A Taxonomy of Wireless Micro-Sensor Network Models

Sameer Tilak†, Nael B. Abu-Ghazaleh† and Wendi Heinzelman‡

†Computer System Research Laboratory
Dept. of CS, Binghamton University
Binghamton, NY 13902–6000
{sameer,nael}@cs.binghamton.edu

‡Electrical and Computer Engineering
University of Rochester
Rochester, NY 14627–0126
wheinzel@ece.rochester.edu

Abstract—
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 subspaces, 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. Clearly, there is a wide range of applications for sensor networks with differing requirements. We believe that a better understanding of the micro-sensor network requirements as well as the underlying differences between different micro-sensor applications is needed to assist designers. To this end, in this paper we attempt to classify wireless micro-sensor networks from a communication protocol perspective. We look at 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 the characteristics of sensor networks. Section III classifies the communication models present in sensor networks and makes the distinction between application and infrastructure related communication. Section IV classifies the data delivery models. In Section V, the network organization and dynamics are classified. Finally, Section VI presents a summary and some concluding remarks.

II. Micro-sensor Network Characteristics

Throughout 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.
- *Phenomenon*: The entity of interest to the observer that is being sensed and optionally analyzed/filtered by the

sensor network. There may be multiple phenomena under observation concurrently in the same network.

In a sensing application, the observer is interested in monitoring phenomena under some latency and accuracy restrictions. In a typical sensor network, the individual sensors sense 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.

An observer (or application-level) interest is a query from the observer about the physical phenomenon as approximated by the distributed data that the sensors are capable of sensing. Ideally, the observer interest is in terms of the phenomenon and is oblivious to the underlying sensor network implementation. The query is implemented as one or more specific low-level interests (e.g., requesting a specific sensor to report a specific measurement at some specific interval). In this work, 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. Furthermore, the network may participate in synthesizing the query (for example, by filtering some sensor data or summarizing several measurements into one value), but we consider such intelligence to be part of the translation process between observer interests and low-level implementation.

Sensor networks share many of the challenges of traditional wireless networks, including batter-powered nodes, limiting the 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 [1]. More specifically, the function of the network is to report the phenomenon of interest to the observer who is not necessarily interested in (or aware of) specific sensors as another end-point of communication. Furthermore, energy is often much more limited in sensor networks than in other wireless networks since it is often impossible to recharge the batteries of sensor nodes. We propose using the following metrics to evaluate sensor network protocols with regard to these unique goals and constraints:

- *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. Precise semantics of latency are data delivery model 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 the surrounding physical conditions or because their energy ran out. It may be difficult to replace existing sensors, so the network must be fault-tolerant so that actual network conditions are transparent to the given application.

III. 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, the communication within a sensor network can be classified into two categories: *application* and *infrastructure*. 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. Non-cooperative sensors do not cooperate at the application level for information dissemination. One extreme case is where no sensor communicates with its neighbors– all the sensors work independently and continuously relay sensed data to the observer. In the second case, co-operative sensors, a given sensor might be required to communicate with its neighbors either periodically or after the occurrence of a specific event. An example of co-operative sensing is in a clustering protocol when a cluster-head and the non-cluster-head members communicate with each other for information dissemination related to the actual phenomenon.

Infrastructure communication refers to the communication needed to configure, maintain and optimize operation. More specifically, because of the ad hoc nature of sensor networks, sensors must be able to discover paths to other sensors of interest to them and to the observer regardless of sensor mobility or failure. Thus, infrastructure communication is needed to keep the network functional,

ensure robust operation in dynamic environments, as well as optimize overall performance. We note that such infrastructure communication is highly influenced by the application interests since the network must reconfigure itself to best satisfy these interests.

In static sensor networks, an initial phase of infrastructure communication is needed to set up the network. Furthermore, if the sensors are energy-constrained, there will be additional communication for reconfiguration. Similarly, if the sensors are mobile, additional communication is needed for path discovery/reconfiguration. For example, in a clustering protocol, infrastructure communication is required for the formation of clusters and cluster-head selection; under mobility or sensor failure, this communication must be repeated (periodically or upon detecting failure). Finally, infrastructure communication is used for network optimization. Consider the Frisbee model, where the set of active sensors follows a moving phenomenon to optimize energy efficiency [2]. In this case, the sensors wake up other sensors in the network using infrastructure communication.

Sensor networks require both application and infrastructure communication. The amount of required communication is highly influenced by the networking protocol used. Application communication is optimized by reporting measurements at the minimal rate that will satisfy the accuracy and delay requirements given sensor abilities and the quality of the paths between the sensors and the observer. The infrastructure communication is generated by the networking protocol in response to application requests or events in the network. Investing in infrastructure communication can reduce application traffic and optimize overall network operation.

IV. Data Delivery Models

Sensor networks can be classified in terms of the data delivery required by the application (observer) interest as: *continuous*, *event-driven*, *observer-initiated* and *hybrid*. These models govern the generation of the application traffic. In the continuous model, the sensors communicate their data continuously at a prespecified rate. Heinzelman et al. showed that clustering is most efficient for static networks where data is continuously transmitted [3], [4]. For dynamic sensor networks, depending upon the degree of mobility, clustering may be applicable as well. In the event-driven data model the sensors report information only if an event of interest occurs. In this case, the observer is interested only in the occurrence of a specific phenomenon or set of phenomena. In the observer-initiated (or request-reply) model, the sensors only report their results in response to an explicit request from the observer (either directly, or indirectly through other sensors). Finally, the three approaches can coexist in the same network; we refer to this model as the hybrid model.

Thus far, we have only discussed data delivery from the application perspective, and not the actual flow of data packets between the sensors and the observer (which is subject to the network protocol). For any of the abovementioned models, we can classify the communication approach as: flooding (broadcast-based), unicast, or multicast/other. Using a flooding approach, sensors broadcast their information to their neighbors, who rebroadcast this data until it reaches the observer. This approach incurs high overhead but is immune to dynamic changes in the topology of the network. Research has been conducted on techniques such as data aggregation that can be used to reduce the overhead of the broadcast [3], [5], [1]. Alternatively, the sensors can either communicate to the observer directly (possibly using a multi-hop routing protocol) or communicate with the cluster-head using one-to-one unicast. Finally, in a multicast approach, sensors form application-directed groups and use multicast to communicate among group members. The observer could communicate with any member of the group to obtain the desired data. A major advantage of flooding or broadcast is the lack of a complex network layer protocol for routing, address and location management; existing sensor network efforts have mostly relied on this approach.

V. Network Dynamics Models

A sensor network forms a path between the phenomenon and the observer. The goal of the sensor network protocol is to create and maintain this path (or multiple paths) under dynamic conditions while meeting the application requirements of low energy, low latency, high accuracy, and fault tolerance. Without loss of generality, this discussion assumes a single observer. The problem of setting up paths for information dissemination is similar to the problem of routing in ad hoc networks [6]. However, there are a few critical differences, including: (i) the sensors are not generally addressed individually; rather, the interest is in the set of sensors that are *in a position to contribute to the active observer interests*. The mapping between the observer interest and a set of sensors is influenced by the network dynamics and the application; and (ii) nodes along the path can take an active role in the information dissemination and processing. In this respect, sensor networks are analogous to Active Networks [7] where ad hoc networks are traditional "passive" networks.

There are several approaches to construct and maintain the path between the observer and the phenomenon. These will differ depending on the network dynamics, which we classify as: *static sensor networks* and *mobile sensor networks*. We focus on mobility because it is the most common source of dynamic conditions; other sources include sensor failure and changes in observer interests.

Static Sensor Networks

In static sensor networks, there is no motion among communicating sensors, the observer and the phenomenon. An example is a group of sensors spread for temperature sensing. For these types of sensor networks, previous studies have shown that localized algorithms can be used in an effective way [3], [1]. The sensors in localized algorithms communicate with nodes in their locality. An elected node relays a summary of the local observations to the observer, perhaps through one on more levels of hierarchy. Such algorithms extend the lifetime of the sensor network because they trade-off local computation for communication [3]. In this type of network, sensor nodes require an initial one time set-up infrastructure communication to create the path between the observer and the sensors with the remaining traffic exclusively application communication[1].

Dynamic Sensor Networks

In dynamic sensor networks, either the sensors themselves, the observer, or the phenomenon are mobile. Whenever any of the sensors associated with the current path from the observer to the phenomenon moves, the path may fail. In this case, either the observer or the concerned sensor must take the initiative to rebuild a new path. During initial set-up, the observer can build multiple paths between itself and the phenomenon and cache them, choosing the one that is the most beneficial at that time as the current path. If the path fails, another of the cached paths can be used. If all the cached paths are invalid then the observer must rebuild new paths. This observer-initiated approach is a *reactive* approach, where path recovery action is only taken after observing a broken path.

Another model for rebuilding new paths from the observer to the phenomenon is a sensor-initiated approach. In a sensor-initiated path recovery procedure, path recovery is initiated by a sensor that is currently part of the logical path between the observer and the phenomenon and is planning to move out of range. The sensor might perform some local patching procedure to build a new path by broadcasting a *participation request* for a given logical flow to all its neighboring sensors. Any one of the neighboring sensors can send a *participation reply* message to the given initiator sensor indicating willingness to participate and become a part of the requested path. If none of the neighboring sensors respond, the sensor can default to sending a path invalidation request to the observer so that the observer can start building the path. This is similar to soft hand-off in traditional Mobile IP based networks [8]. This sensor-initiated approach is a *proactive* approach where path recovery operations are begun in anticipation of a future broken path.

Dynamic sensor networks can be further classified by considering the motion of the components. This motion is important from the communications perspective since the degree and type of communication is dependent on network dynamics. We believe that each of the following require different infrastructures, data delivery models, and protocols:

- *Mobile observer*. In this case the observer is mobile with respect to the sensors and phenomena. An example of this paradigm is sensors deployed in an inhospitable area for environment monitoring. For example, a plane might fly over a field periodically to collect information from a sensor network. Thus the observer, in the plane, is moving relative to the sensors and phenomena on the ground.
- *Mobile sensors*. In this case, the sensors are moving with respect to each other and the observer. For example, consider traffic monitoring implemented by attaching sensors to taxis. As the taxis move, the attached sensors continuously communicate with each other about their own observations of the traffic conditions. If the sensors are co-operative, the communication paradigm imposes additional constraints such as detecting the link layer addresses of the neighbors and constructing localization and information dissemination structures. From previous work [1], we know that the overhead of maintaining a globally unique sensor ID in a hierarchical fashion like an IP address is expensive and not needed. Instead, these sensors should communicate only with their neighbors with the link layer MAC address. In such networks, the above-mentioned proactive algorithm with local patching for repairing a path can be used so that the information about the phenomenon is always available to the observer regardless of the mobility of the individual sensors.
- *Mobile phenomena*. In this case, the phenomenon itself is moving. A typical example of this paradigm is sensors deployed for animal detection. In this case the infrastructure level communication should be event-driven. Depending on the density of the phenomena, it will be inefficient if all the sensor nodes are active all the time. Only the sensors in the vicinity of the mobile phenomenon need to be active. The number of active sensors in the vicinity of the phenomenon can be determined by application specific goals such as accuracy, latency, and energy efficiency. A model that is well-suited to this case is the Frisbee model [2].

Often, it is possible to implement a sensor network for a specific phenomenon in a number of different ways. Consider the problem of monitoring a tornado. One option would be to fly airplanes to sense the tornado (mobile phe-

[1] Note that if energy is limited among the nodes, the network will require infrastructure communication to maintain a path between the observer and the phenomenon as nodes run out of energy.

nomenon; mobile sensors; continuous data delivery). Another would be to have a sensor grid statically placed on the ground and report data as the tornado passes through (mobile phenomenon; static sensors; continuous data delivery). Yet another would be to release lightweight sensors into the tornado (static phenomenon; mobile sensors; continuous data delivery). The primary concern here is the ability of the sensor network to report the desired level of accuracy under latency constraints within an acceptable deployment cost. The accuracy is a function of the sensing technology of the sensors and their distance from the phenomenon. However, since the performance is measured at the observer end, it is also a function of the performance of the communication model. We hope that this taxonomy will assist in developing relevant simulation models to enable empirical study of the performance of the different sensor network organizations and assist in making design and deployment decisions.

VI. Conclusion

The overall communication behavior in a wireless micro-sensor network is application driven. We believe that it is useful to decouple the application communication used for information dissemination from the infrastructure communication used to configure and optimize the network. This separation will aid network designers in selecting the appropriate sensor network architecture that will best match the characteristics of the communication traffic of a given application. This will allow the network protocol to achieve the application-specific goals of energy-efficiency, low latency, and high accuracy in the sensing application. We also believe that a sensor-initiated proactive path recovery approach with local patching will be beneficial in the efficient information dissemination in wireless micro-sensor networks.

We plan to study the behavior of various communication protocols for the different application subspaces described in this paper. This will be done through analysis and simulation to determine the advantages and disadvantages of existing approaches, such as DSR (Dynamic Source Routing) [9], directed diffusion [1], and LEACH [3]. We hope that the taxonomy we have presented will be helpful in designing and evaluating network protocols for wireless micro-sensor networks.

References

[1] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," *Proc. 4th ACM International Conference on Mobile Computing and Networking (Mobicom'98),* Aug. 2000.

[2] A. Cerpa, J. Elson, D. Estrin, L. Girod, M. Hamilton, and J. Zhao, "Habitat Monitoring: Application Driver for Wireless Communications Technology ," in *Proc. ACM SIGCOMM Workshop on Data Communications in Latin America and the Caribbean,* Apr. 2001.

[3] W. Heinzelman, *Application-Specific Protocol Architectures for Wireless Networks,* Ph.D. thesis, Massachusetts Institute of Technology, 2000.

[4] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-Efficient Routing Protocols for Wireless Microsensor Networks," in *Proc. 33rd Hawaii International Conference on System Sciences (HICSS '00),* Jan. 2000.

[5] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," in *Proceedings of the Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '99),* Aug. 1999, pp. 174–185.

[6] Internet Engineering Task Force MANET Working Group, "Mobile ad hoc networks (MANET) charter," http://www.ietf.org/html.charters/manet-charter.html.

[7] D. Tennenhouse, J. Smith, W. Sincoskie, D. Wetherall, and G. Minden, "A survey of active network research," *IEEE Communications Magazine,* vol. 35, no. 1, pp. 80–86, Jan. 1997.

[8] "IETF MobileIP Working Group Internet Draft," http://www.ietf.org/rfc/rfc2002.txt, 1996.

[9] "IETF MANET Working Group Internet Draft– Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-05.txt, 2001.