International Journal of Computational Intelligence Systems, Vol. 5, No. 5 (September, 2012), 914-923

Secure Sensor Localization in Wireless Sensor Networks based on Neural Network

Ting Zhang
College of Computer Science and Technology
Beijing University of Technology, Beijing 100124, China
E-mail: zhangting06@emails.bjut.edu.cn

Jingsha He*, Yang Zhang
School of Software Engineering
Beijing University of Technology, Beijing 100124, China
E-mail: jhe@bjut.edu.cn

Received 30 Nobember 2011
Accepted 19 June 2012

Abstract

Localization of sensor nodes in wireless sensor networks (WSNs) is very important since it associates spatial context with the data collected by sensor nodes and used in applications. Rapid development of wireless sensor technologies and wide applications of wireless sensor networks have also made security in sensor localization a primary concern as well as a great challenge. Without adequate security measures, the performance of sensor localization, e.g., the accuracy of localization results, cannot be ensured in hostile environments. In this paper, we propose a trust-based secure sensor localization scheme (TSLS) for WSNs following the theory of neural network (NN). The proposed TSLS scheme can ensure that unknown sensor nodes will get credible information to perform localization through the evaluation of beacon nodes in a WSN. The evaluation model is comprised of the evaluation of both the identity and the behavior of beacon nodes as well as a filtering mechanism to deal with the slander behaviors between beacon nodes. Simulation results show that the proposed TSLS scheme can improve the accuracy of sensor localization in hostile environments for both static and dynamic WSNs.

Keywords: Wireless sensor networks, localization, security, trust, neural network.

1. Introduction

Along with the development of electronics and networking technologies, new technologies and applications of wireless sensor networks (WSNs) are rapidly emerging. Examples of sensor network applications include deployments for underwater detection and for intelligent monitoring and control in smart home scenarios. In short, applications of WSNs have been moving along the general trend of ubiquity to bring more convenience in many aspects of human life.

Localization of sensor nodes is one of the basic services and has become a pivotal technological issue in WSNs. In most real applications, data collected from wireless sensors need to be associated with the respective locations of sensor nodes to make the data meaningful and useful. Location information is required for providing many services such as network topology, geographical coverage of networks, routing and other location-based services. Some novel and generic sensor localization algorithms have been proposed among which range-based localization algorithms[1,2] and range-free localization algorithms[3,4] are the most recognized methods. Meanwhile, computational intelligence has been applied to solving various challenging problems in WSNs in recent years including sensor localization[5-8]. Chatterjee proposed the development of a Fletcher–Reeves update-based conjugate gradient multilayered feed-forward neural network for multihop connectivity-based localization of a large number of sensor nodes[6]. Massimo et al. proposed evolutionary algorithms to

* Corresponding author.

ensure localization accuracy for WSNs[7]. Lavanya et al. introduced particle swarm optimization into sensor localization[8] and compared its performance with localization based on artificial bee colony algorithms.

Meanwhile, in many applications, sensor localization often has to confront with the threat of malicious attacks. Thus, the lack of effective security mechanisms has become a serious issue that can affect the correctness and reliability of localization mechanisms. Secure sensor localization has become a great challenge in WSNs. As the result, some methods have been proposed to ensure the security of sensor localization. Some of the methods implement verification measures to reduce the impact of the presence of false location information[9,10] with the common shortcomings being that detection would fail should the signals from beacon nodes get blocked. Some other methods apply robust computing algorithms to improve the reliability of localization schemes[11,12] with the common shortcomings being that they could not effectively fight against conspiracy attacks when too many nodes have been compromised and hence become attackers. Still, some more methods have been proposed to use check pointing as the means of reducing the impact of attacks[13]. However, such methods would have to rely on centralized detection and can thus result in unbalanced load in the WSNs.

Security threats for sensor localization may come in many different ways from both external hostile attacking nodes and internal compromised nodes. A secure localization scheme should be able to fight against both types of attacks. Although most external attacks can be dealt effectively with cryptographic techniques, attacks from internal compromised nodes would render such schemes less effective. Ultimately, the most important thing in a localization system is that sensors need an effective evaluation method so that they can get credible location information from beacon nodes in order to calculate their own locations correctly.

Some methods have already been proposed to fight against attacks from internal compromised nodes, an issue that is more difficult to deal with. Srinivasan proposed a beacon trust system based on distributed reputation[14] in which beacon nodes monitor each other to supervise the location service provided by the beacon nodes. This method can reduce the impact of attacks from malicious internal nodes to a certain degree, but it cannot resist conspiracy attacks. Xu et al. proposed a reputation–based revising scheme[15] in which reputation values are used to reduce the impact of irregular signal patterns and environment noises. This method is only suitable in an more ideal environment since it fails to sufficiently consider malicious attacks. As an effective means of resolving security problems in sensor localization in WSNs, the notion of trust has been introduced. For example, reputation enabled self-modification was proposed to deal with the acoustic target localization problem[16].

In this paper, we propose a trust-based secure sensor localization scheme in WSNs following the approach of neural network (NN), which we call the TSLS scheme. In our proposed scheme, we apply trust evaluation to all the beacon nodes so that trustworthy beacon nodes can be selected through evaluation to provide credible location information. We also perform some simulation to show that our proposed TSLS scheme can improve the accuracy of sensor localization in hostile environments.

The main contributions of this paper are as follows. First, we propose a trust-based secure range-based sensor localization scheme to improve the performance of localization of unknown sensor nodes in WSNs. Second, we propose a trust evaluation model for beacon nodes that evaluates not only the identity but also the behavior of beacon nodes to determine their trustworthiness and hence the credibility of their location information they provide. Third, we introduce a median method in our proposed secure localization scheme to deal with slander behaviors between beacon nodes. Fourth, considering the dynamic characteristics of WSNs, we introduce the notion of probability into our simulation, analyze our proposed TSLS scheme with respect to the accuracy of sensor localization and compare our scheme with some other existing methods to demonstrate the effectiveness and advantages of our TSLS scheme.

The rest of this paper is structured as follows. In Section 2, we present a framework for sensor localization based on the theory of neural network. In Section 3, we propose a trust model for sensor localization in WSNs. In Section 4, we present the details of the TSLS scheme and describe its working process with respect to neural network. In Section 5, we perform some simulation on the TSLS scheme to evaluate its performance and to compare it with some other existing methods. Finally, in Section 6, we

conclude this paper in which we also describe our future work.

2. Neural Network based Framework for Sensor Localization

In sensor localization, the location of an unknown sensor node is usually calculated or estimated using the location information provided by beacon nodes in which it is assumed that the beacon nodes are able to position themselves and the unknown sensor nodes need to determine their own locations based on location information from other nodes that have located themselves such as the beacon nodes.

In general, unknown sensor nodes estimate their own locations based on location information from beacon nodes. Consequently, the correctness and reliability of the location information from beacon nodes becomes critical. However, since unknown sensor nodes are not capable of positioning themselves independently, it is difficult for them to verify the correctness of the location information from the beacon nodes.

Thus, the goal is clear and simple, i.e., to derive localization results for unknown nodes based on location information from beacon nodes. This process can be modeled using the theory of neural network as a mapping from beacon information to localization results that requires some data processing in the middle. The theory of neural network can thus guide us to design a secure localization scheme in WSNs as neural network is a simplified model that is abstracted from artificial neural network with the point of view of information processing through mathematical methods. The structure and function of artificial neural can be shown in Fig. 1 in which the input layer simulates the dendrite of neurons to receive the input signals, P_1 simulates the soma of neurons to process the received data, P_2 simulates the axon of neurons to control the data output, and the output layer simulates the synapse of neurons to output the results, respectively.

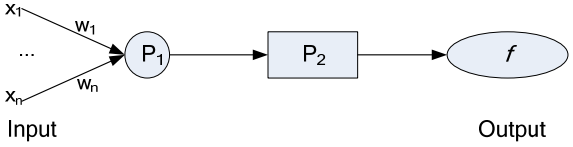


Fig.1. The structure and function of artificial neural.

To achieve secure localization and to ensure the accuracy of localization results in hostile environments, we apply neural network classification in processing the information from the beacon nodes in WSNs, classify the beacon nodes using a threshold trust value set for the localization system, screen out untrusted beacon nodes and use position information only from trustworthy beacon nodes to perform localization for unknown sensor nodes.

3. The Trust Model

Based on the above framework, we first propose a trust evaluation model for the unknown sensor nodes to evaluate and establish trust on the beacon nodes, filter out untrustworthy beacon nodes, and then apply location information received from trustworthy beacon nodes for them to perform localization. Evaluation of the beacon nodes in our trust model includes the use of both identity evaluation and behavior evaluation and the corresponding trust evaluation scheme is therefore described in three parts: identity evaluation, behavior evaluation and colligation evaluation model.

We assume in our description that every beacon node has a unique identifier (ID) and all the legal beacon nodes share a group key k in the network. The hash value of the ID, i.e., $H(ID)$, of a legal beacon node is made public information.

3.1. *Identity evaluation*

The purpose of identity evaluation is to not use location information from illegal nodes. In the network, legal beacon node i sends a message $\{ID_i \| (x_i, y_i) \| H(ID_i \| (x_i, y_i) \| H(ID_i))\}_k$ in which $H()$ denotes a hash function and $\{\}_k$ denotes an encryption function using key k.

All the neighboring beacon nodes to node i verify the identity of i after receiving the message from i by applying decryption to the message with k, computes $H(ID_i \| (x_i, y_i) \| H(ID_i))$ using the public information $H(ID_i)$ as well as the decrypted information, and then compares it with the received information. If the computed value is the same as the received one, beacon node i passes the verification and the identity evaluation value on node i is set to 1. Otherwise, the verification fails and the identity evaluation value for node i is set to 0.

3.2. *Behavior evaluation*

Identity evaluation cannot fight against attacks from compromised beacon nodes. Therefore, the detection of internal attacking nodes can rely on the evaluation of node behavior. In order to obtain a more reasonable evaluation result, in our model, we use both self-evaluation and reference evaluation by other beacon nodes in the evaluation process.

However, we need to deal with a new issue in reference evaluation of other beacon nodes, that is, malicious beacon nodes may slander their neighboring beacon nodes. In a real network, there may be some malicious beacon nodes who can slander other trustworthy beacon nodes, thus affecting trust evaluation on each other. To reduce the impact of this problem to localization, we introduce a filtering mechanism using a median value. After a beacon node collects the evaluation values on behavior from its neighboring beacon nodes, it will calculate the median evaluation value and apply it following the steps of the trust model described below so that the beacon node can reject the slanderous evaluation values that deviate from normal evaluation values and finally calculate a more reasonable value for behavior evaluation.

The behavior evaluation value is determined using Eq. (1) in which $T_{B_{ji}}$ denotes the behavior evaluation value on beacon node B_i by beacon node B_j, $T_{s_{ji}}$ denotes the behavior trust value on B_i based on self-evaluation by B_j, $T_{s_{Nji}}$ denotes the behavior trust value on B_i based on evaluation by B_j's neighboring beacon nodes, $Me()$ denotes the median function, and α denotes the weight for the evaluation values.

$$T_{B_{ji}} = \alpha \cdot T_{s_{ji}} + (1-\alpha) Me(T_{s_{Nji}}) \tag{1}$$

The behavior evaluation value from self-evaluation is determined using Eq. (2) in which $T_{s_{ji}}$ denotes the behavior trust value on beacon node B_i from beacon node B_j, R denotes the normal transmission radius of beacon nodes, and Δd_{ji} denotes the difference between the distance estimated by B_j using coordinate information claimed by B_i and the one estimated by using a ranging technique, such as time of arrival (TOA)[17,18], time difference of arrival (TDOA)[19,20], received signal strength indicator (RSSI)[21,22] and angle of arrival (AOA)[23,24].

$$T_{s_{ji}} = \begin{cases} (R - \Delta d_{ji}) / R & \Delta d \le R \\ 0 & \Delta d > R \end{cases} \tag{2}$$

The evaluations by other beacon nodes are essential when behavior trust value of a beacon node is determined. As illustrated in Fig. 2, all the nodes B_1, B_2, B_3 and B_4 have legal *ID*s and share a key k. They are thus all legal nodes according to identity evaluation. But if B_1 lies to other nodes about its location, e.g., B_1', it would be difficult for B_2 to identify the false location information unless it is able to measure both signal strength and signal angle. If B_2 takes into account the evaluations on B_1 from the other beacon nodes, B_2 can easily detect that B_1 is not a trustworthy beacon node and can consequently reduce the trust value for B_1.

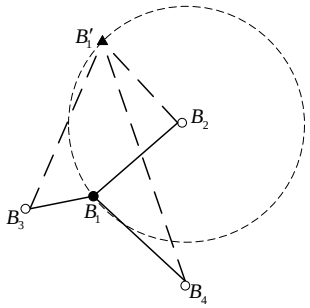


Fig.2. An example attack.

Fig. 3 illustrates the algorithm for the behavior evaluation model that serves our proposed TSLS at beacon node B_i.

Algorithm 1. The behavior evaluation model.

```
while (true) {
  for (node j : neighbors_i)
  {
    // neighbors_i denotes all the neighbors of beacon node i
    if ( Δd_ji < R )
      T_si = (R − Δd_ji) / R
    else
      T_si = 0
    if ( Count(neighbors_i) > 0 )
      T_si = α × T_si + (1 − α) Median(T_neighbors_i)
    else
      T_Bji = T_si
    send()
  }
  sleep( Δt )
}
```

Fig.3. Algorithm for the behavior evaluation model.

3.3. *General evaluation*

Every beacon node can thus derive an identity trust value and a behavior trust value for each of its neighboring beacon nodes and thus compute a general evaluation value for each neighboring beacon node. The general trust value on B_i from beacon node B_j can be computed using Eq. (3) in which T_{ji} denotes the general trust value on B_i by B_j and, $T_{I_{ji}}$ and $T_{B_{ji}}$ denote the identity trust value and the behavior trust value on B_i by B_j, respectively, $Me()$ denotes the median function, and α denotes the weight for the evaluation values.

$$T_{ji} = T_{I_{ji}} \cdot T_{B_{ji}} = T_{I_{ji}}(\alpha \cdot T_{s_{ji}} + (1-\alpha) Me(T_{s_{Nji}})) \quad (3)$$

4. The Sensor Localization Scheme

Our proposed TSLS scheme is an application of the multilayer feed-forward neural network theory for sensor localization in WSNs. The scheme filters out untrusted beacon nodes before completing secure localization. The structure of TSLS is similar to data handling in multilayered feed-forward neural network as shown in Fig. 4.

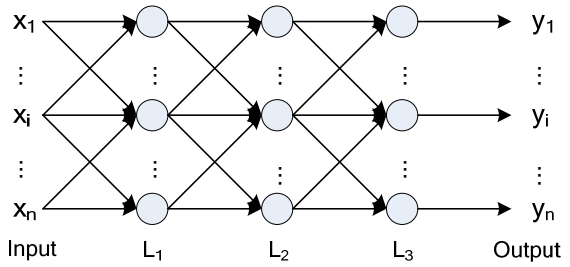


Fig.4. The structure of TSLS.

There are three layers in our proposed TSLS, among which the middle layer includes three components for handling the data and for filtering out untrusted beacon nodes so that their information would not be used in sensor localization. Further details are described as follows:

In the Input layer, location information is received from the beacon nodes.

In the L_1 layer, a beacon node analyzes the identity and behavior information of neighboring beacon nodes and transmits it out.

In the L_2 layer, a beacon node performs trust evaluation on its neighboring beacon nodes based on individual evaluation by its neighboring beacon nodes and by itself.

In the L_3 layer, an unknown sensor node derives a trust value on each and every of its neighboring beacon node, filters out untrusted beacon node by comparing the corresponding trust value with a trust threshold value, and then computes its location by using location information only from trusted beacon nodes.

In the Output layer, reliable localization results computed using location information from the trusted beacon nodes are output.

The proposed TSLS scheme can deal with attacks from compromised nodes due to the use of trust evaluation on the beacon nodes during sensor localization in WSNs, which helps in improving the accuracy of localization and makes sensor localization more secure. Following are the main steps of our algorithm.

Step 1: Every beacon node send its location and related information to its neighboring beacon nodes as described in the identity evaluation model.

Step 2: Each beacon node calculates an identity trust value and an behavior trust value on every other beacon node and computes the general trust value as described in the trust evaluation model.

Step 3: Every unknown node collects the evaluation values from its neighboring beacon nodes and computes the average value using Eq. (4) in which $T_{U_{mi}}$ denotes the trust value on beacon node B_i for unknown node U_m, $T_{U_{Nmi}}$ denotes the trust value on B_i evaluated by the neighboring beacon nodes to U_m, and $Me()$ denotes the median function. Then the unknown node ranks the neighboring beacon nodes based on the trust values from high to low.

$$T_{U_{mi}} = Me(T_{U_{Nmi}}) \quad (4)$$

However, there is still the possibility of slander behavior of malicious beacon nodes in this phase, which would result in unknown sensor nodes getting false trust evaluation values on trustworthy beacon nodes and consequently eliminating trustworthy beacon nodes so that correct localization information cannot be obtained. This will affect the accuracy of final localization results. Therefore, we apply the median method to substitute the average method to derive the final trust value of an unknown sensor node on a beacon node so as to eliminate the deviation of the normal value and improve the security of localization.

Step 4: Every unknown sensor node would select the trustworthy beacon nodes whose trust values are above

the threshold value T_β and estimate its own location using the location information provided by these trustworthy beacon nodes through maximum likelihood estimation as follows. Suppose the number of trustworthy beacon nodes around an unknown sensor node is n with coordinates $(x_1, y_1), (x_2, y_2), ..., (x_n, y_n)$, respectively, and the distance between the unknown sensor node $U(x_{U_m}, y_{U_m})$ and the beacon nodes are $d_1, d_2, ..., d_n$, respectively. Using Eq. (5), the location of the unknown sensor node can be calculated.

$$(x_{U_m} - x_n)^2 + (y_{U_m} - y_n)^2 = d_n^2, i = 1, 2, ..., \text{n} \tag{5}$$

In addition, n distance equations about the unknown sensor node $U(x_{U_m}, y_{U_m})$ and the n beacon nodes $B_1(x_1, y_1)$, $B_2(x_2, y_2)$,…, $B_n(x_n, y_n)$ are displayed below in Eq. (6), resulting from subtracting the last equation from each of the first $n-1$ equations.

$$\begin{cases} x_1^2 - x_n^2 - 2(x_1 - x_n)x_{U_m} + y_1^2 - y_n^2 - 2(y_1 - y_n)y_{U_m} = d_1^2 - d_n^2 \\ \cdots \\ x_{n-1}^2 - x_n^2 - 2(x_{n-1} - x_n)x_{U_m} + y_{n-1}^2 - y_n^2 - 2(y_{n-1} - y_n)y_{U_m} = d_{n-1}^2 - d_n^2 \end{cases} \tag{6}$$

The unknown sensor node U_m 's coordinate (x_{U_m}, y_{U_m}) can then be calculated using Eq. (7).

$$U_m = A^{-1}b \tag{7}$$

The matrices in Eq. (7) can be expressed using those in Eq. (8) - (10) below.

$$A = 2\begin{bmatrix} x_1 - x_n & y_1 - y_n \\ \cdots & \\ x_{n-1} - x_n & y_{n-1} - y_n \end{bmatrix} \tag{8}$$

$$b = \begin{bmatrix} x_1^2 - x_n^2 + y_1^2 - y_n^2 - d_1^2 + d_n^2 \\ \cdots \\ x_{n-1}^2 - x_n^2 + y_{n-1}^2 - y_n^2 - d_{n-1}^2 + d_n^2 \end{bmatrix} \tag{9}$$

$$U_m = \begin{bmatrix} x_{U_m} \\ y_{U_m} \end{bmatrix} \tag{10}$$

The final solution to Eq. (7) is shown in Eq. (11).

$$U_m = (A^T A)^{-1} A^T b \tag{11}$$

It requires that at least three beacon nodes be present and their credible location information be used for each unknown sensor node to complete localization. However, in practice, the above condition may not be met. Therefore, we need to make sure that the above requirement can be met through some mechanisms. In the TSLS scheme, we propose that the threshold value is made adjustable to suit different application environments. For instance, if the number of trustworthy beacon nodes is not enough to localize an unknown sensor node, we should increase the number of adopted beacon nodes by reducing the threshold value T_β for the trustworthy beacon nodes. If the unknown sensor node still cannot complete its localization when the trust value of adopted beacon nodes falls below threshold T_η, the localization fails.

Each beacon node is evaluated based on its identity and behavior and the evaluation of beacon nodes includes evaluation performed both by an evaluating beacon node and by other beacon nodes in an objective way. Table 1 summarizes the list of notations that have been used throughout this paper.

Table 1. List of notations.

Notation	Explanation
B_i	Beacon node i
U_m	Unknown sensor node m
T_{ji}	General trust value on beacon node i from beacon node j
$T_{I_{ji}}$	Identity trust value on beacon node i from beacon node j
$T_{B_{ji}}$	Behavior trust value on beacon node i from beacon node j
$T_{S_{ji}}$	Behavior trust value on beacon node i based on beacon node j 's self-evaluation
$T_{S_{Nji}}$	Behavior trust value on beacon node i based on evaluation by beacon node j 's neighboring beacon nodes
$T_{U_{mi}}$	Trust value on beacon node i for unknown node m
$T_{U_{Nmi}}$	Trust value on beacon node i based on evaluation by neighboring beacon nodes to unknown node m
(x_p, y_p)	Coordinate of beacon node p
(x_{U_m}, y_{U_m})	Coordinate of unknown node m

Note that the proposed TSLS scheme can be further optimized using back propagation feed-forward neural network (BPNN) according to the energy capacity of sensor nodes in WSNs. The BPNN model can be applied to the basic scheme to adjust the parameters of the evaluation model through analyzing the localization error, to train and optimize the model for trust evaluation of the beacon nodes, and to improve the

localization accuracy of sensors, which will be thoroughly studied in our future work.

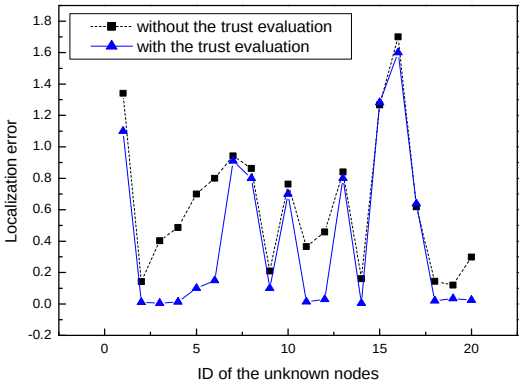
5. Simulation and analysis

We have performed some simulation with the TSLS scheme to show its performance on sensor localization.

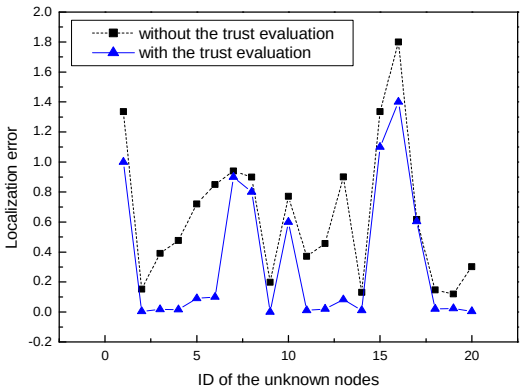
The network configuration for our simulation is set up as follows: 20 unknown sensor nodes, 10 trustworthy beacon nodes and 5 malicious beacon nodes, all of which are deployed randomly in a 650×600m^2 area. The false location information provided by malicious beacon nodes is generated randomly. The transmission radius of beacon nodes and unknown sensor nodes are 200m and 50m, respectively. The threshold trust value for trustworthy beacon nodes is setting up to be 0.75 in the range of [0-1].

Localization error is an important measurement of performance for sensor localization in WSNs, which is calculated using Eq. (12) in which (x_{U_m}, y_{U_m}) denotes the measured coordinates of unknown sensor node U_m while (x'_{U_m}, y'_{U_m}) denotes the actual coordinates and R denotes the transmission radius of the nodes. The simulation results on localization error for the 20 unknown sensor nodes are shown in Fig. 5, from which we can see that the proposed TSLS scheme is effective in helping the unknown sensor nodes reduce localization error in hostile environments.

$$e_u = \frac{\sqrt{(x_u - x_u')^2 + (y_u - y_u')^2}}{R} \tag{12}$$



(a)



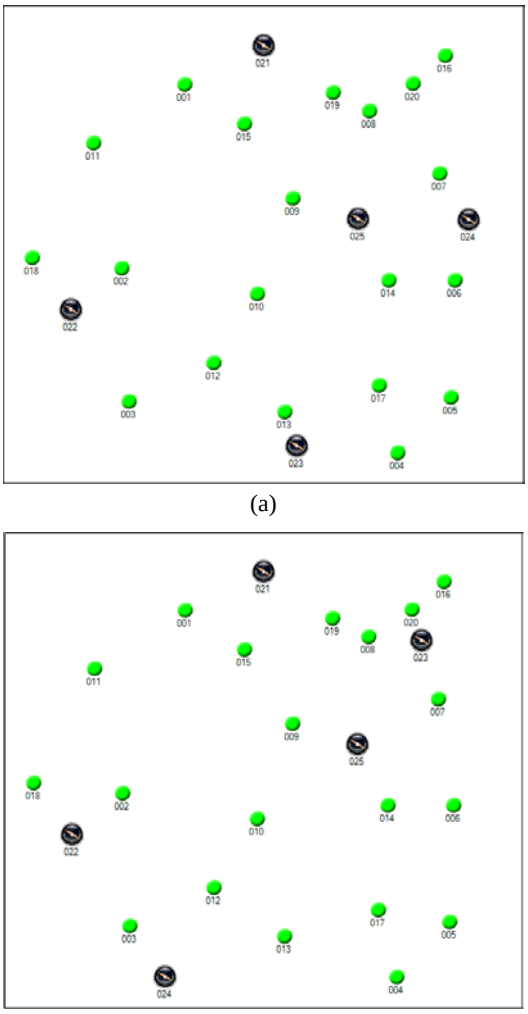
(b)

Fig.5. Comparison of localization errors: (a) $\alpha = 0.3$; (b) $\alpha = 0.8$.

Dynamism is one of the main characteristics of WSNs, that is, scale of the networks and locations of sensor nodes among many other factors are often changing along the time in real applications. Therefore, it is worth evaluating the performance of the proposed TSLS scheme under the assumption of network dynamism. We hereby introduce the notion of average localization error to evaluate our TSLS scheme using Eq. (13) in which N denotes the number of unknown sensor nodes in a network.

$$\overline{e} = \sum_{i=1}^{N} e_i / N \tag{13}$$

We now investigate the effect on the localization of unknown sensor nodes based on the locations of beacon nodes. In the evaluation, the deployment of the 20 unknown sensor nodes and the 5 trustworthy beacon nodes in an area of 650×600m^2 is shown in Fig. 6 (a). We can increase the power of the signals emitted from the beacon nodes to fully cover the entire area. The experiment starts at the 0th minute and then we make beacon node 22 report false location information without actually changing its location at the 1st minute, make beacon node 23 change its location without reporting correct location information at the 2nd minute, and make beacon node 24 change its location normally at the 3rd minute, i.e., it would provide updated information after moving to a new location as shown in Fig. 6 (b).



(a)

(b)

Fig.6. Topology of beacon nodes and unknown nodes: (a) before the state changing; (b) afer the state changing.

The average localization error of unknown nodes in the network computed using the proposed TSLS scheme and that using general localization without trust evaluation (GLS) are shown in Fig. 7. In order to raise the standard of trust on beacon nodes and extrude the performance of localization, we choose the threshold value for the trust of trustworthy beacon nodes to be 0.95 and the weight for the evaluation values to be 0.8.

The number of nodes also changes frequently in WSNs. We now investigate the effect on localization of unknown nodes when the number of beacon nodes in the network increases. We deploy 3 trustworthy beacon nodes and 10 unknown nodes to start with and will add one beacon node into the network at the interval of 1 minute starting from the 1st minute, and trustworthy and malicious beacon nodes are added alternately. The malicious beacon nodes claim false location information randomly. The localization results of this experiment are shown in Fig. 8 from which we can see that the localization result of using GLS can be affected by malicious beacon nodes due to its inability of distinguishing beacon nodes and consequently filtering out false location information. In contrast, the proposed TSLS scheme is able to filter out false location information for localization, hence increasing the accuracy of sensor localization.

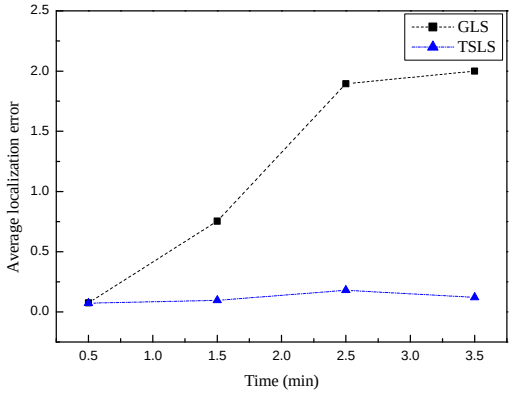


Fig.7. Average localization error of unknown nodes when changing the status of beacon nodes.

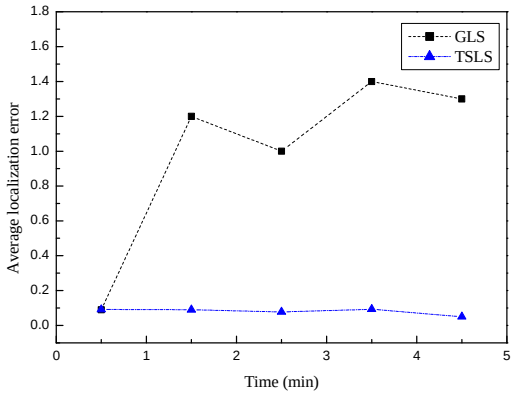


Fig.8. Average localization error of unknown nodes when adding beacon nodes into the network.

In real applications, wireless sensor nodes often leave the network due to power outage or equipment failure. We now investigate the performance of the proposed TSLS scheme under this circumstance.

We deploy 20 unknown sensor nodes and 5 trustworthy and 3 malicious beacon nodes in the same area. We remove one beacon node from the network at the interval of one minute starting from the 1st minute and trustworthy and malicious beacon nodes are

removed alternately. The average localization errors for the 20 unknown sensor nodes are shown in Fig. 9 from which we can see that the localization error varies within a small range in the proposed TSLS scheme and the improvement is significant compared with general localization without trust evaluation (GLS).

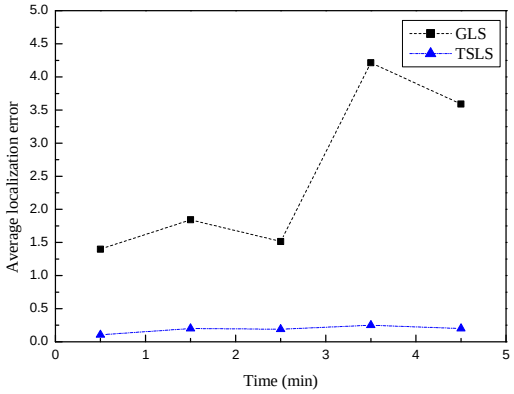


Fig.9. Average localization error of unknown nodes when removing beacon nodes from the network.

The above simulation and analysis show significant performance improvement brought by the proposed TSLS scheme under different network scenarios. The first simulation illustrates the influence on sensor localization when different weights are assigned to the direct and indirect evaluation values in the computation of trust values by unknown sensor nodes. The second simulation shows the average localization error of unknown nodes when malicious beacon nodes provide false location information. The third simulation describes the localization results when new beacon nodes are added into the network, which includes both trustworthy and malicious beacon nodes. And the last simulation shows the average localization error of unknown sensor nodes when beacon nodes are removed from the network.

The set of simulations have been focused on demonstrating the localization performance of unknown sensor nodes in both static and dynamic WSNs, thus fully considered the main characteristics of WSNs. The simulation results show that the proposed TSLS scheme can distinguish between trustworthy and malicious beacon nodes effectively, reduce the effect of malicious beacon nodes on sensor localization, and ultimately improve the security and accuracy of sensor localization in WSNs. It also indicates that the TSLS scheme can scale well not only in static but also in dynamic WSNs. Moreover, following the BPNN model, the TSLS scheme can be further optimized to suit different WSNs and to improve localization results.

6. Conclusions

In this paper, we first analyzed the security aspects of sensor localization in WSNs and the consequence of external and internal attacks to sensor localization and pointed out that cryptographic schemes cannot fight effectively against attacks from compromised beacon nodes. To deal with this security problem in sensor localization, we proposed TSLS, a trust based secure localization scheme, by relying on trust evaluation on beacon nodes in which we considered both the identities and the behaviors of the beacon nodes closely following the principles of neural network. In the proposed TSLS scheme, we introduced a filtering mechanism to prevent slander behavior of malicious beacon nodes. In trust evaluation, the derived trust values are no longer just the discrete values of 0 and 1, but a decimal value to achieve a higher level of granularity in trust evaluation. We also performed some simulations to evaluate the proposed TSLS scheme and to show that it can improve the accuracy of sensor localization for unknown sensor nodes in hostile environments in both static and dynamic WSNs.

In the future, we will extend our TSLS scheme by considering more factors in trust evaluation and under different network scenarios to further improve the applicability, creditability and reliability of the evaluation results. We will also investigate other aspects of performance in sensor localization, such as computational cost and communication overhead, and analyze and compare the resulting schemes with other secure sensor localization methods. Further optimization of the TSLS scheme using the BPNN model is also part of our future work for improving sensor localization in WSNs.

References

1. P.J. Chuang and C.P. Wu, Employing PSO to enhance RSS range-based node localization for wireless sensor networks, *Journal of Information Science and Engineering*, 27(5) (2011) 1597-1611.
2. G.W. Shen, R. Zetik, O. Hirsch, and R.S. Thoma, Range-based localization for UWB sensor networks in realistic environments, *EUROSIP Journal on Wireless Communications and Networking*, 2010 (2010) 1-9.

3. Z.Q. Zhong and T. He, RSD: A metric for achieving range-free localization beyond connectivity, *IEEE Transactions on Parallel and Distributed Systems*, 22(11) (2011) 1943-1951.
4. Y.W.E. Chan and B.H. Soong. A new lower bound on range-free localization algorithms in wireless sensor networks, *IEEE Communications Letters*, 15(1) (2011) 16-18.
5. R.V. Kulkarni, A. Forster, G.K. Venayagamoorthy, Computational intelligence in wireless sensor networks: a survey, *IEEE Communications Surveys & Tutorials*, 13(1) (2011) 68-96.
6. A. Chatterjee, A fletcher-reeves conjugate gradient neural-network-based localization algorithm for wireless sensor networks, *IEEE Transactions on Vehicular Technology*, 59(2) (2010) 823-830.
7. V. Massimo, L.V. Roberto, M. Francesco, A two-objective evolutionary approach based on topological constraints for node localization in wireless sensor networks, *Applied Soft Computing Journal*, 12(7) (2012) 1891-1901.
8. D. Lavanya, S.K. Udgata, Swarm intelligence based localization in wireless sensor networks, in *Proc. 5th Multi-Disciplinary International Workshop on Artificial Intelligence*, (Hyderabad, India, 2011), pp. 317-328.
9. S. Capkun, K.B. Rasmussen, M. Cagalj, and M. Srivastava, Secure location verification with hidden and mobile base stations, *IEEE Transactions on Mobile Computing*, 7(4) (2008) 470-483.
10. L. Lazos, P. Radha, and S. Capkun, ROPE: robust position estimation in wireless sensor networks, in *Proc. 4th International Symposium on Information Processing in Sensor Networks*, (United States, Los Angeles, 2005), pp. 324-331.
11. D. Liu, P. Ning, A. Liu, C. Wang, and W.L. Du, Attack-resistant location estimation in wireless sensor networks, *ACM Transactions on Information and Systems Security*, 11(4) (2008) 22-39.
12. Z. Li, W.Y. Xu, R. Miller, and W. Trappe, Securing wireless systems via lower layer enforcements, in *Proc. 5th ACM Workshop on Wireless Security*, (United states, Los Angeles, 2006), pp. 33-42.
13. D. Liu, P. Ning, and W.L. Du, Detecting malicious beacon nodes for secure location discovery in wireless sensor networks, in *Proc. 25th IEEE International Conference on Distributed Computing Systems*, (United States, Columbus, 2005), pp. 609-619.
14. A. Srinivasan, J. Teitelbaum, and J. Wu, DRBTS: distributed reputation-based beacon trust system, in *Proc. 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing*, (United States, Indianapolis, 2006), pp. 277-283.
15. X.Y. Xu, H.Q. Jiang, L.S. Huang, H.L. Xu, and M.J. Xiao, A reputation-based revising scheme for localization in wireless sensor networks, in *Proc. 2010 IEEE Wireless Communications & Networking Conference*, (Australia, Sydney, 2010), pp. 1-6.
16. X. Wang, L. Ding, and D.W. Bi, Reputation-enabled self-modification for target sensing in wireless sensor networks, *IEEE Transactions on Instrumentation and Measurement*, 59(1) (2010) 171-179.
17. X. Wang and Z.S. He, Single-sensor parametric location algorithm and accuracy Analysis of TDMA moving target based on TOA and DOA measurements, *Information Technology Journal*, 10(6) (2011) 1252-1257.
18. S.H. Zhu and Z.Q. Ding, Joint synchronization and localization using TOAs: a linearization based WLS solution, *IEEE Journal on Selected Areas in Communications*, 28(7) (2010) 1016-1025.
19. M. Sun, K.C. Ho, An asymptotically efficient estimator for TDOA and FDOA positioning of multiple disjoint sources in the presence of sensor location uncertainties, *IEEE Transactions on Signal Processing*, 59(7) (2011) 3434-3440.
20. T. Wang, Ranging energy optimization for a TDOA-based distributed robust sensor positioning system, *International Journal of Distributed Sensor Networks*, 2010 (2010) 1-12.
21. X.W. Wang, S.P. Yuan, R. Laur, and W. Lang, Dynamic localization based on spatial reasoning with RSSI in wireless sensor networks for transport logistics, *Sensors and Actuators: A Physical*, 171(2) (2011) 421-428.
22. H.C. Shi, X.L. Li, Y. Shang, and D.F. Ma, Error analysis of quantized RSSI based sensor network localization, *International Journal of Wireless and Mobile Computing*, 4(1) (2010) 31-40.
23. B. Omidali and S.A.-A.B. Shirazi, Sensor placement to improve the positioning performance based on angle of arrival (AOA), *Wireless Engineering and Technology*, 1(1) (2010) 41-45.
24. T. Aso and T. Miyajima, Sensor localization based on AOA-assisted NLOS identification, *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences*, E93-A(6) (2010) 1274-1276.