

2012 International Conference on Medical Physics and Biomedical Engineering

## A Signcryption-based Secure Localization Scheme in Wireless Sensor Networks

Ting Zhang<sup>1</sup>, Jingsha He<sup>2</sup>, Xiaohui Li<sup>1</sup>, Qian Wei<sup>1</sup>

<sup>1</sup>College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China

<sup>2</sup>School of Software Engineering, Beijing University of Technology, Beijing 100124, China  
[zhangting06@emails.bjut.edu.cn](mailto:zhangting06@emails.bjut.edu.cn), [jhe@bjut.edu.cn](mailto:jhe@bjut.edu.cn), [lixiaohui@emails.bjut.edu.cn](mailto:lixiaohui@emails.bjut.edu.cn)

---

### Abstract

Localization technology in wireless sensor networks has great significance for theoretical study and practical applications. However, most current localization schemes have failed to pay enough attention to security issues. In this paper, we propose a novel secure localization algorithm named signcryption-based secure localization scheme (SSLS) that allows sensors to ensure the confidentiality and integrity of their location information. Analysis shows that SSLS can enhance the security and robustness of localization through the signcryption mechanism while simulation results help to verify the performance of SSLS in that distance measurement errors can be limited within a small range.

© 2012 Published by Elsevier B.V. Selection and/or peer review under responsibility of ICMPE International Committee.

**Keywords**-wireless sensor networks, secure localization, signcryption.

---

### Introduction

Wireless sensor networks (WSNs) have gone through rapid development in recent years and have been applied widely in military and industrial applications. The technologies of WSNs are becoming popular along with the decreasing cost of sensors and increasing functionality of sensor nodes. As core functionality in WSNs, localization technology has been paid a great deal of attention.

Most current localization methods in WSN are based on the assumption of a secure network environment. However, the actual application scenarios are more complex. Any mechanism must guarantee the accuracy of localization under threats and attacks. In addition, with various requirements of different applications, the secrecy of localization has also received increasing attention and some progress has been made. Nonetheless, there are still many security problems that need to be solved. There are two common types of attacks with one being to deploy a beacon node to broadcast fake location messages and

the other being to intercept messages from legal beacon nodes in order to cheat other nodes in a WSN. To fight against the above attacks, in this paper, we propose a signcryption-based secure localization scheme (SSLS) to improve the security and robustness of localization against attacks in WSNs.

The rest of this paper is organized as follows. In Section II, we review related work on localization in WSNs. In Section III, we present the secure localization scheme based on signcryption and describe some implementation details. In Section IV, we analyze SSLS in terms of security and localization performance. Finally, we conclude this paper in Section V in which we also describe our future work.

## Related Work

For most applications of WSNs, the data collected by a sensor node are not very useful without the position information. Therefore, localization is significant for many WSN applications. Current localization algorithms can be divided into two groups: range-based algorithms and range-free algorithms with the difference being whether the distance between the nodes is determined through physical measurement. Typical range-based algorithms include Ad Hoc positioning system (APS) [1], Ad Hoc localization algorithm (AHLs) [2] while typical range-free algorithms include the centroid algorithm [3], the distance vector-hop (DV-Hop) algorithm [4] and the convex optimization algorithm [5]. Although these algorithms can estimate the position of unknown nodes in different ways, they don't have the abilities to resist threats. Recently, some attention has been paid to secure localization technology and, as the result, some new schemes have been proposed with security capabilities. Among them, double guarantee security sensor localization (DGSSL) [6] validates the security of localization information by identifying illegal nodes and the robust position estimation (ROPE) algorithm [7] has a good anti-jamming capability and good performance in preventing Sybil attacks. However, these secure localization schemes have some limitations such as possessing high cost of communication and limited capability to resist multiple types of attacks. To enhance the security of localization with low cost, we present a novel scheme that can improve the reliability and integrity of position messages.

## Signcryption-based Secure Localization Scheme

### *Security Goals*

In this paper, the position of an unknown node is calculated by using the location information of the beacon nodes in a WSN. Therefore, the integrity of location messages as well as the reliability of message sources is very important during the localization process. In some applications, location information should also be kept secret to protect the privacy of the corresponding sensors. In this paper, an appropriate encryption scheme is presented to protect location messages.

The requirements of secure localization scheme in WSNs are as follows.

- Guarantee that the messages for position calculation are sent by legal beacon nodes.
- Guarantee that the messages for position calculation are not tampered with.

In order to meet the first requirement, we should ensure the security of message sources by preventing malicious nodes from broadcasting fake location information. In order to meet the second requirement, we should ensure the integrity of location messages by preventing malicious nodes from modifying the correct position information. In SSLS, we apply an appropriate encryption and signature scheme in WSN localization to resolve the above issues. Due to limited calculation capability of wireless sensors, the simplicity and feasibility of the encryption scheme should also be considered. Therefore, we propose a signcryption scheme based on elliptic curve for WSN localization since elliptic curve encryption has a shorter key and a faster computing speed to improve the security of localization. Compared to existing localization methods, our scheme has smaller distance measurement errors and more stable accuracy against attacks. In addition, signcryption on the curves can save 58% computational cost and 40% communication overhead compared to signature-then-encryption on elliptic curves [8]. In the localization process, the computational cost of localization nodes is more than that of the beacon nodes. We improve

the signcryption scheme to reduce the unnecessary computation in unsigncryption and verification of SSLS. Sensors will discard the fake messages before any hash computation. We also introduce the notion of node groups in a WSN in which we divide the nodes into different groups and the nodes in the same group share a pair of keys in signcryption. The above measures help to make localization more effectively.

### *Secure Localization Algorithm*

SSLS solves the problems of identity authentication and location message protection, which helps reduce the chance of attacks, increase the accuracy of localization and make the localization system more secure. Main steps of the algorithm are described as follows.

- Each beacon node signcrypts the location information and send the message to the sensor nodes around.
- Each unknown sensor node verifies the received location message through unsigncryption. If successful, the message will be accepted by the unknown node; otherwise, the message will be discarded.
- The unknown node calculates its positions using all the collected location information.
- Nodes will update their positions if necessary.

One implementation of the SSLS is described as follows. In the SSLS, each node  $i$  has its unique identifier  $ID_i$  and each beacon node has a pair of keys. For example, beacon node  $A$ 's keys can be expressed as  $(P_A, S_A)$  in which  $P_A$  and  $S_A$  are the public key and the private key of  $A$ , respectively. In this scheme, nodes in a WSN are organized into groups and all the nodes in the same group  $j$  share a pair of key  $(P_{g_j}, S_{g_j})$ . An elliptic curve  $E$  over finite field  $F_p$  is used in the scheme,  $q$  is a large prime number whose length is approximately that of  $p$ , and  $Q$  is a point with the order  $q$  which is chosen randomly from the points on  $E$ .

1) *Message signcryption*: A beacon node signcrypts its location information using its private key and the group's public key and then broadcasts the information to the nodes around. Signcryption could allow a receiver to verify the identity of the sender. Meanwhile, since illegal receivers cannot recover the original message, the signcryption could filter out attackers in localization. This measure guarantees the security of localization in two ways. First, a location message can be trusted only when it is sent by the beacon node. Second, the receiver can recover the original message only when it is a legal member in the same group. The steps of signcryption in the beacon node  $A$  are described as follows.

- Choose an integer  $k$  from  $[1, \dots, q-1]$  randomly.
- Compute the keys for encryption and signature  $(k_1, k_2) = H(kP_{g_j})$ .
- Compute digest  $r = \text{HMAC}(k_1, m)$ .
- Compute  $s = (k / (r + S_A)) \bmod q$ .
- Encrypt  $c = E_{k_2}(m)$ .
- Broadcast message  $\{ID_A \parallel r \parallel s \parallel c\}$ .

2) *Message unsigncryption and verification*: An unknown node unsigncrypts a received location message using the group's private key and the beacon node's public key following the steps below.

- Receive message  $\{ID_A \parallel r \parallel s \parallel c\}$  and calculate  $M = sS_{g_j}(rQ + P_A)$ .
- Compare  $M$  and  $kP_{g_j}$ . If  $M \neq kP_{g_j}$ , discard the message and mark the sender node as a malicious node. If  $M = kP_{g_j}$ , continue with the following steps.

- Calculate  $(k_1, k_2) = H(M)$ .
- Decrypt  $m = D_{k_2}(c)$ .

3) *Position calculation*: The message from a beacon node contains the ID and location of the node. Every time such a message is received from a trusted beacon node, an unknown node calculates the

distance between itself and the beacon node using time difference of arrival (TDOA) measurement [2] and stores the message {beacon node's ID, distance} in a list.

TDOA measurement can achieve high accuracy and low hardware requirement. In this measurement, a node would send two signals of different frequencies, e.g., Ultrasonic and RF signals, as shown in Fig. 1. The receiver calculates the distance  $d$  between itself and the sender based on difference between the arrival times of the two signals based on equation (1) in which the propagation velocities of the RF and the Ultrasonic signals are  $c_1$  and  $c_2$ , respectively and the arrival times of the RF and the Ultrasonic signals are  $t_1$  and  $t_2$ , respectively.

$$d = (t_2 - t_1) \cdot c_1 \cdot c_2 / (c_1 - c_2). \quad (1)$$

The purpose of computing the distance between an unknown node and the beacon nodes is to get the location of the unknown node. In order to give the localization a better convergence, SSLS uses trilateration [9] to compute the location of the unknown node immediately after receiving the messages from three trusted beacon nodes. This method can help save a lot of time waiting for location messages from more beacon nodes. The principle of trilateration is shown in Fig. 2 in which we assume that the two-dimensional coordinate of an unknown node  $U$  is  $(x, y)$ , the coordinates of the three detected beacon nodes around  $U$  are  $(x_1, y_1)$ ,  $(x_2, y_2)$ ,  $(x_3, y_3)$  and the distance between  $U$  and the three beacon nodes are  $d_1$ ,  $d_2$ ,  $d_3$ , respectively. According to Euclidean distance formula in equation (2) and assuming that  $n=3$ , the unknown node's position can be inferred in the two-dimensional space as shown in equation (3).

$$(x - x_i)^2 + (y - y_i)^2 = d_i^2, i = 1, 2, \dots, n. \quad (2)$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = 2 \begin{bmatrix} x_1 - x_3 & y_1 - y_3 \\ x_2 - x_3 & y_2 - y_3 \end{bmatrix}^{-1} \begin{bmatrix} x_1^2 - x_3^2 + y_1^2 - y_3^2 + d_1^2 - d_3^2 \\ x_2^2 - x_3^2 + y_2^2 - y_3^2 + d_2^2 - d_3^2 \end{bmatrix} \quad (3)$$

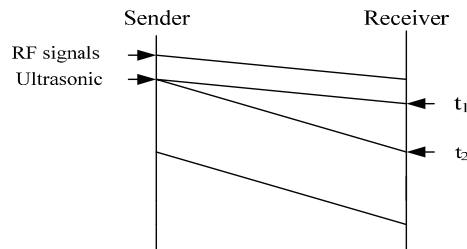


Figure 1. TDOA location principle

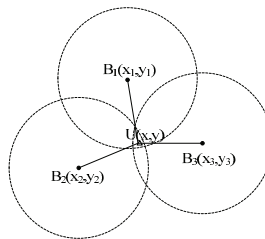


Figure 2. Elements of trilateration

If the number of messages received and accepted by an unknown node is less than three, SSLS will make the trusted nodes send location messages to it. Due to the requirement for fast computation, updating the position of nodes is essential and important.

4) *Position update*: A position update mechanism is proposed here to improve the accuracy of localization. After the first localization, normal nodes may accept location messages from other trusted beacon nodes continuously. If the messages can pass verification, the nodes repeat the localization steps to update their positions.

Every node in the network has a list in which to store the information about beacon nodes around it. The system uses a time threshold  $t$  based on location requirements. After time  $t$  is elapsed since the first location estimation, if the number of beacon nodes accumulated in the list is changed to more than three, the system will start maximum likelihood estimation to update the location. And if the number stays the same, no update is performed. This method helps to ensure accuracy of localization while avoiding excessive computations.

The calculation principle of maximum likelihood estimation is similar to trilateration. Suppose the number of beacon nodes around the unknown node increases to  $n$  with coordinates  $(x_1, y_1), (x_2, y_2) \dots (x_n, y_n)$ , respectively, and the distance between unknown node  $U$  and the beacon nodes are  $d_1, d_2 \dots d_n$ , respectively. According to (2), the unknown node's position can be inferred. In addition,  $n$  distance equations about  $U$  and  $n$  beacon nodes are listed with each of the first  $n-1$  equations minus the last equation. The results are show in (4).

$$\begin{cases} x_1^2 - x_n^2 - 2(x_1 - x_n)x + y_1^2 - y_n^2 - 2(y_1 - y_n)y = d_1^2 - d_n^2 \\ \dots \\ x_{n-1}^2 - x_n^2 - 2(x_{n-1} - x_n)x + y_{n-1}^2 - y_n^2 - 2(y_{n-1} - y_n)y = d_{n-1}^2 - d_n^2 \end{cases} \quad (4)$$

$U(x, y)$  can be calculated by (5) and (6).

$$U = A^{-1}b \quad (5)$$

$$A = 2 \begin{bmatrix} x_1 - x_n & y_1 - y_n \\ \dots & \dots \\ x_{n-1} - x_n & y_{n-1} - y_n \end{bmatrix}, b = \begin{bmatrix} x_1^2 - x_n^2 + y_1^2 - y_n^2 + d_1^2 - d_n^2 \\ \dots \\ x_{n-1}^2 - x_n^2 + y_{n-1}^2 - y_n^2 + d_{n-1}^2 - d_n^2 \end{bmatrix} \quad (6)$$

## Analysis

### Security

In this paper, we improve the security of localization in wireless sensor network in two main aspects with one being that SSLS insures the reliability of location message sources and the other being that SSLS ensures the integrity of location messages. We introduce authentication and signcryption based on elliptic curve in the localization scheme to ensure that location messages can only be sent by legal beacon nodes and cannot be modified by malicious nodes. In the scheme, we can verify the identities of beacon nodes and insure that only the legal group numbers can receive and recover the location messages from the beacon nodes. Our method can limit the flow of location information, filter out malicious nodes and protect confidentiality and privacy of location information effectively.

### Performance

Since the main characteristics of WSN have been fully considered in this localization scheme, SSLS has a better convergence, which helps save consumption in localization and meets the requirements for localization accuracy. This scheme shortens the first time position estimation and lower consumption in localization. When unknown nodes collect enough messages to perform location estimation, the system starts the process immediately and the nodes no longer have to wait for more location messages from other beacon nodes. Further improvement on the accuracy is achieved by updating the positions. Update mode is very flexible so that we can modify the update threshold based on application environment to lower the cost of repeated computation.

We have performed simulations to evaluate SSLS using MATLAB version 7.1, Microsoft Windows XP professional version 2002 and Intel Pentium 4 CPU 3.00GHz with 512MB. The localization scheme implements signcryption mechanism on an elliptic curve  $y^2 \equiv x^3 + ax + b \pmod{q}$ ,  $a=3$ ,  $b=22$ ,  $p=131$ ,  $q=127$ ,  $Q=(2, 6)$ . The distance measurement errors of the experiment are shown in Fig. 3 from which we can see that SSLS can limit the distance measurement errors within a small range.

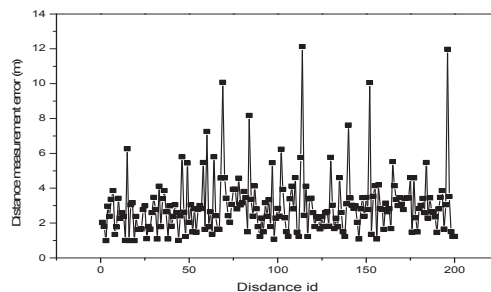


Figure 3. Distance measurement errors

### Conclusion

WSN localization technology should be considered for various application environments. We also need to improve the accuracy of localization through different approaches, such as insuring the reliability of location message sources through authentication, improving localization accuracy through better updating algorithms and improving localization efficiency through introducing trust models. In this paper, we proposed SSLS to improve the security of localization in which the signcryption can effectively filter out malicious nodes without incurring too much computational overhead and communication cost. We also proposed a novel location update mechanism to make the scheme more flexible to meet the requirements of different WSNs. Analysis showed that SSLS has a high security and efficient communication ability in localization.

### References

- [1] D. Niculescu and B. Nath, "Ad hoc positioning system (APS) using AoA," Proc. 22nd Annual Joint Conference of the IEEE Computer and Communications Societies, 2003, pp. 1734-1743.
- [2] A. Savvides, C. Han and M. Strivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," Proc. 7th Annual International Conference on Mobile Computing and Networking, July 2001, pp. 166-179.
- [3] N. Bulusu, J. Heidemann and D. Estrin, "GPS-less low-cost outdoor localization for very small devices," IEEE Personal Communications, Vol 7, Oct. 2000, pp. 28-34.

- [4] D. Niculescu and B. Nath, "DV based positioning in ad hoc networks," *Journal of Telecommunication Systems*, Vol. 22, 2003, pp. 267-280.
- [5] L. Doherty, K. pister and L. El Ghaoui, "Convex position estimation in wireless sensor networks," *Proc. 20th Annual Joint Conference of the IEEE Computer and Communications Society*, April 2001, pp. 1655-1663.
- [6] G. Jingjing, C. Songcan and Z. Yi, "Double guarantee for security localization in wireless sensor network," *Proc. 5th International Conference on Wireless and Mobile Communications*, Aug. 2009, pp. 99-104.
- [7] L. Lazos, P. Radha and S. Capkun, "ROPE: Robust position estimation in wireless sensor networks," *Proc. 4th International Symposium on Information Processing in Sensor Networks*, April 2005, pp. 324-331.
- [8] Y. L. Zheng and H. Imai, "How to construct efficient signcryption schemes on elliptic curves," *Information Processing Letters*, Vol. 68, Dec. 1998, pp. 227-233.
- [9] W.Navidi, W. Murphy and W. Hereman, "Statistical methods in surveying by trilateration," *Computational Statistics & Data Analysis*, Vol. 27, April 1998, pp. 209-227.