Sensors and Sensor Networks are Growing Applications

From June 2006 *High Frequency Electronics*

Wireless sensor technology has rapidly moved from basic research to practical development. University research papers, an indicator of what technical issues require resolution, have recently been focused on operational matters such as sensor range, power consumption and large network communications management. One of the more active research topics is the investigation of methods for processing a large amount of data that may be gathered over a very large physical area.

Sensor networks are primarily being developed to operate as ad hoc networks. This is a requirement for any network that is dynamic in the number of sensors and uncertain availability of any particular sensor at any given time. An overview of ad hoc sensor networks is given in the following section, from a summary by the National Institute for Standards and Technology (NIST).

Wireless Ad Hoc Sensor Networks

A wireless ad hoc sensor network consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data. Some examples of wireless ad hoc sensor networks are the following:

- Military sensor networks to detect and gain as much information as possible about enemy movements, explosions, and other phenomena of interest.
- Sensor networks to detect and characterize Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) attacks and material.
- Sensor networks to detect and monitor environmental changes in plains, forests, oceans, etc.
- Wireless traffic sensor networks to monitor vehicle traffic on highways or in congested parts of a city.
- Wireless surveillance sensor networks for providing security in shopping malls, parking garages, and other facilities.
- Wireless parking lot sensor networks to determine which spots are occupied and which are free.

The above list suggests that wireless ad hoc sensor networks offer certain capabilities and enhancements in operational efficiency in civilian applications as well as assist in the national effort to increase alertness to potential terrorist threats.

Two ways to classify wireless ad hoc sensor networks are whether or not the nodes are individually addressable, and whether the data in the network is aggregated. The sensor nodes in a parking lot network should be individually addressable, so that one can determine the locations of all the free spaces. This application shows that it may be necessary to broadcast a message to all the nodes in the network. If one wants to determine the temperature in a corner of a room, then addressability may not be so important. Any node in the given region can respond. The ability of the sensor network to aggregate the data collected can greatly reduce the number of messages that need to be transmitted across the network. This function of data fusion is discussed more below.

The basic goals of a wireless ad hoc sensor network generally depend upon the application, but the following tasks are common to many networks:

- Determine the value of some parameter at a given location—In an environmental network, one might want to know the temperature, atmospheric pressure, amount of sunlight, and the relative humidity at a number of locations. This example shows that a given sensor node may be connected to different types of sensors, each with a different sampling rate and range of allowed values.
- Detect the occurrence of events of interest and estimate parameters of the detected event or events—In the traffic sensor network, one would like to detect a vehicle moving through an intersection and estimate the speed and direction of the vehicle.
- Classify a detected object—Is a vehicle in a traffic sensor network a car, a mini-van, a light truck, a bus, etc.
- Track an object—In a military sensor network, track an enemy tank as it moves through the geographic area covered by the network.

In these four tasks, an important requirement of the sensor network is that the required data be disseminated to the proper end users. In some cases, there are fairly strict time requirements on this communication. For example, the detection of an intruder in a surveillance network should be immediately communicated to the police so that action can be taken.

Wireless ad hoc sensor network requirements include the following:

- Large number of (mostly stationary) sensors—Aside from the deployment of sensors on the ocean surface or the use of mobile, unmanned, robotic sensors in military operations, most nodes in a smart sensor network are stationary. Networks of 10,000 or even 100,000 nodes are envisioned, so scalability is a major issue.
- Low energy use: Since in many applications the sensor nodes will be placed in a remote area, service of a node may not be possible. In this case, the lifetime of a node may be determined by the battery life, thereby requiring the minimization of energy expenditure.
- Network self-organization—Given the large number of nodes and their potential placement in hostile locations, it is essential that the network be able to self-organize; manual configuration is not feasible. Moreover, nodes may fail (either from lack of energy or from physical destruction), and new nodes may join the network. Therefore, the network must be able to periodically reconfigure itself so that it can continue to function. Individual nodes may become disconnected from the rest of the network, but a high degree of connectivity must be maintained.
- Collaborative signal processing—Yet another factor that distinguishes these networks from MANETs is that the end goal is detection/estimation of some events of interest, and not just communications. To improve the detection/estimation performance, it is often quite useful to fuse data from multiple sensors. This data fusion requires the transmission of data and control messages, and so it may put constraints on the network architecture.
- Querying ability—A user may want to query an individual node or a group of nodes for information collected in the region. Depending on the amount of data fusion performed, it may not be feasible to transmit a large amount of the data across the network. Instead, various local sink nodes will collect the data from a given area and create summary messages. A query may be directed to the sink node nearest to the desired location.

Sensor Types and System Architecture

With the coming availability of low cost, short range radios along with advances in wireless networking, it is expected that wireless ad hoc sensor networks will become commonly deployed. In these networks, each node may be equipped with a variety of sensors, such as acoustic, seismic, infrared, still/motion video camera, etc. These nodes may be organized in clusters such that a locally occurring event can be detected by most of, if not all, the nodes in a cluster. Each node may have sufficient processing power to make a decision, and it will be able to broadcast this decision to the other nodes in the cluster. One node may act as the cluster master, and it may also contain a longer range radio using a protocol such as IEEE 802.11 or Bluetooth.

[from the Advanced Network Technologies Division of NIST, http://w3.antd.nist.gov/wahn_ssn.shtml]

Security and Privacy Issues in Sensors and Sensor Networks

Any time a large-scale monitoring system is deployed, there are concerns about the security of the system itself and the privacy of the individuals whose activities may become part of the monitoring regimen.

Security can largely be maintained through common types of encryption, although the computing resources of low power sensors may not always support the most robust encryption methods. The biggest risk is corruption of the acquired data, whether accidental or intentional, which will skew the resulting analysis. For example, in a system of sensors monitoring the HVAC system of a large building, the risk may seem quite low, but the network may have a fire detection function that must operate with high reliability.

In some cases, the acquired data may have value (e.g. security monitoring systems or personnel/vehicle location monitors). These systems must incorporate a level of data security to avoid both unwanted intrusion and passive monitoring or data collection.

Privacy is always a controversial subject, but is an essential consideration for many sensor network scenarios. In particular, sensor networks have been proposed that would piggyback on existing wireless technologies such as RFID and wireless handsets. When systems are used outside of their core purpose, the user may claim that such use is surreptitious. In these cases, a published privacy policy may be acceptable, although a more prominent notice may be preferred by most people.

Less clear are external networks that monitor various activities, such as a roadside sensor system that monitors traffic, or security cameras capable of monitoring beyond the boundaries of the public or private enterprise that is using them. With high interest in various location-tracking systems, these networks could become commonplace. Maintaining the anonymity of the population being monitored is an issue receiving much attention at this time.

The level of sophistication of the sensor networks varies greatly. Simple sensors that only detect presence or movement of vehicles or persons provide no specific data on individuals. At the other extreme is the information collected on the location of all wireless handset users, as is done with the E-911 system. Each individual user has his or her location identified with significant precision. The primary questions concern how much control that person should have over the use of that information.

The issue of privacy is one of high importance to the public, particularly in the U.S. The debate is not likely to end soon regarding what types of information should have privacy protected, and which are considered either too important or too mundane to be concerned with. With the growing number of wireless sensor networks, a continuing discussion is guaranteed.