Secure 3D: Secure and Energy Efficient Localization in 3D Environment using Wireless Sensor Networks

Kalpana A V (kalpanavijay21@gmail.com)
SRM Institute of Science and Technology (Deemed to be University) https://orcid.org/0000-0003-2289-4968

Geetha Vijayaraghavan
Anna University

Malla Sree Jagadeesh
Vellore Institute of Technology - Amaravati Campus: VIT-AP Campus

Shobana J
SRMIST: SRM Institute of Science and Technology (Deemed to be University)

Research Article

Keywords: 3D Localization, WSN, ALE, Secure, Sybil

Posted Date: June 14th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-3049403/v1

Secure 3D: Secure and Energy Efficient Localization in 3D Environment using Wireless Sensor Networks

Kalpana A V[1*], Geetha A V[2†], Jagadeesh M S[3†] and Shobana J[4†]

[1*]Assistant Professor, Department of Data Science and Business Systems, SRM Institute of Science and Technology, Kattankulathur, India.
[2]Department of Information Science and Technology, College of Engineering, Anna University, Guindy, India.
[3*]Department of Computer Applications, National Institute of Technology (NIT), Tiruchirappalli, Bhimavaram, India.
[4*]Assistant Professor, Department of Data Science and Business Systems, SRM Institute of Science and Technology, Kattankulathur, India.

*Corresponding author(s). E-mail(s): kalpanavijay21@gmail.com;
Contributing authors: geethu15@gmail.com;
malla.sree@gmail.com; shobanaj1@srmist.edu.in;
†These authors contributed equally to this work.

Abstract

In recent decades, there has been tremendous technological advancement in innovative communications, consumer electronics, and medical electronics. The hot spot of communication technology offers low cost and low power nodes, which led to Wireless Sensor Network (WSN). In WSN, the location of the node is vital to decide the location of an incident called event detection. Localization technologies have been technologically advanced over the last few years by using technical improvement in digital circuitry to offer location and navigation facilities to its users. Localization is required to further functionalities such as routing, self-organization capability, etc. Many methodologies and algorithms have been proposed to solve the localization problem for

a 2D or 3D region. Although various studies have been conducted in this field, many of the proposed approaches have yielded unsatisfactory results in 3D localization. However, the usual localization techniques, such as the 3D APIT algorithm and the 3D DV-Hop algorithm, have the following drawbacks: 1) Beacon node localization accuracy is low; 2) coverage rate in sparse environments is low. Obtaining higher localization accuracy is a significant challenge due to the target of an attacker, and the overall network gets collapsed by providing malicious information. The presence of malicious nodes degrades the viability of WSN and offers misguiding location information to sensors, and reduces battery life. The location information in a 3D environment should withstand against malicious nodes and also needs to be secure against attacks. In this paper, a novel Secure 3D algorithm is proposed to overcome the problem of malicious beacon nodes in WSN and provides lower Average Localization Error (ALE) by consuming less energy

Keywords: 3D Localization, WSN, ALE, Secure, Sybil

1 Introduction

Recent technological advancements have driven significant changes in innovative communications, consumer electronics, medical electronics, and automotive electronics. The hotspot of communication technology aims for various sensing units that offer low cost and low power, which led to future ultra-large networks. A Wireless Sensor Network (WSN) is a cluster of low-power, light-weight sensor nodes that are comprised of multiple and self-contained to monitor physical characteristics. Sensor nodes in a WSN can detect, gather, and process data from other nodes[1]. According to Fortune Business Insights, the WSN market was worth USD 46.76 billion in 2020 and is predicted to grow to USD 123.93 billion by 2026 [2]. WSNs serves as a link between the physical world and digital activity. Wireless sensor networks (WSNs) have gained a lot of attention in the last decade because of their wide range of applications, including environmental monitoring, object tracking, traffic control, and medical apps. As a result, WSN applications are now highly prized in both the commercial and military sectors.

A gateway enables connectivity to nodes and the rest of the world in a WSN system. Sensor nodes only communicate information to neighbor nodes or base stations when they have determined their own specific area, and data will not be delivered unless the position is known. It is incredibly hard for the base station to determine the node's position, and it is also critical to delivering accurate location information obtained from its neighbor. As a result, nodes must locate themselves[3][4].

Localization is the process of using reference nodes to find a location inside any topographical zone[5][6]. There are different kinds of localization

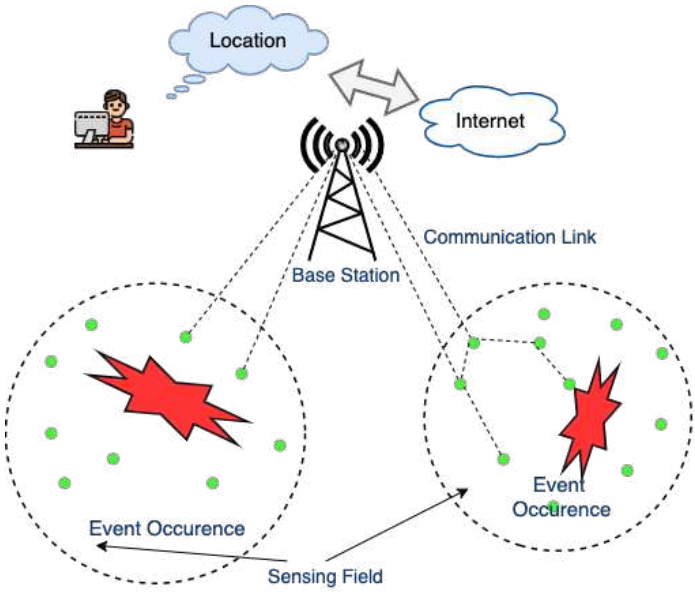

Fig. 1 Need for Localization

techniques: range-based and range-free. The associated nodes in the aforementioned systems can calculate absolute point-to-point distance or angle using time-of-arrival (TOA) [7], time-difference-of-arrival (TDOA) [8], AOA [9], or RSS indicators [10].Beacon nodes are reference nodes that carry out the localization process and are equipped with GPS, whereas non-beacon nodes are nodes that are not equipped with GPS. It is impracticable to integrate all sensor nodes using GPS, increasing overall size and cost. The non-beacon nodes use the trilateration principle to retrieve their position from at least three beacon nodes. Most localization methods employ the 2D region, i.e., the x and y plane. In a 2D plane, the computation technique is straightforward, efficient, and takes less energy to compute the location. In the case of computing the location in a 3D region, there exist fewer localization algorithms, which are simple and efficient. In a 3D region, in addition to the x and y coordinates, a z-coordinate must be added so that the technique can be employed in slopes, mountains, terrains, and hills with high precision.

Most of the applications require the origin of the information that has been sensed. Sensor networks connect many sensing devices, each with limited processing and radio communication capabilities, to detect and communicate physical phenomena and events of interest. The sensor nodes need to know their locations to be ready to specify where a definite event takes place, as shown in Figure 1. Therefore, the localizing of sensors is significantly vital for several sensor network applications. Localization is defined as the location or the geographic coordinates of the sensor nodes. It can either be determined by Global Positioning System (GPS) into it or GPS-free. It is impracticable to equip all nodes with GPS because this would increase the sensor node's

Fig. 2 Basic process of Localization

size and cost. When the nodes are provided with locations, they are termed as beacon nodes; otherwise, they are called non-beacon nodes. To determine the distance, the transmitting and receiving nodes must be synchronized with one another. Three or four beacon nodes are crucial to acquire the position of a non-beacon node by exploiting a trilateration or multi-lateration construct. During the localization process, malicious nodes enter into the networks provide false information, thus affecting the localization accuracy, leading to improper operation of many WSNs. Most of the existing algorithms in WSN are vulnerable to attacks in the untethered environment, so adversaries can easily disrupt the normal functioning of location-dependent WSNs by knowing the flaws of localization algorithms[11][12][13].

The localization problem involves locating all or a subset of sensor nodes in a particular WSN and implementing the solution based on the sensor nodes' data. Usually, special nodes called beacon nodes are used in the process of localization. Figure 2 shows the basic process of localization. The flow diagram for the basic localization depicts the detailed process of node selection, distance estimation, and position computation, which is elucidated in 3. The localization process uses the input data to localize the nodes, such as the location of the beacon nodes, if any, available in the network. Other aspects are investigated in addition to connectivity information with range-free approaches and range or angle between nodes for range-based solutions. The localization method in Figure 3 uses three beacon nodes for a basic localization process.

The paper is structured as follows: Section 2 gives a broad overview of localization and related works. Section 3 discusses the motivation of the work.The proposed work is discussed in Section 4. The performance measures are briefly discussed in Section 5, and the proposed work's evaluation findings are presented in Section 6. Finally, Section 8 provides the concluding remarks.

2 Related Work

Boustani et.a l [14]formulated a new and deterministic approach for securing beacon-based location discovery by employing CDMA(Code Division Multiple Access) based jamming strategy. This approach detects the cheating nodes during localization and removes the nodes. Compared to other secured localization strategies, our methodology performs well in terms of localization accuracy, according to detailed simulations.

A novel and efficient collaborative attack model termed as Collaborative Collusion Attack Mechanism (CCAM) is presented by Jiang et.al [15] for secure localization. In static WSNs, a new approach called Two-Step Format Detection (TSFD) is introduced. With a high detection rate and an improved localization scheme, TSFD is efficient and resilient against malicious nodes in

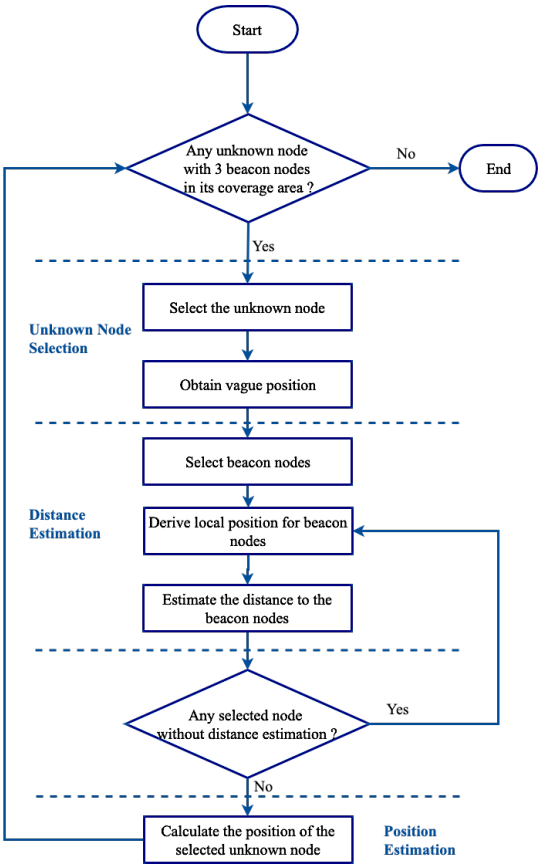

Fig. 3 Flow diagram of localization process

CCAM, delivering significant localization accuracy. The TSFD had reasonable and tolerable communication cost and algorithm complexity.

Han et al. [11] suggested an innovative Two-Step Secure Localization (TSSL) focused on the arrival time difference of localization against so many harmful attacks to locate the position of unknown nodes. The positions, identities, and time of sending information are used to identify malicious nodes. Thereafter, malicious nodes are also segregated via an improved mesh generation method, and the WSN is partitioned into zones using different levels of trust. The TSSL finds malicious nodes efficiently with high localization accuracy in simulation and proved with testbed results.

Mi et al. [16] propose Secure Walking GPS as a secured localization and key exchange method for sensor nodes placed manually in low-human-contact circumstances, where an attacker could interrupt the localization procedure and interfere with the authorized connection. The location information given by the GPS and inertial assistance components on a specific master node is used to gain effective localization and location-based key distribution at the

same time. According to simulation results, it is proved that the mechanism is resistant to DolevYao attacks, GPS-denial attacks, and wormhole attacks. The Secure Walking GPS has good localization and key distribution performance at a low cost and is applied for large-scale WSNs.

Jadliwala et al. [17] proposed a beacon-based localization in a robust environment. A polynomial-time method and two heuristic-based algorithms were proposed as innovative techniques for secure localization. Though in the existence of cheating beacon nodes, these methods provide better localization accuracy; nonetheless, they only work in a 2D environment.

Liu et al. [12] presented two methods for resilient localization in the context of malignant beacon nodes. The very first approach picks out malignant beacon nodes based on abnormalities in multiple beacon signals. In contrast, the second method uses an iteratively rebuilt voting strategy to accept malicious beacon signals.

Fiore et al. [18] introduced a method called Neighbor Position Verification (NPV) that allows every node in the network to check the positioning of communicating neighbors by requiring priori dependable nodes. The proposed scheme is fully distributed, cooperative, and robust against colluding and independent adversaries, even when the adversary has a perfect idea about the neighborhood of the verifying node. The effectiveness of the protocol is degraded only when there is an overwhelming presence of colluding adversaries in the neighborhood of the verifying node. Simulation results prove that the protocol can impede more number of attacks, even in the presence of adversaries.

Chiang et al. [19] suggested a secure multi-lateration approach to verify the prover to be within a given distance from the verifier as well as the location information. The suggested study has delivered the highest detection rate of bogus location claims based on time-of-flight data. It also employs signal strength variance to allow verifiers to detect and evade the distance enlargement attack. The findings of the experiments suggest that by avoiding the distance enlargement assault, the generic collusion attack may also be avoided.

SCLoc is a model of a secure localization node for indoor Wireless Sensor Networks suggested by Prima et al. (SeCure Localization) [20]. In wireless sensor networks, the sensor node is equipped with the AES 128 cryptographic scheme. This approach is used to protect the coordinates and estimated position of beacon nodes that have been determined in unknown nodes. The prototype includes a range-based distance estimate algorithm that is combined with trilateration for position estimation. The Advanced Encryption Standard (AES) and Message Digest 5 (MD5) algorithms are being used to protect the position of the beacon node and unknown node during data exchange in the transmission process. These methods meet the confidentiality and data integrity security requirements simultaneously. Waspmote nodes are used to examine the system, which is linked to a Data Encryption Standard (DES) cryptographic technique incomparable nodes. The analysis results reveal that the security method used to safeguard the position of the beacon node and

unknown node during data exchange in the transmission process met both confidentiality and data integrity security standards.

Liu et al. (2018) [21] evaluated two algorithms, Malicious Node Detection algorithm based on Clustering (MNDC) and Enhanced Malicious Node Detection algorithm based on Clustering (EMDC), to detect malicious beacons and pursue information to defer reliable node location procurement in range-based localization techniques. The anomalous clusters are obtained using the Density-Based Adaptive Spatial Clustering (DBSCAN) technique, which is then evaluated using a Sequential Probability Ratio Test (SPRT). The malicious nodes that jeopardize networks are recognized to limit the number of initial parameters and avoid local outliers being grouped into normal clusters. Furthermore, SPRT provides reliable detection results based on the consistency aspects of two distance measurements. Regarding detection accuracy and effectiveness of the enhanced reference error interval in EMDC, the simulation results reveal that the suggested algorithms surpass alternative methods for malicious beacon detection. The step length between the clusters' core and matching samples is chosen empirically in the existing adaptive clustering technique.

Garg et al. [22] developed a localization approach that is both computationally efficient and secure and can survive localization attacks. The proposed method combines iterative gradient descent with a selective pruning stage that removes conflicting measurements to improve localization accuracy. When the distance between the beacon and non-beacon nodes is calculated using Time-Of-Arrival (TOA) and Time-Difference-Of-Arrival (TDOA) measurements, the algorithm's efficiency is determined. In the case of coordinate attack, simulation results show that the proposed method has localization accuracy compared to existing methods. In contrast, in the case of non-coordinated attacks, there is a gradual improvement in localization accuracy of around 1 m in the presence of Gaussian measurement noise when more than 50 percent of nodes are compromised.

Jha et al. [23] introduced a new method for securing sensor localization that integrates game-theoretic reputations with gradient descent search, resulting in a computationally lightweight solution. Even when there are a lot of fraudulent beacon nodes, the suggested method computes sensor location more correctly and reliably.

Nasir et al. [24] suggested a novel robust localization algorithm based on Multi-Dimensional scaling (MDS) for large-scale three-dimensional (3D) WSNs. This approach has two significant enhancements over the conventional MDS algorithm. Initially, it uses a heuristic approach for distance matrix calculation. Furthermore, it relates the Levenberg-Marquardt (LM) method for absolute map improvement using Received Signal Strength (RSS) measurements to obtain shortest path error reduction between non-neighboring nodes and LM-based refinement of the absolute network map. This algorithm shows better performance than the existing 3D localization algorithms in terms of

network density because it does not depend on the configuration of the beacons. It has been shown that this algorithm is very robust to range error inconsistency and attains stability for range errors greater than 30

3 Motivation

An attacker's objective may be the localization system, which could disrupt the entire operation of a WSN and cause problems with decision-making. Obtaining higher localization accuracy is inevitable, so localization and tracking issues play a vital role in WSNs and may be a target of an attacker to collapse the overall network by providing malicious information. The presence of malicious nodes will essentially damage the viability of WSNs and mislead information to sensors, resulting in sensor battery life being drained. Hence, the location information designed for a 3D environment should withstand malicious nodes and need to be secure against attacks.

Substantial advancement should secure the localization system of WSNs. Most of the existing algorithms in WSN are vulnerable to attacks in the untethered environment, so adversaries can easily disrupt the normal functioning of location-dependent WSNs by knowing the weaknesses of localization algorithms. Usually, the localization algorithms are exposed against security attacks. The proposed Secure 3D algorithm prevents attacks during localization in WSNs for a 3D region.

The rest of this paper is organized as follows. Section IV describes System Design and the proposed Secure 3D algorithm in detail. Section V describes the performance metrics used to evaluate the proposed model. Section VI demonstrates the simulation results and presents a discussion on the Secure 3D algorithm. Summary and conclusion are given in Section VII.

4 Proposed Work

4.1 System Design

3D localization is the method of finding the location of a sensor node deployed in a 3D region like mountains, valleys, hills, and alternative areas. The following issues are faced during 3D localization algorithms implementation when compared to 2D localization algorithms: With 3D localization, an additional number of beacon nodes is necessary, i.e., a total of three beacon nodes is required for 2D localization, but a minimum of 4 beacon nodes is required for 3D localization. The obstacles considerably deteriorate the transmission signals. A tiny difference influences the localization accuracy in the distances detected by the Received Signal Strength Indicator (RSSI). Imagine there are four beacon nodes only within locations defined as A, B, C, and D, respectively, at positions $(x_1, y_1, z_1), (x_2, y_2, z_2), (x_3, y_3, z_3), (x_4, y_4, z_4)$ in Fig. 4 The target position that needs to be identified with the coordinate (x, y, z) is named as K.

The distances between beacon nodes and unknown node are found as,d_{KA}, d_{KB}, d_{KC} and d_{KD}, which is shown in Eq. (1), (2), (3) and (4).

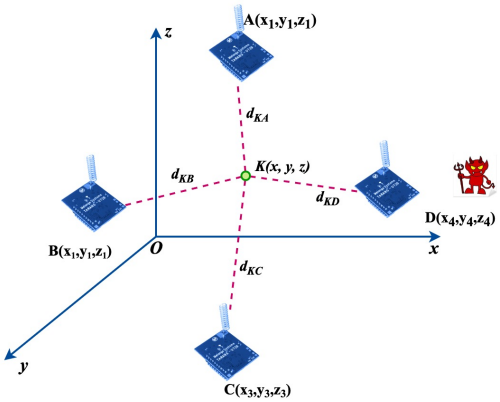

Fig. 4 Distance based localization in the presence of cheating beacon which affects the localization process

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

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

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

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

The coordinate of the unknown node K termed as $(x,\ y,\ z)$ is given in the Eq. (5) and obtained by solving the Eq. (1), (2), (3) and (4).

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = \frac{1}{2}\begin{bmatrix} x_2-x_1 & y_2-y_1 & z_2-z_1 \\ x_3-x_1 & y_3-y_1 & z_3-z_1 \\ x_4-x_1 & y_4-y_1 & z_4-z_1 \end{bmatrix} \cdot \begin{bmatrix} \left(x_2^2-x_1^2\right)+\left(y_2^2-y_1^2\right)+\left(z_2^2-z_1^2\right)+\left(d_{KA}^2-d_{KB}^2\right) \\ \left(x_3^2-x_1^2\right)+\left(y_3^2-y_1^2\right)+\left(z_3^2-z_1^2\right)+\left(d_{KA}^2-d_{KC}^2\right) \\ \left(x_4^2-x_1^2\right)+\left(y_4^2-y_1^2\right)+\left(z_4^2-z_1^2\right)+\left(d_{KA}^2-d_{KD}^2\right) \end{bmatrix} \tag{5}$$

The $(x,\ y,\ z)$ coordinate of the unknown node K as is obtained through Quadrilateration. The malicious beacons falsify the location information, and therefore the localization method fails in location calculation, which is shown in Fig. 5. Nodes $A,\ B$ and C behave normally, however beacon D fakes the location coordinate, resulting in an inaccurate target location estimation referred to as M rather than K

Apart from GPS, each beacon node is equipped with a controlling unit to store the authentication Identity (ID). When a non-beacon node queries for the target location, the beacon node requests the authentication ID. This ID

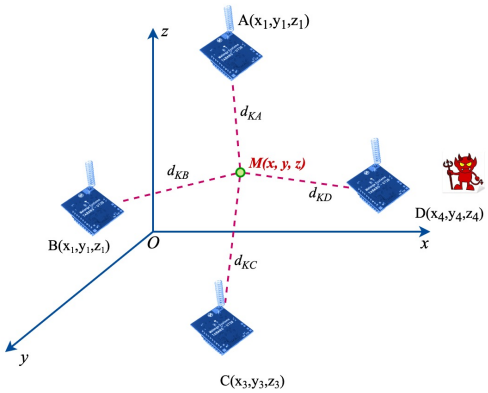

Fig. 5 Localization process after communicating with the malicious node D

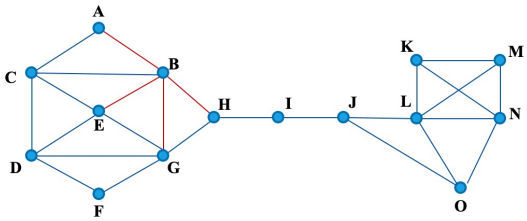

Fig. 6 Closeness Centrality

needs to be registered and must receive the public authentication key before any message transmission occurs.

4.2 Terminologies and Notations

4.2.1 Closeness Centrality (CC)

Closeness Centrality is defined as the closest path between the nodes or simply the shortest path between the nodes, which is represented in Fig. 6. The node B obtains the location information from the closest nodes, namely A, E and G.

4.2.2 Degree of Co-planarity (DCP)

In a 2D region, a set of 3 beacon nodes can be used to locate an unknown node; however, in a 3D region, a total of 4 beacon nodes must be used, which is known as Quadrilateration. The Quadrilateration process is always assumed to be an intersection of 3 spheres, and the target node lies normally in the intersection of the spheres. There can be an error while computing the RSS values and the spherical region and do not have a common intersection region. The node E gets many distance measurements from the available beacon nodes as shown in Fig. 7. Only there exist two possible locations for the un-localized node. The first location is mentioned as E and the other one as E'. If node E

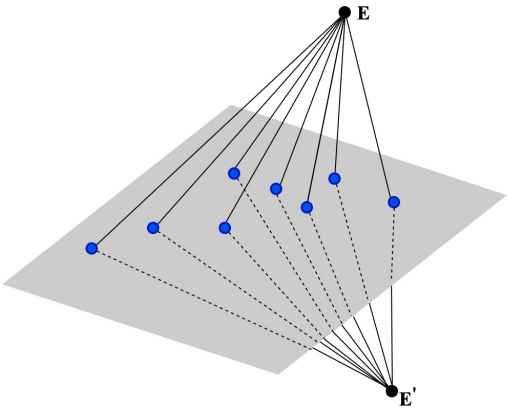

Fig. 7 The non-localized node cannot be localized due to Degree of Coplanarity

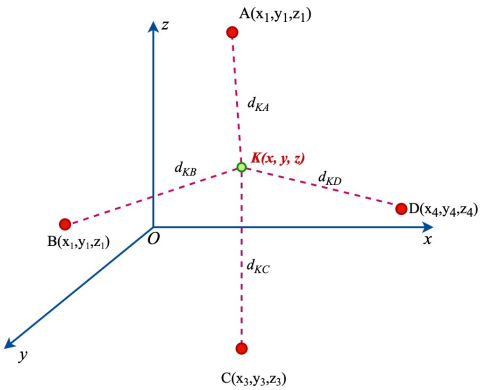

Fig. 8 Degree of Co-planarity (DCP)

does not be coplanar with the beacon node, there is no differentiation between E and E'.

If the four beacon nodes lie in the same plane, it is said to be coplanar. Therefore, in order to find the location of the unknown node, it should be verified that the beacon node should not lie in the same plane. DCP is represented as the degree of four beacon nodes in the 3D space and shown in Fig. 8.

Mitrinovic et al. (1989) expressed the radius ratio of the tetrahedron as shown in Eq. (6).

$$\rho = \frac{216v^2}{\sum_{i=0}^{3} s_i \sqrt{(a+b+c)(a+b-c)(a-b+c)(-a+b+c)}} \tag{6}$$

Degree of Coplanarity (DCP) can be represented as shown in Eq. (7)

Notations	Descriptions
CU_G	Global CU
CU_L	Local CU
ID_x	x Node's ID
PU_x	Public Key of Node x
PK_x	Private Key of Node x
PK_{O-x}	Old Private Key of Node x
PU_{N-x}	New Public Key of Node x
PU_{CU_L}	Public Key of CU_L
PK_{CU_L}	Private Key of CU_L
PK_{O-CU_L}	Old Private Key of CU_L
PU_{N-CU_L}	New Public Key of CU_L
PU_{CU_G}	Public Key of CU_G
PK_{CU_G}	Private Key of CU_G
PK_{O-CU_G}	Old Private Key of CU_G
PU_{N-CU_G}	New Public Key of CU_G

Fig. 9 Initial Message structure

$$DCP = \begin{cases} 0, & coplanar \\ \rho & otherwise \end{cases} \tag{7}$$

where $DCP \in [1, 0]$.

Thus, the best localization unit can be obtained with the maximum DCP value. The notations that are used during message transmissions are shown in Table 3.1

4.2.3 Secure 3D Algorithm

WSN is made up of beacon and non-beacon nodes that are placed in a 3D region. The unknown nodes utilize the location information computed from a set of 4 beacon nodes. Therefore, beacon nodes that give the location information need to be authenticated and they should not be malicious nodes. The beacon nodes are to be deployed with a public key and private key as PUnode and PKnode, respectively. The PUnode and PKnode keys are preinstalled and should be used only once and then ignored. Each data sent out of a beacon node towards a non-beacon node contains the node ID, message ID, and the information to be conveyed as shown in Fig. 9.

The algorithm uses two control units, namely CU_L and CU_G, called Local Control Unit and Global Control Unit.

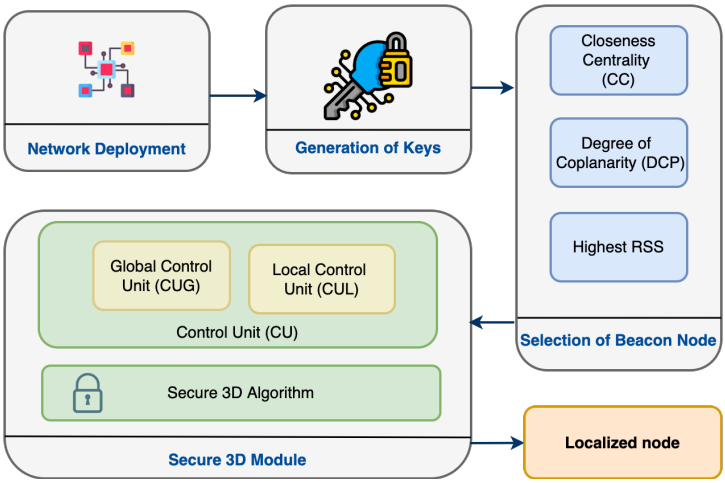

Fig. 10 Architecture of Secure 3D Algorithm

The beacon nodes involved in the localization process must coordinate with the control units as mentioned in the proposed Secure 3D algorithm to have secure communication. The proposed architecture is shown in Fig 10 and algorithm steps as below.

5 Performance Metrics

5.1 Average Localization Time

Average localization time is defined as the time it takes sensor nodes to calculate their location divided by the number of nodes in the network that are accessible as shown in Eq. 5.1.

$$Average\ Localization\ Time\ = \frac{\sum Localization\_Time}{Number\_Of\_Nodes} \tag{8}$$

5.2 Localization Error (LE)

The disparity between real and estimated node coordinates is known as the localization error. Eq.9 shows how to calculate the LE of each target node:

$$Average\ Localization\ Error\ = \sqrt{(X_j - X_i)^2 + (Y_j - Y_i)^2 + (Z_j - Z_i)^2} \tag{9}$$

5.3 Average Location Error (ALE)

The average distance between all sensor nodes' estimated locations(X_j, Y_j, Z_j) and their real locations (X_i, Y_i, Z_i) using Eq. 10.

Algorithm 1 Secure 3D Algorithm

Require: Node with unknown position information of WSN
Ensure: Localized node

1: Generate public and private key pairs for local CU and global CU Public key of $CU_L - PU_{CU_L}$; Private key of $CU_L - PK_{CU_L}$ Public key of $CU_G - PU_{CU_G}$; Private key of $CU_G - PK_{CU_G}$
2: **if** node = beacon node **then**
3: send PU_A and PK_A to CU_L
4: **end if**
5: Encrypt the new public key by the current public key of the local control unit and then by the old private key of the node, PK_{O-Node} (node A acting as beacon node) Node $A \rightarrow CU_L : E[PK_{O-A}, E(PU_{CU_L}, PU_{N-A})]$
6: CU_L uses similar encryption to send the key to Node A CU_L →Node A : $E[PK_{O-CU_L}, E(PU_A, PU_{N-CU_L})]$
7: Select beacon nodes based on DCP and CC
8: Each CU_L send its public key to CU_G and the CU_G will provide its new public key to the four attached CU_L's $CU_L \rightarrow CU_G$: $E[PK_{O-CU_L}, E(PU_{CU_L}, PU_{N-CU_L})]$
9: Each CUG in turn respond to the CUL as follows: $CU_G \rightarrow CU_L$: $E[PK_{O-CU_G}, E(PU_{CU_G}, PU_{N-CU_G})]$
10: **if** the unit is local CU **then**
11: **for** $i = 1, 2, \ldots n$ **do**
12: verify public key and ID details of all the members in the group
13: prepare the message containing the public key, ID and timestamp to node i
14: encrypt the message M_i with the private key of the node A and with the public key of the node A
15: **end for**
16: **end if**

$$Average\ Localization\ Error\ = \sum \frac{\sqrt{(X_j - X_i)^2 + (Y_j - Y_i)^2 + (Z_j - Z_i)^2}}{Number\_of\_nodes} \tag{10}$$

5.4 Detection Rate (DR)

The proportions of detected Sybil nodes to the number of nodes that are Sybil outlined as percentage, which is called as detection rate and is shown in Eq. 11.

$$DR = \frac{Detected\_Sybil\_node}{Total\_Sybil\_nodes} \times 100\% \tag{11}$$

Table 1 Simulation Parameters

Parameter	Value
Area	100m × 100m ×100 m
No. of nodes	10 - 60
MAC	802.11
Propagation Model	Two-ray interference model
Simulation time	10 s
Antenna	Omni-directional
Placement	Random
Pause time	2 s
Packet Size	500

5.5 Localization Error Ratio (LER)

Localization Error Ratio is outlined as the fraction of the average localization error and the communication range of nodes as shown in Eq. 12.

$$LER = \frac{\sum_{i=1}^{n} \sqrt{(x_n - x'_n)^2 + (y_n - y'_n)^2}}{n \times R} \tag{12}$$

5.6 Localized Node Proportion (LNP)

LNP is outlined as the fraction of nodes, which are successfully localized (nSL) to the nodes that are unknown in the network. The degree of positioning coverage is entitled as LNP and shown in Eq. 13.

$$LNP = \frac{n_{SL}}{n} \tag{13}$$

5.7 Bad Node Proportion (BNP)

Bad nodes indicate the nodes where the Localization error is higher than their communication ranges. BNP is the fraction of the number of nodes that are bad ($n_{BadNodes}$) to the nodes that are localized successfully (n_{SL}), as shown in Eq. 14. The measure of the stability of the algorithm is entitled as BNP.

$$BNP = \frac{n_{BadNodes}}{n_{SL}} \tag{14}$$

6 Results and Discussions

The proposed Secure 3D method was tested using NS2, and the simulation parameters are listed in Table 3.2. The efficiency and network performance of the proposed Secure 3D algorithm were evaluated.

The simulation results and analysis of the results for various performance metrics are discussed in this section. To verify the performance of Secure-3D with 3D DV-Hop [25] and 3D APIT [26], several simulations are conducted over NS2 under a 3D environment. The quantity of the node, communication

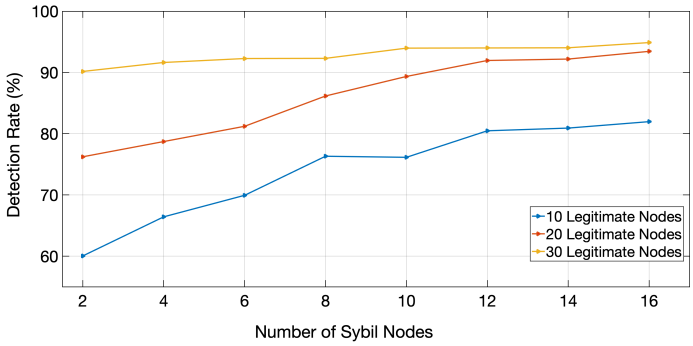

Fig. 11 Detection rate over different number of malicious nodes

range, and beacon proportions also act as additional parameters for evaluating the performance of the algorithm. The simulations run randomly for 30 times for each result, and the average values have been considered as the final result. The network region is assumed to be of fixed size, i.e., 100 m × 100 m × 100 m for all the algorithms. The sensor nodes are randomly spread out in the network region, including 100 beacon and unknown nodes with random location coordinates. The communication radius is set to be the same for all the nodes in the network.

6.1 Effect of Detection Rate Over Different Number of Malicious Nodes

Fig. 11 explains that the detection rate of the Secure 3D algorithm increases when the number of legitimate nodes in the network gets increased. For example, when there are ten legitimate nodes, even though the number of malicious nodes increases, the network's stability does not get affected.

6.2 Effect of Localization Estimation Error

The localization estimation error decreases as the number of beacon nodes in the network grows. Fig. 12 shows that there is an increase in the number of Sybil nodes in the network, the localization error tends to increase and lies between 0.8 and 0.9, whereas the Sybil nodes are removed from the network, there is a slight decline in the localization estimation error and lies between 0.5 and 0.6. Finally, when there are no Sybil nodes in the network, the localization estimation error is comparatively reduced and lies between 0.3 and 0.4.

It has been evident that more Sybil attacks are detected when the number of Sybil attacks increases. The detection rate gets increased when the number of legitimate nodes is higher in the network because the possibility of having a Sybil node decreases with the number of legitimate nodes increasing. Thus the simulation results reveal that 30 legitimate nodes have accomplished more than 90%.

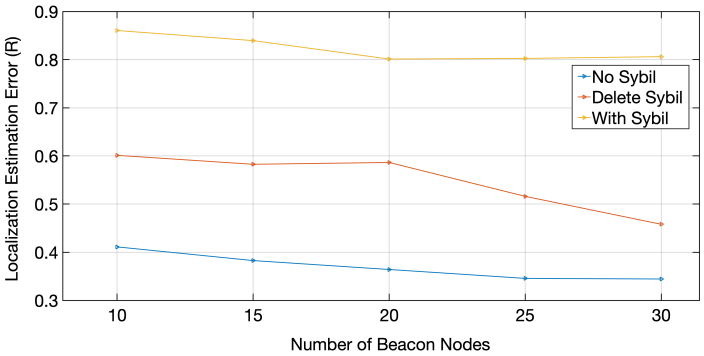

Fig. 12 Localization estimation error rate over different number of beacon nodes

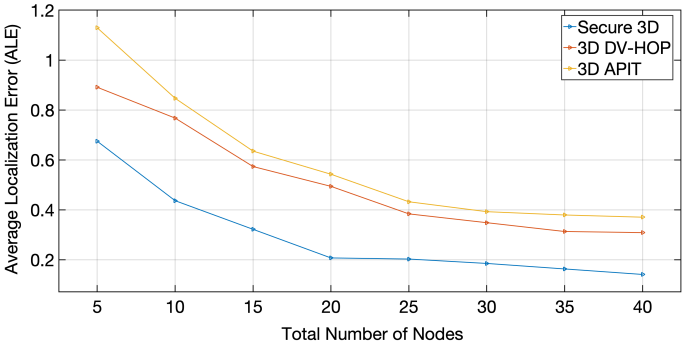

Fig. 13 Communication range vs ALE

6.3 Effect of Communication Range on Average Localization Error

The communication range of sensor nodes also influences each localization algorithm's performance. The impact of communication range on ALE is explored and shown in Fig.13 for different localization techniques by deploying 100 sensor nodes and 25% beacon nodes with a communication range of 15-45m.

The average distance between both the sensor nodes' estimated and actual locations is characterized as the average localization error (ALE). The proposed Secure 3D algorithm, ALE, lies between 3.0 and 6.5, which is minimal compared to the other localization algorithms, namely 3D DV-Hop and 3D APIT.

In general, erroneous distance estimation can cause a position miscomputation which propagates to the localization algorithm and causes a significant localization error for the sensor nodes. A compromised node can send supplementary packets as if it were a different node(s) in a different location, in addition to sending its own packet with the incorrect position(s).

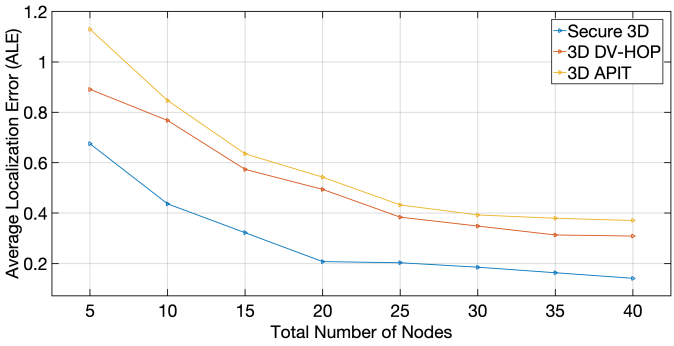

Fig. 14 ALE vs Total number of nodes

It is observed from the simulated results that the communication range of sensor nodes increases, ALE for each algorithm decreases significantly. It has been shown that only minor changes took place in localization errors beyond a 25-30 m communication range. It also shows that the proposed Secure 3D algorithm obtains better localization accuracy when compared with the existing algorithms, namely 3D APIT and 3D DV-Hop, as shown in Table 3.5.

6.4 Effect of Average Localization Error on Node Density

The influence of ALE with different node density is shown in Fig. 14 when a total of 10 to 50 sensor nodes and 25% beacon nodes are deployed in the simulation environment. This is because as the number of sensor nodes increases, the connectivity between nodes also increases, and more location information can be collected from a dense network. It is also noted from the simulation results that the proposed Secure 3D algorithm is recognized more precisely as compared to 3D APIT and 3D DV-Hop.

ALE is defined as the average distance between the estimated location and the actual location of the sensor nodes. As the number of nodes gets increased in the network, ALE gets decreased for all the algorithms. The proposed Secure 3D is compared with the other two algorithms, namely 3D APIT and 3D DV-Hop, the ALE gets decreased for the proposed Secure 3D algorithm.

6.5 Effect of Ratio of Beacon Nodes on Average Localization Error

The effect of the ratio of beacon nodes on ALE is shown in Figure 3.13, using a total of 100 sensor nodes with 5% to 40% beacon nodes in a simulation area of 100 100 100 m3. It has been confirmed that the ratio of beacon nodes increases, ALE for each algorithm decreases. Due to the authentication and encryption of beacon communications and globally, the keys are preloaded, thereby ALE gets reduced as shown in Fig. 15. The proposed Secure 3D algorithm uses a few selection criteria for opting the beacon nodes, which plays a significant

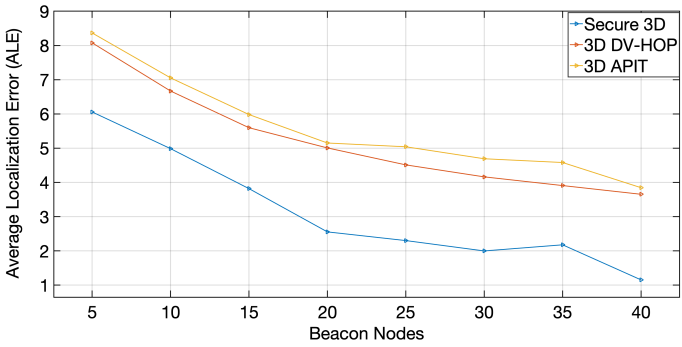

Fig. 15 ALE vs Beacon Nodes

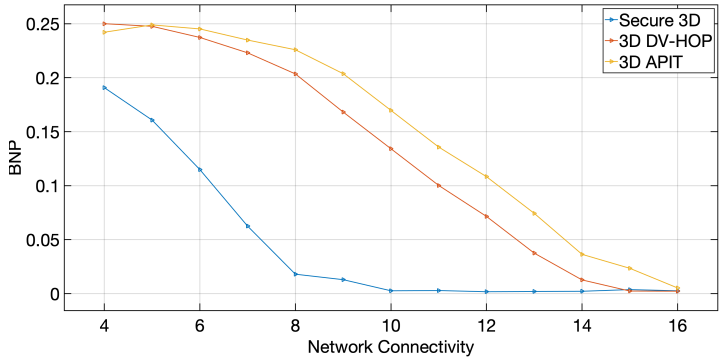

Fig. 16 LNP vs Network Connectivity

role in reducing the ALE. In the case of the other two algorithms, namely 3D APIT and 3D DV-Hop, no cryptographic technique is imposed in the network, thereby increasing the localization estimation error.

6.6 Effect of Bad Node Proportion

When the communication range is increased, the BNP of the algorithm tends to show a gradual decrease. Here, in the proposed Secure 3D algorithm, the number of bad nodes can be easily identified by signal strength and through cryptographic techniques. The nodes that are closer will have a higher signal strength than the node that is far, and this factor is utilized in the proposed Secure 3D algorithm, and cryptographic techniques make the system more secure when compared to 3D DV-Hop and 3D APIT.

In the proposed Secure 3D algorithm, the network connectivity comes up to 10, there does not exist any bad node in the localization and hence stable than the 3D APIT and 3D DV-Hop as shown in Fig. 16.

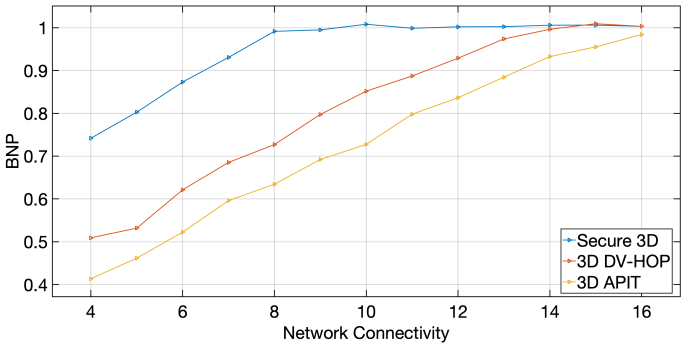

Fig. 17 BNP vs Network Connectivity

6.7 Effect of Localized Node Proportion

The number of successfully located nodes divided by the number of target nodes is known as the Localized Node Proportion (LNP). The fraction of target nodes that are effectively localized is represented by LNP, which is a measure of positioning coverage.

When the communication range is increased, the LNP of the algorithm tends to show a gradual increase since the detection rate of the Secure 3D algorithm is more when compared to 3D APIT and 3D DV-Hop algorithms. Typically, the compromised node affects position computation directly by advertising incorrect known positions, thereby affecting the nodes getting localized. In the other two algorithms, namely 3D DV-Hop and 3D APIT, security is not a primary concern, and the main focus is on position computation in a 3D environment. Therefore, the proportion of localized nodes tends to be higher when compared to 3D DV-Hop and 3D APIT, as shown in Fig. 17.

6.8 Effect of Localization Time

The localization time is defined as the time required for all the sensor nodes to compute their locations. The effect of localization time for the proposed Secure 3D algorithm is shown in Fig. 18.

The proposed Secure 3D algorithm computes its position using the multilateration technique, so by iterative multilateration technique, the nodes in the network get easily localized, making the localization process simpler and more efficient. In the case of 3D DV-Hop, the time required to compute each hop tends to increase, and then it uses the information in the multilateration process, which increases the overall time. In the 3D APIT algorithm, computing the nodes inside/outside the tetrahedron is a time-consuming process, then the multilateration process is done, making the localization process cumbersome.

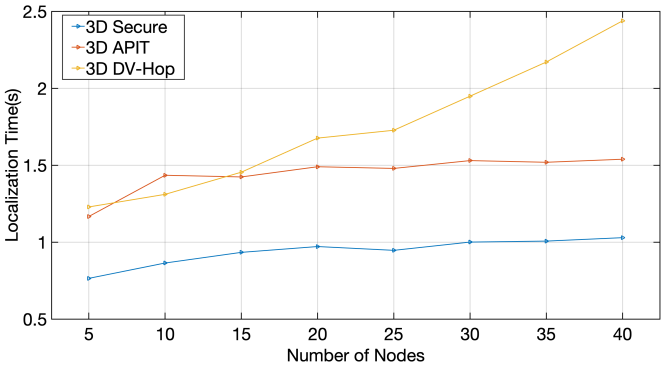

Fig. 18 Localization Time(s) vs Number of nodes

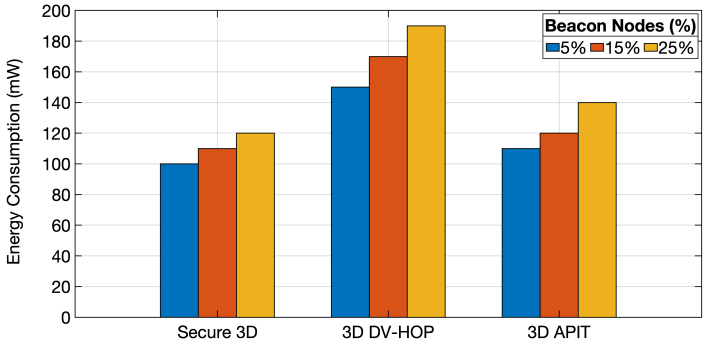

Fig. 19 Energy Consumption vs Beacon Nodes

6.9 Effect of Energy Consumption

Fig. 19 shows the effects of energy consumed by nodes in the network. The energy consumption occurs due to the multi-hop nature of the network, where the unreachable target nodes will be made reachable by communicating with the midway nodes between the source and destination nodes. Furthermore, the unknown node must cooperate with the beacons by broadcasting its location to its neighbors in order to finish the localization process. In the case of 3D APIT, the maximum energy consumption is inquired while selecting the paired beacon nodes in each tetrahedron and for selecting the tetrahedron from the number of K beacon nodes. If paired beacon nodes are found in one tetrahedron, then delete them from the neighbor list of the sensor node. Then, in the next step, the whole communication needs to happen for each sensor node which drains the energy of each sensor node.

The energy consumption of the 3D DV-Hop is higher because the first step degrades the localization process by making the hop count aberrant; as a result, the second step, which is a frequency hopping challenge, is also harmed, and the complete localization scheme is harmed.

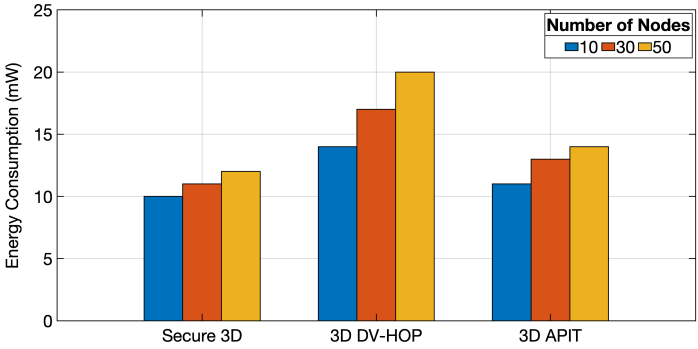

Fig. 20 Energy Consumption vs Number of nodes

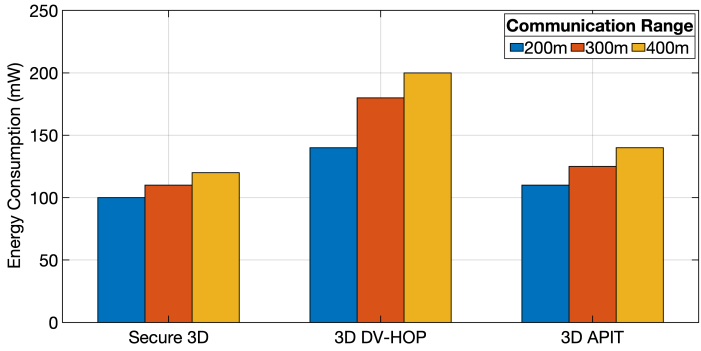

Fig. 21 Energy Consumption vs Communication Range

In the proposed Secure 3D algorithm, due to efficient cryptographic techniques, there is a slight decrease in the energy consumption of beacon nodes in the network, and it is tested for 5%, 10% and 15% beacon nodes. It is observed that when 5% nodes are used, the Secure 3D requires 100mW of energy to transmit the data from one node to the other because of the lesser computation made for validation of data that has been transmitted from one node to the other. It has also been observed that when 10% and 15% of nodes are used, the proposed Secure 3D algorithm consumes lesser energy than the existing 3D DV-Hop and 3D APIT algorithms.

Fig. 20 depicts the total number of nodes that impact the energy consumption in the network in the case of 10, 30, and 50 nodes with different algorithms. When the number of nodes increases, the energy consumption will be more. Due to the simple localization process utilized in the proposed Secure 3D algorithm, the energy consumption is less than 3D DV-Hop and 3D APIT. When a network uses 3D APIT and 3D DV-Hop, the number of transmitted packets increases as the number of nodes in the network grows.

The amount of packets transmitted with nodes in the network for 3D APIT is fewer than for 3D DV-Hop because 3D DV-Hop requires more dispersion of

information from the beacon to the neighbor node during its broadcast phase. The 3D DV-Hop requires more energy because the nodes closest to the beacons must transfer the packet back to the beacons during the first broadcasting phase and the second rectification phase. Due to the random topology, each node transfers the packet to the next node by computing the shortest path, which is time-consuming. As for the Secure 3D method, the number of packets transmitted and received by the node is directly proportional with the density of the node, and it is the lowest among 3D APIT and 3D DV-Hop algorithms, which in turn reduces the overall consumption of the network.

7 Conclusion

In a real-time environment, the location of the node is very likely to be static or dynamic. Many well-known 3D localization algorithms analyze the localization algorithm with different ratios of beacon nodes and communication ranges. The algorithm concentrates on security and accuracy. The performance of the real-time network is greatly affected by the presence of malicious nodes. Therefore, a secure localization algorithm called Secure 3D is proposed to send the localization information securely in a 3D region. The proposed Secure 3D algorithm performs very well when compared to 3D DV-Hop and 3D APIT in terms of Average Localization Error (ALE), Bad Node Proportion (BNP), and Localized Node Proportion (LNP) and is also energy efficient. The proposed Secure 3D algorithm provides the ALE in the range of 3.0 and 6.5, BNP less than 0.2, and LNP greater than 0.8 by consuming 100-130mW of energy.

Funding

The authors have no relevant funding for this research work to disclose.

Conflicts of interest

The author(s) declare(s) that there is no conflict of interest.

Availability of data and material

The data is not available, since it will be used for extension of the work.

Code availability

Codes and results will be used for extension of the work, cannot be made available.

References

[1] Liu, X., Li, W., Han, F., Xie, Y.: An optimization scheme of enhanced adaptive dynamic energy consumption based on joint network-channel coding in WSNs. IEEE Sensors Journal **17**(18), 6119–6128 (2017)

[2] Wireless Sensors Network Market | 2021 - 26 | Industry Share, Size, Growth - Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/wireless-sensor-networks-market Accessed 2022-01-17

[3] Ou, C.-H.: A localization scheme for wireless sensor networks using mobile anchors with directional antennas. IEEE Sensors Journal **11**(7), 1607–1616 (2011)

[4] Kwong, K.H., Wu, T.T., Goh, H.G., Sasloglou, K., Stephen, B., Glover, I., Shen, C., Du, W., Michie, C., Andonovic, I.: Implementation of herd management systems with wireless sensor networks. IET wireless sensor systems **1**(2), 55–65 (2011)

[5] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. IEEE Communications magazine **40**(8), 102–114 (2002)

[6] Ihler, A.T., Fisher, J.W., Moses, R.L., Willsky, A.S.: Nonparametric belief propagation for self-localization of sensor networks. IEEE Journal on Selected Areas in Communications **23**(4), 809–819 (2005). https://doi.org/10.1109/JSAC.2005.843548

[7] Yu, K., Guo, Y.J., Hedley, M.: ToA-based distributed localisation with unknown internal delays and clock frequency offsets in wireless sensor networks. IET Signal Processing **3**(2), 106–118 (2009)

[8] Xiao, J., Ren, L., Tan, J.: Research of TDOA Based Self-localization Approach in Wireless Sensor Network. In: 2006 IEEE/RSJ International Conference on Intelligent Robots and Systems, pp. 2035–2040 (2006). https://doi.org/10.1109/IROS.2006.282415

[9] Niculescu, D., Nath, B.: Ad hoc positioning system (APS) using AOA. In: IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428), vol. 3, pp. 1734–17433 (2003). https://doi.org/10.1109/INFCOM.2003.1209196

[10] Hood, B.N., Barooah, P.: Estimating DoA From Radio-Frequency RSSI Measurements Using an Actuated Reflector. IEEE Sensors Journal **11**(2), 413–417 (2011). https://doi.org/10.1109/JSEN.2010.2070872

[11] Han, G., Jiang, J., Shu, L., Guizani, M., Nishio, S.: A two-step secure

localization for wireless sensor networks. The Computer Journal **56**(10), 1154–1166 (2013)

[12] Liu, D., Ning, P., Liu, A., Wang, C., Du, W.K.: Attack-resistant location estimation in wireless sensor networks. ACM Transactions on Information and System Security (TISSEC) **11**(4), 1–39 (2008)

[13] Liu, D., Ning, P., Liu, A., Wang, C., Du, W.K.: Attack-resistant location estimation in wireless sensor networks. ACM Trans. Inf. Syst. Secur. **11**(4), 1–39 (2008). https://doi.org/10.1145/1380564.1380570

[14] V, G.A.: Neuromuscular blocking drugs in man. In: Zaimis, E. (ed.) Neuromuscular Junction. Handbook of Experimental Pharmacology, vol. 42, pp. 593–660. Springer, Heidelberg (1976)

[15] Jiang, J., Han, G., Shu, L., Chao, H.-C., Nishio, S.: A novel secure localization scheme against collaborative collusion in wireless sensor networks. In: 2011 7th International Wireless Communications and Mobile Computing Conference, pp. 308–313 (2011). https://doi.org/10.1109/IWCMC.2011.5982551

[16] Mi, Q., Stankovic, J.A., Stoleru, R.: Secure walking gps: A secure localization and key distribution scheme for wireless sensor networks. In: Proceedings of the Third ACM Conference on Wireless Network Security, pp. 163–168 (2010)

[17] Jadliwala, M., Zhong, S., Upadhyaya, S.J., Qiao, C., Hubaux, J.-P.: Secure distance-based localization in the presence of cheating beacon nodes. IEEE Transactions on mobile computing **9**(6), 810–823 (2010)

[18] Fiore, M., Casetti, C.E., Chiasserini, C.-F., Papadimitratos, P.: Discovery and verification of neighbor positions in mobile ad hoc networks. IEEE Transactions on Mobile Computing **12**(2), 289–303 (2011)

[19] Chiang, J.T., Haas, J.J., Choi, J., Hu, Y.-C.: Secure location verification using simultaneous multilateration. IEEE Transactions on Wireless Communications **11**(2), 584–591 (2011)

[20] Kristalina, P., Sudarsono, A., Syafrudin, M., Putra, B.K.: SCLoc: secure localization platform for Indoor wireless sensor network. In: 2016 International Electronics Symposium (IES), pp. 420–425 (2016). IEEE

[21] Liu, X., Su, S., Han, F., Liu, Y., Pan, Z.: A range-based secure localization algorithm for wireless sensor networks. IEEE Sensors Journal **19**(2), 785–796 (2018)

[22] Garg, R., Varna, A.L., Wu, M.: An efficient gradient descent approach to

secure localization in resource constrained wireless sensor networks. IEEE Transactions on Information Forensics and Security **7**(2), 717–730 (2012)

[23] Jha, S., Tripakis, S., Seshia, S.A., Chatterjee, K.: Game theoretic secure localization in wireless sensor networks. In: 2014 International Conference on the Internet of Things (IoT), pp. 85–90 (2014). IEEE

[24] Saeed, N., Stojkoska, B.R.: Robust localisation algorithm for large scale 3D wireless sensor networks. International Journal of Ad Hoc and Ubiquitous Computing **23**(1-2), 82–91 (2016)

[25] Cai, X., Wang, P., Du, L., Cui, Z., Zhang, W., Chen, J.: Multi-Objective Three-Dimensional DV-Hop Localization Algorithm With NSGA-II. IEEE Sensors Journal **19**(21), 10003–10015 (2019). https://doi.org/10.1109/JSEN.2019.2927733

[26] Shu, J., Yan, C., Liu, L.-l.: Improved three-dimensional localization algorithm based on volume-test scan for wireless sensor networks. The Journal of China Universities of Posts and Telecommunications **19**(2), 1–6 (2012). https://doi.org/10.1016/S1005-8885(11)60452-4

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- Biography.pdf