I. J. Computer Network and Information Security, **2015, 12, 52-59**
Published Online November 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2015.12.06

Enhanced Voting based Secure Localization for Wireless Sensor Networks

M. B. Nirmala
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumakuru, Karnataka, India
Email: nirmalamb@sit.ac.in

A. S. Manjunatha
Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumakuru, Karnataka, India
Email: asmanju@gmail.com

***Abstract*—**Development of location estimation algorithms with improvement in location precision with lower cost, less energy consumption and less hardware support has become more important for many applications in Wireless Sensor Networks (WSNs)**.** This paper addresses the problem of secure location determination, known as secure localization in WSNs using voting based technique which gives a search region in presence of anchor nodes. From the obtained search region trilateration is applied to know the position of sensor nodes. To avoid the involvement of sensor nodes in further location estimation process, bilateration is applied. Experimental analysis shows that the maximum number of nodes can be localized and accurate location of a node can be determined efficiently with low estimation error. To avoid the attacks and involvement of malicious nodes in the localization process, we implement an improved authentication and security algorithm. Using few location reference points in the localization process reduces the communication cost. The proposed scheme also provides very good localization accuracy.

***Index Terms*—**Wireless Sensor Networks (WSNs), Secure Localization, Trilateration, Bilateration.

I. Introduction

The rapid growth of wireless communication technology has promoted the development of WSNs [1]. In recent years, large amount of WSN-related applications such as physical environment monitoring, health monitoring, security surveillance, medical systems, nuclear plant have been proposed. Location estimation is one of the interesting research area for the last couple of years and many protocols and algorithms have been developed. Localization system is not used, only for location identification, but also provides the base for routing, target tracking, environment monitoring and number of other communication aspects [2].

At present, many localization algorithms for sensor networks have been proposed and most of the WSNs include a small number of anchor nodes, which know their own positions beforehand by either using GPS or being manually configured [3]. These anchor nodes help other sensor nodes to know their positions. But for the existence of many obstacles and errors, the location precision will be restricted, and some nodes even cannot be located. So the improvement of localization precision with lower cost, less energy consumption and less hardware support has become more important. One of the main methods to improve localization accuracy is to increase the number of anchor nodes, but the number of anchor nodes is always limited because of the hardware restrict, such as cost, energy consumption and so on.

WSNs may be deployed in hostile environments where malicious adversaries attempt to spoof the locations of the sensors by attacking the localization process. For example, an attacker may alter the distance estimations of a sensor to several reference points, or replay beacons from one part of the network to some distant part of the network, thus providing false localization information [4]. Hence, we need to ensure that the location estimation is performed in a robust way, even in the presence of attacks [5]. Furthermore, adversaries can compromise the sensor devices and force them to report a false location. It is a challenging task to provide location accuracy in the presence of malicious nodes. Therefore, localization should be done in secure way [2].

Many secure localization algorithms are developed [7-10][13] to securely localize the sensor nodes using anchor nodes. Trilateration in the basic localization technique mainly used in practice [15]. To accurately determine the location using trilateration three anchor nodes are needed. It is possible to identify the location using trilateration, but a small subset of sensor nodes is not localized. Localization algorithms using voting based approach are developed in [5][6][11][12][15][17].

A secure efficient localization scheme developed in [6] is based on voting and trilateration method for location discovery. In sensor networks voting method provides us the portable region where unknown node exists and trilateration helps to find sensor node position in that portable region. It is noticed that some subsets of sensor nodes don't get the vote count greater than two and hence they can't be localized using trilateration. Trilateration requires minimum three anchor nodes in communication range. In order to localize such sensor nodes, already localized sensor nodes who know their position are

considered as the anchor nodes. Involvement of sensor nodes in the localization process continues until all the nodes are localized. Many sensor nodes are involved in this process, hence consuming much of their energy. In order to avoid involvement of sensor nodes in the localization process, if the vote count is two, we employ bilateration [18] to localize the sensor nodes.

This paper deals with enhanced secure voting based localization scheme. In this scheme we consider the voting based scheme discussed in [6] and if the vote count is greater than three, minimum three nearest anchor node positions are used for trilateration. If the vote count is less than three, bilateration is applied for location estimation. With this, sensor nodes involved in localization process are avoided and hence the energy consumption is reduced. The sensor node whose vote count is one is not localized. Experimental analysis and simulation results shows that almost all the sensor nodes are localized with minimum localization error. Rest of the paper is organized as follows. Next section gives the literature survey on secure localization protocols. Section III gives proposed scheme. Simulation results are explained in section IV and finally section V gives conclusion.

II. Related Work

Several secure localization algorithms are proposed in the recent years. Some algorithms are range dependent and some are range independent [21]. Range dependent localization algorithms estimate the location of a sensor node based on Received Signal Strength indexing (RSSI), Angle of Arrival (AoA) and Time difference of Arrival (TDoA). Range independent localization scheme determine the location based on the information received from Beacon nodes. Ours is range independent voting based localization algorithm hence we discuss range independent and voting based secure localization algorithms.

Various types of attacks are possible in localization process. Attacks can be divided as external attacks and internal attacks [22]. External attacker is outside the WSN and tries to spoof the location information using cryptographic keys. Internal attacker take hold of the normal nodes and controls them.

Loukas lazos et al. proposed SeRLoc[5], ROPE[8], HiRLoc[10] secure localization algorithms, where all these protocols provide encryption, authentication of beacon nodes using global preloaded keys. These protocols require extra hardware like directional or sectored antennas in the beacon nodes.

Liu et.al., [4] propose an attack resistant MMSE based location estimation and a voting based localization scheme in which a localization area is divided into a grid and a vote count of the grid is incremented if the distance from the anchor node is equal to the distance measurement obtained from the anchor. The centroid of the nearest cells with the highest vote count is estimated as the position of the unknown node.

SeRLoc[5] is based on a two-tier network architecture that allows sensor to passively determine their location without interacting with other sensors and uses voting method. Authors use the concept of sectored Antenna for location discovery. Malicious attack is reduced by considering the majority of vote count. The paper also shows that SeRLoc is robust against known attacks on WSNs such as the wormhole attack, the Sybil attack and compromise of network entities but the sensor node estimate its location as the center of gravity of the overlapping region hence precise location is not estimated.

Some schemes utilize clustering algorithm in localization mitigate the impact of malicious attacks. Wang *et al.* proposed a cluster-based MMSE (CMMSE) [12] which uses an MMSE to identify and construct a consistent location reference set for the final location estimation. However, the random selection of initial location references makes CMMSE obtain different results in different runs, and might cause more rounds of execution failure.

SeLoc[11] provides grid based secure localization scheme. To reduce the probability of attack the actors in home and neighbor actors are used to verify the location. SeLoc is robust against wormhole and Sybil attack. The number of actor nodes involved is more. The performance of the SeLoc depends on the crossover point [11]. The performance of SeLoc scheme increases with the value of crossover point.

Monte Carlo based approach for localization was proposed in [20], a fixed number of candidate sample locations that satisfy a constraint on the maximum velocity of the nodes are randomly generated. Samples that are inconsistent with the measurements obtained from anchor nodes are filtered out and a final estimate of the location is found by averaging the remaining samples. The localization accuracy of the algorithm is low. These algorithms did not consider the presence of malicious anchor nodes in the network.

Chen et al.,[14], Sohail et al.,[19] propose localization algorithms based on genetic algorithm and bio inspired computing respectively where computation cost is high. Ravi Garg et.al [16] have proposed a secure localization algorithm using gradient decent approach. If the distance between the sensor nodes and anchor nodes is large then it takes time to converge and computation cost increases. Authors of [23] discuss localization based on mobile nodes. Security of localization schemes can certainly be enhanced by using efficient key management schemes [24][25].

Secure voting based localization scheme is proposed in [6] uses vote count and selects three anchor nodes and applies trilateration to compute the location of a sensor node. In this paper we propose to use trilateration and bilateration to reduce the energy consumption at sensor nodes. Sensor node authenticates the anchor nodes before receiving the location information. Anchor nodes send the location information securely to the sensor nodes. To secure the location information a key is generated using the preloaded key.

III. Proposed Scheme

This section presents an enhanced voting based localization scheme which includes voting based method, security scheme for authentication and confidentiality, trilateration and bilateration for finding the absolute or relative position estimation of sensor nodes.

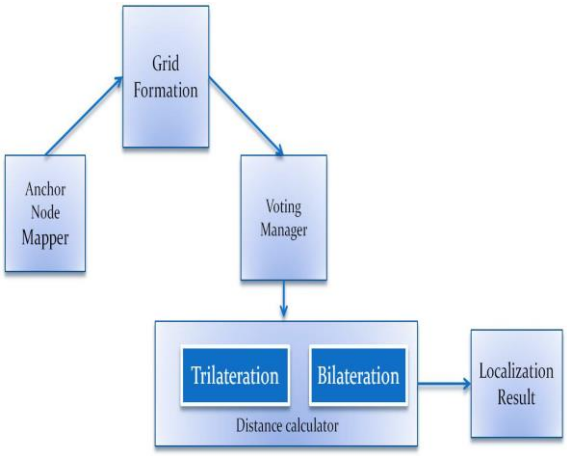

Fig. 1. Block diagram of Enhanced voting based secure localization scheme

Section A explains the voting method, section B gives the security scheme, Section C explains trilateration process. Bilateration process is explained in section D and section E gives the Algorithm for enhanced voting based secure localization scheme and explains the steps involved.

A. Voting Algorithm

The network is divided into N x N cell. Initially all cell will have vote count zero. If the anchor node communication range intersects with the cell, then the cell value is incremented. If the sensor node lies within the cell then the total cell count becomes the vote count of the sensor node. The total vote count represents the total number of healthy anchor nodes within its communication range. For example fig 2 shows 8 x 8 grid formation and anchor nodes a_1, a_2 and a_3 sending the beacon message to sensor nodes and sensor node s_1 getting the vote count. Fig 3 shows the vote count of s_1. If the vote count of the sensor node is greater than three, any three anchor nodes are selected. Which anchor to select is decided by the sensor node based on the time difference of arrival of the data from the anchor nodes. Preference of the anchor node selection is based on distance and trust worthiness of the anchor node which is verified using security scheme. If the anchor nodes proved to be malicious, such nodes are removed from the localization process and the vote count is decremented. Now the Sensor node authenticates the anchor nodes and decrypt the location information of the anchor node using the secret key and also verifies the integrity of the location information.

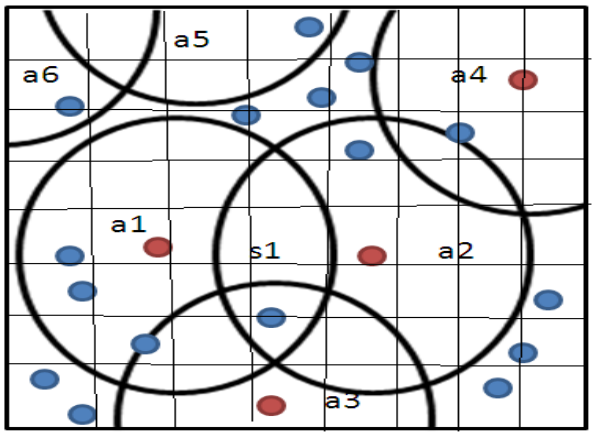

Fig. 2. Example of 8 ×8 grid with anchor node intersection region

2	2	1	1	2	1	1	1
1	2	1	1	1	1	1	1
2	2	1	2	2	2	2	1
1	1	2	2	1	2	2	1
1	1	2	2	1	1	1	1
1	2	3	3	2	1	1	1
1	2	3	3	2	2	1	0
0	2	2	3	2	2	0	0

Fig. 3. Vote count for the 8 x 8 example grid of Fig 2

B. Security Scheme

The security requirements in the enhanced secure voting based scheme are authentication of nodes, securing the location information sent from anchor nodes to sensor nodes and checking the integrity of the location information. In this security scheme both the sensor nodes and anchor nodes are preloaded with a key K_0. Shared key K_0 is assumed to be known by the trusted users in the network. Anchor nodes sends its id a_i and a random number r_n to sensor node. Sensor node sends its id s_i and r_n +1 to anchor node. Anchor nodes generate a session key k_s concatenate with r_n +1 encrypt with the shared key, compute hash on the same and sends it to sensor node. Sensor nodes check the integrity of the session key. Anchor nodes send the encrypted location information to sensor nodes. Sensor nodes decrypt the location information using the session key k_s. Fig 4 shows the interaction between anchor node and sensor node for session key establishment and secure location information communication.

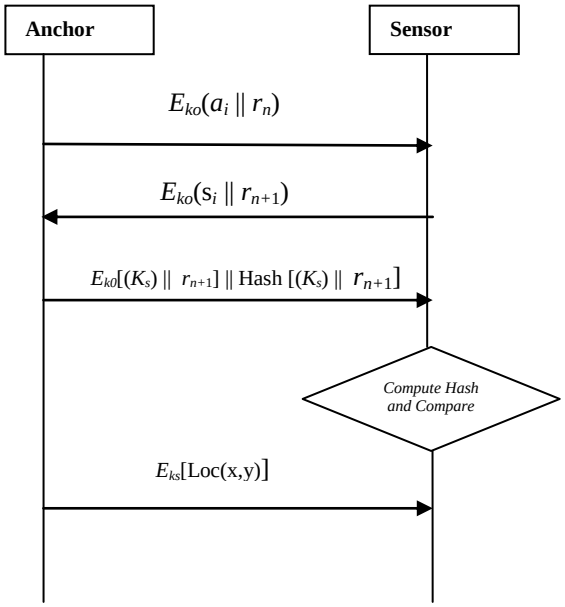

Fig. 4. Security scheme

C. Trilateration

After finding the number of anchor nodes around each grid having the sensor node, trilateration is applied. If the vote count is greater than two, trilateration is selected. Trilateration is the process of determining absolute position or relative location of point by measurement of distance using the geometry of circle, spheres or triangles. Trilateration is shown in fig 5. If the number of neighbour anchors for the sensor node S_i is three or more, then choose three intersecting anchor nodes as shown in fig 5. Calculate the midpoint between any two anchor node that is between A_1 and A_2 in equation 1 and again calculate the midpoint between this midpoint and third anchor node A_3 in equation 2. Calculated midpoint $mid(X_m, Y_m)$ gives the sensor node location. To simplify the calculations, the equations are formulated so that the centers of the spheres are on the z = 0 plane.

$$mid(X_m + Y_m) = \left(\frac{X_1+X_2}{2}, \frac{Y_1+Y_2}{2}\right) \quad (1)$$

$$mid(X_m + Y_m) = \left(\frac{X_m+X_m}{2}, \frac{Y_3+Y_3}{2}\right) \quad (2)$$

D. Bilateration

When the number of neighbour anchors for the sensor nodes S_i is two, bilateration is applied. Choose any two intersecting anchors nodes. Calculate the midpoint between the centers of any two anchor nodes as in equation 3. Calculated midpoint $mid(X_m, Y_m)$ gives the sensor node location as shown in fig 5.

$$mid(X_m + Y_m) = \left(\frac{X_1+X_2}{2}, \frac{Y_1+Y_2}{2}\right) \quad (3)$$

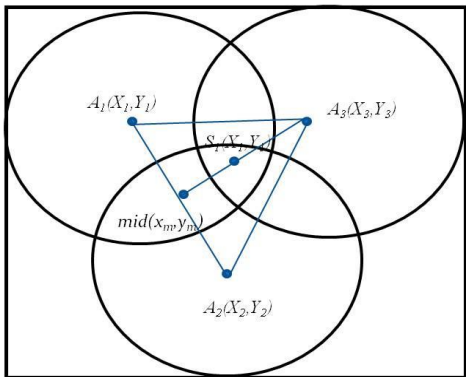

Fig. 5. Trilateration

E. Algorithm for Enhanced Voting based Secure Localization

In Step 1,2 and 3 the network controller deploys the sensor nodes and anchor nodes. Divides the network region into N x N grid and sets the vote count of each sensor node to zero. Anchor node broadcast the message. Sensor nodes which are in the communication range of anchor nodes receive the message and increase the vote count depending on the number of anchor nodes. This is explained in step 4 and 5. If the vote count is greater or equal to 3, sensor node authenticates three anchor nodes otherwise if the vote count is two it authenticates to anchor nodes. Step 6 explains authentication and encryption process. If three nodes are authenticated, location estimation is performed using trilateration as explained in step 7 otherwise if two anchor nodes are authenticated then bilateration is performed to estimate the location as given in step 8.

Algorithm: Enhanced voting based secure localization.

For the sensor node S_i where $I = 1, \ldots, k$, where k is total number of sensor nodes in the network

1. Consider the deployment area having anchor node a_j where $j = 1, \ldots l$, where l is the total number of anchor nodes.
2. Construct a grid of N x N where N is a natural number.
3. Initially consider the vote value $V = 0$ for each cell.
4. Voting scheme executed at sensor nodes checks If any anchor node's communication range lies within the cell, evaluates the trust worthiness of anchor nodes and then the vote count is incremented (V++).
5. Sensor nodes request for trusted anchor nodes position.
6. Selected Anchor node's position information is securely sent to sensor nodes using security scheme as explained in section B .
7. If the number of neighbouring anchor nodes for the unknown node $S_i \geq 3$ then apply trilateration and calculate the position of a nodes as explained below.

i) Choose any three intersecting node among the m anchors.

ii) Anchor nodes be $A_1(X_1,Y_1)$, $A_2(X_2,Y_2)$ and $A_3(X_3,Y_3)$.

iii) Calculate the midpoint between any two anchor nodes

$$mid(Xa + Ya) = \left(\frac{X_1+X_2}{2}, \frac{Y_1+Y_2}{2}\right)$$

iv) Again calculate the midpoint between $(Xa + Ya)$ and $(X3 + Y3)$

$$mid(Xa + Ya) = \left(\frac{X_a+X_3}{2}, \frac{Y_3+Y_3}{2}\right)$$

v) $mid(Xa + Ya)$ gives the position of the sensor nodes S_i.

8. Else if the number of neighbour anchors for the unknown node $S_i = 2$, apply bilateration and find the location of a node.

a. Choose any two intersecting nodes of the *m* Anchor.
b. Anchor nodes be $A_1(X_1,Y_1)$ and $A_2(X_2, Y_2)$
c. Calculate the midpoint between two anchor nodes

$$mid(Xa + Ya) = \left(\frac{X_1+X_2}{2}, \frac{Y_1+Y_2}{2}\right)$$

d. $mid(Xa + Ya)$ gives the position of the sensor node S_i.

IV. Performance Analysis

Simulation is carried out with the varying network size of 100 to 400 nodes and varying set of anchor nodes. The network region is divided into 12 x 12 grids. Fig 6 shows simulation result of dividing the network into 12 x 12 and anchor nodes broadcasting the message and sensor nodes collecting the information. Fig 7 and Fig 8 shows the sensor nodes performing trilateration and bilateration respectively. Fig 9 shows localization graph for the deployment of different network size using trilateration and bilateration. The graph shows that as the number of anchor nodes increases maximum number of nodes can be localized by trilateration. If maximum number of nodes need to be localized using trilateration, the sensor nodes which are already localized should also act as anchor nodes which creates a burden on the sensor nodes and consumes more energy. To reduce the energy consumption at sensor nodes, which is a major concern for a battery powered and deployed in hostile environment, bilateration is used in localization process. If the sensor nodes are not able to localize using trilateration with only anchor nodes, bilateration is applied. In our scheme sensor nodes are not involved in computing other sensor node's location. Sensor nodes need 3 anchor nodes to use trilateration. Initially when the anchor nodes are less, the number of localized nodes using trilateration is also less, but as the anchor nodes increases the number of nodes localized using trilateration also increases. We noticed, using bilateration along with trilateration, with lesser number of anchor nodes, number of localized nodes increases. Using trilateration and bilateration the total time taken for localization process is reduced. The number of anchor nodes required in our scheme reduced by 30% to 15% as the network size increases from 100 to 400 nodes.

Table 1, gives the time taken for trilateration and bilateration for network size of 100 sensor nodes. As sensor nodes using bilateration involves communication only with two anchor nodes, the time taken for bilateration is reduced. Table 2 gives location estimation $S_i(X, Y)$ compared with the actual location of the sensor nodes. Accuracy of the location estimation using bilateration is same as trilateration.

Fig 10 gives the total time taken to localize the sensor nodes in presence of varying number of anchor nodes. Fig 11 shows the calculated localization position using our scheme compared to actual position of the sensor node. It shows the difference between the actual position and the sensor node position is ± 5 units.

Total energy required by the sensor node and the anchor node in our scheme is 143.2 mJ and 72.52 mJ respectively for trilateration. Total energy required by the sensor node and the anchor node in our scheme is 95.5 mJ and 72.52 mJ respectively for bilateration. If the sensor node act as an anchor node for the localizing process of the next sensor nodes, the energy consumed is 284.13mJ for trilateration, this amount of energy consumption is reduced. Thus our enhanced secure localization scheme is energy efficient.

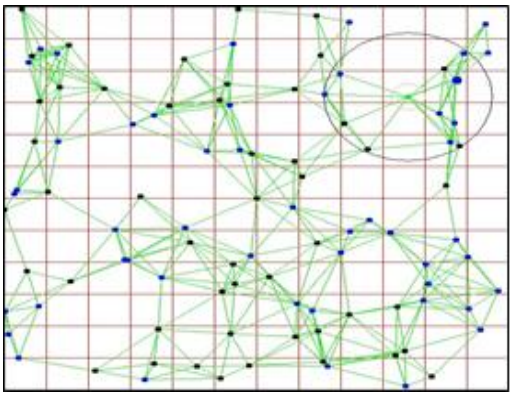

Fig. 6. Sensor nodes collecting voting information

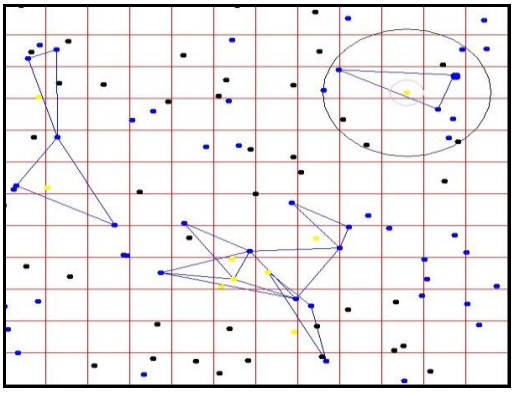

Fig. 7. Sensor nodes performing trilateration

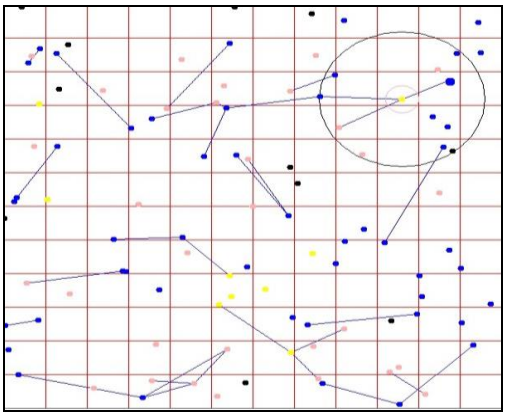

Fig. 8. Sensor performing bilateration

Table 1. No. of nodes localized and time taken for trilateration and bilateration for network size of 100 sensor nodes.

No. of Anchor node	Method	No. of localized node	Time taken (ms)
20	Trilateration	25	5843
	Bilateration	21	4056
25	Trilateration	38	4268
	Bilateration	27	3553
30	Trilateration	38	4452
	Bilateration	31	3913
35	Trilateration	48	5572
	Bilateration	37	4753

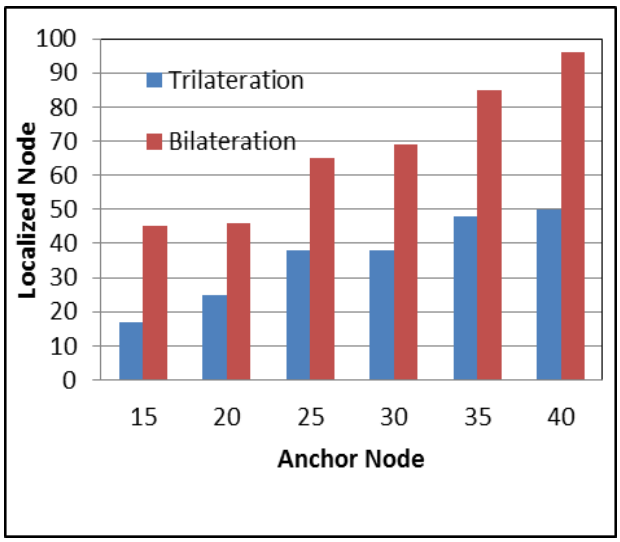

Fig. 9.a. With Network size of 100 Nodes

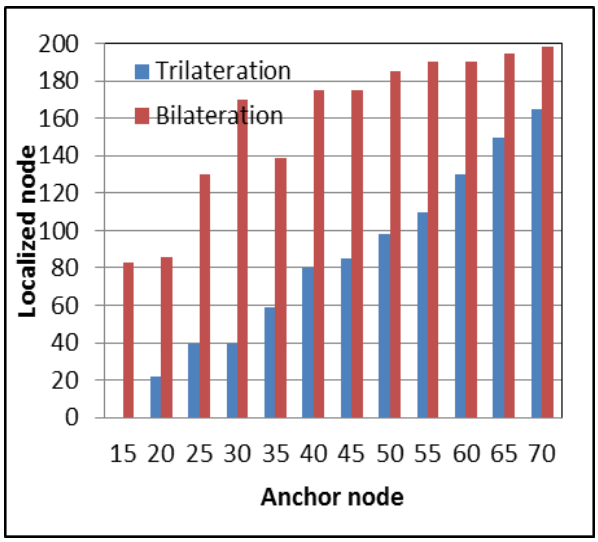

Fig. 9.b. With Network size of 200 Nodes

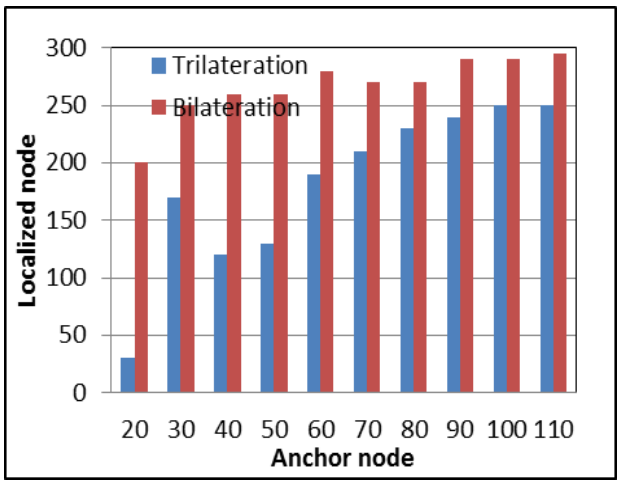

Fig. 9.c. With Network size of 300 Nodes

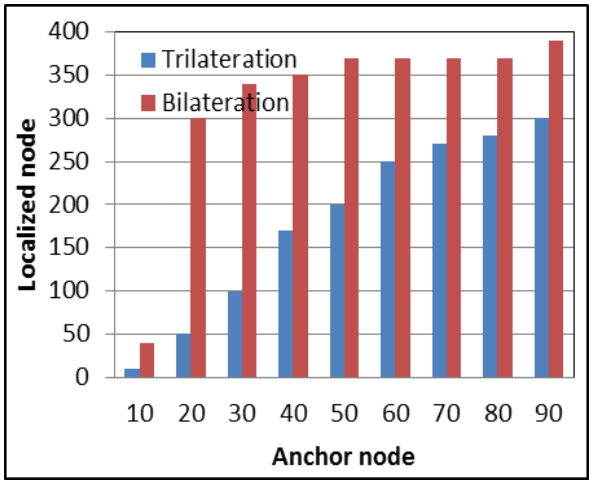

Fig. 9.d. With Network size of 400 Nodes

Fig. 9. Number of Localized sensor nodes using trilateration and bilateration with varying set of anchor nodes

Table 2. Computed localization value compared to actual value for randomly selected sensor nodes.

No of Anchor node	Method	Node ID	Actual Value		Computed Value	
			X	Y	X	Y
20	Trilateration	98	391	368	394	375
		21	294	464	310	463
	Bilateration	63	263	111	277	103
		32	419	371	415	353
30	Trilateration	33	175	506	208	506
		48	157	123	169	114
	Bilateration	79	238	273	248	286
		77	513	254	507	240
35	Trilateration	92	416	306	433	307
		89	497	51	509	50
	Bilateration	54	35	236	37	231
		93	316	474	345	470

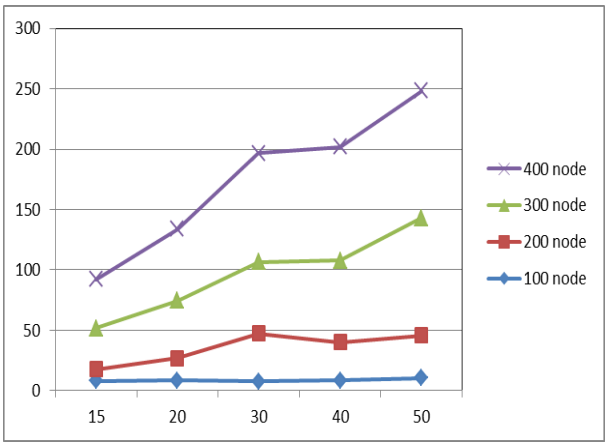

Fig. 10. Localization of sensor nodes using trilateration and bilateration with varying set of anchor nodes

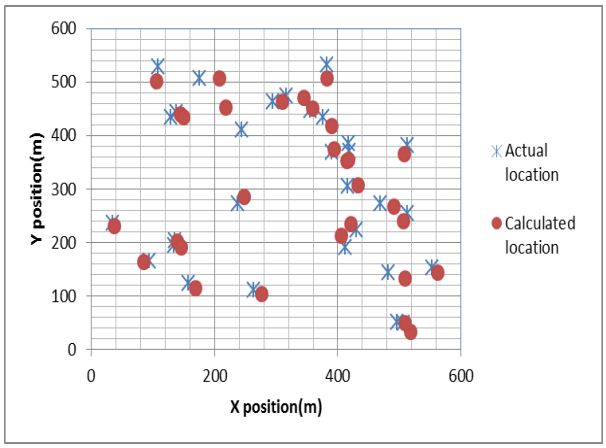

Fig. 11. Difference between actual location and estimated location

V. Conclusion

Enhanced voting based secure localization calculates the location of sensor nodes by communicating with the anchor nodes using trilateration and bilateration. Sensor nodes who know their position are not involved in the localization process thus reducing the energy consumption at sensor nodes which are battery powered. Simulation results show that using bilateration along with trilateration saves energy consumption at sensor nodes and requires 25% to 12% of anchor nodes to localize all the nodes. Position accuracy of the node using bilateration is same as trilateration with reduced communication cost.

References

[1] I.F. Akyildiz, Weilian Su,Y. Sankarasubramaniam, and E. Cayirci. A survey on Sensor Networks.Communications Magazine, IEEE, 40(8):102-114, 2002.

[2] Lowell J.R. Military applications of localization, tracking, and targeting, IEEE Wireless Communications, Volume 18 issue2, pp1536-1284, 2011.

[3] Srinivasan, Avinash, and Jie Wu. A survey on secure localization in wireless sensor networks. Encyclopedia of Wireless and Mobile communications(2007).

[4] D. Liu, p. Ning, a. Liu, c. Wang, and w. K. Du. Attack-resistant location estimation in wireless sensor networks. ACM trans. Inf. Syst. security, vol. 11, no. 4, pp. 1–39, 2008.

[5] L. Lazos and R. Poovendran. SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks. In Proceedings of WISE, Philadelphia, PA, Oct. 2004, pp.21–30.

[6] Nirmala M B, A S Manjunath and Rajani M. Secure and Efficient Voting Based Localization Scheme for Wireless Sensor Networks. BIJIT -2014, *BVICAM's International Journal of Information Technology*. July - December, 2014, Vol. 6 No. 2, ISSN 0973 – 5658.

[7] L. Lazos, R. Poovendran, and S. Capkun. ROPE: Robust position estimation in wireless sensor networks. In Proceedings of IPSN, April 2005.

[8] Srdjan Capkun and Jean Pierre Hubaux. Secure Positioning in Sensor Networks. IEEE Journal on Selected Areas in Communications (**JSAC**): Special Issue on Security in Wireless Ad Hoc Networks, February 2006.

[9] L. Lazos and R. Poovendran. HiRLoc: High-Resolution Robust Localization for Wireless Sensor Networks. IEEE Journal on Selected Areas in Communications, VOL. 24, NO. 2, February 2006.

[10] T. Zhang, J. He and Y. Zhang. Trust Based Secure Localization in Wireless Sensor Networks. In International Symposium on Intelligence Information Processing and Trusted Computing, 2011.

[11] Jianqing Ma, Shiyong Zhang, Yi-Ping Zhong and Xiaowen Tong. SeLoc: Secure Localization for Wireless Sensor and Actor Network. Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference. pp.864-869, Oct. 2006.

[12] Wenbo Yang; Wen Tao Zhu, "Voting-On-Grid Clustering for Secure Localization in Wireless Sensor Networks," Communications (ICC), 2010 IEEE International Conference. pp.1-5, 23-27 May 2010.

[13] Ning Yu, Liru Zhong and Yongji Ren. BRS-Based Robust Secure Localization Algorithm for Wireless Sensor Networks, Volume 2013, doi:10.1155/2013/107024.

[14] Jie Chen, An Improved Downhill Simplex-Genetic Multiple-Source Localization in Wireless Sensor Networks. Journal of Computational Information Systems 7:11(2011) 4007-4014.
[15] Amit gupta, shashikala tapaswi," Recurrent grid based voting approach for location Estimation in wireless sensor networks," IEEE Doi 10.1109/uic-atc.2009.43.
[16] Ravi garg , Avinash varna and Min wu "An efficient gradient descent approach to secure localization in resource constrained Wireless sensor networks," IEEE transactions on information forensics and security, vol. 7, no. 2, april 2012.
[17] Feng li and jie wu "A probabilistic voting-based filtering scheme in wireless Sensor networks,"iwcmc'06, july 3–6, 2006, vancouver, british columbia, canada.
[18] Juan Cota-Ruiz, Jose-Gerardo Rosiles, Ernesto Sifuentes and Pablo Rivas-Perea." A Low-Complexity Geometric Bilateration Method for Localization in Wireless Sensor Networks and Its Comparison with Least-Squares Methods", Sensors 2012, 12, 839-862.
[19] Sohail Jabbar, Rabia Iram, Abid Ali Minhas, Imran Shafi and Shahzad Khalid, Intelligent Optimization of Wireless Sensor Networks through Bio-inspired Computing; survey and Future Directions. International Journal of Distributed Sensor Networks, Volume 2013, Article ID 421084, 13 pages.
[20] L. Hu And D. Evans, "Localization For Mobile Sensor Networks", In Proc. 10th ACM ANNU. Int. Conf. Mobile Comput. Netw. (Mobicom), Philadelphia, Pa, 2004, Pp. 45–57.
[21] Han, Guangjie, Huihui Xu, Trung Q. Duong, Jinfang Jiang, and Takahiro Hara. Localization algorithms of wireless sensor networks: a survey." Telecommunication Systems 52, no. 4 (2013): 2419-2436.
[22] Gonzalez-Tablas Ferreres, A.I.; Ramos Alvarez, B.; Garnacho, A.R., "Guaranteeing the Authenticity of Location Information," Pervasive Computing, IEEE, vol.7, no.3, pp.72,80, July-Sept. 2008.
[23] BELKADI, Malika, Rachida AOUDJIT, Mehammed DAOUI, and Mustapha LALAM. "Mobile Localization Based on Clustering." International Journal of Computer Network and Information Security (IJCNIS) 5, no. 9 (2013): 37.
[24] Verma, Seema. "A Comparative Study of Key Management Protocols for WSN." *International Journal of Computer Network and Information Security (IJCNIS)* 6.4 (2014): 29.
[25] Diop, Abdoulaye, Yue Qi, and Qin Wang. "Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks." *International Journal of Computer Network and Information Security (IJCNIS)* 6.8 (2014): 9.

Authors' Profiles

M.B. Nirmala received B.E degree in Computer Science and Engineering in 1998 from Kuvempu university and M.Tech degree in Computer Science in 2003 from Visvesvaraya Technological University, Belgaum, India. She is currently pursuing her Ph.D under Visvesvaraya Technological University, Belgaum, India. She is working as Associate Professor in the Dept of Computer Science and Engineering, Siddaganga Institute of Technology, Tumakuru, India. Her research interest includes Computer Networks, Wireless Sensor Networks, Multimedia Communication, Cryptography and Network Security.

A.S. Manjunatha received his M.Tech and PhD in Computer Science 1988 and 2003 from Mysore University and Bangalore University, India respectively. He is working as Professor in the Dept of Computer Science and Engineering, Siddaganga Institute of Technology, Tumakuru, India. His research interests are Embedded Systems and solutions, Networking and communications, Wireless Networks and soft computing. He has published several papers in refereed International Journals and conferences.

How to cite this paper: M. B. Nirmala, A. S. Manjunatha,"Enhanced Voting based Secure Localization for Wireless Sensor Networks", IJCNIS, vol.7, no.12, pp.52-59, 2015.DOI: 10.5815/ijcnis.2015.12.06

