1

Motivation for a Network of Wireless Sensor Nodes

Sensors link the physical with the digital world by capturing and revealing real-world phenomena and converting these into a form that can be processed, stored, and acted upon. Integrated into numerous devices, machines, and environments, sensors provide a tremendous societal benefit. They can help to avoid catastrophic infrastructure failures, conserve precious natural resources, increase productivity, enhance security, and enable new applications such as context-aware systems and smart home technologies. The phenomenal advances in technologies such as very large scale integration (VLSI), microelectromechanical systems (MEMS), and wireless communications further contribute to the widespread use of distributed sensor systems. For example, the impressive developments in semiconductor technologies continue to produce microprocessors with increasing processing capacities, while at the same time shrinking in size. The miniaturization of computing and sensing technologies enables the development of tiny, low-power, and inexpensive sensors, actuators, and controllers. Further, embedded computing systems (i.e., systems that typically interact closely with the physical world and are designed to perform only a limited number of dedicated functions) continue to find application in an increasing number of areas. While defense and aerospace systems still dominate the market, there is an increasing focus on systems to monitor and protect civil infrastructure (such as bridges and tunnels), the national power grid, and pipeline infrastructure. Networks of hundreds of sensor nodes are already being used to monitor large geographic areas for modeling and forecasting environmental pollution and flooding, collecting structural health information on bridges using vibration sensors, and controlling usage of water, fertilizers, and pesticides to improve crop health and quantity.

This book provides a thorough introduction to the fundamental aspects of *wireless sensor networks* (WSNs), covering both theoretical concepts and practical aspects of network technologies and protocols, operating systems, middleware, sensor programming, and security. The book is targeted at researchers, students, and practitioners alike, with the goal of helping them to gain an understanding of the challenges and promises of this exciting field. It has been written primarily as a textbook for graduate or advanced undergraduate courses in wireless sensor networks. Each chapter ends with a number of exercises and questions that will allow students to practice the described concepts and techniques. As the field of wireless sensor networks is based on numerous other domains, it is recommended that

Fundamentals of Wireless Sensor Networks: Theory and Practice Waltenegus Dargie and Christian Poellabauer

students have taken courses such as networking and operating systems (or comparable courses) before they take a course on sensor networks. Also, some topics covered in this book (e.g., security) assume previous knowledge in other areas or require that an instructor provides an introduction into the basics of these areas before teaching these topics.

1.1 Definitions and Background

1.1.1 Sensing and Sensors

Sensing is a technique used to gather information about a physical object or process, including the occurrence of events (i.e., changes in state such as a drop in temperature or pressure). An object performing such a sensing task is called a *sensor*. For example, the human body is equipped with sensors that are able to capture optical information from the environment (eyes), acoustic information such as sounds (ears), and smells (nose). These are examples of *remote sensors*, that is, they do not need to touch the monitored object to gather information. From a technical perspective, a sensor is a device that translates parameters or events in the physical world into signals that can be measured and analyzed. Another commonly used term is *transducer*, which is often used to describe a device that converts energy from one form into another. A sensor, then, is a type of transducer that converts energy in the physical world into electrical energy that can be passed to a computing system or controller. An example of the steps performed in a sensing (or *data acquisition*) task is shown in Figure 1.1. Phenomena in the physical world (often referred to as *process*, *system*, or *plant*) are observed by a sensor device. The resulting electrical signals are often not ready for immediate processing, therefore they pass through a *signal conditioning* stage. Here, a variety of operations can be applied to the sensor signal to prepare it for further use. For example, signals often require amplification (or attenuation) to change the signal magnitude to better match the range of the following analog-to-digital conversion. Further, signal conditioning often applies *filters* to the signal to remove unwanted noise within certain frequency ranges (e.g., highpass filters can be used to remove 50 or 60 Hz noise picked up by surrounding power lines). After conditioning, the analog signal is transformed into a digital signal using an *analog-to-digital converter* (ADC). The signal is now available in a digital form and ready for further processing, storing, or visualization.

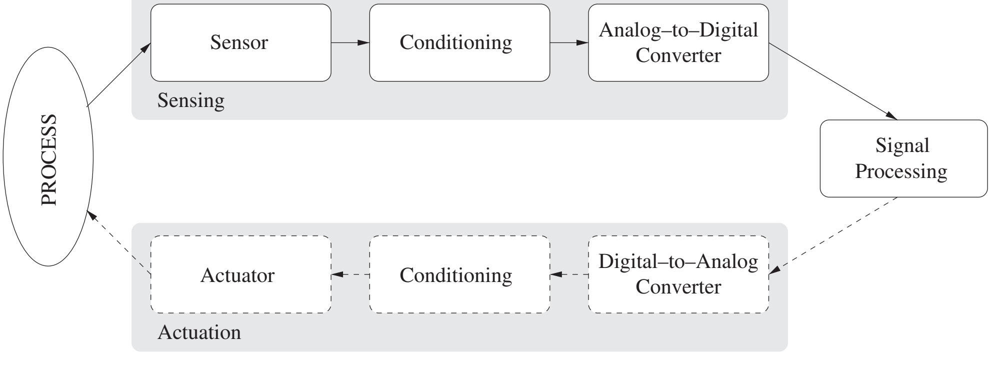

Figure 1.1 Data acquisition and actuation.

Many wireless sensor networks also include *actuators* which allow them to directly control the physical world. For example, an actuator can be a valve controlling the flow of hot water, a motor that opens or closes a door or window, or a pump that controls the amount of fuel injected into an engine. Such a *wireless sensor and actuator network* (WSAN) takes commands from the processing device (controller) and transforms these commands into input signals for the actuator, which then interacts with a physical process, thereby forming a closed control loop (also shown in Figure 1.1).

1.1.1.1 Sensor Classifications

Which sensors should be chosen for an application depends on the physical property to be monitored, for example, such properties include temperature, pressure, light, or humidity. Table 1.1 summarizes some common physical properties, including examples of sensing technologies that are used to capture them. Besides physical properties, the classification of sensors can be based on a variety of other methods, for example, whether they require an external power supply. If the sensors require external power, they are referred to as *active* sensors. That is, they must emit some kind of energy (e.g., microwaves, light, sound) to trigger a response or to detect a change in the energy of the transmitted signal. On the other hand, *passive* sensors detect energy in the environment and derive their power from this energy input – for example, passive infrared (PIR) sensors measure infrared light radiating from objects in the proximity.

The classification of sensors can also be based on the methods they apply and the electrical phenomena they utilize to convert physical properties into electrical signals. *Resistive* sensors rely on changes to a conductor's electrical resistivity, ρ, based on physical properties such as temperature. The resistance, R, of a conductor can be determined as:

$$R = \frac{l \times \rho}{A} \tag{1.1}$$

where l is the length of the conductor and A is the area of the cross-section. For example, the well-known Wheatstone bridge (Figure 1.2) is a simple circuit that can be used to convert a physical property into an observable electric effect. In this bridge, R_1, R_2, and R_3 are

Table 1.1 Classification and examples of sensors

Type	Examples
Temperature	Thermistors, thermocouples
Pressure	Pressure gauges, barometers, ionization gauges
Optical	Photodiodes, phototransistors, infrared sensors, CCD sensors
Acoustic	Piezoelectric resonators, microphones
Mechanical	Strain gauges, tactile sensors, capacitive diaphragms, piezoresistive cells
Motion, vibration	Accelerometers, gyroscopes, photo sensors
Flow	Anemometers, mass air flow sensors
Position	GPS, ultrasound-based sensors, infrared-based sensors, inclinometers
Electromagnetic	Hall-effect sensors, magnetometers
Chemical	pH sensors, electrochemical sensors, infrared gas sensors
Humidity	Capacitive and resistive sensors, hygrometers, MEMS-based humidity sensors
Radiation	Ionization detectors, Geiger–Mueller counters

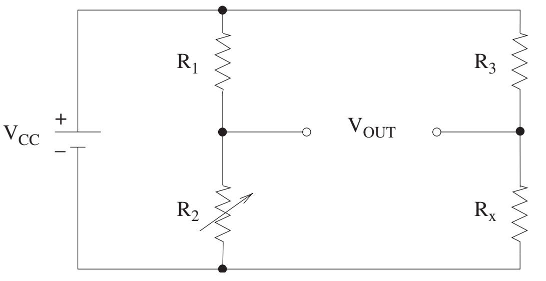

Figure 1.2 Wheatstone bridge circuit.

resistors of known resistance (where the resistance of R_2 is adjustable) and R_x is a resistor of unknown value. If the ratio R_2/R_1 is identical to the ratio R_x/R_3, the measured voltage V_{OUT} will be zero. However, if the resistance of R_x changes (e.g., due to changes in temperature), there will be an imbalance, which will be reflected by a change in voltage V_{OUT}. In general, the relationship between the measured voltage V_{OUT}, the resistors, and the supply voltage (V_{CC}) can be expressed as:

$$V_{OUT} = V_{CC} \times \left(\frac{R_x}{R_3 + R_x} - \frac{R_2}{R_1 + R_2} \right) \tag{1.2}$$

A similar principle can be applied to *capacitive* sensors, which can be used to measure motion, proximity, acceleration, pressure, electric fields, chemical compositions, and liquid depth. For example, in the parallel plate model, that is, a capacitor consisting of two parallel conductive plates separated by a dielectric with a certain permittivity ε, the capacitance is determined as:

$$C = \frac{\varepsilon \times A}{d} \tag{1.3}$$

where A is the plate area and d is the distance between the two plates. Similar to the resistive model, changes in any of these parameters will change the capacitance. For example, if pressure is applied to one of the two plates, the separation d can be reduced, thereby increasing the capacitance. Similarly, a change in the permittivity of the dielectric can be caused by an increase in temperature or humidity, thereby resulting in a change in capacitance.

Inductive sensors are based on the electrical principle of inductance, that is, where an electromagnetic force is induced by a fluctuating current. Inductance is determined by the dimensions of the sensor (cross-sectional area, length of coil), the number of turns of the coil, and the permeability of the core. Changes in any of these parameters (e.g., caused by movements of the core within the coil) change the inductance. Inductive sensors are often used to measure proximity, position, force, pressure, temperature, and acceleration.

Finally, *piezoelectric* sensors use the piezoelectric effect of some materials (e.g., crystals and certain ceramics) to measure pressure, force, strain, and acceleration. When a pressure is applied to such a material, it causes a mechanical deformation and a displacement of charges, proportional to the amount of pressure. The main advantage of piezoelectric devices over other approaches is that the piezoelectric effect is not sensitive to electromagnetic fields or radiation.

1.1.2 Wireless Sensor Networks

While many sensors connect to controllers and processing stations directly (e.g., using local area networks), an increasing number of sensors communicate the collected data wirelessly to a centralized processing station. This is important since many network applications require hundreds or thousands of sensor nodes, often deployed in remote and inaccessible areas. Therefore, a *wireless* sensor has not only a sensing component, but also on-board processing, communication, and storage capabilities. With these enhancements, a sensor node is often not only responsible for data collection, but also for in-network analysis, correlation, and fusion of its own sensor data and data from other sensor nodes. When many sensors cooperatively monitor large physical environments, they form a *wireless sensor network* (WSN). Sensor nodes communicate not only with each other but also with a *base station* (BS) using their wireless radios, allowing them to disseminate their sensor data to remote processing, visualization, analysis, and storage systems. For example, Figure 1.3 shows two *sensor fields* monitoring two different geographic regions and connecting to the Internet using their base stations.

The capabilities of sensor nodes in a WSN can vary widely, that is, simple sensor nodes may monitor a single physical phenomenon, while more complex devices may combine many different sensing techniques (e.g., acoustic, optical, magnetic). They can also differ in their communication capabilities, for example, using ultrasound, infrared, or radio frequency technologies with varying data rates and latencies. While simple sensors may only collect and communicate information about the observed environment, more powerful devices (i.e., devices with large processing, energy, and storage capacities) may also perform extensive processing and aggregation functions. Such devices often assume additional responsibilities in a WSN, for example, they may form communication backbones that can be used by other resource-constrained sensor devices to reach the

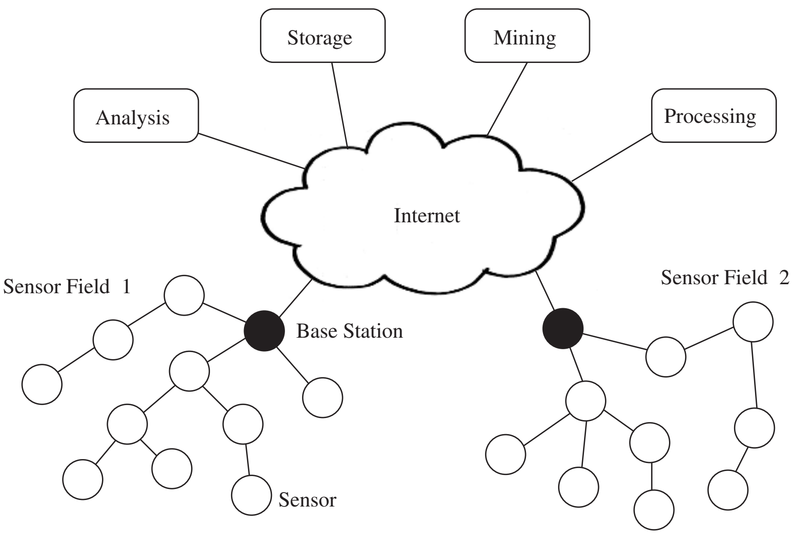

Figure 1.3 Wireless sensor networks.

base station. Finally, some devices may have access to additional supporting technologies, for example, Global Positioning System (GPS) receivers, allowing them to accurately determine their position. However, such systems often consume too much energy to be feasible for low-cost and low-power sensor nodes.

1.1.2.1 History of Wireless Sensor Networks

As with many other technologies, the military has been a driving force behind the development of wireless sensor networks. For example, in 1978, the Defense Advanced Research Projects Agency (DARPA) organized the Distributed Sensor Nets Workshop (DAR 1978), focusing on sensor network research challenges such as networking technologies, signal processing techniques, and distributed algorithms. DARPA also operated the Distributed Sensor Networks (DSN) program in the early 1980s, which was then followed by the Sensor Information Technology (SensIT) program.

In collaboration with the Rockwell Science Center, the University of California at Los Angeles proposed the concept of Wireless Integrated Network Sensors or WINS (Pottie 2001). One outcome of the WINS project was the Low Power Wireless Integrated Microsensor (LWIM), produced in 1996 (Bult *et al.* 1996). This smart sensing system was based on a CMOS chip, integrating multiple sensors, interface circuits, digital signal processing circuits, wireless radio, and microcontroller onto a single chip. The Smart Dust project (Kahn *et al.* 1999) at the University of California at Berkeley focused on the design of extremely small sensor nodes called *motes*. The goal of this project was to demonstrate that a complete sensor system can be integrated into tiny devices, possibly the size of a grain of sand or even a dust particle. The PicoRadio project (Rabaey *et al.* 2000) by the Berkeley Wireless Research Center (BWRC) focuses on the development of low-power sensor devices, whose power consumption is so small that they can power themselves from energy sources of the operating environment, such as solar or vibrational energy. The MIT μAMPS (micro-Adaptive Multidomain Power-aware Sensors) project also focuses on low-power hardware and software components for sensor nodes, including the use of microcontrollers capable of dynamic voltage scaling and techniques to restructure data processing algorithms to reduce power requirements at the software level (Calhoun *et al.* 2005).

While these previous efforts are mostly driven by academic institutions, over the last decade a number of commercial efforts have also appeared (many based on some of the academic efforts described above), including companies such as Crossbow (www.xbow.com), Sensoria (www.sensoria.com), Worldsens (http://worldsens.citi.insa-lyon.fr), Dust Networks (http://www.dustnetworks.com), and Ember Corporation (http://www.ember.com). These companies provide the opportunity to purchase sensor devices ready for deployment in a variety of application scenarios along with various management tools for programming, maintenance, and sensor data visualization.

1.1.2.2 Communication in a WSN

The well-known IEEE 802.11 family of standards was introduced in 1997 and is the most common wireless networking technology for mobile systems. It uses different frequency bands, for example, the 2.4-GHz band is used by IEEE 802.11b and IEEE 802.11g, while the IEEE 802.11a protocol uses the 5-GHz frequency band. IEEE 802.11 was frequently used in early wireless sensor networks and can still be found in current networks when bandwidth

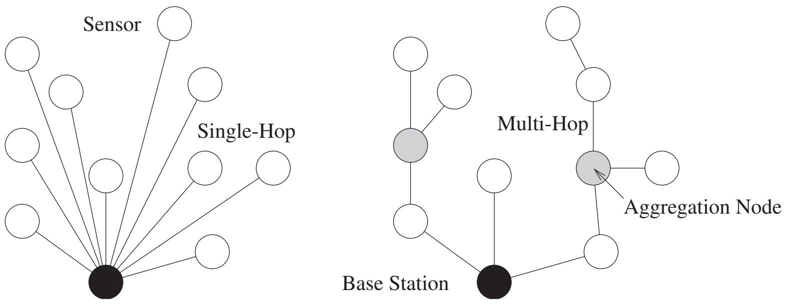

Figure 1.4 Single-hop versus multi-hop communication in sensor networks.

demands are high (e.g., for multimedia sensors). However, the high-energy overheads of IEEE 802.11-based networks makes this standard unsuitable for low-power sensor networks. Typical data rate requirements in sensor networks are comparable to the bandwidths provided by dial-up modems, therefore the data rates provided by IEEE 802.11 are typically much higher than needed. This has led to the development of a variety of protocols that better satisfy the networks' need for low power consumption and low data rates. For example, the IEEE 802.15.4 protocol (Gutierrez *et al.* 2001) has been designed specifically for short-range communications in low-power sensor networks and is supported by most academic and commercial sensor nodes.

When the transmission ranges of the radios of all sensor nodes are large enough and the sensors can transmit their data directly to the base station, they can form a star topology as shown on the left in Figure 1.4. In this topology, each sensor node communicates directly with the base station using a single hop. However, sensor networks often cover large geographic areas and radio transmission power should be kept at a minimum in order to conserve energy; consequently, *multi-hop communication* is the more common case for sensor networks (shown on the right in Figure 1.4). In this *mesh topology*, sensor nodes must not only capture and disseminate their own data, but also serve as *relays* for other sensor nodes, that is, they must collaborate to propagate sensor data towards the base station. This *routing* problem, that is, the task of finding a multi-hop path from a sensor node to the base station, is one of the most important challenges and has received immense attention from the research community. When a node serves as a relay for multiple routes, it often has the opportunity to analyze and pre-process sensor data in the network, which can lead to the elimination of redundant information or aggregation of data that may be smaller than the original data.

1.2 Challenges and Constraints

While sensor networks share many similarities with other distributed systems, they are subject to a variety of unique challenges and constraints. These constraints impact the design of a WSN, leading to protocols and algorithms that differ from their counterparts in other distributed systems. This section describes the most important design constraints of a WSN.

1.2.1 Energy

The constraint most often associated with sensor network design is that sensor nodes operate with limited energy budgets. Typically, they are powered through batteries, which must be either replaced or recharged (e.g., using solar power) when depleted. For some nodes, neither option is appropriate, that is, they will simply be discarded once their energy source is depleted. Whether the battery can be recharged or not significantly affects the strategy applied to energy consumption. For nonrechargeable batteries, a sensor node should be able to operate until either its *mission time* has passed or the battery can be replaced. The length of the mission time depends on the type of application, for example, scientists monitoring glacial movements may need sensors that can operate for several years while a sensor in a battlefield scenario may only be needed for a few hours or days.

As a consequence, the first and often most important design challenge for a WSN is energy efficiency. This requirement permeates every aspect of sensor node and network design. For example, the choices made at the physical layer of a sensor node affect the energy consumption of the entire device and the design of higher-level protocols (Shih *et al.* 2001). The energy consumption of CMOS-based processors is primarily due to switching energy and leakage energy (Sinha and Chandrakasan 2000):

$$E_{\mathrm{CPU}} = E_{\mathrm{switch}} + E_{\mathrm{leakage}} = C_{\mathrm{total}} V_{\mathrm{dd}}^2 + V_{\mathrm{dd}} I_{\mathrm{leak}} \Delta t \tag{1.4}$$

where C_{total} is the total capacitance switched by the computation, V_{dd} is the supply voltage, I_{leak} is the leakage current, and Δt is the duration of the computation. While the switching energy still dominates the energy consumption of processors, it is expected that in future processor designs, the leakage energy will be responsible for more than half the energy consumption (De and Borkar 1999). Some techniques to control leakage energy include progressive shutdown of idle components and software-based techniques such as Dynamic Voltage Scaling (DVS).

The medium access control (MAC) layer is responsible for providing sensor nodes with access to the wireless channel. Some MAC strategies for communication networks are *contention-based*, that is, nodes may attempt to access the medium at any time, potentially leading to collisions among multiple nodes, which must be addressed by the MAC layer to ensure that transmissions will eventually succeed. Downsides of these approaches include the energy overheads and delays incurred by the collisions and recovery mechanisms and that sensor nodes may have to listen to the medium at all times to ensure that no transmissions will be missed. Therefore, some MAC protocols for sensor networks are *contention-free*, that is, access to the medium is strictly regulated, eliminating collisions and allowing sensor nodes to shut down their radios when no communications are expected. The network layer is responsible for finding routes from a sensor node to the base station and route characteristics such as length (e.g., in terms of number of hops), required transmission power, and available energy on relay nodes determine the energy overheads of multi-hop communication.

Besides network protocols, the goal of energy efficiency impacts the design of the operating system (e.g., small memory footprint, efficient switching between tasks), middleware, security mechanisms, and even the applications themselves. For example, *in-network processing* is frequently used to eliminate redundant sensor data or to aggregate multiple sensor readings. This leads to a tradeoff between computation (processing the sensor data) and communication (transmitting the original versus the processed data), which can often be exploited to obtain energy savings (Pottie and Kaiser 2000; Sohrabi *et al.* 2000).

1.2.2 Self-Management

It is the nature of many sensor network applications that they must operate in remote areas and harsh environments, without infrastructure support or the possibility for maintenance and repair. Therefore, sensor nodes must be *self-managing* in that they configure themselves, operate and collaborate with other nodes, and adapt to failures, changes in the environment, and changes in the environmental stimuli without human intervention.

1.2.2.1 Ad Hoc Deployment

Many wireless sensor network applications do not require predetermined and engineered locations of individual sensor nodes. This is particularly important for networks being deployed in remote or inaccessible areas. For example, sensors serving the assessment of battlefield or disaster areas could be thrown from airplanes over the areas of interest, but many sensor nodes may not survive such a drop and may never be able to begin their sensing activities. However, the surviving nodes must autonomously perform a variety of setup and configuration steps, including the establishment of communications with neighboring sensor nodes, determining their positions, and the initiation of their sensing responsibilities. The mode of operation of sensor nodes can differ based on such information, for example, a node's location and the number or identities of its neighbors may determine the amount and type of information it will generate and forward on behalf of other nodes.

1.2.2.2 Unattended Operation

Many sensor networks, once deployed, must operate without human intervention, that is, configuration, adaptation, maintenance, and repair must be performed in an autonomous fashion. For example, sensor nodes are exposed to both system dynamics and environmental dynamics, which pose a significant challenge for building reliable sensor networks (Cerpa and Estrin 2004). A *self-managing* device will monitor its surroundings, adapt to changes in the environment, and cooperate with neighboring devices to form topologies or agree on sensing, processing, and communication strategies (Mills 2007). Self-management can take place in a variety of forms. Self-organization is the term frequently used to describe a network's ability to adapt configuration parameters based on system and environmental state. For example, a sensor device can choose its transmission power to maintain a certain degree of connectivity (i.e., with increasing transmission power it is more likely that a node will reach more neighbors). Self-optimization refers to a device's ability to monitor and optimize the use of its own system resources. Self-protection allows a device to recognize and protect itself from intrusions and attacks. Finally, the ability to self-heal allows sensor nodes to discover, identify, and react to network disruptions. In energy-constrained sensor networks, all these self-management features must be designed and implemented such that they do not incur excessive energy overheads.

1.2.3 Wireless Networking

The reliance on wireless networks and communications poses a number of challenges to a sensor network designer. For example, *attenuation* limits the range of radio signals, that is, a radio frequency (RF) signal fades (i.e., decreases in power) while it propagates through a medium and while it passes through obstacles. The relationship between the received power and transmitted power of an RF signal can be expressed using the *inverse-square law*:

$$P_{\mathrm{r}} \propto \frac{P_{\mathrm{t}}}{d^2} \tag{1.5}$$

which states that the received power P_{r} is proportional to the inverse of the square of the distance d from the source of the signal. That is, if P_{r}^x is the power at distance x, doubling the distance to $y = 2x$ decreases the power at the new distance to $P_{\mathrm{r}}^y = P_{\mathrm{r}}^x/4$.

As a consequence, an increasing distance between a sensor node and a base station rapidly increases the required transmission power. Therefore, it is more energy-efficient to split a large distance into several shorter distances, leading to the challenge of supporting *multi-hop* communications and routing. Multi-hop communication requires that nodes in a network cooperate with each other to identify efficient routes and to serve as relays. This challenge is further exacerbated in networks that employ *duty cycles* to preserve energy. That is, many sensor nodes use a power conservation policy where radios are switched off when they are not in use. As a consequence, during these down-times, the sensor node cannot receive messages from its neighbors nor can it serve as a relay for other sensors. Therefore, some networks rely on *wakeup on demand* strategies (Shih *et al.* 2002) to ensure that nodes can be woken up whenever needed. Usually this involves devices with two radios, a low-power radio used to receive wakeup calls and a high-power radio that is activated in response to a wakeup call. Another strategy is *adaptive duty cycling* (Ye *et al.* 2004), when not all nodes are allowed to sleep at the same time. Instead, a subset of the nodes in a network remain active to form a network backbone.

1.2.4 Decentralized Management

The large scale and the energy constraints of many wireless sensor networks make it infeasible to rely on *centralized* algorithms (e.g., executed at the base station) to implement network management solutions such as topology management or routing. Instead, sensor nodes must collaborate with their neighbors to make localized decisions, that is, without global knowledge. As a consequence, the results of these *decentralized* (or *distributed*) algorithms will not be optimal, but they may be more energy-efficient than centralized solutions. Consider routing as an example for centralized and decentralized solutions. A base station can collect information from all sensor nodes, establish routes that are optimal (e.g., in terms of energy), and inform each node of its route. However, the overhead can be significant, particularly if the topology changes frequently. Instead, a decentralized approach allows each node to make routing decisions based on limited local information (e.g., a list of the node's neighbors, including their distances to the base station). While this decentralized approach may lead to nonoptimal routes, the management overheads can be reduced significantly.

1.2.5 Design Constraints

While the capabilities of traditional computing systems continue to increase rapidly, the primary goal of wireless sensor design is to create smaller, cheaper, and more efficient devices.

Driven by the need to execute dedicated applications with little energy consumption, typical sensor nodes have the processing speeds and storage capacities of computer systems from several decades ago. The need for small form factor and low energy consumption also prohibits the integration of many desirable components, such as GPS receivers. These constraints and requirements also impact the software design at various levels, for example, operating systems must have small memory footprints and must be efficient in their resource management tasks. However, the lack of advanced hardware features (e.g., support for parallel executions) facilitates the design of small and efficient operating systems. A sensor's hardware constraints also affect the design of many protocols and algorithms executed in a WSN. For example, routing tables that contain entries for each potential destination in a network may be too large to fit into a sensor's memory. Instead, only a small amount of data (such as a list of neighbors) can be stored in a sensor node's memory. Further, while in-network processing can be employed to eliminate redundant information, some sensor fusion and aggregation algorithms may require more computational power and storage capacities than can be provided by low-cost sensor nodes. Therefore, many software architectures and solutions (operating system, middleware, network protocols) must be designed to operate efficiently on very resource-constrained hardware.

1.2.6 Security

Many wireless sensor networks collect sensitive information. The remote and unattended operation of sensor nodes increases their exposure to malicious intrusions and attacks. Further, wireless communications make it easy for an adversary to eavesdrop on sensor transmissions. For example, one of the most challenging security threats is a *denial-of-service* attack, whose goal is to disrupt the correct operation of a sensor network. This can be achieved using a variety of attacks, including a *jamming attack*, where high-powered wireless signals are used to prevent successful sensor communications. The consequences can be severe and depend on the type of sensor network application. While there are numerous techniques and solutions for distributed systems that prevent attacks or contain the extent and damage of such attacks, many of these incur significant computational, communication, and storage requirements, which often cannot be satisfied by resource-constrained sensor nodes. As a consequence, sensor networks require new solutions for key establishment and distribution, node authentication, and secrecy.

1.2.7 Other Challenges

From the discussion so far, it becomes clear that many design choices in a WSN differ from the design choices of other systems and networks. Table 1.2 summarizes some of the key differences between traditional networks and wireless sensor networks. A variety of additional challenges can affect the design of sensor nodes and wireless sensor networks. For example, some sensors may be mounted onto moving objects, such as vehicles or robots, leading to continuously changing network topologies that require frequent adaptations at multiple layers of a system, including routing (e.g., changing neighbor lists), medium access control (e.g., changing density), and data aggregation (e.g., changing overlapping sensing regions). A heterogeneous sensor network consists of devices with varying hardware

Table 1.2 Comparison of traditional networks and wireless sensor networks

Traditional networks	**Wireless sensor networks**
General-purpose design; serving many applications	Single-purpose design; serving one specific application
Typical primary design concerns are network performance and latencies; energy is not a primary concern	Energy is the main constraint in the design of all node and network components
Networks are designed and engineered according to plans	Deployment, network structure, and resource use are often ad hoc (without planning)
Devices and networks operate in controlled and mild environments	Sensor networks often operate in environments with harsh conditions
Maintenance and repair are common and networks are typically easy to access	Physical access to sensor nodes is often difficult or even impossible
Component failure is addressed through maintenance and repair	Component failure is expected and addressed in the design of the network
Obtaining global network knowledge is typically feasible and centralized management is possible	Most decisions are made localized without the support of a central manager

capabilities, for example, sensor nodes may have more hardware resources if their sensing tasks require more computation and storage or if they are responsible for collecting and processing data from other sensors within the network. Also, some sensor applications may have specific performance and quality requirements, for example, low latencies for critical sensor events or high throughput for data collected by video sensors. Both heterogeneity and performance requirements affect the design of wireless sensors and their protocols. Finally, while traditional computer networks are based on established standards, many protocols and mechanisms in wireless sensor networks are proprietary solutions, while standards-based solutions emerge only slowly. Standards are important for interoperability and facilitate the design and deployment of WSN applications; therefore, a key challenge in WSN design remains the standardization of promising solutions and the harmonization of competing standards.

Exercises

1.1 What is the difference between passive sensors and active sensors and can you name a few examples for each category (e.g., using Table 1.1)?

1.2 Consider a Wheatstone bridge circuit using a resistive temperature sensor R_x as shown in Figure 1.2. Further assume that $R_1 = 10\,\Omega$ and $R_3 = 20\,\Omega$. Assume that the current temperature is $80\,^\circ$F and $R_x(80) = 10\,\Omega$. You wish to calibrate the sensor such that the output voltage V_{OUT} is zero whenever the temperature is $80\,^\circ$F.

(a) What is the desired value of R_2?

(b) What is the output voltage (as a function of the supply voltage) at a temperature of $90\,^\circ$F, when this increase in temperature leads to an increase in resistance of 20% for R_x?

1.3 As described in this chapter, using multiple communication hops instead of a single hop affects the overall energy consumption. Describe other advantages or disadvantages of multi-hop communications, for example, in terms of performance (latency, throughput), reliability, and security.

1.4 The relationship between the transmitted and the received power of an RF signal follows the inverse-square law shown in Equation (1.5), that is, power density and distance have a quadratic relationship. This can be used to justify multi-hop communication (instead of single-hop), that is, energy can be preserved by transmitting packets over multiple hops at lower transmission power. Assume that a packet p must be sent from a sender A to a receiver B. The energy necessary to directly transmit the packet can be expressed as the simplified formula $E_{AB} = d(A, B)^2 + c$, where $d(x, y)$ (or simply d in the remainder of this question) is the distance between two nodes x and y and c is a constant energy cost. Assume that you can turn this single-hop scenario into a multi-hop scenario by placing any number of equidistant relay nodes between A and B.

(a) Derive a formula to compute the required energy as a function of d and n, where n is the number of relay nodes (that is, $n = 0$ for the single-hop case).

(b) What is the optimal number of relay nodes to send p with the minimum amount of energy required and how much energy is consumed in this optimal case for a distance $d(A, B) = 10$ and (i) $c = 10$ and (ii) $c = 5$?

1.5 Name at least four techniques to reduce power consumption in wireless sensor networks.

References

Bult, K., Burstein, A., Chang, D., Dong, M., Fielding, M., Kruglick, E., Ho, J., Lin, F., Lin, T.H., Kaiser, W.J., Marcy, H., Mukai, R., Nelson, P., Newburg, F.L., Pister, K.S.J., Pottie, G., Sanchez, H., Sohrabi, K., Stafsudd, O.M., Tan, K.B., Yung, G., Xue, S., and Yao, J. (1996) Low power systems for wireless microsensors. *Proc. of the International Symposium on Low Power Electronics and Design*.

Calhoun, B.H., Daly, D.C., Verma, N., Finchelstein, D.F., Wentzloff, D.D., Wang, A., Cho, S.H., and Chandrakasan, A.P. (2005) Design considerations for ultralow energy wireless microsensor nodes. *IEEE Transactions on Computers* **54** (6), 727–749.

Cerpa, A., and Estrin, D. (2004) Ascent: Adaptive self-configuring sensor network topologies. *IEEE Transactions on Mobile Computing* **3** (3), 272–285.

DAR (1978) *Proceedings of the Distributed Sensor Nets Workshop*. Pittsburgh, PA, Department of Computer Science, Carnegie Mellon University.

De, V., and Borkar, S. (1999) Technology and design challenges for low power and high performance. *Proc. of the International Symposium on Low Power Electronics and Design (ISLPED)*.

Gutierrez, J.A., Naeve, M., Callaway, E., Bourgeois, M., Mitter, V., and Heile, B. (2001) IEEE 802.15.4: A developing standard for low-power low-cost wireless personal area networks. *IEEE Network* **15** (5), 12–19.

Kahn, J.M., Katz, R.H., and Pister, K.S.J. (1999) Mobile networking for smart dust. *Proc. of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*.

Mills, K.L. (2007) A brief survey of self-organization in wireless sensor networks. *Wireless Communications and Mobile Computing* **7** (7), 823–834.

Pottie, G.J. (2001) Wireless integrated network sensors (WINS): The web gets physical. *National Academy of Engineering: The Bridge* **31** (4), 22–27.

Pottie, G.J., and Kaiser, W.J. (2000) Wireless integrated network sensors. *Communications of the ACM*.

Rabaey, J., Ammer, J., da Silva, Jr J.L., and Patel, D. (2000) Picoradio: Ad hoc wireless networking of ubiquitous low-energy sensor/monitor nodes. *Proc. of the IEEE Computer Society Annual Workshop on VLSI.*

Shih, E., Bahl, P., and Sinclair, M. (2002) Wake-on wireless: An event driven energy saving strategy for battery operated devices. *Proc. of the ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom)*.

Shih, E., Cho, S.H., Ickes, N., Min, R., Sinha, A., Wang, A., and Chandrakasan, A. (2001) Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks. *Proc. of the 7th Annual International Conference on Mobile Computing and Networking*.

Sinha, A., and Chandrakasan, A.P. (2000) Energy aware software. *Proc. of the 13th International Conference on VLSI Design*.

Sohrabi, K., Gao, J., Ailawadhi V., and Pottie, G. (2000) Protocols for self-organization of a wireless sensor network. *IEEE Personal Communications Magazine* **7** (5), 16–27.

Ye, W., Heidemann, J., and Estrin, D. (2004) Medium access control with coordinated adaptive sleeping for wireless sensor networks. *IEEE/ACM Transactions on Networking* **12** (3), 493–506.