WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. (2014)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/wcm.2462

RESEARCH ARTICLE

On providing wormhole-attack-resistant localization using conflicting sets

Honglong Chen[1]*, Wei Lou[2,3] and Zhi Wang[4]

[1] College of Information and Control Engineering, China University of Petroleum, Qingdao, China
[2] Department of Computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong
[3] Shenzhen Research Institute, The Hong Kong Polytechnic University, Shenzhen, China
[4] State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou, China

ABSTRACT

Wormhole attack is a severe attack that can be easily mounted on a wide range of wireless networks without compromising any cryptographic entity or network node. In the wormhole attack, an attacker sniffs packets at one point in the network and tunnels them through the wormhole link to another point. Such kind of attack can deteriorate the localization procedure in wireless sensor networks. In this paper, we first analyze the impacts of the wormhole attack on the localization procedure. Then, we propose a secure localization scheme against the wormhole attacks called SLAW including three phases: wormhole attack detection, neighboring locators differentiation, and secure localization. The main idea of the SLAW is to build a so-called conflicting set for each locator based on the abnormalities during the message exchanges, which can be used to differentiate the dubious locators to achieve secure localization. We first consider the simplified system model in which there is no packet loss and all the nodes have the same transmission range. We further consider the general system model where the packet loss exists and different types of nodes have different transmission radii. We conduct the simulations to illustrate the effectiveness of the proposed secure localization scheme and compare it with the existing schemes under different network parameters. Copyright © 2014 John Wiley & Sons, Ltd.

KEYWORDS

secure localization; wormhole attacks; wireless sensor networks; conflicting set

***Correspondence**

Honglong Chen, College of Information and Control Engineering, China University of Petroleum, Qingdao, China.
E-mail: chenhl@upc.edu.cn

1. INTRODUCTION

In many wireless sensor network (WSN) applications, such as the 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 for the nodes in the networks. Most of the localization algorithms for WSNs estimate the positions of location-unknown nodes on the basis of the position information of a set of nodes (*locators*) and the inter-node measurements. Generally, the localization techniques can be classified into two categories: *range-based* and *range-free* schemes. The range-based localization schemes assume that the distances between sensors and locators can be estimated using different measurements, such as time of arrival [1], time difference of arrival [2,3], angle of arrival [4], or received signal strength indicator (RSSI [5]). In contrast, the range-free localization schemes rely on other features of the network, such as hop count [6], centroid [7], Approximate-Point-In-Triangulation (APIT) [8], amorphous computation [9], directional antenna [10], signal fingerprinting [11], LANDMARC [12], and so on.

Because of the natural vulnerability of the wireless communications, that is, it is easy for a malicious node to sniff packets from or inject packets into the wireless networks, security becomes a challenging issue in WSNs [13]. 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 compromise attack [14] may induce the node to get incorrect distance measurements, leading to the malfunction of the range-based localization technique. Therefore, security is a necessary characteristic of the localization process in the hostile wireless networks.

Attackers, which can threaten the localization of nodes in a hostile WSN, can generally be classified into two

categories, *external* attackers and *internal* attackers [13]. External attackers can distort network behaviors without obtaining the system's authorization, while internal attackers are authenticated ones and thus more devastating to the system's security. The wormhole attack can be easily launched by two colluding external attackers and can deteriorate or even collapse the self-localization of nodes in WSNs, which motivates us to propose the wormhole-attack-resistant localization scheme.

In this paper, we first analyze the impacts of the wormhole attack on the localization procedure of sensor nodes in WSNs and then propose a secure localization scheme against the wormhole attack called SLAW. SLAW consists of three phases: wormhole attack detection, neighboring locators differentiation, and secure localization. The main idea of SLAW is to make use of network properties to detect the existence of the wormhole attack and build a so-called conflicting set for each locator so as to identify and eliminate the dubious locators to achieve secure localization. In SLAW, we first consider a simplified system model in which there is no packet loss and all the nodes have the same transmission range. We further extend the simplified system model to be more applicable to real application scenarios; that is, we consider a general system model in which the packet loss exists and different types of nodes have different transmission radii. For the general system model, we also consider that the attackers can drop the received packets with random probabilities.

The main contributions of this paper are summarized as follows:

- We analyze the impacts of the wormhole attack on the range-based localization procedure in WSNs.
- We propose a novel secure localization scheme that is composed of three phases: wormhole attack detection, neighboring locators differentiation, and secure localization. Both the simplified system model and general system model are considered respectively.
- We conduct simulations to demonstrate the effectiveness of the proposed secure localization scheme under different network parameters.

The rest of the paper is organized as follows. In Section 2, the related work on secure localization is discussed. Section 3 proposes the system model including the network model and attack model. Section 4 describes the proposed secure localization scheme in detail, and Section 5 presents the performance evaluation. Section 6 concludes the paper and outlines the future work.

2. RELATED WORK

The security of localization in WSNs has been studied in the past few years. The approaches of providing secure localization in the hostile WSNs are summarized in [15]. Most of these solutions achieve the security by using the method of cryptography (such as the global preloaded key in robust position estimation (ROPE) [16], the network-wide group key in distributed reputation-based beacon trust system (DRBTS) [17], and the message authentication in [18]), detecting nodes' misbehavior (such as malicious beacon signals in [19], time-bounded nonces in [20], and position validity in [21]), verifying location information (such as the verifiable multilateration in secure positioning in sensor networks [13], the distance verification in ROPE [16], and the group-based deployment model in localization anomaly detection [22]), filtering out erroneous and outlier data (attack-resistant minimum mean square estimation (MMSE) [14], cluster-based MMSE [23], and Temporal Spatial Consistency based Detection (TSCD) [24,25]), making statistical decision (such as voting-based scheme in [14], reputation-based scheme in DRBTS [17], robust statistical method in [26], and fault-tolerant scheme in [27]), and so on. As all these approaches are application dependent, their performances are affected by the types of attacks and the allocated resources.

As wormhole attacks are launched by external attackers that do not need to compromise any system cryptography, they cannot be defeated by using the cryptographic solutions. Thus, the researchers have proposed many wormhole attack detection approaches: The 'packet leashes' mechanism [28] uses geographical and temporal leashes to detect whether or not the packets are attacked by wormhole attacks. A similar approach is proposed in [29] based on end-to-end location information rather than hop-by-hop geographical leashes. Another set of wormhole-attack-preventing techniques [30–32] use the round-trip time of packets as a measurement to detect the existence of wormhole attacks, which are similar in nature to temporal packet leaches. In [33], a hop-counting procedure is proposed to reconstruct the local map for each node and use a 'diameter' feature to detect abnormalities caused by wormholes. LiteWorp [34] takes advantage of two-hop neighborhood information of the stationary network to reject the packets relayed by wormhole attacks. MobiWorp [35] uses a secure central authority to isolate the malicious nodes globally when it detects the wormhole.

As the wormhole attack dramatically changes the network topology, the network topology information is used to detect the wormhole attack. Wang *et al.* [36] propose to detect wormholes by visualizing the entire network topology with some anomalies introduced by the wormhole attacks. The network connectivity information [37] is used to detect wormhole attacks on the basis of the fact that the number of independent neighbors of two non-neighboring nodes is upper bounded. Another connectivity-based wormhole detection approach is proposed in [38], which is robust to different communication models and energy efficient. A topological approach is proposed in [39] to detect the wormhole attacks. In [40], 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.

All the aforementioned wormhole-attack-detection schemes, however, emphasize the detection without considering the localization procedure. SeRLoc [10] uses the directional antennae to detect the wormhole attack on the basis of the *sector uniqueness property* and the *communication range violation property*, and the secure localization can be achieved after identifying and eliminating the attacked locators. High-resolution robust localization (HiRLoc) [41] further improves the secure range-independent localization (SeRLoc) by utilizing antenna rotations and multiple transmitting power levels, which provide richer information to increase the localization accuracy. SeRLoc and HiRLoc, however, can only detect partial attacked locators and leave a number of undetected attacked ones to affect the localization procedure, which fundamentally limit the accuracy level of the localization. The schemes in [14] can also be applied into the localization against wormhole attacks, but it does not suit for the scenario when a large percentage of locators are attacked. In [42,43], Chen *et al.* propose to use the distance consistency to identify the valid locators that can achieve the secure localization against the wormhole attacks. In [44], a secure localization that defends against the wormhole attack in the rang-free distance-vector-hop localization is proposed. However, those schemes only work well under the scenario where all the nodes have the same transmission range. The SLAW proposed in this paper applies a novel mechanism based on the conflicting set of each locator to achieve better performance without extra hardware such as directional antennae required in SeRLoc and HiRLoc. Moreover, we consider various network scenarios including that different types of nodes in the network may have different transmission ranges and suffer different packet loss rates.

3. SYSTEM MODEL

3.1. Network model

In this paper, we consider a WSN that consists of three types of nodes: locators, sensors, and attackers. The locators are location-fixed nodes with unique identifications. The locators can obtain their location information in advance by manual deployment or through GPS devices and provide the location information to their neighboring sensors. The sensors are stationary or even mobile nodes in the networks that do not know their locations. They can estimate their locations using standard localization methods with the measured distances from themselves to their neighboring locators via message exchanges. The localization of each sensor is independent of other sensors. The attackers exist in pairs colluding with each other to launch a wormhole attack. We first consider a simplified system model, in which all the nodes in the network have the same transmission range R, and there is no packet loss during the communication between any two nodes when they are within the transmission range of each other. We further consider a general system model that is more applicable

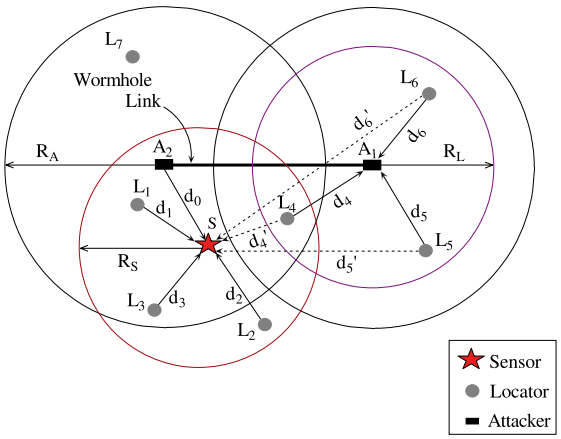

Figure 1. Wormhole attack in the range-based localization for the general system model.

to real application scenarios, in which the transmission radii of the sensors, locators, and attackers, denoted as R_S, R_L, and R_A respectively, are different. For simplicity of description, we assume $R_S \leq R_L \leq R_A$ [†], as shown in Figure 1. We further consider the packet loss during the inter-node communication under the general system model. For the communication between two colluding attackers, however, their communication is not limited by their transmission range R_A as they can communicate with each other using certain communication technique. For example, the wormhole attackers can communicate with each other via the *wormhole link*, which may be implemented with the wired communication.

The sensor can conduct the self-localization, during which it will broadcast a localization request message *LocReq* to its neighboring locators. Upon receiving the requesting message, each neighboring locator replies an acknowledgement message *LocAck* to the sensor. The sensor can then build the set of its neighboring locators using the received *LocAck* messages. Furthermore, the sensor can measure the RSSI of the *LocAck* message to determine the distances to all the neighboring locators and then estimate its location using the maximum likelihood estimation (MLE) approach [45].

During the aforementioned localization procedure, the sensor can estimate the response time of each locator, which can be used to countervail the locator's random delay at its media access control (MAC) layer. As the response time of the locator is affected by the random queueing delay at its MAC layer, we adopt the approach in [46] to countervail this random delay: When broadcasting the *LocReq* message, the sensor records its local time t_0. Every locator gets the local time t_1 by time stamping the message at the MAC layer (i.e., the time when the message is received at the MAC layer) instead of time stamping the

[†]Note that the secure localization scheme proposed in this paper works well in other cases where R_S, R_L, and R_A vary differently.

message at the application layer. Similarly, when responding with the *LocAck* message, the locator puts its local time t_2 at the MAC layer; both t_1 and t_2 are attached in the *LocAck* message. When receiving the *LocAck* message, the sensor records its local time t_3, after which it can calculate the response time of the locator as $(t_3 - t_0) - (t_2 - t_1)$. In this procedure, only the random delays at the MAC layer of the locators are eliminated from the response time, while the delays introduced by attackers still exist.

3.2. Attack model

A wormhole attack is typically launched by two colluding attackers who communicate with each other via a wired or wireless link, that is, the *wormhole link*. During the wormhole attack, one attacker sniffs packets at one point in the network, forwards them via the wormhole link to the other attacker that locates at another point of the network, and then the other one relays the received packets to its neighbors. The wormhole attack can disturb the functionalities of WSNs in many aspects, such as the routing or the localization. In the routing process, the attackers may provide a shorter path between a source-destination pair via the wormhole link during the routing setup phase, while during the packet delivery phase, the attackers can 'absorb' and then drop the packets that go through themselves, making the routing totally collapse [47].

In this paper, we focus on the impacts of the wormhole attack on the localization procedure. We consider a hostile WSN where the sensor node's self-localization procedure is threatened by the wormhole attack. We assume that the wormhole link is bi-directional and symmetrical so that the packets can be transmitted via either direction. We also assume that the wormhole attacks are distributed sparsely enough in the network so that each node will be attacked by at most one wormhole attack. Note that if the length of the wormhole link is less than the transmission range of the attacker, both attackers will be within the transmission range of each other such that the packet transmitted by one attacker can be received by the other attacker, resulting in an endless packet transmission loop. To exclude this exceptional scenario, we assume that the length of the wormhole link is larger than the transmission range of the attacker. In the simplified system model, we assume that the attackers will not drop any packet but simply relay it when they sniff the packet. While in the general system model, we assume a more general scenario where the attackers can randomly drop the packets they overheard partially or completely. However, we do not consider the case that the attackers can intensionally drop certain types or modify certain fields of the received packets. This is because we treat the wormhole attackers as external attackers that 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 in this paper.

Figure 1 shows the impacts of the wormhole attack on the localization procedure in a WSN for the general system model. Before conducting the self-localization, the sensor S uses the RSSI-based method[‡] to measure the distances between itself and its neighboring locators. During the distance measurement, the wormhole can forward the packets from the locators L_4, L_5, and L_6 to S, then S will obtain the measured distance 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 some locators outside its transmission range because of the existence of the wormhole link. Obviously, when S receives messages relayed by the wormhole, it will use false distance measurements in 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, that is, $L_5 \rightarrow A_1 \rightarrow A_2 \rightarrow S$, will take a longer delay to reach S than the other one going directly from L_5 to S.

Upon the view of the sensor, the locators within its vicinity are classified into the following three categories due to the existence of the wormhole attack:

Definition 1. *Neighboring locator: The locators that 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 the transmission range of the locator (R for the simplified system model and R_L for the general system model).*

Definition 3. *Dubious locator: The locators that 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) because their distance measurements can negatively affect the localization procedure. The distance between each D-locator and the attacker is less than the transmission range of the locator (R for the simplified system model and R_L for the general system model).*

We denote the sets of N-locators, V-locators, and D-locators as $\mathcal{L}_N$, $\mathcal{L}_V$, and $\mathcal{L}_D$, respectively. In the sample network shown in Figure 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 $\mathcal{L}_V$ and $\mathcal{L}_D$ can have an intersection such as $\{L_4\}$ in Figure 1 and L_7 does not belong to any set since it is not an

[‡]We adopt the RSSI-based localization scheme in this work. Note that other range-based localization schemes such as time-of-arrival-based or time-difference-of-arrival-based schemes can also work here.

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 it enters the transmission area of either attackers and communicates with the locators via the wormhole link. Without special treatments, the self-localization of the sensor would be deteriorated when it is under a wormhole attack. Therefore, the critical task for the sensor is to detect the existence of the wormhole attack and then identify and eliminate the D-locators before localization to fulfill the valid localization procedure. The proposed SLAW is shown in Algorithm 1, which 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 differentiates its N-locators into D-locators and V-locators.
- Secure localization: After eliminating the D-locators, the sensor uses the V-locators to conduct the MLE localization with the correct distance measurements.

Algorithm 1 SLAW scheme

1: When the sensor needs to conduct the self-localization, it runs *wormhole attack detection* process.
2: **if** the wormhole attack is detected **then**
3: The sensor runs *neighboring locators differentiation* process.
4: **end if**
5: The sensor runs *secure localization* process.

We classify the wormhole attack as two types, named *closed-loop wormhole attack* and *open-loop wormhole attack*, which are defined according to the geographical relationships between the sensor and the wormhole attackers as follows:

Definition 4. *Closed-loop wormhole attack: The node is under a closed-loop wormhole attack when the message the node transmits can arrive at itself via the wormhole link. That is, the message flows from the node to one attacker and then to another attacker and finally back to the node, which forms a closed loop.*

For the simplified system model, when a sensor is under a closed-loop wormhole attack (as shown in Figure 2(a)), the distance between the sensor and either one of the attackers is less than R, that is, the sensor lies in $\mathcal{D}_R(A_1) \cap \mathcal{D}_R(A_2)$. For the general system model, when a sensor is under a closed-loop wormhole attack (as shown in Figure 3(a)), 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, that is, the sensor lies in $(\mathcal{D}_{R_S}(A_1) \cap \mathcal{D}_{R_A}(A_2)) \cup (\mathcal{D}_{R_S}(A_2) \cap \mathcal{D}_{R_A}(A_1))$.

Definition 5. *Open-loop wormhole attack: The node is under an open-loop wormhole attack when it can communicate with the locators via the wormhole link but cannot receive the message it transmits.*

For the simplified system model, when a sensor is under an open-loop wormhole attack (as shown in Figure 2(b)), the distance between the sensor and one of the attackers is less than R, and the distance between the sensor and the other attacker is larger than R, that is, the sensor lies in $(\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)) \cup (\mathcal{D}_R(A_2) \setminus \mathcal{D}_R(A_1))$. For the general system model, when a sensor is under an open-loop wormhole attack (as shown in Figure 3(b)), 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 larger than R_A, that is, the sensor lies in $(\mathcal{D}_{R_S}(A_1) \setminus \mathcal{D}_{R_A}(A_2)) \cup (\mathcal{D}_{R_S}(A_2) \setminus \mathcal{D}_{R_A}(A_1))$.

4.1. Wormhole attack detection

In a hostile WSN where wormhole attacks exist, the sensor has to determine whether it is attacked by a wormhole attack before conducting the self-localization. Before the self-localization, the sensor broadcasts a *LocReq* message

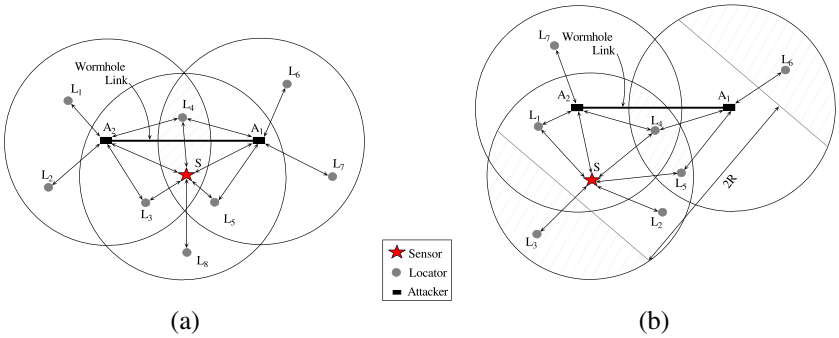

Figure 2. Illustrations of wormhole attacks for the simplified system model: (a) closed-loop wormhole attack and (b) open-loop wormhole attack.

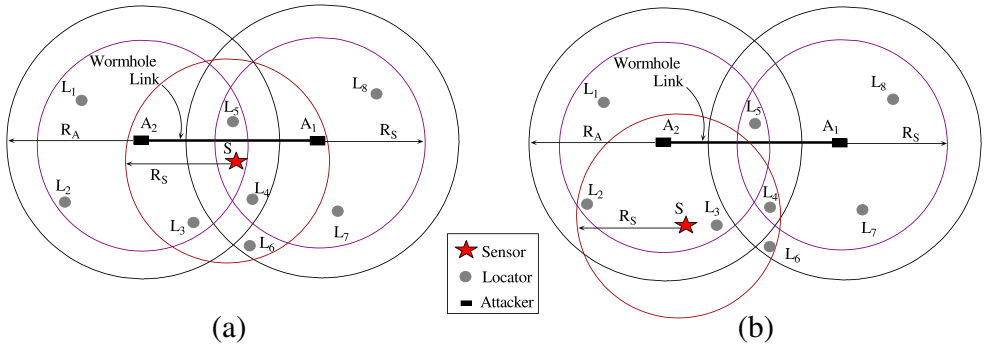

Figure 3. Illustrations of wormhole attacks for the general system model: (a) closed-loop wormhole attack and (b) open-loop wormhole attack.

and waits for the reply messages, that is, the *LocAck* messages from its neighboring locators. When receiving the *LocReq* message, each locator replies a *LocAck* message. The sensor will use the received *LocAck* messages to build the set of its neighboring locators. It can also measure the distance to each neighboring locator on the basis of the RSSI of the received *LocAck* message. Furthermore, the sensor measures the response time of each locator using the method we mentioned in the network model.

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

- Node's self-exclusion property: each node cannot receive any message transmitted by itself in a loop-free path.
- Packet unduplication property: each node can receive at most one copy of the same message from each of its neighboring nodes.
- Neighboring nodes' spatial constraint property: each node cannot receive the reply messages from its two neighboring nodes simultaneously if the distance between them is larger than $2R$ (or $2R_S$) for the simplified (or general) system model.

Detection scheme D1 is based on the node's self-exclusion property, which is stated as follows:

- For the simplified system model, when the sensor is under a closed-loop wormhole attack as shown in Figure 2(a), it can detect the wormhole attack as follows: When the sensor S broadcasts the *LocReq* message, as A_1 lies in $\mathcal{D}_R(S)$, it can receive the message from S and then relay the message through the wormhole link to A_2. After being relayed by A_2, this message can arrive at S as S lies in $\mathcal{D}_R(A_2)$. Similarly, the broadcasted *LocReq* 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 closed-loop wormhole attack if it receives the *LocReq* message transmitted by itself.
- For the general system model, when the sensor is under a closed-loop wormhole attack as shown in Figure 3(a), it can also detect the wormhole attack similarly using the aforementioned scheme.

Detection scheme D2 is based on packet unduplication property, which is stated as follows:

- For the simplified system model, as shown in Figure 2(b), a D-locator L_4 may lie in the region $\mathcal{D}_R(S) \cap \mathcal{D}_R(A_1)$. When L_4 replies S's *LocReq* message, the *LocAck* message can be received by S twice, one directly from L_4 and the other from A_2 that is relayed from A_1 to A_2 via the wormhole link. Therefore, if S receives more than one copy of message from the same neighboring locator for each request, it determines that it is under a wormhole attack.
- For the general system model, as shown in Figure 3(b), a D-locator L_4 may lie in the region $\mathcal{D}_{R_S}(S) \cap \mathcal{D}_{R_L}(A_1)$. Similarly, S can detect that it receives more than one copy of message from L_4 for each request, after which it determines that it is under a wormhole attack.

Detection scheme D3 is based on neighboring nodes' spatial constraint property, which is stated as follows:

- For the simplified system model, as shown in Figure 2(b), L_3 lies farther than $2R$ away from L_6. After receiving the *LocReq* message from N-locators, S will check whether the distance between any two of its N-locators is larger than $2R$. If S detects that the distance between L_3 and L_6 is larger than $2R$, it derives that it is under a wormhole attack.
- For the general system model, as shown in Figure 3(b), L_2 lies farther than $2R_S$ away from L_8. Then S can detect that it is under a wormhole attack using the aforementioned method.

The wormhole detection procedure is shown in Algorithm 2. After receiving the *LocAck* messages from its N-locators, the sensor can use the wormhole detection scheme D1 to detect a closed-loop wormhole attack and use the wormhole detection schemes D2 or D3 to detect an open-loop wormhole attack.

Algorithm 2 Wormhole attack detection process

```
Broadcast a LocReq message.
Wait for the LocAck messages to measure the distance and calculate the response time of each locator.
if detect the wormhole attack based on Scheme D1 then
    A closed-loop wormhole attack is detected.
else if detect the wormhole attack based on Schemes D2 or D3 then
    An open-loop wormhole attack is detected.
else
    No wormhole attack is detected.
end if
```

For the simplified system model, as there is no packet loss, the sensor can always correctly detect the type of the wormhole attack. However, for the general system model where the packet loss exists, the sensor may detect the type of the wormhole attack incorrectly. That is, when the sensor is under a closed-loop wormhole attack, it may fail to detect the closed-loop wormhole attack by the scheme D1 but detect it as an open-loop wormhole attack by the schemes D2 or D3. To reduce this false alarm, we use the following approach: When the sensor receives packets from itself or from any neighboring locator for three times, which happens only when the sensor is under the closed-loop wormhole attack (such as L_4 in Figure 3(a)), it will realize that it is under the closed-loop wormhole attack instead of the open-loop wormhole attack, and it will re-conduct the algorithm for the closed-loop wormhole attack.

4.2. Neighboring locators differentiation

Because each locator periodically broadcasts the *Beacon* message, it can recognize its neighboring locators. Meanwhile, on the basis of the periodical *Beacon* message exchanges with its neighboring locators, each locator can build its so-called conflicting set. The conflicting set is defined as follows:

Definition 6. *Conflicting set: The conflicting set of a locator L_i, denoted as $\mathcal{C}(L_i)$, contains all the abnormal neighboring locators of the locator L_i, including (i) L_i itself if it can receive the Beacon message transmitted by itself; (ii) neighboring locators that are within the transmission range of L_i, but L_i can receive several copies of the same Beacon message through different paths; and (iii) neighboring locators that are outside the transmission range of L_i, but their Beacon messages can still be received by L_i.*

When a locator detects the abnormality of the *Beacon* message, it will put the locator that sends this *Beacon* message into its conflicting set. After building the conflicting set, each locator, when receiving a *LocReq* message from a sensor, will reply a *LocAck* message including its conflicting set to this sensor.

The core idea of the neighboring locators differentiation algorithms is to let the sensor differentiate the D-locators from the V-locators by analyzing the conflicting sets of the N-locators. In the following subsections, we will describe the neighboring locators differentiation procedures for the simplified system model and the general system model respectively.

4.2.1. Neighboring locators differentiation for the simplified system model.

For the simplified system model, when a WSN is under a wormhole attack as shown in Figure 2, the relationship between each locator and its conflicting set can be elaborated as Theorem 1.

Theorem 1. *Given a WSN under a wormhole attack, (i) if L_i lies in $\mathcal{D}_R(A_2) \setminus \mathcal{D}_R(A_1)$, $\mathcal{C}(L_i)$ contains all the locators in $\mathcal{D}_R(A_1)$; (ii) if L_i lies in $\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)$, $\mathcal{C}(L_i)$ contains all the locators in $\mathcal{D}_R(A_2)$; and (iii) if L_i lies in $\mathcal{D}_R(A_1) \cap \mathcal{D}_R(A_2)$, $\mathcal{C}(L_i)$ contains all the locators in $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$.*

Please see Appendix A for a proof.

Corollary 1. *A locator is in its own conflicting set if and only if it lies in $\mathcal{D}_R(A_1) \cap \mathcal{D}_R(A_2)$.*

Please see Appendix B for a proof.

Take Figure 2(a) for example: L_1, L_2, L_3 lie in $\mathcal{D}_R(A_2) \setminus \mathcal{D}_R(A_1)$, L_4 lies in $\mathcal{D}_R(A_1) \cap \mathcal{D}_R(A_2)$, and L_5, L_6, L_7 lie in $\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)$. For L_3, it will build its conflicting set as $\mathcal{C}(L_3) = \{L_4, L_5, L_6, L_7\}$. For L_4, its conflicting set is $\mathcal{C}(L_4) = \{L_1, L_2, L_3, L_4, L_5, L_6, L_7\}$. For L_8, its conflicting set is empty.

When the sensor is under a closed-loop wormhole attack as shown in Figure 2(a), all the locators in $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$ are D-locators. The sensor needs to check the conflicting sets of its N-locators to differentiate the V-locators and the D-locators to achieve secure localization.

Theorem 2. *When the sensor is under a closed-loop wormhole attack, $\forall L_i$ such that $\mathcal{C}(L_i) \neq \emptyset$, $L_i \in \mathcal{L}_D$.*

Please see Appendix C for a proof.

Identification scheme I1: When the sensor detects that it is under a closed-loop wormhole attack, it can obtain the conflicting sets of the N-locators on the basis of the received *LocAck* messages. Then, the sensor considers the ones with non-empty conflicting set as D-locators.

When the sensor is under an open-loop wormhole attack as shown in Figure 2(b), only the locators in $\mathcal{D}_R(A_1)$ are

D-locators. We propose the following three identification schemes to identify the D-locators in this scenario.

Theorem 3. *When the sensor is under an open-loop wormhole attack, $\forall L_i$ such that $\exists L_j \in \mathcal{C}(L_i)$ but $L_j \notin \mathcal{L}_N$, $L_i \in \mathcal{L}_D$.*

Please see Appendix D for a proof.

Identification scheme I2: When the sensor is under an open-loop wormhole attack, it obtains the conflicting sets of the N-locators on the basis of the received *LocAck* messages. By detecting whether there exists a locator, which is not the neighbor of the sensor, in the conflicting set of one of the sensor's N-locators, the sensor can determine whether this N-locator is a D-locator or not. In the scenario of Figure 2(b), L_4, L_5, and L_6 will add L_7 into their conflicting sets, and L_7 is not the neighbor of the sensor; thus, the sensor can identify L_4, L_5, and L_6 as D-locators.

Theorem 4. *When the sensor is under an open-loop wormhole attack, $\forall L_i$ such that $\mathcal{C}(L_i) = \mathcal{C}(L_j)$ where $L_j \in \mathcal{L}_D$ and $L_j \notin \mathcal{C}(L_j)$, $L_i \in \mathcal{L}_D$.*

Please see Appendix E for a proof.

Identification scheme I3: When the sensor is under an open-loop wormhole attack, if it detects a D-locator whose conflicting set does not include itself, then any locator whose conflicting set equals to that of this D-locator will be considered as a D-locator. For example, in Figure 2(b), if the sensor detects that L_5 is a D-locator who lies in $\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)$, then L_6 having the same conflicting set with L_5 will be considered as a D-locator.

Theorem 5. *When the sensor is under an open-loop wormhole attack, if the distance between two neighboring locators of the sensor, L_j and L_k, is larger than $2R$ and $\mathcal{C}(L_j) = \emptyset$, $\mathcal{C}(L_k) \neq \emptyset$, and $L_k \notin \mathcal{C}(L_k)$, then $\forall L_i$ such that $\mathcal{C}(L_i) = \mathcal{C}(L_k)$, $L_i \in \mathcal{L}_D$.*

Please see Appendix F for a proof.

Identification scheme I4: When the sensor is under an open-loop wormhole attack, if it detects that the distance between its two N-locators L_j and L_k is larger than $2R$, L_j's conflicting set is empty, and L_k's conflicting set is not empty and does not contain itself, then all the locators having the same conflicting set with L_k are considered as D-locators. Take L_3 and L_6 in Figure 2(b) as examples; the distance between them is larger than $2R$, so the sensor can determine that L_6 lies in $\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)$. As $\mathcal{C}(L_5) = \mathcal{C}(L_6)$, L_5 will be considered as a D-locator.

The neighboring locators differentiation procedure for the simplified system model is shown in Algorithm 3. After the locators build their conflicting sets, if the sensor detects that it is under a closed-loop wormhole attack, it identifies the D-locators using the identification scheme I1. Otherwise, if the sensor detects that it is under an open-loop wormhole attack, it identifies the D-locators using the identification schemes I2, I3, and I4. At the end, all other N-locators that have not been identified as the D-locators will be considered as the V-locators.

Algorithm 3 Neighboring locators differentiation process for the simplified system model

1: Each locator Periodically exchanges the *Beacon* messages with all its N-locators and builds its conflicting set based on the received *Beacon* messages.
2: When receiving the *LocReq* message from the sensor S, each locator replies the *LocAck* message including its conflicting set to S.
3: **if** S detects a closed-loop wormhole attack **then**
4: Conduct scheme I1 to build $\mathcal{L}_D$.
5: **end if**
6: **if** S detects an open-loop wormhole attack **then**
7: Conduct schemes I2, I3, and I4 to build $\mathcal{L}_D$.
8: **end if**
9: **for** each N-locator $L_i \notin \mathcal{L}_D$ **do**
10: $L_i \rightarrow \mathcal{L}_V$.
11: **end for**

4.2.2. Neighboring locators differentiation for the general system model.

For the general system model, we will consider that different types of nodes have different transmission radii. Moreover, the packet loss is taken into account because of the communication errors or the random drop-offs by the wormhole attackers. For a given network shown as Figure 4, Theorem 6 states the relationship among a locator L_i, its conflicting set $\mathcal{C}(L_i)$, 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 6. *Given a network under a wormhole attack, (i) if L_i lies in $\mathcal{D}_{R_A}(A_2) \setminus \mathcal{D}_{R_A}(A_1)$, all the locators in $\mathcal{C}(L_i)$ lie in $\mathcal{D}_{R_L}(A_1)$; (ii) if L_i lies in $\mathcal{D}_{R_A}(A_1) \setminus \mathcal{D}_{R_A}(A_2)$, all the locators in $\mathcal{C}(L_i)$ lie in $\mathcal{D}_{R_L}(A_2)$; and (iii) if L_i lies in $\mathcal{D}_{R_A}(A_1) \cap \mathcal{D}_{R_A}(A_2)$, all the locators in $\mathcal{C}(L_i)$ lie in $\mathcal{D}_{R_L}(A_1) \cup \mathcal{D}_{R_L}(A_2)$.*

Please see Appendix G for a proof.

In Figure 4, the locators L_1, L_2, L_3 lie in $\mathcal{D}_{R_A}(A_2) \setminus \mathcal{D}_{R_A}(A_1)$, the locators 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 builds its conflicting set as $\mathcal{C}(L_3) = \{L_4, L_5, L_7, L_8\}$ (or a subset of $\mathcal{C}(L_3)$ when packet loss exists). For the locator L_4, its conflicting set is $\mathcal{C}(L_4) = \{L_1, L_2, L_3, L_4, L_5, L_7, L_8\}$ (or a subset of $\mathcal{C}(L_4)$ when the packet loss exists). L_6 cannot be a conflicting node of any locator as it lies out of $\mathcal{D}_{R_L}(A_1) \cup \mathcal{D}_{R_L}(A_2)$.

After receiving the conflicting set information from its n neighboring locators, the sensor S can build a *conflicting matrix* based on the conflicting sets of all its neighboring locators as follows:

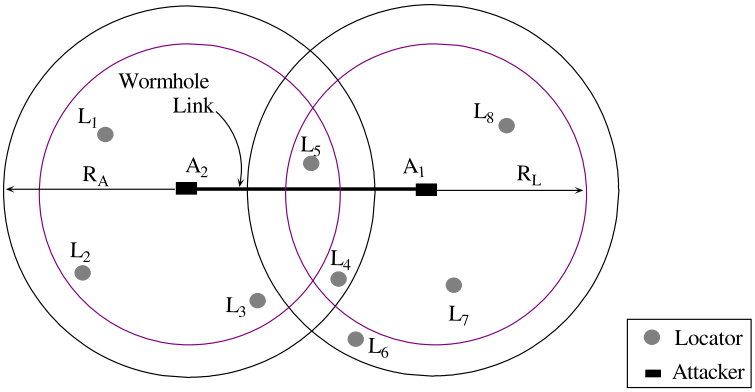

Figure 4. Illustrations for building the conflicting sets.

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

where

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

Because of the packet loss, the conflicting matrix may be asymmetric, for example, for some i and j, $m_{ij} \neq m_{ji}$. We adopt the conservative strategy to decide the confliction relationship among the locators in the conflicting matrix: the sensor sets $m_{ij} = m_{ji} = (m_{ij} \& m_{ji})$. That is, the sensor will consider the confliction relationship between i and j valid only if $L_i \in \mathcal{C}(L_j)$ and $L_j \in \mathcal{C}(L_i)$. For instance, the locator L_6 in Figure 4 may include L_3 into its conflicting set, that is, $L_3 \in \mathcal{C}(L_6)$, 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 take L_3 out of $\mathcal{C}(L_6)$.

After this operation, we can easily get the following Corollary:

Corollary 2. *Given a sample network as shown in Figure 4, (i) if L_i lies in $\mathcal{D}_{R_L}(A_2) \setminus \mathcal{D}_{R_A}(A_1)$, all the locators in $\mathcal{C}(L_i)$ lie in $\mathcal{D}_{R_L}(A_1)$; (ii) if L_i lies in $\mathcal{D}_{R_L}(A_1) \setminus \mathcal{D}_{R_A}(A_2)$, all the locators in $\mathcal{C}(L_i)$ lie in $\mathcal{D}_{R_L}(A_2)$; and (iii) 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 $\mathcal{C}(L_i)$ lie in $\mathcal{D}_{R_L}(A_1) \cup \mathcal{D}_{R_L}(A_2)$.*

When the sensor is under a closed-loop wormhole attack as shown in Figure 3(a), all the locators that 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 N-locators.

For the general system model, the neighboring locators differentiation procedure under the closed-loop wormhole attack is described in Algorithm 4.

Each locator periodically broadcasts the *Beacon* message to all its N-locators and builds its conflicting set. The sensor S broadcasts a *LocReq* message to all its N-locators. When receiving the *LocReq* message from S, each locator replies the *LocAck* message including its conflicting set to S. S then builds the conflicting matrix using the conservative strategy to handle the confliction relationship among the locators. S checks the conflicting set of each N-locator: If the conflicting set is not empty, the locator is considered as a D-locator; otherwise, if the conflicting set is an empty set, the locator is considered as a V-locator.

Algorithm 4 Neighboring locators differentiation under the closed-loop wormhole attack for the general system model

1: Each locator periodically broadcasts the *Beacon* message to all its neighboring locators and builds its conflicting set based on the received *Beacon* messages.
2: When receives the *LocReq* message from the sensor S, each locator replies a *LocAck* message including its conflicting set to S.
3: S builds the conflicting matrix using the conservative strategy.
4: **for** each neighboring locator L_i **do**
5: **if** $\mathcal{C}(L_i) \neq \emptyset$ **then**
6: Add L_i into $\mathcal{L}_D$;
7: **else**
8: Add L_i into $\mathcal{L}_V$.
9: **end if**
10: **end for**

When the sensor is under an open-loop wormhole attack shown in Figure 3(b), only the locators in $\mathcal{D}_{R_L}(A_1)$ are D-locators. To identify all the D-locators in this scenario, our algorithm adopts the following identification schemes.

Identification scheme I5: When the sensor is under an open-loop wormhole attack, the locators, which are detected by the sensor with the packet unduplication property, are considered as D-locators. As shown in Figure 3(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 I6: When under an open-loop 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 3(b), the distance between L_2 and L_8 is larger than $2R_L$ and 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 7. *When the sensor is under an open-loop 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 $\mathcal{C}(L_i) \neq \emptyset$, then $\forall L_j \in \mathcal{C}(L_i)$, $L_j \in \mathcal{L}_D$.*

Please see Appendix H for a proof.

Identification scheme I7: When the sensor detects that a V-locator and a D-locator using identification scheme I6, the V-locator L_i cannot belong to $\mathcal{L}_D$. If L_i's conflicting set $\mathcal{C}(L_i)$ is not empty, the sensor considers all locators in $\mathcal{C}(L_i)$ as D-locators.

Theorem 8. *When the sensor is under an open-loop 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 $\mathcal{C}(L_i) \neq \emptyset$, then $\forall L_j$ such that $L_i \in \mathcal{C}(L_j)$, $L_j \in \mathcal{L}_D$.*

Please see Appendix I for a proof.

Identification scheme I8: When the sensor detects a V-locator and a D-locator using identification scheme I6, it determines that the V-locator L_i does not belong to $\mathcal{L}_D$. If L_i's conflicting set $\mathcal{C}(L_i)$ is not empty, the locator that includes L_i into its conflicting set will be considered as a D-locator.

When the sensor detects that it is under an open-loop wormhole attack, it can identify all the D-locators on the basis of the aforementioned identification schemes. The procedure for identifying the D-locators is shown in Algorithm 5.

Each locator periodically broadcasts the *Beacon* message to all its N-locators and builds its conflicting set. The sensor S broadcasts a *LocReq* message to all its N-locators. When receiving the *LocReq* message from S, each locator replies the *LocAck* message including its conflicting set to S. S then builds the conflicting matrix using the conservative strategy to handle the confliction relationship among the locators. S then uses the identification schemes I5, I6, I7, and I8 to identify all the D-locators. After that, for each N-locator that is not identified as a D-locator, it will be considered as a V-locator.

Algorithm 5 Neighboring locators differentiation process under the open-loop wormhole attack for the general system model

1: Each locator periodically broadcasts the *Beacon* message to all its neighboring locators and builds its conflicting set based on the received *Beacon* messages.
2: When receiving the *LocReq* message from the sensor S, each locator replies the *LocAck* message including its conflicting set to S.
3: S builds the conflicting matrix using the conservative strategy.
4: S conducts schemes I5, I6, I7, and I8 to build $\mathcal{L}_D$.
5: **for** each neighboring locator $L_i \notin \mathcal{L}_D$ **do**
6: Add L_i into $\mathcal{L}_V$.
7: **end for**

4.3. Secure localization

After wormhole-attack detection and neighboring locators differentiation, the sensor can identify some of the V-locators. However, among the D-locators, there may exist some locators that are also V-locators, such as L_3, L_4, and L_5 in Figure 2(a) and L_4 and L_5 in Figure 2(b) for the simplified system model and L_3, L_4, and L_5 in Figure 3(a) and L_4 in Figure 3(b) for the general system model. Therefore, their distance measurements can be correctly used in the 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 distance measurements that are larger than the transmission range of the locator because of the wormhole attack or measurement error, the sensor filters them out before localization. At the end, the MLE localization is conducted on the basis of the valid distance measurements between the sensor and the V-locators.

The MLE localization works as follows [45]: Assume that the sensor has obtained valid distance measurements to m different V-locators. The coordinates of the m locators are (x_1, y_1), (x_2, y_2), (x_3, y_3), ..., (x_m, y_m) respectively, and the distance measurements from the m locators to the sensor are $d_1, d_2, d_3, ..., d_m$. Then, the coordinate of the sensor (x, y) satisfies

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

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

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

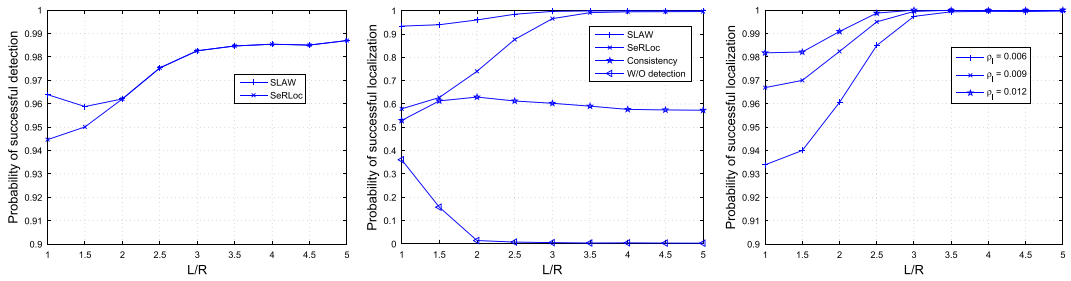

Figure 5. Performance comparison under the simplified system model: (a) the probability of successful wormhole detection, (b) the probability of successful localization, and (c) the effects of locator density ρ_l.

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

The coordinate of the sensor can be finally calculated as

$$X = (A^T A)^{-1} A^T b.$$

5. PERFORMANCE EVALUATION

In this section, we present the simulation results to demonstrate the effectiveness of the SLAW under the simplified and general system models respectively. Particularly, we evaluate the performance of the SLAW when the length of the wormhole link varies.

5.1. Performance evaluation under the simplified system model

For the simplified system model, we employ the unique disk graph (UDG) as the communication model in the simulations, in which there is no packet loss when the distance between two nodes is less than the transmission range.

The network settings are as follows: the sensors, locators, and attackers have equal transmission range, which is set as $R = 15m$; the locators are deployed independently with a density $\rho_l = 0.006/m^2$[§]; L/R denotes the ratio of the distance between two attackers to the transmission range of the attacker. For simplicity, we assume that the distance measurement error follows a normal distribution $N(\mu, \sigma^2)$ with the mean $\mu = 0$ and the standard deviation $\sigma = 0.5$.

[§]This node density results in that the average number of neighboring locators of each sensor is around four because the range-based localization requires each sensor to have at least three neighboring locators.

We repeat each simulation for 20 000 times by randomly deploying locators with the Poisson distribution. The average successful probabilities of the wormhole-attack-detection process and the secure localization process are reported. The localization is considered as successful only if $d_{err1} \leq d_{err2} + f_{tol} * R$, where d_{err1} (or d_{err2}) denotes the localization error with (or without) using the secure localization scheme; f_{tol} is the factor of localization error tolerance (0.1 in our simulations). We compare the SLAW with other three solutions: one standard localization approach without any wormhole attack detection (labeled as 'W/O detection') and two secure localization approaches, SeRLoc[10] and Consistency[14]. The SeRLoc scheme identifies some D-locators using the sector uniqueness property and communication range violation property, then conducts self-localization based on the rest locators. The consistency scheme identifies the D-locators on the basis of the consistency check of the estimation result; the most inconsistent locator will be considered as a D-locator.

Figure 5(a) shows the performance comparison of the SLAW and SeRLoc under the simplified system model in terms of the probability of successful wormhole attack detection. It shows that the SLAW outperforms the SeRLoc under different values of the length of the wormhole link. As the SLAW takes the closed-loop and open-loop wormhole attacks into consideration, which are overlooked by the SeRLoc, the SLAW can achieve better performance. It also shows that the SLAW provides successful wormhole-attack-detection probability at least 96% with different lengths of the wormhole link.

Figure 5(b) shows the performance comparison of the SLAW, SeRLoc, consistency, and the scheme without any detection process when the sensor is under the wormhole attack in terms of the probability of successful localization under the simplified system model. The simulation shows that our proposed scheme provides much better performance than the other schemes: our proposed scheme obtains a probability higher than 93% when $L/R < 2.5$ and a probability very close to 100% when $L/R \geq 2.5$. The performance of the scheme without any detection process clearly shows the severe impact of the wormhole

attack on the localization process. The localization process completely fails when the L/R is over 2. The under-performance of the SeRLoc is due to that it does not distinguish the closed-loop wormhole attack and open-loop wormhole attack, and the communication range violation property is likely invalid under the closed-loop wormhole attack.

In Figure 5(c), the effects of locator density on the performance of the SLAW under the simplified system model are illustrated. Evidently, the improvement of locator density conduces to better secure localization performance. When the locator density $\rho_l = 0.012$ (with average degree around 8), our proposed scheme achieves a performance with the probability of successful localization larger than 98%.

5.2. Performance evaluation under the general system model

We also conduct the simulation to illustrate the effectiveness of the SLAW under the general system model where packet loss exists and different types of nodes have different transmission radii. For the general system model, we adopt the quasi-UDG communication model [37]. In the quasi-UDG model, 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 r is the transmission range and $0 \leq \alpha \leq 1$. Moreover, the wormhole attack will drop the received packets with a probability ω ($0 \leq \omega \leq 1$).

The network settings for the general system model are as follows: the transmission range of sensors, locators and attackers are $R_S = 13m, R_L = 14m$, and $R_A = 15m$ respectively; $\alpha = 0.75$; $\omega = 0.2$; the localization is considered as successful only if $d_{err1} \leq d_{err2} + f_{tol} * R_S$. Except the aforementioned, all the other settings are similar to those under the simplified system model.

Figure 6(a) shows the performance comparison of the SLAW and SeRLoc in terms of the probability of successful wormhole attack detection under the general system model. It is shown that the SLAW outperforms the SeRLoc when $L/R_A \leq 2$ while there is no difference when $L/R_A > 2$. This is because the SLAW considers both the closed-loop and open-loop wormhole attacks while the SeRLoc only considers the open-loop wormhole attack. In the worst case, the SLAW provides a successful detection probability at least 70% while the SeRLoc does about 61%. When L/R_A is large enough, the probability of successful wormhole attack detection of the SLAW approximates 90%.

Figure 6(b) demonstrates the probability of false alarm when the sensor is under the wormhole attack. The reason that false alarms occur is that the sensor may miss some packets because of the transmission collisions or the random drop-offs. Figure 6(b) shows that the misidentification of the wormhole attack happens only when L/R_A is less than 2 and the probability is at most 1.2%. Note that the

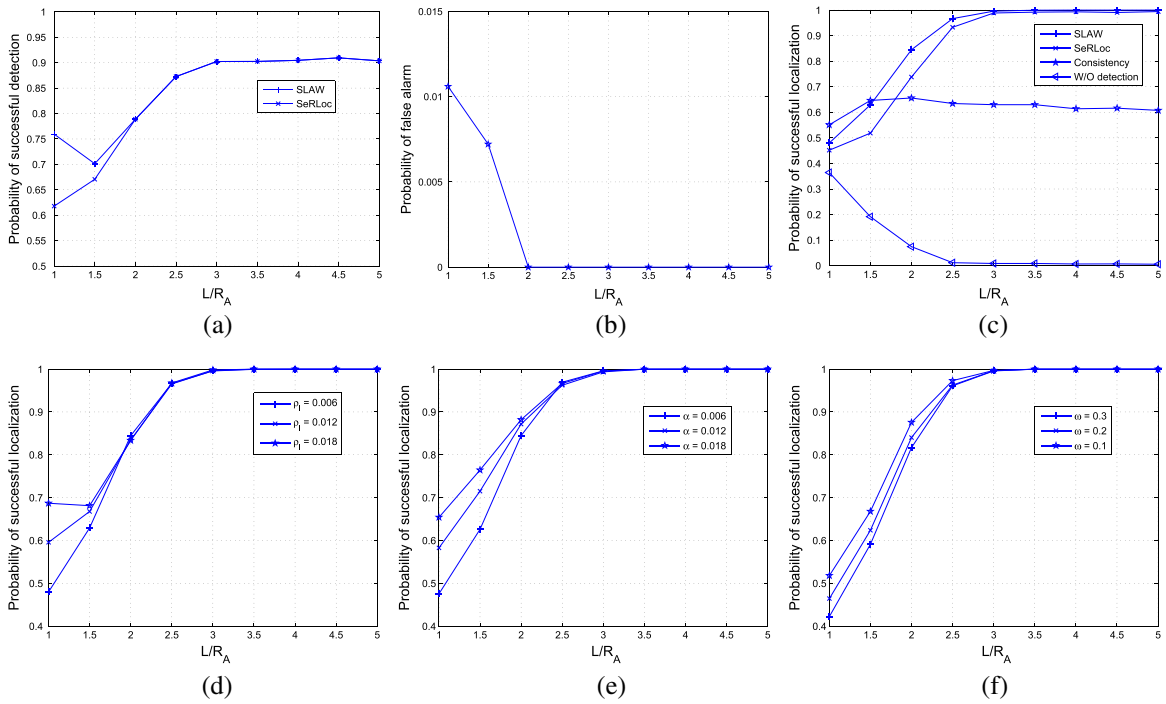

Figure 6. Performance comparison under the general system model: (a) the probability of successful wormhole detection, (b) the probability of false alarm for the SLAW, (c) the probability of successful localization, (d) the effects of locator density ρ_l, (e) the effects of α, and (f) the effects of ω.

false alarm only occurs under the general system model because of the packet loss.

Figure 6(c) shows the performance of successful localization of the SLAW, SeRLoc, consistency, and 'W/O detection' schemes under the general system model. Among these schemes, the SLAW obtains the best performance. The performance of the SLAW and SeRLoc increases with the increase of L/R_A while the performance of the consistency is insensitive to the value of L/R_A. When L/R_A is larger than 3, the probability of successful localization gets close to 100%.

Figure 6(d) shows the effects of the locator density ρ_l on the probability of successful localization of the SLAW. It shows that the performance of SLAW improves greatly with the increase of locator density when L/R_A is less than 2. When L/R_A is larger than 2, however, it seems that the increase of locator density has almost no improvement.

Figure 6(e) and (f) shows the effects of the α and ω on the probability of successful localization under the general system model respectively. As shown in Figure 6(e), when the value of α gets larger, the probability of packet loss will get smaller, resulting in the better performance of secure localization. Similarly, as shown in Figure 6(f), when the value of ω gets larger, the probability that the wormhole attackers drop the received packets will also become larger; thus, the performance of the secure localization will be worse. To sum up, the packet loss (caused by the packet collision during the inter-node communication or the random drop-off by the wormhole attackers) will deteriorate the performance of the secure localization.

6. CONCLUSION AND FUTURE WORK

In this paper, we analyze the severe impacts of the wormhole attack on the localization in the hostile WSNs. To tackle this security problem, we propose a novel secure localization scheme called SLAW, which includes three phases: wormhole attack detection, neighboring locators differentiation, and secure localization. We first consider the simplified system model in which there is no packet loss and all types of nodes have the same transmission range. We further extend the simplified system model to the general system model to be more applicable to the real application scenario, in which the packet loss exists and different types of nodes have different transmission radii. We conduct simulations to demonstrate the effectiveness of our proposed secure localization scheme and compare it with the existing schemes under different network parameters.

In this paper, we adopt the conservative strategy to handle the conflicting relationship among neighboring locators. In our future work, we will apply the topology inference theory to make the conflicting sets of neighboring locators consistent and trustable. The other direction of our future work will focus on the secure localization when a sensor node is under simultaneous multiple wormhole attacks.

ACKNOWLEDGEMENTS

We would like to express our thanks to both editor and referees for carefully reviewing this paper and for providing some insightful suggestions. Some parts of this paper have been published in IEEE UIC 2009 [48] and IPCCC 2010 [49]. This work was supported in part by NSFC grants (No.61309023, No.61272463, No.61273079), Shandong Provincial Natural Science Foundation, China (No.ZR2013FQ032), the Fundamental Research Funds for the Central Universities (No.13CX02100A), Open Project in Zhejiang Provincial Key Lab of Intelligent Processing Research of Visual Media (No.2012008), Hong Kong GRF grants (PolyU-524308, PolyU-521312), HKPU grants (A-PL16, A-PL84), and State Key Laboratory of Industrial Control Technology under (No.ICT1206 and No.ICT1207).

APPENDIX:

A. 1. Proof of theorem 1

Proof. We prove the theorem under the following three cases:

Case 1: For a locator L_j in $\mathcal{D}_R(A_1)$, it can exchange the *Beacon* message with its neighboring locators. As L_i lies in $\mathcal{D}_R(A_2) \setminus \mathcal{D}_R(A_1)$, it can calculate the distance between L_j and itself on the basis of their coordinates (the coordinate of L_j can be obtained from the received *Beacon* message). If L_i lies out of $\mathcal{D}_R(L_j)$, it derives that it receives a packet from a locator outside $\mathcal{D}_R(L_i)$; hence, L_i adds L_j into $\mathcal{C}(L_i)$; otherwise, if L_i lies in $\mathcal{D}_R(L_j)$, a direct transmission path between L_i and L_j exists in addition to the transmission path through the wormhole link. Consequently, L_i can receive the same message from L_j for more than once. Thus, L_j will be added into $\mathcal{C}(L_i)$. Moreover, because any other locator L_k outside $\mathcal{D}_R(A_1)$ cannot exchange messages with L_i through the wormhole link, there is no abnormality during the communication between L_i and L_k. Thus, $L_k \notin \mathcal{C}(L_i)$. Therefore, $\mathcal{C}(L_i)$ contains all the locators in $\mathcal{D}_R(A_1)$.

Case 2: Similar to Case 1, if L_i lies in $\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)$, $\mathcal{C}(L_i)$ contains all the locators in $\mathcal{D}_R(A_2)$.

Case 3: If L_i lies in $\mathcal{D}_R(A_1) \cap \mathcal{D}_R(A_2)$, it can exchange the *Beacon* message with all the locators in $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$. For each locator L_j in $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$, L_i will add it into $\mathcal{C}(L_i)$. As L_i can also receive the message transmitted by itself, L_i will then add itself into $\mathcal{C}(L_i)$. Meanwhile, for any other locator L_k outside $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$, it cannot be in $\mathcal{C}(L_i)$ as the message exchange between itself and L_i is not interfered by the wormhole link. Therefore, $\mathcal{C}(L_i)$ contains all the locators in $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$. □

A. 2. Proof of corollary 1

Proof. For a locator L_i in the region $\mathcal{D}_R(A_1) \cap \mathcal{D}_R(A_2)$, the *Beacon* message it sends can be received by the attacker A_2 that is within the transmission range of L_i, that is, $\mathcal{D}_R(L_i)$. After that, A_2 will relay the received *Beacon* message to A_1 via the wormhole link, and A_1 will then broadcast this message. Then, L_i can receive the broadcasted message as it lies in $\mathcal{D}_R(A_1)$. Similarly, the *Beacon* message can also travel from L_i to A_1 and then be relayed to A_2 and finally be received by L_i. Thus, according to the definition of conflicting set, L_i will add itself into $\mathcal{C}(L_i)$.

Otherwise, for a locator L_j outside the region $\mathcal{D}_R(A_1) \cap \mathcal{D}_R(A_2)$, the *Beacon* message it sends cannot travel through the wormhole link to itself, that is, travel within a loop, as L_j is not within the transmission range of both the two attackers simultaneously. Thus, L_j determines that $L_j \notin \mathcal{C}(L_j)$.

Therefore, we can conclude that a locator is in its own conflicting set if and only if it lies in $\mathcal{D}_R(A_1) \cap \mathcal{D}_R(A_2)$.□

A. 3. Proof of theorem 2

Proof. When the sensor is under a closed-loop wormhole attack as shown in Figure 2(a), all locators in $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$ are N-locators of the sensor. According to Theorem 1, for each L_i in $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$, all the locators in $\mathcal{C}(L_i)$ must lie in $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$. For each L_j outside $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$, as its message cannot travel via the wormhole link, there will be no abnormality during the message exchanges between L_j and its neighboring locators; thus, $\mathcal{C}(L_j) = \emptyset$. Therefore, $\forall L_i$ such that $\mathcal{C}(L_i) \neq \emptyset$, $L_i \in \mathcal{L}_D$. □

A. 4. Proof of theorem 3

Proof. When the sensor is under an open-loop wormhole attack, as shown in Figure 2(b), according to Theorem 1, if $\exists L_j \in \mathcal{C}(L_i)$, L_j must lie in $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$. If $L_j \notin \mathcal{L}_N$, then L_j lies in $\mathcal{D}_R(A_2) \setminus (\mathcal{D}_R(A_1) \cup \mathcal{D}_R(S))$. Therefore, L_j lies inside $\mathcal{D}_R(A_2) \setminus \mathcal{D}_R(A_1)$. Considering $L_j \in \mathcal{C}(L_i)$ leads to the conclusion that $L_i \in \mathcal{L}_D$. □

A. 5. proof of theorem 4

Proof. When the sensor is under an open-loop wormhole attack, if $L_j \in \mathcal{L}_D$ and $L_j \notin \mathcal{C}(L_j)$, according to Corollary 1, L_j is outside $\mathcal{D}_R(A_1) \cap \mathcal{D}_R(A_2)$. As $L_j \in \mathcal{L}_D$, L_j lies in $\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)$, and $\mathcal{C}(L_j)$ contains all the locators in $\mathcal{D}_R(A_2) \setminus \mathcal{D}_R(A_1)$. Therefore, $\forall L_i$ such that $\mathcal{C}(L_i) = \mathcal{C}(L_j)$; L_i also lies in $\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)$, which indicates $L_i \in \mathcal{L}_D$. □

A. 6. Proof of theorem 5

Proof. When the sensor is under an open-loop wormhole attack as shown in Figure 2(b), if $\mathcal{C}(L_k) \neq \emptyset$ and $L_k \notin \mathcal{C}(L_k)$, then L_k cannot lie in $\mathcal{D}_R(A_1) \cap \mathcal{D}_R(A_2)$; therefore, L_k can only lie in $(\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)) \cup (\mathcal{D}_R(A_2) \setminus \mathcal{D}_R(A_1))$. As $\mathcal{C}(L_j) = \emptyset$, L_j must be inside $\mathcal{D}_R(S) \setminus (\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2))$. Because the distance between two N-locators L_j and L_k is larger than $2R$, L_k does not lie in $\mathcal{D}_R(S)$. Because L_k is an N-locator of S, which means L_k lies in $\mathcal{D}_R(S) \cup \mathcal{D}_R(A_1)$, L_k must lie in $\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)$. According to Theorem 4, $\forall L_i$ such that $\mathcal{C}(L_i) = \mathcal{C}(L_k)$, $L_i \in \mathcal{L}_D$. □

A. 7. Proof of theorem 6

Proof. We first consider the scenario that different types of nodes have different transmission radii and there is no packet loss due to the communication errors or packet drop-offs. Similar to Theorem 1, we prove this under three cases:

Case 1: Considering a locator L_j in $\mathcal{D}_{R_L}(A_1)$, its *Beacon* message can be received by all its neighboring locators. As L_i lies in $\mathcal{D}_{R_A}(A_2) \setminus \mathcal{D}_{R_A}(A_1)$ and $(\mathcal{D}_{R_A}(A_2) \setminus \mathcal{D}_{R_A}(A_1)) \subseteq \mathcal{D}_{R_A}(A_2)$, it can calculate the distance between L_j and L_i after receiving the *Beacon* message from L_j. If the distance is larger than R_L, L_i derives that it receives a packet from a locator outside $\mathcal{D}_{R_L}(L_i)$, and then, $L_j \in \mathcal{C}(L_i)$; if the distance is less than R_L, L_i lies in $\mathcal{D}_{R_L}(L_j)$, and a direct transmission path between L_i and L_j exists in addition to the transmission path through the wormhole link. Consequently, L_i can receive the same message from L_j more than once. Therefore, $L_j \in \mathcal{C}(L_i)$. Moreover, for any other locator $L_k \notin \mathcal{D}_{R_L}(A_1)$, its message cannot arrive at L_i through the wormhole link; there is no abnormality during the message exchanges between L_i and L_k. Thus, $L_k \notin \mathcal{C}(L_i)$. Therefore, all locators in $\mathcal{C}(L_i)$ lie in $\mathcal{D}_{R_L}(A_1)$.

Case 2: Similar to Case 1, if L_i lies in $\mathcal{D}_{R_A}(A_1) \setminus \mathcal{D}_{R_A}(A_2)$, all the locators in $\mathcal{C}(L_i)$ lie in $\mathcal{D}_{R_L}(A_2)$.

Case 3: If L_i lies in $\mathcal{D}_{R_A}(A_1) \cap \mathcal{D}_{R_A}(A_2)$, it can receive the *Beacon* messages from all the locators in $\mathcal{D}_{R_L}(A_1) \cup \mathcal{D}_{R_L}(A_2)$ via the wormhole link. For each locator L_j inside $\mathcal{D}_{R_L}(A_1) \cup \mathcal{D}_{R_L}(A_2)$, L_i can detect the abnormality by either receiving the message for more than once or receiving the message from L_j, which is beyond the transmission range of itself. Therefore, $L_j \in \mathcal{C}(L_i)$. If L_i lies in $\mathcal{D}_{R_L}(A_1) \cap \mathcal{D}_{R_L}(A_2)$, it can also receive the message transmitted by itself; then, $L_i \in \mathcal{C}(L_i)$. Meanwhile, for any other locator L_k outside $\mathcal{D}_{R_L}(A_1) \cup \mathcal{D}_{R_L}(A_2)$, it cannot be in $\mathcal{C}(L_i)$ as its *Beacon* message cannot be received by L_i via the wormhole link. Thus, all the locators in $\mathcal{C}(L_i)$ lie in $\mathcal{D}_{R_A}(A_1) \cup \mathcal{D}_{R_A}(A_2)$.

We then discuss the scenario that the packet loss is taken into account. Because of the packet loss, some locators may fail to receive the *Beacon* messages from its neighboring locators, these locators' conflicting sets may lose integrity. That is, for a locator L_i locating in $\mathcal{D}_{R_A}(A_2) \setminus \mathcal{D}_{R_A}(A_1)$, $\mathcal{C}(L_i)$ is just a subset of the locators in $\mathcal{D}_{R_L}(A_1)$. However, it still satisfies that all the locators in $\mathcal{C}(L_i)$ lie in $\mathcal{D}_{R_L}(A_1)$. Similarly, if L_i lies in $\mathcal{D}_{R_A}(A_1) \setminus \mathcal{D}_{R_A}(A_2)$, all the locators in $\mathcal{C}(L_i)$ lie in $\mathcal{D}_{R_L}(A_2)$; if L_i lies in $\mathcal{D}_{R_A}(A_1) \cap \mathcal{D}_{R_A}(A_2)$, all locators in $\mathcal{C}(L_i)$ lie in $\mathcal{D}_{R_L}(A_1) \cup \mathcal{D}_{R_L}(A_2)$.□

A. 8. Proof of theorem 7

Proof. As shown in Figure 4, if the length of the wormhole link is larger than R_A+R_L, then $\mathcal{D}_{R_L}(A_2)\cap\mathcal{D}_{R_A}(A_1) = \emptyset$. When the sensor is under an open-loop wormhole attack, $\forall L_i$ such that $\mathcal{C}(L_i) \neq \emptyset$, L_i must lie in $\mathcal{D}_{R_L}(A_1)\cup\mathcal{D}_{R_L}(A_2)$. As $L_i \notin \mathcal{L}_D$, that is, L_i lies outside $\mathcal{D}_{R_L}(A_1)$, L_i can only lie in $\mathcal{D}_{R_L}(A_2)\setminus\mathcal{D}_{R_L}(A_1)$. Moreover, as $\mathcal{D}_{R_L}(A_2)\cap\mathcal{D}_{R_A}(A_1) = \emptyset$, we can obtain that L_i lies in $\mathcal{D}_{R_L}(A_2)\setminus\mathcal{D}_{R_A}(A_1)$. According to the result of the conflicting sets among the locators, as L_i lies in $\mathcal{D}_{R_L}(A_2) \setminus \mathcal{D}_{R_L}(A_1)$, all locators in $\mathcal{C}(L_i)$ lie in $\mathcal{D}_{R_L}(A_1)$. Therefore, $\forall L_j \in \mathcal{C}(L_i)$, $L_j \in \mathcal{L}_D$. □

A. 9. Proof of theorem 8

Proof. As shown in Figure 4, if the length of the wormhole link is larger than R_A+R_L, then $\mathcal{D}_{R_L}(A_1)\cap\mathcal{D}_{R_L}(A_2) = \emptyset$. As $L_i \notin \mathcal{L}_D$ and $\mathcal{C}(L_i) \neq \emptyset$, L_i must lie in $\mathcal{D}_{R_L}(A_2) \setminus \mathcal{D}_{R_A}(A_1)$ according to Theorem 7 when the sensor is under an open-loop wormhole attack. As $L_i \in \mathcal{C}(L_j)$, L_j cannot lie in $\mathcal{D}_{R_L}(A_2) \setminus \mathcal{D}_{R_A}(A_1)$; otherwise, if L_j lies in $\mathcal{D}_{R_A}(A_2) \setminus \mathcal{D}_{R_A}(A_1)$, all the locators in $\mathcal{C}(L_j)$, including L_i, lie in $\mathcal{D}_{R_L}(A_1)$, which contradicts to the condition that L_i lies in $\mathcal{D}_{R_L}(A_2) \setminus \mathcal{D}_{R_A}(A_1)$. Moreover, as $\mathcal{C}(L_j) \neq \emptyset$, L_j must lie in $\mathcal{D}_{R_L}(A_1) \cup \mathcal{D}_{R_L}(A_2)$. Because of $\mathcal{D}_{R_L}(A_1) \cap \mathcal{D}_{R_L}(A_2) = \emptyset$, L_j can only lie in $\mathcal{D}_{R_L}(A_1)\setminus\mathcal{D}_{R_A}(A_2)$, which means $L_j \in \mathcal{L}_D$. □

REFERENCES

1. Patwari N, Hero A, Perkins M, Correal N, O'Dea R. Relative location estimation in wireless sensor networks. *IEEE Transactions on Signal Processing* 2003; **51**(8): 2137–2148.
2. Savvides A, Han C, Srivastava M. Dynamic fine-grained localization in ad-hoc networks of sensors. In *Procedings of ACM International Conference on Mobile Computing and Betworking (MobiCom)*, Rome, Italy, 2001; 166–179.
3. Cheng X, Thaeler A, Xue G, Chen D. TPS: a time-based positioning scheme for outdoor wireless sensor networks. In *Proceedings of Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, Hong Kong, 2004; 2685–2696.
4. Niculescu D. Positioning in ad hoc sensor networks. *IEEE Network Magazine* 2004; **18**(4): 24–29.
5. Bouchereau F, Brady D. Bounds on range-resolution degradation using RSSI measurements. In *Proceedings of IEEE International Conference on Communications (ICC)*, Paris, France, 2004; 3246–3250.
6. Sit TC, Liu Z, Ang MH, Seah WK. Multi-robot mobility enhanced hop-count based localization in ad-hoc networks. *Robotics and Autonomous Systems* 2007; **55**(3): 244–252.
7. Liu C, Wu K. Sensor localization with ring overlapping based on comparison of received signal strength indicator. In *Proceedings of IEEE Internation Conference on Mobile Adhoc and Sensor Systems (MASS)*, Florida, USA, 2004; 516–518.
8. He T, Huang C, Blum BM, Stankovic JA, Abdelzaher T. Range-free localization and its impact on large scale sensor networks. *ACM Transactions on Embedded Computing Systems* 2005; **4**(4): 877–906.
9. Nagpa R. Organizing a global coordinate system from local information on an amorphous computer. *A. I. Memo 1666*, MIT, 1999.
10. Lazos L, Poovendran R. SeRLoc: robust localization for wireless sensor networks. *ACM Transactions on Sensor Networks* 2005; **1**(1): 73–100.
11. Bshara M, Orguner U, Gustafsson F, Biesen LV. Fingerprinting localization in wireless networks based on received-signal-strength measurements: a case study on WiMAX networks. *IEEE Transactions on Vehicular Technology* 2010; **59**(1): 283–294.
12. Ni LM, Liu Y, Lau YC, Patil AP. LANDMARC: indoor location sensing ssing active RFID. *Wireless Networks* 2004; **10**(1): 701–710.
13. Capkun S, Hubaux JP. Secure positioning in wireless networks. *IEEE Journal on Selected Areas in Communications* 2006; **24**(2): 221–232.
14. Liu D, Ning P, Liu A, Wang C, Du W. Attack-resistant location estimation in wireless sensor networks. *ACM Transactions on Information and Systems Security* 2008; **11**(4): 1–36.
15. Boukerche A, Oliveira HA, Nakamura EF, Loureiro AA. Secure localization algorithms for wireless sensor networks. *IEEE Communications Magazine* 2008; **46**(4): 96–101.
16. Lazos L, Poovendran R, Capkun S. ROPE: robust position estimation in wireless sensor networks. In *Proceedings of ACM/IEEE International Symposium on Information Processing in Sensor Networks (IPSN)*, New Jersey, USA, 2005; 324–331.
17. Srinivasan A, Teitelbaum J, Wu J. DRBTS: distributed reputation-based beacon trust system. In *Proceedings of IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC)*, Indiana, USA, 2006; 277–283.
18. Pirretti M, Vijaykrishnan N, McManiel P, Madan B. SLAT: secure localization with attack tolerance. *Technical Report*, 2006.
19. Liu D, Ning P, Du W. Detecting malicious beacon nodes for secure location discovery in wireless sensor networks. In *Proceedings of IEEE Internation Conference on Distributed Computing Systems (ICDCS)*, Ohio, USA, 2005; 609–619.

20. Anjum F, Pandey S, Agrawal P. Secure localization in sensor networks using transmission range variation. In *Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems (MASS)*, Washington, DC, USA, 2005; 195–203.
21. Capkun S, Rasmussen KB, Cagalj M, Srivastava M. Secure location verification with hidden and mobile base stations. *IEEE Transactions on Mobile Computing* 2008; **7**(4): 470–483.
22. Du W, Fang L, Ning P. LAD: localization anomaly detection for wireless sensor networks. *Journal of Parallel and Distributed Computing* 2006; **66**(7): 874–886.
23. Wang C, Liu A, Ning P. Cluster-based minimun mean square estimation for secure and resilient localization in wireless sensor networks. In *Proceedings of IEEE International Conference on Wireless Algorithms, Systems and Applications (WASA)*, Chicago, USA, 2007; 29–37.
24. Chen H, Lou W, Ma J, Wang Z. TSCD: a novel secure localization approach for wireless sensor networks. In *Proceedings of the International Conference on Sensor Technologies and Applications (SensorComm)*, Cap Esterel, France, 2008; 661–668.
25. Chen H, Lou W, Wang Z. A novel secure localization approach in wireless sensor networks. *Eurasip Journal on Wireless Communications and Networking* 2010; **2010**: 1–12, DOI: 10.1155/2010/981280.
26. Li Z, Trappe W, Zhang Y, Nath B. Robust statistical methods for securing wireless localization in sensor networks. In *Proceedings of ACM/IEEE International Symposium on Information Processing in Sensor Networks (IPSN)*, California, USA, 2005; 91–98.
27. Ding M, Chen D, Xing K, Cheng X. Localized fault-tolerant event boundary detection in sensor networks. In *Proceedings of Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, Florida, USA, 2005; 902–913.
28. Hu YC, Perrig A, Johnson DB. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications* 2006; **24**(2): 370–380.
29. Wang W, Bharat B, Lu Y, Wu X. Defending against wormhole attacks in mobile ad hoc networks. *Wireless Communication and Mobile Computing* 2006; **3** (4): 483–503.
30. Capkun S, Buttyan L, Hubaux JP. SECTOR: secure tracking of node encounters in multi-hop wireless networks. In *Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks*, Virginia, USA, 2003; 21–32.
31. Hu YC, Perrig A, Johnson DB. Rushing attacks and defense in wireless ad hoc network routing protocols. In *Proceedings of ACM Workshop on Wireless Security (WiSec)*, California, USA, 2003; 30–40.
32. Eriksson J, Krishnamurthy S, Faloutsos M. TrueLink: a practical countermeasure to the wormhole attack in wireless networks. In *Proceedings of IEEE Internation Conference on Network Protocols (ICNP)*, California, USA, 2006; 75–84.
33. Xu Y, Chen G, Ford J, Makedon F. Critical infrastructure protection. In *Detecting Wormhole Attacks in Wireless Sensor Networks*, Vol. 253, Goetz E, Shenoi S (eds). Springer: Heidelberg, 2008; 267–279.
34. Khalil I, Bagchi S, Shroff NB. LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks. In *Proceedings of the International Conference on Dependable Systems and Networks (DSN)*, Washington, DC, USA, 2005; 612–621.
35. Khalil I, Bagchi S, Shroff NB. MobiWorp: mitigation of the wormhole attack in mobile multihop wireless networks. In *Proceedings of Securecomm and Workshops*, Amsterdam, The Netherlands, 2006; 344–362.
36. Wang W, Kong J, Bhargava B, Gerla M. Visualisation of wormholes in underwater sensor networks: a distributed approach. *International Journal of Security and Networks* 2008; **3**(1): 10–23.
37. Maheshwari R, Gao J, Das SK. Detecting wormhole attacks in wireless networks using connectivity information. In *Proceedings of Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, Alaska, USA, 2007; 107–115.
38. Ban X, Sarkar R, Gao J. Local connectivity tests to identify wormholes in wireless networks. In *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Paris, France, 2011; 1–10.
39. Dong D, Li M, Liu Y, Li XY, Liao X. Topological detection on wormholes in wireless ad hoc and sensor networks. *IEEE/ACM Transactions on Networking* 2011; **19**: 1787–1796.
40. Dimitriou T, Giannetsos A. Wormholes no more? Localized wormhole detection and prevention in wireless networks. In *Proceedings of IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS)*, California, USA, 2010; 334–347.
41. Lazos L, Poovendran R. HiRLoc: high-resolution robust localization for wireless sensor networks. *IEEE Journal on Selected Areas in Communications* 2006; **24**(2): 233–246.
42. Chen H, Lou W, Wang Z. A consistency-based secure localization scheme against wormhole attacks in WSNs. In *Proceedings of IEEE International*

Conference on Wireless Algorithms, Systems and Applications (WASA), Massachusetts, USA, 2009; 368–377.
43. Chen H, Lou W, Sun X, Wang Z. A secure localization approach against wormhole attacks using distance consistency. *Eurasip Journal on Wireless Communications and Networking* 2010: 1–11, Article ID 627039.
44. Wu J, Chen H, Lou W, Wang Z, Wang Z. Label-based DV-hop localization against wormhole attacks in wireless sensor networks. In *Proceedings of IEEE International Conference on Networking, Architecture, and Storage (NAS)*, Macau, 2010; 79–88.
45. Zhao M, Servetto SD. An analysis of the maximum likelihood estimator for localization problems. In *Proceedings of IEEE International Conference on Broadband Networks (BroadNets)*, Massachusetts, USA, 2005; 982–990.
46. Ganeriwal S, Popper C, Capkun S, Srivastava MB. Secure time synchronization in sensor networks. *ACM Transactions on Information and Systems Security* 2008; **11**(4): 1–31.
47. Khabbazian M, Mercier H, Bhargava VK. Wormhole attack in wireless ad hoc networks: analysis and countermeasure. In *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM)*, California, USA, 2006; 1–6.
48. Chen H, Lou W, Wang Z. Conflicting-set-based wormhole attack resistant localization in wireless sensor networks. In *Proceedings of IEEE International Conference on Ubiquitous Intelligence and Computing (UIC)*, Brisbane, Australia, 2009; 296–309.
49. Chen H, Lou W, Wang Z. Secure localization against wormhole attacks using conflicting sets. In *Proceedings of IEEE International Performance Computing and Communications Conference (IPCCC)*, New Mexico, USA, 2010; 25–33.

AUTHORS' BIOGRAPHIES

Honglong Chen received his BE degree in automation from China University of Petroleum, China, in 2006, his ME degree in the Department of Control from Zhejiang University, China, in 2008, and his PhD degree in computer science from The Hong Kong Polytechnic University, Hong Kong, in 2012. He is currently a lecturer in the College of Information and Control, China University of Petroleum, China. His research interests are in the areas of wireless sensor networks, delay tolerant networks, security and privacy. His research work is supported by NSFC grant, Shandong Provincial NSF grant, and so on.

Wei Lou received his BE degree in electrical engineering from Tsinghua University, China, in 1995, his ME degree in telecommunications from Beijing University of Posts and Telecommunications, China, in 1998, and his PhD degree in computer engineering from Florida Atlantic University, in 2004. He is currently an assistant professor in the Department of Computing, The Hong Kong Polytechnic University, HKSAR, China. His current research interests are in the areas of mobile ad hoc and sensor networks, peer-to-peer networks, and mobile computing. He has worked intensively on designing, analyzing, and evaluating practical algorithms with the theoretical basis, as well as building prototype systems. His research work is supported by several Hong Kong GRF grants, NSFC grant, and Hong Kong Polytechnic University ICRG grants.

Zhi Wang received his BS degree from Shenyang Jian Zhu University, Shenyang, China, in 1991, his MS degree from Southeast University, China, in 1997, and his PhD degree from Shenyang Institute of Automation, Chinese Academy of Sciences, Shenyang, China, in 2000. From 2001 to 2002, he was a postdoctoral researcher at the Lorraine Laboratory of IT Research and Applications (LORIA), France. From 2007 to 2008, he was a visiting researcher with Jonkoping University and the Royal Institute of Technology, Sweden. He is currently an associated professor of Control Science and Engineering with Zhejiang University. His research interests include mobile sensing systems including agent-based information processing, real-time classification, and tracking; industrial communication and systems including reliable and real-time communication protocols; and networked control systems.