Chapter 1
Introduction

The development of microcontrollers, communication technology, microelectromechanical systems (MEMS), and nanotechnology allowed for research and development of new systems for sensing and communication called wireless sensor networks. Such networks are characterized as ad hoc (no previous setup or supporting infrastructure is required), utilize novel communication protocols, cooperatively monitor phenomena of interest, and communicate recorded data to the central processing station, usually called the base station. As the word *wireless* indicates, such networks of sensors communicate using wireless communication channels, allowing for easy deployment, control, maintenance, and possible sensor replacements.

Wireless sensors in networked systems are often called *nodes*, as they are built of many more components than just sensors. Sensor nodes are, from a hardware perspective, small form-factor embedded computers coupled with a variety of sensors that are chosen by the user depending on the targeted application. Sensor nodes usually have built-in microprocessors or microcontrollers, power supply in form of a battery, a memory, a radio, communication ports, interface circuits, and finally sensors for specific applications. They are complex embedded devices that combine from computer, communication, networking, and sensors technologies.

Being a network of small computer-like embedded devices, wireless sensor networks are significantly different from general computer-based data networks such as the Internet or Ethernet. Wireless sensor networks (WSNs) do not have topologies that are characteristic for Local Area Networks (LAN) such as bus, ring, or star. They are mostly ad hoc networks deployed randomly in the field relying mostly on the widely adopted underlying IEEE 802.15.4 standard for embedded devices. They are application-specific with communication and networking sometimes specifically designed to accommodate targeted applications. Bounded by numerous constraints, usually not seen in general data networks, such as limited energy and bandwidth availability, small form-factor, large number of nodes deployed over wide open areas, and others, WSNs' networking and communication must be creatively adjusted to support specific applications which we discuss in

R.R. Selmic et al., *Wireless Sensor Networks*,
DOI 10.1007/978-3-319-46769-6_1

later chapters. Thus, a new cross-layer optimization and changes in communication protocols have been developed to address specific requirements for sensor networks.

Exposed to numerous constraints, environmental and technological difficulties, and driven by market needs, WSNs have evolved and developed numerous characteristics that distinguish them from standard computer-based networked systems. They are capable of unattended operation with very limited or no supervision. The main sensor network components, the sensor nodes, are inexpensive and usually disposable. The sensor network supports dynamic topologies that can overcome node or sensor failures, drops in communication links, or movement of nodes. Nodes can also operate in harsh and dangerous environments with a human operator standing at a safe distance. Due to their small size and lack of cables, WSNs are not disruptive for the environment or industrial processes. Compared to individual sensors assigned to measure and observe specific phenomena of interest, sensor networks are capable of cooperative measurements and cooperative in-network data processing.

In the following sections, we first give an overview of the sensor networks which are a super set of the wireless sensor networks and then give brief details of wireless sensor networks and the applications of wireless sensor networks.

1.1 Sensor Networks

Sensor networks are composed of a large number of sensor nodes that are deployed to collectively monitor and report any phenomena of interest. In a sensor network, the physical layer specifies electrical and mechanical interface to the transmission medium and can be wired, wireless, or a combination of both. Sensor networks are a superset of WSNs and, as such, share some common attributes that are integral to all sensor network systems.

We first discuss general attributes of sensor networks and in subsequent sections focus on sensor networks with wireless signal transmission.

- **Phenomena of Interest:** Based on the domain or environment in which a sensor network operates, phenomena of interest can be purely physical (for example, leakage of hazardous plumes in a chemical factory, radiation activity leakage in a nuclear waste storage facility, occurrence of forest fires, etc.) or can be observable manifestations of a dynamical physical phenomenon (for example, occurrence of anomalies in aerial imagery due to aircraft jitter, occurrence of a runtime faults in an embedded system due to an ill-conceived electronic circuitry, etc.).
- **Composition and Type:** A sensor network can be homogenous (i.e., composed of same type of sensors) or heterogeneous (i.e., different types of sensors) in composition. Further, a sensor network can be a passive network, comprising sensors that detect phenomena via radiations emitted by an object or its

surrounding environment (e.g., acoustic, seismic, video, and magnetic sensor networks) or an active sensor network comprising sensors that probe into the environment by sending signals and measuring responses (e.g., radar and lidar). A sensor network can be stationary (e.g., seismic sensor network) or mobile (e.g., sensors mounted on mobile robots and unmanned aerial vehicles).

- **Sensor Deployment:** It involves placing sensor nodes within the permissible neighborhood of the phenomena of interest, so that all defined constraints on the quality of sensing are satisfied. Based on the sensing environment, sensor network deployment can be planned (e.g., as in inventory storage facilities, nuclear power plants, etc.,) or ad hoc (e.g., air-dropped for monitoring movement in hostile territories).
- **Monitoring, Processing, and Reporting:** It involves communication and processing within groups of sensor nodes, base stations, command and control units, and all other entities that gather pertinent measurements about the phenomena of interest and eventually make decisions to actuate appropriate response. Communication can be wired or wireless, depending upon the application requirement and sensing environment. Similarly, depending on the target application, processing can be centralized, i.e., all data are sent to and processed by a centralized base station or autonomous, i.e., each node takes its own decision, or a hybrid, i.e., semi-autonomous or loosely centralized.

Fundamental advances in microelectromechanical systems (MEMS), fabrication technologies, wireless communication technologies, low-power processing, and distributed computational intelligence have led to the development of low-cost high-density sensor networks, which not only provide large spatial coverage and high-sensing resolutions but also have high levels of fault tolerance, endurance, and flexibility in handling operational uncertainty. Consequently, sensor networks are becoming ubiquitous in many application areas as diverse as military, health, environment and habitat monitoring, and home, to name a few. Below is a partial list of some application areas in which sensor networks have shown promising utility.

- **Military Applications:** Sensor network research was initially motivated by military applications such as monitoring equipment and inventory, battlefield surveillance and reconnaissance, target tracking, battlefield damage assessment, nuclear, chemical, and biological weapon detection and tracking, etc. Military applications demand rapid deployment, robust sensing in hostile terrains, high levels of longevity, energy conservation, and information processing to extract useful, reliable, and timely information from the deployed sensor network.
- **Environment Monitoring Applications:** Include chemical or biological detection, large scale monitoring and exploration of land and water masses, flood detection, monitoring air, land, and water pollution, etc.
- **Habitat Monitoring Applications:** Include forest fire detection, species population measurement, species movement tracking in biological ecosystems, tracking bird migrations, vegetation detection, soil erosion detection, etc.

- **Health Applications:** Include real-time monitoring of human physiology, monitoring patients and doctors in hospitals, monitoring drug administration, blood glucose level monitors, organ monitors, cancer detectors, etc.
- **Infrastructure Protection Applications:** Include monitoring nation's critical infrastructure and facilities (e.g., power plants, communication grids, bridges, office buildings, museums, etc.) from naturally occurring and human-caused catastrophes. Sensor networks in these applications are expected not only to provide reliable measurements to facilitate early detection but are also required to provide effective spatial information for localization.
- **Home Applications:** Sensor networks are being deployed in homes to create smart homes and improve the quality of life of its inhabitants. Recently, a new paradigm of computing, called 'ambient intelligence' has emerged with a goal to leverage sensor networks and computational intelligence to recreate safe, secure, and intelligent living spaces for humans.

Next, we briefly discuss some important design factors that arise in the application of sensor networks.

- **Fidelity and Scalability:** Depending on the operational environment and the phenomenon being observed, fidelity can encompass a multitude of quality or performance parameters such as spatial and temporal resolution, consistency in data transmission, misidentification probability, event detection accuracy, latency of event detection, and other quality of service-related measures. Scalability broadly refers to how well all the operational specifications of a sensor network are satisfied with a desired fidelity, as the number of nodes grows without bound. Depending on the measure of fidelity, scalability can be formulated in terms of reliability, network capacity, energy consumption, resource exhaustion, or any other operational parameter as the number of nodes increases. While it is very difficult to simultaneously maintain high levels scalability and fidelity, tuning sensor networks to appropriately tradeoff scalability and fidelity has worked well for most applications.
- **Energy Consumption:** Individual sensor nodes, electronic circuitry supporting the nodes, microprocessors, and onboard communication circuitry are the primary consumers of energy. In case of WSNs, the most likely energy source is a lithium-ion battery. Depending on the operational environment, energy constraints can be an important factor in sensor network design. In structured and friendly environments (e.g., industrial infrastructure, hospitals, and homes), specific arrangements can be conceived to replenish onboard batteries on individual nodes for WSNs. However, in harsh environments and large territories (typical in military and habitat monitoring applications), replenishing energy may be impractical or even impossible. In such situations, energy conservation becomes a critical issue for extending a sensor network's longevity. Energy conservation can be addressed at multiple levels, starting from the designing energy-aware sensors, energy-aware electronic circuitry to energy conserving communication, processing, and tasking.

- **Deployment, Topology, and Coverage:** Depending on the operational environment, constituent nodes in a sensor network can be deployed in a planned fashion (choosing specific positions for each node) or in a random fashion (dropping nodes from an aircraft). Deployment can be an iterative process, i.e., sensors can be periodically added into the environment or can be a one-time activity. Deployment affects important parameters such as node density, coverage, sensing resolution, reliability, task allocations, and communications. Based on the deployment mechanism, environment characteristics, and operational dynamics, a sensor network's topology can range from static and properly defined to dynamic and ad hoc. In some environments, the topology of a sensor network can be viewed as a continuous time dynamical system that evolves (or degrades) over time largely due to exogenous stimuli or internal activity (for example, node tampering is an external stimuli while power exhaustion is an internal activity—both have a potential to drastically change the topology of the sensor network). In its simplest form, a sensor network can form a single-hop network with every node communicating with its base station. Centralized sensor networks of this kind form a star-like network topology. A sensor network may also form an arbitrary multi-hop network, which takes two or more hops to convey information from a source to a destination. Multi-hop networks are more common in mobile sensing, where the ad hoc topology demands message delivery over multiple hops. Topology affects many network characteristics such as latency, robustness, and capacity. The complexity of data routing and processing also depends on the topology. Coverage measures the degree of coverage area of a sensor network. Coverage can be sparse, i.e., only parts of environment fall under the sensing envelope, or dense, i.e., most parts of environment are covered. Coverage can also be redundant, i.e., the same physical space is covered by multiple sensors. Coverage is mainly determined by the sensing resolution demands of an application.
- **Communication and Routing:** Because sensor networks deal with limited bandwidth, processing, and energy, operate in highly uncertain and hostile environments (e.g., battlefields), constantly change topology and coverage, lack global addressing, and have nodes that are noisy and failure-prone, traditional Internet communication protocols such as Internet Protocols (IP), including mobile IP may not be adequate. Most communication specifications originate from answering the following question: Given a sensor network, what is the optimal way to route messages so that the delivery between source and destination occurs with a certain degree of fidelity? Many routing schemes have been proposed, with each routing scheme optimizing a suitable fidelity metric (e.g., sensing resolution) under defined constraints of operation (e.g., energy constraints). Popular routing schemes include data-centric routing, in which data are requested on demand through queries to specific sensing regions (e.g., directed diffusion, SPIN: Sensor Protocols for Information via Negotiation, CADR: Constrained Anisotropic Diffusion Routing, and ACQUIRE: Active Query Forwarding In Sensor Networks); flooding, and gossiping, which are based on

broadcasting messages to all or selected neighbor nodes; energy-aware routing (e.g., SMECN: Small Minimum Energy Communication Network, GAF: Geographic Adaptive Fidelity, and GEAR: Geographic and Energy Aware Routing); hierarchical routing, in which messages are passed via multi-hop communication within a particular cluster and by performing data aggregation and fusion to decrease the number of transmitted messages (e.g., LEACH: Low-Energy Adaptive Clustering Hierarchy, PEGASIS: Power-Efficient Gathering in Sensor Information Systems, and TEEN: Threshold Sensitive Energy Efficient Sensor Network Protocol).

- **Security:** Security Requirements of a sensor network encompass the typical requirements of a computer network plus the unique requirements specific to the sensor network application. Security in sensor networks aims to ensure data confidentiality—an adversary should not be able to steal and interpret data/communication; data integrity—an adversary should not be able to manipulate or damage data; and data availability—an adversary should not be able to disrupt data flow from source to sink. Sensor networks are vulnerable to several key attacks. Most popular are eavesdropping (adversary listening to data and communication), denial-of-service attacks (range from jamming sensor communication channels to more sophisticated exploits of 802.11 MAC protocol), Sybil attack (in which malicious nodes assume multiple identities to degrade or disrupt routing, data aggregation, and resource allocation), traffic analysis attacks (aim to identify base stations and hubs within a sensor network or aim to reconstruct topologies by measuring the traffic flow rates), node replication attacks (involves adding a new node which carries the id of an existing node in the sensor network to mainly disrupt routing and aggregation), and physical attacks (range from node tampering to irreversible node destruction). Several defenses have been proposed against attacks on sensor networks. Solutions that ensure data confidentiality use energy-aware cryptographic protocols, which are mostly based on Triple-DES, RC5, RSA, and AES algorithms. Defenses against denial-of-service attacks include rouge node identification and elimination, multi-path routing, and redundant aggregation. Primary defenses against Sybil attacks are direct and indirect node validation mechanisms. In direct validation a trusted node directly tests the joining node's identity. In indirect validation, another two levels of trusted nodes are allowed to testify for (or against) the validity of a joining node. Defenses against node replication attacks include authentication mechanisms and multicast strategies, in which new nodes are either authenticated through the base station or (in the case of multicast strategy) the new nodes are authenticated via a group of designated nodes called 'witnesses'. Strategies to combat traffic analysis attacks include random walk forwarding, which involves occasionally transferring messages to a pseudo base station, fake packet generation, and fake flow generation.

1.2 Wireless Sensor Networks

1.2.1 Historical Perspective, Aloha Networks

The first experiment with wireless signal transmission was carried out in 1893 by Nikola Tesla. A few years later, Tesla was able to remotely control small boats, setting a path for the later development of guided missiles and precision-guided weapons. The first amplitude modulation (AM) signals were generated in 1906 and high frequency radio signals in 1921. Armstrong is credited for development of first frequency modulated signal 1931. Metcalfe and Boggs at Xerox PARC are credited for creation of Ethernet in 1973 with an initial transmission rate of 2.9 Mbit/s. That was later a foundation for creation of IEEE 802.3 standard that is still being developed and expanded. In 1997, IEEE 802.11 standard was created with a bandwidth of 2 Mbit/s with subsequent modification and addition to the standard. In 1999, 802.15.1, commonly called Bluetooth, was formulated for short-range wireless communication between embedded devices.

Aloha communication scheme, invented by Norman Abramson in 1970 at the University of Hawaii [1], was one of the first networking protocols that successfully networked computer systems, in this case different campuses of the University of Hawaii on different islands. The concepts are widely used today in Ethernet and sensor networks communications, Figs. 1.1 and 1.2. The protocol allows computers on each island to transmit a data packet whenever there is a packet ready to be sent. If the packet is received correctly, the central computer station sends an acknowledgment. If the transmitting computer does not receive the acknowledgment after some time due to transmission error, which can be due to collision of packets transmitted at the same time from another system, the transmitting computer resends the packet. This process is repeated until the sending computer receives the acknowledgment from the central computer. The protocol works well for simple networks with low number of transmitting stations. However, for networks with multiple nodes, the protocol causes small throughput due to increase of collisions.

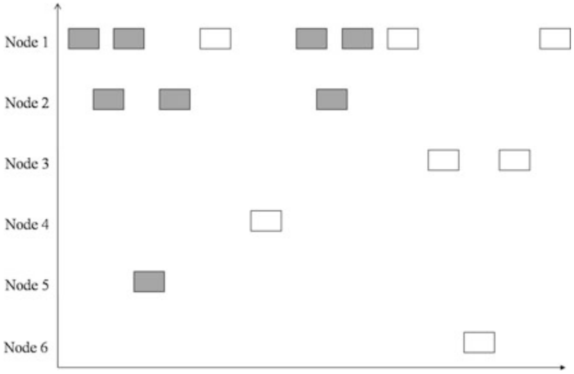

Fig. 1.1 Pure Aloha protocol where nodes transmit packets randomly with possible collisions with packets from other nodes (*gray*)

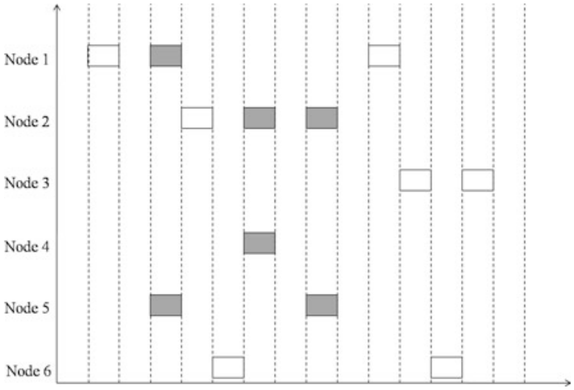

Fig. 1.2 Slotted Aloha protocol where nodes transmit packets only at pre-assigned time intervals; however, the collisions with packets from other nodes are still possible (*gray*)

A modification of the algorithm allows nodes to transmit the same size packets only at pre-specified slot boundary. In this case transmission is not completely random and the number of collisions is reduced in half compared to the pure aloha protocol.

Aloha protocols fall into the category of contention-based protocols where there is a possible contention between nodes on the network (all nodes contend for the channel causing possible collisions). Other Medium Access Control (MAC) contention-based protocols include multiple access collision avoidance protocol (MACA), modified version such as multiple access with collision avoidance for wireless (MACAW), busy tone multiple access (BTMA), floor acquisition multiple access (FAMA), IEEE 802.11, and others [22].

1.2.2 *Background on Wireless Sensor Networks*

Wireless sensor networks (WSNs) are networks of autonomous sensor devices where communication is carried out through wireless channels. WSNs have integrated computing, storing, networking, sensing, and actuating capabilities [2, 3, 6, 7, 8, 20, 30, 35] with overlapping sensing, computing, and networking technologies (other important references and books in this area are given at the end of the section; for a good overview paper see for instance [19]). These networks consist of a number of sensor nodes (static and mobile) with multiple sensors per node that communicate with each other and the base station through wireless radio links (see Fig. 1.3). The base station, or the gateway, is used for data processing, storage, and control of the sensor network. Sensor nodes are usually battery powered; hence the whole sensor network is limited by fundamental tradeoffs between sampling rates and battery lifetimes [20].

Wireless Sensor Node Wireless sensor nodes are the main building blocks of WSNs. Their purpose is to “sense, process, and report”. Requirements for sensor

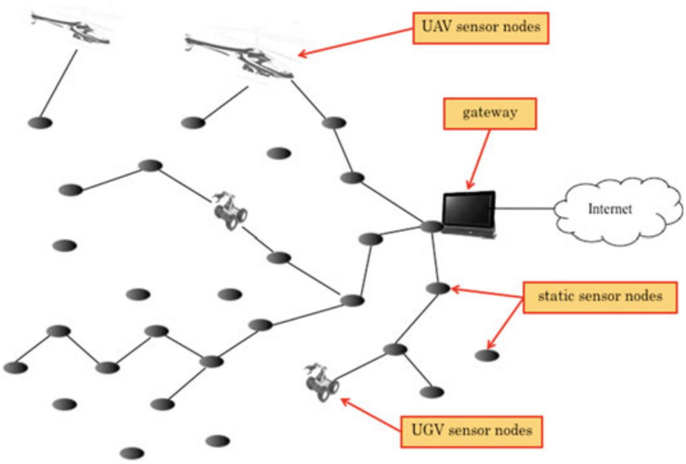

Fig. 1.3 Ad hoc wireless sensor network with static and mobile nodes placed on unmanned ground vehicles (UGVs) or unmanned aerial vehicles (UAVs)

nodes are to be small, energy efficient, and capable of in situ reprogramming. Examples include sensor nodes such as MICA motes from MEMSIC, Moteiv from Sentilla, EmbedSense from MicroStrain, Inc., and others. Figure 1.4 shows two typical sensor nodes.

Sensor nodes consist of a variety of sensors (sometimes built in on a separate module called sensor module), a microcontroller for on-board communication and signal processing, memory, radio transceiver with antenna for communication with neighboring nodes, power supply, and supporting circuitry and devices. Most of the sensor nodes run their own operating system developed for small form-factor, low-power embedded devices, such as TinyOS [5] or embedded Linux, that provides inter-processor communication with the radio and other components in the system, controls power consumption, controls attached sensor devices, and provides support for network messaging and other protocol functions.

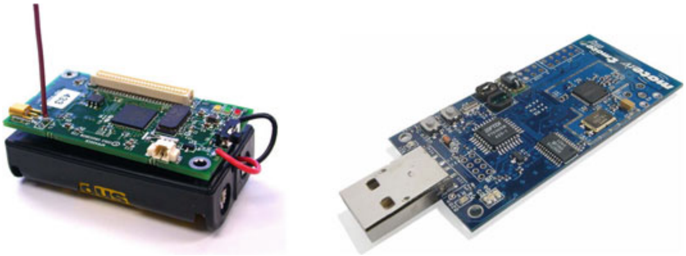

Fig. 1.4 Sensor node MICA2 (*left*, *source* MEMSIC) and Tmote Sky (*right*, *source* www.advanticsys.com)

Sensors measure a physical quantity of the external world and convert it into a readable signal. For example, a thermometer measures the temperature and converts it into expansion or contraction of a fluid. A thermocouple on the other hand converts the temperature into an electronic signal. For integration with other electronic components on a wireless sensor node, it is desired that sensors produce an electronic output. Common requirements for sensors to be integrated with a WSN system are to be small in size, low power, and low cost. Recent advancements in microelectromechanical systems (MEMS) technology allowed development of sensors with those low-power/cost/size requirements [27]. Such technology not only allows for small form-factor and ultra-low-power sensors devices, but opens research and development opportunities toward future on-chip integration of sensors, radio, memory, microcontroller, and other wireless sensor node components (see about Smart Dust technology [30]).

Often, sensors are grouped in a separate module, called a sensor board, that can be connected to the microprocessor and radio module. Such modular approach allows users to combine different sensors with the same WSN platform, thus minimizing the development time for new applications, for instance, Fig. 1.5 shows Louisiana Tech University sensor board connected to MEMSIC Technology's Mica2 radio module. The sensor module supports three chemical sensors that can detect three chemical agents simultaneously, namely CO, NO_2, and CH_4.

Gateway/Base Station The gateway or the base station for wireless communication provides sensor data collection into a database. The radio transceiver of the base station is communicating with the sensor nodes in the field. The base station is a stand-alone system with a chassis that is against an inhospitable environment. The gateway/base station provides *gateway* connection with other networks. If possible, base station is connected to the Internet, thus allowing some remote system monitoring and data acquisition. It can run database software applications for the management of sensing data. Base station sub-system can host any user interface application accessible through Internet or locally at the base station.

Wireless Sensor Network Protocols Wireless sensor network protocols are designed to accommodate specific features and properties of wireless sensor networks including their geographically distributed deployment, self-configuration,

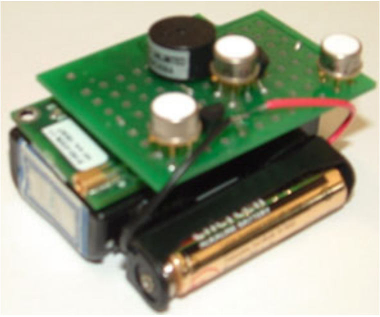

Fig. 1.5 Louisiana Tech Univ. wireless sensor node for chemical agent monitoring applications built on MEMSIC Mica2 platform

energy constraints usually limited by battery supply, wireless communication in often noisy environment, long lifetime requirements, and high fault tolerance. Most of the protocols are specific for or related to one of the features of sensor networks. An overview of wireless sensor networks protocols is provided in [23].

Medium Access Control (MAC) Initial MAC protocols such as Aloha [39] stem from computer network protocols. Such protocol for wireless sensor networks is given in [7]. The drawback of such protocols is that the on-board processor consumes power during idle periods. A suggested improvement is to avoid listening to the channel when it is idle. This could be implemented by transmitting signals having a preamble in front of sent packets. On waking up periodically to check the signal preamble, the receiver decides if it needs to be active or can continue to sleep.

Other examples of MAC protocols include Carrier Sense Multiple Access (CSMA), where a transmitter listens for a carrier signal before trying to send packets. In this scheme, the transmitter tries to detect or "sense" a carrier before attempting to transmit. If there is a carrier in a medium, the node wishing to transmit waits for the completion of the present transmission before initiating its own transmission. Sensor-MAC (S-MAC) [33, 34] is a protocol designed for wireless sensor networks that supports energy conservation of nodes and self-configuration, and its variations such as Timeout-MAC (T-MAC), DMAC, TRaffic-Adaptive Medium Access (TRAMA), and others [23]. In S-MAC protocol all nodes go to a sleep mode periodically. If a node wants to communicate with its neighbor, it must contend with other neighbors of the destination node for the communication medium. The transmitting node waits for the destination node to wake up, and sends Request to Send (RTS) packet. If the packet is received successfully, node wins the medium, and receives Clear to Send (CTS) packet. Each node maintains a sleep schedule for its neighbors through synchronization process, carried out by periodically sending a synchronization packet. The duty cycle of sleep schedule is fixed. Improvements of S-MAC such as Pattern-MAC [36] offer adaptable sleep–wake up schedule for sensor nodes.

Standard medium access control protocols include Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA) [24, 26]. In TDMA, radio transmits in specifically allocated time slots. Duty cycle of the radio is reduced, and energy efficiency improved, since sensor nodes do not need to listen during idle periods. Microcontroller and transceivers can be in the sleep mode. TDMA protocol has some disadvantages when applied to ad hoc sensor networks. When the number of nodes changes, it is difficult for TDMA protocol to dynamically specify new time slots for new nodes. To alleviate the problem, a modified TDMA protocol [28] uses super frames where a node schedules different time slots to communicate with neighboring nodes. The problem with this communication scheme is a low bandwidth where the node cannot reuse time slots allocated for communication with some other sensor node.

In terms of routing protocols, a shortest radio path algorithm was proposed in [32] where the metric used is the received signal strength. Each radio receiver has the coded information about the strength of the signal, enabling the receiver to find the closest sensor node in the field and communicate with it. The base station starts initialization process, where all sensor nodes identify themselves and thus identify distance between each other. This way all sensors can be located with respect to the base station.

1.3 WSN Applications

Convenience and cost savings of wireless communication, the small form factor of microprocessors, microcontrollers, memory, radio, and other electronic components, and variety of sensors developed recently as a result of advancement in MEMS and other sensor technologies, allowed for a broad adoption of WSNs in a range of applications in many different areas. Here, we list a few examples of deployed WSNs from different application domains.

Wireless Sensor Networks for Habitat Monitoring Deployed for habitat monitoring on Great Duck Island of the coast of Maine [20], this sensor network testbed was one of the first applications of WSNs used in real time in the wild. A team from Intel Corporation and University of California, Berkeley deployed 32 wireless sensor nodes on Duck Island where the system was used for seabird colonies monitoring. The advantage of this system is that it does not disrupt nature and species being monitored.

The system has a hierarchical structure and wireless sensor nodes are deployed in clusters or patches. Every cluster has a gateway, which transmits the data to one central location, the base station, located on the island. Sensor nodes communicate using multi-hop protocol where information hops from lower level leaves toward the gateway. The base station has Internet connection through satellite two-way communication link as well as database management for data processing and storage. The architecture of the system for habitat monitoring is shown in Fig. 1.6.

Mica sensor nodes were used as the sensor network platform. Nodes are equipped with 916 MHz radio, small form-factor Atmel ATmega103 [40]—an 8-bit microcontroller that runs at 4 MHz, has 128 Kbytes of flash memory, and built-in 10-bit analog-to-digital converters, two batteries and other supporting circuitry.

The system can operate at least 9 months from non-rechargeable batteries. Increased battery lifetime can be achieved using innovative methods for energy harvesting from the environment (see for instance [12, 14, 25]), by applying intelligent/adaptive control methods [29], and/or efficient coordination methods [4]. Sensor nodes can be reprogrammed in the field online, in situ. Sensor nodes are equipped with light, temperature, infrared, humidity, and barometric pressure sensors. Packaging that consists of acrylic enclosure has been developed specifically for this application. Proposed scheduled communication between sensor nodes are the following:

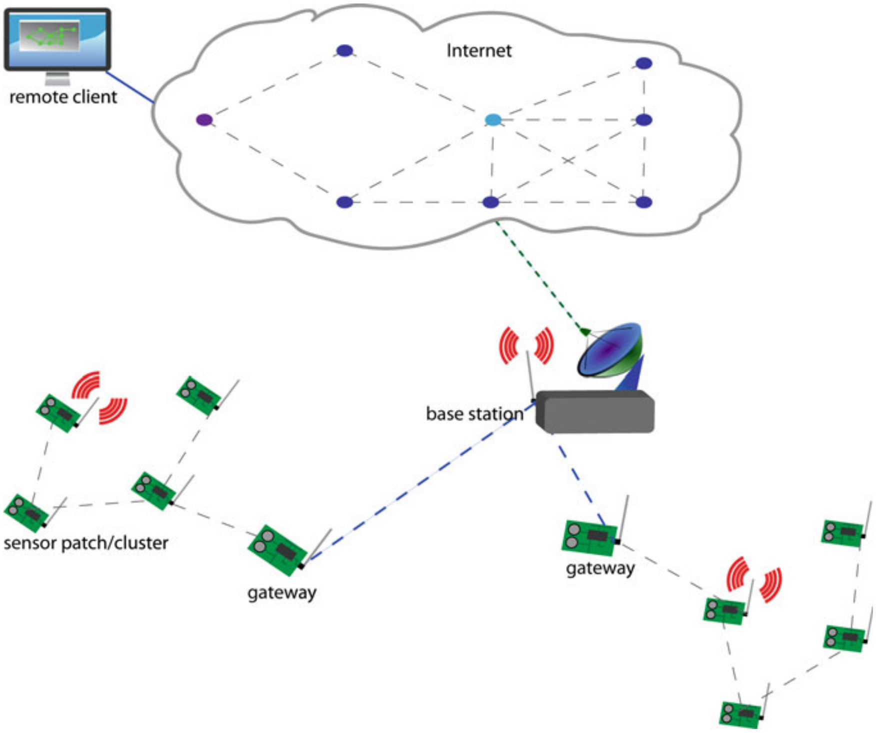

Fig. 1.6 Wireless sensor network monitoring system for habitat monitoring [20]

1. Nodes determine the number of hops (hop-level) from the gateway. Leaf nodes transmit first to the next level that has one less hop-level. After transmission is completed, sensor nodes go to a sleep mode where unused node components are shut down. The nodes are awaken again at a specific time instant, resembling to TDMA policy.
2. Nodes are awaken from the leaves toward the base station, independently of the nodes at the same hop-level. Data are passed from the leaves to the upper nodes in the network tree. The drawback is that the number of sub-trees and paths can be much larger than the number of hop-levels.
3. Low-power MAC protocols such as S-MAC [33, 34] and Aloha with preamble sampling [7] can also be used. They do not require communication scheduling but require additional energy and bandwidth for collision avoidance.

Industrial Control and Monitoring Compared with standard data networks where bandwidth, and therefore the data rate, is the most important network parameter, in industrial control and monitoring applications reliability and scalability are the most important performance measures. Monitoring and controlling temperature in an industrial boiler system does not require large data rate transfer; it necessitates reliable data transfer. Any significant loss or delay of data transfer can result in closed-loop system instability. Robust control and monitoring using WSN technology required development of new network protocols and device interfaces. Global markets, with many different device manufacturers, have required standardization in network protocol and device interfaces, resulting in the development of the ZigBee specification for IEEE 802.15.4 wireless sensor network protocol standard and the IEEE 1451 standard for smart sensors and actuators (transducers) including wireless interfaces [38].

Structural Health Monitoring Traditional methods for structural health monitoring consist of accelerometers, strain gages and other sensors connected to the data acquisition boards that are interfaced to a PC computer. Such systems are difficult and expensive to install, hard to maintain, and bulky to carry around. It is particularly expensive to achieve high spatial density with such conventional approach.

WSNs offer improved functionality, higher spatial density, and cheaper solutions than traditional wired systems. WSNs can cover large structures, and can be quickly and easily installed. The system does not need a complicated wiring, thus disruption due to the installation and maintenance of the WSN to the structure operation and usage is almost negligible.

An example of a structural health monitoring application is the WSN designed, implemented, deployed, and tested on the 4200 ft long main span and the south tower of the Golden Gate Bridge [15] (Fig. 1.7). Ambient structural vibrations are reliably measured at a low cost and without interfering with the operation of the bridge. Total of 64 nodes are distributed over the main span and the tower of the bridge. Sensor nodes measure vibrations with 1 kHz sampling rate, which was considered more than enough for civil structure monitoring applications. The accelerometer data are passed through low-pass anti-aliasing filter, fed into the analog-to-digital converter on the sensor node, and processed and transmitted wirelessly. The data are transmitted over a 56-hop network toward the base station. The system uses MicaZ sensor nodes with accelerometer sensor boards designed for this specific application that monitors acceleration in two directions. The nodes were packaged into plastic enclosing to protect it from gusty wind, fog, and rain, and installed on the bridge. Data sampling duty cycle is an order of magnitude

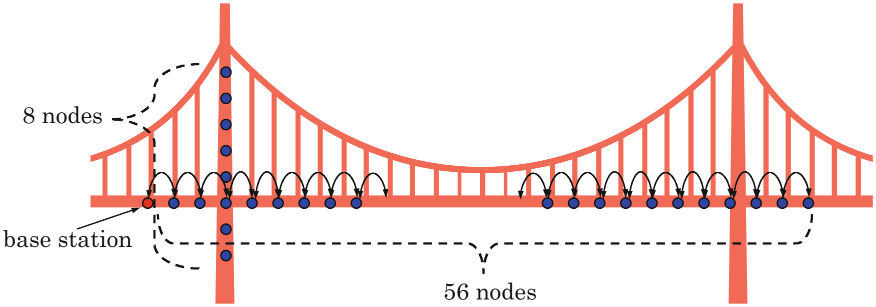

Fig. 1.7 Wireless sensor network used for structural monitoring at the Golden Gate Bridge [15]

higher than in environmental monitoring applications. Time synchronization across the network is required to correlate vibration measurements at different bridge locations. For larger network this can be challenging problem due to drift of clocks at each sensor node. The Flooding Time Synchronization Protocol [21] has been implemented to guarantee precise and coordinated measurements across the network. Embedded software is based on TinyOS operating system with newly developed software components.

Chemical Agents Monitoring Monitoring of chemical agents, their detection, and identification are of great importance for national security, homeland defense, consumer industry, and environmental protection. Being aware of potentially dangerous chemical agents in our surroundings can save our lives and provide crucial information for countermeasures. One of the challenges of emergency responses to weapons of mass destruction is to develop portable distributed sensor network capable of monitoring, detecting, and identifying different chemical agents at the same time. Important wireless sensor network requirements are multiple chemical agent detection and identification, distributed sensor network infrastructure, lightweight, and user-friendly.

The chemical agent monitoring applications are closely related to microelectromechanical systems (MEMS) technology that allows for small-form factor sensor arrays that can be easily integrated into low-power wireless sensor nodes, [11]. An example of MEMS chemical sensor that is suitable for WSN application is a microcantilever sensor using adsorption-induced surface tension that can be used to detect part-per-trillion (ppt) level of species both in air and solution. An electron micrograph of a cantilever and its structure are shown in Fig. 1.8 [11, 37].

The technology is based upon changes in the deflection and resonance properties induced by environmental factors in the medium in which a microcantilever is immersed. By monitoring changes in the bending and resonance response of the cantilever, mass and stress changes induced by chemicals can be precisely and accurately recorded. Usually MEMS sensors provide low-voltage signals, and interface electronics between chemical sensors and wireless sensor node is needed that includes signal conditioner (amplifier and filter) and signal multiplexer, Fig. 1.9.

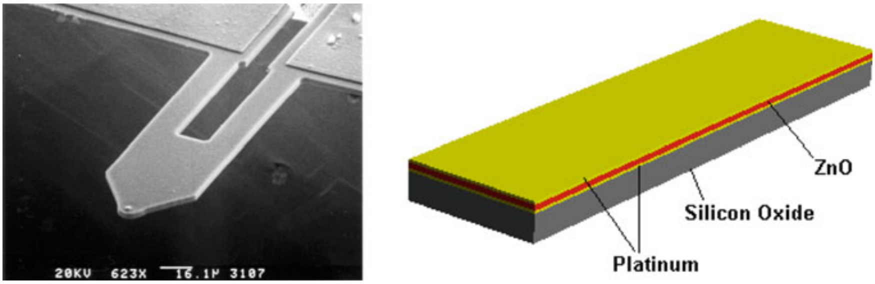

Fig. 1.8 Electron micrograph of microcantilever with a length of 200 μm (*left*) and structure of the microcantilever sensor (*right*)

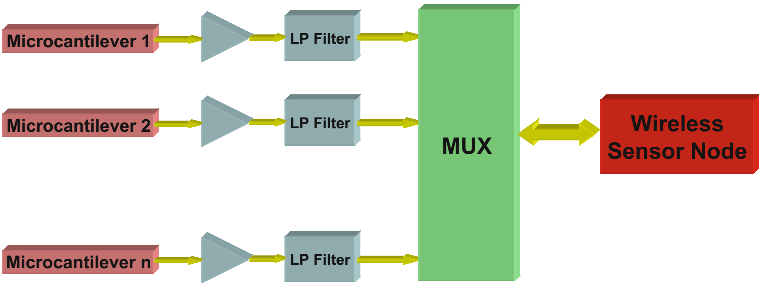

Fig. 1.9 Interface electronics for chemical sensor array on wireless sensor node

Military Applications Due to its small form-factor, possibility of ad hoc deployment, and no strict requirement for other power or communication infrastructure, WSNs find numerous use in military applications. For instance, shooter localization in urban environment cannot be accurately estimated with standard, centralized-based approach due to large multipath effects and limited coverage area. WSNs provide technology platform for a distributed solution where acoustic sensor data are cooperatively processed to estimate the shooter localization in an urban environment [16, 17].

The system [17] consists of a WSN with acoustic sensors, implemented as a custom-based sensor boards with DSP or FPGA devices, measures shockwaves and their time of arrivals. The measured data are sent to the base station for data fusion and shot trajectory estimation based on collected information from distributed sensor network. Time synchronization among sensor nodes and their known deployment location allows for accurate fusion of acoustic measurements and localization of the shooter or multiple shooters. The system can easily be extended into self-localizing sensor network where sensor nodes will localize themselves in real time using GPS or other localization techniques and then use sensor data to estimate the shooter location.

Surveillance Applications Such applications leverage recent technology advancements in WSNs to effectively and safely study volcanic activities [31]. An example of such a system is deployed to monitor Tungurahua volcano in central Ecuador. Scientists collect seismic data to monitor and study volcanic activity. To distinguish the volcano eruption with earthquakes or mining explosions, a correlation of infrasonic and seismic events is needed. Wireless sensor nodes can be placed close to the volcano crater and transmit the data to the base station on a safe distance for future processing.

The WSN consists of sensor nodes equipped with a specially constructed microphone to monitor infrasonic (low-frequency acoustic) signals from the volcanic vent during eruptions. Data are transferred to a gateway that forwards data wirelessly using long-range radio link to the base station at the volcano observatory. Time synchronization is achieved using a GPS node that supplies other nodes and the gateway with the timestamp data, Fig. 1.10.

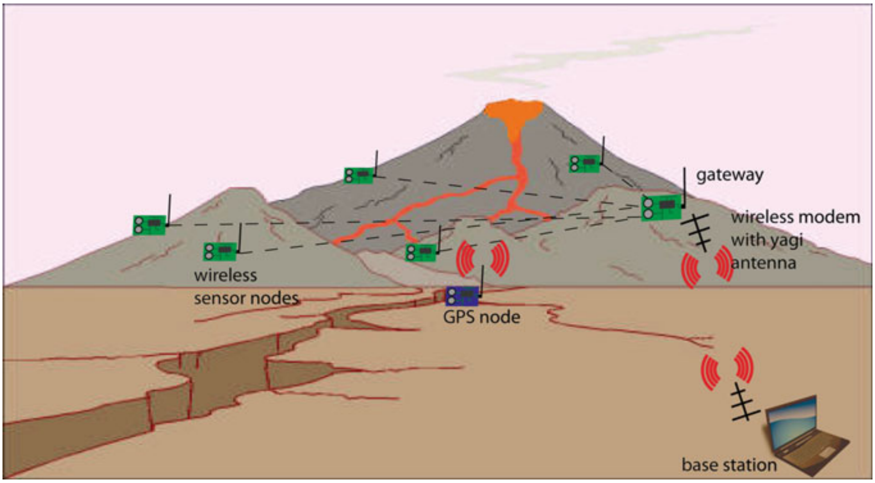

Fig. 1.10 WSN used for monitoring volcano activities [31]

Since volcano data are sampled at a higher rate than environmental sensor network applications (100 Hz), in-network data aggregation and distributed event detection is required. Such constraints require precise time synchronization, either using extra GPS equipped node or time-synchronizing protocols, and correlation of data among spatially close sensor nodes. Sensor nodes communicate with their neighbors to determine if an event of interest has occurred, [31] based on a decentralized voting scheme. Nodes keep track of window of data and also run event detection algorithm. In case a local event occurs, the node broadcasts a vote. If a node receives sufficient number of votes, a global data collection starts. This distributed event detection reduces the bandwidth usage and allows larger spatial resolution and larger sensing coverage areas. Sensor nodes are enclosed in waterproof packaging with antennas sealed with silicone.

1.4 WSN Common Communication Standards

ZigBee is a standard developed for low-power WSN monitoring and control applications which require reliable and secure wireless data transfers. It uses the existing IEEE 802.15.4 Physical layer and Medium Access Control sub-layer while adding networking, routing, and security of data transfers. It supports multi-hop routing protocols that can extend the network coverage. The physical layer operates at 868 MHz, 20 Kbps (Europe), or 915 MHz 40 Kbps (USA), and 2.4 GHz, 250 Kbps. Direct sequence spread spectrum is used with offset-quadrature phase shift keying modulation at 2.4 GHz band or with binary-phase-shift keying modulation at 868 and 915 MHz bands. Figure 1.11 shows ZigBee layered stack

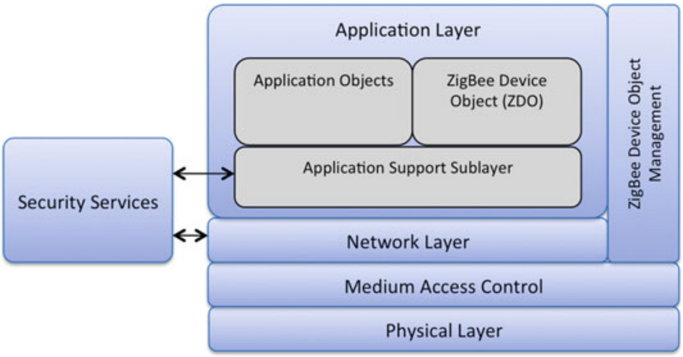

Fig. 1.11 ZigBee stack architecture [39]

architecture. The Application Layer has Application Support Sub-layer (provides an interface between the network layer and the application layer), Application objects (defined by manufacturers), and ZigBee Device Object (an interface between the application objects, the device profile, and the application support sub-layer, responsible for initialization of application support sub-layer, the network layer, and security services as well as processing configuration information from applications).

ZigBee's network layer allows for mesh, star, and tree topologies. The mesh topology supports peer-to-peer communication. In a star topology, there is a network Coordinator node that initiates and maintains devices on the network and can connect to other networks, [39]. In tree topology, Router Devices are responsible for moving data and control messages. ZigBee End Device communicates with the coordinator or router and cannot be used for hopping data from other devices.

ZigBee offers improved security features over IEEE 802.15.4 protocol—it uses a 128-bit Advanced Encryption Standard-based algorithm. It provides mechanisms for moving security keys around the network, key establishment, key transport, frame protection, and device management. These services form the building blocks for implementing security policies within a ZigBee device.

The IEEE 1451 standard for smart sensors and actuators was developed under leadership from the National Institute of Standards and Testing (NIST). A detailed description of the standards is given in [13, 18]. This standard is also used in integrated system health management [9] and in smart actuator control with transducer health monitoring capabilities [10]. The standard has been divided into six subgroups. IEEE 1451.0 defines a set of commands, operations, and transducers electronic data sheets for the overall standard. The access to the devices is specified and it is independent of the physical layer. IEEE 1451.1 defines communication with the Network Capable Application Processor (NCAP). This part of the standard specifies client–server or client–client type of communication between NCAP and other network devices, or between several NCAPs as is often case in a complex system with many smart sensors and actuators. IEEE 1451.2 includes the definition of Transducer Electronic Data Sheets (TEDS) and an interface between transducer

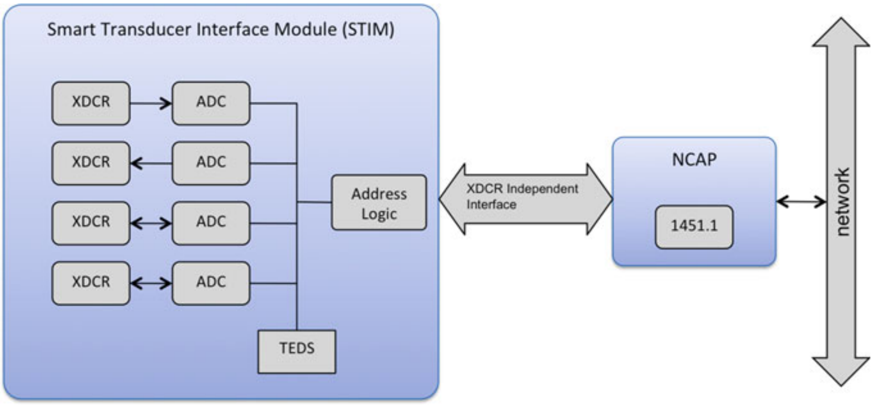
Smart Transducer Interface Module (STIM)
XDCR
ADC
XDCR
ADC
XDCR
ADC
XDCR
ADC
Address Logic
TEDS
XDCR Independent Interface
NCAP
1451.1
network

Fig. 1.12 IEEE 1451 Smart transducer block diagram that includes Smart Transducer Interface Module (STIM) with Transmission Electronic Data Sheet (TEDS) and Network Capable Application Processor (NCAP)

and the NCAP. It allows a variety of devices to have same hardware interface to the microprocessor. Figure 1.12 shows a system block diagram with the IEEE 1451.1 and 1451.2 interfaces.

The IEEE 1451.3 specifies the interface between the NCAP and smart transducers and TEDS for multi-transducers structure connected to the bus. The standard allows variety of sensors and actuators to be connected to the same NCAP through the bus structure, including both low and fast sampling rate sensors and actuators. IEEE 1451.4 deals with analog transducers and how they can be interfaced with microprocessors. The standard specifies TEDS connection for analog devices. The network can access TEDS data through digital communication first, and then send analog data to the analog actuator, for example. IEEE 1451.5 specifies a transducer to NCAP interface and TEDS for wireless communication scenarios. Common wireless communication protocols are included as transducer interfaces. The NCAP can then be implemented on some of the wireless devices and not physically attached to the sensor or actuator. IEEE 1451.7 defines interfaces for transducer-to-RFID (Radio Frequency Identification) systems.

Questions and Exercises

1. Describe Aloha protocol. What is the difference between Pure Aloha and Slotted Aloha protocols?
2. What are important design factors when wireless sensor networks are considered?
3. Describe one military application that uses wireless sensor networks. Can you think of a novel military application that uses the power of distributed sensing?

4. Research and articulate your own idea about a novel WSN application. Ask yourself who would buy such product/application and why? Research if there exist already a similar application using WSNs.
5. What are Medium Access Control (MAC), TDMA, FDMA?
6. What are specifics of an S-MAC protocol?
7. Describe basics of ZibBee protocol. What is the difference between ZigBee and IEEE 802.15.4 protocol?
8. What is the IEEE 1451 standard used for and why it is developed originally?
9. Describe chemical agents monitoring application and how cantilever-based sensors can be interfaced with wireless sensor networks?
10. What is a difference between wireless sensor node and the base station?

References

1. N. Abramson, "The Aloha System – Another alternative for computer communications," *Proc. AFIPS Joint Computer Conferences*, 1970.
2. F. Bennett, D. Clarke, J.B. Evans, A. Hopper, A. Jones, and D. Leask, "Piconet: embedded mobile networking," *IEEE Personal Communications Magazine*, vol. 4, no. 5, pp. 8–15, Oct. 1997.
3. E.H. Callaway, *Wireless Sensor Networks: Architectures and Protocols*, CRC Press LLC, Boca Raton, FL, 2004.
4. B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: an energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks," *Proc. 7th ACM International Conference on Mobile Computing and Networking*, Rome, Italy, July 2001.
5. TinyOS Community Forum at http://www.tinyos.net/.
6. L. Doherty and K.S.J. Pister, "Scattered data selection for dense sensor networks," *Proc. the Third International Symposium on Information Processing in Sensor Networks*, April 26–27, 2004, Berkeley, California, USA.
7. A. El-Hoiydi, "Aloha with preamble sampling for sporadic traffic in ad hoc wireless sensor networks," *Proc. IEEE International Conference on Communications (ICC 2002)*, New York, USA, pp. 3418–3423, April 2002.
8. D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," *Proc. ACM/IEEE International Conference on Mobile Computing and Networking*, pp. 263–270 Seattle, Washington, August, 1999.
9. F. Figueroa and J. Schmalzel, "Rocket Testing and Integrated System Health Management", in *Condition Monitoring and Control for Intelligent Manufacturing* (Eds. L. Wang and R. Gao), pp. 373–392, Springer Series in Advanced Manufacturing, Springer Verlag, UK, 2006.
10. D. Jethwa, R.R. Selmic and F. Figueroa, "Real-time implementation of intelligent actuator control with a transducer health monitoring capability," *Proc. 16th Mediterranean Conference on Control and Automation*, Corsica, France, June 25–27, 2008.
11. H.-F. Ji, K.M. Hansen, Z. Hu, T. Thundat, "An Approach for Detection pH using various microcantilevers," *Sensor and Actuators*, 2001, 3641, 1–6.
12. X. Jiang, J. Polastre, and D. Culler, "Perpetual environmentally powered sensor networks," *IEEE Information Processing in Sensor Networks*, 2005, pp. 463–468.
13. R.N. Johnson, "Building plug-and-play networked smart transducers," *National Institute of Standards and Technology IEEE 1451 Website*.

14. A. Kansal, J. Hsu, S. Zahedi, and M.B. Srivastava, “Power management in energy harvesting sensor networks,” *ACM Transactions on Embedded Computing Systems*, 2006.
15. S. Kim, S. Pakzad, D. Culler, J. Demmel, G. Fenves, S. Glaser, and M. Turon, “Health Monitoring of Civil Infrastructures Using Wireless Sensor Networks,” *Proc. the 6th International Conference on Information Processing in Sensor Networks (IPSN ‘07)*, Cambridge, MA, April 2007, ACM Press, pp. 254–263.
16. P. Kuckertz, J. Ansari, J. Riihijarvi, P. Mahonen, “Sniper fire localization using wireless sensor networks and genetic algorithm based data fusion,” *IEEE Military Communications Conference*, Oct. 2007.
17. A. Ledeczi, A. Nadas, P. Volgyesi, G. Balogh, B. Kusy, J. Sallai, G. Pap, S. Dora, K. Molnar, M. Maroti, and G. Simon, “Countersniper system for urban warfare,” *ACM Transactions on Sensor Networks*, vol. 1, no. 2, Nov. 2005, pp. 153–177.
18. K. Lee, “Brief description of the family of IEEE 1451 standards,” *National Institute of Standards and Technology*, IEEE 1451 Website (cited July 2010): http://ieee1451.nist.gov/1451Family.htm.
19. F.L. Lewis, “Wireless Sensor Networks,” book chapter in *Smart Environments: Technologies, Protocols, and Applications*, ed. D.J. Cook and S.K. Das, John Wiley, New York, 2004.
20. A. Mainwaring, J. Polastre, R. Szewczyk, and D. Culler, “Wireless sensor networks for habitat monitoring,” *Intel Research*, June 2002.
21. M. Maroti, B. Kusy, G. Simon, and A. Ledeczi, “The flooding time synchronization protocol,” *Proc. ACM Second International Conference on Embedded Networked Sensor Systems*, pp. 39–49, Baltimore, MD, November 3, 2004.
22. C.S.R. Murthy and B.S. Manoj, *Ad Hoc Wireless Networks: Architectures and Protocols*, Prentice Hall, Upper Saddle River, NJ, 2004.
23. M.A. Perillo and W.B. Heinzelman, “Wireless sensor network protocols,” in *Algorithms and Protocols for Wireless and Mobile Networks*, Eds. A. Boukerche et al., CRC Hall Publishers, 2004.
24. J.G. Proakis, *Digital Communication*, McGraw-Hill, New York, NY, 2001.
25. M. Rahimi, H. Shah, G.S. Sukhatme, J. Heidemann, and D. Estrin, “Studying the feasibility of energy harvesting in a mobile sensor network,” *Proc. IEEE International Conference on Robotics and Automation (ICRA)*, 2003.
26. T.S. Rappaport, *Wireless Communications*, Principles and Practice, Prentice Hall, Upper Saddle River, NJ, 2nd edition, 2002.
27. S. Senturia, *Microsystems Design*, Kluwer Academic Publishers, Norwell, MA, 2001.
28. K. Sohrabi and G.J. Pottie, “Performance of a novel self-organization protocol for wireless ad hoc sensor networks,” *Proc. IEEE 50th Vehicular Technology Conference*, 1999.
29. C.M. Vigorito, D. Ganesan, A.G. Barto, “Adaptive control of duty cycling in energy-harvesting wireless sensor networks,” *4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, SECON ‘07, pp. 21–30, June 2007.
30. B. Warneke, M. Last, B. Liebowitz, K.S.J. Pister, “Smart Dust: Communicating with a Cubic-Millimeter Computer,” *IEEE Computer*, January 2001.
31. G. Werner-Allen, J. Johnson, M. Ruiz, J. Lees, M. Welsh, “Monitoring volcanic eruptions with a wireless sensor network,” *Proc. the Second European Workshop on Wireless Sensor Networks* (EWSN’05), 2005.
32. B. West, P. Flikkema, T. Sisk, and G. Koch, “Wireless sensor networks for dense spatio-temporal monitoring of the environment: a case for integrated circuit, system, and network design,” *2001 IEEE CAS Workshop on Wireless Communications and Networking*, Notre Dame, Indiana, August 2001.
33. W. Ye, J. Heidemann, and D. Estrin, “An energy-efficient MAC protocol for wireless sensor networks,” *Proc. IEEE INFOCOM*, New York, June 2002.
34. W. Ye, J. Heidemann, and D. Estrin, “Medium access control with coordinated adaptive sleeping for wireless sensor networks,” *IEEE/ACM Transactions on Networking*, vol. 12, no. 3, June 2004.

35. F. Zhao and L. Guibas, *Wireless Sensor Networks*, Elsevier, 2004.
36. T. Zheng, S. Radhakrishnan, and V. Sarangan, PMAC: An adaptive energy-efficient MAC protocol for Wireless Sensor Networks," *Proc. IEEE International Parallel and Distributed Processing Symposium*, 2005.
37. W. Zhou, A. Khaliq, Y. Tang, H.-F. Ji, and R.R. Selmic, "Simulation and design of piezoelectric microcantilever chemical sensors," *Sensors and Actuators A*, vol. 125, no. 1, pp. 69–75, October 2005.
38. L.Q. Zhuang, K.M. Goh and J.B. Zhang, "The Wireless Sensor Networks for Factory Automation: Issues and Challenges," *Proc. IEEE Conference on Emerging Technologies and Factory Automation*, September 2007.
39. ZigBee Specification, publication by ZigBee Alliance, http://www.zigbee.org.
40. www.atmel.com.