A Consistency-Based Secure Localization Scheme against Wormhole Attacks in WSNs*

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

[1] Department of Computing,
The Hong Kong Polytechnic University, Kowloon, Hong Kong
{cshlchen,csweilou}@comp.polyu.edu.hk
[2] State Key Laboratory of Industry Control Technology,
Zhejiang University, Hangzhou, P.R. China
wangzhizju@gmail.com

Abstract. Wormhole attacks can negatively affect the localization in wireless sensor networks. A typical wormhole attack can be launched by two colluding external attackers, one of which sniffs packets at one point in the network, tunnels them through a wired or wireless link to another point, and the other of which relays them within its vicinity. In this paper, we investigate the impact of the wormhole attack on the localization process and propose a novel consistency-based secure localization scheme against wormhole attacks, which includes wormhole attack detection, valid locators identification and self-localization. We also conduct the simulations to demonstrate the effectiveness of our proposed scheme.

Keywords: Consistency, secure localization, wormhole attack, wireless sensor networks.

1 Introduction

Wireless sensor networks (WSNs) 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 inter-node measurements such as distance measurements or hop counts. Localization in WSNs has drawn growing attention from the researchers and many range-based and range-free approaches [1, 2, 3] have been proposed. However, most of the localization systems are vulnerable under the hostile environment where malicious attacks, such as the *replay attack* or *compromise attack* [4], can disturb the localization procedure. Security, therefore, becomes a significant concern of the localization process in hostile environments.

The *wormhole attack* is a typical kind of secure attacks in WSNs. It is launched by two colluding *external attackers* [4] which cannot compromise legitimate nodes or their cryptographic keys. One of the wormhole attackers overhears packets at one point

* This work is supported in part by grants PolyU 5236/06E, PolyU 5232/07E, PolyU 5243/08E, ZJU-SKL ICT0903, and NSFC No. 60873223 and No. 90818010.

B. Liu et al. (Eds.): WASA 2009, LNCS 5682, pp. 368–377, 2009.

in the network, tunnels them through the wormhole link to another point in the network, and the other wormhole attacker broadcasts the packets among its neighborhood nodes. This may cause a severe impact on the routing and localization procedures in WSNs. Khabbazian et al. [5] 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 have been proposed [6, 7]; however, range-based approaches have not been well addressed.

In this paper, we propose a consistency-based secure localization scheme to defend against the wormhole attack on the range-based localization. It makes the following contributions: 1) A novel wormhole attack detection scheme is proposed to detect the existence of a wormhole attack and further distinguish the types of the wormhole attack; 2) A valid locator identification approach is designed to identify the valid neighboring locators of the sensor. Two independent algorithms are proposed to handle different wormhole attacks; 3) The simulations are conducted to demonstrate that our proposed scheme outperforms other existing schemes.

2 Related Work

The secure localization in hostile environment has been investigated for several years and many secure localization systems have been proposed.

To resist the compromise attack, Liu et al. [8] propose the range-based and range-free secure localization schemes respectively. SPINE [4] utilizes the verifiable multilateration and verification of positions into the secure localization in hostile network. ROPE [9] is a robust positioning system with a location verification mechanism that verifies the location claims of the sensors before data collection. TSCD [10] 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 [11], *packet leashes* based on the notions of geographical and temporal leashes is proposed to detect the wormhole attack. Wang et al. [12] detect the wormhole attack by means of visualizing the anomalies introduced by incorrect distance measurements between two nodes caused by the wormhole attack. [13] further extends the method in [12] for large scale network by selecting some feature points to reduce the overlapping issue and preserving the major topology features. In [14], a detection scheme is elaborated by checking whether the maximum number of independent neighbors of two non-neighbor nodes is larger than the threshold.

To achieve secure localization in a WSN suffered from wormhole attacks, SeRLoc [6] detects the wormhole attack based on the *sector uniqueness* property and *communication range violation* property, then filters out the attacked locators. HiRLoc [7] further utilizes antenna rotations and multiple transmit power levels to improve the localization resolution. The schemes in [8] can also be applied into the localization against wormhole attacks. However, SeRLoc and HiRLoc needs extra hardware such as directional antennae and cannot obtain satisfied localization performance in that some attacked locators may still be undetected. [8] requires a large amount of computation and possibly becomes incompetent when malicious locators are more than the legitimate ones. In [15], 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 [15], the 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 [8].

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 randomly deployed in an Euclidean two-dimensional plane. The location-unknown sensors conduct self-localization based on their distances to neighboring locators. The attackers collude in pair to launch a wormhole attack to disrupt the localization of the sensors. All the nodes 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. For simplicity, we assume that the measurement error of the distance follows a normal distribution $N(\mu, \sigma)$ with the mean value $\mu = 0$ and the standard deviation σ. The sensors estimate their locations using the Maximum Likelihood Estimation (MLE) method [2].

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, 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, e.g., the type, of the sniffed packets. However, the attackers can drop off the sniffed packets purposely to further deteriorate the sensor's localization process. The length of the wormhole link is assumed to be larger than R to avoid the endless packet transmission loops caused by the both attackers.

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

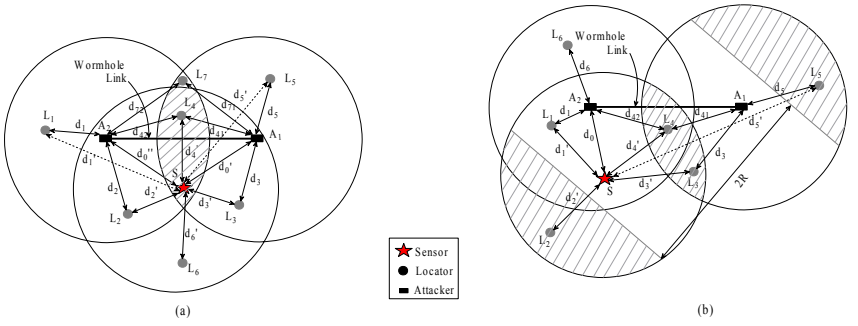


Fig. 1. (a) Duplex wormhole attack; (b) Simplex wormhole attack

common transmission area of the two attackers. On the other hand, a node is under a simplex wormhole attack when it lies in the transmission area of only one of the two attackers but not in the common transmission area. Fig. 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 Fig. 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 Fig. 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 which 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 which can exchange messages with the sensor via the wormhole link are called *dubious locators* (D-locators), as their distance measurements may be incorrect and mislead the localization; the locators which 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 Fig. 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

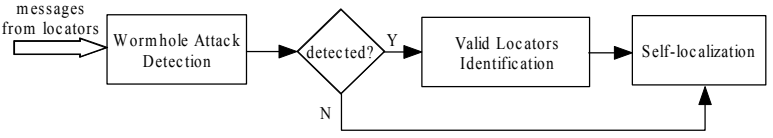


Fig. 2. Flow chart of the proposed secure localization scheme

propose a novel secure localization scheme against wormhole attack, which includes three phases shown in Fig. 2, namely wormhole attack detection, valid locators identification and self-localization:

- *Wormhole Attack Detection:* The sensor detects the wormhole attack using the proposed detection schemes and identifies the type of the wormhole attack.
- *Valid Locators Identification:* Corresponding to the duplex wormhole attack and the simplex wormhole attack, the sensor identifies the V-locators using different identification approaches.
- *Self-localization:* After identifying enough V-locators, the sensor conducts the self-localization using the MLE method with the 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 which 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, i.e., 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:

- 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;
- 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 [10] to countervail the random delay on the MAC layer of the locator.

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 Fig. 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. 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 the 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 V-locators identification but not affect the self-localization result.

Algorithm 1. Wormhole Attack Detection Scheme

```
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.
```

The pseudocode of 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 including 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, it determines that it is under duplex wormhole attack. Otherwise, if the sensor is informed by any N-locator that the abnormality is detected, it declares that it is under simplex wormhole attack. If no wormhole attack is detected, the sensor conducts the MLE localization.

4.2 Valid Locators Identification Approach

Duplex Wormhole Attack: When detecting that it is currently under a duplex wormhole attack, the sensor tries to identify all its V-locators for secure localization. Take L_2 in Fig. 1(a) for example, when receiving the *Loc_req* message from the sensor, L_2 responds a *Loc_ack* message. 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 Fig. 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 Fig. 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 Fig. 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 from a 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 Fig. 1(a)). As the sensor only countervails the MAC layer delay of the locators but not the attackers when calculating the response time, the message traveling via the wormhole link is considered to take 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 a N-locator for 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 Fig. 1(a)). For the last scenario, if the sensor receives the *Loc_ack* message of a N-locator for 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 Fig. 1(a)).

Distance consistency property of V-locators: Assuming a set of locators $\mathbb{L} = \{(x_1, y_1), (x_2, y_2), ..., (x_m, y_m)\}$ and corresponding measured distances $\mathbb{D} = \{d_1, d_2, ..., d_m\}$, where (x_i, y_i) is the location of L_i and d_i is the measured distance from the sensor to L_i, $i = 1, 2, ..., m$. 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 $\delta^2 = \sum_{i=1}^{m} \frac{[d_i - \sqrt{(\tilde{x}_0 - x_i)^2 + (\tilde{y}_0 - y_i)^2}]^2}{m}$. The distance consistency property of V-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 that threshold.

Identification scheme I2: If the sensor determines no less than two V-locators using the identification scheme I1, it can identify other V-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 Fig. 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 location 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.

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 is under a simplex wormhole attack as shown in Fig. 1(b), if it receives the *Loc_ack* message from a N-locator twice, this N-locator will be considered as a V-locator. For example, when L_3 in Fig. 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 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 one 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.

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 Fig. 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. For instance, the distance between L_2 and L_5 in Fig. 1(b) is larger than $2R$, after receiving *Loc_ack* messages from them, the sensor can detect that the spatial property is broken. 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 the locator with a shorter response time (L_2 in this case) as a V-locator, and the other (L_5) as a D-locator. The distance measurement to L_2 is also considered correct.

Identification scheme I5: When the sensor is under a simplex wormhole attack, similar to the identification scheme I2, if the sensor detects at least two V-locators using the identification schemes I3 and I4, it can identify other V-locators based on the distance consistency property of V-locators. Take the scenario in Fig. 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 L_1 is a V-locator and the distance measurement to L_1 is correct.

The procedure of valid locators identification approach is listed in Algorithm 2: If the sensor detects that it is under a duplex wormhole attack, it will conduct the identification scheme I1 to identify V-locators. As the distance consistency check needs as least 3 locators, if the sensor identifies no less than 2 V-locators, it can use the 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 the identification schemes I3 and I4 to identify the V-locators. After that, if at least 2 V-locators are identified, the sensor conducts the scheme I5 to detect other V-locators.

5 Simulation Evaluation

In this section, we present the simulation results to demonstrate the effectiveness of the proposed consistency-based secure localization scheme. The network parameters are set as follows: the transmission range R of all types of nodes is set as $15m$; the standard deviation of the distance measurement $\sigma = 0.5$; the threshold for the distance

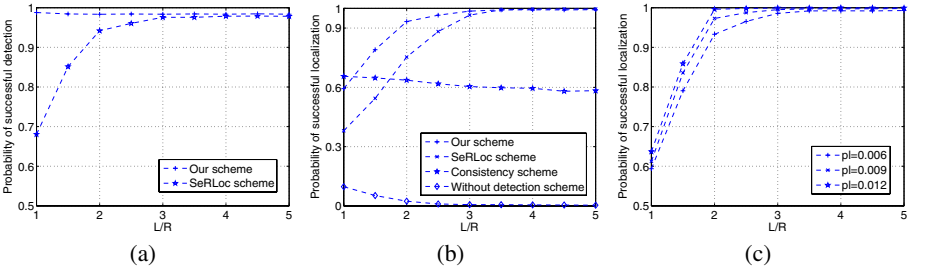
Algorithm 2. Valid Locators Identification Approach

```
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:         Conduct scheme I2 to identify other V-locators.
5: else if S detects a simplex wormhole attack then
6:     Conduct schemes I3 and I4 to identify V-locators.
7:     if the identified V-locators ≥ 2 then
8:         Conduct scheme I5 to identify other V-locators.
```

consistency $\tau^2 = 1$; the network packet loss rate is 5%. We show the performance results of the proposed scheme when the density of locators, denoted as ρ_l, and the ratio of the length of the wormhole link (i.e., the distance between two attackers) to the transmission range, denoted as L/R, are various.

Fig. 3(a) demonstrates the performance comparison of wormhole attack detection probability between our scheme and SeRLoc scheme when $\rho_l = 0.006/m^2$ (with the average degree around 4) and L/R is from 1 to 5. It can be observed that our scheme obtain a performance with the probability higher than 97%. Although the two schemes gain the similar performance when $L/R > 3.5$, our scheme outperforms SeRLoc scheme, especially when $L/R < 2$.

Fig. 3(b) shows the performance of our proposed scheme, SeRLoc scheme, the consistency scheme [8] and the scheme without any detection process when $\rho_l = 0.006/m^2$ and L/R is from 1 to 5. The SeRLoc scheme identifies some D-locators first, then conducts self-localization based on the rest locators. However, SeRLoc scheme does not distinguish the duplex wormhole attack and simplex wormhole attack, and it may be invalid when 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. The localization result is considered as 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 the error tolerance of the localization (f_{tol} is set as 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 fail when L/R is larger than 2. Fig. 3(b) shows that our proposed scheme obtains much better performance than the other schemes.



(a) (b) (c)

Fig. 3. Performance evaluation: (a) Probability of wormhole attack detection; (b) Probability of successful localization; (c) Probability of successful localization under different locator densities

Fig. 3(c) shows the performance of successful localization of the proposed scheme under different locator densities. We can see that the increase of locator density only has some slight improvement on the probability of the successful localization.

6 Conclusion and Future Work

In this paper, we analyze the impact of the wormhole attack on the range-based localization. We propose a novel consistency-based secure localization mechanism against wormhole attacks. The simulation results are presented to demonstrate the effectiveness of our proposed scheme on the wormhole attack detection and secure localization. Although the proposed approach is described based on the RSSI method, it can be easily applied to the localization based on the time-of-arrival or time-difference-of-arrival methods. In the future, our work will focus on the secure localization when the sensor is under multiple wormholes' attack simultaneously and we also intend to consider the secure localization when different nodes have different transmission radii.

References

1. Savvides, A., Han, C., Srivastava, M.: Dynamic Fine-Grained Localization in Ad-hoc Networks of Sensors. In: Proc. of ACM MOBICOM (2001)
2. Zhao, M., Servetto, S.D.: An Analysis of the Maximum Likelihood Estimator for Localization Problems. In: Proc. of IEEE ICBN (2005)
3. Bahl, P., Padmanabhan, V.N.: RADAR:An In-building RF-based User Location and Tracking System. In: Proc. of IEEE INFOCOM (2000)
4. Capkun, S., Hubaux, J.P.: Secure Positioning of Wireless Devices with Application to Sensor Networks. In: Proc. of IEEE INFOCOM (2005)
5. Khabbazian, M., Mercier, H., Bhargava, V.K.: Wormhole Attack in Wireless Ad Hoc Networks: Analysis and Countermeasure. In: Proc. of IEEE GLOBECOM (2006)
6. Lazos, L., Poovendran, R.: SeRLoc: Robust Localization for Wireless Sensor Networks. ACM Trans. on Sensor Networks, 73–100 (2005)
7. Lazos, L., Poovendran, R.: HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks. IEEE Journal on Selected Areas in Communications 24, 233–246 (2006)
8. Liu, D., Ning, P., Du, W.: Attack-Resistant Location Estimation in Sensor Networks. In: Proc. of IEEE IPSN (2005)
9. Lazos, L., Poovendran, R., Capkun, S.: ROPE: Robust Position Estimation in Wireless Sensor Networks. In: Proc. of IEEE IPSN (2005)
10. Chen, H., Lou, W., Ma, J., Wang, Z.: TSCD: A Novel Secure Localization Approach for Wireless Sensor Networks. In: Proc. of the 2nd Int'l Conf. on Sensor Technologies and Applications (2008)
11. Hu, Y.C., Perrig, A., Johnson, D.B.: Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks. In: Proc. of IEEE INFOCOM (2003)
12. Wang, W., Bhargava, B.: Visualization of Wormholes in Sensor Networks. In: Proc. of ACM WiSe (2004)
13. Wang, W., Lu, A.: Interactive wormhole detection and evaluation. Information Visualization 6, 3–17 (2007)
14. Maheshwari, R., Gao, J., Das, S.R.: Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information. In: Proc. of IEEE INFOCOM (2007)
15. Chen, H., Lou, W., Wang, Z.: Conflicting-Set-Based Wormhole Attack Resistant Localization in Wireless Sensor Networks. In: Proc. of the 6th International Conference on Ubiquitous Intelligence and Computing (2009)