IJMETMR
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Energy-Efficient, Reliable Routing and Robust Data Aggregation Method for Mobile Wireless Sensor Networks

Swaathi S V
M.Tech,
Computer Network and Engineering,
Dayananda Sagar College of Engineering.

Dr.S.Venkatesan
Professor,
Department of Computer Science and Engineering,
Dayananda Sagar College of Engineering.

ABSTRACT:

The sensor nodes are inexpensive, disposable, and expected to last until their energy drains out. Therefore, energy is a very limited resource for a WSN system, and it needs to be managed in an optimal fashion. Reliable and successful data delivery at the BS is desired. Energy efficiency is an important aspect of any application of WSN. Routing of data in WSN is a critical task, and significant amount of energy can be saved if routing can be carried out tactfully. Routing is an issue linked to the network layer of the protocol stack of WSN. We present a novel energy-efficient routing protocol for Wireless sensor networks. The protocol is reliable in terms of data delivery at the base station (BS).

The proposed protocol is hierarchical and cluster based. Each cluster consists of one cluster head (CH) node, two deputy cluster head nodes, and some ordinary sensor nodes. The reclustering time and energy requirements have been minimized by introducing the concept of cluster head panel. Depending on the topology of the network, the data transmission from the cluster head node to the base station is carried out either directly or in multihop fashion. We will develop model for attacks show detection and prevention mechanism at the first stage of the protocol, the base station selects a set of probable cluster head nodes and forms the cluster head panel. Reliability aspect of the protocol, it puts best effort to ensure a specified throughput level at the base station by avoiding attacks in the network. Simulation results the energy efficiency, throughput, and prolonged lifetime of the nodes under the influence of the proposed protocol.

Introduction

Wireless sensor networks (WSN), sometimes called wireless sensor and actuatornetworks (WSAN), are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location.

The WSN is built of nodes from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. The propagation technique between the hops of the network can be routing or flooding.

Wireless Sensor Network (WSN) consists of several resource-constrained sensor nodes randomly deployed over a geographic region. These sensor nodes forward sensory data toward a resourceful base station (BS). Depending on the application type, the BS is located either far away from the sensor field or within the sensor field the sensor nodes generate sensory data from the environment of interest. Such networks have wide range of applications in military and civil domains. Some application areas of WSN are as follows: combat field surveillance, target tracking in battlefields, intrusion detection, postdisaster rescue operations, smart home, monitoring and alarming systems for supermarkets, wildlife monitoring systems, and many safety and security related applications. The sensed data are finally forwarded toward BS for further processing and decision making with regard to the control for meeting the objectives of the system in place.

Mobility of sensor nodes in wireless sensor network (WSN) has posed new challenges particularly in packet delivery ratio and energy consumption. Some real applications impose combined environments of fixed and mobile sensor nodes in the same network, while othersdemandacompletemobilesensorsenvironment.Pack etlossthatoccursduetomobility of the sensor nodes is one of the main challenges which come in parallel with energy consumption. Energy is an extremely critical resource for battery-powered wireless sensor networks (WSN), thus making energy-efficient protocol design a key challenging problem. Most of the existing energy-efficient routing protocols always forward packets along the minimum energy path to the sink to merely minimize energy consumption, which causes an unbalanced distribution of residual energy among sensor nodes, and eventually results in a network partition Depending on the application type, the sensor nodes and the BS can be static or mobile. In a typical WSN, the sensor nodes are highly resource constrained. The sensor nodes are inexpensive, disposable and expected to last until their energy drains out Therefore, energy is a very limited resource for a WSN system, and it needs to be managed in an optimal fashion. Reliable and successful data delivery at the BS is desired. Energy efficiency is an important aspect of any application of WSN. Routing of data in WSN is a critical task, and significant amount of energy can be saved if routing can be carried out tactfully. Routing is an issue linked to the network layer of the protocol stack of WSN. In multi hop communication, the major issue may be the selection of the intermediate nodes in the route.

Existing System

The existing system has been on maximizing end-to-end throughput and minimizing delay. Apart from these two design objectives, there are two more dominating design issues. These are energy constraintsand signal interference. Due to the unattended nature of the sensor nodes in the WSN applications, the energy efficiency issue has become extremely important. Multi-path and Multi-SPEED routing protocol are some routing protocols designed for WSN. Directed Alternative Spanning Tree and energy-efficient routing algorithm to prolong lifetime are some recent work of energy-efficient routing. The proposed energy-balanced routing protocol, in which the packets move toward the BS through dense energy area and thus protect the nodes with relatively low residual energy The protocol prolongs the lifetime of the network, but it does not consider the issue of reliable data delivery. The protocol does not consider mobility of the sensor nodes and the BS. The modified LEACH (MLEACH)is an extension of the LEACH protocol, which can handle mobility of sensor nodes. M-LEACH,again, does not consider mobility in the BS. LEACH is enhanced in order to support mobile sensor nodes.

Limitations of Existing

None of the existing protocols can achieve all the following goals at the same time:

1) Guaranteeing reliability in an energy-efficient manner in presence of node and BS mobility

2) Managing mobility of the nodes and maintaining connectivity through alternate paths

3) Minimizing message overhead and overcoming less reliable wireless links.

4) Guaranteeing robust data aggregation.

Problem Statement

To acquire energy-efficient and reliable routing protocol for a mobile WSN that operates in an unattended manner and, sometimes, in hostile environment has become the major goal to be achieved. As the sensor nodes are

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

resource constrained, the routing protocol should consume low power and should not burden the nodes with storage overhead.

MODULE IMPLEMENTATION

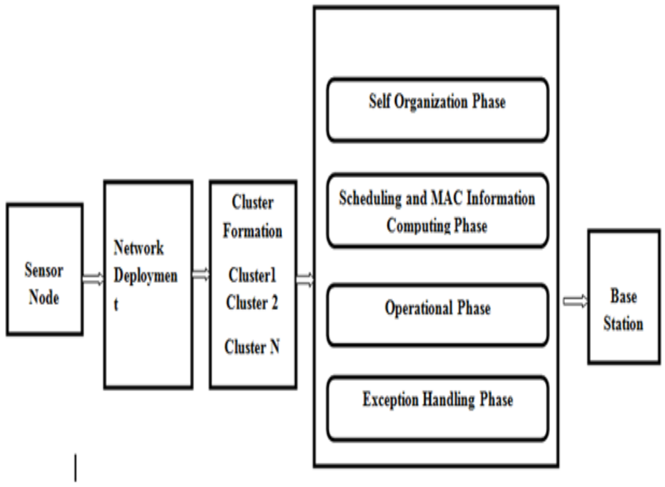


Fig 1: Different Modules

The protocol is divided into four phases fig.8 describes the overall protocol in terms of its different phases.

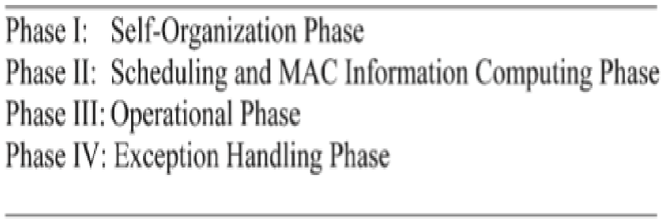

Phase I: Self-Organization Phase
Phase II: Scheduling and MAC Information Computing Phase
Phase III: Operational Phase
Phase IV: Exception Handling Phase

Fig:2 Overall protocol description of E2R2.

Self-Organization Phase

The clusters are formed. The CH set, the current CH, and the two DCH nodes are selected by the BS. BS collects the current location information from each of the sensor nodes and then forms a sensor field map. The nodes in the CH panel can take the role of CH node and DCH node. This selection is based on the cumulative credit point earned from the three parameters, namely, residual energy level of the node, degree of the node, and mobility level of the node. The self-organization phase, each node broadcasts it's three attributes, namely, geographic location information, residual energy level, and mobility level or velocity. This broadcast is intended for the BS so that the BS can utilize those for cluster formation and CH panel selection. The designer can use a suitable normalization function to compute the cumulative credit point earned by a node considering these three non-homogeneous parameters.

Scheduling and MAC Information Computing Phase

The sensor nodes can be in either of the two states active and dormant. Sensor nodes are scheduled for dormant state, which is a low-power state. A node in dormant state does neither any sensing task nor any relaying task.

The node does state transition from its dormant state to the active state as signaled by the BS. BS distributes a time-division multiple access (TDMA)- based medium access time slot for each of the CH and DCH nodes in order to enable communication with the BS.

Operational Phase

During this phase, actual sensory data transmissions take place. The sensor nodes forward data toward the CH node according to their respective medium access time slots. The CH nodes remove the redundancies in the data sent by the sensor nodes by the process of data aggregation and finally forward the aggregated data toward the BS as per the communication pattern distributed by the BS. DCH nodes do only cluster management tasks such as monitoring the mobility of the nodes and exception handling. Normally, they do not take part in data sensing and data forwarding tasks, but they do data forwarding under exceptional circumstances, which is described in the following. This phase, i.e., operational phase, has the longest time interval in comparison with the other afore mentioned phases.

Exception Handling Phase

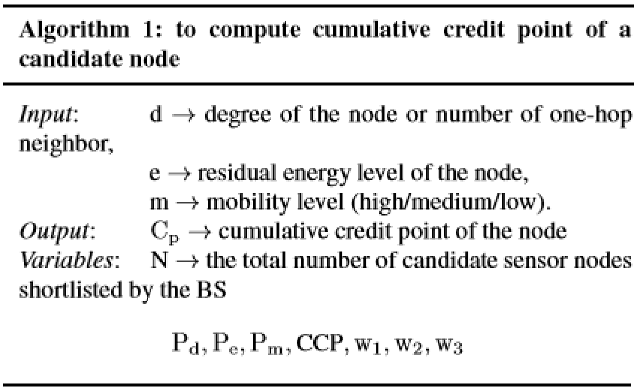
This phase is an occasional one. Due to the node mobility and the sudden death of some sensor nodes, the CH node may lose enough links with its cluster members. This may significantly degrade the throughput level in terms of packet delivery at the BS. Under this

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

situation, the BS may send feedback to the CH, and the CH then checks the current connectivity with its cluster members. If there is significant loss of connectivity with its cluster members, then the CH is asked to relinquish the charge of cluster headship, and a new one is selected either from the CH panel or one from within the two DCH nodes already selected. If a DCH node becomes the CH (as shown in Fig. 3), another node from the CH panel is selected by the BS as the DCH. We consider this as the first exception condition. These condition may be the link failure between the CH and the DCH. This link is not required all the time. However, if this link is not available at the time of need, either party, i.e., CH or DCH, informs the BS.

Then, the BS checks and compares the geographic locations of both CH and DCH. The BS selects a new suitable DCH from within the CH panel if it finds that there is no chance of return of the current DCH node to the proximity of the CH node. The third exception condition is as follows: the CH may lose the link with the next hop in its communication pattern toward the BS. This is a critical situation, and the CH becomes unable to transmit data toward the BS. Then, the CH requests the DCH nodes to inform if it has a route available toward the BS. If such a route is available, then data packets follow the route through one of the two DCH nodes toward the BS. This process goes on until the next hop in the communication pattern of the CH becomes available or the BS distributes a new communication pattern to the CH for routing.

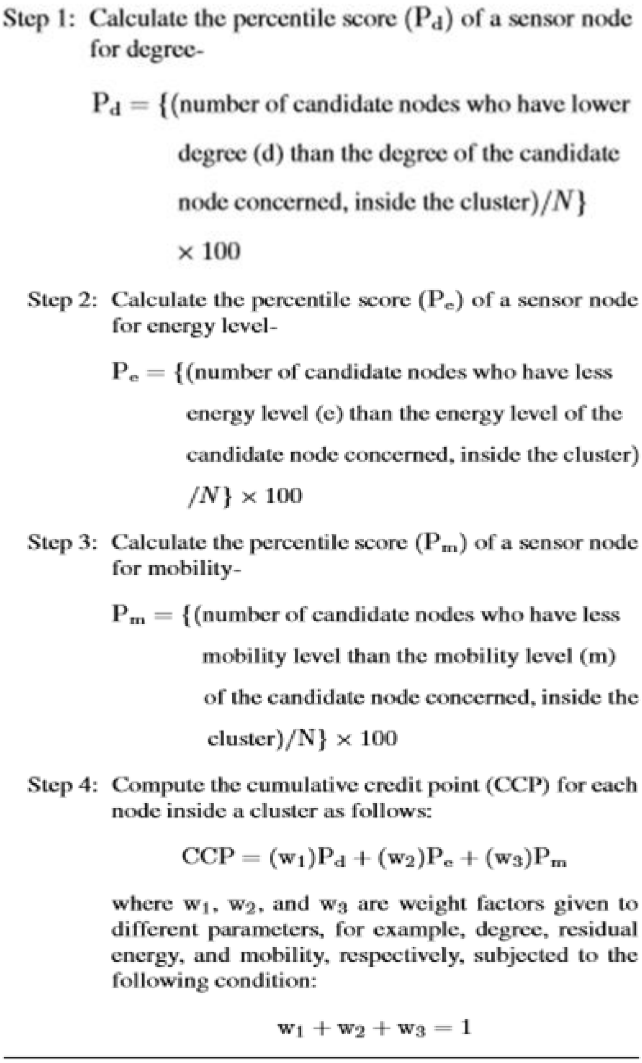
Algorithm



Algorithm 1: to compute cumulative credit point of a candidate node

Input: d → degree of the node or number of one-hop neighbor,
e → residual energy level of the node,
m → mobility level (high/medium/low).
Output: C_p → cumulative credit point of the node
Variables: N → the total number of candidate sensor nodes shortlisted by the BS

$$P_d, P_e, P_m, CCP, w_1, w_2, w_3$$



Step 1: Calculate the percentile score (P_d) of a sensor node for degree-

$$P_d = \{(\text{number of candidate nodes who have lower degree (d) than the degree of the candidate node concerned, inside the cluster})/N\} \times 100$$

Step 2: Calculate the percentile score (P_e) of a sensor node for energy level-

$$P_e = \{(\text{number of candidate nodes who have less energy level (e) than the energy level of the candidate node concerned, inside the cluster})/N\} \times 100$$

Step 3: Calculate the percentile score (P_m) of a sensor node for mobility-

$$P_m = \{(\text{number of candidate nodes who have less mobility level than the mobility level (m) of the candidate node concerned, inside the cluster})/N\} \times 100$$

Step 4: Compute the cumulative credit point (CCP) for each node inside a cluster as follows:

$$CCP = (w_1)P_d + (w_2)P_e + (w_3)P_m$$

where w_1, w_2, and w_3 are weight factors given to different parameters, for example, degree, residual energy, and mobility, respectively, subjected to the following condition:

$$w_1 + w_2 + w_3 = 1$$

Iterative filtering algorithm:

Using the above algorithm Cluster head and deputy cluster head is selected, but Data from multiple sensors is aggregated at an aggregator node which then forwards to the base station only the aggregate values. At present, due to limitations of the computing power and energy resource of sensor nodes, data is aggregated by extremely simple algorithms such as averaging.

However, such aggregation is known to be very vulnerable to faults, and more importantly, malicious attacks [1]. This cannot be remedied by cryptographic methods, because the attackers generally gain complete access to information stored in the compromised nodes.

For that reason data aggregation at the aggregator node has to be accompanied by an assessment of trustworthiness of data from individual sensor nodes
Such an algorithm should have following feature.

The algorithm should also be robust in the presence of non-stochastic errors, such as faults and malicious attacks, and, besides aggregating data, such algorithm should also provide an assessment of the reliability and trustworthiness of the data received from each sensor node. The main goal of data aggregation method to gather and aggregate data in any energy efficient manner so that network lifetime is enhanced.

Trust and reputation system have a significant role in supporting operation of a range of distributed systems from wireless sensor networks and e-commerce infrastructure to social networks, by providing an assessment of trustworthiness of participants in such distributed systems. A trustworthiness assessment at any given moment represents an aggregate of the behaviour of the participants up to that moment and has to robust in the presence of various attacks and malicious users.

There are number of incentives for attackers to manipulate the trust and reputation scores of participants in a distributed system. The main target of the malicious attackers are aggregation algorithms of trust and reputation systems. Iterative Filtering algorithms are an attractive for WSNs because they solve the data aggregation and data trustworthiness assessment using single iterative procedure. Such trustworthiness estimate of each sensor is biased on the distance of the readings of such a sensor from the estimate of the correct values, obtained in the previous round of iteration by some form of aggregation of the readings significantly differ from such estimate are assigned less trustworthiness and consequently in the aggregation process in the present round iteration their readings are given a lower weight. If the attackers have a high level of knowledge about the aggregation algorithm and its parameters, they can conduct the sophisticated attacks on WSNs by exploiting false data injection through a number of compromised nodes.

This paper presents a new sophisticated collusion attack scenario against a number of existing IF algorithms based on the false data injection. In such an attack scenario, colluders attempt to skew the aggregate value by forcing such IF algorithms to converge to skewed values provided by one the attackers.

PROPOSED SYSTEM

The proposed system is mainly to avoid the attacks availability on the each sensor nodes reading. An improvement is made on iterative filtering technique by providing an initial approximation which not only makes the algorithm collusion robust, but also faster converging. Iterative Filtering algorithms are an efficient and reliable option for wireless sensor networks because they solve both problems of data aggregation and data trustworthiness estimation using a single iterative procedure. This algorithm is for robust aggregation along with which different collusion attacks are identified and avoided in the proposed system. These attacks are described by estimating sensor's error and uses MLE for robust aggregation. The trustworthiness of nodes is estimated from their data aggregated from them. The computational cost is also reduced by the proposed method. A Proposed system architecture In the wireless sensor network consists of sensor nodes these sensor nodes are scattered then deployed environment in the network and then to form the cluster ,each cluster has a cluster head and then data send to the aggregator node before sending base station to verify the data if any error in the data then to estimate the value using parameters such as bias and variance and also estimate

MLE using iterative filtering algorithm. The proposed system architecture view can be shown in Fig 3

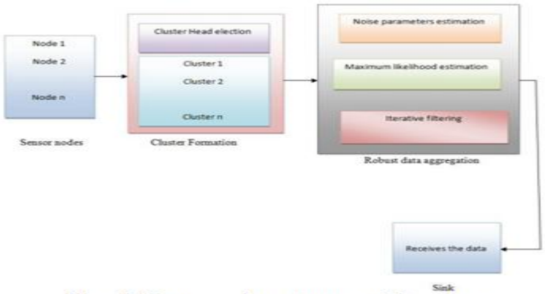


Fig .3.Proposed system architecture.

B. Enhanced Iterative Filtering Algorithm

IF algorithm is robust against the simple outlier injection by the compromised nodes. An adversary employs three compromised nodes in order to launch a collusion attack.

It listens to the reports of sensors in the network and instructs the two compromised sensor nodes to report values far from the true value of the measured quantity.

It then computes the skewed value of the simple average of all sensor readings and commands the third compromised sensor to report such skewed average as its readings. In other words, two compromised nodes distort the simple average of readings, while the third compromised node reports a value very close to such distorted average thus making such reading appear to the IF algorithm as highly reliable reading.

As a result, IF algorithms will meet to the values provide by the third compromised node, because in the first iteration of the algorithm the third compromised node will achieve the highest influence, radically dominate the weights of all other sensors. Initial test vector based on the IF method provide a robust nature of the security system.

ALGORITHM

```
Do iterative filtering
{
If( no. of packets== threshold && bandwidth==threshold && hash value is same)
}
Do( introduce extra packets into the system)
{
If( node parameters remain same)
{
Normal operation;
}
Else
{
Block the node, and declare it to be malicious
}
}
```

ROBUST DATA AGGREGATION

A. Robust Data Aggregation Framework Robust Data

Aggregation model is operates on batches of consecutive readings of sensors, proceeding in several stages. In the first stage provide an initial estimate of two noise parameters for sensor nodes, bias and variance details of the computations for estimating bias and variance of sensors. A novel approach for estimating the bias and variance of noise for sensors based on their readings. The variance and the bias of a sensor noise can be interpreted as the distance measures of the sensor readings to the true value of the signal. In fact, the distance measures obtained as our estimates of the bias and variances of sensors also make sense for non-stochastic errors. Based on such an estimation of the bias and variance of each sensor, the bias estimate is subtracted from sensors readings and in the next phase of the proposed framework, we provide an initial estimate of the reputation vector calculated using the MLE as shown in Fig 4.

B. Bias Estimation

All sensors may have some errors in their readings. Such error is denoted as of sensor s and it is modeled by the Gaussian distribution random variable with bias bs and variance σ_s. Let rs denotes the true value of the sensor at time t. Sensor readings x_s^t can be written as

$$x_s^t = r_s + e_s^t$$

since there is no true value, the error value of sensor s is not to be found. But the difference values of such sensors are calculated with the equation given below. Let $\delta = \delta(i,j)$ be an estimator for mutual difference of sensor bias.

$$\delta(i,j) = \frac{1}{m}\sum_{i=0}^{m}(e_i^t - e_j^t) = \frac{1}{m}\sum_{t=1}^{m} e_i^t = \frac{1}{m}\sum_{t=1}^{m} e_j^t \quad (2)$$

Let $a_i = \frac{1}{m}\sum_{t=1}^{m} e_i^t$ be the sample mean of the random variable and m be the number of readings for each sensor. Then the expected value is calculated by minimizing the obtained value with respect to the mean value and the equation is given below

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

$$\delta(i,j)=a_i\text{-}a_j \approx b_i\text{-}b_j \qquad (3)$$

Where $\sigma_i^2 = v_i$ is the variance of sensor from the matrix $\beta = \{\beta(i,j)\}$

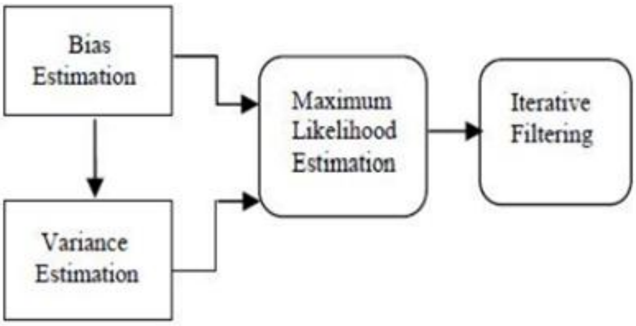


Fig.4.Data Aggregation Framework

D. Maximum Likelihood Estimation

The unbiasing sensor readings are extracted and take place with help of the bias estimated result which is calculated from the above section.After that the variance estimated result from equation 4 is considered and the extracted unbiasing sensor is used to make the maximum likelihood estimation with variance value By differentiating the likelihood function the true values are obtained and are measured in the form of weighted average. It is defined as

$$r = \sum_{s=1}^{n} w_s x_s \qquad (5)$$

Thus it estimates the reputation vector without any iteration. Hence the computational complexity of the estimation is less than the existing IF algorithms.

E. Iterative Filtering

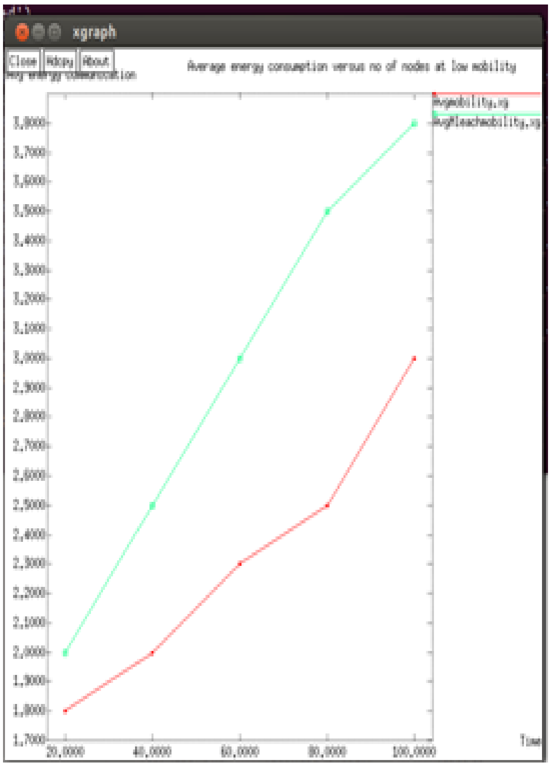
For the proposed collusion attack the results from the above is considered as an initial reputation for this filtering. It estimates the trustworthiness of each sensor based on the distance of sensors readings. From this process the estimation is made with an initial level itself.

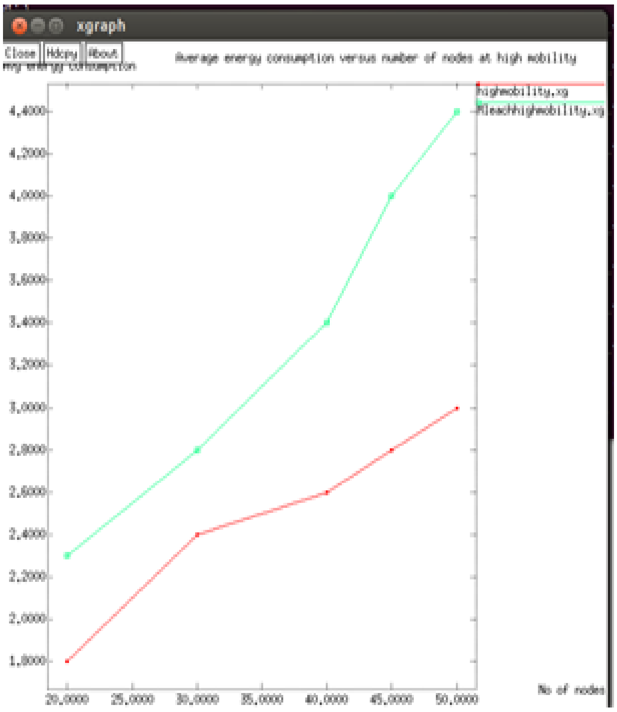
Using this initial reputation the efficiency of the IF algorithm is improved and reduces the required number of iterations.

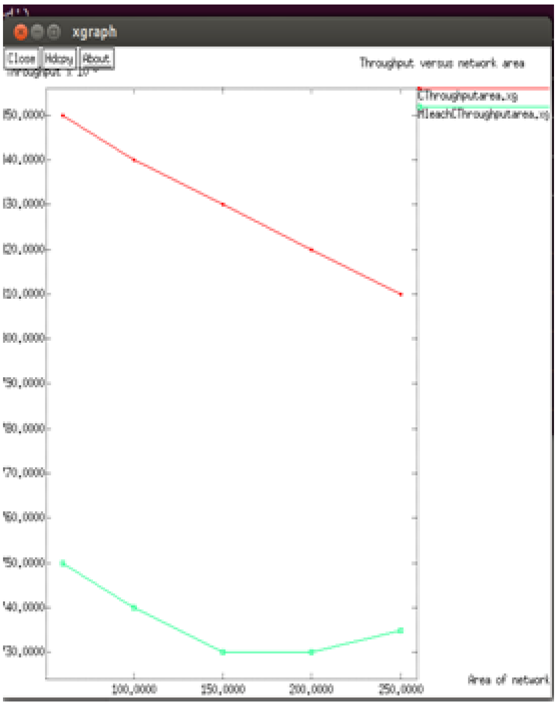
Results and Analysis:

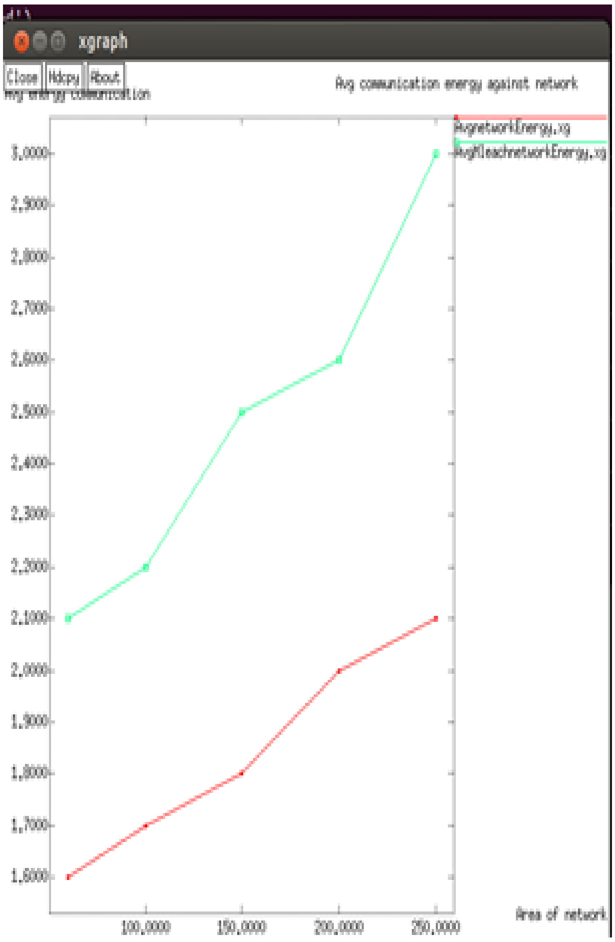
In our experiment, we consider a sensor network of 50 sensor nodes randomly deployed over a field of dimension 210 ×210 m2 area. The BS is located in the left side of the sensor field. The radio transmission range of the sensor nodes is 50 m. The sensor nodes move in random direction with a random value of speed in the range of 1–4 m/s. In our simulation, we compute the location of each of the nodes after a regular interval of 120 s.We run the simulation for a period of 1800 s. All nodes are assumed to have equal amount of initial energy. The initial energy in each sensor node is considered to be 10 J. It is considered that the sensor nodes use different power levels in order to transmit data packets across different physical distances.

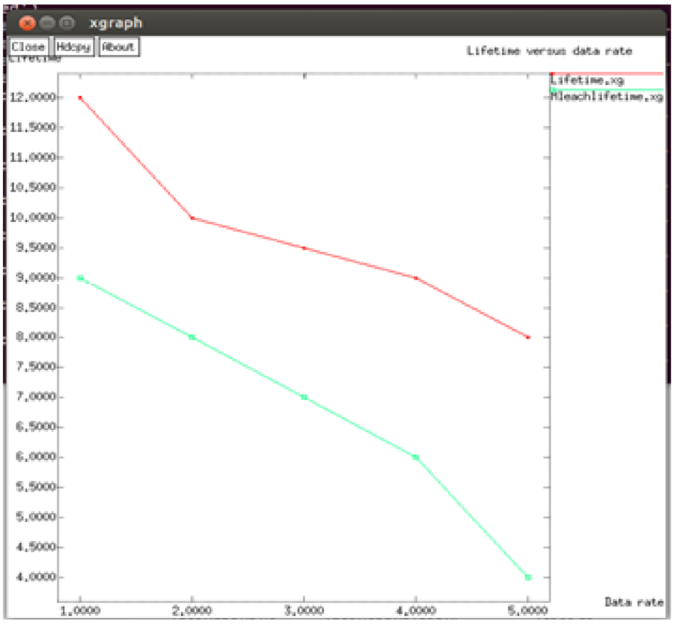
The sensor nodes are considered to be constant bit rate source. In one set of simulation, the nodes generate report only at a single rate such as 1 or 2 report/s. Each report consists of 64 B or 512 b. We assume a packet drop probability in the range of 0.0–0.2 at each intermediate hop.We measure the throughput after every 300 s and finally compute the average throughput after 1800 s of simulation.











CONCLUSION

In this paper, we have proposed an energy-efficient and reliable routing protocol for mobile WSNs. The proposed protocol is hierarchical and cluster based. Each cluster contains one CH node, and the CH node is assisted by two DCH nodes,which are also called cluster management nodes. We analyze the performance of the proposed protocol through simulations and compare with

M-LEACH. The proposed protocol outperforms M-LEACH in terms of lifetime and throughput. In the proposed protocol, the throughput improvement is 15% on average over M-LEACH. Such a routing protocol is useful when the sensor nodes and the BS are mobile.

And to estimate the trustworthiness of data aggregated iterative filtering algorithm is utilized Furthermore, this have a novel data collection technique from the sensor reading data in the presence of the collusion attack and it prevents from the sensor faults. The whole performance will be evaluated in terms of time consumption. It makes the IF algorithms not only collusion robust but also gives more accurate and faster.

REFERENCES

[1] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, “Highly-resilient, energy-efficient multipath routing in wireless sensor networks,” ACM SIGMOBILE Mobile Comput. Commun. Rev., vol. 5, no. 4, pp. 10–24, Oct. 2001.

[2] V.Raghunathan, C.Schurgers, S. Park, and M. Srivastava, “Energy-aware wireless microsensor networks,” IEEE Signal Process. Mag., vol. 19, no. 2, pp. 40–50, Mar. 2002.

[3] W. Ye, J. Heidemann, and D. Estrin, “An energy-efficient MAC protocol for wireless sensor networks,” in Proc. IEEE INFOCOM, 2002, pp. 1527–1576.

[4] E. Felemban, C.-G. Lee, and E. Ekici, “MMSPEED: Multipath multispeed protocol for QOS guarantee of reliability and timeliness in wireless sensor networks,” IEEE Trans. Mobile Computing., vol. 5, no. 6, pp. 738–754, Jun. 2006

[5] P. J. M. Havinga and G. J. M. Smit, “Design techniques for low power systems,” J. Syst. Archit., vol. 46, no. 1, pp. 1–21, Jan. 2000.

[6] D. P. Agrawal and Q. A. Zeng, Wireless and Mobile Systems. Bangalore, India: Thomson India Edition, 2007

[7] K. Akayya and M. Younis, “An energy-aware QoS routing protocol for wireless sensor networks,” in Proc. 23rd Int. Conf. Distributed.Computing. Syst. Workshops, 2003, pp. 710–715.

[8] D. B. Johnson, and D. A. Maltz, “Dynamic source routing in ad hoc wirelessnetworks,”inMobileComputing. Norwell,MA,USA:Kluwer Publishers, 1996, pp. 153–181.

[9] C. Perkins and E. Royer, “Ad hoc on demand distance vector routing,” in Proc. 2nd IEEE Workshop Mobile Comput. Syst. Appl., 1999, pp. 90–100.

[10] C. E. Perkins and P. Bhagwat, “Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers,” in Proc. Conf. Commun. Archit. ,Protocols Appl., 1994, pp. P234–P244.

[11] C. Siva Ram Murthy and B. S. Manoj, Ad hoc Wireless Networks: Architectures and Protocols, 1st ed. Delhi, India: Prentice-Hall, 2004.

[12] C. Lu, B. M. Blum, T. F. Abdelzaher, J. A. Stankovic, and T. He, “RAP: A real-time communication architecture for large-scale wireless sensor networks,” in Proc. IEEE RTAS, pp. 55–60, 2002.

[13] W.Heinzelman, A.Chandrakasan, andH.Balakrishnan, “Energy-efficient communication protocol for wireless microsensor networks,” in Proc. 33rdAnnu. HICSS, 2000, pp. 1–10.

[14] S. Lindsey and C. S. Raghavendra, “PEGASIS: Power-efficient gathering in sensor information systems,” in Proc. IEEE Aerosp. Conf., 2002, pp. 1125–1130.

[15] W.Heinzelman, A.Chandrakasan, andH.Balakrishnan, “Energy-efficient communication protocol for wireless microsensor networks,” in Proc. 33rd Annu. HICSS, 2000, pp. 1–10.

[16] A. Manjeshwar and D. P. Agarwal, "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks," in Proc. 15th IPDPS Workshops, 2000, pp. 2009–2015.

[17] A. Manjeshwar and D. P. Agarwal, "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," in Proc. IPDPS, 2002.

[18] O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," IEEE Trans. Mobile Comput., vol. 3, no. 4, pp. 366–379, Oct.–Dec. 2004.

[19] M. Handique, P. Rai, S. R. Biradar, and H. K. D. Sarma "Energy efficient hierarchical cluster based communication protocol for wireless sensor networks with base station mobility," in Proc. IEEE CODEC, Kolkata, India, pp. 214–221, 2006.

[20] S.Mao,andY.ThomasHou"BeamStar:An Edge-Based Approach to Routing in Wireless Sensor Networks," IEEE Trans. Mobile Comput., vol. 6, no. 11, pp. 1284–1296, Nov. 2007

[21] M. Ye , C . Li , F . Chen , and G . J . Wu, "EECS:Anenergyefficient clustering scheme in wireless sensor networks," Int. J. Ad Hoc Sens. Netw., vol. 3, no. 2/3, pp. 99–119, 2007.

[22] M. Liu, J. Cao, G. Chen, and X. Wang, "An energy-aware routing in wireless sensor networks," Sensors, vol. 9, pp. 445–462, 2009.

[23] M. S. Al Fares, Z. Sun, and H. Cruickshank, "A hierarchical routing protocol for survivability in wireless sensor network (WSN)," in Proc. IMECS, 2009, vol. 1, pp. 1–7.

[24] P. Ji, C. Wu, Y. Zhang, and Z. Jia, "DAST: A QoS-aware routing protocol for wireless sensor networks," in Proc. ICESS, 2008, pp. 259–264.

[25] Y.-H. Zhu, W.-D.Wu, J. Pan, and Y.-P.Tang, "An energy-efficient data gathering algorithm to prolong lifetime of wireless sensor networks," Comput.Commun., vol. 33, no. 5, pp. 639–647, Mar. 2010.

[26] F. Ren, J. Zhang, T. He, C. Lin, and S. K. Das, "EBRP: Energybalanced routing protocol for data gathering inwireless sensor networks," IEEE Tran. Parallel Distrib. Syst., vol. 22, no. 12, pp. 2108–2125, Dec. 2011.

[27] L. Tien Nguyen, X. Defago, R. Beuran, and Y. Shinoda, "An energy efficient routing scheme for mobile wireless sensor networks," in Proc. IEEE ISWCS, 2008, pp. 568–572.

[28] S. A. B. Awwad, C. K. Ng, N. K. Noordin, and M. F. A. Rashid, "Cluster based routing protocol for mobile nodes in wireless sensor network," in Proc. Int. Symp. CTS, May 18–22, 2009, pp. 233–241.