

Energy Efficient Routing Protocol for Sensing Data

Md. Abdul Mukib
Lecturer
Department of CSE
Hamdard University
Bangladesh

Md. Shahidul Islam
Lecturer
Department of CSE
Hamdard University
Bangladesh

Md. Solaiman Mia
Lecturer
Department of CSE
Hamdard University
Bangladesh

ABSTRACT

In the near future, wireless sensor networks are expected to find wide applicability and increasing deployment. In this paper, a formal classification of sensor networks based on their mode of functioning: such as proactive and reactive networks is proposed. Reactive networks respond immediately to the changes in the relevant parameters of interest, while proactive networks collect passive data in a periodic way. A new energy efficient routing protocol named TSEESNP (Threshold Sensitive Energy Efficient Sensor Network Protocol) for reactive networks is introduced in this paper. The performance is well evaluated using the TSEESNP routing protocol for a simple temperature sensing application. In terms of energy efficiency, this protocol has been observed to outperform existing conventional sensor network protocols.

General Terms

Wireless sensor network routing protocol for such situation when time is short and need urgently data to be sensed and energy loss need to be optimized. This is a reactive approach which is compared with some proactive approaches.

Keywords

Reactive, Directed Diffusion, Report Time, Time Frame, Hard Threshold, Soft Threshold etc.

1. INTRODUCTION

In recent days, the use of wired sensor networks is being advocated for all the application areas where sensor network is used. Some examples include distribution of thousands of sensors and wires over strategic locations in a structure such as an airplane, so that conditions can be constantly monitored both from the inside and the outside and a real-time warning can be issued when the monitored structure is about to fail.

Normally sensor networks are unattended and must be fault-tolerant so that the need for maintenance is optimized. Especially this is much more desirable in those applications where the sensor nodes may be embedded in the structure or are in inhospitable terrain and are inaccessible for any service.

The advancement in technology has made it possible to have extremely small, low powered devices equipped with programmable computing, multiple parameters sensing and wireless communication capability. The main feature of sensor network is the low cost of sensors makes it easy to have a network of hundreds or thousands of these wireless sensors, thereby enhancing the reliability and accuracy of data and the area coverage as well. Also, it is necessary that the sensors be easy to deploy (i.e., require no installation cost etc). Protocols for these networks must be designed in such a way that the limited power in the sensor nodes is efficiently used. Environments in which these nodes operate and respond are very dynamic, with fast changing physical parameters.

Some of the parameters which might change dynamically depending on the application are:

- Power availability.
- Location (if the nodes are mobile).
- Target reaching ability.
- Type of task (i.e. attributes the nodes need to operate on)

So, the routing protocol should be fault-tolerant in such a dynamic environment. The traditional routing protocols defined for wireless ad hoc networks [1], [9] are not well organized due to the following reasons:

1. Sensor networks are “data centric” i.e., unlike traditional networks where data is requested from a specific node, requested data is based on certain attributes such as, which area has temperature > 70°F?
2. The requirements of the network change with the application and so, it is application-specific [3]. For example, in some applications the sensor nodes are fixed like a static device, while others need data based only on one attribute (i.e., attribute is fixed in this network).
3. Adjacent nodes may have similar data. So, rather than sending data separately from each node to the requesting node, it is desirable to aggregate similar data together and make a combination and send it.
4. In traditional wired and wireless networks, each node is given a unique node id, used for routing. This cannot be effectively used in sensor networks. This is because, these networks being data centric, routing to and from specific nodes is not required. Also, the huge number of nodes in the network implies huge number of ids [2], which might be substantially larger than the actual data being transmitted.

Thus, sensor networks need protocols which are application specific, data centric, capable of aggregating data and optimizing energy consumption. An ideal sensor network should have the following additional features:

Attribute dependent addressing is typically employed in sensor networks. The attribute dependent addresses are composed of a series of attribute-value pairs which specify certain physical parameters to be sensed. For example, an attribute address may be (temperature > 120°F, location =?). So, all nodes which sense a temperature greater than 120°F should respond with their location.

Location awareness is another important issue. Since most data collection is based on location, it is desirable that the nodes must know their own position whenever needed.

2. RELATED WORKS

In this section, we provide a brief overview of some related research work.

A hierarchical clustering method with emphasis on localized behavior and the need for asymmetric communication and energy conservation in sensor networks is discussed by Estrin [3].

Intanagonwiwat have introduced *directed diffusion* [7], a data dissemination paradigm for sensor networks. It is a data-centric paradigm and its application to query dissemination and processing has been demonstrated in this work.

Heinzelman introduce a hierarchical clustering algorithm for sensor networks, called LEACH (Low-Energy Adaptive Clustering Hierarchy) [5]. We discuss this in greater detail in later part of this paper.

A Cluster Based Routing Protocol (CBRP) has been proposed by Jiang et al. in [8] for mobile ad-hoc networks. It divides the network nodes into a number of overlapping or disjoint two-hop-diameter clusters in a distributed manner. However, this protocol is not suitable for energy constrained sensor networks in this form.

3. MOTIVATION

In the current body of research done in the area of wireless sensor networks, it is seen that particular attention has not been given to the time criticality of the target applications. There are two major types of networks like Proactive and Reactive networks. As in Proactive networks most current protocols assume a sensor network collecting data periodically from its environment or responding to a particular query. We feel that there exists a need for networks geared towards responding immediately to changes in the sensed attributes. For this reason, this paper focused on Reactive network protocols. One thing must agree that sensor networks should provide the end user with the ability to control the trade-off between energy efficiency, accuracy and response times dynamically. So, in this research, we have focused on developing a communication protocol which can fulfill these requirements. The main focus is to develop such a protocol which can respond immediately and can provide data to end user as early as possible.

4. CLASSIFICATION OF SENSOR NETWORKS

In this section, a simple classification of sensor networks on the basis of their mode of functioning and the type of target application is presented.

4.1 Proactive Networks

The nodes in this network periodically switch on their sensors and transmitters, sense the environment and transmit the data of interest. Thus, they provide a snapshot of the relevant parameters at regular intervals. They are well suited for applications requiring periodic data monitoring. Fig.2 explains the timeline uses in an ideal proactive routing protocol. Their main advantage is their periodic switch of sensing data. It helps some power consumption of sensor nodes and make energy efficient network.

4.2 Reactive Networks

In this method the nodes react immediately to dynamic changes in the value of a sensed attribute. As such, they are well suited for time critical applications. This type of

networks especially uses when the energy efficiency is not a big deal and some urgent data needs to be sensed.

5. SENSOR NETWORK MODEL

Consider a model which is well suited for these sensor networks. It is based on the model developed by Heinzelman [5]. It consists of a Base Station (BS), away from the nodes, through which the end user can access data from the sensor network. All the nodes in the network are homogeneous and begin with the same initial energy level. The BS however has a constant power supply and so, has no energy problem. It can transmit with high power to all the nodes. Thus, there is no need for routing from the BS to any specific node. However, the nodes cannot always reply to the BS directly due to their power constraints, resulting in asymmetric communication. This model uses a hierarchical clustering scheme. Consider the partial network structure shown in Fig.1; each cluster has a cluster head which collects data from its cluster members, aggregates it and sends it to the BS or an upper level cluster head. For example, nodes 4.1.1, 4.1.2, 4.1.3, 4.1.4, and 4.1 form a cluster with node 4.1 as the cluster head. Similarly, there exist other cluster heads such as 4.2, 1, 3 etc. These cluster-heads, in turn, form a cluster with node 1 as their cluster-head. So, node 1 becomes a second level cluster head too. This system is repeated to form a hierarchy of clusters with the uppermost level cluster nodes reporting directly to the BS. The BS forms the root of this hierarchy and supervises the entire network. The clusters heads must need to collect data from its cluster nodes and forward to the BS. The BS aggregates all the data received from all the cluster heads and then provide a full data which is sensed to the end user.

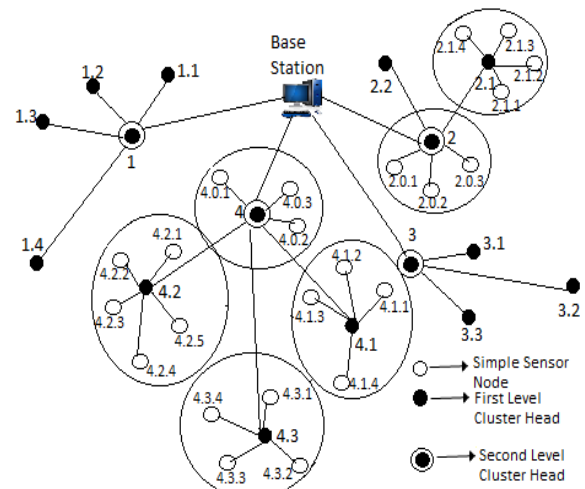


Fig.1: Hierarchical Clustering

The main features of such architecture are:

- All the nodes need to transmit data only to their immediate cluster-head, thus saving energy.
- Only the cluster head is responsible to perform additional computations on the data. So, energy is again conserved.
- Cluster-heads at increasing levels in the hierarchy need to transmit data over correspondingly larger distances. Combined with the extra computations they perform; they end up consuming energy faster than the other nodes. For evenly distribute this consumption, all the nodes take turns to be the cluster head for a time interval T , called the cluster turning period.

6. SENSOR NETWORK PROTOCOLS

The sensor network model described in Section 5 is used extensively in the following discussion of sensor network protocols.

6.1 Proactive Network Protocol

This sub section is discussed the functionality and the behavior expected in a protocol for proactive networks uses in wireless sensor network.

At each cluster change time, once the cluster-heads are decided, the cluster-head broadcasts the following parameters:

Report Time (T_R): This is the time period between every successive report sent by a sensor node.

Attribute (A): This is a set of physical parameters which the user is interested in obtaining data about.

At each report time, the cluster members sense the parameters specified in the attributes and send the data to the cluster-head. The cluster-head aggregates this data and sends it to the *BS* or the higher level cluster-head. This ensures that the user has a complete view of the entire area covered by the network.

Important Features

The important features of this scheme are mentioned below:

1. Since the nodes switch off their sensors and transmitters at all times except the report times, the energy of the network is saved.
2. At every cluster changing time, T_R and A are transmitted a fresh data and so, can be changed. Thus, the user can decide what parameters need to sense and how often to sense them by changing A and T_R respectively.

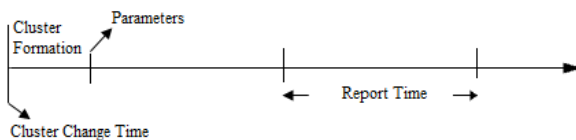


Fig.2: Time Line for Proactive protocol

This method has an important drawback. Because of the periodicity with which the data is sensed, it is possible that time critical data may reach the user only after the report time. Thus, this method may not be very suitable for data sensing applications when time is short.

LEACH

LEACH (Low-Energy Adaptive Clustering Hierarchy) is a family of protocols developed by Heinzelman and his team in [5]. LEACH is a good approximation of a proactive network protocol, with some minor differences. The cluster heads broadcast a TDMA (Time-Division Multiple Access) schedule giving the order in which the cluster members can transmit their data when the clusters are formed. The total time required to complete this schedule is called the frame time T_F . Every node in the cluster has its own slot in the frame, during which it transmits data to the cluster head. When the last node in the schedule has transmitted its data, the schedule repeats.

The *frame time* (T_F) in LEACH is equivalent to the *report time* (T_R) discussed earlier. The *frame time* (T_F) is not broadcast by the cluster head, though it is derived from the TDMA schedule.

However, it is not under user control. Also, the attributes are predetermined and are not changed midway.

Example Applications

This network can be used to monitor machinery for fault detection and diagnosis. It can also be used to collect data about temperature change patterns over a particular area.

6.2 Proposed Reactive Network Protocol: (TSEESNP)

In this section, a new network protocol called TSEESNP (*Threshold Sensitive Energy Efficient Sensor Network Protocol*) is presented. It is targeted at reactive networks and is one of the protocols developed for reactive networks.

In this scheme, the cluster-head broadcasts to its members at every cluster change time, in addition to the attributes are:

Soft Threshold (ST): This is a small change in the value of the sensed attribute which triggers the node to switch on its transmitter and transmit.

Hard Threshold (HT): This is a threshold value for the sensed attributes. It is the absolute value of the attribute beyond which the node sensing this value must switch on its transmitter and report to its cluster head.

Continuously the nodes sense their environment. The first time a parameter from the attribute set reaches its hard threshold value, the node switches on its transmitter and sends the sensed data. The sensed value is stored in an internal variable in the node, called the *Sensed Value* (SV). The nodes will next transmit data in the current cluster period, only when both the following conditions are true:

1. The current value of the sensed attribute is greater than the hard threshold.
2. The current value of the sensed attribute differs from SV by an amount equal to or greater than the soft threshold.

Whenever a node transmits data, SV is set equal to the current value of the sensed attribute. Thus, the hard threshold tries to reduce the number of transmissions by allowing the nodes to transmit only when the sensed attribute is in the range of interest.

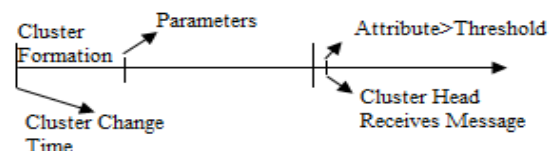


Fig.3: Time line for TSEESNP

The soft threshold further reduces the number of transmissions by eliminating all the transmissions which might have otherwise occurred when there is little or no change in the sensed attribute once the hard threshold. Fig.3 shows an ideal timeline used in this proposed protocol.

Important Features

The main features of this scheme are as follows:

1. Time critical data reaches the user almost instantaneously. So, this method is eminently suited for time critical data sensing applications.
2. The soft threshold can be varied, depending on the criticality of the sensed attribute and the target application.
3. Message transmission consumes much more energy than data sensing. So, even though the nodes sense repeatedly, the energy consumption in this scheme can potentially be much less than in the proactive network because data transmission is done less frequently.

4. A smaller value of the soft threshold gives a more accurate picture of the network, at the expense of increased energy consumption. Thus, the user can control the trade-off between energy efficiency and accuracy.
5. At every cluster change time, the attributes broadcast a fresh data and so, the user can change them as required.

The main drawback of this method is that, if the thresholds are not reached, the nodes will never communicate; the user will not get any data from the network at all and will not come to know even if all the nodes die. Thus, this method is not well suited for applications where the user needs to get data on a regular basis. Another possible problem with this scheme is that a practical implementation would have to ensure that there are no collisions in between clusters. TDMA scheduling of the nodes can be used to avoid this problem. This will however introduce a delay in the reporting of the time-critical data. CDMA (Code Division Multiple Access) is another possible solution to this problem.

Example Applications

This protocol is best suited for time critical applications such as intrusion detection, explosion detection etc.

7. PERFORMANCE EVALUATION

This work is done by using the ns-2 simulator [10] with the LEACH extension [4], based on the simulation results and is prepared the charts to show the comparisons.

7.1 Simulation

The goals in conducting the simulation are as follows:

- Compare the performance of the TSEESNP and LEACH protocols on the basis of energy dissipation and the longevity of the network.
- Study the effect of the soft threshold **ST** and Hard threshold **HT** on TSEESNP.

The simulation has been performed on a network of 100 nodes and a fixed base station. The nodes are placed randomly in the network. All the nodes start with an initial energy of 2J (Joule). Cluster formation is done as in the LEACH protocol [5-6]. However, their radio model is modified to include idle time power dissipation (set equal to the radio electronics energy) and sensing power dissipation (set equal to 10% of the radio electronics energy). The idle time power is the same for all the networks and hence does not affect the performance comparison of the protocols.

Simulated Environment

For these experiments, this work simulated an environment with varying temperature in different regions. 150 sensor network nodes are first placed randomly in a bounding area of square 100×100 units. The actual area covered by the network is then divided into four quadrants. Then each quadrant assigned a random temperature between 0°F and 200°F every 5 seconds during the simulations. It is observed that most of the clusters have been well distributed over the four quadrants.

Experiments

Two metrics to analyze and compare the performance of the protocols are used in this experiment. They are average energy dissipated and total number of nodes alive. These are explained below:

Average energy dissipated

This metric shows the average dissipation of energy per node over time in the network as it performs various functions such as transmitting, receiving, sensing, aggregation of data etc.

Total number of nodes alive

This metric indicates the overall lifetime of the network. More importantly, it gives an idea of the area coverage of the network over time.

Now, various parameters used in the implementation of these protocols are considered. A common parameter for both the protocols is the attribute to be sensed, which is the temperature. The performance of TSEESNP is studied in two modes, one with only the hard threshold (*hard mode*) and the other with both the hard threshold and the soft threshold (*soft mode*). The hard threshold is set at the average value of the lowest and the highest possible temperatures, 100°F. The soft threshold is set at 2°F for these experiments.

7.2 Results

The simulation is executed 5 times of run of the simulator for each protocol and for each mode of TSEESNP. The readings from these 5 trials were then averaged and plotted.

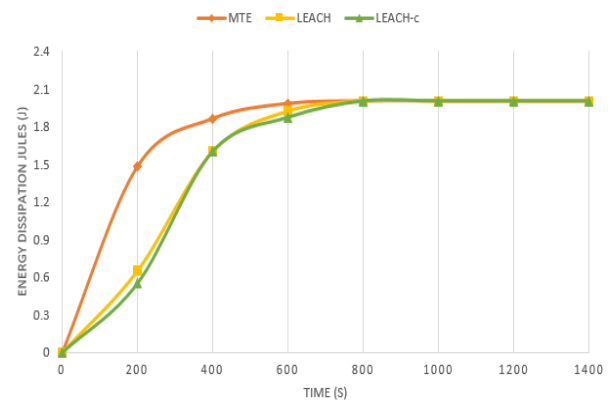


Fig.4: Energy Dissipation of LEACH protocol

A lower value of the energy dissipation metric and a higher number of nodes alive at any given time indicates a more efficient protocol. Fig.4 and Fig.5 show the behavior of the network in proactive mode. Here we can see the comparison of LEACH, LEACH-c (a variant of LEACH) and MTE protocol based on the energy dissipation and number of nodes alive after time. This comparison was originally done in LEACH [6]. It is repeated here taking into account then modified radio energy model of the four protocols [6], MTE (minimum transmission energy) lasts for the longest time. However, the observation from Fig.5 shows that only one or two nodes are really alive. As such, LEACH and LEACH-c can be considered the most efficient protocols, in terms of both energy dissipation and longevity.

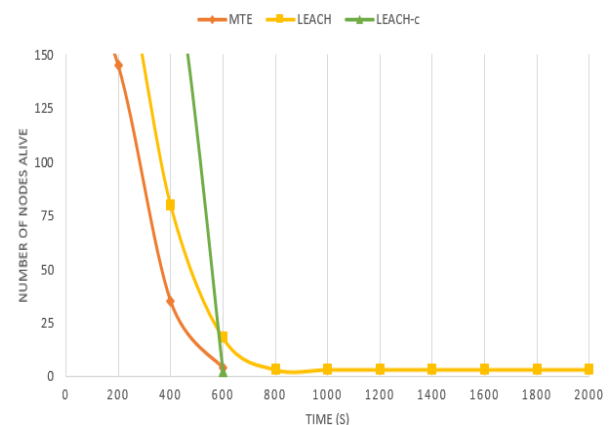


Fig.5: Number of nodes alive in LEACH protocol

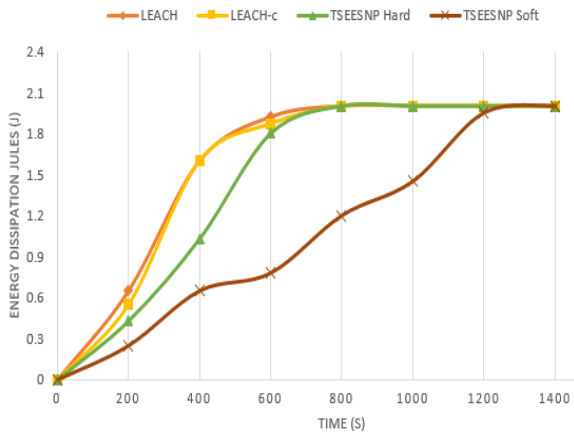


Fig.6: Comparison of average energy dissipation with LEACH and LEACH-c

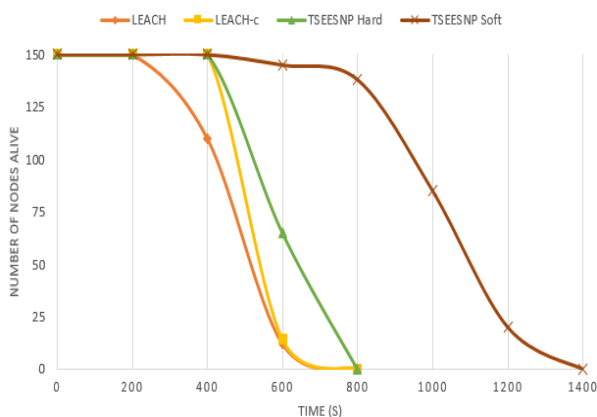


Fig.7: Comparison of number of nodes alive

But while comparing LEACH and LEACH-c with TSEESNP in both Hard and Soft threshold, as expected *soft mode* TSEESNP performs much better than LEACH, LEACH-c and hard mode TSEESNP because of the presence of the soft threshold. Though both soft and hard threshold of TSEESNP method provides better results than the proactive methods, but among them, the TSEESNP soft threshold methods provides better results.

8. CONCLUSION

A formal classification of sensor networks is presented in this paper. A new network protocol, TSEESNP for reactive networks is introduced. TSEESNP is well suited for time critical applications and is also quite efficient in terms of energy consumption and response time. It also allows the user to control the energy consumption and accuracy to suit the

application. As this protocols helps to get immediate data with optimized energy dissipation and less number of dead nodes. But, as the energy of sensor node is very low, the energy dissipation may be optimized a little and then it may be possible to keep alive more number of nodes which are died for losing more energy.

9. REFERENCES

- [1] Broch, J., Maltz, D., Johnson, D., Hu, Y., and Jetcheva, J. 1998. A Performance Comparison of Multi-Hop Wireless AdHoc Network Routing Protocols. In Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM), ACM.
- [2] Elson, J., and Estrin, D. 2000, An Address-Free Architecture for Dynamic Sensor Networks. Technical Report 00-724, Computer Science Department, USC.
- [3] Estrin, D., Govindan, R., Heidemann, J., and Kumar, S. 1999. Next Century Challenges: Scalable Coordination in Wireless Networks. In Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM), pages 263–270.
- [4] Heinzelman, W., Chandrakasan, A., and Balakrishnan, H. uAMPS ns Code Extensions. <http://www.mtl.mit.edu/research/icystems/uamps/leach>.
- [5] Heinzelman, W., Chandrakasan, A., and Balakrishnan, H. 2000. Energy-Efficient Communication Protocols for Wireless Microsensor Networks. In Proceedings of Hawaiian International Conference on Systems Science.
- [6] Heinzelman, W. B. 2000. Application-Specific Protocol Architectures for Wireless Networks. PhD thesis, Massachusetts Institute of Technology.
- [7] Intanagonwiwat, C., Govindan, R., and Estrin, D. 2000. Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks. In Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM), pages 56–67.
- [8] Jiang, M., Li, J., and Tay, Y. C. 1999. Cluster Based Routing Protocol. Internet Draft.
- [9] Royer, E. M., and Toh, C. K. 1999. A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks. In IEEE Personal Communications Magazine, pages 46–55.
- [10] UCB/LBNL/VINT. Network Simulator-ns. <http://wwwmash.cs.berkeley.edu/ns>