# TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks*

Arati Manjeshwar and Dharma P. Agrawal
Center for Distributed and Mobile Computing, ECECS Department,
University of Cincinnati, Cincinnati, OH 45221-0030

## Abstract

*Wireless sensor networks are expected to find wide applicability and increasing deployment in the near future. In this paper, we propose a formal classification of sensor networks, based on their mode of functioning, as* proactive *and* reactive *networks. Reactive networks, as opposed to passive data collecting proactive networks, respond immediately to changes in the relevant parameters of interest. We also introduce a new energy efficient protocol, TEEN (***T***hreshold sensitive* **E***nergy* **E***fficient sensor* **N***etwork protocol) for reactive networks. We evaluate the performance of our protocol for a simple temperature sensing application. In terms of energy efficiency, our protocol has been observed to outperform existing conventional sensor network protocols.*

## 1. Introduction

In recent years, the use of wired sensor networks is being advocated for a number of applications. 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.

Sensor networks are usually unattended and need to be fault-tolerant so that the need for maintenance is minimized. This is especially desirable in those applications where the sensors 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 parameter sensing and wireless communication capability. Also, the low cost of sensors makes it possible 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. In addition, environments in which these nodes operate and respond are very dynamic, with fast changing physical parameters. The following are some of the parameters which might change dynamically depending on the application:

- Power availability.
- Position (if the nodes are mobile).
- Reachability.
- 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 suited due to the following reasons:

1. Sensor networks are "data centric" i.e., unlike traditional networks where data is requested from a specific node, data is requested based on certain attributes such as, which area has temperature $> 50°F$?
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 and not mobile, 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 and send it.
4. In traditional wired and wireless networks, each node is given a unique 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 large number of nodes in the network implies large ids [2], which might be substantially larger than the actual data being transmitted.

*This work is supported by the Ohio Board of Regents' Doctoral Enhancement Funds

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 based addressing* is typically employed in sensor networks. The attribute based 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 $> 100°F$, location = ??). So, all nodes which sense a temperature greater than $100°F$ 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 know their position whenever needed.

## 2. Related Work

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

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

Estrin et. al [3] discuss a hierarchical clustering method with emphasis on localized behavior and the need for asymmetric communication and energy conservation in sensor networks.

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.

Heinzelman et. al [5] introduce a hierarchical clustering algorithm for sensor networks, called *LEACH*. We discuss this in greater detail in section 6.1.

## 3. Motivation

In the current body of research done in the area of wireless sensor networks, we see that particular attention has not been given to the time criticality of the target applications. 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. We also believe 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 our research, we have focussed on developing a communication protocol which can fulfill these requirements.

## 4. Classification of Sensor Networks

Here, we present a simple classification of sensor networks on the basis of their mode of functioning and the type of target application.

### 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.

### Reactive Networks

In this scheme the nodes react immediately to sudden and drastic changes in the value of a sensed attribute. As such, they are well suited for time critical applications.

## 5. Sensor Network Model

We now consider a model which is well suited for these sensor networks. It is based on the model developed by Heinzelman et. al. in [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. The *BS* however has a constant power supply and so, has no energy constraints. 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 1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5 and 1.1 form a cluster with node 1.1 as the cluster head. Similarly there exist other cluster heads such as 1.2, 1 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 pattern 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 main features of such an architecture are:

- All the nodes need to transmit only to their immediate cluster-head, thus saving energy.
- Only the cluster head needs to perform additional computations on the data. So, energy is again conserved.

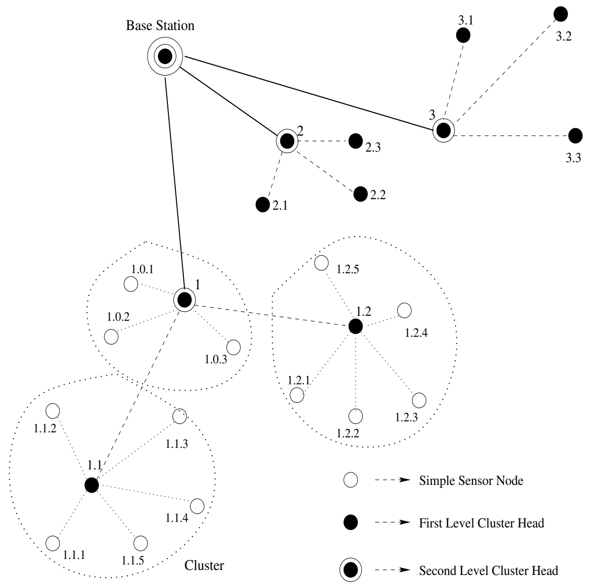


**Figure 1.** *Hierarchical Clustering*

- 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. In order to evenly distribute this consumption, all the nodes take turns becoming the cluster head for a time interval *T*, called the cluster 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

In this section, we discuss the functionality and the characteristics expected in a protocol for proactive networks.

#### Functioning

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 successive reports sent by a node.

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

At every 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 base station or the higher level cluster-head, as the case may be. This ensures that the user has a complete picture of the entire area covered by the network.

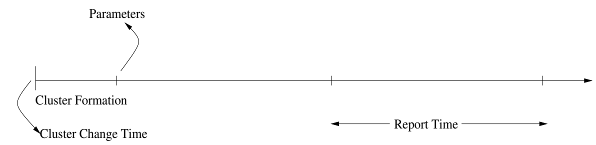


**Figure 2.** *Time line for proactive protocol*

#### 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 conserved.

2. At every cluster change time, $T_R$ and *A* are transmitted afresh and so, can be changed. Thus, the user can decide what parameters to sense and how often to sense them by changing *A* and $T_R$ respectively.

This scheme, however, 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 scheme may not be very suitable for time-critical data sensing applications.

#### LEACH

LEACH (Low-Energy Adaptive Clustering Hierarchy) is a family of protocols developed in [5]. LEACH is a good approximation of a proactive network protocol, with some minor differences.

Once the clusters are formed, the cluster heads broadcast a TDMA schedule giving the order in which the cluster members can transmit their data. 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 *report time* discussed earlier is equivalent to the *frame time* in LEACH. The *frame time* 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. Reactive Network Protocol: TEEN

In this section, we present a new network protocol called TEEN *(**T**hreshold sensitive* **E***nergy* **E***fficient sensor* **N***etwork protocol)*. It is targeted at reactive networks and is the first protocol developed for reactive networks, to our knowledge.

### Functioning

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

***Hard Threshold ($H_T$)*:** This is a threshold value for the sensed attribute. 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.

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

The nodes sense their environment continuously. 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. 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.

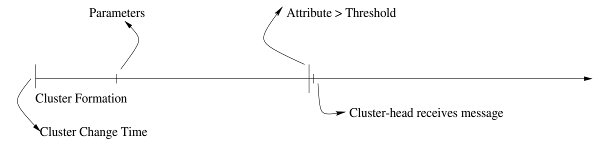


**Figure 3.** *Time Line for TEEN*

### Important Features

The main features of this scheme are as follows:

1. Time critical data reaches the user almost instantaneously. So, this scheme is eminently suited for time-critical data sensing applications.

2. Message transmission consumes much more energy than data sensing. So, even though the nodes sense continuously, the energy consumption in this scheme can potentially be much less than in the proactive network, because data transmission is done less frequently.

3. The soft threshold can be varied, depending on the criticality of the sensed attribute and the target application.

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 are broadcast afresh and so, the user can change them as required.

The main drawback of this scheme 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 scheme 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 the cluster. 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 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

### 7.1. Simulation

To evaluate the performance of our protocol, we have implemented it on the ns-2 simulator [10] with the *LEACH* extension [4]. Our goals in conducting the simulation are as follows:

- Compare the performance of the TEEN and LEACH protocols on the basis of energy dissipation and the longevity of the network.
- Study the effect of the soft threshold $S_T$ on TEEN.

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. 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 our experiments, we simulated an environment with varying temperature in different regions. The sensor network nodes are first placed randomly in a bounding area of 100x100 units. The actual area covered by the network is then divided into four quadrants. Each quadrant is later 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

We use two metrics to analyze and compare the performance of the protocols. They are:

**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.

We now look at the various parameters used in the implementation of these protocols. A common parameter for both the protocols is the attribute to be sensed, which is the temperature.

The performance of TEEN 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 our experiments.

### 7.2. Results

We executed 5 runs of the simulator for each protocol and for each mode of TEEN. The readings from these 5 trials were then averaged and plotted. A lower value of the energy-dissipation metric and a higher number of nodes alive at any given time indicates a more efficient protocol.

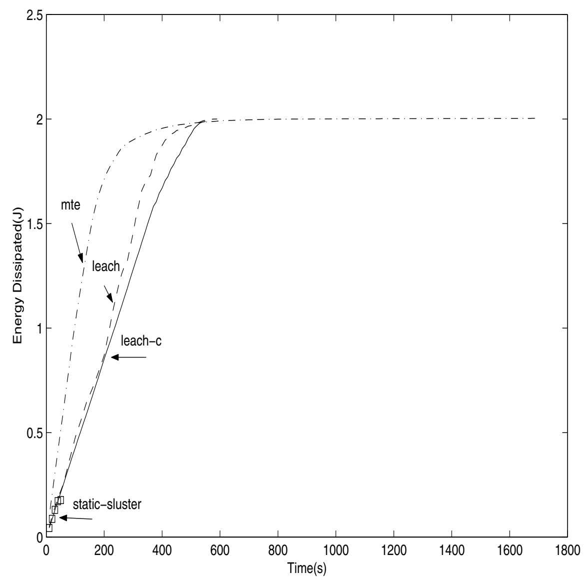


**Figure 4.** *Energy dissipation: LEACH*

Figures 4 and 5 show the behavior of the network in proactive mode. This comparison was originally done in LEACH [6]. It is repeated here taking into account the modified radio energy model. Of the four protocols [6], *mte (minimum transmission energy)* lasts for the longest time. However, we observe from Fig. 5 that only one or two nodes are really alive. As such, *leach* and *leach-c* (a variant of *leach*) can be considered the most efficient protocols, in terms of both energy dissipation and longevity.

In Figures 6 and 7, we compare the two protocols. We see that both modes of TEEN perform much better than *leach*. If the cluster formation is based on the *leach-c* protocol, the performance of the TEEN protocol is expected to be correspondingly better.

As expected, *soft mode* TEEN performs much better than

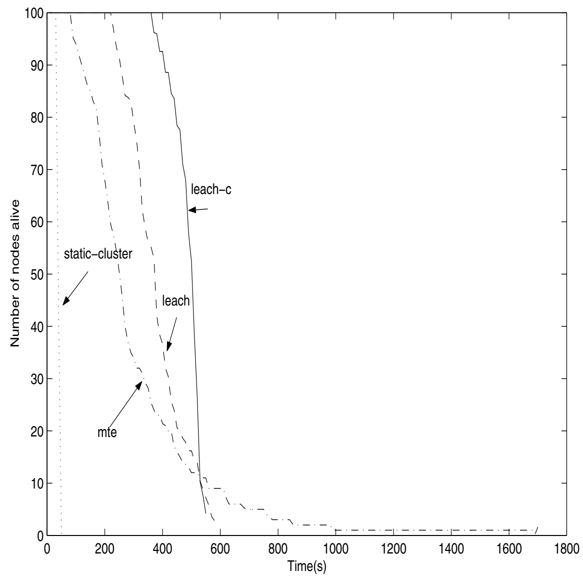


**Figure 5.** *No. of nodes alive: LEACH*

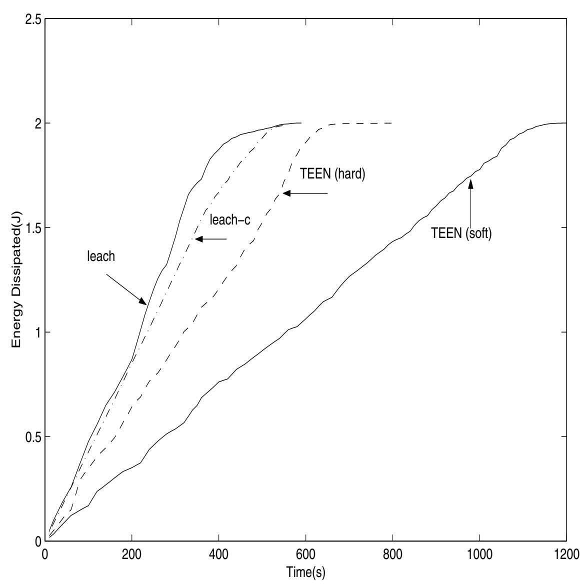


**Figure 6.** *Comparison of average energy dissipation*

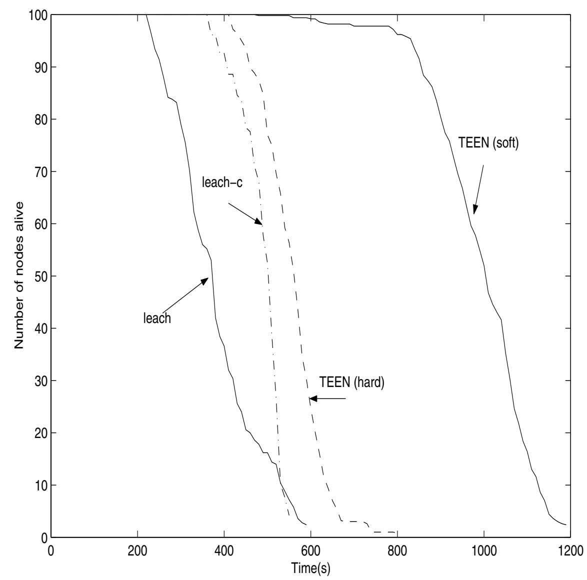


**Figure 7.** *Comparison of the no. of nodes alive*

*hard mode* TEEN because of the presence of the soft threshold.

## 8. Conclusions

In this paper, we present a formal classification of sensor networks. We also introduce a new network protocol, *TEEN* for reactive networks. TEEN 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.

## Acknowledgment

We would like to thank Wendi Heinzelman for her valuable suggestions and for letting us use her *LEACH* extension to the *ns* simulator for our experiments.

## References

[1] J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva. "A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols". In *Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking(MOBICOM), ACM*, October 1998.

[2] J. Elson and D. Estrin. "An Address-Free Architecture for Dynamic Sensor Networks". Technical Report 00-724, Computer Science Department, USC, January 2000.

[3] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar. “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, 1999.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan. *“uAMPS ns Code Extensions”*. http://www-mtl.mit.edu/research/icsystems/uamps/ leach.

[5] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan. “Energy-Efficient Communication Protocols for Wireless Microsensor Networks”. In *Proceedings of Hawaiian International Conference on Systems Science*, January 2000.

[6] W. B. Heinzelman. *“Application-Specific Protocol Architectures for Wireless Networks”*. PhD thesis, Massachusetts Institute of Technology, June 2000.

[7] C. Intanagonwiwat, R. Govindan, and D. Estrin. “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, August 2000.

[8] M. Jiang, J. Li, and Y. C. Tay. “Cluster Based Routing Protocol”. Internet Draft, 1999.

[9] E. M. Royer and C.-K. Toh. “A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks”. In *IEEE Personal Communications Magazine*, pages 46–55, April 1999.

[10] UCB/LBNL/VINT. *“Network Simulator-ns”*. http://www-mash.cs.berkeley.edu/ns.