmatrix}.
\tag{2}
$$

Using the MLE method, the location of the sensor can be obtained as $\hat{X} = (A^T A)^{-1} A^T b$.

3.2. Attack Model. The network is assumed to be deployed in hostile environment where wormhole attacks exist to disrupt the localization of sensors. During the wormhole attack, one attacker sniffs packets at one point in the network and tunnels them through the wormhole link to another point. Being as external attackers that cannot compromise legitimate nodes or their cryptographic keys, the wormhole attackers cannot acquire the content, for example, the type of the sniffed packets. However, the attackers may drop off the received packets randomly which severely deteriorates the sensor's localization process. We assume that the length of the wormhole link is larger than R so that the endless packet transmission loop caused by both attackers is avoided.

The wormhole attack endured by a node can be classified into *duplex wormhole attack* and *simplex wormhole attack* according to the geometrical relation between the node and the attackers. A node is under a duplex wormhole attack when it lies in the common transmission area of these two attackers; a node is under a simplex wormhole attack when it lies in the transmission area of only one of these two attackers but not in the common transmission area of both. Figure 1 shows the impact of the wormhole attack on the distance measurement of the sensor. When measuring the distance, the sensor broadcasts a request signal and waits for the responding beacon signals from the locators within its neighboring vicinity, based on which the sensor can use the RSSI method to estimate the distances to neighboring locators. For the duplex wormhole attack as shown in Figure 1(a), when L_1 sends a beacon message to the sensor S, S will only get the distance measurement as d_0' instead of the actual distance d_1' because the RSSI received by S just reflects the propagational attenuation from A_1 to S. For L_2's beacon message, as the packet will travel through two different paths to reach S, $L_2 \rightarrow S$ and $L_2 \rightarrow A_2 \rightarrow A_1 \rightarrow S$, respectively, S will obtain two distance measurements d_2' and d_0'. For L_4's beacon message, it travels through three paths to reach S, $L_4 \rightarrow S$, $L_4 \rightarrow A_2 \rightarrow A_1 \rightarrow S$, and $L_4 \rightarrow A_1 \rightarrow A_2 \rightarrow S$, respectively, thus S will get three distance measurements as d_4', d_0', and d_0''. For the simplex wormhole attack as shown in Figure 1(b), when S receives the beacon message from L_5, it will measure the distance to L_5 as d_0. For L_3, two different distance measurements d_3' and d_0 will be obtained. Thus, the locators which can communicate with the sensor via the wormhole link will introduce incorrect distance measurements.

All the locators that can exchange messages with the sensor, either via the wormhole link or not, are called *neighboring locators* (N-locators) of the sensor. Among these neighboring locators, the ones that can exchange messages with the sensor via the wormhole link are called *dubious locators* (D-locators), as their distance measurements may be incorrect and distort the localization; the locators that lie in the transmission range of the sensor are called *valid locators* (V-locators), as the sensor can obtain correct distance measurements with respect to them and assist the localization.

In this paper, we denote the set of N-locators, D-locators, and V-locators as $\mathcal{L}_N, \mathcal{L}_D$, and $\mathcal{L}_V$. For the scenario in Figure 1(a), $\mathcal{L}_N = \{L_1, L_2, L_3, L_4, L_5, L_6, L_7\}$, $\mathcal{L}_D = \{L_1, L_2, L_3, L_4, L_5, L_7\}$, and $\mathcal{L}_V = \{L_2, L_3, L_4, L_6\}$. It is obvious that $\mathcal{L}_N = \mathcal{L}_V \cup \mathcal{L}_D$.

4. Secure Localization Scheme Against Wormhole Attack

As the D-locators will negatively affect the localization of the sensor, it is critical for the sensor to identify the V-locators before the self-localization. In this section, we propose a novel secure localization scheme against wormhole attacks, which includes three phases shown in Figure 2, namely the wormhole attack detection, valid locators identification and self-localization.
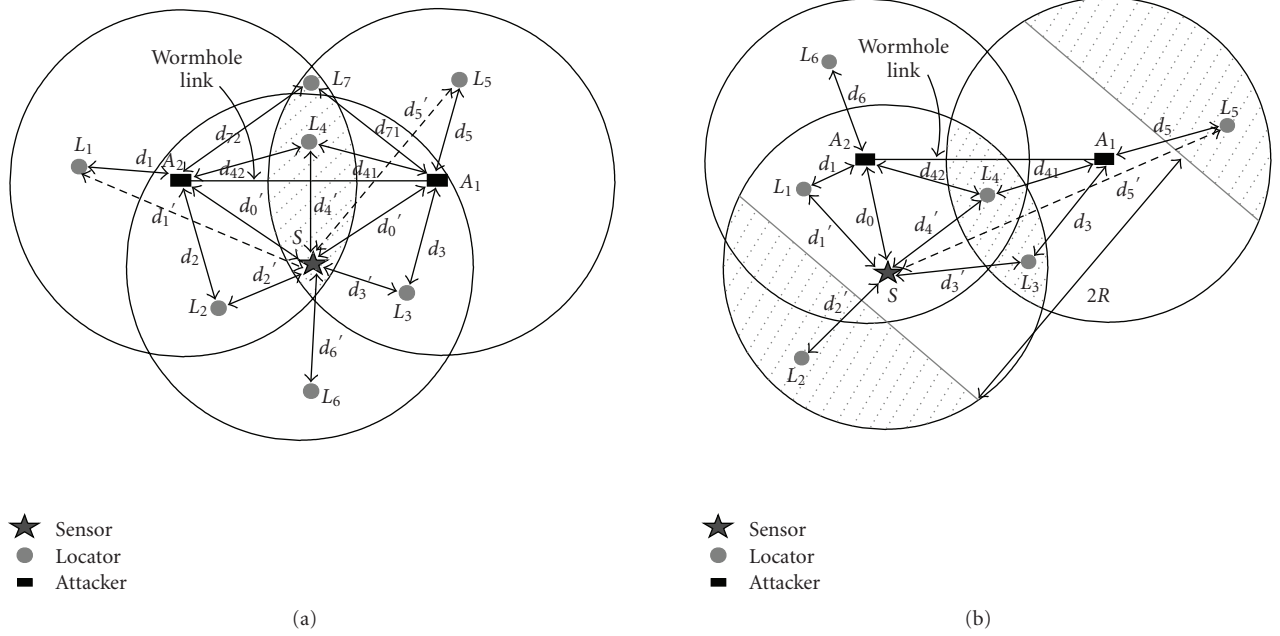
FIGURE 1: Illustrations of wormhole attack: (a) Duplex wormhole attack, (b) Simplex wormhole attack.
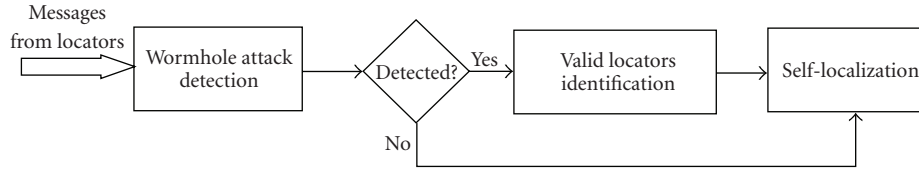

FIGURE 2: Flow chart of the proposed secure localization scheme.

(i) *Wormhole Attack Detection*: The sensor detects the existence of a wormhole attack using the proposed detection schemes, and identifies whether it is under a duplex wormhole attack or a simplex wormhole attack.

(ii) *Valid Locators Identification*: Corresponding to the duplex wormhole attack and the simplex wormhole attack, the sensor identifies the V-locators using different identification approaches.

(iii) *Self-localization*: After identifying enough V-locators, the sensor conducts the self-localization using the MLE method with correct distance measurements.

4.1. Wormhole Attack Detection. We assume that each locator periodically broadcasts a beacon message within its neighboring vicinity. The beacon message will contain the ID and location information of the source locator. When the network is threatened by a wormhole attack, some affected locators will detect the abnormality through beacon message exchanges. The following scenarios are considered abnormal for locators: (1) a locator receives the beacon message sent by itself; (2) a locator receives more than one copy of the same beacon message from another locator via different paths; (3) a locator receives a beacon message from another locator,

whose location calculated based on the received message is outside the transmission range of receiving locator. When the locator detects the message abnormality, it will consider itself under a wormhole attack. Moreover, if the locator detects the message abnormality under the first scenario, that is, the locator receives the beacon message sent by itself, it will further derive that it is under a duplex wormhole attack. The beacon message has two additional bits to indicate these two statuses for each locator:

(i) detection bit: this bit will be set to 1 if the locator detects the message abnormality through beacon message exchanges; otherwise, this bit will be 0;

(ii) type bit: this bit will be 1 if the locator detects itself under a duplex wormhole attack; otherwise, this bit will be 0.

When the sensor performs self-localization, it broadcasts a *Loc_req* message to its N-locators. As soon as the locator receives the *Loc_req* message from the sensor, it replies with an acknowledgement message *Loc_ack* similar to the beacon message, which includes the ID and location information of the locator. The *Loc_ack* message also includes above two status bits. When the sensor receives the *Loc_ack* message, it can measure the distance from the sending locator to itself using the RSSI. The sensor also calculates the response time

of each N-locator based on the Loc_ack message using the approach in [17] to countervail the random delay on the MAC layer of the locator: when broadcasting the Loc_req packet, the sensor records the local time T_0. Every locator gets the local time T_1 by time-stamping the packet at the MAC layer (i.e., the time when the packet is received at the MAC layer) instead of time-stamping the packet at the application layer. Similarly, when responding to the Loc_ack packet, the locator puts the local time T_2 at the MAC layer; both T_1 and T_2 are attached in the Loc_ack packet. When receiving the Loc_ack packet, the sensor gets its local time T_3, and calculates the response time of the locator as $(T_3 - T_0) - (T_2 - T_1)$. Note that this response time only eliminates the random delay at the MAC layer of the locators, but not the delay affected by attackers.

When conducting the localization, the sensor may also detect the message abnormality when it receives the Loc_req message sent by itself. Moreover, the sensor can check the detection bit of the Loc_ack message to decide if its N-locator is under a wormhole attack or not.

We propose to use the following two detection schemes for the sensor to detect the wormhole attack.

Detection Scheme D1. If the sensor S detects that it receives the Loc_req message sent from itself, it can determine that it is currently under a duplex wormhole attack. For example, when the sensor is under the duplex wormhole attack as shown in Figure 1(a), the Loc_req message transmitted by the sensor can travel from A_1 via the wormhole link to A_2 and then arrive at S after being relayed by A_2. Similarly, the Loc_req message can also travel from A_2 through the wormhole link to A_1 and then be received by S. Thus, S can determine that it is currently under a duplex wormhole attack.

Detection Scheme D2. If the sensor S detects that the detection bit of the received Loc_ack message from any N-locator is set to 1, S can determine that it is under a simplex wormhole attack. Note that when using detection scheme D2, the sensor may generate a false alarm if the sensor is outside the transmission areas of the attackers but any of its N-locators is inside the transmission areas of the attackers. However, this will only trigger the validate locators identification process but not affect the self-localization result.

The pseudocode of the wormhole attack detection is shown in Algorithm 1. The sensor broadcasts a Loc_req message for self-localization. When receiving the Loc_req message, each N-locator replies a Loc_ack message with the status bits indicating whether it has detected the abnormality. The sensor measures the distances to its N-locators based on the Loc_ack messages using RSSI method and calculates the response time of each N-locator. If the sensor receives the Loc_req message sent by itself (detection scheme D1), it determines that it is under a duplex wormhole attack. Otherwise, if the sensor is informed by any N-locator that the abnormality is detected (detection scheme D2), it declares that it is under a simplex wormhole attack. If no wormhole attack is detected, the sensor conducts the MLE localization.

1: Sensor broadcasts a Loc_req message.
2: Each N-locator sends a Loc_ack message to the sensor, including the message abnormality detection result.
3: Sensor waits for the Loc_ack messages to measure the distance to each N-locator and to calculate the response time of each N-locator.
4: **if** sensor detects the attack using scheme D1 **then**
5:     A duplex wormhole attack is detected.
6: **else if** sensor detects the attack using scheme D2 **then**
7:     A simplex wormhole attack is detected.
8: **else**
9:     No wormhole attack is detected.
10: **end if**

ALGORITHM 1: Wormhole attack detection scheme.

4.2. Basic Valid Locators Identification Approach

4.2.1. Duplex Wormhole Attack. When detecting that it is currently under a duplex wormhole attack, the sensor tries to identify all its V-locators before the self-localization. Take L_2 in Figure 1(a) for example, when receiving the Loc_req message from the sensor, L_2 will respond a Loc_ack message to the sensor. As the sensor lies in the transmission range of L_2, the Loc_ack message can be received by the sensor directly. In addition, the Loc_ack message can also travel from A_2 via the wormhole link to A_1 then arrive at the sensor. Therefore, the sensor can receive the Loc_ack message from L_2 for more than once. However, there will be three different scenarios: (1) the locator lies in the transmission range of the sensor and its message is received by the sensor for three times (such as L_4 in Figure 1(a)); (2) the locator lies out of the transmission range of the sensor and its message is received by the sensor for twice (such as L_7 in Figure 1(a)); (3) the locator lies in the transmission range of the sensor and its message is received by the sensor for twice (such as L_2 in Figure 1(a)). We can see that L_2 and L_4 are V-locators, but not V_7. The sensor will use the following valid locator identification scheme to find the V-locators.

Identification Scheme I1. When the sensor is under a duplex wormhole attack, if the sensor receives the Loc_ack message of an N-locator for three times and the type bit in the Loc_ack message is set to 1, this N-locator will be considered as a V-locator (such as L_4 in Figure 1(a)). As the sensor only countervails the MAC layer delay of the locators but not that of the attackers when calculating the response time, the message traveling via the wormhole link has taken a longer response time. Thus, the distance measurement based on the Loc_ack message from this V-locator which takes the shortest response time will be considered correct. If the sensor receives the Loc_ack message of an N-locator just twice and the type bit in the Loc_ack message is set to 1, this N-locator will be treated as a D-locator (such as L_7 in Figure 1(a)). For the last scenario, if the sensor receives the Loc_ack message of an N-locator twice and the type bit in the Loc_ack message is set to 0, this N-locator will be

considered as a V-locator, and the distance measurement based on the Loc_ack message with a shorter response time will be considered as correct (such as L_2 in Figure 1(a)).

Distance Consistency Property of Valid Locators. Assuming a set of locators $\mathbb{L} = \{(x_1, y_1), (x_2, y_2), \ldots, (x_m, y_m)\}$ and corresponding measured distances $\mathbb{D} = \{d_1, d_2, \ldots, d_m\}$, where (x_i, y_i) is the location of locator L_i and d_i is the measured distance from the sensor to L_i, $i = 1, 2, \ldots, m$. Based on $\mathbb{L}$ and $\mathbb{D}$, the estimated location of the sensor is $(\tilde{x}_0, \tilde{y}_0)$. The mean square error of the location estimation is $\delta^2 = \sum_{i=1}^{m} [d_i - \sqrt{(\tilde{x}_0 - x_i)^2 + (\tilde{y}_0 - y_i)^2}]^2 / m$. The distance consistency property of valid locators states that the mean square error of the location estimation based on the correct distance measurements is lower than a small threshold while the mean square error of the location estimation based on the distance measurements which contains some incorrect ones is not lower than the threshold.

We can further identify more V-locators using the distance consistency property of valid locators.

Identification Scheme I2. If the sensor has determined no less than two valid locators using identification scheme I1, it can identify other valid locators by checking whether the distance estimation is consistent. A predefined threshold τ^2 of the mean square error is determined, that is, a distance estimation with a mean square error smaller than τ^2 is considered to be consistent. As shown in Figure 1(a), the sensor can identify L_2, L_3, and L_4 as V-locators and obtain the correct distance measurements to them. For other undetermined locators, the sensor can identify them one by one. For example, to check whether L_1 is a V-locator, the sensor can estimate its own location based on the distance measurements to L_1, L_2, L_3, and L_4. As the distance measurement to L_1 is incorrect, the mean square error of the estimated distance measurements may exceed τ^2, which means that L_1 is not a V-locator. When the sensor checks the distance consistency of L_2, L_3, L_4, and L_6, it can get that the mean square error is lower than τ^2, thus L_6 is treated as a V-locator, and the distance measurement to L_6 is correct. After checking each of the undetermined N-locators, the sensor can identify all V-locators with the correct distance measurements.

4.2.2. Simplex Wormhole Attack.
If the sensor detects that it is under a simplex wormhole attack, it will adopt the following valid locators identification schemes.

Identification Scheme I3. When the sensor under a simplex wormhole attack as shown in Figure 1(b), if the sensor receives the Loc_ack message of an N-locator twice, this N-locator will be considered as a V-locator. For example, when L_3 in Figure 1(b) replies a Loc_ack message to the sensor, this message will travel through two different paths to the sensor, one directly from L_3 to the sensor and the other from L_3 to A_1 via the wormhole link to the sensor. Therefore, the sensor can conclude that L_3 is a V-locator. To further obtain the correct distance measurement to L_3, the sensor compares the response times of the Loc_ack message from L_3

through different paths, and the distance measurement with a shorter response time is considered correct. Similarly, L_4 can also be identified as a V-locator and its correct distance measurement can be obtained.

The following spatial property can also be used to identify V-locators:

Spatial Property. The sensor cannot receive messages from two N-locators simultaneously if the distance between these two N-locators is larger than $2R$.

Identification Scheme I4. When the sensor is under a simplex wormhole attack as shown in Figure 1(b), if the spatial property is violated by two N-locators, it is obviously that one of them is a V-locator and the other is a D-locator. Take L_2 and L_5 in Figure 1(b) for example, the distance between them is larger than $2R$, after receiving Loc_ack messages from them, the sensor can detect that the spatial property does not hold by these two N-locators. The response times of both N-locators can be used to differentiate the V-locator from the D-locator. As the Loc_ack message from L_5 travels via the wormhole link to the sensor, it will take a longer response time than that from L_2. The sensor will regard L_2 as a V-locator and L_5 as a D-locator because L_2 has a shorter response time. The distance measurement to L_2 is also considered correct.

We can also use the distance consistency property of valid locators to identify more V-locators when the sensor is under a simplex wormhole attack.

Identification Scheme I5. When the sensor is under a simplex wormhole attack, similar to identification scheme I2, if the sensor detects at least two V-locators using identification schemes I3 and I4, it can identify other V-locators based on the distance consistency property of V-locators. Take the scenario in Figure 1(b) for example, the sensor can identify L_2, L_3, and L_4 as V-locators and obtain the correct distance measurements to them. The sensor can further identify other V-locators by checking the distance consistency. A mean square error smaller than τ^2 can be obtained when the sensor estimates its location based on L_1, L_2, L_3, and L_4 because they are all V-locators. So the sensor can conclude that L_1 is a V-locator and the distance measurement to L_1 is correct.

The procedure of basic valid locators identification approach is listed in Algorithm 2: If the sensor detects that it is under a duplex wormhole attack, it will conduct identification scheme I1 to detect V-locators. As the distance consistency check needs as least three locators, if the sensor identifies no less than two V-locators, it can use identification scheme I2 to identify other V-locators. On the other hand, if the sensor detects that it is under a simplex wormhole attack, it adopts identification schemes I3 and I4 to identify the V-locators. After that, if at least two V-locators are identified, the sensor conducts identification scheme I5 to detect other V-locators.

4.3. Enhanced Valid Locators Identification Approach.
In the basic valid locators identification approach, if the sensor

```
1: if S detects a duplex wormhole attack then
2:     Conduct scheme I1 to identify V-locators.
3:     if the identified  V-locators ≥2 then
4:         Conduct scheme I2 to identify other V-locators.
5:     end if
6: else if S detects a simplex wormhole attack then
7:     Conduct schemes I3 and I4 to identify V-locators.
8:     if the identified V-locators ≥2 then
9:         Conduct scheme I5 to identify other V-locators.
10:     end if
11: end if
```

ALGORITHM 2: Basic Valid Locators Identification Approach.

```
1: if S detects a duplex wormhole attack then
2:     Conduct scheme I1 to identify V-locators.
3:     if the identified V-locators ≥2 then
4:         repeat
5:             Conduct scheme I2 to identify other V-locators.
6:             τ² ⇐ τ² + Δτ²
7:         until the identified V-locators ≥3 or τ² > τ²max
8:     end if
9: else if S detects a simplex wormhole attack then
10:     Conduct schemes I3 and I4 to identify V-locators.
11:     if the identified V-locators ≥2 then
12:         repeat
13:             Conduct scheme I5 to identify other V-locators.
14:             τ² ⇐ τ² + Δτ²
15:         until the identified V-locators ≥3 or τ² > τ²max
16:     end if
17: end if
```

ALGORITHM 3: Enhanced Valid Locators Identification Approach.

identifies less than three V-locators, it will terminate the self-localization because the MLE method used in the self-localization needs at least three distance measurements. However, when using the identification schemes based on distance consistency property of V-locators, many V-locators may not be identified if the threshold of mean square error, τ^2, is set inappropriately a small value.

To overcome the above problem, we propose an enhanced valid locators identification approach which can adaptively adjust the threshold τ^2 to make the sensor easier to identify more V-locators: If the sensor detects that it is under a duplex wormhole attack, it conducts identification scheme I1 to detect V-locators. If the sensor identifies no less than two V-locators, it repeats to identify other V-locators using identification scheme I2 and update the τ^2 with an increment of $\Delta\tau^2$ until at least three V-locators are identified or τ^2 is larger than τ^2_{max}. On the other hand, if the sensor detects that it is under a simplex wormhole attack, it adopts schemes I3 and I4 to identify the V-locators. If at least two V-locators are identified, the sensor repeats to conduct scheme I5 to detect other V-locators and update τ^2 with an increment of $\Delta\tau^2$ until at least three V-locators are identified or τ^2 is larger than τ^2_{max}. The procedure of the enhanced valid locators identification approach is listed in Algorithm 3.

After the wormhole attack detection and valid locators identification, the sensor can identify V-locators from its N-locators. Furthermore, the sensor can estimate the correct distance measurements to the V-locators. When the sensor obtains at least three correct distance measurements to its N-locators, it conducts the MLE localization based on these distance measurements and the locations of the corresponding N-locators.

5. Theoretical Analysis

In this section, we formulate the mathematical models for the probability of wormhole attack detection and the probability of successfully identifying all the V-locators. To simplify our description, we denote the disk centered at U with radius R as $\mathcal{D}_R(U)$. The overlapped region of the transmission areas of two attackers is denoted as D_1 and the overlapped region of the transmission areas of attacker A_1 and sensor S is denoted as D_2, which are illustrated in Figure 3.

5.1. Probability of Wormhole Attack Detection.
For the probability of the wormhole attack detection, we denote it as P_{det}, including the probability of the duplex wormhole attack detection P^D_{det} and the probability of the simplex wormhole attack detection P^S_{det}. Thus,

$$P_{det} = P^D_{det} + P^S_{det}. \tag{3}$$

For P^D_{det}, it equals to the probability that the sensor lies in the region D_1. Therefore,

$$P^D_{det} = \frac{D_1}{\pi R^2}. \tag{4}$$

Here,

$$D_1 = 2R^2 \arccos\frac{L}{2R} - L\sqrt{R^2 - \frac{L^2}{4}}, \tag{5}$$

where L is the length of the wormhole link.

For P^S_{det}, the probability that the sensor lies in region $\mathcal{D}_R(A_2) \setminus D_1$ in Figure 3 equals to $(\pi R^2 - D_1)/\pi R^2$. When the sensor lies in this region, the sensor can detect the wormhole attack only if at least one locator lies in D_1 or each of the regions $\mathcal{D}_R(A_2) \setminus D_1$ and $\mathcal{D}_R(A_1) \setminus D_1$ in Figure 3 has at least one locator, which means that the N-locators can detect the abnormality and inform the sensor. We define the event that at least one locator lies in D_1 as A and the event that each of the regions $\mathcal{D}_R(A_2) \setminus D_1$ and $\mathcal{D}_R(A_1) \setminus D_1$ in Figure 3 has at least one locator as B. Thus,

$$P^S_{det} = \frac{\pi R^2 - D_1}{\pi R^2}\left(P(A) + P(\overline{A})P(B)\right). \tag{6}$$

As the locators follow Poisson distribution, we get

$$P(A) = 1 - e^{-D_1\rho_l}$$
$$P(B) = \left[1 - e^{-(\pi R^2 - D_1)\rho_l}\right]^2, \tag{7}$$
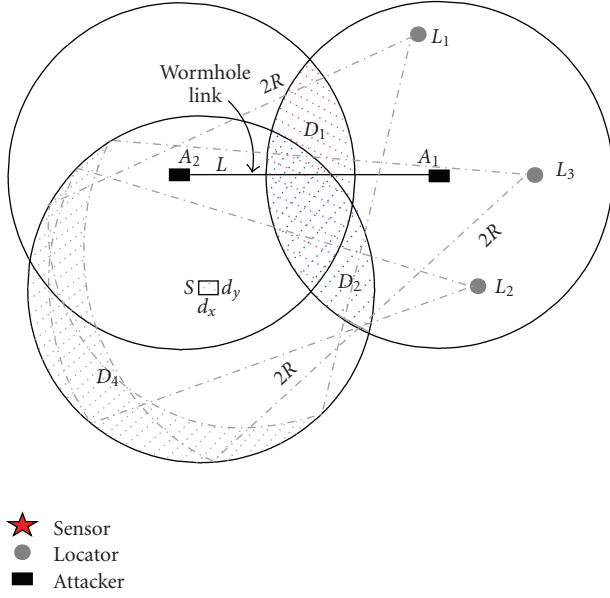
★ Sensor
● Locator
■ Attacker

FIGURE 3: Theoretical analysis of the mathematical model of a wormhole attack.

where ρ_l is the density of the locators. Therefore, the probability that the sensor can detect the simplex wormhole attack can be expressed as follows:

$$
\begin{aligned}
P_{\det}^S &= \frac{\pi R^2 - D_1}{\pi R^2} \left\{ 1 - e^{-D_1 \rho_l} + e^{-D_1 \rho_l} \left[1 - e^{-(\pi R^2 - D_1)\rho_l} \right]^2 \right\} \\
&= \frac{\pi R^2 - D_1}{\pi R^2} \left\{ 1 - e^{-\pi R^2 \rho_l} \left[2 - e^{-(\pi R^2 - D_1)\rho_l} \right] \right\}.
\end{aligned}
$$

(8)

Therefore, we can get

$$
\begin{aligned}
P_{\det} &= P_{\det}^D + P_{\det}^S \\
&= \frac{D_1}{\pi R^2} + \frac{\pi R^2 - D_1}{\pi R^2} \left\{ 1 - e^{-\pi R^2 \rho_l} \left[2 - e^{-(\pi R^2 - D_1)\rho_l} \right] \right\} \\
&= 1 - \frac{\pi R^2 - D_1}{\pi R^2} e^{-\pi R^2 \rho_l} \left[2 - e^{-(\pi R^2 - D_1)\rho_l} \right].
\end{aligned}
$$

(9)

5.2. Probability of Successfully Identifying All V-locators. For the probability that the sensor can successfully identify all the V-locators, we denote it as P_{ide}. Similarly,

$$
P_{\text{ide}} = P_{\text{ide}}^D + P_{\text{ide}}^S,
$$

(10)

where P_{ide}^D is the probability that the sensor can successfully identify all the V-locators when under a duplex wormhole attack, and P_{ide}^S is for the simplex wormhole attack.

The probability that the sensor is under a duplex wormhole attack equals to $D_1/\pi R^2$ as shown in Figure 3. The sensor is capable of successfully identifying all the V-locators under a duplex wormhole attack means that it can identify at least two V-locators using identification scheme I1. That is,

the region $(\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)) \cap \mathcal{D}_R(S)$ in Figure 1(a) has at least two locators. Thus,

$$
\begin{aligned}
P_{\text{ide}}^D &= \frac{D_1}{\pi R^2} \left(1 - e^{-D_3 \rho_l} - D_3 \rho_l e^{-D_3 \rho_l} \right) \\
&= \frac{D_1}{\pi R^2} \left[1 - e^{-D_3 \rho_l} \left(1 + D_3 \rho_l \right) \right],
\end{aligned}
$$

(11)

where

$$
D_1 = 2R^2 \arccos \frac{L}{2R} - L \sqrt{R^2 - \frac{L^2}{4}}
$$

(12)

and D_3 is the area of $(\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)) \cap \mathcal{D}_R(S)$ in Figure 1(a). We can approximate D_3 by

$$
D_3 \approx D_{\mathcal{D}_R(A_2) \cap \mathcal{D}_R(S)} + D_2,
$$

(13)

where

$$
D_2 = 2R^2 \arccos \frac{L'}{2R} - L' \sqrt{\left(R^2 - \frac{L'^2}{4} \right)},
$$

$$
L' = \sqrt{(x - L)^2 + y^2}.
$$

(14)

We can get

$$
\begin{aligned}
D_3 &\approx 2R^2 \arccos \frac{L'}{2R} - L' \sqrt{\left(R^2 - \frac{L'^2}{4} \right)} \\
&\quad + 2R^2 \arccos \frac{\sqrt{x^2 + y^2}}{2R} - \sqrt{(x^2 + y^2) \left(R^2 - \frac{x^2 + y^2}{4} \right)}.
\end{aligned}
$$

(15)

When the sensor is under a wormhole attack, the probability that it lies in the $dxdy$ domain in Figure 3 equals to $dxdy/\pi R^2$. When lying in the $dxdy$ domain, if the sensor can identify at least two V-locators using identification schemes I3 and I4, it can successfully identify other V-locators. Assuming that the sensor can identify m V-locators using scheme I3 and identify n V-locators using scheme I4, the probability that the sensor can identify at least two V-locators using schemes I3 and I4 is calculated as

$$
\begin{aligned}
&1 - P(m = 0)P(n = 0) - P(m = 0)P(n = 1) \\
&\quad - P(m = 1)P(n = 0),
\end{aligned}
$$

(16)

where

$$
\begin{aligned}
P(m = 0) &= e^{-D_2 \rho_l}, &\quad P(m = 1) &= D_2 \rho_l e^{-D_2 \rho_l}, \\
P(n = 0) &= e^{-D_4 \rho_l}, &\quad P(n = 1) &= D_4 \rho_l e^{-D_4 \rho_l}.
\end{aligned}
$$

(17)

Here, D_4 is the region in $\mathcal{D}_R(S)$ which is more than $2R$ away from at least one of the locators in $\mathcal{D}_R(A_1)$, that is the area of the corresponding shading region D_4 in Figure 3. Note that if any locator lies in D_4, the sensor can identify it as a V-locator using identification scheme I4.
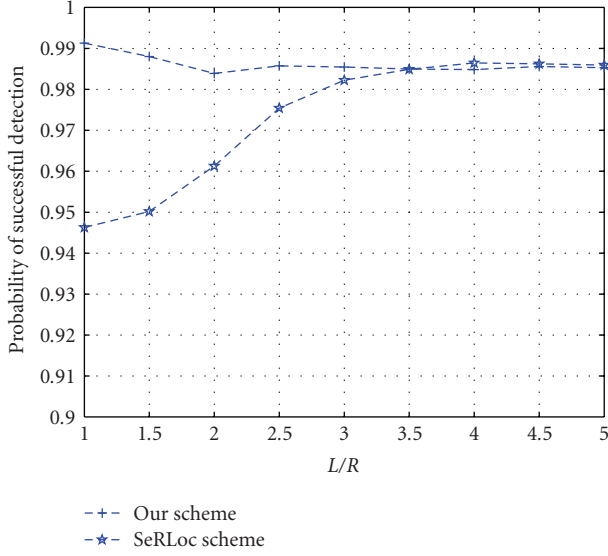
FIGURE 4: Probability of wormhole attack detection: Our scheme versus SeRLoc scheme.

FIGURE 5: Probability of wormhole attack detection: Simulation versus Theoretical.

Thus,

$$P_{ide}^{S} = \frac{1}{\pi R^2} \iint_{\mathcal{D}_R(A_2) \backslash D_1} P_{xy} \, dx \, dy, \tag{18}$$

where

$$P_{xy} = 1 - e^{-(D_2+D_4)\rho_l} \left[1 + (D_2 + D_4)\rho_l \right]. \tag{19}$$

Therefore, we can obtain

$$P_{ide} = \frac{D_1}{\pi R^2} \left[1 - e^{-D_3\rho_l} (1 + D_3\rho_l) \right] + \frac{1}{\pi R^2} \iint_{\mathcal{D}_R(A_2) \backslash D_1} P_{xy} \, dx \, dy. \tag{20}$$

6. Simulation Evaluation

In this section, we present the simulation results to demonstrate the effectiveness of the proposed secure localization scheme and to validate our theoretical results. The network parameters are set as follows: the transmission range R of all types of nodes is identical and is set to 15 m; the density of locators $\rho_l = 0.006/\text{m}^2$ (with the average degree around 4); the standard deviation of the distance measurement $\sigma = 0.5$; the label L/R of the x axis denotes the ratio of the length of the wormhole link (i.e., the distance between two attackers) to the transmission range. The threshold for the distance consistency $\tau^2 = 1$. For the enhanced secure localization scheme, $\Delta\tau^2 = 1$ and $\tau_{max}^2 = 5$.

Figure 4 demonstrates the performance comparison of the probability of detecting the wormhole attack between our scheme and SeRLoc scheme. It can be observed that our scheme obtains a good performance with the probabilities higher than 98% for different values of L/R. Although both schemes have the similar performance when $L/R > 3.5$, our scheme outperforms SeRLoc scheme, especially when $L/R < 2$.
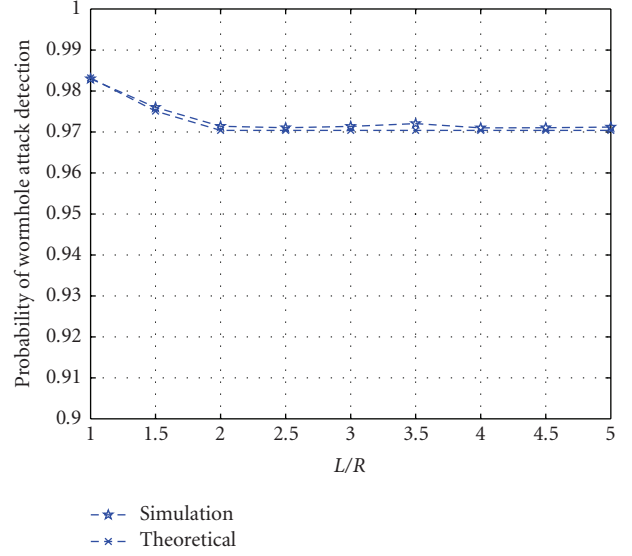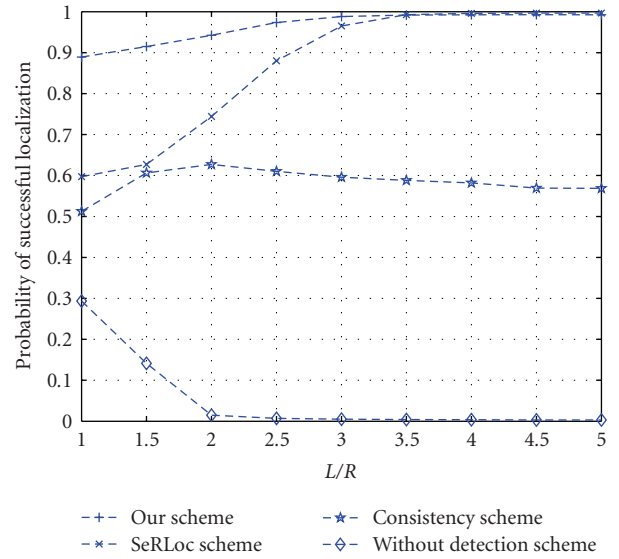

FIGURE 6: Probability of successful localization.

Figure 5 demonstrates the validity of our theoretical analysis on the probability of the wormhole attack detection. We find that the maximum difference between the simulation and the theoretical result is smaller than 0.4%, which indicates that the theoretical result matches the simulation result very well.

Figure 6 shows the performance comparison, in terms of the probability of successful localization, of our proposed basic scheme, SeRLoc scheme, the consistency scheme [13], and the scheme without any detection process when the sensor is under a wormhole attack. The SeRLoc scheme first identifies some D-locators using the sector uniqueness property and communication range violation property, then conducts self-localization based on the rest locators. However, SeRLoc scheme does not distinguish the duplex
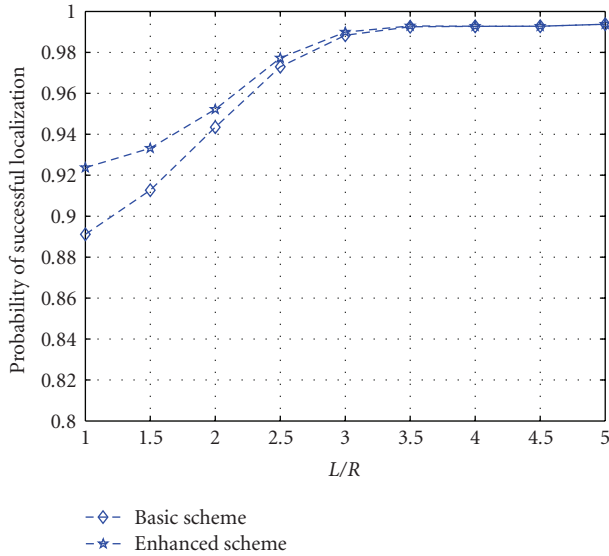
FIGURE 7: Probability of successful localization: Basic scheme versus Enhanced scheme.

FIGURE 8: Probability of successful localization under different locator densities.

FIGURE 9: Probability of successfully identifying all *V*-locators: Simulation versus Theoretical.

wormhole attack and simplex wormhole attack, and the communication range violation property may be invalid under the duplex wormhole attack. The consistency scheme identifies the *D*-locators based on the consistency check of the estimation result. The locator which is the most inconsistent one will be considered as a *D*-locator. In this simulation, the localization result is considered successful when $d_{err1} \leq d_{err2} + f_{tol} * R$, where d_{err1} (and d_{err2}) denotes the localization error with (and without) using the secure localization scheme, f_{tol} is the factor of localization error tolerance (0.1 in our simulations). The performance of the scheme without any detection process shows the severe impact of the wormhole attack on the localization process, which makes the localization totally defunct when *L/R* is larger than 2. Figure 6 shows that our proposed scheme obtains much better performance than the other schemes.

Figure 7, we compare the basic secure localization scheme with the enhanced secure localization scheme. The enhanced scheme outperforms the basic scheme a bit higher (with the maximum improvement of about 3%) when *L/R* < 3.

Figure 8 shows the performance of successful localization of the enhanced scheme under different locator densities. It demonstrates that the increase of the locator density has a greater improvement when *L/R* < 3 than when *L/R* > 3.

Figure 9 is to validate the correctness of the theoretical result of the probability of successfully identifying all *V*-locators. The maximum difference between the simulation and the theoretical result is about 4%, showing that the theoretical result matches the simulation result well.

7. Conclusion and Future Work

In this paper, we analyze the impact of the wormhole attack on the range-based localization. We propose a novel distance-consiste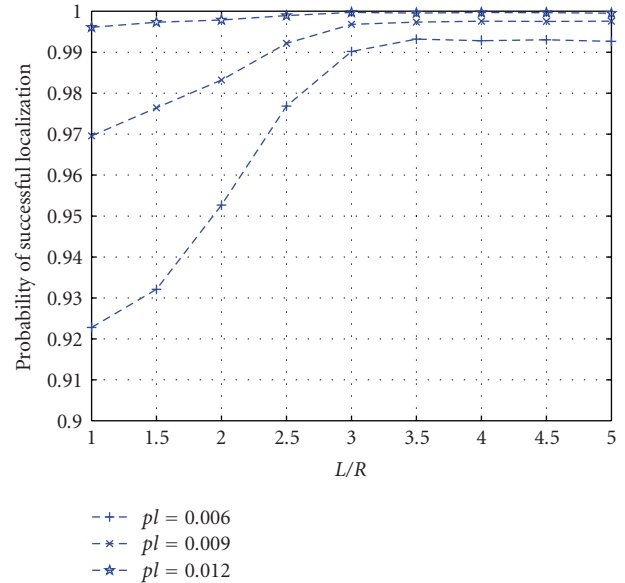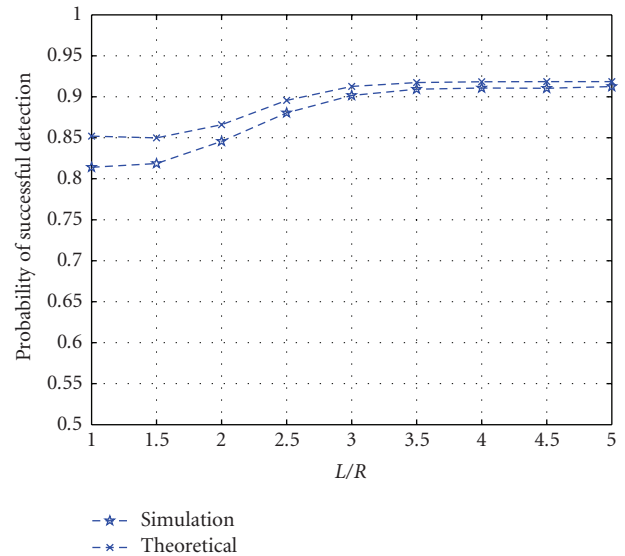ncy-based secure localization mechanism against wormhole attacks including the wormhole attack detection, valid locators identification and self-localization. To analyze the performance of our proposed scheme, we build the theoretical model for calculating the probability of detecting the wormhole attack and the probability of identifying all *V*-locators. We also present the simulation results to demonstrate the out-performance of our schemes and the validity of the proposed theoretical analysis. Although the proposed approach is described based on the RSSI method, it can be easily applied to the localization approaches based on the time-of-arrival (ToA) or time-difference-of-arrival (TDoA) methods.

In the future, our work will focus on the secure localization when the sensor is under multiple wormholes' attack simultaneously. We also intend to consider the secure localization when different nodes have different transmission ranges.

Acknowledgments

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, 2002.

[2] A. Savvides, C. Han, and M. Strivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proceedings of the ACM Annual International Conference on Mobile Computing and Networking (MOBICOM '01)*, pp. 166–179, Rome, Italy, July 2001.

[3] M. Zhao and S. D. Servetto, "An analysis of the maximum likelihood estimator for localization problems," in *Proceedings of the 2nd International Conference on Broadband Networks (ICBN '05)*, pp. 59–67, Boston, Mass, USA, October 2005.

[4] P. Bahl and V. N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system," in *Proceedings of the 9th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '00)*, vol. 2, pp. 775–784, Tel Aviv, Israel, March 2000.

[5] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust statistical methods for securing wireless localization in sensor networks," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05)*, pp. 91–98, Los Angeles, Calif, USA, April 2005.

[6] G. Mao, B. Fidan, and B. D. O. Anderson, "Wireless sensor network localization techniques," *Computer and Telecommunications Networking*, vol. 51, no. 10, pp. 2529–2553, 2007.

[7] S. Capkun and J. P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *Proceedings of the 24th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '05)*, vol. 2, pp. 1917–1928, March 2005.

[8] M. Khabbazian, H. Mercier, and V. K. Bhargava, "Wormhole attack in wireless ad hoc networks: analysis and countermeasure," in *Proceedings of the Global Telecommunications Conference (GLOBECOM '06)*, San Francisco, Calif, USA, December 2006.

[9] L. Lazos and R. Poovendran, "SeRLoc: robust localization for wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 1, no. 1, pp. 73–100, 2005.

[10] L. Lazos and R. Poovendran, "HiRLoc: high-resolution robust localization for wireless sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 233–246, 2006.

[11] A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Secure localization algorithms for wireless sensor networks," *IEEE Communications Magazine*, vol. 46, no. 4, pp. 96–101, 2008.

[12] A. Srinivasan and J. Wu, "A survey on secure localization in wireless sensor networks," in *Encyclopedia of Wireless and Mobile Communications*, 2007.

[13] D. Liu, P. Ning, and W. Du, "Attack-resistant location estimation in sensor networks," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05)*, pp. 99–106, Los Angeles, Calif, USA, April 2005.

[14] S. Capkun, M. Cagalj, and M. Srivastava, "Secure localization with hidden and mobile base stations," in *Proceedings of the 25th IEEE International Conference on Computer Communications Societies (INFOCOM '06)*, Barcelona, Spain, April 2006.

[15] L. Lazos, R. Poovendran, and S. Capkun, "ROPE: robust position estimation in wireless sensor networks," in *Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05)*, pp. 324–331, Los Angeles, Calif, USA, April 2005.

[16] D. Liu, P. Ning, and W. Du, "Detecting malicious beacon nodes for secure location discovery in wireless sensor networks," in *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS '05)*, June 2005.

[17] H. Chen, W. Lou, J. Ma, and Z. Wang, "TSCD: a novel secure localization approach for wireless sensor networks," in *Proceedings of the 2nd International Conference on Sensor Technologies and Applications (SensorComm '08)*, pp. 661–666, Cap Esterel, France, August 2008.

[18] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Proceedings of the 22nd Annual Conference of the IEEE Computer and Communications Societies (INFOCOM '03)*, vol. 3, pp. 1976–1986, San Franciso, Calif, USA, April 2003.

[19] W. Wang and B. Bhargava, "Visualization of wormholes in sensor networks," in *Proceedings of the ACM Workshop on Wireless Security (WiSec '04)*, pp. 51–60, New York, NY, USA, 2004.

[20] W. Wang and A. Lu, "Interactive wormhole detection and evaluation," *Information Visualization*, vol. 6, no. 1, pp. 3–17, 2007.

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

[22] H. Chen, W. Lou, and Z. Wang, "Conflicting-set-based wormhole attack resistant localization in wireless sensor networks," in *Proceedings of the 6th International Conference on Ubiquitous Intelligence and Computing (UIC '09)*, Brisbane, Australia, July 2009.