Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2010, Article ID 981280, 12 pages
doi:10.1155/2010/981280

Research Article

A Novel Secure Localization Approach in Wireless Sensor Networks

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

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

Correspondence should be addressed to Honglong Chen, honglongchen1984@gmail.com

Received 11 February 2010; Revised 14 June 2010; Accepted 3 November 2010

Academic Editor: Xiang-Yang Li

Recent advances in wireless networking technologies, along with ubiquitous sensing and computing, have brought significant convenience for location-based services. The localization issue in wireless sensor networks under the nonadversarial scenario has already been well studied. However, most existing localization schemes cannot provide satisfied performance under the adversarial scenario. In this paper, we propose three attack-resistant localization schemes, called basic TSCD, enhanced TSCD and mobility-aided TSCD secure localization schemes, respectively, to stand against the distance-consistent spoofing attack in wireless sensor networks. The idea behind the basic TSCD scheme is to adopt the temporal and spatial properties of locators to detect some attacked locators firstly and then utilize the consistent property of the detected attacked locators to identify other attacked locators. Enhanced TSCD and mobility-aided TSCD schemes are designed based on the basic TSCD scheme to improve the performance. Simulation results demonstrate that our proposed schemes outperform other existing approaches under the same network parameters.

1. Introduction

Wireless sensor networks (WSNs) [1] have increasingly drawn attentions of researchers in the areas of wireless communication, sensor technology, distributed systems, and embedded computing. These sensor networks consist of a large number of low-cost, low-power, and multifunctional sensor nodes that communicate through wireless media. Various WSN applications have been proposed, for example, military target tracking, environment monitoring, medical treatment, emergency rescue and smart home, and so forth. A fundamental requirement in the above applications is the location awareness of the system. Therefore, the acquisition of sensors' location becomes an important issue since sensing results without location information are mostly inapplicable. Considering the nature of random deployment of most sensor networks, it is laborious, if not impossible, to predetermine the location of each sensor node before deployment. A common approach in most localization schemes is to use enough special nodes, called *locators* or *beacons*, which can obtain their locations by GPS or from infrastructure. Locations of normal sensor nodes are then estimated by interacting with locators to obtain the distance or angle information. Once the location information of at least three noncollinear locators are available, the relative positions of the sensors can be converted into physical positions.

Energy efficiency, accuracy and security account for the major metrics in localization systems. The former two metrics have already been investigated for nearly a decade and a large amount of achievements [2–4] have been published. The security, however, has been addressed only in recent years. In practice, localization schemes in WSNs may work under the adversarial scenario where malicious attacks exist. For example, a simple replay attack [5] can modify the distance measurement, leading to the malfunction of the localization schemes. Therefore, it is necessary to design a secure localization scheme which can be competent in the hostile environment.

There are many different kinds of attackers in the hostile wireless sensor networks. Generally, these attackers

can be classified into two categories, *external* attackers and *internal* attackers [6]. External attackers can distort the network behavior without the system's authentication, while internal attackers are authenticated ones, and thus, more dangerous to the system security. Most attacks in WSNs are coming from the aforementioned two types of attackers. For instance, the wormhole attack [7] is conducted by two colluding external attackers, and the false position and distance dissemination attack [8] is accomplished by an internal attacker.

In range-based localization procedure, the internal attackers can revise the measured distances randomly to disrupt the localization. This kind of attack can be defended using the consistency check method proposed in [9]. However, if the attackers do not revise the measured distances randomly, but make the modified distances be consistent, which is called the *distance-consistent spoofing attack*, the strategy proposed in [9] will be failed under this scenario. In this paper, the distance-consistent spoofing attack in WSNs is therefore investigated, based on which we propose an attack-resistant localization scheme, called basic TSCD (Temporal Spatial Consistent based Detection) secure localization. By further exploring the consistency and the mobility properties of the sensor, enhanced TSCD and mobility-aided TSCD schemes are proposed, respectively, to improve the localization performance. Simulation results demonstrate that our proposed schemes achieve better performance than existing approaches under the same network settings.

The main contributions of this paper are summarized as follows.

(i) We address a new distance-consistent spoofing attack which can easily attack the localization in WSNs,

(ii) We summarize four secure properties of a WSN when it is under the distance-consistent spoofing attack,

(iii) We propose three secure localization schemes, which make use of these properties to detect and defend against the distance-consistent spoofing attack,

(iv) We conduct theoretical analysis on the probability of identifying all the attacked locators, which is validated by simulations,

(v) We analyze the effects of network parameters on the performance of our proposed schemes and compare them with other existing methods.

The remainder of this paper is organized as follows. In Section 2, we provide the related work on secure localization. Section 3 gives the problem statement and Section 4 summarizes four secure properties of wireless communication in WSNs. In Section 5, the basic TSCD, enhanced TSCD, and mobility-aided TSCD schemes are proposed as well as the theoretical analysis. Section 6 presents the performance evaluation and Section 7 concludes the paper and puts forward our future work.

2. Related Work

There have been some recent achievements [5] on secure localization. In [10], message authentication is used to prevent wholesale beacon location report forgeries, and a location reporting algorithm is proposed to minimize the impact of compromised beacons. Lazos et al. propose a robust positioning system called ROPE [11] that allows sensors to determine their locations without centralized computation. In addition, ROPE provides a location verification mechanism that verifies the location claims of the sensors before data collection. DRBTS [12] 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 then enables them to decide which should be trusted.

To provide secure location services, Liu et al. [13] introduce a suit of techniques to detect malicious beacons that supply incorrect information to sensor nodes. These techniques include a method to detect malicious beacon signals, techniques to detect replayed beacon signals, the identification of malicious beacons, the avoidance of false detections, and the revoking of malicious beacons. By clustering of benign location reference beacons, Wang et al. [14] propose a resilient localization scheme that is computational efficiency. In [15], robust statistical methods are proposed, including triangulation and RF-based fingerprinting, to make localization attack-tolerant. SPINE [8] is a range-based positioning system that enables verifiable multilateration and verification of positions of mobile devices for secure computation in the presence of attackers. In [16], a secure localization scheme is presented to make the location estimation of the sensor secure, by transmission of nonces at different power levels from the beacon nodes. In [17], Chen et al. propose to make each locator build a conflicting-set and then the sensor can use all conflicting sets of its neighboring locators to filter out incorrect distance measurements of its neighboring locators. The limitation of the scheme is that it only works properly when the system has no packet loss. As the attackers may drop the packets purposely, the packet loss is inevitable when the system is under a wormhole attack. The distance-consistency-based secure localization scheme proposed in [18, 19] can also tolerate the packet loss.

By localizing the sensor node with directional antennae equipped on locators, SeRLoc [20] is robust against wormhole attacks, sybil attacks and sensor compromises. On the basis of SeRLoc, HiRLoc [21] further utilizes antenna rotations and multiple transmit power levels to provide richer information for higher localization resolution. Liu et al. [9] propose two secure localization schemes. The first one is attack-resistant Minimum Mean Square Estimation, which filters out malicious beacon signals by the consistency check. The other one is voting-based location estimation. However, SeRLoc requires directional antennae which are complex in real deployment. The schemes in [9] would fail under the distance-consistent spoofing attack when the attacked location references are malicious colluding ones, that is, consistent. The TSCD secure localization scheme, proposed in this paper, is able to conquer both the two drawbacks. It does not require any complex hardware, and works well even when the revised distance measurements of the attacked locators are consistent. In addition, it consumes

less computation time than that of [9] while obtaining better performance.

3. Problem Statement

In this section, the network model and related assumptions as well as the localization approach are given, followed by the attack model which we focus on.

3.1. Network Model. We assume that there are three types of nodes in a WSN, namely locators, sensors, and attackers, respectively. The locators are location-fixed nodes which know their coordinates after deployment. The sensors, while continuously moving around the network, estimate their own locations by measuring distances to neighboring locators. Each sensor and locator has its own unique identification and they also share a hash function which is used for the verification (we will describe it in next subsection). The attackers, known as adversarial nodes, intentionally disturb the localization procedure of the sensors. A pair of attackers can collude to spoof a sensor in the network. We assume that all the nodes in the network have the same transmission range R. However, the communication range between two colluded attackers is unlimited as they can communicate with each other using certain communication technique.

We also assume that the locators are deployed independently with a density of ρ_l, and the probability that a sensor hears k locators follows the Poisson distribution: $P(L_S = k) = ((\pi R^2 \rho_l)^k / k!) e^{-\pi R^2 \rho_l}$. Each locator is able to measure the distances to neighboring sensors. The measurement error follows a Gaussian distribution $N(\mu, \sigma^2)$, where the mean μ is 0 and the standard deviation σ is within a threshold. The attackers also measure the distances to neighboring locators and send the distance measurements to its colluder—another attacker—to replay the measurements to a sensor in another region, thus providing faulty measurements.

3.2. Localization Approach. As a sensor always moves around in the network, it continuously changes its locations. Whenever needed, the sensor can rely on the localization procedure to determine its current position. The localization procedure is as follows. The sensor maneuvers in the region, stops and broadcasts a requesting signal *Loc_request* including its local timestamp t_s to its neighboring locators whenever it needs localization. Upon receiving the *Loc_request* signal, each locator, within the communication range of the sensor, estimates the distances to the sensor based on the *Loc_request* signal (e.g., TDoA [3] or RSSI [22]). Then each locator replies a *Loc_ack* signal to the sensor which includes its ID, the measured distance and $H(t_s)$, here $H(\cdot)$ denotes the hash function shared by the nodes in the network. When receiving the *Loc_ack* signal from its neighboring locator, the sensor will check whether the $H(t_s)$ in *Loc_ack* is valid by comparing it with its own generated hash number $H(t_s)$. The sensor will only accept the verified *Loc_ack* signal.

The sensor also measures the response time of each locator during the above process to eliminate the random delay at the MAC layer of the locators. Once enough distance measurements obtained, the sensor starts location estimation using the maximum likelihood estimation (MLE) method [23]: Assume that the coordinates of the n neighboring locators of the sensor are $(x_1, y_1), (x_2, y_2), (x_3, y_3), \ldots, (x_n, y_n)$, respectively, and the distance measurements from the n locators to the sensor are $d_1, d_2, d_3, \ldots, d_n$. Then the location of the sensor, denoted as $X = \begin{bmatrix} x \\ y \end{bmatrix}$, can be obtained by

$$X = \left(A^T A\right)^{-1} A^T b, \tag{1}$$

where

$$A = \begin{bmatrix} 2(x_1 - x_n) & 2(y_1 - y_n) \\ 2(x_2 - x_n) & 2(y_2 - y_n) \\ \vdots & \vdots \\ 2(x_{n-1} - x_n) & 2(y_{n-1} - y_n) \end{bmatrix},$$
$$b = \begin{bmatrix} x_1^2 - x_n^2 + y_1^2 - y_n^2 - d_1^2 + d_n^2 \\ x_2^2 - x_n^2 + y_2^2 - y_n^2 - d_2^2 + d_n^2 \\ \vdots \\ x_{n-1}^2 - x_n^2 + y_{n-1}^2 - y_n^2 - d_{n-1}^2 + d_n^2 \end{bmatrix}. \tag{2}$$

3.3. Attack Model. In this paper, we consider an adversarial WSN where a pair of colluding attackers can launch a so-called *distance-consistent spoofing attack*. In [9], the attacker can only revise the distance measurement randomly to disrupt the localization procedure. The distance consistency check proposed in [9] claimed that all distance measurements from neighboring locators to a sensor are consistent, that is, these distance measurements can converge to an identical location. Therefore, this distance consistency check scheme can be used to resist such kind of attack effectively because the malicious distance measurements generated by attacker will be inconsistent. In the distance-consistent spoofing attack, to increase their capacity of localization disrupting, the colluding attackers can deliberately revise the distance measurement messages sent from all the attacked locators and make the revised distance measurements fake a virtual location, which makes the distance consistency check scheme lose its efficacy. Note that the attackers in this paper belong to the internal attackers, which can revise the message content in the network, but they are not able to compromise any node in the network which requires more resource for the attackers. For example, the attackers cannot obtain the hash function $H(\cdot)$ shared by the nodes. Therefore, they cannot generate fake messages for nonexisted locators due to the verification procedure with $H(t_s)$.

An example of the distance-consistent spooking attack is shown in Figure 1(a). As two colluding attackers A_1 and A_2 can communicate with each other via an *attack link*, locators L_4, L_5 and L_6 can, therefore, communicate with the sensor S through the attack link. For L_6, the *Loc_request* signal sent from S travels through the attack link to reach L_6, and L_6 responds a *Loc_ack* signal. Attacker A_1 measures the distance

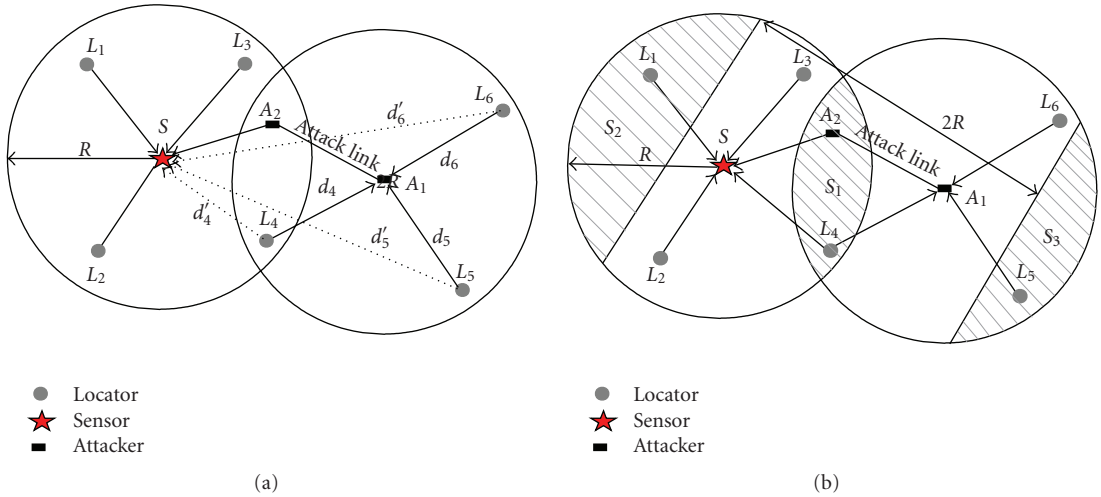

Figure 1: The attack scenarios in WSN. (a) Attacker model in range-based localization; (b) Attacked locators with temporal and spatial properties.

to L_6 as d_6 after receiving the *Loc_ack* signal. A_1 forwards the *Loc_ack* signal with the distance measurement information to A_2 through the attack link. A_2 modifies the distance measurement information in the *Loc_ack* signal to make it consistent with others. For example, when A_2 received the message sent from L_6 to S, if A_2 modifies the distance measurement information in the message to be d_6 and relays the message to S, S will consider the distance to L_6 as d_6 instead of the actual distance d'_6. Similarly, S considers the distances to L_4 and L_5 as d_4 and d_5, respectively, instead of the actual distances d'_4 and d'_5. Consequently, the revised distance measurements d_4, d_5 and d_6 will be consistent, and they can converge to an identical location, that is, the point of A_1 in Figure 1(a).

4. Secure Properties and Corresponding Detection Schemes

In this section, we summarize the characteristics of a WSN as four secure properties when it is under a distance-consistent spoofing attack: the temporal property of the locators, the spatial property of the locators, the consistent property of the legitimate locators, and the consistent property of the attacked locators. The detection schemes are therefore proposed based on the corresponding properties. Though the detection schemes based on the temporal and spatial properties have been used in [20] and the detection scheme based on the consistent property of legitimate locators has been used in [9], we jointly use these properties to defend against the distance-consistent spoofing attack.

4.1. Temporal Property and Corresponding Detection Scheme

4.1.1. Temporal Property. The sensor can receive at most one message from the same locator for each localization procedure. That is, if the sensor receives more than one signals from a locator, this locator is attacked.

4.1.2. Detection Scheme D1 Based on Temporal Property. As shown in Figure 1(b), suppose an attacked locator lies in the shading domain S_1, which is the common transmission area of sensor S and attacker A_1. When S broadcasts the *Loc_request* signal, L_4 can hear it twice, one directly from S, and the other from A_1 which is replayed by A_2 to A_1 through the attack link. L_4 will also reply the *Loc_ack* signal through these two pathes. Therefore, S will receive more than one messages from L_4, based on which S can determine that L_4 is attacked.

The sensor S can also differentiate the correct distance message from the incorrect one based on the following scheme: As the localization approach only countervails the time delay at the MAC layer of the locators when measuring the response time of the message, if the message goes through the attack link, the MAC layer delay introduced by the two attackers still exists. Therefore, the response time of the revised *Loc_ack* signal from L_4 to S, which travels through the attack link, will be longer than that of the original *Loc_ack* signal which travels from L_4 to S directly. S will consider the *Loc_ack* signal with a shorter response time from a locator to be correct while treating the other as attacked.

4.2. Spatial Property and Corresponding Detection Scheme

4.2.1. Spatial Property. The sensor cannot receive messages from two different locators for each localization procedure if the distance between these two locators are larger than $2R$. That is, if the sensor has received messages from two locators whose distance between each other is larger than $2R$, one of these two locators is attacked.

4.2.2. Detection Scheme D2 Based on Spatial Property. When an attacked locator lies farther than $2R$ away from one of the legitimate locators, the sensor can detect it based on the spatial property. As shown in Figure 1(b), L_5 is an attacked locator which lies farther than $2R$ away from L_1. S can detect

that one of the two locators is attacked. To differentiate the attacked locator from these two locators, observing that the MAC layer delay introduced by the attackers will increase the response time of the *Loc_ack* signal sent from the attacked locator, the response time of the message from the attacked locator will be longer than the one from the legitimate locator. Therefore, by comparing the response time of the two locators, S can further determine that the locator with a longer response time is the attacked one, which is L_5 in this case.

4.3. Consistent Property of Legitimate Locators and Corresponding Detection Scheme

4.3.1. Consistent Property of Legitimate Locators. Assume that the coordinates of the n locators are (x_1, y_1), $(x_2, y_2), (x_3, y_3), \ldots, (x_n, y_n)$, and the distance measurements from the n locators to the sensor are $d_1, d_2, d_3, \ldots, d_n$. The estimated location of the sensor is $(\tilde{x}, \tilde{y})$. The mean square error of the estimated location $\delta^2 = \sum_{i=1}^{n}((d_i - \sqrt{(\tilde{x} - x_i)^2 + (\tilde{y} - y_i)^2})^2/n)$. The consistent property of legitimate locators means that the mean square error of the location estimation, generated from legitimate distance measurements, is lower than that containing malicious distance measurements.

4.3.2. Detection Scheme D3 Based on Consistent Property of Legitimate Locators. To detect the attacked locators, a predefined threshold of the mean square error, τ^2, has to be determined in advance. The sensor estimates its location based on distance measurements to all its neighboring locators, and determines whether the mean square error based on the estimation result is lower than the threshold. If yes, the estimated result will be considered as correct; otherwise, it calculates its location repeatedly using all possible subsets of these locators with one fewer locator, and chooses the subset with the least mean square error to eliminate the locator which is out of the subset. The sensor repeats the above process until the mean square error is lower than the threshold or there are only 3 locators left. Note that this scheme works only when the majority of locators are legitimate.

4.4. Consistent Property of Attacked Locators and Corresponding Detection Scheme

4.4.1. Consistent Property of Attacked Locators. The distance-consistent spoofing attack can make the sensor measure the distances to the attacked locators consistent to a fake location. That is, the location estimation based on the attacked locators has a low mean square error.

4.4.2. Detection Scheme D4 Based on Consistent Property of Attacked Locators. If the sensor has already detected two or more attacked locators, it can identify other attacked locators using the consistent property of attacked locators. Let L_{ts} denote the set of attacked locators that have been detected and L_r denote the set of remaining locators. The sensor repeats to select one locator L_i from L_r each time and calculates the mean square error based on $L_{ts} \cup \{L_i\}$. If the mean square error is lower than the threshold τ^2, L_i is considered as an attacked one; otherwise, L_i is considered as a legitimate one. The sensor repeats this until all locators in L_r have been checked.

5. TSCD Secure Localization Schemes

In this section, we propose three novel schemes that apply the properties described in the previous section. We first propose a secure localization scheme, namely basic TSCD (B-TSCD), which applies the temporal property, spatial property, and consistent property of attacked locators. Based on B-TSCD, we also propose an enhanced TSCD (E-TSCD) scheme which further applies the consistent property of legitimate locators. Another extended scheme, called mobility-aided TSCD (M-TSCD), is further designed to improve the overall performance. At the end, we analyze the theoretical probability of identifying all the attacked locators and the computational complexity of these schemes.

5.1. Basic TSCD Secure Localization. As mentioned above, the idea behind the B-TSCD scheme is to apply the temporal property, spatial property, and consistent property of attacked locators to detect all attacked locators. The sensor first applies both temporal and spatial properties to detect some attacked locators. If two or more attacked locators are successfully detected, the sensor can identify other attacked locators based on their consistency. After attacked locators are removed, the sensor can conduct the localization based on the remaining locators.

The procedure of B-TSCD is listed in Algorithm 1. When the sensor requires the location estimation, it broadcasts the *Loc_request* message to the network, and waits for the *Loc_ack* messages from neighboring locators. If it receives *Loc_ack* messages from the same locator more than once, it uses the detection scheme D1 to distinguish the correct distance measurement and the spoofing distance measurement. Meanwhile, when it receives *Loc_ack* signals from neighboring locators, it checks whether there are two locators whose distance between each other is larger than $2R$. If yes, it uses the detection scheme D2 to identify the legitimate locator and the attacked one. If the sensor has successfully detected at least two attacked locators, it further uses the detection scheme D4 to detect all other locators. When all neighboring locators are checked, the sensor conducts the MLE localization based on the remaining locators.

5.2. Enhanced TSCD Secure Localization. In the B-TSCD scheme, if the sensor fails to detect at least two attacked locators based on the detection schemes D1 and D2, it cannot use the detection scheme D4. It then conducts the localization using the remaining locators. However, there may still exist some attacked locators undetected, leading to the deterioration of the localization. The enhanced TSCD secure localization (E-TSCD) scheme is based on

(1) Broadcast the *Loc_request* message.
(2) Wait for the *Loc_ack* message, conduct the distance estimation and calculate the response time of each locator.
(3) Use the detection schemes D1 and D2 to detect attacked locators.
(4) **if** the detected attacked locators ≥ 2 **then**
(5) Use the detection scheme D4 to detect other attacked locators.
(6) **end if**
(7) Conduct the MLE localization based on the remaining locators.

Algorithm 1: Basic TSCD secure localization scheme.

the observation that if the sensor cannot use the detection schemes D1 and D2 to detect two attacked locators, the sensor most likely has more legitimate neighboring locators than undetected attacked ones. Therefore, if the sensor has detected fewer than two attacked locators, it can further use the detection scheme D3 to detect other attacked ones.

The procedure of the E-TSCD is shown in Algorithm 2. The sensor firstly uses the schemes D1 and D2 to detect attacked locators. If the number of detected attacked locators is over two, the detection scheme D4 is used to detect other attacked locators; otherwise, the sensor uses the detection scheme D3 to eliminate other attacked locators. At the end, the MLE localization based on the remaining locators is used to obtain the location result. Note that we do not use those attacked locators detected from the detection scheme D3 as a priori for conducting the detection scheme D4. Those locators are considered "attacked" because they are beyond the distance consistency threshold. However, these excesses might be not due to the attack, but other reasons, such as the measurement error.

5.3. Mobility-Aided TSCD Secure Localization. As the sensor moves around, it may need to conduct the localization process continuously because its location continues changing. We assume that a sensor periodically conducts the localization process and marks itself a state after the localization. The sensor marks itself with an attacked state if it detects any attacked locator; otherwise, it marks itself with a safe state. Thus, there will be four possible state transitions for the two consecutive states of a sensor, which is shown in Figure 2: (1) from previous safe state to current safe state; (2) from previous safe state to current attacked state; (3) from previous attacked state to current safe state; and (4) from previous attacked state to current attacked state. Although the historical data obtained from the previous secure localization process may not be useful in the former three state transitions, it can be used in the last state transition to assist the sensor to detect the current attacked locators.

We propose an extended secure localization scheme, called mobility-aided TSCD (M-TSCD), which allows a sensor to utilize its historical data to detect the current attacked locators. For the sensor, if it detects some attacked locators based on the temporal and spatial properties, it knows that it is currently in an attacked state. Then, it checks its historical data and treats all those detected attacked locators in the previous state as the attacked locators in the current state. It also records the current detected attacked locators as the historical data for the next state. Otherwise, if it detects no attacked locator, it empties the historical data. Since the attacked locators recorded in the historical data for the previous state are also considered attacked on the current state, it increases the probability that a sensor detects at least two attacked locators. If the detected attacked locators are more than two, the sensor can use the detection scheme D4 to detect other attacked locators; otherwise, it uses the detection scheme D3 to detect other attacked locators. Finally, it conducts the MLE localization based on the remaining locators. The procedure of M-TSCD is shown in Algorithm 3.

Note that there is a precondition for the M-TSCD scheme, which assumes that the distance between two consecutive localization processes is relatively short so that when a distance-consistent spoofing attack occurs on the current state it is impossible for another different distance-consistent spoofing attack to occur on the previous state or the next state. In other words, if the sensor is attacked on both the previous state and current state, these two attacks come from the same attack source and they attack the same group of locators. This precondition makes sense when the density of the attack sources is low and the behavior of the attack sources does not change dramatically.

5.4. Probability of Identifying All Attacked Locators. To analyze the probability of identifying all the attacked locators for the B-TSCD scheme, we assume for simplicity that the sensor can achieve this goal if it can detect at least two attacked locators. We denote the disk with center U and radius R as $\mathcal{D}_R(U)$. As illustrated in Figure 3, the overlapped region of the transmission areas of the sensor S and attacker A_1 is denoted as S_1.

As shown in Figure 3, when the sensor is under the distance-consistent spoofing attack, the probability that it lies in the region $dxdy$ equals to $dx\,dy/\pi R^2$. Assuming that the sensor can identify m attacked locators using the detection scheme D1 and identify n attacked locators using the detection scheme D2, the probability that the sensor can identify at least two attacked locators using schemes D1 and D2 can be calculated as

$$P_{xy} = 1 - P(m=0)P(n=0) - P(m=0)P(n=1) - P(m=1)P(n=0), \tag{3}$$

(1) Broadcast the *Loc_request* message.
(2) Wait for the *Loc_ack* message, conduct the distance estimation and calculate the response time of each locator.
(3) Use the detection schemes D1 and D2 to detect attacked locators.
(4) **if** the detected attacked locators ≥ 2 **then**
(5) Use the detection scheme D4 to detect other attacked locators.
(6) **else**
(7) Use the detection scheme D3 to detect other attacked locators.
(8) **end if**
(9) Conduct the MLE localization based on the remaining locators.

Algorithm 2: Enhanced TSCD secure localization scheme.

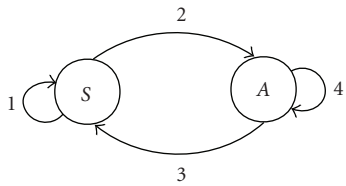

Figure 2: State transitions of the sensor in a WSN under the distance-consistent spoofing attack. S and A denote the safe state and attacked state, respectively.

where

$$\begin{aligned} P(m=0) &= e^{-S_1\rho_l}, \\ P(m=1) &= S_1\rho_l e^{-S_1\rho_l}, \\ P(n=0) &= e^{-S_2\rho_l}, \\ P(n=1) &= S_2\rho_l e^{-S_2\rho_l}. \end{aligned} \tag{4}$$

Here, S_2 is the region in $\mathcal{D}_R(A_1)$ which is more than $2R$ away from at least one of the locators in $\mathcal{D}_R(S)$, that is, the area of the corresponding shadow region S_2 in Figure 3. Note that all the locators in $\mathcal{D}_R(A_1)$ are attacked by the distance-consistent spoofing attack, and if any locator lies in S_2, the sensor can identify it as an attacked locator using the detection scheme D4.

Thus, we can obtain

$$P = \frac{1}{\pi R^2} \iint_{\mathcal{D}_R(A_2)\setminus S_1} P_{xy}\, dx\, dy, \tag{5}$$

where

$$\begin{aligned} P_{xy} &= 1 - e^{-(S_1+S_2)\rho_l}\left[1 + (S_1+S_2)\rho_l\right], \\ S_1 &= 2R^2 \arccos\frac{L}{2R} - L\sqrt{\left(R^2 - \frac{L^2}{4}\right)}. \end{aligned} \tag{6}$$

L is the distance between S and A_1 as shown in Figure 3.

For the E-TSCD and M-TSCD schemes, the probability of identifying all the attacked locators cannot be explicitly represented as a mathematical formula. However, the probability P obtained from the B-TSCD scheme can be considered as the lower bound of that probability for these two schemes.

6. Simulation Evaluation

In this section, we evaluate the performance of our proposed schemes in terms of the probability of successful localization and time consumption. The localization is considered successful if the distance difference between the estimated position and the real position of the sensor is less than a threshold. Because of the existence of the distance measurement error, the sensor's position estimated by the localization algorithm cannot be the same as its real position even there has no attack at all. When the attack exists, the sensor's estimated position may be further deviated. Therefore, we consider the localization of the sensor to be successful under the attack if the distance between the estimated position without the attack and the real position, say d_1, and the distance between the estimated position with the attack detection and the real position, say d_2, satisfy the condition $d_2 \leq 2d_1$. That is, the localization is considered successful if the impact of the attack on the localization is bounded by the double of the distance measurement error. We also interest in the time consumption cost of the proposed algorithms considering the energy-constrained nature of sensor nodes. As the communication cost is similar among different algorithms, the difference of time consumption cost indicates the effectiveness of these algorithms.

We adopt the following parameters in our simulation: the transmission range $R = 15$ m; the density of locators $\rho_l = 0.006/\text{m}^2$ (with the average degree of the network equals to 4.24); the standard deviation of the distance measurement error $\sigma = 0.5$; the threshold of the mean square error used in the consistent property is 1. The label L/R of the x axis denotes the ratio of the distance L between the sensor S and the attacker A_1 to the transmission range R.

Figure 4 shows the performance comparison of the following schemes: the scheme using only the temporal and spatial properties (TSD), the scheme using the consistency property of legitimate locators (CD) [9], B-TSCD, E-TSCD and M-TSCD. For the M-TSCD scheme, we assume that the sensor conducts the localization periodically and we denote the distance for two consecutive localization processes as the length of one step. We can see that all TSCD schemes yield much better performance than the other two schemes, especially when L/R is less than 2. Among these TSCD

(1) Broadcast the *Loc_request* message.
(2) Wait for the *Loc_ack* message, conduct the distance estimation and calculate the response time of each locator.
(3) Use the detection schemes D1 and D2 to detect attacked locators.
(4) **if** the attacked locators are detected **then**
(5) Treat previous detected attacked locators as current detected attacked locators.
(6) Update the historical data with current detected attacked locators.
(7) **else**
(8) Empty the historical data.
(9) **end if**
(10) **if** the current detected attacked locators ≥ 2 **then**
(11) Use the detection scheme D4 to detect other attacked locators.
(12) **else**
(13) Use the detection scheme D3 to detect other attacked locators.
(14) **end if**
(15) Conduct the MLE localization based on the remaining locators.

Algorithm 3: Mobility-aided TSCD secure localization scheme.

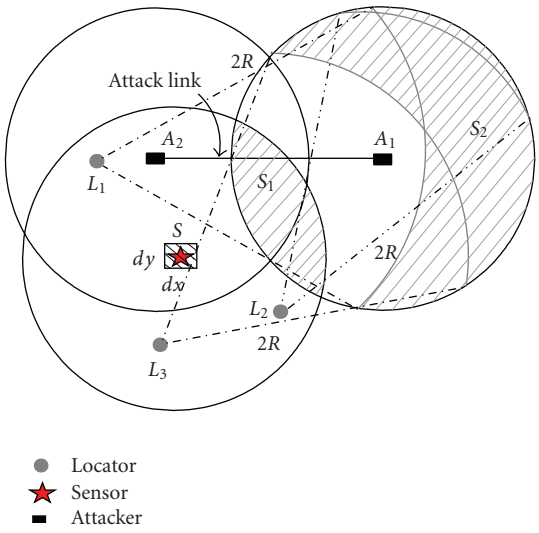

Figure 3: Theoretical analysis of the mathematical probability under the distance-consistent spoofing attack.

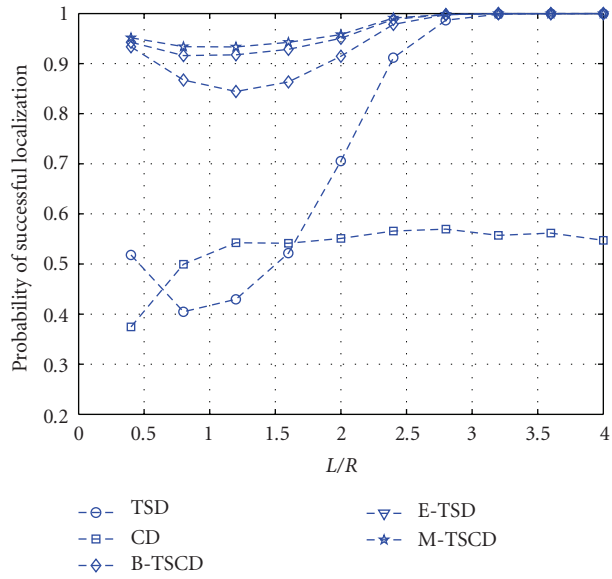

Figure 4: Performance of existing schemes and our schemes (the step length is 0.25R for the mobility-aided TSCD scheme).

schemes, E-TSCD achieves an improvement over B-TSCD, and M-TSCD outperforms E-TSCD.

As the signals from attacked locators always come later than that from legitimate ones, an intuitive approach, referred to as first-three-locators scheme, is to only take the first-three-signals from neighboring locators into account for the sensor's localization. However, due to the existence of distance measurement errors, the first-three-locators scheme will deteriorate the localization accuracy remarkably. The reason is that it takes no account of the remaining legitimate locators when there exist more than three legitimate locators. Figure 5 shows the performance comparison of the first-three-locators scheme and the B-TSCD scheme at different densities of locators. The simulation result shows that the B-TSCD scheme outperforms the first-three-locators scheme dramatically for all densities of locators.

The effects of ρ_l on the performance of B-TSCD and E-TSCD are shown in Figures 6(a) and 6(b), respectively. From both figures, we can see that as the ρ_l increases, the probability of successful localization also increases. This is mainly because the increase of ρ_l enlarges the probability of detecting at least two attacked locators by the temporal and spatial properties. However, when ρ_l is large enough, the improvement of increasing ρ_l is insignificant. The performance of B-TSCD, when ρ_l is large, is similar to that of E-TSCD. Therefore, A tradeoff can be made between hardware deployment (applying B-TSCD when ρ_l is large) and computation capability (applying E-TSCD).

The effect of the step length on the performance of M-TSCD is shown in Figure 7, compared to the E-TSCD scheme. It can be observed that M-TSCD with different

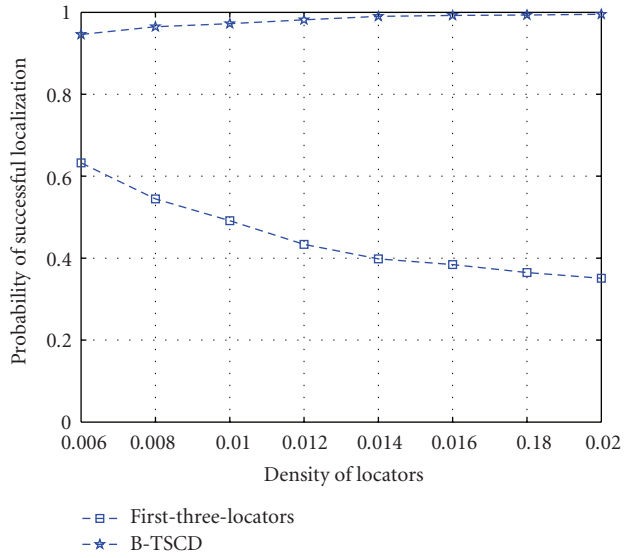

Figure 5: Performance of the first-three-locators scheme and the B-TSCD scheme.

step lengths all outperform E-TSCD. For M-TSCD, the performance is increased when the step length increases. However, as the step length increases, the probability that the historical data are valid also gets lower. To get the best performance, a tradeoff of the step length should also be taken into account.

Figure 8 validates the correctness of the theoretical analysis of the probability of successfully identifying all attacked locators. The maximum difference between the simulation and the mathematical result is about 3%, showing that the theoretical analysis matches the simulation result quite well.

To study the time consumption of each scheme, we conducted 20,000 times self-localization in a simulation program running on a PC with Pentium 2.4 G CPU. Figure 9 shows the time consumed by TSD, CD, B-TSCD, E-TSCD, and M-TSCD, respectively. Apparently, TSD scheme is the most timesaving and CD scheme consumes the most time since the detection scheme D3 is the most time-consuming scheme. As E-TSCD uses the detection scheme D3 when fewer than two attacked locators are detected by the detection schemes D1 and D2, it requires more time than B-TSCD. Compared to E-TSCD, M-TSCD increases the probability of detecting at least two attacked locators, which lowers the probability to use the detection scheme D3. Therefore, M-TSCD always consumes less time than E-TSCD, and does less than B-TSCD when L/R is over 1.5. When the L/R is over 2.5, M-TSCD is even comparable to TSD.

Figures 10, 11, and 12 show the effects of the packet loss on the performance of B-TSCD, E-TSCD and M-TSCD secure localization schemes, respectively. For the packet loss, we assume that 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 $(d - \alpha R)/(R - \alpha R)$, where $0 \leq \alpha \leq 1$. From Figures 10, 11, and 12, we can find that when increasing the packet loss ratio (reducing α), the secure localization performance of our proposed three schemes will

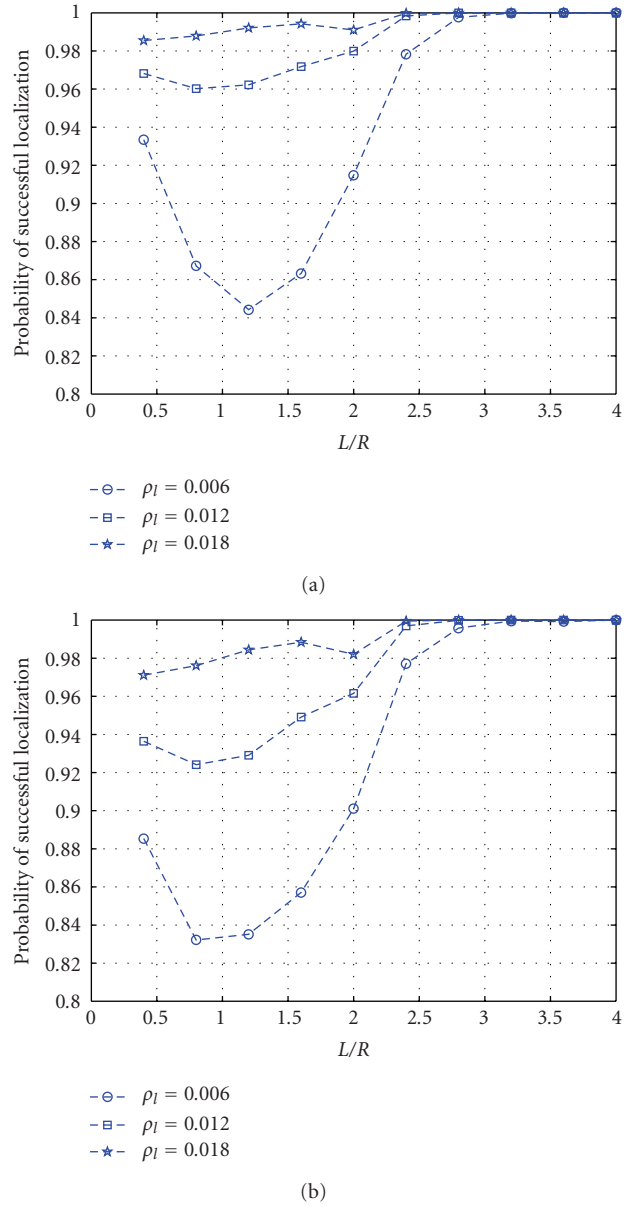

Figure 6: Performance evaluation: (a) the effect of ρ_l on basic TSCD scheme; (b) the effect of ρ_l on enhanced TSCD scheme.

descend. However, even when $\alpha = 0.85$, the descending scales of the performance of the three schemes are limited (less than 10%), which indicates that our proposed schemes are effective when the packet loss exits.

7. Conclusion and Future Work

In this paper, we address the distance-consistent spoofing attack in hostile wireless sensor networks and discuss the drawbacks of the existing secure localization schemes. Based on the secure properties of wireless communication under the distance-consistent spoofing attack, we propose three secure localization schemes: basic TSCD, enhanced TSCD and mobility-aided TSCD. We evaluate the performances

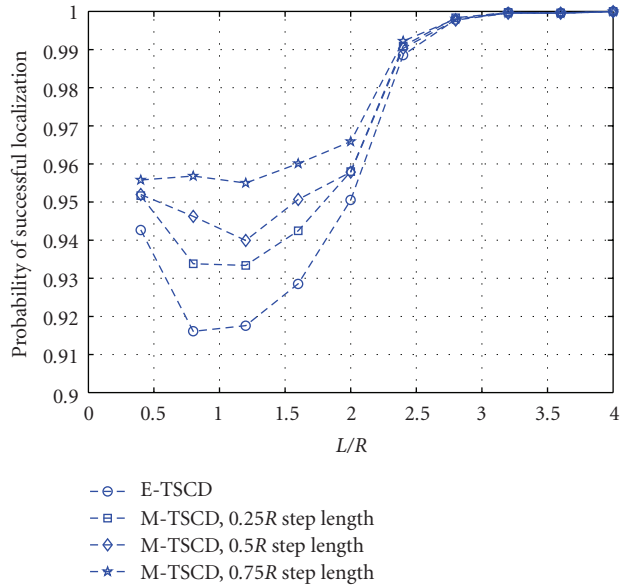

Figure 7: The effect of step length on mobility-aided TSCD scheme.

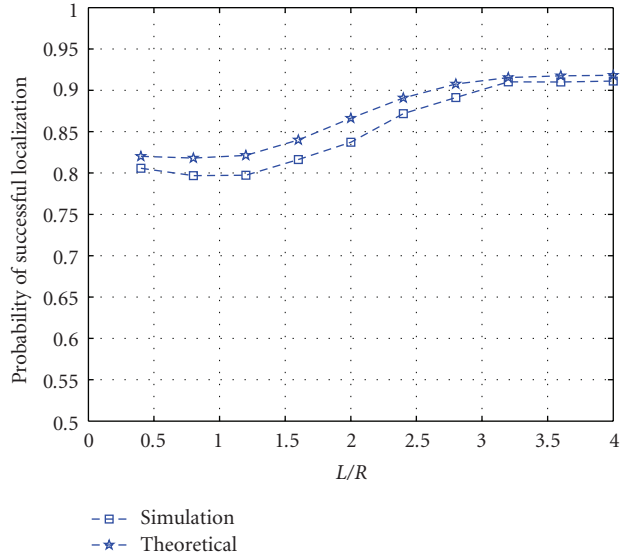

Figure 8: Probability of successfully identifying all attacked locators: simulation versus theoretical.

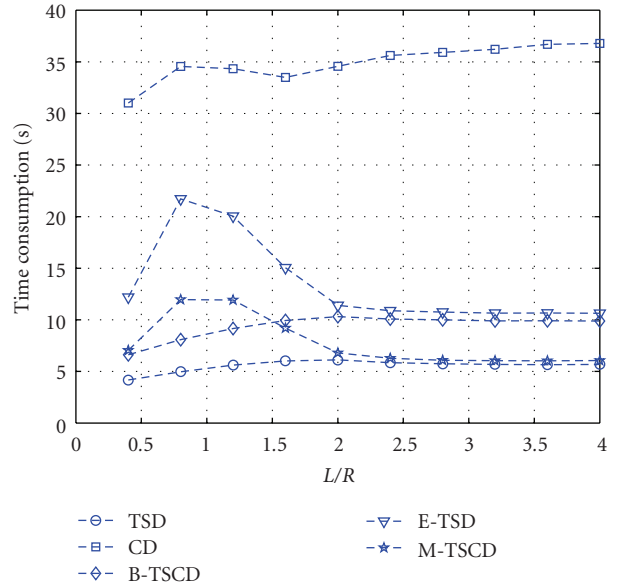

Figure 9: Time consumption of existing schemes and our schemes (the step length is $0.25R$ for the mobility-aided TSCD scheme).

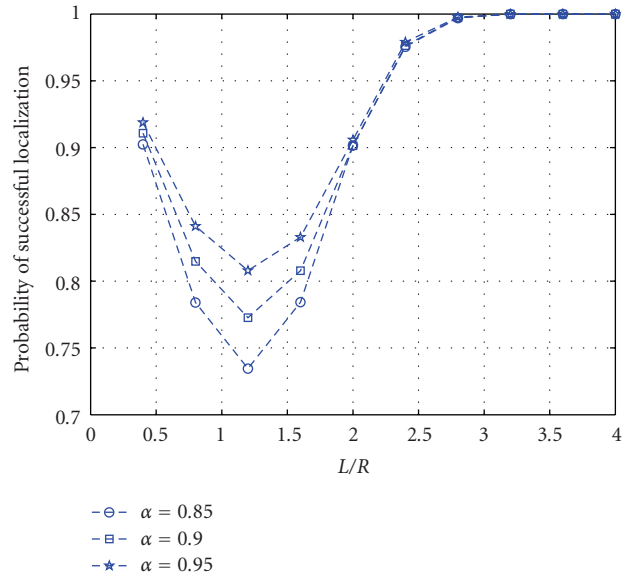

Figure 10: The effect of α on basic TSCD scheme.

of our proposed schemes and compare them with exiting schemes by simulations. The simulation results demonstrate that our schemes outperform the existing schemes under the same network parameters.

In this paper, we assume that no region is attacked by multiple attacks simultaneously. When a sensor is attacked by several attacks simultaneously, it will be very complicated and difficult to obtain secure localization. A potential solution is to separate the localization from the attack detection. That is, when multiple attacks are detected, the system can try to identify the locations of the attackers and then eliminate them. We will focus on the detection of multiple attacks and the localization of the attackers in the future work. In the M-TSCD scheme, we have a precondition that the distance between two consecutive localization processes is relatively short so that when a distance-consistent spoofing attack occurs on the current state it is impossible for another different distance-consistent spoofing attack to occur on the previous state or the next state. A possible solution to release this precondition is to verify whether it is attacked by the same attacker by checking its neighborhood of the two consecutive states. The M-TSCD scheme will be conducted only if the node verifies that it is attacked by the same attacker on the two consecutive states. Thus, the other direction of our future work is to release this precondition.

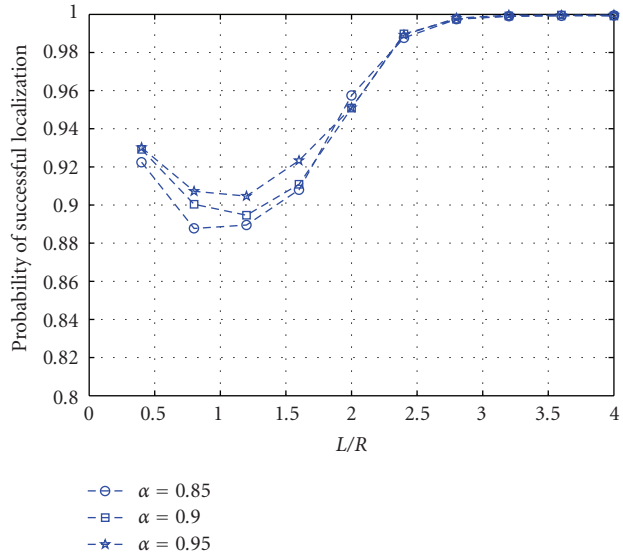

Figure 11: The effect of α on enhanced TSCD scheme.

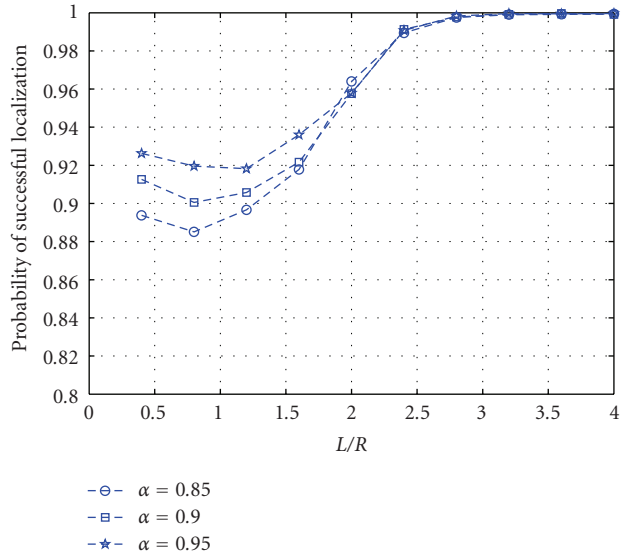

Figure 12: The effect of α on mobility-aided TSCD scheme (the step length is $0.25R$).

Acknowledgment

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

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–105, 2002.

[2] P. Bahl and V. N. Padmanabhan, "RADAR: an in-building RF-based user location and tracking system," in *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE INFOCOM '00)*, pp. 775–784, March 2000.

[3] A. Savvides, C. C. Han, and M. B. Strivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (INFOCOM '00)*, pp. 166–179, July 2001.

[4] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks," in *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MobiCom '03)*, pp. 81–95, September 2003.

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

[6] Y. C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: a secure on-demand routing protocol for ad hoc networks," in *Proceedings of The 8th Annual International Conference on Mobile Computing and Networking*, pp. 12–23, September 2002.

[7] Y. C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies*, pp. 1976–1986, April 2003.

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

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

[10] M. Pirretti, N. Vijaykrishnan, P. McManiel, and B. Madan, "SLAT: secure localization with attack tolerance," Tech. Rep., 2006.

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

[12] A. Srinivasan, J. Teitelbaum, and W. Jie, "DRBTS: distributed reputation-based beacon trust system," in *Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC '06)*, pp. 277–283, October 2006.

[13] D. Liu, P. Ning, and W. Du, "Detecting malicious Beacon nodes for secure localization discovery in wireless sensor networks," in *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS '05)*, pp. 609–619, Columbus, Ohio, USA, 2005.

[14] C. Wang, A. Liu, and P. Ning, "Cluster-based minimum mean square estimation for secure and resilient localization in wireless sensor networks," in *Proceedings of the 2nd Annual International Conference on Wireless Algorithms, Systems, and Applications (WASA '07)*, pp. 29–37, August 2007.

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

[16] F. Anjum, S. Pandey, and P. Agrawal, "Secure localization in sensor networks using transmission range variation," in *Proceedings of the 2nd IEEE International Conference on Mobile*

Ad-Hoc and Sensor Systems (MASS '05), vol. 2005, pp. 195–203, 2005.

[17] H. Chen, W. Lou, and Z. Wang, "Conflicting-set-based wormhole attack resistant localization in wireless sensor networks," in *Proceedings of the 6th International Conference on Ubiquitous Intelligence and Computing (UIC '09)*, vol. 5585 of *Lecture Notes in Computer Science*, pp. 296–309, 2009.

[18] H. Chen, W. Lou, and Z. Wang, "A Consistency-based secure localization scheme against wormhole attacks in WSNs," in *Proceedings of the 4th International Conference on Wireless Algorithms, Systems, and Applications (WASA '09)*, vol. 5682 of *Lecture Notes in Computer Science*, pp. 368–377, 2009.

[19] H. Chen, W. Lou, X. Sun, and Z. Wang, "A secure localization approach against wormhole attacks using distance consistency," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, 11 pages, 2010.

[20] L. Lazos and R. Poovendran, "SeRLoc: robust localization for wireless sensor networks," *ACM Transactions on Sensor Networks*, pp. 73–100, 2005.

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

[22] F. Bouchereau and D. Brady, "Bounds on range-resolution degradation using RSSI measurements," in *Proceedings of the IEEE International Conference on Communications*, pp. 20–24, June 2004.

[23] M. Zhao and S. D. Servetto, "An analysis of the maximum likelihood estimator for localization problems," in *Proceedings of the 2nd International Conference on Broadband Networks*, pp. 982–990, 2005.