Indian Journal of Science and Technology, *Vol 9(39), DOI: 10.17485/ijst/2016/v9i39/96039, October 2016*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Detecting and Replacing Beacon Node Failure and Secure Communication in WSNs (DRBF)

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

[1]Department of Electronics and Communication Engineering, St. Peter's University, Chennai - 600054, Tamil Nadu, India; velmuruganstpeters@gmail.com
[2]Department of Electronics and Communication Engineering, Sathyabama University, Chennai - 600119, Tamil Nadu, India

Abstract

Objective: The objective of this scheme is to improve the quality of service in WSNs. **Method:** In this paper, we propose Detecting and Replacing Beacon Node Failure (DRBF) and Secure Communication in WSNs. DRBF focus on Beacon Node Failure and reliable data transmission in WSNs. **Findings:** The beacon node fails due to resource, hardware failure or some other reasons whereas the Base Station (BS) replaces that beacon node by mobile user. This mobile user acts as the beacon nodes and updates the location information to the sensor nodes. The cryptography key technique provides secure data transmission to the network. **Improvement:** The DRBF reduces both the packet loss rate and delay, which are shown in the simulation results.

Keywords: Beacon Node, Clustering, Key Management, Localization, Mobile User, Security

1. Introduction

Advances in recent technology have made it likely to extend distributed sensor networks consisting of a large number of low powers, least-cost and multi-serviceable sensor nodes that communicate in short distances through wireless links. This distributed sensor networks has wide range of applications such as data acquisition in harmful environments, military operations and health monitoring. The appropriate features of distributed sensor networks have attracted many researchers to widen and develop protocols and algorithms that can accomplish the necessities of these applications. Sensor's locations play a critical role in many sensor network applications. A simple solution is to give each sensor with a GPS (Global Positioning System) receiver that can precisely supply the sensors with their exact location. However, in distributed sensor networks, the GPS is a very expensive tool and low production cost of node is one of most vital factors in WSN design. Thus, the number of network nodes that have this system should be low as possible. Therefore, it is only possible to fit a small portion of all sensor nodes with GPS receivers. These GPS enabled nodes called beacon nodes or anchors provide position information. Non-beacon nodes obtain the location information from nearby beacon nodes to estimate their own positions, thus reduce the high cost of GPS across many nodes.

Localization[1] based on QoS by using One Beacon method focus on low energy consumption for placing in WSNs. This protocol uses fuzzy logic and gives significance to different paths in order to improve the precision of routing and reduce the energy consumption. Anonymous Location[2] based Efficient Routing protocol (ALERT) energetically divides the network into zones and arbitrarily chooses nodes in zones as intermediate relay nodes. A non-traceable anonymous route was formed by using the intermediate relay nodes. ALERT protocol offers anonymity defense to sources, destinations and routes. It also has strategies to efficiently come across timing attacks. It

*Author for correspondence

accomplished with enhanced path anonymity protection, lower cost and routing efficiency.

Reliable Anchor based Localization (RAL)[3] method can reduce the localization error due to irregular deployment region. RAL scheme employs the reliable minimal hop length from the table as the threshold to differentiate between reliable anchors and unreliable ones and it allows each sensor to determine its position utilizing only distance constraints obtained from reliable anchors. RAL can effectively filter out unreliable anchors and therefore improve the localization accuracy. Secure Localization[4] and Location Verification provides authentication and key exchange protocol that trims down the overhead in node re-authentication and in turn facilitates interact-ability of localized nodes. It increased the lifetime of sensor network. Tree-Cluster-Based Data-Gathering Algorithm (TCBDGA)[5] introduced weight-based tree-construction method to reduce the energy consumption and prolong the network lifetime.

Regional Energy Aware Clustering[6] with Isolated Nodes (REAC-IN) proposed energy aware clustering method using isolated nodes for WSN. In REAC-IN, CHs are selected based on weight. Weight is determined according to the remaining energy of every sensor and the regional average energy of all sensors in each cluster. Improperly formed distributed clustering algorithms can cause nodes to become isolated from CHs. Such isolated nodes transmit the data to sink by consuming excess amount of energy. To prolong network lifetime, the regional average energy and the distance between sensors and the sink are used to determine whether the isolated node sends its data to a CH node in the previous round or to the sink. Location Estimation Scheme[7] using Connectivity method was proposed to evaluate the location of nodes in a sensor network. The nodes estimate their location based on neighborhood relationships. It improves the accuracy of location estimation as compared to only utilizing neighbor relationships.

Energy-aware[8] target detection and localization strategy for cluster-based WSNs had proposed based on a posteriori algorithm with a two-step communication protocol between the CH and the sensors within the cluster. The localization procedure executed by Cluster Head determines the subset of sensors that queried for detailed target information. This approach reduces both transmission bandwidth requirement and energy consumption and prolongs the lifetime of the WSN. Node-to-Node[9] Location verification scheme has the ability to achieve satisfactory performance via extensive real world Global-Positioning-System-based WSN. This location verification scheme is comprised of mainly two parts: Location estimation and location claim verification. In this approach, the node-to-node location estimation is based on distance and exploiting an encrypted location claim for authentication. Attack-Resistant Location Estimation[10] had used to endure malevolent attacks against beacon-based location discovery in WSNs. In this approach, the malicious beacon signals are first filtered based on the consistency among multiple beacon signals and then it tolerates malicious beacon signals by adopting an iteratively refined voting scheme.

The Collaborative Localization[11] and Location Verification scheme introduced the virtual force model to determine the location by incremental refinement. The drifting problem and malicious anchor problem were solved by using this method based on the virtual force mode. An anchor promotion algorithm using the localization reliability model is used to re-locate the drifted nodes. The localization algorithm has relatively high precision and the location verification algorithm has relatively high accuracy, low communication overhead and the localization methods is practical as well as comprehensive.

Secure Probabilistic Location Verification (PLV)[12] algorithm leverages the probabilistic depend on number of hops to transmit packet to reach a destination and the Euclidean distance between the source and the destination. The plausibility of the claimed location was determined by using some of the nodes that is represented by a real number among 0 and 1. It is feasible to create arbitrary number of trust levels in the claimed location. This solution provides high performance in face of various types of attacks. Beacon Less Location Discovery[13] proposed efficient location discovery WSNs without using beacons. In this method, the sensors can determine their locations by detecting the group memberships of its neighbors.

Secure Range-free Localization Scheme[14] introduced Wormhole-free DV-hop Localization scheme. This scheme contains two phases: Infection prevention and DV-Hop-based secure localization. The infection prevention was performed to remove the fake connections. In DV-Hop-based secure localization, the minimum hop-count value per beacon of all beacons messages received was maintained by each and every receiving node. However, this scheme does not detect the beacon node failure.

Although[15–19] many other methods had proposed for the efficient routing in Wireless Sensor Networks, they have their own limitations and difficulties.

The paper is structured as follows. Section 2 presents the proposed method. Section 3 illustrates the results and discussion for evaluating the efficiency of the proposed method. Finally, Section 4 concludes the paper.

2. Proposed Method

In this paper, we propose Detecting and Replacing Beacon Node Failure and Secure Communication in WSNs. In this scheme, the failure beacon node is identified and the failure beacon node is replaced by the mobile user. The cryptography key technique provides secure data transmission to the network. The beacon nodes are updating the location information to the sensor nodes. In this approach, we mainly focus on beacon node failure. In WSN, beacon node failure occurs due to resource, hardware failure or some other reasons while the BS replace that beacon node to mobile user. This mobile user consists of movement activity that carries beacon or listener. The mobile user dynamically estimates the surrounding node location information and broadcast the failure beacon nodes to its neighborhood nodes. The Figure 1 shows the architecture of the proposed scheme.

The DRBF consist of 4 phases: System initialization, Mobile User Preprocessing, Mobile User Verification and Clustering. In the system initialization phase, The BS creates public key and private key of sensor nodes, assigns the privilege to the Mobile User. In Mobile User preprocessing phase, the BS replaces the Failure Beacon nodes. In Mobile User Verification Phase, the sensor node verifies whether the mobile user is a privilege or not. If the Mobile User is a privilege, the sensor node accepts the location information. In the clustering phase, the sensor nodes are formed to the clusters and transmit the data to the BS via CHs.

2.1 System Initialization Phase

Initially the beacon nodes are registered to the BS. Before deployment, the BS performs the following steps:

The sensor node public parameters are $\{G, GT, e, p, Q, h1, h2\}$

Here G is a cyclic additive group and G_T is a cyclic multiplicative group of a prime order p. Q is a generator of G and e is $G \times G \to G_T$. $h1$ and $h2$ represents the cryptographic hash functions $h1 = \{0,1\}^* \to Z_p$ $h2 = \{0,1\}^* GT \to Z^*_p$.

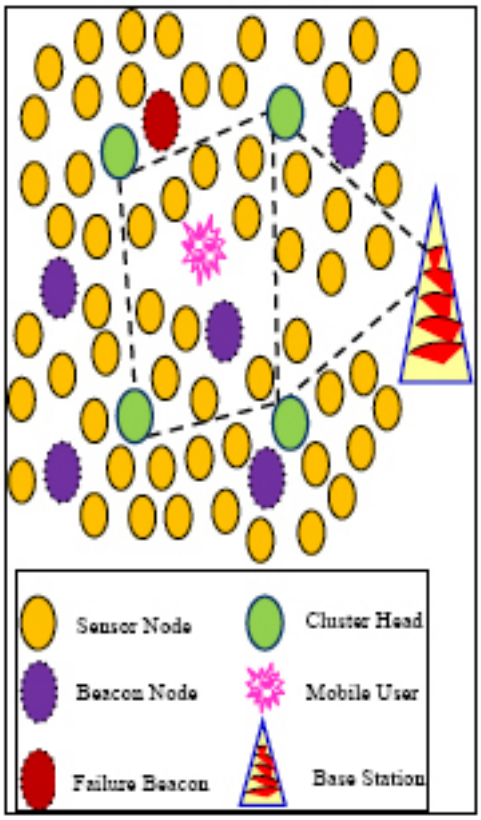

Figure 1. Architecture of the DRBF scheme.

Select a random number $s \in Z^*_P$

The sensor node generates the public key $pu = s.Q$

The sensor node generate a private key $1/(pu + s)$

The Mobile User computes the signature $h1(MU_{id}, pri) \in Z^*_p$

$pri \rightarrow$ Privilege of the mobile user

2.2 Mobile User Pre-Processing

If there is any beacon node failure, the sensors nodes in that location cannot get the location information from the beacon node. Then the neighborhood nodes send the notification message to the BS. BS receives this message and it sends RREQ message to the privilege mobile user. This RREQ message includes the Beacon ID, position and neighborhood of failure beacon sensor node ID. The privilege mobile user receives the RREQ message from BS. The mobile user switches to the location of failure beacon

node and acts as a beacon node and update the location information to the neighborhood node.

2.3 Mobile User Verification

In this phase, the mobile user sends HELLO message to the failure beacon neighborhood sensor nodes. This message includes the mobile user signature. The sensor node receives this HELLO message from Mobile User and checks with the Mobile User signature. If the mobile user is authenticated, then the sensor node accepts the mobile user location information. Otherwise, the sensor nodes will not recognize the location information from the fake mobile information and send notification message to the BS.

2.4. Clustering Operations

The sensor nodes gather the location information from the near beacon nodes or mobile user and the clusters are formed based on the node distance. The highest Received Signal Strength (RSS) and highest residual energy node is selected as CHs. The sensor nodes encrypt the data based on the public key and send the data to CHs. The CHs gathers the encrypted data from its cluster sensor nodes. Then the CHs aggregate these data and send the data to the BS. Finally, the BS decrypts and obtains the original data using the private key.

3. Performance Evaluation

The simulation analysis is achieved by using the tool namely, Network Simulator 2 (NS2). Since WSNs are configured both as static and mobile sensors, IEEE 802.11 network scenario is considered. The NS2 is an open source programming language written in C++ and OTCL (Object Oriented Tool Command Language). NS2 is a discrete event time driven simulator, which is used to mainly model the network protocols. The parameters used for the simulation of the proposed scheme are tabulated in Table 1.

The proposed scheme has 28 nodes deployed for simulation in the simulation area 1000 × 1000. User Datagram Protocol (UDP) is the communication protocol used for nodes communication. The traffic is handled with the help of traffic model CBR. The propagation model two-ray ground is used for propagation of radio waves. The signal is received from all the nodes from all the directions by using the Omni directional antenna. The performance of the proposed scheme is evaluated by the parameters such as packet delivery rate, packet loss rate, average delay and throughput.

Table 1. Simulation parameters

Parameter	Value
Channel Type	Wireless Channel
Simulation Time	50 ms
Number of nodes	28
MAC type	802.11
Traffic model	CBR
Simulation Area	1000×1000
Network interface Type	WirelessPhy
Traffic Model	CBR
Communication Protocol	UDP

3.1 Packet Delivery Rate

The Packet Delivery Rate (PDR) is the ratio of number of data packets delivered to the receiver nodes to the number of data packets sent by the source node. The PDR is calculated by the Equation 1.

$$PDR = \frac{\sum_0^n Packets\ Received}{\sum_0^n Packets\ Sent} \quad (1)$$

The Figure 2 shows the PDR of the DRBF scheme is greater than the PDR of the existing SRLS scheme. The greater value of PDR means the better performance of the protocol.

3.2 Packet Loss Rate

The Packet Loss Rate (PLR) is the ratio of the number of packets dropped by the receiver node to the number of

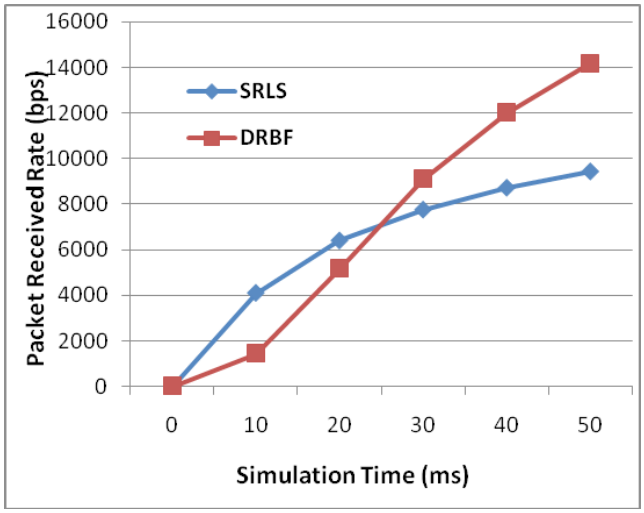

Figure 2. Packet Delivery Rate.

data packets sent by the source node. The formula used to calculate the PLR is given in Equation 2.

$$PLR = \frac{\sum_0^n Packets\ Dropped}{\sum_0^n Packets\ Sent} \quad (2)$$

The PLR of the proposed scheme DRBF is relatively lower than the existing scheme SRLS in Figure 3. Lower the PLR indicates the higher performance of the network.

3.3 Average Delay

The average delay is defined as the time difference or duration between the current packets received and the earlier packet received. It is measured by the Equation 3.

$$Average\ Delay = \frac{\sum_0^n Pkt\ Recvd\ Time - Pkt\ Sent\ Time}{n} \quad (3)$$

Figure 4 shows that the average delay value is low for the proposed scheme DRBF than the existing scheme SRLS. The minimum value of delay means that higher value of the throughput of the network.

3.4 Throughput

The average number of successful packets or messages delivered to the destination from the source is called as throughput. The average throughput is estimated using Equation 4.

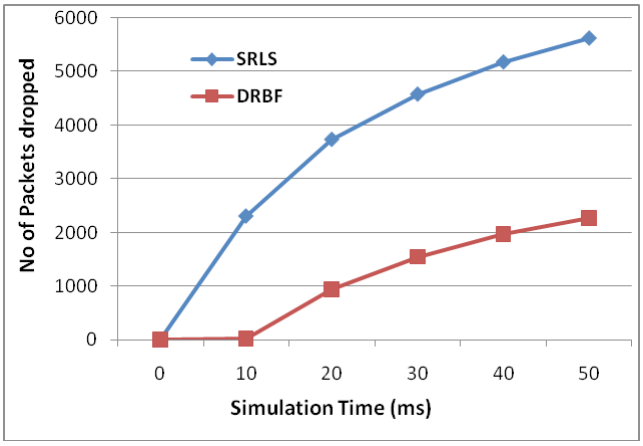

Figure 3. Packet Loss Rate.

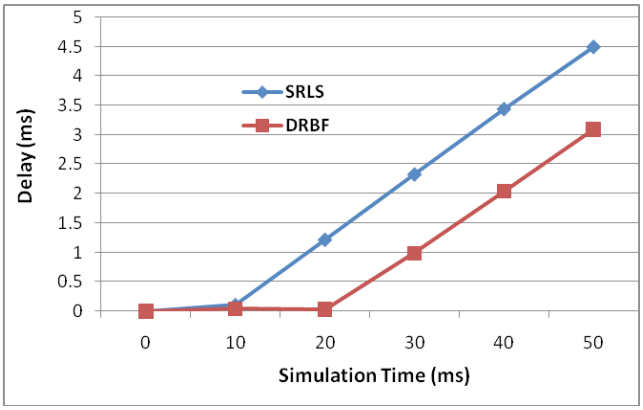

Figure 4. Average delay.

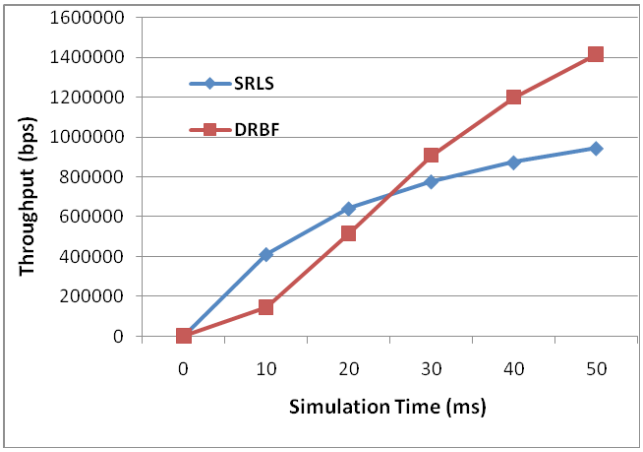

Figure 5. Throughput.

$$Throughput = \frac{\sum_0^n Pkts\ Received\ (n) * Pkt\ Size}{1000} \quad (4)$$

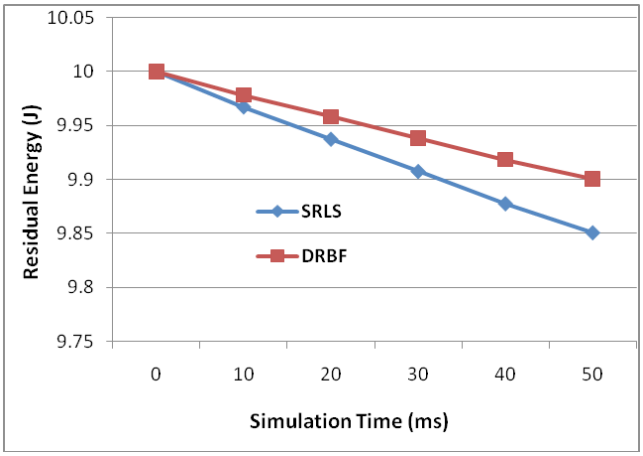

Figure 6. Residual energy.

Figure 5 shows that proposed scheme DRBF has higher average throughput when compared to the existing scheme SRLS.

3.5 Residual Energy

The amount of energy remains or residue in a node at the current instance of time is said to be residual energy. A measure of the residual energy gives the rate at which energy is consumed by the network operation.

Figure 6 shows that the residual energy of the network is better for the DRBF scheme when compared with the SRLS scheme.

4. Conclusion

In this paper, we introduced Detecting and Replacing Beacon node Failure (DRBF) and secure communication in WSNs. In this scheme, the failure beacon node is detected and replaced by the privilege mobile user and it updates the location information to the sensor nodes. The sensor nodes verify the mobile user privilege and obtain the location information. The sensor nodes encrypt the original data based on the public key. The CHs are elected based on the residual energy and RSS. The CH gathers the encrypted data and send to the BS. The BS collects the data from CH; decrypt the original data using private key. The simulation results show that the DRBF increases the packet delivery rate and reduces both the packet loss rate and delay.

5. References

1. Panahi FT, Haghighat AT, Panahi FT. Wireless Sensor Networks localization based on QoS by using one beacon. Third IEEE International Conference on Ubiquitous and Future Networks (ICUFN); Dalian. 2011. p. 214–9.
2. Shen H, Zhao L. ALERT: An Anonymous Location-based Efficient Routing protocol in MANETs. IEEE Transactions on Mobile Computing. 2013; 12(6):1079–93.
3. Xiao B, Chen L, Xiao Q, Li M. Reliable anchor-based sensor localization in irregular areas. IEEE Transactions on Mobile Computing. 2010; 9(1):60–72.
4. Edake GM, Pathak GR, Patil SH. Secure Localization and location verification of Wireless Sensor Network. Fourth IEEE International Conference on Communication Systems and Network Technologies (CSNT); DC. 2014. p. 673–6.
5. Zhu C, Wu S, Han G, Shu L, Wu H. A Tree-Cluster-Based Data-Gathering Algorithm for Industrial WSNs with a mobile sink. IEEE Access. 2015; 3(1):381–96.
6. Leu JS, Chiang TH, Yu MC, Su, KW. Energy efficient clustering scheme for prolonging the lifetime of Wireless Sensor Network with Isolated Nodes. Communications Letters, IEEE. 2015; 19(2):259–62.
7. Shang Y, Ruml W, Zhang Y, Fromherz M. Localization from connectivity in sensor networks. IEEE Transactions on Parallel and Distributed Systems. 2004; 15(11): 961–74.
8. Zou Y, Chakrabarty K. Energy-aware target localization in Wireless Sensor Networks. Proceedings of the First IEEE International Conference on Pervasive Computing and Communications (PerCom 2003); 2003. p. 60–7.
9. Liu D, Lee MC, Wu D. A node-to-node location verification method. IEEE Transactions on Industrial Electronics. 2010; 57(5):1526–37.
10. Liu D, Ning P, Du WK. Attack-resistant location estimation in sensor networks. Proceedings of the IEEE 4th International Symposium on Information Processing in Sensor Networks; 2005. p. 13.
11. Miao C, Dai G, Ying K, Chen Q. Collaborative localization and location verification in WSNs. Sensors. 2015; 15(5):10631–49.
12. Ekici E, Vural S, McNair J, Al-Abri D. Secure probabilistic location verification in randomly deployed Wireless Sensor Networks. Ad Hoc Networks. 2008; 6(2):195–209.
13. Fang L, Du W, Ning P. A beacon-less location discovery scheme for Wireless Sensor Networks. INFOCOM. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. 2005; 1(1):161–71.
14. Labraoui N, Mourad G, Makhlouf A. Secure DV-hop localization scheme against wormhole attacks in Wireless Sensor Networks. Transactions on Emerging Telecommunications Technologies. 2012; 23(4):303–16.
15. Cuong DD, Tam NV, Hieu NG. Improving multipath routing protocols performance in mobile ad hoc networks based on QoS cross-layer routing. Indian Journal of Science

and Technology. 2016 May; 9(19). DOI: 10.17485/ijst/2016/v9i19/92304.
16. Kaliyamurthie KP, Parameswari D, Udayakumar R. QoS aware privacy preserving location monitoring in Wireless Sensor Network. Indian Journal of Science and Technology. 2013 May; 6(S5). DOI: 10.17485/ijst/2013/v6i5S/33368.
17. Rajkumar K, Swaminathan P. Combining TCP and UDP for secure data transfer. Indian Journal of Science and Technology. 2015 May; 8(S9). DOI: 10.17485/ijst/2015/v8iS9/65569.
18. Abinaya R, Kamakshi S. Improving QoS using Artificial Neural Networks in Wireless Sensor Networks. Indian Journal of Science and Technology. 2015 Jun; 8(12). DOI: 10.17485/ijst/2015/v8i12/63283.
19. Sasi SB, Sivanandam N. A survey on cryptography using optimization algorithms in WSNs. Indian Journal of Science and Technology. 2015 Feb; 8(3). DOI: 10.17485/ijst/2015/v8i3/59585.