An Overview of Wireless Sensor Networks Towards Internet of Things

Mustafa Kocakulak[†] and Ismail Butun[†*]

[†] *Department of Mechatronics Engineering*
Bursa Technical University, Bursa, Turkey
mustafa.kocakulak@btu.edu.tr

[*] *Department of Electrical and Computing Engineering*
University of Delaware, Newark, Delaware, USA
ibutun@udel.edu

***Abstract*— With the advancements in wireless technology and digital electronics, some tiny devices have started to be used in numerous areas in daily life. These devices are capable of sensing, computation and communicating. They are generally composed of low power radios, several smart sensors and embedded CPUs (Central Processing Units). These devices are used to form wireless sensor network (WSN) which is necessary to provide sensing services and to monitor environmental conditions. In parallel to WSNs, the idea of internet of things (IoT) is developed where IoT can be defined as an interconnection between identifiable devices within the internet connection in sensing and monitoring processes. This paper presents detailed overview of WSNs. It also assesses the technology and characteristics of WSNs. Moreover, it provides a review of WSN applications and IoT applications.**

***Index Terms*— Wireless Sensor Networks, Internet of Things, Sensor Node, Ad-hoc Network, WSN Security, IoT.**

I. Introduction

WITH the rapid technological development of wireless technology and embedded electronics, Wireless Sensor Networks (WSNs) have started to attract researchers' interest. A typical WSN is composed of tiny devices which are known as nodes. These nodes include embedded CPU, limited computational power and some smart sensors. With these sensors, Nodes are used to monitor surrounding environmental factors such as humidity, pressure, heat and vibration. Typically, a node in any WSN contains sensor interface, computing unit, transceiver unit and power unit. These units perform crucial tasks by making nodes able to communicate among each other to transmit data obtained by their sensors. Communication between the nodes is necessary to have a centralized system. The necessity of this system leads to development of the notion of internet of things (IoT). With the notion of IoT, immediate access to environmental data becomes feasible. So that in numerous processes, efficiency and productivity increases dramatically.

In this paper, a detailed overview of WSNs is given. The objectives of this paper are assessing WSNs technology and characteristics, reviewing WSNs applications and providing information on the challenges and future of WSNs. Section2 starts with the definition of WSNs and it provides the architecture of WSNs. Section3 gives historical background of WSNs and Section4 explains how WSNs work. In Section5 advantages and disadvantages of WSNs are listed. Section6 provides information on application of WSNs and Section7 addresses the challenges of WSNs security and privacy. Lastly, Section 8 addresses the future trends of WSNs and IoT applications.

II. What is a WSN?

Typically, a WSN can be defined as a network of nodes that work in a cooperative way to sense and control the environment surrounding them. These nodes are linked via wireless media. Nodes use this connection to communicate among each other. The architecture of a typical WSN consists of following 3 components: sensor nodes, gateway and observer (user). Sensor nodes and gateways constitute the sensor field. Gateways and observers are interconnected via special networks or more commonly via internet (please see Fig. 1).

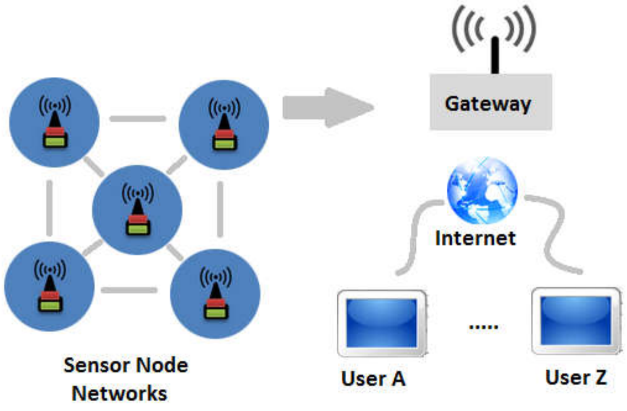

Fig. 1. Wireless Sensor Network (WSN)

Conceptually a WSN is based on a simple equation which

978-1-5090-4228-9/17/$31.00 ©2017 IEEE

depends on the fact that Sensing + CPU + Radio = Lots of Potential [1]. Sensing Unit is necessary to monitor surrounding environment and its conditions such as humidity, pressure and vibration. After completing monitoring and sensing processes, necessary computations are accomplished in CPU. Lastly, computed environmental data are transferred by Radio Unit through the wireless communication channels among the nodes. Finally, these data are sent towards the Gateway.

III. History of WSNs

The first wireless network that can be defined as modem WSN is known as the Sound Surveillance System (SOSUS). SOSUS was developed to detect Soviet submarines by the U.S. Military in the 1950s. SOSUS network is designed to have submerged sensors and hydrophones which are scattered in the Atlantic and Pacific Oceans [2].

U.S. DARPA has pioneered the Distributed Sensor Network (DSN) initiative in 1980s to find out the unique challenges of implementing WSNs. The potential of DSN and its progression in academia have attracted researchers' attention. These factors led the explore potential of WSN has started to be searched in academia and in civilian scientific researches.

As an example for WSN researches, IEEE has noticed the following fact: The low cost and high capabilities of these tiny devices. IEEE organization has defined a standard for this fact - the IEEE 802.15.4; to cover low data rate wireless personal area networks. Based on this standard, ZigBee Alliance has published the ZigBee standard that can be used in WSNs.

IV. How it works?

WSNs are collection of nodes and these nodes are individual small computers. These tiny devices work cooperatively to form centralized network systems. There are some requirements for nodes to be used in these networks such as efficiency, multi-functionality and being wireless.

Moreover, each node in any network has a predefined goal. For example, if it is aimed to collect information about microclimates across all sections of any forest, these nodes are placed in different trees in the forest to form a network. In this network, they should have a centralized and synchronized structure for communicating and data sharing. The sensor nodes are placed in a connected network according to a certain topology such as linear, star and mesh. Nodes of the network in any topology have a limited broadcast range which is generally 30 meters.

In WSNs, data collection and data transfer are accomplished in 4 steps: collecting the data, processing the data, packaging the data and transferring the data.

A. Technology

A WSN is composed of several numbers of sensors and a gateway to provide connection to the Internet.

Sensor Node

Sensor node is one of the main components of any WSN [3]. A sensor node is a low powered small device. Although it has limited energy resources, it has concurrent processing feature and also it has a low cost. Fig. 2 has shown the components of a sensor node. Data collection and data transfer steps are accomplished by specific units of a sensor node.

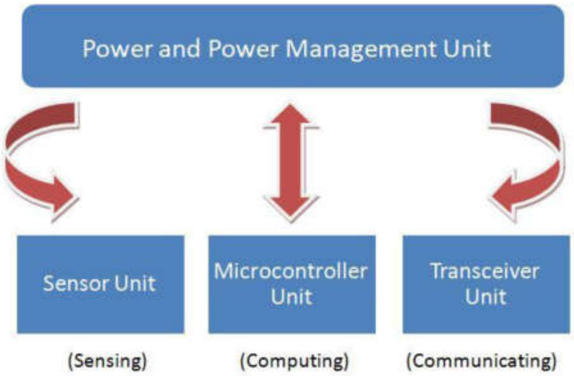

Fig. 2. Components of a WSN

Power Source

Power Source is placed to the sensor node's base. It supplies energy for various units of sensor nodes like sensing units (sensors), CPU and radio. In order to continue to perform sensing, computing and communicating tasks; energy is needed. Therefore, ambient energy harvesting techniques (from external resources) are used to power small sensor nodes. Power resources can be AA batteries, watch batteries, solar cells or smart systems.

Ambient energy harvesting can be accomplished in various ways such as through the conventional optical cell power generation and through miniature piezoelectric crystals, micro oscillators and thermoelectric power generation elements, etc. [3]. For any sensor nodes the energy resources are limited and energy is crucial to perform all tasks. Therefore, nodes spend as much as 99% of their time in sleep to conserve energy. They only wake up to record data, to send data and to receive data.

Microcontroller

Typically, the CPU (also called the electronic brain) of a sensor is composed of a microprocessor and a flash memory. In most of sensor nodes, it includes connectors to add external processing units and sensors to the main unit easily. Making decision and dealing with collected data can be listed as examples for the crucial functions of the CPU. The CPU stores data in flash memory until enough data has been collected. Once enough data is collected by the system, then microprocessor unit of the CPU puts the data in envelopes because envelopes provide great efficiency in data transmission. Then, these envelopes are sent to the radio for broadcast. Meanwhile the brain communicates also with other nodes in much the same way it deals with data to maintain the most effective network structure. The CPU is connected to the base and it interacts with the sensors and radio [4].

Sensor Transducer

The most crucial part of a WSN is the sensors. Sensors convert environmental variables like light, smoke, heat, and sound etc. into electrical signals. In the past two decades, there has been rapid development in multiple sensing technologies which eased the way of the sensors being produced:

- Micro-electro-mechanical systems (MEMS) such as gyroscopes, acoustic sensors, accelerometers, smoke sensors, magnetometers, chemical sensors, pressure sensors, and piezoelectric sensors.
- CMOS-based sensors such as chemical composition sensors, humidity sensors, temperature sensors, and capacitive proximity sensors.
- LED sensors such as chemical composition sensors, proximity sensors, and ambient light sensors.

These advancements have made sensors widely in use in daily life notably in sensor nodes. A typical node consists of three types of sensors which are temperature, vibration and moisture. But some nodes can have extra features such as taking photographs of surroundings, sensing motion, sensing pressure, sensing smoke, sensing light, etc.

Transceiver

It is responsible for the wireless communications of a sensor node. Transceiver has mainly four operational states which are Receive, Transmit, Idle and Sleep. As a wireless media, Radio Frequency (RF), Infrared and Laser can be chosen in transceiver. Among these wireless communication technologies, RF is widely preferred for WSNs. Typical operation range of RF (for the operation frequencies of WSNs) is 10s of meters indoors and 100s of meters outdoors.

Operating System

Tiny OS, Contiki, MANTIS, BTunt are the examples of operating systems that are used for WNSs. Among these systems, Tiny OS is the one that is open source and energy efficient. Instead of multithreading, Tiny OS uses event-driven programming methodology.

B. Gateways

Gateways let the system administrators to interface nodes to Personal Digital Assistants (PDAs) and Personal Computers (PCs). Gateways can be in three different states as active, passive, and hybrid. Active gateway lets the nodes to send its data actively to the gateway server. Passive gateway cannot act free as the active gateway does. It sends a request to sensor nodes to send its data. Hybrid gateway is the combination of these two gateways, which can operate in both of the states.

C. Task Managers

They connect to the gateways by some defined media such as satellite link, or Internet. Task Managers consist of two sections: Client Data Browsing/Processing and Data Service. Task Managers can be considered as an information processing and retrieval platform. All collected sensor data is stored and analyzed in this part. Users and administrators can use an interface to get and analyze these data locally and/or remotely [5].

D. Communication Architecture for WSNs

A typical radio consists of a radio transmitter and a radio receiver. These two components should be supplied for any node so as to make it fully communicate (bi-directional) with other nodes. During the transmission of data, the radio receives data from the brain and broadcasts it to other sensor nodes. During the reception of data, the radio receives data from another node's radio and it transmits data to the brain.

All data collected by the sensor node is routed to the parent node. This parent node is connected to a multi-functional computer so as to make other nodes' data accessible by user's computer interface. If the user gives directives, these directives will be sent over the Internet to the multi-functional computer. This computer will send these directives to the parent node and parent node will send the same message to its children nodes.

Standards and Specifications:

Here are the most widely used WSN communication standards:

ZigBee: Normally, communication range of ZigBee is up to 10 meters. However, it can transmit data over long distances. This is achieved by passing the data over short distances between the intermediate devices. Its power consumption is ultralow. Data Range is up to 20 kbps.

Bluetooth: It is a wireless technology standard designed to exchange data over short distances in between mobile devices. Communication range is from 1 meter up to 100 meters. Its power consumption is low. Data range is up to 3 Mbps.

6LoWPAN: It is a mechanism that allows IPv6 packets to be sent and to be received from over IEEE 802.15.4 based networks. Its communication range is from 45 meters up to 90 meters. Its power consumption is medium.

The Architecture of the Protocol Stack for WSNs

Fig. 3 shows the architecture of protocol stack that is used by the sink and sensor nodes. This protocol stack integrates power with routing awareness. It integrates data with networking protocols and it communicates through the wireless medium power efficiently [6].

The mentioned protocol stack consists of the following layers and planes: 1) Physical Layer, 2) Data Link Layer, 3) Network Layer, 4) Transport Layer, 5) Application Layer;

a) Power Management Plane, b) Mobility Management Plane, c) Task Management Plane.

The *Physical Layer* is designed to handle frequency selection, frequency generation, modulation, signal detection and encryption.

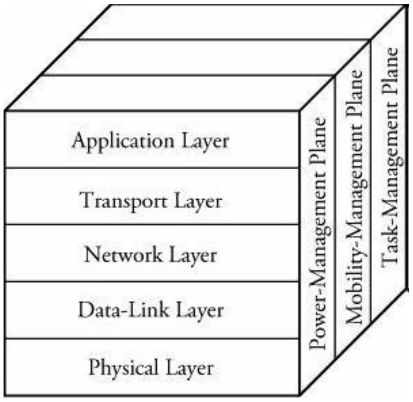

Fig. 3. Protocol Stack for WSNs [7]

The *Data Link Layer* is designed to handle error control and the Medium Access. This layer ensures reliable end-to-end connections in a communication network.

The *Network Layer* is responsible for routing the data provided by the transport layer.

The *Transport Layer* is responsible for maintaining the flow of data to keep WSN operable when needed.

The *Power Management Plane* manages how a sensor node uses its power and also it decides on power consumption rates among three operations: sensing, computing, and communicating.

The *Mobility Management Plane* detects the movement of sensor nodes. It also registers the mobility of sensor nodes. Hence a route back to the user is always kept. Therefore, the nodes can manage their power to complete their tasks by considering this situation.

The *Task Management Plane* organizes the events which are mainly sensing and detecting events from a specific area. Thus, not all of the sensor nodes perform the sensing tasks at the same time and at the same area.

E. Set Up

Design Factors and Requirements:

Fundamental design factors that have been addressed by many researchers are shown below:

Reliability: Reliability (in other words, fault tolerance) of a sensor node is the ability of sensor to maintain its network functionalities without any interruption. Sensor node failure is a kind of interruption which can occur due to energy shortage, physical damage and environmental interference.

Density and Network Size/ Scalability: Innumerable sensor nodes may be deployed by the user to study a phenomenon of his interest. So, the density of these nodes increases dramatically and the density affects the coverage area of interest, reliability and accuracy.

Sensor Network Topology: Network latency, network capacity, and robustness of the network are affected by network topology. Furthermore, the complexity of data routing depends on network topology.

Energy Consumption: Sensor nodes are battery operated and therefore the life time of each node depends possibly on the life time of batteries.

Hardware Constraints: Sensor nodes mainly consist of 4 components: sensing unit, power unit, processing unit, and transmission unit. They may also possess external units and additional plug-ins.

Data Aggregation (Fusion): It is a useful function that is accomplished by computation unit to reduce data size by compressing (meaningfully) the data into meaningful information.

Transmission Media: In order to establish links for the nodes, a wireless medium is used for communication goals.

Security: Security aspects of WSNs are focused on the centralized communication approaches. So, there is a need to develop a distributed security approaches for WSNs.

Self-Configuration: It is essential for WSNs to be self-organized. Since sensor node failure can occur in any network, new sensor nodes may join the network so as to decrease the negative effects of these failures.

Network Dynamics: In many applications of WSNs, the mobility of sensor nodes or the base station is essential, which means that sensor nodes are wandering around. This has arisen many issues from the routing stability to energy, bandwidth, etc.

Quality of Service: For some applications, data delivery within a bounded and suggested latency is considered as crucial. Sensing data after the bounded certain latency possibly would be useless.

Coverage: It is defined as an ability of sensor nodes to cover physical area of the surrounding environment which is limited in range and also limited in accuracy.

Connectivity: Network connectivity is defined by a permanent connection between any two different sensor nodes. These nodes are densely deployed in a sensor network.

F. WSN Development Platforms

Following platforms are some of the mostly used development platforms for WSNs: Crossbow, Dust Networks and Sensoria Corporation [8].

G. WSN Simulators

Following simulators are some of the mostly used simulators in the world: NS3, GloMoSim, J-Sim, SensorSim, OPNET and OMNET++. Such simulators make users to verify new ideas and also compare their solutions in a virtual environment. Due to working in virtual environment, unexpected and expensive implementation costs are avoided [9].

H. WSN Emulators

Following emulators are some of the most well-known emulators in use: TOSSIM, ATEMU, AVRORA and EMSTAR. Such emulation tools make users to verify new ideas and compare their proposed solutions in a virtual environment. Due to working in virtual environment, expensive implementation costs are avoided [9].

V. Advantages and Disadvantages of WSNs

Advantages: Since WSNs use wireless communication instead of hard wiring, they do not need complex infrastructure. Owing to wireless structure, WSNs become cheaper. They spend less energy since devices are usually in sleep to conserve energy. Furthermore, WSNs are compatible with external devices and new plug-ins. This feature increases their usage areas and also their functionality.

Disadvantages: WSNs have comparatively low speed of communications, limited memory space and narrow bandwidth. They are battery dependent. Since they have limited power sources, they are designed to consume less operating energy. But, consumption of less energy can cause avoidance of taking essential security precautions. Since there are some security leaks that can occur due to energy saving policies, WSNs may be attacked by malicious attackers. Moreover, WSNs are affected by surroundings such as walls and far distance etc. [10].

VI. Applications

As it is known, WSNs provide sensing, monitoring and controlling options. Therefore, they have vast amount of application fields such as military applications, environmental applications, and industrial applications. In military applications, monitoring friendly forces or battlefield surveillance are realized by WSNs. In environmental applications, air and water quality can be monitored by WSNs. In industrial applications, control and automation processes like transportation and object tracking can be accomplished by WSNs [11].

VII. Security

Security of WSNs is an important issue, especially if they have mission-critical tasks [12]. For example, confidentiality of a patient health record should not be released to third parties in a health care application. Attacks against the security of WSNs can be grouped into two branches as; active and passive. In active attacks, an attacker actually affects the operations badly in the targeted network. This might be the main objective of the attacker, which can be detected easily when compared to the passive attacks. Active attacks can be grouped into hole attacks (black hole, sink hole, worm hole, etc.), Denial-of-Service (DoS) attacks, jamming attacks, flooding attacks and finally, Sybil attacks [13]. In passive attacks, attackers are generally hidden physically and either tap the data link to collect data; or destroy or destroy any operating units of the network. Passive attacks can be grouped into eavesdropping attack, node tampering attack, node malfunctioning attack, node destruction attack and finally, traffic analysis attack.

As in all networks; in order to assess security for WSNs, two actions can be taken against attacks: Intrusion Prevention and Intrusion Detection [14]. Intrusion prevention techniques can be thought as the first line of defense against intruders (attackers). However, as in any kind of security system, intrusions cannot be prevented totally. The intrusion and compromise of a single node can result in revealing of important security information (passwords, etc.) of the network to intruders. This results in the failure of the preventive security mechanism [15]. Therefore, Intrusion Detection Systems (IDSs) are designed to reveal intrusions, before they can disclose information about the secured system resources. IDSs are always considered as a second wall of defense from the security point of view. IDSs can be thought as the cyberspace equivalent of the burglar alarms that are being used in today's physical security systems.

VIII. Future Scope

By the development of Micro-Electrical Systems (MEMS), wireless network systems are expected to be widely in use. MEMS are the combination of electrical devices and mechanical structures at an extremely small scale. Many researches need to be done so as to implement MEMS in WSNs. For example, the effects of very large node densities need to be investigated. The increase in the usage of WSN devices and the expected difficulty to access specific device among the entire network should not be ignored.

Moreover, IoT is expected to have dramatic impact in our lives in near future. WSNs will be integrated into IoT and innumerable sensor nodes will join the Internet. They will cooperate with other nodes to sense and to monitor the environment.

IoT will provide an interaction between people and environment more in near future as shown in Fig. 4. So, their usage areas will increase continuously and dramatically. For example in near future widely used smart driver systems will be feasible that can inform drivers before they encounter some meteorological events such as heavy rain and secret ice etc.

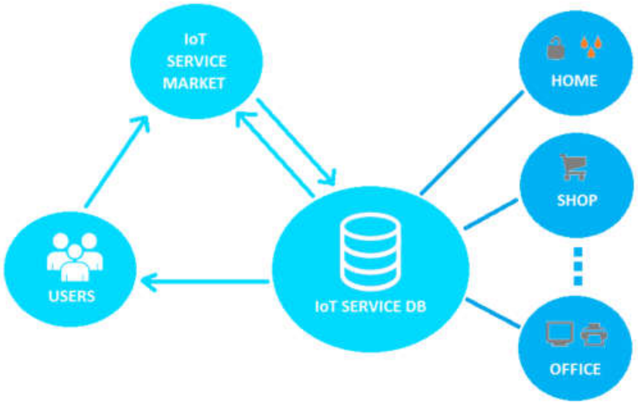

Fig. 4. Internet of Things (IoT)

VIII. Conclusion

A WSN is a network of nodes which work cooperatively to monitor the surrounding environment. It is necessary to provide an interaction between people and nodes' environment. In this paper, WSNs are described in a compact manner and technical details of their characteristics are provided. Moreover, widely used applications of WSNs are presented and the potential of WSNs for many other application areas is emphasized. Protocol Stacks, advantages and disadvantages of WSNs are listed. As a future expectation, the usage of WSNs in a wide range of application areas especially in IoT is foreseen.

X. References

[1] Ephrem, E. (2015, June 8). Architecture of Wireless Sensor Networks. Retrieved October 8, 2015, from http://servforu.blogspot.com.tr/2012/12/architecture-of-wireless-sensor-networks.html

[2] Q. Wang, I. Balasingham, *Wireless Sensor Networks – An Introduction*, Wireless Sensor Networks: Application-Centric Design, 2010.

[3] Yinbiao, D., & Lee, D. (2014). IEC White Paper Internet of Things: Wireless Sensor Networks. International Electrotechnical Commission White Paper.

[4] Culler-Mayeno, E. (2006). A Technical Report: Wireless Sensor Networks and How They Work. Retrieved October 8, 2015, from http://www.writing.ucsb.edu/faculty/holms/2E_motes_report.pdf

[5] M.A.E. Villegas, S.Y. Tang, Y. Qian, *Wireless Sensor Network Communication, Architecture for Wide-Area Large Scale Soil Moisture Estimation and Wetlands Monitoring,* Department of Electrical and Computer Engineering, University of Puerto Rico at Mayaguez, 2007.

[6] A. Holmes, *A Technical Report: Wireless Sensor Networks and How They Work,* University of California Santa Barbara, 2006.

[7] S. Ramesh, *A Protocol Architecture for Wireless Sensor Networks,* School of Computing, University of Utah, 2008.

[8] K. Sohraby, D. Minoli, T. Znati, *Wireless Sensor Network,* John Wiley and Sons Inc., 2006.

[9] M.A. Matin, M.M. Islam, *Overview of Wireless Sensor Network,* INTECH Open Access Publisher, 2012.

[10] T. Soylu, *Wireless Sensor Networks Applications and Design of A Sensor Node,* Computer Engineering Department, Trakya University, 2012.

[11] T.E Kalayci, *Wireless Sensor Networks and Applications,* Computer Engineering Department, Ege University, 2009.

[12] J. Sen, *Security in Wireless Sensor Networks,* Department of Computer Science and Engineering, National Institute of Science and Technology, India, 2010.

[13] I. Butun, S.D. Morgera, R. Sankar, *A survey of intrusion detection systems in wireless sensor networks*, Communications Surveys & Tutorials, IEEE, 16(1), pp. 266-282, 2014.

[14] I. Butun, *Prevention and Detection of Intrusions in Wireless Sensor Networks*, PhD Dissertation, University of South Florida, 2013.

[15] I. Butun, Y. Wang, Y.S. Lee, R. Sankar, *Intrusion prevention with two–level user authentication in heterogeneous wireless sensor networks,* International Journal of Security and Networks, 7(2), 107 -121, 2012