ISSN (e): 2250 – 3005 || Volume, 06 || Issue, 03||March – 2016 ||
International Journal of Computational Engineering Research (IJCER)

MINIMIZING LOCALIZATION ERROR AND ENSURE SECURITY OF DVHOP APPROACH

[1]Priyanka Arora
M-Tech(CSE)
Global Institute of Management and
Emerging Technology

[2] Kantveer
Assistant Professor
Global Institute of Management and
Emerging Technology

ABSTRACT

In case of wireless sensor network there exist problem of determining the nodes which are symmetrical to each other. The nodes which are symmetrical and are at lesser distance are selected for data transfer. This identification of the distance between nodes is known as localization. In the proposed paper work on DVHOP is done. The DVHOP is the distance vector routing based protocol which is used to indicate whether there exist a path from source to destination or not. The malicious node can also be present which can take over the actual node causing problems in the transfer process. The most common attack which results from this will be DDOS attack. This will result in the duplication of the information and will cause traffic jamming. DVHOP with random key is used to handle DDOS attack.

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. In the last section we will describe the localization error and references.

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) 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) 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)Consequently, providing effective security is crucial for the successful adoption and operation of WSNs. (Yang, 2014)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. (Yang, 2014)The 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) 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.

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 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. With the help of 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

```
a)  Generate Ids for the nodes.
b)  Assign the Ids to the nodes.
c)  Detect the malicious Entry
d)  If Malicious(Node) then
e)  Block the node
    Else
f)  Move onto next step in sequence
    End of if
g)  Calculate localization Error
h)  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.

RESULTS

The algorithm ensures the security and also decreases the localization error. The algorithm is implemented using the MATLAB software. The Results are as follows

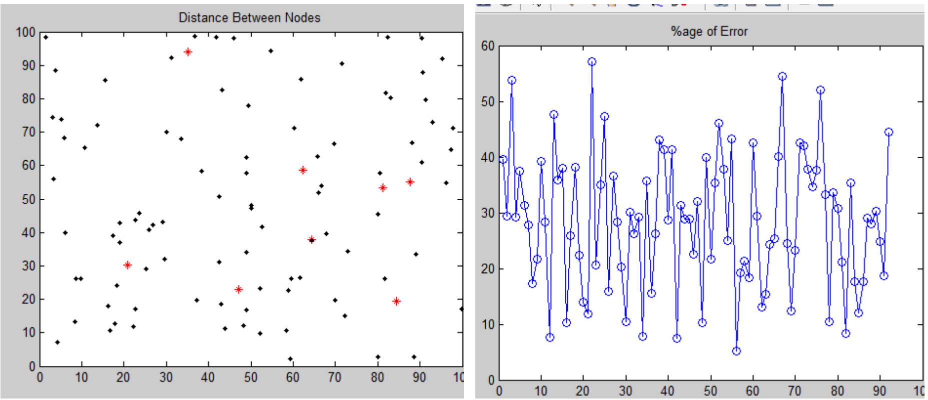

Fig 1

The localization error is significantly reduced by the use of technology however the result could have been better if ids are used.

CONCULSION AND FUTURE WORK

The DVHOP 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. (2007). Communication Security in Wireless Sensor.

[2]. Almuzaini, K. K. (2010). Range-Based Localization in Wireless Networks Using Density-Based Outlier Detection. *Wireless Sensor Network*, *02*(11), 807–814. 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 :, 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), 1224–1227. 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), 25–28. 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), 1903–1917. 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. (2011). Range Free Localization Schemes for Wireless Sensor Networks. *International Journal of Computer Networks & Communications*, *3*(6), 115–129. 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. http://doi.org/10.1109/ICACT.2006.206151

[13]. Stoleru, R., He, T., & Stankovic, J. A. (2007). Range-free localization. *Secure Localization and Time Synchronization for*

Wireless Sensor and Ad Hoc Networks, 3–31.

[14]. Walters, J., & Liang, Z. (2007). Wireless sensor network security: A survey. *Security in Distributed, …*, 1–50. Retrieved from 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. Retrieved from 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), 3087–3096. 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), 254–271. http://doi.org/10.3390/jsan1030254

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