Secure and Lightweight Localization Method for Wireless Sensor Networks*

Myung-Ho PARK†, Ki-Gon NAM††, Jin Seok KIM†, Dae Hyun YUM†††, Nonmembers, and Pil Joong LEE††††, Member

SUMMARY With the increased deployment of wireless sensor networks (WSNs) in location-based services, the need for accurate localization of sensor nodes is gaining importance. Sensor nodes in a WSN localize themselves with the help of anchors that know their own positions. Some anchors may be malicious and provide incorrect information to the sensor nodes. In this case, accurate localization of a sensor node may be severely affected. In this study, we propose a secure and lightweight localization method. In the proposed method, uncertainties in the estimated distance between the anchors and a sensor node are taken into account to improve localization accuracy. That is, we minimize the weighted summation of the residual squares. Simulation results show that our method is very effective for accurate localization of sensor nodes. The proposed method can accurately localize a sensor node in the presence of malicious anchors and it is computationally efficient.

key words: security, wireless sensor networks, secure localization, algorithms

1. Introduction

Wireless sensor networks (WSNs) have recently received considerable attention with the proliferation in Micro-Electro-Mechanical Systems (MEMS) technology, which has facilitated the development of smart sensors. These sensors, which may be deployed into the field in an ad hoc manner, are small, with limited processing and computing resources, and they are less expensive than traditional sensors. A WSN consists of a number of sensor nodes (a few tens to thousands), and it has been used in many applications such as military target tracking and surveillance, natural disaster relief, biomedical health monitoring, and hazardous environment exploration and seismic sensing [1].

One of the key challenges in a WSN is ascertaining the physical locations of the sensor nodes. This location information is used to route packets using geometric-aware routing, or to annotate the sensory data with geographic location relating where the data were collected. For secure localization of a sensor node, all the sensor nodes in the WSN can be equipped with a global positioning system (GPS). However, this solution is costly, consumes high power, and requires large volume. Most other localization methods can be grouped into two categories: range-free methods and range-based methods. In range-free methods [2], [3], network connectivity is used to proximate node locations. Although these methods can be used even when the internode distance information is not available, they are not as accurate as range-based methods and often require extensive messaging between the nodes.

In range-based methods, a few anchor nodes equipped with the GPS are aware of their own positions and the remaining sensor nodes localize themselves using the distance estimates obtained from the anchors. There are two approaches in range-based methods. One approach is based on the trilateration method. Savvides et al. [4] presented the least-squares (LS) method for estimating the locations of the sensor nodes by minimizing the summation of the residual squares. The advantage of the LS method is that it is lightweight, i.e., its computational cost is low. Li et al. [5] proposed the least-median-squares (LMS) method for achieving better accuracy in the presence of malicious anchors. They minimized the median of the residual squares instead of the summation of the residual squares. The LMS method performs better than the LS method against non-colluding malicious anchors. If malicious anchors work cooperatively, the LS method shows a better performance for short lying distances and the LMS method is more accurate for long lying distances. A drawback of the LMS method is its high computational cost (when compared with the LS method). The other approach is based on maximum likelihood techniques. Maximum likelihood problems can be solved by convex optimization [6], [7]. Although this approach has better accuracy than the trilateration approach, it cannot be applied to WSNs because of the large memory required and the high power consumption for computation. Practically, in a WSN, sensor nodes are severe constraints on the computation power and memory. Therefore, this sophisticated optimization approach is not practicable for WSNs [8].

In this paper, we propose a secure and lightweight lo-
localization method for WSNs, which belongs to range-based methods with the trilateration method. Generally, distance measurements performed on sensor nodes are inexact, and their variances are not constant across individuals, that is, as the distance increases, its measurement error also increases. However, previous localization methods such as the LS and the LMS methods implicitly assume that the measurements have a constant error variance. In order to enhance the accuracy of localization of sensor nodes, we take the variance of the measurements into account. We assign high weights to measurements by near anchors and low weights to those by distant anchors. Mathematically, we minimize the weighted summation of the residual squares. When malicious anchors do not collude, our proposed method shows better accuracy than the LS and the LMS methods. When malicious anchors collude, the proposed method has the best accuracy for short lying distances. Moreover, the proposed localization method is computationally efficient: although the computational resources in the proposed method and the LS method are almost the same, the proposed method has much lower computational complexity than does the LMS method.

The remainder of this paper is organized as follows. Section 2 presents the system model, Sect. 3 proposes the localization method, Sect. 4 reports the simulations performed to characterize the performance of our method, and Sect. 5 concludes the paper.

2. System Model

A WSN can be modeled as a collection of points in 2-D Euclidean space, where each point represents an anchor node or a sensor node. Each anchor \( A_i \) (for \( i = 1, \ldots, n \)) is fixed after deployment, and it knows its own position. All communications between the anchors and a sensor node are bidirectional, and error-resilient encoding is used in the physical layer to make the wireless communication error-free. The error proportion in the measurement of the distance between \( A_i \) and a sensor node \( S_t \) is given as \( \epsilon_i \), where \( \epsilon_i \) is a Gaussian random variable with zero mean and variance \( \sigma_i^2 \) and all \( \epsilon_i \) (for \( i = 1, \ldots, n \)) values are independent of each other. The variance \( \sigma_i^2 \) is a known system parameter. Let \( d_{it} \) be the true distance between \( A_i \) and \( S_t \). If \( S_t \) obtains a distance estimate \( \hat{d}_{it} \) from a truthful anchor, then

\[
\hat{d}_{it} = d_{it} \cdot (1 + \epsilon_i) \quad (1)
\]

holds true. \( A_i \) may lie to \( S_t \) about the distance between \( A_i \) and \( S_t \), with the lying proportion given by \( \theta_i \). Thus, the incorrect distance measurement of \( S_t \) is given by

\[
\hat{d}_{it} = d_{it} \cdot (1 + \epsilon_i) \cdot (1 + \theta_i) \quad (2)
\]

where if \( \theta_i = 0 \), then \( A_i \) is truthful; otherwise, \( A_i \) is malicious. If malicious anchors collude with one another, they effect localization in the same wrong direction; otherwise, they falsify the measurement of \( S_t \) with the random lying proportion \( \theta_i \).

3. Proposed Localization Method

Let the position of \( A_i \) be \((x_i, y_i)\), the position of \( S_t \) be \((x_0, y_0)\), and the number of anchors in the communication range of \( S_t \) be \( N \). From Eq. (1), we find that the distance measurements \( \hat{d}_{it}^2 \) for \( i = 1, \ldots, N \) are

\[
\hat{d}_{it}^2 = [(x_i - x_0)^2 + (y_i - y_0)^2] \cdot (1 + \epsilon_i)^2
= [(x_i - x_0)^2 + (y_i - y_0)^2] \cdot (1 + 2\epsilon_i + \epsilon_i^2)
= [(x_i - x_0)^2 + (y_i - y_0)^2] + 2d_{it}\epsilon_i + d_{it}\epsilon_i^2 \quad (3)
\]

where \( d_{it} = (x_i - x_0)^2 + (y_i - y_0)^2 \). To convert these equations into linear equations, we subtract \( \hat{d}_{it}^2 \) (\( i = 2, \ldots, N \)) from \( \hat{d}_{i1}^2 \),

\[
\hat{d}_{i1}^2 - \hat{d}_{it}^2 = [(x_1 - x_0)^2 + (y_1 - y_0)^2] + 2d_{i1}\epsilon_i + d_{i1}\epsilon_i^2
- [(x_i - x_0)^2 + (y_i - y_0)^2] - 2d_{it}\epsilon_i - d_{it}\epsilon_i^2
= x_1^2 - 2x_1x_0 + x_0^2 + y_1^2 - 2x_1y_0 + y_0^2 + 2d_{i1}\epsilon_i + d_{i1}\epsilon_i^2
- x_i^2 + 2x_ix_0 - x_0^2 - y_i^2 + 2y_ix_0 - y_0^2 - 2d_{it}\epsilon_i - d_{it}\epsilon_i^2
= -(x_1^2 - x_1^2) - (y_1^2 - y_1^2) + 2(x_1 - x_1)x_0 + 2(y_1 - y_1)y_0
+ 2d_{i1}\epsilon_i - 2d_{it}\epsilon_i + d_{i1}\epsilon_i^2 - d_{it}\epsilon_i^2 \quad (4)
\]

From Eq. (4), we have the following linear equations.

\[
\alpha_i = (x_i - x_1) \cdot x_0 + (y_i - y_1) \cdot y_0 + \beta_i, \quad i = 2, \ldots, N \quad (5)
\]

where

\[
\alpha_i = \frac{1}{2} \left[ (\hat{d}_{i1}^2 - \hat{d}_{it}^2) + (x_1^2 - x_1^2) + (y_1^2 - y_1^2) \right],
\]

\[
\beta_i = (d_{i1}\epsilon_i - d_{it}\epsilon_i) + \frac{1}{2}(d_{i1}\epsilon_i^2 - d_{it}\epsilon_i^2).
\]

Equation (5) can be written in matrix form, that is,

\[
\mathbf{b} = \mathbf{Ax} + \mathbf{w} \quad (6)
\]

where

\[
\mathbf{b} = \begin{bmatrix} \alpha_2 \\ \vdots \\ \alpha_N \end{bmatrix}, \mathbf{x} = \begin{bmatrix} x_0 \\ y_0 \end{bmatrix}, \mathbf{w} = \begin{bmatrix} \beta_2 \\ \vdots \\ \beta_N \end{bmatrix},
\]

\[
\mathbf{A} = \begin{bmatrix} (x_2 - x_1) & (y_2 - y_1) \\ \vdots & \vdots \\ (x_N - x_1) & (y_N - y_1) \end{bmatrix}.
\]

To solve Eq. (6), we minimize the quadratic error given by

\[
\mathbf{J} = \frac{1}{2} \left( \mathbf{b} - \mathbf{Ax} \right)^T \mathbf{W}^{-1} \left( \mathbf{b} - \mathbf{Ax} \right) \quad (7)
\]

where the superscript \( T \) denotes a transpose and \( \mathbf{W} \) is a positive definite weighted matrix. \( \mathbf{J} \) implies the weighted summation of the residual squares and \( \mathbf{W} \) can be obtained as
\[ W = E[w \cdot w^T] = \begin{bmatrix} w_{22} & \cdots & w_{2N} \\ \vdots & \ddots & \vdots \\ w_{N2} & \cdots & w_{NN} \end{bmatrix} \]  

(8)

where \( w_{ij} \) (for \( i = 2, \ldots, N, j = 2, \ldots, N \)) is the covariance of \( \beta_i \) and \( \beta_j \). \( \beta_i \) and \( \beta_j \) are the sum of a Gaussian random variable and a chi-square random variable and all \( \epsilon_i \) (for \( k = 1, \ldots, N \)) are independent of each other. Thus, using the moment generating function (MGF) [9], \( w_{ij} \) can be given by

\[
\begin{align*}
\begin{cases}
      (d_{ij}^2 + d_{ij}^4) \sigma^2 + (d_{ij}^2 + d_{ij}^4) \sigma^4 & \text{for } i = j \\
      d_{ij}^2 \sigma^2 + d_{ij}^4 \sigma^4 & \text{for } i \neq j.
\end{cases}
\end{align*}
\]

(9)

However, we do not know the true distance \( d_{ij} \) between \( A_i \) and \( S_i \). Using the measured distance \( d_{ij}^2 \), we can consider \( \hat{w}_{ij} \) instead of \( w_{ij} \). \( \hat{w}_{ij} \) is obtained from

\[
\hat{w}_{ij} = \begin{bmatrix}
      (d_{ij}^2 + d_{ij}^4) \sigma^2 + (d_{ij}^2 + d_{ij}^4) \sigma^4 \\
      d_{ij}^2 \sigma^2 + d_{ij}^4 \sigma^4
\end{bmatrix} \text{ for } i = j \]

(10)

Using Eq. (10), we can convert Eq. (7) into

\[
J = \frac{1}{2} [b - Ax]^T \hat{W}^{-1} [b - Ax]
\]

(11)

where

\[
\hat{W} = \begin{bmatrix}
      \hat{w}_{22} & \cdots & \hat{w}_{2N} \\ \vdots & \ddots & \vdots \\ \hat{w}_{N2} & \cdots & \hat{w}_{NN} \end{bmatrix}
\]

To minimize Eq. (11), the gradient of the equation must be set to zero with respect to \( x \), that is,

\[
\nabla_x J = -A^T \hat{W}^{-1} [b - Ax] = 0.
\]

(12)

Consequently, we can localize the sensor node using the measured distances and the measurement uncertainty from the following equation.

\[
x = (A^T \hat{W}^{-1} A)^{-1} A^T \hat{W}^{-1} b.
\]

(13)

4. Simulation Results

To evaluate the performance of the proposed localization method, we considered a WSN in which the anchors and the sensor nodes were uniformly randomly deployed. The variance \( \sigma^2 \) of the measurement noise was set to 0.1. We assumed that the adversary could modify the distance measurements for a fraction \( \gamma \) of the anchors within the communication range of the sensor node. We executed Monte Carlo simulations with 1000 runs using MATLAB for each simulation scenario.

To investigate the localization accuracy of the proposed method, we computed the root-mean-square errors (RMSEs) of the true positions of the sensor nodes and the localization results for various \( \gamma \) values (see Fig. 1). In this scenario, we assumed that malicious anchors did not collude, that is, a malicious anchor \( A_i \) provides incorrect distance information to \( S_i \) by \( \theta_i \), according to Eq. (2). \( \theta_i \) was uniformly random from 0 to 1, and \( N \) was set to 20. As \( \gamma \) increased, the RMSE of the LS method increased rapidly. Although both the LMS method and the proposed method have stable accuracy, the latter has better accuracy (about 29% greater) than does the former. Moreover, our method has a lower time complexity than does the LMS method. Table 1 shows the comparison of the time complexity of our method with that of the previously reported methods for various \( N \) values. The computation time was measured as the CPU time elapsed when using MATLAB on an Intel(R) Xeon(R) E5430 2.66-GHz CPU. According to Table 1, the number of computational resources consumed in the proposed method and the LS method is almost the same, and the proposed method has a lower time complexity than does the LMS method. For example, when \( N = 20 \), the CPU time in the LMS method was approximately 66 times higher than that in the proposed method. Therefore, it was confirmed that the proposed method is more accurate than the previously reported localization methods, and more efficient in reducing the power consumed by a sensor node in WSNs than is the LMS method.

Figure 2 shows the performance of the localization methods in the presence of colluding malicious anchors. 

![Fig. 1 Performance of the localization methods in the presence of non-colluding malicious anchors.](image)

Table 1 Comparison of time complexity between localization methods.

<table>
<thead>
<tr>
<th>( N )</th>
<th>LS (A)</th>
<th>LMS (B)</th>
<th>Proposed (C)</th>
<th>A / C</th>
<th>B / C</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>51</td>
<td>274</td>
<td>66</td>
<td>0.79</td>
<td>4.18</td>
</tr>
<tr>
<td>6</td>
<td>57</td>
<td>689</td>
<td>75</td>
<td>0.75</td>
<td>9.15</td>
</tr>
<tr>
<td>8</td>
<td>62</td>
<td>1,403</td>
<td>85</td>
<td>0.73</td>
<td>16.48</td>
</tr>
<tr>
<td>10</td>
<td>67</td>
<td>2,228</td>
<td>94</td>
<td>0.72</td>
<td>23.71</td>
</tr>
<tr>
<td>12</td>
<td>72</td>
<td>3,278</td>
<td>103</td>
<td>0.70</td>
<td>31.71</td>
</tr>
<tr>
<td>14</td>
<td>78</td>
<td>4,455</td>
<td>114</td>
<td>0.68</td>
<td>38.98</td>
</tr>
<tr>
<td>16</td>
<td>83</td>
<td>5,862</td>
<td>121</td>
<td>0.69</td>
<td>48.26</td>
</tr>
<tr>
<td>18</td>
<td>89</td>
<td>7,490</td>
<td>131</td>
<td>0.68</td>
<td>57.16</td>
</tr>
<tr>
<td>20</td>
<td>93</td>
<td>9,295</td>
<td>141</td>
<td>0.66</td>
<td>66.14</td>
</tr>
</tbody>
</table>
Colluding malicious anchors tamper with the measurements and influence the localization result so that it tends toward \((x_a, y_a)\). Let the lying distance be the distance between \((x_0, y_0)\) and \((x_a, y_a)\). In this scenario, \(N\) and \(\gamma\) were set to 20 and 0.3, respectively. In Fig. 2, when the lying distance was less than approximately 90 m, the proposed method had the best accuracy; in other cases, the LMS method had the best accuracy. In a typical WSN, a sensor node has a very limited transmission range (e.g., tens of meters). Therefore, the proposed method shows a preferable performance for most of practical communication ranges in WSNs.

5. Conclusion

In this paper, we address the problem of secure localization in WSNs. We propose a trilateration-based secure localization method that retains preferable accuracy against location attacks. The proposed method has lesser computational complexity than does the previously reported LMS localization method. Simulation results show that the proposed method can accurately localize a sensor node in WSNs and that it is computationally efficient.

References