AN INCREMENTAL TRUST-BASED METHOD FOR ROBUST POSITION IDENTIFICATION IN WSNs

VINAY T.P\(^1\), SANDHYA P.N\(^2\)

\(^1\)(Assistant Professor, Department of ISE, Channabasaveshwara Institute of Technology, Tumkur, India)
\(^2\)(Assistant Professor, Department of CSE, Channabasaveshwara Institute of Technology, Tumkur, India)

ABSTRACT

In an Wireless Sensor Networks (WSNs) determining the location of sensors is a basic and essential knowledge for most WSN algorithms. In this paper, we propose and discuss a technique that aims to localize all the sensor nodes in the network using 2D trilateration and a security protocol is used for providing confidentiality and authentication between locators nodes and sensor nodes. Two issues about unknown nodes secure localization need to be considered. First, the attackers may disguise as or attack the unknown and anchor nodes to interfere with localization process. Second, the attackers may forge, replay or modify localization information to make the estimated positions incorrect.

Keywords: Secure Localization, Verifiable Trilateration, Wireless Sensor Networks.

1. INTRODUCTION

Wireless sensor networks (WSNs) are envisioned to be widely used in medical, military, and environmental monitoring applications. A future WSN might consist of hundreds to thousands of deployed sensor nodes which are expected to self-organize into an autonomous network, perform desired sensing tasks, and react properly to the environment or specific events. Localization is one of the most important services provided by a WSN, because in most applications we are interested not only in the types of events that have taken place, but also in where the events have taken place.
2. RELATED WORK

WSN may be deployed in hostile environments where malicious adversaries attempt to spoof the locations of the sensors by attacking the localization process[1]. For example, an attacker may alter the distance estimations of a sensor to several reference points, or replay beacons from one part of the network to some distant part of the network, thus providing false localization information. Therefore, a secure positioning system must have a mechanism to verify the location claim of any sensor. Some of the existing secure localization techniques are reviewed below.

2.1 SeRLoc

Lazos and Poovendran propose a novel scheme for localization of nodes in WSNs in untrusted environments called SeRLoc. SeRLoc is a distributed, range-free, resource-efficient localization technique in which there is no communication requirement between nodes for location discovery[2]. SeRLoc is robust against sybil attacks, wormhole attacks and sensor compromise.

2.2 Attack Resistant Location Estimation

Liu, Ning, and Du put forward two range-based robust methods to tolerate malicious attacks against beacon-based location discovery in sensor networks. The first method, attack-resistant Minimum Mean Square Estimation, filters out malicious beacon signals. This is accomplished by examining the inconsistency among location references of different beacon signals, indicated by the mean square error of estimation, and beating malicious attacks by removing such malicious data. The second method, voting-based location estimation quantizes the deployment field into a grid of cells and has each location reference ‘vote’ on the cells in which the node may reside. This method tolerates malicious beacon signals by adopting an iteratively refined voting scheme. Both methods survive malicious attacks even if the attacks bypass authentication[5].

2.3 Robust Statistical Methods

Li, Trappe, Zhang, and Nath introduced the idea of being tolerant to attacks rather than trying to eliminate them by exploiting redundancies at various levels within wireless networks[3].

2.4 SPINE

Capkun and Hubaux devise secure positioning in sensor networks (SPINE), a range-based positioning system based on verifiable multilateration which enables secure computation and verification of the positions of mobile devices in the presence of attackers. SPINE works by bounding the distance of each sensor to at least three reference points[7].

2.5 DRBTS

DRBTS[8] is a distributed reputation and trust-based security protocol aimed at providing a method for secure localization in sensor networks. In this model, incorrect location information provided by malicious beacon nodes can be excluded during localization. This is achieved by enabling beacon nodes to monitor each other and provide information so that sensor nodes can choose who to trust, based on a majority voting approach. In order to trust beacon node’s information, a sensor must get votes for its trustworthiness from at least half of their common neighbors.

2.6 HiRLoc

Lazos and Poovendran propose a high-resolution, range independent localization technique called HiRLoc. In HiRLoc, sensors passively determine their location without any interaction
amongst themselves. HiRLoc also eliminates the need for increased beacon node density and specialized hardware. Table 1 illustrates the summary of security attacks addressed by each algorithm.

TABLE 1: Summary of security attacks addressed by each algorithm

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Distance Fraud</th>
<th>Mafia Fraud</th>
<th>Terrorist Fraud</th>
<th>Wormhole</th>
<th>Sybil</th>
<th>Spoofing</th>
<th>Jamming</th>
<th>Shadowing</th>
<th>Manipulation</th>
<th>Replay</th>
</tr>
</thead>
<tbody>
<tr>
<td>SeRLoc</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Attack Resistant Location Estimation</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>DRBTS</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>HiRLoc</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

3. PROPOSED SYSTEM

An Incremental Trust based Robust Position Identification algorithm contains two phases. First phase is location estimation in which the sensor node broadcast its ID to locators which comes in sensor-to locator communication range and those locators perform distance bounding with sensor node and included within the set $LDB_s$[4]. Then for every locator of set $LDB_s$, trust evaluation value is estimated by sensor node. If the trust evaluation value is greater than or equal to threshold then it is included within set $LT_s$. If the number of locators within set $LT_s$ is greater than or equal to 3 and any 3 locators of set $LT_s$ forms an triangle around sensor, then location of sensor node is estimated through Verifiable Trilateration. Otherwise localization fails. Second phase is location verification in which location claim of sensor node is verified by locator through distance bounding protocol.

3.1 An Incremental Trust Based Robust Position Identification

Consider a two tier network which contains randomly deployed sensors to sense the environment and randomly deployed locators which act as data collection points know their position via manual configuration or a secure GPS system. The network assumptions are showed in Table 2. Both sensors and locators perform nanosecond processing and measure time with nanosecond precision, required for distance bounding[6]. It is assumed that sensor-to sensor communication range equal to $r$. Locator-to locator communication range equal to $R > r$. Sensor-to locator communication range equal to $r_{sL}$ which is computed as $r_{sL} = rG^{1/\gamma}$, where $G$ denotes the antenna directivity gain of locators’ antenna and $\gamma$ denotes the signal attenuation factor. It is assumed that each sensor $s$ shares a pair wise key $K_{Li}$ with each $L_i$ to perform cryptographic operations. The locators which come in the power range are assumed as neighbors in trust evaluation. At least three locators are required for performing Verifiable Trilateration.
An Incremental Trust based Robust Position Identification algorithm contains two phases. First phase is location estimation in which the sensor node broadcast its ID to locators which comes in sensor-to locator communication range and those locators perform distance bounding with sensor node and included within the set $LDB_s$. Then for every locator of set $LDB_s$, trust evaluation value is estimated by sensor node. If the trust evaluation value is greater than or equal to threshold then it is included within set $LT_s$. If the number of locators within set $LT_s$ is greater than or equal to 3 and any 3 locators of set $LT_s$ forms an triangle around sensor, then location of sensor node is estimated through Verifiable Trilateration[9]. Otherwise localization fails. Second phase is location verification in which location claim of sensor node is verified by locator through distance bounding protocol. Table 2 illustrates the network assumption.

### Table 2: Network Assumptions

<table>
<thead>
<tr>
<th></th>
<th>Sensors</th>
<th>Locators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Area</td>
<td>$A$</td>
<td>$A$</td>
</tr>
<tr>
<td>Density</td>
<td>$p_s$</td>
<td>$p_L &lt;&lt; p_s$</td>
</tr>
<tr>
<td>Antenna Type</td>
<td>Omni directional</td>
<td>M directional Antenna with beam width $\frac{2\pi}{M}$</td>
</tr>
</tbody>
</table>

#### 3.2 Location Identification Phase

Step 1: The sensor $s$ broadcasts its $ID_s$ to the locators, $s : ID_s$.

Step 2: Any locator $L_i$ which can communicate bi-directionally with sensor $s$ performs distance bounding with $s$. Distance bounding protocol verifies that sensor $s$ being at a distance $d_{sl_i}$ from $L_i$ cannot claim to be at a distance less than $d_{sl_i}$

$$LDB_s = \{L_i : \|L_i - s\| \leq r_{sl_i}\}$$

Step 3: For every locator $L_i$ which belongs to set $LDB_s$, sensor node $s$ collects the trust evaluation value of locator $L_i$ as in trust model and checks whether the trust evaluation value of locator $L_i$ is greater than or equal to threshold value. If the trust evaluation value of locator $L_i$ is greater than or equal to threshold then the locator is added in the set $LT_s$.

$$LT_s = \{L_i : L_i \in LDB_s, T_{sl_i} \geq Threshold\}$$

Step 4: Sort the set $LT_s$ of locators in the order based on trust evaluation value of locators from high to low.

Step 5: If $|LT_s| \geq 3$ then the sensor $s$ performs Verifiable Trilateration with the locators $L_i \in LT_s$. Otherwise the localization fails. Sensor $s$ can perform Verifiable Trilateration if it is in the triangle of three locators.

Step 6: If sensor $s$ estimates its position by Verifiable Trilateration, then it notifies all the locators $L_i \in LDB_s$, with the transmission of computed position encrypted by the pair wise key and terminates the algorithm.

Fig.1 shows the Algorithm for An Incremental Trust Based Robust Position Identification Scheme.
3.3 Location verification phase
Whenever a sensor node sends data along with the position to the locator, locator needs to check the claimed position of sensor node. Hence, locator performs distance bounding with s. So, the sensor cannot claim to be at a distance which is smaller than the actual one.

```
01: s: broadcast ID_s
02: for all L_i that receive broadcast from s
03:   L_i: perform Distance Bounding with s
04:   s: define LDB_s = { L_i : || L_i - s || ≤ r_{sl} }
05: endfor
06: for all L_i ∈ LDB_s
07:   s: compute Trust Evaluation Value of L_i
08:   s: define LT_s = { L_i : L_i ∈ LDB_s, T_{sl_i} ≥ Threshold }
09:   s: sort LT_s such that
10:   LT_s = { L_i : L_i ∈ LT_s, T_{sl_i} ≥ T_{sl_i+1} }
11: if (L_i, L_j, L_k) ∈ LT_s such that
12:   ∃ s inside Δ L_i L_j L_k
13:   s: compute ŝ := Verifiable Trilateration
14:   s: notify E_K_s (Termination), ∀ L_i ∈ LDB_s
15: else
16:   Localization fails
17: Endfor
```

Fig. 1: Algorithm for an Incremental Trust Based Robust Position Identification Scheme

4. SECURITY ANALYSIS

4.1 Attacker model
It is assumed that attacker can spoof the location estimated by the sensors. As a result sensors try to estimate the position than the actual one. However, the attacker does not restrict sensors from estimating the position. If the localization of sensor node fails, it is believed that it is under attack. Also it is assumed that attacker is capable of jamming the signals of network entities. However, jamming signals from all the entities results in failure of localization of the sensor node.

4.2 Wormhole attack
In wormhole attack an attacker receives packet at one point in the network, “tunnels” them to alternative point in the network. In specified scheme, when the sensor node broadcasts ID_s, the attacker receives this information and tunnels this information to another point in the network and
replies from that point. Further, locators sends location information as reply, the attacker collects this information and tunnels this to another point in the network and replies them.

It is assumed that a set of locators replied to the sensor $s$ is under attack and $s$ performs Verifiable Trilateration with the three locators $L_i, L_j, L_k \in LT_s$ such that $s$ lies within $\Delta L_i L_j L_k$. If the attacker jams the signal from one locator, assume $L_i$ and replies as $L_i$ after some time, then $s$ still resides within $\Delta L_i L_j L_k$. Suppose the distance from sensor node $s$ to $L_i$ is enlarged then any one of the other to locators need to reduce the distance. This is impossible due to distance bounding protocol. Hence, the spoofing of position of $s$ by attacker is not possible. If the attacker jams the signals from all the locators of set $LT_s$ then localization fails.

### 4.3 Compromised node attack

A network entity is said to be compromised if attacker gains authority of all the information related to the entity. Suppose if the attacker compromise the locators then it can jam the signals of those locator which results in failure of localization if significant locators are compromised. However, if the attacker adds bogus location information to the compromised locators, then this can be detected by the trust model and those untrustworthy locators are not included in localization.

### 5. PERFORMANCE ANALYSIS

**Case 1: Successful localization**

In the case of successful localization there are 3 or more trustworthy locators are there within the power range of given sensor node. And these trustworthy locators form a triangle around the given sensor node. So the location of sensor node is computed using the 3 most trustworthy locators which form triangle around sensor node.

Snapshot 1 shows the initial deployment of sensors and locators. There are 20 nodes in the snapshot in which 8 nodes are locators, rest are sensor nodes. Sensor nodes are shown in green color and locators are shown in blue color.

Snapshot 2 shows sensor node 11 is selected for localization. Node 11 is shown in red color to indicate that this sensor node is selected for localization.

Snapshot 3 shows sensor node 11 broadcasting init message to locators which comes in the power range of 11. The locators which receive broadcast from sensor node 11 are turned to pink color.

Snapshot 4 shows the locators which receives broadcast of INIT message from sensor node 11. The locator which comes in sensor-to locator range of sensor node 11 receives this broadcast. Locators which received broadcast from sensor node 11 are turned as pink, otherwise blue. Here locators 6, 9, 12, 13, 15, 17 received broadcast from sensor node 11.

Snapshot 5 shows the locators which performed distance bounding with sensor node 11. Locators which performed distance bounding with sensor node 11 is indicated in orange color, other locators which are not involved in localization are turned as blue. Here the locators 9, 12, 13, 15, 17 are performing distance bounding with sensor node 11.
Snapshot 6 shows locators passed in in trust evaluation by sensor node 11. The locator which passed in trust evaluation are shown in purple color. Rest of the locators which are not involved in localization are shown in blue color. Here the trusted locators are 9, 12, 13, 15, and 17.

Since sensor node 11 is within the triangle formed by trusted locators, it is localized and it is shown in yellow color in the snapshot 7.
Locators = {0, 6, 17, 15, 13, 12, 9, 1}
Enter the sensor to be localized: 11
Transmitting INIT Message to locators
Locators in the set LDBs = {17, 15, 13, 12, 9}
Locators in the set LTs = {17, 15, 13, 12, 9}
Verifiable Trilateration computed coordinates for Node 11 is: 375.935, 260.499

Case 2: Unsuccessful localization due to less number of locators in the set LTs.

In the case of unsuccessful localization due to less number of locators in the set LTs, there are not sufficient trustworthy locators are there to form a triangle around the sensor node. Hence localization fails.

Snapshot 8 shows sensor node 7 is selected for localization. Node 7 is shown in red color to indicate that this sensor node is selected for localization.

Snapshot 9 shows sensor node 7 broadcasting init messages to locators which comes in the power range of 7. The locators which receive broadcast from sensor node 7 are turned to pink color.

Snapshot 10 shows the locators which receives broadcast of INIT message from sensor node 7. The locator which comes in sensor-to locator range of sensor node 7 receives this broadcast. Locators which received broadcast from sensor node 7 are turned as pink, otherwise blue. Here locators 0, 1, 6, 9, 13 received broadcast from sensor node 7.

Snapshot 11 shows the locators which performed distance bounding with sensor node 7. Locators which performed distance bounding with sensor node 7 is indicated in orange color, other locators which are not involved in localization are turned as blue. Here the locators 0, 1, 6, 9, 13 are performing distance bounding with sensor node 7.

Snapshot 12 shows locators passed in trust evaluation by sensor node 7. The locator which passed in trust evaluation are shown in purple color. Rest of the locators which are not involved in localization are shown in blue color. Here the trusted locators is 0.

Snapshot 13 shows sensor node 7 which fails to localize. Since there is only one trusted locator Verifiable Trilateration cannot be performed, localization fails.
Locators = \{0, 6, 17, 15, 13, 12, 9, 1\}
Enter the sensor to be localized: 7
Transmitting INIT Message to locators
Locators in the set LDBs = \{0, 1, 6, 13, 9\}
Locators in the set LTs = \{0\}
Localization fails.

Case 3: Unsuccessful localization due to failure of Verifiable Trilateration.

In the case of unsuccessful localization due to failure of Verifiable Trilateration, even though there are sufficient trustworthy locators are there any 3 locators of those trustworthy locators does not form triangle around the sensor node. Hence localization fails.

6. RESULTS

Simulation parameters are as follows. 20 sensor nodes are randomly placed within the square area of size 500*500 and locators are randomly placed with varying number. Threshold is set to 0.7.

Fig.2 shows the percentage of trusted locators a sensor can get vs. number of locators for varying G. Since the trust evaluation depends on G, as the G and number of locators increases, the percentage of trusted locators also increases.

![Fig. 2: Percentage of trusted locators a sensor can get vs. number of locators for varying G](image)
Fig. 3 shows the probability, that a sensor can perform Verifiable Trilateration vs. $|LT_s|$. Since the sensor is included within more than one triangle of locators. The probability of performing Verifiable Trilateration increases as the number of locators increases.

![Fig. 3: Probability, that a sensor can perform Verifiable Trilateration vs. $|LT_s|$](image)

Fig. 4 shows percentage of sensors localized vs. number of locators for varying G. The percentage of sensors localized increases as the number of locators increases. As G increases the sensor-to-locator range also increases. As a result more locators are included in localization process hence the percentage of sensor getting localized also increases.

![Fig. 4: Percentage of sensors localized vs. number of locators for varying G](image)

7. CONCLUSION

Here we propose a secure localization scheme by modifying Robust Position Estimation algorithm, which provides more security than the existing one. WSN localization is used to estimate the locations of the sensors with initially unknown positions in a network using the available priori knowledge of positions of a few specific sensors in the network. In this work distance bounding
protocol is used find the distance enlargement attack, and trust model is employed to rule out the untrustworthy locators.

And finally Verifiable Trilateration scheme is used to compute the position of the sensor node in which any three locators which form a triangle around sensor node are selected for localization process. Verifiable Trilateration and Distance Bounding protocol together resist wormhole attack and trust model helps to reduce the impact of compromised network entities. In order to compute the position of the sensor node successfully at least three locators are needed and any three trusted locators should form triangle around the sensor node.

REFERENCES

Proceedings Papers


Books


Conferences

