Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2012, Article ID 732381, 11 pages
doi:10.1155/2012/732381

*Research Article*

# Secure Localization in Wireless Sensor Networks with Mobile Beacons

**Ting Zhang,[1] Jingsha He,[2] and Hong Yu[1]**

[1] *College of Computer Science, Beijing University of Technology, Beijing 100124, China*
[2] *School of Software Engineering, Beijing University of Technology, Beijing 100124, China*

Correspondence should be addressed to Ting Zhang, zhangting06@emails.bjut.edu.cn

Received 6 July 2012; Revised 4 September 2012; Accepted 4 September 2012

Academic Editor: An Liu



We present a scheme, called SLMB, for secure sensor localization in WSNs in which we propose to use a mobile beacon node with the goal of reducing the overall energy consumption in sensor nodes during sensor localization. In the SLMB scheme, a mobile beacon node traverses through the network, collects information from unknown sensor nodes, figures out position relationship with these nodes, and sends the information to the base station where analysis and location calculation is carried out to relieve unknown sensor nodes from energy-consuming computation. The proposed SLMB scheme is also designed to resist wormhole attacks, and localization is developed based on a mathematical model to design a path for the mobile beacon node to traverse in order to cover the entire sensor network. To evaluate our scheme, we have performed simulations to demonstrate that the SLMB scheme can improve the success rate and the accuracy of sensor localization compared to other sensor localization schemes in hostile environments. Our simulation results also show that the SLMB scheme consumes much less energy than traditional distributed sensor localization schemes, which is an important metric in measuring the effectiveness and usefulness of any schemes targeted for applications in WSNs.

## 1. Introduction

Sensor localization in wireless sensor networks (WSNs) is a fundamental technical issue, for it is critical for monitoring applications and for most location-based routing protocols and services. Therefore, in recent years, sensor localization has generated a great deal of interest in which researchers have considered various technical issues, such as efficiency [1], accuracy [2], and security [3] during sensor localization. Methods for the localization of wireless sensor nodes are generally classified into two types: range-based localization and range-free localization. The first type includes schemes in which positions of the unknown sensor nodes are calculated using measurement means to derive relevant information about distances and angles between sensor nodes [4]. The second type includes schemes in which positions of the unknown sensor nodes are estimated using connectivity information as well as multihop routing information to derive relevant information between sensor nodes [5].

In real applications, however, there may be other types of localization methods owing to 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 localization schemes to 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 localization schemes. Meanwhile, we should also consider the main constraints of wireless sensor networks such as constrained energy supply of the sensor nodes as well as the complexity of network environments in the development of effective localization methods.

Most existing localization algorithms, whether range-free or range-based, are distributed in nature in which unknown sensor nodes need to get position information about nearby beacon nodes so that they can calculate their own positions. The calculated position results are then sent to the base station or a central server to be used in real applications. One major drawback of such distributed localization algorithms is that it makes energy-constrained unknown sensor nodes

bear all the responsibility of communication and computation, resulting in high energy consumption in the sensor nodes. Another problem with such distributed algorithms is the increased security risks due to frequent communication between the sensor nodes.

In this paper, we propose a secure centralized sensor localization scheme by using a mobile beacon node (SLMB) to address the above-mentioned critical issues for WSNs and by developing some secure mechanisms to resist wormhole attacks in sensor localization. The proposed SLMB scheme has the following general features.

(1) It uses a mobile beacon node to travel along a calculated path in the network to collect information about the position relationship with nearby unknown sensor nodes. The collected information is then sent to the base station where the positions of the unknown sensor nodes are calculated, which can greatly lower the communication cost for the unknown sensor nodes.

(2) It takes a centralized approach so as to reduce the amount of calculation in the unknown sensor nodes by transferring the calculation work to the base station, which is a node in the network that is considered to be free from resource constraint.

(3) It calculates a reasonable mobile path for the beacon node to traverse so as to cover the entire network to ensure that every unknown sensor node can get connected to the mobile beacon node at some point of time so that necessary information can be collected for position calculation. The development of the mobile path follows the design principle of the cellular network and includes a quantitative method for the determination of efficient and necessary points for the mobile beacon node to visit for information collection.

(4) It includes some secure mechanisms to fight against wormhole attacks, thus improving the security of the centralized sensor localization algorithm in general.

The rest of this paper is organized as follows. In Section 2, we review some related work on sensor localization in WSNs. In Section 3, we present our centralized sensor localization scheme and describe some implementation and application issues. In Section 4, we describe the experiment we have performed to evaluate the proposed SLMB scheme and show some favorable simulation results in comparison to other localization methods. Finally, in Section 5, we conclude this paper in which we also discuss some future work.

## 2. Related Work

Existing sensor localization schemes can be generally classified into two types, that is, distributed and centralized schemes based on where calculation of sensor positions is performed in the localization process. In distributed localization, the unknown sensor nodes collect position information about nearby beacon nodes and calculate their own coordinates by themselves [6, 7]. That is, unknown sensor nodes are responsible for position calculation. In contrast, in centralized localization, beacon nodes collect the position information about unknown sensor nodes and send the information to the base station for data integration and position calculation [8, 9]. That is, the base station is responsible for position calculation.

Although distributed localization schemes have been widely popular, since in most WSNs, the number of beacon nodes is usually too limited, and the status of such nodes is too static to meet the needs of large WSNs. For these reasons, if an unknown sensor node wants to use beacon information more effectively, it may need to get the beacon information through multihop data transmission. In [10], the authors proposed a self-positioning algorithm that can run efficiently and independently at individual sensor nodes based on locally collected information. However, the requirement on the distance measurement error is quite strict. In [11], the authors proposed an algorithm and showed that even when only the connectivity information was given, the Euclidean distance between the estimated and the correct position of every unknown sensor node can be bounded and would decay at a rate that is inversely proportional to the radio range. However, this scheme incurs a larger amount of calculation in the unknown sensor nodes. In [12], the authors proposed a classic distributed localization scheme called DV-Hop based on distance vector routing. In DV-Hop, each unknown node needs to get the hop-count to the beacon nodes which estimate the average size for one hop between nodes in the network. Then the unknown nodes calculate their positions using the obtained information about the distances between the beacon nodes and themselves. DV-Hop can provide approximate positions for the nodes in a network where only a small fraction of nodes have self-positioning capability, but it requires more message exchanges between nodes in the network.

Due to energy constraint and thus limited life of sensor nodes, many researchers have proposed some centralized localization methods to reduce energy consumption through lowering computation and communication cost for the sensor nodes. Such localization approaches can bring significant benefits to applications, for it can extend the life of sensor nodes since most computations will now be completed at the central server or base station. In [13], the authors presented a multihop localization technique for WSNs by exploiting the strength indications of received signals. The proposed scheme aims at providing a solution for the localization of sensor nodes in static WSNs. In [14], the authors made some major modifications to improve the performance of the simulated annealing-based localization algorithm to increase localization accuracy. However, this type of localization schemes requires a large number of beacon nodes and involves complicated localization algorithms in order to complete the localization of all unknown sensor nodes in the network.

In order to overcome the shortcomings of requiring a large number of beacon nodes, in [15], some schemes based on mobile beacon nodes were proposed to transfer beacon information to help unknown sensor nodes in

performing self-localization. The problem is that some of the methods cannot be easily integrated into the centralized framework and some others lack methods for concise calculation of effective mobile beacon path. In [16], the authors demonstrated a range-free localization mechanism based on the location information from mobile beacons and on the principles of elementary geometry. But all the position calculation is still completed in the unknown sensor nodes, which makes it more like a distributed localization scheme. In [17], the authors proposed a novel mobile beacon-assisted localization algorithm based on network density clustering for WSNs by combining node clustering, incremental localization, and mobile beacon assisting together. Although this scheme is suitable for clustering large networks, it may not be suitable for networks that require faster convergence.

Some more research work has also be carried out to address security issues in sensor localization for WSNs. In [18], the authors improved the security and accuracy of sensor localization using location-based key distribution. In [19], the authors presented a novel defense mechanism against attacks in the DV-Hop localization algorithm. However, the security mechanisms proposed in these algorithms are not applicable to the mobile beacon scenario in WSNs.

In this paper, we introduce a mobile beacon node into centralized localization while improving the security of the scheme. In order to keep the computation cost and therefore the energy cost low for the sensor nodes, we propose a specific centralized localization scheme in which the mobile beacon node traverses the entire network following a well-designed path during which it stops at every collection point to collect position information from nearby unknown sensor nodes before moving to the next collection point. The mobile beacon node sends a position request at each collection point to nearby unknown sensor nodes, estimates the position relationship to these unknown sensor nodes based on received information and sends the information along with its own current position to the base station. It is the base station that will eventually complete all the position calculation.

The proposed SLMB scheme has the following obvious advantages.

(1) It can balance energy consumption of sensor nodes in the network, for it would prevent the sensor nodes that are closer to the base station from consuming excessive energy to deliver position information to the base station from far away sensor nodes in a multihop manner.

(2) It can improve localization accuracy as well as success rate compared to other similar schemes.

(3) It can improve the security of localization since securing only the beacon node should be much easier than securing a large number of unknown sensor nodes in the network.

(4) It can effectively reduce the communication overhead for the sensor nodes and overall transmission delay.

## 3. The Proposed Scheme

*3.1. The Network Model.* There are three types of nodes in the network model for our SLMB scheme. The first type includes the base station, which is capable of managing and integrating data for the entire network including the calculation of positions of unknown sensor nodes and the application of the results in real applications. The second type includes the mobile beacon nodes, which is capable of positioning themselves, traversing the network to collect information from unknown sensor nodes, and transmitting the collected information to the base station for position calculation. In addition, beacon nodes are mobile nodes that are assumed to have unlimited energy supply. The third type includes the unknown sensor nodes whose positions or locations in the network need to be determined through calculation based on collected information.

*3.2. The Localization Model.* The scheme that we propose is appropriate for applications and networks in which there is not enough stationary beacon nodes as position references for the unknown sensor nodes but localization still needs to be finished in time. In the proposed SLMB scheme, the information about the distribution of the unknown sensor nodes in the network can be obtained by using a mobile beacon node, and the positions of the unknown sensor nodes can be calculated quickly by the base station. In addition, in the SLMB scheme, we use a mathematical model to make the mobile beacon node follow a designated path to cover the entire network so as to improve the effectiveness and efficiency of sensor localization.

Following are the main steps of our centralized sensor localization algorithm, that is, the SLMB scheme.

(1) The mobile beacon node moves along a calculated path, sending position requests at every collection point to nearby unknown sensor nodes, collecting responses from unknown sensor nodes, and sending the collected information along with its current position to the base station.

(2) The mobile beacon node moves to the next collection point after completing the work at a previous collection point until it completes the traversal of the whole path to cover the entire network. The mobile beacon node can decide to aggregate information collected at more than one collection point before sending the collected information to the base station to further improve the performance of communication although energy consumption is not an issue under consideration.

(3) The base station integrates all the information received from the mobile beacon node and calculates the positions of all the unknown sensor nodes.

*3.3. The Mobile Path Model.* Mobility of the beacon node is required in our SLMB scheme. Consequently, the path that the mobile beacon node travels is very important for the performance of the scheme.

The purpose of using a mobile beacon node is to collect position information from unknown sensor nodes. Therefore, the path for the mobile beacon node to travel needs to meet the following two requirements.

(1) It must cover the entire network. Since sensor nodes in the network may be deployed randomly, the beacon node needs to connect to as many unknown sensor nodes as possible in order to improve the efficiency of localization.

(2) It must complete localization quickly. The path for the mobile beacon node to travel along should support efficient localization and make the number of collection points as minimal as possible.

The area that the mobile beacon node can effectively cover at anytime is modeled by a round area or circle with its present position as the center point and the signal transmission range as the radius. We can thus build a mathematical model to optimize the path that the mobile beacon node should follow as it traverses the entire network, which can be viewed and solved as the area coverage problem.

We assume that all sensor nodes in the network are deployed within a rectangular area, and the size of the area as well as the communication radius of the sensor nodes are known in advance. Our objective is to have the circles of the beacon node cover the entire rectangular area as it traverses through the network while keeping the overlapping regions of the circles as minimal as possible. This requires that with a collection of points $\{(x_{c_1}, y_{c_1}), (x_{c_2}, y_{c_2}), \ldots, (x_{c_n}, y_{c_n})\}$ that the mobile beacon node stops during its journey, for any arbitrary point $(x_o, y_o)$ that represents the position of an unknown sensor node, the following condition must be met: if $(x_o, y_o)$ is located in the rectangular network area, it must be covered by at least one circle of the mobile beacon node with a collection point of the mobile beacon node as the center and the signal transmission range as the radius.

From the above analysis, we can see that the circular areas that the mobile beacon node generates as it moves along a path could have some parts overlapping with each other in order to cover the entire rectangular area. Therefore, we have to make sure that the circles would cover each and every unknown sensor node deployed in the network while making the overlapping parts as small as possible, which is the basic principle in the design of the mobile path for the mobile beacon node to traverse and cover the entire network. When the overlapping areas of different circles are the same, the polygon that is constructed with the chords of each circle becomes straight polygons. We can thus transform the original area coverage problem of using circles to cover a rectangular area to the problem of using the polygons to cover a rectangular area.

**Lemma 1.** *The number of edges of a straight polygon for dividing a rectangle can only be 3, 4, or 6.*

*Proof.* We assume that the rectangle is covered by one or more straight polygons each of which has $p$ edges ($p \geq 3$). If $\alpha$ is the interior angle of the polygon, then $\alpha = (180^\circ(p - 2))/p$.

Let $q$ be the total number of polygons to which a vertex belong. Then, $q = 360^\circ/\alpha$. Since $q$ must be a natural number and $q$ can be calculated using

$$q = 360^\circ \cdot \frac{p}{180^\circ(p-2)} = \frac{2p}{p-2}. \tag{1}$$

Thus, $p$ can be calculated using

$$p = \frac{2q}{q-2} = \frac{2(q-2)+4}{q-2} = 2 + \frac{4}{q-2}. \tag{2}$$

From formula (2), we can get the following results:

$$\begin{cases} q = 3 \\ p = 6, \end{cases} \quad \begin{cases} q = 4 \\ p = 4, \end{cases} \quad \begin{cases} q = 6 \\ p = 3. \end{cases} \tag{3}$$

Therefore, the number of edges $p$ can only be 3, 4, or 6. The three specific coverage situations are demonstrated in Figure 1. In the figure, $S_c$ shows the overlapping part between two adjacent circles. Let $S_s$ and $S_t$ denote the area of the sector and that of the triangle, respectively. Thus, $S_c = 2(S_s - S_t)$. We can then use formula (4) to get $S_s$, $S_t$, and $S_c$, respectively, in which $\chi$ is the degree of the central angle of the sector, and $x$ is the percentage of $S_c$ over the circle.

$$\begin{aligned} S_s &= \left(\frac{\chi}{360^\circ}\right) \cdot \pi R^2, \\ S_t &= \frac{1}{2} R^2 \sin\chi, \\ S_c &= x\pi R^2. \end{aligned} \tag{4}$$

We can then derive

$$x\pi R^2 = 2\left(\left(\frac{\chi}{360^\circ}\right) \cdot \pi R^2 - \frac{1}{2} R^2 \sin\chi\right). \tag{5}$$

Thus, we get

$$x = 2\left(\frac{\chi}{360^\circ}\right) - \frac{\sin\chi}{\pi}, \tag{6}$$

when $p = 3, 4, 6$, $\chi = 120^\circ, 90^\circ, 60^\circ$, and $x = 0.39, 0.18, 0.06$, respectively.

It is thus clear that using straight hexagons to cover a rectangular area can achieve the highest efficiency, which coincides with the core idea of the honeycomb network principle.

We design the path for the mobile beacon node to travel as follows.

First, we need to determine the minimum number of circles to cover the rectangle with hexagons. Let's deduce the formulas for solving this problem.

Suppose the size of a rectangular area is $M * N$ and the communication radius of the wireless nodes is $R$. Let $m$ be the number of circles in one odd-numbered horizontal line, $n$ be the number of circles in one vertical line. Let $l$ and $d$ be the distances shown in Figure 1. We can thus calculate $l$ and $d$ by using

$$\begin{aligned} l &= 2 \cdot R \cdot \cos\frac{\pi}{6} = \sqrt{3}R, \\ d &= R \cdot \sin\frac{\pi}{6}. \end{aligned} \tag{7}$$

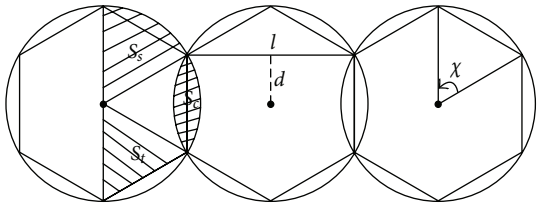



Figure 1: Relationship between the coverage areas with the mobile beacon node at different collection points.

Then, $n$ can be calculated using formulas (8) or (9) when it is an odd or an even number, respectively.

$$\left(\underbrace{\left(\frac{1}{2}+1\right)+1+2+1+2+\cdots+1+2+1}_{n-1}\right)R<N$$
$$\leq\left(\underbrace{\left(\frac{1}{2}+1\right)+1+2+1+2+\cdots+1+2+1+\left(1+\frac{1}{2}\right)}_{n}\right)R. \tag{8}$$

$$\left(\underbrace{\left(\frac{1}{2}+1\right)+1+2+1+2+\cdots+1+\left(1+\frac{1}{2}\right)}_{n-1}\right)R<N$$
$$\leq\left(\underbrace{\left(\frac{1}{2}+1\right)+1+2+1+2+\cdots+1+2+1}_{n}\right)R. \tag{9}$$

And $m$ can be calculated using

$$\sqrt{3}r\cdot(m-1)<M\leq\sqrt{3}r\cdot m. \tag{10}$$

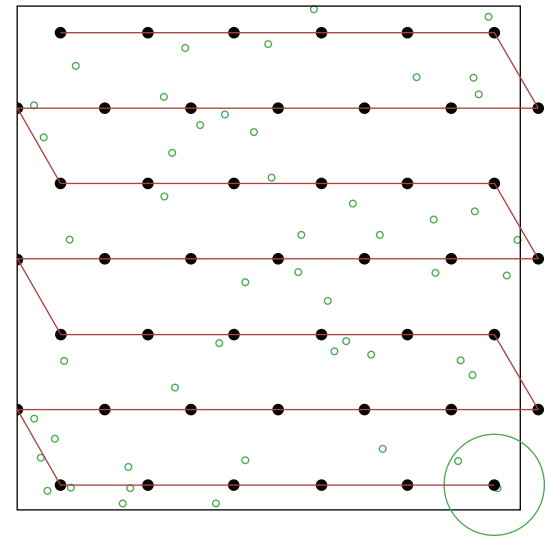
We are now ready to compute the minimum number of circles that can cover the entire rectangular network area through using formula (11) in which $P$ is the total number of collection points.

$$P=\begin{cases}n\cdot m+\dfrac{n-1}{2}, & n \text{ is an odd number.}\\ n\cdot m+\dfrac{n}{2}, & n \text{ is an even number.}\end{cases} \tag{11}$$

The path thus derived for the mobile beacon node to traverse and cover the entire network is shown in Figure 2. □

*3.4. Position Calculation.* The calculation of the position of each and every unknown sensor node is performed by the base station in our SLMB scheme, which is different from the traditional range-based localization methods in order to reduce the convergence time of localization as well as the cost of information collection by the mobile beacon node. Most existing range-based localization methods need multiple measurement points to measure the distances to unknown sensor nodes, whether they are based on the means of arrival time, signal strength, or angle. In the SLMB scheme, we combine the measurements of angle and arrival time to determine the distances so as to reduce the requirement on the number for collection points. As shown in Figure 3, the mobile beacon node can sense the directional angle $\theta$ of received messages from an unknown sensor node using an antenna array and, at the same time, measure the distance to the same node using time information in the messages. Then, the position of the unknown sensor node can be calculated using both pieces of information.

Since there are only a limited number of collection points, the measurement in the proposed SLMB scheme may incur errors. As shown in Figure 3 in which the angle error is $\pm\Delta\theta$ and the range error is $\pm\Delta d$, we take the centroid of the area with angle interval $\{(\theta-\Delta\theta),(\theta+\Delta\theta)\}$ and length interval $\{(d-\Delta d),(d+\Delta d)\}$ as the position of the unknown sensor node.



○ Unknown nodes
● Collection points for the beacon nodes

Figure 2: Mobile path for the mobile beacon node.

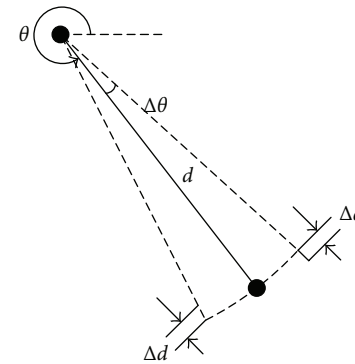



Figure 3: Position relationship between the mobile beacon node and a to-be-located unknown sensor node.

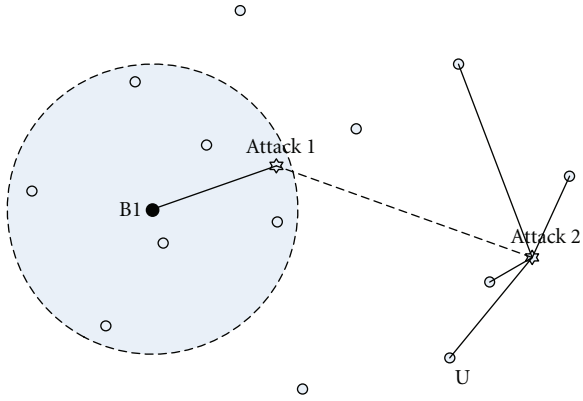



Figure 4: The wormhole attack model.

*3.5. The Security Mechanism.* Wormhole attacks are the primary type of attacks that can be launched without compromising any cryptographic keys. It can cause serious consequences to localization, especially when the beacon node wakes up the neighboring unknown sensor nodes through a localization request and when an unknown sensor node responds to the request. A communication channel between two attackers is shown in Figure 4 from which we can see that attack1 can transmit a request from B1 to the unknown sensor nodes that are outside of the coverage area of B1. The communication channel can also be used to replay the response of U to B1.

In order to detect information that is replayed from outside of the normal communication range, when the beacon node receives some information from the same unknown sensor node at different collection points, the beacon node should check whether one position information has been received repeatedly from the same exit of a wormhole, then compare the distances of the repeated positions $d$ with the threshold $T$. If $d \leq T$, it means that this is a normal error caused by the overlapping area of the two collection points. If $d > T$, it could mean an attack. If the wormhole attack is launched against just one node, the beacon node is not able to determine the location of the attacker. However, if the wormhole attack is launched towards multiple nodes, the attacker could be detected according to the wormhole attack filtering principle that is based on the same exit.

In addition, the beacon node may also receive messages with the same ID of an unknown sensor node since the replayed information is within the same communication radius. According to the signal transmission characteristics, we will only accept the first received information, discard the latter ones, and include it in the blacklist since the replayed information couldn't arrive at the object earlier than the original signal with the same transmission power.

*3.6. Application Issues.* The SLMB scheme has been designed to make sure that the mobile beacon node fully covers the entire deployment area, thus making it suitable for static WSNs. In dynamic WSNs in which the location of a sensor node may change from time to time due to mobility or the network environment, the SLMB scheme can be enhanced so that the mobile beacon node will periodically traverse the network to calculate and update the information on sensor locations. The interval between repeated SLMB applications can follow a strategy that can be determined based on application requirements as well as network environments. In addition, we can also adapt the basic SLMB scheme for huge WSNs by dividing the sensor deployment area into multiple regions and then deploying multiple mobile beacon nodes in the area with each for a different region to meet the real-time requirement of sensor localization. The model allows us to derive satisfactory localization results by making each beacon node cover minimum number of collection points with particular time constraints to achieve desired performance for sensor localization.

As it has been widely known, the application of WSNs has now spread to a lot of different areas including those in harsh environments such as battlefields and wildlife monitoring as well as many emerging applications in our daily life. Both distributed and centralized sensor localization schemes have their distinctive strengths and weaknesses to deal with different application scenarios. In a harsh environment where it is almost impossible for human beings to get near the sensors, a remotely controlled wireless mobile device can be used to traverse the deployment area acting as the beacon node to accomplish the functionality of sensor localization. If there are mountains and hills in the deployment area, we can manage to map the three-dimensional area into our two-dimensional model and thus still use a wireless flying device to collect location information from the sensor nodes. If sensor nodes are deployed in a well-developed area, a vehicle can be operated to move along a designated route to cover the entire deployment area to collect location information from the sensor nodes. In extreme situations where it is not feasible to use a mobile device as the beacon, distributed sensor localization algorithms should be considered as a complementary scheme. As WSNs find more and more diverse applications ranging from traditional applications to the Internet of Things scenario, there are certainly many applications in which our SLMB scheme can be used to perform sensor localization to achieve a wide variety of performance objectives.

We also would like to note that the proposed SLMB scheme is appropriate for WSNs that do not have a too high requirement on the accuracy of localization. To improve the accuracy of localization though, we can increase the number of collection points for the mobile beacon node to collect more position information about unknown sensor nodes and calculate the positions of the unknown sensor nodes through maximum likelihood estimation, which is a future work in our research in which we will demonstrate how accuracy improves along with the increase in the number of collection points. This is a tradeoff between accuracy and required completion time in addition to some other considerations such as the cost of communication and computation.

## 4. Simulation and Analysis

*4.1. Performance on Sensor Localization.* We have performed several simulations to evaluate the performance of

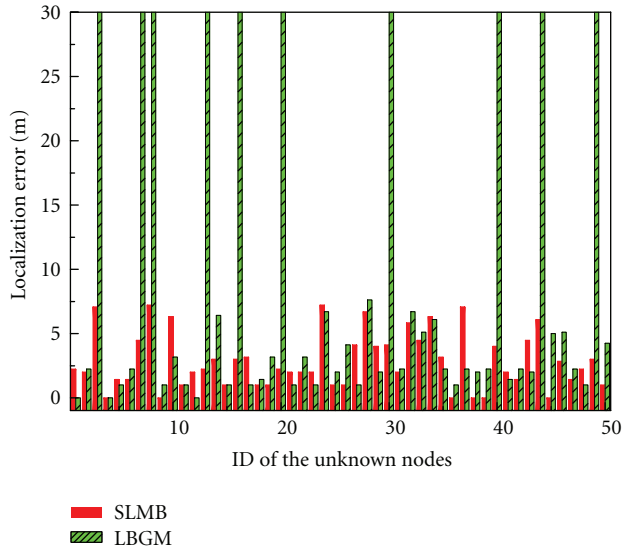



Figure 5: Comparison of localization errors.

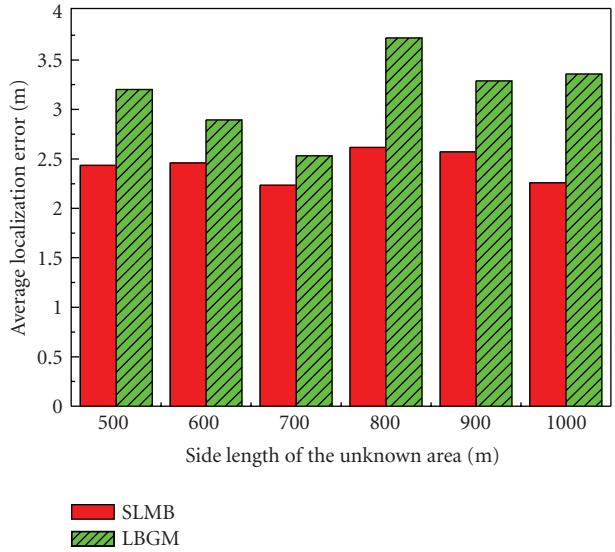



Figure 6: Average localization error of unknown sensor nodes for various network sizes.

the proposed SLMB scheme on sensor localization. The network configuration for our first simulation is set up as follows: there are 50 unknown sensor nodes and a mobile beacon node deployed randomly in an area of $800 \times 800\,\text{m}^2$. The transmission range $R$ of the wireless nodes is set up to be 100 m. The distance error and angle error between the mobile beacon node and any unknown sensor node are set up in the range of 0–0.05 and 0–$0.05 * \pi$, respectively.

We compare localization error between our proposed SLMB scheme and a localization scheme based on the general mobile path (LBGM). Localization error is an important metric to measure the performance of sensor localization in WSNs, which is the distance between localization coordinates and the actual coordinates calculated using (12) in which $(x_U, y_U)$ and $(x'_U, y'_U)$ denote the measured and the actual coordinates of unknown sensor node $U$, respectively.

$$e_U = \sqrt{(x_U - x'_U)^2 + (y_U - y'_U)^2}. \tag{12}$$

The simulation results on localization error for 50 unknown sensor nodes are shown in Figure 5 from which we can see that there are several unknown sensor nodes that have an localization error of infinite value, which means that these nodes cannot be located using the LBGM scheme. Our proposed SLMB scheme is shown to be more effective, for it can improve the success rate of localization of unknown sensor nodes for about 20% while reducing localization errors in general.

Since there are a variety of applications that need the location information about deployed sensor nodes but sensors may be different, it is worthwhile to investigate the performance of the proposed SLMB scheme for different network sizes in terms of coverage area and for different transmission ranges of the sensor nodes. We hereby use the notion of average localization error in evaluating our SLMB scheme using (13) in which $N$ denotes the number of unknown sensor nodes in a network as follows:

$$\bar{e} = \frac{\sum_{i=1}^{N} e_i}{N}. \tag{13}$$

We first investigate the effect of network size on sensor localization. In the evaluation, 100 unknown sensor nodes and a mobile beacon node are deployed in the network, the network is set up to cover an area of $500 * 500\,\text{m}^2$, $600 * 600\,\text{m}^2$, $700 * 700\,\text{m}^2$, $800 * 800\,\text{m}^2$, $900 * 900\,\text{m}^2$, and $1000 * 1000\,\text{m}^2$, respectively, and $R$ is set up to be 100 m. The distance error and angle error between the mobile beacon node and any unknown sensor node are also set up in the range of 0–0.05 and 0–$0.05 * \pi$, respectively.

The average localization error of the unknown sensor nodes using the proposed SLMB scheme and that using the LBGM scheme are shown in Figure 6 and the success rates of localization of these two schemes are shown in Figure 7. From these two figures, we can see that our SLMB scheme is more effective in covering the entire network area and in improving the accuracy of localization of unknown sensor nodes.

We then investigate the effect of transmission range of the nodes on localization. In the evaluation, 100 unknown sensor nodes and a mobile beacon node are deployed in a network area of $600 * 600\,\text{m}^2$, and the transmission range of the wireless nodes is set up to be 50 m, 60 m, 70 m, 80 m, 90 m, and 100 m, respectively. The distance error and angle error between the mobile beacon node and unknown sensor nodes are also set up in the range of 0–0.05 and 0–$0.05 * \pi$, respectively. The average localization errors for the 100 unknown sensor nodes using the proposed SLMB and the LBGM schemes as well as the localization success rates are shown in Figures 8 and 9, respectively. From these two figures, we can see that the SLMB scheme can achieve better performance both on localization accuracy and on

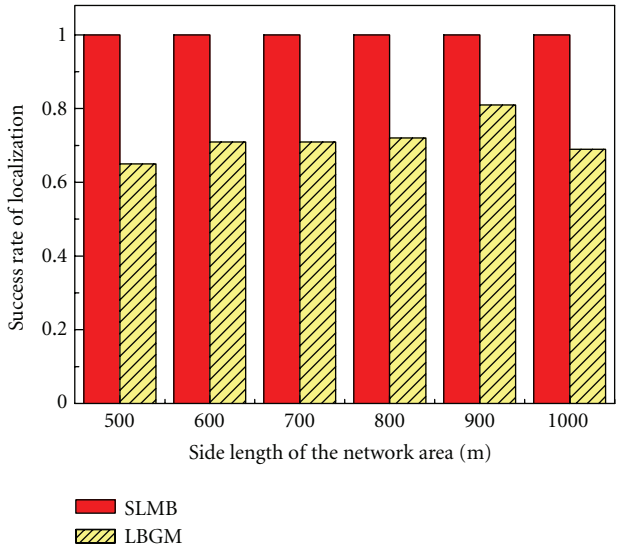



Figure 7: Success rate of sensor localization for various network sizes.

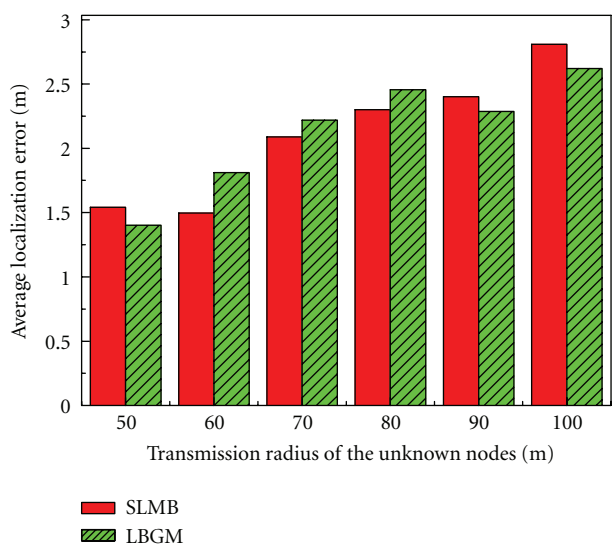



Figure 8: Average localization error of unknown sensor nodes for various transmission radiuses.

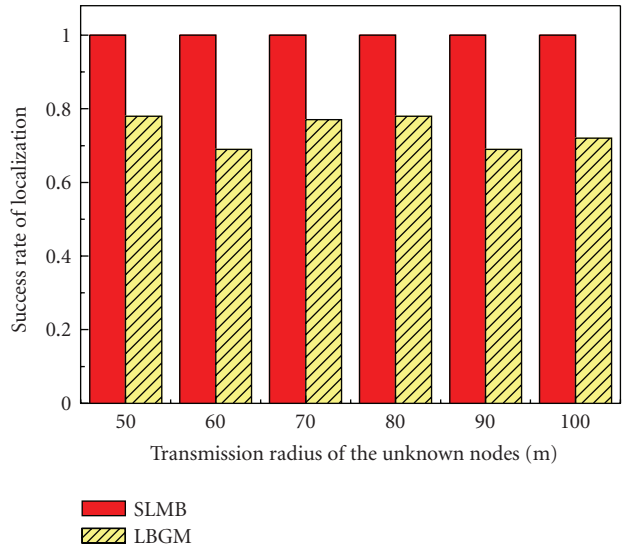



Figure 9: Success rate of localization for various transmission radiuses.

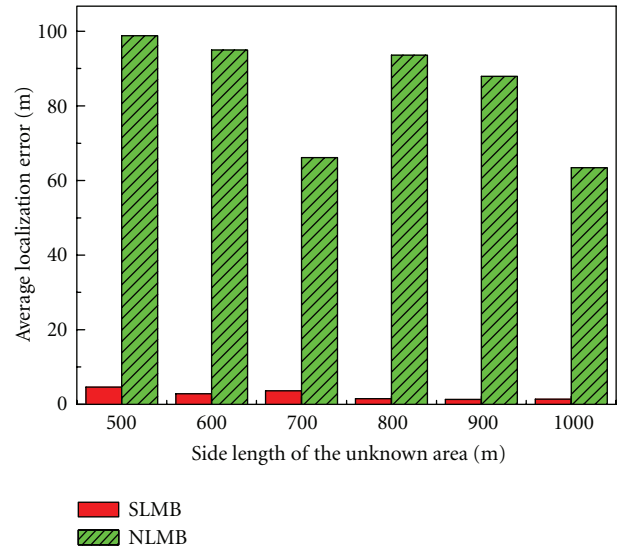



Figure 10: Average localization error for various network sizes in a hostile environment.

localization success rate with very stable results. The reason for the small difference shown in Figure 8 in localization accuracy between SLMB and LBGM is that it only includes the simulation results of those nodes that can be successfully located.

Finally, we investigate the performance of the SLMB scheme in terms of its ability of resisting against wormhole attacks. We randomly distribute two pairs of wormhole attackers in the experiment environments that we set up above for various network sizes and different transmission radiuses. The average localization errors of the unknown sensor nodes under these two environments are shown in Figures 10 and 11, respectively, from which, we can see that the SLMB scheme is able to fight against wormhole attacks, thus improving the localization accuracy for WSNs compared to normal localization by using a mobile beacon (NLMB).

*4.2. Performance on Energy Consumption.* Batteries are usually used to supply power in the sensor nodes in WSNs, and a sensor node is considered to be no longer functional when the battery in the node is exhausted. Therefore, the efficiency of energy usage must be considered in any protocol design for WSNs. The energy consumption of a sensor node mainly consists of energy consumption for data transmission and that for data processing. We now analyze the performance

of SLMB with respect to energy consumption and compare it to DV-Hop [12], a classic distributed sensor localization method.

First, let us develop an energy consumption model for the proposed SLMB scheme. In our model, the operations in each sensor node that consumes energy include data transmission, data reception, and position calculation, and the energy consumed for each of these operations is denoted as $E_s$, $E_r$, and $E_c$ in which it is widely recognized that $E_s$ and $E_r$ are normally much higher than $E_c$. The total amount of energy consumed by each sensor node can then be calculated using Formula (14) in which $E_s$ and $E_r$ can be calculated using formulas (15) and (16), respectively. In all the formulas, $k_1$ and $k_2$ denote the number of bits that have been sent and received, respectively, during sensor localization and $E_0$ denotes energy consumption for sending or receiving a single bit of data. Energy consumption for sending a message includes two parts; one is calculated based on the amount of data sent and the other is on the distance between the sender and the receiver that we denote as $E_{s1}$ and $E_{s2}$, respectively, and $d$ is the distance and $x$ a constant multiplier.

$$E = E_s + E_r + E_c, \tag{14}$$

$$E_s = E_{s1} + E_{s2} = E_0 * k_1 + x * k_1 * d^2, \tag{15}$$

$$E_r = E_0 * k_2. \tag{16}$$

In our SLMB scheme, we assume that the amount of data is fixed and is the same for every message sent and received and that any data that is sent by a node can be received by all the neighboring nodes within the radius of the communication of the sending node. We now compare the performance on energy consumption of SLMB to that of DV-Hop. In DV-Hop, an unknown sensor node needs to transmit localization information through multiple hops and calculates its position coordinates by itself.

The network configuration for our simulation on energy consumption is set up as follows: 500 unknown sensor nodes are deployed randomly in an area of $500 \times 500\,\text{m}^2$; the transmission range $R$ of the wireless nodesis assumed to be 50 m. We can then get $E_0 = 50\,\text{nj/bit}$ and $x = (0.1\,\text{nj/bit})/m^2$. The localization results may also need to be updated in some applications. Thus, we evaluate the performance on energy consumption for multiple applications of sensor localization, and the results for the accumulative energy consumption are shown in Figure 12. We now investigate the energy consumption for varying numbers of unknown sensor nodes in the network, and the results are shown in Figure 13.

We can see from the above evaluation that energy consumption in SLMB is much smaller than that in DV-Hop. SLMB can keep energy consumption at a very low level with various numbers of unknown sensor nodes, especially for some networks in which multiple applications of sensor localization are needed. Under both circumstances, our proposed SLMB scheme achieves a much better performance on energy consumption. Another obvious advantage of the SLMB scheme is that it not only can lower energy consumption in each sensor node, but it can also keep energy consumption evenly across all the unknown sensor nodes in the network, thus preventing some unknown sensor node from exhausting energy prematurely and becoming unusable before some others and, as a result, prolonging the life of the network. The main factors that lead to the improved performance are that the SLMB scheme has been designed to achieve the goals of reducing the number of data transmissions, making the unknown sensor nodes in the network transmit messages with same amount of data and same signal strength, all contributing to significant reduction in the total amount of energy consumed in unknown sensor nodes for the functionality of sensor localization.

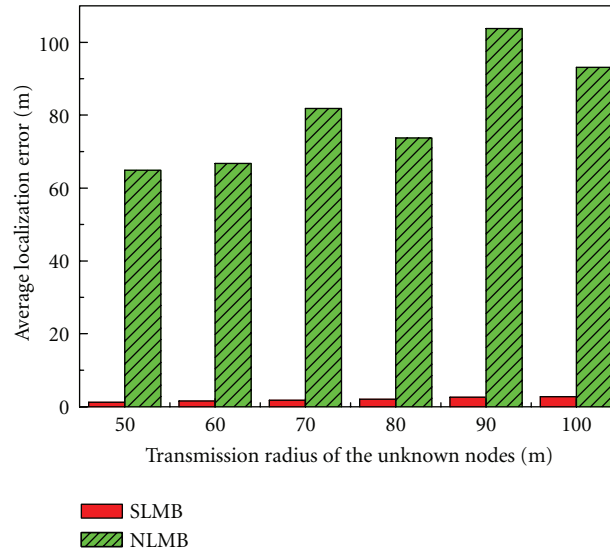



Figure 11: Average localization error for various transmission radiuses in a hostile environment.

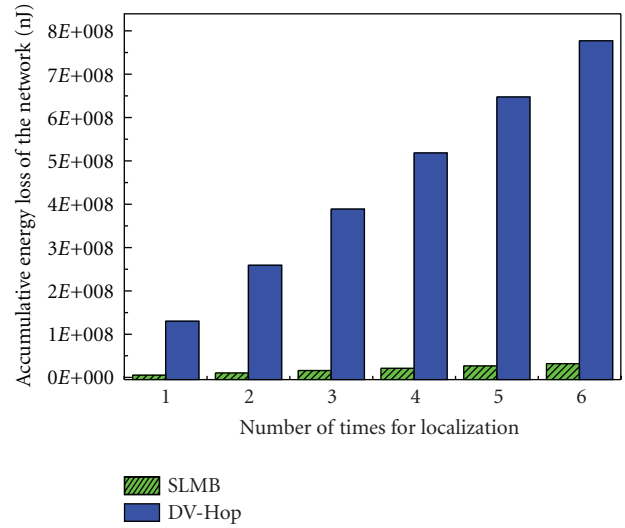



Figure 12: Accumulative network energy consumption for multiple applications of sensor localization.

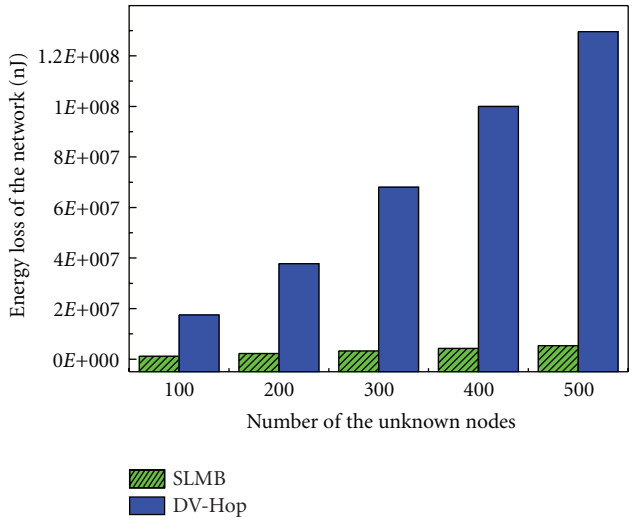



Figure 13: Network energy consumption for varying numbers of unknown sensor nodes in the network.

## 5. Conclusions

In this paper, we presented a secure centralized localization scheme by using a mobile beacon node. In the scheme, the mobile beacon node is responsible for collecting information about position relationship with unknown sensor nodes and for sending the information to the base station where the positions of the unknown sensor nodes are calculated. The scheme can greatly reduce the computation cost compared to distributed localization algorithms and lower the communication overhead for sending position information to the base station compared to some other centralized localization algorithms for the unknown sensor nodes. In the scheme, most work on collecting and sending information is done by the mobile beacon node, thereby also reducing the security risks in sensor localization. Specifically, the proposed scheme is designed to resist wormhole attacks in localization to improve the security. The scheme also includes a mathematical computation model to determine the collection points for the mobile beacon node to completely and efficiently cover the entire sensor network. The proposed scheme only requires that the beacon node to have an antenna array.

In the future, we will extend our secure localization scheme to improve the security of localization in the presence of other kinds of malicious attacks without incurring too much computational overhead and communication cost. We will also investigate the performance of sensor localization schemes that use different mobile beacon paths, different types of deployment, and different transmission radius for the sensor nodes.

## Acknowledgment

This work is supported by National Natural Science Foundation of China (61272500).

## References

[1] S. K. Yang and K. F. Ssu, "An energy efficient protocol for target localization in wireless sensor networks," *Proceedings of World Academy of Science, Engineering and Technology*, vol. 56, pp. 398–407, 2009.

[2] 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.

[3] R. Sugihara and R. K. Gupta, "Sensor localization with deterministic accuracy guarantee," in *Proceedings of IEEE Conference on Computer Communications (INFOCOM '11)*, pp. 1772–1780, April 2011.

[4] 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.

[5] 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.

[6] K. Langendoen and N. Reijers, "Distributed localization in wireless sensor networks: a quantitative comparison," *Computer Networks*, vol. 43, no. 4, pp. 499–518, 2003.

[7] M. Karakaya and H. Qi, "Distributed target localization using a progressive certainty map in visual sensor networks," *Ad Hoc Networks*, vol. 9, no. 4, pp. 576–590, 2011.

[8] A. Karbasi, "From centralized to distributed sensor localization," in *Proceedings of Annual International Conference on Mobile Computing and Networking (MOBICOM '10)*, pp. 5–7, September 2010.

[9] M. Simek, D. Komosny, R. Burget, P. Moravek, and R. Silva, "Centralized boundary discovery algorithms for anchor-free localization in wireless sensor networks," in *Proceedings of the International Conference on Ultra Modern Telecommunications and Workshops (ICUMT '09)*, pp. 1–7, October 2009.

[10] S. Zhu and Z. Ding, "Distributed cooperative localization of wireless sensor networks with convex hull constraint," *IEEE Transactions on Wireless Communications*, vol. 10, no. 7, pp. 2150–2161, 2011.

[11] A. Karbasi and S. Oh, "Distributed sensor network localization from local connectivity: performance analysis for the HOP-TERRAIN algorithm," in *Proceedings of the ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems (SIGMETRICS'10)*, pp. 61–70, June 2010.

[12] D. Niculescu and B. Nath, "DV based positioning in ad hoc networks," *Telecommunication Systems*, vol. 22, no. 1–4, pp. 267–280, 2003.

[13] C. Alippi and G. Vanini, "A RSSI-based and calibrated centralized localization technique for wireless sensor networks," in *Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, pp. 301–305, March 2006.

[14] M. Shahrokhzadeh, A. T. Haghighat, and B. Shahrokhzadeh, "An efficient centralized localization method in wireless sensor networks," in *Proceedings of the 17th International Workshop on Energy-Aware Communications (EUNICE '11)*, vol. 6955 of *Lecture Notes in Computer Science*, pp. 217–220, September 2011.

[15] E. C. Kim and K. Kim, "Distance estimation with weighted least squares for mobile beacon-based localization in wireless sensor networks," *IEEE Signal Processing Letters*, vol. 17, no. 6, pp. 559–562, 2010.

[16] K. F. Ssu, C. H. Ou, and H. C. Jiau, "Localization with mobile anchor points in wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 54, no. 3, pp. 1187–1197, 2005.

[17] F. Zhao, H. Y. Luo, and Q. Lin, "An mobile beacon-assisted localization algorithm based on network-density clustering for wireless sensor networks," in *Proceedings of the 5th International Conference on Mobile Ad-hoc and Sensor Networks (MSN '09)*, pp. 304–310, December 2009.

[18] Q. Mi, J. A. Stankovic, and R. Stoleru, "Practical and secure localization and key distribution for wireless sensor networks," *Ad Hoc Networks*, vol. 10, no. 6, pp. 946–961, 2012.

[19] N. Labraoui, M. Gueroui, and M. Aliouat, "Secure DV-Hop localization scheme against wormhole attacks in wireless sensor networks," *European Transactions on Telecommunications*, vol. 23, no. 2012, pp. 303–316, 2012.