Adaptive Secure Energy Efficiency Routing Protocol for Wireless Sensor Network

Sravankumar Bethi* and Nageswara Rao Moparthi

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India
E-mail: sravan.researcher@gmail.com; mnrphd@gmail.com
**Corresponding Author*

Received 16 September 2021; Accepted 05 January 2022;
Publication 05 March 2022

Abstract

Wireless Sensor Network (WSN) is highly used in many applications for monitoring purposes. Many researchers were carried out in energy efficiency and security to improve network performance. In this research, the Adaptive Secure Energy Efficiency Routing Protocol (ASEERP) is proposed to improve security and reduce the energy consumption of the WSN. Gaussian distribution is used in this model to improve the synchronization of the model for the routing. Initialization of the node is carried out based on the residual energy of the node and neighbor node of WSN. The model routing phase transmits the data based on direct transmission and relay transmission based on path availability and distance. The direct transmission is carried out in a possible scenario to save energy in the neighbor nodes. The cooperation phase in the model helps to select the best relay based on the residual energy if the transmission is carried out based on the relay node. The source information and relay information are combined to analyze the neighbourhood information to adaptively select the optimal path in the model. The incoming packets and outgoing packets of the sensor nodes are measured

Journal of Mobile Multimedia, Vol. 18_4, 1009–1034.
doi: 10.13052/jmm1550-4646.1843

to detect the attack and attack indicator estimation is used to detect the malicious node to deny access to it. The proposed ASEERP model has an energy consumption of 57 J, the existing LEACH-C model has 80 J and the SMEER model has 72 J for 600 ms time.

Keywords: Attack indicator, co-operation phase, energy efficiency, Gaussian distribution, wireless sensor network.

1 Introduction

Wireless Sensor Network (WSN) consists of thousands of sensor nodes organized in the network to transfer the data. WSNs are usually applied for various purposes such as sensing, collecting, processing and communicating the data with other nodes [1]. WSN consists of small devices scattered over a remote area for various monitoring purposes such as humidity, temperature, and border surveillance, etc. Small devices have resource constraints in terms of computation and battery. Therefore, routing algorithms need to be designed to operate in resource constraint devices for low power consumption from the sensor devices [2]. Energy and bandwidth are the two main challenges in the WSN and mobile systems in the current researches. The effective protocol needs to be designed for optimal energy consumption and to provide higher bandwidth to transmit the data for overcoming the current challenges in the WSN routing protocol [3]. Energy consumption in the routing protocol often causes the failure of nodes in the system and energy efficiency in WSN is important [4]. However, it is difficult to improve transmission performance and reduce the energy consumption in WSN. WSN requires enhanced energy efficiency, throughput, and reduced end-to-end delay, to have improved performance [5].

WSN data communication requires more energy compared to data processing and sensing. WSN requires the routing method to reduce the energy consumption and to improve its security for gaining enhanced network performance [6]. Malicious nodes in the WSN often cause high energy consumption in the network, hence elimination of the malicious nodes contributes towards effective energy saving. Recently, various researches have involved the application of routing methods to improve the efficiency and security in WSN. Routing protocols based on location, central data routing protocols, and hierarchical routing protocols were developed to provide guaranteed service quality and data flow in the networks. Networks were classified as homogeneous and heterogeneous networks based on the sensor nodes' initial

energies [7, 8]. Sensor nodes are activated using the battery in WSN and energy efficiency is the major problem in WSN. The energy usage needs to be managed in the WSN to improve the system lifetime [9, 10]. Since WSN nodes are operated using a battery, an efficient routing protocol needs to be developed to provide efficient performance in terms of energy and security. In the traditional WSN routing protocols, factors such as synchronization, delay, and traffic rate were neglected in the optimization of energy for WSN [11, 12]. In this research, the ASEERP method is proposed to analyze the synchronization and delay to improve the energy efficiency of the WSN. The objectives of the proposed method are given as below.

1. The proposed ASEERP method applies co-operative phase to share the information between the nodes. The combine strategy method uses the weight value to update the routing table. The co-operative phase and combine strategy method helps to identify the malicious node in the network.
2. The proposed ASEERP method finds the optimal path for the packet transfer to reduce the energy consumption in the network. The proposed ASEERP method finds the optimal path based on the path weight.

This paper is organized as follows: Review of recent methods in WSN energy efficiency model is given in Section 2, ASEERP routing protocol explanation is given in Section 3, simulation setup is given in Section 4, the result and discussion are given in Section 5, and a conclusion is given in Section 6.

2 Literature Review

Secure transmission and energy efficiency are the two important research challenges in Wireless Sensor Nodes (WSN) applications. Some of the notable researches involved in developing energy efficiency and secure transmission are reviewed in this section.

Liu et al. [13] developed a model named Security Cooperation Collection Tree Protocol (SC-CTP) to detect uncoordinated behavior like trustless control, uncontrollable accuracy, and an inextensible protocol. A security model has been applied to couple the state vector to the time synchronization and topology control. The model performed weight synchronization and controlling a number of parameters to improve efficiency. The model measured the neighbor nodes' time synchronization to judge the node control behavior. The model involved in the analysis of the state vector calculation and other

parameters such as clock delay, clock drift, signal intensity reduction, and the coupling strength rate of topology. The simulation result showed that the developed model had higher performance in malicious node detection and reduced the energy consumption of the WSN. The model had lower efficiency in the dynamic network and the real-time systems are largely based on dynamic networks.

Dhand and Tyagi [14] proposed an Ant Lion Optimizer and k-means methods for the optimal CH selection and grouping of the nodes for energy efficiency. The multi-curve Elliptic curve cryptographic method was applied with a hybrid method to improve the security in WSN. The hybrid and cryptographic model in this research aimed to improve the secure transmission and energy efficiency of the system in WSN. This model encrypted the message with two keys based on multi-tier routing of the spherical grid and forwarded the packets into a spherical format. The proposed method achieved greater performance compared to existing methods in terms of minimum energy, delay, and throughput. The random initialization in k-means and Ant Lion optimization of local optimum degrades the performance of the model.

Saraereh et al. [15] proposed a method of selective neighbor discovery algorithm and this method enabled the node to search for neighbor nodes to reduce the long-time waiting delay. The prediction model was also incorporated in the developed method to analyze the distance and movement speed of the neighborhood for determining the next neighborhood set, so that it improves the neighborhood discovery accuracy and delay. The simulation result showed that the developed model had very efficiently performed energy reduction in WSN. The node clock synchronization requirement was higher and this increased the drift of the node's clock. This increase in the clock drifts affected the performance of the model in the energy efficiency.

Ezhilarasi and Krishnaveni [16] applied cuckoo search optimization and clustering method to increase the energy efficiency of the WSN. The developed method was tested on various sizes of nodes up to 200 nodes to evaluate the performance of the method. The clustering and cuckoo search method was tested against the conventional methods; TEEN, and LEACH method. The results showed that the developed method achieved higher performance in terms of network efficiency and network lifetime. The local optimum was caused in the cuckoo search optimization due to the initialization of the nest and exploitation capacity was less.

Elsmany et al. [17] proposed Energy Efficient Scalable Routing Algorithm (EESRA) based on a hierarchical routing algorithm and clustering method. This method aimed to increase the network lifetime by increasing

the size of nodes. A three-layer hierarchy method was applied to reduce the cluster heads random selection and cluster head loads. The simulation result showed that the developed method had higher efficiency in terms of energy efficiency and load balancing. The network model and energy model were developed to apply the EESRA method to test the performance. The model had lower efficiency in the dynamic network type and the delay of the method was high.

Haseeb et al. [18] proposed energy efficient and secure routing protocol to avoid intrusion in IoT network to increase the data trustworthiness. Various energy efficient clusters were applied based on intrinsic qualities of nodes. The threshold-based Shamir secret sharing method was applied to increase the security and reliability of the node. Selvi et al. [19] proposed energy aware based secure routing protocol to find malicious users in WSN. Decision tree algorithm was applied with spatio-temporal constraints to find the optimal path for WSN. The developed method had higher performance in energy aware secure routing protocol.

Mathapati et al. [20] applied progressive key generation process for authentication and multi-dimension trust computation was used to maintain resource efficiency. The developed model's aim was to effectively balance the trust reputation and resource efficiency in more predictable energy dissipation trend. Sathya and Umadevi [21] applied key distribution with a dynamic rate aware method to improve the security of the model. The secure route method was carried out to identify each route and optimum route was selected for transmission. Khot and Naik [22] applied Particle Water Wave Optimization which was used for routing the data packets in secure path. The PSO based cellular automata with fitness measure was applied for selection of cluster head. Factors such as maintainability, consistency, trust, delay and energy were considered as the fitness measures.

The review of the recent methods shows that an effective method is required to reduce the energy consumption and latency in WSN. Some common limitations such as optimization local optima, lower efficiency in a dynamic network, and k-means random initialization, affect the WSN performance. This study proposes the ASEERP model to overcome the above-mentioned limitations and to reduce energy consumption.

3 Proposed Method

In this research, the ASEERP model is proposed to improve security and reduce the energy consumption in WSN. Gaussian distribution is applied in

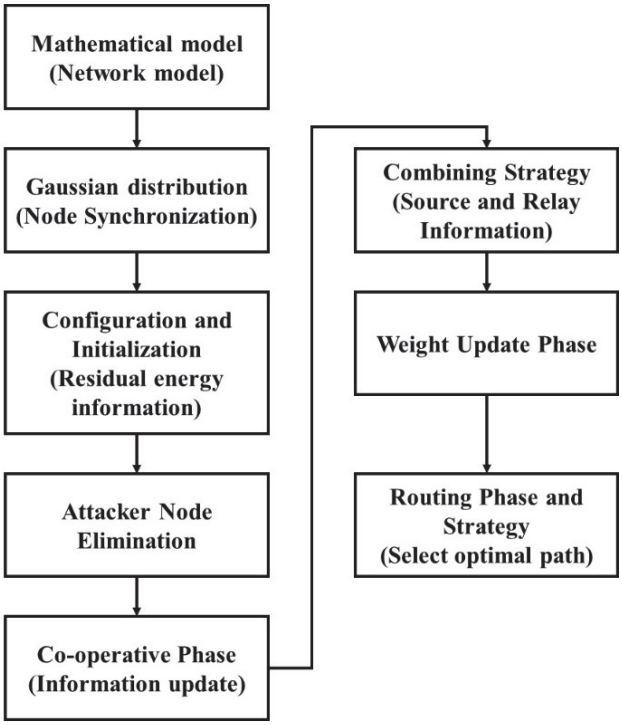

Figure 1 The ASEERP model block diagram.

the model to improve the node synchronization and to effectively handle the dynamic networks. Initialization and configuration are applied to measure the residual energy of the node. The attack indicator measures the node's incoming and outgoing data to deny access to suspicious nodes. The co-operative phase provides the neighbourhood information in the network and helps in the routing phase. The combination strategy provides the source and relays information for the weight update in the model. The routing phase provides the optimal path selection based on the provided information in the network. The ASSERP model block diagram is shown in Figure 1.

Black hole attack drops all the data packets in the network and network performance is significantly affected [23]. The proposed method provides the solution to detect the black hole attack in AODV routing. The cooperative phase and combine strategy method helps to detect the malicious node in the network. Elimination of malicious node phase helps to remove the malicious node before it receives the data packets.

3.1 Clock Synchronization

The sending and receiving time of a single clock message is only tens of microseconds in the sensor nodes' hardware. Synchronization clock drift affects the accuracy and this is ignored in the process of actual synchronization. Clock synchronization error is assumed to create the phase synchronization error in the model. The sending and receiving process of bi-directional time message of i timestamp set is defined as $\{T_{1,i}, T_{2,i}, T_{3,i}, T_{4,i}\}_{i=1}^{n}$, where node B and A sending time stamps are denoted as $T_{1,i}$ and $T_{3,i}$, and node B and A receiving time stamps are denoted as $T_{2,i}$ and $T_{4,i}$, respectively. Time difference $T_{2,i} - T_{1,i}$ is random in executing multiple bidirectional time message exchanges due to random delay in the processing and transmission of time messages. The phase difference calculation is introduced with a random delay, as shown in Equations (1) and (2) [24].

$$T_{2,i} = T_{1,i} - \Delta\varphi + d^{BA} + X_i^{BA} \tag{1}$$

$$T_{4,i} = T_{3,i} + \Delta\varphi + d^{AB} + X_i^{AB} \tag{2}$$

Where phase difference of nodes A and B is calculated as $\Delta\varphi$, random delays and fixed delays of the time message from B to A are denoted as d^{BA} and X_i^{BA}, and the delay from A to B is denoted as d^{AB} and X_i^{AB}, respectively. Sensor nodes with software architecture and same hardware are considered, hence $d^{AB} = d^{BA} = d$ [25, 26] which assumes Probability Density Function (PDF) is followed by X_i^{AB} and X_i^{BA}. The X_i mean is 0 and variance is twice as much of X_i^{AB}. WSN's practical application causes the synchronous error accumulation in the model and X_i mean and variance tends to increase the network scale to satisfy the above assumption. The random difference occurs in real-time systems in various nodes. For example, the intertidal zone is monitored using WSN, ambient temperature affects the clock frequency of nodes that leads to small changes in sending and receiving delay. Therefore, X_i is considered as a non-zero random variable. The i^{th} message exchange delay U, V is defined in Equations (3) and (4).

$$U_i = T_{2,i} - T_{1,i} \tag{3}$$

$$V_i = T_{4,i} - T_{3,i} \tag{4}$$

The nodes' real phase difference is given in Equations (5)–(6).

$$\Delta\varphi = \Delta\widehat{\varphi}_i - X_i \tag{5}$$

Where X_i is given by

$$X_i = (X_i^{AB} - X_i^{BA})/2 \tag{6}$$

The i^{th} round time message of real phase difference $\Delta\varphi$ is given as $\Delta\widehat{\varphi}_i = (V_i - U_i)/2$. The real phase difference $\Delta\varphi$ is measured using Equation (5), X_i information is not given to node B, thus $\Delta\widehat{\varphi}_i$ compensates the clock difference that results in synchronization errors. The Equation (5) is re-written as $X_i = \Delta\widehat{\phi} - \Delta\varphi_i$ and measurement error is consistent in the form. In this study, X_i is defined as the clock synchronization error and this is also used in various clock synchronization fields. The X_i is applied with various kinds of PDFs such as single server $M/M/1$ queue model, exponential distribution, and gamma distribution. Since series of small delays in the transmission path and random delay of time message delivery, Gaussian distribution is selected in this study. Gaussian distribution converges its sum based on the central limit theorem [24].

3.2 Secure Energy Efficient Routing Protocol

The ASEERP method is applied with co-operation technique to use WSN in multi-hop networking mode. The source node generates the data packets and forwards them to the destination node or sink node via hop by hop. The relay node is deployed at the joint and two consecutive hops at the joint collects the packets and amplifies them for re-transmitting the packets to the destination. The ASEERP detects the malicious nodes based on common active routing attacks for packet drop and eliminates the malicious nodes to improve the network efficiency.

The proposed ASEERP method is based on AODV routing protocol to transmit the data in the network. The AODV algorithm [27] is a reactive routing protocol that is developed based on routing protocol of DSDV. AODV is hop by hop method and each intermediate node determine the next node to forward the routed packet. A route table contain routing node to maintain new route information that consists of three important fields that are: a sequence number, next hope node and a hop count. This method is adaptive to condition of dynamic link, has less memory and overhead.

AODV protocol maintains the routing table to provide the node information and nodes in the network have access to the routing table. Once the malicious node is identified, the routing table updates the node as error and prevents the malicious node from accessing the routing table. The other nodes in the network identify the blocked nodes as malicious nodes and thus, do not transfer the information to those malicious nodes.

3.2.1 Network model

A WSN network model consists of relay nodes of R_1 and R_b, the source node of S, destination node of D, and malicious nodes of A_1 and A_2. The best relay node is denoted as R_b in the available relay nodes of R_1 and R_b. The relay node is check for the malicious node to eliminate the malicious node for data transmission [28–30].

3.2.2 Configuration and initialization

Residual energy information of each sensor node is broadcasted to the neighbors using hello packets for initialization of the network operation [31, 32]. Neighbour sensor nodes have information about each other sensor node in this phase. The destination node sends the hello packet to all sensor nodes and the weight of each sensor node is denoted in Equation (7).

$$W_i = \frac{T_l \times R_i}{D_w - D_i} \tag{7}$$

where node weight is denoted as W_i of node i, the path loss is denoted as T_l, residual energy node is denoted as R_i, depth of water is denoted as D_w and the depth of node i is denoted as D_i.

3.2.3 Eliminating malicious nodes

The packets sent and received in neighbor sensor nodes are analyzed for the detection and elimination of malicious nodes [33–35]. The Q_j stores the incoming packets P_{in} and Q_k stores the outgoing packets in sensor nodes. The Q_j and Q_k are compared after the packets are store and if the values are not equal, then there are chances for the sensor node to be a malicious node. The malicious node value A_i is incremented by 1 and if the A_i value reaches x for a sensor node, then this is considered as a malicious node. Then the malicious node is eliminated in the WSN routing process to improve the energy efficiency. The x value is set to 3 and x value is adjusted based on the environment. The x value needs to be selected carefully, the higher value lets the malicious node in the network and the lower value has the chance of removing the genuine sensor node.

All sensor nodes perform the detection and elimination process of the malicious node to ensure malicious nodes are participating in any network. The storage of the incoming and outgoing packets in the network is given in Equations (8), (9).

$$Q_j = P_{in} \tag{8}$$

The incoming packets P_{in} is stored in Q_j a sensor node, as given in Equation (8).

$$Q_k = P_{out} \tag{9}$$

The outgoing packets P_{out} stored in Q_k a sensor node, as given in Equation (9).

If $Q_j = Q_k$

No malicious node is detected

Else If $Q_j \neq Q_k$ and $Q \neq S_k$

$$A_i = A_i + 1$$

where S_k represents destination and A_i is the malicious indicator.

If $A_i \geq x$ separate sensor node from the network.

3.2.4 Cooperation phase

In the WSN environment, direct transmission and best relay node transmission are based on the co-operation phase [36, 37], as given in Equation (10).

Where D denotes the destination, the best relay node is denoted as R_b and the source is denoted as S.

$$Y_{sd} = H_s \times g_{sd} + n_{sd} \tag{10}$$

where the signal from the source to destination node directly is denoted as Y_{sd}, the source and destination node channel is denoted as H_s, the information that is applied from source to destination is denoted as g_{sd}, and the ambient noise is denoted as n_{sd} in the channel H_s, as given in Equation (11).

$$Y_{sr} = H_s \times g_{sr} + n_{sr} \tag{11}$$

Where signal transmitted from source to relay node is denoted as Y_{sr}, the information transmitted from source to relay is denoted as g_{sr}, and the ambient noise n_{sr} is added to the channel H_s.

$$Y_{rd} = Y_{sr} \times g_{rd} + n_{rd} \tag{12}$$

If the relay node starts the transmission and sends the data packets, then the destination node does not receive packets from the source node in the network operation, as given in Equation (12). The data transmission from source to relay to a destination node is denoted as Y_{rd}, the forwarded information from the relay node is denoted as g_{rd} and n_{rd} denotes the noise that is added on the channel H_s to the information Y_{sr}.

3.2.5 Routing phase and relay strategy

A sensor source node S consists of n sensor nodes in its vicinity based on channel conditions to find out the neighbors suitable for data transfer to a destination node. The source node equates the weight value to select the relay node. The maximum value of the sensor node is denoted as W_i to select the data transmission. If source residual energy is more than or equal to relay residual energy, then the direct transmission is selected or transmission is carried out through the relay node.

If $R_s \geq R_r$ direct transmission
Else If $R_s \geq R_r$, transmission is carried out via relay node

where relay node residual energy is denoted as R_r and source node residual energy is denoted as R_s. The relay node carried out amplification and forward amplification factors on the signal received from the source and before forwarding the signal to a destination node.

3.2.6 Combining strategy

The destination node D uses Signal To Noise Ratio Combining (SNRC) to combine the signal from the relay R and source S. The SNRC is the signals combined at the receiver that has a weight equation to SNR at each array element. SNRC have better measure than Equal Ratio Combining (ERC) as it considers the weights of low SNR and small scale fluctuations. The SNRC is calculated in Equation (13).

$$Y_d = X_1 Y_{sd} + X_2 Y_{rd} \tag{13}$$

where the output signal is denoted as Y_d that is a combination of relay path weight X_2, direct path weight X_1 and destination node D. The combine strategy uses the signal and path weight for the detection of malicious node. The signal value is measured in co-operative phase and path weight, from weight updating phase. The combine strategy applies the both information to determine the malicious node. The path weight X_1 and X_2 are updated based on weight update phase.

3.2.7 Weight updating phase

The weight of the sensor node is the same as the weight calculated in initialization, when the number of dead nodes are less than or equal to 20%, as in Equation (7). The weight is calculated using the 'if' condition when the number of dead nodes is more than 20% and less than 75% in the WSN

environment. The weight is computed using the 'else' condition when a number of nodes are more than 75% and the statement condition is as follows.

If $N_d > 20$ and $N_d < 75$

$$W_i = (T_l \times D_i)/R_i$$

Else If $N_d \geq 75$

$$W_i = (T_l \times R_i)/D_i$$

where N_d is a number of dead nodes, D_i is the depth of the node i, T_l is path loss, and R_i denotes the residual energy.

4 Simulation Setup

This section provides the implementation details of the proposed ASEERP method used for energy efficiency in WSN. The data, metrics, system configuration and parameter settings of the model are discussed in this section.

Metrics: Energy consumption, Throughput, End-to-End delay, Packet Delivery Ratio, and Packet loss are the metrics used to test the performance of the proposed ASSERP model in improving energy efficiency and security.

Energy consumption: The amount of energy consumed by each node can be obtained at the end of each simulation, as given in Equation (14).

$$E_{consumption} = \frac{E_{Total}}{Number\ of\ packets\ successfully\ transmitted} \tag{14}$$

End to End delay: End to end delay is defined as the time of a packet generated at sensor nodes to the time it is received by the sink.

Throughput: Throughput refers to the amount of data that can be transferred from one location to another in a given amount of time, as given in Equation (15). Throughput is the total amount of data analysed per unit of time. Throughput can be calculated by dividing packet size analysed with respect to time.

$$throughput = \frac{received\ size}{stop\ time - start\ time} \tag{15}$$

System Configuration: The system consists of an Intel i9 Processor with 128 GB of RAM, 22 GB Graphics card and Windows 10-64bit OS. The Network

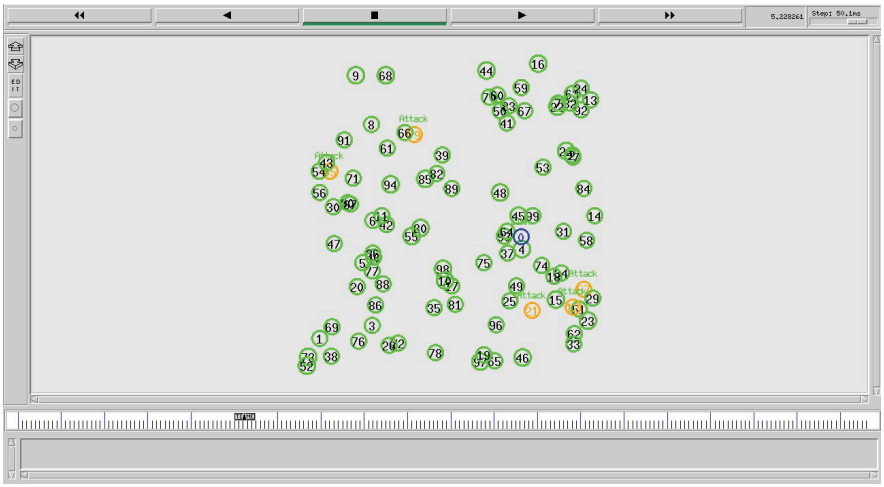

Figure 2 Node simulated in NS-2.

Table 1 Parameter settings of the proposed model

Parameter	Value
Total number of nodes	100
Distance among adjacent nodes	100 m
Deployment area	50 m × 2500 m
Simulation duration	600 s
Total number of relay nodes	98
Source node	1
Sink node	1
Packet size	1024 bits
Initial energy	1 J
Packet sending rate	1 packet/s

Simulator – 2 (NS-2) tool was used to implement and test the performance of the model. The OTL script is used to develop the AODV protocol and developed method is developed in C++ language. The node simulated image is shown in Figure 2.

Parameter Settings: The network parameter details were given in Table 1. In this simulation, 36429 number of transmissions are carried out and number of transmissions will change based on clock cycle. The one node which acts as a source node is randomly changed for every transmission and one sink node is set for the network.

5 Results and Discussion

Security and energy efficiency are the two main key aspects in WSN application and various researches were carried out considering these aspects. In this research, the ASEERP model is proposed to improve the energy efficiency and security of the method. The ASEERP model performance is measured for various nodes and compared with existing methods. Various metrics were measured to analyze the performance of the method.

The energy consumption of the proposed ASEERP model is measured in the simulation and compared with existing methods, as given in Table 2. For 600 s, the proposed method shows lower energy consumption than existing methods. The proposed method shows a gradual increase in the energy consumption with increase in time. The LEACH-C method performs weight calculation for the node synchronization and SMEER performs hybrid methods for secure transmission. The existing LEACH-C and SMEER methods have high energy consumption due to the hybrid methods that were applied to process the nodes. The proposed method applies co-operative phase and combine strategy to iteratively update the network information that helps to identify the malicious node and doesn't require the optimization process. Table 2 shows that the ASEERP model has lower energy consumption compared to other existing methods such as Leach-C and SMEER methods. The proposed ASEERP model has the advantage of initialization of node based on residual energy, which selects the best relay node for transmission and updates the model based on neighborhood information. The proposed

Table 2 Energy consumption of proposed ASEERP method

Time (Sec)	LEACH-C [13]	SMEER [14]	ASEERP (Proposed)
0	29	27	15
50	35	30	19
100	40	38	27
150	48	40	32
200	50	47	38
250	55	50	41
300	57	52	43
350	61	60	47
400	65	62	48
450	70	65	50
500	73	68	52
550	76	70	55
600	80	72	57

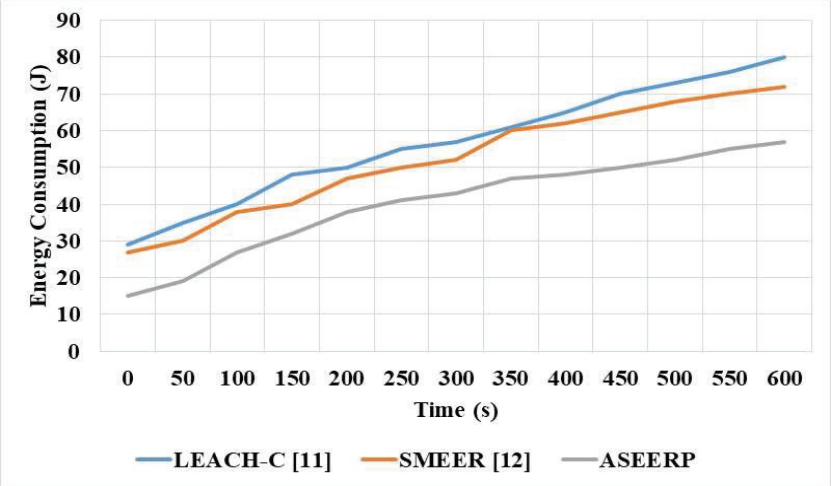

Figure 3 Comparison of routing methods in energy efficiency.

ASEERP model processes the direct transmission in a possible scenario and this reduces the energy consumption. The proposed ASEERP model has 57 J of energy consumption compared to the 80 J of energy consumption by the Leach-C model and 72 J of energy consumption by SMEER model in the simulation for 600 s time.

The energy consumption of the proposed ASEERP model is graphically compared with the energy consumption of existing methods which are Leach-C and SMEER, as shown in Figure 3. The proposed ASEERP model has lower energy consumption compared to existing methods. The Leach-C method has a lower performance in the dynamic network due to time delay estimation in the synchronization of the model. The SMEER model has the limitation of random initialization of the k-means and local optimum of the Ant Lion Optimizer. The estimation of delay in the proposed ASEERP method is based on Gaussian distribution which helps to improve the model synchronization. The proposed ASEERP model has an energy consumption of 52 J, the SMEER model has 68 J, and Leach-C has 73 J in the analysis for 500 s of simulation time.

The throughput of the proposed ASEERP method is measured in the simulation and is compared with that of the existing methods, as shown in Table 3. The table shows that the proposed ASEERP method has higher throughput compared to existing methods. The proposed ASEERP model has the advantage of proper relay node selection and direct transmission based

Table 3 Throughput of the ASEERP model

Time (Sec)	LEACH-C [13]	SMEER [14]	ASEERP (Proposed)
0	6	7	8
100	12	14	15
200	13	15	17
300	18	20	22
400	22	27	31
500	28	37	40
600	35	41	50

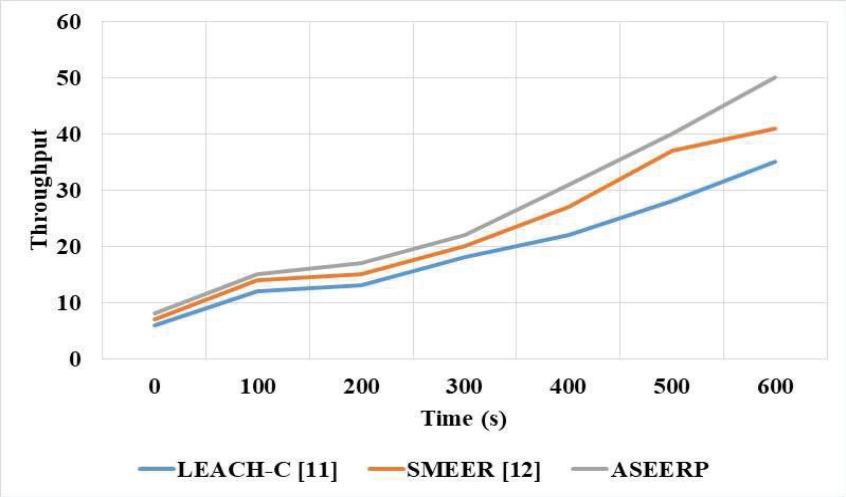

Figure 4 Comparison of throughput in routing method.

on source and relay neighborhood information. The co-operation phase helps to improve the performance of the model by using the relay analysis and combined strategy. The proposed ASEERP method has a higher throughput of 50 bps, the SMEER method has 41 bps, and the Leach-C method has 35 bps in the simulation for 600 s time.

The throughput of the proposed ASEERP model is graphically compared with the throughput of the existing methods of Leach-C and SMEER, as shown in Figure 4. The proposed ASEERP method has a higher throughput compared to existing methods. The combined strategy method utilizes the source and relay information to update the neighborhood information in the model and the best relay node is identified based on this process. The Leach-C has lower efficiency in the estimation of synchronization and time delay.

Table 4 End to End delay of proposed ASEERP method

Time (Sec)	LEACH-C [13]	SMEER [14]	ASEERP (Proposed)
0	36	34	2
100	44	42	28
200	50	48	36
300	60	55	44
400	75	68	60
500	88	79	68
600	97	94	75

The SMEER method has local optima in the ant lion optimizer and random initialization in k-means. The proposed ASEERP model has the throughput of 40 bps, the SMEER model has 37 bps, and the Leach-C model has 28 bps for 500 s of simulation time.

The end-to-end delay of the proposed ASEERP model is calculated on the simulation and is compared with that of the existing methods which are SMEER and Leach-C, as shown in Table 4. The ASEERP model has the lowest end-to-end delay compared to the existing methods. The relay selection is based on the neighborhood information that aims to reduce the delay in the transmission. The combined strategy method provides the source and relays information for adaptive relay selection. The proposed ASEERP method has an end-to-end delay of 75 ms, the SMEER method has 94 ms, and the Leach-C method has 97 ms in the simulation for 600 s.

The end-to-end delay of the proposed ASEERP method is graphically compared with end-to-end delay of the existing methods; Leach-C and SMEER, as shown in Figure 5. The proposed ASEERP method has the lowest end-to-end delay due to the advantage of selecting the best relay based on Gaussian distribution. The SMEER method has the limitation of local optima of the ant lion optimizer and random initialization of the k-means method. The Leach-C method has limitation of lower performance in the dynamic network.

The packet delivers ratio of the proposed ASEERP model is compared with that of the existing methods of SMEER and Leach-C, as shown in Figure 6. The ASEERP model has a higher packet delivery ratio compared to Leach-C and SMEER methods. The ASEERP method selects the suitable relay for the effective transmission that helps to improve the Packet Delivery Ratio.

The packet loss is measured for the proposed ASEERP model and compared with the packet loss of existing methods such as Leach-C and SMEER,

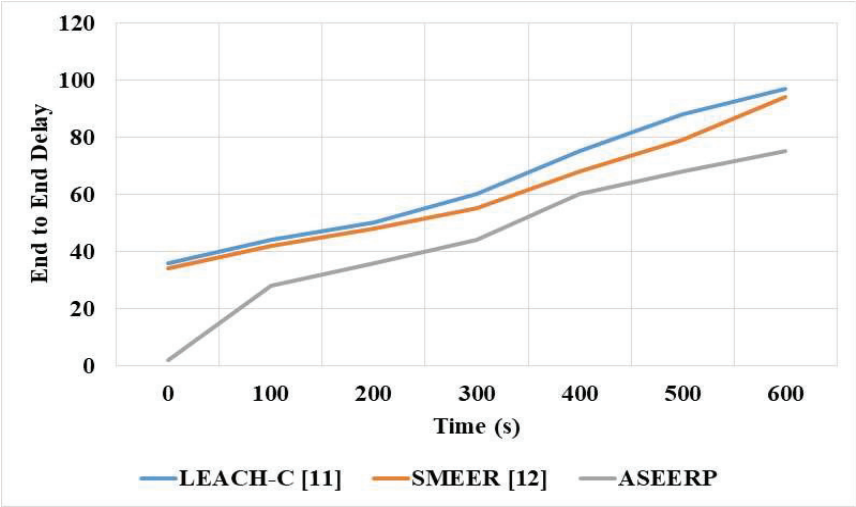

Figure 5 Comparison of routing model of End-to-End delay.

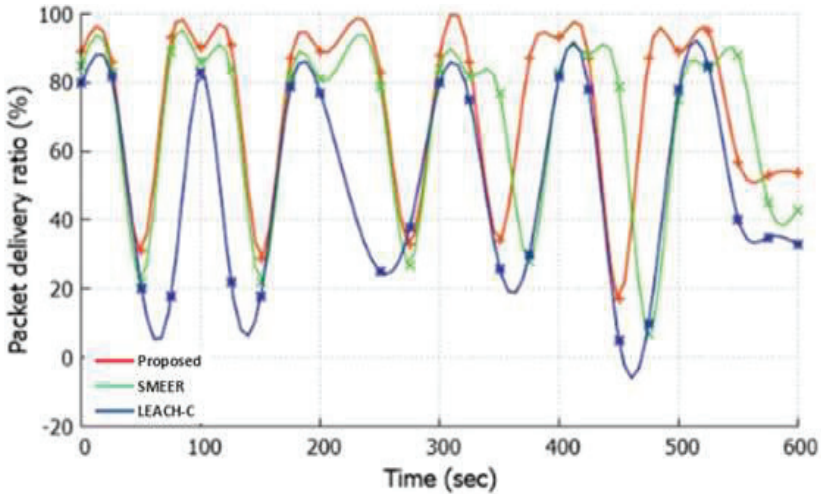

Figure 6 Comparison of packet delivery ratio.

as shown in Figure 7. The proposed ASEERP model has a lower packet loss compared to the existing methods. In the ASEERP model, Gaussian distribution is applied to select the suitable relay based on the combined strategy information that helps to decrease the packet loss ratio.

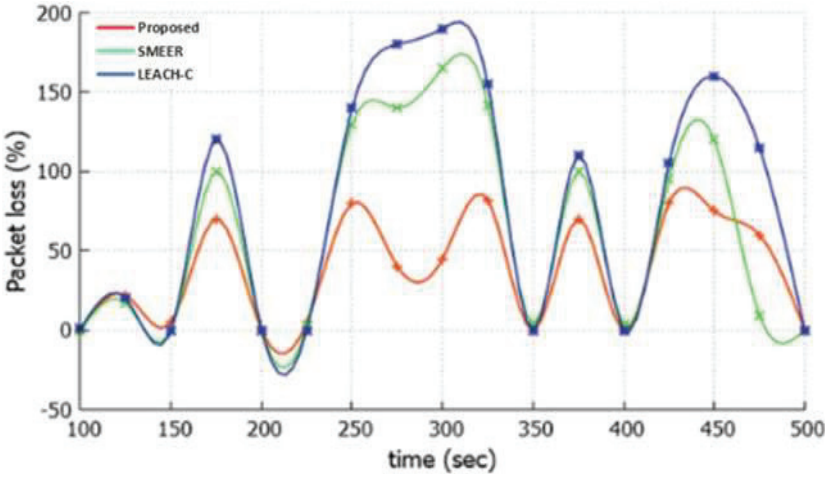

Figure 7 Comparison analysis of Packet loss.

Table 5 End to End delay of proposed ASEERP method

Methods	Number of Packets Sent	Number of Packets Received	Packet Delivery Rate (%)
LEACH [19]	36429	28738	78.87
HEED [19]	36429	29454	80.85
STRM [19]	36429	31569	86.65
EATRSA [19]	36429	34544	94.8
Proposed ASEERP method	36249	34645	95.6

The proposed and existing methods' packet delivery rate are shown in the Table 5, from which it can be inferred that the proposed ASEERP method has higher packet delivery rate due to its capacity in identification of malicious node. The proposed ASEERP method has advantage of applying the co-operative phase and combination strategy to improve the performance. The EATRSA [19] method applies decision tree method to improve the performance and this has instable performance in malicious node.

The proposed ASEERP method is compared with the existing method for various number of nodes and malicious node, as given in Table 6. Table 6 shows that developed method has higher performance in terms of energy and coverage. The proposed method has higher coverage due to sharing of node information in co-operative phase and combine strategy method provides efficient performance in energy balancing. The PSO based PWWO [22] method has limitation of easily trap into local optima and has poor convergence.

Table 6 End to End delay of proposed ASEERP method

Number of Nodes	Metrics	CA-based Node Scheduling [22]	CA-based Malware Propagation [22]	DICMLA [22]	PSMO [22]	PWWO [22]	Proposed ASEERP
50 nodes/7 Malicious Nodes	Energy balancing index	0.81	0.74	0.76	0.87	0.88	0.88
	Coverage %	79.64	62.57	55.88	98.03	98.56	99.40
	Number of nodes alive	46.00	22.00	28.00	92.00	95.00	97.00
	Energy left	0.36	0.36	0.41	0.45	0.58	0.66
100 nodes/15 Malicious Nodes	Energy balancing index	0.81	0.74	0.75	0.87	0.88	0.88
	Coverage %	79.06	62.36	55.37	97.23	98.12	99.25
	Number of nodes alive	41.00	17.00	23.00	87.00	90.00	92.00
	Energy left	0.36	0.36	0.41	0.45	0.58	0.66
150 nodes/22 Malicious Nodes	Energy balancing index	0.81	0.74	0.75	0.87	0.88	0.88
	Coverage %	78.48	61.23	55.10	97.44	97.84	98.30
	Number of nodes alive	35.00	13.00	21.00	85.00	87.00	88.00
	Energy left	0.36	0.36	0.41	0.45	0.58	0.66

6 Conclusion

Reliable transmission is an important requirement in the WSN to enable transmission of data through a highly secured channel or medium, with less energy consumption. Existing routing methods in WSN have the limitation of lower efficiency in dynamic networks and have local optima in the optimizer. In this research, the ASEERP model is proposed to improve security and reduce the energy consumption in WSN. The ASEERP model matches the incoming data and outgoing data in the nodes to detect the attack. The attack indicator is measured based on the data transmission so that access to the malicious node is eliminated. Gaussian distribution is applied to improve the synchronization in the node and the model performs effectively on the dynamic networks. Node initialization is carried out based on the node residual energy and neighborhood information of nodes in WSN. In this proposed model, the type of transmission for the data, whether direct transmission or relay-based transmission, is decided based on the path availability and distance. The co-operative phase selects the best relay to transmit the data to reduce the energy consumption in WSN. The model uses the source information and relay information to select the optimal path to transmit the data. The simulation result shows that the model improves transmission efficiency, security and reduces energy consumption. The model outperforms the existing methods such as LEACH-C and SMEER models

in terms of energy consumption, throughput, and end-to-end delay. The ASEERP model has 57 J energy consumption, the LEACH-C model has 80 J energy consumption and the SMEER model has 72 J energy consumption in 600 s simulation time. There are some of ways to further improve the proposed method. The optimization method can be applied to select the optimal path and neural network for prediction, to effectively reduce energy consumption. The clustering method can be applied for optimal selection of cluster heads and cluster members. Encryption method can be integrated to further improve the security of the data.

Declarations:

Funding: This research received no external funding.

Conflict of Interest: The authors declare that they have no conflict of interest.

Data Availability: The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

References

[1] W. Elsayed, M. Elhoseny, S. Sabbeh, A. Riad, 'Self-maintenance model for wireless sensor networks', Comput. Electr. Eng., vol. 70, pp. 799–812, Aug., 2018.

[2] H. Mostafaei, 'Energy-efficient algorithm for reliable routing of wireless sensor networks', IEEE Trans. Ind. Electron., vol. 66, no. 7, pp. 5567–5575, Sep., 2018.

[3] A. Sangaiah, M. Sadeghilalimi, A. Hosseinabadi, W. Zhang, 'Energy consumption in point-coverage wireless sensor networks via bat algorithm', IEEE Access, vol. 7, pp. 180258–180269, Nov., 2019.

[4] K. Chu, D. Horng, K. Chang, 'Numerical optimization of the energy consumption for wireless sensor networks based on an improved ant colony algorithm', IEEE Access, vol. 7, pp. 105562–105571, Jul., 2019.

[5] X. Yang, L. Wang, J. Xie, Z. Zhang, 'Energy efficiency TDMA/CSMA hybrid protocol with power control for WSN', Wireless Commun. Mobile Comput., pp. 4168354, Jan., 2018.

[6] S. Jha, E. Eyong, 'An energy optimization in wireless sensor networks by using genetic algorithm', Telecommunication Systems, vol. 67, no. 1, pp. 113–121, Jan., 2018.

[7] Z. Zhao, D. Shi, G. Hui, X. Zhang, 'An energy-optimization clustering routing protocol based on dynamic hierarchical clustering in 3D WSNs', IEEE Access, vol. 7, pp. 80159–80173, Jun., 2019.
[8] K. Dattatraya, K. Rao, 'Hybrid based cluster head selection for maximizing network lifetime and energy efficiency in WSN', Journal of King Saud University-Computer and Information Sciences, Apr., 2019.
[9] A. Vinitha, M. Rukmini, 'Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm', Journal of King Saud University-Computer and Information Sciences, Nov., 2019.
[10] N. Mazumdar, A. Nag, S. Nandi, 'HDDS: Hierarchical Data Dissemination Strategy for energy optimization in dynamic wireless sensor network under harsh environments', Ad Hoc Networks, vol. 111, pp. 102348, Feb., 2021.
[11] R. Bhardwaj, D. Kumar, 'MOFPL: Multi-objective fractional particle lion algorithm for the energy aware routing in the WSN', Pervasive Mob. Comput., vol. 58, pp. 101029, Aug., 2019.
[12] F. Engmann, F. Katsriku, J. Abdulai, K. Adu-Manu, F. Banaseka, 'Prolonging the lifetime of wireless sensor networks: a review of current techniques', Wireless Commun. Mobile Comput., pp. 8035065, Aug., 2018.
[13] Z. Liu, W. Liu, Q. Ma, G. Liu, L. Zhang, L. Fang, V. Sheng, 'Security cooperation model based on topology control and time synchronization for wireless sensor networks', J. Commun. Networks, vol. 21, no. 5, pp. 469–480, Aug., 2019.
[14] G. Dhand, S. Tyagi, 'SMEER: secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks', Wireless Personal Communications, vol. 105, no. 1, pp. 17–35, Mar., 2019.
[15] O. Saraereh, I. Khan, B. Lee, 'An efficient neighbor discovery scheme for mobile WSN', IEEE Access, vol. 7, pp. 4843–4855, Dec., 2018.
[16] M. Ezhilarasi, V. Krishnaveni, 'An evolutionary multipath energy-efficient routing protocol (EMEER) for network lifetime enhancement in wireless sensor networks', Soft Comput., vol. 23, no. 18, pp. 8367–8377, Sep., 2019.
[17] E. Elsmany, M. Omar, T. Wan, A. Altahir, 'EESRA: Energy efficient scalable routing algorithm for wireless sensor networks', IEEE Access, vol. 7, pp. 96974–96983, Jul., 2019.

[18] K. Haseeb, A. Almogren, N. Islam, I. Ud Din, Z. Jan, 'An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN', Energies, vol. 12, no. 21, pp. 4174, Nov., 2019.

[19] M. Selvi, K. Thangaramya, S. Ganapathy, K. Kulothungan, H.K. Nehemiah, A. Kannan, 'An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks', Wireless Personal Communications, vol. 105, no. 4, pp. 1475–1490, Apr., 2019.

[20] M. Mathapati, T.S. Kumaran, A. Muruganandham, M. Mathivanan, 'Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network', J. Ambient Intell. Hum. Comput., vol. 12, no. 6, pp. 6047–6055, Jun., 2021.

[21] S.S. Sathya, K. Umadevi, 'An optimized distributed secure routing protocol using dynamic rate aware classified key for improving network security in wireless sensor network', J. Ambient Intell. Hum. Comput., vol. 12, no. 7, pp. 7165–7171, Jul., 2021.

[22] P.S. Khot, U. Naik, 'Particle-Water Wave Optimization for Secure Routing in Wireless Sensor Network Using Cluster Head Selection', Wireless Personal Communications, vol. 119, pp. 2405–2429, Aug., 2021.

[23] A. Kumar, V. Varadarajan, A. Kumar, P. Dadheech, S.S. Choudhary, V.D.A. Kumar, B.K. Panigrahi, K.C. Veluvolu, 'Black hole attack detection in vehicular ad-hoc network using secure AODV routing algorithm', Microprocess. Microsyst., vol. 80, pp. 103352, Feb., 2021.

[24] T. Yang, Y. Niu, J. Yu, 'Clock synchronization in wireless sensor networks based on Bayesian estimation', IEEE Access, vol. 8, pp. 69683–69694, Apr., 2020.

[25] W. Hu, L. Gao, T. Dong, 'Data-driven optimal synchronization for complex networks with unknown dynamics', IEEE Access, vol. 8, pp. 224083–224091, Dec., 2020.

[26] H. Zhu, K. Liu, Y. Yan, H. Zhang, T. Huang, 'Measures to improve the accuracy and reliability of clock synchronization in time-sensitive networking', IEEE Access, vol. 8, pp. 192368–192378, Oct., 2020.

[27] A.M. El-Semary, H. Diab, 'BP-AODV: Blackhole protected AODV routing protocol for MANETs based on chaotic map', IEEE Access, vol. 7, pp. 95197–95211, Jul., 2019.

[28] K. Saeed, W. Khalil, S. Ahmed, I. Ahmad, M. Khattak, 'SEECR: Secure energy efficient and cooperative routing protocol for underwater wireless sensor networks', IEEE Access, vol. 8, pp. 107419–107433, Jun., 2020.

[29] C. Zhou, M. Wang, W. Qu, Z. Lu, 'A wireless sensor network model considering energy consumption balance', Math. Probl. Eng., pp. 8592821, Jan., 2018.
[30] F. Lei, J. Cai, Q. Dai, H. Zhao, 'Deep learning based proactive caching for effective wsn-enabled vision applications', Complexity, pp. 5498606, May., 2019.
[31] M. Gunasekaran, S. Periakaruppan, 'GA-DoSLD: genetic algorithm based denial-of-sleep attack detection in WSN', Secur. Commun. Netw., pp. 9863032, Jan., 2017.
[32] G. Rahman, K. Wahid, 'LDAP: Lightweight Dynamic Auto-Reconfigurable Protocol in an IoT-Enabled WSN for Wide-Area Remote Monitoring', Remote Sens., vol. 12, no. 19, pp. 3131, Jan., 2020.
[33] P. Devi, B. Jaison, 'Protection on wireless sensor network from clone attack using the SDN-enabled hybrid clone node detection mechanisms', Comput. Commun., vol. 152, pp. 316–322, Feb., 2020.
[34] K. Cho, Y. Cho, 'HyperLedger fabric-based proactive defense against inside attackers in the WSN with trust mechanism', Electron., vol. 9, no. 10, pp. 1659, Oct., 2020.
[35] M. Premkumar, T. Sundararajan, 'DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks', Microprocess. Microsyst., vol. 79, pp. 103278, Nov., 2020.
[36] J. Luo, Z. Zhang, C. Liu, H. Luo, 'Reliable and cooperative target tracking based on WSN and WiFi in indoor wireless networks', IEEE Access, vol. 6, pp. 24846–24855, Apr., 2018.
[37] S. Lee, J. Yoon, B. Jung, 'A cooperative phase-steering technique with on-off power control for spectrum sharing-based wireless sensor networks', Sens., vol. 20, no. 7, pp. 1942, Jan., 2020.

Biographies

Sravankumar Bethi is a research scholar in the Department of Computer Science and Engineering from KL University, India, and working as Assistant Professor in Vaagdevi College of Engineering, Warangal, India. His major domain/specialization is Wireless Sensor Networks.

Nageswara Rao Moparthi is working as a Professor in the Department of Computer Science and Engineering from KL University, India. His major domain/specialization in the doctorate is Software Engineering application with Data Mining techniques. His areas of expertize are Data Mining, Data Analytics, Machine Learning, Soft Engineering, Networking & IoT. He has around 13 years of IT-Industry exposure with major MNCs as well. Currently active as Reviewer member (SCI, Scopus) & Editorial board member of International journals' publishers like Inderscience, Springer, IGI Global & Science Publishing and Organize member/TPC for 15 International conferences.