A NEW SECURE LOCALIZATION APPROACH OF WIRELESS SENSOR NODES INTHE PRESENCE OF MISBEHAVING ANCHOR NODES

ZohrehSobhanifar[1] and AbolfazlToroghiHaghighat[2]

[1,2]Department of Electrical, Computer and Biomedical Engineering, Qazvin branch, Islamic Azad University, Qazvin, Iran

ABSTRACT

This paper proposes a new algorithm to find and isolate the nodes which lies about their position in a Wireless Sensor Network (WSN). Also the proposed method enables the sensor nodes to find their location in presence of liar nodes. In the proposed method, a given number of neighbors for all sensors is determined wherethe number of liars is below a predefined threshold value. The proposed method is evaluated in finding the liars and also the correct location of each node. The minimum error rate on the determination of liars and the location of sensors proves the ability of the algorithm for localization of sensors in the WSNs.

KEYWORDS

Wireless Sensor Network (WSN),Secure Localization,Wireless Security, Network Security

1. INTRODUCTION

Wireless Sensor Networks (WSNs) provides many shared activities among all users where the activities are considered as a small part of pervasive technology. They are used in many interesting applications. Realization of these applications requires wireless ad hoc networking techniques [1].The applications of WSNs in both military and civilian cases reveal the necessity of wireless ad hoc networking such as target tracking, environmental monitoring,and traffic regulation, to name just a few [2].

WSNs are build up by deploying multiple microtransceivers called sensor nodes that allow users to gather and transmit data from regions which might be inaccessible or hostile to human beings. The data transmission is performed independently by each node in a wireless medium. All sensors in WSNs use multi-hop communications where they collaborate with each other to route collected data to the target [3]. In WSNs, routing algorithms is based on different measures such as network structure or the protocol operations [1]. In the routing protocol, the sensor node positions are utilized to route the packet data in the network. In the geographical area, the information of all sensors must be collected in order to locate their positions.

The location of sensors must be secured to provide the integrity of the WSN and its associated services. At the first step, the necessary parameters for each node are determined to find all paths in order to lead their data towards the targets [4].The information of node's positions is utilized to analyse the data collected by the sensors, i.e. the origin of collected data should be known for the

DOI : 10.5121/ijcseit.2014.4301

user before using it. Finally, when the end user needs to collect information from some nodes, it should be send the position the query nodes. The localization process is therefore crucial [5].Note that the false information on the geography of the phenomenonprovided by attacker is received by sensors. To secure the localization of WSN, most of the work is based on the use of trust models when the trusted nodescalled anchors provide information to localization processes (e.g. localization process using several GPS-based anchors [3].

A new class of anchor nodes is verifiers which review the information provided by the anchors. This model is often too expensive and not always realistic. Firstly, to ensure the coverage of network, the distribution of anchors and verifiers should be determined a priori. The representation of these special nodesis likely to be inferior because their cost is higher than the cost of regular nodes [6]. On the other hand, the cryptographic approach is necessary to apply trust on WSNs. It is important that the localization process should have a minimum effect on the energy consumption.Finally, to deploy the integrity of sensors, the trusted nodes should be monitored and so too much trust may decrease the independently of a WSN [3].

In this paper, the goal is the providing the information bout the location of regular nodes in the presence of neighboring sensors which may lie about their location.In this paper, it is considered that the liar sensors known their locations,but that, for any reason, inform false position to their neighbors. Their reasons may be malicious(i.e., to mislead regular sensors into wrong locations)or inadvertent (i.e., due to the presence of obstacles that prevent them from providing correct locations). The proposed method, it is considered that the position of regular nodes is determined in the situation that the number of liar nodes in the neighborhood of each regular node is below a predefined threshold value. The proposed method enables regular nodes to find and isolate the liar nodes.

2. LOCALIZATION IN THE PRESENCE OF LIARS

Assume that the location of the specific node A should be determined. The point with location $(a_x,a_y)$is the intersection of three circles which arecentred atB_1 و B_2 و$B_3$and with radii $d(A,B_1), d(A,B_2)$and $d(A,B_3)$, respectively. Note that the locations of B_1 و B_2 وB_3 are $B_1(b_{1x},b_{1y})$و$B_2(b_{2x},b_{2y})$ and $B_3(b_{3x},b_{3y})$, respectively [3-4,7].

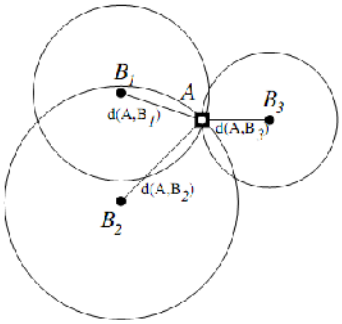

Figure 1.Localization of sensor *A* using three nodes B1, B2, and B3 that are located in its distance one neighborhood (Captured from [3]).

The function *d* is calculated using following equations [3]:

$$(b_{1x} - a_x)^2 - (b_{1y} - a_y)^2 = d(A, B_1)^2 (1)$$
$$(b_{2x} - a_x)^2 - (b_{2y} - a_y)^2 = d(A, B_2)^2 (2)$$
$$(b_{3x} - a_x)^2 - (b_{3y} - a_y)^2 = d(A, B_3)^2 (3)$$

Consider now that the sensor *A* may receive signals from the nodes which announce incorrect locations to *A*. Assume that $N_1(A)$shows the set of neighborhoodsensors which is located at the distance one hop away from *A*, and *l*refers to the number of liar nodes($l \leq N_1(A)$) (see Figure2).

Let us that the liar is parameterised with *S*. In this paper, a method is described to findthe correctposition of regular nodes in the presence of liar nodes. Also, the proposed algorithm is able to exclude the incorrect and at isolating the set of liars. Note that *A* knows the upper bound *l* of sensor nodes lying in the geographical area. The proposed method is analyzedfor a given number of liars.

In Section 3, the proposed algorithm uses the pairs of signals received from two nearest neighbor and also a majority rule. We assume that $B_i, B_j \in N_1(A)$ is the pair of points in the neighbor of *A*which computes the pairs of points $(a_x, a_y), (a'_x, a'_y)$ as the intersection of two circlescentered at B_i, B_j with radii $d(A, B_i)$ and $d(A, B_j)$, respectively. Note that the majority rule is utilized to correct location of *A*.We show that if the numberof liars among the nodes in $N_1(A)$ is higher than one, *A* isable to determine its proper location if$n > \frac{4l+1+\sqrt{8l^2+1}}{2}$.

3. SECURE LOCALIZATION USING TWO NEIGHBOR SIGNALS

Let us sensor *A* uses the signals of two neighbors and so the correct location is one the two points of intersection of the two circles centered at these two neighbours [11]. In this method, for every pair of neighbors$B_i, B_j \in N_1(A)$, sensor *A*computes a pair of locations {*x*,*x'*} which is the intersection of two circles with centersB_i, B_j.

As the shown inFigure 2, the proper location of *A* is either *x* or *x'*. After that, *A* may use the majority rule to find the best position for *A* and to report liar nodes. It is important that at least one of the nodes in all possible pairs ofthem is liar. In this regard, this paper can have either [3,8]:

1- both sensors are liars, for a total of $\binom{l}{2}$ pairs,or

2- exactly one sensor is liars for a total of $\binom{n-l}{1}.\binom{l}{1}$pairs.

If a pair of locations is determined by two truth tellers, this pair is correct, otherwise it is incorrect. The majority rule is utilized to accept the best position [9]. The rule is accepted if the number of incorrect location is lower than the number of correctpairs of locations. This amounts to having the inequality [10,12]:

$$\binom{n}{2} - \binom{l}{2} - \binom{n-l}{1}.\binom{l}{1} > \binom{l}{2} + \binom{n-l}{1}.\binom{l}{1} \quad (4)$$

from which we derive the inequality:

$$\binom{l}{2} > 2\left(\binom{l}{2} + \binom{n-l}{1}.\binom{l}{1}\right) \quad (5)$$

Table 1.Relation between the minimum number of liars and the minimum number of neighborsto determine a correct pair of locations (using Algorithm 2) for a specific node.

Number of liars	Minimum number of neighbors
1	5
2	7
3	9
4	11
5	13
10	23
15	33
20	43

As the previous mentioned, the proposed method works for a given number of liars. In this regard, the minimum number of neighbor for a given number of *l* liars is presented in Table2. To prove the Table 2, reader can refer to [3-4].

Let us that the number of neighbors andliars characterized with *n* and *l*, respectively.Assume that $n = 5$and $l = 1$, the proposed method can be used to find a correct pair of locations, {*x*,*x'*}. Since there is 5 neighborsfor *A*, from which one sensor is liar, the remaining sensors are truth tellers. To find the liar node, following approach is proposed: at first, all intersection nodes{*x*,*x'*} of all possible pairs of 5 nodes are produced. After that the pair of sensor which produces two intersection nodes with maximum distance from the other intersection nodes, are selected as the possibly liar nodes (suspicious pair).The next step is analyzing of each of sensor of the suspicious pair in the other pairs of these sensors. Finally, the sensor that in all its pairs, most of the produced intersection nodes have the maximum distance to the other intersection nodes is chosen as the final liar node. The liar node is removed from 5 neighbor are truth tellers. After removing of the liar node, the task is determination of actual location of *A.* For this purpose, the sensor where the average of its intersection node's locations (local average) has the nearest distance to the average of all intersection node's locations (global average), is chosen as the actual location of *A.* It means that the selected node which produces the best intersection nodes is considered as the best choice. At the final stage, the majority rule is employed to select one of the intersection points of the best sensor, {$\underline{x}$,$\underline{x}$'}, as the actual location of *A.*

It is clear that the distribution of intersection nodes is the criterion of secure localization which consists of finding the correct location of a specific sensor and reporting the liars. It is reasonable that the node with maximum distance to other nodes is considered as the liar node and the node with the minimum distance to the mean of all intersection nodes is considered as the correct location a specific node.

4.SIMULATION

In this section, the proposed method is evaluated to prove the ability of the method to allow their sensors to find their own location in an arbitrary WSN under the presence of liars. For this purpose, a uniform distribution of *n* sensors located randomly and independentlyin the interior of a unit square is considered. Note that in this simulation, n is set from twenty to 100-sensors and the number of liars is the percentage of all sensors. The evaluation step is divided into two parts,

one part is about the ability of the proposed method in liar detection and the second one is about the evaluation of the proposed method in finding the correct location of each node. Results of the proposed method is compared the basis algorithm [3]. The difference between the basis algorithm [3] and the proposed method is that in the basis algorithm [3], distribution of the intersection nodes is not considered which is effective in the localization process.

In Figure2, the error rate on the detection of liar nodes is demonstrated in different number of nodes, [20,100], using the following equation

$$\text{Error Rate} = \frac{\text{No.of detected liars which are incorrect}}{\text{Total no.of liars}} \quad (6)$$

In the above equation, the error rate is computed on the detected liars which are incorrect. This simulation tests the ability of the proposed method in finding actual liars. According to the figure, maximum value is obtained in the size if twenty nodes (minimum size). Note that in each number of nodes, 30% of all sensor are liars. This figure proves that the number of liar nodes is increased with increasing number of nodes while the error rate on the liar node detection is not increased and so, the proposed algorithm is robust to increasing number of liars.

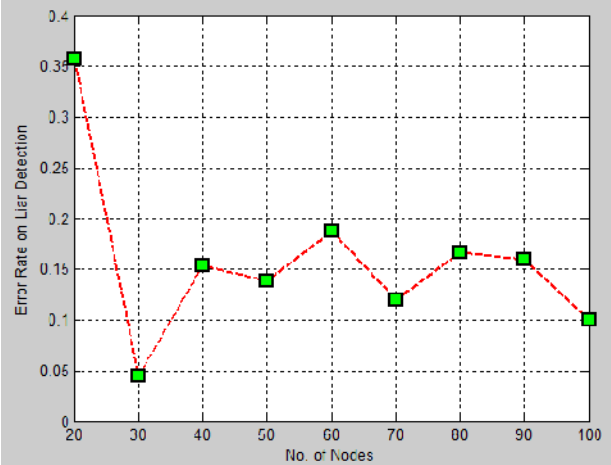

Figure 2.Error rate on the detection of liar nodes in different number of nodes.

In Table 2, the results of error rate on liar detection are reported in all number of liars. In this table, the minimum number of neighbors for each number of liars is determined. In each case, the average value is the mean of error rate during 10 iterations. In this simulation, the average error rate is increased along with increasing in the both of the number of liars and the minimum number of neighbors. In comparison to Algorithm 2 [3], the best results is achieved using the proposed method because of the idea of distribution of sensors. In the other words, the pair of intersection nodes with maximum distance to the other intersection nodes is reasonable to consider as the liars.

In Figure 3, the percentage of correct localization of all nodes is shown. In this regard, each node unaware of its location requests the location of its neighbors. The simulation was run for 100 times for each network size. Results of the simulation for the networks with size of twenty to 100-sensors aredemonstratedinFig. 3 which provesthe ability of the method to increase the number of sensors that aware of their position when the average of liars is low.

Table 2. Simulation results in different number of liars obtained using the Alg. 2 [3] and the proposed method

Case	Number of liars	Minimum number of neighbors	Average of error rate	
			Alg. 2 [3]	Proposed method
1	1	5	18.17%	**15.87%**
2	2	7	20.21%	**16.91%**
3	3	9	21.98%	**17.99%**
4	4	11	23.50%	**19.10%**
5	5	13	24.65%	**20.36%**
6	10	23	25.13%	**21.85%**
7	15	33	27.18%	**23.24%**
8	20	43	28.91%	**24.79%**

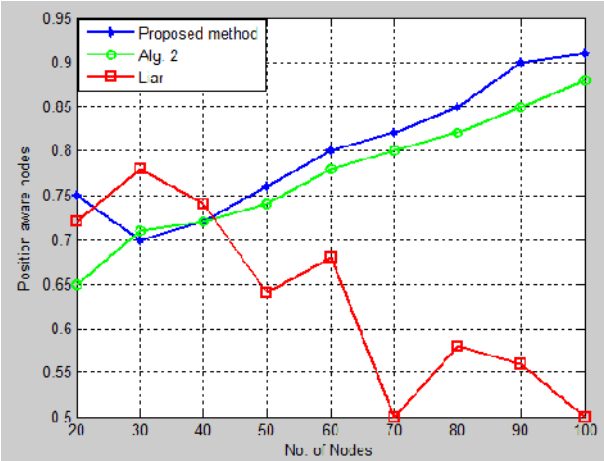

Figure 3.Percentage of correct localization of all nodes in different number of nodes.

Note that in this simulation, the proposed method is evaluated in the case which the number of liars is decreased with increasing of network size. It is important that the minimum number of liars is 50% of total network size. It is important that the percentage of position aware nodes is improved in the proposed method. The reason of superiority of the proposed method to the other algorithm refers to the idea of distance between the intersection nodes and mean of all intersection node locations. According to this idea, the intersection nodes which are near to the mean of all intersection nodes are reasonable to be the correct location of a specific node.

5. CONCLUSION

This paper presents a new methodology to deal the localization process of WSN nodes in the presence of liars. The proposed method has two properties: providing of correct position of each sensor, and finding and isolation of the liar nodes.The proposed method utilizes the distribution of intersection nodes where the intersection nodes with maximum distance to the other nodes can be considered as the liars and the intersection node with minimum distance to mean of all

intersection nodes is considered as the correct location of a specific sensor. The simulation results show the best results in finding the liars and the correct location of each node.

REFERENCES

[1] Al-Karaki, J. N. &Kamal, A. E. (2004)"Routing techniques in wireless sensor networks: A survey",IEEE Wireless Communications, Vol. 11, No. 6, pp. 6–28.

[2] Barbeau, M., Kranakis, E., Krizanc, D. & Morin, P. (2004) "Improving Distance Based Geographic Location Techniques in Sensor Networks", 3rd International Conference on AD-HOC Networks & Wireless (ADHOC-NOW'04), pp. 197–210, LNCS 3158, Springer.

[3] Alfaro J.G., Barbeau M. &Kranakis E. (2009) "Secure localization of nodes in wireless sensor networks with limited number of truth tellers". In: 7th annual communication networks and services research (CNSR) conference. IEEE, Piscataway, NJ, pp. 86–93.

[4]Alfaro, J.G., Barbeau, M. &Kranakis E. (2011) "Secure Geolocalization of Wireless Sensor Nodes In The Presence of Misbehaving Anchor Nodes", Annals of Telecommunications-Annales des telecommunications, Vol. 66, No. 9-10, pp. 535-552.

[5] Bahl P., Padmanabhan V.N. &Balachandran A. (2000) "Enhancements to the RADAR user location and tracking system", Microsoft Research, Technical Report MSR-TR-2000-12, Microsoft, p 13.

[6] Capkun, S. &Hubaux JP (2005) "Secure positioning of wireless devices with application to sensor networks. In: 24th annual conference of the IEEE computer and communications societies, Vol. 3. IEEE, Piscataway, NJ, pp. 1917–1928.

[7] Capkun, S, Cagalj, M, Srivastava, M. (2006) "Secure localization with hidden and mobile base stations". In: 25th annual conference of the IEEE computer and communications societies. IEEE, Piscataway, NJ, pp. 1–10.

[8] Capkun, S. &Hubaux J.P. (2006) "Secure positioning in wireless networks",IEEE J Sel Areas Commun,Vol. 24, No. 2, pp.221–232.

[9] Delaet S., Mandal P., Rokicki M. &Tixeuil S. (2008) "Deterministic secure positioning in wireless sensor networks", In: IEEE international conference on distributed computing in sensor networks (DCOSS). Springer, Berlin, pp 469–477

[10] Doherty, L. &Ghaoui L.E. (2002) "Convex position estimation in wireless sensor networks", In: 20th annual joint conference of the IEEE computer and communications societies. IEEE, Piscataway, NJ, pp. 1655–1663.

[11] He T., Huang C., Blum B.M., Stankovic, J.A., Abdelzaher, T. (2003) "Range-free localization schemes for large scale sensor networks", In: 9th annual international conference on mobile computing and networking. ACM, New York, NY, pp. 81–95.

[12] Hwang J., He T. & Kim Y. (2008) "Secure localization with phantom node detection", Ad Hoc Networks Vol. 6, No. 7, pp.1031–1050.

[13] Ji, X. &Zha, H. (2004) "Sensor positioning in wireless ad-hoc sensor networks using multidimensional scaling", In: 23rd annual joint conference of the IEEE computer and communications societies. IEEE, Piscataway, NJ, pp. 2652–2661.