Research Article

Reputation-Based Secure Sensor Localization in Wireless Sensor Networks

Jingsha He,¹ Jing Xu,² Xingye Zhu,¹ Yuqiang Zhang,² Ting Zhang,² and Wanqing Fu³

¹ School of Software Engineering, Beijing University of Technology, Beijing 100124, China

² College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China

³ Information Center, SINOPEC Research Institute of Petroleum Processing, Beijing 100083, China

Correspondence should be addressed to Jingsha He; jhe@bjut.edu.cn

Received 7 March 2014; Accepted 25 April 2014; Published 20 May 2014

Academic Editor: Yuxin Mao

Copyright © 2014 Jingsha He 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.

Location information of sensor nodes in wireless sensor networks (WSNs) is very important, for it makes information that is collected and reported by the sensor nodes spatially meaningful for applications. Since most current sensor localization schemes rely on location information that is provided by beacon nodes for the regular sensor nodes to locate themselves, the accuracy of localization depends on the accuracy of location information from the beacon nodes. Therefore, the security and reliability of the beacon nodes become critical in the localization of regular sensor nodes. In this paper, we propose a reputation-based security scheme for sensor localization to improve the security and the accuracy of sensor localization in hostile or untrusted environments. In our proposed scheme, the reputation of each beacon node is evaluated based on a reputation evaluation model so that regular sensor nodes can get credible location information from highly reputable beacon nodes to accomplish localization. We also perform a set of simulation experiments to demonstrate the effectiveness of the proposed reputation-based security scheme. And our simulation results show that the proposed security scheme can enhance the security and, hence, improve the accuracy of sensor localization in hostile or untrusted environments.

1. Introduction

The technologies of wireless sensor networks (WSNs) are becoming popular along with the rapid advancement of wireless communication technology, more remarkable performance of integrated circuits as well as decrease in cost and increase in functionality of sensor nodes. Since WSNs are a kind of intelligence networks that are able to integrate data collection, fusion, and transmission, such networks have been widely used in fields such as military defense, industrial and agricultural control, urban management, environment monitoring, health care, emergency rescue, and disaster relief. In addition, sensor networks also have a broad prospect of applications in tracking logistics management and space exploration. Depending on different application scenarios in the above areas, researchers have put forward some new technology and strategy, such as sensor deployment methods suitable for underwater detection [1] and intelligent monitoring technologies in Smart Home scenarios [2]. In short,

the applications of WSNs are being developed to achieve ubiquity that can bring more convenience for human beings in many areas.

In most applications, sensor nodes are used to collect physical data, such as temperature, humidity, water level, pressure, and wind speed, that are sent along with the location information to the data center to ensure that the collected data have spatial meaning. Furthermore, the location information of sensor nodes can also serve as the basis for some network functions, such as network configuration and real-time statistics of network coverage. Therefore, in massively deployed WSNs, location information of sensor nodes is very important for enabling many applications, which makes sensor localization one of the basic services and a core technology for WSNs.

Since sensor localization in wireless sensor networks (WSNs) is a fundamental technical issue and is critical for monitoring applications and for most location-based routing protocols and services, research in sensor localization

technology has generated a wide spread interest and various issues on different aspects have been studied, which include efficiency [3], accuracy [4], and security [5], among many hot issues in sensor localization.

Current algorithms for sensor localization fall into two categories: range-free algorithms [6] and range-based algorithms [7]. In a range-free algorithm, such as Centroid [8] or CTDV-Hop [9], a node estimates its location using information of connectivity between different nodes. In a range-based algorithm, a sensor node estimates its own location based on information about distances or angles between sensor nodes and through using techniques such as time of arrival (TOA) [10], time difference of arrival (TDOA) [11], received signal strength indicator (RSSI) [12], and angle of arrival (AOA) [13] as well as methods such as trilateration, triangulation, or maximum likelihood estimation [14]. Among the many different sensor localization algorithms, RSSI-based positioning technology is perhaps the most popular due to its low cost and easy implementation. On the other hand, sensor localization results can be greatly affected by malicious nodes in hostile or untrusted environments. This is because sensor nodes can hardly perform accurate localization if they use location information that is provided by untrusted beacon nodes. Security in sensor localization has thus received a great deal of attention along with the development of sensor localization technologies for WSNs.

In the past few years, researchers have proposed several security strategies for sensor localization from different aspects. Some of the methods implement verification measures to reduce the impact of using unreliable or false location information [15] while some others apply a series of schemes in which temporal, spatial, and consistent properties are considered to deal with distance-consistent spoofing attacks [16]. However, in these schemes, sensor nodes are divided into just two types: secure and insecure sensor nodes through the mechanisms of comparing the nodes and their behavior against normal situations. However, such an approach cannot be very objective, which could cause many false positive and false negative results.

Meanwhile, some other researchers have proposed localization methods that are able to fight against attacks launched by compromised sensor nodes, a problem that is more difficult to deal with. Liu et al. proposed robust computing algorithms to improve the reliability of localization schemes [17]. Park and Shin proposed an attack-tolerant localization protocol that would perform adaptive management of a profile for normal localization behavior [18]. However, the limitation of these schemes is that they did not consider the security of sensor localization when sensor nodes are joining and leaving the network along with the passage of time. In addition, they did not pay enough attention to secure sensor localization in dynamic wireless networks.

As an effective means of ensuring security, the notion of reputation has been introduced and some reputation-based schemes have since been proposed for sensor localization. Srinivasan et al. proposed a distributed reputation-based beacon trust system [19] and Xu et al. proposed a reputation-based revising scheme for sensor localization which would incur high computation cost [20]. However, complicated

reputation evaluation in the above schemes for sensor localization makes it necessary to further improve the efficiency of evaluation for beacon nodes. Any sensor localization method that can achieve good performance should ensure the reliability of location information before such information can be actually used for sensor localization.

In real applications, there may be other types of sensor localization methods to fit different application scenarios. Therefore, specific localization methods in real applications need to be continuously developed and improved based on orientation methods in order to adapt basic sensor localization schemes to the many different network scenarios. Consequently, in order to develop effective sensor localization methods, we should analyze and understand the main characteristics of specific networks and develop proper performance metrics that can be used to measure the performance of sensor localization schemes. In addition, we should also consider limitations of wireless sensor networks such as constrained energy supply in the sensor nodes as well as the complexity of network environments in the development of effective sensor localization methods.

In this paper, we propose a novel reputation-based secure sensor localization scheme to improve the accuracy of sensor localization for WSNs in hostile environments. In the proposed reputation model, the reputation of each beacon node is evaluated by each other to ensure that sensor nodes will get credible location information to perform sensor localization. The proposed scheme can therefore effectively reduce the impact of malicious beacon nodes on the localization of regular sensor nodes by relying on the security mechanism of beacon node evaluation. Our simulation results show that the proposed reputation-based secure sensor localization scheme can improve the accuracy of sensor localization in hostile or untrusted environments. In addition, the proposed secure sensor localization scheme possesses the desirable characteristics of expandability and flexibility since it can be used in both static and dynamic networks.

The remainder of this paper is structured as follows. In Section 2, we present a reputation model in which we first describe the network model and then propose a reputation evaluation model. In Section 3, we present our sensor localization scheme which is based on the evaluation of the reputation of beacon nodes. In Section 4, we describe the simulation that we have performed and present the simulation results. Finally, in Section 5, we conclude this paper in which we also discuss some future work.

2. The Reputation Model

In hostile network environments, which most current WSN deployments would assume, regular sensor nodes need to be confronted with security threats during the process of sensor localization. If a sensor node can identify the security and credibility of location information that it receives and subsequently use the information appropriately, the accuracy of sensor localization can be greatly improved or ensured in such environments. Therefore, in order to develop effective sensor localization schemes, we should understand the main

characteristics of the specific networks as well as the performance goals of the localization schemes. To achieve the above objective, we need to consider such characteristics as resource constraints in the sensor nodes and the complexity of the environment where the sensor nodes are deployed. Any sensor localization scheme must be effectively working in a specific WSN after the above-mentioned factors are considered in the design.

To achieve the above goal, we first propose a reputation scheme to be used in the sensor localization scheme we will propose later in this paper to deal with a hostile deployment environment in which malicious nodes can be dropped into the network at will and regular sensor nodes can also be easily compromised to make them behave in a malicious manner. We call the scheme that we propose the reputation-based localization scheme (RBL). The main characteristics of the reputation model and the RBL are as follows.

- (1) The proposed secure sensor localization scheme is developed based on a reputation model and on the evaluation of all the beacon nodes for deriving a reputation value for each and every beacon node.
- (2) In the reputation model, the reputation of each beacon node is evaluated and consequently used by regular sensor nodes to determine the credibility of the location information provided by the beacon node.
- (3) In the reputation model, the reputation of each beacon node is updated continuously with the passage of time if sensor localization needs to be carried out from time to time.

In the following sections, we will first describe the network model followed by the threat model and the reputation model.

2.1. The Network Model. The WSN under consideration is composed of beacon nodes and regular sensor nodes. Beacon nodes are capable of positioning themselves (e.g., by determining their positions through GPS) while the regular sensor nodes need to locate their own positions based on position information from other nodes, especially from the beacon nodes.

Our sensor localization method in this paper requires that a regular sensor node first estimates its relative position to some of the beacon nodes through the means of receiving signals from credible beacon nodes and by computing the distances between them using a signal attenuation formula. Then, the sensor node estimates its position using the maximum likelihood estimation method [21] after it has collected enough position information.

2.2. The Threat Model. An analysis of the network model described above indicates that position information received from beacon nodes and the estimation of relative positions between a regular sensor node and the referenced beacon nodes can determine the accuracy of sensor localization. There are, however, two primary types of security threats for the network model as described below.

FIGURE 1: An example of sensor localization in hostile environments.

- (1) Sending false beacon information: if malicious beacon nodes send false position information, such information received by regular sensor nodes may not be accurate. Then, the estimated position of a regular sensor node cannot be guaranteed to be accurate and will lose its credibility because it is calculated based on received false information from beacon nodes. The impact to sensor localization from this type of attacks is shown in Figure 1. We can see from the figure that B'_2 is the false position of beacon node B_2 , which makes sensor node U_1 receive a false localization result U'_1 .
- (2) Obstructing physical property: if malicious nodes interfere with normal signals from beacon nodes, no regular sensor node would be able to estimate its relative position to the beacon nodes accurately by the means of signal attenuation, leading to reduced accuracy for sensor localization.

Consequently, the scheme that we propose in this paper needs to deal with the potential threats that result from the above two types of attacks in order to improve the accuracy of sensor localization in WSNs.

2.3. The Proposed Reputation Model. To deal with the above security threats, we propose a novel reputation model for sensor localization in WSNs. In the reputation model, beacon nodes evaluate each other using information such as the characteristics about the perception of positions and provide the evaluation results to the regular sensor nodes. The regular sensor nodes use the evaluation results provided by the beacon nodes to rank the beacon nodes and base the credibility of the location information provided by beacon nodes on such ranking.

First, let us make the following assumptions in our reputation model.

- (1) The reputation value for each and every beacon node is a number between 0 and 1, indicating values from the lowest to the highest reputations.

- (2) The reputation value for each and every beacon node is initialized to be 0.5, a medium value to start with.
- (3) In the reputation model, each beacon node performs evaluation only on its neighboring beacon nodes, that is, the beacon nodes that are one hop away from it.

Pseudocode 1 contains the pseudocode for our proposed reputation model for beacon node B_j and sensor node U_m .

The details of the evaluation procedure in the proposed reputation model are as follows.

- (1) Beacon node B_i sends its coordinate (x_i, y_i) to its neighboring beacon nodes.
- (2) Each neighboring beacon node to B_i will calculate its distance to B_i using the received coordinate information and the signal strength information independently. Let $l_{B_{ji}}$ denote the distance between B_j and B_i based on the coordinate information and let $d_{B_{ji}}$ denote the distance based on the signal strength information. B_j can then calculate $l_{B_{ji}}$ using the coordinate information from B_i and calculate $d_{B_{ji}}$ through a signal strength ranging algorithm based on the strength of the signals received from B_i .
- (3) All the neighboring beacon nodes evaluate the reputation of B_i . The value of reputation evaluation is determined using (1) in which $R_{B_{ji}}^t$ and $R_{B_{ji}}^{t+\Delta t}$ denote the reputation values on B_i by B_j at times t and $t + \Delta t$, respectively, and Δt denotes the time interval of two reputation values. Let Δd be the threshold for the distance, that is, the error that can be tolerated for the distance, and let α be the weight of the evaluation value which is determined using (2)

$$R_{B_{ji}}^{t+\Delta t} = \alpha \times R_{B_{ji}}^t + (1 - \alpha), \quad |l_{B_{ji}} - d_{B_{ji}}| \leq \Delta d \quad (1)$$

$$R_{B_{ji}}^{t+\Delta t} = (1 - \alpha) \times R_{B_{ji}}^t, \quad |l_{B_{ji}} - d_{B_{ji}}| > \Delta d,$$

$$\alpha = \frac{|l_{B_{ji}} - d_{B_{ji}}|}{l_{B_{ji}} + d_{B_{ji}}}. \quad (2)$$

- (4) The neighboring sensor nodes get the reputation values for B_i from the beacon nodes. Each regular sensor node collects the evaluation values from all the neighboring beacon nodes and computes the average reputation value using (3) in which $R_{U_m, B_i}^{t+\Delta t}$ and $R_{B_{ki}}^{t+\Delta t}$ denote the reputation value on beacon node B_i from a sensor node U_m and that on B_i evaluated by B_k at time $t + \Delta t$, where B_k is a neighboring beacon node to B_i and n is the number of such neighboring nodes. Consider

$$R_{U_m, B_i}^{t+\Delta t} = \frac{\sum_{k=1}^n R_{B_{ki}}^{t+\Delta t}}{n}. \quad (3)$$

- (5) Every regular sensor node ranks the neighboring beacon nodes from high to low based on the received reputation values.

3. The Sensor Localization Scheme

The sensor localization scheme in this paper uses the proposed reputation evaluation scheme described above in which the reputation model is relied upon by the beacon nodes to evaluate each other. In the illustration below, we use the RSSI ranging technology for sensor localization although the same reputation scheme can be applied equally to TOA, TDOA, and AOA ranging methods in practical applications.

After receiving the evaluation results, a regular sensor node will select credible beacon nodes based on the reputation values. Afterwards, the sensor node will measure the distance to the credible beacon nodes using the RSSI ranging technology and estimate its location through maximum likelihood estimation. The main steps in our localization scheme are described as follows.

- (i) Every beacon node provides its location information to all the neighbor nodes. As shown in Figure 2, beacon node B_1 sends its position coordinate (x_1, y_1) to all the neighboring nodes.
- (ii) Beacon nodes in the network will evaluate each other using the proposed reputation model and each will send its evaluation results to all the neighboring nodes. As shown in Figure 2, beacon nodes B_2, B_3, B_4 , and B_5 evaluate the reputation of B_1 after receiving the location information from B_1 using the proposed reputation model and each will send the evaluation result to their neighboring sensor nodes including node U_1 .
- (iii) Each regular sensor node will select credible beacon nodes based on the results from the reputation evaluation. Sensor node U_1 computes the reputation value for B_1 and collects the reputation values from neighboring beacon nodes using (3). Then, U_1 ranks the neighboring beacon nodes according to the reputation values in the order of high to low, based on which it selects the credible beacon nodes accordingly.
- (iv) Regular sensor nodes estimate their relative positions to the credible beacon nodes using the signal attenuation formula in RRSI [12].
- (v) Regular sensor nodes calculate their coordinates using maximum likelihood estimation. Suppose that the number of credible neighboring beacon nodes around U_1 is p with coordinates $(x_1, y_1), (x_2, y_2), \dots, (x_p, y_p)$, respectively, and the distances between $U_1(x_{U_1}, y_{U_1})$ and the beacon nodes are $d_1, d_2, \dots, d_p$, respectively; then the position of U_1 can be calculated using the following:

$$(x_{U_1} - x_i)^2 + (y_{U_1} - y_i)^2 = d_i^2, \quad i = 1, 2, \dots, p. \quad (4)$$

In addition, p distance equations about U_1 and the p beacon nodes are listed as in (5) that result from subtracting

```

// Beacon nodes evaluate each other between neighbor beacon nodes
 $R_{B_{ji}}^t = 0.5$ 
while(true)
     $\alpha = \frac{|l_{B_{ji}} - d_{B_{ji}}|}{l_{B_{ji}} + d_{B_{ji}}}$ 
    if  $|l_{B_{ji}} - d_{B_{ji}}| \leq \Delta d$ 
         $R_{B_{ji}}^{t+\Delta t} = \alpha \times R_{B_{ji}}^t + (1 - \alpha)$ 
    else
         $R_{B_{ji}}^{t+\Delta t} = (1 - \alpha) \times R_{B_{ji}}^t$ 
    sleep( $\Delta t$ )
// Beacon nodes send the reputation value to their neighbor sensor nodes
Send (node  $B_j$ , node  $U_m$ , reputation value)
// Sensor nodes compute the reputation value of their neighbor beacon nodes
 $R_{U_m, B_i}^{t+\Delta t} = \frac{\sum_{k=1}^n R_{B_{ki}}^{t+\Delta t}}{n}$ 

```

PSEUDOCODE 1: Pseudocode for the reputation model.

FIGURE 2: The network topology.

the last equation from each of the first $p - 1$ equations. Consider

$$\begin{aligned}
 & x_1^2 - x_p^2 - 2(x_1 - x_p)x_{U_1} + y_1^2 - y_p^2 \\
 & - 2(y_1 - y_p)y_{U_1} = d_1^2 - d_p^2 \\
 & \dots
 \end{aligned} \tag{5}$$

$$\begin{aligned}
 & x_{p-1}^2 - x_p^2 - 2(x_{p-1} - x_p)x_{U_1} + y_{p-1}^2 - y_p^2 \\
 & - 2(y_{p-1} - y_p)y_{U_1} = d_{p-1}^2 - d_p^2.
 \end{aligned}$$

$U_1(x_{U_1}, y_{U_1})$ can then be calculated using the following:

$$U_1 = A^{-1}b. \tag{6}$$

The matrices in (6) can then be expressed as the following expressions:

$$\begin{aligned}
 A &= 2 \begin{bmatrix} x_1 - x_p & y_1 - y_p \\ \dots & \dots \\ x_{p-1} - x_p & y_{p-1} - y_p \end{bmatrix}, \\
 b &= \begin{bmatrix} x_1^2 - x_p^2 + y_1^2 - y_p^2 - d_1^2 + d_p^2 \\ \dots \\ x_{p-1}^2 - x_p^2 + y_{p-1}^2 - y_p^2 - d_{p-1}^2 + d_p^2 \end{bmatrix}, \\
 U_1 &= \begin{bmatrix} x_{U_1} \\ y_{U_1} \end{bmatrix}.
 \end{aligned} \tag{7}$$

The final solution to (6) can be obtained using the following:

$$U = (A^T A)^{-1} A^T b. \tag{8}$$

From the above steps, we can see that a regular sensor node would treat the location information from neighboring beacon nodes differently according to the result of reputation evaluation. There is no need to determine the position relationship between regular sensor nodes and beacon nodes that have low reputation values, which are required in the signal attenuation formula, resulting in reducing a certain amount of computational overhead.

4. Simulation and Analysis

We have performed some simulation on wireless sensors localization with the proposed RBL to evaluate the performance of the scheme.

The network configuration for the simulation is set up as follows. The regular sensor nodes and beacon nodes are deployed randomly in an area of $650 \text{ m} \times 600 \text{ m}$. The transmission radius of each beacon and sensor node is set

FIGURE 3: Sensor localization error with a different number of malicious beacon nodes: (a) 10 normal and 5 malicious beacon nodes; (b) 10 normal and 10 malicious beacon nodes.

at 200 m. There exist some malicious beacon nodes that randomly send out false location information.

Localization error is one important indicator of the performance in sensor localization for WSNs, which is calculated using (9). In the formula, (x_{U_m}, y_{U_m}) and (x'_{U_m}, y'_{U_m}) denote the measured coordinates and the actual coordinates for node U_m , respectively, R denotes the transmission radius of the nodes, and e_m is the localization error. Consider

$$e_m = \frac{\sqrt{(x_{U_m} - x'_{U_m})^2 + (y_{U_m} - y'_{U_m})^2}}{R}. \quad (9)$$

The localization error from the simulation for 20 sensor nodes is shown in Figure 3. We can see from the figure that reputation evaluation is effective for reducing localization error in hostile environments and the improvement is more significant as the number of malicious beacon nodes increases.

There are two types of threats in sensor localization: attacks targeted at the nodes and attacks targeted at the location information. RBL evaluates the credibility of beacon nodes by evaluating the location information that beacon nodes provide in order to reduce the influence of compromised beacon nodes on localization results and to resist the threat of location information tampering by the malicious beacon nodes. To measure the capability of RBL on countering the above security threats, in our evaluation, we deploy 40 regular sensor nodes to expand the scale of our experiment in which we measure the average localization error using (10) where N denotes the number of regular sensor nodes in the network. The average localization error from our simulation on a network in which there exist one or more compromised beacon nodes is shown in Figure 4. We can see from the figure that although the average localization error fluctuates with the number and the locations of the regular sensor nodes,

the result of RBL is much better than that of the primary localization scheme (PLS) using RRSI in which no evaluation of beacon nodes is performed. Consider

$$\bar{e} = \frac{\sum_{i=1}^N e_i}{N}. \quad (10)$$

Since WSNs possess the characteristics of dynamic network topology, an advanced secure sensor localization scheme should not only be able to ensure the security of sensor localization in a static network, but also be able to handle the cases of nodes joining, leaving, and removing from the network. We have performed some simulations on sensor localization for the above scenarios.

In order to expand the coverage of beacon nodes in a network so as to make more regular sensor nodes the neighbors of the beacon nodes in the network, consequently improving the utilization of beacon information, we can increase the signal transmission power of the beacon nodes to effectively expand the signal transmission radius of the beacon nodes.

In the simulations, we first deploy 20 regular nodes and 4 normal beacon nodes in the area. Then, we add more beacon nodes into the network at the rate of one node per minute starting at the moment of 1.5 min with normal and malicious beacon nodes being added alternately. Malicious beacon nodes that are added into the network would send out false position information randomly while normal beacon nodes always send out their real position information. Figure 5 shows the average localization error for regular sensor nodes during the first seven minutes from which we can see that the average localization error for regular sensor nodes fluctuates noticeably in the primary localization scheme but exhibits a good performance in our proposed RBL.

We have also performed some simulations to evaluate the impact of nodes leaving the network on sensor localization.

FIGURE 4: Average sensor localization error with a varying number of regular sensor nodes.

FIGURE 6: Average sensor localization error as beacon nodes are removed from the network.

FIGURE 5: Average sensor localization error as beacon nodes are added into the network.

In the simulation, we first deploy 20 regular nodes, 4 normal beacon nodes, and 4 malicious beacon nodes in the area. Then, we remove the beacon nodes from the network at the rate of one node per 1 minute starting at the moment of 1.5 min with normal and malicious beacon nodes being removed alternately. Again, normal beacon nodes always claim their real positions while malicious beacon nodes would send out false position information randomly. Figure 6 shows the average sensor localization error for regular sensor nodes during the process from which we can see that the average localization error of RBL is noticeably lower than that of PLS in most cases. However, when the number of normal beacon nodes falls below three in the whole network,

TABLE 1: State situations for the beacon nodes.

Categories	1	2	3	4
Situations	$RP_1 \cap CP_2$	$RP_2 \cap CP_1$	$RP_2 \cap CP_2$	$RP_2 \cap CP_3$

the advantage would disappear, which seems to be a limitation of the current RBL.

Lastly, we evaluate the impact of status change among the existing beacon nodes on regular sensor nodes under the assumption that the total number of beacon nodes remains the same. Four possibilities exist for such status change as illustrated in Table 1 in which RP_1 and RP_2 represent the cases in which a beacon node does not change its real position and changes its real position, respectively, and CP_1 , CP_2 , and CP_3 represent the cases in which a beacon node does not change its claimed position information, changes its claimed position information randomly, and changes its claimed position information consistently, respectively.

We perform evaluations for four scenarios. In the first evaluation, we deploy 20 regular sensor nodes and 8 normal beacon nodes in the area and then change the status of 4 beacon nodes to the state that corresponds to situation 1 in Table 1 gradually during a 4-minute time period starting at the moment of 1.5 min. In the second evaluation, we deploy 20 regular sensor nodes and 8 normal beacon nodes in the area and then change the status of 4 beacon nodes to the state that corresponds to situation 2 in Table 1 gradually during a 4-minute time period starting at the moment of 1.5 min. In the third evaluation, we deploy 20 regular sensor nodes and 8 normal beacon nodes in the area and then change the status of 4 beacon nodes to the state that corresponds to situation 3 in Table 1 gradually during a 4-minute time period starting at the moment of 1.5 min. In the last evaluation, we deploy 20 regular sensor nodes and 8 normal beacon nodes in

FIGURE 7: Average sensor localization error as beacon nodes change their status in various scenarios.

the area and then change the status of 4 beacon nodes to the state that corresponds to situation 4 in Table 1 gradually during a 4-minute time period starting at the moment of 1.5 min.

Figures 7(a), 7(b), 7(c), and 7(d) show the results of the evaluations that correspond to the above four evaluation scenarios. We can see from the figure that RBL can effectively filter out abnormal (or malicious) beacon nodes when some of the beacon nodes change their status in an unpredictable manner, which demonstrates that RBL is an effective scheme for secure sensor localization for WSNs, which clearly shows that RBL can improve the accuracy of sensor localization in hostile or untrusted environments.

In summary, so far, we have performed three sets of simulation experiments to verify the performance and

the effectiveness of the proposed security scheme for sensor localization in hostile or untrusted environments. In the first one, we evaluated the performance of localizing regular sensor nodes in the presence of a varying number of malicious beacon nodes. In the second one, we evaluated the average sensor localization error for different numbers of regular sensor nodes in hostile or untrusted environment. In the third one, we evaluated sensor localization results; when new beacon nodes join the network, existing beacon nodes leave the network and existing beacon nodes change their status that determines how they would make claims on their positions. It is clear that the purpose of the last experiment is to evaluate the influence on the localization of regular sensor nodes due to changes on the credibility of the beacon nodes. That is, the first two experiments are

mainly aimed at showing the performance of RBL on secure sensor localization in static WSNs while the third one is aimed at verifying the effectiveness of RBL on secure sensor localization in dynamic WSNs. All the simulation results that we have obtained clearly show that RBL can reduce the effect of malicious beacon nodes on the localization of regular sensor node, thus allowing us to conclude that RBL can effectively improve the security and the accuracy of sensor localization in WSNs. The experiments also indicate that RBL can scale well with the size of the network and can be applied in dynamic WSNs, especially when new sensor nodes can join and existing sensor nodes can leave networks with the passage of time.

5. Conclusion

In this paper, we proposed a novel reputation model for regular sensor nodes to evaluate the credibility of beacon nodes in sensor localization. In the model, beacon nodes first evaluate each other and then provide the evaluation results to regular sensor nodes for them to determine the credibility of beacon nodes to ensure that they will receive and use credible position information from the beacon nodes in locating their own positions. The proposed security scheme can improve the accuracy of sensor localization in hostile or untrusted environments. The scheme can help to ensure the reliability of received location information under the scenario of signal attenuation by minimizing the effects of false location information as well as interfering signals caused by malicious beacon nodes.

In the future, we will extend our security scheme to counter other types of malicious attacks in sensor localization without incurring too much additional computational cost and communication overhead and to apply our reputation-based sensor localization scheme to different network environments to further verify and improve the scheme. We will also study the impact on evaluation due to other factors of sensor nodes to further improve the performance and usability of our secure sensor localization scheme in WSNs.

Notations

B_i :	Beacon node i
U_m :	Sensor node m
Δt :	The time interval of the two reputation values
$l_{B_{ji}}$:	The distance between beacon node j and i based on the coordinate information
$d_{B_{ji}}$:	The distance between beacon node j and i based on the ranging techniques (such as received signal strength indicator)
$R_{B_{ki}}^t$:	The reputation value on beacon node i from a beacon node k
R_{U_m, B_i}^t :	The reputation value on beacon node i from a sensor node m at time t
(x_p, y_p) :	The coordinate of beacon node p
(x_{U_m}, y_{U_m}) :	The coordinate of sensor node m .

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The work in this paper has been supported by National Natural Science Foundation of China (Grant no. 61272500) and Beijing Natural Science Foundation (Grant no. 4142008).

References

- [1] E. F. Golen, B. Yuan, and N. Shenoy, "An evolutionary approach to underwater sensor deployment," *International Journal of Computational Intelligence Systems*, vol. 2, no. 10, pp. 184–201, 2009.
- [2] J. C. Augusto, J. Liu, P. McCullagh, H. Wang, and J.-B. Yang, "Management of uncertainty and spatio-temporal aspects for monitoring and diagnosis in a smart home," *International Journal of Computational Intelligence Systems*, vol. 1, no. 4, pp. 361–378, 2008.
- [3] S.-K. Yang and K.-F. Ssu, "An energy efficient protocol for target localization in wireless sensor networks," *World Academy of Science, Engineering and Technology*, vol. 56, no. 8, pp. 398–407, 2009.
- [4] M. Boushaba, A. Hafid, and A. Benslimane, "High accuracy localization method using AoA in sensor networks," *Computer Networks*, vol. 53, no. 18, pp. 3076–3088, 2009.
- [5] R. Sugihara and R. K. Gupta, "Sensor localization with deterministic accuracy guarantee," in *Proceedings of the IEEE INFOCOM*, pp. 1772–1780, April 2011.
- [6] J. Park, Y. Lim, K. Lee, and Y.-H. Choi, "A polygonal method for ranging-based localization in an indoor wireless sensor network," *Wireless Personal Communications*, vol. 60, no. 3, pp. 521–532, 2011.
- [7] Y. W. E. Chan and B. H. Soong, "A new lower bound on range-free localization algorithms in wireless sensor networks," *IEEE Communications Letters*, vol. 15, no. 1, pp. 16–18, 2011.
- [8] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low-cost outdoor localization for very small devices," *IEEE Personal Communications*, vol. 7, no. 5, pp. 28–34, 2000.
- [9] H. Wu, M. Deng, L. Xiao, W. Wei, and A. Gao, "Cosine theorem-based DV-hop localization algorithm in wireless sensor networks," *Information Technology Journal*, vol. 10, no. 2, pp. 239–245, 2011.
- [10] I. Güvenç and C.-C. Chong, "A survey on TOA based wireless localization and NLOS mitigation techniques," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 3, pp. 107–124, 2009.
- [11] 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*, pp. 166–179, July 2001.
- [12] 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*, pp. 775–784, March 2000.
- [13] D. Niculescu and B. Nath, "Ad hoc positioning system (APS) using AOA," in *Proceedings of the 22nd Annual Joint Conference on the IEEE Computer and Communications Societies*, pp. 1734–1743, April 2003.

- [14] Y. Zhang, L. Bao, S.-H. Yang, M. Welling, and D. Wu, "Localization algorithms for wireless sensor retrieval," *Computer Journal*, vol. 53, no. 10, pp. 1594–1605, 2010.
- [15] S. Čapkun, K. B. Rasmussen, M. Čagalj, and M. Srivastava, "Secure location verification with hidden and mobile base stations," *IEEE Transactions on Mobile Computing*, vol. 7, no. 4, pp. 470–483, 2008.
- [16] H. Chen, W. Lou, and Z. Wang, "A novel secure localization approach in wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2010, pp. 1–12, 2010.
- [17] D. Liu, P. Ning, A. Liu, C. Wang, and W. K. Du, "Attack-resistant location estimation in wireless sensor networks," *ACM Transactions on Information and System Security*, vol. 11, no. 7, pp. 22–39, 2008.
- [18] T. Park and K. G. Shin, "Attack-tolerant localization via iterative verification of locations in sensor networks," *Transactions on Embedded Computing Systems*, vol. 8, no. 12, pp. 1–24, 2008.
- [19] 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.
- [20] X. Xu, H. Jiang, L. Huang, H. Xu, and M. Xiao, "A reputation-based revising scheme for localization in wireless sensor networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '10)*, pp. 1–6, April 2010.
- [21] R.-I. Rusnac and A. Ş. Gontean, "Maximum Likelihood Estimation Algorithm evaluation for wireless sensor networks," in *Proceedings of the 12th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC '10)*, pp. 95–98, September 2010.