Research Article

BRS-Based Robust Secure Localization Algorithm for Wireless Sensor Networks

Ning Yu, Lirui Zhang, and Yongji Ren

School of Instrumentation Science and Optoelectronics Engineering, Beijing University of Aeronautics and Astronautics (Beihang University), Beijing 100191, China

Correspondence should be addressed to Ning Yu; nyu@buaa.edu.cn

Received 6 October 2012; Revised 23 January 2013; Accepted 5 February 2013

Academic Editor: Sunho Lim

Copyright © 2013 Ning Yu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Localization is the key supporting technology for wireless sensor networks (WSNs). Security and accuracy are the premise of the localization application. Real-world applications of wireless sensor networks are often subject to a variety of adverse circumstances interference, and the localization performance is seriously affected. In this paper, we propose a BRS-based robust secure localization (BRSL) algorithm in order to reduce the impact of the malicious attackers in WSNs. The BRSL method includes two phases. In the first stage, the trust evaluation framework is established on the basis of beta reputation system. In the second phase, we employ the weighted Taylor-series least squares method to estimate the coordinates of sensor nodes. Simulation results demonstrate that the proposed algorithm is robust and effective.

1. Introduction

Wireless sensor networks (WSNs) are based on the technology of sensor, wireless communication, tiny embedded devices, and distributed computing. They exchange information with the environment through sensors and implement the function of collecting and dealing with data. Wireless sensor networks have been widely used in the fields of environmental monitoring, target tracking, military applications, disaster management, and so forth [1–3].

Self-localization technology of nodes is the prerequisite and basis for the application of wireless sensor networks, especially the position information that is needed for the perceived data. Node localization of WSNs is to determine the positions of normal nodes based on the positions of beacon nodes and the constraint relations between normal and beacon nodes. Positions or coordinates of normal nodes are unknown. Beacon nodes usually get their positions or coordinates through global positioning system (GPS) modules or by manual deployments. Being an essential support technology of wireless sensor networks, node localization has got more and more attention in the recent years [4–10].

Most localization methods depend on measuring the distances or hops between normal and beacon nodes to obtain the coordinates of normal nodes. In many typical localization algorithms [11–13], the coordinates of beacon nodes are generally assumed to be completely correct without any disturbs of adverse factors, and the normal nodes can use beacon information in security. However, in the actual hostile situations, some malicious nodes may intrude into sensor networks. They pretend to be true beacon nodes or attack other anchor nodes and make them declare false coordinates [14, 15]. The false coordinates or distance estimation will cause a major localization error for normal sensor nodes [16]. In this case, some methods should be explored to eliminate or reduce the adverse influence caused by malicious beacon nodes and ensure safe localization in wireless sensor networks.

In this paper, we develop a BRS-based robust secure localization (BRSL) algorithm for solving the node self-localization problem in the case of malicious nodes existence. In BRSL, normal sensor node first observes the anchor nodes in its communication range and evaluates the trust values of these anchor nodes. Specially, the concepts of the beta reputation system are employed to deal with the uncertain factors in trust evaluation. Then, each anchor node obtains a final trust value, and sensor nodes compare the final trust values of anchor nodes in their multihop communication range.
with the stored threshold. Finally, the normal sensor nodes utilize the trustful anchor nodes to estimate their coordinates. All the above operations can be carried out by each node. The method is a completely distributed localization approach. Through simulations, we demonstrate that the BRSL method can efficiently reduce the influence of malicious attackers in WSNs.

The remainder of the paper is organized as follows: Section 2 introduces related works on secure localization algorithms. Section 3 presents the network model, attack model, and related definitions. Section 4 provides the details of the BRS-based robust secure localization (BRSL) algorithm. Section 5 presents the simulation results. Section 6 concludes the paper.

2. Related Works

Alfaro et al. [17] consider the localization security of sensor nodes under limited trust anchor nodes. It introduces three algorithms to enable the sensor nodes to determine their positions, but it would fail when the malicious anchor nodes are in colluding conditions.

Liu et al. [18] propose two secure localization algorithms. One is attack-resistant minimum mean square estimation, which excludes malicious anchor nodes by the consistency check. The other is voting-based location estimation. The algorithms are difficult to work for the malicious anchor nodes in colluding conditions.

Zhu et al. [19] propose an attack detection module which can detect compromised beacons and provide a localization service in terms of bounded estimation error by secure localization module, but it mainly concentrates on the one-hop localization.

Liu et al. [20] present a secure localization mechanism that detects malicious anchor nodes claiming fake positions. It uses redundant anchor nodes instead of normal nodes in the sensing field to verify malicious anchors. The method relies on a centralized base station for the detection.

Li et al. [21] introduce a secure scheme “Bilateration” which is derived from multilateration. It calculates the weight of anchor nodes and decides which anchor nodes are malicious. After ignoring the coordinates caused by compromised nodes, it uses the average value of the left candidate positions as the estimated location of the sensor node, but it mainly focuses on the one-hop localization.

3. Preliminaries

3.1. Network Model. We consider a network consisting of two types of nodes, namely, anchor nodes and sensor nodes. The anchor nodes are specially equipped and aware of their coordinates after deployment. The sensor nodes, whose positions are yet to be discovered, estimate their locations by measuring distances to neighboring anchor nodes. All nodes are randomly distributed in a 2D spatial region. Every node has a unique identity (ID). The transmission range or ranging radius of each node is R. Every node is capable of measuring the distance to any of its immediate neighbors.

The ranging error e follows a Gaussian distribution \( N(u, \lambda^2) \), where the mean \( u \) is 0 and the standard deviation \( \lambda \) is within a threshold. Measurement error e is bounded by \( |e| \leq e_{\max} \), and the maximum physical inaccuracy \( e_{\max} \) can be obtained experimentally. In multihop localization, each anchor node broadcasts a message that carries its declared position to its one-hop neighbors. Then, the message is propagated in the network in a controlled flooding manner. When a sensor node obtains three or more anchor messages, the sensor node can estimate its location by the localization algorithm.

3.2. Attack Model. We assume that the WSN is in a hostile environment, that is, there are malicious attackers in the network. The attackers attack the anchor nodes in order to make them declare dishonest coordinates. When an anchor node is attacked and broadcasts erroneous locations, we call it malicious anchor node. The nodes claiming actual coordinates are called benign anchor nodes. We consider an adversarial environment where the malicious anchor nodes are in noncolluding scenario or colluding scenario. If the malicious anchor nodes are noncolluding, they cannot know whether other anchor nodes are malicious or not. They can only fake their own declared locations to affect the localization process. While the malicious anchor nodes are colluding, they can detect whether other anchor nodes are the same type, and each pair of colluding malicious anchor nodes can revise the measure distance between them by changing their declared locations.

As shown in Figure 1, when a sensor node \( M \) gets enough measurement distances \( d_{mj} \) \((i = 1, 2, \ldots, k)\), where \( k \geq 3 \), to anchor nodes \( A_i \), a system of the Euclidean equations can be set up:

\[
\begin{align*}
\|X_m - X_1\|_2 &= d_{m1} \\
\|X_m - X_2\|_2 &= d_{m2} \\
&\vdots \\
\|X_m - X_k\|_2 &= d_{mk},
\end{align*}
\]

where \( X_m = [x_m, y_m]^T \) is \( M \)'s coordinates that need to be estimated and \( X_i = [x_i, y_i]^T \) is anchor node \( A_i \)'s declared position.

If the anchor node \( A_1 \) is attacked, it will become a malicious anchor node \( A_1' \) with fake coordinates. When \( M \) utilizes \( A_1' \) to compute its position, its estimated position \( M' \) will deviate far from its physical position, and its location accuracy will be very low.

3.3. Related Definitions. To be convenient, some necessary definitions are given in the following.

(i) Measurement distance: node \( i \) is in the communication radius of node \( j \). The physical measurement distance from \( i \) to \( j \) (through RSSI, TDOA, etc.) is called measurement distance.
distribution \( B(a, \beta) \) can be expressed by using the gamma function as
\[
f(x | \alpha, \beta) = \frac{\Gamma(\alpha + \beta)}{\Gamma(\alpha) \Gamma(\beta)} x^{\alpha-1} (1 - x)^{\beta-1},
\]
where \( 0 < x < 1, \alpha > 0, \beta > 0, \) and \( \Gamma(a) \) is the gamma function.

The gamma function \([23]\) (represented by the capital Greek letter \( \Gamma \)) is an extension of the factorial function, with its argument shifted down by 1, to real and complex numbers. If \( n \) is a positive integer, we get the formula \( \Gamma(n) = (n-1)! \). If \( z \) is a complex number, we get the formula \( \Gamma(z) = \int_{0}^{\infty} e^{-t} t^{z-1} dt \), where the real part of \( z \) must be larger than zero (\( \text{Re}(z) > 0 \)). The gamma function is applicable in the fields of probability and statistics. It is also a component in various probability-distribution functions.

The beta reputation system consists of two elements \((\alpha, \beta)\) that can be used separately or in combination to provide a flexible framework for reputation services of WSNs applications. We use the beta reputation system to establish the trust evaluation framework of anchor nodes. In the network, anchor nodes have two types: benign anchor nodes and malicious anchor nodes. And the two elements \((\alpha, \beta)\) of beta reputation system are the most appropriate parameters here to judge the anchor nodes. The probability expectation value of the beta distribution is given by
\[
E(x) = \frac{\alpha}{\alpha + \beta},
\]
and the variance is
\[
Var(x) = \frac{\alpha \beta}{(\alpha + \beta)^2 (\alpha + \beta + 1)}.
\]

In the network, every anchor node has a unique ID, and the sensor node is assumed to have the detecting function. We utilize the beta reputation system to detect the malicious anchor nodes. The detecting process is considered with two possible outcomes (benign anchor node and malicious anchor node). Let \((a + 1)\) be the observed outcome number of benign anchor nodes, and let \((b + 1)\) be the observed outcome number of malicious anchor nodes. Then, we have a beta function expressed as \( f(x | (a + 1), (b + 1)) \), where \( x \) denotes the benign anchor node. The observed number of benign anchor nodes and malicious anchor nodes is used in the beta function to estimate the probability of anchor nodes to be benign ones, which equals to the expectation value of \( x \).

As we do not know whether the anchor nodes are benign or not at the beginning, we initially assume all anchor nodes to be benign ones.

Let \( \text{Rep}_{T} \) denotes the reputation of anchor nodes and \( \text{Rep}_{T} \sim B(a+1, b+1) \). Let \( \text{Tru}_{T} \) denotes the trust value of the anchor node. From the beta reputation system, we know that the expectation value of \( \text{Rep}_{T} \) is equal to \( \text{Tru}_{T} \), that is, \( E(\text{Rep}_{T}) = \text{Tru}_{T} \). Assume that there are \( N_{1} + N_{2} \) anchor nodes and \( N_{2} \) sensor nodes randomly deployed in the network. Assume \( n \) \((n \leq N_{1} + N_{2})\) anchor nodes \((A_{1}, A_{2}, \ldots, A_{n})\) are available to an arbitrary sensor node \( M_{j} \).
We deploy the network $Q$ times in total. The detail of the detecting process is given as follows.

(1) Compute $a_i$ and $b_i$ through the geometric relationship among anchor nodes. The values of $a_i$ and $b_i$ are set to 0 initially. The value of $d_{ij}$ is the Euclidean distance between $A_i$ and $A_j$, and $d_{ij}'$ denotes the measurement distance between $A_i$ and $A_j$ (if $A_i$ and $A_j$ are neighbors).

(a) If inequality $|d_{ij} - d_{ij}'| \leq e_{\text{max}}$ or $0 < d_{ij} < 2R$ is satisfied, let $a_i' = 1$. Otherwise, let $a_i' = 0$.

(b) If inequality $|d_{ij} - d_{ij}'| > e_{\text{max}}$ or $d_{ij} > 2R > 0$ is satisfied, let $b_i' = 1$. Otherwise, let $b_i' = 0$.

For example, Figure 2 shows the geometric relationship among anchor nodes, in which $A_i$ ($i = 1, 2, \ldots, 6$) represents the anchor nodes and $M_j$ ($j = 1, 2, \ldots, 5$) represents the sensor nodes. Anchor node $A_2$ is attacked, and $A_2'$ is the declared position of $A_2$. As anchor node $A_3$ is not the neighbor of $A_2$, we can only obtain the Euclidean distance $d_{23}$ between them. A set of inequalities can be set up: $|d_{12} - d_{12}'| > e_{\text{max}}$, $|d_{14} - d_{14}'| \leq e_{\text{max}}$, $|d_{15} - d_{15}'| \leq e_{\text{max}}$, $|d_{16} - d_{16}'| \leq e_{\text{max}}$, and $0 < d_{23} < 2R$. Sensor nodes $M_1$ and $M_3$ are in anchor node $A_1$’s communication range. Therefore, we can get $a_1' = 2$, $b_1' = 1$ and $a_1^3 = 2$, $b_1^3 = 0$.

(2) Compute the trust value of anchor node $A_i$ in each network deployment.

(a) Assume that $m$ ($m \leq N_5$) sensor nodes $(M_1, M_2, \ldots, M_m)$ are available to anchor node $A_i$. These $m$ sensor nodes utilize step (1) to detect anchor node $A_i$. The observed number of anchor node $A_i$ to be a benign one is

$$a_i' + 1 = \sum_{j=1}^{m} a_i^j + 1$$

and the observed number of anchor node $A_i$ to be a malicious one is

$$b_i' + 1 = \sum_{j=1}^{m} b_i^j + 1.$$  

(b) The $\text{Rep} \cdot T_{A_i} \sim B(a_i' + 1, b_i' + 1)$. The trust value of anchor node $A_i$ is

$$\text{Tru} \cdot T_{A_i} = E(\text{Rep} \cdot T_{A_i}) = \frac{a_i' + 1}{a_i' + b_i' + 2},$$

and the variance of anchor node $A_i$ is

$$\sigma_{A,p} = \frac{(a_i' + 1) \times (b_i' + 1)}{(a_i' + b_i' + 2)^2} - (a_i' + b_i' + 3).$$

(3) Compute the trust value of anchor node $A_i$ after the $Q$ times network deployment. Let $p$ denotes the current deployment time. Repeat step (1) and step (2) until $p > Q$. The final trust value of anchor node $A_i$ is

$$\text{Tru} \cdot T_{A_i} = \frac{\sum_{p=1}^{Q} \text{Tru} \cdot T_{A_i,p}}{Q},$$

and the final variance of anchor node $A_i$ is

$$\sigma_{A_i} = \frac{\sum_{p=1}^{Q} \sigma_{A,p}}{Q}.$$ (11)

(4) Judge whether anchor node $A_i$ is a benign anchor node.

(a) After the anchor node $A_i$ obtains the final trust value $\text{Tru} \cdot T_{A_i}$, it broadcasts $\text{Tru} \cdot T_{A_i}$ to the network in a multihop flooding manner. The sensor nodes store the final trust values they obtained, based on which they can decide whether $A_i$ is a benign anchor node.

(b) The sensor nodes compare the $\text{Tru} \cdot T_{A_i}$ that they received from step (3) with threshold $\mathbb{V}$. If $\text{Tru} \cdot T_{A_i} \geq \mathbb{V}$, sensor nodes will consider anchor node $A_i$ as a benign anchor node and utilize $A_i$ in the localization phase. If $\text{Tru} \cdot T_{A_i} < \mathbb{V}$, sensor nodes will take anchor node $A_i$ as a malicious anchor node, and $A_i$ will be revoked before the localization stage.

The determination of threshold $\mathbb{V}$ depends on the final trust value of each anchor node. The threshold $\mathbb{V}$ is defined as follows

$$\mathbb{V} = \sum_{q=1}^{N_1 + N_2} \left( \frac{\sigma_q}{\sum_{q=1}^{N_1 + N_2} \sigma_q} \right) \times \text{Tru} \cdot T_q.$$ (12)
where \( N_1 + N_2 \) is the total number of anchor nodes, \( q \) is the ID of anchor node, and \( \sigma_q \) is the final variance of anchor node \( q \).

From the above steps, we will get the trust evaluation of anchor nodes. The situation we investigated in this paper is that the percentage of malicious anchor nodes is less than half of the number of anchor nodes. When the malicious anchor nodes are noncolluding, they will not cooperate with each other. Therefore, it is hard for these malicious anchor nodes to obtain high value of \( d'_i \). As the number of malicious anchor nodes is less than that of benign ones, the colluding malicious anchor nodes will be given more value on \( b'_i \). When malicious anchor nodes are cooperated, some malicious anchor nodes may obtain more value on \( a'_i \) than \( b'_i \), but such nodes are very few. Generally, \( a'_i \) is smaller than \( b'_i \) for malicious anchor nodes, and \( a'_i \) is bigger than \( b'_i \) for benign anchor nodes. Therefore, most benign anchor nodes’ trust values are larger than that of malicious anchor nodes in each network deployment.

Formula (8) shows that the bigger \( a'_i \) is, the larger \( Rep_T \) is. Similarly, the bigger \( b'_i \) is, the smaller \( Rep_T \) is. The variance of anchor node \( q \) denotes the deviating degree of anchor node \( q \)’s trust value from the expectation value. If the final variance of anchor node \( q \) is big, it means the distribution of anchor node \( q \)’s trust values is relatively concentrated. The differences between most benign anchor nodes’ trust values and their average trust value are larger than those of malicious anchor nodes, that is, \( \sigma_{benign} > \sigma_{malicious} \). The weight \( \sum_{q=1}^{N_1+N_2} \sigma_q \) of trust values of anchor nodes in formula (12) demonstrates that the trust values of benign anchor nodes account for a higher proportion than malicious anchor nodes’ trust values in the judging threshold, which is helpful in excluding malicious anchor nodes. Therefore, formula (12) indicates the most appropriate threshold here.

4.2. The Localization of Sensor Nodes. When utilizing malicious anchor nodes to localize the sensor nodes, the localization accuracy of sensor nodes is very low. To resolve this problem, we eliminate the malicious anchor nodes before the localization phase. The sensor node \( M \) utilizes all its multihop communication anchor nodes to estimate its coordinates. The traditional method like maximum likelihood estimation (MLE) has a high computational complexity and always loses much coordinates information. We employ the weighted Taylor-series least squares algorithm to estimate the coordinates of sensor nodes and the final trust values \( Tru_T_1, Tru_T_2, \ldots, Tru_T_K \) (\( q = 1, 2, \ldots, K, K \geq 3 \)) of benign anchor nodes are used as the weight in the localization stage. The weighted Taylor-series least squares method can make better use of the anchor information, and the computing accuracy can be greatly improved. The localization processes are as follows.

Assume \( d_{mi} (i = 1, 2, \ldots, K) \) are the measurement distances from the \( k \) anchor nodes to the sensor node \( M \) and \( X_i = (x_i, y_i) \) is the declared coordinates of anchor node \( i \). The position of sensor node \( M \) is denoted as \( X = (x_0, y_0) \). Therefore, we have a set of the Euclidean equations:

\[
Tru_T_i \times \| X - X_i \|_2 = Tru_T_i \times d_{mi}. \tag{13}
\]

Firstly, calculate the centroid coordinates \( X_C = (x_C, y_C) \) of \( K \) anchor nodes, that is, \( X_C = (1/K) \sum_{i=1}^{K} X_i \).

Secondly, expand the function \( f(X) = \| X - X_i \|_2 \) in Taylor series at \( X_C \), and ignore the high-order terms. Equation (13) is transformed into the following modus:

\[
Tru_T_1 \left( \frac{x_C - x_1}{d_{1C}} \Delta x + \frac{y_C - y_1}{d_{1C}} \Delta y \right) = Tru_T_1 \left( d_1 - d_{1C} \right),
\]

\[
Tru_T_2 \left( \frac{x_C - x_2}{d_{2C}} \Delta x + \frac{y_C - y_2}{d_{2C}} \Delta y \right) = Tru_T_2 \left( d_2 - d_{2C} \right),
\]

\[
\vdots
\]

\[
Tru_T_K \left( \frac{x_C - x_K}{d_{KC}} \Delta x + \frac{y_C - y_K}{d_{KC}} \Delta y \right) = Tru_T_K \left( d_K - d_{KC} \right).
\tag{14}
\]

where \( d_q \) denotes the Euclidean distance between \( X_i \) and \( X_j \). Therefore, \( \Delta X_C = (\Delta x_C, \Delta y_C) \) can be obtained by \( \Delta X_C = (A^TW^WA)^{-1}A^TW^T \), where

\[
W = \begin{bmatrix}
Tru_T_1 & 0 & 0 \\
0 & Tru_T_2 & 0 \\
\vdots & \ddots & 0 \\
0 & 0 & Tru_T_K
\end{bmatrix},
\]

\[
B = \begin{bmatrix}
d_1 - d_{1C} \\
d_2 - d_{2C} \\
\vdots \\
d_K - d_{KC}
\end{bmatrix},
\tag{15}
\]

\[
A = \begin{bmatrix}
x_C - x_1 & x_C - x_2 & \cdots & x_C - x_K \\
x_C - y_1 & x_C - y_2 & \cdots & x_C - y_K \\
\vdots & \vdots & \ddots & \vdots \\
x_C - x_1 & x_C - x_2 & \cdots & x_C - x_K
\end{bmatrix}^T.
\]

Thirdly, let \( d = \sqrt{\Delta x_C^2 + \Delta y_C^2} \), and judge whether the iteration termination condition \( d \leq \eta \) is satisfied, where \( \eta \) is a prior-defined threshold. If \( d \leq \eta \), we stop the iteration process. Otherwise, we set \( X_C = X_C + \Delta X_C \) and go to the second step.

Finally, repeat the second step and the third step until the iteration termination condition is satisfied or the maximum iteration number is reached. The final output \( X_C \) is the estimated coordinates of sensor node \( M \).
5. Performance Evaluation

In this section, the performance of the BRSL algorithm is tested. All simulations are executed in MATLAB.

The WSN is in a hostile environment, and the malicious anchor nodes are in two conditions: noncolluding or colluding. The default network configuration parameters are shown in Table 1. Unless specified, the default parameters are used in the simulations.

Figure 3 shows the random network deployment, and each anchor node has a unique ID in all the simulations, where benign anchor nodes’ IDs are from 1 to 20 and malicious anchor nodes’ IDs are from 21 to 30.

5.1. Trust Evaluation of Anchor Nodes. Firstly, we analyze the trust evaluation of anchor nodes. Figures 4 and 5 show that the final variances of benign anchor nodes are bigger than those of the malicious anchor nodes, no matter whether the malicious anchor nodes are noncolluding or colluding. Therefore, the weight $\sigma_q/\sum_{q=1}^{N_1+N_2} \sigma_q$ is proper in this paper. When malicious anchor nodes are in noncolluding condition, from Figure 6, we can see that the final trust values of benign anchor nodes are much larger than those of malicious anchor nodes, and the threshold $V$ is about 0.267032. Therefore, we can remove all the malicious anchor nodes before the localization stage. When malicious anchor nodes are colluding, as Figure 7 shows, some of the malicious anchor nodes’ final trust values are bigger than those of benign anchor nodes, and the threshold $V$ is about 0.297201. Although all the malicious anchor nodes can be excluded by the threshold, some benign anchor nodes are also removed. But in Section 5.2, it proves that the localization accuracy is still high although some benign anchor nodes are excluded.

5.2. Evaluation of BRSL Algorithm. In this subsection, we compare the average localization error (ALE) of the BRSL algorithm with other localization techniques: RMLA2 [15], RMLA1 [15], Bilateral [21], and the traditional multihop

Table 1: Default network configuration parameters.

| Parameters               | Values                  |
|--------------------------|-------------------------|
| Network size ($A$)       | 200 m × 200 m           |
| Deployment strategy      | Random                  |
| Number of nodes ($N = N_1 + N_2 + N_3$) | 200 |
| Number of benign anchor nodes ($N_1$) | 20 |
| Number of malicious anchor nodes ($N_2$) | 10 |
| Number of normal sensor nodes ($N_3$) | 170 |
| Number of simulation rounds ($Q$) | 1000 |
| TTL                      | 4                      |
| Trust threshold value $V$ | Formula (12)           |
| Communication radius ($R$) | 30 m               |
| $\epsilon_{max}$         | 0.1R                   |
| The standard deviation $\lambda$ | 1                  |
| Network connectivity     | 8~12                   |
localization method without trust evaluation in which Taylor-series least squares solver is used (t-TLS for short). Based on our simulations, we show that BRSL has superior performance in localization accuracy.

The ALE is normalized by the nodes’ communication radius $R$:

$$\text{ALE} = \frac{1}{N_3 R} \sum_{i=N_1+N_2+1}^{N} \|X_i - X_i'\|_2,$$

(16)

where $X_i$ is the estimated coordinates of sensor node $i$ and $X_i'$ is the real coordinates of sensor node $i$.

Figures 8 and 9 show the impact of malicious anchor number on the localization accuracy of BRSL, RMLA2, RMLA1, Bilateralation, and t-TLS. With the increase of number of malicious anchor nodes, the ALE of RMLA2, RMLA1, Bilateralation, and t-TLS rises obviously, while that of BRSL remains stable (no more than 22% in noncolluding scenario and 30% in colluding scenario). Therefore, BRSL is robust for multihop localization and can greatly improve the average localization accuracy no matter the malicious anchor nodes are noncolluding or colluding.

Figures 10 and 11 show the comparison results of ALE under different standard deviation $\lambda$ of ranging errors in noncolluding and colluding scenario, respectively. The ALE of each algorithm increases with standard deviation $\lambda$. Compared with RMLA2, RMLA1, Bilateralation, and t-TLS, BRSL may approximately improve the localization accuracy by 10%, 15%, 55%, and 110%, respectively, in noncolluding scenario and 15%, 20%, 65%, and 150% in colluding scenario. The BRSL performs much better than other algorithms.

Figures 12 and 13 illustrate the relationship of ALE with the times of network deployment. The number of simulation rounds equals to the times of network deployment. The
A L E almost does not change with the number of simulation rounds whether the malicious anchor nodes are in noncolluding or colluding condition. The variety of network topology does not affect the detecting and localization process.

5.3. Cost Analysis. Finally, we analyze the costs of five algorithms. Assume a sensor node $M_i$ can hear $n$ anchor nodes in its one-hop range. In BRSL method, $M_i$ needs to compute $\binom{n}{2}$ times to detect each anchor node. Thus, the cost of reputation computation in the network is $O(N_3 \cdot n^2)$. The computation complexity of the localization stage in our method is $O(n)$. Then the total cost of BRSL method is $O(N_3 \cdot n^2) + O(n)$. The costs of RMLA2 equals to that of RMLA1. The communication complexity of RMLA1 or RMLA2 is $O(N_3 \cdot n^2)$. And the computation complexity of RMLA1 or RMLA2 is $O(n)$. Thus, the total cost of RMLA1 or RMLA2 is $O(N_3 \cdot n^2) + O(n)$, which is the same as BRSL algorithm. The costs of Bilateration and t-TLS mainly focus on the computation stage. The computation complexity of Bilateration is $O(n^2)$, while that of t-TLS is $O(n)$. Therefore, the cost of our method is moderate and acceptable.

6. Conclusions

In this paper, we propose a BRS-based robust secure localization algorithm for the case of presence of malicious anchor nodes. Based on the beta reputation system and the trust evaluation, the malicious anchor nodes are detected and excluded. By utilizing the weighted Taylor-series least squares
method, the coordinates of sensor nodes are estimated. The simulation results demonstrate that the BRSL algorithm can effectively distinguish malicious anchor nodes and improve localization accuracy, as well as resist topology variety and ranging uncertainties. In the future, our work will focus on the secure localization when there are multiple and different attacks in complex environments.

Acknowledgments

The authors are grateful to the anonymous reviewers for their industrious work and insightful comments. This work is supported by National Natural Science Foundation of China under Grant nos. 61001138 and 61201317.

References

[1] J. Albowicz, A. Chen, and L. Zhang, “Recursive position estimation in sensor networks,” in Proceedings of the 9th International Conference on Network Protocols, pp. 35–41, 2001.

[2] H. A. Oliveira, E. F. Nakamura, A. A. F. Loureiro, and A. Boukerche, “Directed position estimation: a recursive localization approach for wireless sensor networks,” in Proceedings of the 14th IEEE International Conference on Computer Communications and Networks, pp. 557–562, San Diego, Calif, USA, 2005.

[3] 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 Mobile Computing and Networking (MobiCom ’03), pp. 81–95, ACM Press, San Diego, Calif, USA, 2003.

[4] M. L. Sichitiu and V. Ramadurai, “Localization of wireless sensor networks with a mobile beacon,” in Proceedings of the 1st IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, pp. 174–183, Fort Lauderdale, Fla, USA, October 2004.

[5] X. L. Guo, R. J. Feng, Y. F. Wu, and J. W. Wan, “Grid-Scan-Based multi-hop Localization algorithm for wireless sensor networks,” in Proceedings of IEEE Sensors Conference, pp. 668–672, Waikoloa, Hawaii, USA, 2010.

[6] D. Niculescu and B. Nath, “DV based positioning in ad hoc networks,” Telecommunication Systems, vol. 22, pp. 267–280, 2003.

[7] K. Yu, Y. J. Guo, and M. Hedley, “TOA-based distributed localization with unknown internal delays and clock frequency offsets in wireless sensor networks,” IET Signal Processing, vol. 3, no. 2, pp. 106–118, 2009.

[8] J. Wan, N. Yu, R. Feng, Y. Wu, and C. Su, “Localization refinement for wireless sensor networks,” Computer Communications, vol. 32, pp. 1515–1524, 2009.

[9] H. Lim and J. C. Hou, “Localization for anisotropic sensor networks,” in Proceedings of 24th Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 1, pp. 138–149, 2005.

[10] J. W. Wan, X. L. Guo, N. Yu, Y. F. Wu, and R. J. Feng, “Multi-hop localization algorithm based on grid-scanning for wireless sensor networks,” Sensors, vol. 11, no. 4, pp. 3908–3938, 2011.

[11] Y. Shang, H. Shi, and A. A. Ahmed, “Performance study of localization methods for ad-hoc sensor networks,” in Proceedings of the IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, pp. 184–193, October 2004.