ADVANCES in NATURAL and APPLIED SCIENCES

ISSN: 1995-0772
EISSN: 1998-1090
2016 September 10(13): pages 174-182

Published BY **AENSI Publication**
http://www.aensiweb.com/ANAS
Open Access Journal

Secure 3-D Localization in Wireless Sensor Networks

[1]Kalpana A.V and [2]Dr. Rukmani Devi S

[1]Assistant Professor)Department of Computer Science &Engineering, Velammal Institute of Technology, Chennai, India.
[2]Professor)Department of Electronics&Communication Engineering, R.M.D. Engineering College, Chennai, India.

Received 7 June 2016; Accepted 12 September 2016; Available 20 September 2016

Address For Correspondence:
A.V. Kalpana, Department of Computer Science &Engineering, Velammal Institute of Technology, Chennai, India.
Email:kalpanavijay21@gmail.com

Copyright © 2016 by authors and American-Eurasian Network for Scientific Information **(AENSI Publication).**
This work is licensed under the Creative Commons Attribution International License (CC BY).
http://creativecommons.org/licenses/by/4.0/

Open Access

ABSTRACT

Background: The essential capacity of a sensor system is to gather and forward information to destination. It is vital to think about the area of gathered information, which is used to sort data that can be acquired utilizing confinement strategy as a part of Wireless Sensor Networks (WSNs). **Objective:** Localization is a standout amongst the most imperative advancements since it assumes a basic part in numerous applications, e.g., target tracking. In the event that the clients can't acquire the exact area data, the related applications can't be proficient. **Result:**The fundamental thought in most confinement strategies is that some deployed nodes (milestones) with known positions (e.g., GPS-equipped nodes) transmit signals with their coordinates in order to help other nodes to localize themselves. This paper focuses mainly on the algorithm that has been proposed to securely determine the location of a sensor node. By "secure", we mean that malicious nodes should not easily affect the accuracy of the localized sensors. **Conclusion:**In earlier research papers were proposed based on 2-D localization, but in this paper in addition to security and robustness, accurate localization can be determined for 3-D regions by using an efficient localization algorithm. The performance of the algorithm is analyzed by comparing it with other two 3-D approaches used for localization.

KEYWORDS: localization, secure, robust, 3-D, malicious nodes, cheating nodes, range-based, range-free

INTRODUCTION

WSN has turned into a rising field in innovative work because of the substantial number of utilizations thatcan turn out to be essentially helpful from such frameworks and has prompted the improvement of savvy not-reusable, small, modest and independent battery fueled computers, likewise called sensor nodes. These sensor nodes can acknowledge contribution from a connected sensor and process the information accumulated from the sensor nodes. After that the process information remotely transmits the outcomes to transit network.Wireless Sensor Network (WSN) is a collection of light weight and low power sensor nodes which are spatially distributed and self-sufficient to monitor physical parameters. A WSN system consists of a gateway which provides wireless connectivity to the nodes and to the world. Its applications are utilized as part of military and battlefield surveillance, habitat monitoring, health care applications and environmental monitoring, etc. Sensor nodes send the information to neighbor node or base station, yet before it they have to know their own particular area, on the grounds that the information have no importance without location information [23][24]. It is very difficult for the base station to calculate the node's position, since they are large, so it is necessary to send the location information which is collected from its neighbor and it should provide accurate information also. Therefore, nodes need to localize themselves.

In any topographical region with the assistance of reference nodes, the definite location can be found with the help of reference nodes which is termed as "Localization".Localization techniques can be classified as range-based and range-free approach.Thereference nodes which carry out the localization process are called as

beacons, that are equipped with GPS and the nodes which are not equipped with GPS are called as non-beacon nodes, since it is highly impractical to equip all the nodes with GPS, which increases the sensor node size factor, but sensor nodes need to be small. Each sensor node must be furnished with special hardware to accomplish localization. In order to calculate the distance, the transmitted and received nodes need to be synchronized. The non-beacon nodes get their location from minimum 3 beacon nodes by using trilateration concept [25].

Most of the localization algorithm works based on the 2-dimensional plane i.e., x and y plane. In a 2-dimensional plane, the computation process is quite simple and efficient and requires less energy to compute when considering a 3-dimensional location. When we confront an unforeseen situation such as hurricane, earthquake or similar disasters, wireless sensor nodes turn to be valuable one in search and rescue operations.

Wireless sensor networks can help in directing the search and rescue operation and give look in opportune way. The localization algorithms are used to find the position of non-beacon nodes and thus act as a new reference nodes for the non-localized beacon nodes. In a 3-dimensional plane, we need to add an extra plane apart from x and y coordinate, which is called as z-coordinate. It can be used in slopes, mountains, terrains, hills to provide a good accuracy. In any case, when mapping these evaluated positions to this present reality a blunder can happen, on the grounds that it comprises of every one of the three planes. Any edge between the reference plane and the ground where it present result might be an error during mapping. By utilizing a localization system for 3D this issue is dispensed completely.

Due to their key part in WSNs, localization system can be a target of an attacker that could trade off the whole working of a WSN and lead to mistaken military arrangements and choice making, among other issues. The presence of malicious nodes can essentially degrade the viability of WSNs. For instance, an attacker can prompt the computation of false positions and distances. An attacker can give wrong directing ways to sensors in order to deplete their battery life [13]. It might prompt reporting false data on the geography of the phenomenon examined by sensors. Substantial advancement has been made to secure the localization system of WSNs[11, 12, 5, 6, 7, 10]. In this article we demonstrate how current localization algorithms are defenseless against these security attacks. Likewise, we show our algorithm to forestall such attacks or make them hard to perform in WSNs.

Background and Related Works:

A beacon node sends their localization information to non-beacon nodes that keep track of all received beacons. Utilizing the aggregate information, straightforward centroid model is applied to estimate the non-beacon nodes [14].DV- Hop expects that a system consisting of unique sensing nodes and beacon nodes [8]. Rather than going for the single hop broadcast, anchors flood their locations all over the network. As the message spreads over every hop, a counter is incremented. The non-beacon nodes calculate their location based on the received beacon locations, average distance per hop, hop count from the corresponding anchor;

In a large-scale network, Multi-Dimensional Scaling (MDS) just uses the network data; This procedure has three stages: it roughly evaluate the distance between all the sensor pairs. Apply the MDS to determine the locations fitted generally to the evaluated distances. Then finally upgrade by taking the known sensor node locations.

The APIT [9] is the one of the spine system utilized by the greater part of the range-free approach. In this approach the entire sensor system environment is partitioned into triangles. The triangles are framed by picking the combinations of the anchor nodes. If the sensor node is within the area bounded by the triangular region formed by the three sensor nodes, then there is a possibility of presence of sensor node.

To complete the process of localization, the algorithm uses minimum number of trusted nodes [4]. When the number of liars is below a certain threshold value, the algorithm works purely for a given number of neighbors, which is also determined. In UWASN, an acoustic multilateration ranging technique is used to determine the location [3]. In a Sybil attack, the WSN is subverted by malicious nodes which construct an extensive number of fake personalities keeping in mind the end goal to upset the entire network [2]. In case of dispute, the scheme used in VANET provides conditional anonymity and preserves privacy in both beacons and ERMs [1].

Liu et al. [17] propose a technique for secure localization by avoiding malicious data. This method is known as attack resistant Minimum Mean Square Estimation (MMSE) takes into consideration that malicious location information given by malicious nodes are usually incorrect with the correct ones. Lazos et al. [16] propose a range independent localization technique by using sectored antennas called SeRLoc, which does not require any correspondence among nodes. Be that as it may, SeRLoc depends on the suspicion that wireless medium jamming is not possible. Unlike SeRLoc, ROPE (Robust Position Estimation) [18] provides robust localization computation and verification, but there is a possibility of wireless jamming.

Moore et. Al [15] defined the two-dimensional localization problem in wireless sensor network, which is a beacon less, distributed, linear-time algorithm for localization. But the localization results consist of large measurement errors.Jadliwala et.al [19] defined three algorithms for secure localization framework. These algorithms provide good accuracy but it works only in a 2-dimensional region.

The rest of this article is arranged as follows. In the next section we quickly present an overview and meaning of a secure localization framework. We recognize the vulnerabilities to which limitation frameworks are uncovered, and depict methods used to dispense with these vulnerabilities. At last, we display our decisions and future enhancements for secure localization frameworks for a 3D location.

3-D Localization:

Localization: It is the process of finding the localization in a 3- D space such as mountains, valleys, hills and other areas.

Contrasted to two-dimensional localization algorithms , three-dimensional localization algorithms have the following issues:

(i) In 3-D localization more number of beacon nodes are required, ie., for 3-D minimum four beacon nodes whereas for 2-D localization minimum three beacon nodes are required to find the unknown node. It needs to expand the node density as well as make the calculation more complex.

(ii) The transmission signals are greatly affected by the terrain obstacles. The effect of the obstacles can't be overlooked. There is a slight deviation in the distances measured by RSSI, which will influence the localization accuracy.

The localization mode is shown in [20] needs no less than four anchor nodes to decide the location of unknown nodes. It can be also seen that four anchor nodes ought not be in the same keeping in mind the end goal to guarantee the localization.

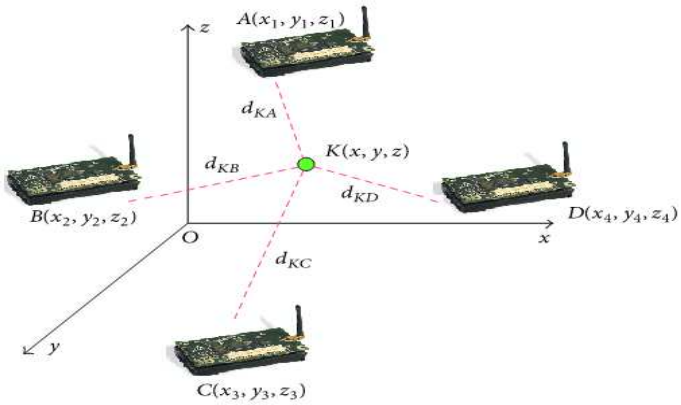

Fig. 2: Distance based localization

Assume there are four beacon nodes in the positions namely A, B, C and D located 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 shown in Fig.1.K is the target position which needs to be found with the coordinate (x,y,z).

The distances between beacon nodes and unknown node are d_{KA}, d_{KB}, d_{KC} andd_{KD}.Equation (1) is obtained according to the distance between the nodes:

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

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

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

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

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

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

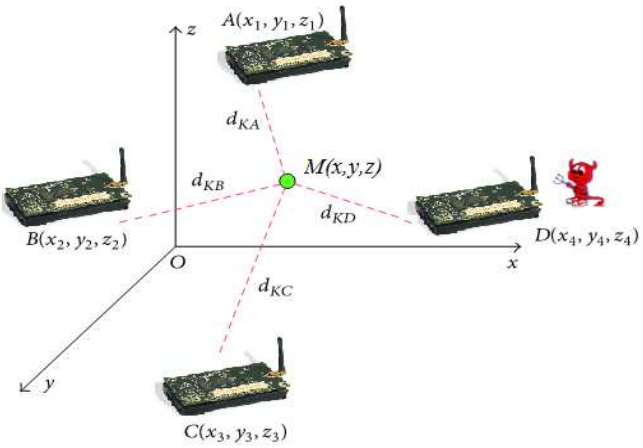

Fig. 3: Distance based localization in the presence of malicious beacon which affects the localization process

The unknown node K is obtained through quadrilateration, which is not astonishing thatbeacon-based methods perform well when all the beacon nodes do not lie. Be that as it may, their accuracy suffers impressively in the presence of malicious or cheating beacon nodes.

Beacons can fake by broadcasting their own locations erroneously or by controlling the distance estimation process, thus affecting the localization process which is depicted in Fig 3. In this figure, we can say that A, B and C behave properly, whereas beacon D fake the location coordinate and thus lead to incorrect estimation of the target location called M instead of K.

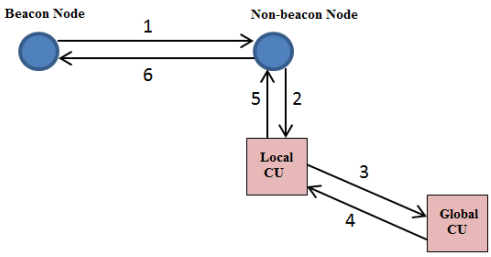

Fig. 4: Authentication process

The beacon or anchor nodes are equipped with a controlling unit, which stores authentication ids apart from GPS. Whenever the non-beacon node requests for target location, the beacon or anchor node asks for the authentication id. This id should be registered in a group and receive its public authentication key (AK) before any message transmission.

For signing a message, thenode uses groupauthentication key and encryption function and sends it along with original message to othernodes. Consequently it is not compulsory for every part to have other individuals' private data, for example,their identity and public key for authenticating them. Receiverscheck a member's identity by signature verification. It is achieved by reconfirmation ofencryption function with authentication key to the obtained message and contrasting the outcome tothe signature.

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

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

Step 2: Local CU don't have a private key of CU_L, so local CU cannot decryptthe message. It sends a request to CU_L to decryptthe ID of beacon. In this step, it decrypts only the ID of beacon.

Step 3: Since CU_L don't have private key of beacon node A, so CU_Lcannot decrypt.H_{PK}(ID(Beacon),H_{AK}(M)) , therefore send a request private key of node A to the CU_G.

Step 4: CU_G reply private key of beacon node A to CU_L and CU_Lattained by reconfirmation ofencryption function with key of vehicle A to the ($ID_A|H_{AK}$(M)) and comparing the result to theH_{PK}($ID_A|H_{AK}$(M)). Also, CU_Lcan detect the Sybil attack, if result of this comparison isdifferent.

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

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

The notations used during a message transmissionare shown below:

NOTATIONS	DESCRIPTION
REQ	Request from Beacon node
REP	Reply from Local CU/Global CU
E(…)	Encryption of message
EH	Encryption with Hash function
D(…)	Decryption of 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 tostep 6***
6. ***REPORT 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***

Performance Analysis:

In this section, we will evaluate our 3D localization technique from the aspect of efficiency and network performance.The proposed scheme has been experimented in NS2. The simulation parameters are shown in Table 1. The initial network which is created by using 10 sensor nodes is shown in Fig. 6 and step by step it is increased by 10.

Table 1: Simulation Parameters

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

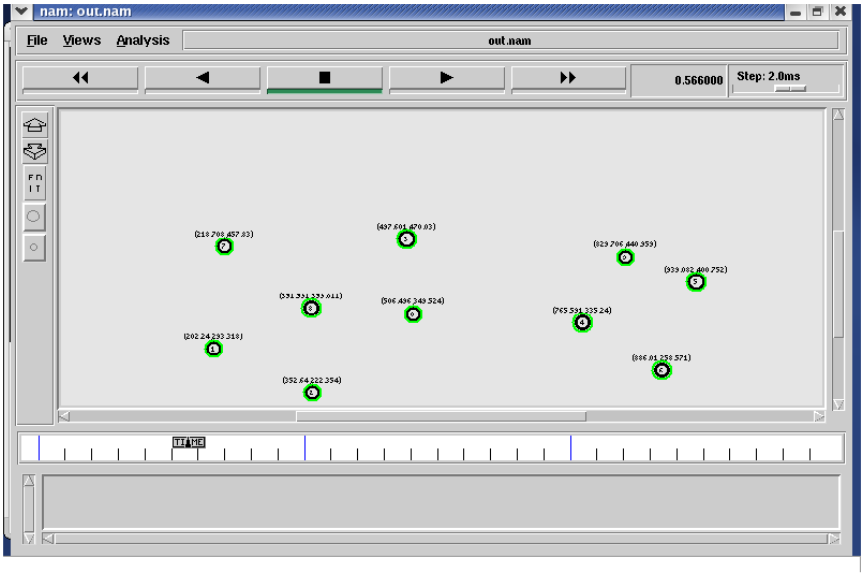

Fig. 5: Creation of nodes in the network

Each of the nodes can communicate with each other, during communication it also checks authentication of nodes, so that the localization data transmitted from one node to the other is accurate. The malicious beacon nodes starts to emerge in the network as the nodes start moving which is shown as solid green circles in Fig. 7.

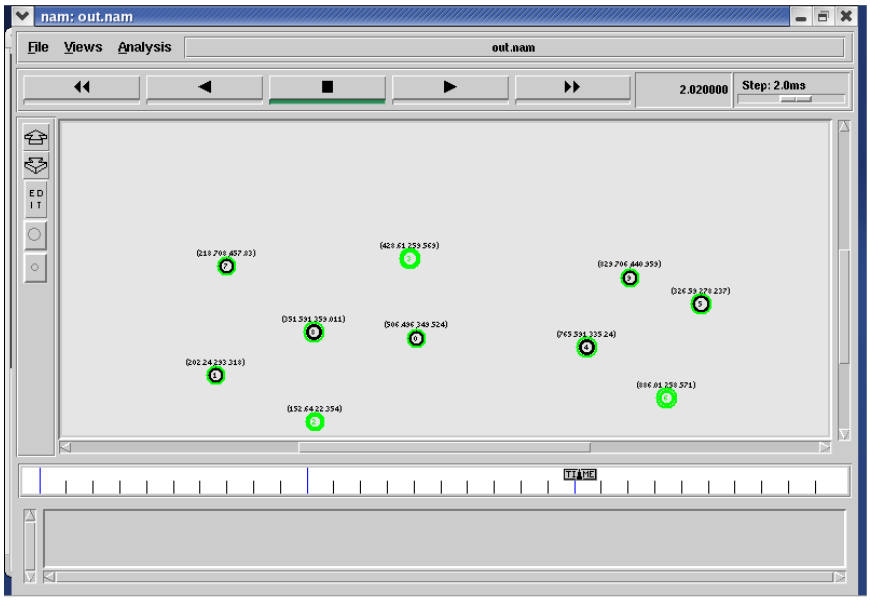

Fig. 7: Malicious beacon nodes emerging in the network which is shown in solid green

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

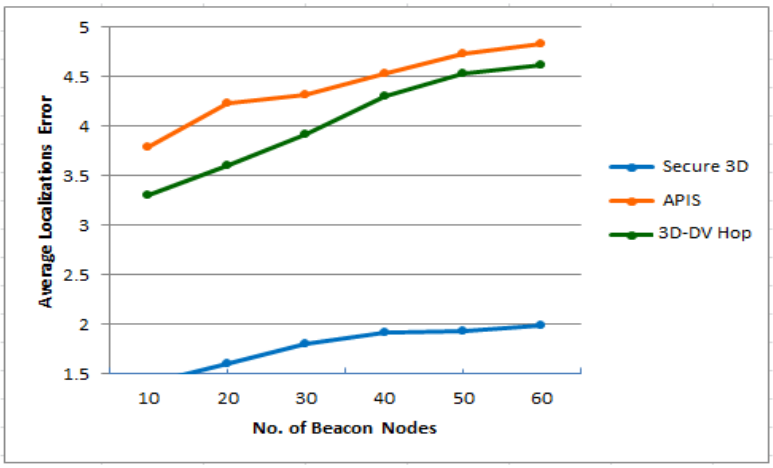

Fig. 8: Average Localization Error

When the localization error and the cheating of beacon nodes are minimized, there will be a considerable increase in the throughput for the Secure 3D algorithm. As shown in Fig. 9 the Secure 3D algorithms' throughput is high when compared to 3D-DV Hop and APIS algorithm, due to the efficient algorithm which is implemented in localization process for a 3D location[21], [22].

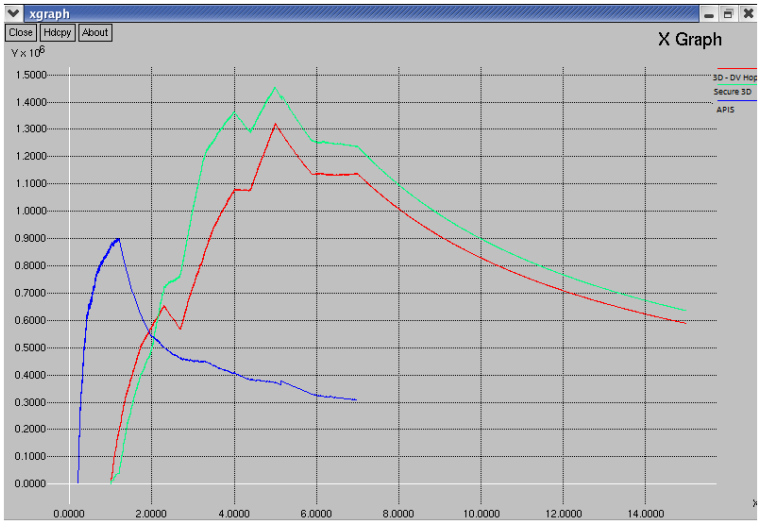

Fig. 9: Throughput Comparison of Secure 3D with APIS and 3D-DV Hop

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[21], [22].

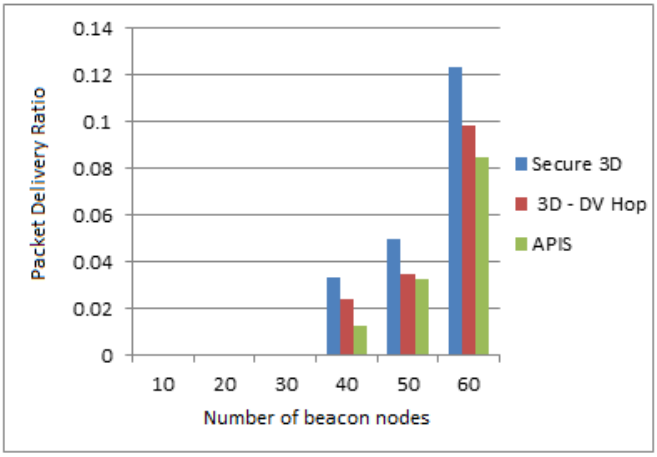

Fig. 10: Packet Delivery Ratio for Secure 3D, APIS and 3D-DV Hop

Conclusion and Future Work:

In conclusion, a Secure 3D algorithm is proposed to handle efficient 3D localization in wireless sensor networks. The performance of Secure 3D, 3D-DV Hop and APIS algorithms are analyzed in terms of throughput, localization error and packet delivery ratio.In this paper, a survey recent contributions that was made to compare the security of wireless sensor node and the performance of Secure 3D algorithm performs better when compared to the other two algorithms since the algorithms focuses not only on accurate localization but also on security issues. There are accomplishments in 3D localization algorithmshowever; 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.In this manner, further research on localization algorithms for WSN with less beacon nodes and low complexity is still necessary.

REFERENCES

1. Hussain, R., H. Oh, 2014. On Secure and Privacy-Aware Sybil Attack Detection in Vehicular Communications", ACM -Wireless personal communications, 77(4): 2649-2673.
2. Kuo-Feng Ssu, Wei-Tong Wang, Wen-Chung Chang, 2009. Detecting Sybil attacks in Wireless Sensor Networks using neighboring information, Computer Networks, 53(18): 3042-3056.
3. Tian, C., W. Liu, 2007. Localization and Synchronization for 3D Underwater Acoustic Sensor Networks,4th International Conference, Hong Kong, China, pp: 622-631.
4. Alfaro, J.G., M. Barbeau and E. Kranakis, 2009. Secure Localization of Nodes inWireless Sensor Networks with Limited Number of Truth Tellers, Communication Networks and Services Seventh Annual Research Conference, pp: 86-93.
5. Capkun, S. and J.P. Hubaux, 2005. Secure positioning of wireless devices with application to sensor networks, 24th Annual Conference of theIEEE Computer and Communications Societies.
6. Capkun, S., J.P. Hubaux and M. Srivastava, 2006. Secure Localization with Hidden and Mobile Base Stations, 25th Annual Conference ofthe IEEE Computer and Communications Societies.
7. Delaet, S., P. Mandal, M. Rokicki, S. Tixeuil, 2008. Deterministic secure positioning in wireless sensor networks, IEEE International Conferenceon Distributed Computing in Sensor Networks (DCOSS).
8. Niculescu, D. and B. Nath, 2003. DV Based Positioning in Ad hoc Networks, In Journal of Telecommunication Systems.
9. He, T., C. Huang, B. Blum, J. Stankovic and T. Abdelzaher, 2003. Rangefree localization schemes in large scale sensor networks, in Proceedings of ACM/IEEE 9th Annual International Conference Mobile Computing and Networking (MobiCom'03).
10. Hwang, J., T. He and Y. Kim, 2008. Secure localization with phantom node detection. Ad Hoc Networks, 6(7): 1031-1050, Elsevier.
11. Lazos, L. and R. Poovendran, 2005. SeRLoc: Robust localization for wireless sensor networks., ACM Transactions on Sensor Networks (TOSN), 1(1): 73-100.
12. Lazos, L., R. Poovendran, S. Capkun, 2005. ROPE: Robust position estimation in wireless sensor networks. 4th International symposium on Informationprocessing in sensor networks.
13. Newsome, J., E. Shi, D. Song and A. Perrig, 2004. The sybil attack in sensor networks: analysis & defenses, 3rd International Symposiumon Information Processing in Sensor Networks(ACM), pp: 259-268.

14. Chen, H., P. Huang, M. Martins, H. Cheung, 2008. Novel Centroid Localization Algorithm for Three-Dimensional Wireless Sensor Networks, 4th IEEE International Conference on Wireless Communications, Networking and Mobile Computing, pp: 1-4.
15. Moore, D., J. Leonard, D. Rus and S. Teller, 2004. Robust Distributed Network Localization with Noisy Range Measurements, in Proceedings of the 2nd International Conference on Embedded Networked Sensor Systems (SenSys '04), Baltimore, USA.
16. Lazos, L. and R. Poovendran, 2004. SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks, in Proceedings of the ACM Workshop on Wireless Security (WiSe '04), Philadelphia, USA.
17. Liu, D., P. Ning and W. Du, 2005. Attack-Resistant Location Estimation in Sensor Networks, in Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05), Los Angeles, USA.
18. Lazos, L., R. Poovendran and S. Capkun, 2005. Rope: RObust Position Estimation in Wireless Sensor Networks, in Proceedings of the 4th International Symposium on Information Processing in Sensor Networks (IPSN '05), Los Angeles, USA.
19. Jadliwala, M., Sheng Zhong, S. Updhyaya, C. Qiao, 2009. Secure Distance-Based Localization in the Presence of Cheating Beacon Nodes, IEEE Transactions on Mobile Computing, 9(6): 810-823.
20. Yan Xu, Yi Zhuang, and Jing-jing Gu, 2015. An Improved 3D Localization Algorithm for the Wireless Sensor Network, International Journal of Distributed Sensor Networks, 11(6): 1-9.
21. Ming Liu, Yaping Bao, Hanyi Liu, 2009. An Improvement of DV-Hop Algorithm in Wireless Sensor Networks, Journal of Micro Computer Information, 25(4-1): 128-129.
22. Jianyun Xu, Aiyan Guo, 2010. Mobile agent routing algorithm for 3D space based on APIT, Journal on Application Research of Computers., 27(6): 2246-2253.
23. Muhammad Umar Aftab, Omair Ashraf, 2015. A Review Study of Wireless Sensor Networks and Its Security, Communications and Network, 7(4): 172-179.
24. Akyildiz, I.F., W.L. Su, Y. Sankarasubramaniam and Cayirci, 2002. A Survey on Sensor Networks, IEEE CommunicationsMagazine, 40: 102-114.
25. JerilKuriakose, Sandeep Joshi and V.I. George, 2013. Localization in Wireless Sensor Networks: A Survey, CSIR Sponsored X Control Instrumentation System Conference (CISCON).