INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

SECURE AND ENERGY EFFICIENT SENSOR LOCALIZATION SCHEME USING CLUSTERING MECHANISM

[1]Shanthi M B & [2]Ashwini Basavaradder

[1]Dept. of Computer science & Engg. CMRIT, Bangalore, India
[2]Visvesvaraya Technological University, Bangalore, India
E-Mail: ashwinisb92@gmail.com, shanthi.mb@cmrit.ac.in

Abstract - The location information in the wireless sensor networks is an important factor. All the nodes in the network have to collect the information and send it to the neighboring nodes. In the localization scheme the regular nodes will collect the location information from the beacon nodes and then identify their position in an untrusted environment. The security and accuracy becomes essential factor. Using reputation value of each node location can be found. The reputation is an unique value each node will have, based on that the nodes will calculate the location information. The reputation needs all the nodes to be involved in transmission of information. The node information will be stored in a trace file along with energy level. The clustering mechanism is used where the nodes will form a cluster and all the nodes elect cluster head and gets localized with that particular cluster by sending acknowledgment. The cluster heads will send the packet to the other cluster head. Security can be provided to the network using RSA algorithm. The lifetime of the network and the performance can be increased by using reputation model with the clustering mechanism. The security and performance of the network will get increased and packet drop will get reduced.

Keywords -component; Reputation model, Intrusion detection system, clustering mechanism.

I. INTRODUCTION

The wireless sensors networks are commonly in most of the wireless communication technologies.WSN are commonly used in many applications like agriculture, defense, military etc. In all this applications the sensor nodes are used to collect the information about temperature, water pressure, humidity etc. Depending upon the applications researchers will use different technologies. Most of the sensor nodes are used in underwater detection, smart home scenarios etc. Along with all this applications we need to find out the geographical location of the sensor nodes. The location of the nodes depends on the availability of the nods. The location information can be found by various formalities like 1) geographical routing and 2) location based routing. Sensor nodes are used to collect physical data, such as temperature, pressure, water level, wind speed, humidity, that are sent along with the location information to the data center to ensure that the collected data have spatial meaning. The location of the sensor nodes is an important factor in WSN.

In the current algorithms for sensor localization fall into two categories: range-free for a certain range in the given network. Range should be fixed. The security can be provided using RSA algorithm. And performance can be increased. . The location of the sensor nodes is an important factor in WSN. The location of the nodes depends on the availability of the nods. Algorithms and range-based algorithms. In range-free algorithms, such as centroid or CTDV-hop, a node estimates its location using information of connectivity between different nodes. In a range-based algorithm, a sensor nodes estimates its own location based on information about distance or angle between sensor nodes and by using technique such as time of arrival (TOA), time difference of arrival (TDOA), received signal strength indicator (RSSI), and angle of arrival (AOA) as well as methods such as trilateration, triangulation, or maximum likelihood estimation. Among many sensor localization algorithms, RSSI-based positioning technology is perhaps the most popular due to its low cost and easy implementation. On the other hand sensor localization result can be greatly affected by malicious nodes in hostile or untrusted environments. This is because the sensor nodes can hardly perform accurate localization if they use location information that is provided by untrusted beacon nodes. Security in sensor localization has thus received a great deal of attention along with the development of sensor localization technologies for WSNs

In the past few years, researchers have proposed several security strategies for sensor localization from different aspects. Some of the methods implementation verification measures to reduce the impact of using unreliable or false location information while some others apply a series of schemes in which temporal, spatial, and consistent properties are considered to deal with distance-consistent spoofing attacks. But in these schemes sensor nodes are divided just into two types secure and insecure sensor nodes through the mechanisms of comparing the nodes and their behavior against the normal situation. However, such an approach cannot be very objective, which could cause many false positive and false negative results. Clustering mechanism can be used .The sensor node localization is an essential feature. The location of the nodes depends on the accuracy of the information provided by the beacon nodes. So the beacon node information should be accurate. So to provide more accurate location of the nodes reputation model is introduced. Here each node will be having a reputation value based on that the sensor nodes will identify their position. But it will lead to many problems like space in the network and life time of the network is less. Many algorithms are there to get the location of the information. In the current existing method the localization depends upon the information provided by the beacon nodes to the regular nodes.

The localization is a process which is used to identify the location of the sensor node in an untrusted environment. All the nodes must be localized in a network. It is a method of identifying the node position in a network

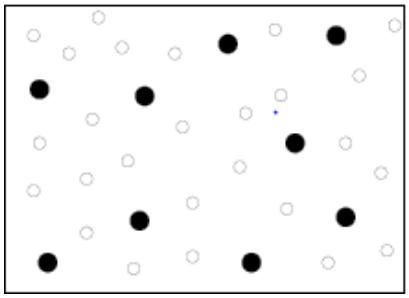

Figure 1: Localization Scheme

The reputation model is to get the location of the sensor nodes. Here each node will be having a reputation value based on that the regular nodes will find out the location. So we are grouping the nodes into cluster and each cluster will have cluster head. So all the cluster heads will communicate with each other and transmit the information. And here we can reduce the network delay and network overhead and also we can increase the network lifetime. And effectively the packet drop can be reduced and the nodes will get the better location in an accurate way using reputation value. All the sensor localization schemes developed based on this reputation model. So that we can provide more accuracy and security to the location information. In the reputation model all the beacon nodes evaluate their node position based on the model and then send their value to the regular nodes. The regular nodes will take the information from the highly reputed beacon node. Then by using that location information regular nodes will identify their position accurately. We can also perform some simulation experiments to demonstrate the effectiveness of reputation-based security scheme. Since we will get the accurate location of the nodes and security can be increased by this reputation model.

II. RELATED WORK

The sensor localization is an important factor. The localization scheme can be classified into 2 types: 1) range based algorithm 2) range free algorithm. In a range free algorithm, a node estimates its connectivity between the different nodes. In a range based algorithm, a sensor node estimates its own location based on information about distance or angles between the sensor nodes and through different technologies like TOA, TDOA, RSSI, and AOA. Some of the methods are used to reduce the impact of using false location information. Other properties are used to identify the different attacks. Some others researchers have proposed localization methods that are able to fight against attacks launched by compromised sensor nodes, a problem that is more difficult to deal with. Liu et al. proposed robust computing algorithms to improve the reliability of localization schemes. Park and shine proposed an attack-tolerant localization protocol that would perform adaptive management of a profile for normal localization behavior. However, the limitation of these schemes is that they did not consider the security of sensor localization when these sensor nodes are joining or living the network along with the passage of time. In addition, they did not pay enough attention to secure sensor localization in dynamitic wireless networks

E. F. Golen, B. Yuan, and N. Shenoy [1] Sensor networks are generally used to monitor the areas of the ocean, a part of military installation. To solve this problem we have 6 parameters they are sensing range, communication range, sensor and deployment cost, link redundancy, range dependence of the environment, probabilistic visitation. It is used to create highly effective field and sensing area.

M.Boushaba, A.Hafid and A.Benslimane[2] The network uses a large number of network to communicate with each other and to provide accurate results. Sensor location can be estimated using hardware called GPS (Global Positioning System). The sensor location in an GPS is based on the position of the nodes in a network. In this localization scheme the distance is estimated based on the RSSI (Received Signal Strength Indicator) and by using many different techniques like AOA, TDOA. Jaun carlos[8] The technique we are going to make use of Rule Based Inference methodology using evidential reasoning. Intelligent monitoring is required to fully exploit the potential of this supported environment. The smart home provides the potential to use preventive and assistive techniques to vulnerable sectors of the smart home city. The system allows for the specification of the uncertainty both in terms of knowledge representation and we can achieve the evidential conclusion.

Shabnum Sholey [4] In target tracking most commonly used method is clustering. The target tracking may cause due to node failure, network failure etc. Recovery method is to to recover from all these location based problems. EBSOTI protocol is used to recover from all the errors. It reduces the number of packet loss in the transmission. Energy consumption needs clustering mechanism. Target tracing is the main factor in wireless sensor networks. Different protocols have been implemented to provide more security to the localization scheme. Protocol is nothing but a set of rules for systematic communication over the network. The localization process follow some actions to perform and het the accurate location.

J.C Augusto, H.Wang [5] the smart home provides assistive and preventive technique for the vulnerable sectors of the population. Much of the researchers and developers focused on the technological side and less effort on the cost side. It is based on the condition-action rule together with a new inference of the intellectual monitor situation. A reasoning system called as RIMER is used to control the situation and to perform some actions. Many actions are taken up to solve the uncertainty in the network.

M.Boushe [12] In this localization method a new technique called as HA-A2L (high accuracy-location based angle to land mark) it has many protocols that exchanges the information and the protocols consist of set of rules required for the communication to takes place. And also we can estimate the distance between the nodes in the network relative distance between the nodes.

III PROPOSED SYSTEM

In the untrusted network the regular nodes should be secured with the location information. For providing the security reputation model has been introduced. Reliability of location information is increased in sensor localization scheme. The accuracy of the location information depends on the accuracy of the information provided by the beacon nodes. In the existing reputation based sensor localization method we can improve the security of the sensor nodes. In this method each beacon node is evaluated based on the reputation mode. Then the evaluation result is sent to the regular nodes. The regular nodes will collect the location information from the beacon nodes and identify their position. First will discuss about network model, threat model and then the reputation model.

Network model: WSN is composed of regular nodes and the beacon nodes. Beacon nodes are capable of positioning themselves. Regular nodes need to locate their own position based on the information provided by the

beacon nodes. The regular nodes estimate their position based on their information provided by the beacon nodes and then compute the distance between them using received signal strength formula. Then the nodes will estimate their position using information from the highly reputed beacon node.

Threat model: The analysis of the network model indicates that the position information received from the beacon nodes and estimates the relative position and determines the accuracy of the sensor localization.

Reputation Model: This model is used to deal with the potential threats that result from the above 2 types of attacks to improve the accuracy. In the sensor localization scheme, the regular nodes should get accurate location information. The security and the accuracy of the information should be maintained. In order to achieve some goals we need to concentrate on resource constraints in the sensor nodes. The reputation model is mainly to deal with all the security threats. Beacon nodes valuate using each other using information such as the characteristics about the perception of positions and provide the evaluation result to the regular nodes. Each node will be having its own reputation values it is based on the information provided by the beacon node. The reputation value for each and every beacon node is a number between 0 and 1.Indicating the values from higher level to lower level. The value will be stored in an trace file and each node will be having its own value stored in an trace file. The nodes will form a cluster and elect the cluster head and transmit the packets.

Clustering: In this mechanism the nodes will form a cluster. And all the nodes within a cluster will elect the header that is cluster head. The nodes in the cluster have to send an acknowledgement once they get localized to that particular area. Malicious nodes can be identified if the nodes did not send any acknowledgment then is malicious or infected nodes. Clustering makes the data transmission easier. All the nodes need not to involve in the data transmission only cluster head will transfer the data to the other cluster head. Energy can be saved using this mechanism. Only the cluster head will involve in the communication so the node energy can be saved. Several clustering methods are there to reduce the network overhead. The localization scheme uses the clustering mechanism by considering the energy level of the nodes. The nodes are localizes if they send acknowledgement to the cluster head

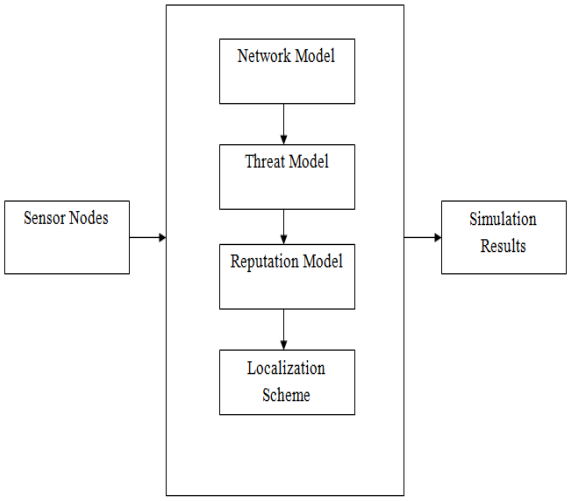

Figure 2: System Architecture

Localization Scheme: The RSSI ranging technology for sensor localization although the same reputation scheme can be applied equally to TOA, TDOA, and AOA ranging methods in practical applications. After receiving the evaluation results, a regular sensor node will select credible beacon nodes based on the reputation values. Afterwards, the sensor node will measure the distance to the credible beacon nodes using the RSSI ranging technology and estimate its location through maximum likelihood estimation..Here we check for the node localization in an accurate way. Finally the result will be sent to the simulation part.

Advantages of proposed system:

- More number of malicious beacon nodes on the localization of regular nodes can be detected.
- The accuracy and the security of the sensor localization can be improved in the untrusted environment.
- The effect of false location information can be minimized.

The use of mobile beacon nodes assists the nodes of a WSN in estimating their position. A mobile beacon is a node that is aware of it position and has the ability to move around the sensor field. The mobile beacon nodes travel through the sensor field broadcasting messages that contain its current coordinates. When a free node receives more than 3 messages from the mobile beacon it computes it position, based on the RSSI (Received signal strength indicator) method.

IV. IMPLEMENTATION

The reputation model has some disadvantages so to overcome from that we are making use of energy Clustering mechanism is used with the reputation to provide more security to the network and also it increases the performance of the network and delay will be reduced. The clustering model has number of nodes in a network. The clustering involves grouping the nodes into a network and electing a cluster head and cluster head will communicate in information transmission. The node having higher priority that will be elected as a cluster head. By using this mechanism in the localization scheme we can save the node energy and also we can improve the network lifetime and performance.

Technology Used

NS2 uses 2 languages OTcl and C++. OTcl is an object oriented language and c++ is an extended version of c language. The NS2 uses TCL scripting language. It has some features like, it increases the efficiency of the network

V. RESULTS AND PERFORMANCE ANALYSIS

The main aim of this project is to identify the node position in the untrusted environment. The clustering mechanism is used where the nodes will elect the cluster head and all the nodes in a cluster have to send an acknowledgement to the cluster head. If the node sends TRUE then they are localized to that particular cluster. If the node sends FALSE then they are not localized means they are malicious nodes. To provide security RSA algorithm has been implemented. The network should be scalable and dynamic enough to manage the nodes.

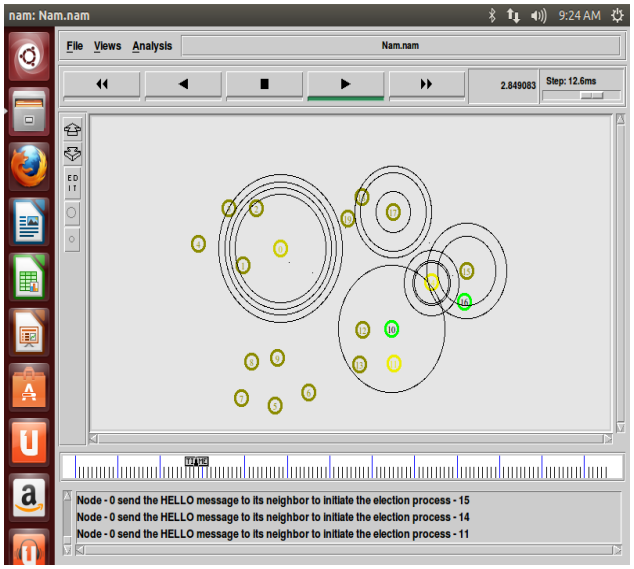

Figure 3: Sending Hello message

In the clustering mechanism the node will communicate with each other by using cluster head and transmit the packets. We have to initialize the communication by sending a message. It is used to initiate the communication between the nodes in a network in secured way.

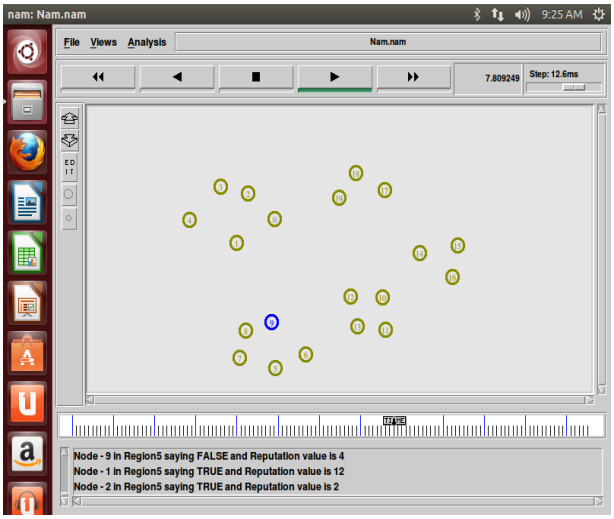

Figure 4: Sending Acknowledgement

In the above figure, the nodes will form a cluster having some nodes. The nodes will elect the cluster head and all the nodes have to send the acknowledgement to the cluster head and that nodes are localized within that particular area. The nodes will send TRUE if they are localized to that particular area. Or else nodes will send FALSE if they are malicious nodes. The cluster nodes will communicate with other cluster head within some communication range. The nodes which are belongs to that cluster are localized to that particular area.

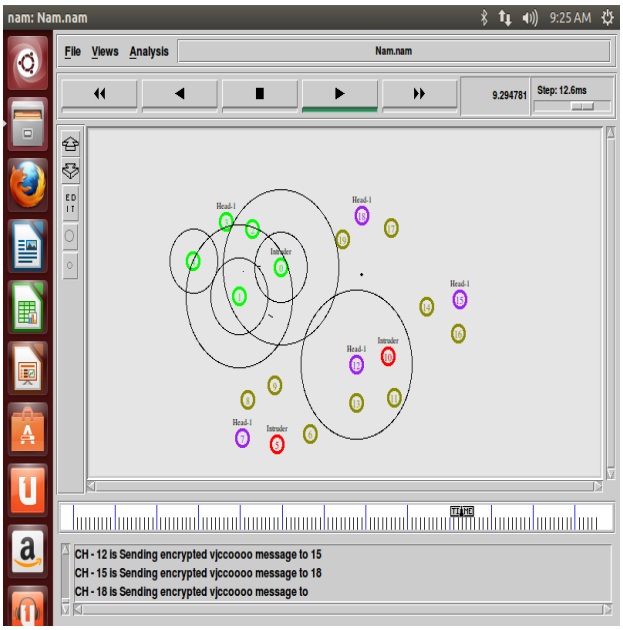

Figure 5: Encrypted Message

As shown in the above NAM window, all the nodes have to send an acknowledgement message to the cluster head. To provide better security RSA algorithm has been implemented. It uses public key for encryption and private key for decryption. It gives more security to the network and also secure packet transmission. The message is encrypted

with the public key at the sender and it is decrypted with the private key at the receiver side. Since the network becomes more secure and reliable for communication.

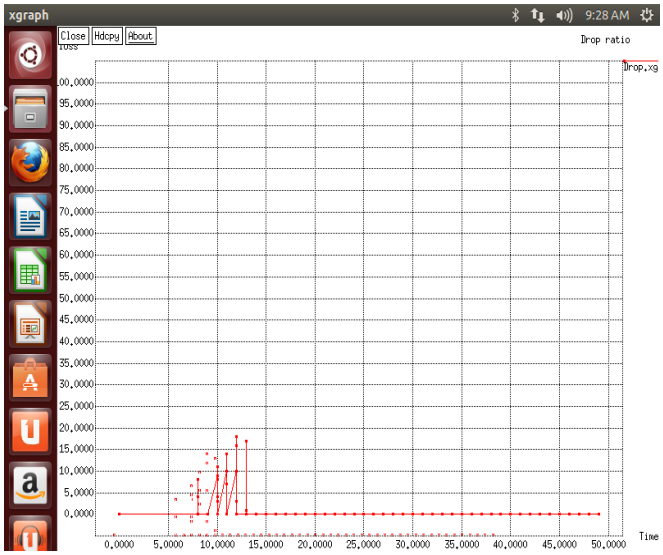

Figure 6: Drop Ratio

As shown in the above graph, drop ratio is nothing but number of packets lost during the transmission. It is also called as packet loss. The drop ratio can be calculated using number of packets sent to the number of packets received. Some malicious nodes will effect on packet transmission at that time the data may loss and drop ratio may get increases. If the drop ratio gets increases then network performance will decrease and delay will increase.

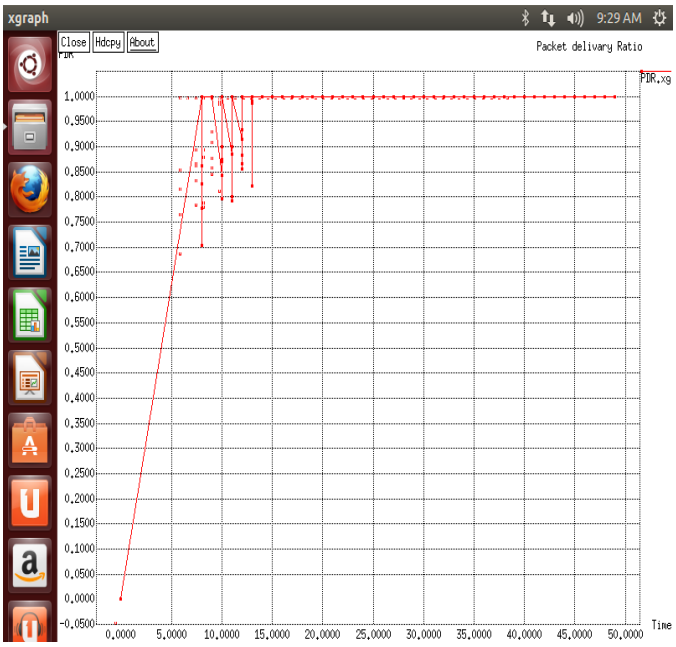

Figure 7: Packet Delivery Ratio

The packet delivery ratio is the total number of packets sent to the total number of packets received by the receiver. Some packets may or may not loss during the transmission. The packet delivery ratio will becomes 1 if all the packets are received properly by the receiver. Orelse it will be less than 1. If the graph reaches constant value then all the packets will transmit succcessfully without loss.

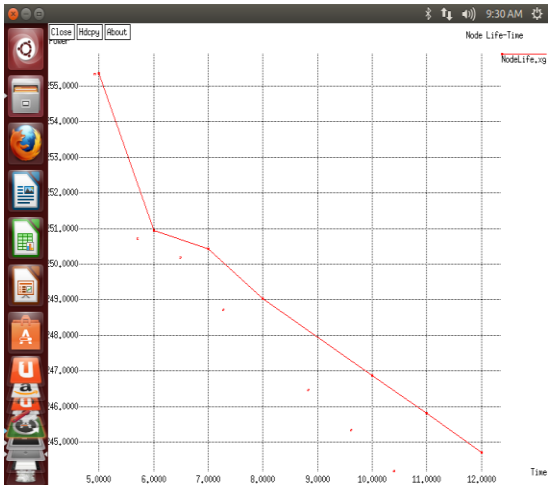

Figure 8: Node Lifetime In a network

The nodes in the network have to communicate with the other nodes since the lifetime of the network should be high. So that it can be able to accommodate large number of nodes. By giving more security to the network we can enhance the lifetime. RSA algorithm is implemented to provide better security.

VI. CONCLUSION

In the proposed secure and energy efficient sensor localization process clustering concept is used. It mainly reduces the network delay in and increases the node performance in the network. The localization process becomes very powerful in the wireless sensor networks using the reputation value of the nodes. The network becomes so secure because RSA algorithm is used for security purpose. The public key is used while encrypting the message and while decrypting private key is used. The nodes in the cluster has to elect cluster head and all the nodes has to send TRUE value if they are localized otherwise they will send FALSE. The malicious nodes can be detected in the cluster nodes. Energy efficiency will be more in the cluster based sensor localization process. The sensor localization using energy efficient clustering gives the better accurate secure sensor node localization in the network

REFERENCES

[1] E. F. Golen, B. Yuan, and N. Shenoy “An evolutionary approach to understand sensor deployment” vol. 2, no.10, pp.184-201, 2009

[2] M. Boushaba, A.Hafid and A.Benslimane, “High accuracy localization method using AoA in sensor networks” vol. 4, no 4.pp. 371-378, 2008

[3] Jaun carlos “Management of uncertainty and spatiotemporal aspects for monitoring diagnosis in a smart home,” Vol.1, No. 4 (December, 2008), 361-378

[4] Shabnum Sholey “An efficient protocol for target tracking in wireless sensor networks.” Vol. 2, Issue 5, No.6 , November 2013 ISSN : 2322-5157

[5] M.Boushe “High accuracy localization method using AOA in sensor network” vol. 53 no-18 pp. 3076-3088,2009

[6] N.Bulusu and D.Estern "GPS less low cost outdoor localization for small sensor devices" vol-87, October 2004.

[7] D.Niculuscus "Ad HOC positioning system using AOA" in proceeding of IEEE INFOCOM , 2003

[8] T. He *et al.*, "Range-Free Localization Schemes for Large Scale Sensor Networks," *MobiCom '03*, ACM Press, 2003, pp. 81-95.

[9] Y. Fu *et al.*, "The Localization of Wireless Sensor Network Nodes Based on DSSS," *Electro/Infor. Tech., 2006 IEEE Int'l. Conf.*, 2006, pp. 465–69.

[10] V. Ramadurai and M. L. Sichitiu, "Localization in Wireless Sensor Networks: A Probabilistic Approach," *Proc. ICWN 2003*, Las Vegas, NV, June 2003, pp. 275–81.

[11] S. Capkun, M. Hamdi, and J.-P. Hubaux, "GPS-Free Positioning in Mobile Ad Hoc Networks," *Cluster Computing*,vol. 5, no. 2, 2002, pp. 157–67

[12] M. L. Sichitiu and V. Ramadurai, "Localization of Wireless Sensor Networks with A Mobile Beacon," *Proc. 1st IEEE Int'l. Conf. Mobile Ad Hoc and Sensor Sys.*, FL, Oct. 2004, pp. 174–83

[13] B. Karp and H. T. Kung, GPSR: Greedy Perimeter Stateless Routing for Wireless Networks, In *Proceedings of MOBICOM '00*, New York, August 2000.

[14] B. H. Wellenhoff, H. Lichtenegger and J. Collins, *Global Positions System: Theory and Practice*, Fourth Edition. Springer Verlag, 2007.

[15] N. Bulusu, J. Heidemann and D. Estrin, Density Adaptive Algorithms for Beacon Placement in Wireless Sensor Networks, In *IEEE ICDCS '01*, Phoenix, AZ, April 2001.