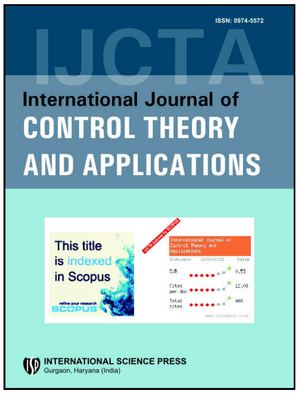


International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 13 • 2017

Position Count Based Trust Aware Rotuing Protocol for Wireless Sensor Network

Pooja Chaturvedi[1] and A. K. Daniel[1]

[1] *Department of Computer Science & Engineering, M. M. M. University of Technology, Gorakhpur, U. P., India,*
Emails: chaturvedi.pooja03@gmail.com, danielak@rediffmail.com

Abstract: The development of semiconductor technology and significant advancement in the information technology has made wireless interface platforms more popular. This had resulted in diverse applications of these networks ranging from daily activities to military services. The key factors which determine the success of the network functionality are: network lifetime and data collection process. The network lifetime is based on the optimization of energy consumption whereas the data collection process directly affects the network traffic. The paper proposes a position count based routing approach to address the problem of data collection reliability and energy efficiency. The trust based routing strategy is introduced which confronts the uncertainty and dynamism of the network. The simulation results shows that the proposed protocol improves the network efficiency in terms of the energy consumption and relay node optimization as compared to existing approach.

Keywords: position count, routing, trust, energy efficient, network lifetime.

1. INTRODUCTION

The recent technological advances have made the production of small and low cost sensors technically and economically possible, which forms the basis of the organization of the wireless networks. A wireless sensor network consists of a number of nodes having the communication capability either among each other or to a central processing unit known as the base station. The large number of the nodes provides the capability of the sensing the environmental conditions with greater accuracy. These networks gain numerous applications ranging from environmental monitoring to critical applications in battlefield surveillance, due to their inherent features such as self-organizing, fault tolerance. Routing the sensed information is a challenging task in the wireless sensor networks due to its inherent characteristics such as absence of global addressing mechanism, flow of data between the source nodes and the base station and resource constrained sensor nodes in terms of energy, storage and processing capacities. Due to these limitations several routing techniques have been proposed which consider these inherent features along with the application and architecture requirements which employs the following functionality as: data aggregation, in network processing, clustering, different role assignment and data centric mechanisms. Most of the routing approaches are based on employing the techniques which can maximize the network lifetime by determining the optimal paths towards the base station on the basis of several parameters such as residual energy, load, distance from the base station etc. In this paper position count based trust aware routing protocol for WSN is proposed which considers the resource constraints and data reliability [1].

The organization of the paper is as follows: quality of service (QoS) issues in routing in WSN in section 2, a brief study of the routing strategies in WSN in section 3, network model in section 4, proposed protocol in section 5, mathematical validation for route discovery in section 6, simulation results and analysis in section 7 and conclusion and future scope in section 8.

2. ROUTING PROTOCOLS IN WSN

The routing protocols in the WSN are classified into two types as: network structure based and network operation based [3].The network structure plays a crucial role in operation of the routing protocol. The network structure based routing protocols are further classified as: flat, hierarchical or location based. In flat routing protocol all the nodes have the same status and they communication the information between each other via collaboration. These protocols are data centric and multichip routing protocol. Flooding is the easiest routing mechanism in which the information is broadcast in all directions which results in the increased overhead and inefficient use of energy resources. Gossiping is another routing protocol which wastes a significant amount of energy. To overcome the limitation of the flooding and gossiping approaches, negotiation based routing protocol SPIN (Sensor Protocol for Information via Negotiation is proposed which is a 3 stage protocol and uses three types of messages as advertisement, request and data. The other variants of SPIN protocols are SPIN-1, SPIN-2, SPIN BC, SPIN PP, SPIN EC and SPIN RL. Although SPIN protocols achieve energy savings but the data delivery is not guaranteed in these protocols [3]. Directed diffusion is another gradient based data centric routing protocol. Although it achieves the energy savings but it cannot be applied in the applications which require continuous data delivery to the base station [4]. Rumor routing protocol which uses agents to respond to client queries hence it reduces the energy consumption of the network. But it can't be applied to applications having a large number of queries [5]. In hierarchical routing protocol the nodes in the network are divided into a number of levels. In hierarchical routing protocols the higher energy nodes are used for the aggregation and in network processing whereas the lower energy node performs the sensing operation. LEACH is the pioneer protocol based on the clustering. This protocol doesn't provide the load balancing as the cluster heads are selected randomly [6]. In location based the node location is used to determine the route from the source node towards the base station. Geographic adaptive fidelity is an energy aware location based routing protocol. In this protocol the network is divided into fixed regions and a number of virtual grids. There is an active node in each grid which transmits the sensed information towards the base station via the optimal paths [10]. Geographic and energy aware routing protocol is proposed as an enhancement to the directed diffusion. In this protocol the number of interests by localizing the region rather than the whole region [11].

A routing protocol is said to be adaptive if the system parameters can be controlled in order to adapt to dynamic network conditions. On the basis of the network operation the routing protocols can be classified as: negotiation based, multipath based, query based, QoS based, coherent based. There are a number of evolutionary routing protocols which exploit of a number of optimization techniques such as fuzzy logic, ant colony optimization, genetic algorithm, particle swarm optimization. SPAN protocol is proposed for multi hop ad hoc networks and it reduces energy consumption such that the network connectivity is not degraded. In this protocol the nodes join a backbone topology to forward the data packets. It offers significant energy savings but it doesn't extend the network lifetime to a great extent [12]. In [13], Geographic Random Forwarding (GeRaF) protocol is proposed which focuses on the multi hop communication, in terms of average number of hops to reach a destination which is based on a function of the distance and average number of available neighbors. In [14], energy efficient technique based on graph theory is used to find out minimum path based on some defined conditions from a source node to the destination node. This technique always find the minimum path and an alternate path is also saved in case of node failure. The length of the alternative path will be extended due to the node failure which in turn minimizes the energy savings. In [15], routing protocol based on forward address based shortest path routing in the network is proposed. GA based elitism concept is used to obtain energy efficient routing by minimizing the path length and thus maximizing the life of the network. In [16], Particle Swarm Optimization Routing (PSOR) protocol is proposed. The PSOR does routing by taking energy as a fitness value. By calculating the fitness value of the nodes, the protocol finds a new path to route the packets. From the various paths found it selects the optimized one that consumes less energy to route the packets. In case of node failure, choosing an alternate path is difficult.

3. MOTIVATION

The literature survey indicates that there is a considerable research in the field of data routing along with the consideration of lifetime maximization and connectivity issues, but there is a need of considerable research in the field of QoS metrics such as data reliability as none of the protocols discuss about the data delivery or the quality of data transmitted. The main contributions of our work are as follows:

1. Propose an energy efficient routing protocol which minimizes the energy consumption.
2. Propose a routing protocol which takes less setup time.
3. Ensure the QoS parameters for the transmitted data.

To achieve these objectives we have proposed a position count based trust aware routing protocol. The trust value of the nodes is computed as the weighted sum of direct trust, recommendation trust and indirect trust. The direct trust is computed as the weighted sum of data trust, communication trust and energy trust. The recommendation trust ensures the credibility of the recommender nodes by determining the recommendation reliability and familiarity. The position count mechanism is used to find the optimal routes among the several paths between the source and the destination.

4. NETWORK MODEL

In this paper we have considered a network of randomly deployed nodes in a square region of area A. The nodes in the network have the following properties:

1. The nodes in the network are homogenous; it means all the nodes have the same sensing and communication.
2. The sensing and communication model of the sensor node is considered as a circular disc of radius r where r represents the sensing range of the nodes and the sensor node is located at the center of the disc.
3. All the nodes are aware of their locations using some positioning devices such as GPS.
4. The network consists of a single base station is located at the center of the deployment region. The base station is considered to have infinite energy.
5. The standard energy model is considered for the processing and communication of the data packets [1].

4.1. Trust Model

The proposed model determines the trust values as the weighted average of the direct trust, recommendation trust and the indirect trust. The data trust is calculated as the weighted average of the data trust, communication trust and energy trust. To ensure the reliability of the recommender node we have incorporated the recommender node's reliability and familiarity [17][18].

4.1.1. Data Trust

The data trust (T_D) is calculated as the number of the correct data packets received at the base station:

$$T_D = (1 - \frac{N_{err}}{N}) \times 100\% \tag{1}$$

where N_{err} is the number of incorrect data packets and N is the total number of data packets transmitted. The incorrect data packets are identified by the variation in the readings of the nearby nodes.

4.1.2. Communication Trust

Communication trust (T_C) of the sensor node depends on the previous behavior of the nodes and it reflects the uncertainty of the network. In the proposed protocol subjective logic framework is used in which the trust is defined as a 3-triplet value: $\{b, d, u\}$, where b, d and u denotes the belief, disbelief and uncertainty of the nodes. b, d, u [0, 1] and $b+d+u=1$, s and f represents the number of successful and the failed communication for a node respectively. The Communication Trust is calculated as:

$$T_C = \frac{2b + u}{2} \tag{2}$$

where Belief $b = \frac{s}{s + f + 1}$ and Uncertainty $u = \frac{1}{s + f + 1}$

4.1.3. Energy Trust

Energy conservation is a major issue in the field of the wireless sensor networks so energy trust (T_E) is considered on the basis of energy consumption rate p_{ene}. The Energy Trust is calculated as:

$$T_E = \begin{cases} 1 - p_{ene}, & \text{if } E_{res} \geq \theta \\ else & 0 \end{cases} \tag{3}$$

where E_{res} is the Residual Energy of the node. Energy consumption rate p_{ene} is calculated as:

$$p_{ene} = \frac{IE - RE}{r} \tag{4}$$

where IE and RE represents the initial and residual energy of the nodes and r is the round number.

4.1.4. Direct Trust

Direct Trust (T_{Direct}) is calculated as the weighted average of the Data, Communication and Energy Trust as follows:

$$T_{Direct} = w_1 T_D + w_2 T_C + w_3 T_E \tag{5}$$

where w_1, w_2 and w_3 are the weight values for the Data, Communication and Energy trust respectively and

$$w_1 \in [0,\ 1], w_2 \in [0,\ 1]\ \ w_3 \in [0,\ 1]\ \ \&\ w_1 + w_2 + w_3 = 1.$$

4.1.5. Recommendation Familiarity

Recommendation Familiarity (T_F) represents the duration for which the recommender node is the neighbor of the object node. The longer the duration higher will be its trust value.

$$T_F = \frac{n}{N} \times reg^{\frac{1}{n}} \tag{6}$$

where n represents the number of successful communication between the recommender R and object node Y and N represents the number of successful communication by the recommender node R. reg is the regulatory factor for the number of communication and $reg \in [0, 1]$.

4.1.6. Recommendation Reliability

Recommendation Reliability (T_R) is calculated to eliminate the false trust values from the several trust values and is defined as:

$$T_R = 1 - \left| T_R^Y - T_{avg}^Y \right| \tag{7}$$

where T_R^Y is the recommendation value of object node Y calculated by recommender node R and T_{avg}^Y is the average value of all the recommendations.

4.1.7. Recommendation Trust

When direct communication between two nodes is not possible, the recommendation trust is calculated on the basis of the recommender node. There is a possibility of false recommendation from the recommender node, so to avoid this recommendation familiarity and reliability is calculated. Recommendation Trust $(T_{\mathrm{Re}\,com})$ is calculated as:

$$T_{\mathrm{Re}com} = \frac{\sum_{i=1}^{n} 0.5 + (T_R^Y - 0.5) \times T_F \times T_R}{n_0} \tag{8}$$

where n_0 is the number of recommender.

4.1.8. Indirect Trust

When the subject and object node are not directly reachable but have several intermediate nodes between them, a recommendation chain of the nodes, which comprise of the optimal path based on the distance and energy is determined. Indirect trust $(T_{IDR}^{\;Y})$ is calculated as:

$$T_{IDR}^{\;Y} = \begin{cases} T_R \times T_R^Y & \text{if } T_R^Y < 0.5 \\ 0.5 + (T_R - 0.5) \times T_R^Y, & \text{else} \end{cases} \tag{8}$$

$$T_{IDR+1}^{\;Y} = \begin{cases} T_{R+1} \times T_{IDR}^{\;Y}, & \text{if } T_{IDR}^{\;Y} < 0.5 \\ 0.5 + (T_{R+1} - 0.5) \times T_{IDR}^{\;Y}, & \text{else} \end{cases} \tag{9}$$

The trust values are updated as follows:

$$T(i+1)_{new} = w_i T(i) + w_{i+1} T(i+1) \tag{10}$$

where $T(i+1)_{new}$ represents the trust value in the next cycle, $T(i)$ and $T(i+1)$ represents the trust value at *ith* and *(i+1) th* time slot, w_i and w_{i+1} represents the aging factor.

5. PROPOSED POSITION COUNT BASED ROUTING PROTOCOL

In the proposed protocol the number of hop counts and the trust values of each path between the source and destination node is obtained. The trust value of a path is determined as the average of the trust values of the nodes included in the path. The hop counts and the trust values of each path is sorted in the increasing order and decreasing order respectively. Then the position count is assigned to each path. When a source node has an information to send to the destination the path with the minimum position count is selected.

Table 1
Pseudo code for the proposed routing protocol

1. Select all the possible data forwarding route from the source node to the base station BS.
2. Calculate the hop count for all the route from the source node to the base station
3. Calculate the trust values of all the routes from the source node to the base station
4. Implement sorting on calculated hop counts in ascending order,
   SORTEDVALUEShopcount = Sort [hop count from source node to the base station]
5. Implement sorting on calculated trust values in descending order,
   SORTEDVALUEStrust= Sort [Trust values of the nodes from source to the base station]
6. Assign POSITION_COUNT to all the possible routes R1, R2….Rn from source node to the base station
7. $\forall$ [(SORTEDVALUEShopcount) $\wedge$ (SORTEDVALUEStrust)]
8. Calculate the sum of POSITION_COUNT for all the possible routes.
9. FINAL_PATH for source node=MIN [$\forall$ (Sum of POSITION_COUNT)].
10. If EResidual of any inetrnediate node j in FINAL_PATH is EResidual< Thr then select node k where $k \in nei(j)$ where neig(j) represents the set of one hop neighbor nodes of node j and establish the route again
11. INFORM _MESS to source and destination.

6. MATHEMATICAL VALIDATION FOR ROUTE DISCOVERY

Consider a network of 30 nodes deployed randomly in the target region of dimensions 50*50. The base station is located far away from the target region. The other simulation parameters are shown in the Table 2 as:

Table 2
Simulation parameters

Simulation Parameter	*Value*
Area of the region	50×50 m^2
Location of sink	(25,75)
No. of Nodes	30
Sensing Range	5 m
Communication Range	15 m
Initial energy of the nodes	1 joule
Packet Size (L)	500 byte
Regulatory factor (R)	0.5

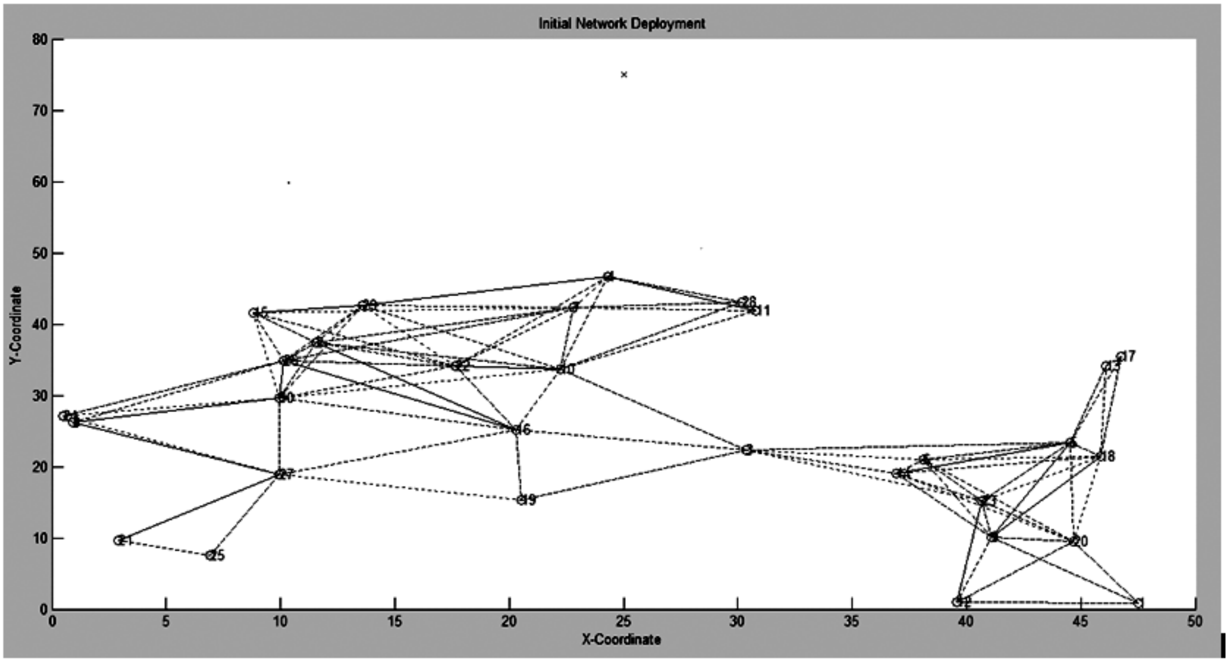


Figure 1: Snapshot of the deployed network of 30 nodes

If the source node is 19 and the destination node is 4 the different routes obtained are as:

$R_1 \rightarrow$ 19-16-10-7-4, $R_2 \rightarrow$19-27-30-26-2-29-4, $R_3 \rightarrow$ 19-16-22-7-4, $R_4 \rightarrow$ 19-3-10-7-4, $R_5 \rightarrow$ 19-3-10-11-28-4

The hop count and the trust values of the routes are as follows:

Table 3
Values of the parameters for different routes

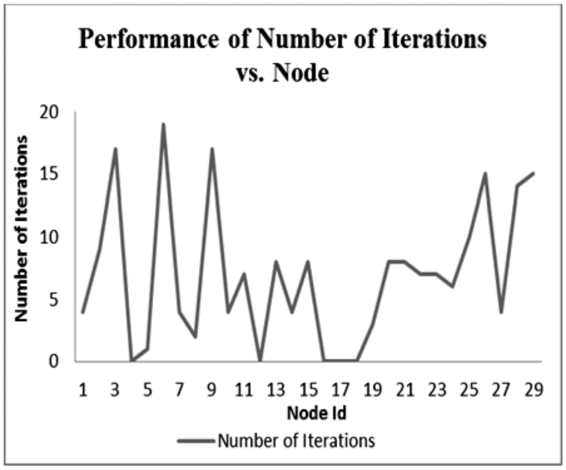
Route	*Hop Count*	*Trust Value*	*Position Count*
R_1	5	2.9183	6
R_2	7	5.1034	6
R_3	5	3.341	5
R_4	5	3.0372	7
R_5	6	3.6746	6

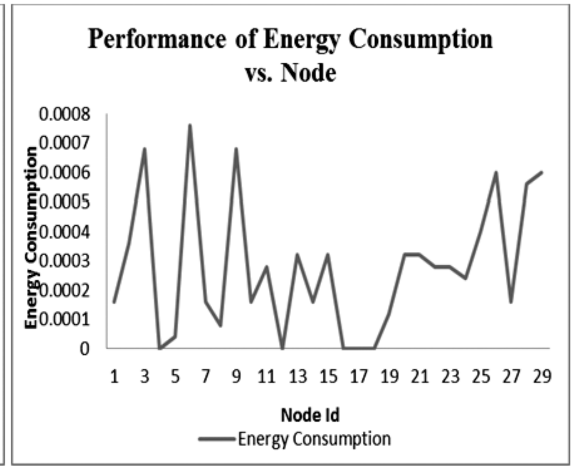
The results shows that the optimal route is R_3 with the position count value=5.

7. SIMULATION RESULTS AND ANALYSIS

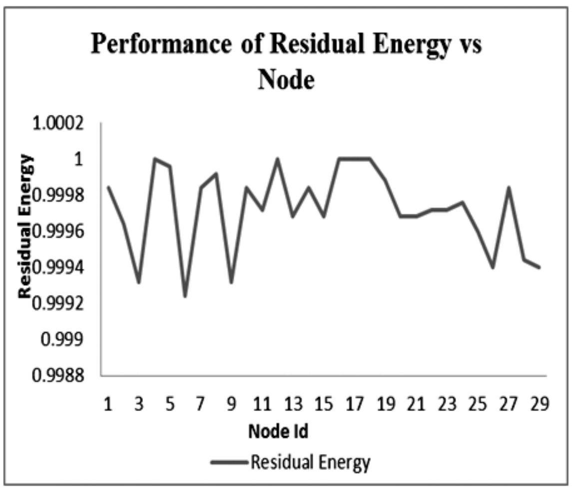
We have implemented both the routing protocols in MATLAB. The performance of the proposed routing protocol is shown in Fig. 2 a -2c. Fig 2a represents the number of iterations a node is involved in data transmission. Fig. 2 b represents the energy consumption of each node. Fig. 2 c represents the residual energy of each node.

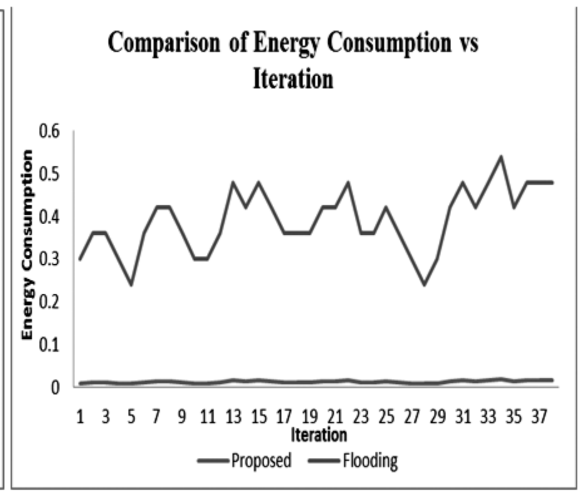
The performance of the proposed protocol is compared with the flooding protocol in terms of energy consumption in each iteration, number of active nodes and energy consumption of the network as shown in Fig. 2d and Fig.3 a and Fig. 3b. It is observed from the results that the proposed protocol outperforms the exisiting approach.





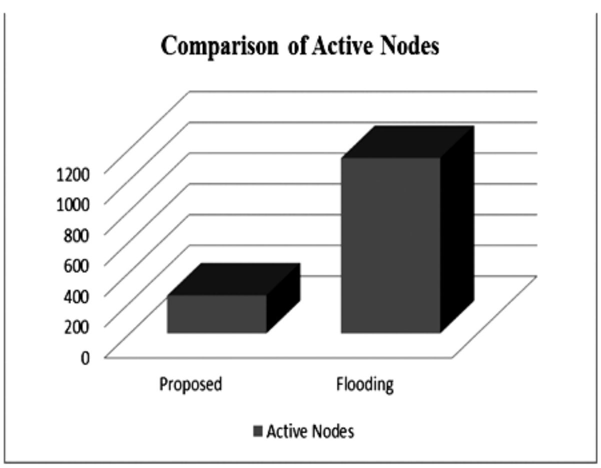
(a) **(b)**

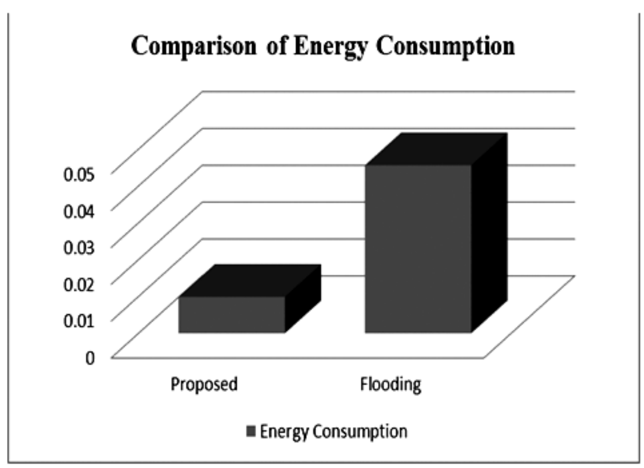




(c) **(d)**

Figure 2: (a) Performance of Number of Iterations vs. node (b) Performance of energy consumption vs. node (c) Performance of residual energy vs. node (d) Comparison of energy consumption vs. iteration





(a) **(b)**

Figure 3: (a) Comparison of active nodes (b) Comparison of energy consumption

8. CONCLUSION

In this paper position count based trust aware routing protocol is proposed. To overcome the uncertainties and dynamism of the network trust concept is used. The optimal paths based on trust values and hop counts is used which ensures the energy conservation, hence improves the network lifetime. The trust concept ensures that the data transmission between the source node and the destination node is reliable. The performance of the proposed protocol is compared with the existing approach and results shows an improvement in the network performance in terms of energy consumption and number of active nodes.

To evaluate the performance of the proposed protocol for the heterogeneous network is our future work.

REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, Volume: 40 Issue: 8, pp.102-114, August 2002.

[2] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," Proc. 5th ACM/IEEE Mobicom Conference (MobiCom '99), Seattle, WA, August, 1999. pp. 174-85.

[3] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless Networks, Volume: 8, pp. 169-185, 2002.

[4] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," Proceedings of ACM MobiCom '00, Boston, MA, 2000, pp. 56-67.

[5] D. Braginsky and D. Estrin, Rumor Routing Algorithm for Sensor Networks," in the Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, October 2002.

[6] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient Communication Protocol for Wireless Microsensor Networks," Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00), January 2000.

[7] Y. Xu, J. Heidemann, D. Estrin,Geography-informed Energy Conservation for Ad-hoc Routing," In Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking 2001, pp. 70-84.

[8] Y. Yu, D. Estrin, and R. Govindan, Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks", UCLA Computer Science Department Technical Report, UCLA-CSD TR-01-0023, May 2001.

[9] Benjie Chen, Kyle Jamieson, Hari Balakrishnan and Robert Morris, "Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad hoc Wireless Networks", Wireless Networks, Vol. 8, No. 5, pp. 481-494, 2002.

[10] Michele Zorzi and Ramesh R. Rao, "Geographic random forwarding (GeRaF) for ad hoc and sensor networks: Multihop performance", IEEE Transactions on mobile Computing, Vol. 2, No. 4, pp. 337-348, 2003.

[11] Shilpa Mahajan and Jyoteesh Malhotra, "Energy Efficient Path Determination in Wireless Sensor Networks using BFS Approach", Computer Science and Communications, Vol. 3, No.11, pp. 351-356, 2011.

[12] Vinay Kumar Singh and Vidushi Sharma, "Elitist Genetic Algorithm based Energy Efficient Routing Scheme for Wireless Sensor Networks", International Journal of Advanced Smart Sensor Network Systems, Vol. 2, No. 2, pp. 15-21, 2012.

[13] Snehal Sarangi and Biju Thankchan, "Particle Swarm Optimization based A Novel Routing Algorithm for Wireless Sensor Network", International Journal of Research in Engineering, Information Technology and Social Sciences, Vol. 2, No. 11, 2012.

[14] Jinfang Jiang, Guangjie Han, Feng Wang, Lei Shu, Mohsen Guizani, "An Efficient Distributed Trust Model for Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, 2014.

[15] Hyo Sang Lim, Yang Sae Moon, Elisa Bertino, Provenance based Trustworthiness Assessment in Sensor Networks, DMSN'10, September 13, 2010, Singapore.