1 Introduction to wireless sensor networks

Wireless sensor networks (WSNs) are a new class of wireless networks that are becoming very popular with a huge number of civilian and military applications. A wireless sensor network (WSN) is a wireless network that contains distributed independent sensor devices that are meant to monitor physical or environmental conditions. A WSN consists of a set of connected tiny sensor nodes, which communicate with each other and exchange information and data. These nodes obtain information on the environment such as temperature, pressure, humidity or pollutant, and send this information to a base station. The latter sends the info to a wired network or activates an alarm or an action, depending on the type and magnitude of data monitored [1–24].

Typical applications include weather and forest monitoring, battlefield surveillance, physical monitoring of environmental conditions such as pressure, temperature, vibration, pollutants, or tracing human and animal movement in forests and borders [1–23]. They use the same transmission medium (which is air) for wireless transmission as wireless local area networks (WLANs). For nodes in a local area network to communicate properly, standard access protocols like IEEE 802.11 are available. However, this and the other protocols cannot be directly applied to WSNs. The major difference is that, unlike devices participating in local area networks, sensors are equipped with a very small source of energy (usually a battery), which drains out very fast. Hence the need arises to design new protocols for MAC that are energy aware. Clearly there is some difference between a traditional WLAN and a WSN, as the latter has limited resources.

The objective of this chapter is to provide an up-to-date treatment of the fundamental techniques, applications, taxonomy, and challenges of wireless sensor networks.

1.1 Background

A wireless sensor network consists of hundreds, if not thousands, of small and inexpensive nodes, which could have a static location or be dynamically deployed to monitor the intended environment. Owing to their miniature size, they have a number of constraints. The function of a WSN is basically monitoring. There are three classes of monitoring that a WSN can observe: (a) entity monitoring, which means monitoring something such as civil structures like bridges, tunnels, highways, and buildings, or the human body, such as monitoring the organs of the body; (b) area monitoring, which includes monitoring the environmental area alarms; and (c) area-entity monitoring, which includes monitoring vehicles on the highway, and monitoring movement of an object [1–15, 23, 24].

The key positive feature of WSNs does not come from the strength of the individual sensor nodes; it comes from the entire array of interconnected sensor nodes. Hence, WSNs are expected to be large in scale from the point of view that they have a lot of nodes and they are apt to be self-configuring, in order to achieve reliability. Since a wireless sensor node is usually inexpensive, we would expect to have a huge number of nodes in a WSN.

Typically, sensor nodes communicate with each other by means of a multi-hop scheme. The flow of information and data stops at particular nodes called base stations or sinks. A sink or base station usually connects the sensor network to a fixed network to distribute the data sensed for further processing. In general, base stations have enhanced capabilities over regular nodes as they should carry out compound processing. This substantiates the actuality that sinks have more advanced processors such as PCs/laptops with more RAM memory, secondary storage, battery and computational power as they are expected to perform more tasks than regular sensor nodes. It is worth noting here that one of the biggest drawbacks of sensor networks is power use, which is really influenced by the interaction between nodes. In order to work out this problem, aggregation points are set up to the network, which reduce the overall communication traffic between nodes and save energy. Typically, collection points are ordinary nodes that get data from nearby nodes, carry out some sort of processing, and then advance the filtered data to the subsequent hop. Sensor nodes are arranged into groups, each group having a "group/cluster head" as the leader. Communication within a group should travel all the way through the cluster head. Then it is advanced to an adjacent group head until it arrives at its destination, which is the sink or base station. A different scheme for saving energy is to let the nodes go into sleep mode, if they are not needed, and to wake them up when they are needed.

The progress of wireless sensor networks was initially provoked by military applications; however, wireless sensor networks are now employed in many civilian applications such as environment monitoring, industrial process monitoring, health care applications, road and highway traffic control, smart homes and cities, and office automation. In health care applications, wireless devices make patient monitoring less invasive, thus improving health care. For utilities applications, wireless sensors provide an inexpensive scheme for collecting system health data to minimize energy usage and enhance management of resources. As for remote monitoring, a wide range of applications are covered where wireless networks can go together with fixed networks and systems by minimizing wiring costs and permitting new sorts of testing and measurement applications. The main applications of remote monitoring are: (a) environmental monitoring of air, soil, and water, (b) building and structural monitoring of bridges, subways, and buildings, (c) process monitoring, (d) machine monitoring, (e) habitat monitoring, (f) intelligent transportation systems, (g) air traffic control, (h) traffic surveillance, (i) video surveillance, and (j) monitoring carbon transfer in rain forests, among others [1–24]. Each node in a wireless sensor network is usually equipped with a radio transceiver, a tiny microcontroller, and a power source (typically a battery). The cost of a sensor node ranges from hundreds of dollars to a quarter of a dollar, depending on the size of the network and the functionality and sophistication required of each node. The size and price restrictions on sensor nodes produce constraints on resources such as energy, memory, computational power, and throughput. In general, a sensor network forms a wireless ad-hoc computer network, which means that each sensor supports a multi-hop routing scheme.

The major components of a wireless sensor network, which include sensors, signal convertors such as analog-to-digital (A/D) and digital-to-analog (D/A) convertors, processors, communication devices, and a power supply, are all becoming more and more inexpensive and smaller. Stringent power expenditure requirements are necessary because the sensor node needs to be reliable and able to run unattended for a long time, which can be years. Among the factors that should be considered in the design of power sources of a WSN are: (a) choice of power harvesting scheme or battery type, and (b) choice of small power electronic design schemes. Companies that produce these devices are now developing small sensor nodes and networks. Moreover, commercial off-the-shelf personal digital assistants (PDAs) or pocket computers contain impressive computing power in a small package. Such devices can easily be used as powerful sensor nodes. Wireless LANs like the popular IEEE 802.11 standards can now offer performance very close to those of wired networks. Moreover, we have now IEEE 802.15 standard that gives specifications for personal area networks (PANs), which can be employed for WSNs as well.

Furthermore, advances in semiconductor technology allow us to have more chip capacity and more processor capabilities. This progress allows a reduction in the energy/bit requirements for both the computing and communication systems. It is expected that advances in micro-electro-mechanical-systems (MEMS) technology will produce more powerful and versatile sensors. MEMO technology integrates mechanical elements, sensors, actuators, and electronics on a common silicon substrate through microfabrication technology, whereas the electronics are fabricated by using integrated circuit (IC) process sequences such as bipolar, CMOS transistors. The micromechanical elements are made up using well-suited micromachining techniques that purposely add new structural layers to create the mechanical and electromechanical devices [1–14].

1.2 Components of a wireless sensor node

The central component of a wireless sensor network is the sensor node. It is a very tiny device that has the ability to sense its immediate environment and map or store the information. Owing to the progress in semiconductor technology, the cost of these devices is decreasing all the time. These tiny devices consist of the following main components [8, 9].

- Microcontroller. This is a computer-on-a-chip which is very tiny in size although capable of doing powerful tasks including controlling the functions of other devices connected to it. In general, a microcontroller consists of a microprocessor,

Table 1.1 The industrial, scientific and medical (ISM) bands

Band	Frequency range
UHF ISM band	902 to 928 MHz
S-band ISM	2.4 to 2.5 GHz
C-band ISM	5.725 to 5.875 GHz

a RAM memory, and associated peripherals. These days, there are other devices available on the market that can be used in place of microprocessors for performing the same actions. Examples include: field programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs), and digital signal processors (DSPs). Each of these devices has its advantages and disadvantages, but microprocessors are the best choice for small scale to very small scale embedded systems owing to their low power consumption and moderate to good computing capabilities.

- Transceiver. This is a transmitter–receiver that is used for communication purposes to send and receive data, and commands. The choice of communication means of WSNs is the radio-frequency. These sensor nodes usually use the industrial, scientific and medical (ISM) frequency bands. The ISM bands are shown in the Table 1.1 [15].
- External memory. Wireless sensor nodes usually use flash [8–14] memories owing to their small size and reasonable storage capacity, which is always increasing. Based on the requirement of the nodes, we can have a user and a program memory. The size of the external memory depends on the application.
- Power source. The sources of power consumption in the nodes are the node programming, sensing and data collecting, data processing, and data communication. Usually, most of the power is needed for transmitting data. Power is stored in the sensor nodes in the form of batteries. The cost of batteries has recently decreased drastically [7–9]. Typically these batteries are for one-time use.

In general, power sources are typically divided into primary and secondary sources. The primary sources cannot be recharged, where secondary sources have to be charged on a regular basis. The major factors of primary and secondary sources are: range, capacity, temperature, current depletion level, and self-discharge characteristics. Fuel cells are expected to come into use as power sources for the sensors of the WSNs [9–14]. Where secondary cells are employed, the charging source may be harvested from the cell's operational environment. The famous example of this is the harvesting of solar energy in order to charge a battery. However, there are other harvesting energy methods that can be used such as wind power, thermal energy, and vibration. In mechanical driven settings, harvesting a battery may not be needed as the harvested movement is constant, for instance in a pipeline. One popular method is solar systems, which necessitate some degree of installation to guarantee the best direction, especially at soaring elevations. We can obtain only about 25% efficiency from the best available silicon solar cell systems.

Some reported accomplishments were found with vibration harvesting used in industrial applications as well as from oil pipelines [12–14].

- Sensors. In general, sensors may be categorized into classes based on their operating principles: (a) physical sensors, (b) thermal sensors, (c) chemical sensors, (d) biological sensors, and (e) electromagnetic, optical, and acoustic sensors.

  Sensors are typically hardware devices that sense the data from the monitored environments and produce some response that is measurable in nature. An analog-to-digital (A/D) convertor is used for converting the analog collected data to the digital form to be processed further by the microcontroller. The sensors in wireless sensor nodes are typically very small sized micro-electronic sensing devices which are equipped with a very limited supply of battery power. Examples of some commercial sensors include: BTnode, BEAN, COTS and DOT, MICA and KMote. Sensors can be placed in any kind of environment for days without any attention. The major challenge for a sensor is the life of the battery, which is limited. The battery has usually short life. Thus, schemes are needed to conserve as much energy as possible. If we envisage that such devices are deployed in the battle ground in enemy areas, we can clearly see that it is not possible to recharge or change the battery of these devices. It is true that we may be able to deploy these sensors in enemy territory by the use of aircraft/helicopter, but it may not be possible to invade the enemy territory just to replace the battery. The major source of energy consumption is the communication between the nodes. Moreover, nodes tend to coordinate with each other for some particular tasks [1–24].

1.3 Classification of sensor networks

Owing to the rapid progress in wireless sensor networks, a variety of applications with different needs have emerged. In order to deal with these changing requirements, there are many distinct network designs, in which protocols for distinct layers of the network have been implemented. Although there are many different ways to categorize the sensor network designs, here we show some of the essential differences in sensor networks.

- Data sink(s). One of the most crucial features of sensor networks is the characteristic of data sink(s). In some circumstances, the end user(s) may be entrenched inside the sensor network or may be mobile access points that gather data once in a while. This difference may be crucial, as efficient dispersed data storage methods may be effective in the latter case.
- Sensor mobility. Another classification of sensor networks may be based on the nature of the sensor being organized. Normally, sensors can be interpreted as being stationary; however, some recent sensor networks projects like ZebraNet use mobile sensor nodes. Moreover, in military applications, sensors may be placed on soldiers' bodies or clothes, or on unmanned aerial vehicles (UAVs) to communicate with an

organized sensor network. These sensors can manipulate protocols at the networking layer as well as for the services of localization with the feature of mobility.

- Sensor resources. Sensor nodes may differ with the availability of computer resources. It is apparent that memory and the conditions of processing should affect the implementation of protocols.
- Traffic patterns. Another important feature to be considered is the traffic that is generated in the network. In most of the event-driven applications, sensors may function for the bulk of the time, producing data traffic only when an event of significance is found, whereas in other applications such as environmental monitoring the data have to be produced constantly.

Wireless sensor network taxonomy can be based on the following dimensions [3, 8–13].

(1) Spatial resolution. This is measured in metric units such as centimeters, meters, or millimeters.
(2) Latency. Here, we can classify the network into categories such as negligible, moderate, or high.
(3) Coverage. In this regard we can have the following classes: partial, full, or redundant.
(4) Control. Classes here can be external, central, or distributed.
(5) Temporal resolution. This is usually measured in seconds.
(6) User types. In this case, we can have single, competitive, cooperative, and collaborative classes.
(7) Lifetime. Here, we can have simple with fixed duration, or complex with multiple phase-specific fixed durations.
(8) Bandwidth. This is an important criterion and characteristic. We can have episodic-small, episodic-large, continuous-small, and continuous-large categories. Units of bandwidth can be bytes/episode or byte/second.
(9) Sense of occurrence. We can identify: single discrete-target, multiple discrete-targets, and single distributed phenomena, and multiple distributed phenomena [1–24].

Others classify WSNs based on the following two concepts: (a) network organization or structure, and (b) node fairness and capabilities [13].

The authors in [12] devised a WSN application requirement taxonomy based on two application classes: precision agriculture, and wildfire management. For each dimension, they listed the class for each application. For instance, control is central for precision agriculture while it is distributed for wildfire management; or users can be single for precision agriculture or cooperative for wildfire management and so on.

1.4 Characteristics of wireless sensor networks

Wireless sensor networks have been recognized as one of the most vital technologies of this century. Inexpensive, smart devices with many on-board sensors networked through wireless links and the Internet and deployed in huge numbers present unique prospects for instrumenting and controlling homes, cities, factories, and the environment.

Moreover, networked sensors offer a new means for surveillance and other tactical applications. While sensor networks for various applications may be quite different, they share common characteristics.

Primarily, sensors are electrical, electronic, or electromechanical devices, even though other kinds of sensors exist. In general, a sensor is a type of transducer that converts an input to another, usually electrical, form. Sensors can be direct or paired. An example of a direct sensor is a thermometer or an electrical meter which indicates directly. A paired sensor uses an analog-to-digital (A/D) converter in order to convert an analog signal to a digital signal. Sensors are often used in applications such as medicine, industry, environment, robotics, and military. With the advances in material technology, more and more sensors are being built with Micro-Electro-Mechanic-Systems (MEMS) technology.

A good sensor/transducer should have the following main characteristics [16–24].

(1) It should be responsive to the considered property.
(2) It should be insensible to any other property.
(3) It is desirable that the output signal of the sensor is exactly proportional to the value of the measured characteristic.
(4) It should have a reasonable lifetime.
(5) It should not consume much power.

A WSN is made up of hundreds or even thousands of nodes that use sensing devices (sensors) to observe different conditions and environments, such as motion, pressure, temperature, sound, vibration, pollution, levels of oxygen or carbon dioxide, traffic intensity and patterns, among many others, at different sites. In general, these devices are tiny and low-cost so they can be manufactured and deployed in large quantities. One major difference between traditional MANETs (Mobile Ad hoc NETworks) and WSNs is that WSNs often have strictly limited resources in terms of power, memory, computational power, and bandwidth. The sensor node is a self-contained unit equipped with a radio transceiver, a tiny microcontroller, and a power source that is usually a battery. The nodes dynamically self-organize their configuration based on different network circumstances. Owing to the limited life of batteries, nodes are built with power saving in mind and generally spend large amounts of time in the “sleep” mode or in handing out the sensor data. Hence, each sensor is equipped with wireless communication capability, and signal processing and networking abilities. The main functions of any WSN are sensing, communication, and computing [1–15]. One scheme to categorize wireless sensor networks is based on whether the nodes are separately addressable, and another is based on whether the data in the network are aggregated. For instance, the sensor node in a parking-lot network should be individually addressable, so that one can find out the spots of all free spaces. However, if a person wants to find out the temperature or pressure in a specific corner area of a room, then addressability may not be so important. The capability of the WSN to combine the gathered data can significantly decrease the number of messages needed to be sent through the network. In some situations, it is vital to send the signal by the sensor in a timely manner such as when it is needed to send a data alert signal to the police indicating that an intruder is trying to enter someone’s house or office.

1.5 Challenges of wireless sensor networks

There are several challenges that face the progress of WSNs. Among these are [1–15] the following.

(1) Scalability. Most nodes in intelligent sensor networks are stationary. Networks of huge numbers of nodes on the order of 10 000 or more are expected. This means that scalability is a crucial issue in designing or launching any new WSN because we like to see proportional improvement in performance as the size of the network is increased. The algorithms and protocols designed for WSNs should consider communication cost with respect to network size.

(2) Power limitation. Since WSNs are often installed in remote areas such as deserts, forests, or military zones, their nodes are usually powered by batteries with limited life. Recharging such batteries may not be feasible. Given this constraint, the lifetime of any node is decided by the life of the battery powering it. As a result, the reduction of consumed power is vital. There are protocols and schemes that have been proposed to control power consumption by WSNs. These schemes are based on energy efficient MAC protocols, data aggregation, topology management, data compression, or intelligent use of batteries. Of course, using electronic devices and chips that consume less power is also a key design issue.

(3) Self-organization. Given the fact that WSNs may be installed in hostile environments, it is essential that they are designed to be self-organized. Nodes may fail due to harsh environment or depletion of the batteries; therefore, the network must be able to periodically re-configure itself so that it can continue to function and new nodes can be added, if possible. Individual nodes may be disconnected from the network, but the major portion of the network must continue to function.

(4) End objective. The ultimate objective of a WSN is not only communication; it has to detect and estimate certain events of interest. In order to enhance the detection and estimation capabilities, it is helpful to merge data from multiple sensors. Such a data fusion necessitates the transmission of data and control messages, which may put a limitation on the network design and structure. Furthermore, it is vital to distinguish between false data gathered and data reflecting a real emergency. For example, a high temperature in factory may indicate a real fire or may be due to sensing or processing errors.

(5) Querying capability. In WSN environments, a user may need to make an inquiry of an individual node or a selected cluster of nodes, for information gathering in the area. Based on the degree of data fusion performed, it may not be practicable to send a huge volume of data over the network. As an alternative, different neighboring sink nodes can gather data from a given area and generate summary messages. An inquiry may be sent to the sink node closest to the preferred location.

(6) Interoperability. With the impressive progress in sensing and communications technology, we start to see inexpensive, short-range radios, along with wireless networking devices and links. Of course, it is expected that WSNs will be widely deployed for all sorts of applications. Each node in the network may be equipped

with different sensors including seismic, acoustic, video camera, and infrared light, among others. Nodes may be configured in groups and they can synchronize with each other in a way that makes locally transpiring events be identified by the majority, if not all, of the nodes of the cluster. Such nodes will collaborate in order to make local decisions based on the data gathered by each node in the cluster. In such an arrangement, one node may act as the master node and the rest may act as the slaves.

(7) Cost. An important issue in the cost of wireless microcontrollers is the size of memory needed. Designers of wireless sensor networks will expect to have access to a range of chips or wireless microcontrollers with optimized memory size to meet the needs of a variety of applications. Likewise, the need for larger applications development such as gateway devices, and third party network layer development, show that there is a need for a much larger memory size, greater than 250 kB in some cases.

(8) Transmission time. One issue that is sometimes neglected is the amount of time needed to send the packets. Transmission time affects performance, quality of service, power consumption, and interference. It is necessary to have reliable data transmission and extended battery life in wireless sensor networks. We can improve the reliability of data transmission by using a small practical packet size since this gives the highest probability of a packet being delivered to the destination in the presence of interference. Extended battery life is obtained by minimizing the on time of the radio device, where most power is consumed. In general, a small packet size and occasional transmission can help to reach this goal in saving power.

(9) Compression of data. Compressing sensor data before transmission can offer a key decrease in transmission time. In sensor nodes like gas level, temperature, pressure, and light level sensors, the transmission of data on transition or exception, instead of normal planned transmissions, is an efficient way to minimize network traffic. Moreover, having the ability to perform digital filtering or data compression at the sensor node is a valuable approach to minimize the data size as well as the rate of recurrence of transmissions.

(10) Interference and environment. In general, interference from other nearby wireless networks such as Bluetooth or wireless LANs, should be addressed. Usually, this only presents a transitory state of interference to the WSN. For example, the capability of an IEEE 802.15.4 or ZigBee-based network to carry out automatic repeat will probably overwhelm any effect of interference from Bluetooth. Similarly, for WSNs employing occasional transmissions and for Bluetooth with frequency hopping, the probability of a frame collision is small. By utilizing collision avoidance schemes, wireless LANs (WLANs) can listen for a clear radio-frequency (RF) channel before they send data. However, under heavy traffic conditions in WLANs, we may get limited availability of the RF channel to the WSN due to the continuous state of interference. In such a situation, it is recommended for the WSN to be set on a different channel. Surrounding building structures also affect the RF environment. Steel reinforced concrete floors, stone

walls and analogous construction resources bring in high levels of attenuation as well as multipath fading. Similarly, the movement of persons or equipment considerably affects the signal level at any specific position. In general, effects of complex building structures can be alleviated by using additional router nodes in a mesh network that are installed to get around such obstacles.

(11) Security. Owing to the characteristics of the wireless communication medium, there are various security challenges that face WSNs including eavesdropping, man-in-the-middle attack, spoofing, and distributed denial of service (DDoS). The worry for security in WSNs can be even larger than that in a traditional ad-hoc wireless network as, in many cases, the computational and energy-consumption limitations create barriers in the implementation of powerful and effective security solutions in WSNs. Therefore, advances in the design of security mechanisms in WSNs for protecting the confidentiality, availability and integrity, are essential for the proper operation of such systems [3–15].

The acceptance of the Advanced Encryption Standard (AES) with a 128-bit key length guarantees data integrity and resistance to hacking. An AES security scheme can be implemented in software, while a dedicated hardware encryption processor offers a better solution since this reduces software overheads and permits faster encryption/decryption operation. Clearly, this is essential for sensor nodes, which must spend the least time possible awake, as staying awake consumes a lot of the power of the node's battery. Furthermore making the AES encryption chip accessible to the application software facilitates a higher level of security [3].

1.6 Comparison between wireless sensor networks and wireless mesh networks

The major applications of WSNs are logistics, environmental monitoring, industrial supervision, intelligent buildings, and military applications. WSNs have limited data capabilities and power saving requirements when compared to mesh networks. Typically, WSNs necessitate only a few bits per second per day, on average; they are not used when latency is crucial. Researchers have tried VoIP over IEEE 802.15.4, which specifies the physical layer and media access control for low-rate wireless personal area networks, with limited success. The main source of power saving of WSNs is their short duty cycle, which can be lower than 1%.

The key general differences between WSNs and mesh networks are as follows.

(1) The WSN traffic is less complex, not real, at low data rate.

(2) The WSN traffic is, in general, application specific; hence node design is driven by application. This means that the nodes are not flexible.

(3) Since the nodes in WSNs are inexpensive, they are less reliable than in a mesh network.

(4) The WSNs have more nodes at a high density, and the radio range is shorter.

Even though there are differences between WSNs and wireless mesh networks, there are many similarities [1–24].

(1) Basically, both do not require infrastructure; however, it is worth mentioning that mesh networks make use of the access points to enhance QoS and WSNs benefit from routers to enhance power consumption for edge nodes.
(2) The two technologies are self-organizing networks.
(3) Both have security and privacy weaknesses.
(4) The two networks bring in a reliance of the network on node behavior.
(5) Both benefit from clustering to get around scalability concerns.

It is interesting to point out that both WSNs and mesh networks are cooperative networks, which means that the MAC layer is decentralized and there is an aspect of fair contention for resources related to each node [3, 4, 9–14]. After showing the difference between WSNs and mesh networks, it is worth showing the difference of WSNs from radio-frequency identification (RFID) systems. The term RFID refers to the use of an object (usually called an RFID tag) that is applied to, or integrated into, a product, animal, or person for the intention of identification and tracking using radio waves. Various tags can be read from somewhat a few meters away and more than the line of sight of the reader. The overwhelming majority of RFID tags contain as a minimum two elements. One is an integrated circuit (IC) for saving and processing the data, modulating and demodulating a radio-frequency signal as well as other necessary operations. The second element is an antenna for getting and sending the signal. Table 1.2 shows the main differences between WSNs nodes, mesh networks nodes and RFID [1–12].

1.7 Summary

In this chapter, we have shed some light on the basic foundations of wireless sensor networks including components, structure, classifications and taxonomy, and characteristics. Fundamental related background has been given along with examples. We have

Table 1.2 Comparison between WSN nodes, mesh networks nodes, and RFID

Criteria	Wireless sensor node	Mesh network node	RFID
Size	Small	It can be handheld or larger	Embeddable
Cost	Low cost	Usually expensive	Trivial price for simplest RFID
Energy resources	Limited energy resources	High-quality batteries that are rechargeable	Typically, no power source is needed
Mobility	None or nomadic	Full mobility	None or nomadic
Radio range	Small	It can be large	Usually small to medium; powered RFID has a medium range
Processing power	Limited small processing	It cannot run large protocols such as TCP/IP	Very limited

elaborated on the challenges in operating and building wireless sensor networks that include: scalability, power limitation, organization, querying, capability, interoperability with other systems, cost, transmission time and speed, compression of data, interface with working environment, and security. Finally, we compared wireless sensor networks with wireless mesh networks and RFID systems.

References

[1] S. Dhurandher, S. Misra, M. S. Obaidat and S. Khairwal, “UWSim: a simulator for underwater wireless sensor networks,” *Simulation: Transactions of the Society for Modeling and Simulation International, SCS*, Vol. **84**, No. 7, pp. 327–338, July 2008.

[2] S. Misra, K. Abraham, M. S. Obaidat and P. Krishna, “LAID: a learning automata based scheme for intrusion detection in wireless sensor networks,” *Security and Communications Networks, Wiley*, Vol. **2**, No. 2, pp. 105–115, March/April 2009.

[3] M. S. Obaidat, P. Nicopolitidis and J.-S. Li, “Security in wireless sensor networks,” *Security and Communications Networks, Wiley*, Vol. **2**, No. 2, pp. 101–103, March/April 2009.

[4] S. Misra, M. S. Obaidat, S. Sanchita and D. Mohanta, “An energy-efficient, and secured routing protocol for wireless sensor networks,” in *Proceedings of the 2009 SCS/IEEE International Symposium on Performance Evaluation of Computer and Telecommunication Systems, SPECTS 2009*, pp. 185–192, Istanbul, Turkey, July 2009.

[5] S. Misra, K. I. Abraham, M. S. Obaidat and P. V. Krishna, “Intrusion detection in wireless sensor networks: the S-model learning automata approach,” in *Proceedings of the 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications: The First International Workshop in Wireless and Mobile Computing, Networking and Communications (IEEE SecPriWiMob’08)*, pp. 603–607, Avignon, France, October 12–14, 2008.

[6] S. K. Dhurandher, S. Misra, M. S. Obaidat and N. Gupta, “QDV: a quality-based distance vector routing for wireless sensor networks using ant colony optimization,” in *Proceedings of the 4th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications: The First International Workshop in Wireless and Mobile Computing, Networking and Communications (IEEE SecPriWiMob’08)*, pp. 598–602, Avignon, France, October 12–14, 2008.

[7] S. Misra, V. Tiwari and M. S. Obaidat, “Adaptive learning solution for congestion avoidance in wireless sensor networks,” in *Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2009*, pp. 478–484, Rabat, Morocco, May 2009.

[8] A. Swami, Q. Zhao, Y.-W. Hong and L. Tong (Eds.), *Wireless Sensor Networks: Signal Processing and Communication Perspectives*, John Wiley & Sons, 2007.

[9] Y.-C. Tseng, M.-S. Pan and Y.-Y. Tsai, “Wireless sensor networks for emergency navigation,” *IEEE Computer*, Vol. **39**, No. 7, pp. 55–62, 2006.

[10] C.-Y. Chong and S. P. Kumar, “Sensor networks: evolution, opportunities, and challenges,” *Proceedings of IEEE*, Vol. **91**, No. 8, pp. 1247–1256, 2006.

[11] S. Cheekiralla and D. W. Engels, “A functional taxonomy of wireless sensor network devices,” *Proceedings of the 2005 International Conference on Broadband Networks Conference, BroadNets 2005*, Vol. **2**, pp. 949–956, 2005.

[12] R. MacRuairi, M. T. Keane and G. Coleman, “A wireless sensor network application requirements taxonomy,” in *2008 IEEE International Conference on Sensor Technologies and Applications, IEEE Computer Society*, pp. 209–216, 2008.

[13] S. Methley, *Essentials of Wireless Mesh Networking*, Cambridge University Press, 2009.

[14] J. Zheng and A. Jamalipour, *Wireless Sensor Networks: A Networking Perspective*, John Wiley & Sons, 2009.

[15] P. Nicopolitidis, M. S. Obaidat, G. I. Papadimitriou and A. S. Pomportsis, *Wireless Networks*, John Wiley & Sons, 2003.

[16] M. S. Obaidat and J. W. Ekis, “An automated system for characterizing ultrasonic transducers using pattern recognition,” *IEEE Transactions on Instrumentation and Measurement*, Vol. **40**, No. 5, pp. 847–850, October 1991.

[17] M. S. Obaidat and D. S. Abu-Saymeh, “Methodologies for characterizing ultrasonic transducers using neural network paradigms,” *IEEE Transactions on Industrial Electronics*, Vol. **39**, No. 6, pp. 529–536, Dec. 1992.

[18] M. S. Obaidat, “On the characterization of ultrasonic transducers using pattern recognition techniques,” *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. **23**, No. 5, pp. 1443–1450, Sep./Oct. 1993.

[19] M. S. Obaidat, H. Khalid and B. Sadoun, “Ultrasonic transducers characterization by neural networks,” *Information Sciences Journal, Elsevier*, Vol. **107**, No. 1–4, pp. 195–215, June 1998.

[20] M. S. Obaidat and H. Khalid, “Performance evaluation of neural network paradigms for ultrasonic transducers characterization,” in *Proceedings of the IEEE International Conference on Electronics, Circuits and Systems*, pp. 370–376, Dec. 1995.

[21] M. S. Obaidat and D. S. Abu-Saymeh, “Performance comparison of neural networks and pattern recognition techniques for classifying ultrasonic transducers,” in *Proceedings of the 1992 ACM Symposium on Applied Computing*, pp. 1234–1242, Kansas City, MO, March 1992.

[22] M. S. Obaidat and D. S. Abu-Saymeh, “Neural network and pattern recognition techniques for characterizing ultrasonic transducers,” in *Proceedings of the 1992 IEEE Phoenix Conference on Computers and Communications*, pp. 729–735, April 1992.

[23] W. Dargie and C. Poellabauer, *Fundamentals of Wireless Sensor Networks: Theory and Practice*, John Wiley & Sons, 2010.

[24] K. Sohraby, D. Minoli and T. Znati, *Wireless Sensor Networks: Technology, Protocols, and Applications*, John Wiley & Sons, 2007.