1

INTRODUCTION AND OVERVIEW OF WIRELESS SENSOR NETWORKS

1.1 INTRODUCTION

A *sensor network*[1] is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives an administrator the ability to instrument, observe, and react to events and phenomena in a specified environment. The administrator typically is a civil, governmental, commercial, or industrial entity. The environment can be the physical world, a biological system, or an information technology (IT) framework. Network(ed) sensor systems are seen by observers as an important technology that will experience major deployment in the next few years for a plethora of applications, not the least being national security [1.1–1.3]. Typical applications include, but are not limited to, data collection, monitoring, surveillance, and medical telemetry. In addition to sensing, one is often also interested in control and activation.

There are four basic components in a sensor network: (1) an assembly of distributed or localized sensors; (2) an interconnecting network (usually, but not always, wireless-based); (3) a central point of information clustering; and (4) a set of computing resources at the central point (or beyond) to handle data correlation, event trending, status querying, and data mining. In this context, the sensing and computation nodes are considered part of the sensor network; in fact, some of the computing

[1] Although the terms *networked sensors* and *network of sensors* are perhaps grammatically more correct than the term *sensor network*, generally in this book we employ the de facto nomenclature *sensor network*.

Wireless Sensor Networks: Technology, Protocols, and Applications, by Kazem Sohraby, Daniel Minoli, and Taieb Znati

may be done in the network itself. Because of the potentially large quantity of data collected, algorithmic methods for data management play an important role in sensor networks. The computation and communication infrastructure associated with sensor networks is often specific to this environment and rooted in the device- and application-based nature of these networks. For example, unlike most other settings, in-network processing is desirable in sensor networks; furthermore, node power (and/or battery life) is a key design consideration. The information collected is typically parametric in nature, but with the emergence of low-bit-rate video [e.g., Moving Pictures Expert Group 4 (MPEG-4)] and imaging algorithms, some systems also support these types of media.

In this book we provide an exposition of the fundamental aspects of *wireless sensor networks* (WSNs). We cover wireless sensor network technology, applications, communication techniques, networking protocols, middleware, security, and system management. There already is an extensive bibliography of research on this topic; the reader may wish, for example, to consult [1.4] for an up-to-date list. We seek to systematize the extensive paper and conference literature that has evolved in the past decade or so into a cohesive treatment of the topic. The book is targeted to communications developers, managers, and practitioners who seek to understand the benefits of this new technology and plan for its use and deployment.

1.1.1 Background of Sensor Network Technology

Researchers see WSNs as an "exciting emerging domain of deeply networked systems of low-power wireless motes[2] with a tiny amount of CPU and memory, and large federated networks for high-resolution sensing of the environment" [1.93]. Sensors in a WSN have a variety of purposes, functions, and capabilities. The field is now advancing under the *push* of recent technological advances and the *pull* of a myriad of potential applications. The radar networks used in air traffic control, the national electrical power grid, and nationwide weather stations deployed over a regular topographic mesh are all examples of early-deployment sensor networks; all of these systems, however, use specialized computers and communication protocols and consequently, are very expensive. Much less expensive WSNs are now being planned for novel applications in physical security, health care, and commerce. Sensor networking is a multidisciplinary area that involves, among others, radio and networking, signal processing, artificial intelligence, database management, systems architectures for operator-friendly infrastructure administration, resource optimization, power management algorithms, and platform technology (hardware and software, such as operating systems) [1.5]. The applications, networking principles, and protocols for these systems are just beginning to be developed [1.48]. The near-ubiquity of the Internet, the advancements in wireless and wireline communications technologies, the network build-out (particularly

[2] The terms *sensor node*, *wireless node*, *smart dust*, *mote*, and *COTS* (commercial off the shelf) *mote* are used somewhat interchangeably; the most general terms, however, are *sensor node* and *wireless node*.

in the wireless case), the developments in IT (such as high-power processors, large random-access memory chips, digital signal processing, and grid computing), coupled with recent engineering advances, are in the aggregate opening the door to a new generation of low-cost sensors and actuators that are capable of achieving high-grade spatial and temporal resolution.

The technology for sensing and control includes electric and magnetic field sensors; radio-wave frequency sensors; optical-, electrooptic-, and infrared sensors; radars; lasers; location/navigation sensors; seismic and pressure-wave sensors; environmental parameter sensors (e.g., wind, humidity, heat); and biochemical national security–oriented sensors. Today's sensors can be described as "smart" inexpensive devices equipped with multiple onboard sensing elements; they are low-cost low-power untethered multifunctional nodes that are logically homed to a central sink node. Sensor devices, or wireless nodes (WNs), are also (sometimes) called *motes* [1.91]. A stated commercial goal is to develop complete microelectromechanical systems (MEMSs)–based sensor systems at a volume of 1 mm^3 [1.93]. Sensors are internetworked via a series of multihop short-distance low-power wireless links (particularly within a defined *sensor field*); they typically utilize the Internet or some other network for long-haul delivery of information to a point (or points) of final data aggregation and analysis. In general, within the sensor field, WSNs employ contention-oriented random-access channel sharing and transmission techniques that are now incorporated in the IEEE 802 family of standards; indeed, these techniques were originally developed in the late 1960s and 1970s expressly for wireless (not cabled) environments and for large sets of dispersed nodes with limited channel-management intelligence [1.6]. However, other channel-management techniques are also available.

Sensors are typically deployed in a high-density manner and in large quantities: A WSN consists of densely distributed nodes that support sensing, signal processing [1.7], embedded computing, and connectivity; sensors are logically linked by self-organizing means [1.8–1.11] (sensors that are deployed in short-hop point-to-point master–slave pair arrangements are also of interest). WNs typically transmit information to collecting (monitoring) stations that aggregate some or all of the information. WSNs have unique characteristics, such as, but not limited to, power constraints and limited battery life for the WNs, redundant data acquisition, low duty cycle, and, many-to-one flows. Consequently, new design methodologies are needed across a set of disciplines including, but not limited to, information transport, network and operational management, confidentiality, integrity, availability, and, in-network/local processing [1.12]. In some cases it is challenging to collect (extract) data from WNs because connectivity to and from the WNs may be intermittent due to a low-battery status (e.g., if these are dependent on sunlight to recharge) or other WN malfunction.[3] Furthermore, a lightweight protocol stack is desired. Often, a very large number of client units (say 64k or more) need to be supported by the system and by the addressing apparatus.

[3] Special statistical algorithms may be employed to correct from biases caused by erratic or poorly placed WNs [1.91].

Sensors span several orders of magnitude in physical size; they (or, at least some of their components) range from nanoscopic-scale devices to mesoscopic-scale devices at one end, and from microscopic-scale devices to macroscopic-scale devices at the other end. *Nanoscopic* (also known as *nanoscale*) refers to objects or devices on the order of 1 to 100 nm in diameter; mesoscopic scale refers to objects between 100 and 10,000 nm in diameter; the microscopic scale ranges from 10 to 1000 μm, and the macroscopic scale is at the millimeter-to-meter range. At the low end of the scale, one finds, among others, biological sensors, small passive microsensors (such as Smart Dust[4]), and "lab-on-a-chip" assemblies. At the other end of the scale one finds platforms such as, but not limited to, identity tags, toll collection devices, controllable weather data collection sensors, bioterrorism sensors, radars, and undersea submarine traffic sensors based on sonars.[5] Some refer to the latest generation of sensors, especially the miniaturized sensors that are directly embedded in some physical infrastructure, as *microsensors*. A sensor network supports any type of generic sensor; more narrowly, networked microsensors are a subset of the general family of sensor networks [1.13]. Microsensors with onboard processing and wireless interfaces can be utilized to study and monitor a variety of phenomena and environments at close proximity.

Sensors can be simple point elements or can be multipoint detection arrays. Typically, nodes are equipped with one or more application-specific sensors and with on-node signal processing capabilities for extraction and manipulation (preprocessing) of physical environment information. *Embedded network 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). Sensors may be passive and/or be self-powered; farther down the power-consumption chain, some sensors may require relatively low power from a battery or line feed [1.14–1.19]. At the high end of the power-consumption chain, some sensors may require very high power feeds (e.g., for radars).

Sensors facilitate the instrumenting and controlling of factories, offices, homes, vehicles, cities, and the ambiance, especially as commercial off-the-shelf technology becomes available. With sensor network technology (specifically, with embedded networked sensing), ships, aircraft, and buildings can "self-detect" structural faults (e.g., fatigue-induced cracks). Places of public assembly can be instrumented to detect airborne agents such as toxins and to trace the source of the contamination should any be present (this can also be done for ground and underground situations). Earthquake-oriented sensors in buildings can locate potential survivors and can help assess structural damage; tsunami-alerting sensors are useful for nations with extensive coastlines. Sensors also find extensive applicability on the battlefield for reconnaissance and surveillance [1.20].

[4] The Smart Dust mote is an autonomous sensing, computing, and communication system that uses the optical visible spectrum for transmission [1.89]. They are tiny inexpensive sensors developed by UC–Berkeley engineers (see also Chapter 2).

[5] Although satellites can be used to support sensing, we do not include them explicitly in the technical discussion.

In this book we emphasize the emergence of open standards in support of WSNs; standardization drives commercialization of the technology. “New things” generally start out as advanced research projects pursued at government and/or academic labs. Typically, pure and/or applied research goes on for a number of years. At this early stage, specialized, one-of-a-kind, complex, and noninterworking prototypes, pilots, or deployments are common. Eventually, however, if a new thing is to become a ubiquitous technology, commercial-level open standards, chipsets, and products are needed, which must meet commercial service- and operational-level agreements in terms of reliability, cost, usability, durability, and simplicity. Following is a sample classification of research topics by frequency of publication based on a fair-sized sample of recent scientific WSN articles.

Deployment	9.70%
Target tracking	7.27%
Localization	6.06%
Data gathering	6.06%
Routing and aggregation	5.76%
Security	5.76%
MAC protocols	4.85%
Querying and databases	4.24%
Time synchronization	3.64%
Applications	3.33%
Robust routing	3.33%
Lifetime optimization	3.33%
Hardware	2.73%
Transport layer	2.73%
Distributed algorithms	2.73%
Resource-aware routing	2.42%
Storage	2.42%
Middleware and task allocation	2.42%
Calibration	2.12%
Wireless radio and link characteristics	2.12%
Network monitoring	2.12%
Geographic routing	1.82%
Compression	1.82%
Taxonomy	1.52%
Capacity	1.52%
Link-layer techniques	1.21%
Topology control	1.21%
Mobile nodes	1.21%
Detection and estimation	1.21%
Diffuse phenomena	0.91%
Programming	0.91%
Power control	0.61%
Software	0.61%
Autonomic routing	0.30%

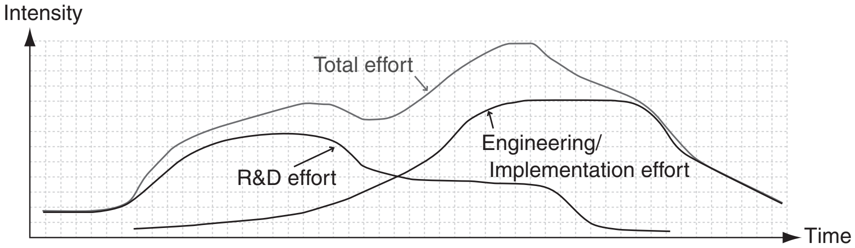

Figure 1.1 Shift and progression in emphasis over time in support of commercialization.

To appreciate the importance and criticality of simplicity-fostering standards in making a technology a pervasive reality, one need only study the progression of late-1960s wireless random-access systems (e.g., [1.21–1.23]) to the present-day LANs and WLAN/2.5G/3G systems (e.g., [1.6]); or the early-1970s ARPAnet (e.g., among many, [1.24]) to the present-day Internet (e.g., [1.25]); or the mid-1970s Voice Over Packet (e.g., [1.26–1.30]) to the current Voice Over IP technology (e.g., [1.31,1.32]); or the late-1980s video compression (e.g., [1.33]) to the current MPEG-2 and MPEG-4 digital video transmission revolution (e.g., [1.34]). See Figure 1.1 for a pictorial representation of the shift in technical emphasis over time.

Indeed, at this juncture, sensor networking is becoming a burgeoning field; there is currently extensive interest in this discipline not only from academia and government, but also from developers, manufacturers, startup companies, investors, and original equipment manufacturers (OEMs). According to industry observers, the wireless sensor market is now poised to take off commercially. Current market reports indicate that more than half a billion nodes are expected to ship for wireless sensor applications by 2010, for a market worth more than $7 billion [1.35]. As an example, advanced radio-frequency integrated circuits (RFICs) are now available for $3 or less, and smart sensor integrated circuits have become commonplace [1.35]. In the next few years, advances in the areas of sensor design and materials that have taken place in the recent past will lead, almost assuredly, to significant reductions in the size, weight, power consumption, and cost of sensors and sensor arrays; these advances will also affect an increase in their spatial and temporal resolution, along with improved measuring accuracy.

Implementations of WSNs have to address a set of technical challenges; however, the move toward standardization will, in due course, minimize a number of these challenges by addressing the issues once and then result in off-the-shelf chipsets and components. A current research and development (R&D) challenge is to develop low-power communication with low-cost on-node processing and self-organizing connectivity/protocols; another critical challenge is the need for extended temporal operation of the sensing node despite a (typically) limited power supply (and/or battery life). In particular, the architecture of the radio, including the use of low-power circuitry, must be properly selected. In practical terms this implies low power consumption for transmission over low-bandwidth channels and low-power-consumption logic to preprocess and/or compress data. Energy-efficient wireless communications systems are being sought and are typical of WSNs. Low power consumption is a key factor in ensuring long operating horizons for non-power-fed systems (some systems can indeed be power-fed and/or rely on other power sources). Power efficiency in WSNs is generally accomplished in three ways:

1. Low-duty-cycle operation.
2. Local/in-network processing to reduce data volume (and hence transmission time).
3. Multihop networking reduces the requirement for long-range transmission since signal path loss is an inverse exponent with range or distance. Each node in the sensor network can act as a repeater, thereby reducing the link range coverage required and, in turn, the transmission power.

Conventional wireless networks are generally designed with link ranges on the order of tens, hundreds, or thousands of miles. The reduced link range and the compressed data payload in WSNs result in characteristic link budgets that differ from those of conventional systems. However, the power restrictions, along with the desire for low node cost, give rise to what developers call "profound design challenges" [1.36]. Cooperative signal processing between nodes in proximity may enhance sensitivity and specificity to environmental event detection [1.36,1.37]. New CMOS (complementary metal-oxide semiconductor) chipsets optimized for WSNs are the key to commercialization success and are, in fact, being developed.

In this book we taxonomize (commercial) sensor networks and systems into two categories:

- *Category 1 WSNs* (C1WSNs): almost invariably mesh-based systems with multihop radio connectivity among or between WNs, utilizing dynamic routing in both the wireless and wireline portions of the network. Military-theater systems typically belong to this category.
- *Category 2 WSNs* (C2WSNs): point-to-point or multipoint-to-point (star-based) systems generally with single-hop radio connectivity to WNs, utilizing static routing over the wireless network; typically, there will be only one route from the WNs to the companion terrestrial or wireline forwarding node (WNs are pendent nodes). Residential control systems typically belong to this category.

C1WSNs support highly distributed high-node-count applications (e.g., environmental monitoring, national security systems); C2WSNs typically support confined short-range spaces such as a home, a factory, a building, or the human body. C1WSNs are different in scope and/or reach from evolving wireless C2WSN technology for short-range low-data-rate wireless applications such as

RFID (radio-frequency identification) systems, light switches, fire and smoke detectors, thermostats, and, home appliances. C1WSNs tend to deal with large-scale multipoint-to-point systems with massive data flows, whereas C2WSNs tend to focus on short-range point-to-point, source-to-sink applications with uniquely defined transaction-based data flows.

For a number of years, vendors have made use of proprietary technology for collecting performance data from devices. In the early 2000s, sensor device suppliers were researching ways of introducing standardization. WNs typically transmit small volumes of simple data (e.g., "Is the temperature at the set level or lower?"). For *within-building* applications, designers ruled out Wi-Fi (wireless fidelity, IEEE 802.11b) standards for sensors as being too complex and supporting more bandwidth than is actually needed for typical sensors. Infrared systems require line of sight, which is not always achievable; Bluetooth (IEEE 802.15.1) technology was at first considered a possibility, but it was soon deemed too complex and expensive. This opened the door for a new standard IEEE 802.15.4 along with ZigBee (more specifically, ZigBee comprises the software layers above the newly adopted IEEE 802.15.4 standard and supports a plethora of applications). C2WSNs have lower layers of the communication protocol stack (Physical and Media Access Control), which are comparable to that of a personal area network (PAN), defined in the recently developed IEEE 802.15 standard: hence, the utilization of these IEEE standards for C2WSNs. IEEE 802.15.4 operates in the 2.4-GHz industrial, scientific, and medical (ISM) radio band and supports data transmission at rates up to 250 kbps at ranges from 30 to 200 ft. ZigBee/IEEE 802.15.4 is designed to complement wireless technologies such as Bluetooth, Wi-Fi, and ultrawideband (UWB), and is targeted at commercial point-to-point sensing applications where cabled connections are not possible and where ultralow power and low cost are requirements [1.35].

With the emergence of the ZigBee/IEEE 802.15.4 standard, systems are expected to transition to standards-based approaches, allowing sensors to transfer information in a standardized manner. C2WSNs (and C1WSN, for that matter) that operate *outside a building and over a broad geographic area* may make use of any number of other standardized radio technologies. The (low-data-rate) C2WSN market is expected to grow significantly in the near future: The volume of low-data-rate wireless devices is forecast to be three times the size of Wi-Fi by the turn of the decade, due to the expected deployment of the systems based on the ZigBee/IEEE 802.15.4 standard (industry observers expect the number of ZigBee-compliant nodes to increase from less than 1 million in 2005 to 100 million in 2008). A discussion of both categories of technology, C1WSNs and C2WSNs, is provided in this book, but the reader should keep in mind that the technical issues affecting these two areas are, to a large degree, different.

There is also considerable research in the area of mobile ad hoc networks (MANETs). WSNs are similar to MANETs in some ways; for example, both involve multihop communications. However, the applications and technical requirements for the two systems are significantly different in several respects [1.38–1.41,1.48]:

1. The typical mode of communication in WSN is from multiple data sources to a data recipient or sink (somewhat like a reverse multicast) rather than communication between a pair of nodes. In other words, sensor nodes use primarily multicast or broadcast communication, whereas most MANETs are based on point-to-point communications.
2. In most scenarios (applications) the sensors themselves are not mobile (although the sensed phenomena may be); this implies that the dynamics in the two types of networks are different.
3. Because the data being collected by multiple sensors are based on common phenomena, there is potentially a degree of redundancy in the data being communicated by the various sources in WSNs; this is not generally the case in MANETs.
4. Because the data being collected by multiple sensors are based on common phenomena, there is potentially some dependency on traffic event generation in WSNs, such that some typical random-access protocol models may be inadequate at the queueing-analysis level; this is generally not the case in MANETs.
5. A critical resource constraint in WSNs is energy; this is not always the case in MANETs, where the communicating devices handled by human users can be replaced or recharged relatively often. The scale of WSNs (especially, C1WSNs) and the necessity for unattended operation for periods reaching weeks or months implies that energy resources have to be managed very judiciously. This, in turn, precludes high-data-rate transmission.
6. The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in a MANET.

For these reasons the plethora of routing protocols that have been proposed for MANETs are not suitable for WSNs, and alternative approaches are required [1.48]. Note that MANETs per se are not discussed further in this book.

Others also study wireless mesh networks (WMNs) (see, e.g., [1.94] for an extensive tutorial). Wi-Fi-based WMNs are being applied as hot zones, which cover a broad area such as a downtown city district. Although WMNs have many of the same networking characteristics as WSNs, their application can, in principle, be more general. Also, a fairly large fraction of the commercial WSNs of the near future are expected to be of the C1WSN category, which does not (obligatorily) require or entail meshing. Like WSNs, WMNs can use off-the-shelf radio technology such as Wi-Fi, WiMax (worldwide interoperability for microwave access), and cellular 3G. As an observation, the topic of network mobility (NEMO) is unrelated to WSNs in general terms. NEMO is concerned with managing the mobility of an entire network, which changes, as a unit, its point of attachment to the Internet and thus its reachability in the topology. The mobile network includes one or more mobile routers which connect it to the global Internet. A mobile network is assumed to be a leaf network, i.e., it will not carry transit traffic [1.96]. As should be clear by now, the focus of this book is on WSNs; hence, we do not spend any time covering WMNs.

1.1.2 Applications of Sensor Networks

Traditionally, sensor networks have been used in the context of high-end applications such as radiation and nuclear-threat detection systems, "over-the-horizon" weapon sensors for ships, biomedical applications, habitat sensing, and seismic monitoring. More recently, interest has focusing on networked biological and chemical sensors for national security applications; furthermore, evolving interest extends to direct consumer applications. Existing and potential applications of sensor networks include, among others, military sensing, physical security, air traffic control, traffic surveillance, video surveillance, industrial and manufacturing automation, process control, inventory management, distributed robotics, weather sensing, environment monitoring, national border monitoring, and building and structures monitoring [1.13]. A short list of applications follows.

- Military applications
  - Monitoring inimical forces
  - Monitoring friendly forces and equipment
  - Military-theater or battlefield surveillance
  - Targeting
  - Battle damage assessment
  - Nuclear, biological, and chemical attack detection

  and more . . .
- Environmental applications
  - Microclimates
  - Forest fire detection
  - Flood detection
  - Precision agriculture

  and more . . .
- Health applications
  - Remote monitoring of physiological data
  - Tracking and monitoring doctors and patients inside a hospital
  - Drug administration
  - Elderly assistance

  and more . . .
- Home applications
  - Home automation
  - Instrumented environment
  - Automated meter reading

  and more . . .

- Commercial applications
    - Environmental control in industrial and office buildings
    - Inventory control
    - Vehicle tracking and detection
    - Traffic flow surveillance

  and more ...

Chemical-, physical-, acoustic-, and image-based sensors can be utilized to study ecosystems (e.g., in support of global parameters such as temperature and microorganism populations). Defense applications have fostered research and development in sensor networks during the past half-century. On the battlefield, sensors can be used to identify and/or track friendly or inimical objects, vehicles, aircraft, and personnel; here, a system of networked sensors can detect and track threats and can be utilized for weapon targeting and area denial [1.13,1.20]. "Smart" *disposable* microsensors can be deployed on the ground, in the air, under water, in (or on) human bodies, in vehicles, and inside buildings. Homes, buildings, and locales equipped with this technology are being called *smart spaces.*

Wireless sensors can be used where wireline systems cannot be deployed (e.g., a dangerous location or an area that might be contaminated with toxins or be subject to high temperatures). The rapid deployment, self-organization, and fault-tolerance characteristics of WSNs make them versatile for military *command*, *control*, *communications*, *intelligence*, *surveillance*, *reconnaissance*, and *targeting systems* [1.38]. Many of these features also make them ideal for national security. Sensor networking is also seen in the context of pervasive computing [1.42].

The deployment scope for sensing and control networks is poised for significant expansion in the next three to five years as we have already mentioned; this expansion relates not only to science and engineering applications but also to a plethora of "new" consumer applications. Industry players expect that in the near future it will become possible to integrate sensors into commercial products and systems to improve the performance and lifetime of a variety of products; industry planners also expect that with sensors one can decrease product life-cycle costs. Consumer applications include, but are not limited to, critical infrastructure protection and security, health care, the environment, energy, food safety, production processing, and quality of life [1.35]. WSNs are also expected to afford consumers a new set of conveniences, including remote-controlled home heating and lighting, personal health diagnosis, automated automobile maintenance telemetry, and automated in-marina boat-engine telemetry, to list just a few. The ultimate expectation is that eventually wireless sensor network technologies will enable consumers to keep track of their belongings, pets, and young children [1.35]. Ubiquitous high-reliability public-safety applications covering a multithreat management are also on the horizon.

Near-term commercial applications include, but are not limited to, industrial and building wireless sensor networks, appliance control [lighting, and heating, ventilation, and air conditioning (HVAC)], automotive sensors and actuators, home automation and networking, automatic meter reading/load management, consumer electronics/entertainment, and asset management. Commercial market segments include the following:

- Industrial monitoring and control
- Commercial building and control
- Process control
- Home automation
- Wireless automated meter reading (AMR) and load management (LM)
- Metropolitan operations (traffic, automatic tolls, fire, etc.)
- National security applications: chemical, biological, radiological, and nuclear wireless sensors
- Military sensors
- Environmental (land, air, sea) and agricultural wireless sensors

Suppliers and products tend to cluster according to these categories.

1.1.3 Focus of This Book

This book focuses on wireless sensor networks.[6,7] We look at basic WSN technology and supporting protocols, with emphasis placed on standardization. The treatise provides an exposition of the fundamental aspects of wireless sensor networks from a practical engineering perspective. The text provides an introductory up-to-date survey of WSNs, including applications, communication, technology, networking protocols, middleware, security, and management. Both C1WSNs and C2WSNs are addressed.

The present chapter aims at assessing, from an introductory perspective, sensor technology as a whole, including some of the recent history of the field. We also address some of the challenges to be faced and addressed by the evolving practice. In Chapter 2 we discuss near-term and longer-range applications of WSNs and look at network sensor applications for both business- and government-oriented applications. In Chapter 3 we look at basic sensor systems and provide a survey of sensor technology, including classification in terms of microsensors (tiny sensors), radar sensors, nanosensors, and other sensors. We address sensor functionality, sensing and actuation units, processing units, communication units, power units, and other application-dependent units. We also look at design issues, the operating environment and hardware constraints, transmission media, radio-frequency integrated circuits, power constraints, communications network interfaces, network architecture and protocols, network topology, performance issues, fault tolerance, scalability, and self-organization and mobility capabilities. Sensor arrays and networks are also discussed.

Chapter 4 begins a discussion of sensor network protocols. We address physical layer issues such as channel-related concerns, radio-frequency bands, bandwidth,

[6] Some sensor networks are not wireless; although many of the issues are similar, others are not. Our discussion focuses on the wireless situation.

[7] Control and actuation are covered here only in passing.

propagation modes (ground wave, sky wave, line of sight), and channel impairments (e.g., refraction, atmospheric absorption, fading, multipath, free space, Gaussian noise, Rayleigh fading, Rician fading). Reference is made to the gamut of off-the-shelf radio technologies that can be used for WSNs. Chapter 5 extends the topics introduced in Chapter 4 by covering medium access control protocols in some detail; we provide a survey of media access control (MAC) protocols for sensor networks, including the IEEE 802.11 family, the IEEE 802.15 family (e.g., Bluetooth and ZigBee), and other protocols. In Chapter 6 we discuss routing protocols in sensor networks, providing a survey of key routing protocols for sensor networks and discussing the main design issues (e.g., scalability, mobility, power awareness, self-organization, naming). In Chapter 7 we look at transport protocols, provide a survey of transport layer protocols for sensor networks, and discuss design requirements (e.g., error control, reliability, power awareness, delay guarantees).

Chapter 8 begins a discussion of sensor network middleware, operating systems (OSs), and application programming interfaces (APIs). Chapter 8 covers middleware for sensor networks, including data dissemination models (data aggregation and follow-on data dissemination protocols), compression techniques, and data storage. In Chapter 9 we examine sensor management, including naming and localization and maintenance and fault tolerance. In Chapter 10 we address operating systems for sensor networks. The discussion includes design factors (size constraints, power awareness, distribution and reconfiguration; and APIs and programming language paradigms). A survey of commercially available operating systems for sensor networks is provided. Chapter 11 covers performance and traffic management.

1.2 BASIC OVERVIEW OF THE TECHNOLOGY

In Section 1.1 we provided a high-level description of the approach, issues, and technologies associated with WSNs. Some additional details are provided in this section from a generic perspective; many of these issues and concepts are then discussed in greater detail in the chapters that follow. As we proceed, the reader should keep in mind that sensor networks deal with space and time: location, coverage, and data synchronization. Data are the intrinsic "currency" of a sensor network. Typically, there will be a large amount of time-stamped time-dependent data. Therefore, sensor networks often support in-network computation. Some sensor networks use source-node processing; others use a hierarchical processing architecture. Instead of sending the raw data to the nodes responsible for the data fusion, nodes often use their processing abilities locally to carry out basic computations, and then transmit only a subset of the data and/or partially processed data. In a hierarchical processing architecture, processing occurs at consecutive tiers until the information about events of interest reaches the appropriate decision-making and/or administrative point. Sensor nodes are almost invariably constrained in energy supply and radio channel transmission bandwidth; these constraints, in conjunction with a typical deployment of large number of sensor nodes, have posed a plethora of challenges to the design and management of WSNs. These challenges necessitate energy awareness at all layers of a communications protocol stack [1.92]. Some of the key technology and standards elements that are relevant to sensor networks are as follows:

- Sensors
  - Intrinsic functionality
  - Signal processing
  - Compression, forward error correction, encryption
  - Control/actuation
  - Clustering and in-network computation
  - Self-assembly
- Wireless radio technologies
  - Software-defined radios
  - Transmission range
  - Transmission impairments
  - Modulation techniques
  - Network topologies
- Standards (de jure)
  - IEEE 802.11a/b/g together with ancillary security protocols
  - IEEE 802.15.1 PAN/Bluetooth
  - IEEE 802.15.3 ultrawideband (UWB)
  - IEEE 802.15.4/ZigBee (IEEE 802.15.4 is the physical radio, and ZigBee is the logical network and application software)
  - IEEE 802.16 WiMax
  - IEEE 1451.5 (Wireless Sensor Working Group)
  - Mobile IP
- Standards (de facto)
  - Tiny OS (TinyOS is being developed by the University of California–Berkeley as an open-source software platform; the work is funded by DARPA and is undertaken in the context of the Network Embedded Systems Technology Research Project at UC–Berkeley in collaboration with the University of Virginia, Palo Alto Research Center, Ohio State University, and approximately 100 other organizations)
  - Tiny DB (a query-processing system for extracting information from a network of TinyOS sensors)
- Software applications
  - Operating systems
  - Network software

- Direct database connectivity software
- Middleware software
- Data management software

1.2.1 Basic Sensor Network Architectural Elements

In this section we briefly highlight the basic elements and design focus of sensor networks. These elements and design principles need to be placed in the context of the C1WSN sensor network environment, which is characterized by many (sometimes all) of the following factors: large sensor population (e.g., 64,000 or more client units need to be supported by the system and by the addressing apparatus), large streams of data, incomplete/uncertain data, high potential node failure; high potential link failure (interference), electrical power limitations, processing power limitations, multihop topology, lack of global knowledge about the network, and (often) limited administrative support for the network [1.43] (C2WSNs have many of these same limitations, but not all). Sensor network developments rely on advances in sensing, communication, and computing (data-handling algorithms, hardware, and software). As noted, to manage scarce WSN resources adequately, routing protocols for WSNs need to be energy-aware. Data-centric routing and in-network processing are important concepts that are associated intrinsically with sensor networks [1.44–1.48]. The end-to-end routing schemes that have been proposed in the literature for mobile ad hoc networks are not appropriate WSNs; data-centric technologies are needed that perform in-network aggregation of data to yield energy-efficient dissemination [1.48].

Sensor Types and Technology A sensor network is composed of a large number of sensor nodes that are densely deployed [1.38,1.39]. To list just a few venues, sensor nodes may be deployed in an open space; on a battlefield in front of, or beyond, enemy lines; in the interior of industrial machinery; at the bottom of a body of water; in a biologically and/or chemically contaminated field; in a commercial building; in a home; or in or on a human body. A sensor node typically has embedded processing capabilities and onboard storage; the node can have one or more sensors operating in the acoustic, seismic, radio (radar), infrared, optical, magnetic, and chemical or biological domains. The node has communication interfaces, typically wireless links, to neighboring domains. The sensor node also often has location and positioning knowledge that is acquired through a global positioning system (GPS) or local positioning algorithm [1.13,1.49–1.52]. (Note, however, that GPS-based mechanisms may sometimes be too costly and/or the equipment may be too bulky.) Sensor nodes are scattered in a special domain called a *sensor field*. Each of the distributed sensor nodes typically has the capability to collect data, analyze them, and route them to a (designated) *sink* point. Figure 1.2 depicts a typical WSN arrangement. Although in many environments all WNs are assumed to have similar functionality, there are cases where one finds a heterogeneous environment in regard to the sensor functionality.

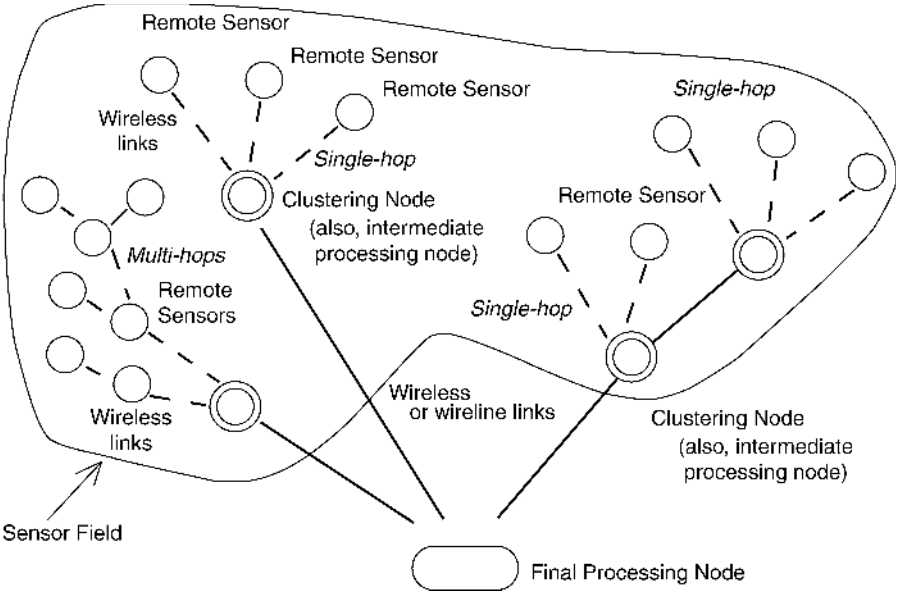

Figure 1.2 Typical sensor network arrangement.

The following are important issues pertaining to WSNs (see also Table 1.1): sensor type; sensor placement; sensor power consumption, operating environment, computational/sensing capabilities and signal processing, connectivity, and telemetry or control of remote devices. It is critical to note in this context that node location and fine-grained time (stamping) are essential for proper operation of a sensor network; this is almost the opposite of the prevalent Internet architecture, where server location is immaterial to a large degree and where latency is often not a key consideration or explicit design objective. In sensor networks, fine-grained time synchronization and localization are needed to detect events of interest in the environment under observation. Location needs to be tracked both in local three-dimensional space (e.g., On what floor and in which quadrant is the smoke detected? What is the temperature of the atmosphere at height h?) and over a broader topography, to assess detection levels across a related set (array) of sensors (e.g., What is the wind direction for wind containing contaminated particles at milepost i, $i+1$, $i+2$, etc., along a busy highway?). Localization is used for functionality such as beamforming for localization of target and events, geographical forwarding, and geographical addressing [1.5].

Embedded sensor networks are predicated on three supporting components: embedding, networking, and sensing. *Embedding* implies the incorporation of numerous distributed devices to monitor the physical world and interact with it; the devices are untethered nodes of small form factors that are equipped with a control and communication subsystem. Spatially- and temporally-dense arrangements are common. *Networking* implies the concept of physical and logical connectivity.

TABLE 1.1 Categorization of Issues Related to Sensors and Their Communication/Computing Architecture

Sensors	*Size:* Small [e.g., nanoscale electromechanical systems (MEMS)], medium [e.g., microscale electromechanical systems (MEMS)], and large (e.g., radars, satellites): cubic centimeters to cubic decimeters *Mobility:* stationary (e.g., seismic sensors), mobile (e.g., on robot vehicles) *Type:* passive (e.g., acoustic, seismic, video, infrared, magnetic) or active (e.g., radar, ladar)
Operating environment	*Monitoring requirement:* distributed (e.g., environmental monitoring) or localized (e.g., target tracking) *Number of sites:* sometimes small, but usually large (especially for C1WSNs) *Spatial coverage:* dense, spars: C1WSN: low-range multihop or C2WSN: low-range single-hop (point-to-point) *Deployment:* fixed and planned (e.g., factory networks) or ad hoc (e.g., air-dropped) *Environment:* benign (factory floor) or adverse (battlefield) *Nature:* cooperative (e.g., air traffic control) or noncooperative (e.g., military targets) *Composition:* homogeneous (same types of sensors) or heterogeneous (different types of sensors) *Energy availability:* constrained (e.g., in small sensors) or unconstrained (e.g., in large sensors)
Communication	*Networking:* wired (on occasion) or wireless (more common) *Bandwidth:* high (on occasion) or low (more typical)
Processing architecture	Centralized (all data sent to central site), distributed or in-network (located at sensor or other sides), or hybrid

Source: Modified from [1.13], with permission.

Logical connectivity has the goal of supporting coordination and other high-level tasks; physical connectivity is typically supported over a wireless radio link [1.53]. *Sensing* implies the presence of these capabilities in a tightly coupled environment, typically for the measurement of physical-world parameters. Some of the characteristic features of sensor networks include the following [1.38,1.39]:

- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes very frequently.
- Sensor nodes are limited in power, computational capacities, and memory.
- Sensor nodes may not have global *identification* because of the large amount of overhead and the large number of sensors.

Sensor networks require sensing systems that are long-lived and environmentally resilient. Unattended, untethrered, self-powered low-duty-cycle systems are typical.

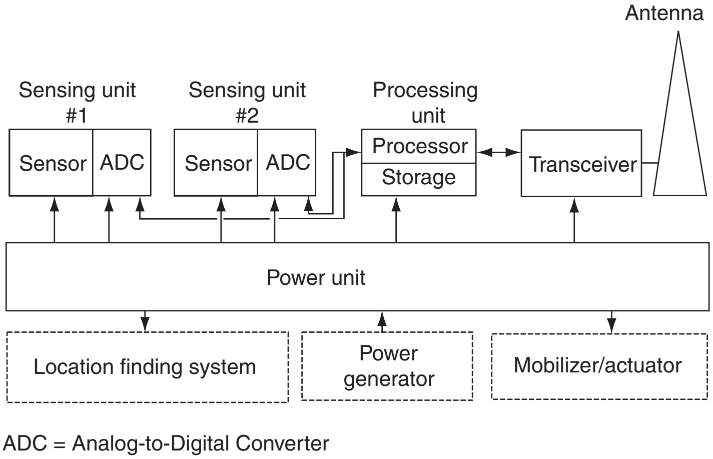

Figure 1.3 Typical sensing node.

Power consumption is often an issue that needs to be taken into account as a design constraint. In most instances, communication circuitry and antennas are the primary elements that draw most of the energy [1.54–1.58]. Sensors are either passive or active devices. *Passive sensors* in element form include seismic-, acoustic-, strain-, humidity-, and temperature-measuring devices. Passive sensors in array form include optical- [visible, infrared 1 micron (μm), infrared 10 μm], and biochemical-measuring devices. Passive sensors tend to be low-energy devices. *Active sensors* include radar and sonar; these tend to be high-energy systems. The trend is toward VLSI (very large scale integration), integrated optoelectronics, and nanotechnology; work is under way in earnest in the biochemical arena. The components of a (remote) sensing node include (see Figure 1.3) the following:

- A sensing and actuation unit (single element or array)
- A processing unit
- A communication unit
- A power unit
- Other application-dependent units

Figure 1.4 depicts an example on an (ultra)miniature sensor.

In addition to (embedded) sensing there is a desire to build, deploy, and manage unattended or untethered embedded *control and actuation systems*, sometimes called *control networks*. Such a control system acts on the environment either in a self-autonomous manner or under the telemetry of a remote or centralized node. Key applications require more than just sensing: They need control and actuation. To the extent that we cover the topic in this book, *control* refers to some “minor” activity internal to the sensor (e.g., zoom, add an optical filter, rotate

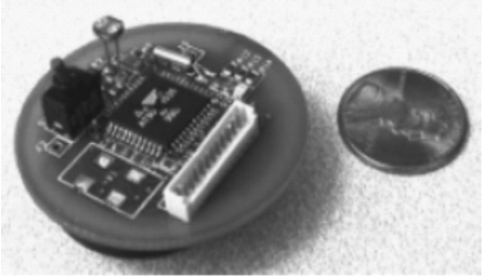

Figure 1.4 Miniature sensor: the MacroMote, developed at UC–Berkeley. (Courtesy of UC–Berkeley.)

an antenna); *actuation* refers to a ‘‘major’’ activity external to the sensor itself (e.g., open a valve, emit some fluid into the environment, engage a motor to relocate somewhere else). Applications requiring control and/or actuation include transportation, high-tech agriculture, medical monitoring, drug delivery, battlefield interventions, and so on. In addition to standard concerns (e.g., reliability, security), actuation systems also have to take into account factors such as safety. The topic of WSN applications is revisited in Chapter 2.

Software (Operating Systems and Middleware) To support the node operation, it is important to have *open-source operating systems* designed specifically for WSNs. Such operating systems typically utilize a *component-based architecture* that enables rapid implementation and innovation while minimizing code size as required by the memory constraints endemic in sensor networks. TinyOS is one such example of a de facto standard, but not the only one. TinyOS’s *component library* includes network protocols, distributed services, sensor drivers, and data acquisition tools; these can be used as-is or be further refined for a specific application. TinyOS’s event-driven execution model enables fine-grained power management, yet allows the scheduling flexibility made necessary by the unpredictable nature of wireless communication and physical world interfaces. TinyOS has already been ported to over a dozen platforms and numerous sensor boards. A wide community uses TinyOS in simulation to develop and test various algorithms and protocols, and numerous groups are actively contributing code to establish standard interoperable network services [1.90]. This topic is revisited in Chapter 8.

Standards for Transport Protocols The goal of WSN engineers is to develop a cost-effective standards-based wireless networking solution that supports low-to-medium data rates, has low power consumption, and guarantees security and reliability [1.66–1.73]. The position of sensor nodes does not have be predetermined, allowing random deployment in inaccessible terrains or dynamic situations; however, this also means that sensor network protocols and algorithms must possess self-organizing capabilities [1.38,1.39]. For military and/or national security

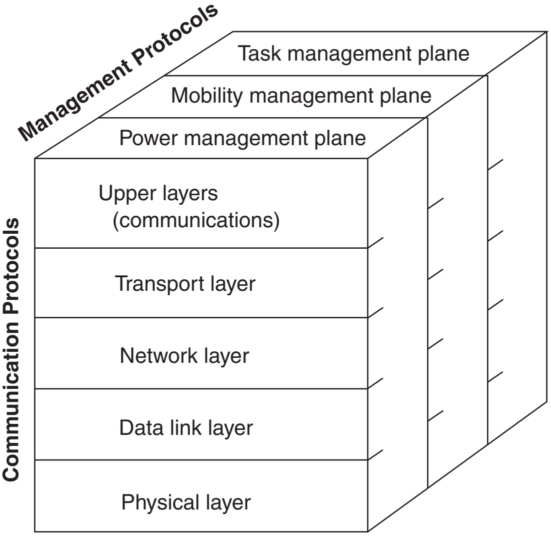

Figure 1.5 Generic protocol stack for sensor networks.

applications, sensor devices must be amenable to rapid deployment, the deployment must be supportable in an ad hoc fashion, and the environment is expected to be highly dynamic.

Researchers have developed many new protocols specifically designed for WSNs, where energy awareness is an essential consideration; focus has been given to the routing protocols, since they might differ from traditional networks (depending on the application and network architecture) [1.92]. Networking per se is an important architectural component of sensor networks, and standards play a major role in this context. Figure 1.5 depicts a generic protocol stack model that can be utilized to describe the communications apparatus (also see Table 1.2). Table 1.3 shows some typical lower-layer protocols that are in principle applicable to

TABLE 1.2 Possible WSN Protocol Stack[a]

Upper layers	In-network applications, including application processing, data aggregation, external querying query processing, and external database
Layer 4	Transport, including data dissemination and accumulation, caching, and storage
Layer 3	Networking, including adaptive topology management and topological routing
Layer 2	Link layer (contention): channel sharing (MAC), timing, and locality
Layer 1	Physical medium: communication channel, sensing, actuation, and signal processing

[a] Table modeled after [1.05].

TABLE 1.3 Possible Lower-Layer WSN Protocols

	GPRS/GSM 1xRTT/CDMA	IEEE 802.11b/g	IEEE 802.15.1	IEEE 802.15.4
Market name for standard	2.5G/3G	Wi-Fi	Bluetooth	ZigBee
Network target	WAN/MAN	WLAN and hotspot	PAN and DAN (desk area network)	WSN
Application focus	Wide area voice and data	Enterprise applications (data and VoIP)	Cable replacement	Monitoring and control
Bandwidth (Mbps)	0.064–0.128+	11–54	0.7	0.020–0.25
Transmission range (ft)	3000+	1–300+	1–30+	1–300+
Design factors	Reach and transmission quality	Enterprise support, scalability, and cost	Cost, ease of use	Reliability, power, and cost

WSNs; overall, a lightweight protocol stack is sought for WSNs. Issues here relate to the following:

1. Physical connectivity and coverage: How can one interconnect dispersed sensors in a cost-effective and reliable manner, and what medium should be used (e.g., wireless channels)?
2. Link characteristics and capacity, along with data compression (see, e.g., [1.59])
3. Networking security and communications reliability (including naturally occurring phenomena such as noise impairments, and malicious issues such as attacks, interference, and penetration)
4. Physical-, link-, network-, and transport-layer protocols, with an eye to reliable transport, congestion detection and avoidance, and scalable and robust communication (e.g., [1.60–1.64])
5. Communication mechanisms in what could be an environment with highly correlated and time-dependent arrivals (where many of the queueing assumptions used for system modeling could break down [1.6,1.65])

Although sensor electronics are becoming inexpensive, observers see the lack of networking standards as a potentially retardant factor in the commercial deployment of sensor networks. Because today there are still numerous proprietary network protocols, manufacturers have created vendor-specific and consequently, expensive products that will not work with products from other manufacturers.

The lack of open standards has not only prevented the possibility for interoperability but has also limited innovation. Evolving standards may provide, on a going-forward basis, a common framework on which developers can create applications that will leverage the hardware advances with radios and sensors. The goal of standards is to enable developers to design solutions that will lower installation and maintenance costs for a variety of sensors used in industrial, commercial, and residential settings [1.35]. As one example of an applicable standard, particularly for C2WSNs, the IEEE 802.15.4 specification for the physical, media access, and data link layers was formally ratified in 2003; at press time, ZigBee Alliance[8] members were defining a global specification for reliable, cost-effective, low-power wireless applications based on the IEEE 802.15.4 standard. Another standard of potential interest is the IEEE 802.16, also known as WiMax. This topic is revisited in Chapters 4, 5, 6, and 7.

Routing and Data Dissemination Routing and data dissemination issues deal with data dissemination mechanisms for large-scale wireless networks, directed diffusion (see, e.g., [1.74]), data-centric routing [also known as data aggregation (see, e.g., [1.44])], adaptive routing, and other specialized routing mechanism. Routing protocols for WSNs generally fall into three groups: data-centric, hierarchical, and location-based. The concept of data aggregation is to combine the data arriving from different sources along the way (enroute). This allows one to eliminate redundancy, minimize the number of transmissions, and in turn, be parsimonious with energy consumption. This routing approach shifts the emphasis from the traditional *address-centric* approaches (finding short routes between pairs of addressable end nodes) to a *data-centric* approach (finding routes from multiple sources to a single destination that allows in-network consolidation of redundant data) [1.48]; see Table 1.4.

As already noted, there is interest in handling in-network processing, even while the data are being routed. Communications 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 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). It follows that one wants to perform data processing in the network, in proximity of the source of the data, and then only forward summarized, aggregated, fused, and/or synthesized results.

To support data-centric routing and directed diffusion, one needs to name the data (rather than the nodes) with relevant attributes such as (but not limited to)

[8] The ZigBee Alliance is a nonprofit industry consortium of leading semiconductor manufacturers, technology providers, OEMs, and end users worldwide. Membership is open to all. ZigBee Alliance members are defining a global specification for reliable, cost-effective, low-power wireless applications based on the IEEE 802.15.4 standard. Over 68 member companies are working actively to define the ZigBee specification, including six promoters (Honeywell, Invensys, Mitsubishi, Motorola, Philips, and Samsung) and participants that include semiconductor manufacturers, wireless IP providers, and OEMs.

TABLE 1.4 Summary of Routing Protocols Utilized in WSNs

Routing Protocol Category	Description	Examples
Data centric	The sink sends queries to certain WSN regions and waits for data from WNs located in the regions selected. Because data are being requested through queries, attribute-based naming is necessary to specify the properties of data. Due to the large number of nodes deployed, in many WSNs it is not practical to assign global identifiers to each node. This, along with potential random deployment of WNs, makes it challenging to select a specific (or a specific set of) WNs to be queried. Hence, data are typically transmitted from every WN with in the deployment region; this gives rise, however, to significant redundancy along with inefficiencies in terms of energy consumption. It follows that it is desirable to have routing protocols that will be able to select a set of sensor nodes and utilize data aggregation during the relaying of data. This has led to the development of data-centric routing (in traditional address-based routing, routes are created between addressable nodes managed in the network layer mechanism).	Sensor protocols for information via negotiation (SPIN) Directed diffusion Rumor routing Gradient-based routing (GBR) Constrained anisotropic diffusion routing (CADR) COUGAR ACQUIRE
Hierarchical	A single-tier (gateway or cluster-point) network can cause the gateway node to become overloaded, particularly as the density of sensors increases. This, in turn, can cause latency in event status delivery. To permit WSNs to deal with a large population of WNs and to cover a large area of interest, multipoint clustering has been proposed. The goal of hierarchical routing is to manage the energy consumption of WNs efficiently by establishing multihop communication within a particular cluster, and by performing data aggregation and fusion to decrease the number of transmitted packets to the sink.	Energy-adaptive clustering hierarchy (LEACH) Threshold-sensitive energy-efficient sensor network protocol (TEEN) and adaptive threshold-sensitive energy-efficient sensor network protocol (APTEEN) Power-efficient gathering in sensor information systems (PEGASIS)

(*Continued)*

TABLE 1.4 (*Continued)*

Routing Protocol Category	Description	Examples
Location based	Location information about the WNs can be utilized in routing data in an energy-efficient manner. Location information is used to calculate the distance between two given nodes so that energy consumption can be determined (or at least, estimated). For example, if the region to be sensed is known, the query can be diffused only to that specific region, limiting and/or eliminating the number of transmissions in the out-of-region space. Location-based routing is ideal for mobile ad hoc networks, but it can also be used for generic WSNs. (Note that non-energy-aware location-based protocols designed for wireless ad hoc networks, such as Cartesian and trajectory-based routing, are not desirable or ideal in WSNs.)	Minimum energy communication network (MECN) and small minimum energy communication network (SMECN) Geographic adaptive fidelity (GAF) Geographic and energy aware routing (GEAR)
QoS-oriented	Quality of service (QoS)–aware protocols consider end-to-end delay requirements in setting up the paths in the sensor network.	Sequential assignment routing (SAR) Stateless protocol for end-to-end delay (SPEED)

Source: Based partially on [1.92].

data type, time, and location. One needs to diffuse requests and responses over the network with application-cognizant routing; and one must support in-network data aggregation and processing [1.75,1.76]. Some view sensor networks as being peer to peer at the logical level, even though the physical communication topology is generally hierarchical; here one peer is the data source that “publishes” the data (could be a basic sensor node or an aggregation node) and the other peer is the data client that subscribes to a data content list. This topic is revisited in Chapter 6.

Sensor Network Organization and Tracking Areas of interest involving network organization and tracking include distributed group management (maintaining organization in large-scale sensor networks); self-organization, including authentication, registration, and session establishment; and entity tracking: target detection, classification, and tracking. Dynamic sensor allocation (i.e., how to deal with impaired or unreliable sensors and/or how to “clean” and query noisy sensors) is also of interest. Some of the factors that come into play include the following: area of coverage (portion of topography of interest that is covered by sensors); detectability (probability that the sensor will detect an event such as a value variation or a moving object); and node coverage (portion of sensor population that is covered, in an overlapping sense, by other sensors that could be used in case of malfunction of the primary sensor). In case of control or actuation, factors include assessments as to where one needs to add new nodes (or to reorient or rotate a measuring probe) for optimal coverage and/or how to move a sensor (autonomously) to a new location for maximal coverage. This topic is revisited in Chapter 9.

Computation Computation deals with data aggregation, data fusion, data analysis, computation hierarchy, grid computing (utility-based decision making in wireless sensor networks), and signal processing. We have already mentioned the desire for data-centric protocols that support in-network processing; however, it must be noted that per-node processing by itself is not sufficient: One needs interpretation of spatially distributed events and data related to those events. The network may be required to handle in-network processing based on the locality of the data, and queries must be directed automatically to the node or nodes that have the best view of the system (environment) in the context of the data queried. An area of recent research is networked information processing: how to extract useful, reliable, and timely information from the sensor network deployed; this implies leveraging the distributed computing environment created by these sensors for signal and information processing in the network and for dynamic and interactive querying and tasking the sensor network [1.13]. This topic is revisited in Chapter 10.

Data Management Data management deals with data architectures; database management, including querying mechanisms; and data storage and warehousing. In a traditional environment (even in a traditional sensor network environment), data are collected to a centralized server for storage, against which queries are issued. In a more elaborate environment, particularly in support of true-real-time data querying, a mechanism can be deployed to support distributed data storage (possibly extending to clustering nodes) and to support distributed data querying [1.77–1.81]. In particular, one is interested in multiresolution/multitiered data storage and retrieval. The data need to be indexed for efficient temporal and spatial searching; at the same time, one wants to be able easily to generate global values associated with variables or requirements of interest. This topic is revisited in Chapter 8.

Security Security deals with confidentiality (encryption), integrity (e.g., identity management, digital signatures), and availability (protection from denial of service).

Network Design Issues We have already noted that in sensor networks, issues relate to reliable transport (possibly including encryption), bandwidth-and power-limited transmission, data-centric routing, in-network processing, and self-configuration. Design factors include operating environment and hardware constraints such as transmission media, radio-frequency integrated circuits, power constraints, communications network interfaces; and network architecture and protocols, including network topology and fault tolerance, scalability, self-organization, and mobility [1.82,1.83].

Sensor networks are generally self-configuring systems. The goal is to be able to adapt to unpredictable situations and states. Static or semidynamic topologies lend themselves easily to preconfiguration, but highly dynamic environments require self-configuration. In designing a sensor network, one is naturally looking for acceptable accuracy of information (even in the presence of failed nodes and/or links, and possibly conflicting or partial data); low network and computing latency; and optimal resource use (specifically, power and bandwidth). Work is under way to develop techniques that can be employed to deal with these and other pertinent issues, such as how to represent sensor data, how to structure sensor queries, how to adapt to changing node or network conditions, and how to manage a large network environment where nodes have limited network management functionality.

Sensor networks often employ data processing directly in the network itself. Part of the motivation is the potential for large pools of data being generated by the sensors. By utilizing computation close to the source of the data for trending, averaging, maxima and minima, or out-of-range activities, one is able to reduce the communication throughput that would otherwise be needed. Intrinsic to this is the development of localized algorithms that support global goals; it follows that forms of collaborative signal processing are desired.

Researchers are looking at new system architectures to manage interactions. Currently, many sensor systems suffer from being one-of-a-kind with piecemeal design approaches. This predicament leads to suboptimal economics, longevity, interoperability, scalability, and robustness. Standards will go a long way to address a number of these concerns. A number of researchers [1.5] are taking the position that the traditional approach and/or protocol suite is not adequate for embedded, energy-constrained, untethered, small-form-factor, unattended systems, because these systems cannot tolerate the communication overhead associated with the routing and naming intrinsic in the Internet suite of protocols. Proponents are making a pitch for special-purpose system functions in place of the general-purpose Internet functionality designed for elastic applications. In effect, resource constraints require a more streamlined and more tightly integrated communications layer than that possible with a TCP–IP or ISO (International Organization for Standardization) stack. This topic is revisited in Chapter 9 and 11.

1.2.2 Brief Historical Survey of Sensor Networks

The history of sensor networks spans four phases, described briefly below [1.13].

Phase 1: Cold-War Era Military Sensor Networks During the cold war, extensive acoustic networks were developed in the United States for submarine surveillance; some of these sensors are still being used by the National Oceanographic and Atmospheric Administration (NOAA) to monitor seismic activity in the ocean. Also, networks of air defense radars were deployed to cover North America; to handle this, a battery of Airborne Warning and Control System (AWACS) planes operated as sensors.

Phase 2: Defense Advanced Research Projects Agency Initiatives The major impetus to research on sensor networks took place in the early 1980s with programs sponsored by the Defense Advanced Research Projects Agency (DARPA). The distributed sensor networks (DSN) work aimed at determining if newly developed TCP–IP protocols and ARPAnet's (the predecessor of the Internet) approach to communication could be used in the context of sensor networks. DSN postulated the existence of many low-cost spatially distributed sensing nodes that were designed to operate in a collaborative manner, yet be autonomous; the goal was for the network to route information to the node that can best utilize the information [1.84,1.85]. The DSN program focused on distributed computing, signal processing, and tracking. Technology elements included acoustic sensors, high-level communication protocols, processing and algorithm calculations (e.g., self-location algorithms for sensors), and distributed software (dynamically modifiable distributed systems and language design) [1.13]. Researchers at Carnegie Mellon University focused on providing a network operating system for flexible transparent access to distributed resources, and researchers at the Massachusetts Institute of Technology focused on knowledge-based signal-processing techniques. Testbeds were developed for tracking multiple targets in a distributed environment; all components in the testbed network were custom built. Ongoing work in the 1980s resulted in the development of a multiple-hypothesis tracking algorithm to address difficult problems involving high target density, missing detections, and false alarms [1.86]; multiple-hypothesis tracking is now a standard approach to challenging tracking problems.

Phase 3: Military Applications Developed or Deployed in the 1980s and 1990s (These can properly be called first-generation commercial products.) Based on the results generated by the DARPA–DSN research and the testbeds developed, military planners set out in the 1980s and 1990s to adopt sensor network technology, making it a key component of network-centric warfare. An effort was made at the time to start employing commercial off the shelf (COTS) technology and common network interfaces, thereby reducing cost and development time. In traditional warfare environments each platforms "owns" its weapons in a fairly autonomous manner (distinct platforms operate independently). In network-centric warfare, weapon systems are not (necessarily) tightly affiliated with a specific platform; instead, through the use of distributed sensors, the weapon systems and platforms collaborate with each other over a sensor network, and information is sent to the appropriate node. Sensor networks can improve detection and tracking performance through multiple observations, geometric and phenomenological diversity, extended detection range, and faster response time [1.13]. An example of network-centric warfare include the cooperative engagement capability, a system that consists of multiple radars collecting data on air targets. Other sensor networks in the military arena include acoustic sensor arrays for antisubmarine warfare, such as the fixed distributed system and the advanced deployable system, and autonomous ground sensor systems such as the remote battlefield sensor system and the tactical remote sensor system.

Phase 4: Present-Day Sensor Network Research (These can properly be called second-generation commercial products.) Advances in computing and communication that have taken place in the late 1990s and early 2000s have resulted in a new generation of sensor network technology. Evolving sensor networks represent a significant improvement over traditional sensors [1.38,1.39]. Inexpensive compact sensors based on a number of high-density technologies, including MEMS and (in the next few years) nanoscale electromechanical systems (NEMS), are appearing. Standardization is a key to wide-scale deployment of any technology, including WSN (e.g., Internet–Web, MPEG-4 digital video, wireless cellular, VoIP). Advances in IEEE 802.11a/b/g-based wireless networking and other wireless systems such as Bluetooth, ZigBee,[9] and WiMax are now facilitating reliable and ubiquitous connectivity. Inexpensive processors that have low power-consumption requirements make possible the deployment of sensors for a plethora of applications. Commercially-focused efforts are now directed at defining mesh, peer-to-peer, and cluster-tree network topologies with data security features and interoperable application profiles. Table 1.5 summarizes these generations of commercial products and alludes to a next-generation (third-generation) set of products.

TABLE 1.5 Commercial Generations of Sensor Networks

	First Generation (1980s–1990s)	Second Generation (Early 2000s)	Third Generation (Late 2000s)
Size	Attaché or larger	Paperback book or smaller	Small, even a dust particle
Weight	Pounds	Ounces	Grams or less
Deployment mode	Physically installed or air-dropped	Hand-placed	Embedded or "sprinkled," possibly nanotechnology-based
Node architecture	Separate sensing, processing, and communication	Integrated sensing, processing, and communication	Fully integrated sensing, processing, and communication
Protocols	Proprietary	Proprietary	Standard: Wi-Fi, ZigBee, WiMax, etc.
Topology	Point-to-point, star, and multihop	Client–server and peer-to-peer	Fully peer to peer
Power supply	Large batteries or line feed	AA batteries	Solar or possibly nanotechnology-based
Life span	Hours, days, and longer	Days to weeks	Months to years

[9] Although ZigBee proper comprises the software layers above the newly adopted IEEE 802.15.4 standard, at times we use *ZigBee* to mean "IEEE 802.15.4 with ZigBee middleware software running on top of the 802.15.4 MAC/PHY."

1.2.3 Challenges and Hurdles

For WSNs to become truly ubiquitous, a number of challenges and hurdles must be overcome. Challenges and limitations of wireless sensor networks include, but are not limited to, the following:

- Limited functional capabilities, including problems of size
- Power factors
- Node costs
- Environmental factors
- Transmission channel factors
- Topology management complexity and node distribution
- Standards versus proprietary solutions
- Scalability concerns [1.95]

Hardware Constraints A sensor may need to fit into a tight module on the order of 2 × 5 × 1 cm or even as small as a 1 × 1 × 1 cm. As shown in Figure 1.3, a sensor node is typically comprised of four key components and four optional components. The key components include a *power unit* (batteries and/or solar cells), a *sensing unit* (sensors and analog-to-digital converters), a *processing unit* (along with storage), and a *transceiver unit* (connects the node to the network). The optional components include a *location-finding system*, a *power generator*, a *control actuator*, and *other application-dependent elements*. The environmentally-intrinsic analog signals measured by the sensors are converted to digital signals by analog-to-digital converters and then are supplied to the processing unit. Sensor nodes may also have to be disposable, autonomous, and adaptive to the environment. R&D must be directed to solving the issue of reliable packaging of sensors despite the hardware constraints and challenges.

Power Consumption The sensor node lifetime typically exhibits a strong dependency on battery life. In many cases, the wireless sensor node has a limited power source (<500 mAh, 1.2 V), and replenishment of power may be limited or impossible altogether. Battery operation for sensors used in commercial applications is typically based on two AA alkaline cells or one Li-AA cell. It follows, as already noted, that power management and power conservation are critical functions for sensor networks, and one needs to design power-aware protocols and algorithms. The function of a sensor node in a sensor field is to detect events, perform local data processing, and transmit raw and/or processed data. Power consumption can therefore be allocated to three functional domains: *sensing*, *communication*, and *data processing*, each of which requires optimization. In the context of communications, in a multihop sensor network a node may play the dual role of data collection and processing and of being a data relay point. As can easily be understood, (excessive) rerouting and/or retransmission will require additional power.

Node Unit Costs Almost by definition, a sensor network consists of a large set of sensor nodes. It follows that the cost of an individual node is critical to the overall financial metric of the sensor network. Clearly, the cost of each sensor node has to be kept low for the global metrics to be acceptable. Current sensor systems based on Bluetooth technology cost about $10; however, Bluetooth is limited as a transmission technology in terms of both bandwidth and distance. However, the cost of a sensor node is generally targeted to be less than $1, which is lower than the current state-of-the-art technology.

Environment Sensor networks often are expected to operate in an unattended fashion in dispersed and/or remote geographic locations: Nodes may be deployed in harsh, hostile, or widely scattered environments. Such environments give rise to challenging management mechanisms. At the other end of the spectrum, sensor nodes are occasionally deployed densely either in close proximity with or directly inside the environment to be observed.

Transmission Channels Sensor networks often operate in a bandwidth- and performance-constrained multihop wireless communications medium. These wireless communications links operate in the radio, infrared, or optical range. Some low-power radio-based sensor devices use a single-channel RF transceiver operating at 916 MHz [1.87]; some sensor systems use a Bluetooth-compatible 2.4-GHz transceiver with an integrated frequency synthesizer [1.88]; yet other systems use 2.4 GHz (IEEE 802.11b technology), 5.0 GHz (IEEE 802.11a technology), or possibly other bands (for IEEE 802.15.4/IEEE 802.16 and/or for international use). To facilitate global operation of these networks, the transmission channel selected must be available on a worldwide basis.

Connectivity and Topology Deploying and managing a high number of nodes in a relatively bounded environment requires special techniques. Hundreds to thousands of sensors in close proximity (feet) may be deployed in a sensor field. The density of sensors may be as high as 27 nodes/m^3 [1.88]. Sensor network applications require ad hoc networking techniques; although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited to the unique features and application requirements of sensor networks [1.38,1.39]. Nodes could be deployed *en mass* or be injected in the sensor field individually (e.g., they could be deployed by dropping them from an helicopter, scattered by an artillery shell or rocket, or deployed individually by a human or a robot). Any time after deployment, topology changes may ensue, due to changes in sensor node position; power availability, dropouts, or brownouts; malfunctioning; reachability impairments; jamming; and so on. At some future time, additional sensor nodes may need to be deployed to replace malfunctioning nodes, for example; hence, although some sensor nodes may fail or be blocked due to lack of power or have physical damage or environmental interference, this failure should not affect the overall mission of the sensor network.

Standards As implied by the protocol stack of Figure 1.4, a suite of protocols and open standards are needed at the physical, link, network, and transport layers; in addition, other management protocols and standards are required (physical layer standards are also known as air interface standards). Historically, sensor networks have used network- and application-specific protocols. This has had the effect of slowing cost-effective commercial deployment on a wide scale. Standards are now beginning to be incorporated into sensor networks. The highest degree of standardization has occurred at the lower layers. Within-building WSNs now tend to look to use ZigBee/IEEE802.15.4; WSNs that are in the open (outside buildings and over a broad geography) may find other technologies useful. In particular, IEEE-based wireless LAN standards have been given consideration. IEEE 802.11 supports 1- or 2-Mbps transmission in the 2.4-GHz band using either frequency-hopping spread spectrum or direct-sequence spread spectrum. IEEE 802.11a is an extension of 802.11 that provides up to 54 Mbps in the 5-GHz band and uses orthogonal frequency-division multiplexing encoding. IEEE 802.11b is an extension to 802.11 that provides 11-Mbps transmission in the 2.4-GHz band using DSSS. IEEE 802.11g provides up to 54 Mbps in the 2.4-GHz band. Extensions of these standards were also under way at the time of this writing (e.g., IEEE 802.11n). Another transmission method is free-space optics operating in the 1-μm wavelength (infrared). Infrared is license-free line-of-sight technology that operates at short range (300 to 3000 m). The new WiMax standard (IEEE 802.16) may also be useful for metropolitan environments, as is the application of cellular third-generation technologies. Earlier we also mentioned the Smart Dust mote, which uses the visible optical spectrum to communicate.

1.3 CONCLUSION

In this chapter we introduced the basic concept of WSNs and supportive technologies. The chapters that follow address in much greater detail and technical depth the issues that have been highlighted here.

REFERENCES

[1.1] C. S. Raghavendra, K. M. Sivalingam, T. Znati Eds., *Wireless Sensor Networks*, Kluwer Academic, New York, 2004.

[1.2] E. Cayirci, R. Govindan, T. Znati, M. Srivastava, Editorial: “Wireless Sensor Networks,” *Computer Networks: International Journal of Computer and Telecommunications Networking*, Vol. 43, No. 4, Nov. 2003.

[1.3] T. Znati, C. Raghavendra, K. Sivalingam, Guest editorial, Special Issue on Wireless Sensor Networks, *Mobile Networks and Applications*, Vol. 8, No. 4, Aug. 2003.

[1.4] B. Krishnamachari, “A Wireless Sensor Networks Bibliography,” Autonomous Networks Research Group, University of Southern California–Los Angeles, http://ceng.usc.edu/~anrg/SensorNetBib.html#0103.

[1.5] J. Kurose, V. Lesser, E. de Sousa e Silva, A. Jayasumana, B. Liu, *Sensor Networks Seminar*, CMPSCI 791L, University of Massachusetts, Amherst, MA, Fall 2003.

[1.6] D. Minoli, *Hotspot Networks: Wi-Fi for Public Access Locations*, McGraw-Hill, New York, 2003.

[1.7] R. Nowak, U. Mitra, "Boundary Estimation in Sensor Networks: Theory and Methods," *Proceedings of the 2nd Workshop on Information Processing in Sensor Networks* (IPSN'03), Palo Alto, CA, Apr. 2003.

[1.8] K. Sohraby et al., "Protocols for Self-Organization of a Wireless Sensor Network," *IEEE Personal Communications*, Vol. 7, No. 5, Oct. 2000, pp. 16ff.

[1.9] A. Cerpa, D. Estrin, "ASCENT: Adaptive Self-Configuring Sensor Networks Topologies," *Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies* (InfoCom'02), New York, Vol. 3, June 2002.

[1.10] H. Gupta et al., "Connected Sensor Cover: Self-Organization of Sensor Networks for Efficient Query Execution," *Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing* (MobiHoc'03), Annapolis, MD, June 2003.

[1.11] Q. Huang *et al.*, "Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks," *Proceedings of the 2nd Workshop on Sensor Networks and Applications* (WSNA'03), San Diego, CA, Sept. 2003.

[1.12] R. Kumar et al., "Computation Hierarchy for In-Network Processing," *Proceedings of the 2nd Workshop on Sensor Networks and Applications* (WSNA'03), San Diego, CA, Sept. 2003.

[1.13] C.-Y. Chong, S. P. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges," *Proceedings of the IEEE*, Vol. 91, No. 8, Aug. 2003, pp. 1247ff.

[1.14] A. Salhieh et al., "Power Efficient Topologies for Wireless Sensor Networks," *Proceedings of the 2001 International Conference on Parallel Processing* (ICPP'01), Valencia, Spain, Sept. 2001, pp. 156ff.

[1.15] A. Sinha, A. Chandrakasan, "Dynamic Power Management in Wireless Sensor Networks," *IEEE Design and Test of Computers*, Vol. 18, No. 2, Mar. 2001.

[1.16] D. Rakhmatov, S. Vrudhula, "Energy Management for Battery-Powered Embedded Systems," *ACM Transactions on Embedded Computing Systems*, Vol. 2, No. 3, Aug. 2003.

[1.17] J. M. Rabaey *et al.*, "PicoRadios for Wireless Sensor Networks: The Next Challenge in Ultra-Low Power Design," *Proceedings of the 7th IEEE International Symposium on Computers and Communications* (ISCC'02), July 2002.

[1.18] M. Kubisch *et al.*, "Distributed Algorithms for Transmission Power Control in Wireless Sensor Networks," *Proceedings of the IEEE Wireless Communications and Networking Conference* (WCNC'03), Vol. 1, Mar. 2003.

[1.19] S. Coleri *et al.*, "Power Efficient System for Sensor Networks," *Proceedings of the 8th IEEE International Symposium on Computers and Communication* (ISCC'03), July 2003.

[1.20] T. Clouqueur et al., "Sensor Deployment Strategy for Target Detection," *Proceedings of the 1st Workshop on Sensor Networks and Applications* (WSNA'02), Atlanta, GA, Sept. 2002.

[1.21] D. Minoli, I. Gitman, "On Connectivity in Mobile Packet Radio Networks," *28th IEEE Vehicular Technology Conference Record*, Mar. 1978, pp. 105–109.

[1.22] D. Minoli, W. Nakamine, "A Taxanomy and Comparison of Random Access Protocols for Computer Networks," *Networks'80 Conference Record*, 1980. Included in S. Ramani, Ed., *Data Communication and Computer Networks*, pp. 187–206.

[1.23] D. Minoli, I. Gitman, "Combinatorial Issues in Mobile Packet Radio," *IEEE Transactions on Communication*, Vol. 26, Dec. 1978, pp. 1821–1826.

[1.24] D. Minoli, "Intelligent Terminal Standards Could Enhance Net Efficiency," *Data Communications*, Vol. 8, No. 11, Nov. 1979, pp. 59–68.

[1.25] D. Minoli, A. Schmidt, *Internet Architectures*, Wiley, New York, 1999.

[1.26] D. Minoli, "Packetized Speech Networks, Part 1: Overview," *Australian Electronics Engineer*, Apr. 1979, pp. 38–52.

[1.27] D. Minoli, "Packetized Speech Networks, Part 2: Queueing Model," *Australian Electronics Engineer*, July 1979, pp. 68–76.

[1.28] D. Minoli, "Packetized Speech Network, Part 3: Delay Behavior and Performance Characteristics," *Australian Electronics Engineer*, Aug. 1979, pp. 59–68.

[1.29] D. Minoli, "Issues in Packet Voice Communication," *Proceedings of the IEE*, Vol. 126, No. 8, Aug. 1979, pp. 729–740.

[1.30] D. Minoli, "Digital Voice Communication over Digital Radio Links," *SIGCOMM Computer Communications Review*, Vol. 9, No. 4, Oct. 1979, pp. 6–22.

[1.31] D. Minoli, E. Minoli, *Delivering Voice over IP and the Internet*, 2nd ed., Wiley, New York, 2002.

[1.32] D. Minoli, *Voice over MPLS*, McGraw-Hill, New York, 2002.

[1.33] D. Minoli, "Putting Video on Desktops," *Computerworld*, Oct. 1986, pp. 35ff.

[1.34] D. Minoli, E. Minoli, et al., "Digital Video," in *The Telecommunications Handbook*, K. Terplan and P. Morreale, Eds, IEEE Press, Piscataway, NJ, 2000.

[1.35] M. Hatler, *Wireless Sensor Networks: Mass Market Opportunities*, ON World, Inc., San Diego, CA, Feb. 22, 2004.

[1.36] T.-H. Lin, W. J. Kaiser, G. J. Pottie, "Integrated Low-Power Communication System Design for Wireless Sensor Networks," *IEEE Communications*, Dec. 2004, pp. 142ff.

[1.37] C. M. Okino, M. G. Corr, "Statistically-Accurate Sensor Networking," *Proceedings of the IEEE Wireless Communications and Networking Conference* (WCNC'02), Vol. 1, Mar. 2002.

[1.38] I. F. Akyildiz et al., "A Survey of Sensor Networks," *IEEE Communications*, Aug. 2002, pp. 102ff.

[1.39] W. Su et al., "Communication Protocols for Sensor Networks," in *Wireless Sensor Networks*, C. S. Raghavendra, K. Sivalingam, and T. Znati, Eds., Kluwer Academic, New York, 2004.

[1.40] A. B. McDonald, T. Znati, "Session A: Routing—Predicting Node Proximity in Ad-Hoc Networks: A Least Overhead Adaptive Model for Selecting Stable Routes," *Proceedings of the 1st ACM International Symposium on Mobile Ad Hoc Networking and Computing*, (MobiHoc'00), Nov. 2000.

[1.41] G. H. Lynn, T. Znati, "ROMR: Robust Multicast Routing in Mobile Ad-Hoc Networks," doctoral dissertation, University of Pittsburgh, Jan. 2003.

[1.42] D. Estrin, D. Culler, K. Pister, "Connecting the Physical World with Pervasive Networks," *IEEE Pervasive Computing*, Jan.–Mar. 2002.

[1.43] J. Pan et al., “Topology Control for Wireless Sensor Networks,” *Proceedings of the 9th ACM Conference on Mobile Computing and Networking* (MobiCom’03), San Diego, CA, Sept. 2003.

[1.44] A. Boukerche et al., “Energy-Aware Data-Centric Routing in Microsensor Networks,” *International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems,* San Diego, CA, Sept. 2003.

[1.45] D. Braginsky, D. Estrin, “Rumor Routing Algorithm for Sensor Networks,” *Proceedings of the 1st Workshop on Sensor Networks and Applications* (WSNA’02), Atlanta, GA, Oct. 2002.

[1.46] D. Ganesan et al., “Highly-Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks,” *Mobile Computing and Communications Review*, Vol. 1, No. 2, 2002.

[1.47] R. Kannan, et al., “Sensor-Centric Quality of Routing in Sensor Networks,” *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies* (InfoCom’03), Vol. 1, Apr. 2003.

[1.48] B. Krishnamachari, D. Estrin, S. Wicker, “Modelling Data-Centric Routing in Wireless Sensor Networks,” *Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies* (InfoCom’02), New York, June 2002.

[1.49] N. Bulusu et al., “Adaptive Beacon Placement,” *Proceedings of the 21st International Conference on Distributed Computing Systems* (ICDCS’21), Phoenix, AZ, Apr. 2001, pp. 489ff.

[1.50] P. Bergamo, G. Mazzini, “Localization in Sensor Networks with Fading and Mobility,” *Proceedings of the 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications* (PIMRC’02), Vol. 2, Sept. 2002.

[1.51] Q. Li et al., “Distributed Algorithms for Guiding Navigation Across a Sensor Network,” *Proceedings of the 9th ACM International Conference on Mobile Computing and Networking* (MobiCom’03), San Diego, CA, Sept. 2003.

[1.52] R. Iyengar, B. Sikdar, “Scalable and Distributed GPS-Free Positioning for Sensor Networks,” *Proceedings of the IEEE International Conference on Communications*, (ICC’03), Vol. 1, 2003.

[1.53] P. Morreale, K. Sohraby, B. Li, Y. Lin, Guest editorial: “Active, Programmable, and Mobile Code Networking,” *IEEE Communications*, Vol. 38, No. 3, Mar. 2000, pp. 122–123.

[1.54] M. Gerla et al., “The Mars Sensor Network: Efficient, Energy Aware Communications,” *Proceedings of the IEEE Military Communications Conference* (MilCom’01): *Communications for Network-Centric Operations—Creating the Information Force*, McLean, VA, Vol. 1, Oct. 2001.

[1.55] M. Haenggi, “Energy-Balancing Strategies for Wireless Sensor Networks,” *Proceedings of the 2003 International Symposium on Circuits and Systems* (ISCAS’03), Vol. 4, May 2003, pp. 25ff.

[1.56] J. Zhu, S. Papavassiliou, “On the Connectivity Modeling and the Tradeoffs Between Reliability and Energy Efficiency in Large Scale Wireless Sensor Networks,” *Proceedings of the IEEE Wireless Communications and Networking Conference* (WCNC’03), Vol. 2, Mar. 2003.

[1.57] R. Min, A. Chandrakasan, “Top Five Myths About the Energy Consumption of Wireless Communication,” *ACM Mobile Computing and Communications Review*, Vol. 7, No. 1, Jan. 2003.

[1.58] S. Lindsey et al., "Data Gathering in Sensor Networks Using the Energy Delay Metric," presented at the International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, Apr. 2001.

[1.59] J. Kusuma et al., "Distributed Compression for Sensor Networks," *Proceedings of the International Conference on Image Processing* (ICIP'01), Vol. 1, Oct. 2001.

[1.60] C. Wang, B. Li, K. Sohraby, "A Simple Mechanism on MAC Layer to Improve the Performance of IEEE 802.11 DCF," *Proceedings of the 1st Annual International Conference on Broadband*, (Broadnets'04), San Jose, CA, Oct. 2004.

[1.61] L. C. Zhong et al., "Data Link Layer Design for Wireless Sensor Networks," *Proceedings of the IEEE Military Communications Conference* (MilCom'01): Communications for Network-Centric Operations—Creating the Information Force, McLean, VA, Vol. 1, Oct. 2001.

[1.62] C. Y. Wan et al., "A Reliable Transport Protocol for Wireless Sensor Networks," *Proceedings of the 1st Workshop on Sensor Networks and Applications* (WSNA'02), Atlanta, GA, Sept. 2002.

[1.63] F. Stann, J. Heidemann, "A Reliable Data Transport in Sensor Networks," *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications* (SNPA'03), Anchorage, AK, May 2003.

[1.64] R. R. Kompella, A. C. Snoeren, "Practical Lazy Scheduling in Sensor Networks," *Proceedings of the 1st ACM Conference on Embedded Networked Sensor Systems* (SenSys'03), Los Angeles, Nov. 2003.

[1.65] D. Minoli, "Aloha Channels Throughput Degradation," *1986 Computer Networking Symposium Conference Record*, pp. 151–159.

[1.66] Promotional materials, ZigBee Alliance, Bishop Ranch, CA.

[1.67] E. Shih et al., "Physical Layer Driven Protocol and Algorithm Design for Energy-Efficient Wireless Sensor Networks," *Proceedings of the 7th ACM International Conference on Mobile Computing and Networking* (MobiCom'01), Rome, Italy, July 2001, pp. 272–287.

[1.68] J. Kulik et al., "Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks," *Proceedings of the 5th ACM/IEEE International Conference on Mobile Computing and Networking* (MobiCom'99), Seattle, WA, Aug. 1999.

[1.69] R. Kannan et al., "Energy and Rate Based MAC Protocol for Wireless Sensor Networks," *SIGMOD Record*, Vol. 32, No. 4, Dec. 2003.

[1.70] W. R. Heinzelman et al., "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," *Proceedings of the 5th ACM/IEEE International Conference on Mobile Computing and Networking* (MobiCom'99), Seattle, WA, Aug. 1999, pp. 174ff.

[1.71] W. R. Heinzelman et al., "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," *Proceedings of the 33rd Hawaii International Conference on System Sciences* (HICSS'00), Maui, HI, Jan. 2000.

[1.72] L. Zhou, Z. J. Haas, "Securing Ad Hoc Networks," *IEEE Networks*, Special Issue on Network Security, Dec. 1999.

[1.73] S. Slijepcevic et al., "On Communication Security in Wireless Ad-Hoc Sensor Networks," *Proceedings of the IEEE 11th International Workshops on Enabling*

Technologies: Infrastructure for Collaborative Enterprises (WETICE'02), Pittsburgh, PA, June 2002.

[1.74] C. Intanagonwiwat et al., "Directed Diffusion: A Scalable and Robust Communication Paradigm for Sensor Networks," *Proceedings of the 6th ACM International Conference on Mobile Computing and Networks* (MobiCom'00), Boston, MA, Aug. 2000.

[1.75] B. Krishnamachari et al., "The Impact of Data Aggregation in Wireless Sensor Networks," *International Workshop on Distributed Event-Based Systems* (DEBS'02), Vienna, Austria, July 2002.

[1.76] B. Przydatek et al., "Secure Information Aggregation in Sensor Networks," *Proceedings of the 1st ACM Conference on Embedded Networked Sensor Systems* (SenSys'03), Los Angeles, Nov. 2003.

[1.77] G. Gupta, M. Younis, "Performance Evaluation of Load-Balanced Clustering of Wireless Sensor Networks," *Proceedings of the 10th International Conference on Telecommunications* (ICT'03), Vol. 2, Mar. 2003.

[1.78] S. Ratnasamy et al., "A Geographic Hash Table for Data-Centric Storage," *Proceedings of the 1st Workshop on Sensors Networks and Applications* (WSNA'02), Atlanta, GA, Sept. 2002.

[1.79] S. Ratnasamy et al., "Data-Centric Storage in Sensornets with GHT: A Geographic Hash Table," Special Issue on Wireless Sensor Networks, *Mobile Networks and Applications*, Aug. 2003, pp. 427ff.

[1.80] Y. Yao, J. Gehrke, "Query Processing for Sensor Networks," *Proceedings of the 1st Biennial Conference on Innovative Data Systems Research (CIDR'03), Asilomar, CA, Jan. 2003.*

[1.81] Y. Yao, J. Gehrke, "The Cougar Approach to In-Network Query Processing in Sensor Networks," *SIGMOD Record*, Vol. 31, No. 1, Mar. 2002.

[1.82] S. Adlakha, M. Srivastava, "Critical Density Thresholds for Coverage in Wireless Sensor Networks," *Proceedings of the IEEE Wireless Communications and Networking Conference* (WCNC'03), Vol. 3, Mar. 2003.

[1.83] S. Dhillon, K. Chakrabarty, "Sensor Placement for Effective Coverage and Surveillance in Distributed Sensor Networks," *Proceedings of the IEEE Wireless Communications and Networking Conference* (WCNC'03), Vol. 3, Mar. 2003.

[1.84] *Proceedings of the Distributed Sensor Nets Workshop*, Department of Computer Science, Carnegie Mellon University, Pittsburgh, PA, 1978.

[1.85] R. F. Sproull, D. Cohen, "High-Level Protocols," *Proceedings of the IEEE*, Vol. 66, Nov. 1978, pp. 1371–1386.

[1.86] C. Y. Chong et al., "Distributed Multitarget Multisensor Tracking," in *Multitarget Multisensor Tracking: Advanced Applications*, Artech House, Norwood, MA, 1990.

[1.87] A. Woo, D. Culler, "A Transmission Control Scheme for Media Access in Sensor Networks," *Proceedings of the 7th ACM International Conference on Mobile Computing and Networking* (MobiCom'01), Rome, Italy, July 2001, pp. 221–235.

[1.88] E. Shih et al., "Physical Layer Driven Protocol and Algorithm Design for Energy-Efficient Wireless Sensor Networks," *Proceedings of the 7th ACM International Conference on Mobile Computing and Networking* (MobiCom'01), Rome, Italy, July 2001, pp. 272–286.

[1.89] J. M. Kahn et al., "Next Century Challenges: Mobile Networking for Smart Dust," *Proceedings of the 5th ACM International Conference on Mobile Computing and Networking* (MobiCom'99), Seattle, WA, Aug. 1999, pp. 270–278.

[1.90] Mission statement, TinyOS Community Forum, http://www.tinyos.net/.

[1.91] A. Deshpande et al., "Model-Driven Data Acquisition in Sensor Networks," *Proceedings of the 30th International Conference on Very Large Data Bases*, 2004, pp. 588–599.

[1.92] K. Akkaya, M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks," Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore, MD, Aug. 18, 2003.

[1.93] M. Welsh, D. Malan, B. Duncan, T. Fulford-Jones, S. Moulton, "Wireless Sensor Networks for Emergency Medical Care," presented at GE Global Research Conference, Harvard University and Boston University School of Medicine, Boston, MA, Mar. 8, 2004.

[1.94] I. Akyildiz, X. Wang, "A Survey on/of Wireless Mesh Networks," *IEEE Radio Communications*, Sept. 2005, pp. S23–S30.

[1.95] E. Egea-Lopez, J. Vales-Alonso et al., "Simulation Scalability Issues in Wireless Sensor Networks," *IEEE Communications*, July 2006, pp. 64ff.

[1.96] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, "Network Mobility (NEMO) Basic Support Protocol," *IETF RFC 3963*, January 2005.