Asian Journal of Information Technology 15 (12): 2064-2070, 2016
ISSN: 1682-3915

Effective Load Balancing Secure Energy Efficient Approach for WSN

[1]S. Bharathidasan and [2]P. Ramamoorthy
[1]KTVR KPET, Coimbatore, India
[2]Adithya Institute of Technology, Coimbatore, India

Abstract: Wireless Sensor Network (WSN) is 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 research, either energy or suspicious node was focused to improved the performance of the network. In this research 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 increase the lifetime of the network. Based on the simulations using NS 2 tool, the proposed work achieves better performance in the presence of suspicious environment.

Key words: WSN, energy, suspicious node, load balancing, reliability model, network lifetime, detection rate and detection time

INTRODUCTION

Wireless sensor networks consist of nodes which are unattended. These nodes are organized in random manner which supports an ad hoc network. It has limited capacity and consumes minimum energy compared to mobile nodes. Some other nodes are acting as gateway nodes used for processing and storing the data collected from the network. Energy is an essential 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 increase network lifetime, energy must be saved in every hardware and software solution composing the network architecture. According to the radio model proposed in (Heinzelman *et al*., 2000), data communication is responsible for the greatest weight in the energy budget when compared with data sensing and processing. Therefore, it is desirable to use short range instead of long-range communication between sensor nodes because of the transmission power required. In most WSN scenarios, events can be sensed by many source nodes near the phenomenon of interest and far away from the sink nodes. Then, the use of short-range communication leads obligatorily to data packets being forwarded through intermediate nodes along a multi-hop path (Chong and Kumar, 2003).

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.

Literture review: Jabbar *et al*. (2015) 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 according to threshold values of node parameters. From the results, it is justified that more clusters produces less packet dropping and choosing reliable nodes which leads to increased throughput.

Babbar *et al*. (2015) performed the analysis 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

Corresponding Author: S. Bharathidasan, KTVR KPET, Coimbatore, India

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.

Anandh and Baburaj (2013) have made an analytical results 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 basic requirement for data communication. The reconnection of routing process was initiated based on 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.

Venumadhav (2012) 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*. (2015) 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 confidentially to safeguard network from attackers. The packets are forwarded through trusted intermediate nodes to destination node based on location privacy algorithm.

Nikolidakis *et al*. (2013) developed a equalized cluster head election routing protocol to extend the network lifetime. 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 *et al*. (2010) proposed an energy-aware, cluster-based routing algorithm to maximize the network's lifetime. The cluster head is chosen based on Voronoi diagrams and it is rotated to balance load in a cluster group. The two tier architecture was also proposed to enhance the performance of the cluster based routing. All the intermediate sensor nodes transmit their 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.

Kirankumar and coauthors 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.

Singh and Sharma (2014) 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 and Joshi (2015) 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.

Das and Bala (2013) proposed a zone based clustering head selection algorithm for homogeneous wireless sensor networks. All the nodes in the network are uniformly distributed. Network performance is increased by choosing cluster heads based on remaining energy of sensor nodes and next hop distance.

Supriya *et al*. (2013) proposed a clustering routing algorithm to increase the sensor network lifetime based on cluster head's residual energy and the distance between the cluster members and corresponding cluster heads. It was designed to enhance the overall lifetime of the network by increasing the lifetime of each of the nodes and next hop distance between cluster member and cluster head. Self selection of optimized clusters were also proposed to provide improved network performance.

Luo *et al*. (2015) focused on minimizing energy consumption and maximizing network lifetime of sensor networks. The opportunistic routing theory was established to optimize the network energy efficiency based on the difference between sensor nodes in terms of distance to destination node. The opportunistic routing theory was determined to realize the relay node based on the optimal transmission distance. The network lifetime is prolonged by keeping nodes with low residual energy proactively.

Bhagwan and Pawan (2015) introduced the concept of fuzzy based PEGASIS to enhance the lifetime of network by the 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 during the transmission of data from one sensor node to another.

Arya and Sharma (2015) proposed an energy efficient and bandwidth estimation based on hierarchical protocol. The data centric protocol with optimization scheme 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*. (2009) presented a model of self-optimized multipath routing algorithm for WSN. There are some parameters like energy level, delay and velocity were considered. This selection of parameters have come up with the optimal and organized route for WSN. In addition, the stated algorithm was enhanced with the multipath capability to avoid congestion state. It helps WSN in maximizing the data throughput rate and minimizing the data loss.

MATERIALS AND METHODS

Proposed energy efficient secuiry system: The main aim of the 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.

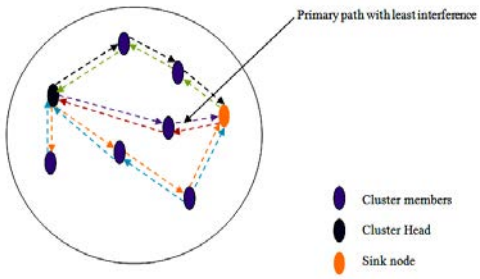

Fig. 1: Multipath construction

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:

$$S_{Avg} = \frac{\Sigma_d}{\Sigma_t}$$

Where:

$\sum_d$ = The sum of distances between the neighbor nodes
$\sum_t$ = The sum of delay times of the intermediate nodes with minimum hop count

In Fig. 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 $\{N_s, N_{i1}, N_{i2}\ N_{i13},..., N_D\}$ is calculated as:

$$RM_n = \begin{cases} TV_s \times ..... \times TV_D & \forall TV_n > 0 \\ -1 & \forall TV_n < 0 \end{cases} \quad (2)$$

where, N_{i1}, N_{i2} 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:

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

Where:

W_s = Number of packets successfully sent from source nodes

W_d = 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:

$$CR_n = TT_c \times SR_n \quad (4)$$

The Previous Communication ($PC_{s,d}$) of source node s and destination node d is determined as:

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

Where:

$R_{s,d}$ = Reliable communication in the past history of source and destination node

$Ur_{s,d}$ = Unreliable communication in the past history of source and destination node

$H_s t_s$ = 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 evaluated 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 Eq. 6:

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

Where $0 < W_k \leq 1$.

Energy efficient model: The security system considers both transmitter energy and receiver energy. The energy consumed by transmitter and receiver is calculated based on data packets, node location estimation, energy spent for suspicious node removal and distance between the transmitter and receiver. In transmitter side, energy consumption is calculated as:

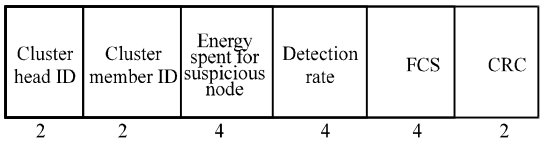

Fig. 2: Proposed packet format

$$E_{tr}(K, d) = E_{elec} \times K + \chi_{amp} \times K \times d^2 - E_{spent}(N_s)$$

K = A bit that contains information spent for node location identification and header information

E_{elec} = An energy to be spent by the electronic model located at transmitter and receiver (100 nJ/bit)

χ_{amp} = Transmitter Amplifier (114 pJ/bit/m^2)

d = Distance between neighbor nodes

$E_{spent}(N_s)$ = Energy spent on suspicious node removal

The receiver model consumes energy for transmitting K bits and it is calculated as:

$$E_{rr} = E_{elec} \times K$$

Proposed packet format: In Fig. 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 for error correction and detection in packet during route maintenance process.

Performance evaluation

Simulation model and parameters: The proposed approach is simulated with Network Simulator tool (NS 2.34). In this simulation, 100 mobile nodes move in a 1000×1000 m^2 region for 100 sec simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 200 m. The simulated traffic is Constant Bit Rate (CBR). The simulation settings and parameters are given in Table 1.

Performance metrics: We evaluate mainly the performance according to the following metrics.

Detection rate: The ratio of detected malicious nodes to the total number of nodes.

Table 1: Elseea simulation settings

Variables	Para meters
No. of nodes	100
Area size	1000×1000 Sq.m
Mac	802.11
Radio range	200 m
Simulation time	100 sec
Traffic source	CBR
Packet size	512 bytes
Mobility model	Random way point
Protocol	LEACH

Average delay: The-delay is averaged over all surviving data packets including end to end delay, access delay from the sources to the destinations.

Packet delivery ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

The simulation results are presented in the next part. We compare our proposed approach with ECHERP (Nikolidakis *et al*., 2013) and ENSOR (Luo *et al*., 2015) in the presence of suspicious node environment.

RESULTS AND DISCUSSION

In our First experiment, we vary the no of suspicious nodes as 20, 30 up to 100. Figure 3 shows the results of pause time vs communication overhead. From the results, we can see that proposed approach achieves less overhead than previous schemes. It is because of link stability determination. Cluster head chooses only high stable link for data forwarding. So the network delivery rate is getting increased. Packet overhead will be suppressed because of link quality and reliability of neighbor nodes.

Figure 4 show the results of packet delivery ratio for the Simulation time. Clearly our system achieves more packet delivery ratio than previous intrusion detection systems. The proposed system comprises two major aspects i.e., malicious detection and network authentication. Packet is delivered via reliable nodes through stable link. Successfully all the packets are delivered to the destination.

Figure 5 shows the results of Average delay Vs No. of Nodes From the results, we can see that proposed system has less delay than previous systems. The proposed system reduces delay by means of cluster based routing. Network partitioning will be reduced by integrating this routing in all networks.

Figure 6 shows the results of simulation time Vs detection rate. From the results, we can see that proposed system has high detection rate than previous systems. The proposed system increases packet integrity rate by adding reliability model.

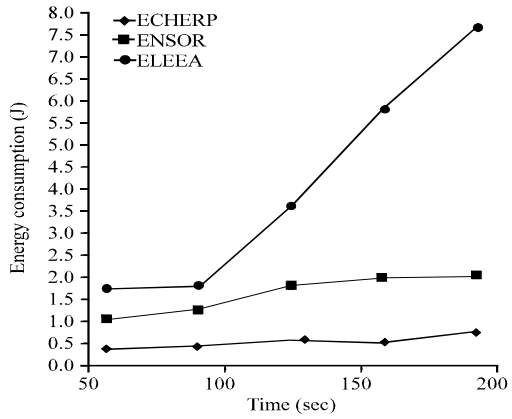

Fig. 3: Pause time vs communication overhead

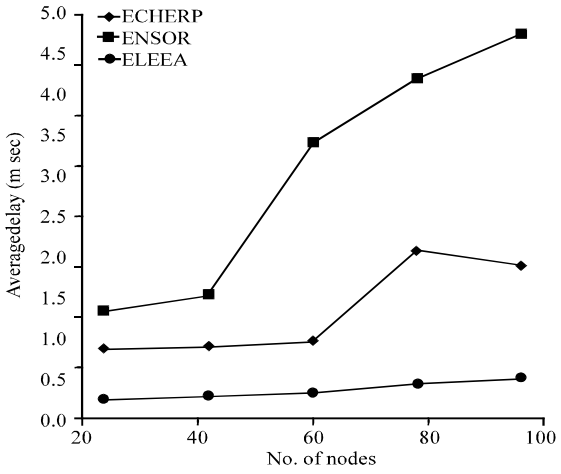

Fig. 4: Packet delivery ratio vs packet delivery ratio

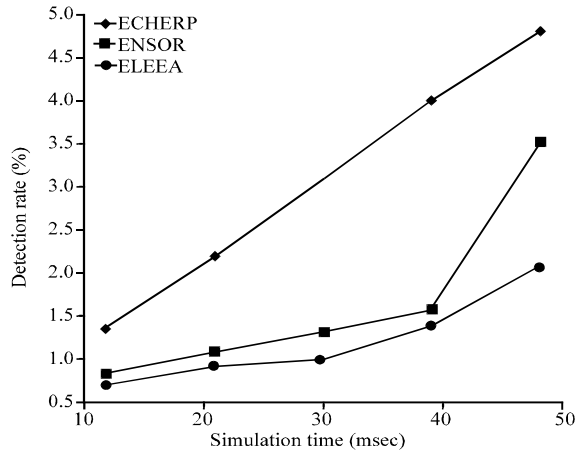

Fig. 5: Average delay Vs No. of Nodes

Figure 7 shows the results of pause time vs network Lifetime. From the results, we can see that proposed

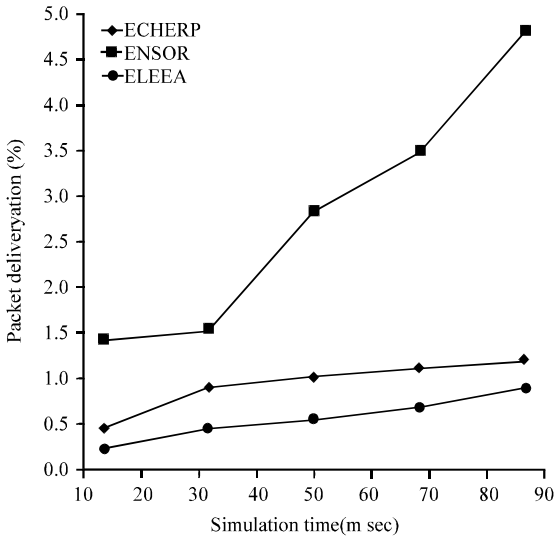

Fig. 6: Time Vs Packet Integrity Rate

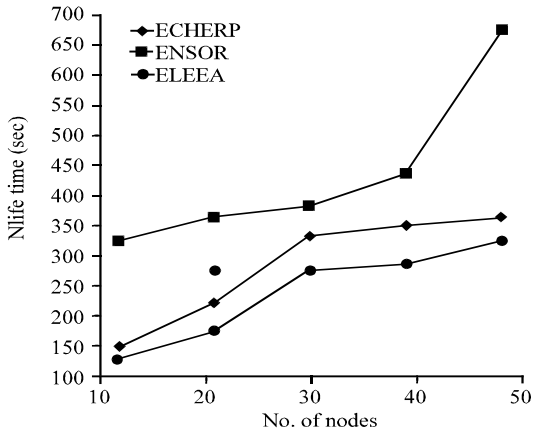

Fig. 7: Pause time Vs Network Lifetime

system has more lifetime than previous systems. The proposed system increases network lifetime by 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 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

Anandh, S.J. and E. Baburaj, 2013. Energy efficient routing strategies for clustered wireless sensor networks: An analytical framework. Int. J. Comput. Appl., 74: 19-27.

Arya, R. and S.C. Sharma, 2015. WSN: Lifetime maximization of rumor routing protocol with optimization scheme and bandwidth evaluation. Br. J. Math. Comput. Sci., 7: 266-279.

Babbar, K., K.L. Jain and G.N. Purohit, 2015. Implementation of energy efficient coverage aware routing protocol for wireless sensor network using genetic algorithm. Int. J. Found. Comput. Sci. Technol, 5: 23-34.

Bhagwan, S., L. Pawan, 2015. Energy efficiency improvement of wireless sensor networks using pegasis combined with fuzzy rules. Int. J. Curr. Eng. Sci. Res., 2: 22-27.

Chang, J.H., 2010. An energy-aware, cluster-based routing algorithm for wireless sensor networks. J. Inf. Sci. Eng., 26: 2159-2171.

Chong, C.Y. and S.P. Kumar, 2003. Sensor networks: Evolution, opportunities and challenges. Proc. IEEE, 91: 1247-1256.

Das, S. and P.S. Bala, 2013. A cluster-based routing algorithm for WSN based on residual energy of the nodes. Int. J. Comput. Appl., 74: 16-19.

Heinzelman, W.R., A. Chandrakasan and H. Balakrishnan, 2000. Energy-efficient communication protocol for wireless microsensor networks. Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, January 4-7, 2000, Maui, HI., USA., pp: 1-10.

Jabbar, S., A.M. Abid, I. Muhammad, K. Shehzad and S. Kashif, 2015. Energy efficient strategy for throughput improvement in wireless sensor networks. Sens., 15: 2473-2495.

Luo, J., J. Hu, D. Wu and R. Li, 2015. Opportunistic routing algorithm for relay node selection in wireless sensor networks. IEEE. Transac. Ind. Inf., 11: 112-121.

Nikolidakis, S.A., D. Kandris, D.D. Vergados and C. Douligeris, 2013. Energy efficient routing in wireless sensor networks through balanced clustering. Algorithms, 6: 29-42.

Parekh, P. and J.H. Joshi, 2015. Novel approach on energy efficient cluster based routing algorithm for wireless sensor network. Int. J. Innovative Res. Comput. Commun. Eng., 3: 1064-1070.

Prabha, R., M. Krishnaveni, S.H.K.R. Manjula and L.M.P. Venugopal, 2015. TAEER: Trust aware energy efficient routing frame work for wireless sensor networks. Int. J. Innovative Sci. Mod. Eng., 3: 67-74.

Saleem, K., N. Fisal, S. Hafizah, S. Kamilah and R.A. Rashid, 2009. A self-optimized multipath routing protocol for wireless sensor networks. Int. J. Recent Trends Eng., 2: 93-97.

Singh, S.P. and S.C. Sharma, 2014. Cluster based routing algorithms for wireless sensor networks. Int. J. Eng. Technol. Innovations, 1: 1-8.

Taruna, S., J.K. Lata and G.N. Purohit, 2011. Zone based routing protocol for homogeneous wireless sensor network. Int. J. Ad Hoc Sens. Ubiquitous Comput., 2: 99-111.

Venumadhav, T., 2012. Energy efficient routing protocol with improved clustering strategies for homogeneous wireless sensor networks. Int. J. Comput. Appl., 38: 22-29.