Journal of Theoretical and Applied Information Technology
10th January 2013. Vol. 47 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A TWO-STEP FILTRATE LOCALIZATION METHOD FOR WIRELESS SENSOR NETWORKS

JUN ZHANG
School of Computer Science and Engineering, University of Electronic Science and Technology of China, No. 2006, XiYuan Ave. Chengdu 611731, P.R.China
E-mail: zhangjun@uestc.edu.cn

ABSTRACT

In this paper, we address a wireless sensor network localization problem that has high reliability in an environment where physical node destruction is possible. We propose a range-independent localization algorithm called Two-Step Filtrate Localization (TSFL), that allows sensors to passively determine their location with high reliability, without increasing the number of reference points, or the complexity of the hardware of each reference point or node. Based on analyzing the principles of the two-step filtrate method, it is pointed out that the importance of the second step to determine the maximum distance estimation error conditions. In different attack mode, by the simulation of the algorithm's security is discussed. The results of the simulation show the algorithm can get lower average positioning error, meantime malicious attacks have little side effects to location performance.

Keywords: *Sensor Network, Localization, Two-Step Filtrate*

1. INTRODUCTION

Wireless sensor networks comes from the equation that perception + CPU (computation) + wireless communication technology=thousands potential applications. In these applications most of them require correlated location information. But WSN adopts the mode of self organized network deployment usually and node can not know its location in advance. So on the phase of network initialization node need to confirm its location through localization. At the same time WSN is liable to be attacked in practice and it would affect localization precision to different extent. Then it would make localization information useless entirely. Thus the process of localization is very important [1]-[3].

In this paper we make the following contributions. We introduce a novel location scheme for WSN called security location based on Detecting malicious beacon nodes (TSFL) that allows sensors to passively determine their location with high accuracy.

2. TSFL ALGORITHM

A. Problem Describing of Secure Location

Assuming that there are some malicious adversaries in WSN whose aims are to increase the deviation between the real location and estimated one, not to disable the location of nodes[4],[5]. For this reason, this paper will not analyze easily found attacks and these ones based on other network protocols, such as DOS [6]. In addition, malicious node attack mode is divided to Joint attack and Non-joint attack. The concept of the Joint attack is all the attack anchor nodes move certain distance in one direction. And the concept of the Non-joint attack is attack anchor node moves a random distance in the random direction.

We use (x_i, y_i) 、 (x_j, y_j) and d_{ij} separately to denote the real coordinates of unknown node i and the anchor, also the metric distance between them. As a result, achieving security location can be seen as optimizing the formula (1) with the presence of wormhole attacks, Sybil attacks, sinkhole attacks, inject misdate attacks and monitor to location information, etc[7]-[10].

$$\min \quad f(x_i, y_i) = d_{ij} - \sqrt{(x_i - x_j) + (y_i - y_j)} \quad i = M+1, M+2, \cdots, N \quad (\square)$$

Here, d_{ij} obtained by RSSI ranging, and P_{ij} denotes the received power of unknown node i from the anchor j . As there are reflection, multipath and background interference in the wireless channels, different transmission loss exists,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

so the Gauss noises x^{σ} will be added to the simulation. The formula is,

$$P_r(d) = P_0(d_0) - 10n_p \log_{10}(\frac{d}{d}) + X_\sigma \quad (2)$$

Here, $p_r(d)$ is the received power, $p_0(d_0)$ as the reference power at distance d_0, n_p as the loss index based on specific path, X_σ as the Gaussian random variable with the zero-mean standard deviation. In the ideal case, the stronger signal intensity will be obtained by shortening the distance between two nodes. The distances between different nodes can be determined, when the unknown nodes find all the RSSI values obtained by one-hop communicating with the anchor.

$$d_{ij} = d_{kl}^{\frac{p_r(d_{ij}) - p_0(d_0)}{p_r(d_{kl}) - p_0(d_0)}} \quad (3)$$

In formula （3）, $p_r(d_{ij})$ 、 $p_r(d_{kl})$ and d_{kl} separately denote the signal received power of node i from node j and node k from node l, also the estimated distance between node k and l.

B. TSFL Algorithm

In this paper, we comprehensively consider the reliability threshold and residual power of every anchor, also the effects, generated by the distances between anchors and the unknown node, on the location of unknown nodes and the performance of the whole network. Then we determine the real location of the unknown node securely by using genetic algorithm.

(1) Calculation of the beacon nodes set LN in the direct communication domain of unknown nodes and distance

(2) Judgment of possible vicious beacon nodes and voting

Let e_max denote the maximum measurement error, for different beacon nodes A and B in the set Γ, if formula (5) is held, at least one in these two nodes A and B is the vicious attack beacon nodes, then let (A,B)=1 ; otherwise, no vote。

$$(D(A,B) > D\_\max) or (D(A,B) < D\_\min) \quad (4)$$
$$\forall A, B \in \Gamma$$

Which

$$D\_\max = \min((d\_est(A) + d\_est(B) + 2 \times e\_\max), 2r) \quad (5)$$

$$D\_\min = \max((|d\_est(A) - d\_est(B)| - 2e\_\max), 0) \quad (6)$$

$$|d\_est(A,B) - d(A,B)| \le e\_\max \quad (7)$$

(3) Confirmation of vicious attack beacon nodes

Calculating total votes of each beacon nodes using V, and finding the beacon nodes with the most vote, it is denoted as v_max. If v_max is not zero, it is marked as vicious attack node, and the votes regarding v_max are set to zero, i.e. V (v_max, :)=0,V(:,v_max)=0。

(4) Ending condition

Loop runs alternatively three to four times until v_max=0, which means all vicious attack nodes have already been marked.

All marked vicious attack beacon nodes should be eliminated. The ordinates of the rest nodes and the estimated distances d_est are saved as M.

(5) Second step filtrate

Calculate the mean_x, mean_y which separately denote the x, y coordinates average value of the all nodes in M. Then a square area 2r*2r is founded whose mid-point is (mean_x, mean_y) and side length is 2r. Where, mid-point is in the middle of the square area.

N coordinates are randomly generated in the square area, and denote D_pc(i) as the distance between each coordinate and anchor i. If D_pc(i) satisfied the formula |D_pc(i)-d_est(i)|<=e_max, the counter add 1. Or not to vote, each randomly generated coordinates of the initial votes are set to zero.

Find the maximum of vote counter, defined as vote_max, after finishing all vote from anchors to n coordinates in M. The max_x,max_y, min_x and min_y are separately denoted the maximum and minimum value of horizontal and vertical coordinates in vote_max. Then, the area is expanded to

$$\max\_x + r \times 2^{(-num)} \square\square \max\_y + r \times 2^{(-num)} \quad (8)$$

$$\max\_x - r \times 2^{(-num)} \ \max\_y - r \times 2^{(-num)} \quad (9)$$

(6) Estimate location of unknown node

Loop 5 step num times, and calculate node coordinates with maximum votes in all loops. Therefore, the estimate location of unknown node is expressed as the mean of node coordinates.

Journal of Theoretical and Applied Information Technology
10th January 2013. Vol. 47 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. ANALYSIS OF THE SIMULATION

For analyzing the performance of the mentioned algorithm, this paper executes a series of simulation experiment. In this part, we will introduce the simulation environment, the standard of performance evaluation and the analysis of simulation result.

A. Configuration on the simulation environment

The experiment is done by Matlab 7.0. Assuming that the communication radium of the node is r=10m, the experiment is done on 100 randomly distributed nodes in the 5r×5r perceptive area. At the same time assume that the percentage of anchor is 11%, malicious attacks anchor number is C, E_max=4m， a term of a m distance error is introduced in each attack node.

B. Standard of performance evaluation

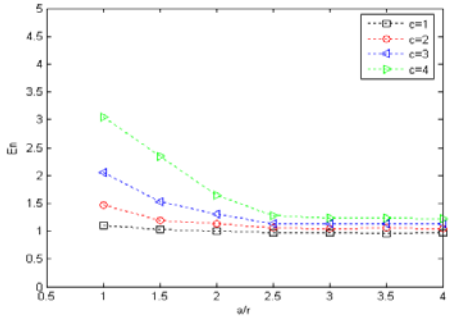
（1） Location error En : the ratio of the wireless range to the distance between the estimated location and the real one. The formula is:

$$En = \sum_{i=M+1}^{N} \sqrt{(x_i - \tilde{x}_i) + (y_i - \tilde{y}_i)} \qquad (10)$$

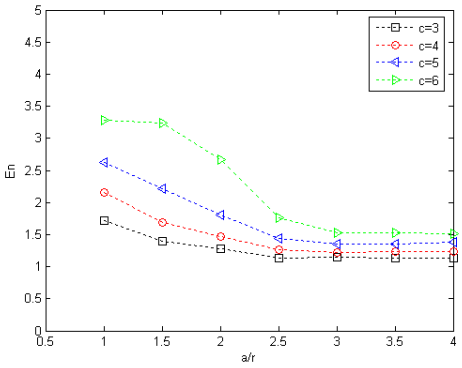
（2）The security of algorithm: It consists of the performance to resist the inject misdated attack and the influence from different proportional malicious attacks on anchors.

C. Analysis of simulation result

For studying the location error of the TSSL in the case of different density of malicious beacon nodes and attack mode, we only change the density and attack mode in the standard network. For analysis the performance of the algorithm, we separately utilize the noise factor as 10% ， number of malicious beacon nodes is C, and other parameters remain unchanged.



C=1:4 In Joint Attack



C=3:6 In Non-Joint Attack

Fig.1and Fig.2 demonstrates the robustness of TSSL algorithm against vicious beacon nodes with joint attack and Non-joint attack, respectively. It is obvious that，As can easily lead to a larger relative error by the error by the malicious beacon node in Non-joint attack. The error caused by the joint attack in the same direction， not change the correlation distance between malicious beacon nodes，thus each other can still be considered to be benign beacon nodes. Therefore, with the same vicious beacon nodes, group attack can result in larger localization error, in other words, the attack is more effective. However, in the whole, for different attack modes, TSSL algorithm can highly reduce the localization error by the vicious attack. So, TSSL well defends vicious attack.

4. CONCLUSION

The security localization of nodes is important part of network recovery and location computing, also is the central and difficult issue in network security and location study. In this paper new security localization (TSFL) is proposed, the algorithm first to use the constraints of the network itself, find and delete malicious beacon nodes. Followed by a second step the maximum distance constraint filter, Then uses calculate the location of unknown node by centroid method, improve the robustness of the position calculation process and defense performance by malicious attack.

In this paper, analysis performance of security localization of TSSL algorithm in different attack mode. The simulation results show that the algorithm is able to receive a lower average location error in post-attack, and small influence of localization performance of TSSL algorithm in the case of have malicious attack.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ACKNOWLEDGMENT

The work reported here is supported in NSFC under agreement number 61001125 and China Postdoctoral Science Foundation funded project(20090461326) .

REFRENCES:

[1] Fredric Newberg. Wireless sensor networks design and implementation[D]. Los Angeles: University of California, Los Angeles, 2002

[2] C.-Y. Chong, S. Kumar, Sensor networks: evolution, opportunities, and challenges, Proceedings of the IEEE 91(8) (2003) 1247–1256.

[3] Donggang Liu. Security Mechanisms for Wireless Sensor Networks [D]. Raleigh: North Carolina State University PHD Thesis, 2005.

[4] L.Lazos and R.Poovendran. HiRLoc:High resolution Robust Localization for Wireless Sensor Networks [J]. IEEE Journal on Selected Areas in Communications , 2006,24(2): 233-246.

[5] Z.Li, W. Trappe, Y. Zhang, and B.Nath. Robust Statistical Methods for Securing Wireless Localization in Sensor Networks[C] //Proc. of Proceedings of the Fourth International Conference on Information Processing in Sensor Networks(IPSN 05). UCLA: IEEE Signal Processing Society and ACM SIGBED, 2005, pp. 91-98.

[6] Q.Wang, Y.Zhu, and L.Cheng. Reprogramming Wireless Sensor Networks: Challenges and Approaches[J]. IEEE Network. 2006, 20(3): 48–55.

[7] Ayong Ye. Secure node positioning in Wireless sensor networks [D]. Xian: Xidian University PHD Thesis, 2009.

[8] Yang Feng. Research on the technique of countering malicious node in wireless sensor networks [D]. Hefei: University of science and technology of china PHD Thesis, 2009.

[9] Meiling Sun. Research on GA based self-localization algorithm in wireless sensor networks [D]. Dongying: China University of Petroleum Master Degree Thesis, 2009.

[10] R.Mudubai, G.Barriac, U.Madhow. On the Feasibility of Distributed Beamforming in Wireless Networks [J]. IEEE Trans Wireless Communications,2007, 6(5):1754－1763