Effective Load balancing Secure Energy Efficient Approach for WSN

Natraj N.A.* and Bhavani S.
Department of ECE, Karpagam University, Coimbatore, INDIA
*vallanat@gmail.com

Abstract

Wireless Sensor Network (WSN), a major network which is widely used in both commercial and domestic applications. It is also used in security environment. It consists of sensor nodes which is located either stationery or dynamic. Compared to ad hoc node, sensor node consumes less energy and its lifetime is more. In previous work, either energy or suspicious node was focused to progress the performance of the network. In this work, an Effective Load balancing Secure Energy Efficient Approach (ELSEEA) is proposed to attain more energy efficiency in the presence of suspicious environment. In the first part of this approach, load balancing between cluster head and cluster member is achieved through the discovery of multipath routes. In second part, detection of suspicious node is achieved through the reliability model. In third part, energy spent for routing after the removal of suspicious node is estimated to improve the lifespan of the network. Based on the simulations using NS 2 tool, the projected work attains greater performance in the presence of suspicious environment.

Keywords: WSN, Energy, Suspicious node, Load balancing, Reliability model, Network lifetime, Detection rate and Detection time.

Introduction

WSNs contain nodes which are unattended. These nodes are organized in random manner which supports an ad hoc network. It has restricted capacity and consumes minimum energy compared to mobile nodes. Some other nodes are acting as gateway nodes used for progression and storing the data gathered from the network. Energy is an important resource in data gathering process. Here battery is a major concern which is neither replaceable nor rechargeable. Energy generating unit is a major part which conserves around 1J or 2J. It totally limits the span of sensor networks.

To improve the network lifespan, energy should be accumulated in all the hardware and software solution composed in the network architecture. In accordance with the radio model projected in[1], data communication is accountable for the large energy weight budget while compared to the data sensing and processing. Hence, use of shorter range is desirable in its place of longer-range communication among sensor nodes due to its requirement of transmission power. In WSN situations, events can be sensed through source nodes close to the fact of interest and distant from the sink nodes.

Next, shorter-range of communication leads to data packets being presumptuous by means of intermediate nodes along with a multi-hop path[2].

Security is also taking another impact of WSN. It also affects the energy level during route maintenance process. To control energy consumption, it is desired to defend attackers in the network. Suspicious node is a major issue that affects the whole performance of the system. It also consumes more resources in the network i.e. bandwidth, energy etc. To identify these nodes, there are several methods developed for security purpose.

In the proposed research work, it is mainly focusing on balancing suspicious node detection and energy conservation in the WSN.

Related Work

Sohail Jabbar et al[3] developed an energy based routing for increasing throughput in WSN. The multilayer cross design is exploited in this routing to select nodes, to provide rotation of cluster head and to achieve cluster routing both inside and outside network. To reduce packet dropping and to increase throughput, the role of cluster head is modified in accordance with threshold values of node parameters. From the results, it is justified that more clusters produce less packet dropping and choosing reliable nodes which leads to increased throughput.

Khushbu Babbar et al[4] performed the investigation of energy efficient routing in wireless sensor networks. It was concluded that genetic algorithm supports energy efficiency. Genetic algorithm based cluster routing was introduced for increasing network lifetime. During Cluster head election, the K mean algorithm is deployed in routing. Cluster head was chosen by Base station using genetic algorithm. Coverage region was also improved with the help of genetic algorithm.

Jeba anandh and Baburaj[5] have made an analytical result for hierarchical routing protocol to detect basic issues related to clustered routing protocols and the impact on energy consumption. The techniques for creating cluster group which is a basic requirement for data communication. The reconnection of routing process was initiated based on the mobility of nodes. Load balancing over variable cluster sizes was also discussed. It was concluded that hierarchical routing consumes minimum energy and increases the network lifetime of WSN.

Venu Madhav and Sarma[6] introduced an Improved Energy Efficient LEACH to increase the network lifetime in all scale networks. Network stability and date aggregation were considered in cluster design. It achieved more energy efficiency by choosing minimum hop between the nodes.

Prabha et al[7] proposed the Trust Aware Energy Efficient Routing algorithm to accomplish network level security. The vulnerability of intruders is reduced by means of trust aware routing. The identity, location and data privacy of nodes were kept confidential to safeguard network from attackers. The packets are forwarded through trusted intermediate nodes to destination node based on location privacy algorithm.

Nikolidakis et al[8] developed an Equalized Cluster Head Election Routing Protocol to expand the network lifespan. The cluster head election was implemented based on linear network model using Gaussian elimination algorithm. Newly joining nodes were allowed in the system and its behaviour was also adjusted based on Signal to Noise Ration (SNR) with the inclusion of node mobility.

Chang[9] proposed an Energy-Aware, Cluster- Based Routing Algorithm to enhance the network's lifespan. The cluster head is chosen based on Voronoi diagrams and it is rotated to balance load in a cluster group. The two-tier architecture had been intended to improve the performance of the cluster based routing. All the intermediate sensor nodes transmitted its data to cluster head which forward total data to destination node. During intra cluster head rotation, cluster head is chosen and load is balanced to avoid collisions.

Balavalad et al[10] have proposed Multipath-LEACH for energy efficient routing in wireless sensor networks. Each area with individual cluster head is divided into cells and the communication of nodes will be with particular cluster head only. The cluster head communicates with sensor nodes of particular cell and the corresponding base station which results in more energy efficiency and high network lifetime.

Santar Pal singh and Sharma[11] reviewed the performance analysis of cluster routing algorithms. The taxonomy of relevant attributes of clustering techniques was also done. The merits and limitations of different cluster based routing algorithms were presented. Based on the analysis, it was concluded that cluster based routing algorithms are useful for energy efficiency in WSN.

Parekh Pranav and Joshi[12] developed an Energy-LEACH protocol to increase the easiest way of cluster head election process. The residual energy of node acts as main matrix to decide cluster head selection. In the initial round, cluster head election was done. In second round communication, residual energy of nodes was estimated.

Taruna et al[13] proposed a zone based clustering head selection algorithm for homogeneous wireless sensor networks. All the network nodes are evenly distributed. Network performance was increased by choosing cluster heads based on residual energy of sensor nodes and next hop distance.

Supriya das and Shanthis bala[14] proposed a clustering routing algorithm to enhance the lifetime of the sensor network lifetime based on cluster head's remaining energy and the space amid the cluster members and consequent cluster heads. It was intended to improve the entire network lifespan by means of improving all nodes lifetime and next hop distance between cluster member and cluster head. Self-selection of optimized clusters were also proposed to provide improved network performance.

Juan Luo et al[15] focused on minimizing energy utilization and maximizing sensor networks lifetime. The opportunistic routing theory was established for optimizing the energy efficiency of the network on the difference between sensor nodes regarding distance to destination node. The opportunistic routing theory was determined to recognize the relay node with respect to the optimal transmission distance. The network lifetime was prolonged by keeping nodes along with low remaining energy proactively.

Bhagwan Singh and Pawan Luthra[16] introduced the concept of Fuzzy Based PEGASIS to extend the network lifespan by reduction of overhead and delay. The transmission of data is entirely based on the formation of double cluster heads which works on the LEACH hierarchical routing scheme. It minimizes the time required in data transmission from one sensor node to another.

Rajeev Arya and Sharma[17] proposed energy efficient and bandwidth assessment based on hierarchical protocol. The data centric protocol with optimization method was considered in this work. Ant Colony Optimization (ACO) was used with rumor routing protocol. The route search was optimized and established with minimum probability of loop route.

Saleem et al[18] presented a form of self-optimized multipath routing algorithm for WSN. There were some constraints considered as energy level, delay and velocity. This selection of parameters has turned up with the optimal and systematized path for WSN. Additionally, the stated algorithm was improved with the multipath capability to evade congestion state. It helps WSN in maximizing the data throughput rate and to minimize the data loss.

Proposed energy efficient security system: The major objective of this proposed system is to identify the suspicious node in the network during dynamic environment. This system is designed based on reliability of nodes, route reputation, and node's reputation based on control packets and data packets. Multipath is constructed once the cluster organization is completed. Routes are initialized once the reliability of nodes is computed. The proposed system weakens the vulnerability of attackers in ad hoc network. To combat against attackers, the routes are installed with high link stability. Links are discovered with low bit error rate. The proposed system consists of three modules i.e. construction of Multipath routing, Detection of suspicious nodes through reliable model and Energy efficient model.

Construction of Multipath Routing: In the existing multipath algorithms, the paths are node – disjoint which leads to maximum interference and maximum collision. It is required to construct the individual paths with least interference. In our proposed multipath routing, shortest path is established initially and then packets are forwarded from Cluster Head (CH) to cluster member. To avoid such interference, a segment is formed and the distance between two paths is orthogonal to CH to cluster member nodes. Optimal path is chosen based on energy consumption, traffic and stability of links.

Step 1: Multiple paths are established between CH and cluster members.
Step 2: Cluster Head sends the Route Query (RQ) packets to cluster members to find optimum route.
Step 3: Cluster member collects the status of path selection and send the report in terms of Route Reply (RREP) packets to Cluster Head (CH). In these control packets, only the status of path information will be collected.
Step 4: If any node does not reply to CH, the path may be considered as broken and it will be recovered based on Path Re- Initialization procedure. In this procedure, the rate of packet lost and path elapsed time will be measured.
Step 5: Construct the path with least interference rate and minimum energy consumption.
Step 6: Choose the optimal path based on average speed (S_{Avg}). The selection of optimal path is as follows,

$$S_{Avg} = \frac{\sum d}{\sum \tau}$$

$\sum d$ is the sum of distances between the neighbor nodes. $\sum \tau$ means the sum of delay times of the intermediate nodes with minimum hop count.

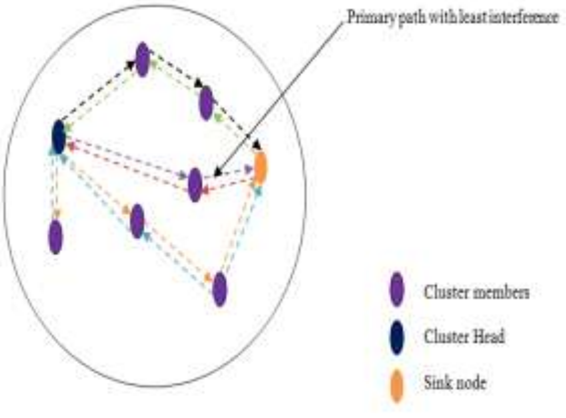

Figure 1: Multipath construction

In figure 1, multiple paths are discovered from cluster head to cluster members. To increase the data forwarding, paths are chosen based on least interference to avoid collision. The traffic is regulated once the paths are discovered. Primary path is chosen based on minimum energy consumption, least interference and more data forwarding rate. Packets are forwarded through primary path to destination via cluster members. Cluster head is responsible for deciding path selection to route the packets. If any path goes beyond the packet lost level, the path will be given as second priority. Using path re-initialization procedure, path is installed with more stability with least interference.

In the proposed cluster multipath routing, cluster members communicate to CH via multipath routes. In each and every route discovery process, CH records the status of link stability, Link Expiry Rate (LER) and Energy Consumption Rate (ECR). For data forwarding process, CH will choose only reliable links based on the above said parameters.

Detection of Suspicious Nodes through reliability model: The proposed reliable model is used to estimate node's reputation and implement route reputation relying on data packets and control packets. The reputation of route is determined based on number of hop between nodes, and neighbor node's reliability. Reliability of Route $\{N_s, N_{i_1}, N_{i_2}, N_{i_{13}}, ...N_D\}$ is calculated as,

$$RM_n = \begin{cases} TV_s \times ...... \times TV_D & \forall TV_n > 0 \\ -1 & \forall TV_n < 0 \end{cases}$$

Where $N_{i_1}, N_{i2} \cdots$ are neighbor node's. The reliability of route is composed of trust values of neighbor nodes in all routes. Trust value of neighbor nodes is ranged between 0 and 1, when the route contains more forwarding nodes. The shorter route achieves high route reliability even the trust value closes 1. If more number of malicious nodes present in particular route, the value of route reliability will be lower. The efficiency and reliability of path can be improved based on the route reliability. In this case, node reliability is independent of route reliability. A node can select more reliable nodes with low reliability of routes.

The proposed system determines the suspicious nodes based on the estimation of straight and circuitous recommendation of nodes, estimation of trust recommendation records, and clock based certificate determination.

Step 1: Straight recommendation of nodes
The straight recommendation of node is defined as the ratio of number of packets successfully sent to the number of packets successfully received at the destination. Including this, stability of node is also added to improve reliability. It is given as follows:

$$SR_n = \frac{\sum W_s}{\sum W_d}$$

W_s is number of packets successfully sent from source nodes.

W_d is number of packets successfully received from destination nodes.

Step 2: Circuitous recommendation of nodes
Once the direct recommendation is announced to all neighbor nodes, the information about target node is initiated to gather from all neighbor nodes. Hence the recommendation control request packets will be broadcasted to all multicast nodes. The reply packets from multicast neighbor nodes will be sent to source node.

The trust threshold counter value (TT_c) is determined in this recommendation estimation and it is used to find the experience of nodes based on its previous communication. The circuitous recommendation is given as below,

$$CR_n = TT_c \times SR_n$$

The previous communication $(PC_{s,d})$ of source node *s* and destination node *d* is determined as,

$$PC_{s,d} = 1 - \frac{1}{\max\left[(h_s R_{(s,d)} - t_s UR_{(s,d)}),0\right]+1}$$

$R_{(s,d)}$ is reliable communication in the past history of source and destination node.

$UR_{(s,d)}$ is unreliable communication in the past history of source and destination node.

h_s, t_s are the process period spent on reliable communication and unreliable communication. It is given as low, medium and high.

Trust Recommendation Record Estimation: Trust recommendation involves the trust factors are assigned with weights and these are estimated and quantified in trust quantification step. It is defined W_i as a weight which represents importance from 0 (unimportant) to +1 (most important). *PRC* is the packet receiving capability of neighbor nodes. This weight is dynamic and based on the application. Hence, the TRR for node *k* is computed by the following equation:

$$TRR_k = \frac{W_1 SR + W_2 CR + W_3 RM + W_4 PRC}{\sum_{k=1}^{n} W_k} \qquad (6)$$

where $0 < W_k \leq 1$.

Energy Efficient Model: The security system concerned with transmitter energy and receiver energy. The energy devoured by transmitter and receiver is computed with respect to the data packets, node location estimation, energy spent for doubtful node elimination and distance among the transmitter and receiver.

Proposed packet format:

Cluster head ID	Cluster member ID	Energy spent for suspicious node	Detection rate	FCS	CRC
2	2	4	4	4	2

Figure 2: Proposed Packet format

In figure 2. the proposed packet format is shown. Here the cluster head and cluster member ID carries 2 bytes. Third one is energy spent for suspicious node. Detection rate occupies the fourth field which updates the status of suspicious node arrival and it is reported to cluster head. Frame Check Sequence is the fifth field to denote error identification in the packet. The last filed CRC i.e. Cyclic Redundancy Check which is meant for error correction and detection in packet during route maintenance process.

Performance Evaluation
A. Simulation Model and Parameters: The proposed approach is simulated in Network Simulator tool (NS 2.34). In this simulation, 100 mobile nodes progress in a 1000 meter x 1000 meter square region for 100 seconds of simulation time. We presume that the entire nodes moves independently with the similar average speed. Each and every node has the similar transmission range of 200 meters. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and parameters are given in table 1.

Table 1. ELSEEA simulation settings

No. of Nodes	**100**
Area Size	1000 X 1000 Sq.m
Mac	802.11
Radio Range	200m
Simulation Time	100 sec
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Protocol	LEACH

B. Performance Metrics: We assess majorly the performance in accordance with Detection rate, Average delay, and Packet Delivery Ratio. The simulation results are presented in the next part. We compare our proposed approach with ECHERP[8] and ENSOR[15] in the presence of suspicious node environment.

C. Results: In our First experiment, we vary the no. of suspicious nodes as 20, 30 up to 100.

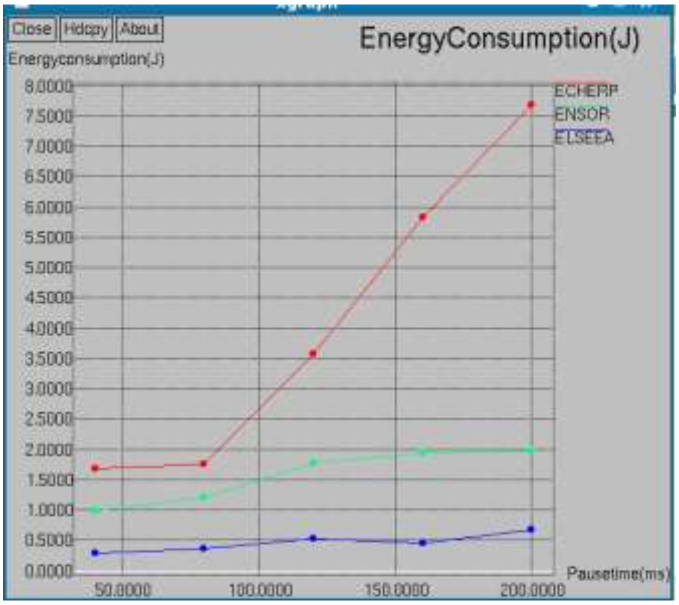

Figure 3: Pause time Vs Communication Overhead

Figure 3 shows the results of Pause time Vs Communication overhead. It can be observed that projected method attains less overhead over previous methods. Due to the link stability computation, nodes with higher stable link is chosen as cluster head for data forwarding. Thus, the network delivery rate is improved and the Packet overhead restrained.

Figure 4 shows the results of packet delivery ratio for the Simulation time. Obviously this system attains more packet delivery ratio over the previous intrusion detection systems.

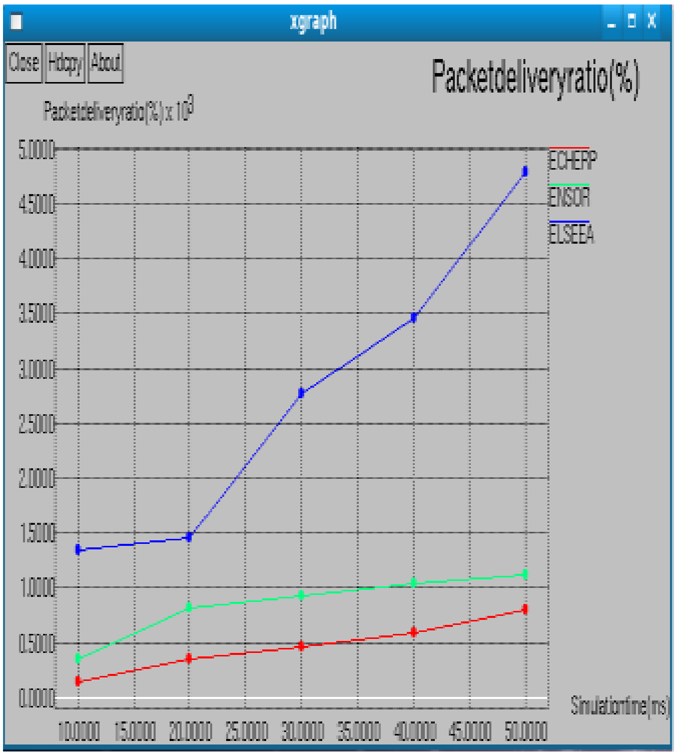

Figure 4: Packet Delivery Ratio Vs Packet delivery ratio

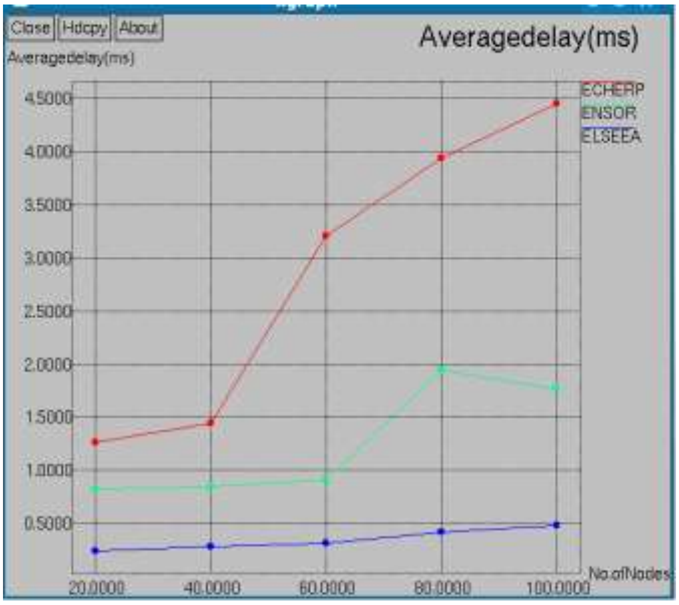

Figure 5: Average delay Vs No. of Nodes

Figure 5 shows the results of Average delay Vs No. of Nodes. It is observed that proposed system has less delay over previous systems. This proposed system has diminished through cluster based routing. Network partitioning will be decreased by means of integrating this routing in all networks.

Figure 6 shows the results of Simulation time Vs Detection rate. It is observed that proposed system has high detection rate over previous systems. This proposed system has increases packet integrity rate via adding reliability model.

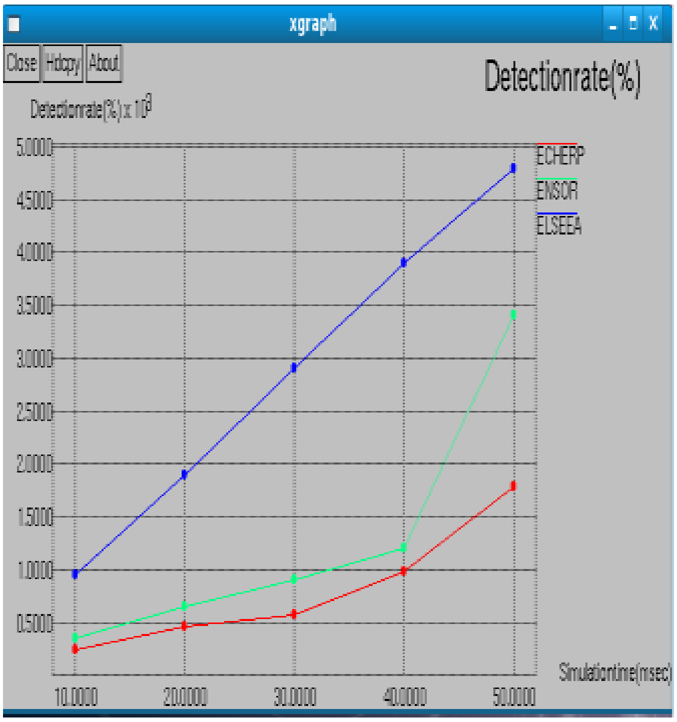

Figure 6: Time Vs Packet Integrity Rate

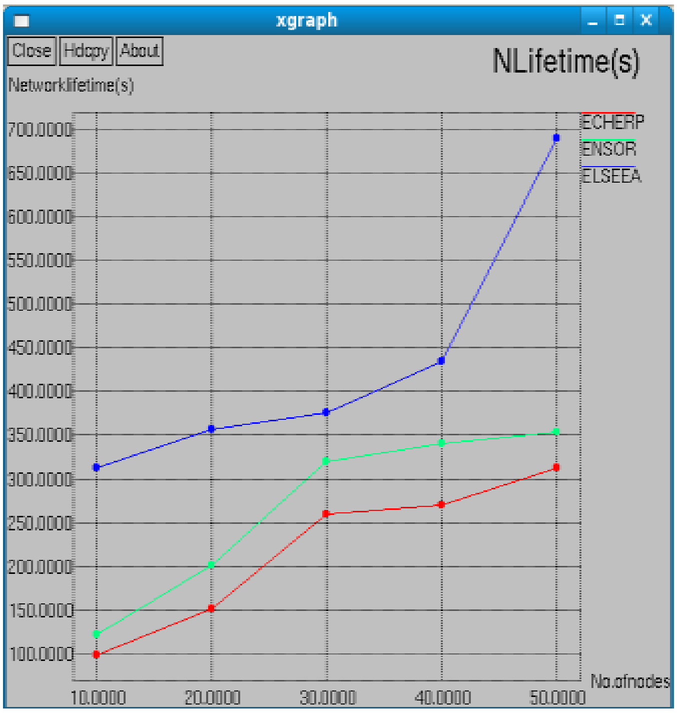

Figure 7: Pause time Vs Network Lifetime

Figure 7 shows the results of Pause Time Vs Network Lifetime. It is observed that proposed system has more lifespan over previous systems. This proposed system has increased network lifetime by means of adding link stability rate.

Conclusion

In this research work, the proposed approach ELSEEA consists of load balancing, detecting suspicious node and energy model. These three models are mainly focused on efficient routing for network lifetime improvement. Load balancing model is majorly developed for individual routes to reduce the packet loss rate. It provides support to detect suspicious node by integrating the reliability metric in entire routes in the network. Once the recommendation of route and node is measured, the packet arrival rate is measured. If it is high, then the reliability model will be announced by the cluster head to all the members in the cluster. If the performance is highly achieved, it will be adopted in remaining clusters. In last case, the energy spent for suspicious node detection is removed in the electronic module of transmitter. If the bits are not corrupted, then the energy spent for transmission is less. Based on the extensive simulation results, the proposed work achieves high detection rate, less delay, more network lifetime, high packet delivery ratio and less energy consumption.

References

1. Heinzelman W.R., Chandrakasan A. and Balakrishnan H., Energy efficient communication protocol for wireless microsensor networks, Proceedings of the 33rd IEEE Hawaii International Conference on System Sciences (HICSS), 1-10 **(2000)**

2. Chong C.Y. and Kumar S., Sensor networks: Evolution, opportunities, and challenges, *Proc. IEEE*, **91(8)**, 1247-1256 **(2003)**

3. Sohail Jabbar, Abid Ali Minhas, Muhammad Imran, Shehzad Khalid and Kashif Saleem, Energy Efficient Strategy for Throughput Improvement in Wireless Sensor Networks, *Sensors*, **15(2)**, 2473-2495 **(2015)**

4. Babbar Khushbu, Jain Kusum Lata and Purohit G.N., Implementation of Energy Efficient Coverage Aware Routing Protocol for Wireless Sensor Network using Genetic Algorithm, *International Journal in Foundations of Computer Science & Technology (IJFCST)*, **5(1)**, 23-34 **(2015)**

5. Anandh Jeba S. and Baburaj E., Energy Efficient Routing Strategies for Clustered Wireless Sensor Networks: An Analytical Framework, *International Journal of Computer Applications*, **74(8)**, 19-27 **(2013)**

6. Venu Madhav T. and Sarma, Energy Efficient Routing Protocol with Improved Clustering Strategies for Homogeneous Wireless Sensor Networks, *International Journal of Computer Applications*, **38(8)**, 22-29 **(2012)**

7. Prabha R., Krishnaveni M., Manjula S.H., Venugopal K.R. and Patnaik L.M., TAEER: Trust Aware Energy Efficient Routing Frame Work for Wireless Sensor Networks, *International Journal of Innovative Science and Modern Engineering (IJISME)*, **3(2)**, 67-74 **(2015)**

8. Nikolidakis Stefanos A., Kandris Dionisis, Vergados Dimitrios D. and Douligeris Christos, Energy Efficient Routing in Wireless Sensor Networks Through Balanced Clustering, *Sensors*, **6**, 29-42 **(2013)**

9. Jyh-Huei Chang, An Energy-Aware, Cluster-Based Routing Algorithm for Wireless Sensor Networks, *Journal of Information Science and Engineering*, **26**, 2159-2171 **(2010)**

10. Balavalad Kirankumar B., Katageri Ajaykumar C., Biradar Balaji M., Chavan Deepa and Angadi Basavaraj M., Multipath-LEACH an Energy Efficient Routing Algorithm for Wireless Sensor Network, *Journal of Advances in Computer Networks*, **2(3)**, 229-232 **(2014)**

11. Singh Santar Pal and Sharma, Cluster Based Routing Algorithms for Wireless Sensor Networks, *International Journal of Engineering & Technology Innovations*, **1(4)**, 1-8 **(2014)**

12. Pranav Parekh and Joshi J. H., A Novel Approach on Energy Efficient Cluster Based Routing Algorithm for Wireless Sensor Network, *International Journal of Innovative Research in Computer and Communication Engineering*, **3(2)**, 1064-1070 **(2015)**

13. Taruna S., Jain Kusum Lata and Purohit G.N., Zone Based Routing Protocol for Homogeneous Wireless Sensor Network, *International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC)*, **2(3)**, 99-111 **(2011)**

14. Das Supriya and Bala P. Shanthi, A Cluster-based Routing Algorithm for WSN based on Residual Energy of the Nodes, *International Journal of Computer Applications*, **74(2)**, 16-19 **(2013)**

15. Juan Luo, Jinyu Hu, Di Wu and Renfa Li, Opportunistic Routing Algorithm for Relay Node Selection in Wireless Sensor Networks, *IEEE Transactions on industrial informatics*, **11(1)**, 112-121 **(2015)**

16. Singh Bhagwan and Luthra Pawan, Energy Efficiency Improvement of Wireless Sensor Networks using PEGASIS Combined with Fuzzy Rules, *International Journal of Current Engineering and Scientific Research (IJCESR)*, **2(2)**, 22-27 **(2015)**

17. Arya Rajeev and Sharma S. C., WSN: Lifetime Maximization of Rumor Routing Protocol with Optimization Scheme and Bandwidth Evaluation, *British Journal of Mathematics & Computer Science*, **7(4)**, 266-279 **(2015)**

18. Saleem K., Fisal N., Hafizah S., Kamilah S. and Rashid R. A., A Self-Optimized Multipath Routing Protocol for Wireless Sensor Networks, *International Journal of Recent Trends in Engineering*, **2(1)**, 93-97 **(2009)**.