1

INTRODUCTION TO WIRELESS SENSOR NETWORKS

Jun Zheng

Southeast University, China

Abbas Jamalipour

University of Sydney, Australia

1.1 OVERVIEW OF WIRELESS SENSOR NETWORKS

Wireless Sensor Networks (WSNs) have been widely considered as one of the most important technologies for the twenty-first century [1]. Enabled by recent advances in microelectronicmechanical systems (MEMS) and wireless communication technologies, tiny, cheap, and smart sensors deployed in a physical area and networked through wireless links and the Internet provide unprecedented opportunities for a variety of civilian and military applications, for example, environmental monitoring, battle field surveillance, and industry process control [2]. Distinguished from traditional wireless communication networks, for example, cellular systems and mobile ad hoc networks (MANET), WSNs have unique characteristics, for example, denser level of node deployment, higher unreliability of sensor nodes, and severe energy, computation, and storage constraints [3], which present many new challenges in the development and application of WSNs. In the past decade, WSNs have received tremendous attention from both

Wireless Sensor Networks: A Networking Perspective, Edited by Jun Zheng and Abbas Jamalipour

academia and industry all over the world. A large amount of research activities have bee carried out to explore and solve various design and application issues, and significant advances have been made in the development and deployment of WSNs. It is envisioned that in the near future WSNs will be widely used in various civilian and military fields, and revolutionize the way we live, work, and interact with the physical world [4].

1.1.1 Network Characteristics

A WSN typically consists of a large number of low-cost, low-power, and multifunctional sensor nodes that are deployed in a region of interest. These sensor nodes are small in size, but are equipped with sensors, embedded microprocessors, and radio transceivers, and therefore have not only sensing capability, but also data processing and communicating capabilities. They communicate over a short distance via a wireless medium and collaborate to accomplish a common task, for example, environment monitoring, battlefield surveillance, and industrial process control. Compared with traditional wireless communication networks, for example, cellular systems and MANET, sensor networks have the following unique characteristics and constraints:

- *Dense Node Deployment.* Sensor nodes are usually densely deployed in a field of interest. The number of sensor nodes in a sensor network can be several orders of magnitude higher than that in a MANET.
- *Battery-Powered Sensor Nodes.* Sensor nodes are usually powered by battery. In most situations, they are deployed in a harsh or hostile environment, where it is very difficult or even impossible to change or recharge the batteries.
- *Severe Energy, Computation, and Storage Constraints.* Sensor nodes are highly limited in energy, computation, and storage capacities.
- *Self-Configurable.* Sensor nodes are usually randomly deployed without careful planning and engineering. Once deployed, sensor nodes have to autonomously configure themselves into a communication network.
- *Application Specific.* Sensor networks are application specific. A network is usually designed and deployed for a specific application. The design requirements of a network change with its application.
- *Unreliable Sensor Nodes.* Sensor nodes are usually deployed in harsh or hostile environments and operate without attendance. They are prone to physical damages or failures.
- *Frequent Topology Change.* Network topology changes frequently due to node failure, damage, addition, energy depletion, or channel fading.
- *No Global Identification.* Due to the large number of sensor nodes, it is usually not possible to build a global addressing scheme for a sensor network because it would introduce a high overhead for the identification maintenance.

- *Many-to-One Traffic Pattern.* In most sensor network applications, the data sensed by sensor nodes flow from multiple source sensor nodes to a particular sink, exhibiting a many-to-one traffic pattern.
- *Data Redundancy.* In most sensor network applications, sensor nodes are densely deployed in a region of interest and collaborate to accomplish a common sensing task. Thus, the data sensed by multiple sensor nodes typically have a certain level of correlation or redundancy.

The unique characteristics and constraints present many new challenges in the design of sensor networks.

1.1.2 Network Applications

Sensors can be used to detect or monitor a variety of physical parameters or conditions [5], for example,

- Light
- Sound
- Humility
- Pressure
- Temperature
- Soil composition
- Air or water quality
- Attributes of an object such as size, weight, position, speed, and direction.

Wireless sensors have significant advantages over conventional wired sensors [6]. They can not only reduce the cost and delay in deployment, but also be applied to any environment, especially those in which conventional wired sensor networks are impossible to be deployed, for example, inhospitable terrains, battlefields, outer space, or deep oceans. WSNs were originally motivated by military applications, which range from large-scale acoustic surveillance systems for ocean surveillance to small networks of unattended ground sensors for ground target detection [1]. However, the availability of low-cost sensors and wireless communication has promised the development of a wide range of applications in both civilian and military fields. This section introduces a few examples of sensor network applications.

1.1.2.1 Environmental Monitoring. Environmental monitoring is one of the earliest applications of sensor networks. In environmental monitoring, sensors are used to monitor a variety of environmental parameters or conditions.

- *Habitat Monitoring.* Sensors can be used to monitor the conditions of wild animals or plants in wild habitats, as well as the environmental parameters

of the habitats. For example, Mainwaring et al. [7], from the University of California at Berkeley and the college of the Atlantic in Bar Harbor, conducted an experiment to monitor the habitat of the nesting petrels on Great Duck Land in Maine by deploying 190 wireless sensors, including humidity, pressure, temperature, and radiation.

- *Air or Water Quality Monitoring.* Sensors can be deployed on the ground or under water to monitor air or water quality. For example, water quality monitoring can be used in the hydrochemistry field. Air quality monitoring can be used for air pollution control.
- *Hazard Monitoring.* Sensors can be used to monitor biological or chemical hazards in locations, for example, a chemical plant or a battlefield.
- *Disaster Monitoring.* Sensors can be densely deployed in an intended region to detect natural or non-natural disasters. For example, sensors can be scattered in forests or revivers to detect forest fires or floods. Seismic sensors can be instrumented in a building to detect the direction and magnitude of a quake and provide an assessment of the building safety.

1.1.2.2 Military Applications. WSNs are becoming an integral part of military command, control, communication, and intelligence (C3I) systems [5]. Wireless sensors can be rapidly deployed in a battlefield or hostile region without any infrastructure. Due to ease of deployment, self-configurability, untended operation, and fault tolerance, sensor networks will play more important roles in future military C3I systems and make future wars more intelligent with less human involvement.

- *Battlefield Monitoring.* Sensors can be deployed in a battlefield to monitor the presence of forces and vehicles, and track their movements, enabling close surveillance of opposing forces.
- *Object Protection.* Sensor nodes can be deployed around sensitive objects, for example, atomic plants, strategic bridges, oil and gas pipelines, communication centers, and military headquarters, for protection purpose.
- *Intelligent Guiding.* Sensors can be mounted on unmanned robotic vehicles, tanks, fighter planes, submarines, missiles, or torpedoes to guide them around obstacles to their targets and lead them to coordinate with one another to accomplish more effective attacks or defences.
- *Remote Sensing.* Sensors can be deployed for remote sensing of nuclear, biological, and chemical weapons, detection of potential terrorist attacks, and reconnaissance [5].

1.1.2.3 Health Care Applications. WSNs can be used to monitor and track elders and patients for health care purposes, which can significantly relieve the severe shortage of health care personnel and reduce the health care expenditures in the current health care systems [8].

- *Behavior Monitoring.* Sensors can be deployed in a patient's home to monitor the behaviors of the patient. For example, it can alert doctors when the patient falls and requires immediate medical attention. It can monitor what a patient is doing and provide reminders or instructions over a television or radio.
- *Medical Monitoring.* Wearable sensors can be integrated into a wireless body area network (WBAN) to monitor vital signs, environmental parameters, and geographical locations, and thus allow long-term, noninvasive, and ambulatory monitoring of patients or elderly people with instantaneous alerts to health care personal in case of emergency, immediate reports to users about their current health statuses, and real-time updates of users' medical records [9].

1.1.2.4 Industrial Process Control. In industry, WSNs can be used to monitor manufacturing processes or the condition of manufacturing equipment. For example, wireless sensors can be instrumented to production and assembly lines to monitor and control production processes. Chemical plants or oil refiners can use sensors to monitor the condition of their miles of pipelines. Tiny sensors can be embedded into the regions of a machine that are inaccessible by humans to monitor the condition of the machine and alert for any failure. Traditionally, equipment is usually maintained on a schedule basis, for example, every 3 months for a check-up, which is costly. According to related statistics, a US equipment manufacturer spends billions of dollars in maintenance every year [6]. With sensor networks, maintenance can be conducted based on the condition of equipment, which is expected to significantly reduce the cost for maintenance, increase machine lifetime, and even save lives.

1.1.2.5 Security and Surveillance. WSNs can be used in many security and surveillance applications. For example, acoustic, video, and other kinds of sensors can be deployed in buildings, airports, subways, and other critical infrastructure, for example, nuclear power plants or communication centers to identify and track intruders, and provide timely alarms and protection from potential attacks. Unlike applications that do not require a fixed infrastructure, many security applications can afford to establish an infrastructure for power supply and communications [6].

1.1.2.6 Home Intelligence. WSNs can be used to provide more convenient and intelligent living environments for human beings.

- *Smart Home.* Wireless sensors can be embedded into a home and connected to form an autonomous home network. For example, a smart refrigerator connected to a smart stove or microwave oven can prepare a menu based on the inventory of the refrigerator and send relevant cooking

parameters to the smart stove or microwave oven, which will set the desired temperature and time for cooking [10]. The contents and schedules of TV, VCR, DVD, or CD players can be monitored and controlled remotely to meet the different requirements of family members.

- *Remote Metering.* Wireless sensors can be used to remotely read utility meters in a home, for example, water, gas, or electricity, and then send the readings to a remote center through wireless communication [11].

In addition to the above applications, self-configurable WSNs can be used in many other areas, for example, disaster relief, traffic control, warehouse management, and civil engineering. However, a number of technical issues must be solved before these exciting applications become a reality.

1.1.3 Network Design Objectives

The characteristics of sensor networks and requirements of different applications have a decisive impact on the network design objectives in terms of network capabilities and network performance. The main design objectives for sensor networks include the following several aspects:

- *Small Node Size.* Reducing node size is one of the primary design objectives of sensor networks. Sensor nodes are usually deployed in a harsh or hostile environment in large numbers. Reducing node size can facilitate node deployment, and also reduce the cost and power consumption of sensor nodes.
- *Low Node Cost.* Reducing node cost is another primary design objective of sensor networks. Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers and cannot be reused, it is important to reduce the cost of sensor nodes so that the cost of the whole network is reduced.
- *Low Power Consumption.* Reducing power consumption is the most important objective in the design of a sensor network. Since sensor nodes are powered by battery and it is often very difficult or even impossible to change or recharge their batteries, it is crucial to reduce the power consumption of sensor nodes so that the lifetime of the sensor nodes, as well as the whole network is prolonged.
- *Self-Configurability.* In sensor networks, sensor nodes are usually deployed in a region of interest without careful planning and engineering. Once deployed, sensor nodes should be able to autonomously organize themselves into a communication network and reconfigure their connectivity in the event of topology changes and node failures.
- *Scalability.* In sensor networks, the number of sensor nodes may be on the order of tens, hundreds, or thousands. Thus, network protocols designed for sensor networks should be scalable to different network sizes.

- *Adaptability.* In sensor networks, a node may fail, join, or move, which would result in changes in node density and network topology. Thus, network protocols designed for sensor networks should be adaptive to such density and topology changes.
- *Reliability.* For many sensor network applications, it is required that data be reliably delivered over noisy, error-prone, and time-varying wireless channels. To meet this requirement, network protocols designed for sensor networks must provide error control and correction mechanisms to ensure reliable data delivery.
- *Fault Tolerance.* Sensor nodes are prone to failures due to harsh deployment environments and unattended operations. Thus, sensor nodes should be fault tolerant and have the abilities of self-testing, self-calibrating, self-repairing, and self-recovering [12].
- *Security.* In many military applications, sensor nodes are deployed in a hostile environment and thus are vulnerable to adversaries. In such situations, a sensor network should introduce effective security mechanisms to prevent the data information in the network or a sensor node from unauthorized access or malicious attacks.
- *Channel Utilization.* Sensor networks have limited bandwidth resources. Thus, communication protocols designed for sensor networks should efficiently make use of the bandwidth to improve channel utilization.
- *QoS Support.* In sensor networks, different applications may have different quality-of-service (QoS) requirements in terms of delivery latency and packet loss. For example, some applications, for example, fire monitoring, are delay sensitive and thus require timely data delivery. Some applications, for example, data collection for scientific exploration, are delay tolerant but cannot stand packet loss. Thus, network protocol design should consider the QoS requirements of specific applications.

Most sensor networks are application specific and have different application requirements. It is not necessary and actually impractical to implement all the design objectives in a single network. Instead, only part of these objectives should be considered in the design of a specific network in order to meet its application requirements.

1.1.4 Network Design Challenges

The unique network characteristics present many challenges in the design of sensor networks, which involve the following main aspects:

- *Limited Energy Capacity.* Sensor nodes are battery powered and thus have very limited energy capacity. This constraint presents many new challenges

in the development of hardware and software, and the design of network architectures and protocols for sensor networks. To prolong the operational lifetime of a sensor network, energy efficiency should be considered in every aspect of sensor network design, not only hardware and software, but also network architectures and protocols.

- *Limited Hardware Resources.* Sensor nodes have limited processing and storage capacities, and thus can only perform limited computational functionalities. These hardware constraints present many challenges in software development and network protocol design for sensor networks, which must consider not only the energy constraint in sensor nodes, but also the processing and storage capacities of sensor nodes.
- *Massive and Random Deployment.* Most sensor networks consist of a large number of sensor nodes, from hundreds to thousands or even more. Node deployment is usually application dependent, which can be either manual or random. In most applications, sensor nodes can be scattered randomly in an intended area or dropped massively over an inaccessible or hostile region. The sensor nodes must autonomously organize themselves into a communication network before they start to perform a sensing task.
- *Dynamic and Unreliable Environment.* A sensor network usually operates in a dynamic and unreliable environment. On one hand, the topology of a sensor network may change frequently due to node failures, damages, additions, or energy depletion. On the other hand, sensor nodes are linked by a wireless medium, which is noisy, error prone, and time varying. The connectivity of the network may be frequently disrupted because of channel fading or signal attenuation.
- *Diverse Applications.* Sensor networks have a wide range of diverse applications. The requirements for different applications may vary significantly. No network protocol can meet the requirements of all applications. The design of sensor networks is application specific.

1.2 TECHNOLOGICAL BACKGROUND

The concept of WSNs was originally introduced three decades ago [2]. At that time, this concept was more a vision than a technology that could widely be exploited because of the state-of-the-art in sensor, computer, and wireless communication technologies. As a result, its application was mostly limited to large military systems. However, recent technological advances in MEMS, wireless communication, and low-cost manufacturing technologies have enabled the development of tiny, cheap, and smart sensors with sensing, processing, and communications capabilities, which has therefore stimulated the development of sensor networks and their applications.

1.2.1 MEMS Technology

MEMS is a key technology for manufacturing tiny, low-cost, and low-power sensor nodes. It is based on micromachining techniques, which have been developed to fabricate micron-scale mechanical components that are controlled electrically, resulting in MEMS. Through highly integrated processes, these electromechanical components can be fabricated with microelectronics, yielding complex systems. There are different micromachining techniques, for example, planar micromachining, bulk micromachining, and surface micromachining, which involve different fabrication processes [13,14]. Most micromachining processes begin with a substrate 100–100 μm thick, usually composed of silicon, other crystalline semiconductors, or quartz, on which a number of subsequent steps are performed, for example, thin-film deposition, photolithography, etching, oxidation, electroplating, machining, and wafer bonding. Different processes may involve different specific steps. By integrating different components together into a single process, the size of a sensor node can significantly be reduced. Of particular interest are the processes that combine CMOS transistors with micromachining capabilities. There are a number of techniques for performing post-process micromachining on foundry CMOS [15]. By using the MEMS technology, many components of sensor nodes can be miniaturized, for example, sensors, communication blocks, and power supply units, which can also lead to a significant reduction in cost through batch fabrication, as well as in power consumption. For a more detailed introduction of the MEMS technology and related techniques, the reader is referred to Refs. [13,14].

1.2.2 Wireless Communication Technology

Wireless communication is a key technology for enabling the normal operation of a WSN. Wireless communication has been extensively studied for conventional wireless networks in the last couple of decades and significant advances have been obtained in various aspects of wireless communication. At the physical layer, a variety of modulation, synchronization, and antenna techniques have been designed for different network scenarios and application requirements. At higher layers, efficient communication protocols have been developed to address various networking issues, for example, medium access control, routing, QoS, and network security. These communication techniques and protocols provide a rich technological background for the design of wireless communication in WSNs.

Today most conventional wireless networks use radio frequency (RF) for communication, including microwave and millimetre wave. The primary reason is that RF communication does not require a line of sight and provides omnidirectional links. However, RF has some limitations, for example, large radiators and low transmission efficiencies [16], which make RF not the best communication medium for tiny energy-constrained sensor nodes. Another possible medium for communication in sensor networks is free-space optical communication, which has many advantages over RF communication [16]. For example, optical

radiators, for example, mirrors and laser diodes, can be made extremely small. Optical transmission provides extremely high antenna gain, which produces higher transmission efficiencies. The high directivity of optical communication enables the use of spatial division multiple access (SDMA) [17], which requires no communication overhead and has the potential to be more energy efficient than the medium access schemes used in RF, such as time, frequency, and code division multiple access (TDMA, FDMA, and CDMA). However, optical communication requires a line of sight and accurate pointing for transmission, which also limit the use in many sensor network applications.

On the other hand, most communication protocols for conventional wireless networks, for example, cellular systems, wireless local area networks (WLANs), wireless personal area networks (WPANs), and MANETs, do not consider the unique characteristics of sensor networks, in particular, the energy constraint in sensor nodes. Therefore, they cannot be applied directly without modification. A new suite of network protocols are needed to address various networking issues, taking into account the unique characteristics of WSNs.

1.2.3 Hardware and Software Platforms

The development of WSNs largely depends on the availability of low-cost and low-power hardware and software platforms for sensor networks. With the MEMS technology, the size and cost of a sensor node have been significantly reduced. To achieve low-power consumption at the node level, it is necessary to incorporate power awareness and energy optimization in hardware design for sensor networks [18]. Low-power circuit and system design [19] has enabled the development of ultralow power hardware components, for example, microprocessors and microcontrollers. Meanwhile, power consumption can further be reduced through efficiently operating various system resources using some dynamic power management (DPM) technique [20]. For example, a commonly used DPM technique is to shutdown idle components or put them in a low-power state when there is little or no load to process, which can significantly reduce power consumption. Furthermore, additional energy savings also are possible in the active state by using a dynamic voltage scaling (DVS) technique [21]. It has been shown that DVS based power management has significantly higher energy efficiency compared to shutdown-based power management [18].

On the other hand, energy efficiency can significantly be enhanced if energy awareness is incorporated in the design of system software, including the operating system, and application and network protocols. At the core of the operating system is a task scheduler, which is responsible for scheduling a given set of tasks in the system under certain timing constraints. System lifetime can considerably be prolonged if energy awareness is incorporated into the task scheduling process [22].

The low-power circuit and system design, as well as power management techniques, have enabled the development of many low-power sensor hardware

and software platforms. The commercial availability of these platforms has significantly stimulated the further development of WSNs.

1.2.3.1 Hardware Platforms. Sensor node hardware platforms can be classified into three categories [6]: augmented general-purpose personal computers (PCs), dedicated sensor nodes, and system-on-chip (SoC) sensor nodes.

- *Augmented General-Purpose PCs.* This class of platforms include various low-power embedded PCs (e.g., PC104) and personal digital assistants (PDAs), which typically run off-the-shelf operating systems, for example, Win CE, Linux, or real-time operating systems, and use standard wireless communication protocols, for example, IEEE 802.11 or Bluetooth. Compared with dedicated and SoC sensor nodes, these PC-like platforms have higher processing capability and thus can incorporate a richer set of networking protocols, popular programming languages, middleware, application programming interfaces (APIs), and other off-the-shelf software. However, they require more power supply.
- *Dedicated Sensor Nodes.* This class of platforms include the Berkeley mote family [23], the UCLA Medusa family [24], and MIT μAMP [25], which typically use commercial off-the-shelf chips and are characterized by small form factors, low-power processing and communication, and simple sensor interfaces.
- *System-on-chip Sensor Nodes.* This class of platforms include Smart Dust [26] and the BWRC PicoNode [27], which are based on CMOS, MEMS, and RF technologies, and aims to have extremely low power and small footprint with certain sensing, computation, and communication capabilities.

Among all the above hardware platforms, the Berkeley Motes have received wide popularity in the research community of sensor networks due to their small form factor, open source software development, and commercial availability [6].

1.2.3.2 Software Platforms. A software platform can be an operating system that provides a set of services for applications, including file management, memory allocation, task scheduling, peripheral device drivers, and networking, or it can be a language platform that provides a library of components to programmers [6]. Typical software platforms for sensor networks include TinyOS [22], nesC [28], TinyGALS [29], and Moté [30]. TinyOS is one of the earliest operating systems supporting sensor network applications on resource-constrained hardware platforms, for example, the Berkeley motes. This system is event driven and uses only 178 bytes of memory, but supports communication, multitasking, and code modularity. It has no file system, supports only static memory allocation, implements a simple task scheduler, and provides minimal

device and networking abstractions. The nesC is an extension of C language to support the design of TinyOS. It provides a set of language constructs and restrictions to implement TinyOS components and applications. TinyGALS is a language for TinyOS, which provides a way of building event-triggered concurrent execution from thread-unsafe components. Unlike nesC, it addresses concurrency at the system level rather than at the component level. Moté is a virtual machine for the Berkeley motes. It defines virtual machine instructions to abstract those common operations, for example, polling sensors and accessing internal states. Therefore, software written in Moté instructions does not have to be rewritten to accommodate a new hardware platform with support for the virtual machine.

1.2.4 Wireless Sensor Network Standards

To facilitate the worldwide development and application of WSNs, there is a need for building a large low-cost market for sensor products in the field. For this purpose, it is important to specify relevant standards so that sensor products from different manufacturers may interoperate. A lot of efforts have been made and are under way in many standardization organizations in order to unify the market, leading to low-cost and interoperable devices, and avoiding the proliferation of proprietary incompatible network protocols. To a certain extent, the success of WSNs as a technology will largely rely on the success of these standardization efforts.

1.2.4.1 The IEEE 802.15.4 Standard. The IEEE 802.15.4 [31] is a standard developed by IEEE 802.15 Task Group 4, which specifies the physical and MAC layers for low-rate WPANs. As defined in its Project Authorization Request, the goal of Task Group 4 is to "provide a standard for ultralow complexity, ultralow cost, ultralow power consumption, and low-data rate wireless connectivity among inexpensive devices". The first release of the IEEE 802.15.4 standard was delivered in 2003 and is freely distributed in [32]. This release was revised in 2006, but the new release is not yet freely distributed. Its protocol stack is simple and flexible, and does not require any infrastructure. The standard has the following features [32]:

- Data rates of 250 kbps, 40 kbps, and 20 kbps.
- Two addressing modes: 16-bit short and 64-bit IEEE addressing.
- Support for critical latency devices, for example, joysticks.
- The CSMA-CA channel access.
- Automatic network establishment by the coordinator.
- Fully handshaking protocol for transfer reliability.
- Power management to ensure low-power consumption.
- Some 16 channels in the 2.4-GHz ISM band, 10 channels in the 915-MHz band, and 1 channel in the 868-MHz band.

The physical layer of the IEEE 802.15.4 standard has been specified to coexist with other IEEE standards for wireless networks, for example, IEEE 802.11 (WLAN) and IEEE 802.15.1 (Bluetooth). It features activation and deactivation of the radio transceiver and transmission of packets on the physical medium. It operates in one of the following three license-free bands:

- 868–868.6 MHz (e.g., Europe) with a data rate of 20 kbps.
- 902–928 MHz (e.g., North America) with a data rate of 40 kbps.
- 2400–2483.5 MHz (worldwide) with a data rate of 250 kbps.

The MAC layer provides data and management services to the upper layers. The data service enables transmission and reception of MAC packets over the physical layer. The management services include synchronization, timeslot management, and association and disassociation of devices to the network. Moreover, the MAC layer implements basic security mechanisms. For a comprehensive introduction of the IEEE 802.15.4 standard, the author is referred to Chapter 13.

1.2.4.2 The ZigBee Standard. The IEEE 802.15.4 standard only defines the physical and MAC layers without specifying the higher protocol layers, including the network and application layers. The ZigBee standard [33] is developed on top of the IEEE 802.15.4 standard and defines the network and application layers. The network layer provides networking functionalities for different network topologies, and the application layer provides a framework for distributed application development and communication. The two protocol stacks can be combined together to support short-range low data rate wireless communication with battery-powered wireless devices. The potential applications of these standards include sensors, interactive toys, smart badges, remote controls, and home automation.

The ZigBee protocol stack was proposed at the end of 2004 by the ZigBee Alliance [34], an association of companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring, and control products based on an open global standard. The first release of ZigBee was revised at the end of 2006, which introduces extensions on the standardization of application profiles and some minor improvements to the network and application layers. Both releases can be freely downloaded at Ref. [34]. For a comprehensive introduction of the IEEE 802.15.4 standard, the author is referred to Ref. [35] or Chapter 13.

1.2.4.3 The IEEE 1451 Standard. The IEEE 1451 standards are a family of Smart Transducer Interface Standards that defines a set of open, common, network-independent communication interfaces for connecting transducers (i.e., sensors or actuators) to microprocessors, instrumentation systems, and control/field networks [36]. Transducers have a wide variety of applications in industry, for example, manufacturing, industrial control, automotive, aerospace, building,

and biomedicine. Since the transducer market is very diverse, transducer manufacturers are seeking ways to build low-cost, networked, and wireless smart transducers. But one problem for transducer manufacturers is the large number of wired and wireless networks on the market today. Currently, it is too costly for transducer manufacturers to produce unique smart transducers for the large number of networks on the market. Therefore, a set of open standards that are universally accepted, for example, the suite of IEEE 1451 smart transducer interface standards, are developed to address these issues.

The key feature of these standards is the definition of transducer electronic data sheets (TEDS), which is a memory device attached to a transducer for storing transducer identification, calibration, correction data, measurement range, manufacture-related information, and so on. The objective of 1451 is to make it easier for transducer manufacturers to develop smart devices and to interface those devices to networks, systems, and instruments by incorporating existing and emerging sensor and networking technologies. In another word, it is to allow the access of transducer data through a common set of interfaces whether the transducers are connected to systems or networks via a wired or wireless medium. The family of IEEE 1451 standards is sponsored by the Sensor Technology Technical Committee of the IEEE Instrumentation and Measurement Society. The definitions of the IEEE 1451 standards [36] are briefly described below:

- IEEE P1451.0 defines a set of common commands, common operations, and TEDS for the family of IEEE 1451 smart transducer standards. Through this command set, one can access any sensors or actuators in the 1451-based wired and wireless networks.
- IEEE 1451.1 defined a common object model describing the behavior of smart transducers, a measurement model that streamlines measurement processes, and the communication models used for the standard, which includes the client-server and publish-subscribe models.
- IEEE 1451.2 defined a transducers-to-NCAP interface and TEDS for a point-to-point configuration.
- IEEE 1451.3 defined a transducer-to-NCAP interface and TEDS for multidrop transducers using a distributed communication architecture. It allowed many transducers to be arrayed as nodes, on a multidrop transducer network, sharing a common pair of wires.
- IEEE 1451.4 defined a mixed-mode interface for analog transducers with analog and digital operating modes.
- IEEE P1451.5 defines a transducer-to-NCAP interface and TEDS for wireless transducers. Protocol standards for wireless networks, for example, 802.11 (WiFi), 802.15.1 (Bluetooth), and 802.15.4 (ZigBee), are being considered as some of the physical interfaces for IEEE P1451.5.
- IEEE P1451.6 defines a transducer-to-NCAP interface and TEDS using the high-speed CANopen network interface. Both intrinsically safe and nonintrinsically safe applications are being supported.

1.3 FEATURES OF THIS BOOK

Networking is one of the most important aspects in the design of WSNs, which involves a variety of network architectural and protocol design issues. Due to the unique characteristics of sensor networks, conventional network protocols cannot be applied directly to sensor networks without modification. A new suite of network protocols must be developed to address the unique characteristics and constraints, in particular, the energy constraint, in sensor networks. This book focuses on the major networking issues in the design of WSNs, including medium access control, routing and data dissemination, node clustering, node localization, transport protocols, time synchronization, and network security. The aim of this book is to provide a comprehensive and systematic introduction of the fundamental concepts, major issues, and effective solutions in the networking aspect of WSNs. The main features of this book include the following:

- Giving an insight into wireless sensor networks from a networking perspective.
- Providing a comprehensive and systematic introduction of the fundamental concepts, major issues, and effective solutions in wireless sensor networking.
- Striking a balance between fundamental concepts and state-of-the-art technologies.
- Contributed by a group of leading researchers who are internationally recognized in the field.
- Intended for a wide range of audience, including academic researchers, graduate students, industry practitioners, and research engineers.
- Including a comprehensive up-to-date bibliography.

1.4 ORGANIZATION OF THIS BOOK

This book is organized into 14 chapters. Chapter 1 serves as an introduction to the whole book. The unique network characteristics, typical network applications, and technological background are introduced. Then the major network design objectives and challenges, and the focus and features of this book are described.

Chapter 2 presents a brief overview of network architectures and introduces a protocol stack for WSNs.

Chapter 3 is dedicated to medium access control (MAC) in WSNs. The fundamental concepts on MAC and traditional MAC protocols for wireless networks are introduced, the major challenges in MAC design for sensor networks are discussed, and an overview of MAC protocols for WSNs are presented.

Chapter 4 focuses on routing and data dissemination in WSNs. The fundamental concepts on routing and data dissemination are introduced and the major challenges in routing and data dissemination are discussed. Moreover, a taxonomy

of routing protocols for WSNS is introduced and based on this taxonomy a survey of routing and data dissemination protocols for WSNs is presented.

Chapter 5 is dedicated to broadcasting, multicasting, and geocasting in WSNs. The concepts of broadcasting, multicasting, and geocasting are introduced, the major challenges in geocasting, multicasting, and broadcasting are discussed, and an overview of typical broadcasting, multicasting, and geocasting algorithms are presented.

Chapter 6 concentrates on node clustering in WSNs. The purpose of node clustering and the fundamental concepts on node clustering are introduced, and a variety of node clustering algorithms for WSNs is presented.

Chapter 7 is dedicated to query processing and data aggregation in WSNs. The concept of query processing and the importance of data aggregation are introduced. The major challenges in query processing and data aggregation are discussed. The chapter also presents an overview of typical query processing and data aggregation techniques for WSNs.

Chapter 8 focuses on node localization in WSNs. The importance of node localization is introduced, the major challenges in node localization are discussed, and an overview of typical localization algorithms is presented.

Chapter 9 addresses time synchronization in WSNs. The importance of time synchronization is explained, the major challenges in time synchronization are introduced, and effective synchronization protocols for WSNs are presented.

Chapter 10 is dedicated to energy efficiency and power control in WSNs. The need for energy efficiency and power control is explained, the major challenges in designing efficient power conservation mechanisms are discussed, and an overview of major power conservation mechanisms for WSNs are presented.

Chapter 11 focuses on transport protocols and quality of service in WSNs. The fundamental concepts on transport protocols and QoS are introduced, the major challenges in the design of transport protocols for quality of service are discussed, and an overview of transport protocols for WSNs are presented.

Chapter 12 is dedicated to network security in WSNs. The importance of security in WSNs is described, the major challenges in designing security mechanisms are discussed, and a variety of effective security techniques for WSNs are presented.

Chapter 13 presents an overview of standardization activities and relevant standards for WSNs, focused on the IEEE 802.15.4 and ZigBee standards.

Chapter 14 presents an overview of the recent evolution of the sensor network paradigm, as well as future research directions in the networking aspect of WSNs.

REFERENCES

[1] "21 ideas for the 21st century", *Business Week*, Aug. 30 1999, pp. 78–167.

[2] C.-Y. Chong and S. P. Kumar, "Sensor networks: Evolution, opportunities, and challenges", *Proceedings of the IEEE*, vol. 91, no. 8, Aug. 2003, pp. 1247–1256.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", *IEEE Communications Magazine*, vol. 40, no. 8, Aug. 2002, pp. 102–114.

[4] D. Estrin, D. Culler, K. Pister, and G. Sukhatme, "Connecting the physical world with pervasive networks", *IEEE Pervasive Computing*, Jan. 2002, pp. 59–69.

[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey", *Computer Networks*, vol. 38, no. 4, Mar. 2002, pp. 393–422.

[6] F. Zhao and L. Guibas, *Wireless Sensor Networks: An Information Processing Approach*, Morgan Kaufmann Publishers, San Francisco, CA, 2004.

[7] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless sensor networks for habitat monitoring", in *Proceedings of 1st ACM International Workshop on Wireless Sensor Networks and Applications (WSNA'02)*, Atlanta, GA, Sept. 2002, pp. 88–97.

[8] R. Jafari, A. Encarnacao, A. Zahoory, F. Dabiri, H. Noshadi, and M. Sarrafzadeh, "Wireless sensor networks for health monitoring", in *Proceedings of 2nd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'05)*, July 2005, pp. 479–481.

[9] D. Trossen and D. Pavel, "Sensor networks, wearable computing, and healthcare Applications", *IEEE Pervasive Computing*, vol. 6, no. 2, Apr.–June 2007, pp. 58–61.

[10] C. Herring and S. Kaplan, "Component-based software systems for smart environments", *IEEE Personal Communications*, vol. 7, no. 5, Oct. 2000, pp. 60–61.

[11] A. J. Goldsmith and S. B. Wicker, "Design challenges for energy-constrained ad hoc wireless networks", *IEEE Wireless Communications*, vol. 9, no. 4, Aug. 2002, pp. 8–27.

[12] F. Koushanfar, M. Potkonjak, and A. Sangiovanni-Vincentelli, "Fault-tolerance techniques for ad hoc sensor networks", *Proceedings of IEEE Sensors*, vol. 2, June 2002, pp. 1491–1496.

[13] R. F. Pierret, *Introduction to Microelectronic Fabrication*, Addison-Wesley, Menlo Park, CA, 1990.

[14] S. D. Senturia, *Microsystem Design*, Kluwer Academic Publishers, Norwell, MA, 2001.

[15] A. E. Franke, T.-J. King, and R. T. Howe, "Integrated MEMS technologies", *MRS Bull.*, vol. 26, no. 4, 2001, pp. 291–295.

[16] B. Warneke, "Miniaturizing sensor networks with MEMS", *SMART DUST: Sensor Network Applications, Architecture, and design (edited)*, CRC, Boca Raton, FL, 2006, pp. 5-1–5-9.

[17] J. M. Kahn, R. You, P. Djahani, A. G. Weisbin, Beh Kian Teik, and A. Tang, "Imaging diversity receivers for high-speed infrared wireless communication", *IEEE Communications Magazine*, vol. 36, no.12, Dec. 1998, pp. 88–94.

[18] V. Raghunathan, C. Schurgers, S. Park, and M. B. Srivastava, "Energy-aware wireless microsensor networks", *IEEE Signal Processings Magazine*, vol. 19, no. 2, Mar. 2002, pp. 40–50.

[19] A. P. Chandrakasan and R. W. Broderson, *Low Power CMOS Digital Design*, Kluwer Academic Publishers, Norwell, MA, 1996.

[20] L. Benini and G. DeMicheli, *Dynamic Power Management: Design Techniques and CAD Tools*, Kluwer Academic Publishers, Norwell, MA, 1997.

[21] T. A. Pering, T. D. Burd, and R. W. Brodersen, "The simulation and evaluation of dynamic voltage scaling algorithms", in *Proceedings of 1998 International Symposium on Low Power Electronics and Design (ISLPED'98)*, Monterey, CA, Aug. 1998, pp. 76–81.

[22] J. Hill, R. Szewcyk, A. Woo, D. Culler, S. Hollar, and K. Pister, "System architecture directions for networked sensors", in *Proceedings of 9th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS IX)*, Cambridge, MA, Nov. 2000, pp. 93–104.

[23] A. Savvides and M. B. Srivastava, "A distributed computation platform for wireless embedded sensing", in *Proceedings of International Conference on Computer Design (ICCD'02)*, Freiburg, Germany, Sept. 2002, pp. 220–225.

[24] A. Chandrakasan, R. Min, M. Bhardwaj, S.-H. Cho, and A. Wang, "Power aware wireless microsensor systems", in *Proceedings of 32nd European Solid-State Device Research Conference (ESSDERC'02)*, Florence, Italy, Sept. 2002, pp. 47–54.

[25] J. M. Khan, R. H. Katz, and K. Pister, "Next century challenges: Mobile networking for smart dust", in *Proceedings of 5th International Conference on Mobile Computing and Networking (MobiCom'99)*, Seattle, WA, Aug. 1999, pp. 271–278.

[26] J. Rabaey, J. Ammer, J. da Silva, D. Patel, and S. Roundy, "Picoradio supports ad-hoc ultra-low power wireless networking", *IEEE Computer Magazine*, July 2002, pp. 42–48.

[27] F. Yao, A. Demers, and S. Shenker, "A scheduling model for reduced CPU energy", in *Proceedings of 36th Annual Symposium on Foundations of Computer Science (FOCS'95)*, Oct. 1995, pp. 374–382.

[28] D. Gay, P. Levis, R. von Behren, M. Welsh, E. Brewer, and D. Culler, "The nesC language: A holistic approach to network embedded systems", in *Proceedings of 2003 ACM SiGPLAN Conference on Programming Language Design and Implementation (PLDI'03)*, San Diego, CA, June 2003, pp. 1–11.

[29] E. Cheong, J. Liebman, J. Liu, and F. Zhao, "TinyGALS: A programming model for event-driven embedded systems", in *Proceedings of 18th Annual ACM Symposium on Applied Computing (SAC'03)*, Melbourne, FL, Mar. 2003, pp. 698–704.

[30] P. Levis and D. Culler, "Moté: A tiny virtual machine for sensor networks", in *Proceedings of 10th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS X)*, San José, CA, Oct. 2002, pp. 85–95.

[31] Institute of Electrical and Electronics Engineers, Inc., "IEEE Std. 802.15.4–2003: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (LR-WPANs)", New York, IEEE Press. Oct. 2003.

[32] Available at http://www.ieee802.org/15/pub/TG4.html

[33] ZigBee Alliance, "ZigBee Specifications", Dec. 2006.

[34] Available at http://www.ZigBee.org/en/index.asp

[35] P. Baronti, P. Pillai, V. Chook, S. Chessa, A. Gotta, and Y. F. Hu, "Wireless Sensor Networks: a Survey on the State of the Art and the 802.15.4 and ZigBee Standards", *Computer Communications*, vol. 30, no. 7, May 2007, pp. 1655–1695.

[36] Available at http://ieee1451.nist.gov/