

# Conflicting-Set-Based Wormhole Attack Resistant Localization in Wireless Sensor Networks <sup>★</sup>

Honglong Chen<sup>1</sup>, Wei Lou<sup>1</sup>, and Zhi Wang<sup>2</sup>

<sup>1</sup> Department of Computing,  
The Hong Kong Polytechnic University, Kowloon, Hong Kong  
{cshlchen, csweilou}@comp.polyu.edu.hk

<sup>2</sup> State Key Laboratory of Industry Control Technology,  
Zhejiang University, Hangzhou, P. R. China  
wangzhi@iipc.zju.edu.cn

**Abstract.** The wormhole attack sniffs packets in one point in the network, tunnels them through a wired or wireless link to another point to cause severe influence on the localization process or routing process in the network. In this paper, we analyze the impact of the wormhole attack on the localization in wireless sensor networks and we propose a wormhole attack resistant secure localization scheme. The main idea of our proposed scheme is to build a so-called conflicting set for each locator based on the abnormalities of message exchanges among neighboring locators, and then to identify all dubious locators which are filtered out during localization. Our proposed scheme can identify the dubious locators with a very high probability to achieve secure localization. The simulation results show that it outperforms the existed schemes under different network parameters.

**Keywords:** Conflicting Set; Secure Localization; Wireless Sensor Networks; Wormhole Attack.

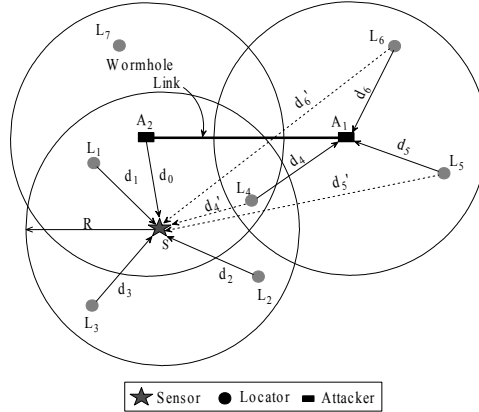
## 1 Introduction

Wireless sensor networks (WSNs) have been well studied in the past few years and numerous related applications have been developed. Particularly, sensor networks are usually deployed in a hostile environment, where the sensor nodes are vulnerable to various types of attacks in the network. In this paper, we concentrate on the localization against the *wormhole attack* [1], which can be mounted by two colluding external attackers. In such network, there are three types of nodes deployed including sensors, locators and attackers, which all have the same transmission range  $R$ . The locators have fixed locations and have known their own locations in advance. The sensors are location-unknown and they can estimate their locations by measuring the distances to the locators. Two colluding attackers disrupt the localization procedure of the sensors by relaying the received packets through a *wormhole link*, which provides a direct low-latency transmission channel between them. Being as external attackers that cannot compromise

---

<sup>★</sup> This work is supported in part by grants PolyU 5236/06E, PolyU 5232/07E, PolyU 5243/08E, and NSFC No. 60873223 and No. 90818010.

legitimate nodes or their cryptographic keys, the wormhole attackers cannot acquire the content, e.g., the type, of the sniffed packets. In this paper, we assume that there is no region in the network attacked by more than one wormhole attack. Fig. 1 illustrates the impact of the wormhole attack on the localization when the Time Difference of Arrival (TDoA) method is applied to estimate the distances between the locators and the sensor. Without the wormhole attack, the sensor  $S$  will conduct the self-localization based on  $d_1$ ,  $d_2$ ,  $d_3$  and  $d'_4$  using the maximum likelihood estimation (MLE) approach [2]. However, as the packets transmitted by the locators  $L_4$ ,  $L_5$  and  $L_6$  can be relayed to  $S$  through the wormhole link. When  $S$  measures the distances with the packets from  $L_4$ ,  $L_5$  and  $L_6$  using TDoA method, take  $L_6$  for example, the packet from  $L_6$  goes through the path  $L_6 \rightarrow A_1 \rightarrow A_2 \rightarrow S$  to reach  $S$ . As the transmission time in the wormhole link can be ignored, the time difference of arrival is introduced only in two segments of the transmission path, from  $L_6$  to  $A_1$  and from  $A_2$  to  $S$ . Thus, the measured distance between  $S$  and  $L_6$  is  $d_6 + d_0$ , instead of the actual distance  $d'_6$ . Similarly,  $S$  will measure the distances to  $L_4$  and  $L_5$  as  $d_4 + d_0$  and  $d_5 + d_0$ , respectively. As  $A_2$  relays the packets from  $A_1$  with the maximum transmitting power level, the upper limit of  $d_0$  is  $R$ , thus the measured distances introduced by the wormhole attack may be larger than  $R$ . Consequently,  $S$  will adopt false distance measurements into localization, leading to an incorrect estimation of the location. Therefore, an ordinary localization scheme without considering the adversarial attacks cannot fulfil the positioning task in the scenario under the wormhole attack.



**Fig. 1.** Wormhole attack in the TDoA-based localization.

To overcome the impact of the wormhole attack on the localization, we propose an attack-resistant localization scheme in this paper. The main idea of our proposed scheme is to build a so-called *conflicting set* for each locator based on the abnormalities of message exchanges among neighboring locators, and then identify all the *dubious* locators (such as  $L_4$ ,  $L_5$  and  $L_6$  in Fig. 1) which can be filtered out during localization. The main contributions of this paper are summarized as follows: 1) We propose

a mechanism to build conflicting set for each locator according to the abnormalities of message exchanges among neighboring locators; 2) We propose a novel secure localization scheme which is wormhole attack resistant including wormhole attack detection and dubious locators identification; 3) We present simulations to demonstrate the effectiveness of our proposed scheme.

The remainder of this paper is organized as follows. In Section 2, we provide the related work on secure localization. In Section 3, we propose the secure localization scheme which is wormhole attack resistant. Section 4 presents the performance evaluation. Section 5 gives the concluding remarks on this work.

## 2 Related Work

Many localization mechanisms [3, 4] in WSNs have been developed recently. However, these systems can not obtain satisfied performance when adversarial attacks exist in the network. Thus, researchers have proposed several secure localization systems [5] for the hostile environment.

Liu et al. [6] propose two secure localization schemes against the compromise attack, range-based and range-free respectively. SPINE [7] applies the verifiable multilateration and verification of positions of mobile devices into the secure localization in the hostile network. The mechanism in [8] introduces a set of covert base stations (CBS), whose positions are not known to the attackers, to check the validity of the nodes. Lazos et al. ROPE [9] is a robust positioning system with a location verification mechanism that verifies the location claims of the sensors before data collection. DRBTS [10] is a distributed reputation-based beacon trust security protocol aimed at providing secure localization in sensor networks. Based on a quorum voting approach, DRBTS drives beacons to monitor each other and therefore enables them to decide which should be trusted. A suit of techniques in [11] are introduced to detect malicious beacons which supply incorrect information to the sensor nodes.

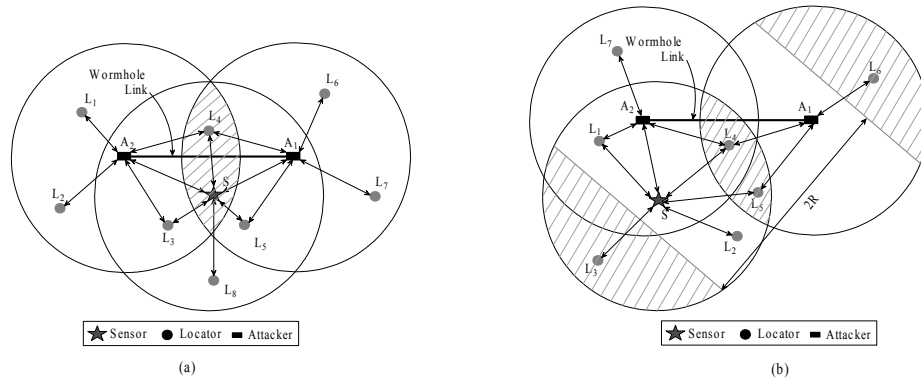
Khabbazian et al. [12] formulate the influence of wormhole attack on building the shortest path in routing protocols. In [1] a new, general mechanism called *packet leashes* based on the notions of geographical and temporal leashes is proposed to detect the wormhole attack. Wang et al. [13] detect the wormhole attack by visualizing the anomalies introduced by the attack based on all the distance messages between each two nodes. [14] further improves [13] to make it more suitable for large scale network by selecting some feature points to reduce the overlapping issue and preserving the major topology features. Xu et al. [15] propose a wormhole attack detection algorithm which uses a hop counting technique as a probe procedure, reconstructs local maps for each node and uses a feature called “diameter” to detect abnormalities caused by wormholes. In [16], a wormhole attack detection scheme is proposed using the maximum number of independent neighbors of two non-neighbor nodes. However, all the above wormhole detection schemes emphasize the detection without considering the localization scenario.

The above schemes only consider the detection of wormhole attack without the secure localization. SeRLoc [17] detects the wormhole attack based on the *sector uniqueness* property and *communication range violation* property using the directional anten-

nas, then filters out the attacked locators to obtain secure localization. HiRLoc [18] further utilizes antenna rotations and multiple transmit power levels to provide higher localization resolution. The schemes in [6] can also be applied in localization against wormhole attacks. However, all these schemes have drawbacks: SeRLoc and HiRLoc cannot obtain satisfied localization performance as some attacked locators may still be undetected, and [6] can not be competent in the scenario with many attacked locators. Our proposed scheme in this paper can overcome the above drawbacks without using extra hardware such as directional antennae required in SeRLoc and HiRLoc.

### 3 Wormhole Attacks Resistent Secure Localization Scheme

In this section, we first give several definitions about the network, after which we propose the wormhole attack resistant localization scheme.



**Fig. 2.** Illustrations of wormhole attack: (a) Duplex wormhole attack; (b) Simplex wormhole attack.

The localization of the sensor is attacked by the wormhole only if the sensor enters the transmission area of either attacker and exchange messages with the locators through the wormhole link. Two different types of wormhole attacks, named *duplex wormhole attack* (Fig. 2(a)) and *simplex wormhole attack* (Fig. 2(b)), are defined as follows:

**Definition 1.** *Duplex wormhole attack:* The sensor is under a duplex wormhole attack when it lies in the common transmission area of the two attackers. That is, messages transmitted from either attacker can arrive at the sensor.

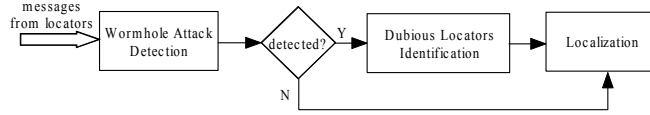
**Definition 2.** *Simplex wormhole attack:* The sensor is under a simplex wormhole attack when it lies in the transmission range of either one attacker but not in the common transmission area of the two attackers. That is, messages transmitted from only one attacker can arrive at the sensor.

**Definition 3. Neighboring locator:** The neighboring locators of a sensor refer to the locators that can exchange messages with the sensor, either via the wormhole link or not.

**Definition 4. Valid locator:** The neighboring locators, which are in the transmission range of the sensor, are called valid locators (V-locators) because their messages can be directly received by the sensor to obtain correct distance measurements.

**Definition 5. Dubious locator:** The locators, which are inside the transmission range of the attacker and can exchange messages with the sensor via the wormhole link, are called dubious locators (D-locators) since their distance measurements may negatively affect the localization process. In the following of this paper, we denote the set of V-locators, D-locators, and neighboring locators of the sensor as  $\mathcal{L}_V$ ,  $\mathcal{L}_D$  and  $\mathcal{L}_N$ . We also denote  $\mathcal{D}_R(u)$  as a disk centered at  $u$  with radius  $R$ . As shown in Fig 1, for the sensor  $S$ ,  $\mathcal{L}_V = \{L_1, L_2, L_3, L_4\}$ ,  $\mathcal{L}_D = \{L_4, L_5, L_6\}$ , and  $\mathcal{L}_N = \{L_1, L_2, L_3, L_4, L_5, L_6\}$ .

When the sensor is under a wormhole attack, the localization process would be disrupted as the existence of dubious locators. As shown in Fig. 3, our proposed scheme firstly detects the wormhole attack. If the wormhole attack is detected, dubious locators identification scheme will be triggered, after which the localization based on the correct distance measurements is conducted.



**Fig. 3.** Flow chart of the proposed secure localization scheme.

### 3.1 Wormhole Attack Detection

Before conducting self-localization, the sensor first detects the existence of wormhole attack. The sensor broadcasts a *Loc\_req* message and waits for 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 as well as measure the distance to each neighboring locator using the received *Loc\_ack* message. To counteract the random queueing delay introduced on the locators and sensor, the sensor measures the response time of each locator using the mechanism described in [19]: When broadcasting the *Loc\_req* packet, the sensor records the local time  $T_0$ . Every locator gets the local time  $T_1$  by time-stamping the packet at the MAC layer (i.e. the time when the packet is built at the MAC layer) instead of time-stamping the packet at the application layer. Similarly, when responding the *Loc\_ack* packet, the locator puts the local time  $T_2$  at the MAC layer, both  $T_1$  and  $T_2$  are attached in the *Loc\_ack* packet. When receiving the *Loc\_ack* packet, the sensor gets its local time  $T_3$ , and calculates the response time of the locator as  $(T_3 - T_0) - (T_2 - T_1)$ . It is noted that this mechanism only only eliminates the random delay at the MAC layer of the locators from the response time.

The following four detection schemes can detect the wormhole attack independently.

**Detection scheme D1 based on node's self-exclusion property:** The node's self-exclusion states that a node cannot receive packets transmitted by itself in a loop-free path. Therefore, if the sensor receives packets transmitted by itself, it can simply determine that it is under a wormhole attack.

**Detection scheme D2 based on packet unduplication property:** The packet unduplication property states that a node can receive at most one copy of the same message from one neighboring node. As  $L_4$  in Fig. 2(b), when locator  $L_4$  responds  $S$ '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.

**Detection scheme D3 based on node's spatial constraint property:** The node's spatial constraint property states that the measured distance between two neighboring nodes cannot be larger than  $R$ . As we mentioned in the introduction, the measured distance between the sensor and its neighboring locator may be larger than  $R$  due to the wormhole attack. Therefore, the sensor can check whether any measured distance is larger than  $R$  to detect a wormhole attack.

**Detection scheme D3 based on neighboring nodes' spatial constraint property:** The neighboring nodes' spatial constraint property suggests that a node cannot receive messages from two neighboring nodes simultaneously if the distance between these two nodes is larger than  $2R$ . As shown in Fig. 2(b), after receiving the *Loc\_req* message from neighboring locators,  $S$  checks whether the distance between any two locators is larger than  $2R$ . If  $S$  detects that the distance of two locators (e.g.,  $L_3$  and  $L_6$ ) is larger than  $2R$ , it derives that it is under a wormhole attack.

The procedure of the wormhole attack detection uses the above four detection schemes: The sensor first builds the set of its neighboring locators with the received *Loc\_ack* messages from the neighboring locators. It then uses detection scheme D1 to detect the duplex wormhole attack and uses detection schemes D2, D3 or D4 to detect the simplex wormhole attack. The algorithm of the wormhole attack detection process lists in Algorithm 1:

---

**Algorithm 1** Wormhole attack detection

---

- 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:     A duplex wormhole attack is detected.
  - 5: **else if** detect the wormhole attack based on schemes D2, D3 or D4 **then**
  - 6:     A simplex wormhole attack is detected.
  - 7: **else**
  - 8:     No wormhole attack is detected.
  - 9: **end if**
-

### 3.2 Dubious Locators Identification

The main idea of the dubious locators identification algorithm is to build a so-called conflicting set for each locator based on the abnormalities of message exchanges among neighboring locators. The conflicting set is defined as below:

**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 message sent by itself, (2) neighboring locators that are within the transmission range of  $L_i$  but receive the same message from different paths for more than once, and (3) neighboring locators that are outside the transmission range of  $L_i$  but can exchange messages with  $L_i$ .

Each locator can build its conflicting set based on the periodical *Beacon* message exchanges with its neighboring locators. When a locator detects the *Beacon* message abnormality, it will consider the sender locator of this *Beacon* message as the abnormal neighboring locator and put this sender locator into its conflicting set. When such a locator receives a *Loc\_req* message from the sensor, it will response a *Loc\_ack* message including its conflicting set to the sensor.

The relation between the locator and its conflicting set is elaborated as the following theorem.

**Theorem 1.** Given a network under a wormhole attack, (1) if  $L_i$  lies in  $\mathcal{D}_R(A_2) \setminus \mathcal{D}_R(A_1)$ ,  $C(L_i)$  contains all the locators in  $\mathcal{D}_R(A_1)$ ; (2) if  $L_i$  lies in  $\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)$ ,  $C(L_i)$  contains all the locators in  $\mathcal{D}_R(A_2)$ ; (3) if  $L_i$  lies in  $\mathcal{D}_R(A_1) \cap \mathcal{D}_R(A_2)$ ,  $C(L_i)$  contains all the locators in  $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$ .

*Proof:* (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  $L_i$ . 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,  $L_j \in C(L_i)$ ; 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. Therefore,  $L_j \in C(L_i)$ . Moreover, since any other locators  $L_k \notin \mathcal{D}_R(A_1)$  cannot exchange message with  $L_i$  through the wormhole link, there is no abnormality in the communication between  $L_i$  and  $L_k$ . Therefore,  $C(L_i)$  contains all the locators in  $\mathcal{D}_R(A_1)$ .

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

(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  $C(L_i)$ . As  $L_i$  can also receive the message transmitted by itself,  $L_i \in C(L_i)$ . Meanwhile, locator  $L_k \notin \mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$  cannot be in  $C(L_i)$  as the message exchange between  $L_i$  and  $L_k$  is not interfered by the wormhole link. Therefore,  $C(L_i)$  contains all the locators in  $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$ . ■

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

As shown in Fig 2(a),  $L_1, L_2, L_3$  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  $C(L_3) =$

$\{L_4, L_5, L_6, L_7\}$ . For  $L_4$ , its conflicting set is  $C(L_4) = \{L_1, L_2, L_3, L_4, L_5, L_6, L_7\}$ . for  $L_8$ , its conflicting set is empty.

**Duplex Wormhole Attack** When the sensor is under a duplex wormhole attack as shown in Fig. 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 neighboring locators to identify the V-locators and D-locators.

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

**Proof:** When the sensor is under a duplex wormhole attack as shown in Fig. 2(a), all locators in  $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$  are neighboring locators of the sensor. According to Theorem 1,  $\forall L_i \in \mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$ ,  $C(L_i) \in \mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$ . For each  $L_j \notin \mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$ , as its message cannot travel through the wormhole link, there will be no abnormality of the message exchange between  $L_j$  and other locators, thus  $C(L_j) = \emptyset$ . Therefore,  $\forall L_i$  such that  $C(L_i) \neq \emptyset$ ,  $L_i \in \mathcal{L}_D$ . ■

**Identification scheme I1:** When the sensor detects that it is under a duplex wormhole, it can obtain the conflicting sets of the neighboring locators from the received *Loc\_ack* messages. The sensor consider the ones with non-empty conflicting set as D-locators.

**Simplex Wormhole Attack** As shown in Fig. 2(b), when the sensor is under a simplex wormhole attack, only the locators in  $\mathcal{D}_R(A_1)$  are D-locators. We propose the following three identification schemes to identify all D-locators in this scenario.

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

**Proof.** When the sensor is under a simplex wormhole attack, as shown in Fig. 2(b), according to Theorem 1, if  $\exists L_j \in C(L_i)$ ,  $L_j$  must lie in  $\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2)$ . If  $L_j \notin \mathcal{L}_N$ ,  $L_j \in \mathcal{D}_R(A_2) \setminus (\mathcal{D}_R(A_1) \cup \mathcal{D}_R(S))$ . Therefore,  $L_j \in \mathcal{D}_R(A_2) \setminus \mathcal{D}_R(A_1)$ . Considering  $L_j \in C(L_i)$ , which leads to the conclusion that  $L_i \in \mathcal{L}_D$ . ■

When the sensor detects that it is under a duplex wormhole, it can obtain the conflicting sets of the neighboring locators from the received *Loc\_ack* messages.

**Identification scheme I2:** When the sensor is under a simplex wormhole attack, it obtains the conflicting sets of the neighboring locators from the received *Loc\_ack* messages. By detecting the existence of non-neighboring locators in the conflicting set of one locator, the sensor can determine that this locator is a D-locator. In the scenario of Fig. 2(b),  $L_4, L_5$  and  $L_6$  will add  $L_7$  into their conflicting sets, so the sensor can identify them as D-locators.

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

**Proof.** When the sensor is under a simplex wormhole attack, if  $L_j \in \mathcal{L}_D$  and  $L_j \notin C(L_j)$ , according to Corollary 1,  $L_j \notin \mathcal{D}_R(A_1) \cap \mathcal{D}_R(A_2)$ . As  $L_j \in \mathcal{L}_D$ ,  $L_j$  lies in  $\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)$ , and  $C(L_j)$  contains all the locators in  $\mathcal{D}_R(A_2) \setminus \mathcal{D}_R(A_1)$ . Therefore,  $\forall L_i$  such that  $C(L_i) = C(L_j)$ ,  $L_i$  must also lies in  $\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)$ , which means  $L_i \in \mathcal{L}_D$ . ■

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

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

**Proof.** When the sensor is under a simplex wormhole attack as shown in Fig. 2(b), if  $C(L_k) \neq \emptyset$  and  $L_k \notin C(L_k)$ , then  $L_k$  cannot lie in  $\mathcal{D}_R(A_1) \cap \mathcal{D}_R(A_2)$ , therefore,  $L_k$  can only lie in  $\mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)$  or  $\mathcal{D}_R(A_2) \setminus \mathcal{D}_R(A_1)$ . As  $C(L_j) = \emptyset$ ,  $L_j \in \mathcal{D}_R(S) \setminus (\mathcal{D}_R(A_1) \cup \mathcal{D}_R(A_2))$ . Since the distance between two neighboring locators  $L_j$  and  $L_k$  is larger than  $2R$ ,  $L_k$  does not lie in  $\mathcal{D}_R(S)$ . Since  $L_k$  is a neighboring 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  $C(L_i) = C(L_k)$ ,  $L_i \in \mathcal{L}_D$ . ■

**Identification scheme I4:** When the sensor is under a simplex wormhole attack, if it detects that the distance of two neighboring locators  $L_j$  and  $L_k$  are larger than  $2R$ ,  $L_j$ 's conflicting set is empty,  $L_k$ 's conflicting set is not empty and does not contain  $L_k$  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 Fig. 2(b) for example, the distance between them is larger than  $2R$ , so the sensor can determine that  $L_6 \in \mathcal{D}_R(A_1) \setminus \mathcal{D}_R(A_2)$ . As  $C(L_5) = C(L_6)$ ,  $L_5$  will be considered as a D-locator.

The procedure to identify the dubious locators works as follows: After the locators build their conflicting sets, if the sensor detects that it is under a duplex wormhole attack, it identifies the D-locators using the identification scheme I1. Otherwise, if the sensor detects that it is under a simplex wormhole attack, it identifies the D-locators using the identification scheme I2, I3, and I4. At the end, all other neighboring locators which are not included into the D-locators are considered as V-locators. The algorithm of the dubious locators identification process lists in Algorithm 2:

---

**Algorithm 2** Dubious locators identification process

---

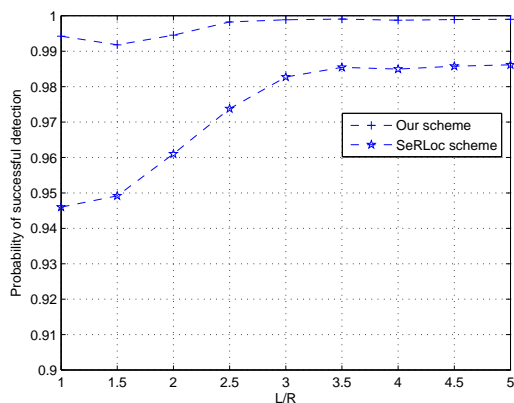
- 1: Each locator Periodically exchanges the *Beacon* messages with all its neighboring locators and builds its conflicting set based on the received *Beacon* messages.
  - 2: When receiving the *Loc.req* message from the sensor  $S$ , each locator replies the *Loc.ack* message including its conflicting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

### 3.3 Localization

After wormhole attack detection and dubious locators identification, 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 Fig. 2(a) and  $L_3$ ,  $L_4$  in Fig. 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.

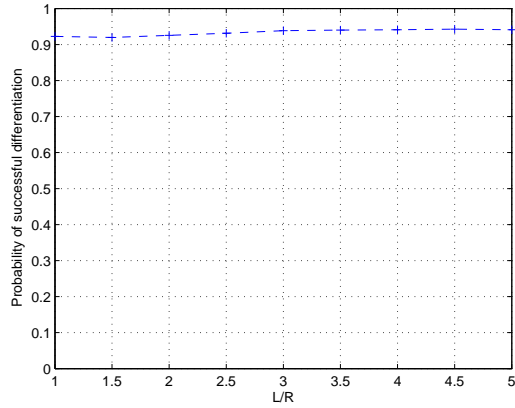
## 4 Simulation Results

In this section, we present the simulation results to demonstrate the effectiveness of our proposed secure localization scheme. The network setting are as following: the transmission range  $R$  is equal and is set to  $15m$ ; the locators are deployed with the Poisson distribution, and their density is set as  $\rho_l = 0.006/m^2$ ; the measurement error of the distance follows a normal distribution  $N(\mu, \sigma^2)$ , where  $\mu = 0$  and  $\sigma = 0.5$ ; we assume the length of the wormhole link  $L > R$  to avoid the endless packet transmission loop of the attackers, the label  $L/R$  of the  $x$  axis denotes the ratio of the length of the wormhole link to the transmission range.



**Fig. 4.** Probability of successful wormhole detection in WSNs.

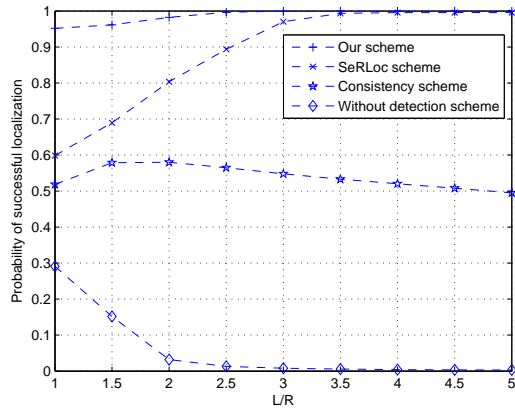
Fig. 4 shows the performance comparison of SeRLoc scheme [17] and our proposed scheme in terms of the probability of successful wormhole attack detection. It shows that our proposed scheme outperforms SeRLoc scheme under different values of the length of the wormhole link. As our proposed scheme takes the duplex wormhole attack and the distance measurement bound into consideration, which SeRLoc does not



**Fig. 5.** Probability of dubious locators identification.

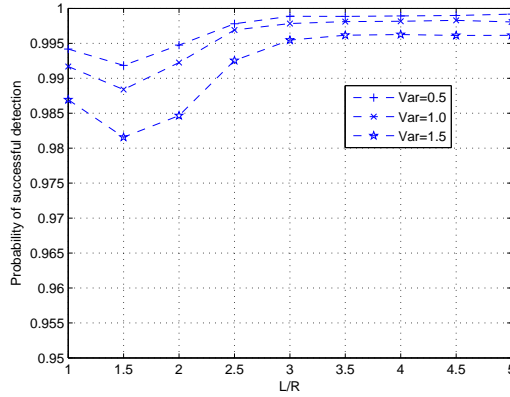
investigate, our proposed scheme can obtain higher performance. It is demonstrated in Fig. 4 that our proposed scheme provides successful wormhole attack detection probability at least 99%, and it gets very close to 100% when  $L/R \geq 2.5$ .

Fig. 5 shows the probability that the sensor successfully identifies all the dubious locators. In the dubious locators identification schemes, if the required condition for any identification scheme is satisfied, the sensor can trigger the corresponding identification scheme to identify all the dubious locators without failure. It shows that our proposed scheme provides perfect performance on identifying dubious locators (with the probability at least 92%).



**Fig. 6.** Probability of successful secure localization.

Fig. 6 shows the performance comparison of our proposed scheme, SeRLoc scheme, the consistency scheme [6] and the scheme without any detection process when the



**Fig. 7.** Effects of distance measurement error on secure localization performance.

sensor is under the wormhole attack in terms of the probability of successful secure localization. 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. However, SeRLoc scheme does not distinguish the duplex wormhole attack and simplex wormhole attack, and the communication range violation property may be invalid under the duplex wormhole attack. The consistency scheme identifies the D-locators based on the consistency check of the estimation result, the most inconsistent locator will be considered as a D-locator. We define the secure localization as successful when  $d_{err1} \leq d_{err2} + f_{tol} * R$ , where  $d_{err1}$  (and  $d_{err2}$ ) denotes the localization error with (and without) using the secure localization scheme,  $f_{tol}$  is the factor of localization error tolerance (0.1 in our simulations). The performance of the scheme without any detection process shows the impact of the wormhole attack on the localization process. It is obvious that our proposed scheme provides much better performance than the other schemes. The simulation shows that our proposed scheme obtains the performance with a probability higher than 95% when  $L/R < 2.5$  and a probability very close to 100% when  $L/R \geq 2.5$ .

Fig. 7 demonstrates the effects of distance measurement error on the performance of our proposed scheme. It shows that when the standard deviation  $\sigma = 0.5$  of the distance measurement error (that is, the error ranges in  $[-1.5, 1.5]m$  with a probability larger than 99%), the proposed scheme obtains the best performance. As the standard deviation  $\sigma$  gets larger, the performance becomes worse. However, even when  $\sigma = 1.5$ , the probability of successful localization is also not smaller than 98%, indicating that our proposed scheme works well even when great distance measurement error exists.

In Fig. 8, the effects of locator density on the performance of our proposed scheme is 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 6), our proposed scheme achieves a performance with the probability equals to 100%.

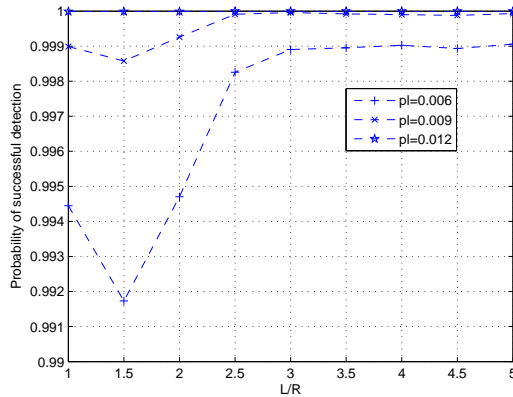


Fig. 8. Effects of locator density on secure localization performance.

## 5 Concluding Remarks

In this paper, we analyze the impact of the wormhole attack on the range-based localization. Based on the analysis, we propose a secure localization mechanism which is wormhole attack resistant by using the wormhole attack detection and dubious locators identification. We also present the simulation results to demonstrate that our proposed scheme outperforms other existing schemes. In this paper, we only consider the scenario where the network has no packet loss when two nodes exchange messages with each other. This requirement can be supported by using acknowledgements for the successful packets and retransmission for the lost packets. Moreover, the proposed scheme is described based on the TDoA ranging method, but it can be easily applied to the localization approach with the radio signal strength indicator (RSSI) method as well. In the future, our work will focus on the secure localization when the sensor is under multiple wormholes' attack simultaneously.

## References

1. Hu, Y.C., Perrig, A., Johnson, D.B.: Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks. In: Proc. of IEEE INFOCOM. (2003)
2. Zhao, M., Servetto, S.D.: An Analysis of the Maximum Likelihood Estimator for Localization Problems. In: Proc. of the 2nd Int'l Conf. on Broadband Networks. (2005)
3. Savvides, A., Han, C., Srivastava, M.: Dynamic Fine-Grained Localization in Ad-hoc Networks of Sensors. In: Proc. of ACM MOBICOM. (2001)
4. Mao, G., Fidan, B., Anderson, B.D.O.: Wireless Sensor Network Localization Techniques. *Computer and Telecommunications Networking* (2007) 2529–2553
5. Boukerche, A., Oliveira, H.A.B.F., Nakamura, E.F., Loureiro, A.A.F.: Secure Localization Algorithms for Wireless Sensor Networks. *IEEE Communications Magazine* (2008)
6. Liu, D., Ning, P., Du, W.: Attack-Resistant Location Estimation in Sensor Networks. In: Proc. of IEEE IPSN. (2005)
7. Capkun, S., Hubaux, J.P.: Secure Positioning of Wireless Devices with Application to Sensor Networks. In: Proc. of IEEE INFOCOM. (2005)

8. Capkun, S., Cagalj, M., Srivastava, M.: Secure Localization With Hidden and Mobile Base Stations. In: Proc. of IEEE INFOCOM. (2006)
9. Lazos, L., Poovendran, R., Capkun, S.: ROPE: Robust Position Estimation in Wireless Sensor Networks. In: Proc. of IEEE IPSN. (2005)
10. Srinivasan, A., Teitelbaum, J., Wu, J.: DRBTS: Distributed Reputation-based Beacon Trust System. In: Proc. of the 2nd IEEE Int'l Symposium on Dependable, Autonomic and Secure Computing. (2006)
11. Liu, D., Ning, P., Du, W.: Detecting Malicious Beacon Nodes for Secure Localization Discovery in Wireless Sensor Networks. In: Proc. of IEEE ICDCS. (2005)
12. Khabbaziyan, M., Mercier, H., Bhargava, V.K.: Wormhole Attack in Wireless Ad Hoc Networks: Analysis and Countermeasure. In: Proc. of IEEE GLOBECOM. (2006)
13. Wang, W., Bhargava, B.: Visualization of Wormholes in Sensor Networks. In: Proc. of ACM WiSe. (2004)
14. Wang, W., Lu, A.: Interactive wormhole detection and evaluation. *Information Visualization* **6** (2007) 3–17
15. Xu, Y., Chen, G., Ford, J., Makedon, F.: Detecting Wormhole Attacks in Wireless Sensor Networks. In: Proc. of IFIP. (2008)
16. Maheshwari, R., Gao, J., Das, S.R.: Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information. In: Proc. of IEEE INFOCOM. (2007)
17. Lazos, L., Poovendran, R.: SeRLoc: Robust Localization for Wireless Sensor Networks. *ACM Transactions on Sensor Networks* (2005) 73–100
18. Lazos, L., Poovendran, R.: HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks. *IEEE Journal on Selected Areas in Communications* **24** (2006) 233–246
19. Chen, H., Lou, W., Ma, J., Wang, Z.: TSCD: A Novel Secure Localization Approach for Wireless Sensor Networks. In: Proc. of The Second Int'l Conf. on Sensor Technologies and Applications. (2008)