Secure Localization Approach in Wireless Sensor Network

Sayyed Majid Mazinani and Mosayeb Safari

***Abstract*—Wireless sensor networks have consisted of more than thousands nodes, which have been jointed together for achieving some specific reasons. The sensor information send to a base station named sink and supply with AC power. In most cases, the place of nodes is important for the network performance because of this reason we are using locating. Locating is one of techniques that have been used in wireless networks. Security and accuracy are the bases of locating applications. Practical wireless networks are faced with destructive interference, which have considerable effects on locating performance. In this article, a great and benign locating plane is introduced in order to reduce the effect of enemy attacks in wireless networks. The proposed method is consisting of two steps. In first step, the correctness investigation has been designed on the base of making a table with valid nodes in the base station. In second step, the mean square of Taylor series is used for estimation the sensor node places. The results of simulation verified the performance gain of our proposed scheme.**

***Index Terms*—Wireless sensor networks, robust locating, min square.**

I. Introduction

Wireless sensor network is on the basis of sensor technologies, wireless communications, small sets and distributed computing. These networks, exchange information with environment by sensors, implement sensing and processing operations. In wide branches wireless sensor networks are used at supervising environment such as object tracking, martial applications, management of natural disasters and etc. Locating the place of nodes is an essential condition for wireless sensor networks, especially when placing information is essential for sensing data [1]-[3].

The node localization technology is required in WSN application, especially when location information is necessary WSN nodes localization is determining coordinates of nodes in result the coordinate or normal nodes location 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 information of anchor nodes location are quite without any interference by adverse factors, so 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 other anchor nodes to force them declare a wrong location [7]. 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 which created by malicious anchor nodes and ensure secure wireless sensor network localization.

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 deicide about other anchor nodes that are benign or malicious. The sink is informed with anchor node decision to judge about anchors. The proposed method will be discussed briefly in following pages. The remainder of the paper is organized as follows: Section I introduces related works on secure localization algorithms. Section II presents the network model, attack model, and related definitions. Section III provides the details of proposed method. Section IV presents the simulation results. Section V concludes the paper.

II. Related Works

Alfaro and his colleagues [8] investigate the security of localization in wireless sensor networks under a limited number of reliable relays. In this article, three algorithms have been introduced to enable sensor nodes to determine their coordinates. However, this method fails when the anchor malicious relays have colluded conditions.

Liu and associates have proposed two algorithms of benign locating [9], the first One is the minimum mean square estimation of sustained attack that ignores the malicious anchor nodes by testing their stability, and other one is positioned estimation which based on voting. Both of these algorithms have encountered a problem when anchor malicious nodes are under collusion conditions.

Zou and his associates [10] have proposed sets of attack detection that can detect active hunts and provides a locating service in terms of limited estimation error with secure locating modules. However, this method is only concentrated on one step locating.

Liu with his partners [11] have offered a secure locating mechanism that detects the anchor malicious nodes under their fake location claims. This method uses the anchor superfluous nodes instead of regular nodes in infected area to deal with malicious anchors. This detection method relies on a centralized base station.

Lee and his associates [12] have introduced a secure plan named biltilateration, which is derived from the Multilateration and calculates the weight of anchor nodes after that decides which node is the anchor malicious. Regardless of the coordinates that created with conformist nodes, the mean of the place of left candidates is used as the estimated location of the sensor node. This planes problem is concentrating on one step locating.

Manuscript received June 18, 2015; revised August 25, 2015.

Sayyed Majid Mazinani is with Electrical Department of Imam Reza International University, Mashhasd, Iran (e-mail: smajidmazinani@hotmail.com).

Mosayeb Safari is with Imam Reza International University, Mashhasd, Iran (e-mail: mosayeb_safari@yahoo.com).

doi: 10.18178/ijmlc.2015.5.6.552

Ling Yu and his co-workers [13] have introduced a secure scheme called BRS and try to detect and neutralizing the effects of anchor malicious nodes in all collision and non-collision condition. In this paper, the Beta Reputation System is used to determine the amount of anchor nodes confidence. If this value is less reliable than the calculated threshold, the node is diagnosed malicious. We are using a method, which based on least squares of Taylor series for locating in this paper. The weakness of this method is its relying on the duplicated arrangement of network primary nodes, although this condition does not arise in practice usually.

III. Network Model

Assumption network consists of two types of nodes called anchor nodes and sensor nodes. Anchor nodes equipped with special equipment, and their coordinates are awarded after designing. Sensor nodes should discover their coordinates and they are achieves this aim with measuring the distance to another anchor node. All nodes are distributed in a two dimensional environment. Transmission range or radius range is considered as R. All nodes can compute their ranges to their near closer ones.

The range of error (e) uses the Gaussian distribution with zero mean and variance of λ. Therefore, measurement error is limited to

$$|ei|<=emax \tag{1}$$

The maximum physical (or real) error emax is achieved experimentally. In multi hop locating, each anchor node broadcasts a message to its one hop contiguous that includes its own position. After that, this message broadcasts in the network with a controlled flooding method.

When a sensor node receives three or more anchor messages, its location can be estimated by locating algorithm. [14].

Attacking Model

We assume that the wireless sensor networks are located in enemy environments, which means that malicious attackers are present in the network. Attackers to anchor nodes attacks subject to forcing them announced false location. When an anchor node was attacked and broadcasted the wrong location, it will be named as a malicious anchor node (hostile). The anchor nodes that have a real coordinates are named as well anchor nodes.

When a sensor node (M) get the sufficient distance dmi (i=1, 2, …, k) for k>=3, the Euclidean equations of the system can be adjusted:

$$\begin{aligned} ||Xm - X1||2&=\text{dm1} \\ ||Xm - X2||2&=\text{dm2} \\ ||Xm - Xk||2&=\text{dmk} \end{aligned} \tag{2}$$

where $Xm=[xm, ym]T$ is the coordinates of sensor node of M, which should be estimated, and $Xi=[xi, yi]T$ is the position of the anchor node of Ai. If anchor nodes such as Ai were attacked, it will be malicious anchor nodes with fake coordinates of A'1.

When M uses the A'1 to calculate its coordinates, the achieved spot is so wrong, which has been completely far from its real location and has a definitely low accuracy.

IV. Proposed Scheme

A. Discovering the Malicious Anchor Nodes

At first, the anchor nodes (Ai) want other anchor nodes to send their coordinates by sending a message to all nodes on the network. The nodes of Ai obtain their distance from other anchor nodes by using the measurement techniques such as RSSI and compensate this distance with the Euclidean distance of anchor nodes. If this distance is more than Euclidean distance (emax), the anchor nodes was considered malicious, otherwise it will be detected as a benign node. Each node repeats the same strategy for all anchor nodes in the networks and reports their results to base station. After this step, a table was constructed in the base station.

Every anchor nodes add a row to this table by starting the calculation of enemy detections. Malicious nodes report the benign nodes as malicious nodes and the malicious nodes as benign nodes. It should be noted as number of malicious nodes that are less than number of benign nodes, the row that the law was not established, should be considered as malicious nodes. For more accuracy in calculations and obtain reliable values for the nodes, which detected benign from this scheme, the following procedure is proposed:

The sensor nodes that have 2 or more anchor nodes at the distance of 2*R, establish the following calculation between every 2 anchor nodes. Details are shown in figure. The sensor node asked the anchor nodes of A1and A2 to send their coordinates with a message. The anchor nodes send their coordinates to sensor node. So, the sensor nodes obtain the coordinates of 2 anchor nodes and also detect the distance and the angle of them. This data can easily be obtained from the common techniques such as RSSI or AOA. Therefore the sensor node can obtains the distance between A1 and A2 from the following equation. The difference of Euclidean distance between A1 and A2 should not exceed from (emax). Also, the trusted number is calculated with the following procedure.

$$c^2 = a^2 + b^2 - a * b * cos\ (\lambda) \tag{3}$$

```
For i=1:1: nodes % Number of Normal Sensors
Error= |measured distance (A1, A2)-Ecludistance (A1, A2)|% calculation by sensory
If error> emax
Tru_TA1.sensori =0
Tru_TA2.sensori =0
Else
Tru_TA1.sensori=emax-error
Tru_TA2.sensori =emax-error
End
```

B. Locating

The trusted number of i_th anchor nodes can be obtained from equation 4. In this equation, (n) is the number of nodes and (i) is the number of anchor node. This number is used for obtaining the place of nodes and controlling other anchor nodes effects. The locating method that used in this section is the Least Squares Taylor Series that mentioned in [15]. In this method, the trust of each anchor obtain from total trust of sensors and used in a matrix named W. Assume that dim (*i*=1, 2, …, *K*) is the distance between the *k*th anchor node and the *M*th sensor node and *Xi*=(*xi*, *yi*) is the mentioned coordinates of *i*th anchor node. The place of *M*th anchor nodes is displayed as X=(*x*0, *y*0). So, we have the following Euclidean equations.

$$〖\ \mathrm{Tru\_T}_i = \sum\nolimits_n^{k=1} \mathrm{Tru\_TA(i).sensor}_k \qquad (4)$$

$$Tru\_T_i \times \|X - X_i\|_2 = Tru\_T_i \times d_{mi} \qquad (5)$$

In the first step, we calculate the coordinates of Kth anchor nodes *Xc*=(*xc*, *yc*), i.e.

$$X_c = \left({}^{1}/_{K}\right) \sum\nolimits_{i=1}^{k} X_i$$

In the second step, we expand the function of *f*(*X*)=‖ *X*-*X_i*‖ _(2) at the Taylor series in the point of *Xc*, and ignore the terms with higher degrees. Therefore, 〖 Δ*X*〗 _*C*=(〖 Δ*x*〗 _*c*,〖 Δ*y*〗 _*c*) can obtain as:

〖 Δ*X*〗 _*c*=〖 (*A^T W^T WA*)〗 ^(-1) *A^T W^T WB* (6)

where

In the third step, we consider d as the 7th equation and make a decision if we have the condition of ending of iteration i.e. (d<=η), where η is the predefined threshold value. If (d<=η), we finish the iteration process. Otherwise, we set *Xc* as *Xc*=*Xc*+Δ*Xc* and go to the second step. Finally, we repeat the second and third steps, until we see the condition of ending of iteration or the maximum number of iterations is reached. The final number of *Xc* is the estimated place of *M*th anchor nodes.

V. Simulation Results

In order to verify the performance of our proposed scheme, we compensate our method with some of reliable methods that mentioned in benign locating context. We use the MATLAB software for our simulation which is used in most papers. Firstly, we defined a network with dimension of 200×200. Also, the total number of nodes is 200, the correct anchor nodes are 20, and the malicious nodes are 20.

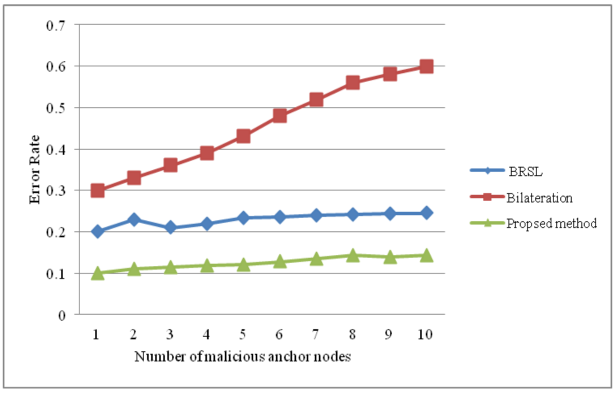

Fig. 1. Comparison the error rates by increasing malicious nodes.

The factors of proposed method are measured with the numbers of locating errors in different conditions. At first we considered a case which anchors nodes number of enemy is start with 1 and increased to 10. The results of this simulation can be seen in Fig. 1. In this figure, the numbers of errors in our proposed scheme are considerably lower than 2 other methods. Figs. 2 and 3, show the compensation of the error rates with different number of variances. The error of each pattern increased with increasing the variance. Our proposed method has better performance, in comparison to BRSL and Bilateration.

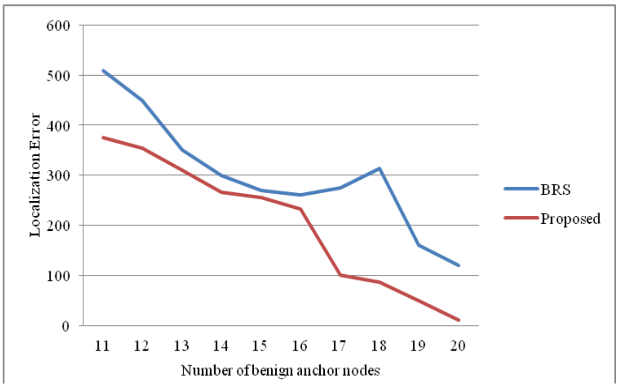

Fig. 2. Compares the error rate for increasing the number of anchor nodes healthy.

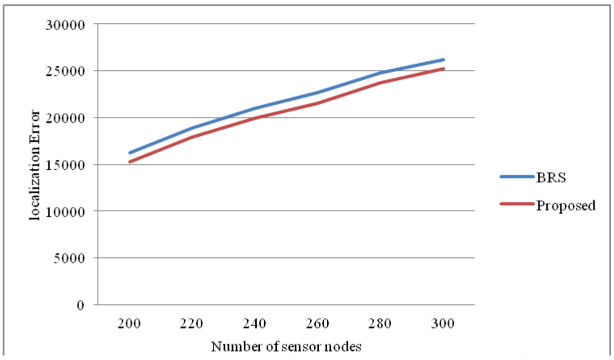

Fig. 3. Compares the error rate for increasing the number of sensor.

VI. Conclusion

Proposing a novel benign locating method in wireless sensor networks under attacks of enemy nodes is our aim. Our method consists of two steps which integrity is designed in the first step, based on formation of benign nodes table in sink. In the next step, Taylor series least square method is used to determine the coordinates of the 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 *Proc. 9th International Conference on Network Protocols*, 2001, pp. 35–41.

[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 *Proc. the 14th IEEE International Conference on Computer Communications and Networks*, San Diego, Calif, USA, 2005, pp. 557–562.

[3] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free localization schemes for large scale sensor networks," in *Proc. 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 *Proc. 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 *Proc. IEEE Sensors Conference*, Waikoloa, Hawaii, USA, 2010, pp. 668–672.

[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. 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.

[9] Y. Shang, H. Shi, and A. A. Ahmed, "Performance study of localization methods for ad-hoc sensor networks," in *Proc. the IEEE International Conference on Mobile Ad-Hoc and Sensor Systems*, October 2004, pp. 184–193.

[10] 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 *Proc. the IEEE 61st Vehicular Technology Conference*, vol. 4, pp. 2551–2555, Stockholm, Sweden, June 2005.

[11] 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.

[12] J. Hwang, T. He, and Y. Kim, "Detecting phantom nodes in wireless sensor networks," in *Proc. the 26th IEEE International Conference on Computer Communications (INFOCOM'07)*, May 2007, pp. 2391–2395.

[13] 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*, p. 13, 2012.

[14] 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.

[15] N. Yu, L. Zhang, and Y. Ren, "BRS-Based Robust Secure Localization Algorithm for Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2013, p. 9.

Sayyed Majid Mazinani was born in Mashhad, Iran on January 28, 1971. He received his bachelor degree in electronics from Ferdowsi University, Mashhad, Iran in 1994 and his master degree in remote sensing and image processing from Tarbiat Modarres University, Tehran, Iran in 1997. He worked in IRIB from 1999 to 2004. He also received his PhD in wireless sensor networks from Ferdowsi University, Mashhad, Iran in 2009. He is currently an assistant professor at the Faculty of Engineering in Imam Reza University, Mashhad, Iran. He was the head of the Department of Electrical and Computer Engineering from 2009 to 2012. His research interests include computer networks, wireless sensor networks and smart grids.