International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-12, October 2019

Performance Analysis of Heterogeneous Wireless Sensor Network using MIMO Concept

Lakshmi M, Prashanth C R

Abstract: ***In a distributed Wireless Communication Technology, the Wireless Sensor Network (WSN) is a technology developing for sensing and performing different monitoring operations. The proposed algorithm dynamically partitions the Heterogeneous Wireless Sensor Network (HWSN) in to clusters. On the basis of initial energy, the cluster head (CH) is selected in the first round and residual energy with low draining rate protocol (RELDR) is used in the next round for selecting CH. The CH senses and aggregates the data, these summarized data is processed between the clusters and the link is maintained with the base station. Cluster Authority (CA) is a member node that acts as a supervising node which contains remove list and maintains the attacker information. The Technology Multiple Input and Multiple Output(MIMO) is used in the proposed system which reduces the noise in the signal and improves the network performance. During transmission, the unauthenticated nodes which are responsible for data leakage or any malicious activities are detected by the algorithm and information of these nodes are updated in the remove list of CA. The listed unauthenticated nodes or the black hole attack nodes in CA are removed from the network. The proposed algorithm removes the malicious nodes which are affecting the network performance and reconstructs the network by considering only the legitimate nodes. Experimental results will be analyzed for the network parameters like throughput, delay, energy and Packet delivery ratio and compared with the existing systems.***

Keywords: HWSN, Cluster Formation, Authentication, Cluster Authority, Black hole attack, MIMO.

I. INTRODUCTION

A WSN [1] is a network composed of autonomous devices that are spatially distributed using sensors applicable for monitoring environmental conditions. Wireless sensor networks have gateway used for connecting wirelessly with the wired world and nodes. Sensor node or mote is defined as a point in WSN that performs processing, grouping certain data which are sensorial and broadcasting with different nodes linked in the network. Figure 1 represents the scenario of WSN consisting of nodes which may vary from several hundreds to thousands.

Revised Manuscript Received on October 30, 2019.
***** Correspondence Author
Mrs.M.Lakshmi*, Department of Telecommunication Engineering, Dr. Ambedkar Institute of Technology, Bangalore, India.
Dr.Prashanth.C.R, Department of Telecommunication Engineering,, Dr. Ambedkar Institute of Technology, Bangalore, India.

Every sensor in the network is equipped with a node; the node in the sensor network [2] consists of radio transceiver having internal antenna connected with microcontroller, external antenna and electronic circuits combined with the sensors and the battery.

Sensor nodes are deployed densely in WSN which are operated by using batteries. These devices are highly energy constrained and it is impossible to charge or change the battery regularly. For improving the stability and energy efficiency of the network in WSN the cluster based algorithms can be implemented and network lifetime is the very important parameter involved in wireless sensor network along with the power consumption.

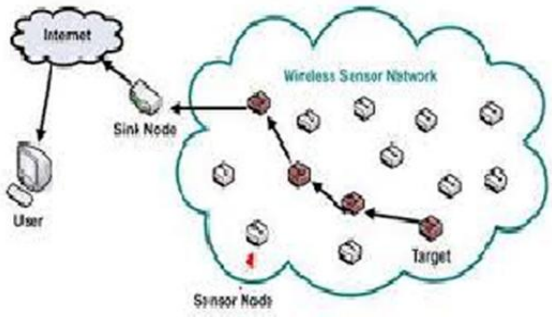

Figure 1. Scenario of WSN

Clustering [3] is the main criteria to overcome the path formation overhead. Cluster Formation is based on the Energy reserve and proximity of sensors to the CH, selected depending on the Initial energy, Residual energy, Rate at which the energy is conserved and average energy of the network. Each cluster consisting of cluster head which collects the data from the cluster members aggregates the data and then sends to the base station [4] thereby reduces the communication overhead. In the network the malicious nodes have the chance of becoming head or member of a cluster during mobility. If the malicious node becomes a cluster head, it controls the whole network or the clusters. To avoid this, the authentication of mobile sensor nodes is necessary and also security can be offered.

A technique or process of eliminating the unnecessary transmission and providing combined information to the base station by aggregating the data by multiple sensors is referred as Data Aggregation. Also network services may be interrupted which results in denial of service. Data delivery, energy efficient routing and scalability can be achieved through clustering of nodes.

Security protocols play an important role in overcoming these attacks.

Attacks are classified in to two types, passive attacks and active attacks. Listening is limited in eavesdropping, i.e. passive attacks and the exchanged traffic is analyzed. The attacker prepares an active attack by knowing the confidential information or the nodes which are significant in the network. Also the attacker modifies the data or removes the data which are broadcasted over the network and disturb the functioning by injecting the own traffic which results in replay of old messages.

Ad Hoc On-Demand Distance Vector (AODV), designed for wireless and ad hoc networks is a routing protocol. Both unicast and multicast routing are supported by establishing paths or routes to destinations on demand. Routes are built among the intermediated nodes if they are requested by source nodes. It will not create any extra traffic for communicating between links and considered as on demand algorithm. Routes will be maintained by the sources as long as it is required. To ensure route freshness, routing protocol uses sequence numbers.

Trustworthiness of the network is exploited by the Black hole attack. Occurrence of these attacks in the network acts as nodes which are not authenticated promises to route the information to the sink node and gives a false report that it has shortest path. Instead of transmitting to the sink node, it drops all the packets by threatening reliability. Malicious node is a black hole which replies falsely for Route Requests without knowing the active route to the sink which is specified and all the receiving packets will be discarded. If the node in the black hole attack is selected as a cluster head, aggregates the data from the cluster members of the cluster, then definitely energy of the node affects seriously the life of the sensors every time during CH selection mechanism. The cluster head selection in this case also affects the Network throughput, PDR and end to end delay.

MIMO Technology as displayed in Figure 2, Multiple Input and Multiple Output (MIMO) is a technology of radio antenna which uses numerous antennas at the source and destination for enabling many paths of the signal to carry the data. It selects path separately for each antenna which enables different signal paths. MIMO wireless systems works on one of the core ideas that space time signal processing in which multiple spatially distributed antennas are used inherently where the time is accomplished with the spatial dimension.

The two main formats of MIMO are described below.

Spatial diversity offers transmit and receive diversity. Signal to noise ratio is improved by the two methodologies and characterized with the improvement in reliability of the system with different fading forms.

In spatial multiplexing, the additional input or data capacity which is utilized by different paths for carrying extra traffic done by this method. It increases the capability of the data throughput.

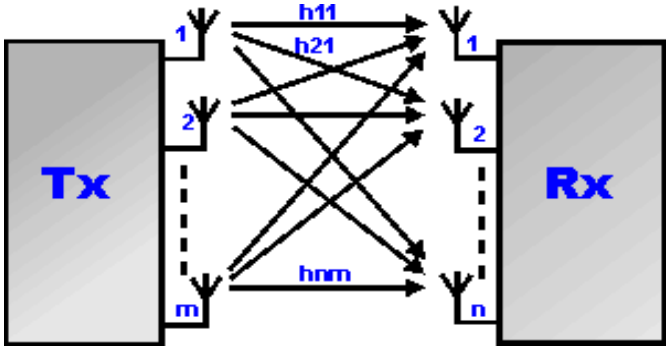

Figure 2. MIMO Technology

The Maximum rate at which error free data can be sent over a given bandwidth in the presence of noise. It is defined by Shannon's law and given by the equation (1),

$$Capacity = C = BW \log_2 (1 + SNR) \quad (1)$$

Channel capacity is denoted by C in bps, BW is the bandwidth in Hz and SNR is signal to noise ratio.

II. LITERATURE SURVEY

Lina Zhu and Zuochang Zhang [5] proposed a scheme in heterogeneous WSN having random key management. They introduced the knowledge of deployment and wireless communication range by considering q-composite random key distribution system. Improved security and connectivity have been achieved. The scheme deals with the key updating mechanism. Mohammad Taybur Rahama et al., [6] recommended a system with a protocol for the improvement of energy efficiency and the dead nodes have been reduced in the wireless sensor networks. Proposed protocol also minimizes the energy consumption, and network lifetime and PDR have been increased for any packet size.

Jin-Shyan Lee and Tsung-Yi Kao [7] have proposed hybrid of centralized gridding and distributed clustering by proposing a protocol HHCA. They introduced the protocol for energy conservation and also dealt with the network lifetime. The proposed algorithm is applicable for the WSN which has stationary sensory nodes. Renjith and Baburaj [8] have presented a survey on several types of data aggregation algorithms in the networks. They selected algorithms based on the network architecture, performance characteristics, and many approaches. They showed that these algorithms can be focused on solving query processing, security issues, and uncertainty in sensor reading.

Mingxin Yang [9] proposed a method of constructing the trees of data aggregation on the basis of the information entropy. In this they applied to the protocol the minimum spanning tree and the information entropy theory in which amount of communication can be reduced while transmitting the data. Navjot Kumar and

Surinder Kaur [10] proposed an algorithm that considers wireless sensor network and divides in to angles and clusters which are distance based regions. Path formation problem and non coverage area will be removed. They also proved that unique path will be created by the algorithm in which the data will be transmitted to the base station by choosing single node from one cluster. The results showed that aggregation improved the energy and bandwidth of the nodes in the sensor network.

Nagamalar and Rangaswamy [11] proposed an energy efficient mechanism based on the clusters using controlled flooding for the collection of data in wsn with mobile multiple sink. They also analyzed the network based on the specifications like packet delivery ratio, delay, energy consumption and life time. Authors used two mobile sinks and compared with the Virtual grid based dynamic route adjustment scheme which is a single mobile sink. They showed the network life time improvement with two mobile sinks and having optimal routes and updating of messages with limited flooding. The proposed algorithm also achieved load balancing.

Debabrata Singh et al., [12] proposed the improved energy balanced routing protocol (IEBRP). Consumption of energy is more in this protocol compared to LEACH and PEGASIS based on the level of the hierarchical routing and regioning. They analyzed the network performance, energy consumption and the no. of alive nodes and malicious nodes.

Thiruppathy Kesavan and Radhakrishnan [13] proposed a secured technique of mobility aware dynamic keying which is used in authentication of WSN. Using the advanced algorithm, they proved that the cluster head selection is based on the weight value. This weight value they calculated using the parameters, like Node Density, Dav and VBP. They also showed that the deletion of malicious nodes from the network using bidirectional malicious node detection technique. Using authenticates key management mechanisms the new cluster members which are leaving or joining the network are tested to ensure security. They also ensured that the reselection of cluster head is by the member of the clusters if the current cluster head leaves the network.

Roshini and Anandakumar [14] proposed a hierarchical cost effective LEACH protocol for enhancing energy efficiency of the sensor nodes. It also improved performance of the network without an extra cost for deployment. In this network structure the aggregators are used for forwarding the data. They used clustering for maximizing the energy efficiency of the sensor nodes. They compared the proposed protocol with other protocols for cost. The protocol decreased the cost ratio of the network deployment in terms of energy factor and capable nodes.

Praveen and Senthil [15] proposed a system for expanding the network lifetime. They achieved this by selecting farthest cluster head instead of the closest node and the formation of cluster occurs. They considered some metrics like the residual energy, density of the node and intra cluster distance. They implemented an optimization technique called Artificial Bees Colony for energy consumption and network lifetime. This effective technique of optimization designed the cluster head closest to the base station. Energy optimization of the extreme node is also done. This proposed system enhanced the network lifetime along with the energy consumption.

Kakelli Anil Kumar et al., [16] proposed Interference minimization clustering multipath routing protocol (IMCMRP) for reducing the multipath interference in heterogeneous wireless sensor networks. Compared to single path protocols, this protocol has given better performance. Multipath routing paths without localization support have been discovered by this protocol through cluster head nodes. This protocol also improved lifetime of the network and throughput.

Navjot Kumar et al., [17] suggested a Distance based angular clustering algorithm with data aggregation techniques. These techniques are used to improve the computation of various parameters which are processed. This protocol removed the flaws and points out during the reach. They also proved that the proposed protocol improves the throughput and network lifetime. Implemented protocol is also compared with other conventional distance based clustering protocols.

Sukhwinder Singh Sran et al., [18] proposed EA-COSEN (Energy Aware Chain Oriented Sensor Network) which is an existing COSEN protocol. The proposed protocol has duty cycles for saving the node energy and also three level hierarchial chains are used. Rotation policy is used for distributing the energy among chain leaders. The technique is also used for increasing the count of levels and chains. They proved that the throughput, residual energy and delay is improved.

Mohamed Saleh and Essam Sourour [19] proposed a protocol in wireless sensor network for authenticating the entities. They showed the execution which is in integration with a part of routing protocols. Proposed protocol implemented authentication which is guided by routing. Authentication of nodes is done on the path of the data to the base station. Irrelevant execution of protocol is eliminated by using advanced implementation. Also they worked out that the attacker nodes will not use the routing protocols to insert themselves in to the path.

Tuah, et al., [20] proposed an algorithm for an Efficient Three Level Energy. They considered three level hierarchical heterogeneous networks. The proposed protocol organizes the network in to the hierarchical clustering, and the cluster nodes gathers the measurement data, aggregate and transmit to the base station. The life span of the network is improved by 10 percent compared to EEHC protocol.

Ying Liao et al., [21] proposed a system by implementing an algorithm with load balanced clustering and distributed self organization for wireless sensor networks. It is of unreliable distribution which considers the optimal cluster configuration. The proposed method improves the network life cycle by forming stability, good cluster structure. Also the algorithm can be applied for different network sizes.

Sunandini Sen et al., [22] proposed an algorithm in which the sensor network has the partition considering the angular clustering and the cluster heads are situated at the network centre. Also the cluster heads acts as gateway and play a vital role in the routing path selection. The gateway nodes are static in behaviour and have computational power with higher dimension of transmission compared to other cluster nodes. The CH / gateway mote transmits sensed data to the base station collected by the sensor nodes. The responsibility of sensor nodes will be reduced by the concept of gateway nodes. The parameters sleep, idle and active is considered and only active nodes sense and broadcast data to the cluster heads. The proposed algorithm improves the node energy.

Min Xiang et al., [23] implemented a system considering a technique of one hop distance. The sensory nodes are partitioned in to static clusters and minimum energy is utilized by the cluster heads due to the network structure such as one hop distance scheme. Due to the static behaviour of the cluster heads, the battery of the cluster head will be replaced by the candidate cluster head during the execution if the cluster head is dead or out of battery.

Prabhleen Kaur et al., [24] introduced an algorithm which is energy efficient. The uniform and well distributed cluster heads are produced for removing an unbalanced cluster formation. The system selects the suitable cluster head by considering two aspects i.e. cluster's residual energy and radius. Also they have considered a self organizing structure in a distributed network which is important for generating cluster heads in WSN.

Ali et al., [25] proposed an approach of data aggregation. The other nodes interact with cluster head which is possible by using multilevel strategy. In this technique, the aggregation of data is possible in both inter cluster and intra cluster data transmission. The redundant data will be removed between the cluster members (Non CH) by aggregating the sensed data in intra cluster data transmission.

Imran Rashid et al., [26] showed a clustering algorithm that is energy efficient and relay based by considering the least distance cluster heads. In both types of wireless sensor networks, this algorithm improves the network lifetime. In this system the cluster head is selected on the basis of maximum energy of the node and the minimum distance to the sink in order to balance the consumption of energy. They also compared the results with LEACH and SEP. The proposed protocol transfers large amount of data to the sink and the network life time will be improved.

Ehsan Heidaril and Ali Movaghar [27] explained an efficient genetic algorithm on the basis of network size. The genetic algorithm depends on the distances. The two ways of calculating the distances are distance between the nodes and the cluster heads, cluster head and the base stations. The genetic algorithm mainly focuses on the shortest path and the small number of cluster heads.

Yan Wu et al., [28] implemented a method of producing sub optimal tree by approximation. Also showed how to find the maximum life time arbitrarily. If the arbitrary tree is deep, the solution results in long delay. The algorithm uses the shortest path tree where the node chooses the least hop count to the sink. The advantages of selecting the shortest path are for shorter delay. Proposed algorithm is suitable for searching an optimal shortest path tree for prolonging the lifetime to the maximum.

III. PROPOSED MODEL

In this section, Definitions and Proposed model of the system have been explained.

3.1. Definitions

Heterogeneous wsn: Heterogeneous WSN is a network having sensory nodes having different capabilities like different computing power and sensing range.

A) Authentication is the designed security measure for protecting communication system against the acceptance of fraudulent simulation or transmission by establishing the message, originator validity.

B) Clustering: For prolonging the network lifetime, it is one of the important methods. Clustering or cluster analysis is the grouping a set of objects. These objects in the same group called cluster are more similar to clusters of other groups.

C) Black hole attack: A Black hole is a node which is malicious and replies falsely for any Route Request (RREQ) to the specified sink without an active route and drops all the packets that have been received.

D) Cluster Authority: It is one of the cluster member node in which the neighbouring nodes inform about the attacker node when attack occurs.

E) Throughput: It is explained as the average number of packets transmitted or received strongly by the transmitter or receiver channel. It is denoted by bits per second.

F) Delay: Delay is a network measurement and it can be measured between messages by the time which is queued for transmission until the last bit acknowledged at the receiving node of the physical layer.

G) Packet Delivery Ratio (PDR): It is termed as the ratio of the data(number of packets) received by the destination to the data generated by the source.

3.2. Proposed Method

Figure. 3 shows the flow diagram of the proposed scheme. In this model, heterogeneous network comprises of many nodes having different energy levels. The networks consisting several nodes are partitioned in to clusters. Implemented method selects the cluster head based on the residual and initial energy and one node acts as cluster authority which receives information about the attacks from the neighboring nodes.

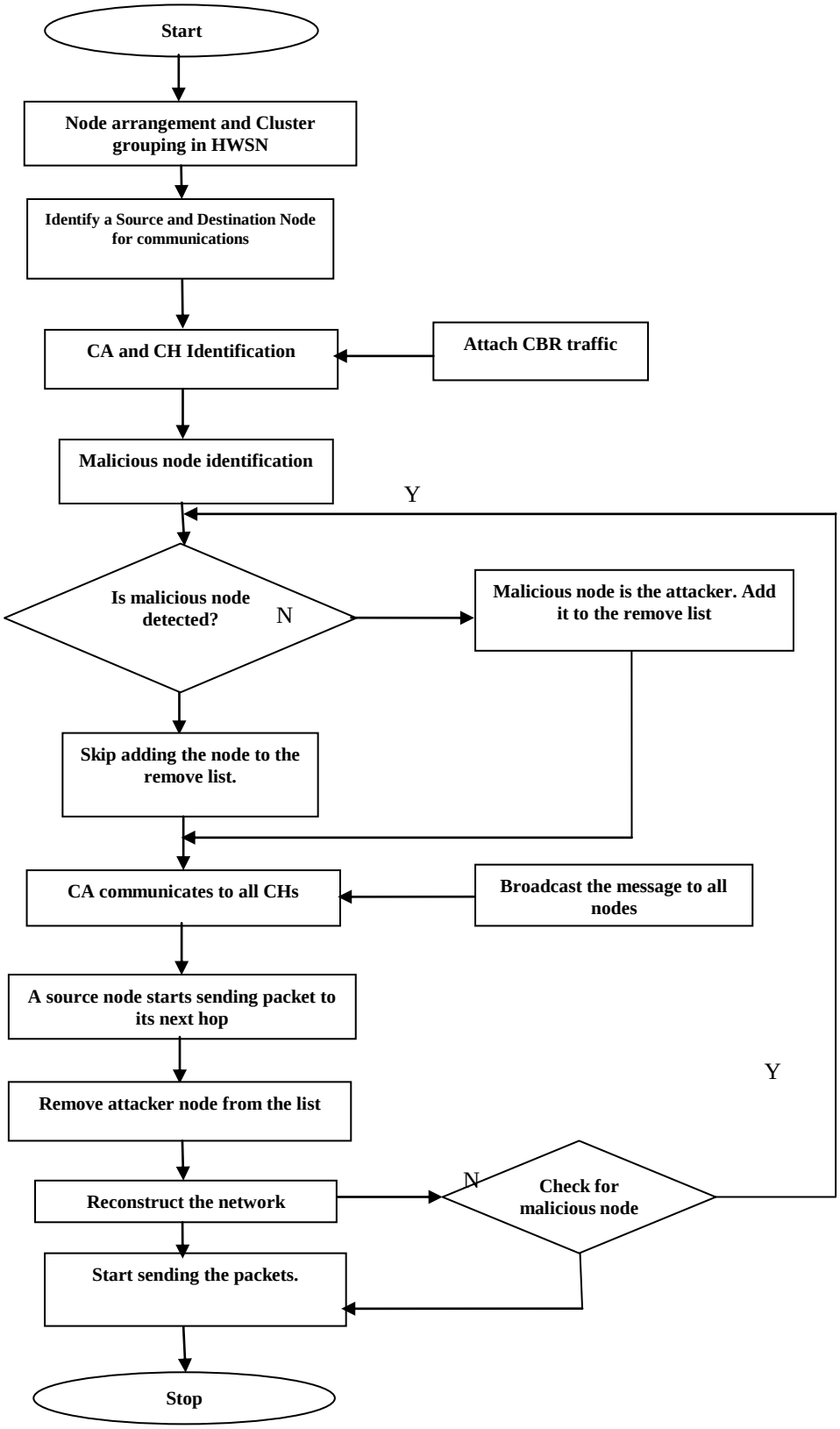

Figure 3. Flow Diagram of the proposed scheme

The main focus of the system is energy consumption and life span of the nodes. The algorithm used in the system reconstructs the Hwsn after removing the malicious nodes which attacks the network. Working stages of the model defines important steps as explained below.

A) Setting up Heterogeneous wireless topology: The heterogeneous network comprises of many nodes having different energy levels. The environmental settings, node configuration and topologies are defined here.

B) Node Arrangement and Cluster Grouping: This includes the node functions, range and channels used in the system. Network is partitioned in to clusters consisting of number of nodes with energy levels. Each node is being assigned certain values of bandwidth and threshold.

C) Specification of source, destination and data: The transmitting node, amount of data to be sent and the receiving node must be specified.

D) CA and CH Identification: Euclidian distance concept is used to identify the intermediate nodes. In the proposed scheme, the CH is elected on the basis of residual and initial energy. One node acts as cluster authority CA receiving information about the attacks from the neighbouring nodes.

E) Malicious Node Identification and detection: Black Hole attack is inserted to the network which degrades network performance. A node is detected using an algorithm which is responsible for data leakage.

F) Insertion in to Remove list: CA receives the node information before transmission. If the attacker node attacks the network, CA receives the attacker information and inserts in to the remove list.

G) Transmission Process: In this process, broadcasting of data from source to the destination takes place. During transmission the attacker information will be entered by the CA and added to remove list.

H) Reconstruction of the network: Malicious nodes under remove list of CA are removed from the network and the reconstruction takes place considering only legitimate nodes.

3.3. Algorithms for Node Placement and Cluster Formation

The random deployment of nodes in the network takes place by an algorithm. Placement of nodes are showed and dispersed across the clusters.

3.3.1 Node Placement Algorithm

Table 1 shows an algorithm for placing of nodes in a grid topology. The distance of the first node is considered as 0 initially. The distance of the next node is calculated based on the position and distance of the previous nodes.

Table 1. Node Placement Algorithm

Step 1. Consider the count of nodes, and distance between the nodes.
Step 2. Assume i as 1 to the ratio of N_{nodes}
Step 3. Distance of the first node = n0-=0
Step 4. Distance of the next node= position of n0+ distance
Step 5. Generate the node id as i
Step 6. Create a map of node id and position of node.
Step 7 Calculate I=i+1

3.3.2 Calculation of Neighbouring nodes

After the nodes deployment in the heterogeneous wsn, the intermediate nodes distance calculation is done using the Euclidian distance concept. Euclidian distance is defined as the straight line distance between two points. Generally in a plane with p1 at (x1, y1) and p2 at (x2, y2), it is $\sqrt{((x1 - x2)^2 + (y1 - y2)^2)}$. In a network, consider two nodes N1 and N2 deployed randomly in a network. Using Euclidian distance formula the distance between the neighbouring nodes can be calculated as given in Equation (2),

$$Dist(N1, N2) = \sqrt{\sum_{i=1}^{n} (N1i - N2i)} \quad (2)$$

3.3.3 Cluster Formation Algorithm

Sensor node is the basic component of a wireless sensor network. These play a vital role in a network by sensing, storing the data, routing and processing. Communication task can be made simpler by the clusters which are the organizational unit of WSNs. The densely populated networks can be broken down in to clusters. Each cluster in a network has an organizational leader referred as cluster head. These cluster heads performs many activities. Data aggregation, scheduling communication of a cluster are the tasks performed by cluster head. Upper level of hierarchical wsn is the base station and the path of interaction is provided between the network and the end user by the base station. There are numerous applications which use the data in a sensor network. The data can be used over the internet by a particular application using desktop computer. End user generates the queries and the required data for these queries will be sent through the network [30 – 39]. Cluster formation algorithm as shown in the Table 2 partitions the heterogeneous wireless sensor network in to regions and districts.

Table 2. Cluster Formation Algorithm

Step 1: Consider the number of clusters, Clusters end points, and Number of nodes in each cluster.
Step 2: Assume node as i and check if i is less than or equal to $N_{Clusters}$
Step 3: If condition is not satisfied go to step 8.
Step 4: Pick the appropriate end points for the i^{th} cluster if the condition is satisfied.
Step 5: Place the nodes in the cluster by executing the node deployment algorithm.
Step 6: Generate the Cluster ID for the cluster.
Step 7: Repeat step 2.
Step 8: Heterogeneous cluster formation is complete**.**

Artificial Hierarchical structure is considered for the partition of network in order to minimize the number of entries in the routing table. This algorithm divides the entire area in to multiple clusters. Deployment of nodes in a cluster is done by using this algorithm. Entire grid area is split in to clusters and each having the limits of X and Y regions i.e. with some Xmin, Xmax and Ymin, Ymax.

3.3.4 Algorithm for detection and prevention of Black hole attack

Table 3 describes a proposed algorithm for detecting and preventing the black hole attack. Only legitimate nodes of the network are considered for the technique. The details of the malicious node will be sent to the cluster authority node which acts as the back bone node for restricted IP address and the transmitted node periodically requests for the information.

If the node sends the data, it simultaneously broadcast RREQ in search of sink node and also Cluster Authority which acts as node with restricted IP address. When the black hole nodes replies for the requests, reply will be with RIP. The source node initiates with the procedure of detecting the malicious nodes.

Table 3. Black Hole Detection and Prevention

Step1: Check the energy of all the nodes. Select the Cluster Head CH based on the maximum initial energy in the first round.

Step 2: Source Node CH, SN_{CH} broadcast Route Request (RREQ) packet.

Step 3: The Intermediate Node IN_{CH} receives Route Reply(RREP), Routing Information Entry(RIE) of IN_{CH}

Step 4: If the Sequence number of IN_{CH} > TF_BH, then current IN_{CH} will be considered as malicious node (Black hole node).

Else Route the data packets to IN_{CH}, Current Intermediate Node, Current_IN= Next Hop Node, NHN_CH.

Step 5: If IN_{CH} is a compromised node, then Broadcast further request of CH, FRst_CH to NHN_CH. Broadcast the information simultaneously Cluster Authority , CA.

Step 6: Further Request Reply, FR_{rp}_CH and RIE of NHN_CH.

Step 7: If malicious node is not found, broadcast packets to the selected NHN_CH.

Step 8: Consider NHN_CH=SN_{CH}

Step 9: Repeat from step 1while NHN_CH is Destination node, DN_{CH}.

IV. WORKING STAGES OF THE PROPOSED MODEL

The implemented work has following phases; in first phase the network performance is analyzed with respect to energy utilization by injecting black hole attack on some nodes in the clusters. In second phase, the malicious node due to black hole attack is detected and prevented in becoming CH and removed from the network. In third phase, the reconstruction of network takes place by including only non malicious nodes. Performance is analyzed in terms of throughput, packet delivery ratio, end to end delay and energy. The simulation tool for the analysis of the work is NS 2.35 which is installed on ubuntu operating system. The simulation parameters are shown in Table 4. The Focus of the work is mainly to analyze the network performance in presence of Black hole attack and using MIMO concept.

Table 4. Simulation Parameters

Description	Values
Network Simulator	2.35
Number of Nodes	100
Simulation area	1300*1300 m
Propagation model	Two Ray ground
Energy Model	Radio
Initial energy of sensor nodes	99 J
Packet size	4000 bits
Traffic source	CBR
Transmission power	0.14
Channel type	Wireless type
Transmission range	250m
Mac type	IEEE 802.11

4.1. Network Initialization

In Figure. 4, nodes animation window shows the deployment of nodes randomly in a flat grid topology. It is necessary to set up environmental settings radio propagation model, type of antenna, link layer, queue type, channel type routing protocol, interface type. There are 103 nodes created in the grid layout.

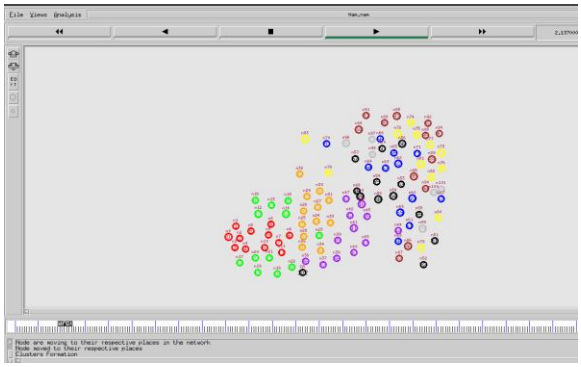

Figure 4. Node Deployment

4.2. Cluster Formation

Figure. 5 shows the design in NS2 in the form of cluster construction. Each node that is deployed randomly should send sample (Hello) packets to its neighbor nodes those within its communication range for updating the topology. Total 103 nodes are considered in which node 102 acts as cluster authority. Grouping of nodes is formed. Out of 102 nodes, 17 groups i.e. clusters are formed. Calculation of distance between each and every pair is done. Cluster member is considered if the distance is within the transmission range.

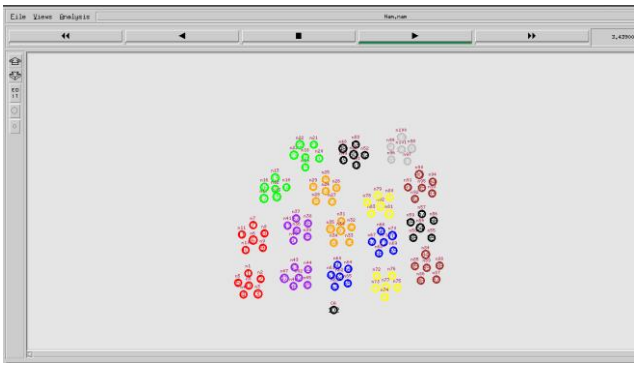

Figure 5. Cluster Formation

Node 102 is cluster authority which is deployed in the cluster based scheme to inform all the nodes on the attacker node. CA has Remove list for holding the malicious node information after detection. The malicious nodes which are in the remove list are removed from the network. The malicious nodes which are dropping the packets damage the network functioning and also the performance. The Malicious nodes detected in the network are removed by reconstructing the network including only the non malicious nodes.

CH is preferred based on highest initial energy of the nodes which are placed randomly in the flat grid field. Since cluster head selection is rotation based, residual energy is also considered while selecting cluster head in the next round. RELDR protocol first calculates the maximum residual energy. The Difference between the consumed energy (Ec) and initial energy(Ei) gives the residual energy. Initial energy is the energy given at the beginning to all the nodes in the network. Consumed energy is rate of packet flow and the packet size. The equation (3) shows the residual energy (Er).

$$Er = Ei - Ec \quad (3)$$

4.3. Routing Protocol (AODV)

There are two packets in route discovery process i.e. ROUTE REQUEST(RREQ) and ROUTEREPLY(RREP). The source node using RREQ packets requests the route. The route request generated by the transmitting node is forwarded to the neighbouring nodes of the source and the process is repeated till the destination is reached. Intermediate node on receiving the RREQ data packets, generates RREP mentioning number of hops needed to reach the destination. Data transmission is established using Constant Bit Rate(CBR) traffic.

In the Implemented work, routing is dynamic that changes the routing table and provides best path for data transmission. Dynamic routing is suitable for selecting best route, detection of route changes, and discovering the remote networks. It consumes more bandwidth as the routers share updates.

AODV routing protocol is used in the implemented work,

- As the destination sequence number is used (Route is measured by the number of hops). Loop freedom and freshness of the route is guaranteed which reduces the number of broadcasts by identifying routes on the basis of demand which is not the case for other protocols.
- As the number of node increments in the network, the End to End Delay and Packet Drop Rate is less in AODV protocol compared to DSR protocol.

4.4. Simulation Results and Analysis

Analysis of simulation results [29] uses NS2 shows improvement in Throughput, Delay, PDR, and Energy shown in the following figures. Adaptive algorithm is used to improve the parameters.

4.4.1 Packet Delivery Ratio (PDR)

PDR is described as the ratio of the packets obtained by the receiver to the total number of packets including the packets which are dropped during transmission.

In the equation (4) $^{D\ Received}$ is the packets received from the sink node. $Dgenerated$ represents the number of data packets which is generated by the sending nodes. n is the number of sensor nodes.

$$PDR = D_{\mathrm{Re}\,ceived} * 10 / \sum_{i=1}^{n} D_{generated} \quad (4)$$

In Figure. 6 the proposed work shows the slots of simulation time in 5, 10, 15, 20 and 25 sec. Here the packet delivery ratio increases with every time slot.

In the existing system, the detection of malicious attack is done but not prevented. In the proposed system PDR is achieved by detecting and preventing malicious nodes such as black hole attack. This can be done by CA that receives the malicious node information and add to the Remove list which in turn reduces the packet drop or data leakage. And also using Dual antenna for simultaneous upload and download of messages to make the processing faster.

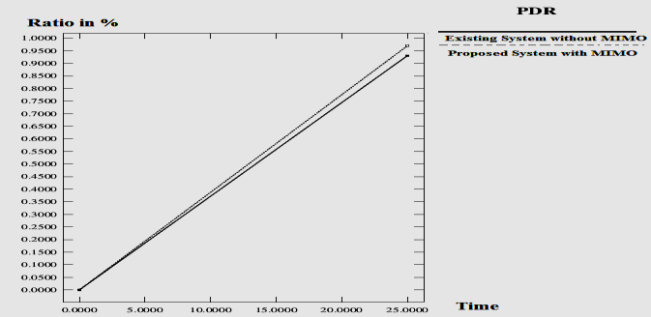

Figure 6. Comparison of PDR

Table 5 presents the comparison of values of both existing and proposed system.

Table 5. PDR of Proposed and Existing System

Simulation Point	Packet Delivery Ratio	
MAC protocol	Without MIMO	With MIMO
5	0.18	0.20
10	0.30	0.38
15	0.55	0.60
20	0.74	0.78
25	0.93	0.99

4.4.2 End to End Delay

End to End Delay can be expressed as the amount of delay which occurs between the delivery of data packets from transmitter and obtaining data at the receiver or the destination node. Figure.7 shows the analysis of end to end delay with respect to the time slots 5, 10, 15, 20 and 25 on the X-axis. Table 6 shows the comparison of Delay values of existing and proposed system.

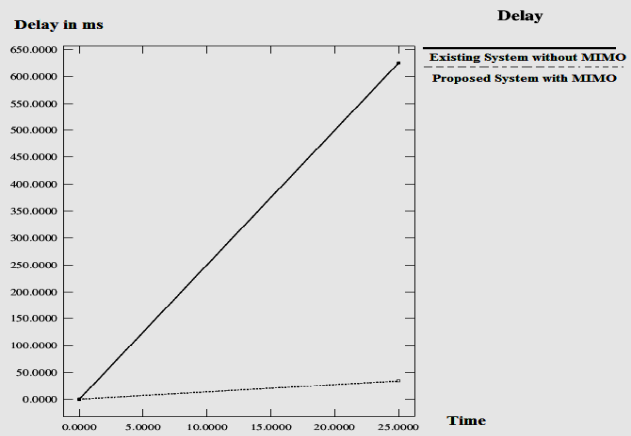

Figure 7. Comparison of End to End Delay

The value of the average delay depends on the time slots. There may be an increase or decrease in the delay value. The delay is improved in the proposed system,

- By increasing/ tuning up MAC parameters such as Short Inter-Frame Space (SIFS) used with Acknowledgement (ACK) and Clear to Send (CTS) frames, Distributed Coordination Function Inter-Frame Space(DISF) and also Clear Channel Assignment.
- And also by adjusting the transmission window size.

Table 6. End to End Delay of Proposed and Existing System

Simulation Point	End to End Delay	
MAC protocol	Without MIMO	With MIMO
5	125.96	6.92
10	248.9	13.94
15	390.25	20.78
20	512.65	27.68
25	624.8	34.6

4.4.3 Throughput

The variation of the Throughput with time in ease of the proposed system and existing system is shown in Figure.8. The Throughput is enhanced in case of proposed system compared to the existing system as the system is designed for receiving multiple inputs, processing all simultaneously and giving multiple outputs and increasing the data rate and Bandwidth.

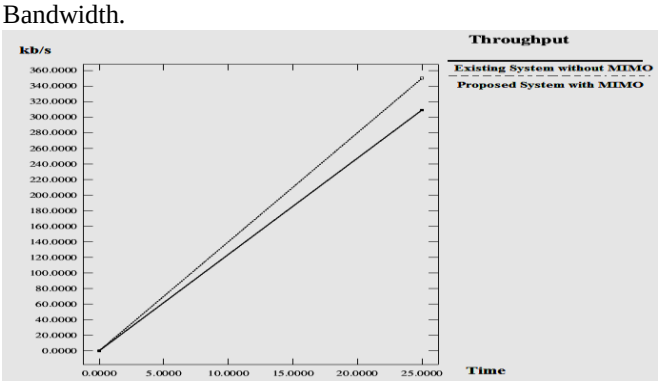

Figure 8. Comparison of Throughput

In the proposed system, AODV shows better throughput by calculating at the destination node. Since AODV avoids freshness of routes and loop throughput has high mobility simulation period. Also MIMO communication is used in the data transmission that has more number of antenna nodes which reduces Bit Error Rate and gives higher data throughput within the cluster. The values of the throughput in the system are compared with the existing for the same packets as shown in Table 7.

Table 7. Throughput of Proposed and Existing System

Simulation Point	Throughput (in kb/s)	
MAC protocol	Without MIMO	With MIMO
5	55	70
10	135	140
15	180	210
20	210	280
25	309	350

4.4.4 Energy

The energy loss in the sensor network does not depend on the size of the network. It is calculated based on the simulation time which varies and shown in Figure. 9. Energy efficiency is improved as the information from source to the destination processes faster due to multiple inputs and receiving multiple outputs. The network lifetime increases with the decrease in the energy consumption.

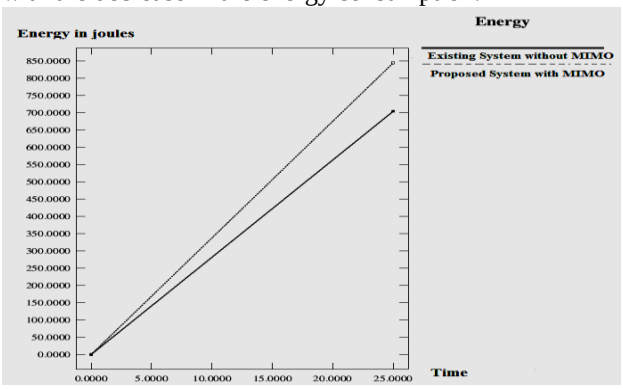

Figure 9. Comparison of Energy

Energy efficiency is improved as the information from source to the destination processes faster due to multiple inputs and receiving multiple outputs which results in extension of network lifetime. This is performed as there is an increase in antennas and the process of data transmission and reception by the nodes is redundant. Best antenna in MIMO technology is about 10% of the nodes in the cluster. Values of energy in joules for both the system is shown in Table 8.

Table 8. Energy graph of Proposed and Existing System

Simulation Point	Energy (in joules)	
MAC protocol	Without MIMO	With MIMO
5	140	169
10	281	338
15	422	507
20	563	676
25	704	845

V. CONCLUSIONS

In heterogeneous WSN, it is very much crucial to authenticate the nodes, exchange the secured data between the cluster heads and base station and avoid malicious activities. In this proposed work, the parametric measures like throughput, packet delivery ratio, end to end delay, energy are considered. Proposed algorithm uses concept of MIMO for improving the network performance by increasing the MAC parameters. RELDR protocol is used for forming clusters cluster head selection on the basis of residual energy of the nodes. Using Dual antenna and concept of MIMO saves energy which maximizes the network lifetime. The secured and efficient data is transmitted by removing the malicious nodes such as Black hole attack nodes from the network by the process of Network reconstruction. Minimal delay is achieved in the work compared to the existing system. Energy is saved that extends network lifetime. There is an improvement in network performance compared with the existing system.

ACKNOWLEDGEMENTS

Authors would like to thank all the staffs of Department of Telecommunication Engineering, Principal, Dr. Ambedkar Institute of Technology for the support given and also thankful to Technical Education Quality Improvement Programme (TEQIP-III) for providing financial support.

REFERENCES

1. Kazem sohraby, Daniel Minoli and Taieb Znati, “Wireless Sensor networks: Technology, Protocols and applications,” A John Wiley & Sons, Inc, pp. 1-303, 2007.
2. Ahmed Jedidi, "Workload Cluster Balance Algorithm to Improve Wireless Sensor Network Performance," International Journal of Communication Networks and Information Security (IJCNIS), Vol. 11, No.1, pp.105-111, 2019.
3. S.Lavanya and S Prakasam, " Performance Analysis of cluster formation schemes for energy conservation in Wireless Sensor networks, " International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies, pp.1-5, 2017.
4. Gholamreza Farahani, "Energy Consumption Reduction In Wireless Sensor Network Based On Clustering," International Journal of computer Networks and communication(IJCNC), Vol. 11, No.2, pp.33-51, 2019.
5. Lina Zhu, and Zuochang Zhang, “A Random key management scheme for Heterogeneous wireless sensor network,” International Conference on Cyber Security of smart cities, Industrial Control system and communications, pp.1-5, 2015.
6. Md.Taybur Rahama, Monir Hossen and Md. Muminur Rahman, “A Routing Protocol for Improving Energy Efficiency in Wireless Sensor Networks," The 3rd International Conference on Electrical Engineering and Information Technology, pp.1-6, 2016.
7. Jin-Shyan Lee and Tsung-Yi Kao, “An Improved Three Layer Low Energy Adaptive Clustering Hierarchy for Wireless sensor Networks,” IEEE Internet of things Journal, Vol. 3, No.6, pp. 951-958, 2016.
8. P.N Renjith and E. Baburaj, “An Analysis on Data Aggregation in Wireless Sensor Networks,” International Conference on Radar, Communication and Computing, pp.62-71, 2012.
9. Mingxin Yang, “Constructing Energy Efficient Data Aggregation Trees based on Information Entropy in Wireless Sensor Networks,” Advanced Information Technology, Electronic and Automation Control Conference, pp.527-531, 2015.
10. Navjot Kumar and Surinder Kaur, “Distance based Angular Clustering Algorithm (DACA) for Heterogeneous Wireless Sensor Networks,” Symposium on Colossal Data Analysis and Networking, pp.1-5, 2016.
11. T. Nagamalar and T. R. Rangaswamy, “Energy Efficient Cluster Based Approach for Data Collection in Wireless Sensor Networks With Multiple Mobile Sink,“ International conference on Industrial Instrumentation and Control, college of Engineering Pune, pp.348-353, 2015.
12. Debabrata Singh, Binod Kumar Pattanayak and Chandan Kumar Panda, “Analysis of an Improved Energy Balanced Routing Protocol for Wireless Sensor Network,” International Conference on Communication and Signal Processing, pp. 1807-1811, 2016.
13. Thiruppathy Kesavan and S.Radhakrishnan, “Cluster Based Secure Dynamic Keying Technique for Heterogeneous Mobile Wireless Sensor Networks,” China Communications, Vol. 13, No.6, pp. 178 - 194, 2016.
14. Roshini and H. Anandakumar, “Hierarchial Cost effective LEACH for Heterogeneous Wireless Sensor Networks,” International Conference on Advanced Computing and Communication Systems, pp. 1-7, 2015.
15. M.K.Praveen and T.Senthil, "Lifetime Maximization of Wireless Sensor Networks Using Energy-Efficient Cluster Formation Strategy," IEEE International Conference on Computational Intelligence and Computing Research, pp.1 - 5, 2014.
16. Kakelli Anil Kumar, K. Shahu Chatrapati and Addepalli V.N. Krishna, “Multipath Interference Minimization in Heterogeneous Wireless Sensor Networks for Reliable Data Transfer,” International Conference on Computer and Communication Engineering, pp. 261-266, 2016.
17. Er. Navjot Kumar and Er. Surinder Kaur, “Performance Evaluation of Distance based Angular Clustering Algorithm (DACA) using Data Aggregation for Heterogeneous WSN,” International Conference on Computation of Power, Energy Information and Communication, pp. 97-101, 2016.
18. Sukhwinder Singh Sran, Lakhwinder Kaur, Gurjeet Kaur and Sukhpreet Kaur Sidhu, “Energy Aware Chain Based Data Aggregation Scheme for Wireless Sensor Network,” International Conference on Energy Systems and Applications, pp.113-117, 2015.
19. Mohamed Saleh and Essam Sourour, “Authentication in Flat Wireless Sensor Networks with Mobile Nodes,” 12th International Conference on Networking, Sensing and Control, pp. 208 - 212, 2015.
20. N.Tuah, M. Ismail and K. Jumari, “Energy Efficient Algorithm for Heterogeneous Wireless Sensor Network,” IEEE International Conference on Control System, Computing and Engineering, pp. 92-96, 2011.
21. Ying Liao, Huan Qi and Weiqun Li, “Load-Balanced Clustering Algorithm With Distributed Self-Organization for Wireless Sensor Networks,” IEEE Sensors Journal, Vol. 13, No. 5, pp. 1498–1506, 2013.
22. Sunandini Sen, Dipanjali Karmakar and S.K Setua, “An Power Efficient Algorithm for Distributed Ad-Hoc Cluster Based Wireless Sensor Network,” Third International Conference on Computer, Communication, Control and Information Technology, pp. 1-6, 2015.
23. Min Xiang, Weiren Shi, Xiaohui Zhang, Zhiyong Luo and Xia Yang, “A New Clustering Algorithm Based on the Optimum One-Hop Distance in Wireless Sensor Networks," International Conference on Embedded Software and Systems, pp. 35-39, 2008.
24. Prabhleen Kaur and Rajdeep Singh, “DDEC: Distance based Deterministic Energy Efficient Clustering Protocol for Wireless Sensor Networks,” International Conference on Advances in Computing, Communications and Informatics, pp. 2169-2173, 2014.

25. Ali, I, Khan R, Hassan M and Ahmad M, "Energy Aware Routing and Data Aggregation in Wireless Sensor Networks," 2nd International Conference on Machine Learning and Computer Science, pp. 6-7, 2013.
26. Imran Rashid, M. Adnan Nasim and Adeel Akram, "Relay based clustering with least distance cluster head selection for wireless sensor networks,"15th IEEE International Conference on Communication Technology, pp.545-548, 2013.
27. Ehsan Heidaril and Ali Movaghar, "An efficient method based on genetic algorithms to solve sensor network optimization problem," International journal on applications of graph theory in wireless ad hoc networks and sensor networks, vol.3, no.1, pp. 18-33, 2011.
28. Yan Wu, Sonia Fahmy and Ness B. Shroff, " On the Construction of a Maximum-Lifetime Data Gathering Tree in Sensor Networks: NP-Completeness and Approximation Algorithm," IEEE INFOCOM 2008 - The 27th Conference on Computer Communications, pp. 1013-1021, April 2008.
29. Rajiv Thapa, Harsukhpreet Singh and Anurag Sharma, "A Comparative Analysis of LEACH and SEP using NS2," 8th International Conference on Computing, Communication and Networking Technologies, pp.1-4, 2017.
30. Rajendran T & Sridhar K P, "Epileptic seizure classification using feed forward neural network based on parametric features". International Journal of Pharmaceutical Research, 10(4): 189-196, 2018.
31. Hariraj V, Khairunizam W, Vikneswaran V, Ibrahim Z, Shahriman A B, Razlan Z M, Rajendran T, Sathiyasheelan R, "Fuzzy multi-layer SVM classification of breast cancer mammogram images", International Journal of Mechanical Engineering and Technology, 9(8): 1281-1299, 2018.
32. Muthu F, Aravinth T S & Rajendran T, "Design of CMOS 8-bit parallel adder energy efficient structure using SR-CPL logic style", Pakistan Journal of Biotechnology, 14(Special Issue II): 257-260, 2017.
33. Yuvaraj P, Rajendran T & Subramaniam K, "Design of 4-bit multiplexer using Sub-Threshold Adiabatic Logic (STAL)", Pakistan Journal of Biotechnology, 14(Special Issue II): 261-264, 2017.
34. Keerthivasan S, Mahendrababu G R & Rajendran T, "Design of low intricate 10-bit current steering digital to analog converter circuitry using full swing GDI", Pakistan Journal of Biotechnology, 14(Special Issue II): 204-208, 2017.
35. Vijayakumar P, Rajendran T & Mahendrababu G R, "Efficient implementation of decoder using modified soft decoding algorithm in Golay (24,12) code", Pakistan Journal of Biotechnology, 14(Special Issue II): 200-203, 2017.
36. Rajendran T & Sridhar K P, "Epileptic Seizure-Classification using Probabilistic Neural Network based on Parametric Features", Journal of International Pharmaceutical Research 46(1): 209-216, 2019.
37. Rajendran T, et al., "Recent Innovations in Soft Computing Applications", Current Signal Transduction Therapy, (Article in Press), 2019.
38. Emayavaramban G, et al., "Identifying User Suitability in sEMG Based Hand Prosthesis Using Neural Networks", Current Signal Transduction Therapy, 2019.
39. Rajendran T & Sridhar K P, "An Overview of EEG Seizure Detection Units and Identifying their Complexity- A Review", Current Signal Transduction Therapy, 2019.

AUTHOR PROFILE

Mrs.M.Laskhmi, received the BE degree in Telecommunication Engineering from R V College of Engineering, Bangalore, and the M. Tech in Digital Communication and Networking from Dr. Ambedkar Institute of Technology in 2014. Currently pursuing PhD in Dr. Ambedkar Institute of Technology, Bangalore. Her research interests include Wireless Sensor Network and Digital Communication.

Dr.Prashanth.C.R, received the B E degree in Electronics, the M E degree in Digital Communication and the Ph.D. degree in Computer Science and Engineering from Bangalore University, Bangalore. He is currently Professor, Department of Telecommunication Engineering, P G Coordinator, and Deputy Controller of Examinations, Dr. Ambedkar Institute of Technology, Bangalore. His research interests include Image Processing, Pattern Recognition
Biometrics, Computer Networks, Communication Engineering and Nano Physics.

He has over 25 research publications in refereed International Journals and Conference Proceedings. He has served as a member of Board of Examiners for Bangalore University and Visvesvaraya Technological University. He is a member of IEEE, ACM and IACSIT, and life member of Indian Society for Technical Education, New Delhi and Fellow of Institution of Engineers (India).