# Secure and Robust 3D Localization in Wireless Sensor Networks

**A.V. Kalpana, D. Rukmani Devi, G. Elangovan, N. Indira, S.Venkatesan**

***Abstract: The fundamental capacity of a sensor system is to accumulate and forward data to the destination. It is crucial to consider the area of gathered data, which is utilized to sort information that can be procured using confinement strategy as a piece of Wireless Sensor Networks (WSNs).Localization is a champion among the most basic progressions since it agreed as an essential part in various applications, e.g., target tracking. If the client can't gain the definite area information, the related applications can't be skillful. The crucial idea in most localization procedures is that some deployed nodes with known positions (e.g., GPS-equipped nodes) transmit signals with their coordinates so as to support other nodes to localize themselves. This paper mainly focuses on the algorithm that has been proposed to securely and robustly decide thelocation of a sensor node. The algorithm works in two phases namely Secure localization phase and Robust Localization phase. By "secure", we imply that malicious nodes should not effectively affect the accuracy of the localized nodes. By "robust", we indicate that the algorithm works in a 3D environment even in the presence of malicious beacon nodes. The existing methodologies were proposed based on 2D localization; however in this work in addition to security and robustness, exact localization can be determined for 3D areas by utilizing anefficient localization algorithm. Simulation results exhibit that when compared to other existing algorithms, our proposed work performs better in terms of localization error and accuracy.***

***Keywords: localization, secure, robust, 3D, malicious nodes, cheating nodes, range-based, range-free*.**

## I. INTRODUCTION

WSN has transformed into a rising field in inventive work as a result of the substantial number of uses that can end up being basically useful from such systems and has provoked the improvement of shrewd not-reusable, small, modest and independent battery fueled PCs, equally called sensor nodes. These sensor nodes can identify assurance from a connected sensor and process the data gathered from the sensor node. After that the process, data remotely transmits the results to travel network. Wireless Sensor Network (WSN) is a gathering of light weight and low power sensor nodes which are spatially distributed and independent to display physical parameters. A WSN system comprises of a gateway, which gives wireless connectivity to the nodes and to the world. Its applications are used as a major aspect of military and battlefield surveillance, habitat monitoring, health care applications and environment checking, and so forth. The information accumulated without location is continually useless, so restriction turns into a key advancement in the Wireless Sensor Network. The location which is to be tested, need to be deployed with sensor nodes haphazardly either physically or deployed through air craft. Global Positioning Systems (GPS) receivers are imparted into the sensor node which can able to determine their location accurately. Be that as it may, this methodology isn't feasible, since instilling every one of the sensors with GPS enlarges the expense. So a superior methodology is that, few nodes are chosen and are conveyed with GPS, which are frequently called as beacon nodes or anchor nodes. The rest of the nodes which are there in the localization area can able to decide their location with the assistance of the anchor nodes, which reduces the cost when contrasted with when all the nodes are furnished with GPS.

Larger part of the localization techniques can be classified into two general classes explicitly, range-based and range-free techniques. Range based techniques [1], [2], [3], [4], [5], [6], [7] require the presence of special nodes that know their very own positions, called beacon nodes (or anchor nodes), at essential positions in the area. Remaining nodes in the area evaluate their area by preparing distance/angle investigations to a fixed set of beacon nodes. Range-free approach doesn't require a special node called beacon node, which is a cost-effective strategy when contrasted with range based technique. The location estimation utilizing range-based techniques are exact, since it depends on beacon nodes too when appropriate algorithm is used. The existing methodology for localization works very well for 2D localization within the presence of malicious nodes.

The vast majority of the localization algorithm works dependent on the 2-dimensional plane i.e., x and y plane. In a 2- dimensional plane, the calculation procedure is very basic and effective which requires less energy to calculate when considering a 3Dimensional location. When we meet an unexpected circumstance, for example, earthquake, hurricane or comparable disasters, wireless sensor nodes go to be important one in search and rescue operations. Wireless sensor networks can help in coordinating the search and rescue operation and give look in advantageous way. The localization algorithms are

**Revised Manuscript Received on November 27, 2019**.

***** Correspondence Author

**A.V. Kalpana,** Assistant Professor, Department of R. M. K Engineering College, Chennai, Tamilnadu, India. kalpanavijay21@gmail.com

**Dr. D. Rukmani Devi**, Professor Department of R.M.D Engineering College, Email: rdrukmani319@gmail.com

**N. Indira,** Assistant Professor, Department of Computer Science and Engineering at Panimalar Engineering College, Chennai, Tamilnadu, India. indiranatarajan13@gmail.com

**S.Venkatesan**, Senior Manager, Tejas Networks Pvt. Ltd. Bangalore, India. Email: Venbose_271@yahoo.co.in

utilized to discover the position of non-beacon nodes and therefore act as a new reference node for the non-localized nodes. In a 3-dimensional plane, we have to include an additional plane aside from x and y coordinate, which is called as z-coordinate. It tends to be utilized in slopes, mountains, terrains, hills to give a good accuracy. Regardless, when mapping these evaluated positions to this present reality a mistake can occur, in light of the fact that it contains all of the three planes. Any edge between the reference plane and the ground where it present result may be a mistake during mapping. By using a localization system for 3D this issue is administered completely.

In spite of the development in the area of efficient localization algorithms, the issue of malicious beacon nodes and localization inside seeing such nodes has not gotten sufficient interest. Malicious nodes can cheat by imparting mistaken position references or, then again transmitting at a lower energy level afterwards affecting the distance estimations and at last the localization based on it. With the extending usage of wireless and sensor systems in military and emergency crisissituations, the issue of malicious nodes can never again be neglected and its impact on location calculations ought to be inspected in more noteworthy detail. The issue of network localization inside the sight of malicious nodes isn't negligible: Eren et al.shown that a subset of the above issue, explicitly the issue of separation based confinement under the supposition that all nodes are straightforward, is itself hard [8]. Simply, localization within the sight of malicious nodes is impressively harder than the localization with each genuine node. Research articles to crush the issue of malicious nodes in localization algorithms used on exhausting the (over)dependence on such unique beacon nodes by using savvy quantifiable instruments and coding hypothesis[9], [10], [11], [12], [13].Our point is to propose a novel secure and robust localization algorithm which works in 3D condition like valley, slopes or mountains.

The remainder of the paper is sorted out as follows. We examine the groundwork and related work in Section II and present our system for 3D Localization in Section III. In Section IV, we demonstrate the Secure Localization phase; in Section V, we propose an algorithm and demonstrate the sufficient condition for robust localization and for finding the intersection of rings. Experimental evaluations are in Section VI and we conclude in Section VII.

## II. BACKGROUND AND RELATED WORKS

With the occasion and utilization of WSN innovation, there's a superior interest for localization accuracy. At present, investigation on two-dimensional localization of the wireless sensor network has become advanced; anyway the investigation of three-dimensional limitations stays in its early stages.

Zhang et al. show the Landscape-3D space localization algorithm [15] using mobile assisted nodes. Landscape-3D is the main robust 3D range based localization algorithm, in which the localization accuracy relies upon the exorbitant mobile beacon nodes. 3D MDS-MAP [16], 3D DVHOP [17], and 3D centroid [18] are sans range free localization algorithms from 2D plane situations explicitly. These strategies are unpredictable and the position isn't adequately exact. Li et al. [16] demonstrated robust statistical techniques, for instance, adaptive minimum squares and least median squares to make anchor based localization. Another technique towards robust localization is to adequately perform localization within the sight of errors while estimating distances. These errors can be an outcome of outside variables like random noise, measurement errors or as a result of malicious nodes. Substantial progression has been made to secure the localization scheme of WSNs [19, 20, 21, 22, 23,24]

Liu et al. [25] likewise proposed two methodologies for robust localization within the nearness of malicious beacon nodes. The principal technique filters through malicious beacon nodes dependent on the reason of irregularity among multiple beacon nodes, while the second system bears malicious beacon nodes by receiving an iteratively refined voting plan. Nizetic et. al [26] defined a localization method which takes into consideration the differences among the assorted access points, orientation of a client device and by hard the common signal strengths from many repetitive measurements, to reduce the unpredictable external interference. Jadliwala et.al [27] presented three algorithms for secure localization framework, which provides good accuracy but it works only in a 2-dimensional region.

Liu et al. [28] plan a shrewd framework, called voting based framework, where the deployment area is isolated into a cross section of cells to such an extent, that the objective hub dwells in one of the cells. Each beacon node votes on every grid relying on the detachment between the objective node and itself and the location of the target node is evaluated as being inside the cell that had the best number of beacon votes. Prima [29] a prototype of secure localization node for indoor wireless sensor network, named SCLoc. The sensor node is furnished with AES 128 cryptography system in wireless sensor networks. This algorithm is utilized to secure anchor node coordinates information and estimated position which has been determined in unknown nodes. A secure multi-lateration scheme proposed by Chiang[30] to verify that a prover is within a certain distance from the verifier and also to securely verify the location information. Fiore[31] presented a solution for Neighbor Position Verification, which permits any node in the network to confirm the position of the communication neighbors without depending on the priori trustworthy nodes.

Liu[32] investigated two algorithms called MNDC and EMDC to detect the nodes that are captured as malicious anchors and forge the information to delay accurate nodes locations acquisition in range-based localization schemes . The algorithms apply the density-based adaptive spatial clustering (DBSCAN) algorithm to obtain the abnormal clusters, which are further inspected via a sequential probability ratio test. The malicious nodes that endanger networks are then determined to minimize the number of initial parameters and avoid the situation that local outliers are categorized into normal clusters. Furthermore, SPRT based on consistency features of two distance measurements is hired to provide accurate detection results.

## III. SYSTEM MODEL FOR 3D LOCALIZATION

In this segment, we depict the system model for the issue of 3Dlocalization of a node K in untethered condition. In various words, K needs to figure its very own location utilizing beacon nodes which know their own locations and these nodes could possibly act maliciously.

Assume that there are n beacon nodes accessible for localization: i=1, 2, 3,… ..,n; m out of n signals are malicious, while the rest are honest[33]. The sensor nodes thought to be real all throughout the localization procedure as appeared in Fig 1.

Differentiated to two-dimensional localization calculations, three-dimensional localization calculations have the following issues:

(I) In 3Dlocalization increasing number of beacon nodes are required, ie., for 3Datleast four beacon nodes while for 2D localization, a minimum of three beacon nodes are compulsory to locate the unknown node. It needs to grow the node thickness as well as the calculation will become more complicated.

(ii) The transmission sign are enormously influenced by the terrain obstacles. The effect of the obstacles can’t be ignored. There is a slight deviation in the distances estimated by RSSI, which will impact the localization exactness.

The localization mode is appeared in [20] needs no less than four anchor nodes to choose the location of unknown nodes. It can also be observed that four anchor nodes should not be in a similar, remembering the end objective to ensure the localization.

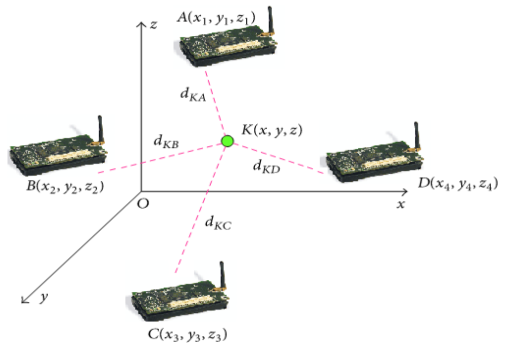



**Fig.1 3D Localization**

Assume there are four beacon nodes in the positions naming A, B, C and D situated at positions($x_1$,$y_1$, $z_1$), ($x_2$,$y_2$,$z_2$), ($x_3$,$y_3$,$z_3$) and ($x_4$,$y_4$,$z_4$) respectively which is appeared in Fig.1.K is the objective position which should be found with the coordinate (x,y,z). The distance between beacon nodes and unknown nodeare $d_{KA}$, $d_{KB}$, $d_{KC}$ and$d_{KD}$. Equation (1) is acquired as indicated by the separation between the hubs:

$$\sqrt{(x_1-x)^2+(y_1-y)^2+\ (z_1-z)^2}\ - d_{KA} = 0,\ldots\ldots\ldots\ldots\ldots\ (1)$$

$$\sqrt{(x_2-x)^2+(y_2-y)^2+\ (z_2-z)^2}\ - d_{KB} = 0,\ldots\ldots\ldots\ldots\ldots\ (2)$$

$$\sqrt{(x_3-x)^2+(y_3-y)^2+\ (z_3-z)^2}\ - d_{KC} = 0\ldots\ldots\ldots\ldots\ldots(3)$$

$$\sqrt{(x_4-x)^2+(y_4-y)^2+\ (z_4-z)^2}\ - d_{KD} = 0\ldots\ldots\ldots\ldots\ldots(4)$$

Resolving the equations (1), (2), (3) & (4) to get the coordinate of the unknown node K as (x, y, z) as shown in equation (5)

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \frac{1}{2}\begin{bmatrix} x_2-x_1 & y_2-y_1 & z_2-z_1 \\ x_3-x_1 & y_3-y_1 & z_3-z_1 \\ x_4-x_1 & y_4-y_1 & z_4-z_1 \end{bmatrix}$$

$$\begin{matrix} x_2^2-x_1^2+y_2^2-y_1^2+z_2^2-z_1^2+d_{KA}^2-d_{KB}^2 \\ .x_3^2-x_1^2+y_3^2-y_1^2+z_3^2-z_1^2+d_{KA}^2-d_{KC}^2 \\ x_4^2-x_1^2+y_4^2-y_1^2+z_4^2-z_1^2+d_{KA}^2-d_{KD}^2 \end{matrix} \ldots\ldots\ldots\ldots\ldots\ (5)$$

Independent of being direct or abusive, each beacon node $B_i$ gives K with an estimation $d_i$ of the distance among $B_i$ and M. Even more especially, each signal $B_i$ gives M with some extra data from which the separation di can be handled viably by M. The exact distance among $B_i$ and K is the Euclidean Distance between the position coordinates of $B_i$and M [6] and is implied byED[$d_i$]= dst($B_i$ , K). Given H be the set containing only the genuine beacon nodes among an aggregate of n beacon nodes. By then, for each signal node$B_i \in$ H, $d_i$ is relied upon to take after few likelihood distribution, showed as msr(dst($B_i$ , K)), with the ultimate objective that

$$ED[d_i] = dst(B_i, K)$$

i.e., the typical (mean) estimation of the evaluated distance $\tilde{d}_i$ for each reference point $B_i$ in H, is the exact distance between the signal $B_i$ and the node K. Furthermore, for the circumstance at whatever point $B_i$ is direct, the distinction between the estimated and the fair node is believed to be practically very little,

$$|d_i - dst(B_i, K)| < \varepsilon$$

where ε is the greatest distance error. Ideally, this distinction should be zero, anyway such variations in distance evaluations can happen due to mistakes, either at the source or target.

## IV. SECURE LOCALIZATION PHASE

The unknown node K is acquired through quadrilateration, which isn't amazing that beacon based strategies perform well when all the beacon nodes don't lie. In any case, their precision endures amazingly within the sight of malicious beacon nodes.

Beacon nodes can counterfeit by communicating their very own locations wrongly or by controlling the distance estimation process, subsequently influencing the restriction localization procedure which is delineated in Fig 3. In this figure, we can say that A, B and C carry on appropriately, though node D counterfeit the location coordinate and along these lines lead to mistaken estimation of the objective area called M rather than K.

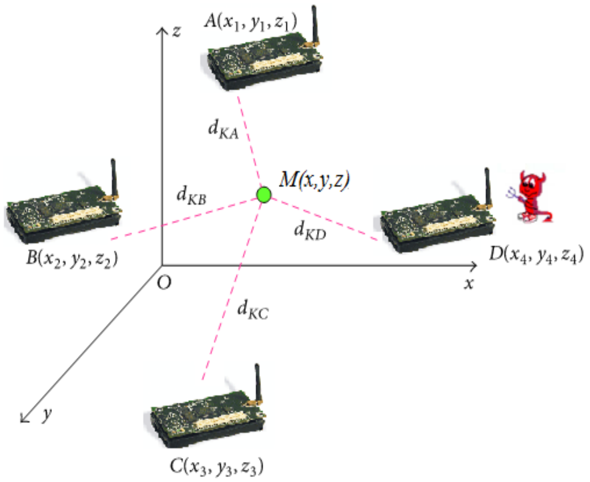



Fig.2 ***Distance based localization in the presence of malicious beacon which disturbs the localization procedure***

The beacon or anchor nodes are furnished with a controlling unit, which stores authentication ids apart from GPS. At whatever points the non-beacon node demands for target location, the beacon or anchor node requests the authentication id. This id ought to be registered in a group and get its public authentication key (AK) before any message transmission [33].

For signing a message, the node practices group authentication key and encryption work and send it alongside unique message to different nodes. Therefore it isn't obligatory for each part to have other node's private information, for instance, their identity and public key for authenticating them. Recipients check a member's identity by signature verification. It is accomplished by reconfirmation of encryption work with authentication key to the obtained message and differentiating the result to the signature.

Step 1: The beacon node transmits the location information as follows:

$\{M , H_{AK}( M),CU_G, ID(Beacon_A) \}$

Step 2: The Local CU cannot decrypt the message, since it doesn't have the private key of $CU_L$. It sends anapplication to $CU_L$ to decrypt the beacon ID. In this step, it decrypts only the id and none other.

Step 3: Since $CU_L$ doesn't have private key of beacon node A, so $CU_L$ cannot decrypt. $H_{PK}(ID(Beacon),H_{AK}(M))$ , therefore send an invitation of the private key of node A to the $CU_G$.

Step 4: $CU_G$ answer with the private key of beacon node A to $CU_L$ and $CU_L$ achieved by reconfirmation of encryption function with key of node A to the $(ID_A|H_{AK}(M))$ and comparing the result to the $H_{PK}(ID_A|H_{AK}(M))$. Also, $CU_L$ can identify the Sybil attack, if outcome of this comparison is dissimilar.

Step 5: $CU_L$ onward the private key of beacon node A to non-beacon node.

Step 6: The non-beacon node onwards the private key to beacon node.

The notations used during a message transmission are shown below:

| NOTATIONS | DESCRIPTION |
|---|---|
| REQ | Beacon node's request |
| REP | Local CU/Global CU Reply |
| E(…) | Encryption of the message |
| EH | Encryption with Hash function |
| D(…) | Decryption of the message |
| $PU_A$ | Public key for node A |
| $PK_A$ | Private key for node A |
| M | Original message |
| AK | Shared Key between all nodes which are located in that area |
| $H_{AK}(M)$ | Encryption Message with key AK |
| $CU_G$ | Global CU |
| $CU_L$ | Local CU |
| $ID_A$ | Node A's ID |

**Secure 3D Algorithm**

1. ***$EH(PU_{AK}(M)$ from beacon node***
2. ***$EH(PK_A(ID_A| H_{AK}(M)))$ from beacon node***
3. ***$E(PU_{CA}(ID_A, H_{PK(A)}(ID_A|H_{AK}(M))))$ from node S***
4. ***$SEND(REQ(M,H_{AK}(M),CU_G)$ from source node S to local CU in local region)***
5. ***$EH(PU_{AK}(M))$ in Local CU and $IF(H_{AK}(M)==H_{AK}(M))$ THEN go to step 7 else go to step 6***
6. ***ECHO to $CU_L$ "The message is from a malicious node"***
7. ***$D(PK_{CL}(ID_A, H_{PK(A)}(Id_A| H_{AK}(M)))$ in $CU_L$***
8. ***$REQ(PU_A)$ to $CU_G$***
9. ***$REP(PU_A)$ to $CU_L$***
10. ***$EH(PK_A(ID_A|H_{AK}(M)))$ and $IF(H_{PK(A)}(ID_A|H_{AK}(M)) = = H_{PK(A)}(ID_A|H_{AK}(M)))$ THEN it is a malicious node***

## V. ROBUST LOCALIZATION PHASE

Once after the secure localization phase, the location information is sent to the robust phase inorder to validate that even in the presence of malicious beacon nodes, the accuracy should not be compromised. The terminologies that are consumed in the algorithm are defined below[34] and as shown in Fig 2:

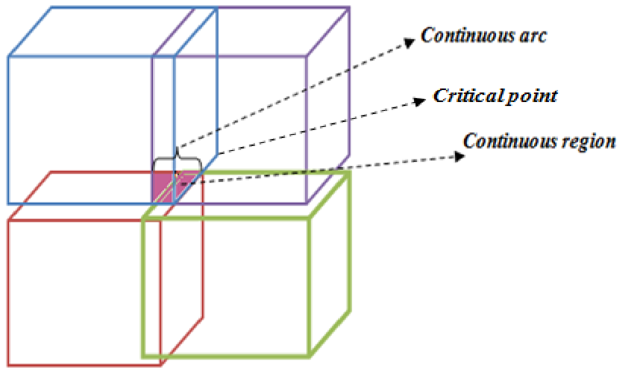



**Fig.2 Terminologies for ROLOC**

Definition 1: A continuous region is one which contains the intersection of all the four regions.

Definition 2: A continuous line is a part of the continuous region

Definition 3: A localization algorithmic rule is within the group of robust localization algorithms if its yield could be a point in a continuous region r specified that r is confined within the crossing of a minimum of k + 4 cubes.

This algorithm attempts to figure the position of the target nearer to the inside (or centroid) of the continuous region of at least $K_{max}$ + 4 cubes. This is since the actual location of the goal is more probable to be close to the focal point of the continuous region than close to the boundary limit. Thus, expecting these continuous region is convex, we first analyze four novel critical points, rather than only one, that lie on the intersection of a huge number of cubes. If ($x_1$, $y_1$, $z_1$), ($x_2$, $y_2$, $z_2$),($x_3$, $y_3$, $z_3$) and ($x_3$, $y_3$, $z_3$) are the directions of these elementary centers, the directions ($x_M$, $y_M$, $z_M$) of the objective location are guessed by computing the centroid of the cube mounted by ($x_1$, $y_1$, $z_1$), ($x_2$, $y_2$, $z_2$),($x_3$, $y_3$, $z_3$) and ($x_3$, $y_3$, $z_3$) as validated as follows:

Centroid of a cube = $\overline{O}$ = ( $x_M$, $y_M$, $z_M$)

$$x_M = \frac{x_1 + x_2 + x_3 + x_4}{4}$$

$$y_M = \frac{y_1 + y_2 + y_3 + y_4}{4}$$

$$z_M = \frac{z_1 + z_2 + z_3 + z_4}{4}$$

***Step 1:*** *Start*
***Step 2:*** *Identify the number of cubes intersecting with each other*
***Step 3:*** *For each cube $C_i$, in the order of lessening number of cubes intersecting with it do*
***Step 4:*** *For each cube $C_i$, $C_{j+1}$, $C_{j+2}$, $C_{j+3}$ ≠$C_i$ in the order of lessening number of lines intersecting with it do*
***Step 5:*** *Calculate the intersection points of the cubes of $C_i$ and $C_j$, $C_i$ and $C_{j+1}$, $C_i$ and $C_{j+2}$ and $C_i$ and $C_{j+3}$*
***Step 6:*** *Pick a point ($x_1$, $y_1$, $z_1$) from the intersection of cube pair $C_i$ and $C_j$ at arbitrary. Choose other three intersection points ($x_2$, $y_2$, $z_2$), ($x_3$, $y_3$, $z_3$) and ($x_3$, $y_3$, $z_3$) from the other three pairs*
***Step 7:*** *Calculate $\overline{O}$ = ($x_M$, $y_M$, $z_M$)*
***Step 8:*** *Sum the number of cubes containing $\overline{O}$*
***Step 9:*** *If there are a minimum of $K_{max}$ + 4 cubes containing $\overline{O}$ then*
***Step 10:*** *Output $\overline{O}$*
***Step 11:*** *Stop*

**Table 1. ROLOC Algorithm**

The above formula is utilized to discover the centroid of each coordinate and that can be utilized as the target location coordinate. On the off chance that the normal point lies in the convergence of $K_{max}$ + 4 cubes, at that point it yields the location of the objective, generally the procedure is continual for another set of critical points. This calculation incorporates the verification of exactness and proficiency of each arrangement of coordinates. The detailed ventures of the calculation are given in detail in Table 1.

## VI. PERFORMANCE ANALYSIS

In this section, we will assess our 3D localization strategy in terms of efficiency and network performance. The proposed strategy has been verified in NS2. The simulation parameters are displayed in Table 1. The underlying network which is made by utilizing 10 sensor nodes is shown in Fig. 6 and step by step it is expanded by 10.

| Parameter | Value |
|---|---|
| Area | 500m X 500 m |
| Propagation Model | Two-ray ground reflection |
| No. of nodes | 10 – 60 |
| MAC | 802.11 |
| Antenna | Omni-directional |
| Simulation time | 10s |
| Placement | Random |
| Packet Size | 500 |
| Pause time | 2s |

**Table 1. Simulation Parameters**

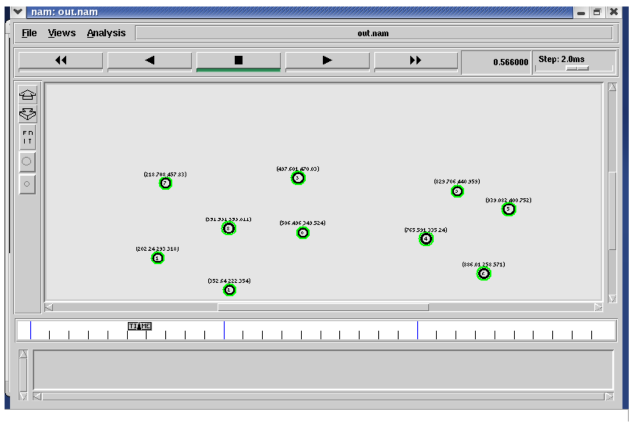



***Fig.5. Creation of nodes in the network***

Every one of the nodes can speak with one another, during communication it additionally checks authentication of nodes, so the localization information transmitted from one node to the next is precise. The malicious beacon nodes begins to develop in the system as the nodes begin moving which is displayed as strong green circles in Fig. 7.

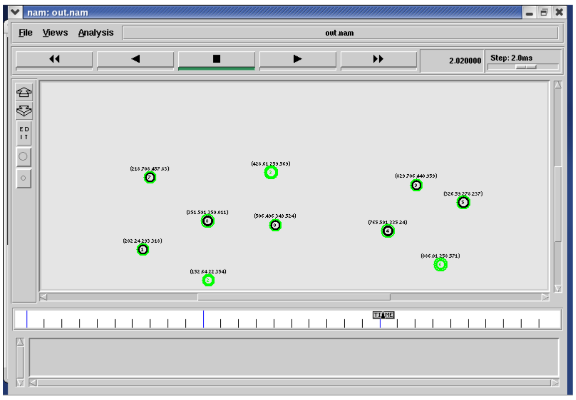



*Fig. 7. Malicious beacon nodes developing in the network which is shown in strong green circles*

The average localization error for Secure 3D, 3D-DV Hop and APIS are presented in Fig. 8. From this graph, it is strong that Secure 3D performs well when compared to the other two methods namely APIS and 3D-DV Hop [21], [22].

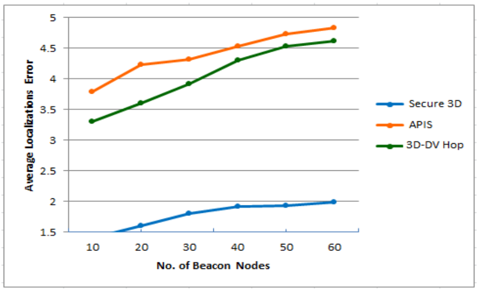



*Fig. 8. Average Localization Error*

When the localization error and the malicious beacon nodes are reduced, there will be a significant growth in the throughput for the Secure 3D algorithm. As shown in Fig. 9 the Secure 3D algorithms' throughput is high when associated to 3D-DV Hop and APIS algorithm, owing to the well-organized algorithm which is implemented in localization process for a 3D location [35], [36].

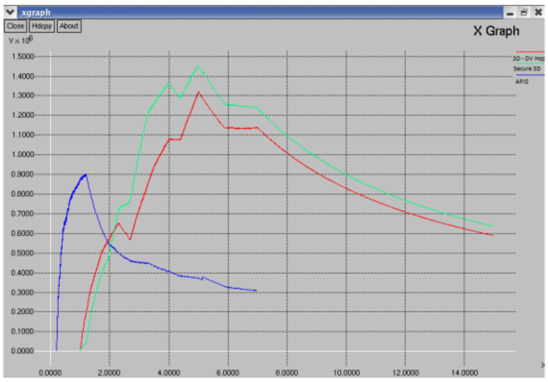



*Fig. 9. Throughput Comparison of Secure 3D with APIS and 3D-DV Hop*

Packet Delivery Ratio is nothing but ratio of no.of packets received to the no. of packets sent, which can be calculated using the formula (5). Packet Delivery Ratio for three different algorithms are analyzed for APIS, 3D-DV Hop and Secure 3D, in which Secure 3D performs better when the no. of nodes get increased.

***PDR = No. of packets received/No .of packets sent***

If the PDR value is more, the approach used is better when compared. In the iteration of time slot, the PDR value is greater than the other two approaches, since the no. of malicious nodes is monitored and controlled from the network [35], [36].

Packet Delivery Ratio is only proportion of no.of packets got to the no. of packets sent, which can be determined utilizing the formula (5). Packet Delivery Ratio for three unique algorithms are observed for APIS, 3D-DV Hop and Secure 3D, in which Secure 3D performs better when the no. of hubs get expanded.

***PDR = No. of packets received/No .of packets sent***

On the off chance that the PDR value is more, the methodology utilized is better when analyzed. In the iteration of time slot, the PDR value is more noteworthy than the other two methodologies, since the no. of malicious node is observed and controlled from the system [35], [36].

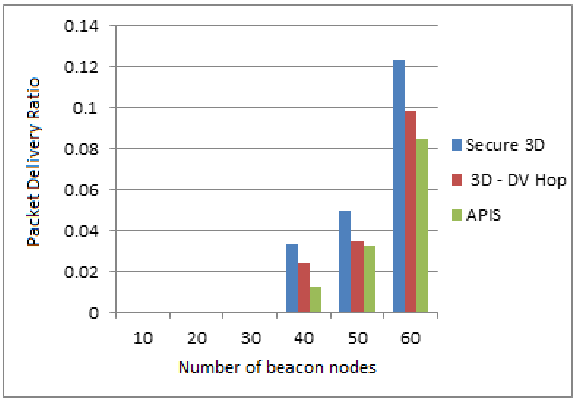
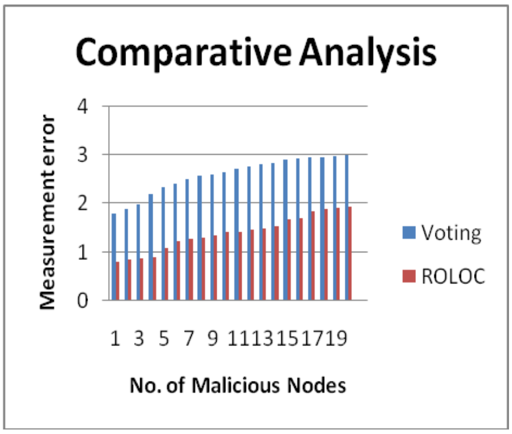



*Fig. 10. Packet Delivery Ratio for Secure 3D, APIS and 3D-DV Hop*




## VII. CONCLUSION

We have investigated the problem of achieving secure and accurate localization even in the presence of malicious beacon nodes, which makes the system robust. The performance of Secure 3D, 3D-DV Hop and APIS algorithms are examined in terms of throughput, localization error and packet delivery ratio. We have shown the accuracy of localization and the measurement errors attained for the existing system and that of the proposed algorithms.

*Retrieval Number: A10241191S19/2019©BEIESP*
*DOI: 10.35940/ijitee.A1024.1191S19*



*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*

Experimental results show that the algorithm performed consistently with different malicious nodes. There are accomplishments in 3D localization algorithms however; 2D limitation calculation is reached out to the 3D space. At present, there are still numerous issues in 3D restriction calculations, for example, high computational complexity, low positioning coverage and depending too much on anchor nodes.

## REFERENCES


[1]T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free Localization Schemes for Large scale Sensor Networks. In MobiCom '03: Proceedings of the 9th annual international conference on Mobile computing and networking, pages 81–95, New York, NY, USA, ACM Press,2003.

[2] R. Want, A. Hopper, V. Falcao, and J. Gibbons, "The Active Badge Location System", ACM Transaction on Information Systems, pages 91–102, Jan 1992.

[3] P. Bahl and V. N. Padmanabhan "Radar: An in-building RF-based User Location and Tracking System", Proc. in IEEE INFOCOM Conference, pages 775–784. IEEE Communications Society, March 2000.

[4]N. Priyantha, A. Chakraborty, and H. Balakrishnan, "The Cricket Location-Support System", In The Sixth Annual International Conference on Mobile Computing and Networking(MOBICOM), pages 32–43. ACM SIGMOBILE, August 2000.

[5] D. Niculescu and B. Nath, "DV based Positioning in Ad hoc Networks", Journal of Telecommunication Systems, 2003.

[6] R. Stoleru and J. A. Stankovic, "Probability grid: A Location Estimation Scheme for Wireless Sensor Networks". In IEEE Sensor and Ad Hoc Communications and Networks, pages 430–438. IEEE Communications Society, October 2004.

[7] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less Low-cost Outdoor Localization for very Small devices," IEEE Personal Communications, vol. 7, no. 5, pp. 28–34, 2000.

[8]T. Eren, D. Goldenberg, W. Whiteley, Y. R. Yang, A. S. Morse, B. Anderson, and P. Belhumeur. "Rigidity, Computation and Randomization of Network Localization". In The IEEE INFOCOM 2004. Proceedings., IEEE Computer and Communications Society, Hong Kong, China, April 2004.

[9] X. Ji and H. Zha. "Sensor Positioning in Wireless Ad-hoc Sensor Networks using Multidimensional Scaling". In Proceedings of IEEE INFOCOM 2004, March 2004.

[10]K. Yedavalli, B. Krishnamachari, S. Ravula, and B. Srinivasan. Ecolocation: "A Sequence based Technique for RF-only Localization in Wireless Sensor Networks". In Proceedings of the Fourth International Conference on Information Processing in Sensor Networks (IPSN '05), Los Angeles, CA, USA, April 2005.

[11]L. Fang, W. Du, and P. Ning. A beacon-less Location Discovery Scheme for Wireless Sensor Networks. Proceedings in the IEEE INFOCOM Conference, IEEE Communications Society, March 2005.

[12] S. Ray, R. Ungrangsi, F. de Pellegrini, A. Trachtenberg, and D. Starobinski. Robust Location Detection in Emergency Sensor Networks. In IEEE INFOCOM Conference Proceedings, Pages 1044–1053, IEEE Communications Society, San Francisco, March 2003.

[13] L. Doherty, L. E. Ghaoui, and K. S. J. Pister. Convex Position Estimation in Wireless Sensor Networks. In IEEE INFOCOM Conference Proceedings, Anchorage, IEEE Communications Society, April 2001.

[14] L. Zhang, X. Zhou, and Q. Cheng, "Landscape-3D: a Robust Localization scheme for Sensor Networks over Complex 3D Terrains," in Proceedings of the 31st Annual IEEE Conference on Local Computer Networks (LCN '06), pp. 239–246, Tampa, Fla, USA, November 2006.

[15] R. Want, A. Hopper, V. Falcao, and J. Gibbons,"The active badge location system", ACM Transaction on Information Systems, pages 91–102, Jan 1992.

[16] G. Tan, H. Jiang, S. Zhang, Z. Yin, and A.-M. Kermarrec, "Connectivity-based and Anchor-free Localization in large-scale 2D/ 3D sensor networks," ACM Transactions on Sensor Networks, vol. 10, no. 1, article 6, 2013.

[17] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-free Localization schemes for Large-scale Sensor Networks," in Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MobiCom '03), pp. 81–95, ACM, September 2003.

[18] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less low-cost outdoor localization for very small devices," IEEE Personal Communications, Vol. 7, No. 5, pp. 28–34, 2000.

[19] Capkun, S. and J.P. Hubaux, "Secure Positioning of Wireless Devices with Application to SensorNetworks", 24th Annual Conference of theIEEE Computer and Communications Societies, 2005.

[20]Capkun, S., J.P. Hubaux and M. Srivastava, "Secure Localization with Hidden and Mobile BaseStations", 25th Annual Conference ofthe IEEE Computer and Communications Societies, 2006.

[21]Delaet, S., P. Mandal, M. Rokicki, S. Tixeuil,"Deterministic Secure Positioning in Wireless SensorNetworks", IEEE International Conferenceon Distributed Computing in Sensor Networks (DCOSS), 2008.

[22] J. Hwang, T. He, and Y. Kim. "Secure Localization with Phantom Node Detection", Ad Hoc Networks, 6(7);1031–1050, Elsevier, 2008.

[23] L. Lazos and R. Poovendran. "SeRLoc: Robust Localization for Wireless Sensor Networks". ACM Transactions on Sensor Networks (TOSN) 1(1):73–100, 2005.

[24] L. Lazos, R. Poovendran, S. Capkun. "ROPE: Robust Position Estimation in Wireless Sensor Networks". 4th Int'l symposium on Information processing in sensor networks, 2005.

[25]D. Liu, P. Ning, and W. Du. "Attack-resistant Location Estimation in Sensor Networks",Proc. of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN '05), pages 99–106. ACM SIGBED and IEEE Signal Processing Society, April 2005.

[26] Nizetic Cosovic I, Jagust I, "Enhanced Weighted Centroid Localization Algorithm for Indoor Environments", International Journal of Electronics and Communication Engineering Vol:8, No:7, 2014.

[27] M. Jadliwala, Sheng Zhong, S. Updhyaya, C.Qiao, "Secure Distance-Based Localization in the Presence of Cheating Beacon Nodes", IEEE Transactions on Mobile Computing (Volume: 9 , Issue: 6 )Page(s): 810 – 823, 2009.

[28] Z. Li, W. Trappe, Y. Zhang, and B. Nath, "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks," in Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05), Los Angeles, USA, 2005.

[29]Prima Kristalina ; Amang Sudarsono ; Mohammad Syafrudin ; Bimantara Ksatria Putra "SCLoc: Secure Localization Platform for Indoor Wireless Sensor Network", Proceedings of the IEEE International Electronics Symposium 2016.

[30]J. T. Chiang, J. J. Haas, J. Choi, and Y.-C. Hu, "Secure Location Verification using Simultaneous Multilateration," IEEE Transactions on Wireless Communications, vol. 11, no. 2, pp. 584–591, February 2012.

[31]M. Fiore, and R. Sadao, "Verification and Inference of Positions in Vehicular Networks through Anonymous beaconing," IEEE Transactions on Mobile Computing, vol. 13, no. 10, pp. 2415–2428, October 2014.

[32]Xingcheng Liu, Senior Member, IEEE, Shaohua Su, Feng Han, Yitong Liu, Zhihong Pan, "A Range-Based Secure Localization Algorithm for Wireless Sensor Networks", IEEE Sensors Journal ( Volume: 19 , Issue: 2), **Page(s):** 785 – 796, 2018.

[33] A.V. Kalpana, S. Rukmani Devi, N.Indira, "Secure 3D Localization in Wireless Sensor Networks", Advances in Natural and Applied Sciences, Vol. No. 10, Issue 13, Page(s):174-182, 2016.

[34] Kalpana A V, Rukmani Devi S, Vinod S, "AROLOC: Advanced & Robust 3D Localization in Wireless Sensor Networks, International Journal of Engineering and Technology, Vol. 7, Issue. 3.12, Pages:357-360, 2018.ISSN: 2227-524X, 2018.

[35] Ming Liu, Yaping Bao, Hanyi Liu, "An Improvement of DV-Hop Algorithm in Wireless SensorNetworks", Journal of Micro Computer Information, 25(4-1): 128-129, 2009.

[36] Jianyun Xu, Aiyan Guo, 2010. "Mobile agent routing algorithm for 3D space based on APIT", Journal onApplication Research of Computers., 27(6): 2246-2253.


## AUTHORS PROFILE

**A.V. Kalpana** is currently an Assistant Professor in Computer Science and Engineering Department R. M. K Engineering College, Chennai, Tamilnadu, India. She obtained her B.E. from University of Madras, Chennai, Tamilnadu, India. She obtained her M. E. from Anna University, Chennai, Tamilnadu, India. Her research interests include Wireless Networks, Mobile Computing and Wireless Sensor Networks.

**Dr. D. Rukmani Devi,** is Professor in the Department of Computer Science and Engineering at R.M.D Engineering College where she has been a faculty member since June 2014. She obtained B.E in Electronics and Communication Engineering in the year 1992 from IRTT, affiliated to Bharthiyar University, M.S in Electronics in the year 1997 at BITS, Pilani and M.E. in VLSI Design in the year 2006 at R. M. K. Engineering College affiliated to Anna University. She has also completed Ph.D under Anna University in the area of VLSI Design. She has 22 years of teaching experience to UG classes and PG classes. She has guided many B.E. and M.E projects. She is guiding 13 Ph.D research scholars in her area. Her areas of interest include VLSI, Embedded, image and video processing and networks. She has published papers in seven international journals. She has delivered many lectures as resource person for many workshops, seminars and faculty development program sponsored by AICTE and Anna University. She has published book on 'VLSI Design' for the benefit of VI semester ECE students. She is a member of many professional societies like ISTE, SCIEI, CSTA, UACEE, ACM and IACSIT.

**N. Indira** is currently working in the Department of Computer Science and Engineering at Panimalar Engineering College, Chennai, Tamilnadu, India. She received her B.E degree in Computer Science and Engineering from Bharathidasan University, Thiruchirapalli, Tamilnadu, India and M.E degree in Computer Science and Engineering from Anna University, Chennai, Tamilnadu, India. She is now working toward the Ph.D degree at Anna University. Her research interests are Cloud Computing, Security systems and Computer Networks.