Science Arena Publications
Specialty Journal of Electronic and Computer Sciences
Available online at www.sciarena.com
2016, Vol, 2 (1): 22-28

A Secure Localization Method in Wireless Sensor Network, Using Two Taylor Series

Elham Ghaffari[1,2], Mohammadreza Eslaminejad[3]*
1Department of Computer Engineering, Fars Science and Research Branch, Islamic Azad University, Marvdasht, Iran
2Department of Computer Engineering, Marvdasht Branch, Islamic Azad University, Marvdasht, Iran
elhamghaffari88@yahoo.com
3Computer Group of Zand Institute of Higher Education, Shiraz, Iran
eslaminejad@zand.ac.ir

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

Introduction

Wireless sensor networks (WSNs) are based on sensor technology, wireless communications, tiny embedded devices, and distributed computing. These networks are exchanging data with the environment by sensors and perform data manipulating and gathering. WSNs are widely used in environment monitoring, target tracking, military application, disaster management and etc [1-3].

The node localization technology is needed in WSN application, especially when location information is necessary. WSN nodes localization is determining coordinates of normal nodes based on anchor nodes coordinates and confined relation between anchor and normal nodes. The coordinate or location of normal node is unknown. On the other hand, Anchor nodes can obtain their location via global positioning system (GPS) modules or manually. In many typical localization algorithms [4-6] assumed that anchor nodes location information are quite properly without any interference by adverse factors or internal attacks and normal nodes can use anchor information safely. However, in real hostile situations, some malicious nodes may enter into the sensor network without authorization in order to sabotage. They are trying to introduce themselves as benign anchor nodes or attack on other anchor nodes in order to force them to declare wrong location [7]. In addition to malicious anchor nodes, faulty anchors should be detected for avoiding errors in localization. Erroneous distance estimation or erroneous coordinate causes irreplaceable fault in normal sensor nodes localization. In this case, some methods should be applied to eliminate or reduce harness effects created by malicious or faulty anchor nodes and ensure secure wireless sensor network localization. We call malicious anchor nodes the both faulty and malicious anchor nodes

In this paper, we propose a robust and secure localization algorithm in order to solve the problem of malicious anchor nodes existence in localization. In the proposed method, each anchor node asks other anchors their locations and decision about other anchor nodes that are benign or malicious by triangulation localization method. The sensor node is informed about anchor node decision in order to localize itself. The proposed method will be discussed briefly later. The remainder of the paper is organized as follows: Section II introduces related works on secure localization algorithms. Section III presents the network model, attack model, and related definitions. Section IV provides the details of proposed method. Section V presents the simulation results. Section VI concludes the paper.

Definition and concepts of informal settlements

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

The domain error e follows Gaussian distribution (N(u,λ2)) that mean u is zero and variance λ is restricted:

$$|ei|<=emax \quad (1)$$

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

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

$$\begin{aligned} &||Xm - X1||2=dm1 \\ &||Xm - X2||2=dm2 \\ &\quad \dots \quad (2) \\ &||Xm - Xk||2=dmk \end{aligned}$$

Where Xm=[xm,ym]T is M's coordinates that need to be estimated and Xi=[xi,yi]T is anchor node Ai's declared position. If the anchor node A1 is attacked, it will become a malicious anchor node A'1 with fake coordinates. When M utilizes A'1 to compute its position, its estimated position M' will deviate far from its physical position, and its location accuracy will be very low.

PROPOSED METHOD

Malicious Anchor Nodes Detection

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

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

In least square Taylor series method location of node is obtained from the following formula as follows. Firstly, calculate the centroid coordinates $X_c=(x_c,y_c)$ of k anchor nodes, that is, $x_c=(1/K)\cdot\Sigma_{i=1}^{k}x_i$. Secondly,

expand the function $f(x)=\|X-X_i\|_2$ in Taylor series at X_c, and ignore the high-order terms. Therefore, $\Delta X_C=(\Delta x_c-\Delta y_c)$ can be obtained such as:

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

Where

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

$$A=\begin{bmatrix} \frac{x_C-x_1}{d_{1C}} & \frac{x_C-x_2}{d_{2C}} & \cdots & \frac{x_C-x_K}{d_{KC}} \\ \frac{y_C-y_1}{d_{1C}} & \frac{y_C-y_2}{d_{2C}} & \cdots & \frac{y_C-y_K}{d_{KC}} \end{bmatrix}^T.$$

Localization Process

Firstly, calculate the centroid coordinates $X_c=(x_c,y_c)$ of k anchor nodes, that is, $x_c=(1/K)\cdot\Sigma_{i=1}^{k} x_i$. Secondly, expand the function $f(x)=\|X-X_i\|_2$ in Taylor series at X_c, and ignore the high-order terms. Therefore, $\Delta X_C=(\Delta x_c-\Delta y_c)$ can be obtained such as:

$$\Delta X_C=\left(A^T W^T W A\right)^{-1} A^T W^T W B \quad (2)$$

Where:

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

$$B=\begin{bmatrix} d_1-d_{1C} \\ d_2-d_{2C} \\ \vdots \\ d_K-d_{KC} \end{bmatrix},$$

$$A=\begin{bmatrix} \frac{x_C-x_1}{d_{1C}} & \frac{x_C-x_2}{d_{2C}} & \cdots & \frac{x_C-x_K}{d_{KC}} \\ \frac{y_C-y_1}{d_{1C}} & \frac{y_C-y_2}{d_{2C}} & \cdots & \frac{y_C-y_K}{d_{KC}} \end{bmatrix}^T.$$

Thirdly, d is calculated by formula 3, and judge whether the iteration termination condition $d<=\eta$ is satisfied, where η is a prior-defined threshold. If $d<=\eta$, we stop the iteration process. Otherwise, we set $X_c=X_c+\Delta X_c$ and go to the second step. Finally, repeat the second step and the third step until the iteration termination condition is satisfied or the maximum iteration number is reached. The final output X_c is the estimated coordinates of sensor node M. The localization algorithm is in below.

$$d=\sqrt{\Delta x_C^2+\Delta y_C^2} \qquad (3)$$

Algorithm . Nodes localization algorithm

```
---------------------------------------------------------------
for i=1:1:length(benginganodes)
   W(i,i)=benginganodes(i).Tru_TA;
   % calculation of W
end
for i=1:1:banodes+manodes
```

```
    % calculation of XC
    sumx=0;
    sumy=0;
    for k=1:1:length(benginganodes)
       sumx=benginganodes(k).xd+sumx;
       sumy=benginganodes(k).yd+sumy;
    end
    Xc=sumx/length(benginganodes);
    Yc=sumy/length(benginganodes);
    XC.xd=Xc;
    XC.yd=Yc;
    steps=0; % prevent of unlimited while loop
    rep=1;
    % repeat lines between while until rep equal to 0
    while (rep~=0)
       steps=steps+1;
    for k=1:1:length(benginganodes)
       d(i,k)=distance1(S(i),benginganodes(k));
       dc(k)=distance1(benginganodes(k),XC);
    end
    for k=1:1:length(benginganodes)
       B(k)=d(i,k)-dc(k);
    end
    for k=1:1:length(benginganodes)
       A(1,k)=(XC.xd-benginganodes(k).xd)/dc(k);
       A(2,k)=(XC.yd-benginganodes(k).yd)/dc(k);
    end
    A=A';
    B=B';
    deltaXC=(A'*W'*W*B)'/(A'*W'*W*A);
    d=sqrt(deltaXC(1)^2+deltaXC(1)^2);
    A=A';
    B=B';
    if d>=n
       XC.xd=deltaXC(1)+XC.xd;
       XC.yd=deltaXC(2)+XC.yd;
    elseif d<n || steps>40
       rep=0; % this line causes stop while
    end
    end
    newS(i).xd=XC.xd;
    newS(i).yd=XC.yd;
  end
  ----------------------------
```

EVALUATION

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

Matlab is the simulation tool used in this paper which is applied in many scientific papers. Initially network size is defined as two dominations square 200*200. Number of all nodes, benign anchor nodes and malicious anchor nodes are 200, 20 and 10 respectively. The nodes distribution strategy is random. Other network parameters are listed in table I. Fig. 1 illustrates a sample nodes deployment where blue cycles,

green stars and red stars are demonstrated normal sensor nodes, benign anchor nodes and malicious anchor nodes respectively.

TABLE I
SIMULATION PARAMETERS

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

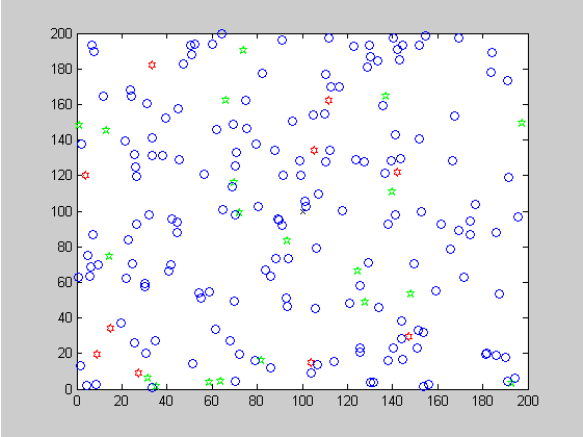

Fig. 1 Nodes randomly deployment

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

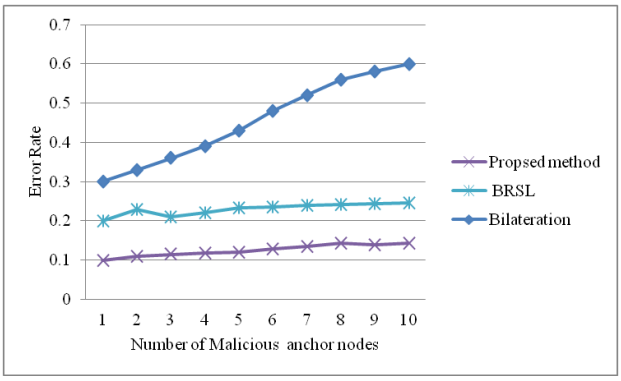

Fig. 2 Compare between error rates with different number of malicious anchor nodes

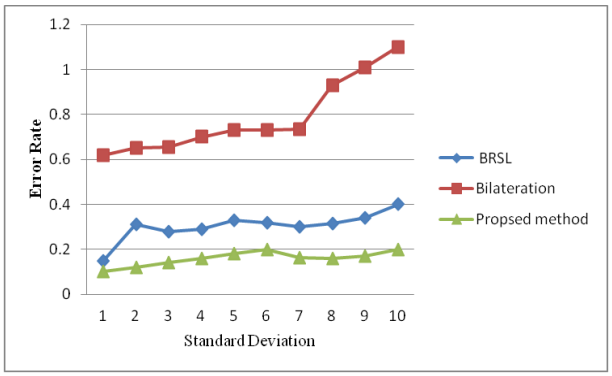

Fig. 3 Compare between error rates with different standard deviation

CONCLUSION

Our aim of doing this research was to propose a novel approach in order to secure localization in wireless sensor network under malicious anchor nodes attacks. The proposed method consists of two steps which in the first step, malicious anchor nodes are detected and nodes' trust values are calculated. In the next step, Taylor series least square method is used to estimate the coordinates of the sensor nodes. Simulation results show that the proposed algorithm is efficient and robust.

References

[1] J. Albowicz, A. Chen, and L. Zhang, "Recursive position estimation in sensor networks," in Proceedings of the 9th International Conference on Network Protocols,pp.35–41,2001.
[2] H.A. Oliveira, E.F. Nakamura, A.A.F. Loureiro, and A. Boukerche, "Directed position estimation: a recursive localization approach for wireless sensor networks," in Proceedings of the 14th IEEE International Conference on Computer Communications and Networks, pp. 557–562, San Diego, Calif, USA, 2005.
[3] T. He, C. Huang, B.M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks," in Proceedings of the 9th Annual International Conference Mobile Computing and Networking (MobiCom '03),pp.81–95, ACM Press, San Diego, Calif, USA, 2003.
[4] M. L. Sichitiu and V. Ramadurai, "Localization of wireless sensor networks with a mobile beacon," in Proceedings of the 1st IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, pp. 174–183, Fort Lauderdale, Fla, USA, October 2004.
[5] X. L. Guo, R. J. Feng, Y. F. Wu, and J. W. Wan, "Grid-Scan-Based multi-hop Localization algorithm for wireless sensor networks," in Proceedings of IEEE Sensors Conference,pp.668–672,Waikoloa, Hawaii, USA, 2010.

[6] D. Niculescu and B. Nath, "DV based positioning in ad hoc networks," Telecommunication Systems,vol.22,pp.267–280,2003.
[7] K. Yu, Y. J. Guo, and M. Hedley, "TOA-based distributed localisation with unknown internal delays and clock frequency of sets in wireless sensor networks," IET Signal Processing, vol.3, no. 2, pp. 106–118, 2009.
[8] J. Wan, N. Yu, R. Feng, Y. Wu, and C. Su, "Localization refinement for wireless sensor networks," Computer Communications, vol. 32, pp. 1515–1524, 2009.
[9] N. Yu, L. Zhang, and Y. Ren, BRS-Based Robust Secure Localization Algorithm for Wireless Sensor Networks, International Journal of Distributed Sensor Networks Volume 2013, Article ID 107024, 9 pages.
[10] J.W. Wan, X.L. Guo, N. Yu, Y.F. Wu, and R.J. Feng, "Multi-hop localization algorithm based on grid-scanning for wireless sensor networks," Sensors, vol. 11, no. 4, pp. 3908–3938, 2011.
[11] Y. Shang, H. Shi, and A.A. Ahmed, "Performance study of localization methods for ad-hoc sensor networks," in Proceedings of the IEEE International Conference on Mobile Ad-Hoc and Sensor Systems, pp. 184–193, October 2004.
[12] S.Y. Wong, J.G. Lim, S.V. Rao, and W.K.G. Seah, "Multihop localization with density and path length awareness in nonuniform wireless sensor networks," in Proceedings of the IEEE 61st Vehicular Technology Conference, vol. 4, pp. 2551–2555, Stockholm, Sweden, June 2005.
[13] Q.J. Xiao, B. Xiao, J.N. Cao, and J.P. Wang, "Multihop range free localization in anisotropic wireless sensor networks: a pattern-driven scheme," IEEE Transactions On Mobile Computing, vol. 9,no.11, pp.1592–1607,2010.
[14] J. Hwang, T. He, and Y. Kim, "Detecting phantom nodes in wireless sensor networks," in Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM'07),pp.2391–2395,May2007.
[15] R.J. Feng, X.L. Guo, N. Yu, and J.W. Wan, "Robust multihop localization for wireless sensor networks with unreliable beacons," International Journal of Distributed Sensor Networks, vol.2012, ArticleID 972101,13pages,2012.