3

BASIC WIRELESS SENSOR TECHNOLOGY

3.1 INTRODUCTION

In this chapter we look at basic sensor node systems technology at several levels. First, we focus on the sensor node technology itself (Section 3.2), providing a survey of sensor technology, including a taxonomy that classifies devices in families, such as large sensors (e.g., radar sensors), microsensors (tiny sensors), nanosensors, tag-reading sensors, and other sensors (Section 3.3). As already noted, WSNs are characterized by the fact that they need to operate in resource-constrained environments; in turn, this fact imposes strict design guidelines and limitations on the WNs; to this end, we address sensor functionality and components, including the sensing and actuation unit, processing unit, communication unit, power unit, and other application-dependent units. Second, we look at fundamental networking and topological issues (Section 3.4). Building on the introduction provided herein, these issues are revisited in more detail in subsequent chapters. Finally, we look at some current research trends in sensor technology (Section 3.5).

The terms *sensor node*, *wireless node* (WN), *Smart Dust*, *mote*, and *COTS* (commercial off-the-shelf) *mote* are used somewhat interchangeably in the industry; the most general terms used here are *sensor node* and *WN*.

Wireless Sensor Networks: Technology, Protocols, and Applications, by Kazem Sohraby, Daniel Minoli, and Taieb Znati
Copyright © 2007 John Wiley & Sons, Inc.

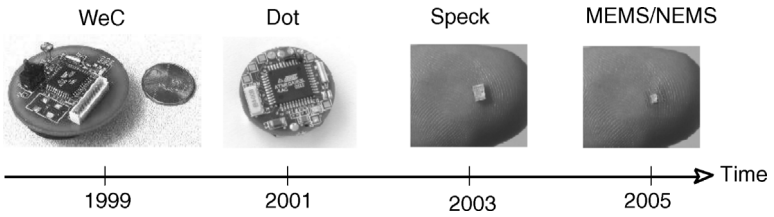

Figure 3.1 Progression of sensor technology (motes) over time (partial sample). (WeC and Dot motes: from Seth Hollar, Kris Pister, and James McClurkin, UC–Berkeley; speck motes: from SpeckNet Consortium/Scottish Higher Education Funding Council; MEMS/NEMS: authors' synthesis.)

3.2 SENSOR NODE TECHNOLOGY

3.2.1 Overview

As we saw in earlier chapters, a WSN consists of a group of dispersed sensors (motes) that have the responsibility of covering a geographic area (the sensor field) in terms of some measured parameter (also known as the measurand); alternatively, a sensor supports a point-to-point link in which the ''reader'' end is attached to a wireline network (e.g., a stationary tag reader sensing a mobile tag). Sensor nodes have wireless communication capabilities and some logic for signal processing, topology management (if and where applicable), and transmission handling (including digital encoding and possibly encryption and/or forward error correction). Figure 3.1 depicts the progression of sensor technology over time during the past few years. WSNs that combine physical sensing of parameters such as temperature, light, or seismic events with computation and networking capabilities are expected to become ubiquitous in the future [3.3]. Successful development of low-cost robust miniaturized sensors and detection equipment (such as mass spectrometers and chromatographs) will be of benefit; design of such systems is now being encouraged by U.S. research agencies (e.g., the National Science Foundation) [3.5]. Some sensor applications also support e-money purchases at point-of-sale locations such as from soft-drink machines, kiosks, gas stations, and checkout counters.

At the design level a WSN sits at the confluence of research in disciplines such as database query processing, networking, algorithms, and distributed systems [3.3]; hence, a lot of thought and engineering go into the development of both WNs and WSNs. The basic functionality of a WN generally depends on the application, but the following requirements are typical [3.4]:

1. Determine the value of a parameter at a given location. For example, in an environment-oriented WSN, one might need to know the temperature, atmospheric pressure, amount of sunlight, and the relative humidity at a number of locations. This example shows that a given WN may be connected to different types of sensors, each with a different sampling rate and range of allowed values.

2. Detect the occurrence of events of interest and estimate the parameters of the events. For example, in a traffic-oriented WSN, one would like to detect a vehicle moving through an intersection and estimate the speed and direction of the vehicle.
3. Classify an object that has been detected. For example, is a vehicle in a traffic sensor network a car, a minivan, a light truck, a bus?
4. Track an object. For example, in a military WSN, track an enemy tank as it moves through the geographic area covered by the network.

Naturally, the data collected must be transmitted to the appropriate data-consumption entity in a timely fashion. In many cases there are real-time or near-real-time requirements; for example, the detection of an intruder should be communicated to the police in real time so that relevant action can be taken promptly.

As noted in Chapter 1, sensors are either passive or active devices. Passive sensors in single-element form include, among others, seismic-, acoustic-, strain-, humidity-, and temperature-measuring devices. Passive sensors in array form include optical- (visible, infrared 1 μm, infrared 10 μm) and biochemical-measuring devices. Arrays are geometrically regular clusters of WNs (e.g., following some topographical grid arrangement). Passive sensors tend to be low-energy devices. Active sensors include radar and sonar; these tend to be high-energy systems.

Sensing principles include, but are not limited to, mechanical, chemical, thermal, electrical, chromatographic, magnetic, biological, fluidic, optical, ultrasonic, and mass sensing. WNs may be exposed to hostile environments; the environment may include high temperatures, high vibration or noise levels, or corrosive chemicals. WNs may be incorporated in mobile robotic systems; they could also be integral to manufacturing systems. As discussed in Chapter 1, *embedded sensing* refers to the synergistic incorporation of microsensors in structures or environments; embedded sensing enables spatially and temporally dense monitoring of the system under consideration (e.g., an environment, a building, a battlefield). In biological systems, the sensors themselves must not affect the system or organism adversely [3.5]. The technology for sensing and control includes electric and magnetic field sensors; radio-wave frequency sensors; optical-, electrooptic-, and infrared sensors; radars; lasers; location and navigation sensors; seismic and pressure-wave sensors; environmental parameter sensors (e.g., wind, humidity, heat); and biochemical national security–oriented sensors. Typical sensor parameters (measurands) include:

- *Physical measurement.* Examples include two-axis magnetometers; light and ultraviolet intensity (photo resistor); radiation levels, radio, and microwave; humidity, temperature (thermistor), atmospheric pressure, fog, and dust; sound and acoustics; two-axis accelerometers, shock wave, seismic, physical pressure, and motion; video and image (visible or infrared); and location (GPS) and locomotion measurements.
- *Chemical and biological measurements.* Examples include the presence or concentration of a substance or agent at specified concentration levels (there are no less than 50 biological agents of interest [3.9]).

- *Event measurement.* Examples include determination of the occurrence of human-made or natural events, including cyber-level events; tracking of internal and external events.

Small, low-cost, robust, reliable, and sensitive sensors are needed to enable the realization of practical and economical sensor networks. Although a large number measurands are of interest for WSN applications, commercially available sensors exist for many of these measurands; one prominent exception is that a wide range of appropriate chemical sensors is not yet broadly available [3.8].

Sensor nodes come in a variety of hardware configurations: from nodes connected to a LAN and attached to permanent power sources, to nodes communicating via wireless multihop RF radio powered by small batteries [3.3]. The trend is toward very large scale integration (VLSI), integrated optoelectronics, and nanotechnology; in particular, work is under way in earnest in the biochemical arena. The goal of recent research and engineering is to build cubic millimeter (mm^3)–scale advanced WNs and motes. As shown in Figure 3.1, motes developed in the early 2000s were on the order of a cubic inch (this is approximately 16,387 mm^3). By 2007, researchers expect to have 1-mm^3 nodes able to operate in a functional network (e.g., SpeckNet research [3.1]).

3.2.2 Hardware and Software

Related to WN design, the following functionality typically needs to be supported: intrinsic node functionality; signal processing, including digital signal processing (e.g., FFT/DCT), compression, forward error correction, and encryption; control and actuation; clustering and in-network computation; self-assembly; communication; routing and forwarding; and connectivity management. To support this functionality, the hardware components of a WN include the sensing and actuation unit (single element or array), the processing unit, the communication unit, the power unit, and other application-dependent units. Figure 3.2 (which builds on Figure 1.3) shows hardware and software components of a typical sensing node.

As we noted in Chapter 1, the following are important sensor-node issues (refer to Table 1.1): sensor type, sensor power consumption, operating environment, computational and sensing capabilities, signal-processing capabilities, connectivity, and telemetry and control of remote devices. Clearly, the sensor node architecture, scope, and complexity depend on the application. Table 2.1 identified over 200 applications, many of which probably have their own sensor technology.

Sensors, particularly Smart Dust and COTS motes [3.2], have four basic hardware subsystems:

1. *Power.* An appropriate energy infrastructure or supply is necessary to support operation from a few hours to months or years (depending on the application).

2. *Computational logic and storage.* These are used to handle onboard data processing and manipulation, transient and short-term storage, encryption, forward

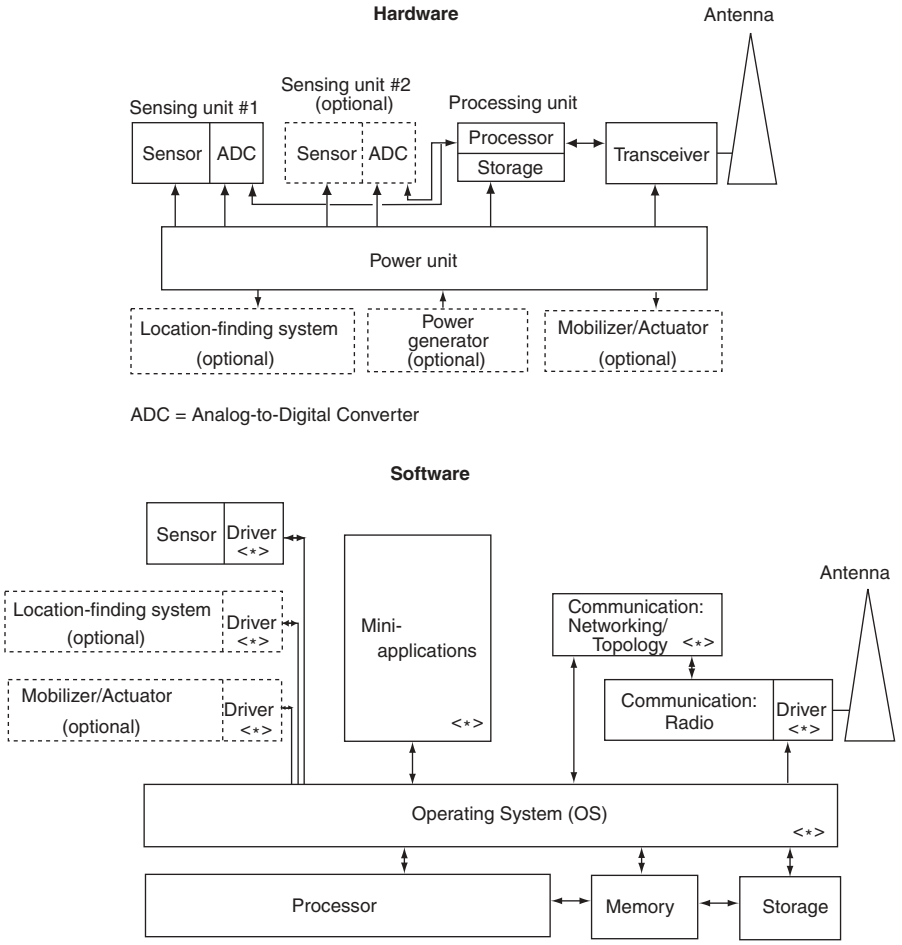

Figure 3.2 Hardware and software components of WNs.

error correction (FEC), digital modulation, and digital transmission. WNs have computational requirements typically ranging from an 8-bit microcontroller to a 64-bit microprocessor. Storage requirements typically range from 0.01 to 100 gigabytes (GB).

3. *Sensor transducer(s).* The interface between the environment and the WN is the sensor. Basic environmental sensors include, but are not limited to, acceleration, humidity, light, magnetic flux, temperature, pressure, and sound.

4. *Communication.* WNs must have the ability to communicate either in C1WSN arrangements (mesh-based systems with multihop radio connectivity among or between WNs, utilizing dynamic routing in both the wireless and wireline portions

of the network), and/or in C2WSN arrangements (point-to-point or multipoint-to-point systems generally with single-hop radio connectivity to WNs, utilizing static routing over the wireless network with only one route from the WNs to the companion terrestrial or wireline forwarding node). Researchers have developed many protocols specifically for WSNs. Transmission range, transmission impairments, modulation techniques, routing, and network topologies are issues of interest. Distances range from a few meters to a few kilometers; lower-layer communication protocols tend to be of the IEEE 802.11/802.15/802.16 class, although other methods have also been used. Throughput ranges from 10 to 256 kbps in most applications (some of the video-based application may require more bandwidth).

Sensors typically have five basic software subsystems:

1. *Operating system (OS) microcode* (also called *middleware*). This is the board-common microcode that is used by all high-level node-resident software modules to support various functions. As is generally the case, the purpose of an operating system is to shield the software from the machine-level functionality of the microprocessor. It is desirable to have *open-source operating systems* designed specifically for *WSNs*; these OSs typically utilize an architecture that enables rapid implementation while minimizing code size. TinyOS is one such example of a commonly used OS.

2. *Sensor drivers.* These are the software modules that manage basic functions of the sensor transceivers; sensors may possibly be of the modular/plug-in type, and depending on the type and sophistication, the appropriate configuration and settings must be uploaded into the sensor (drivers shield the application software from the machine-level functionality of the sensor or other peripheral).

3. *Communication processors.* This code manages the communication functions, including routing, packet buffering and forwarding, topology maintenance, medium access control (e.g., contention mechanisms, direct-sequence spread-spectrum mechanisms), encryption, and FEC, to list a few (e.g., see Figure 3.3).

4. *Communication drivers* (encoding and the physical layer). These software modules manage the minutia of the radio channel transmission link, including clocking and synchronization, signal encoding, bit recovery, bit counting, signal levels, and modulation.

5. *Data processing mini-apps.* These are numerical, data-processing, signal-value storage and manipulations, or other basic applications that are supported at the node level for in-network processing.

3.3 SENSOR TAXONOMY

Because of the variety of sensor types (sensor systems) that exist, a taxonomy is useful. The taxonomy in Table 3.1 is, in effect, an elaboration of Table 1.1. This

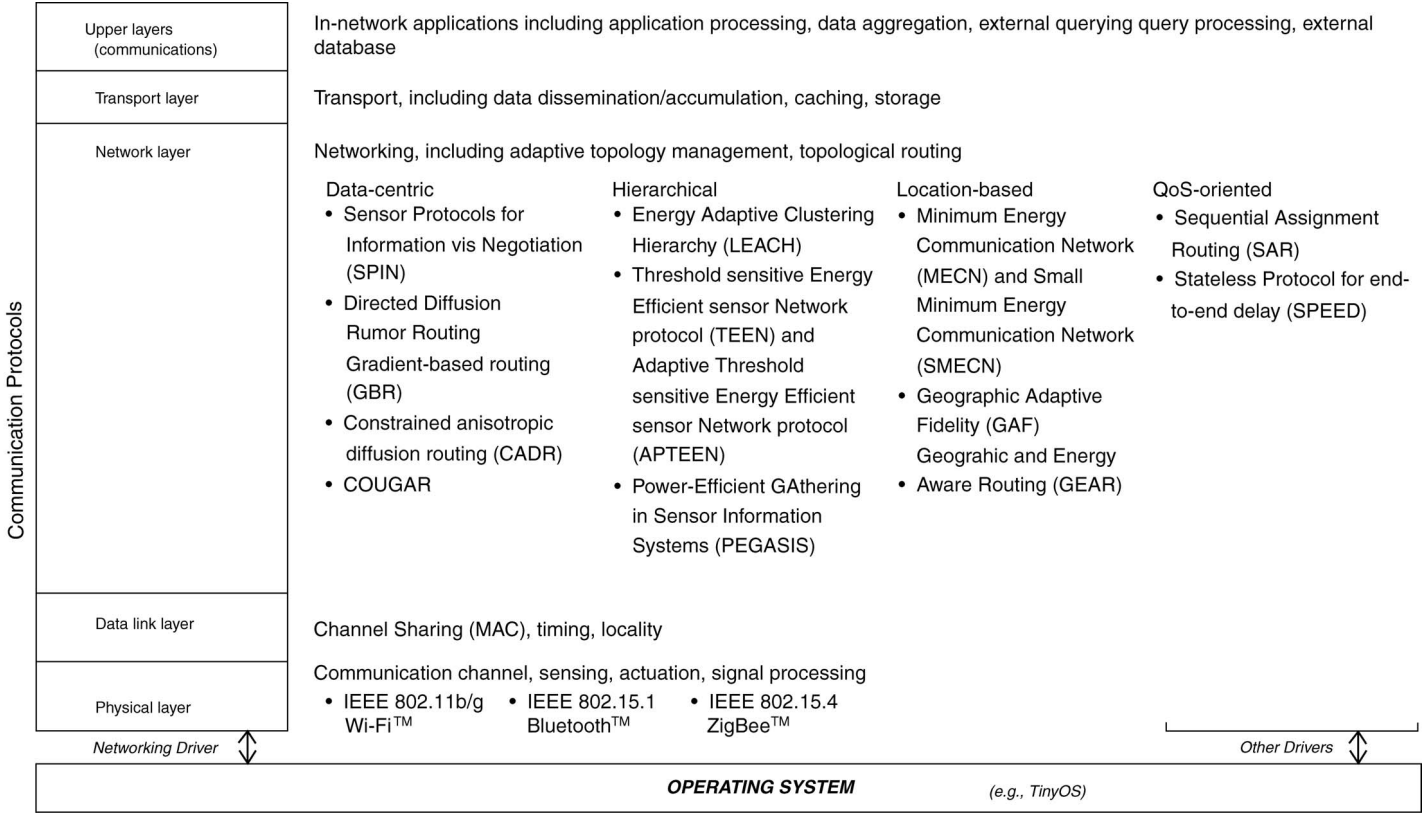

Figure 3.3 Some of the networking protocols supported by WNs.

TABLE 3.1 Basic Taxonomy of Sensor Nodes

Size of Sensor	Mobility of Sensor	Power of Sensor	Computation Logic; Storage Capability of Sensor	Sensor Mode	Communication Apparatus; Lower-Layer Protocols	Communication Apparatus; Upper-Layer Protocols
Very large (10^3 mm^3)	Fully mobile at deployment; fully mobile postdeployment	Self-replenishable, continuous	High-end processor (e.g., 64-bit micro); high-end storage (e.g., 100 GB)	High-end multimodal; physics	Multihop/mesh; hops in 10^1–10^2 m; IEEE MAC	Dynamic routing; data-centric
Large (10^2 mm^3)	Fully mobile at deployment; semimobile postdeployment	Self-replenishable, sporadic	Midrange processor (e.g., 16- or 32-bit micro); high-end storage	High-end multimodal; chemistry–biology	Multihop/mesh; hops in 10^2 to 10^4 m; IEEE MAC	Dynamic routing; hierarchical
Medium (10^1 mm^3)	Fully mobile at deployment; immobile postdeployment	Battery, 10^1 hours	Low-end processor (e.g., 8-bit micro); high-end storage	High-end multimodal; physics–chemistry–biology	Multihop/mesh; hops in 10^4 or more meters; IEEE MAC	Dynamic routing; location-based
Small (10^0 mm^3)	Semimobile at deployment; fully mobile postdeployment	Battery, 10^2 hours	High-end processor (e.g., 64-bit micro); midrange storage (e.g., 1 GB)	Midrange multimodal; physics	Multihop/mesh; hops in 10^1 to 10^2 m; special MAC	Dynamic routing; QOS-based

Very small (10^{-1} mm^3)	Semimobile at deployment; semimobile postdeployment	Battery, 10^3 hours	Midrange processor (e.g., 16- or 32-bit micro); midrange storage	Midrange multimodal; chemistry–biology	Multihop/mesh; hops in 10^2 to 10^4 m; special MAC	Static routing (single hop)
Ultrasmall (10^{-2} mm^3)	Semimobile at deployment; immobile postdeployment	Battery, 10^4 hours	Low-end processor (e.g., 8-bit micro); Midrange storage	Midrange multimodal; physics–chemistry–biology	Multihop/mesh; hops in 10^4 or more meters; special MAC	
Microscale (10^{-3} mm^3)	Immobile at deployment; fully mobile postdeployment	Battery, 10^5 hours	High-end processor (e.g., 64-bit micro); low-end storage (e.g., 0.01 GB)	Single function; physics	Single hop; hops in 10^1 to 10^2 m; IEEE MAC	
Nanoscale ($<10^{-4}$ mm^3)	Immobile at deployment; semimobile postdeployment		Midrange processor (e.g., 16- or 32-bit micro); low-end storage	Single function; chemistry–biology	Single hop; hops in 10^2 to 10^4 m; IEEE MAC	
	Immobile at deployment; immobile postdeployment		Low-end processor (e.g., 8-bit micro); low-end storage	Single function; physics–chemistry–biology	Single hop; hops in 10^4 or more meters; IEEE MAC Single hop; special MAC	

TABLE 3.2 Reduced-Complexity Taxonomy of Sensor Nodes

Size of Sensor, s	Mobility of Sensor, m	Power of Sensor, p	Computation Logic and Storage Capability of Sensor, cp	Sensor Mode, md	Communication Apparatus or Protocols of Sensor, cm
1 Large	1 Mobile	1 Self-replenishable	1 High-end processor and storage	1 Multimodal, physics	1 Multihop/mesh with dynamic routing
2 Small	2 Static	2 Battery, hours–days	2 Midrange processor and storage	2 Multimodal, chemistry/biology	2 Single hop with static routing
3 Microscopic		3 Battery, weeks–months	3 Low-end processor and storage	3 Single function, physics	
4 Nanoscopic		4 Battery, years		4 Single function, chemistry–biology	

taxonomy is somewhat daunting since there are $8 \times 9 \times 7 \times 9 \times 9 \times 10 \times 5 =$ 2,041,200 cases or combinations. However, the classification "buckets" are reasonable, and a large majority of the combinatorial combinations are, in fact, valid. To reduce the scope of the taxonomy, we suggest the use of the modified classification shown in Table 3.2; here one has only $4 \times 2 \times 4 \times 3 \times 4 \times 2 = 768$ cases or combinations. For example, a s(2)m(2)p(3)cp(2)md(1)cm(1) WN is a system that is small, static, battery-powered, has multiple measurands, and supports multihop networking.

3.4 WN OPERATING ENVIRONMENT

As we saw in Chapter 1, networking implies a need to support physical and logical connectivity. In WSNs, physical connectivity is supported over a wireless radio link of one or more hops, at a distance of tens, hundreds, or thousand of meters. Logical connectivity has the goal of supporting topology maintenance and multihop routing (when present). The design and engineering of WNs clearly needs to take into account all the issues described in Section 3.2 as well as in this section.

Sensor nodes have to deal with the following resource constraints [3.3] (see also Table 3.3):

- *Power consumption.* Almost invariably, WNs have a limited supply of operating energy; it follows that energy conservation is a key system design consideration.
- *Communication.* The wireless network usually has limited bandwidth; the networks may be forced to utilize a noisy channel; and the communication channel may be relegated to an unprotected frequency band. The implications

TABLE 3.3 Design Constraints or Requirements for WSNs and WNs

WSN/WN Requirement	Motivation
Collaborative data processing	A factor that distinguishes WSNs from simple ad hoc networks is that the goal in WSNs is detection or estimation of specified events, not just communications. One needs to provide scalable, fault-tolerant, flexible data access and intelligent data reduction [3.3]. This drives the overall architecture because detection and estimation often require fusing data from multiple sensors; data fusion requires the transmission of data and control messages. Quantification of sensor data, including limits of detection, calibration, interferences, sampling, and verification of accuracy, also needs to be taken into account [3.5].
Constrained energy use	In many applications the WNs are deployed in remote areas; in these cases, the lifetime of a node may be determined by the battery life; this in turn requires a minimization of energy consumption.
Large topology support	Networks of 10,000 or even 100,000 nodes are envisioned for some applications. Fortunately, most WSNs/WNs are stationary (aside from the deployment of sensors on the ocean surface or the use of mobile, unmanned, robotic sensors in military operations).
Querying capabilities	A data-consumption entity may need to query an individual node or group of nodes for information collected in the region. Because it may not be feasible to transmit a large amount of the data across a network, various local sink nodes need to collect the data from a given area and create summary messages to reply to the query.
Self-organization	It is typically a requirement that WSNs be able to self-organize: Given the large number of nodes and their potential placement in hostile locations, manual configuration is typically not feasible. Also, nodes may fail (from lack of energy or from physical destruction), and new nodes may join the network: the network must be able to reconfigure itself so that it can continue to operate properly and support reliable connectivity.

Source: Adapted from [3.4].

are limited reliability, poor quality of service (e.g., high latency, high variance, high frame loss), and security exposure (e.g., denial of service, jamming, interference, high bit-error rates).

- *Computation.* WNs typically have limited computing power and memory resources. The implications are restrictions on the types of data-processing algorithms that can run on a sensor node. This also limits the scope and

volume of intermediate results that can be stored in the WNs. Research aims at developing a distributed data management layer that scales with the growth of sensor interconnectivity and computational power on the sensors; the goal is to deploy mechanisms that reside directly on the sensor nodes and create the abstraction of a single processing node without centralizing data or computation.

- *Uncertainty in measured parameters.* Signals that have been often have various detected or collected degrees of intrinsic uncertainty. Desired data may be commingled with noise and/or interference from the environment. Node malfunction could collect and/or forward inaccurate data. Node placement (particularly in ad hoc networks without mobility) may impair operation and bias individual readings.

Some of the intrinsic factors that the design constraints or requirements that WSNs and WNs need to take into account include the following:

- WNs may be deployed in a dense manner (close proximity), implying communication complexity (e.g., in support of packet forwarding and topology management)
- For military and/or national security applications, WNs need to support rapid deployment; the deployment must be supportable in an ad hoc fashion; and the environment is expected to be highly dynamic.
- WNs may be prone to failure. Unattended, untethered, self-powered low-duty-cycle systems are typical, yet some WSNs require sensing systems that are long-lived and environmentally resilient.
- As just noted, WNs are limited in power, computational capacity, and memory. Communication circuitry and antennas are the primary elements that use up most of the energy.
- The topology that the WNs need to maintain may change very frequently. Communication links may be expensive (not only from an electromagnetic spectrum perspective, but also in terms of the operational support of the requisite infrastructure); the bandwidth may be limited; and as just noted, the power availability at the sensor may be limited and/or expensive in reference to supporting a high-capacity, high-range link (i.e., to feed a high-power antenna).
- WNs may not have global addresses because of the potentially large number of sensors and overhead needed to support such global addresses (IPv6 could be applicable in this context).
- WNs require special routing and data dissemination mechanisms (e.g., data-centric, hierarchical, and/or location-based routing).
- WNs often require in-network processing, even while the data are being routed. One wants to be able to perform data processing in the network in the proximity of the source of the data, and then forward only summarized,

aggregated, fused, and/or synthesized results. Typical functionality involves signal processing, data aggregation, data fusion, and data analysis. There is also an interest in database management, including querying mechanisms and data storage and warehousing.

- Arrays of ultralow-power wireless nodes may be incorporated in reconfigurable networks with high-speed connectivity to processing centers for decision and responsive action [3.5].

3.5 WN TRENDS

For WSNs to achieve wide-scale deployment, the size, cost, and power consumption of the nodes must decrease considerably and the intelligence of the WNs must increase [3.6]. To meet evolving functional requirements of the various user communities, it will be necessary for sensor systems to leverage and incorporate advances in adjacent technologies, such as nanofabrication, biosystems, massively distributed networks, ubiquitous computing, broadband wireless communications, and information and decision systems [3.5].

Evolving requirements for new WSNs and WNs include, among others: (1) the ability to respond to new toxic chemicals, explosives, and biological agents; (2) enhanced sensitivity, selectivity, speed, robustness, and fewer false alarms; and (3) the ability to function, perhaps autonomously, in unusual, extreme, and complex environments. These needs can be addressed by the design and synthesis of functionalized receptors and materials, resulting in next-generation devices. The materials may be of varying porosity, enabling them to detect single toxic compounds in complex mixtures or physical configurations that have surfaces with microchannels for microfluidic discrimination. Advanced biological, chemical, and materials research can be brought to bear on this challenge, including the design of functional nano- and mesoscale complex structures (e.g., quantum dots, nanowires, gels). Robustness under anticipated manufacturing schemes is also required [3.5].

Miniaturization, manufacturability, and cost are also critical issues. Integration of sensors, processors, energy sources, and the communications network interface on a chip would facilitate the exchange of sensor data and critical information with the outside world. Information extraction may involve detection of events or objects of interest, estimation of key parameters, and human-in-the-loop or closed-loop adaptive feedback [3.5]. Some of the goals (e.g., as defined by the PicoRadio effort at UC–Berkeley [3.7]) are to develop mesoscale low-cost (i.e., $<$50 cents) transceivers for ubiquitous wireless data acquisition that minimize power or energy dissipation [i.e., minimize energy ($<$5 nJ/(correct) bit)] for an energy-limited source and minimize power (i.e., $<$100 μW for a power-limited source, enabling energy scavenging) by using the following strategies: self-configuring networks, fluid trade-off between communication and computation, an integrated system-on-a-chip (SOC) approach, and aggressive low-energy architectures and circuits.

Standardization is important. As the definition of sockets has made the use of communication services on the Internet independent of the underlying protocol stack, communication medium, and even operating system, the application interface one needs for WSNs should be an abstraction that is offered to any sensor network application and supported by any sensor network platform [3.7]. Research and engineering activity now under way seeks to advance fundamental knowledge in new sensor technologies, including sensors for toxic chemicals, explosives, and biological agents; sensor networking systems in a distributed environment; the integration of sensors into commercial systems; and the interpretation and use of sensor data in decision-making processes [3.5]. Table 3.4 provides a partial list of near-term research efforts as sponsored by U.S. government agencies.

Of late, one has seen targeted efforts to develop chemical sensors for sensor networks, particularly for monitoring soil contamination and for habitat monitoring. Specifically, one needs an array of miniaturized chemical sensors to monitor the flow of contaminants accurately (e.g., see Figure 3.4). Optimally, one is interested in developing microscale liquid chromatography systems [3.8]. According to published reports, the U.S. Department of Homeland Security (DHS) is coordinating an effort for the end-of-decade deployment of a nationwide sensor network to provide a real-time early-warning system for a plethora of chemical, biological, and nuclear threats across the United States. Planners at DHS are working on developing capabilities to deal with multifaceted threats targeted at airports, subways, and buildings; they are also looking at issues related to water sources, animal herds, and flocks of birds that could spread contaminants or harmful biological agents. This type of technology is currently under development [3.9].

National research laboratories have been working on core issues in materials, sensors, networks, and electronics, and have already established field trials of prototype networks. The multifaceted nature of the global threat has led researchers to consider a system that consists of a suite of different types of sensors. Researchers are planning to use MEMSs and nanotechnology for low-cost, high-reliability, and high-accuracy biological and chemical sensors. In one approach, researchers are studying hybrid sensors that use surface-chemical detection as a first trigger, which could then use technology on the same device for more time-consuming techniques, such as DNA testing. Other researchers are studying the use of infrared or ultraviolet spectrum analysis as well as biometric sensors that mimic human cells to create test reactions. Further into the future, MEMS technology is seen as having promise for creating miniature benchtop labs on a chip. Sensors could use polymer- or gel-coated silicon devices to trap targeted chemicals, then send the agents through fluidic channels to on-chip arrays of surface-acoustic-wave detectors. A follow-on device would integrate the fluidics, surface acoustic waves, and support electronics on a single device [3.9]. Other research teams are exploring nanotechnology to deliver new sensor materials (e.g., researchers at the Pacific Northwest National Laboratory have

TABLE 3.4 Partial List of Near-Term Research Efforts as Sponsored by U.S. Government Agencies

Designs, materials, and concepts for new sensors and sensing systems	Examples include novel sensing materials and devices; the design of solid and liquid surfaces with molecular recognition, long lifetime, and regenerability of the sensing site; biomimetic sensors, including hybrids consisting of proteins, enzyme fragments and components, bioorganometallics, or other biocatalysts that can be linked to surfaces; bioMEMS; sensors for toxic agents (biological, chemical, radiation); sensors for operation in harsh environments; wireless sensors; chip-based systems incorporating multiple sensors, computation, actuation, and wireless interfaces; sensor systems capable of remote activation and interrogation; sensor power sources; novel optical imaging concepts; novel techniques for metrology at the nanoscale; new modeling and simulation tools; new techniques for on-sensor self-calibration and self-test; enhanced specificity to maximize accuracy and minimize false alarms; and new methods for sensor fabrication, manufacture, and encapsulation.
Arrayed sensor networks and networking	This area includes: Enabling networking technologies for distributed wireless and wired sensor networks Scalable and robust architectures Design Automated tasking Querying techniques Adaptive management and control of sensor nodes Design trade-offs and performance optimization in resource-constrained sensor networks Design of ultralow-power processing nodes for local information management Investigation of localized versus distributed versus centralized processing of sensor data Common building blocks and interfaces for sensor networking Strategies for using heterogeneous sensor and network nodes to enhance performance and reduce false alarms Security and authentication for resource-constrained sensor networks Embedded and hybrid systems Application-specific network and system services, including data-centric routing, attribute-based addressing, location management, and service discovery Energy-efficient media access, error control, and traffic management protocols

(*Continued*)

TABLE 3.4 (*Continued*)

	Mobile sensor networks Scalable reconfigurability and self-organization
Interpretation, decision, and action based on sensor data	Examples include decision theory for intelligent use of sensed information; detection and identification of false alarms; feedback theory; development of new statistical algorithms, sampling theories, and supervisory control systems tailored to needs; concepts for optimal sensor locations for effective process and system control; mathematical hybrid system tools for monitoring distributed networks of large arrays of sensors and actuators; handheld diagnostic kits; and pattern recognition and state estimation. System-level sensor applications include biomedical health monitoring, diagnostic, and therapeutic systems; image-guided surgery; health monitoring systems for civil structures; crisis management sensor systems; surveillance technology; robotics; mobile sensors; tracking and monitoring of mobile units (endangered species, inventory control, transportation); and sensor assessment (reliability, verification, validation).

Source: National Science Foundation materials [3.5].

developed nanosized preconcentrators for nerve agents, botulism, and other toxins) [3.9].

Sandia has been testing handheld sensors designed to detect chemical-weapons agents on the battlefield with high sensitivity; the detection window is 2 minutes or less. The lab has been asked to explore adding networking and GPS capability

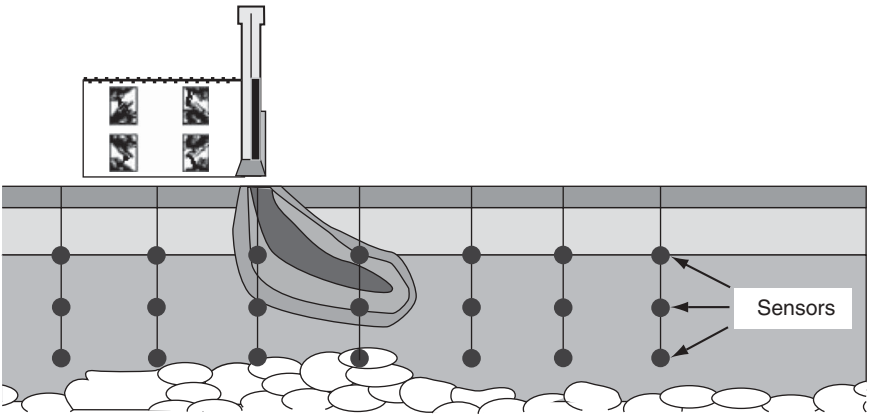

Figure 3.4 Sensor array for chemical contamination analysis.

to those sensors so that they could be mounted on military vehicles, creating a mobile battlefield sensor network. The expectation is that by the turn of the present decade, a bio smoke alarm detector will be ready for commercial deployment [3.9].

On the networking front, researchers are considering peer-to-peer network with multilevel security and quality-of-service guarantees, spanning terrestrial wireless, wireline, and satellite links. The underlying network architecture for a national sensor network has been studied at Oak Ridge National Labs. The aim is to use off-the-shelf technology as much as possible and to leverage existing infrastructure, such as the 30,000 cellular towers and 100,000 cellular base stations in the United States today. However, developing quality-of-service guarantees and multilevel security for a hybrid wired, wireless, and satellite network is a challenge [3.9]. Several pilot sensor network projects are being field tested, including systems developed by Los Alamos and UC–Berkeley researchers to safeguard crops. Trial sensor networks are also in place in Boston subways, at the San Francisco airport, and on the Miami docks. The Washington subway recently went operational with a chemical-sensor system developed by Sandia and Argonne National Laboratories in Chicago [3.9].

3.6 CONCLUSION

In this chapter we looked at basic sensor node technology along with a taxonomy of sensor types. Some current trends were also discussed.

REFERENCES

[3.1] D. Roman, ''Scottish Universities Plan Speckled Computing Net,'' *EE Times*, Oct. 27, 2003.

[3.2] *The Scientist and Engineer's Guide to TinyOS Programming*, University of California–Berkeley, http://tinyos.org. This book was developed as an open source, freely available manuscript on the TinyOS Documentation Project.

[3.3] ''Cougar: The Sensor Network Is the Database,'' Cornell University, Ithaca, NY, http://www.cs.cornell.edu/database/cougar/.

[3.4] ''Smart Sensor Networks,'' National Institute of Standards and Technology, Gaithersburg, MD, http://w3.antd.nist.gov/wahn_ssn.shtml.

[3.5] Sensors and Sensor Networks, Program Solicitation, NSF 03-512, Mar. 6, 2003, National Science Foundation, Directorate for Engineering, http://www.nsf.gov/cgi-bin/getpub?gpg; also, NSF Publications Clearinghouse, pubs@nsf.gov.

[3.6] J. M. Rabaey, M. J. Ammer, J. L. da Silva Jr., D. Patel, S. Roundy, ''PicoRadio Supports Ad Hoc Ultra-low Power Wireless Networking,'' *Computer*, July 2000; wireless sensor network research at the Berkeley Wireless Research Center, http://bwrc.eecs.berkeley.edu/Research/Pico_Radio/.

[3.7] J. M. Rabaey, ‘‘Ultra Low-Power Computation and Communication Enables Ambient Intelligence,’’ presented at the Smart Objects Conference, Grenoble, France, Apr. 2003.

[3.8] Center for Embedded Networked Sensing, University of California–Los Angeles, http://www.cens.ucla.edu/portal/micro_nano_sensor_tech/.

[3.9] R. Merritt, ‘‘Planned U.S. Sensor Network Targets Terror Threats,’’ *EE Times*, July 14, 2003.