BIJIT - BVICAM's International Journal of Information Technology
Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM), New Delhi (INDIA)

Secure and Efficient Voting Based Localization Scheme for Wireless Sensor Networks

Nirmala M. B[1], **A. S. Manjunath**[2] and **Rajani. M**[3]

Submitted in May 2014; Accepted in September 2014

Abstract - Many sensor network applications require sensor node to obtain their locations correctly. Various techniques have been proposed to locate regular sensors based on some special nodes called anchor nodes, which are supposed to know their locations. Providing a certain degree of localization accuracy at the presence of malicious beacons becomes a very challenging task. In this paper, a secure and efficient voting based localization scheme is proposed to mitigate the above impact. In this scheme voting based technique gives a search region in which sensor nodes are present, and then in search region trilateration is applied to know the position of sensor nodes. The communication between anchor and sensor nodes is authenticated and secured by encryption. The proposed scheme can provide very good localization accuracy with the reduced computational cost in presence of malicious nodes. This scheme is resistant to various attacks.

Index Terms – Wireless Sensor Networks (WSNs), Secure Localizations, Voting Based Method, Trilateration.

NOMENCLATURE

Wireless Sensor Networks (WSNs), Angle of Arrival (AoA), Time Difference Of Arrival (TDoA), Time of Arrival (ToA), Received Signal Strength Indicator (RSSI), cluster-based Minimum Mean Square Estimation (CMMSE), Attack-resistant Minimum Mean Square Estimation (ARMMSE), Least Median square(LMds).

1.0 INTRODUCTION

Wireless Sensor Networks (WSNs) is a significant technology attracting considerable research. It is experiencing an explosive growth similar to the internet, this is largely due to the attractive flexibility of anytime, anywhere network access enjoyed by both users and service provider. Knowledge of position of the sensing nodes in a Wireless Sensor Network is a necessary part of many sensor network operations and applications.In hostile environment knowing the position of the sensor is very difficult. The process of determining the position of the sensor nodes in WSNs is defined as localization (location estimation). Sensor node uses anchor node to calculate its location. Anchor nodes are aware of their position through GPS or before deployment and exchange its location information with sensor nodes. The basic idea in D.Liu et al.,[1] is, nodes measure distances to their neighbours and share their position information with them to compute their positions. Sensor node whose position has been uniquely determined can act as a new anchor node to localize other nodes by sharing its position with its neighbours. This iterative process continues until all nodes are localized.

Secure localization as discussed in Jianqing at et al.,[2] is necessary as sensor nodes 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. Hence, the location estimation is performed in a secured way, even in the presence of attacks. Furthermore, adversaries can compromise the sensor devices and force them to report a false location to the data collection points. Therefore, a secure positioning mechanism is required.

Localization has an endless array of potential applications in both military and civilian applications as discussed in John et al.,[3], including land-mine detection, battlefield surveillance, target tracking, environmental monitoring etc, as discussed [21][23][24][25]. There are many advantages of knowing the location information of sensor nodes. Location information is needed to identify the location of an event of interest like the location of enemy tanks in a battlefield, the location of a fire, target-tracking applications for locating survivors in debris, or enemy tanks in a battlefield.

In this paper a secured efficient localization scheme is proposed based on voting and trilateration method for location discovery. In sensor networks voting method provides us the portable region where unknown node is present. After finding the search area trilateration is applied to find the accurate position. Trilateration is a process of determining absolute position or relative location of point by measurement of distance using the geometry of circle, spheres or triangles. In contrast to triangulation it does not involve the measurement of angles. In two-dimensional geometry, it is known that if a point lies on two circles then the circle centers and the two radii provide sufficient information to find one location. In three-dimensional geometry, when it is known that a point lies on the surfaces of three spheres, then the centers of the three spheres along with their radii provide sufficient information to find the possible locations. There are many other methods available to compute the actual location like Triangulation using AoA as references and Multilateration based on the TDoA where overhead is more compared to Trilateration.

In section 2 literature survey on voting based scheme and other schemes is discussed. Section 3 gives the detail discussion of

[1, 2, 3] *Department of Computer Science, Siddaganga Institute of Technology, Tumkur 572103, Karnataka, India*
E-mail: [1]nirmalamb@gmail.com, [2]asmanju@gmail.com and [3]rajani10.manju@gmail.com

the proposed scheme. Section 4 discusses the various type of attacks, analysis of threats to overcome these attacks. Section 5 discusses about computational complexity of our proposed scheme compare to other secure localization scheme.

2.0 RELATED WORK

A number of secure localization schemes have been proposed to estimate the location of sensor and protect the anchor nodes, Some of them defeat attacks by detecting and blocking malicious beacons as discussed in Chin et al.,[16], Jinfang et al., [17], Ning Yu[18]. As in Avinash et al.,[11] there are many approaches in localization a) Direct approaches: This is also known as absolute localization. The direct approach itself can be classified into two types: Manual configuration and GPS-based localization. The manual configuration method is very expensive. It is neither practical nor scalable for large scale WSNs and in particular, does not adapt well for WSNs with node mobility. On other hand, in the GPS-based localization method, each sensor is equipped with a GPS receiver. This method adapts well for WSNs with node mobility and it is not economically feasible to equip each sensor with a GPS receiver since WSNs are deployed with hundreds of thousands of sensors. b) Indirect approaches: The indirect approach of localization is also known as relative localization. In this approach, a small subset of nodes in the network, called the anchor nodes is used. It is classified into the following two categories Range-based and Range-free localization. Range-based localization depends on the assumption that the absolute distance between a sender and a receiver can be estimated by one or more features of the communication signal from the sender to the receiver like AoA, RSSI, ToA and TDoA. Range-free localization never tries to estimate the absolute point to point distance based on received signal strength. This greatly simplifies the design and cost effective.

Some schemes utilize clustering algorithm in localization systems to mitigate the impact of malicious attacks. Wang et al. proposed a CMMSE [4] 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. Along the same line, Misra et al. proposed CluRoL [4], which clusters intersections of reference circles to filter out malicious beacon signals but CluRoL is very slow, requires high computation and storage overheads.

A LMdS approach was proposed in [5] to solve the localization problem for scenarios where less than 50% of the nodes are malicious. This method shares similarity with the random sample consensus (RANSAC) algorithm [6], as it uses several subsets of nodes to identify candidate locations, and then chooses the solution that minimizes the median of the residues. These methods localize the nodes with small error as long as the fraction of malicious nodes is not too large. However, the memory requirement and computational cost of running these algorithms is high and can be difficult to meet in resource limited applications.

Loukas lazos et al.[7] present a distributed SeRLoc based on a two-tier network architecture that allows sensor to passively determine their location without interacting with other sensors. 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 in this sensor estimates its location as the center of gravity of the overlapping region, which is difficult to estimate.

Monte Carlo based approach for localization was proposed in [8], 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 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.

D. Liu, p. Ning et al.,[1] proposed a ARMMSE in which paper two methods to tolerate malicious attacks against beacon-based location discovery in sensor networks have been introduced. The first method filters out malicious beacon signals on the basis of the “consistency” among multiple beacon signals, while the second method tolerates malicious beacon signals by adopting an iteratively refined voting scheme. Both methods can survive even if the attacks bypass authentication, provided that the benign beacon signals constitute the majority of the “consistent” beacon signals. In an extreme case, if all the beacon nodes are compromised, these techniques will fail.

Chen et al.,[19], Sohail et al.,[20] propose localization algorithms based on genetic algorithm and bio inspired computing respectively where computation cost is high.

Our proposed scheme takes a distinct approach by protecting the location privacy of sensor nodes, preventing inaccurate and false location information. Decreasing the computation cost by reducing communication overhead and reduces the location estimation error with no extra localization equipment being employed.

3.0 PROPOSED SECURE LOCALIZATION SCHEME

This section gives the detailed description about the proposed secure localization scheme. proposed secure localization scheme is based on voting and trilateration method. Voting based method provides a search region where the sensor node exists. Once the region of sensor node existence is found, trilateration is applied to find the exact location of a sensor node.

Our proposed scheme is purely based on a set of location references, however this scheme is range-independent localization scheme. The location references are taken from set of anchor nodes, so there is no extra communication overhead involved when compared to the other range based localization schemes as discussed in Avinash et al.,[11]. We propose a new key establishment mechanism to establish a symmetric key between the sensor node and anchor nodes to transmit the location information securely to the sensor node. Voting based method finds the overlapping region, if more than three anchor nodes are in the overlapping region of the sensor node, any three anchor nodes are selected and trilateration is applied to calculate the sensor node location. The anchor nodes encrypt the location information of their's and send it to sensor node. Sensor node uses three anchor node locations to compute its position. Network model assumption is given in section 3.1.

3.1 Network model

Sensor network consists of sensor nodes. We assume that a set of sensor nodes S_i= $S_{1,}\ldots,S_n$ and a set of anchor nodes A_j=$A_{1,}\ldots,A_m$. The number of anchor nodes m deployed is less than 1/4th the of sensor nodes n. We assume that the anchor nodes know their positions accurately (since they are GPS enabled or by other means). Sensor nodes depend on anchor nodes to compute their positions. All the sensor nodes are deployed in the region where its communication range lies within the range of three or more anchor nodes. We consider the anchor nodes which are static and the sensor nodes can be mobile or static. The voting based method and trilateration method is discussed in 3.2 and security scheme in 3.3.

3.2 Location estimation

In this section we discuss about our proposed location estimation scheme based on voting scheme and trilateration. In our proposed scheme the location is calculated based on the anchor nodes location information. The anchor nodes broadcast the location information to the sensor nodes. Based on the number of anchor nodes from which the sensor nodes is able to receive the information vote is collected. To illustrate this we consider an example as shown in figure (1). This figure explains both voting based method and trilateration method used to calculate the location of a sensor node.

Fig(a) shows the set of anchor nodes and sensor nodes deployed in an hostile area. Where sensor nodes have to calculate their location with the help of anchor nodes who know their location information in prior. The figure also shows the communication range of each anchor node. Fig (b) chooses the intersection range of three anchor nodes a_1, a_2, a_3 in which the sensor node s_1 lies. Around this intersection region an N×N grid is formed and split them into a N×N cells as shown in fig(c). each cell will have the communication range of selected anchor nodes. The anchor nodes which have maximum intersection are considered, take the intersection of communication range of those anchor nodes and split them in to number of $N \times N$ cells. Each cell will have communication range of selected anchor node. Take each location reference as vote. Votes in each cell indicate the number of anchor nodes with in the communication range. Initially all cells will have the vote zero. If any anchor node communication range lies in that cell, the vote count is increased by 1. Fig(d) shows the vote count of each cell and vote count for sensor node s_1 which lies within the communication range of three anchor nodes a_1, a_2, $a_{3.}$ Its vote count is three. Now the sensor node s_1 tries to calculate its location using trilateration as show in fig(e). Here three anchor nodes a_1, a_2, a_3 will be considered. Calculate the distance between any two anchor nodes. To simplify the calculations, the equations are formulated so that the nodes (centers of the spheres) are on the $z = 0$ plane. and also the formulation is such that one center is at the origin, and one other is on the x- axis, using this calculate x,y and z value, this gives sensor node position.

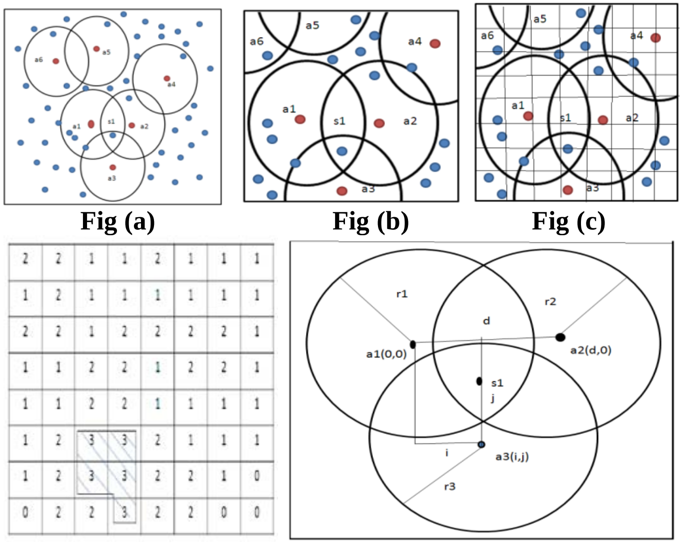

Fig (a) Fig (b) Fig (c)

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 (d) Fig (e)

Figure 1: (a) Secure network k. (b) Intersection of anchor node. (c) N × N grid in anchor node intersection region. (d) Applying voting technique. (e) Trilateration method.

3.3 Security scheme

This section describes the security scheme used to secure the localization information. We assume that before deployment, the sensor node and the anchor are stored with a key k_0. Each sensor node is preloaded with its id i,e s_{id} and a cryptographic hash function $h(\bullet)$ Immediately after the deployment of the anchor nodes and sensor nodes. The sensor node send S_{id} i,e sensor id and random number r_n generated by sensor node, encrypted with symmetric key k_0. Anchor node decrypt the s_{id} and r_{n} with the key k_0. when the sensor node wants to know its position, sensor node will generate a new secrete key, encrypt the key s_{ki} with r_{n} send it to anchor node. Anchor node initiate the communication, then sensor node send E_{sk}(s_{id} and h(r$_{\mathrm{n}}$)) to anchor node. Anchor node decrypts (s_{id} *and* $h(r_n)$) and compare $h(r_n)$ with previously stored value. If the received hash is same as the computed hash, then the sensor node is authenticated and the anchor node will send the location information to sensor node encrypted with s_{ki}. Figure 2 explains this security mechanism used to secure the localization information.

4.0 ATTACKS

Node compromise is the most fundamental attack in WSN that leads to other kinds of attacks[22]. It occurs when an attacker. gains control of a node in the WSN. With compromised node, an attacker can alter the node to listen information in the WSN, revoke legitimate nodes, input malicious data and cause internal attacks, e.g., DoS attack.

A replay attack is the easiest and most commonly used by attackers. Specifically, when an attacker's capability is limited, i.e., the attacker cannot compromise more than 1 node. In a replay attack, the attacker merely jams the transmission between a sender and a receiver and later replays the same message, posing as the sender. If an adversary manages to capture a node and extract the authentication/encryption keys, it can produce a large number of replicas having the same identity (ID) from the captured node and integrate them into the WSN at chose locations, which is called the node replication attack.

Security scheme for location information

Initialization:

1. Sensor node s_{id} chooses a random number sends $E_{k0}(s_{id} + r_n)$ to anchor.
2. Anchor node which are in the communication range of s_{id}, $D_{k0}(E_{k0}(s_{id} + r_n))$ stores the s_{id} and r_n .

Key exchange phase:

1. Later whenever the sensor node wants to know the location information, generates key s_k encrypt with r_n and send it to anchor node which have been selected for location estimation based on voting.
2. Anchor node sends acknowledgment for the received message.
3. Sensor send ($E_{sk}(s_{id}$ and $h(\mathrm{r_n})$) to anchor node.
4. Anchor node $D_{sk}(E_{sk}(s_{id}$ and $h(\mathrm{r_n})$), computes $h(\mathrm{r_n})$ and compare with the previously stored $h'(\mathrm{r_n})$ values. If both are same then, it encrupts $E_{sk}(L_a)$ sends it to anchor node.

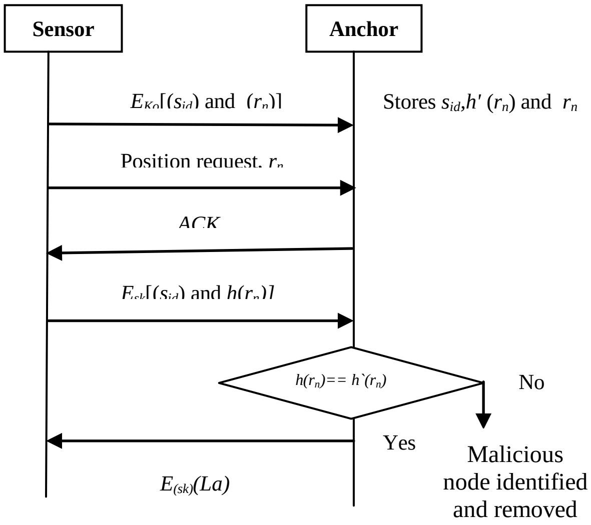
Sensor
Anchor
$E_{K0}[(s_{id})$ and $(r_n)]$
Stores s_{id},$h'(r_n)$ and r_n
Position request, r_n
ACK
$E_{sk}[(s_{id})$ and $h(r_n)]$
$h(r_n)== h`(r_n)$
No
Yes
Malicious node identified and removed
$E_{(sk)}(La)$

Figure 2: security mechanism for secure location information exchange

ALGORITHM: Secure voting based localization scheme.

1. Anchor nodes A_i where i=1,2,…m within the communication range of the sensor nodes, broadcast the message.
2. Initially sensor nodes set the vote count to zero i.e v=0.
3. As it hear the anchor nodes it count gets incremented, it has to hear from at least *3* anchor nodes. If 3 anchor nodes, are in the overlapping region, then the vote count is 3.
4. Sensor nodes generates key s_k, $E_{rn}(s_k)$, encrypts key s_k member with random number and sends it to anchor nodes.
5. Anchor nodes send the acknowledgment for the received message.
6. Sensor nodes sends $E_{sk}(s_{id}+h(r_n))$ to anchor nodes.
7. Anchor nodes sends decrypts$(s_{id}+h(r_n))$ with key s_k which was previous send, computes $h(r_n)$ with the previously stored r_n value and computes $h(r_n)$ with encrypts $E_{sk}(L_A)$ to sensor nodes.
8. Sensor nodes decrypts L_A which as co-ordinands values of $L_i(x_i,y_i)$, $L_{i+1}(x_{i+1},y_{i+1})$, $Li(x_{i+2},y_{i+2})$,…
9. Apply trilateration
   a) Consider that all three centers are in the plane $z = 0$. $a_1(0,0)$ is at origin, $a_2(d,0)$ at x axis.
   b) To find sensor node position calculate(x, y, z)

$$x = \frac{r_1^2 - r_2^2 + d^2}{2d}$$

$$y = \frac{r_1^2 - r_3^2 + i^2 + j^2}{2j} - \frac{i}{j}x$$

$$z = \pm\sqrt{r_1^2 - x^2 - y^2}$$

the adversary replicates one or more sensor nodes, it can execute the malicious operations. For instance, the replicas may inject false localization information into the WSN.

In a sybil attack, a node claims multiple identities in the network. When launched on localization, localizing nodes can receive multiple location references from a single node leading to incorrect location estimation. The Wormhole Attack establishes a direct link between two points in the network. The wormhole attack is very difficult to detect, since it can be launched without compromising any host.

In proposed scheme the authentication is used to identify the authenticated and malicious nodes. In our scheme as hashed random numbers are exchanged whenever sensor node encounters the anchor nodes for communication. Anchor node after receiving the random number verifies it with earlier saved value. If those two values are same then only it sends its location information to sensor nodes. Thus the scheme allows communication between the authenticated nodes thereby preventing above attacks.

As the location information is encrypted with the secret key location information will be secured and it will be difficult for attacker to hack. Table 1 gives summary of various security attacks addressed by our proposed secure voting based scheme scheme compared to other existing schemes.

5.0 PERFORMANCE ANALYSIS

The LMdS approach requires a certain minimum number of subsets of nodes M_1, which increases as the percentage of malicious nodes increases, in order to ensure that one estimate is the correct estimate with very high probability. An LS estimate needs to be found for each of these subsets, which is computationally expensive. The computation complexity associated with the LMdS method is calculated using the linear least squares (LLS) algorithm described in [9]. LMdS algorithm first performs M_1 LLS on different subsets of size n giving a computational complexity of□(M_1n). Comparing the computational complexity of the secure voting based method with CluRoL. Proposed scheme has a computational complexity of O(n^2), which is much less than that of $O(n^4 \log n)$ where n is the number of location references provided. This shows that scheme voting based method is efficient compared to CluRoL. Comparing the our scheme and gradient descent based scheme, we can see that they have similar run time. But gradient descent works well only when all received signals converges. If distance between the sensor node and the anchor node increases then the localization error also increases with high computational cost. In secure voting based method as it requires fewer reference points computational complexity is low. Table 2 shows the comparison of computational complexity of various algorithms.

Figure 3 illustrates the key storage overhead PVFS[14] and voting based scheme. PVFS requires storage of four times more keys in its key assignment process compared to voting based scheme. Voting based method requires fewer location references in its localization process, hence the keys required is also minimal.

We compare our secure voting based scheme experimentally with LMds and Gradient descent approach. Simulation is carried out with varying network size of 100 to 500 sensor nodes and 10 to 50 anchor nodes with a deployment region of 600m × 600m. The deployment region is divided into a 10 square grid with each cell of size 60m × 60m.

Figure 4 shows the run time required to achieve a desired localization accuracy comparing the localization errors with gradient descent approach and least mean squares. Localization error of our proposed method is approximately eight times lower compared to LMdS method. Comparing our secure voting based scheme with gradient descent based scheme, they have similar localization accuracy but in gradient descent based approach as the distance increases the localization error also increases. So proposed secure voting based scheme is efficient compared to other schemes.

Figure 5 explains the time taken for localization of different network sizes varying from 100 to 500 nodes by varying the number of anchor nodes. Simulation result shows that proposed

Algorithm	Localization Attacks				
	Wormhole	Sybil	Replication	Node compromise	Replay
SeRLoc	Y	Y	N	N	N
Attack Resistant Location Estimation	N	Y	N	N	N
Our proposed Secure Efficient Voting Based Localization Scheme	Y	Y	Y	Y	Y

Table 1: Summary of security attacks addressed by each algorithm

Method	Complexity
Least median Square	**θ**(M_1n)
CluRoL	$O(n^4 \log n)$
Gradient descent	**θ**(Mn)
Voting based scheme	**θ**(N_1^2n)

Table 2: Comparison of run time complexity of algorithms

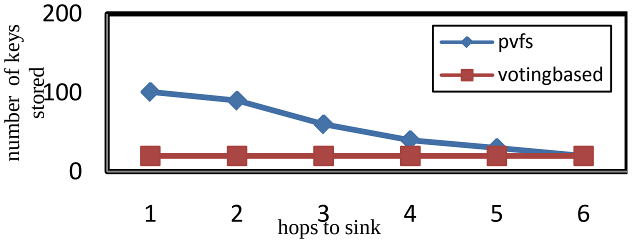

Figure 3: Key storage overhead

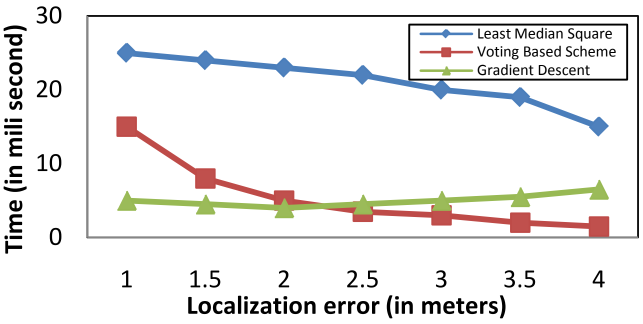

Figure 4: Comparison of localization error for different localization schemes

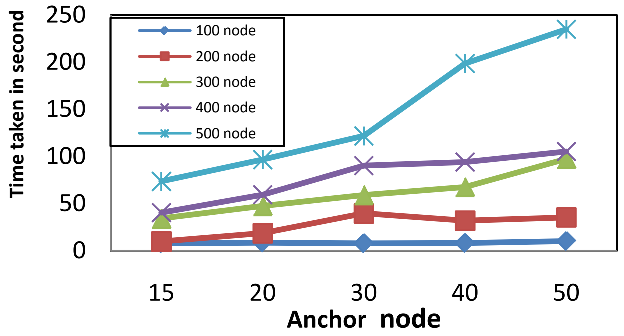

Figure 5: Time taken for localization

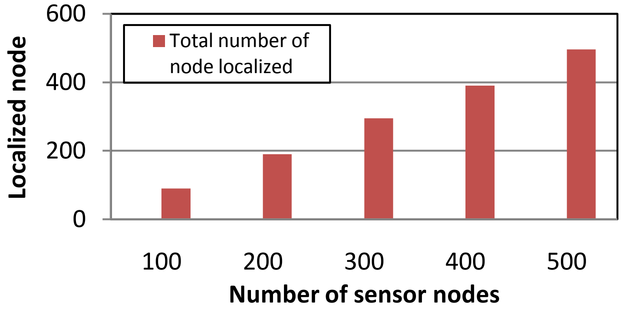

Figure 6: Total number of nodes localized.

scheme works efficiently upto 400 nodes. Above 400 nodes all the nodes will be localized but time taken for localization increases. Figure 6 gives the total number of nodes localized which is approximately 97% for varying network sizes.

6.0 CONCLUSION

In this paper, we proposed a secure and computationally efficient scheme for localization in wireless sensor networks. Voting based method is used to find localizing area of the node with low estimation error even for complex networks. Later trilateration is applied to find their position with the assistance of a small number of trusted entities. Authentication effectively prevents the attacks since it can filter the false information, which is caused by malicious sensor or anchor nodes that disturb the localization process. As the localization process involves fewer reference points the communication cost is reduced compared to other schemes.

7.0 REFERENCES

[1]. 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.

[2]. Jianqing Ma, Shiyong Zhangand Yiping Zhong "Seloc: Secure Localization For Wireless Sensor And Actor Network," ACM Transactions on Sensor Networks, IEEE 2006.

[3]. John R And Lowell, "Military Applications Of Localization,Tracking, And Targeting",IEEE Wireless Communications-April 2011.

[4]. Wenbo Yang And Wen Tao Zhu " Voting-On-Grid Clustering For Secure Localizationin Wireless Sensor Networks", IEEE ICC 2010.

[5]. Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust Statistical Methods For Securing Wireless Localization In Sensor Networks" in Proc. 4th Int Symp. Inf. Process. Sens. Netw. (IPSN), Los Angeles, CA, 2005, p. 12.

[6]. M. A. Fischler and R. C. Bolles, "Random Sample Consensus: A Paradigm For Model Fitting With Applications To Image Analysis And Automated Cartography" , Commun. ACM, vol. 24, no. 6, pp. 381–395, 1981.

[7]. Loukas Lazos And Radha Poovendran, "Serloc: Secure Range-Independent Localization For Wireless Sensor Networks" , Wise'04, October 1, 2004, Philadelphia, Pennsylvania, USA.

[8]. 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.

[9]. R. Szewczyk, E. Osterweil, J. Polastre, M. Hamilton, A. Mainwaring, D. Estrin, "Habitat Moand Nitoring With Sensor Networks", Commun. Vol. 47, No. 6, Pp. 34–40, Jun. 2004.

[10]. A. Savvides, C.-C.Han, Andm. B. Strivastava, "Dynamic FineGrained Localization In Ad-Hoc Networks Of Sensors", In Proc. 7th ACM ANNU. Int. Conf. Mobile Comput. Netw. (Mobicom), Rome, Italy, 2001, Pp.166–179.

[11]. Avinash Srinivasan And Jie Wu, "A Survey On Secure Localization In Wireless Sensor Networks,"Florida Atlantic University, Boca Raton, Fl, USA.

[12]. Amit Gupta, Shashikala Tapaswi, " Recurrent Grid Based Voting Approach For Location Estimation In Wireless Sensor Networks," IEEE Doi 10.1109/Uic-Atc.2009.43.

[13]. Ravi Garg , Avinashl.Varna And Minwu "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, 717.

[14]. 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.

[15]. J.T.Chiang, J. J. Haas, Andy.-C. Hu, “Secure And Precise Location Verificationcusing Distance Bounding And Simultaneous Multilateration,” In Proc. 2nd ACM Conf. Wireless Netw. Security, Zurich, Switzerland, 2009, Pp. 181–192.

[16]. Chin-Mu Yu, Yao-Trg Tsou, Chun-Shien Lu and Sy-Yen Kno, Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks, I086 Transaction of Information Forensics and Security, VOL 8 No.5, may 2013.

[17]. Jinfang Jieng, Guangjie Han, Chddan Zhu, Yuhui Dong, Na Zhang, Secure Localization in Wireless Sensor Networks: A survey, Journal of communication, VOL 6, NO.6, September 2011.

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

[19]. Jie Chen, An Improved Downhill Simplex-Genetic Multiple-Source Localization in Wireless Sensor Networks. Journal of Computational Information Systems 7:11(2011) 4007-4014.

[20]. 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, 13page.

[21]. Ashwani Kush and C Hwang “Hash Security for Ad hoc Routing” in BIJIT - BVICAM’s International Journal of Information Technology January – June, 2011; Vol. 3 No. 1; ISSN 0973 – 5658.

[22]. B B Jayasingh and B Swathi “A Novel Metric for Detection of Jellyfish Reorder Attack on Ad Hoc Network” in BIJIT - BVICAM’s International Journal of Information Technology Jan – June, 2010; Vol. 2 No. 1; ISSN 0973 – 5658.

[23]. B V Ramanamurthy, K Srinivas Babu and Mohammed Sharfuddin “Dynamic Data Updates for Mobile Devices by Using 802.11 Wireless Communication” in BIJIT - BVICAM’s International Journal of Information Technology Jan – Jun, 2011; Vol. 3 No. 1; ISSN 0973 – 5658.

[24]. Pranav M Pawar, Smita Shukla, Pranav Kulkarni and Adishri Pujari “Simulation and Proportional Evaluation of AODV and DSR in Different Environment of WSN” in BIJIT - BVICAM’s International Journal of Information Technology Jan – Jun, 2011; Vol. 3 No. 1; ISSN 0973 – 5658.

[25]. Sulata Mitra and Arkadeep Goswami “Load Balancing in Integrated MANET, WLAN and Cellular Network” in BIJIT - BVICAM’s International Journal of Information Technology Jan – Jun, 2011; Vol. 3 No. 1; ISSN 0973 – 5658**.**