ISSN: 0976-3104
SPECIAL ISSUE: Computer Science

ARTICLE

SECURE MOBILE BEACON BASED OBSTACLE AWARENESS IN WSN

S Velmurugan[1*] and E Logashanmugam[2]

[1]Department of Electronics and Communication Engineering, St. Peter's University, Chennai, INDIA
[2]Department of Electronics and Communication Engineering, Sathyabama University, Chennai, INDIA

ABSTRACT

Localization technology is mainly important to most applications of wireless sensor networks (WSNs). In WSN, Beacon node is send location information to the sensor node. But the obstacle presented environment cannot reach the location information. To overcome this problem, we propose Secure Mobile Beacon based Obstacle Awareness in Wireless Sensor Networks (SMBOA). In this scheme, the mobile Beacon is identified the obstacle present place and send the location information to the sensor nodes. The mobile beacon is verified based on the ID based signature scheme. The authorized mobile beacon sends original sensor location hence secure data transmission in WSN. The simulation result demonstrates that the SMBOA improve the throughput and diminish both the packet loss rate and delay. It also reduces the energy consumption and improves the lifetime of the network.

KEY WORDS
Localization, Security, Obstacle, Mobile Beacon, Wireless Sensor Networks.

Received: 18 Nov 2016
Accepted: 28 Dec 2016
Published: 5 January 2017

***Corresponding Author**
Email: velmuruganstpeters@gmail.com

INTRODUCTION

Localization is critical for several wireless sensor networking applications, including critical infrastructure protection, habitat monitoring, and target tracking. Additionally, location information employs an important part in bounding energy utilization in WSNs. Global Positioning System (GPS) is a usually used and specific method for sensor localization. Regrettably, the GPS method is neither expensive nor energy-efficient. The deployment capability of sensor nodes which are equipped with GPS may be reduced due to the increased size. Also, these GPS equipped sensors have inadequate applicability since GPS works only in an open field. Localization algorithms can handle with the difficulty where they are capable to deduce the location of sensors by using the information of the fixed positions of a few sensors. Usually, these small sizes of sensor nodes with recognized location information are called beacon. WSNs are usually applied for missions where human being process is not possible. Therefore, installing beacon nodes in a preset location is frequently infeasible. The beacon message broadcast the location is unworkable due to the obstacle. Also the precision of the localization raises the number of beacons, cost and energy utilization. Regarding to solve the above mentioned problem we using a mobile beacon can be working as an option solution to localize the whole network. Localization through the use of a mobile beacon is essentially more accurate.

The rest of the paper is ordered as follows: Section 2 summarizes the presented localization methods for mobile beacon and sensors. The secure Mobile Beacon based Obstacle Awareness method in Section 3. The simulation results are described in Section 4 followed by the conclusions in Section 5.

Related work

Exploiting Routing information [1] proposed solves the localization and data routing troubles in WSNs. The system is separated into 1-hop cluster and the localization is hierarchically performed inside each cluster, next among clusters. The benefit of the scheme is that no extra message is necessary to make localization, which is received by a ranging technique, exploiting network topology supplied by the routing algorithm. Clustering based Robust Localization (CluRoL) approach proposed to recognize the malicious anchors and reject them from the localization process. CluRoL explained the bound circle of an anchor with respect to an sensor as the circle whose center is at the anchor and whose radius is the estimation of the distance between the anchor and the sensor. A CluRoL approach helps each Sensor to localize itself perfectly, using a clustering mechanism that executes clustering of these proximal points. A Clustering Algorithm for Localization in WSNs (CFL) scheme [3] designing a localization algorithm based on clustering. This algorithm uses a combined weight function and tries to classify the sensor so that smallest number of clusters with highest number of nodes in each cluster could be achieved.

Cluster-Based Mechanism for Multiple Spoofing Attackers in WSN [4] to detecting spoofing attacks, determining the number of attackers when multiple adversaries masquerading as a same node identity; and localizing multiple adversaries. The spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. Cluster based mechanisms is developed to determine the number of attackers. Support Vector Machines method to improve the accuracy of determining the number of attackers. This algorithm provides strong evidence of high accuracy of localizing multiple adversaries. Cluster-based Localization Method [5] investigates the performance of cluster-based localization using received signal strength indicator (RSSI) used to develop a heterogeneous WSN consisting of inter connected body area networks, or clusters. This localization method is based on a cluster-based version of the Min- Max algorithm that eliminating the need to transmit a large number of localization request packets. This method improves the network's robustness and reliability and the safety of its users.

Cluster based Iterative GPS-Free Localization (CIGL) algorithm [6] depends upon the distances between the sensor nodes and their neighbors obtained by measurements like Time of Arrival (TOA). It selects a subset of nodes to establish Local Coordinate Systems (LCSs) on the basis of clustering results. All the LCSs converge to form the global coordinate system and complete the nodes localization in succession. The successfully located nodes are chosen as new beacons to re-locate the remaining unknown nodes, namely expand localization coverage by iteration. This algorithm achieves localization accuracy and coverage, the communication range is small and the network deployment is sparse. Trusted and Secure Clustering [7] analyzed impact of signal-strength attacks while cluster communication on trust degree and level of security. This scheme provides adaptation of trustworthy and secure communication where information is ubiquitous.

Secure and efficient voting-on-grid clustering (VoGC) scheme [8] proposed to diminish the malicious beacon signal. VoGC method to reduce the computational cost, localization accuracy and identify malicious beacon signals. Mobile beacon-assisted localization algorithm based on network-density clustering (MBL(ndc)) [9] combines node clustering, incremental localization and mobile beacon assisting together. MBL(ndc) algorithm offers localization accuracy and reduce path length. Geometric constraint-based localization method disadvantage is increasing location error with enlarging the communication range [10].

Mobile-beacon assisted localization method [11] utilizes the geometric relationship of the perpendicular intersection to compute node positions. The drawback of this method is expensive. Localization scheme for WSNs using mobile anchors with directional antennas approach [12] for locating static sensor nodes by means of mobile beacon nodes equipped with four directional antennas. The method is efficient where the sensor nodes have no specific hardware requirements. Probabilistic localization algorithm [13] based on a mobile beacon utilizes TOA technique for ranging and uses Centroid formula based on distance information to estimate nodes location.

Received Signal Strength (RSS) based Localization for WSNs [14] investigated the possibility of SN localization by exploiting the inherent property of the WSN technology, particularly the RSS of the exchanged message. The RSS can be used for outdoor localization under well-defined topology constraints.

METHOD

In this paper, we propose Secure Mobile Beacon based Obstacle Awareness in WSNs. In this scheme, the obstacle is identified and secure mobile beacon node (MBN) based obtains location information of sensor node (SN). WSN consists of number of SNs which are randomly disseminated among obstacle in the predetermined environment. In a WSN, the SNs usually localize themselves with the help of BN that know their own locations. In this network, the few BNs are preset the network and it broadcast the sensor node position occasionally.

The obstacles appear in the network field and block to BN transmit the location information of the SNs. While the obstacle presents in the data transmission path, the fixed BN broadcast the sensor localization information is cannot reached to the SNs. Therefore, these SNs send notification message to the Base Station (BS). BS obtains this message and it send (Route Request) RREQ message to the authorized MBN. This RREQ message contain sensor ID, node position. The MBN accepts this RREQ and sending that place and act as the BN. The MBN is able to discover an unknown obstacle is moving or fixed where it occupies within the communication range. If the obstacle is immovable the MBN will work permanently otherwise it will work until that obstacle is change the position in the network. [Fig. 1] shows the architecture of the proposed Scheme.

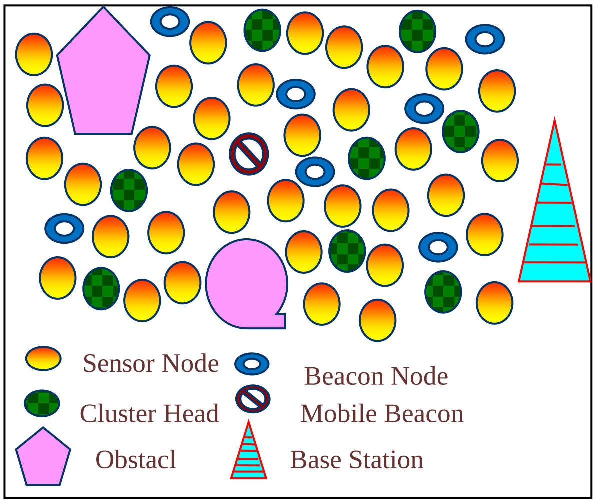

Fig. 1: Architecture of proposed scheme.

Mobile beacon node verification

The MBN received the message from BS and it going to the obstacle present place. Then the MBN send HELLO message to the obstacle near SNs. The SNs are received the HELLO message and checks this MBN is original or not. In this scheme, the MBN is verified based on ID based Signature method. It consists of three steps including Key setup, signature and verification.

- Key Setup: The BS computes a master key s and public parameters par for the Private Key Generation, and gives par to all sensor nodes.

A sensor node generates a private key R associated with the ID using the master key s.

- Signature: The mobile beacon generates a signature SIG based on the message M, time-stamp t and a signing` key.
- Verification: The SN checks the mobile beacon ID, M and SIG. If it match, the SN accept the MBN send the location information otherwise the SN reject the message.

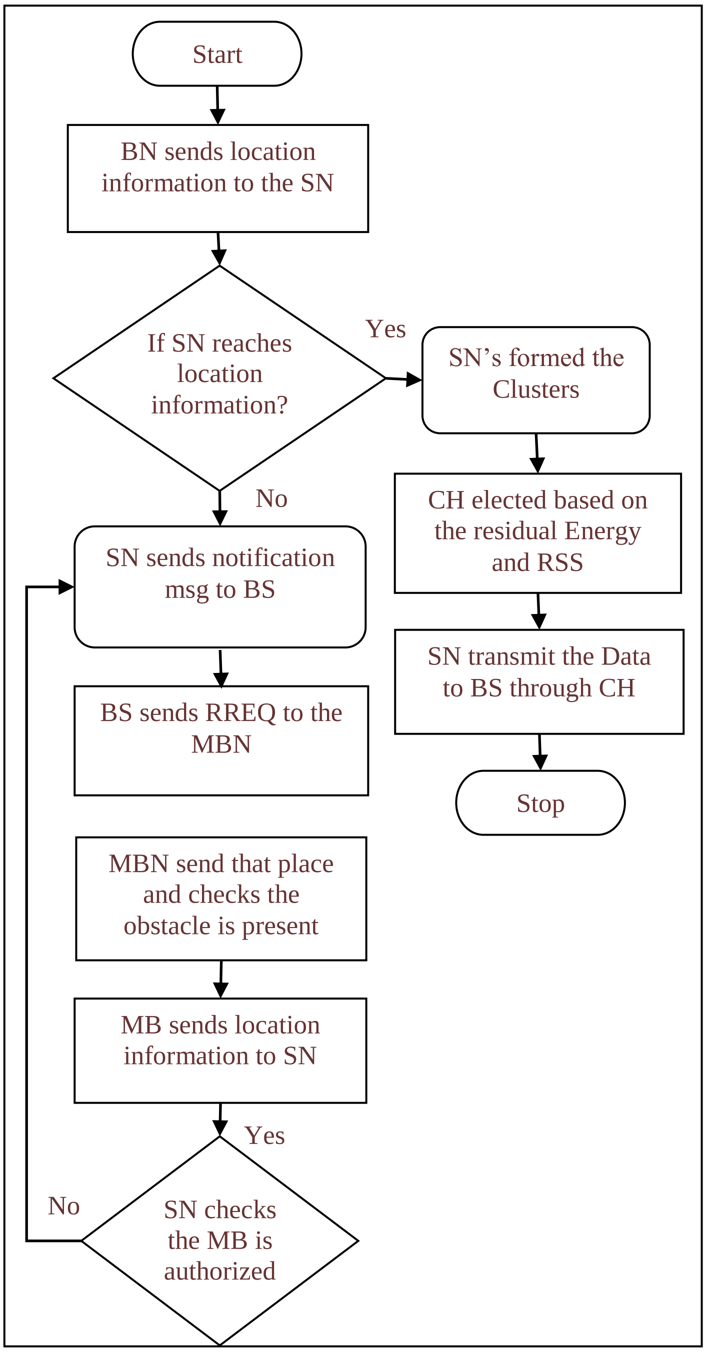
Start
BN sends location information to the SN
If SN reaches location information?
Yes
No
SN's formed the Clusters
CH elected based on the residual Energy and RSS
SN transmit the Data to BS through CH
Stop
SN sends notification msg to BS
BS sends RREQ to the MBN
MBN send that place and checks the obstacle is present
MB sends location information to SN
Yes
No
SN checks the MB is authorized

Fig. 2: Flowchart of SMBOA Scheme.

[Fig. 2] shows that the flowchart of the proposed scheme. The SNs are getting the location information from the BN or MBN and formed the clusters based on the coverage. Clustering is a standard approach for achieving efficient and scalable performance in WSNs. The sensor nodes are transmits the data through the cluster head. The Cluster Head (CH) is elected based on the highest residual energy and RSS. The SNs are transmits the data through the CH. This scheme used to reduce the energy consumption and improve the lifetime of the network.

Simulation analysis

The performance of the Secure Mobile Beacon based Obstacle Awareness in WSNs is examined by using the Network simulator (NS2). It is an open source programming language written in C++ and Object Oriented Tool Command Language. To estimate the proposed scheme we have assumed 65 sensor nodes, a network in an area of 1000x1500 m2. The parameters used for the simulation of the proposed scheme are tabulated in [Table 1]. Random waypoint mobility model is used to the sensor node movement. User Datagram Protocol (UDP) is used to node communication. We consider the packet delivery rate, packet loss rate, delay, residual energy are showing the efficiency of the proposed work.

Table 1: Simulation parameters of SMBOA

Parameter	Value
Number of nodes	63
Routing scheme	RSSL and SMBOA
Traffic model	Constant Bit Rate
Simulation Area	1000x1500 m^2
Channel	Wireless Channel
Transmission range	250m
Communication Protocol	UDP
Antenna	Omni Antenna

Packet delivery rate

Packet Delivery Rate (PDR) is the ratio of the total number of packets effectively delivered to the total packets sent. It is received from the equation (1) below.

$$PDR = \frac{Total\ Pkts\ Received}{Total\ Pkts\ Send} \qquad (1)$$

The [Fig. 3] shows the PDR of the proposed scheme SMBOA is higher than the PDR of the existing method RSSL. The greater value of PDR means better performance of the protocol.

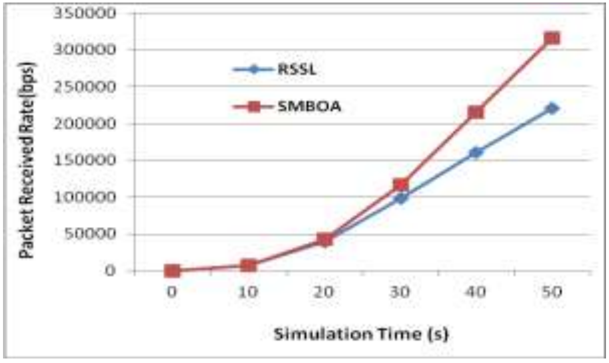

Fig. 3: Packet delivery rate of RSSL and SMBOA.

Packet loss rate

Packet Loss Rate (PLR) is the ratio of the packets lost to the total packets sent, estimated by the equation (2) below.

$$PLR = \frac{Total\ Pkts\ Dropped}{Total\ Pkts\ Send} \qquad (2)$$

The PLR of the proposed scheme SMBOA is lower than the existing scheme RSSL in [Fig. 4]. Lower the PLR indicates the higher performance of the network.

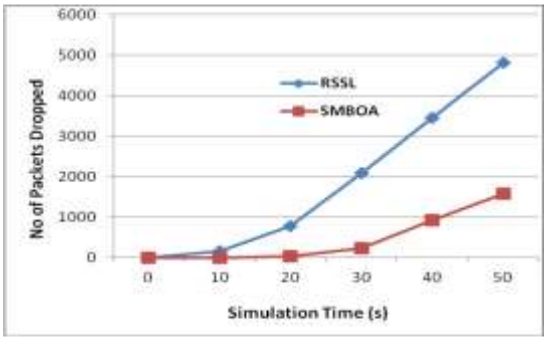

Fig. 4: Packet loss rate of RSSL and SMBOA.

Average delay

Delay is defined as the time difference between the current packets received and the previous packet received. Where n is the number of nodes.

$$Delay = \frac{\sum_{0}^{n} Pkt\, r\, e\, cvd\ time - Pkt\ send\ time}{n} \quad (3)$$

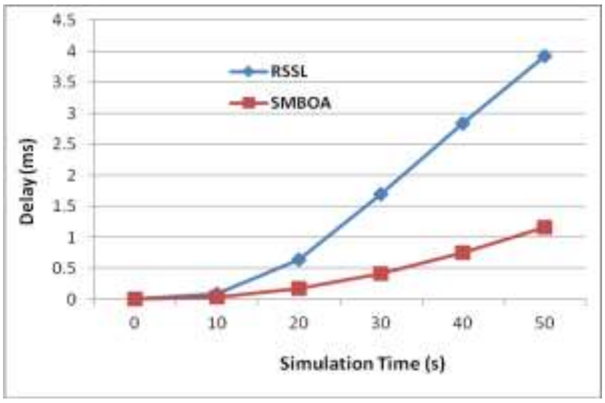

Fig. 5: Average delay of RSSL and SMBOA.

[[Fig. 5] demonstrates that the delay value is low for the proposed scheme SMBOA than the existing scheme RSSL. The minimum value of delay is improves the network performance.

Throughput

Throughput is defined as the rate at data is successfully transmitted for every packet sent.

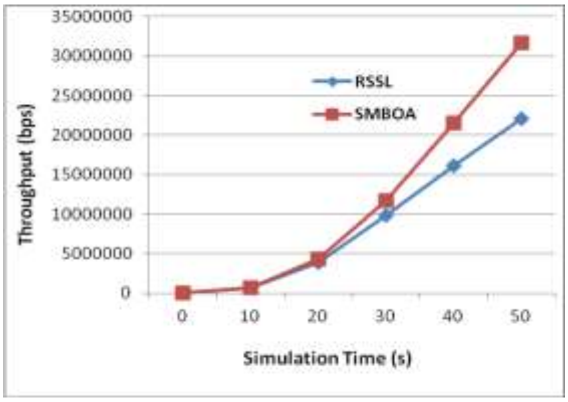

Fig. 6: Throughput of RSSL and SMBOA.

$$Throughput = \frac{\sum_0^n Pkts\, recvd\, (n) * Pkt\, size}{1000} \quad (4)$$

[Fig. 6] show that the proposed scheme SMBOA has greater average throughput when compared to the existing scheme RSSL.

Residual energy

The amount of energy remaining in a node at the current instance of time is called as residual energy. A measure of the residual energy gives the rate at which energy is consumed by the network operations.

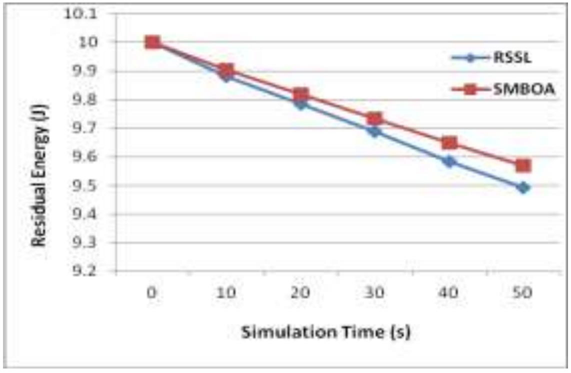

Fig. 7: Residual energy of RSSL and SMBOA.

[Fig. 7] shows that the residual energy of the network is better for the proposed scheme SMBOA when compared with the existing scheme RSSL.

CONCLUSION

Localization is important concept in WSN. In this paper we proposed Secure Mobile Beacon based Obstacle Awareness in WSNs. In SMBOA, the mobile beacon is sends the location information to the obstacle near sensor nodes. The ID based signature method is used to verify the mobile beacon. The clusters are formed based on the coverage. The Cluster Head is elected by Received Signal Strength and Residual Energy. The simulation result shows that the SMBOA improved the Packet delivery rate. It also reduces both the delay and energy consumption in the network.

CONFLICT OF INTEREST

There is no conflict of interest.

ACKNOWLEDGEMENTS

None

FINANCIAL DISCLOSURE

None

REFERENCES

[1] Oliva G, Panzieri S, Pascucci F, Setola R. [2013] Exploiting routing information in Wireless Sensor Networks localization. In Network Science Workshop (NSW), 66-73.

[2] Misra S, Xue G. [2007] CluRoL: Clustering based robust localization in wireless sensor networks. In MILCOM 2007-IEEE Military Communications Conference, 1-7.

[3] Zainalie S, Yaghmaee MH. [2008] CFL: A clustering algorithm for localization in wireless sensor networks. In Telecommunications, 2008. IST 2008. International Symposium on, 435-439.

[4] Meena T, Nishanthy M, Kamalanaban E. [2014] Cluster-based mechanism for multiple spoofing attackers in WSN. In Information Communication and Embedded Systems (ICICES), 2014 International Conference on, 1-5.

[5] Zhong C, Eliasson J, Makitaavola H, Zhang F. [2010, 2014] A cluster-based localization method using RSSI for heterogeneous wireless sensor networks. In 2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), 1-6.

[6] Chen R, Zhong Z, Ni M. [2011] Cluster based iterative GPS-free localization for wireless sensor networks. In Vehicular Technology Conference (VTC Spring), 1-5.

[7] Gaur MS, Pant B. Impact of Signal-Strength on Trusted and Secure Clustering in Mobile Pervasive Environment. Procedia Computer Science, 57:178-188.

[8] Yang W, Zhu WT. [2010] Voting-on-grid clustering for secure localization in wireless sensor networks. In Communications (ICC), 2010 IEEE International Conference on, 1-5.

[9] Yang W, Zhu WT. [2010] Voting-on-grid clustering for secure localization in wireless sensor networks. In Communications (ICC), 2010 IEEE International Conference on, 1-5.

[10] Lee S, Kim E, Kim C, Kim K. [2009] Localization with a mobile beacon based on geometric constraints in wireless sensor networks. IEEE Transactions on Wireless Communications, 8(12): 5801-5805.

[11] Guo Z, Guo Y, Hong F, Jin Z, He Y, Feng Y, Liu Y. [2010] Perpendicular intersection: locating wireless sensors with mobile beacon. IEEE Transactions on Vehicular Technology,

59(7): 3501-3509.

[12] Ou CH. [2011] A localization scheme for wireless sensor networks using mobile anchors with directional antennas. IEEE Sensors Journal, 11(7): 1607-1616.

[13] Sun GL, Guo W. [2004] Comparison of distributed localization algorithms for sensor network with a mobile beacon. In Networking, Sensing and Control, 2004 IEEE International Conference on, 536-540.

[14] Stoyanova T, Kerasiotis F, Antonopoulos C, Papadopoulos G. [2014] RSS-based localization for wireless sensor networks in practice. In Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2014 9th International Symposium on, 134-139.