Volume 6, Issue 5, May 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

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

Namita
Research Scholar,

Tejinderdeep Singh
Assistant Professor,

Abstract: ***In case of wireless sensor network there exist problem of searching the nodes which are similar to each other. The nodes which are similar and are at minimum distance are selected for data transfer. The distance between nodes is known as localization. In the introduced paper work on APIT is done. The APIT is the distance vector routing based protocol which is used to indicate whether there exist a path from source to destination or not. The infected node can also be present which can take over the actual node causing problems in the transfer process. The Proposed pseudo code is energy efficient and grant extend the lifetime of the sensor network. Additionally the proposed pseudo code has the advantage of being simple and economical. The pretense results show that the introduced pseudo code is a practical, effective and accurate method for sensor nodes location in a WSN.***

Keywords: Wireless Sensor Network, APIT, Infected Node, Economical, Simulation.

I. INTRODUCTION

In the APIT the distance vector is used in order to check 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 compose the path from one node to another using this method. APIT is the range free pseudo code. Range free pseudo code 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 pseudo code the distance will be of prime anxiety. 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 APIT pseudo code with irregular key. These were 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 determined 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 pseudo code.

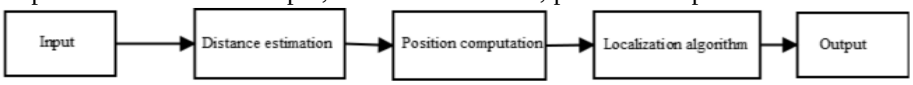


Fig 1: Showing Localization Process

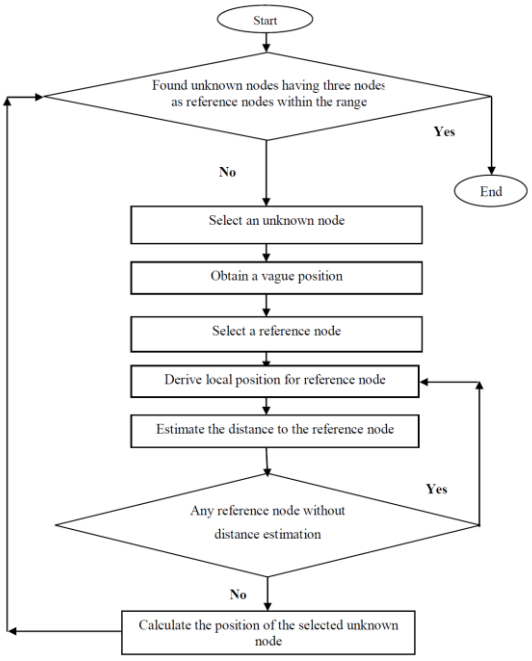


Fig 2: Showing the localization flow sheet

© 2016, IJARCSSE All Rights Reserved

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

III. 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. [3] In the indicated paper the accuracy of range based pseudo code is analyzed. The range based pseudo code is range or distance dependent. When the distance is high then the accuracy of the pseudo code will start to decline. The distance should be less in case of the range based pseudo code. The concept of cooperative localization will be used in this case. [5]Localization in sensor network is determined 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 easy to be performed. In order to solve the problems of the range based pseudo code range free pseudo code is used. The range based pseudo code cannot be operational if the distance between the nodes become high. The range free pseudo code does not consider the distance and hence perform better in case of high distance between the sensor nodes. [11] In the suggested technique range free pseudo code is determined. In this case the course information is derived on the basis of range free pseudo code. The range free pseudo code is free of the distance. Also the cost assigned with the pseudo code is low. [12] The concept of the security is determined in this case. The WSN when comes in Check with the number of different types of users the security of the WSN is sacrificed. The distinct security issues and there rectifications are determined in this case. The infected nodes are handled in this case. [13] In the suggested technique range free pseudo code is determined. In this case the course information is derived on the basis of range free pseudo code. The range free pseudo code is free of the distance. Also the cost assigned with the pseudo code is low. [14] The concept of the security is determined in this case. The WSN when comes in Check with the number of different types of users the security of the WSN is sacrificed. The distinct security issues and there rectifications are determined in this case. The infected nodes are handled in this case. [15] 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. [15] 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) attacks and defenses, 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. [16] 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. The concept of energy management is determined 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 [16] 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. [16] 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. [17] in the suggested technique range free pseudo code is determined. In this case the course information is derived on the basis of range free pseudo code. The range free pseudo code is free of the distance. Also the cost assigned with the pseudo code is low.

IV. COMPARISON OF DISTINCT PSEUDO CODES

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

Table 1: Showing the Comparison of different pseudo codes used to detect NCA

PARAMETERS	APIT without attack	APIT with attack	APIT 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
Infected Nodes Detected	Low	Medium	High

Apit And Localization Pseudo Code

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

© 2016, IJARCSSE All Rights Reserved

1) Unknown node and compute nodes each beacon minimum hops.

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 APIT pseudo code.

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

Here D is the original average hop distance d_{ab} 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 APIT pseudo code 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 assigned 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 infected node. Hence the security will be enhanced. Also the localization error is reduced. The proposed pseudo code is as follows

APIT WITH RANDOM KEY

a) Generate random Ids for the nodes.
b) Assign the Ids to the nodes.
c) Detect the infected Entry
d) If Infected(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 pseudo code 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 infected 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 pseudo code.

V. RESULTS

The APIT without the Node capture attack will work with minimal localization error. The result from the simulation is as shown below

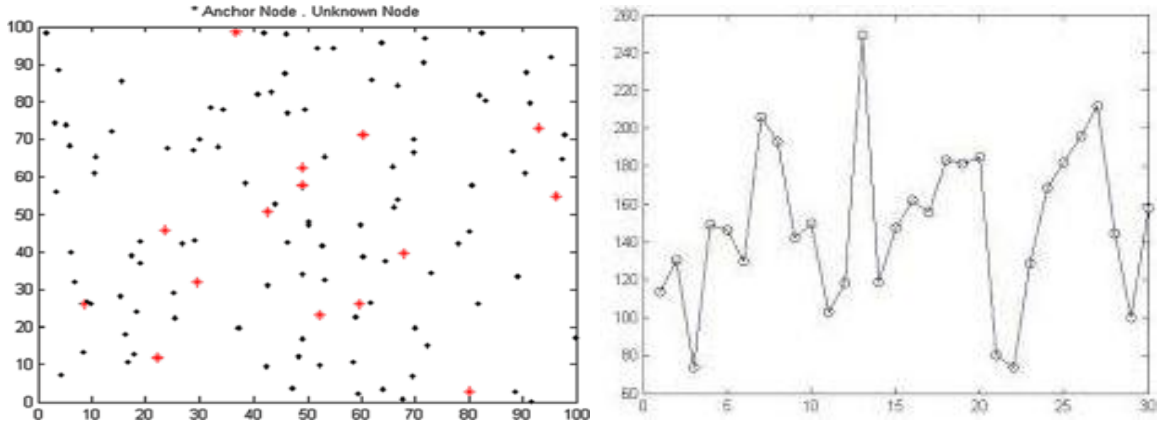


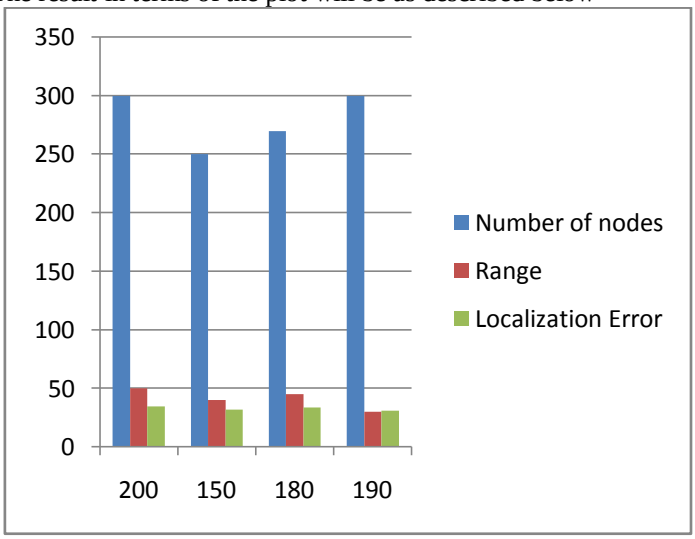
Fig 3: Showing the localization without the node capture attack

© 2016, IJARCSSE All Rights Reserved

Table1: Showing the localization without the node capture attack

Distance	Number of nodes	Range	Localization Error
200	300	50	34.689
150	250	40	32.0987
180	270	45	33.564
190	300	30	30.879
250	310	35	34.1232

In the table above we take 200m distance between anchor and unknown nodes .The number of nodes taken is 300 and the sensing capacity of sensor is in range 0-50. It shows the localization errors between the nodes without node capture attack is 33.07078. The result in terms of the plot will be as described below



The APIT pseudo code with node capture attack is shown through the following simulation

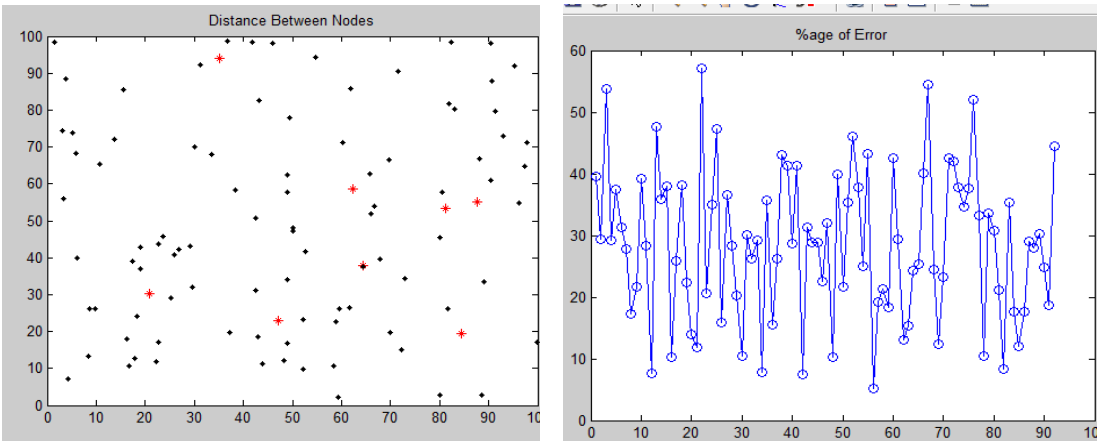


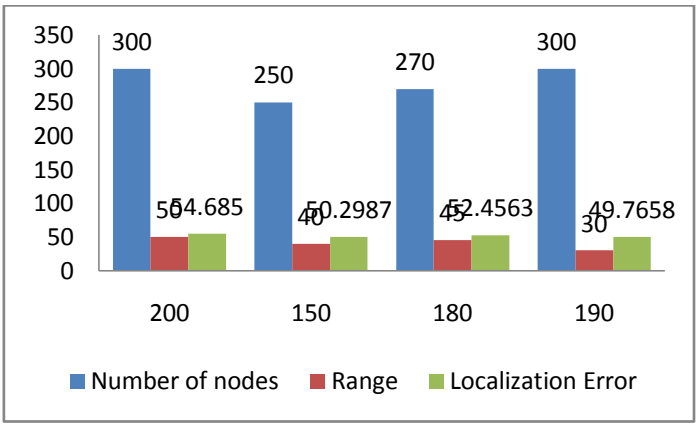
Fig 4(a) Showing the anchor and Unknown nodes with Node capture attack. Fig 4(b) Shows the localization error in case of Existing system

Table2. Shows the localization error in case of Existing system

Distance	Number of nodes	Range	Localization Error
200	300	50	54.685
150	250	40	50.2987
180	270	45	52.4563
190	300	30	49.7658
250	310	35	51.9876

In the table above we take 200m distance between anchor and unknown nodes .The number of nodes taken is 300 and the sensing capacity of sensor is in range 35-50. It shows the localization errors between the nodes in case of existing system is 51.83868. The result in terms of the plot will be as follows

© 2016, IJARCSSE All Rights Reserved



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

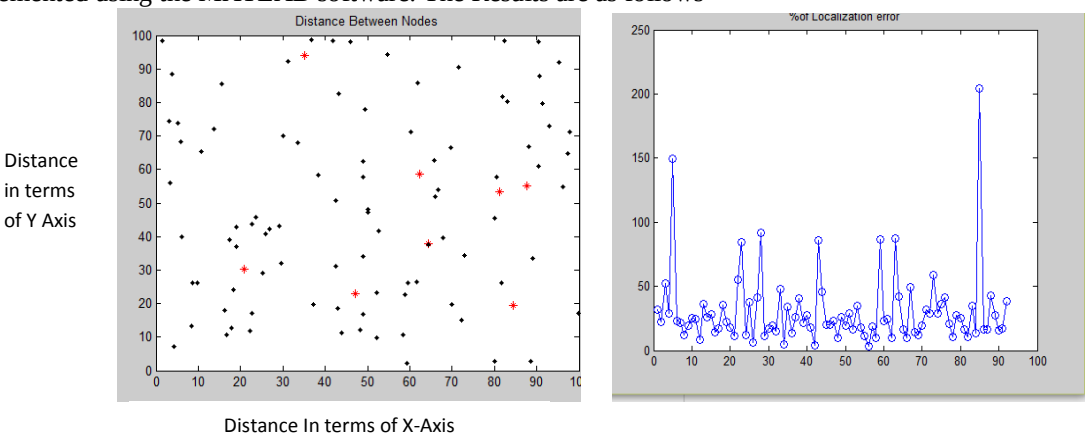


Fig 5(a): Showing the Position of the anchor and unknown nodes. Fig 5(b) Describing the Localization error that appears within the system

Table3.Localization error that appears within the system

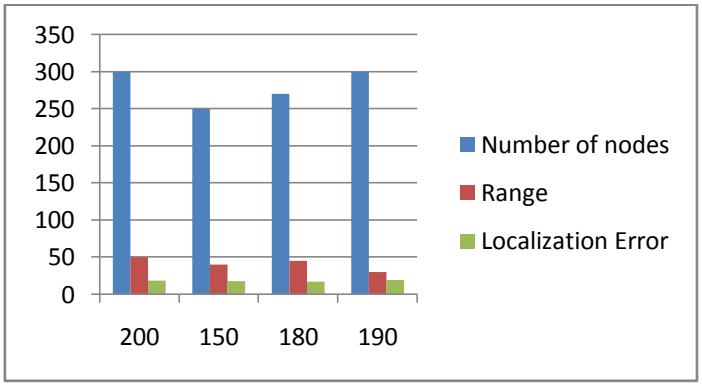
Distance	Number of nodes	Range	Localization Error
200	300	50	18.628
150	250	40	17.768
180	270	45	17.123
190	300	30	19.456

In the table above we take 200m distance between anchor and unknown nodes .The number of nodes taken is 300 and the sensing capacity of sensor is in range 35-50. It shows the localization errors between the nodes that appears within the system is 18.628.

The fig 5(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 5(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.

The result in terms of the Table 3 is as follows



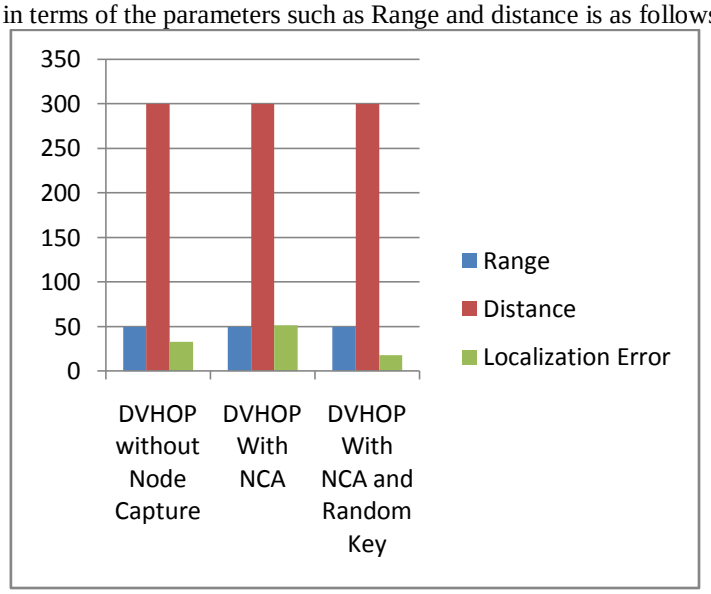
© 2016, IJARCSSE All Rights Reserved

The comparison between the distinct methods implemented in the proposed technique will be as follows

Table 4: Showing the comparison between the techniques implemented

	Range	Distance	Localization Error
APIT without Node Capture	50	300	33.070
APIT With NCA	50	300	51.786
APIT With NCA and Random Key	50	300	18.0923

The performance chart in terms of the parameters such as Range and distance is as follows



Localization Error is significantly reduced by the use of proposed technology. The comparison table indicates the performance of the proposed system.

The localization error in case of existing system is 31.0345 and in case of proposed system is 18.0923.

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

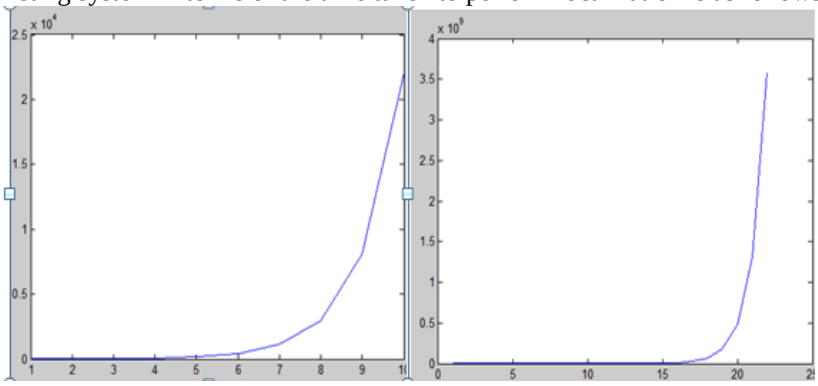


Fig 3: showing the time consumption which is 11ms in case of proposed system and 20 ms in case of existing system.

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

VI. 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 pseudo code. Ids to the nodes will be randomly assigned and hence difficult to detect by the infected 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.

© 2016, IJARCSSE All Rights Reserved

[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. Retrievedfrom 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

© 2016, IJARCSSE All Rights Reserved