A Secure Localization Method in Wireless Sensor Network
Maryam Mirzaei, Mohammad Robatmili and Mehdi Khalili
Dept. of Computer and Informatics Engineering, Payam Noor University, Tehran, Iran
*Corresponding Author's E-mail: mirzaei_2011@yahoo.com

Abstract

Wireless sensor network is composed of hundreds or thousands of sensor nodes that communicate and work together to perform a specific task or tasks. Information sensed by each node sent to a base station, which is called sink and connected to the AC power. In many cases, the location of sensed data is important for decision-making. Localization is used for this purpose. Localization is one of the techniques used in wireless sensor networks. Real applications of wireless sensor networks often are faced with a variety of harmful interferences that have significant impact on the efficiency of locating. In this paper, a secure and robust localization algorithm for wireless sensor networks to reduce the impact of hostility attackers as external attacks and fault and error in networks elements as internal attacks is presented. The proposed method consists of two steps which in the first step, malicious anchor nodes are detected and nodes’ trust values are calculated. In the next step, Taylor series least square method is used to estimate the coordinates of the sensor nodes. Simulation results will show that the proposed algorithm is efficient and robust.

Keywords: wireless sensor network, localization, malicious anchor node, least square

I. Introduction

Wireless sensor networks (WSNs) are based on sensor technology, wireless communications, tiny embedded devices, and distributed computing. These networks are exchanging data with the environment by sensors and perform data manipulating and gathering. WSNs are widely used in environment monitoring, target tracking, military application, disaster management and etc [1-3]. The node localization technology is needed in WSN application, especially when location information is necessary. WSN nodes localization is determining coordinates of normal nodes based on anchor nodes coordinates and confined relation between anchor and normal nodes. The coordinate or location of normal node is unknown. On the other hand, Anchor nodes can obtain their location via global positioning system (GPS) modules or manually. In many typical localization algorithms [4-6] assumed that anchor nodes location information are quite properly without any interference by adverse factors or internal attacks and normal nodes can use anchor information safely. However, in real hostile situations, some malicious nodes may enter into the sensor network without authorization in order to sabotage. They are trying to introduce themselves as benign anchor nodes or attack on other anchor nodes in order to force them to declare wrong location [7]. In addition to malicious anchor nodes, faulty anchors should be detected for avoiding errors in localization. Erroneous distance estimation or erroneous coordinate causes irreplaceable fault in normal sensor nodes localization. In this case, some methods should be applied to eliminate or reduce harness effects created by malicious or faulty anchor nodes and ensure secure wireless sensor network localization. We call malicious anchor nodes the both faulty and malicious anchor nodes. In this paper, we propose a robust and secure localization algorithm in order to solve the problem of malicious anchor nodes existence in localization. In the proposed method, each anchor node asks other anchors their locations and decision about other anchor nodes that are benign or malicious by triangulation localization method. The sensor node is informed about anchor node decision in order
to localize itself. The proposed method will be discussed briefly later. The remainder of the paper is organized as follows: Section 2 introduces related works on secure localization algorithms. Section 3 presents the network model, attack model, and related definitions. Section 4 provides the details of proposed method. Section 5 presents the simulation results. Section 6 concludes the paper.

II. Related Works

A Alfaro et al. [10] consider the localization security of sensor nodes under limited trust anchor nodes. It proposes three algorithms to enable the sensor nodes to determine their positions, but it would fail when the malicious anchor nodes are in colluding conditions. Colluding condition is a case where the malicious anchor nodes can detect whether other anchor nodes are the same type, and each pair of colluding malicious anchor nodes can revise the measure distance between them by changing their declared locations.

Liu et al. [11] introduce two secure localization algorithms. One is attack-resistant minimum mean square estimation, which excludes malicious anchor nodes by the consistency check. The other is voting-based location estimation. The algorithms are difficult to work for the malicious anchor nodes in colluding conditions.

Zhu et al. [12] present an attack detection module which can detect compromised beacons and provide a localization service in terms of bounded estimation error by secure localization module, but it mainly concentrates on the one-hop localization.

Liu et al. [13] propose a secure localization mechanism that detects malicious anchor nodes claiming fake positions. It uses redundant anchor nodes instead of normal nodes in the sensing field to verify malicious anchors. The method relies on a centralized base station for the detection.

Li et al. [14] present a secure scheme “Bilateration” which is derived from multilateration. It calculates the weight of anchor nodes and decides which anchor nodes are malicious. After ignoring the coordinates caused by compromised nodes, it uses the average value of the let candidate positions as the estimated location of the sensor node, but it mainly focuses on the one-hop localization.

Yu et al. [15] propose a secure schema called BRSL and try to detect and thwart malicious anchor nodes. In this paper beta reputation system is used in order to determine anchor nodes’ trust values. If trust value of an anchor is less that calculated threshold, this anchor detects as malicious. The Taylor series least square method is used in order to localization. The weakness of this method is that it relies on several nodes deployment reputation which may be impossible in many situations.

III. PRIMARY DEFINITIONS

All Network Model: The network with two nodes type (anchor and sensor) is considered. The anchor nodes are equipped with special equipments and know their positions. The sensor nodes which their positions should be detected, estimate their locations by measuring distances to neighboring anchor nodes by RSSI. All the nodes are distributed randomly in a 2 domination environment. The communication range is denoted as R in each node and they can calculate ranges of their one-hop neighbors.

The domain error $e$ follows Gaussian distribution ($N(u,\lambda^2)$) that mean $u$ is zero and variance $\lambda$ is restricted:

$$|e_i| \leq e_{\text{max}} \quad (1)$$

The maximum physical error $e_{\text{max}}$ is obtained experimentally. In multihop localization, each anchor node broadcasts a message that carries its declared position to its one-hop neighbors. Then, the message is propagated in the network in a controlled flooding manner. When a sensor node obtains three or more anchor messages, the sensor node can estimate its location by the localization algorithm [8].

Attack model: Assume that WSN is in a hostile environment which means there are malicious attackers. The attackers attack anchor nodes in order to force them to declare false positions. When
an anchor node is attacked and declares false position is called malicious anchor. The anchors that declare real positions are called benign anchor nodes. When a sensor node M gets enough measurement distances \( d_{mi} (i=1,2,\ldots,k) \), where \( k \geq 3 \), to anchor nodes \( A_i \), a system of the Euclidean equations can be set up:

\[
||X_m - X_1||^2 = d_{m1} \\
||X_m - X_2||^2 = d_{m2} \\
\vdots \\
||X_m - X_k||^2 = d_{mk}
\]

Where \( X_m = [x_m,y_m]^T \) is M's coordinates that need to be estimated and \( X_i = [x_i,y_i]^T \) is anchor node \( A_i \)'s declared position. If the anchor node \( A_1 \) is attacked, it will become a malicious anchor node \( A'_1 \) with fake coordinates. When M utilizes \( A'_1 \) to compute its position, its estimated position \( M' \) will deviate far from its physical position, and its location accuracy will be very low.

### IV. PROPOSED METHOD

#### A) Malicious Anchor Nodes Detection

In order to detect malicious anchor nodes, initially, all anchor nodes broadcast their location information among the network. Each anchor nodes estimate its location with other three pare anchor nodes location information by triangulation method. The anchor node estimates its location according to different three pars. The obtained locations are compared with real location. If difference between obtained location and reallocation become more than \( \text{emax} \), at least one of these three involved anchor nodes are malicious. By evaluating other obtained locations, the malicious anchor nodes detects easily.

We consider trust value for each anchor nodes to avoid involving faulty or untrusted anchor nodes in localization process. If deference between estimated location by three anchor nodes and reallocation is more than a pre-defined threshold, the trust value of these three anchors decrease. On the other hand, if the deference between estimated location by three anchor nodes and reallocation is less than a pre-defined threshold, the trust value of these three anchors increase.

![Triangulation method](image)

#### (2)

In triangulation method location of node is obtained from the following formula by three known position.

\[
\begin{align*}
d_a^2 &= x^2 - 2x \cdot x_a + x_a^2 + y^2 - 2y \cdot y_a + y_a^2 \\
d_b^2 &= x^2 - 2x \cdot x_b + x_b^2 + y^2 - 2y \cdot y_b + y_b^2 \\
d_c^2 &= x^2 - 2x \cdot x_c + x_c^2 + y^2 - 2y \cdot y_c + y_c^2
\end{align*}
\]
B) Localization Process

Firstly, calculate the centroid coordinates $X_c=(x_c, y_c)$ of $k$ anchor nodes, that is, $X_c = (\sum_i^k x_i^k \cdot v_i^k) / \sum_i^k v_i^k$.

Secondly, expand the function $f(x) = \|x - X_c\|^2$ in Taylor series at $X_c$, and ignore the high-order terms. Therefore, $\Delta X_C = (\Delta x_c, \Delta y_c)$ can be obtained such as:

$$\Delta X_C = \left( A^T W^T W A \right)^{-1} A^T W^T W B$$

Where:

$$W = \begin{bmatrix} \text{Tru}_T_1 & 0 & 0 \\ \text{Tru}_T_2 & \cdots & 0 \\ 0 & 0 & \text{Tru}_T_K \end{bmatrix},$$

$$B = \begin{bmatrix} d_1 - d_{1C} \\ d_2 - d_{2C} \\ \cdots \\ d_k - d_{kC} \end{bmatrix},$$

$$A = \begin{bmatrix} x_c - x_1 & x_c - x_2 & \cdots & x_c - x_K \\ d_{1C} & d_{2C} & \cdots & d_{kC} \\ y_c - y_1 & y_c - y_2 & \cdots & y_c - y_K \\ d_{1C} & d_{2C} & \cdots & d_{kC} \end{bmatrix}^T.$$ 

Thirdly, $d$ is calculated by formula 7, and judge whether the iteration termination condition $d<=\delta$ is satisfied, where $\delta$ is a priori-defined threshold. If $d<=\delta$, we stop the iteration process. Otherwise, we set $X_c = X_c + \Delta X_c$ and go to the second step. Finally, repeat the second step and the third step until the iteration termination condition is satisfied or the maximum iteration number is reached. The final output $X_c$ is the estimated coordinates of sensor node $M$. The localization algorithm is in below.
Algorithm. Nodes localization algorithm

\[ d = \sqrt{\frac{\Delta x_C^2 + \Delta y_C^2}{2}} \]  

(7)

\[
\begin{align*}
\text{for } i &= 1:1:length(benginganodes) \\
& \quad W(i,i) = benginganodes(i).Tru_TA; \% \text{calculation of } W \\
\text{end}
\end{align*}
\]

\[
\begin{align*}
\text{for } i &= 1:1:banodes+manodes \\
& \quad \% \text{calculation of } XC \\
& \quad \text{sumx} = 0; \\
& \quad \text{sumy} = 0; \\
& \quad \text{for } k = 1:1:length(benginganodes) \\
& \quad \quad \text{sumx} = benginganodes(k).xd + \text{sumx}; \\
& \quad \quad \text{sumy} = benginganodes(k).yd + \text{sumy}; \\
& \quad \end{align*}
\]

\[
\begin{align*}
& \quad Xc = \text{sumx}/\text{length(benginganodes)}; \\
& \quad Yc = \text{sumy}/\text{length(benginganodes)}; \\
& \quad XC.xd = Xc; \\
& \quad XC.yd = Yc; \\
& \quad \text{steps} = 0; \% \text{prevent of unlimited while loop} \\
& \quad \text{rep} = 1; \% \text{repeat lines between while until rep equal to 0} \\
& \quad \text{while } (\text{rep} \neq 0) \\
& \quad \quad \text{steps} = \text{steps} + 1; \\
& \quad \quad \text{for } k = 1:1:length(benginganodes) \\
& \quad \quad \quad d(i,k) = \text{distance1}(S(i), benginganodes(k)); \\
& \quad \quad \quad \text{dc}(k) = \text{distance1}(\text{benginganodes}(k), XC); \\
& \quad \quad \end{align*}
\]

\[
\begin{align*}
& \quad \text{for } k = 1:1:length(benginganodes) \\
& \quad \quad B(k) = d(i,k) - \text{dc}(k); \\
& \quad \end{align*}
\]

\[
\begin{align*}
& \quad \text{for } k = 1:1:length(benginganodes) \\
& \quad \quad A(1,k) = (XC.xd - benginganodes(k).xd)/\text{dc}(k); \\
& \quad \quad A(2,k) = (XC.yd - benginganodes(k).yd)/\text{dc}(k); \\
& \quad \end{align*}
\]

\[
\begin{align*}
& \quad A = A'; \\
& \quad B = B'; \\
& \quad \text{deltaXC} = (A'**W**B'/(A'**W**W*A)); \\
& \quad d = \text{sqrt} (\text{deltaXC}(1)^2 + \text{deltaXC}(1)^2); \\
& \quad A = A'; \\
& \quad B = B'; \\
& \quad \text{if } d > n \\
& \quad \quad \text{XC.xd} = \text{deltaXC}(1) + \text{XC.xd}; \\
& \quad \quad \text{XC.yd} = \text{deltaXC}(2) + \text{XC.yd}; \\
& \quad \text{elseif } d < n \text{ } || \text{ steps} > 40 \\
& \quad \quad \text{rep} = 0; \% \text{this line causes stop while} \\
& \quad \end{align*}
\]

\[
\begin{align*}
& \quad \text{end} \\
& \quad \text{end} \\
& \quad \text{newS}(i).xd = XC.xd; \\
& \quad \text{newS}(i).yd = XC.yd; \\
& \quad \text{end}
\end{align*}
\]
import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

V. Simulation results

To demonstrate the effectiveness of the proposed method in this section, we do a comparison between this method and some of the leading methods in the field of secure localization. We compare the proposed method with BRSL and Bilateration that are robust and effective localization algorithms.

Matlab is the simulation tool used in this paper which is applied in many scientific papers. Initially network size is defined as two dominations square 200*200. Number of all nodes, benign anchor nodes and malicious anchor nodes are 200, 20 and 10 respectively. The nodes distribution strategy is random. Other network parameters are listed in table 2. Figure 2 illustrates a sample nodes deployment where blue cycles, green stars and red stars are demonstrated normal sensor nodes, benign anchor nodes and malicious anchor nodes respectively.

A) Simulation Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Energy</td>
<td>0.5J</td>
</tr>
<tr>
<td>Number of all Nodes</td>
<td>200</td>
</tr>
<tr>
<td>Network Area</td>
<td>Flat 2D</td>
</tr>
<tr>
<td>Network Dimension</td>
<td>200*200</td>
</tr>
<tr>
<td>Sink Position</td>
<td>(100,100)</td>
</tr>
<tr>
<td>Nodes Deployment</td>
<td>Random</td>
</tr>
<tr>
<td>Control Packets</td>
<td>12 bit</td>
</tr>
<tr>
<td>Emax</td>
<td>0.0001</td>
</tr>
<tr>
<td>Pre-defined Threshold</td>
<td>0.00001</td>
</tr>
</tbody>
</table>

Fig. 2. Nodes randomly deployment
The major parameter that should be measured in localization techniques is amount of localization error in different situations. Initially the state is considered that number of malicious anchor nodes increases from 1 to 10. The simulation result of this situation is shown in figure 3 which the error rate of the proposed method is much less than the other two methods. Figure 4 demonstrates results of comparisons between errors with different standard deviation. The error of each algorithm is increased by standard deviation increase. According to these simulation results we can conclude that in comparison with BRSL and Bilateration, the proposed method is more efficient.

![Fig. 3. Compare between error rates with different number of malicious anchor nodes](image1.png)

![Fig. 4. Compare between error rates with different standard deviation](image2.png)

VI. Conclusion

In a wireless sensor network, for sending information, the location of sensed data is important for decision-making. Thus, localization becomes an important issue for this purpose. In this paper, to reduce the impact of hostility attackers as external attacks and also fault and error in networks elements as internal attacks in wireless sensor networks, we proposed a secure and robust localization algorithm, in which, first, malicious anchor nodes detected nodes’ trust values calculated. Then, to estimate the coordinates of the sensor nodes, Taylor series least square method used. The obtained results of simulation indicates that the proposed algorithm not only satisfies efficiency and robustness, but also decreases error rates in the standard deviation and the number of malicious anchor nodes, compared to BRSL and bilateration. Moreover, the proposed algorithm lead researchers to clustering structure as the future work.
References


