SECURED ENERGY EFFICIENT HYBRID ROUTING IN WIRELESS SENSOR NETWORKS

Deepika Srikumar and Seethalakshmi Vijaykumar
Department of Electronics and Communication Engineering, Sri Shakthi institute of Engineering and Technology, Coimbatore, India

ABSTRACT

Energy is the scarcest resource of sensor nodes and it determines the lifetime of wireless sensor networks. The main challenge is to minimize the energy required for wireless communication by developing application independent routing algorithm for reliable and efficient data delivery. In addition to the limited resources, security is a main concern of wireless sensor networks. In this paper the proposed scheme is to revolutionize the contemporary technical arena based on the hybrid routing. The hybrid routing is derived from fundamental radio energy model considering various parameters such as number of hops, threshold energy level, distance between number of hops and Packet Reception Rate (PRR) and also it protects the network against worm hole attacks. This paper evaluates the performance of existing energy efficient based routing algorithms in wireless sensor networks such as Greedy, ODGR, and PEGASIS and it is compared with the proposed EEHR algorithm in terms of energy efficiency. Simulation is done using NS-2(version NS-2.33). The proposed scheme is more efficient than existing methods since it reduces average energy consumption for multihop communication even in the presence of high node density, high throughput, improves system life time and reduces the average latency leads to higher Packet Deliver Ratio(PDR) and provides the defense technique against worm whole attacks.

KEYWORDS: *Average Latency, Hybrid Routing, PRR, Reliable Link, Threshold Energy level*

I. INTRODUCTION

Wireless sensor networks are core technologies in various applications such as Greenhouse monitoring, structural monitoring in industry, area monitoring in military etc. In wireless sensor network spatially distributed sensors are deployed either inside the phenomenon or very close to it. Nodes in the sensor environment have restricted storage, computational and energy resources. The conventional wireless sensor networks support IP style of addressing of sources and destination. They also use intermediate nodes to support end-to-end between attribute nodes in the network. Each node in the wireless sensor networks maintains the neighbor information. The reusability of maintained information widely increases the performance of the wireless sensor network [1] [14].

The many routing algorithms have been proposed among them adaptive algorithms are very popular as it adapts itself to the shortest hop count but it non reliable link quality. The Communication may occur less reliably with nodes faraway, but there are many distant nodes and a few of them are likely to have strong connectivity. Generally, many of the links are lossy and the loss rate may change dynamically with environmental factors or due to contention arising from the highly correlated behaviour of the application [16]. The energy efficient route allocation is found in few works and in majority, it does not evaluate in wireless sensor networks context, but analysis the parameters like shortest path routing, alternate path routing during link breakage etc.

Beyond the above mentioned parameters the most important criteria in wireless sensor networks is threshold energy level and residual energy level. If the energy in the network falls below the threshold value during transmission or reception, it may leads to the loss of packets and error in receiving information. For long distance communication battery power needed for sensor node is

more but for the short distance it is less. Example the power required to transmit 10m is 1mw but the power required to transmit 100m is 100m [8]. This paper also addresses the security concerns in wireless sensor networks. More specifically, we address the wormhole attack, which is a severe attack in wireless sensor networks whereby an attacker stores transmitted packets and then replays them into the network. Defending against such an attack is challenging because it can be launched even if all network communication is authentic and confidential.

Existing algorithms either lead to long distance communication or wastage of energy resources. To overcome the various drawbacks in the existing schemes, the proposed Energy Efficient Hybrid Routing (EEHR) scheme evaluates following parameters in priority manner to forward a packet as follows:

1. Choosing type of transmission either direct transmission or multihop from the radio energy model.
2. If direct transmission follow step5 procedure else following the next step.
3. Optimal number of hops between source and destination.
4. Optimal distance between numerous motes during intermediate transmission.
5. Calculating threshold energy level from initial energy of each node and minimum energy required for efficient operation.

In addition to the above process the hybrid routing also provides the defense mechanism against the worm hole attack in network. The efficient network working is analyzed from above parameters and blacklisting the inefficient route. The rest of the paper is organized as follows. In Section 2, the related work is explained. The new geographic routing algorithm in WSNs is presented in section 3. After that, the results of simulation study that evaluates the performance of proposed method and others are described in Section 4. Finally, conclusion of the proposed work and future extensions of this study are described in Section 5.

II. RELATED WORK

2.1 Greedy Forwarding

Greedy Forwarding is the key mechanism in geographic routing protocols. In Greedy Forwarding, each node knows the location of neighbor nodes for data transmission. Neighbor nodes are located in 1-hop distance of source node. In this way, source node uses the location of neighbor nodes for data transmission. Additionally, it knows the location of destination node. Source node selects a candidate-node in neighbor nodes. A candidate-node is the closest to destination node in neighbor nodes. For forwarding data packets to destination node, Greedy Forwarding repeats this pattern until data packets reach destination node [9].

However, in Greedy Forwarding, source node forwards data packets to a candidate-node without considering wire-less link-quality [6]. Therefore, this method has a problem that delivery rate is dropped without retransmission. If the retransmission is possible, the main problem is that energy-wastage is increased.

2.2. PEGASIS

The main idea in Power-Efficient Gathering in Sensor Information Systems (PEGASIS) is for each node to receive from and transmit to close neighbors and take turns being the leader for transmission to the BS.

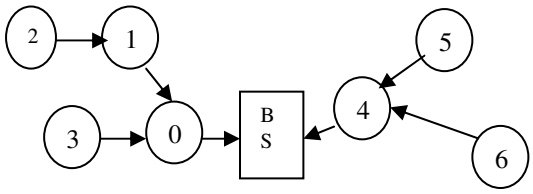

Figure.1. Routing in PEGASIS

This approach will distribute the energy load evenly among the sensor nodes in the network [15]. The nodes are randomly located in network. The nodes will be organized to form a chain, which can either be accomplished by the sensor nodes themselves using a greedy algorithm starting from some node. Alternatively, the BS can compute this chain and broadcast it to all the sensor nodes [5]. PEGASIS improves on LEACH by saving energy in several stages. First, in the local gathering, the distances that most of the nodes transmit are much less compared to transmitting to a cluster-head in LEACH. Second, the amount of data for the leader to receive is at most two messages instead of 20 (20 nodes per cluster in LEACH for a 100-node network) [21]. Finally, only one node transmits to the BS in each round of communication. The main drawback of this method is, it lead to large delay.

2.3. ODGR

Optimal distance geographic routing (ODGR) is an algorithm that uses geographic information and power control in the transmission scheme to dynamically explore the optimal routing path. There are three main key mechanisms in routing techniques. They are
(i) Direct transmission between source and destination.
(ii) Mutihop transmission through neighbor nodes.
(iii) Only few numbers of motes selected between source and destination.

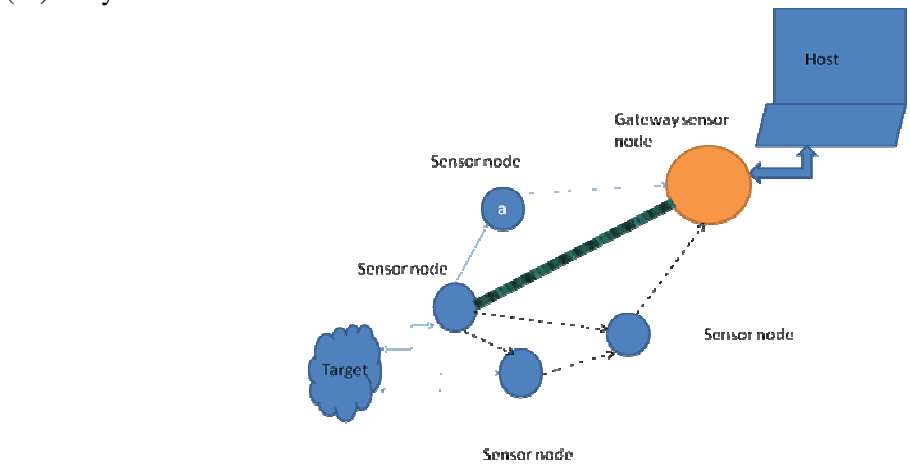

Figure.2. An example of wireless network scenario.

The fundamental radio energy model is given by the following equation.

$$E(d)=2l\varepsilon elec + l\varepsilon fs\text{-}amp\ d2 \quad \text{if } d < d0 \qquad (1)$$

$$=2l\varepsilon elec + l\varepsilon mp\text{-}amp\ d4 \quad \text{if } d > d0 \qquad (2)$$

where l is the number of bits in a packet, h is the distance between the transmitter and the receiver nodes and εelec is the electronics energy for the transceiver circuitry. εfs–amp and εmp–amp denote power amplifier energy dissipations at free-space and multipath modes, respectively, and d0 is the threshold distance [2].
ODGR considers two important physical properties of wireless sensor networks, geographic location and power control. The ODGR algorithm is developed based on the optimal distance analysis and optimal number of hops. ODGR requires each node to know the locations of the neighbor nodes within a specific distance. This distance is set as 1.5 hopt, because for a given distance d and number of hops n, the transmit distance per hop h can be calculated as $n = d/h$ [16].

It is applicable for any node-to-node communication in wireless sensor networks. It can be used, but not limited, in a form of data collection or dissemination among sensor nodes and base station. In an intelligent environment with both sensors and actuators, node-to-node unicast communication may be necessary for task coordination.

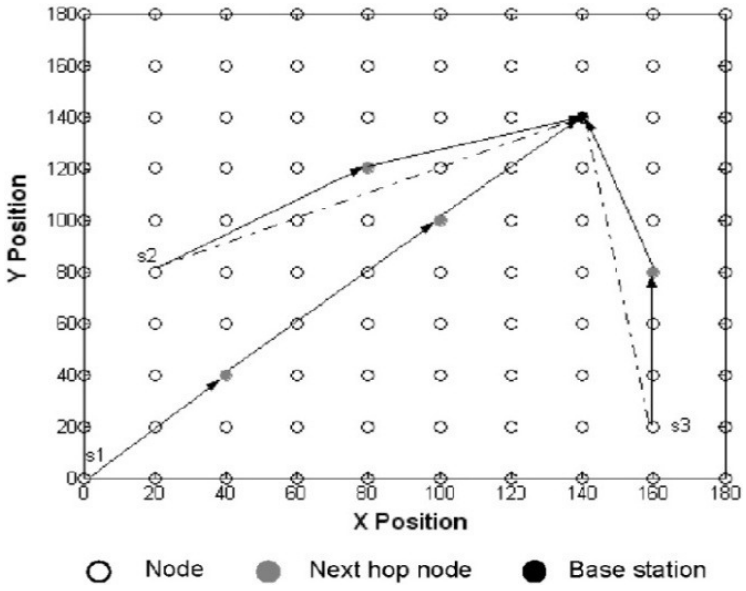

Figure.3. Simulation results of ODGR

The above routing shows the good results by implementing ODGR algorithm. The main constraint in this algorithm is, this algorithm does not consider the threshold energy level in the intermediate nodes. This leads to wastage of energy resources.

III. PROPOSED SCHEME

The proposed EEHR is suitable for geographic routing. It is a new multicast routing algorithm. The minimum numbers of sensor nodes are used to route message to destination. If source need to forward packets to destination which is in the transitional region. It forwards through the neighbor nodes. If residual energy in the neighbor node is not enough to forward the data packets, only few packets are forwarded till its total energy drops in that sensor node, remaining data packets are dropped. The threshold energy level of neighbor node should be calculated before forwards to that particular node. To achieve above goals the EEHR was proposed [19].

3.1 Network Model

EEHR assumes a general wireless sensor network environment. Our method initially decides whether source to destination is direct communication or multihop communication. For example, energy required for direct transmission is 7J and energy required for multihop communication is 8J, i.e. 4J for each hop. From above example we conclude that direct transmission should be done for that case. This follows to optimal number of hops and optimal distance between source to destination. Finally the PRR and threshold energy level are analyzed. In this paper grid network is considered, i.e. distance between neighbor nodes are equal. Nodes are placed 5m distances each [13].

3.2 Link Loss Model

The link loss model of real environment is required to simulate reliable data transmission. PRR is used in the research. PRR is the link quality between two nodes. It varies from 0 to 1. In the

connected region packet reception rate is 1(from 0 to 8m) because in this region nodes can transmit data packets perfectly. The link qualities between two nodes for the transitional region (8m to 35m) are observed by [4] and [8].

3.3 Security Concerns

The hello packets are sends to neighbor nodes from the all nodes in symmetric environment to discover the neighbor nodes and protect against the wormhole attack. A hello packet consists of ID of the particular node that originate hello packet and hop count to destination. The sensor node which receives the hello packet inserts the new entry in its "hello packet list" that contains all the ID of nodes which sends hello packet to that particular node. The hello packet list sorted the various ID and made the ID which has lowest number of hops as higher priority. As soon as the node receives the hello packet, acknowledgment timer is set to expire over a particular period. When the acknowledgement timer got expired the node send acknowledgement packet (ACK_packet) to source node.

The ACK_pack consists of source node ID, destination ID and hop count. The updates are also made in ACK_table (Acknowledgement table). The ACK_table consists of destination ID, hop count, No_ACK_pack (total number of acknowledgement packets) and Rec_Accept (total number of received accepted packets). The destination ID and hop count are initialized in ACK_table but No_ACK_pack and Rec_Accept are made zero. Check timer is set; it will expire after a period of transmission of ACK_packet. As soon as the check timer got expired increment is made in the No_ACK_pack field of ACK_table. Source node which receives the ACK_packet inserts that particular destination ID, hop count and number of identical ACK_packets (ID_ACK_packets) is incremented or it is set to one for newly received packet in acknowledgement list (ACK_list) [21].

Tab 1. Acknowledgement Table

NODE ID
HOP COUNT
No_ACK_pack
Rec_Accept

Accept timer is set upon the reception of the first ACK_packet, when accept timer got expired the source node sends the Acc_packet (accept packet) to the destination for the equivalent entries in ACK_list. Nodes upon receiving the Acc_packet checks whether the source ID is same as the source ID in the ACK_table. If source ID got match update made in ACK_table by incrementing Rec_Accept, if not attacker stores the ACK_packet and reply the Acc_packet to destination. The number of reply in the Acc_packet should be one greater than the No_ACK_pack in ACK_table. If the above condition is not satisfied neglect the Acc_packet and include the ID in the accept packet neglected accepted packet table, set the ACK_table values to zero. Send another ACK_packet that corresponds to next priority in the ACK_list or wait for another ACK_packet if not available [11].

3.4. Design Concerns

If source A is located at (xA, yA) and destination B is located at (xB, yB), the EEHR routing algorithm works as follows.
(i) Set the current node location (xi, yi) as the source node location: xi = xA; yi = yA.
(ii) Computes the Euclidean distance from the current node to destination. If the distance d is less than hopt, jumps to Step (ix), where

$$d = \sqrt{(xi - x\,B)\,2 + (yi - yB)\,2} \qquad (3)$$

(iii) Computes nopt = d/hopt. The distance per hop h is determined as d/n.

(iv) If n = 1, goes to Step (ix). Otherwise, computes the estimated location of the next hop node j as,

$$xi = xi + \Delta x$$

$$= xi + ((xB - xi)/n) \quad (4)$$

$$yi = yi + \Delta y$$

$$= yi + ((yB - yi)/n) \quad (5)$$

(v) For the estimated location, calculate the optimal number of hops and optimal distance between source and destination in priority order for four indirect transmission paths. Choose the one route in priority order.

(vi) Blacklisting the neighbor nodes based on PRR and threshold energy value. A node has initial energy is 12J. The node requires minimum 1.75608J (Emin) energy to operate properly. The threshold energy is mainly based on minimum energy required for the proper operation of the node which depends on the parameters like transceiver energy, bandwidth, bit rate, signal to noise ratio, antenna gain, transmitter efficiency as per mica 2 model. The threshold energy is calculated as follows,

$$Ethreshold = Emin / Einitial \quad (6)$$

$$= 0.14634J$$

Therefore current forwarding node omits neighbor nodes which have lower Energy-level than threshold energy level and go to previous step to choose the next optimal path. In (7) EX (residual) is the residual energy of node X and EX (initial) is the initial energy of node X. The Energy_level of neighbor nodes should be taken into account to analyze the energy of the node. The Energy_level is normalized value between 0 and 1. Energy_level is given by:

$$Energy\_level = EX(residual) / EX(initial) \quad (7)$$

(vii) After blacklisting has done consider the node which has the largest priority value PV.

$$Priority\ Value = W1 * CSL + W2 * Energy\_level \quad (8)$$

Priority value is analyzed from the Change in Status of Link quality (CSL), Energy_level of neighbor node and weighting factors (W1 & W2) CSL is the value that explains link quality between source and neighbor node. Modified Status of Link quality of the data transmission based on size of data packets and ACK message packet. The two factors are applied here which decides the size of the packet (Sdata & SACK) for various sizes of data packets.

$$CSL = (Sdata/(Sdata + SACK) * PRRS\text{-}N + (SACK/(Sdata + SACK) * PRRN\text{-}S \quad (9)$$

W1 and W2 are weighting factors. Weighting factors are defined by Energy_level of the neighbor nodes. If neighbor nodes have sufficient energy to transmit data or receive data, there is no need to consider the relative energy. Concentrating on link quality and optimal number of hops provides good result.

$$W_I = \sum_{i=n}^{n} \frac{Energy\_level_{nbr(i)}}{n} \quad (10)$$

(viii) Sends the packet to the next hop node if it is not in the exclusion list of the current node, and waits for an acknowledgement (ACK). If the ACK is successful, sets the next hop node as the current node and goes to Step (ii) to continue. If the next hop node is in the exclusion list, no matter whether it is discovered from the most recent ACK or from information obtained during previous search, it goes back to Step 5 to choose a different node. If all available neighbor nodes are in the exclusion list, the algorithm terminates with an announcement that no neighbor nodes have energy higher than threshold value and PRR is less than PRR threshold.

(ix) Transmits packets directly (direct transmission) from the current node to the destination. The EEHR algorithm is completed.

3.4. Blacklisting Nodes

The symmetric environment is assumed, nodes are placed equidistance from each other. The value of PRR threshold compares with actual PRR in each data transmission. Nodes should have appropriate Energy_level for data transmission. If the node has lower Energy_level than the Energythreshold in the optimal path transmission that particular optimal path is discarded and transmission is done using next optimal path [7].

3.5 Data Transmission

The current node omits some neighbor nodes using the blacklisting method in data transmission. Then, the current node sends data packets to a candidate node that has highest priority value of neighbor nodes. If the current node does not receive ACK packet from candidate node perfectly, the current node should retransmit. Data delivery will fail, if the number of retransmission time exceeds ARQ. Each node updates the Energy_level of neighbor nodes at the end of data transmission. Each node repeats these steps until the destination node receives data packets.

IV. ANALYSIS OF EXPERIMENTAL RESULTS

4.1 Simulation Environment

The simulations for existing and proposed scheme are performed using the NS2 simulator. The symmetric environment is created in the proposed scheme consists of 7 rows and 7 columns of nodes totally 49 nodes, which is placed 5m equidistance from neighbor nodes. The maximum initial energy for each node is set as 12J. Energy required for transmission and reception of 100 data bytes is 1762.5µJ and ACK packet size is 193.875µJ. The various parameters in proposed scheme and existing schemes are analyzed, and finally comparing each other performance.

4.2 Parameter Analysis

Among the various parameters the most important parameters are analyzed below. Node density is number of nodes within the radio range. During routing process the proposed routing mechanism checks the whether any wormhole attack occurs. If wormhole attack occurs during hybrid routing process the defense mechanism against that attack and recover the network from that attack. Hence routing through the false path is aborted and protects the wireless sensor network from the wormhole attack. Throughput is defined as the ratio of number of packets received to the time seconds. The energy consumed by the sensor node varies depends upon the transmission distance source and destination. The transmitter amplifier energy required for transmission is 100pJ/bit/m. The energy required for idle operation is 40nJ/bit.

$$\text{Throughput} = \frac{\text{Total number of packets received}}{\text{Time(sec)}}$$

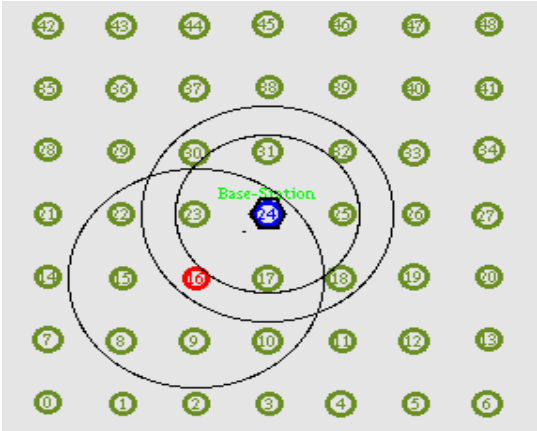

Figure.4. The above simulation result shows direct communication

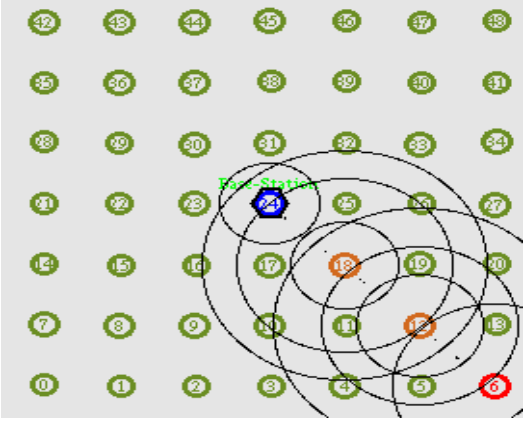

Figure.5. The above simulation result shows multihop communication

In this simulation, all the nodes used to transmit data packets repeatedly. Therefore, we cannot find any advantage at low node densities. As the node density gets higher, the network lifetime gets longer. The node16 is within the connected region so direct transmission is possible with lower energy consumption. The Fig(8) shows that node16 directly transmits the data packets to base station. In Fig(9) the source node 6 sends the data packets to base station through node12 and node18. This shows optimal number of hops and optimal distance between source and destination.

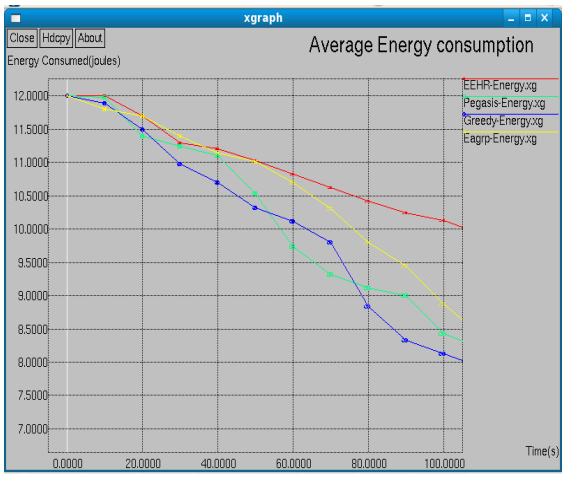

Figure.6. The above simulation results shows the proposed scheme consumes less energy than existing scheme

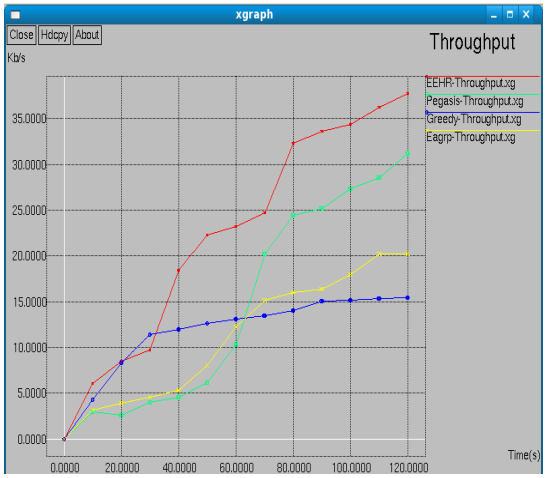

Figure.7. The above simulation results shows the proposed scheme consumes less energy than existing scheme

Comparing with other existing schemes our proposed scheme has high throughput for the same environment of sensor nodes. The Fig (10) shows that EEHR consumes lower energy than the existing algorithms. Energy is measured in joules.

V. CONCLUSION

The simulation results show that this type of routing enhances network lifetime considering limited sensor node's energy. It will be efficiently used routing protocol in future, since it considers both energy level in each node and optimal no of hops. Thus hybrid routing reduces the average latency and energy needed for multihop communication. A great advantage of detection and defense mechanism against wormhole attack is, it doesn't require any geographical information about the sensor nodes, and doesn't take the time stamp of the packet as an approach for detecting a wormhole attack, which is very important for the resource constrained nature of the sensor nodes. In this paper we have evaluated the performance of different routing algorithms for energy efficient in sensor networks. Graph results shows that EEHR consumes minimum energy compared to PEGASIS, Greedy and ODGR. PEGASIS seems to have slightly more balanced energy consumption between nodes. The proposed scheme EEHR is analyzed as the best routing algorithm compared to PEGASIS, Greedy and ODGR, when energy efficiency is taken into consideration.

REFERENCES

[1] Gaafar A Elrahim, Hussein A Elsayed, Salwa E Ramly, Magdy M. Ibrahim, (NOV 2010), "An Energy Aware WSN Geographic Routing Protocol", Universal Journal of Computer Science and Engineering Technology, pp.105-111.

[2] Jabbar S, Butt A.E, Sahar N, Minhas A.A, (2011)," Threshold based load balancing protocol for energy efficient routing in WSN", 13th International Conference on Advanced Communication Technology (ICACT),pp.196 – 201.

[3] Jaewan Seo, Moonseong Kim , In Hur ,Wook Choi and Hyunseung Choo, (2010), " DRDT: Distributed and Reliable Data Transmission with Cooperative Nodes for Lossy Wireless Sensor Networks", ISSN,pp.2793-2811.

[4] Karim Seada, Marco Zuniga, Ahmed Helmy, Bhaskar Krishnamachari, (NOV 2004), "Energy Efficient Forwarding Strategies for Geographic Routing in Lossy Wireless Sensor Networks", Sensys '04, Baltimore, Maryland, USA.

[5] Lindsey S and Raghavendra C S, (2002), "PEGASIS: power-efficient gathering in sensor information systems", Proceedings of the IEEE Aerospace Conference, Big Sky, MT, March, pp.1125–1130.

[6] Maskooki A, Cheong Boon Soh, Gunawan E.; Kay Soon Low, (2011), "Opportunistic routing for body area network", Consumer Communications and Networking Conference (CCNC), IEEE ,pp. 237 – 241.

[7] Myung Kyun Kim, Ngo, Hoai Phong,(2011), " A reliable and energy efficient routing protocol in industrial wireless sensor networks", International Conference on Advanced Technologies for Communications (ATC),pp.32 -35.

[8] Organisation For Economic Co-Operation And Development, OCED, (DEC2009), "Smart Sensor Networks: Technologies and Applications for Green Growth".

[9] Sajjad Ahmad Madani, Daniel Weber, Stefan Mahlknecht, (2010), "Position based Routing Protocol for Low Power Wireless Sensor Networks", Journal of Universal Computer Science, vol. 16, pp.1215-1233

[10] Idris M. Atakli, Hongbing Hu, Yu Chen, Wei-Shinn Ku, Zhou Su,(2008), " Malicious node detection in wireless sensor networks using weighted trusted evaluation" , The symposium on simulation of system security,(SSSS '08).

[11] Khin sandar win, Pathin Gyi,(2008), "Analysis of detecting wormhole attack in wireless sensor networks", World academy of science Engineering and Technology, pp.422-428.

[12] Shahzad Ali and Sajjad Madani, (July 2011), "Distributed Efficient Multi Hop Clustering Protocol for Mobile Sensor Networks", The International Arab Journal of Information Technology, Vol. 8, No. 3, Page No: 320 – 309.

[13] Nauman Aslam, William Phillips, William Robertson, Shyamala Sivakumar, (2010), "A multi-criterion optimization technique for energy efficient cluster formation in wireless sensor networks", Information Fusion - Published by Elsevier.

[14] Banner Engineering (March 2009), Application Notes.

[15] M. Botts, G. Pecivall, C. Reed, and J. Davidson, (2008) "OGC sensor web enablement: Overview and high level architecture," in Lecture Notes in Computer Science, Geo Sensor Networks. New York: Springer, pp. 175–190.

[16] Mustard, S. (2007), "Unraveling today's networks tangle wireless process control network", Process Engineering, vol.88, No.11, pp.154-163.

[17] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, (April 2011), "Home M2M networks: Architectures, Standards, and QoS improvement", Vol.49, pp 43-52.

[18] Zhou Yan-li, Fan Xiao-ping, Liu Shao-qiang, Xiong Zhe-yuan (2010), "Improved LZW Algorithm of lossless Data Compression for WSN", IEEE ICCSIT.
[19] Junguo Zhang; Wenbin Li; Xueliang Zhao; Xiaodong Bai; Chen Chen; , "Simulation and Research on Data Fusion Algorithm of the Wireless Sensor Network Based on NS2," Computer Science and Information Engineering, 2009 WRI World Congress on , vol.7, no., pp.66-70, March 31 2009-April 2 2009
[20] Gutierrez, J.A., Naeve,M., Callaway, E., Bourgeois, M., Mitter, V., and Heile, B," IEEE 802.15.4: A developing standard for low-power low-cost wireless personal area networks," in network,IEEE,2001,p.12.
[21] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. 1st IEEE Int'l. Wksp. Sensor Network Protocols and Applications (SNPA'03), May 2003.

Authors Biographies

Deepika Srikumar is currently doing M.E in Communication Systems at Sri Shakthi Institute of Engineering & Technology, Coimbatore. She has done her B.E in Electronics and Communication Engineering from Anna University of Technology, Coimbatore, Diploma in Electrical and electronics Engineering from PSG Polytechnic college, Coimbatore. Her research interest is Senor Networks. She has presented various papers in symposium, national conference, international conferences and International journal.

Seethalakshmi Vijaykumar is with the ECE department in Sri Shakthi Institute of Engineering & Technology, Coimbatore as Associate professor. She has done her B.E in Electrical and electronics Engineering from PSG college of Technology, Coimbatore, Tamilnadu, M.Tech in Electronics and Communication Engineering from PTU university, Punjab and pursuing PhD under Anna University of Technology, Coimbatore. Her research interest is Network Routing. She has rich 16 years of experience in industry as well as teaching. She has presented 16 papers in national conference and 11 papers in international conferences. She has published 4 papers in international journals.