RESEARCH ARTICLE OPEN ACCESS

Wireless Sensor Networks: Opportunities and Challenges

Matthew N. O. Sadiku[*] and Sarhan M. Musa[*], Omonowo D. Momoh[**]
[*] Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX 77446
[**]College of Engineering, Technology, and Computer Science Indiana University-Purdue University Fort Wayne, IN 46805

ABSTRACT
The popularity of cell phones, laptops, PDAs and intelligent electronics has made computing devices to become cheaper and more pervasive in daily life. The desire for connectivity among these devices has caused an exponential growth in wireless communication. Wireless sensor networks (WSNs) provide an example of this phenomenon. WSNs belong to the general family of sensor networks that employ distributed sensors to collect information on entities of interest. This paper provides a brief introduction to wireless sensor networks. It addresses the opportunities and challenges of WSNs.
Key Words: Wireless networks, sensors, computing

I. INTRODUCTION

A wireless sensor network (WSN) usually consists of a large number (hundreds or thousands) of sensor nodes deployed over a geographical region. The wireless sensor nodes are compact, light-weighted, and battery-powered devices that can be used in virtually any environment [1-3]. The sensor nodes monitor physical or environmental conditions such as temperature/heat, humidity, sound, vibration, pressure, light, object motion, pollutants, presence of certain objects, noise level or characteristics of an object such as weight, size, speed, direction, and its latest position. As shown in Figure 1, each sensor node is made up of four components: a power unit, a transceiver unit, a sensing unit, and a processing unit. The node may also have some application-dependent components such as power generator, location finding system, and mobilizer. Communication among the nodes is done in a wireless fashion, and thus, the name *wireless sensor networks*. Companies such as Crossbow (www.xbow.com) and Monnit (www.monnit.com) have developed the necessary software and hardwire building blocks for WSNs.

In general, there may be both sensing and nonsensing nodes in a WSN; i.e. all sensors are nodes but not all nodes are sensors. A sensor has four operating modes: transmission, reception, idle listening, and sleep. Collision occurs when there are two or more nodes transmit at the same time.

A sensor node is designed to use an operating system (OS). TinyOS (developed at UC Berkeley) is perhaps the first operating system specifically designed for WSNs. It is a general-purpose OS. Both the TinyOS and programs written for it are written in a special programming language called NesC, which is essentially an extension of C programming language.

Figure 2 presents a typical wireless sensor network. Sensors can be deployed on the ground, in the air, under water, in vehicles, on bodies, and inside buildings. A network of sensors can detect and track threats.

II. APPLICATIONS

In September 1999, *Business Week* predicted that WSN would be one of the 21 most important technologies for the 21st century. The number of applications of WSN is increasing rapidly. It is generally true that applications should shape and form the technology for which they are intended. WSNs are no exception to this. WSNs have been technology-driven in their development. Advances in software technology and wireless communication have paved the way for successful adoption of the wireless sensor networks in various applications. Some of the expected applications of WSNs will require a large number of devices in order of tens of thousands of nodes. Applications of WSNs typically involve some kind of monitoring, tracking, or controlling. Some of the specific applications include the following [4-6]:

(a) *Military Applications*: As with many technologies, the development of WSNs was motivated by military applications such as battlefield surveillance. Typically, sensors can report vehicle and personnel movement, allowing a close monitoring of opposing forces. Other military applications include monitoring friendly forces, battlefield surveillance, reconnaissance of opposing forces, and battle damage assessment. Sensitive objects and structures such as atomic plants and

ammunition depots can be protected by intelligent sensors.

(b) *Civil Engineering*: Structural health monitoring for civil structures has been a research focus for academia and industry. Sensors can be placed in bridges to detect structural weakness and in water reservoirs to detect hazardous materials.

(c) *Agriculture and Environment Monitoring:* A number of WSNs have been deployed for agricultural and environmental monitoring. For example, the Zebranet project at Princeton aims at tracking the movement of zebras in Africa. Researchers at University of West Australia are developing a prototype WSN for monitoring of soil water. Fire and floods can be detected by densely deployed sensor networks. WSNs can potentially advance the pursuit of geographical studies of volcanic activity.

(d) *Industrial Applications*: Sensors are already widely deployed in industrial applications, such as in monitoring of assembly lines. Industrial robots are equipped with sensors and are connected wirelessly to a computer. Cars, which have sensors and actuators in them, can be networked to improve the efficiency of traffic.

In addition to traditional applications of wireless sensor networks, they can also be used to protect cultural property. In cultural property protection, setting up fixed structure (with power lines and communication cables) is not allowed. Since WSNs do not require wired infrastructure, they can be used for cultural property protection. For example, Bulguksa temple (a Buddhist temple in South Korea) has been designated as the world's cultural property by UNESCO. Such a temple requires WSN to monitor and protect cultural artifacts in the temple.

III. CHALLENGES

As noted above, wireless sensor networks have a wide range of potential applications. However, there are many challenging problems that must be addressed for efficient operation of WSNs in real applications and current technology is not up to meeting some of these challenges. These challenges include [7-9]:

(a) *Size*: The main challenge is to produce low cost and tiny sensor nodes. Miniaturization and low cost will follow from the recent and future development in the field of micro-electro-mechanical systems (MEMs). Several aspects of WSN nodes can be miniaturized with MEMs technology.

(b) *Energy:* Energy is the scarcest resource of WSN nodes and it determines the lifetime of WSNs. Being a microelectronic device, a sensor node can be equipped with a limited power source (less than 0.5 Ah, 1.2 V). Sensor nodes may be equipped with effective power scavenging techniques, such as solar cells, because it is not easy to access or replace them after deployment. For those that use battery, battery lifetime is one of the critical factors to consider in the network design.

(c) *Storage*: The use of wireless channels and the reliability of sensor nodes lead to a new approach for data storage and retrieval. The new approach is to have data stored
locally within the sensors.

(d) *Routing*: The design of routing protocols in WSNs is influenced by several challenging factors that must be overcome in order to achieve efficient communication. Routing in WSNs differs from the one in conventional IP networks. Getting data from all the thousands of sensors may result in the receipt of irrelevant and redundant data from nodes. This is definitely inefficient at the level of storage and energy.

(e) *Security*: WSNs communicate important private data and security is a crucial issue. We recall that many WSNs are used for military or surveillance purposes. One way to ensure data security is to use encryption, but this is not practical for efficiency and resource constraints.

It is difficult, if not impossible, to meet these challenges in a single network. Most WSNs are application specific and are designed to meet the challenges for that specific application.

IV. CONCLUSIONS

This paper presents an overview of wireless sensor networks. It is hoped that the reader would have an appreciation of the applications for which WSNs are intended. The study of WSNs is challenging because it requires an enormous breadth of knowledge from a variety of disciplines including signal processing, networking and protocols, embedded systems, and distributed algorithms. The field of WSN is gaining interest among researchers and diverse groups such as environmental, public safety, military, and medicine. The development and applications of WSNs have made them to be hot research topics. Sensor network technology will have a significant impact on our lives in the 21st century.

REFERENCES

[1] I. F. Akylidiz et al., "A survey on sensor networks," *IEEE Communications Magazine*, Aug. 2002, pp. 102-114.

[2] l. Mokdad et al., "Performance evaluation tools for QoS MAC protocol for wireless sensor networks," *Ad Hoc Networks*, vol. 12, 2014, pp. 86-99.

[3] R. I. de Silva et al., "Spatial query processing in wireless sensor networks—A survey," *Information Fusion*, vol. 15, 2014, pp. 32-34.

[4] H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks.* Chichester, UK: John Wiley & Sons, 2005, pp. 3-7.

[5] H. K. Patil and T. M. Chen, "Wireless Sensor Network Security,' in J. Vacca (ed.), *Computer and Information Security Handbook*. San Francisco, CA: Morgan Kaufmann Publishers, 2013, 2nd ed.,chapter 15, pp. 349-397.

[6] E. Aleisa, "Wireless sensor networks framework for water resource management that supports QoS in the Kingdom of Saudi Arabia," *Procedia Computer Science*, vol. 19, 2013, pp. 232-239.

[7] M. Ilyas and I. Mahgoub (eds.), *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*. Boca Raton, FL: CRC Press, 2005, pp. 1.1-1.14.'

[8] J. Lopez and J. Zhou, *Wireless Sensor Network Security*. Amsterdam, Neverthelands: IOS Press, 2008, pp. 164-122.

[9] Y. Li, M. T. Thai, and W. Wu, *Wireless Sensor Networks and Applications*. New York, NY: Springer, 2008, pp. 403-421.

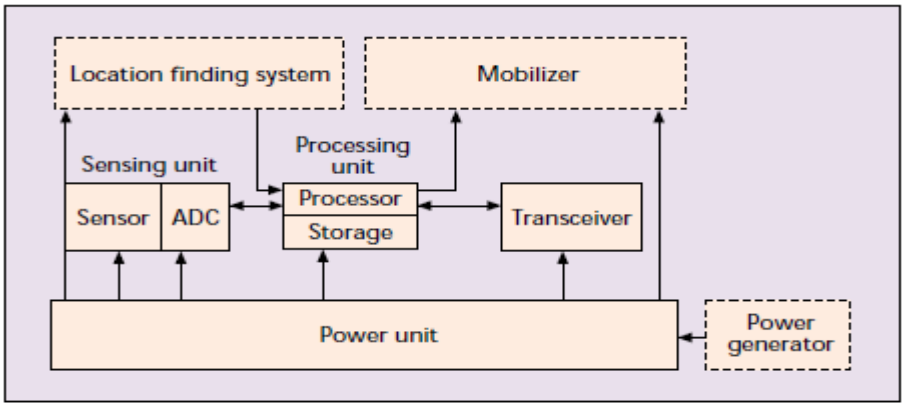

Figure 1 Components of a sensor node.

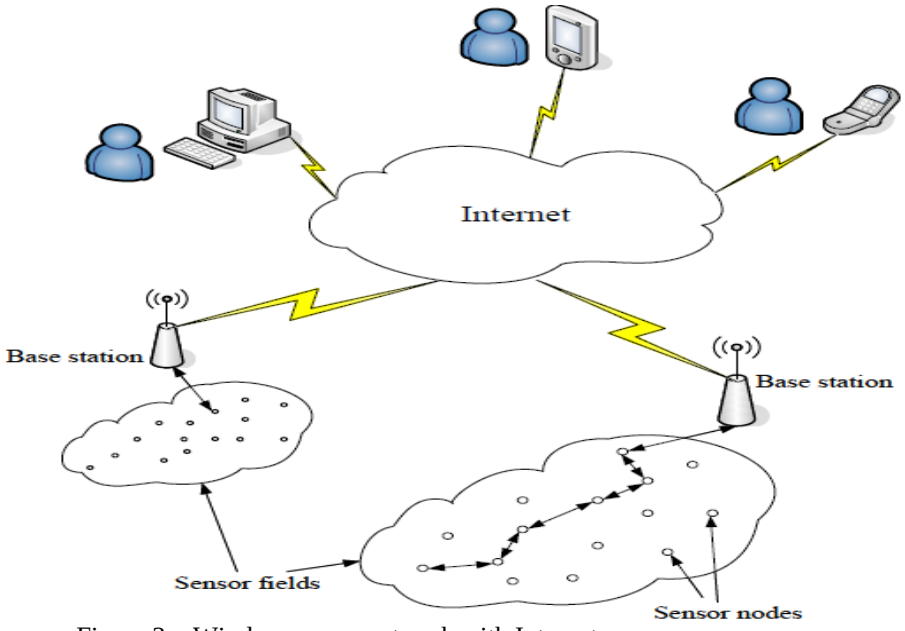

Figure 2 Wireless sensor network with Internet access