A Taxonomy of Wireless Micro-Sensor Network Models *

Sameer Tilak[a] *sameer@cs.binghamton.edu*
Nael B. Abu-Ghazaleh[a] *nael@cs.binghamton.edu*
Wendi Heinzelman[b] *wheinzel@ece.rochester.edu*
[a] Computer System Research Laboratory, Dept. of CS, Binghamton University, Binghamton, NY
[b] Electrical and Computer Engineering, University of Rochester, Rochester, NY

In future smart environments, wireless sensor networks will play a key role in sensing, collecting, and disseminating information about environmental phenomena. Sensing applications represent a new paradigm for network operation, one that has different goals from more traditional wireless networks. This paper examines this emerging field to classify wireless micro-sensor networks according to different communication functions, data delivery models, and network dynamics. This taxonomy will aid in defining appropriate communication infrastructures for different sensor network application sub-spaces, allowing network designers to choose the protocol architecture that best matches the goals of their application. In addition, this taxonomy will enable new sensor network models to be defined for use in further research in this area.

I. Introduction

Advances in hardware and wireless network technologies have placed us at the doorstep of a new era where small wireless devices will provide access to information anytime, anywhere as well as actively participate in creating smart environments. One of the applications of smart spaces is *sensor networks*, networks that are formed when a set of small untethered sensor devices that are deployed in an ad hoc fashion cooperate on sensing a physical phenomenon. Sensor networks hold the promise of revolutionizing sensing in a wide range of application domains because of their reliability, accuracy, flexibility, cost-effectiveness, and ease of deployment.

To motivate the challenges in designing sensor networks, consider the following scenarios: sensors are rapidly deployed in a remote inhospitable area for a surveillance application; sensors are used to analyze the motion of a tornado; sensors are deployed in a forest for fire detection; sensors are attached to taxi cabs in a large metropolitan area to study the traffic conditions and plan routes effectively; and smart Kindergarten [1] where sensor networks are deployed to create a developmental problem-solving environment for early childhood education.

Clearly, there is a wide range of applications for sensor networks with differing requirements. We believe that a better understanding of micro-sensor network requirements as well as the underlying differences between micro-sensor applications is needed to assist designers. To this end, in this paper we attempt to classify wireless micro-sensor networks. In particular, we classify the aspects of wireless micro-sensor networks that we believe are most relevant to communication. We examine the characteristics and goals of typical micro-sensor networks as well as the different types of communication that are required to achieve these goals. We compare different data delivery models and network dynamics to create a taxonomy of wireless micro-sensor network communication. We believe that this taxonomy will aid network designers in making better decisions regarding the organization of the network, the network protocol and information dissemination models. Furthermore, it will aid in developing realistic sensor network models and benchmarks for use in future sensor network research.

The remainder of this paper is organized as follows. Section II presents some basic definitions and an overview of the characteristics of sensor networks. Section III overviews performance metrics of interest for sensor networks. In Section IV, we describe sensor network architectures. Section V classifies the communication models present in sensor networks and makes the distinction between application and infrastructure related communication. Section VI classifies the data delivery models. In Section VII, the network organization and dynamics are classified. Section VIII presents case studies of existing sensor network protocols, showing how they fit into the taxonomy described in this paper. Finally, Section IX presents a summary and some concluding remarks.

*This work was partially supported by NSF grant EIA-9911099.

II. Sensor Network Characteristics

In this paper, we use the following terminology:

- *Sensor*: The device that implements the physical sensing of environmental phenomena and reporting of measurements (through wireless communication). Typically, it consists of five components– sensing hardware, memory, battery, embedded processor, and trans-receiver.
- *Observer*: The end user interested in obtaining information disseminated by the sensor network about the phenomenon. The observer may indicate *interests* (or queries) to the network and receive responses to these queries. Multiple observers may exist in a sensor network.
- *Phenomenon*: The entity of interest to the observer that is being sensed and potentially analyzed/filtered by the sensor network. Multiple phenomena may be under observation concurrently in the same network.

In a sensing application, the observer is interested in monitoring the behavior of the phenomenon under some specified performance requirements (e.g., accuracy or delay). In a typical sensor network, the individual sensors sample local values (*measurements*) and disseminate information as needed to other sensors and eventually to the observer. The measurements taken by the sensors are discrete samples of the physical phenomenon subject to individual sensor measurement accuracy as well as location with respect to the phenomenon.

Sensor networks share many of the challenges of traditional wireless networks, including limited energy available to each node and bandwidth-limited, error-prone channels. However, communication in sensor networks differs from communication in other types of networks in that it is typically not end-to-end [2]. More specifically, the function of the network is to report information regarding the phenomenon to the observer who is not necessarily aware of the sensor network infrastructure and the individual sensors as an end-point of communication. Furthermore, energy is typically more limited in sensor networks than in other wireless networks because of the nature of the sensing devices and the difficulty in recharging their batteries. Studies in the past have shown that 3000 instructions could be executed for the same energy cost as sending a bit 100m by radio [3]. This indicates that the tradeoff between communication and computation in sensor networks should be resolved in favor of computation. In addition, studies have shown that current commercial radio transceivers, for example those used by Bluetooth devices, are unsuitable for sensor network applications because of their energy requirements [4]. Thus sensor networks impose challenges in hardware design as well as in communication protocols.

III. Performance Metrics

We propose using the following metrics to evaluate sensor network protocols.

- *Energy efficiency/system lifetime*. As sensor nodes are battery-operated, protocols must be energy-efficient to maximize system lifetime. System lifetime can be measured by generic parameters such as the time until half of the nodes die or by application-directed metrics, such as when the network stops providing the application with the desired information about the phenomena.
- *Latency*. The observer is interested in knowing about the phenomena within a given delay. The precise semantics of latency are application dependent.
- *Accuracy*. Obtaining accurate information is the primary objective of the observer, where accuracy is determined by the given application. There is a trade-off between accuracy, latency and energy efficiency. The given infrastructure should be adaptive so that the application obtains the desired accuracy and delay with minimal energy expenditure. For example, the application can either request more frequent data dissemination from the same sensor nodes or it can direct data dissemination from more sensor nodes with the same frequency.
- *Fault-tolerance*: Sensors may fail due to surrounding physical conditions or when their energy runs out. It may be difficult to replace existing sensors; the network must be fault-tolerant such that non-catastrophic failures are hidden from the application. Fault-tolerance may be achieved through data replication (e.g., the SPIN protocol [5]). However data replication itself requires energy; there is a trade-off between data replication and energy-efficiency. We suggest that the data replication should be application-specific. The data which have higher priority according to the application might be replicated for

fault tolerance and the other data might not be.

- *Scalability*: Scalability for sensor networks is also a critical factor. For large-scale networks, it is likely that localizing interactions through hierarchy and aggregation will be critical for ensuring scalability.

IV. Sensor Network Architecture

A sensor network is a tool for measuring and relaying information about the phenomenon to the observer within the desired performance bound and deployment cost. As such, the organization of the network may be viewed as follows:

1. Infrastructure: The infrastructure consists of the sensors and their current deployment status. More specifically, the infrastructure is influenced by the characteristics of the sensors (e.g., sensing accuracy, memory size, battery life, transmission range) and deployment strategy (e.g., sensor density, sensor location, sensor mobility).

2. Network Protocol: The network protocol is responsible for creating paths and accomplishing communication between the sensors and the observer(s).

3. Application/Observer: The observer(s) interests in the phenomenon are queries from the observer(s) about the phenomenon as approximated by the distributed data that the sensors are capable of sensing. These queries could be static (the sensors are preprogrammed to report data according to a specific pattern) or dynamic. The network may participate in synthesizing the query (for example, by filtering some sensor data or fusing several measurements into one value); we consider such intelligence to be part of the translation process between observer interests and low-level implementation.

In this work, we focus on classifying issues that influence the second level: the network protocol. We discuss the other two levels only with regard to issues that influence communication. Thus, we do not address the difficult problem of translation between the observer query and the specific low-level interests. This translation could be done by the application software at the observer and/or the sensor nodes, or directly by a human observer. Similarly, we do not discuss the engineering of the infrastructure.

We also note that there is a significant opportunity for optimizations that cut across the three organizational levels. For example, Bhatnagar et al. discuss supporting QoS for sensor networks [6]. More specifically, they discuss discriminating among the type of data that the sensors are reporting and preferentially treating high priority data (for example, by giving it priority in forwarding and using redundancy to increase the chance of its reception). This is an example of an optimization where application-level knowledge provides hints to the network protocol. As another example, consider the case where the deployment of the sensors is chosen to mirror the expected motion pattern of the phenomenon or the interests of the observer. Such a deployment strategy incorporates application knowledge in the infrastructure design.

The network protocol in a sensor network is responsible for supporting all communication, both among sensor nodes as well as between the sensor nodes and the observer(s). The performance of the protocol will be highly influenced by the network dynamics, as well as by the specific data delivery model employed. In order to determine how the network protocol behaves for different scenarios, it is important to classify these features. In the following sections, we classify the different types of communication required in a sensor network and then look at the possible data delivery models and network dynamics.

V. Communication Models

There are multiple ways for a sensor network to achieve its accuracy and delay requirements; a well designed network meets these requirements while optimizing the sensor energy usage and providing fault tolerance. By studying the communication patterns systematically, the network designer will be able to choose the infrastructure and communication protocol that provide the best combination of performance, robustness, efficiency and deployment cost.

Conceptually, communication within a sensor network can be classified into two categories: *application* and *infrastructure*. The network protocol must support both these types of communication. Application communication relates to the transfer of sensed data (or information obtained from it) with the goal of informing the observer about the phenomena. Within application communication, there are two models: cooperative and non-cooperative. Under the cooperative sensor model, sensors communicate with other sensors to realize the observer interest. This communication is beyond the relay function needed for routing. For example, in a clustering protocol a cluster-head and the sensor nodes communicate with each other for information dissemination related to the actual phe-