INTERNATIONALJOURNALOFENGINEERING SCIENCES&MANAGEMENT

LOCALIZATION OF SENSOR NODES TO DETECT MALICIOUS NODES: PROBLEM DEFINITION

Namita[*1] and Tejinderdeep Singh[2]

[*1]Research Scholar and [2]Assistant Professor

ABSTRACT

Localization is the mechanism by which position of the nodes which are transferring the data will be analyzed. The transferred data will reach the destination. As the number of nodes on the network increases so does the security problems. In order to tackle the problems of the malicious nodes ,certification authority will be introduced within the localization process. The localization can be range free or range based in nature. The localization process can depend upon the distance. If the localization depends upon the distance then it is known as range based algorithm. If the localization does not depend upon the distance then it is known as range free algorithm. In the proposed paper we study and compare the various localization mechanisms available.

Keywords*: Wireless Sensor Networks, Sensor Node.*

I. INTRODUCTION

The localization process will be used so that the position of the data being transferred can be analyzed. The concept of sensor nodes will be used in this case. In WSNs sensor nodes are deployed in real world environment and determined some physical behavior. There are many challenges which are involved in this case. Sensor are small devices, the cost involved is low and having low processing capabilities. WSNs applications attracted great interest of researchers in recent years. WSN is different from AD-HOC and mobile networks in many ways. WSNs has different applications. Therefore the protocols designed for AD-HOC networks do not suite WSNs. Different applications of WSNs are the following: Monitoring the various aspects and physical mechanism like temperature, sound and light, habitat monitoring, traffic control, patient health care monitoring and under water acoustic monitoring.

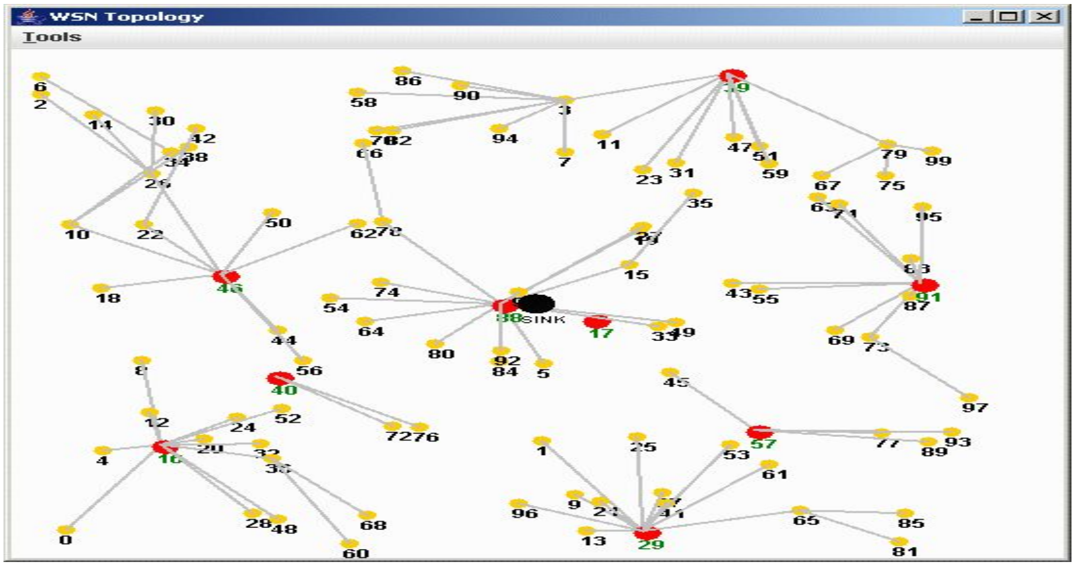

Fig 1 Showing the Localization process in WSN[[19]]

The localization process is divided into two parts

1) Range free algorithm
2) Range Based algorithm

The range free algorithm will be the one in which distance is not the issue. It means that if the distance is neglected then as well it can be easily determined that which node are transferring the data and which node is not transferring the data. The concept of monitoring nodes will be used in this case. The monitoring nodes will check whether the nodes transferring the data are according to the prescribed standards or not. If the data transferred is not according to the prescribed standards then the report will be send to the certification authority. This certification authority will go to determined whether the node is malicious or node. In the proposed paper we will present the review of the various papers we have studied.

II. LITERATURE SURVEY

The sensors will play very important role in the WSN. The data transfer will be with the help of these nodes. The problem with the sensor nodes is that they have limited energy and cannot store large amount of data. The sensors will be used both in range free as well as range based algorithm. The range free algorithms are analyzed in this case. The range free algorithm does not depend upon the distance. The distance can be from few yards to large kilometers. The range free algorithm will not be affected by that. The approximate position of the nodes will be given in this case. Wireless sensor network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, review proposed security mechanisms for wireless sensor networks. The range free algorithms are considered in this case. The DVHOP and APIT algorithms are considered in this case. The distance vector routing will be considered. The localization error is also calculated in this case. As wireless sensor networks continue to grow, so does the need for effective security mechanisms. However, due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional net- work/computer security. We survey the major topics in wireless sensor network security, and present the obstacles and the requirements in the sensor security. Security issues are discussed in these suggested papers. As we all know that due to the universal nature of WSN applications and their access to confidential information makes them attractive targets for unscrupulous individuals to subvert. This chapter provides a general review and categorization of the fundamental security primitives required to establish secure WSNs. This paper studies the difficult feature of energy conservation. 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. 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. The range free algorithm will be considered in this case. This algorithm will be free of distance. In case of large network it will be very difficult to determine the position of the every sensor node. This process will be difficult in nature and also consume time as well as cost. In order to resolve the problem the range free algorithms are proposed in this case. Wireless sensor networks have been proposed for many location-dependent applications. In such applications, the requirement of low system cost prohibits many range-based methods for sensor node localization; on the other hand, range-free localization. Large wireless sensor networks are considered in this case. The wireless sensors have limited capabilities. They can handle little data and energy consumption is also minimized. The range free algorithms are considered in this case. The range free algorithm are distance independent. Node localization is commonly employed in wireless networks. For example, it is used to improve routing and enhance security. Localization algorithms can be classified as range-free or range-based. In this paper, we propose a new range-based algorithm which is based on the density-based outlier detection algorithm (DBOD) from data mining. It requires selection of the K-nearest neighbors (KNN). The new technique of localization is proposed in this case. The localization with the help of 3D is proposed. The localization error is greatly reduced in this case. The range free algorithm is considered in this case. The range free algorithm is considered which is independent of the distance. The localization is the process of determining the position of the nodes within the WSN. The energy consumption has to be minimized and technique for doing so is proposed in this paper.

III. COMPARISON OF THE TECHNIQUES

Attributes	DVHOP	APIT	CLR
Category	Range Free	Range Free	Range Free
Network	Heterogeneous	Heterogeneous	Homogeneous
Area Based	No	Yes	No

PIT Test	Not Enabled	Enabled	Not Enabled
Localization	Distance Vector	Centric	Centric

Table I. Comparison of Techniques [2]

The above said attributes indicates that the routing tables will be updated dynamically in case of DVHOP and all other algorithms are static in nature. The algorithms which are considered are range free in nature. The DVHOP algorithm is generally less expensive in nature. The effect of random key is profound in case of DVHOP and all other algorithms does not respond to random keys. APIT algorithm is also range free in nature. The nodes which are used in this case are heterogeneous in nature. It means that the nodes are of different types. The specific area is attached in case of APIT algorithm. The localization which is used in this case is centric. There exist another test known as CLR. It is range free in nature. The algorithm uses homogeneous nodes. it means same types of nodes are used in this case. It is not based on the area. The algorithm is general purpose in nature.

IV. PROBLEM DEFINITION

In the existing system the APIT algorithm is used in order to determine the distance of nodes so that data transfer and receiver can be determined. The source could be malicious in nature that is very difficult to determine using the existing approach. The APIT is the range free algorithm which does not depend upon the distance. Designing a protocol which can handle such situation can be very difficult. The problem of detecting and rectifying the malicious entry will be the target of the proposed paper.

V. PROPOSED SOLUTION

In order to resolve the problem present within the existing approach concept of random key is introduced. In the proposed paper the IDs to the nodes will not be static rather these IDs will continuously change. Since IDs continuously changes hence it cannot be discoverable by the malicious node. Thus intruder cannot enter into the network. The proposed algorithm will have following steps associated with it.

From the procedures and principles of APIT algorithm; we can see that there are three obvious disadvantages: (1) Average localization error rate cannot lower as communication radius increase; (2) The cover rate of APIT cannot reach 100%; (3) Distribution-aware, the localization error rate and cover rate is different in different distributions. In order to solve this problem, this paper proposed an improved APIT algorithm called IMPROVED APIT algorithm, the main innovations of IMPROVED APIT are as following: (1) Adjust the location of located nodes by formula 1 in order to reduce the localization error rate. (2) Take the located nodes as the secondary anchor node in order to locate more nodes and thus the cover rate of the localization will be increased. And the secondary anchor node can relocate the nodes which cannot locate in the first circle. (3) Give the special tackle of the node in inflexion points.

VI. CONCLUSION

In the proposed paper the comparison of various range free algorithm is made. The attributes of the various techniques are listed in this paper. The future work will be work on one these range free algorithms and minimize the localization error. The security will be enhanced and using some form of random key mechanisms so that the key cannot be guessed easily. The sensor node energy consumption also has to be minimized.

REFERENCES

[1] Singh, S. P., & Sharma, S. C. (2015). Range Free Localization Techniques in Wireless Sensor Networks: A Review. Procedia Computer Science, 57, 7-16.

[2] A. Kumar, N. Chand, V. Kumar, and V. Kumar, "Range Free Localization Schemes for Wireless Sensor Networks," Int. J. Comput. Networks Commun., vol. 3, no. 6, pp. 115–129, 2011.

[3] a. S. K. Pathan, H.-W. L. H.-W. Lee, and C. S. H. C. S. Hong, "Security in wireless sensor networks: issues and challenges," 2006 8th Int. Conf. Adv. Commun. Technol., vol. 2, p. 6 pp.–1048, 2006.

[4] R. Stoleru, T. He, and J. A. Stankovic, "Range-free localization," Secur. Localization Time Synchronization Wirel. Sens. Ad Hoc Networks, pp. 3–31, 2007.

[5] J. Walters and Z. Liang, "Wireless sensor network security: A survey," Secur. Distrib. ..., pp. 1–50, 2007.

[6] S.-H. Yang, "WSN Security," pp. 187–215, 2014.

[7] Y. Yu, V. Prasanna, and B. Krishnamachari, "Energy Minimization for Real-Time Data Gathering in

Wireless Sensor Networks," IEEE Trans. Wirel. Commun., vol. 5, no. 10, pp. 3087–3096, 2006.

[8] V. R. Chandrasekhar and W. K. G. Seah, "Range-free Area Localization Scheme for Wireless Sensor Networks."

[9] Z. Zhong, "Achieving Range-free Localization Beyond Connectivity," Sensys, pp. 281–294, 2009.

[10] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, "Range-Free Localization Schemes for Large Scale Sensor Networks 1," 2003.

[11] K. K. Almuzaini, "Range-Based Localization in Wireless Networks Using Density-Based Outlier Detection," Wirel. Sens. Netw., vol. 02, no. 11, pp. 807–814, 2010.

[12] A. A. Boudhir and B. A. Mohamed, "New Technique of Wireless Sensor Networks Localization based on Energy Consumption," Int. J. Comput. Appl., vol. 9, no. 12, pp. 25–28, 2010.

[13] J. Zheng and A. Dehghani, "Range-Free Localization in Wireless Sensor Networks with Neural Network Ensembles," J. Sens. Actuator Networks, vol. 1, no. 3, pp. 254–271, 2012.

[14] Noman, Nasimul, and Hitoshi Iba. "Accelerating differential evolution using an adaptive local search." Evolutionary Computation, IEEE Transactions on 12.1 (2008): 107-125.

[15] Tušar, Tea, and Bogdan Filipič. "Differential evolution versus genetic algorithms in multiobjective optimization." Evolutionary Multi-Criterion Optimization. Springer Berlin Heidelberg, 2007.

[16] Das, Swagatam, Ajith Abraham, and Amit Konar. "Particle swarm optimization and differential evolution algorithms: technical analysis, applications and hybridization perspectives." Advances of Computational Intelligence in Industrial Systems. Springer Berlin Heidelberg, 2008. 1-38.

[17]Chao-Xue Wang, Chang-Hua Li, Hui Dong and Fan Zhang, 2013. "An Efficient Differential Evolution Algorithm For Function Optimization." Information Technology Journal, 12: 444-448

[18] A. K. Qin, V. L. Huang, and P. N. Suganthan," Differential Evolution Algorithm With Strategy Adaptation for Global Numerical Optimization." 1089-778X/$25.00 © 2008 IEEE

[19]"apit.Image https://www.google.co.in/search?q=localization+process+in+wsn&biw=1280&bih=675&source=lnms&tbm=isch&sa=X&sqi=2&ved=0ahUKEwjBo93Ymp3LAhWQxY4KHUnyAHsQ_AUIBigB#tbm=isch&q=dvhop+localization+process+in+wsn&imgrc=esIx5XKsay5TpM%3A" .