SENSOR NETWORKS: AN OVERVIEW

Malik Tubaishat and Sanjay Madria

Advances in hardware and wireless network technologies have created low-cost, low-power, multi-functional miniature sensor devices. These devices make up hundreds or thousands of ad hoc tiny sensor nodes spread across a geographical area. These sensor nodes collaborate among themselves to establish a sensing network. A sensor network that can provide access to information anytime, anywhere by collecting, processing, analyzing and disseminating data. Thus, the network actively participates in creating a smart environment.

Sensor networks promise to revolutionize sensing in a wide range of application domains. This is because of their reliability, accuracy, flexibility, cost-effectiveness and ease of deployment, according to Tilak *et al*. Smart sensors can offer vigilant surveillance and can detect and collect data concerning any sign of machine(s) failure, earthquakes, floods and, even, a terrorist attack. Sensor networks enable: 1) information gathering, 2) information processing, and 3) reliable monitoring of a variety of environments for both civil and military applications.

The architecture of the sensor node's hardware consists of five components: sensing hardware, processor, memory, power supply and transceiver. These devices are easily deployed because no infrastructure and human control are needed. They sense, compute and actuate into the physical environments. They can self-organize and can adapt to support several applications.

Each sensor node has wireless communication capability and sufficient intelligence for signal processing and for disseminating the data. The limited energy, computational power, and communication resources of a sensor node requires the use of a huge number of sensor nodes in a wider region. This large number also allows the sensor network to report with greater accuracy the exact speed, direction, size, and other characteristics of a moving object than is possible with a single sensor.

Since sensor networks have a large number of sensor nodes, the cost of a single node is very important to justify the overall cost of the network. The cost of a sensor node should be much less than $1 (USD) in order for the sensor network to be feasible according to Akyildiz *et al*.

Communication in sensor networks is not typically end to end. 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. Lastly, studies have shown that current commercial Bluetooth devices are unsuitable for sensor network applications because of their energy requirements, state Tilak *et al* and expected higher costs than sensor nodes (Akyildiz *et al*).

Intuitively, a denser infrastructure would lead to a more effective sensor network. It can provide higher accuracy and has a larger aggregate amount of energy available. However, if not properly managed, a denser network can also lead to a larger number of collisions and potentially to congestion in the network; this will increase latency and reduce energy efficiency. Moreover, the large number of samples reported by the sensors may vastly exceed the data information required.

collectively sending back information

Examples of possible applications

Detecting environmental hazards, monitoring remote terrain, or even customer behavior surveillance are among many sensor network applications. Researchers are trying to adopt sensor network technology to problems hard to solve with conventional wireless networking.

Some examples are the following:

- Sensors are deployed to analyze remote locations (the motion of a tornado, fire detection in a forest);
- Sensors are attached to taxi cabs in a large metropolitan area to study the traffic conditions and plan routes effectively;
- Wireless parking lot sensor networks that determine which spots are occupied and which spots are free;
- Wireless surveillance sensor networks for providing security in a shopping mall, parking garage or at some other facility;
- Military sensor networks to detect, locate or track enemy movements, and
- Sensor networks can increase alertness to potential terrorist threats.

A hierarchical sensor network

We depict a sensor network example in military terms to show how sensors cooperate among themselves and how they disseminate and aggregate the data.

The tactical military network architecture (see Fig. 1) consists of a group of units (i.e., clusters) managed by *commanders* (i.e., parent nodes). These commanders receive orders from *headquarters* (i.e., the sink node) and, in return, send back their report.

The commanders send the order received from headquarters to their *generals* (i.e., cluster heads). Every general is responsible for a group of *soldiers* (i.e., children) in a unit. Soldiers communicate locally (i.e., within a unit) with their counterparts or their general. Soldiers in a unit cannot communicate with generals from other units whereas generals can only communicate among themselves. After hearing the messages from their soldiers, generals send their observations to their commanders.

In a battlefield, soldiers in a unit contact their general to notify the general about a specific observation in their unit. The general, then, can issue an order to his soldiers to take an action regarding their observation, or can contact his commander for an opinion. In case of decisive actions, such as an *attack* command, only headquarters can order a decisive action based on the information from the commanders.

Sensor network challenges

Challenges in hardware design, communication protocols and applications design face sensor network technology to make it a reality. Extending the lifetime of the sensor network and building an intelligent data collecting

0278-6648/03/$17.00 © 2003 IEEE

systems are two. Other challenges include:

• Sensor networks' topology changes very frequently;

• Sensors use a broadcast communication paradigm whereas most networks are based on point-to-point communications;

• Sensors are very limited in power, computational capacities and memory;

• Sensors are very prone to failures;

• Sensors may not have global identification (ID) because of the large amount of overhead;

• Sensors are densely deployed in large numbers. The problem can be viewed in terms of collision and congestion. To avoid collisions, sensors that are in the transmission range of each other should not transmit simultaneously.

• Ad hoc deployment requires that the system identifies and copes with the resulting distribution and connectivity of nodes, and

• Dynamic environmental conditions require the system to adapt over time to changing connectivity and system stimuli.

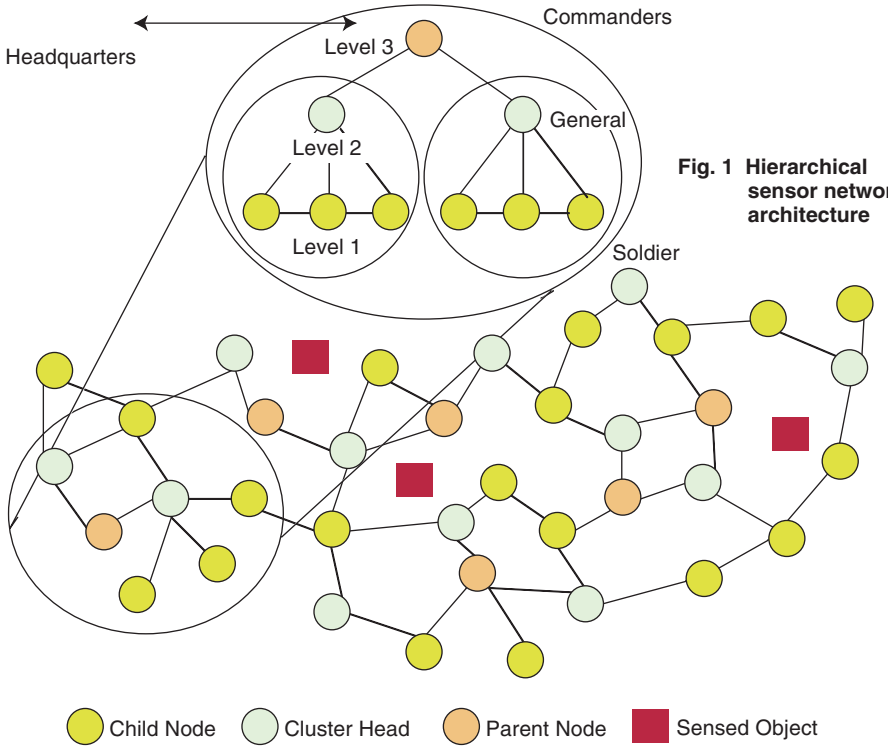

Fig. 1 Hierarchical sensor network architecture

Requirements

Sensor network requirements include the following:

Large number of sensors: To make use of the cheap small-sized sensors, sensor networks may contain thousands of nodes. Scalability and managing these huge numbers of sensors is a major issue. Clustering is one solution to this problem. In clustering, neighbor sensors join to build one cluster (group) and elect a cluster head to manage this group.

Low energy use: In many applications, the sensor nodes will be deployed in a remote area in which case servicing a node may not be possible. Thus, the lifetime of a node may be determined by the battery life, thereby requiring minimal energy expenditure. (Recharging a large number of sensor batteries would be expensive and time consuming.)

Efficient use of the small memory: When building sensor networks, issues such as routing-tables, data replication, security and such should be considered to fit the small size of memory in the sensor nodes.

Data aggregation: The huge number of sensing nodes may congest the network with information. To solve this problem, some sensors such as the cluster heads can aggregate the data, do some computation (e.g., average, summation, highest, etc.), and then broadcast the summarized new information.

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 itself. Moreover, nodes may fail (either from lack of energy or from physical destruction), and new nodes may need to 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 overall must be maintained.

Collaborative signal processing: Yet another factor that distinguishes these networks from *Mobile Ad-hoc Networks* (MANETs) is that the end goal is the detection/estimation of some event(s) of interest, and not just communication. To improve the detection performance, it is often quite useful to fuse data from multiple sensors. This data fusion requires the transmission of data and control messages. This need may put constraints on the network architecture.

Querying ability: there are two types of addressing in sensor network; data-centric, and address-centric according to Intanagonwiwat et al. In data-centric, a query will be sent to specific region in the network. Whereas, in addressing-centric, the query will be sent to an individual node.

Potential advantages of sensor networks over MANET

Although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited to the unique features and applications requirements of sensor networks. Yes, sensor nodes are prone to failures and may not have global identification (ID). Still, sensor networks have many advantages over the traditional wireless ad hoc network.

• Wireless sensor networks improve *sensing accuracy* by providing distributed processing of vast quantities of sensing information (e.g., seismic data, acoustic data, high-resolution images, etc.). When networked, sensors can aggregate such data to provide a rich, multi-dimensional view of the environment;

• They can provide *coverage of a very large area* through the scattering of thousands of sensors;

• Networked sensors can continue to function accurately in the face of fail-

ure of individual sensors. Thus, allowing greater *fault tolerance* through a high level of redundancy;

• Wireless sensor networks can also improve remote access to sensor data by providing sink nodes that connect them to other networks, such as the Internet, using wide-area wireless links.

• They can localize discrete phenomenon to save power consumption;

• They can minimize human intervention and management;

• They can work in hostile and unattended environments; and

• They can dynamically react to changing network conditions.

How ad hoc sensor networks operate

An ad hoc sensor network is a collection of sensor nodes forming a temporary network without the aid of any central administration or support services. In other words, there is no stationary infrastructure such as base stations.

In general, the sensor nodes use wireless radio frequency (RF) transceivers as their network interface and communicate with each other using multi-hop wireless links. Each sensor node in the network also acts as a router, forwarding data packets for its neighbor nodes.

Ad hoc networks must deal with frequent changes in topology. This is because sensor nodes are prone to failure and also new sensor nodes may join the network to compensate the failed nodes or to maximize the area of interest. Because of these characteristics, a central challenge in the design of the ad hoc sensor network is the development of self-organizing sensor network and dynamic routing protocols that can efficiently find routes between two communicating nodes.

For the tiny sensors to coordinate among themselves to achieve a large sensing task in a less power consumption, they should work in a cluster. Each cluster assigns a cluster head to manage its sensors. The advantages of cluster heads are:

• Clustering allows sensors to efficiently coordinate their local interactions in order to achieve global goals;

• Scalability;

• Improved robustness;

• More efficient resource utilization;

• Lower energy consumption; and

• Robust link or node failures and network partitions

In Fig. 2, we show the general architecture of a sensor network. As shown in the figure, there are three layers: the services-layer, the data-layer and the physical-layer. The services include, but are not restricted to, routing protocol, data dissemination and data aggregation.

The physical-layer consists of the physical nodes. These nodes are the sinks, children nodes, the cluster heads and the parents. Parent nodes are those connected to two or more cluster heads. All the messages are virtually modeled in the data-layer.

The sink node(s) broadcast a query either to the entire sensor network or toward a specific region depending on type of query used. When the sensor nodes—close to the sensed object, detect for example a change in heat, location, speed, etc—then they broadcast this data to their neighboring sensor nodes.

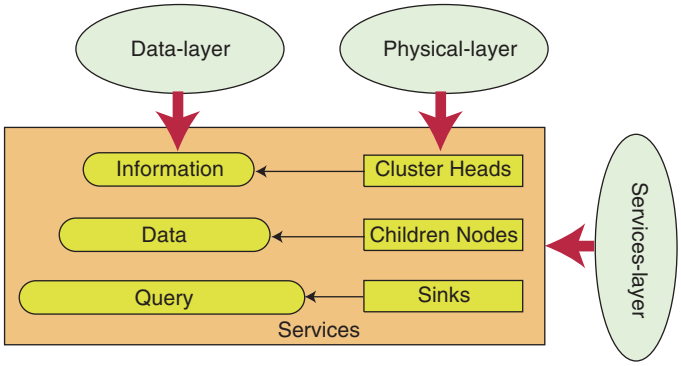

Fig. 2 Sensor network architecture

Since each sensor (i.e., child) is connected to at least one cluster head, cluster head(s) will eventually receive this data. Cluster head's task is to process and aggregate this data and broadcast it to the sink node(s) through the neighboring nodes. This is because the cluster head receives many data packets from its children. Hence, it is the cluster head's task to process and filter this data as information.

To compensate the hardware limitations in the sensor nodes such as memory, battery and computation power, sensor applications deploy a large number of sensor nodes in the targeted region. These sensor nodes then collaborate among themselves to perform as one big wireless ad hoc network. The close distance between the nodes helps also in saving power by reducing the radius of transmission for each node.

Data versus address-centric

Now we will explain why sensor networks should be data-centric instead of address-centric. The principle idea of sensor networks is to design very cheap and simple sensor nodes. This way sensor applications can contain thousands of these disposable nodes are used without any burden. Giving a unique address for each node is costly especially when thousands of nodes are used in a sensor network application.

The limited memory and computational power force one not to depend on the contents of an individual sensor node itself. Rather, we are interested in the observation of a group of sensors.

Data-centric applications focus on data generated by sensors. So, instead of sending a query say to sensor #45, the query will be sent to say region #6 which is known from the Global Positioning System (GPS) device placed on the sensor nodes. The idea of using GPS to easily locate sensors is very important when disseminating the data packet, as we can send the query to a specific region by the help of the GPS embedded in some sensor nodes.

(Unfortunately, embedded GPS sensor nodes can sometimes be misleading when their line of sight is blocked. Further, GPS gives the location within a range (i.e., not exact location). Hence, nodes very close to each other will have the same GPS result.)

Aggregation

Some sensor nodes are assigned to aggregate data received from their neighbors. Aggregator nodes can cache, process and filter the data to more meaningful information and resend to the sink nodes. Aggregation is useful for the following reasons:

• Increase the circle of knowledge;

• Increase the level of accuracy; and

• Data redundancy to compensate for sensor nodes' failing.

Dissemination

Data produced by the sensors usually has to be routed through several intermediate nodes to reach its destination. Problems arise when intermediate nodes fail to forward incoming messages. Other problems are:

• Routing protocol should find the shortest path;

• Redundancy: a sensor may receive the same data packet more than once.

In sensor networks, two scenarios for data dissemination exist: query driven and continuous update. Each scenario is applicable to specific types of sensor applications. The former is used as a one-to-one relation. That is, the sink broadcasts a query and, in turn, receives from the sensor nodes one report in response to this query. For example, the sink may query the first presence of an object such as seeing an enemy tank, or even an animal.

The second scenario is a one-to-many relation. That is, the sink node broadcasts a query and receives continuous updates for this query. For example, the sink may query for the direction of a mobile object. In turn, the sensors will report to the sink the new location of the mobile object. The continuously updated data dissemination scenario has a high rate of energy depletion; but its data is more reliable and accurate than the query driven. This is because more sensors are involved in the query report.

For instance, the sensor nodes in a parking lot network should be individually addressable. This way one can easily determine the locations of all the free spaces. Another example is placing sensors above every passenger's seat in an airplane to detect any unusual movement of any passenger. In case of any danger, a sensor network can collaborate to take control of the airplane (e.g., switching the lights off, closing the pilot's cockpit door, etc.).

Last point

Finally, and most important, the advantage of using these sensors is their ability to maintain connectivity in case of movement. As these sensors are very tiny, they are vulnerable to being accidentally moved. Hence, sensor networks should maintain network connectivity even if some of their sensors are moved. For example, sensors located in a forest may be vulnerable to any kind of mobility (e.g. human, animal, insect, rain, wind).

Read more about it

• Deborah Estrin, David Culler, Kris Pister, Gaurav Sukhatme, "Connecting the Physical World with Pervasive Networks," *IEEE Pervasive Computing*, Volume 1, Number 1, Jan-Mar 2002.

• S. Tilak, N. Abu-Ghazaleh, and W. Heinzelman, "A Taxonomy of Wireless Micro-Sensor Network Models," *ACM Mobile Computing and Communications Review* (MC2R), Volume 6, Number 2, April 2002.

• D. Estrin, R. Govindan, J. Heidemann, and S. Kumar. *Next century challenges: Scalable coordination in sensor networks.* In the Proceedings of the fifth annual ACM/IEEE international conference on mobile computing and networking, pages 263-270, 1999.

• Joanna Kulik, Wendi Rabiner Heinzelman, and Hari Balakrishnan, *Adaptive Protocols for Information Dissemination in Wireless Sensor Networks*, Proc. 5th ACM/IEEE MobiCom Conference (MobiCom '99), Seattle, WA, August, 1999.

• Joanna Kulik, Wendi Rabiner Heinzelman, and Hari Balakrishnan, *Negotiation-based Protocols for Disseminating Information in Wireless Sensor Networks*, Proceedings of 5th ACM/IEEE MobiCom Conference (MobiCom 1999), Seattle, WA, August, 1999

• http://w3.antd.nist.gov/wctg/manet/

• Deborah Estrin, Lewis Girod, Greg Pottie, Mani Srivastava, *Instrumenting the World with Wireless Networks*, in proceedings of the international Conference on Acoustics, Speech and Signal Processing (ICASSP 2001). Salt Lake City, Utah, May 2001.

• Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, *Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks*, In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networks (MobiCOM 2000), August 2000.

• Ian Akyildiz, Weilian Su, Yogesh Sankarasubramanian, Erdal Cayirci, "A Survey on Sensor Network," *IEEE Communications Magazines*, August, 2002.

• Budhaditya Deb, Sudeep Bhatnagar and Badri Nath, *A Topology Discovery Algorithm for Sensor Networks with Applications to Network Management*, in IEEE CAS workshop, September 2002.

About the authors

Malik Tubaishat currently is a Ph.D. student in the Department of Computer Science at the University of Missouri-Rolla. He received his master degree in Computer Science from the University Sains Malaysia, Malaysia in 2000. He obtained his BSc in Computer Science from Yarmouk University, Jordan in 1994. His research interests include self-organizing sensor networks, and routing protocols in sensor networks. He has published papers in International conferences and journals. Contact him at <mma882@umr.edu>.

Sanjay Kumar Madria is an Assistant Professor, Department of Computer Science, at the University of Missouri-Rolla, USA. Earlier he was Visiting Assistant Professor in the Department of Computer Science, Purdue University, West Lafayette, IN. He has widely published papers in journals and conferences in his areas of research interest that include sensor networking, mobile computing, web data management and transaction processing. He is an IEEE Senior Member. Contact him at <madrias@umr.edu>.