TROPE: TRUST BASED SECURE ROBUST POSITION ESTIMATION IN WIRELESS SENSOR NETWORKS

Nirmala M B[1] , A S Manjunath[2]

Department of Computer Science and Engineering,Siddaganga Institute of Technology, Tumkur, Karnataka, India

Abstract

Secure localization is a critical issue in wireless sensor networks. Providing a certain degree of localization accuracy at the presence of malicious beacons becomes a challenging task. Robust Position Estimation (ROPE) is one of the secure localization systems. However, this system suffers from compromised network entities. Trust Based Secure Robust Position Estimation filters the compromised network entities with the use of trust model. Simulation results and analytical reasoning shows that the security is provided by this scheme with minimal energy consumption.

Keywords

Localization, Robust, Trust, Compromised network entities.

1. INTRODUCTION

Location awareness plays a vital role in Wireless Sensor Network (WSN) since the sensors need to report their position information along with the data they sensed. Application such as routing, data tagging, node identification depends on the location information of the sensor node. In addition localization is essential in civilian and military applications including military operations, data acquisition in hazardous environments, health monitoring.

In recent years localization in WSNs attract considerable research interest. As a result numerous localization algorithms are proposed. However, these localization techniques have not taken external and internal attacks into account.

It is important to secure the localization process since the sensors are deployed in hostile environment, in which malicious adversaries can inject bogus location information, extracts cryptographic information and so on. Therefore any localization scheme must have a mechanism to estimate the location securely, and it has to perform location verification.

The Robust Position Estimation (ROPE) [1] is one of the secure localization schemes which perform location estimation and verification in a robust way without central management. ROPE requires deployment of small number of locators. However, in this scheme the impact of compromised node attack can be reduced with the expense of increased reference point density.

To fight against compromised network entities with small number of reference points, a trust evaluation model [5] is added in TROPE scheme. Trust Model rules out the untrustworthy locators, so the impact of compromised entities can be reduced.

The rest of this paper is organized as follows. Section 2 gives the related work. Section 3 describes background work. Section 4 details proposed scheme. Section 5 presents security analysis. Simulation results and analysis is shown in Section 6. Finally, conclusion is in Section 7.

2.Related work

The secure localization and some of the existing secure localization techniques have been discussed in the following sections.

2.1 SPINE

A secure positioning system based on distance bounding and verifiable Multilateration. SPINE[2] is a range-dependent secure positioning scheme, that estimates the location of a sensor by verifying the distance of the sensor to at least three reference points. The location estimation is performed centrally and once a sensor is aware of its location it also becomes a reference point. Hence, sensors rely on other sensors as well as the central authority to securely acquire their location. Though SPINE is robust against attacks in WSN, it requires the deployment of a high number of reference points to achieve localization.

2.2 SeRLoc

Lazos and Poovendran propose a novel scheme for localization of nodes in WSNs in untrusted environments called SeRLoc[3]. SeRLoc is a range-free, distributed, resource-efficient localization technique in which there is no communication requirement between nodes for location discovery. SeRLoc is robust against wormhole attacks, Sybil attacks and sensor compromise.

SeRLoc considers two sets of nodes: *N*, which is the set of sensor nodes equipped with omnidirectional antennas, and *L*, which is the set of locator nodes equipped with directional antennas. The sensors determine their location based on the location information transmitted by these locators. Each locator transmits different beacons at each antenna sector with each beacon containing two pieces of information: the locator coordinates and the angles of the antenna boundary lines with respect to a common global axis. Using directional antennas improves the localization accuracy.

In SeRLoc, an attacker has to impersonate several beacon nodes to compromise the localization process. Also, since sensor nodes compute their own location without any assistance from other sensors, the adversary has no incentive to impersonate sensor nodes. Wormhole attacks are thwarted in SeRLoc due to two unique properties: sector uniqueness property and communication range violation property.

2.3 HiRLoc

Lazos and Poovendran propose a high-resolution, range independent localization technique called HiRLoc[4]. 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. It is robust to security threats like wormhole attacks, Sybil attacks and compromising of the network entities by virtue of two special properties: antenna orientation variation and communication range variation. In HiRLoc, Lazos and Poovendran have used cryptographic primitives to ensure the beacons from the same locator. This relaxation helps in improving the accuracy of location estimation.

2.4 ROPE

Robust Position Estimation (ROPE) a hybrid approach that provides robust location computation and verification, without centralized management and vulnerability to jamming. ROPE limits the ability of an adversary to spoof a sensor's location by launching well known attacks in WSN. To quantify the impact of attacks against ROPE, the authors introduced a novel metric called Maximum Spoofing Impact (MSI) that denotes the maximum distance between the actual location of the sensor under attack, and any possible spoofed location. ROPE limits the MSI while requiring the deployment of a significantly smaller number of reference points, compared to the only previously known jamming resistant solution[2].

2.5 Trust based localization

Trust based localization [5] is a secure localization scheme proposed by T. Zhang, J. He and Y. Zhang, in which the sensor nodes evaluate the trust value of locators. The trust evaluation involves identity evaluation and behaviour evaluation.

3. BACKGROUND

TROPE uses Distance Bounding, Verifiable Trilateration scheme and Trust Model to securely compute position of sensor node. Descriptions of these works are as follows.

3.1 Distance Bounding

Distance bounding protocol verifies that a claimant node u being at a distance d_{uv} from verifier node v cannot claim to be at a distance less than d_{uv}. This protocol is proposed by Brands and Chaum [6]. Fig. 1 shows the algorithm of distance bounding protocol. First claimant u generates a commit to random nonce N_u and sends it to verifier v. Then verifier v replies with a challenge nonce N_v to u. N_v is sent to the claimant u in the reverse order, and verifyer v starts measuring time as soon as the last bit of N_v is sent. After receiving N_v, claimant u sends $N_u \oplus N_v$ to verifier v. As soon as the last bit of $N_u \oplus N_v$ is received by verifier v, it stops the timer and converts the measured time t_{uv} to distance d_{uv}. In the final step u authenticates itself by sending the decommit value d with the transmission encrypted by pair wise key K_{vu}. After that verifier v verifies that N_u received corresponds to commit and decommit pair (c,d').

u: **Generate** random nonce N_u
: **Generate** commitment (c, d) = commit (N_u)
$u \rightarrow v$: c
v: **Generate** random nonce N_v
$v \rightarrow u$: N_v (*bits sent from MSB to LSB*)
$u \rightarrow v$: $N_u' \oplus N_v$ (*bits sent from LSB to MSB*)
v: **Measure** time t_{uv} between sending N_v and receiving $N_u \oplus N_v$
$u \rightarrow v$: $E_{K_{uv}}(u, N_u, N_v, d)$
v: **Decrypt** message and verify if $N_u' = \text{open}(c, d)$

Figure 1. Algorithm for the distance bounding protocol.

3.1 Verifiable Trilateration

Verifiable Trilateration [9] is a technique for determining the position of the sensor nodes in a secure way. Assume that there are three verifiers v_1, v_2 and v_3 which are trustworthy. These three verifiers perform authenticated distance estimation of claimant u. Then estimates the position of the claimant u based on distance obtained. If the computed position falls in the triangle formed by three verifiers then the position of u is verified otherwise not verified.

3.2 Trust Model

The trust evaluation value of a locator is computed using the formula (1) in which T_{ji} denotes evaluation value on locator i by locator j, T_{ji} denotes trust value on i based on self evaluation by j. T_{oi} denotes trust value on i based on evaluation by j's neighbouring locator o, and α denotes weight of the evaluation values.

$$T_{ji} = \alpha . T_{ji} + (1 - \alpha) \frac{\sum_{o=1}^{n} T_{oi}}{n} . \quad (1)$$

The trust evaluation value from self-evaluation is determined using formula (2) in that T_{ji} denotes trust value on locator i for locator j, R is communication range, Δd denotes distance between the position claimed by i and estimated by j [7, 8].

$$T_{ji} = \begin{cases} \frac{(R - \Delta d_{ji})}{R}, & \frac{(R - \Delta d_{ji})}{R} > \Delta d \\ 0, & \frac{(R - \Delta d_{ji})}{R} < \Delta d \end{cases} . \quad (2)$$

Sensor node collects the evaluation values from their neighbouring locators and computes the average value using formula (3) in which T_{ui} denotes the trust value on locator i for senor node u, T_{mi} denotes the trust value on i evaluated by locator m where m is a neighbouring locator to u and n is the number of such neighbouring nodes.

$$T_{ui} = \frac{\sum_{m=1}^{n} T_{mi}}{n} . \quad (3)$$

4. TRUST BASED SECURE ROBUST POSITION ESTIMATION (TROPE)

Consider a two tier network which contains randomly deployed sensors to sense the environment and randomly deployed locators to act as data collection points to know their position via manual configuration or GPS system. The network assumptions are listed in Table 1. Both sensors and locators perform nanosecond processing required for Distance bounding. 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 $r_{sL} = rG^{1/\gamma}$ [6], where G denotes the antenna directivity gain of locators antenna and γ denotes the signal attenuation factor. It is assumed that each sensor s shares a pair wise key $K^{s}_{L_i}$ with each L_i to perform cryptographic operations.

Table 1. Network Assumptions

	Sensors	Locators
Area	A	A
Density	p_s	$p_L << p_s$
Antenna Type	Omnidirectional	M directional Antenna with beamwidth $\frac{2\pi}{M}$

Trust based secure Robust Position Estimation scheme contains two phases. First phase is location estimation in which sensor estimates its location using Distance bounding, Trust Model and Verifiable Trilateration. Second phase is location verification of sensor by locator through Distance Bounding.

Location Estimation 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 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}

$$LDB_s = \{L_i : \| L_i - s \| \leq r_{sL} \} \quad (4)$$

Step 3: For every locator L_i of set LDB_s, sensor node s collects the trust evaluation value of locator L_i as in trust model and checks 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.

$$LT_s = \{L_i : L_i \in LDB_s, T_{sL_i} \geq Threshold\} \quad (5)$$

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.

s: **broadcast** ID_s
for all L_i that receive broadcast from *s*
    L_i: **perform** *Distance Bounding* with *s*
    s: **define** $LDB_s = \{ L_i : \| L_i - s \| \leq r_{sL} \}$
endfor
for all $L_i \in LDB_s$
    s: **compute** *Trust Evaluation Value* of L_i
    s: **define** $LT_s = \{ L_i : L_i \in LDB_s, T_{sL_i} \geq Threshold \}$
    s: **sort** LT_s such that
    $LT_s = \{ L_i : L_i \in LT_s, T_{sL_i} \geq T_{sL_{i+1}} \}$
    if $(L_i, L_j, L_k) \in LT_s$ such that
        $\exists$ *s inside* $\Delta L_i L_j L_k$
        s: **compute** $\hat{s}$:= *Verifiable Trilateration*
        s: **notify** $E_{K_{L_i}^s}$ (Termination), $\forall L_i \in LDB_s$
    else
    Localization fails
Endfor

Figure 2. Algorithm for Trust Based Robust Position Estimation Scheme

the locators $L_i \in LDB_s$, with the transmission of computed position encrypted by the pair wise key and terminates the algorithm.

Fig. 2 shows the algorithm of Trust based Robust Position Estimation scheme.

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.

5. SECURITY ANALYSIS

5.1 Attacker model

It is assumed that attacker can spoof the location estimated by the sensors. As a result sensors try to estimate the position falsely. If the localization of sensor node fails, it is assumed that it is under attack. Also it is assumed that attacker is capable of jamming the signals of network entities.

5.2 Wormhole attack

In TROPE scheme, when sensor node broadcasts ID_s, attacker receives this information and tunnels this information to another point in 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 $L_k \in LT_{sk}$. 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 r s to L_i is enlarged then any one of the other two locators need to reduce the distance. This is impossible due to distance bounding. Hence, the spoofing of position of s by attacker is not possible. If the attacker jams the signals from all the locators then localization fails.

5.3 Compromised node attack

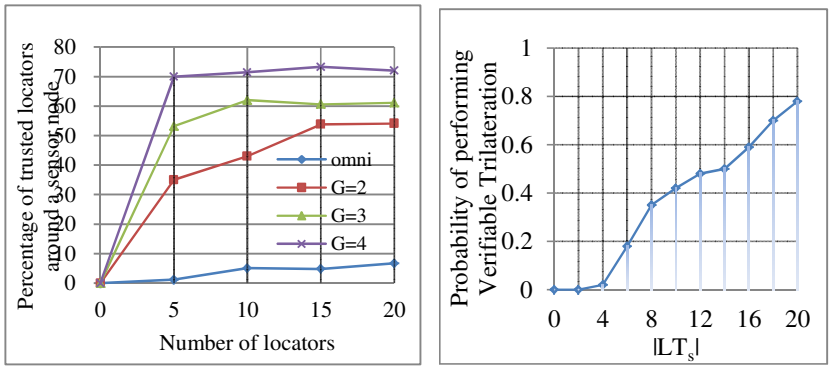
A network entity is said to be compromised if attacker gains authority of all the information related to the entity. In TROPE, if the attacker adds bogus location information to the compromised locators, then this can be detected by the trust model and those untrustworthy locators are not included in localization.

6 PERFORMANCE ANALYSIS

The idea of TROPE is simulated in NS2. The simulation parameters are given in the Table 2.

Table 2. Simulation parameters

Parameters	Details
Area	500*500
Number of sensor nodes	100
Threshold	0.7



(a) (b)

Figure 3 (a) Percentage of trusted locators a sensor can get vs. number of locators for varying G. (b) Probability, that a sensor can perform Verifiable Trilateration vs. $|LT_s|$.

Fig. 3(a) 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. 3(b) 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. 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. Hence more locators are included in localization process and also the percentage of sensor nodes getting localized also increases. Figure 5 shows the energy consumed for sending and receiving one byte of data from a node I to a node j over a distance of d meters. As the number of locators increases the energy consumption also increases.

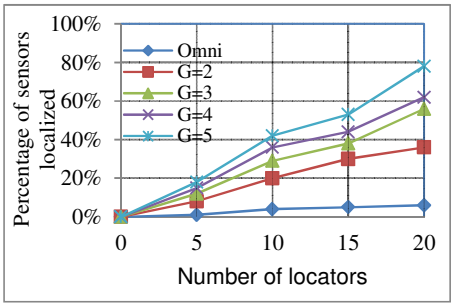


Figure 4. Percentage of sensors localized vs. number of locators for varying *G*

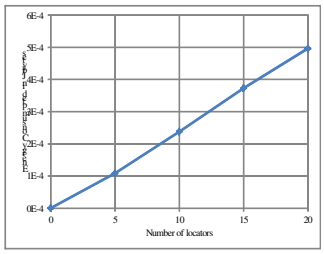


Figure 5: Energy consumed vs. number of locators

7 CONCLUSION

This work presents a secure localization scheme called Trust Based Robust Position Estimation (TROPE) for wireless sensor networks. In this work secure localization and location verification problem is considered. Verifiable Trilateration and Distance Bounding protocol resist wormhole attack and trust model helps to reduce the impact of compromised network entities. The proposed scheme eliminates the compromised entities which provide the bogus location information.

8. REFERENCES

[1] L. Lazos, R. Poovendran, and S. Capkun. ROPE: Robust position estimation in wireless sensor networks, In Proceedings of IPSN, April 2005.

[2] S. Capkun and J.-P. Hubaux. Secure positioning of wireless devices with application to sensor networks, In IEEE INFOCOM 05, 2005.

[3] L. Lazos and R. Poovendran, SeRLoc: Secure Range-Independent Localization forWireless Sensor Networks, in Proceedings of WISE, Philadelphia, PA, Oct. 2004, pp.21–30.

[4] L. Lazos and R. Poovendran. HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks. IEEE Journal on Selected Areas in Communications, VOL. 24, NO. 2, February 2006.

[5] T. Zhang, J. He and Y. Zhang. Trust Based Secure Localization in Wireless Sensor Networks, In International Symposium on Intelligence Information Processing and Trusted Computing, 2011.

[6] S. Brands and D. Chaum, Distance-bounding protocols, In Workshop on the theory and application of cryptographic techniques on Advances in cryptology, pp. 344-359. Springer-Verlag New York, Inc., 1994.

[7] D. Niculescu and B. Nath, Ad Hoc positioning system (APS) using AOA, In Proceedings of 22nd Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE Press, March 2003, pp. 1734- 1743, doi: 10.1109/INFCOM.2003.1209196.

[8] P. Bahl and V.N. Padmanabhan, RADAR: an in-building RF-based user location and tracking system, In Proceedings of 19th Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE Press, March 2000, pp. 775-784, doi: 10.1109/INFCOM.2000.832252.

[9] Srdjan Capkun and Jean-Pierre Hubaux, Secure Positioning in Sensor Networks, IEEE Journal on Selected Areas in Communications (JSAC): Special Issue on Security in Wireless Ad Hoc Networks, February 2006.

[10] D. Liu, P. Ning, W. Du. Attack-Resistant Location Estimation in Sensor Networks. In Proceedings of The Fourth International Conference on Information Processing in Sensor Networks (IPSN ’05), pages 99-106, April 2005.