Secure Localization Against Wormhole Attacks Using Conflicting Sets

Honglong Chen[1], Wei Lou[1], Zhi Wang[2]
[1]Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong
[2]State Key Lab of Industrial Control Technology, Zhejiang University, Hangzhou, China
Email: {cshlchen, csweilou}@comp.polyu.edu.hk, wangzhi@iipc.zju.edu.cn

Abstract

The wormhole attack is a severe attack that can be easily mounted on a wide range of wireless networks without compromising any cryptographic quantity or network node. In the wormhole attack, an attacker sniffs packets at one point in the network, tunnels the packets through a wired or wireless link to another point. Such kind of attack can cause severe problems in wireless sensor networks, especially deteriorate the routing process and the localization process. In this paper, we propose a secure localization scheme against wormhole attacks, which includes three phases: wormhole attack detection, neighboring locators differentiation and secure localization. The main idea of the proposed secure localization scheme is to build a so-called conflicting set for each locator according to the abnormalities of message exchanges among neighboring locators, which is used to differentiate the dubious locators from valid locators for the secure localization. The simulation results show that the proposed scheme outperforms the existed schemes under different network parameters.

1. Introduction

In most wireless sensor network (WSN) applications, such as emergency response systems, military field operations, and environment monitoring systems, the inanition of measurement data without location information makes the self-localization capability a highly desirable characteristic of the systems. Most localization algorithms for WSNs estimate the positions of location-unknown nodes based the position information of a set of nodes (*locators*) and the inter-node measurements. The localization techniques can be classified into *range-based* and *range-free* [1] schemes. Range-based localization assumes that the distances between sensors and locators can be estimated by using different measurements, such as the arrival time (ToA [2]), the time difference of arrival times (TDoA [3]), the arrival angel (AoA [4]), or the received signal strength indicator (RSSI [5]), etc. Range-free localization relies on other features of the network, such as hop counts [4], centroid [6], APIT [1], amorphous computation [7], directional antenna [8], signal fingerprinting [9], etc.

Despite the recent advances of localization in WSNs, most of the existing localization systems are vulnerable under the adversarial scenario where malicious attacks can disturb the localization process. For example, a simple replay attack may defunct the distance measurement, leading to the malfunction of the range-based localization technique. Therefore, security is a significant characteristic of the localization process in the hostile environment.

The attackers, which threaten the localization of the sensor nodes in a hostile WSN, can generally be classified into two categories, *external* attackers and *internal* attackers [10]. External attackers can distort network behaviors without the system's authorization, while internal attackers are authenticated ones and thus more devastating to the security of the system. The wormhole attack, which is a severe attack, can be easily launched by two colluding external attackers. In this paper, we will analyze the impacts of the wormhole attacks on the localization procedure in WSNs.

In our early work [11] [12], secure localization schemes are proposed to defend against wormhole attacks under a simplified system model where all types of nodes have the identical transmission range, the nodes can receive all the transmissions without any message collisions, and attackers will relay all received packets without any message drop-offs. Under such system model, the sensor can easily detect the existence of the wormhole attack and provide dependance against the attack during localization process. However, these schemes do not work well when a general system model is considered where the transmission ranges of different types of nodes are different, the nodes may miss certain packets due to message collisions, and attackers

This work is supported in part by grants PolyU 5236/06E, PolyU 5243/08E, PolyU 5253/09E, 1-ZV5N, ZJU-SKL ICT0903, NSFC 60873223, NSFC 90818010 and International Cooperative Project of Science and Technology Department of Zhejiang Province (2009C34002).

may randomly drop off packets they overheard. In this paper, therefore, we consider the localization problem under this general system model and propose a Secure Localization scheme Against Wormhole attacks called SLAW, which works well under this system model. The SLAW consists of three phases: wormhole attack detection, neighboring locators differentiation and secure localization. The main idea of the SLAW is to make use of the properties of the network to detect the existence of the wormhole attack and to build a so-called conflicting set for each locator so as to identify the dubious locators for the secure localization process.

The main contributions of this paper are summarized as follows: 1) We propose a wormhole attack detection approach which can detect the existence of a wormhole attack when the localization process of a sensor node is under the wormhole attack; 2) We propose to use the conflicting set of each locator to differentiate sensor's neighboring locators. Two independent algorithms are proposed to work for different wormhole attacks; 3) We propose a novel secure localization scheme which is divided into three phases: wormhole attack detection, neighboring locators differentiation and secure localization; 4) We conduct simulations to demonstrate the effectiveness of the proposed scheme with a general system model under different network parameters.

2. Related Work

The security of localization has been well studied in the past few yeas. The approaches of providing secure localization for WSNs in hostile environments are summarized in [13]. Most of these solutions achieve security by using cryptography (such as the global preloaded key in ROPE [14] and the network-wide group key in DRBTS [15]), detecting nodes' misbehavior (such as malicious beacon signals in [16], time-bounded nonces in [17] and position validity in [18]) verifying location information (such as the verifiable multilateration in SPINE [10] and the distance verification in ROPE [14]), filtering out erroneous and outlier data (attack-resistant MMSE [19]), making statistical decision (such as voting-based scheme in [19] and reputation-based scheme in DRBTS [15], robust statistical method in [20]), etc. As all these approaches are application dependent, their performance is affected by the types of attacks and the allocated resources.

As wormhole attacks are launched with external attackers which do not need to compromise any system cryptography, they cannot be defeated by using cryptographic solutions. Thus, the researchers have proposed some wormhole attack detection approaches: The "packet leashes" mechanism [21] uses geographical and temporal leashes to detect whether or not the packets are attacked by wormhole attacks. A similar approach is proposed in [22] based on end-to-end location information rather than hop-by-hop geographical leaches. Another set of wormhole prevent techniques [23, 24] use the round-trip time of packets as a measurement to determine the existence of wormhole attacks, which are similar in nature to temporal packet leaches. EDWA [25] use end-to-end hop counts to detect the wormhole attack and pinpoint location of the attackers. Wang et al. [26] propose to detect wormholes by visualizing the entire network topology with some anomalies introduced by attacks. [27] uses the network connectivity information to detect wormhole attacks based on the fact that the independent neighbors of two non-neighboring nodes are upper-bounded. A topological approach is proposed in [28] to detect the wormhole attacks. In [29], 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. However, all the above wormhole detection schemes emphasize the detection without considering the localization scenario.

The directional antennae are used in the SeRLoc [8] to detect the wormhole attack based on the sector uniqueness property and communication range violation property, and the secure localization can be achieved after identifying the attacked locators. HiRLoc [30] further improves the SeRLoc by utilizing antenna rotations and multiple transmit power levels, which provide more information to increase the localization accuracy. The schemes in [19] can also be applied in localization against wormhole attacks. SeRLoc and HiRLoc, however, cannot obtain satisfied localization performance as some attacked locators may still be undetected, and [19] does not suit for the scenario when many locators are attacked. SLAW proposed in this paper applies a novel mechanism to achieve better performance without using extra hardware such as directional antennae required in SeRLoc and HiRLoc.

3 System Model

3.1 Network Model

We assume that three types of nodes are deployed in the network: locators, sensors, and attackers. The locators have their locations known in advance (by manual deployment or GPS devices). Each locator has its own unique identification. The sensors do not know their locations and they can estimate their locations by measuring distances to neighboring locators via message exchanges. The attackers exist in pairs colluding with each other to launch a *wormhole attack*. We assume that the transmission range of the sensors, locators and attackers is R_S, R_L and R_A respectively. For simplicity of description, we assume $R_S \leq R_L \leq R_A$, as shown in Figure 1. Note that the secure localization scheme pro-

posed in this paper works well in other cases where R_S, R_L and R_A vary different. For the communication between two colluding attackers, however, their communication range is unlimited as they can communicate with each other using certain communication technique. We also assume that the communication channel is not ideal. Even within the transmission range, a packet may be lost due to the transmission collision.

When the sensor needs self-localization, it broadcasts a location request message *Loc_req* to its neighboring locators. Upon receiving the requesting message, each neighboring locator replies an acknowledgement message *Loc_ack* to the sensor. The sensor will use the received *Loc_ack* messages to build the set of its neighboring locators. The sensor can estimate the distances to all the locators based on the *Loc_ack* message by using the RSSI method and estimate its location using the maximum likelihood estimation (MLE) approach. Further more, the sensor measures the response time of each locator, which will be used to countervail the locator's random delay at the MAC layer.

3.2 Attack Model

We consider an adversarial environment where the localization procedure of the sensor may be attacked by a wormhole attack. During the wormhole attack, one attacker sniffs packets at one point in the network, forwards them via the wormhole link to another point of the network. We assume that the wormhole link is bi-directional and symmetrical so that the packets could be transmitted via either direction and no region is attacked by more than one wormhole simultaneously. Note that if the length of the wormhole link is less than R_A, then both attackers will be within the transmission area of each other such that the packet transmitted by one attacker can be received by the other attacker, resulting in endless packet transmission loop. To exclude this exceptional scenario, we assume the length of the wormhole link is larger than R_A. In order to make the wormhole attack more general, we assume that the attackers can randomly change their transmission powers for the packet retransmissions; they can also randomly drop off part or all of the packets they have overheard. However, we do not consider the case that the attackers can intensionally drop off certain types, or modify certain fields, of received packets. This is because we treat the wormhole attackers as external attackers which cannot acquire the content, such as the type of the packet, or modify the content, such as the recorded time stamp, of any overheard packet. The case that the attackers act as internal attackers that can break through the system's authentication protection is out of the discussion of this paper.

Figure 1 shows that if the sensor S uses the RSSI method in the localization, the wormhole can forward the packets

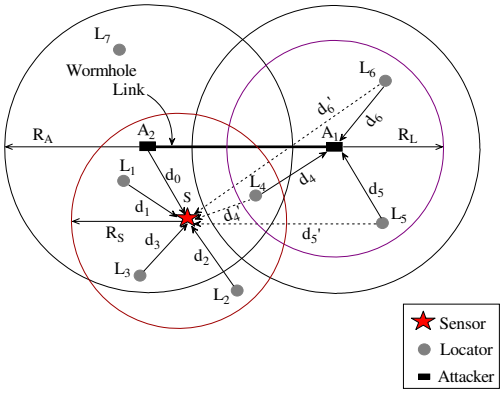

Figure 1. Wormhole attack in the range-based localization.

from the locators L_4, L_5 and L_6 to S, S will obtain the same distance measurement d_0 instead of the actual distances d'_4, d'_5 and d'_6, as the RSSIs from L_4, L_5 and L_6 just reflect the propagational attenuations from A_2 to S. Note that the neighboring locators of S may include locators outside the transmission range of the sensor due to the existence of the wormhole link. Obviously, when S receives messages relayed by the wormhole, it will use false distance measurements for the self-localization. We can also see that, for packets traversing two paths from a locator, say L_5, to S, the one going through the wormhole link, i.e., $L_5 \rightarrow A_1 \rightarrow A_2 \rightarrow S$, will take a longer delay to reach S than the one going directly from L_5 to S.

Upon the view of the sensor, the locators within the sensor's vicinity are classified as the following categories due to the existence of wormhole attack:

Definition 1. *Neighboring locator:* The locators which can communicate with the sensor, either via the wormhole link or not, are defined as the neighboring locators (N-locators) of the sensor.

Definition 2. *Valid locator:* The neighboring locators, which can communicate with the sensor directly, are called valid locators (V-locators) because their messages can be directly received by the sensor to obtain correct distance measurements. The distance between each V-locator and the sensor is less than R_L.

Definition 3. *Dubious locator:* The locators, which are within the transmission range of the attacker and can communicate with the sensor via the wormhole link, are defined as dubious locators (D-locators) since their distance measurements can negatively affect the localization procedure. The distance between each D-locator and the attacker is less than R_L.

We denote the set of N-locators, V-locators, D-locators as $\mathcal{L}_N$, $\mathcal{L}_V$ and $\mathcal{L}_D$, respectively. For the sample

network shown in Fig 1, for the sensor S, $\mathcal{L}_N = \{L_1, L_2, L_3, L_4, L_5, L_6\}$, $\mathcal{L}_V = \{L_1, L_2, L_3, L_4\}$ and $\mathcal{L}_D = \{L_4, L_5, L_6\}$. It is obvious that $\mathcal{L}_N = \mathcal{L}_V \cup \mathcal{L}_D$ Note that L_7 does not belong to any set since it is not a N-locator of S. We also denote $\mathcal{D}_R(u)$ as a disk centered at u with radius R.

4 Secure Localization Scheme Against Wormhole Attacks

The wormhole attack can disrupt the localization procedure of the sensor only if the sensor enters the transmission area of either attacker and communicates with the locators via the wormhole link. Two different types of wormhole attacks, named *Class 1 wormhole attack* (Figure 2(a)) and *Class 2 wormhole attack* (Figure 2(b)), are defined as follows:

Definition 4. *Class 1 wormhole attack:* The sensor is under class 1 wormhole attack when the message it transmits can arrive at itself via the wormhole link. That is, the distance between the sensor and one of the attackers is less than R_S and the distance between the sensor and the other attacker is less than R_A.

Definition 5. *Class 2 wormhole attack:* The sensor is under class 2 wormhole attack when it can exchange messages with some locators via the wormhole link, but cannot receive its own message. That is, the distance between the sensor and one of the attackers is less than R_S, while the distance between the sensor and the other attacker is larger than R_A.

Without special treatments, the localization process would be deteriorated when the sensor is under a wormhole attack. Therefore, the critical task for the sensor is to detect the existence of the wormhole attack and to identify the dubious locators to achieve secure localization. The proposed SLAW includes the following three phases:

- *Wormhole Attack Detection:* The sensor detects whether it is under a wormhole attack using wormhole detection schemes.
- *Neighboring Locators Differentiation:* When a wormhole attack is detected, the sensor identifies its N-locators as D-locators and V-locators.
- *Secure Localization:* After identifying the D-locators, the sensor uses valid locators to conduct the MLE localization with the correct distance measurements.

The procedure of the SLAW is shown as follows:

1: When the sensor receives messages from neighboring locators, it runs *wormhole attack detection* process.
2: **if** the wormhole attack is detected **then**
3: The sensor runs *neighboring locators differentiation* process.
4: The sensor runs *secure localization* process.

4.1 Wormhole Attack Detection

In a hostile WSN where wormhole attacks exist, the sensor has to detect whether it is attacked by a wormhole before conducting the self-localization. The sensor broadcasts a *Loc_req* message and waits for the reply messages, i.e., the *Loc_ack* messages from its neighboring locators. When receiving the *Loc_req* message, each locator responds a *Loc_ack* message. The sensor will use the received *Loc_ack* messages to build the set of its neighboring locators. It also measures the distance to each neighboring locator from the received *Loc_ack* message. Further more, the sensor measures the response time of each locator.

When building the set of neighboring locators, the sensor may observe some abnormalities occur due to the existence of the wormhole attack. The following four properties can be used to detect the existence of the wormhole attack.

Node's self-exclusion property: Each node can not receive any message transmitted by itself in a loop-free path.

Detection scheme D1 based on node's self-exclusion property: When the sensor is under the class 1 wormhole attack like Figure 2(a), it can detect the wormhole attack simply as follows: When the sensor S broadcasts the *Loc_req* message, as A_1 lies in $\mathcal{D}_{R_S}(S)$, it can receive the message from S, and then relayed through the wormhole link to A_2, after relayed by A_2 this message can arrive at S as S lies in $\mathcal{D}_{R_A}(A_2)$. Similarly, the broadcasted *Loc_req* message may also travel from A_2 through the wormhole link to A_1 and then being received by S. Therefore, the sensor can determine that it is under a wormhole attack if it receives the *Loc_req* message sent by itself.

Packet unduplication property: Each node can receive at most one copy of the same message from one of its neighboring nodes.

Detection scheme D2 based on packet unduplication property: As shown in Figure 2(b), a dubious locator L_4 may lie in the common area of the regions $\mathcal{D}_{R_S}(S)$ and $\mathcal{D}_{R_L}(A_1)$. When L_4 responses S's *Loc_req* message, the *Loc_ack* messages can be received by S twice, one directly from L_4 and the other from A_2 which is replayed from A_1 to A_2 through the wormhole link. Therefore, if S receives more than one message from the same neighboring locator for each request, it determines that it is under a wormhole attack.

Neighboring nodes' spatial constraint property: Each node cannot receive messages from its two neighboring nodes simultaneously if the distance between them is larger than $2R_S$.

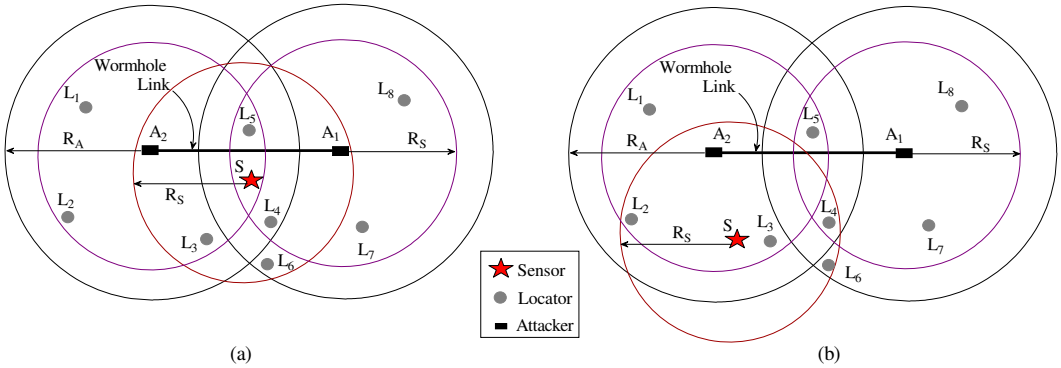

Figure 2. Illustrations of wormhole attack: (a) Class 1 wormhole attack; (b) Class 2 wormhole attack.

Detection scheme D3 based on neighboring nodes' spatial constraint property: As shown in Figure 2(b), L_2 is a locator which lies farther than $2R_S$ away from L_8. After receiving the *Loc_req* message from neighboring locators, S will check whether the distance between any two locators is larger than $2R_S$. If S detects that the distance between L_2 and L_8 is larger than $2R_S$, it derives that it is under a wormhole attack.

The wormhole detection procedure is shown as follows:

1: Broadcast a *Loc_req* message.
2: Wait for the *Loc_ack* messages to measure the distance and calculate the response time of each locator.
3: **if** detect the wormhole attack based on scheme D1 **then**
4: Class 1 wormhole attack is detected.
5: **else if** detect the wormhole attack based on schemes D2 or D3 **then**
6: Class 2 wormhole attack is detected.
7: **else**
8: No wormhole attack is detected.

Since the algorithms that deal with class 1 and class 2 wormhole attacks are independent, the sensor needs to determine the type of the wormhole attack after the wormhole attack detection. However, if considering the general network model that packet loss exists during the message exchanges because of either the packet transmission collisions or the packet drop-off by the wormhole, the sensor may detect the type of the wormhole attack incorrectly. That is, when the sensor is under a class 1 wormhole attack, it may fail to detect the class 1 wormhole attack with the detection scheme D1 but detect a class 2 wormhole attack with the detection schemes D2 or D3. The way to mitigate the impact of this mistake is that, when the sensor receives packets from itself or from any neighboring locator for three times (this scenario happens only when the sensor is under the class 1 wormhole attack, as L_4 in Figure 2(a)) during the neighboring locators differentiation, it will rectify that it is under the class 1 wormhole attack instead of the class 2 wormhole attack and re-conducts the algorithm for the class 2 wormhole attack.

4.2 Neighboring Locators Differentiation

The core idea of these neighboring locators differentiation algorithms is to allow all locators to build their so-called *conflicting sets*, which are based on the abnormalities of the *Beacon* message exchanges among neighboring locators. By analyzing the conflicting sets of neighboring locators, the sensor can differentiate dubious locators from valid locators. The conflicting set is defined as follows:

Definition 6. *Conflicting set:* The conflicting set of a locator L_i, denoted as $C(L_i)$, contains all the abnormal neighboring locators of the locator L_i, including (1) L_i itself if it can receive the *Beacon* message sent by itself, (2) neighboring locators that are within the transmission range of L_i but send several copies of the same *Beacon* message through different paths to L_i, and (3) neighboring locators that are outside the transmission range of L_i but their *Beacon* messages can be received by L_i.

Based on the periodical *Beacon* message exchanges with its neighboring locators, each locator can build its conflicting set. When a locator detects the *Beacon* message abnormality, it will put the locator (the source node of this *Beacon* message) into its conflicting set. When such a locator receives a *Loc_req* message from the sensor, it responses a *Loc_ack* message including its conflicting set to the sensor.

The following theorem shows the relationship among the locater L_i, its conflicting set $C(L_i)$, and $\mathcal{D}_{R_A}(A_1)$, $\mathcal{D}_{R_A}(A_2)$, $\mathcal{D}_{R_L}(A_1)$ and $\mathcal{D}_{R_L}(A_2)$:

Theorem 1. Given a network shown in Figure 3, (1) if L_i lies in $\mathcal{D}_{R_A}(A_2) \setminus \mathcal{D}_{R_A}(A_1)$, all the locators in $C(L_i)$ lie in $\mathcal{D}_{R_L}(A_1)$; (2) if L_i lies in $\mathcal{D}_{R_A}(A_1) \setminus \mathcal{D}_{R_A}(A_2)$, all the locators in $C(L_i)$ lie in $\mathcal{D}_{R_L}(A_2)$; (3) if L_i lies in $\mathcal{D}_{R_A}(A_1) \cap \mathcal{D}_{R_A}(A_2)$, all the locators in $C(L_i)$ lie in $\mathcal{D}_{R_L}(A_1) \cup \mathcal{D}_{R_L}(A_2)$.

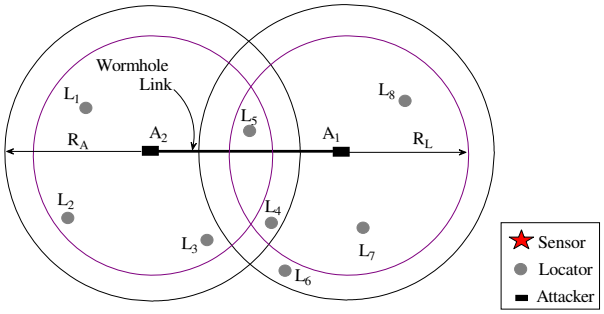

Figure 3. Illustrations for building the conflicting sets.

As shown in Fig 3, the locators L_1, L_2, L_3 lie in $\mathcal{D}_{R_A}(A_2) \setminus \mathcal{D}_{R_A}(A_1)$, the locator L_4, L_5 lie in $\mathcal{D}_{R_A}(A_1) \cap \mathcal{D}_{R_A}(A_2)$, and the locators L_6, L_7, L_8 lie in $\mathcal{D}_{R_A}(A_1) \setminus \mathcal{D}_{R_A}(A_2)$. Take the locator L_3 for example, after each locator broadcasts the *Beacon* messages, L_3 detects its conflicting set as $C(L_3) = \{L_4, L_5, L_7, L_8\}$ (or a subset of $C(L_3)$ when packet loss exists). For the locator L_4, its conflicting set is $C(L_4) = \{L_1, L_2, L_3, L_4, L_5, L_7, L_8\}$ (or a subset of $C(L_4)$ when the packet loss exists). L_6 cannot be a conflicting node of any locator as it lies out of $\mathcal{D}_{R_L}(A_1) \cup \mathcal{D}_{R_L}(A_2)$.

The sensor S can build a *conflicting matrix* of its n neighboring locators as follows:

$$\mathbf{M_c} = \begin{pmatrix} m_{11} & m_{12} & \dots & m_{1n} \\ m_{21} & m_{22} & \dots & m_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n1} & m_{n2} & \dots & m_{nn} \end{pmatrix}$$

Where

$$m_{ij} = \begin{cases} 1, & \text{if } L_j \in C(L_i); \\ 0, & \text{if } L_j \notin C(L_i). \end{cases}$$

Due to the packet loss, the conflicting matrix is not symmetric, e.g., for some i, j, $m_{ij} \neq m_{ji}$. To make the confliction relationship among the locators more reliable, we adopt the conservative strategy to handle the conflicting set. For the conflicting matrix, the sensor conducts $m_{ij} = m_{ji} = (m_{ij} \,\&\, m_{ji})$. That is, if $L_i \in C(L_j)$, the sensor will consider the relationship as valid only if $L_j \in C(L_i)$. For instance, the locator L_6 in Figure 3 may include L_3 into its conflicting set, but L_6 cannot be in the conflicting set of L_3 as A_1 is outside the transmission range of L_6. So the sensor will consider it as invalid.

After this operation, the result of the conflicting sets for the locators can be summarized as follows: Given a sample network as shown in Figure 3, (1) if L_i lies in $\mathcal{D}_{R_L}(A_2) \setminus \mathcal{D}_{R_A}(A_1)$, all the locators in $C(L_i)$ lie in $\mathcal{D}_{R_L}(A_1)$; (2) if L_i lies in $\mathcal{D}_{R_L}(A_1) \setminus \mathcal{D}_{R_A}(A_2)$, all the locators in $C(L_i)$ lie in $\mathcal{D}_{R_L}(A_2)$; (3) if L_i lies in $(\mathcal{D}_{R_A}(A_1) \cap \mathcal{D}_{R_A}(A_2)) \cap (\mathcal{D}_{R_L}(A_1) \cup \mathcal{D}_{R_L}(A_2))$, all the locators in $C(L_i)$ lie in $\mathcal{D}_{R_L}(A_1) \cup \mathcal{D}_{R_L}(A_2)$.

4.2.1 Class 1 Wormhole Attack

When the sensor is under a class 1 wormhole attack as shown in Figure 2(a), all the locators which can exchange messages with the sensor via the wormhole link are D-locators because they will bring the sensor incorrect distance measurements. To identify the V-locators and D-locators, the sensor needs to check the conflicting sets of its neighboring locators.

The procedure of neighboring locators differentiation under the class 1 wormhole attack is described as follows:

1: Each locator periodically exchanges the *Beacon* messages with all its neighboring locators and builds its conflicting set based on the received *Beacon* messages.
2: When receives the *Loc_req* message from the sensor, each locator replies a *Loc_ack* message including its conflicting set to the sensor.
3: The sensor builds the conflicting matrix and conducts the mathematical operation.
4: **for** each neighboring locator L_i **do**
5: **if** $C(L_i) \neq \emptyset$ **then**
6: Add L_i into $\mathcal{L}_D$;
7: **else**
8: Add L_i into $\mathcal{L}_V$.

4.2.2 Class 2 Wormhole Attack

As shown in Figure 2(b), when the sensor is under a class 2 wormhole attack, only the locators in $\mathcal{D}_{R_L}(A_1)$ are D-locators. To identify all D-locators in this scenario, our algorithm adopts the following identification schemes.

Identification scheme I1: When the sensor is under a class 2 wormhole attack, the locators which are detected by the sensor with the packet unduplication property are considered as D-locators. As shown in Figure 2(b), L_4 lies in $\mathcal{D}_{R_S}(S) \cap \mathcal{D}_{R_L}(A_1)$. If it is detected by S with the packet unduplication property, S determines that L_4 is a D-locator.

Identification scheme I2: When under a class 2 wormhole attack, if the sensor has two neighboring locators the distance between which is larger than $2R_L$, one of the two locators is a D-locator while the other is a V-locator. As the message exchanged between the sensor and the D-locator travels through the wormhole link, the response time is larger than that of the V-locator. Therefore, the sensor considers the locator with a shorter response time as a V-locator, and the other locator is labeled as a D-locator. As shown in Figure 2(b), the distance between L_2 and L_8 is larger than $2R_L$, the sensor determines that L_2 (with a shorter response time) is a V-locator and L_8 is a D-locator (with a longer response time).

Theorem 2. When the sensor is under a class 2 wormhole attack and the length of the wormhole link is larger than $R_A + R_L$, if $\exists L_i \notin \mathcal{L}_D$ such that $C(L_i) \neq \emptyset$, then $\forall L_j \in C(L_i)$, $L_j \in \mathcal{L}_D$.

Identification scheme I3: When the sensor detects that a V-locator and a D-locator using identification scheme I2, the V-locator L_i cannot belong to $\mathcal{L}_D$. If L_i's conflicting set $C(L_i)$ is not empty, the sensor considers all locators in $C(L_i)$ as D-locators.

Theorem 3. When the sensor is under a class 2 wormhole attack and the length of the wormhole link is larger than $R_A + R_L$, if $\exists L_i \notin \mathcal{L}_D$ such that $C(L_i) \neq \emptyset$, then $\forall L_j$ such that $L_i \in C(L_j)$, $L_j \in \mathcal{L}_D$.

The proofs of Theorems 1, 2 and 3 are omitted due to space limitations, readers can refer to [31] for the details.

Identification scheme I4: When the sensor detects that a V-locator and a D-locator using identification scheme I2, the V-locator L_i cannot belong to $\mathcal{L}_D$. If L_i's conflicting set $C(L_i)$ is not empty, the locator which includes L_i into its conflicting set will be considered as a D-locator.

When the sensor detects that it is under the class 2 wormhole attack, it can identify all the D-locators based on the above identification schemes. The procedure for identifying the D-locators is shown as follows:

1: Each locator Periodically exchanges the *Beacon* messages with all its neighboring locators and builds its conflicting set based on the received *Beacon* messages.
2: When receiving the *Loc_req* message from the sensor, each locator replies the *Loc_ack* message including its conflicting set to the sensor.
3: The sensor builds the conflicting matrix and conducts the mathematical operation.
4: The sensor conducts schemes I1, I2, I3 and I4 to build $\mathcal{L}_D$.
5: **for** each neighboring locator $L_i \notin \mathcal{L}_D$ **do**
6: Add L_i into $\mathcal{L}_V$.

4.3 Secure Localization

After wormhole attack detection and neighboring locators differentiation, the sensor can identify some valid locators. However, among the dubious locators, there may exist some locators which are also valid locators, such as L_3, L_4 and L_5 in Figure 2(a) and L_4 in Figure 2(b). Therefore, their distance measurements can be used into localization. As the sensor may receive multiple copies of the same message from these locators, it will consider the one with the shortest response time as the correct distance measurement. For the distance measurements which are larger than R due to the wormhole attack or measurement error, the sensor filters them out before localization. At the end, the valid distance measurements of the valid locators are used in the MLE localization.

5 Simulation Results

In this section, we present the simulation results to demonstrate the effectiveness of the SLAW. Particularly, we evaluate the performance of the SLAW when the length of the wormhole link varies. We model the general network model as follows: when the distance d between two nodes is less than αr, there is no packet loss; when d is within $[\alpha r, r]$, the probability of packet loss is $\frac{d-\alpha r}{r-\alpha r}$, where $0 \leq \alpha \leq 1$. Thus, if a node lies outside the transmission range of a sender, this node cannot receive message from the sender. We also assume the wormhole attack will drop the received messages with a probability ω ($0 \leq \omega \leq 1$). The network settings are as following: the locators are deployed independently with a density $\rho_l = 0.006/m^2$ (with the average degree around 4); the label L/R_A 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 of the attacker; the transmission ranges of the sensors, locators and attackers are set as $R_S = 13m$, $R_L = 14m$ and $R_A = 15m$ respectively; $\alpha = 0.75$ and $\omega = 0.2$. For simplicity, we assume that the measurement error of the distance follows a normal distribution $N(\mu, \sigma^2)$ with the mean μ is 0 and the standard deviation σ is within a threshold 0.5.

We repeat each simulation for 20,000 times by randomly deploying locators with the Poisson distribution. The successful probabilities of the wormhole attack detection process and the secure localization process of SLAW are compared with the one without any wormhole attack detection procedure (labeled as "Without detection") and other two secure localization approaches: SeRLoc [8] and Consistency [19]. The localization is considered as successful only if $d_{err1} \leq d_{err2} + f_{tol} * R_S$, 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).

Figure 4(a) shows the performance comparison of SLAW and SeRLoc scheme [8] in terms of the probability of successful wormhole attack detection. It is shown that SLAW outperforms SeRLoc when $L/R_A \leq 2$ while there is no difference when $L/R_A > 2$. This is because SLAW with the RSSI-based localization only improves the wormhole attack detection when the sensor is under the class 1 wormhole attack, which exists only when $L/R_A \leq 2$. It shows that SLAW provides successful detection probability at least 70% while SeRLoc is about 61% in the worst case. When L/R_A is large enough, the probability of successful wormhole attack detection of SLAW approximates 90%.

Upon detecting the wormhole attack, the sensor adopts one of the two differentiation algorithms to identify the du-

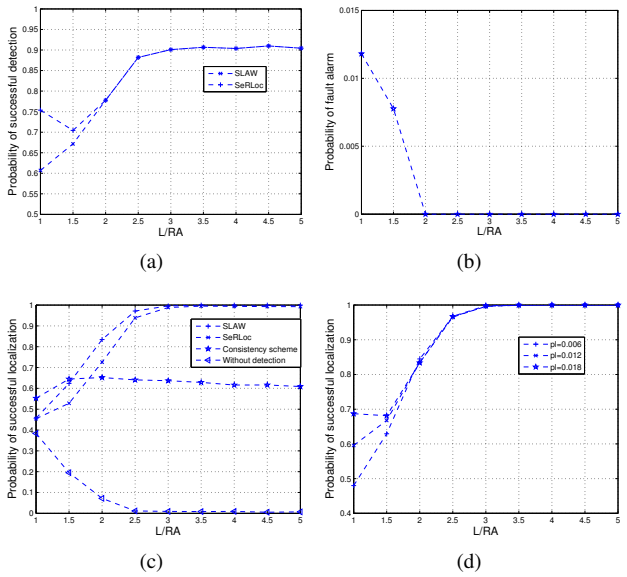

Figure 4. Simulation results: (a) Probability of successful wormhole detection in WSNs; (b) Probability of fault alarm in the wormhole attack detection process of SLAW; (c) Probability of successful localization in WSNs; (d) Probability of secure localization under different locator densities in WSNs.

bious locators according to the type of the wormhole attack. However, the sensor may make false alarm, i.e., it may identify incorrectly that it is under the class 2 wormhole attack while it is actually under the class 1 wormhole attack. The reason that false alarms occur is that the sensor may miss some packets due to the transmission collisions or the random drop-offs. Figure 4(b) demonstrates the probability of false alarm when the sensor is under the wormhole attack. It shows that the misidentification of the wormhole attack happens only when L/R_A is less than $2R_A$ and the probability is at most 1.2%.

Figure 4(c) shows the performance of successful localization of SLAW, SeRLoc, Consistency and "Without detection" schemes. The SeRLoc scheme identifies D-locators using the sector uniqueness and communication range violation properties, then conducts self-localization based on the rest locators. The consistency scheme identifies the most inconsistent locator as a D-locator based on the consistency check of the estimation result. The performance of the "Without detection" scheme shows the severe impact of the wormhole attack on the localization. Among these schemes, SLAW obtains the best performance. The performance of SLAW and SeRLoc increases with the increase of L/R_A while the performance of the consistency scheme is insensitive to the value changes of L/R_A. When L/R_A is larger than 3, the probability of successful localization gets close to 100%.

Figure 4(d) shows the the performance of successful localization of SLAW under different locator densities. It shows that the performance of SLAW improves greatly with the enlargement of locator density when the length of the wormhole link is less than $2R_A$. When the length of the wormhole link is larger than $2R_A$, however, it seems that the enlargement of locator density has no visible improvement.

6 Conclusion and Future Work

In this paper, we analyze the severe impacts of the wormhole attack on the localization in hostile wireless sensor networks. To tackle this secure problem, we propose a novel secure localization scheme SLAW which works well under a general system model. We also conduct simulations that demonstrate our scheme outperforms other existing schemes. In this paper, we only adopt the conservative strategy to handle the conflicting relationship among neighboring locators. In our future work, we will apply the topology inference theories to solve these conflicting relationships and make the conflicting sets of neighboring locators consistent and trustable. When a sensor is attacked by multiple wormhole attacks simultaneously, it will be very complicated and difficult to obtain secure localization. A potential solution is to separate the localization from the wormhole attack detection. That is, when multiple wormhole attacks are detected, the system can try to identify the locations of the attackers and then eliminate them. Thus, the other direction of our future work will focus on the detection of multiple wormhole attacks and the localization of the attackers.

References

[1] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free Localization Schemes for Large Scale Sensor Networks," in *ACM MOBICOM*, 2003.

[2] N. Patwaari, A. Hero, M. Perkins, N. Correal, and R. ODea, "Relative Location Estimation in Wireless Sensor Networks," *IEEE Trans. on Signal Processing*, vol. 51, no. 8, pp. 2137–2148, 2003.

[3] A. Savvides, C. Han, and M. Srivastava, "Dynamic Fine-Grained Localization in Ad-hoc Networks of Sensors," in *ACM MOBICOM*, 2001.

[4] D. Niculescu and B. Nath, "Ad Hoc Positioning System (APS) using AOA," in *IEEE INFOCOM*, 2003.

[5] F. Bouchereau and D. Brady, "Bounds on Range-Resolution Degradation Using RSSI Measurements," in *IEEE ICC*, 2004.

[6] C. Liu and K. Wu, "Sensor Localization with Ring Overlapping Based on Comparison of Received Signal Strength Indicator," in *IEEE MASS*, 2004.

[7] R. Nagpa, "Organizing a Global Coordinate System from Local Information on an Amorphous Computer," MIT, A.I.Memo 1666, 1999.

[8] L. Lazos and R. Poovendran, "SeRLoc: Robust Localization for Wireless Sensor Networks," *ACM Trans. on Sensor Networks*, pp. 73–100, 2005.

[9] K. Kaemarungsi and P. Krishnamurthy, "Modeling of Indoor Positioning Systems Based on Location Fingerprinting," in *IEEE INFOCOM*, 2004.

[10] S. Capkun and J. P. Hubaux, "Secure Positioning of Wireless Devices with Application to Sensor Networks," in *IEEE INFOCOM*, 2005.

[11] H. Chen, W. Lou, and Z. Wang, "Conflicting-Set-Based Wormhole Attack Resistant Localization in Wireless Sensor Networks," in *the 6th International Conference on Ubiquitous Intelligence and Computing (UIC)*, 2009.

[12] H. Chen, W. Lou, X. Sun, and Z. Wang, "A Secure Localization Approach Against Wormhole Attacks Using Distance Consistency," *Eurasip Journal on Wireless Communications and Networking, Spacial Issue on Wireless Network Algorithms, Systems, and Applications*, 2010.

[13] 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*, pp. 96–101, 2008.

[14] L. Lazos, R. Poovendran, and S. Capkun, "ROPE: Robust Position Estimation in Wireless Sensor Networks," in *IEEE IPSN*, 2005.

[15] A. Srinivasan, J. Teitelbaum, and J. Wu, "DRBTS: Distributed Reputation-based Beacon Trust System," in *IEEE International Symposium on Dependable, Autonomic and Secure Computing*, 2006.

[16] D. Liu, P. Ning, and W. Du, "Detecting Malicious Beacon Nodes for Secure Localization Discovery in Wireless Sensor Networks," in *IEEE ICDCS*, 2005.

[17] F. Anjum, S. Pandey, and P. Agrawal, "Secure Localization in Sensor Networks using Transmission Range Variation," in *IEEE MASS*, 2005.

[18] S. Capkun, M. Cagalj, and M. Srivastava, "Secure Localization With Hidden and Mobile Base Stations," in *IEEE INFOCOM*, 2006.

[19] D. Liu, P. Ning, and W. Du, "Attack-Resistant Location Estimation in Sensor Networks," in *IEEE IPSN*, 2005.

[20] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks," in *IEEE IPSN*, 2005.

[21] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks," in *IEEE INFOCOM*, 2003.

[22] W. Wang, B. Bharat, Y. Lu, and X. Wu, "Defending Against Wormhole Attacks in Mobile Ad Hoc Networks," *Wireless Communication and Mobile Computing*, vol. 3, no. 4, pp. 483–503, 2006.

[23] Y. C. Hu, A. Perrig, and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," in *ACM WiSe Workshop*, 2003.

[24] J. Eriksson, S. Krishnamurthy, and M. Faloutsos, "TrueLink: A Practical countermeasure to the Wormhole Attack in Wireless Networks," in *IEEE ICNP*, 2006.

[25] X. Wang and J. Wong, "An End-to-end Detection of Wormhole Attack in Wireless Ad-hoc Networks," in *the 31th Annual International Computer Software and Applications Conference*, 2007.

[26] 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.

[27] R. Maheshwari, J. Gao, and S. R. Das, "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," in *IEEE INFOCOM*, 2007.

[28] D. Dong, M. Li, Y. Liu, X. Y. Li, and X. Liao, "Topological Detection on Wormholes in Wireless Ad Hoc and Sensor Networks," *IEEE ICNP*, 2009.

[29] T. Dimitriou and A. Giannetsos, "Wormholes no more? Localized Wormhole Detection and Prevention in Wireless Networks," *IEEE DCOSS*, 2010.

[30] 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.

[31] H. Chen, W. Lou, and Z. Wang, "SLAW: A Secure Localization Aproach Against Wormhole Attacks Using Conflicting Sets," in *Technical Report, Dept. of Computing, The Hong Kong Polytechnic University*, 2010.