Minimizing Localization Error and Ensure Security of DVHOP Using Random Key Approach

[1]Priyanka Arora, [2]Kantveer
[1]Dept. of CSE, Global Institute of Management and Emerging Technology
[2]Assistant Professor, Global Institute of Management and Emerging Technology

Abstract
Communication through the mobile network is need of the hour. Thus localization becomes important issue discussed in this paper. Algorithms are many which can be range free and range based. The DVHOP algorithm with random key is used to solve the localization problem. The localization is required since node when on the go will require to disseminate data then position determinism is paramount which is achieved with the help of localization. Distance could be of any range when mobile nodes are considered hence range free algorithm is considered. Security aspect of the data is paramount. Since node capture attack is common. Ways to detect and prevent the attack in terms of Random key is suggested. The result obtained will be in terms of the localization error which is given both in terms of localization with and without Node capture attack and random key.

Keywords
Wireless Sensors, Malicious Node, Lifetime, Sensor Network, Economical, Simulation.

I. Introduction

In the DVHOP the distance vector is used in order to detect the distance between the nodes. The routers which are present know the address of the next node in sequence. According to the distance data is transferred forwarded. It is also possible to determine the path from one node to another using this method. DVHOP is the range free algorithm. Range free algorithm is the one in which distance between the nodes does not matter. The nodes can be at very high distance from each other. In range based algorithm the distance will be of prime concern. If distance is not within the range then data cannot be transferred forwarded. In the first section we will describe the related work, in the second section we will focus on localization process and DVHOP algorithm with random key. In the last section we will describe the localization error and references.

II. Localization Process

The localization process uses the position of the anchor node and determines the position of other nodes. Localization process is used to localize the sensor nodes depending upon given input. The localization process consist of the input, distance estimation, position computation and localization algorithm.

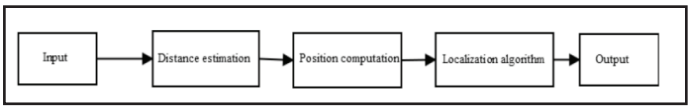

Fig. 1: Showing Localization Process

The localization process will have input from the user. The inputs will include location of the anchor nodes, angle, distances between the nodes etc.

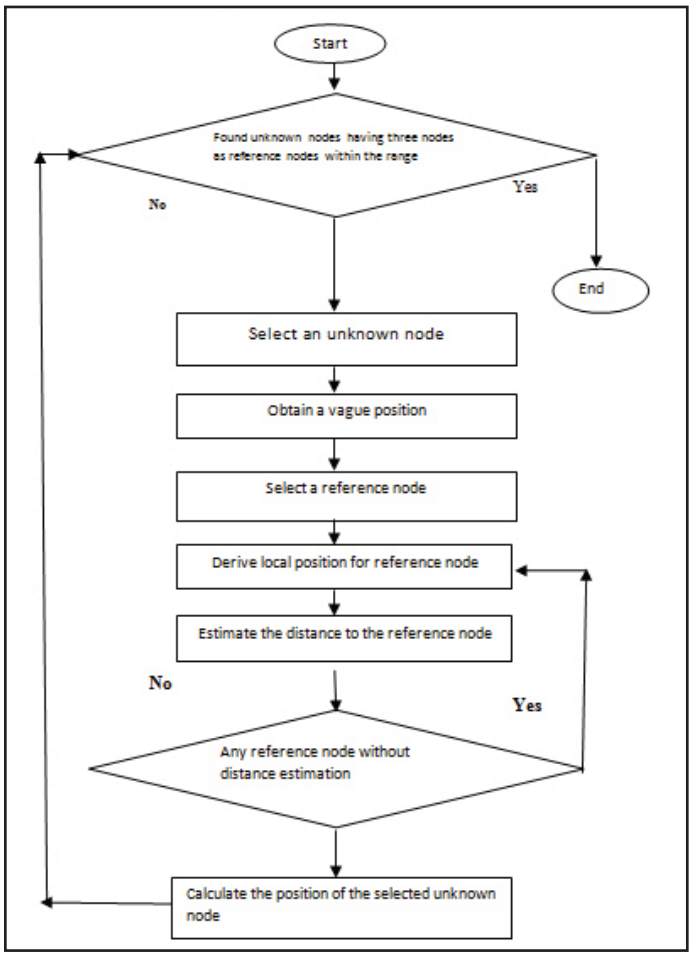

Fig. 2: Showing the Localization Flow Sheet

II. Related Work

The related work describes the work which is already done in the area of distance vector routing. In the distance vector routing each router know the address of the next node in sequence. (Analysis, n.d.) In the suggested paper the accuracy of range based algorithm is analyzed. The range based algorithm is range or distance dependent. When the distance is high then the accuracy of the algorithm will start to decay. The distance should be less in case of the range based algorithm. The concept of cooperative localization will be used in this case. (Bachrach & Taylor, n.d.) Localization in sensor network is considered in this case. Localization will depend upon the distance. If the distance is high than the localization is difficult to be performed otherwise localization is relatively easy to be performed. In order to solve the problems of the range based algorithm range free algorithm is used. The range based algorithm cannot be operational if the distance between the nodes become high. The range free algorithm does not consider the distance and hence perform better in case of high distance between the sensor nodes. (Kumar, Chand, Kumar, & Kumar, 2011) in the suggested technique range free algorithm is considered. In this case the course information is

derived on the basis of range free algorithm. The range free algorithm is independent of the distance. Also the cost associated with the algorithm is low. (Pathan, Lee, & Hong, 2006) The concept of the security is considered in this case. The WSN when comes in contact with the number of different types of users the security of the WSN is sacrificed. The various security issues and there rectifications are considered in this case. The malicious nodes are handled in this case. (Stoleru, He, & Stankovic, 2007) in the suggested technique range free algorithm is considered. In this case the course information is derived on the basis of range free algorithm. The range free algorithm is independent of the distance. Also the cost associated with the algorithm is low. (Walters & Liang, 2007)so does the need for effective security mechanisms. Because sensor networks may interact with sensitive data and/or operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the sys- tem design. However, due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional net- work/computer security. There is currently enormous research potential in the field of wireless sensor network security. Thus, familiarity with the cur- rent research in this field will benefit researchers greatly. With this in mind, we survey the major topics in wireless sensor network security, and present the obstacles and the requirements in the sensor security, classify many of the current attacks, and finally list their corresponding defensive measures.", "author" : [{ "dropping-particle" : "", "family" : "Walters", "given" : "Jp", "non-dropping-particle" : "", "parse-names" : false, "suffix" : "" }, { "dropping-particle" : "", "family" : "Liang", "given" : "Zhengqiang", "non-dropping-particle" : "", "parse-names" : false, "suffix" : "" }], "container-title" : "Security in distributed, \u2026", "id" : "ITEM-1", "issued" : { "date-parts" : [["2007"]] }, "page" : "1-50", "title" : "Wireless sensor network security: A survey", "type" : "article-journal" }, "uris" : ["http://www.mendeley.com/documents/?uuid=eefb1166-dbfb-497f-a4a5-f6068042f01f"] }], "mendeley" : { "formattedCitation" : "(Walters & Liang, 2007 The concept of the security is considered in this case. The WSN when comes in contact with the number of different types of users the security of the WSN is sacrificed. The various security issues and there rectifications are considered in this case. The malicious nodes are handled in this case. (Yang, 2014)either sensed directly or gained from their environments, makes them attractive targets for unscrupulous individuals to subvert, in an attempt to gain access to the WSNs and/or disrupt the interactions of users with both the networks and subsequently with their environment. Consequently, providing effective security is crucial for the successful adoption and operation of WSNs. We cannot deploy such a critical technology without first addressing the security and privacy challenges to ensure that it does not compromise those whom it is meant to benefit. This chapter provides a general review and categorization of the fundamental security primitives required to establish secure WSNs. The ZigBee security service is introduced as an example. The chapter then discusses Denial of Service (DoS The ubiquitous nature of WSN applications and their access to confidential information, either sensed directly or gained from their environments, makes them attractive targets for unscrupulous individuals to subvert, in an attempt to gain access to the WSNs and/or disrupt the interactions of users with both the networks and subsequently with their environment. (Yang, 2014)either sensed directly or gained from their environments, makes them attractive targets for unscrupulous individuals to subvert, in an attempt to gain access to the WSNs and/or disrupt the interactions of users with both the networks and subsequently with their environment. Consequently, providing effective security is crucial for the successful adoption and operation of WSNs. We cannot deploy such a critical technology without first addressing the security and privacy challenges to ensure that it does not compromise those whom it is meant to benefit. This chapter provides a general review and categorization of the fundamental security primitives required to establish secure WSNs. The ZigBee security service is introduced as an example. The chapter then discusses Denial of Service (DoSConsequently, providing effective security is crucial for the successful adoption and operation of WSNs. (Yang, 2014)either sensed directly or gained from their environments, makes them attractive targets for unscrupulous individuals to subvert, in an attempt to gain access to the WSNs and/or disrupt the interactions of users with both the networks and subsequently with their environment. Consequently, providing effective security is crucial for the successful adoption and operation of WSNs. We cannot deploy such a critical technology without first addressing the security and privacy challenges to ensure that it does not compromise those whom it is meant to benefit. This chapter provides a general review and categorization of the fundamental security primitives required to establish secure WSNs. The ZigBee security service is introduced as an example. The chapter then discusses Denial of Service (DoSWe cannot deploy such a critical technology without first addressing the security and privacy challenges to ensure that it does not compromise those whom it is meant to benefit. This chapter provides a general review and categorization of the fundamental security primitives required to establish secure WSNs. (Yang, 2014)either sensed directly or gained from their environments, makes them attractive targets for unscrupulous individuals to subvert, in an attempt to gain access to the WSNs and/or disrupt the interactions of users with both the networks and subsequently with their environment. Consequently, providing effective security is crucial for the successful adoption and operation of WSNs. We cannot deploy such a critical technology without first addressing the security and privacy challenges to ensure that it does not compromise those whom it is meant to benefit. This chapter provides a general review and categorization of the fundamental security primitives required to establish secure WSNs. The ZigBee security service is introduced as an example. The chapter then discusses Denial of Service (DoSThe ZigBee security service is introduced as an example. The chapter then discusses Denial of Service (DoS) attacks and defences, focusing on the threat of a DoS attack on a WSN.(Yang, 2014)either sensed directly or gained from their environments, makes them attractive targets for unscrupulous individuals to subvert, in an attempt to gain access to the WSNs and/or disrupt the interactions of users with both the networks and subsequently with their environment. Consequently, providing effective security is crucial for the successful adoption and operation of WSNs. We cannot deploy such a critical technology without first addressing the security and privacy challenges to ensure that it does not compromise those whom it is meant to benefit. This chapter provides a general review and categorization of the fundamental security primitives required to establish secure WSNs. The ZigBee security service is introduced as an example. The chapter then discusses Denial of Service (DoS A framework for increasing the resistance of WSNs to remote DoS threats is introduced, implemented, and evaluated using a WSN based home automation as a case study. (Yu, Prasanna, & Krishnamachari, 2006)This paper studies the

difficult feature of energy conservation. The energy has to be carefully used since sensors cannot handle large amount of data. The energy conservation hence is compulsory. (Yu et al., 2006) The concept of energy management is considered in this case. WSN does not uses wires hence mobility is present. As more and more people start to use WSN hence security problem is present. (Yu et al., 2006)Then, by discrediting the transmission time, we present a simple, distributed on-line protocol that relies only on the local information available at each sensor node. (Yu et al., 2006)Extensive simulations were conducted for both long and short-range communication scenarios using two different source placement models. We used the baseline of transmitting all packets at the highest speed and shutting down the radios afterwards. (Yu et al., 2006)Our simulation results show that compared with this baseline, up to 90% energy savings can be achieved by our techniques (both off-line and on-line), under different settings of several key system parameters. (Zheng & Dehghani, 2012) in the suggested technique range free algorithm is considered. In this case the course information is derived on the basis of range free algorithm. The range free algorithm is independent of the distance. Also the cost associated with the algorithm is low.

III. Comparison of Various Algorithms

There are legions of algorithms which are used in order to avoid DDOS attack. The algorithm comparison is listed in the tabular form as

Table 1: Showing the Comparison of Different Algorithms Used to Detect NCA

PARAMETERS	Dvhop	APIT	Dvhop With Random Key
Message Propagation delay	10ms per 10 Messages	13ms per 10 Messages	4 ms per 10 Messages
Alarm Time	5ms	7ms	2ms
Redundancy	Medium	High	Low
Localization Error	14.333	16.434	9.898
Malicious Nodes Detected	Low	Medium	High

IV. DVHOP and Localization Algorithm

The DVHOP algorithm is a range free algorithm. In this algorithm distance between nodes is not important. As long as it is possible to transfer the data, then data can be transferred. The DVHOP algorithm is divided into following steps:

A. Unknown Node and Compute Nodes Each Beacon Minimum Hops

1. Beacon nodes broadcast their locations to the neighbors of information packets, including the jump number field is initialized to 0. Receiving node records to each beacon nodes having the minimum number of hops, ignoring a beacon node from the same large number of hops a packet. Then hop count plus one, and forwarded to the neighbors. Through this method, all nodes in the network to be able to record each beacon node under the minimum number of hops.
2. Compute unknown node and beacon node's actual hop distance. Each beacon nodes according to the first stage record other beacon nodes position information and the distance hops, using the equation (1) estimate the average hop actual distance. (2) Calculate and obtain the unknown node average hop distance. Beacon nodes by saving the coordinates of the other beacon nodes and the minimum number of hops using the equation (1) in the network calculate the average hop distance:

$$c_i = \sum_{i \neq j} \frac{\sqrt{(x_i - x_j)^2 - (y_i - y_j)^2}}{\sum_{i \neq j} hop_{ij}}$$

Here x and Y are the co-ordinates of the beacon nodes.

3. Using trilateration measurement or maximum likelihood estimation method to calculate its own position. Unknown node uses the second phase to each record jump distance beacon nodes using trilateration measurement or maximum likelihood estimation method to calculate their coordinates.

There exist more accurate equation which can be used in order to enhance the performance of the DVHOP algorithm.

$D=D/2+d_{ab}/2hop_{ab}$

Here D is the original average hop distance dab is the distance between the nodes between a and b. hop_{ab} is the hops between the anchor nodes.

The localization is the mechanism of determining the path that exists between source and the destination. The DVHOP algorithm is prone to attacks. One of the common attacks is DDOS which means distributed denial of service attack. This attack will going to consume the resources associated with the node and cause the traffic to be jammed. In order to solve the problem random key is proposed. With the help of random key every node within the localization process is assigned a random id which will be difficult to guess by the intruder or malicious node. Hence the security will be enhanced. Also the localization error is reduced. The proposed algorithm is as follows

DVHOP With Random Key

- Generate random Ids for the nodes.
- Assign the Ids to the nodes.
- Detect the malicious Entry
- If Malicious(Node) then
- Block the node
- Else
- Move onto next step in sequence
- End of if
- Calculate localization Error
- Stop

The above algorithm will be used to determine whether the attack has occurred on the node or node. If attack does occur on the system than node which is malicious is blocked. Otherwise node is allowed to perform the suggested operation. In the end localization error will be calculated. From the experiment it is proved that localization error in case of proposed system is less as compared to the previous algorithm.

IV. Results

The result of the existing system in terms of the time taken to perform localization is as follows:

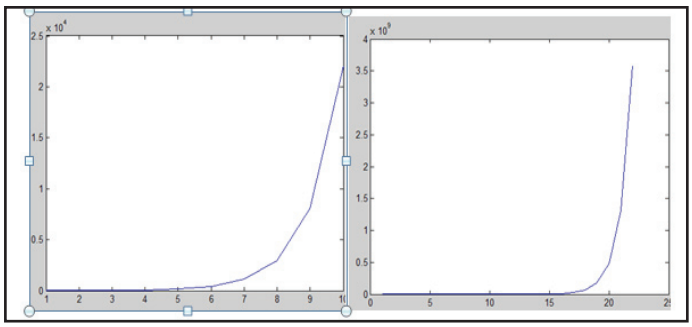

Fig. 3: Showing the Time Consumption Which is 11ms in Case of proposed system and 20 ms in case of existing system.

The localization error in case of existing system is 31.0345 and in case of proposed system is 8.0923.
The proposed algorithm ensures the security and also decreases the localization error. The algorithm is implemented using the MATLAB software. The Results are as follows:

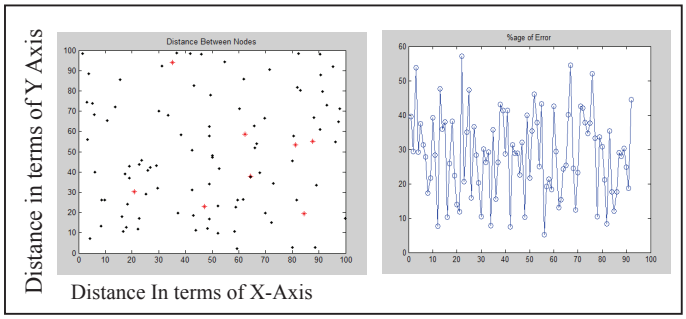

Fig. 4(a): Showing the Position of the anchor and unknown nodes.
Fig 4(b): Describing the Localization error that appears within the system

The fig. 4(a) indicates that the nodes are distributed randomly over the network. The red nodes represent the anchor nodes. The black nodes are the unknown nodes. The node will be synchronized by looking at the position of the anchor and unknown nodes.
The fig. 4(b) indicates localization error it occurs when two anchor nodes are located together, such as A and B , the estimated position, such as, N1, N2 and N3 is on the line connecting two anchor nodes, even though the real positions of normal nodes are N1, N2, and N3. The error propagation is amplified by the distance from anchor nodes.
Localization Error is significantly reduced by the use of proposed technology. The comparison table indicates the performance of the proposed system.

Table 1: Showing the Comparison of the Various Range Free Algorithms

Technique	Node density	Cost	Accuracy	Overhead	Scalability
APIT	>16	Low	Good	Small	Yes
DV-Hop	>8	Medium	Good	Largest	No
Multi-Hop	>12	High	Good	Large	No
Centroid	>0	Low	Fair	Smallest	Yes
Gradient	>6	Low	Average	Large	Yes

From the above comparison table it is clear that the performance of the proposed system including DVHOP is better. The concept of random key is introduced and performance is enhanced.

V. Conculsion and Future Work

The proposed method will handle the attack very well. The localization error is also significantly reduced. The localization process will also produce better result. The nodes from which data can be transferred and destination node which can received the data will be effectively selected using this algorithm. Ids to the nodes will be randomly assigned and hence difficult to detect by the malicious nodes. In the future we will reduce the localization errors further.

References

[1] Advisor, D., Committee, D.,"Communication Security in Wireless Sensor", 2007.
[2] Almuzaini, K. K. (2010),"Range-Based Localization in Wireless Networks Using Density-Based Outlier Detection", Wireless Sensor Network, 02(11), pp. 807–814. [Online] Available: http://doi.org/10.4236/wsn.2010.211097
[3] Analysis, A. L. B. (n.d.),"Accuracy of Range-Based Cooperative Localization in Wireless Sensor Networks", pp. 1–11.
[4] Anwar, R. W., Bakhtiari, M., Zainal, A., Abdullah, A. H., Qureshi, K. N., Computing, F., & Bahru, J. (2014),"Security Issues and Attacks in Wireless Sensor Network", World Applied Sciences Journal, 30(10), pp. 1224–1227," [Online] Available: http://doi.org/10.5829/idosi.wasj.2014.30.10.334
[5] Bachrach, J., Taylor, C. (n.d.),"Localization in Sensor Networks".
[6] Boudhir, A. A., Mohamed, B. A., (2010),"New Technique of Wireless Sensor Networks Localization based on Energy Consumption", International Journal of Computer Application, 9(12), pp. 25–28. [Online] Available: http://doi.org/10.5120/1436-1935
[7] Chandrasekhar, V. R., Seah, W. K. G. (n.d.),"Range-free Area Localization Scheme for Wireless Sensor Networks".
[8] Corke, P., Wark, T., Jurdak, R., Hu, W., Valencia, P., Moore, D. (2010),"Environmental wireless sensor networks", Proceedings of the IEEE, 98(11), pp. 1903–1917, [Online] Available: http://doi.org/10.1109/JPROC.2010.2068530
[9] He, T., Huang, C., Blum, B. M., Stankovic, J. A., Abdelzaher, T. (2003),"Range-Free Localization Schemes for Large Scale Sensor Networks 1".
[10] Kalita, H. K., Kar, A. (2009). W s n s a, 1(1), 1–10.
[11] Kumar, A., Chand, N., Kumar, V., Kumar, V.,"Range Free Localization Schemes for Wireless Sensor Networks", International Journal of Computer Networks & Communications, 3(6), pp. 115–129. [Online] Available: http://doi.org/10.5121/ijcnc.2011.3607
[12] Pathan, a. S. K., Lee, H.-W. L. H.-W., Hong, C. S. H. C. S. (2006).,"Security in wireless sensor networks: Issues and challenges", 2006 8th International Conference Advanced Communication Technology, 2, 6 pp.–1048, [Online] Available: http://doi.org/10.1109/ICACT.2006.206151
[13] Stoleru, R., He, T., & Stankovic, J. A.,"Range-free localization. Secure Localization and Time Synchronization for Wireless Sensor and Ad-Hoc Networks, pp. 3–31, 2007.
[14] Walters, J., Liang, Z., (2007),"Wireless sensor network security: A survey", Security in Distributed, …, 1–50. [Online] Available: http://books.google.com/books?hl=en&lr=&id=KhxxsN3vJuYC&oi=fnd&pg=PA367&dq=Wireless+Sensor+Network+Security+:+A+Survey&ots=R4RpHtOLGz&sig=Z_PWgD18TATEHDJK6qLCzP4CsTk

[15] Yang, S.-H. (2014). WSN Security, 187–215. [Online] Available: http://link.springer.com/chapter/10.1007/978-1-4471-5505-8_9

[16] Yu, Y., Prasanna, V., Krishnamachari, B. (2006),"Energy Minimization for Real-Time Data Gathering in Wireless Sensor Networks", IEEE Transactions on Wireless Communications, 5(10), pp. 3087–3096. [Online] Available: http://doi.org/10.1109/TWC.2006.04709

[17] Zheng, J., Dehghani, A., (2012),"Range-Free Localization in Wireless Sensor Networks with Neural Network Ensembles", Journal of Sensor and Actuator Networks, 1(3), pp. 254–271. [Online] Available: http://doi.org/10.3390/jsan1030254

[18] Zhong, Z. (2009). Achieving Range-free Localization Beyond Connectivity. Sensys, pp. 281–294. [Online] Available: http://doi.org/http://doi.acm.org/10.1145/1644038.1644066