EIRDA: An Energy Efficient Interest based Reliable Data Aggregation Protocol for Wireless Sensor Networks

Hemant Sethi, Devendra Prasad
Department of Computer Science & Engineering,
M.M. University, Mullana (Ambala), India

R. B. Patel
Department of Computer Science & Engineering,
DCRUST, Murthal (Sonepat), India

ABSTRACT

When designing a protocol for data aggregation two things need to be considered; data reliability and energy efficiency. A good data aggregation protocol is one that achieves high data reliability using the least amount of overhead as possible. In case of wireless sensor networks (WSNs), data aggregation is widely accepted as an essential pattern for energy efficiency. In this paper, we propose An Energy Efficient Interest Based Reliable Data Aggregation (EIRDA) Protocol for WSNs. EIRDA effectively delivers the data to the sink. In EIRDA, we consider static clustering scheme for the uniform distribution of sensor nodes (SNs) in each cluster. Simulation result shows that EIRDA is efficient in terms of energy and achieves higher reliability.

Keywords: Sensor Networks, MAC protocol, Data aggregation, Static Cluster.

1. INTRODUCTION

Wireless sensor networks (WSNs) consist of large numbers of resource constrained sensor nodes (SNs) communicating over the wireless medium for the purpose of collaborative information transmission. Data aggregation/fusion is defined as the process of coalescing data from multiple SNs to eliminate redundant data transmission and provide fused information to the base station (BS). The main motive of WSN is to disseminate information about the environment and more important here is, to deliver information correctly with less energy consumption. Recognizing that computation would be less energy consuming than communication, substantial energy savings can be obtained through data aggregation. Data Aggregation is a method to provide energy efficiency at MAC Layer. Two different types of aggregation are possible; namely, lossless aggregation and lossy aggregation [1]. Lossless aggregation refers to concatenating individual data items into larger packets, thus amortizing per-packet protocol overhead. Lossless aggregation is effective if the load on the system is not excessive. If the total communication load exceeds system capacity, the amount of communicated data must be forcibly reduced which is called the lossy aggregation

In case of WSNs, Address Centric protocols and Data-Centric Protocols are the two kinds of sensor routing protocols that performs in network aggregation [2].

In the Address centric (AC) routing Protocol, the short routes between pairs of addressable end nodes are identified. On the basis of the route that the queries took, this protocol permits each source to independently send data along the shortest path to sink.

In Data-centric (DC) Protocol, routes from multiple sources to a single destination that allow in-network consolidation of redundant data are identified. In this protocol, the data is sent to the sink by the sources, however, the content of the data is en-route looked and some form of aggregation/ consolidation function is performed on the data originating at multiple sources by the routing nodes. Data-centric technologies that carry out in-network aggregation of data to capitulate energy-efficient dissemination are essential. Figure 1 shows how data aggregation provides energy efficiency.

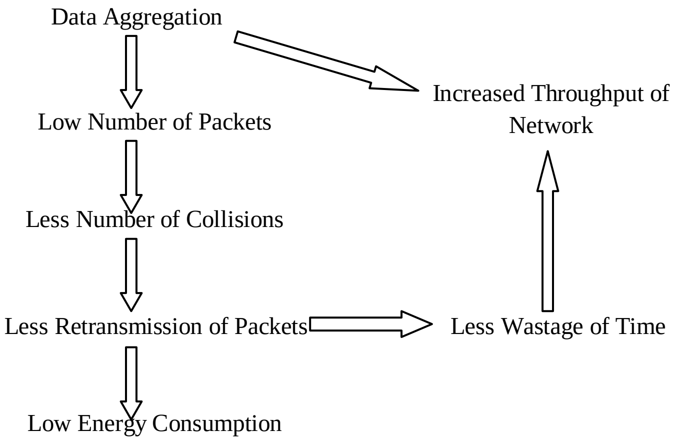
Data Aggregation
Low Number of Packets
Less Number of Collisions
Less Retransmission of Packets
Low Energy Consumption
Increased Throughput of Network
Less Wastage of Time

Figure 1: Effect of Data Aggregation

The ad hoc nature of WSN makes Address centric (AC) routing algorithms unsuitable for real time applications. The key metric in any WSN is delivery reliability per energy. To attain high reliability per energy, we use redundant copies of a packet to increase its end-to-end probability of data delivery [3]. The degree of redundancy introduced, is controlled by the amount of information the packet contains. Reputation and trust concepts can be used to overcome the shortcomings of cryptography based secure and reliable data aggregation. Reputation can be defined as the trustworthiness of an entity whereas trust is the expectation of one entity about the actions of another [3, 4]. Functional reputation [5, 6] of a SN is represented by the beta distribution [7] of the SNs actions with respect to a certain function. The beta distribution function f (p|α, β), where Posteriori probabilities of binary events can be represented as beta distributions which is indexed by the two parameters α and β[7,8] can be expressed using the gamma function Γ as:

$$f\left(\frac{p}{\alpha},\beta\right)=\Gamma\frac{(\alpha+\beta)}{\Gamma(\alpha)+\Gamma(\beta)}\,p^{\alpha-1}(1-p)^{\beta-1}$$

$$0\le p\le 1,\quad \alpha>0,\ \beta>0$$

The probability expectation value of the beta distribution is given by

$$E\,(p) = \alpha / (\alpha + \beta)$$

Compared to general reputation which is computed over all actions of the SN, using functional reputation prevents a compromised node from covering its bad actions with respect to one function by behaving well for other functions

We propose an Energy Efficient Interest based Reliable Data Aggregation (EIRDA) protocol, to effectively deliver the data to the sink. In this approach, we consider static clustering scheme for the uniform distribution of SNs in each cluster [9]. In this, the BS broadcasts an interest message containing its required data model, to all SNs in the deployment area. When the cluster head (CH) receives the data from the sources in each cluster, it fuses the data and applies the aggregation function on it depending on the interest message. To achieve energy efficient aggregation, the MAC protocol uses the partially overlapped channels (POC) [10].

2. RELATED WORK

The main aim of any hierarchical or cluster based routing protocol is to provide energy efficiency, scalability and communicational efficiency by logically arranging nodes in form of clusters. The cluster nodes send data to their common focal point called cluster head, CH. The CH applies certain aggregation function (max, avg etc.) over the collected data and transmits the result to BS; preventing the requirement of direct communication of all network nodes with BS provides energy efficiency.

A protocol E-LAUGH[9] provides uniform cluster size enabling an even load distribution in the network and thus provides energy efficiency. The protocol also saves dynamic clustering overheads by allowing a One-Time setup of clusters. E-LAUGH also provides location awareness to WSN by logically dividing the network into grids of desired granularity.

Several clustering algorithms have been proposed in recent years [11-14]. Many of them have rooted from LEACH. LEACH randomly selects a few nodes as cluster heads, based on certain probability function and rotates this role to balance the energy dissipation of the SNs in the networks. This rotation is done after every round. This repetitious set-up processes results in unnecessary energy consumption and delay. Its randomized nature creates clusters with non-uniform sizes leading to an uneven load distribution. Steady phase in LEACH requires CH to communicate directly with BS at the expenditure of energy.

In Power-Efficient GAthering in Sensor Information Systems (PEGASIS) [12], an enhancement over LEACH protocol was proposed which was a near optimal chain-based protocol. Here nodes need only communicate only with their closest neighbors and they take turns in communicating with the base-station thus enhancing the network lifetime. The rounds repeat, once the round of all SNs communicating with the base-station ends. As the power draining is spread uniformly over all nodes, the power required to transmit data per round is reduced. PEGASIS allows only local coordination between nodes that are close to each other, so that the bandwidth consumption in communication is reduced. To locate the closest neighbor, each node uses the signal strength to measure the distance to all neighboring nodes. The chain in PEGASIS will consist of those nodes that are closest to each other and form a path to the base-station. The protocol provides energy efficiency but induces lots of delay in data transmissions to the BS.

HEED [13] incorporates communication range limits and intra-cluster communication cost information for the decision of selection of CH.

Wendi Rabiner Heinzelman, et. al., have presented a family of adaptive protocols, called Sensor Protocols for Information via Negotiation (SPIN) which efficiently disseminates information among sensors in an energy constrained WSNs. SPIN uses meta-data negotiation and resource-adaptation to overcome several deficiencies in traditional dissemination approaches. They have also discussed the details of two specific SPIN protocols namely SPIN-l and SPIN-2. SPIN-l is a 3-stage handshake protocol for disseminating data, and SPIN-2 is a version of SPIN-l that backs off from communication at a low-energy threshold [15].

Kai-Wei Fan et al. [16] have proposed techniques for data aggregation that do not use any explicit structures. Efficient aggregation requires packets to meet at the same node (spatial convergence) at the same time (temporal convergence). For spatial convergence they have proposed a MAC layer anycast based approach called Data-Aware Anycast (DAA). For temporal convergence they have proposed Randomized Waiting (RW) at the application layer at the source. Also they have modeled the network load generated by the combined DAA with RW approach and shown that the predictions of the analysis match closely with the simulation results. They also defined the normalized network load as the number of packets transmitted in the network normalized by the number of contributing sources (number of nodes whose packets reached the sink with or without aggregation).

In [17], authors define in-network aggregation process "In-network aggregation is the global process of gathering and routing information through a multi-hop network, processing data at intermediate nodes with the objective of reducing resource consumption (in particular energy), thereby increasing network lifetime".

In [18], authors describe a new strategy for data gathering in WSN which considers both issues: energy efficiency and robustness. Authors first say that single path to connect each node to the BS is simple and energy-saving approach but expose a high risk of disconnection due to node/link failures. But multi-path approach would require more nodes to participate with consequent waste of energy. Authors present a clever use of multi-path only when there is loss of packet which is implemented by smart caching of data at SNs. Authors also argue that in many practical situation data may be gathered only from a particular region, so they use a different approach that relies on a spanning tree and provides alternative paths only when a malfunctioning is detected. Algorithm adopts a tree-based approach for forwarding packets through the network. In the ideal situation when no failures occur, this is certainly the best choice, as the minimum numbers of nodes are engaged in the transmission phase. In the presence of link or node failures, the algorithm discovers an alternative path which ensures the delivery of as many packets as possible within the time constraints. The problem with this approach is that it may cause the arising of hot spots and nodes along preferred paths will consume their energy resources quickly, possibly causing disconnection in the network.

3. SYSTEM MODEL

In proposed model we have assumed that the sensors are distributed in a uniformly randomized manner throughout a square field and the network has the following properties:

- There exists a unique BS located away from network.
- Clusters in the sensor field are static.
- Each Sensor Node (SN) has a unique identity.
- Sensors cannot move after being deployed.
- Network is homogeneous, i.e., all SNs are equivalent in computing and communication capacity.
- Each SN in the Sensor field is heterogeneous in role i. e each sensor node has the capability to behave as a general node and also has the ability to become a cluster head.
- The transmitter can adjust its amplifier power based on the transmission distance.

The first assumption about the stationary BS is just to simplify the understanding of protocol, but any variation can be assumed, as it doesn't affect the proposed protocol. The fourth assumption of lack of mobility is typical for WSNs employing some clustering or grouping methodology for network organization. Nodes with rapid mobility in network degrade the cluster quality, because they frequently alter the organization of cluster. Assumptions like node homogeneity are rather advantageous when hardware costs and resource requirements are key issues.

3.1 EIRDA protocol

Generally protocol complexity, node deployment, heterogeneity etc. are major issues for a given system model.

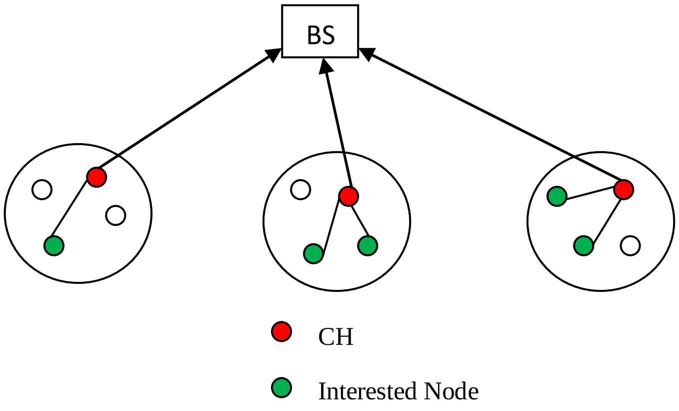

Figure 2: System Model

EIRDA considered a uniform clustering approach as in E-LAUGH [9]. The working of EIRDA is divided in two phases: Setup phase and Steady Phase.

3.1.1 Setup Phase

In the setup phase, the BS broadcast InitSim packet. All SNs in the deployment area receives the InitSim packet and sends a Beacon packet to its neighbor. Format of Beacon packet is as below:

<id, vote, E_{rem} ,δ > , where δ is trustworthiness factor.

After this CH is selected on the basis of E_{rem} if the SN is a reliable one. If more than one SN have the same E_{rem} and both are reliable SNs then CH is selected on the basis of vote which is any dynamic parameter that can be used by anyone who is working on any challenges in WSNs viz. one who is working on routing protocol can use distance as its parameter. If still any ambiguity arises, CH is selected on the basis of Node Id. Finally selected CH sends updateCH packet to each SN and to the BS.

3.1.2 Steady Phase

In steady phase, data communication is initiated and continues for more than one round after the cluster setup, unlike many LEACH based protocols where the steady phase includes only one round of data dissemination towards BS. This variation also prevents the delays involved before the data transmission hence makes it applicable for the time critical applications. To initiate data communications, the BS broadcasts interest packet in the following format, which is received by all SNs in the deployment area.

<nodeinterest, CHinterest> where nodeinterest includes interest id and description of interest message and CHinterest is meant for the CH for applying aggregation function.

On receiving the interest packet, SNs generates self-interest (i.e. actually the sensed data with its Interest Id) and compare it with the interest packet received from the BS [23]. If a match occurs, SNs sends the sensed data to the CH iff CH is believed to be trustworthy for fusion and CH receives data only from those interested nodes which are believed to be trustworthy for sensing and updates trust values $T_{i,j}^{sensin\,g}$ and $T_{i,j}^{routing}$ (as discussed below) of each interested node say N_i based on the first and second hand information regarding N_i and performs aggregation based on CH interest i.e. either sum, average etc. and forwards the aggregated data to BS.

3.2 Beta reputation system

Generally reliability of data transmission in any network model depends on SNs itself and links used for the routing purpose because either node or link catastrophes take place. SNs may fail because of energy diminution, physical damage or may be compromised by an antagonist. For achieving reliability in the proposed model, we evaluate the trustworthiness of each SN by using three types of functional reputation, namely sensing, routing and aggregation [5, 6, 19]. After network setup SNs monitor their neighborhood to obtain first-hand information of their neighbors. For sensing, routing and aggregation tasks, each SN, records good and bad actions of its neighbors in a table referred as functional reputation table (FRT) [5, 6]. These FRT are exchanged among SNs; which is used as second-hand information during trust evaluation. The FRT are piggy backed with other data and control packets in order to reduce the data transmission overhead. When N_i needs to interact with its neighbor N_j, N_i evaluates the trustworthiness using both first-hand and second-hand information about N_j. Functional reputation for aggregation ($R_{i,j}^{fusion}$) about N_j is needed by N_i to evaluate the trustworthiness of CHs. Functional reputations for routing ($R_{i,j}^{routing}$) and sensing ($R_{i,j}^{sensing}$) are used by data CHs to increase the security and reliability of the aggregated data. Functional reputation values are quantified using beta distributions of SN actions defined below.

3.3 Functional reputation and trust Computation

Functional reputation value ($R_{i,j}^{X}$) is computed using beta density function of N$_i$'s previous actions with respect to function X [5, 6, 7]. Trust ($\mathrm{T}_{i,j}^{X}$) is the expected value of $R_{i,j}^{routing}$. Let us take routing task as an example. If SN N$_i$, counts the number of good and bad routing actions of N$_i$ as α and β respectively then, N$_i$ computes the functional reputation $R_{i,j}^{routing}$ about node N$_j$ as *Beta(α+1, β+1)*. Following the definition of trust, $\mathrm{T}_{i,j}^{routing}$ is calculated as the expected value of $R_{i,j}^{routing}$

$$\mathrm{T}_{i,j}^{routing} = \mathrm{E}(Beta(\alpha+1,\beta+1)) \qquad \dots \qquad (1)$$

Equation (1) shows that the expected value of the beta distribution is simply the fraction of events that have had outcome α. Hence, functional reputation value of routing is given by the ratio of good routing actions to total routing actions observed. This is an intuitive decision and it justifies the use of the beta distribution. In the above formula, $R_{i,j}^{routing}$ represents node N$_i$'s observations about node N$_j$. In other words, it just involves first-hand information. Reputation systems that depend only on first-hand information has a very large convergence time, hence, second-hand information is desirable in order to confirm firsthand information. In protocol EIRDA we follow this approach where neighboring SNs exchange their functional reputation tables to provide second-hand information and this information is included in trust evaluation. Let us assume that N$_i$ receives second-hand information about node N$_j$ from a set of n nodes and $S_{in\,fo}(r_{k,j})$ represents the second-hand information received from node N$_k$. N$_i$ already has previous observations about N$_j$ as $\alpha_{i,k}$ and $\beta_{i,j}$. Further assume that, in a period of Δt, N$_i$ records good routing actions $\alpha_{i,j}$ and bad routing actions $\beta_{i,j}$ about N$_j$. Then, N$_i$ computes the trust $\mathrm{T}_{i,j}^{routing}$ about N$_j$ as follows.

$$\alpha_{i,j}^{routing} = v*\alpha_{i,j} + r_{i,j} + \sum_{k\in N} S_{in\,fo}^{routing}\left(r_{k,j}\right)$$

$$\beta_{i,j}^{routing} = v*\beta_{i,j} + r_{i,j} + \sum_{k\in N} S_{in\,fo}^{routing}\left(r_{k,j}\right)$$

$$\mathrm{T}_{i,j}^{routing} = \mathrm{E}(Beta(\alpha_{i,j}^{routing}+1, \beta_{i,j}^{routing}+1))$$

where *v* < 1 is the aging factor that allows reputation to fade with time. Integration of first and second hand information into a single reputation value is studied in [20, 21] by mapping it to Dempster-Shafer belief theory [7]. We follow a similar approach of [5, 6] and use the reporting node N$_k$'s reputation to weight down its contribution to the reputation of node N$_i$. Hence, second-hand information $S_{in\,fo}(r_{k,j})$ is defined as:

$$S_{in\,fo}(r_{k,j}) = \frac{(2*\alpha_{i,k}*r_{k,j})}{(\beta_{i,k}+2)*(r_{k,j}+s_{k,j}+2)*(2*\alpha_{i,k})}$$

$$S_{in\,fo}(s_{k,j}) = \frac{(2*\alpha_{i,k}*s_{k,j})}{(\beta_{i,k}+2)*(r_{k,j}+s_{k,j}+2)*(2*\alpha_{i,k})}$$

The idea here is to give greater weight to SNs with high trust and never give a weight above 1 so that secondhand information does not outweigh first-hand information. In this function, if $\alpha_{i,k}$ = 0 the function returns 0, therefore node N$_k$'s report does not affect the reputation update.

3.4 Analysis of EIRDA

- **Energy:** In LEACH, all SNs within each cluster, participates in data transmission in each round whether or not data transmitted is of concern for BS. But with EIRDA protocol**,**

Number of interested SNs/cluster/round = n
Number of SNs/cluster = 10
Probability of n SNs to be interested out of k:

$$p(n\,out\,of\,k) = \left(\frac{n}{k}\right)*p^{k}*q^{(n-k)} \qquad \dots(2)$$

In our simulation scenario, due to uniform distribution,

p = q = 0.5
Therefore from Equation (2)

$$p = \frac{n!}{k!*(n-k)!}*(0.5)^{k}*(0.5)^{(n-k)}$$

According to our results, k = 4.5. Therefore we consider for

k = 4 and k = 5.
P = P(4/10)+P(5/10)
= $(^{10}{}_{4})$* p^{10} + $(^{10}{}_{5})$* p^{10}
= $(^{10}{}_{4})$* $(0.5)^{10}$ + $(^{10}{}_{5})$* $(0.5)^{10}$
= ((10 !)/(10-4)! * 4!)*$(0.5)^{10}$ + ((10 !)/(10-5)! * 5!)*$(0.5)^{10}$
= 0.45

Therefore, we can say that there is a probability of each node to generate the same interest as of BS to send sensed data is 0.45 in each cluster. So, if we have 10 SNs / Cluster then we can say 0.45*10=4.5 number of SNs generates same interest as of BS and takes part in data transmission which we can verify from our simulation results. Our simulation results also shows that out of 10 SNs/Cluster, on an average 4.5 number of SNs generates same interest and takes part in transmission of sensed data in each round. Hence SNs which do not have data for concern of BS don't transmit data and hence saves energy.

- **Fault Tolerance:** Since less number of SNs transmits data with same interest, it reduces the number of collisions and hence retransmission in the network. Because of less number of collisions, network is more fault-tolerant.

- **Easy CH Selection:** The CH selection is rotated among all SNs within the cluster. Static clustering provides uniform distribution of load at CH as in E-LAUGH.
- **Security:** Each SN generates the interest randomly so the intruder does not know which SN generates which interest Id which makes the network more secure. To provide more security data may be encrypted before transmission.

4. SIMULATION RESULTS AND DISCUSSION

For realistic, our simulation uses the first order radio model [22] as the communication model. Equation (3) and (4) represent the energy dissipation when a SN sends or receives an *l*-bit message.

$$E_{trans} = \begin{cases} l \times (E_{elec} + E_{fs} \times d^2), if d \leq \sqrt{\dfrac{E_{fa}}{E_{mp}}} \\ l \times (E_{elec} + E_{mp} \times d^4), if d > \sqrt{\dfrac{E_{fs}}{E_{mp}}} \end{cases} \quad \ldots \qquad (3)$$

$$E_{recieve} = l \times E_{elec} \qquad \ldots \qquad (4)$$

To verify that EIRDA successfully reduces energy consumption for each SN, while achieving desired level of quality, we ran simulations on OMNeT++ simulator[24] and compare performance of EIRDA with some existing protocols. Following simulation parameters are used to simulate EIRDA.

- Number of SNs/Cluster = 10
- Desired level of Reliability = 0.9
- Area Size = 100 X 100
- Packet Size = 1024 bytes
- Initial Energy = 2.0 Joules
- Number of Rounds/ Steady Phase = 05
- Mac = 802.11

From Figure 3, it can be seen that energy has depleted up to 1.918(approx.) in LEACH where as in EIRDA energy has depleted up to 1.948(approx.) as shown in Figure 3(b). From these values, we can inference a mathematical formula,

$\pi_E = ((E_{cwoEIRDA} – E_{cwEIRDA}) / E_{cwoEIRDA})* 100$

where, π_E is percentage of saving in energy consumption, $E_{cwEIRDA}$ is Energy Consumed with EIRDA, and $E_{cwoEIRDA}$ is Energy Consumed without EIRDA.

Energy Consumed without EIRDA,
$E_{cwoEIRDA} = 2-1.918 = 0.082J$
Energy Consumed with EIRDA,
$E_{cwEIRDA} = 2-1.948 = 0.052J$
Therefore Decrease in Energy Consumption
= (0.082 – 0.052) / 0.082 *100= 36.59%

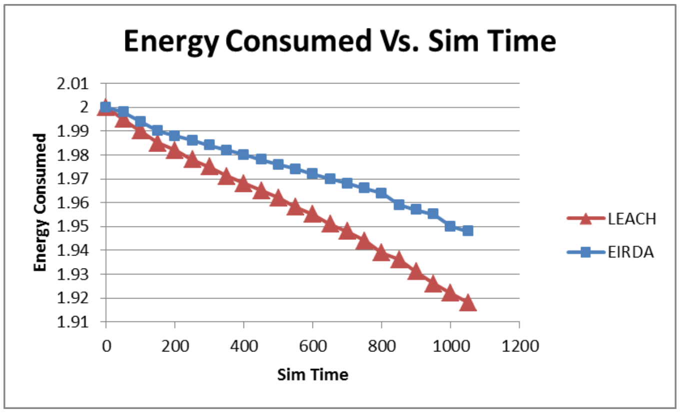

Figure 3: Comparison of Energy Consumed

Figure 4 represents the comparison of number of rounds of transmission when network is dead in EIRDA, which is 975 where as the number of rounds in LEACH comes out to be 620. From these values, we can inference a mathematical formula as:

$\pi_R = ((NR_{wEIRDA} – NR_{woEIRDA}) / NR_{woEIRDA})* 100$, where

π_R : percentage of increase in number of rounds of transmissions.
NR_{wEIRDA} : number of Rounds with EIRDA, and
$NR_{woEIRDA}$: number of rounds without EIRDA

$\pi_R = ((975 – 620)/620)*100 = 57\%$.

From calculations, according to our proposed protocol, there is an increase of 57% in number of rounds for transmissions.

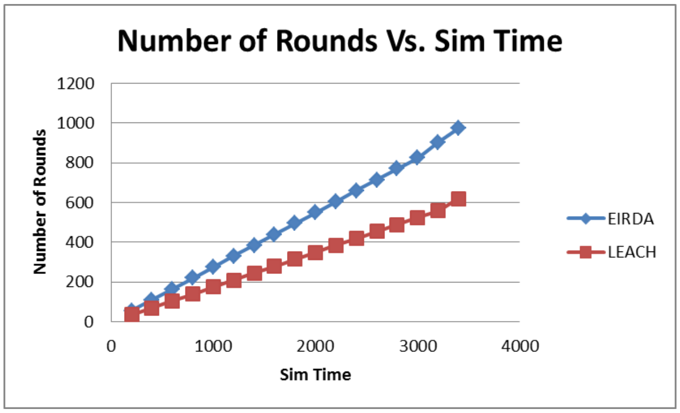

Figure 4: Comparison of Network Life

5. CONCLUSION

In this paper An Energy Efficient Interest Based Reliable Data Aggregation (EIRDA) Protocol for Wireless Sensor Networks is proposed. EIRDA is based on the interest generated by BS. Interest of BS is matched both by the SN and the CH. The SNs which have generated the same interest id, sends the data to the CH. The CH selects the reliable SN's out of the interested SNs and applies the aggregation function on the data received from these SNs within the cluster and delivers the aggregated data to the BS. Reliability is provided in the protocol by the concept of Functional Reputation which is implemented using Beta-distribution function. The overall impact of all measures taken at each phase of protocol implementation is clearly visible on the energy spent in the setup phase of the protocol. The multi-hop variation in steady phase will again provide further energy efficiency.

6. REFERENCES

[1] M. Y. Mohamed Yacoab, V. Sundaram, "An Adaptive Traffic Aware Data Aggregation Technique for WSNs", American Journal of Scientific Research, ISSN 1450-223X, pp. 64-77 Issue 10 , 2010.

[2] B. Krishnamachari, D. Estrin, and S. Wicker,(2002.)" Modeling data centric routing in WSNs, Technical Report CENG 02-14, USC Computer Engineering.

[3] Hong Luo, Qi Li, Wei Guo, RDA: Reliable Data Aggregation Protocol for WSNs, IEEE 2006

[4] Tamara Pazynyuk, JiangZhong Li, George S. Oreku,"Reliable Data Aggregation Protocol for WSNs", *IEEE*, 2008.

[5] Suat Ozdemir,"Functional Reputation Based Data Aggregation for WSNs", IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, 2008.

[6] Suat Ozdemir, Functional reputation based reliable data aggregation and transmission for wireless sensor networks, Computer Communications 31 (2008) 3941–3953, ELSEVIER

[7] A. Josang, R. Ismail, The beta reputation system, in: Proc. of the 15th Bled Conf. Electronic Commerce, 2002, p. 41.

[8] G. Casella, R.L. Berger, Statistical Inference, Duxbury Press, 1990.

[9] Ajay Kr. Gautam and Amit Kr. Gautam **"**A Protocol for Energy Efficient, Location Aware, form and Grid Based Hierarchical Organization of WSNs", Communications in Computer and Information Science, Volume 40, 2009.

[10] Baobing Wang, Xiaohua Jia and Xiaodong Hu. "Reduce Data Aggregation Latency by Using Partially Overlapped Channels in WSNs" Submitted to IEEE Transactions on Wireless Communications.

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

[12] S. Lindsey, C. Raghavendra, "PEGASIS: Power-Effcient Gathering in Sensor Information Systems", IEEE Aerospace Conference Proceedings, Vol. 3, pp.1125-1130, 2002.

[13] Ossama Younis and Sonia Fahmy, "HEED: A Hybird, Energy-Efficient Distributed Clustering Approach for Ad-hoc Sensor networks", IEEE Trans. On Mobile computing, vol.3, No.4, pp.660-669, 2004.

[14] Jalil Jabari Lotf, Mehdi Nozad Bonab and Siavash Khorsandi, "A Novel Cluster-based Routing Protocol with Extending Lifetime for WSNs" ,IEEE, 2008.

[15] Wendi Rabiner Heinzelman, Joanna Kulik, and Hari Balakrishnan, (1999)"Adaptive Protocols for Information Dissemination in WSNs", in proceedings of 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking", pp: 174- 185.

[16] Kai-Wei Fan, Sha Liu, and Prasun Sinha, (August 2007) "Structure-free Data Aggregation in Sensor Networks", IEEE Transactions on Mobile Computing, vol. 6, no. 8, pp: 929-942, Doi: 10.1109/TMC.2007.1011.

[17] E. Fasolo, M. Rossi, J. Widmer, M. Zorzi, "In-network Aggregation Techniques for WSNs: A Survey," IEEE Wireless Communication, 14(2), 2007.

[18] L.Gatani, G.L. Re, M.Ortolani, "Robust and Efficient Data Gathering for WSNs," in Proceeding of 39th Annual Hawaii International Conference on System Sciences, 2006.

[19] Virender kumar Ranga, Jagan Nath & Mohit Dua,"Performance analysis of an optimized energy efficient data aggregation protocol", International Journal of Information Technology and Knowledge Management, July-December 2010, volume 2, no. 2, pp. 523-527.

[20] S. Ganeriwal, M. Srivastava, Reputation based framework for high integrity sensor networks, in: Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, 2004, pp. 66–77.

[21] S. Ganeriwal, L.K. Balzano, M. Srivastava, Reputation based framework for high integrity sensor networks, ACM Transactions on Sensor Networks 4 (3) (2008) 1–37.

[22] Krause, C. Guestrin, A. Gupta, and J. Kleinberg, "Near-optimal sensor placements: Maximizing information while minimizing communication cost", in Proceedings of Information Processing in Sensor Networks, 2006.

[23] C. Kavitha and Dr.K.V.Viswanatha ,"Pull Based Energy Efficient Data Aggregation Scheme for Wireless Sensor Networks" International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 28,2010

[24] "Omnet++: Objective modular network test bed in C++," http://www.omnetpp.org.