

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900

Open access books available

186,000

International authors and editors

200M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Design Model and Deployment Fashion of Wireless Sensor Networks

Sana Akourmis, Youssef Fakhri and Moulay Driss Rahmani

Abstract

The ease deployment of Wireless sensor networks (WSNs) in the harsh and hard environment possesses a paved because the way it is. They are formed by sensor nodes which are responsible for examining environmental and corporal conditions to perform data processing. In this chapter, the manner of deployment will be presented, and how they communicate over a wireless link to unite the necessities of a specific application will be shown.

Keywords: WSN, system monitoring, connectivity, coverage, sensor node, routing protocol, path selection

1. Introduction

Wireless sensor networks considered as a special type of ad hoc network, where the fixed communication infrastructure and centralized administration are absent. Here, the nodes play both the role of hosts and routers [1, 2]. These Nodes can be deployed randomly or regularly in a WSN environment. There is a concession between these in terms of the number of nodes, deployment time, deployment cost, and feasibility of the placement scheme. They are smart and capable of accomplishing three complementary tasks: the reading of a physical quantity, the possible processing of this information, and the communication with other sensors [3]. Coverage guarantees the monitoring area is covered by at least one sensor node while connectivity is needed to make sure that every sensor node is precisely connected to the sink node or indirectly connected to the sink node by any other sensor nodes. In addition to their deployment fashion for an application, they form a wireless sensor network [4]. Its purpose is to monitor a geographic area, and sometimes to operate on it. Examples include a forest fire detector network, or abridging strength monitoring network after an earthquake [5, 6]. The network can include a large number of nodes (thousands). Though, their flexibility besides their ease deployment in unprotected environments, have allowed in improving people's living. Also, the capacity of the sensor on gathering information from surrounding is very helpful for a human being to make information accessible by the user [7]. In addition to their flexibility. Nowadays, they are also used in the construction of a smart home system. Moreover, Routing protocol

design factors: network efficiency and lifetime greatly depend on the quality of the protocols used. So, routing in WSN must proceed to the formation of new routes between the nodes in case the failure of communication links [8, 9]. It turns out that, efficiency in energy consumption represents a significant performance factor that limits node capacity. They are limited in memory of their major constraint but cheaper. They have limited available power because there are depleting their energy in sense as well as in communicating the signal to the base station because communication needs more power than data processing [4, 10]. Therefore, computing [4, 8, 11] resources and batteries are more limited in sensor nodes than in ad hoc nodes. Indeed, to develop this system architecture, it is necessary to start from the high-level requirements for the realization of the requested application, then to the low-level hardware requirements. In this chapter, the focus is on the communication strategy about the Design model and deployment fashion of the wireless node. It is organized as follows: Section2 gives an overview of the wireless sensor network design system, the different sensor network elements are shown in Section3, Section4 explains the deployment model of nodes, Section5 presents the vulnerabilities and challenges in WSN. We will show many areas of application of the WSN in which they are used. And finally, the conclusion is provided in Section 7.

2. Wireless sensor network design system

2.1 Characteristics of a sensor network

A wireless sensor network is a relatively large set of nodes called sensors. These sensors are very small devices scattered a little randomly in an area called “sensing region” (see **Figure 1**). The sensors are autonomous and have the role of collecting information (varied according to the field of application) [6, 12]. These will then be sent to an administrator via the gateway (well node) using appropriate routing techniques which we will see in another part. The well or sink node is the intermediate node between the administrator who is generally very far away and the whole network.

Indeed, when a sensor has to inform the administrator of an event or simply send the information collected, it must first pass this information to the sink. It is the latter that will transfer the said information to the administrator through an extensive network such as the Internet or more simply via the satellite [2, 4, 10].

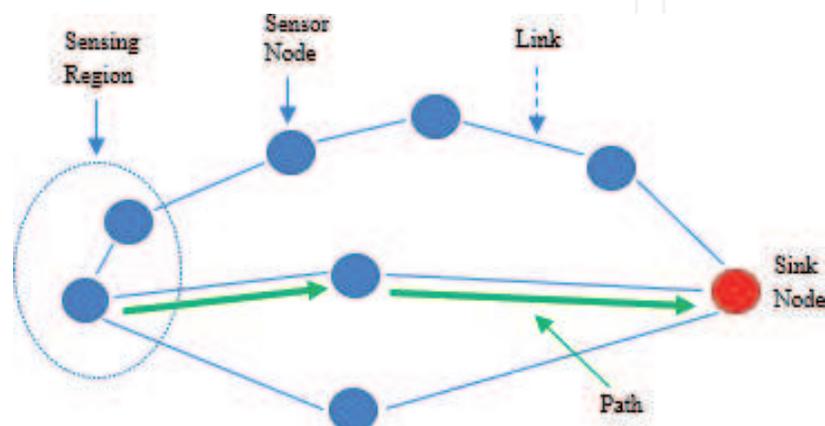


Figure 1.
WSN elements considered into the network.

Conversely, when it is now the administrator who wants to send information or requests to the various sensors of the 4th network or to one in particular, he too will have to go through the sink in order to reach his targets [13].

Thus, we have just seen that each sensor node will send its messages to the well node in order to inform the administrator [14]. However, it would be good to know that there are indeed two distinct types of communication architecture in a wireless sensor network. That are:

- The flat network

And

- The hierarchical network:

No particularity, the first hierarchical network is quite the simplest. All the sensor nodes have the same function and the same power except the well node which keeps its same function. It stipulates for the hierarchical network that the catchment area must be divided into several regions. Each region contains a number of normal sensor nodes added to these one or more nodes more powerful than the others. These sensors will act as a routing gateway between the different regions. This type of infrastructure makes it possible to offload the less powerful (and therefore less expensive) nodes of several network functions [13, 14].

So, we just saw the architecture of a wireless sensor network, defining the overall way of communication between the nodes and the administrator. But we still do not know how we go from an event to information sent to the user. In order to try to answer this, we can see below the hardware architecture of a deep sensor node.

The basic objectives of wireless sensor networks generally depend on the applications; however, the following tasks are common to several applications:

- Determine the values of some parameters according to a given situation. For example, in an environmental network, one can seek to know the temperature, the atmospheric pressure, the amount of sunlight, and the relative humidity in a number of sites, etc. [6].
- Detect the occurrence of events that we are interested in and it estimates the parameters of the events detected. In traffic control networks, one may want to detect the movement of vehicles through an intersection and estimate the speed and the direction of the vehicle [15].
- Classify the object detected, e. g in a traffic network is a vehicle a car, a bus, etc. [12, 15].

In general, WSN is formed by sensor nodes. It is responsible for examining environmental and corporal conditions to perform data processing. It is considered as a special type of ad hoc network where the fixed communication infrastructure and centralized administration are absent routers [16]. The sensor nodes form a network of sensors and the nodes play both; the role of hosts, and they are smart. Sensors are capable of accomplishing three complementary tasks: the reading of a physical quantity, the possible processing of this information, and the communication with other sensors. They are deployed to accomplish an application. Typically, they can be rapidly deployed and distributed over a geographical area in a multi-hop packet radio communication network without the help of an established infrastructure as it is shown in **Figure 2**.

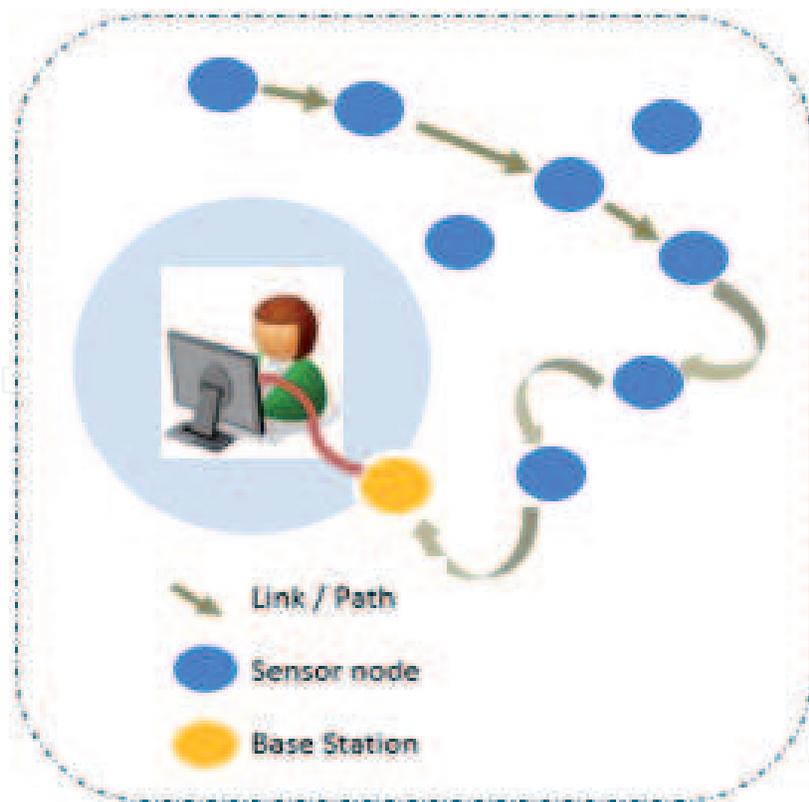


Figure 2.
WSN architecture [6, 17, 18].

Since wireless sensor nodes are usually very small electronic devices. It has been considered as a special type of ad hoc network. It brings an interesting perspective (**Figure 3**). This kind of network is capable of self-configuring and self-managing without the need for intervention human. One of the main design objectives of the WSNs is realizing communication data while trying to extend the lifetime of the network and prevent the degradation of connectivity by using energy management techniques. Low energy nodes are used to perform detection in the area of interest. However, wireless transmission is a significant simplification that can avoid a lot of wiring. Its main advantage is the capacity for self-managing and self-configuring without the need for human intervention. The nodes cooperate and communicate

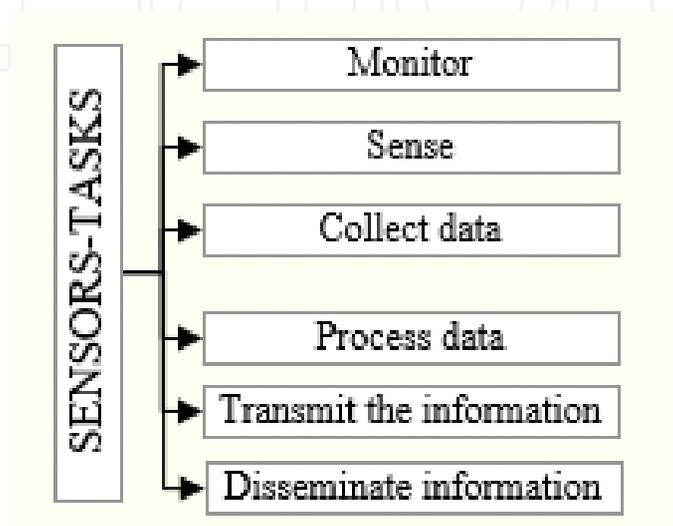


Figure 3.
Sensors-tasks [3-5, 7].

with each other to transmit the data to each other in the WSN network as seen in **Figure 1**. Hence, these two communicative nodes as shown in the same figure (**Figure 1**) are called a one-hop neighbor.

Thus, we have just seen that each sensor node will send its messages to the well-known Base station as expected in WSN architecture we must have one destination.

In order to inform the administrator or the end user. However, it would be good to know that there are indeed two distinct types of communication architecture in a wireless sensor network. There are two types in WSN (Flat and Hierarchical architecture) that we will see in the next section.

2.2 Path selection in WSN

These sensors nodes determine the route/path by routing packets using various routing protocols [2, 9]. Nodes of the WSN network maintain connectivity in a distributed way. This topology instability needs a routing protocol to be run in each node to create and maintain routes between nodes. One of the main design objectives of the WSNs is to realize communication data while trying to extend the lifetime of the network and prevent the degradation of connectivity by using energy management techniques [8, 18]. The Designing security protocols require understanding these limits (sensors in terms of energy, memory, computing capacity) and achieving acceptable performance with security measures to meet the needs of an application. The design of security protocols requires understanding these limits of WSNs and achieving acceptable performance with security measures to meet the needs of an application [12, 13, 15]. Preferentially, the node should be able to enter and leave the network even if the design, implementation, and configuration are correct, resource depletion is possible. This is why WSNs are classified into infrastructure-less networks. Moreover, their ease deployment in the harsh and hard environment possesses a paved to the way for it. Their capacity on gathering information from surrounding is very helpful to improve the quality of living, as it makes life easy because of modern technology in our daily life [4, 10, 11]. The manner of deployment of WSN will be presented in this chapter, and how they are communicated over a wireless link to unite the necessities of a specific application that will be shown. There are a lot of factors that are included the organization of wireless sensor networks that are: network organization, number of nodes, number of routers, network topology, and geographical distribution [8, 18]. They have been recently attracted a lot of interest in the research community due to their wide range of applications. In this way, we can choose any kind of sensors to be used for a specific purpose such logistics, smart agriculture, industrial controls, smart home, military target tracking, and security monitoring. This chapter will describe the design, deployment, and applications in WSN [18, 19].

2.3 Difference between sensor and ad hoc network

Nowadays, Wireless technologies have been developed rapidly, and Wireless sensor networks (WSNs) are one of them [2, 4]. A deployment of several devices equipped with sensors and it has been considered as a special type of ad hoc network that brings an interesting perspective. It can be rapidly deployed by a set of wireless computers in a multi-hop packet radio communication network without the help of established infrastructure [14, 16]. Or, it can only be equipped with limited power and wireless sensor nodes can perform a collaborative measurement process. In this network, the use of wireless transmission in the open-air medium remains the most important thing to make information accessible for the user. In brief, Wireless ad-hoc networks can be used in special areas where wired network

infrastructure may be unsuitable. (Or a wired network infrastructure may not be suitable for reasons such as cost or convenience [3].

In ad hoc mobile networks (MANETS) the nodes usually cooperate and transmit packets to each other to allow communication out of range (out of range). The nodes in WSNs rely on other nodes to transfer their packets [5]. The difference between both Wireless sensor network and Ad hoc network in the following:

- The density of deployed nodes is much higher in sensor networks
- The sensor nodes have limited capacity in energy and memory
- The topology in sensor networks is often dynamic.
- Communication between the nodes is by diffusion and not point to point in a network of sensors.
- Sensors may not have a global identifier due to a large number of nodes.

3. The different sensor network elements

Recent findings on empirical studies have deduced that radio links between low-power sensing devices are far from being reliable. This why making a model that is akin to the reality of radio communication channels is something out of reach or at least very challenging [2, 8]. Computing nodes (usually wireless) in an ad hoc network act as routers to deliver messages between nodes that are not within their wireless communication range [1, 7]. Because of this unique capability, mobile ad hoc networks are envisioned in many critical applications (e.g., in battlefields). Therefore, these critical ad hoc networks should be sufficiently protected to achieve confidentiality, integrity, and availability. Wireless sensors are typically low-power, low-cost, and short-range minuscule devices. Multi routes rely on data from the monitored region to the sink. The measuring nodes are a wireless device, they usually cooperate and transmit packets to each other to allow communication out of range, they rely on other nodes to transfer their packets. Preferentially, the node should be able to enter and leave the network [12, 13]. The self-organizing capability makes them flexible for communication in areas [6].

But in fact, resource depletion is possible even if the design, implementation, and configuration are correct [15]. Or, it can only be equipped with limited power. In WSN. The nodes usually cooperate and transmit packets to each other to allow communication out of range [18]. That's why Multi-hop routes are needed to transfer data from node to another in the network. The tasks that the sensors can perform are shown in **Figure 1**. Every single node in the network must be able to perform these different tasks. Every single node should be made to give a set of basic primitives to combine the interconnected web that will appear as they are scattered. Since sensor nodes are: -small distributed, they may be on a large scale or in a dangerous area [8, 19]. Their battery is small and it maybe not recharged or replaced. So, the network lifetime is prolonged when the battery energy is used wisely. Individual nodes interact with the environment in which they are scattered to perform the functions dictated by the sensor network applications [1, 4, 11]. They focus on interaction with the environment instead of focusing on interaction with humans [10]. So, it can be said that in the hardware architecture of the wireless sensor network has four basic subsystems of sensor nodes:

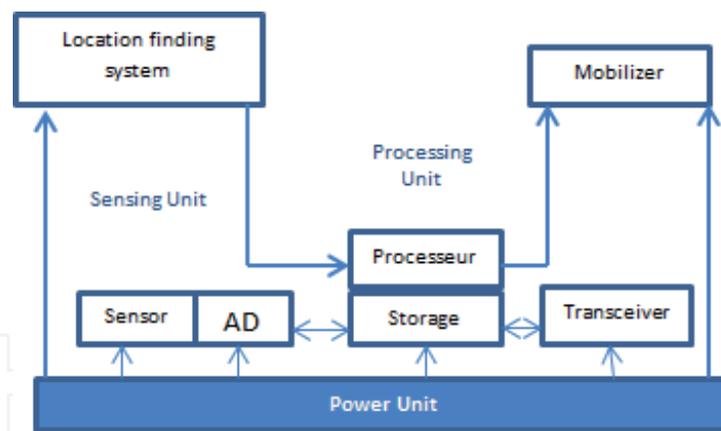


Figure 4.
 Sensing node design [5, 6, 14, 17].

- Computing subsystem
- Power subsystem
- Sensing subsystem
- Communication subsystem

Concerning software architecture, a wireless sensor is a device consisting of a data acquisition unit using a sensor of a physical quantity + (processing) + transmission by wireless technology. A wireless sensor network is a set of sensors grouped within the same wireless network [12, 14]. They are considered as a special type of ad-hoc network composed of “nodes.” These nodes form a catchment field and routing that is using routing protocols which are in star or hybrid form, to an end-user which is the sink it is finally a user request. They have limited available power because there are depleting their energy in sense as well as in communicating the signal to the base station Therefore, computing resources and batteries are more limited in sensor nodes than in ad hoc nodes. A standard sensor type-TelosB has a 16-bit, 8 MHz RISC CPU with 10 K RAM, 1024 K flash storage and 48 K program memory [13–15]. The general overall software architecture of the sensor net is shown in **Figure 4**.

4. Architecture of a sensor node

Advances in miniaturization have enabled sensors to integrate several modules despite their relatively small size. They mainly consist four (4) units [14, 17, 18]:

- A collection unit
- A processing unit
- A transmission unit
- An energy management unit

In addition to these, we can find depending on the field of application of the sensor network, a unit for localization, the unit for movement, and sometimes the unit for producing energy thanks to small solar panels. The diagram in **Figure 4**

shows all of these different modules. In our case, let us dwell on each of these modules in more detail [5, 6, 9, 14].

- **Captive Unit:** it is the module for which wireless sensors have been developed. It breaks down itself into two subunits. The “sensor” or receiver will recognize the event to be monitored by the sensor. Then, it will perceive the analog signals emitted by the receiver to transform them into a digital signal understandable by the processing unit.
- **The Processing Unit:** Consisting of a processor, and sometimes even a small storage memory operates using an operating system specially designed for this type of medium (for example: open source TinyOS). This unit executes communication protocols by allowing the node to collaborate with the rest of the network. Under certain conditions, the processing unit can analyze the observed data in order to reduce the task at the well node.
- **The Transceiver Unit:** it takes care of the operations on the transmission and reception of data. This emission is either optical or the radio-frequency type.
- **The Power Unit:** being the major constraint of this technology, it was necessary to insert a module within the sensors allowing sparse management of the energy in the sensor. Therefore, it will be responsible for distributing the energy available in the sensor optimally; for example, by putting inactive components on standby. It will also be responsible for managing the energy recharging system, but it provided that a module for this purpose.
- **Location Finding System:** it provides the location information required by certain routing protocols. Usually, it is a Global Positioning System (GPS).
- **Mobilizer:** in the case, certain larger sensors are possible to move them. This system what will have the task assigned to it. The different components of the sensor node described above define its possibilities. In other words, they let you know what a sensor is capable of doing and how far it can do it. It brings us to our next point.

5. Deployment model of nodes

Wireless transmission is an important factor that allowed WSN to deploy successfully. It has been increased in recent years and has been appeared even in smart house systems [1, 2]. Many communication technologies, such as IrDA, Bluetooth, and Zigbee, GSM/GPRS (General Packet Radio Service), PSTN (Public Switched Telephone Network), etc. have been developed for different locations [16, 18]. A kind of real-time system in which multiple sensors connected simultaneously to one gateway unit it become indispensable, and they are transformed into wireless sensor networks (WSNs) [10]. A mobile sensor sends data to the nearest sensor which is transferred later to the BS via the shortest path as it is shown in **Figure 2**. Indeed, when a sensor has to inform the administrator of an event or simply send the information collected, it must first pass this information to the sink (see. **Figure 2**). It is the one that will transfer the understood information to the administrator through an extensive network such as the Internet or more simply via the satellite. Conversely, when the administrator wants to send information or requests to the

various sensors of the network or one, in particular, the two will have to go through the sink to reach its targets [4, 11].

It turns out that the use of these technologies makes information more accessible by the user. This would significantly improve people's living quality. Especially that wired network has some problems, such as inconvenience and high cost, unsatisfactory security assurance [2]. Therefore, their concept in sensing with their capabilities in transferring the data into a signal has paved the way for the creation of a lot of potential applications that we will see later in this chapter.

The routing algorithm is used to accomplish this task to support multi-hop communication inside the network by the nodes [9]. So, we will understand how to communicate this data and how to monitor the information shared between nodes. These data are typically relayed from node to another and these links are dynamically built on -demand (reactive routing) or dynamically re-computed (proactive-routing) [3, 12]. Proactive routing protocol: they are presented on the same routing principle as wired networks. The routes in this type of routing are calculated in advance - each node encountered updates several routing tables by exchanging packets between neighbors. Also, they luckily tend to have a communication brink between them for reason that path computation is generated upon request or the occurrence of specific events from the application data to the sink node. Preferentially, the node should be able to enter and leave the network [1].

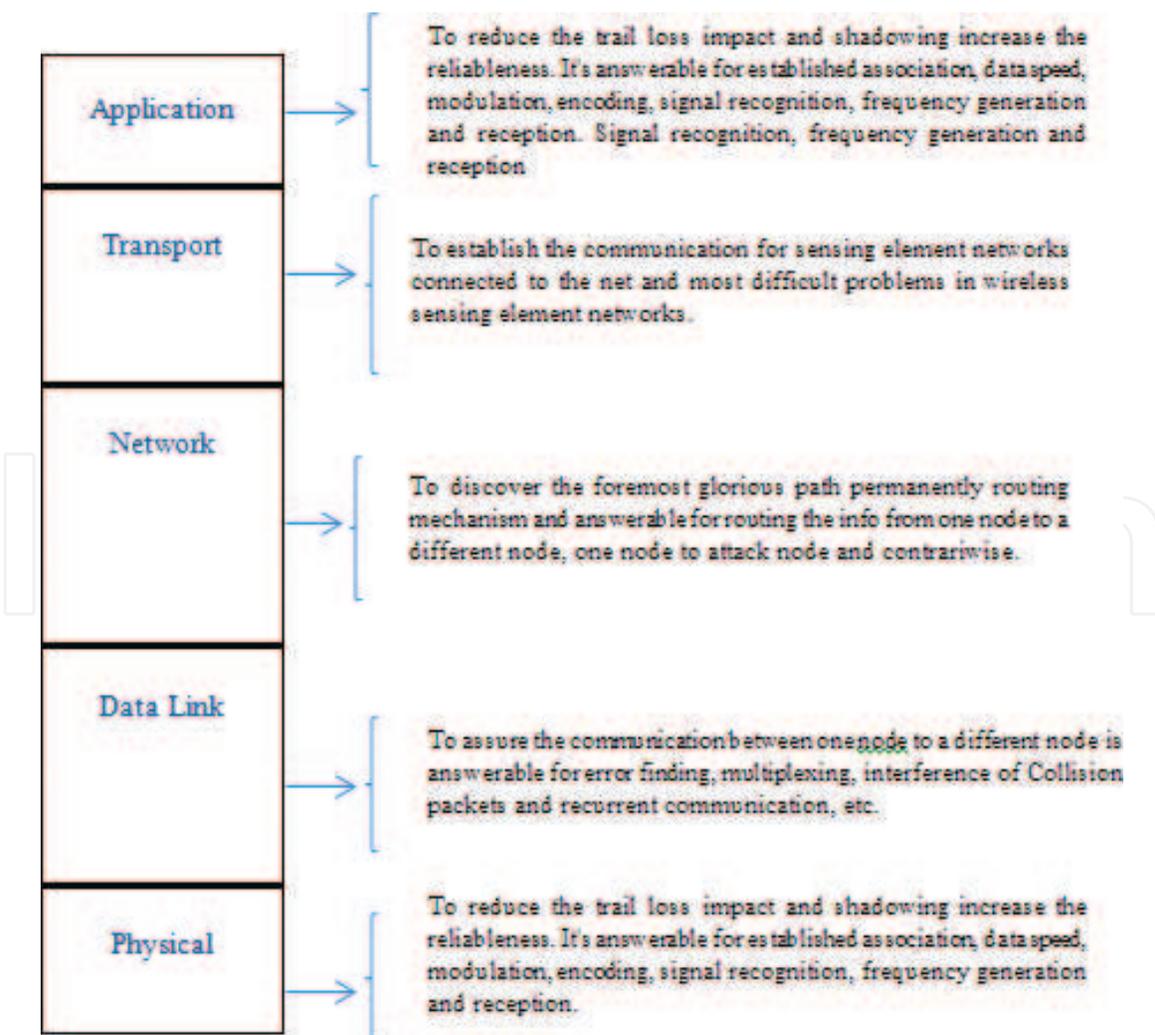


Figure 5.
OSI MODEL and their signifiation [4, 8, 10, 18].

We can use any kind of protocol to communicate the information, and careful protocol design is needed as well as a successful target application [4, 8, 10]. So, the routes are determined before they are used. Since host nodes are mobile. So, it causes frequent and unpredictable topological changes in the network [17]. Dealing with the formation and maintenance of WSN Network is very difficult. In recent years, a lot of routing protocols have been proposed for WSNs, out of two major protocols AODV which is a reactive routing protocol because its uses and efficiency in energy consumption represents a significant performance factor that limits node capacity [8, 11].

Also, each layer of the model communicates with an adjacent layer (that of the top or that of the lower part). Each layer uses the services of the sub-bases and provides some to that of higher level.

As it was mentioned above each layer has its own significant. And to give more detail (see **Figure 5**).

6. Vulnerabilities and challenges in WSN

Wireless sensor network is an interconnection among hundreds, thousands, or millions of sensor nodes. It is capable of sensing, data processing, and communication tasks. During this process, Maintenance and route computation are needed to involve a minimum number of nodes [20].

So, their flexibility is provided by each node which acts as a router to forward each other's packets to enable out of range communication and to forward each other the data packets which is multi-hop; because Their less capable hardware and limited capability such as node limitation, network limitations, physical limitations, the inherent vulnerabilities of wireless communication like physical vulnerability and other related to wireless technology, also, the dense deployment nature in public and hostile environments in many applications, the restricted field of sensing and sensitive nature of collected data, unattended operation [4, 11].

This minimal configuration and lack of infrastructure, also the quick deployment makes WSNs convenient for emergency operations especially for military operations [2, 5]. In WSN, multi-hop routing, higher latency in packet transmission may achieve difficult synchronization which is due to network congestion and processing intermediate nodes.

Being limited by computation resources, WSN process the following limitations as it is shown in **Figure 6** because the position of the sensor nodes in a wireless sensor network (WSN) is of paramount importance for their design and for their implementation that will intersect with their architecture and design requirements in parallel with their specifications techniques like energy consumption, connectivity and coverage. Let us started with the first metric which is the coverage.

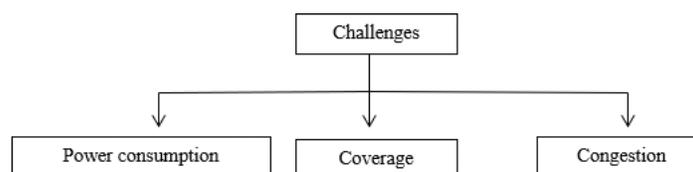


Figure 6.
WSN challenges [1, 3, 7, 8, 18, 19].

6.1 Coverage

Coverage ensures the monitoring area by at least one sensor node while connectivity is required to make sure that every sensor node is directly connected to the sink node or indirectly connected to this last via any other sensor nodes [1, 11, 19]. Two sensor nodes that are outside the communicate directly [11, 19]. Consequently, connectivity cannot be guaranteed. Most applications in WSNs involve battery-powered nodes with limited energy where their batteries may not be convenient for recharging or replacing [7]. Thus, it is very crucial to find a way to reduce the energy consumption because it is inconvenient to keep on changing the battery specially if WSN is installed in remote area. The desired coverage can be assured as the locations of sensor nodes are carefully planned according to certain requirements. A wireless sensor network (WSN) has to maintain a desirable sensing coverage and periodically report sensed data to the administrative center (i.e., base station), and the reporting period may range from months to years.

Coverage and lifetime are two paramount problems in a WSN due to constraint of associated battery power [5]. All the existing theoretical analyses on the coverage and lifetime are primarily focused on the random uniform distribution of sensors or some specific network scenarios (e.g., a controllable WSN) [11, 18].

6.2 Connectivity

Coverage and connectivity can be optimized by deploying a large number of sensor nodes. Unfortunately, the connectivity cannot remain unchanging at any working time. The sensor network is a broadcast network in which any signal can be captured by adversaries at any time. These features make wireless ad-hoc sensor networks more vulnerable than wired networks. This presents real challenges in the implementation of the following security requirements for WSNs [4, 11, 19].

6.3 Energy consumption

This factor is of paramount importance during the design and implementation of WSN network which ensure the network lifetime in its operating system.

Another concern in WSN, is about energy efficiency. In WSN, each sensor node may need to support multiple communication models including unicast, multicast, and broadcast. Therefore, due to the limited battery lifetime, security mechanisms for sensor networks must be energy efficient [1, 10]. Especially, the number of message transmissions and the amount of expensive computation should be a few as possible [17, 19].

Since the transmission distance also affects the energy consumption, it is another factor to be considered [8]. Due to these factors, a sensor node placement algorithm for WSN is needed to ensure that the position of deployed sensor nodes is able to provide maximum coverage, minimum energy without jeopardizing connectivity although the communication methods and protocols of the sensor node may affect the coverage, connectivity and energy consumption, they are only considered after the sensor node positions have been determined [4, 19]. Romoozi [16] stated that these is a tradeoff between energy consumption and network coverage. Bigger coverage is achieved if the distance between two sensor nodes is further [16]. However, their energy consumption will be higher due to longer distance data transmission. The tradeoff between system lifetime and system reliability is a paramount design consideration for wireless sensor networks [2, 4, 11].

Constraint	Description
Energy constraints	Smaller memory capacity Limited battery life
Memory limitations	Limited memory capacity Processing power Low computational power Low bandwidth
Unreliable communication	Open air medium Wireless transmission
Higher latency in communication	Limited radio spectrum Affects multiple access, interference
Node limitations	Frequent path beak
Physical limitations	Lack of tamper resistant packaging No centralized infrastructure Design constraint
Heterogeneous nature of sensor nodes	Limited battery power Inherent limitations in sensor networks

Table 1.
Nodes' constraints in WSN [1, 3, 7, 8, 12, 19].

Due to distributed nature of these networks and their deployment in remote areas, the node constraints have been summarized in **Table 1**.

They are fully distributed, and adaptive regarding frequent changes [2]. Their deployment in ubiquitous and pervasive applications, inherently; a wireless sensor network is an interconnection among hundreds, thousands or millions of sensor nodes. Sensor node is capable of sensing, data processing and communication tasks. During this process, Maintenance and route computation are needed to involve minimum number of nodes [4].

7. Areas of application of the WSN

The basic objectives of wireless sensor networks generally depend on the applications; however, the following tasks are common to several applications.

They have a large catalog of applications where they can be found. We have already mentioned a few that shows just a range of possibilities. Among them, we can try to name few [5–7, 11, 13, 15, 20] in where they can determine the values of some parameters according to a given situation. For example, in an environmental network, one can seek to know the temperature, the atmospheric pressure, the amount of sunlight, and the relative humidity in a number of sites, etc. [12, 17].

Detect the occurrence of events that we are interested in and it estimates the parameters of the events detected. In traffic control networks, one may want to detect the movement of vehicles through an intersection and estimate the speed and the direction of the vehicle [5, 12]. Classify the object detected, e. g in a traffic network is a vehicle a car, a bus, etc. [6]. So, they are fully distributed and adaptive regarding frequent changes. Their deployment in ubiquitous and pervasive applications,

The ease of deployment of wireless sensor networks (WSN) in a harsh and hostile environment has paved the way for the use of several applications.

Wireless Sensor Networks (WSNs) have recently attracted a lot of interest in the research community due to their wide range of applications and have a vast area of application for real-time event detection. Their simplification in wiring and harness

helps in improving people's living quality. They are implicated in smart homes in these last years. Some applications already exist using WSN especially in the following fields [6, 12, 14, 16–18]:

Mission-critical applications in wireless sensor networks (WSN) such as fire alarms, radiation leaks, and monitoring in hostile environments should have a fast, reliable, and tolerant response to protocol failures routing. Otherwise, these applications will not be able to function properly and it will bring unexpected material, financial or human losses [2, 9, 11].

Using the miniaturization of micro-sensors, the increasingly low cost, the wide range of types of sensors available (thermal, optical, vibration, etc.) as well as the wireless communication medium allow the application of sensors in several fields including:

In the Military sector as in many other technologies, the military sector was the initial engine for the development of sensor networks. The rapid deployment, the reduced cost, the self-organization, and the fault tolerance of sensor networks are characteristics that make this type of network an appreciable tool in such a field. Currently, WSNs can be an integral part of a command, control, communication, surveillance, reconnaissance, etc. [2, 16].

The Medical field, Sensor networks are widely used in the medical field. This class includes applications such as: providing a help interface for the disabled, collecting better human physiological information, as well as, facilitating the diagnosis of certain diseases, continuously monitoring the sick and doctors inside the hospital. Also, they can be used to ensure permanent monitoring of the vital organs of human beings thanks to micro-sensors which can be swallowed or implanted on the patient (blood sugar monitoring, cancer detection, ...). They can also facilitate the diagnosis of some diseases by carrying out physiological measurements such as: blood pressure, heartbeat, temperature. Each sensor must have a very specific task for using it. It is mainly a remote monitoring of a patient [12, 16].

The Architectural domain Transformation of buildings into intelligent environments is capable of recognizing people, interpreting their actions, and reacting to them [12, 14].

The commercial domain is among domains where sensor networks have proven their usefulness. Several applications can be listed in this sector, such as: monitoring the condition of the equipment, controlling and automating the machining processes, etc. [7, 13, 14].

The environmental field is fairly varied field. The sensors are used to detect the pollution level of factories as well as to monitor the activity of a volcano. For example, we can mention the real-time detection of forest fires and faster industrial risks and reduce the leakage of toxic products (gas, chemicals, radioactive elements, petroleum, etc.). to detect natural disasters (forest fires, earthquakes, etc.). It detects fumes of toxic products (gases, chemicals, petroleum, etc.) in industrial sites such as nuclear or oil plants [12, 15, 17].

The security domain is the most important and sensitive area or sector in which the sensors can be in buildings in order to detect alterations in their structure or else be used to detect intrusions by building a distributed alarm system, monitoring railways, to prevent accidents, or the detection of water leaks in dams to avoid possible damage [2, 9, 12].

8. Conclusion

Wireless sensor networks have the potential for many applications (military, security, environment, medicine, commerce, etc.). The choice and model of a WSN

depends greatly on the need for the application as well as the type of sensors used. In this chapter, we had the opportunity to discover what is a WSN, and the elements that go with it to lead an application to a specific domain. The advance of technology allowed the creation of prototype WSNs, but the hardware and software both have a way to go before WSNs are cost-effective, practical, and useful. To sum up, it emerged from this first chapter that thanks to their small size, their relatively low cost and their various functional characteristics, sensor networks offer us a truly immense range of possibilities. They can be used both on a civil level and in specialized fields. Unfortunately, the various constraints mentioned still hamper in their use. Indeed, the amount of energy is a big brake on this technology which continues fortunately to develop. On the other hand, another concern in this technology is the assurance of the conduct of information. So, the assurance as a captured phenomenon has been transmitted to the administrator. In this regard, the requirement for the security of its wireless sensor networks is one of the main obstacles. Securing a network of sensors amounts set up the various security services in this network, while taking into account its different characteristics. More precisely, it is to secure the routing protocols of the network layer; and it will be the main point of another next chapter.

Author details

Sana Akourmis^{1*}, Youssef Fakhri^{1,2} and Moulay Driss Rahmani¹

1 LRIT, Research Unit Associated with the CNRST (URAC29), Faculty of Sciences, University Mohammed V-Agdal, Rabat, Morocco

2 LaRIT Laboratory, Faculty of Sciences, University Ibn Tofail, Kenitra, Morocco

*Address all correspondence to: sakourmis@gmail.com

IntechOpen

© 2020 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Ghosh, A., & Das, S. K. (2008). Coverage and connectivity issues in wireless sensor networks: A survey. *Pervasive and Mobile Computing*, 4(3), 303-334.
- [2] Zia, T., & Zomaya, A. (2006, October). Security issues in wireless sensor networks. In *2006 International Conference on Systems and Networks Communications (ICSNC'06)* (pp. 40-40). IEEE.
- [3] BenSaleh, Mohammed Sulaiman, et al. "Wireless Sensor Network Design Methodologies: A Survey." *Journal of Sensors* 2020 (2020).
- [4] Akourmis, S., Fakhri, Y., & Rahmani, M. D. (2017, December). Reducing Blackhole Effect in WSN. In *International Conference on Innovations in Bio-Inspired Computing and Applications* (pp. 13-24). Springer, Cham.
- [5] Matin, M. A., & Islam, M. M. (2012). Overview of wireless sensor network. *Wireless Sensor Networks-Technology and Protocols*, 1-3.
- [6] Amirach, N. (2015). Détection d'évènements simples à partir de mesures sur courant alternatif (Doctoral dissertation).
- [7] Lamine, M. M. (2008). Sécurité dans les Réseaux de Capteurs Sans-Fil. *Memoire de Magistère en Informatique Ecole Doctorale d'Informatique de bejaia*.
- [8] Anisi, M. H., Abdul-Salaam, G., Idris, M. Y. I., Wahab, A. W. A., & Ahmedy, I. (2017). Energy harvesting and battery power based routing in wireless sensor networks. *Wireless Networks*, 23(1), 249-266.
- [9] Khattab, H., & Al-Sharaeh, S. (2018). Performance Comparison of LEACH and LEACH-C Protocols in Wireless Sensor Networks. *Journal of ICT Research and Applications*, 12(3), 219-236
- [10] Sana, A., Youssef, F., & Driss, R. M. (2018, April). Flooding Attack on AODV in WSN. In *2018 Renewable Energies, Power Systems & Green Inclusive Economy (REPS-GIE)* (pp. 1-5). IEEE.
- [11] Wang, D., Xie, B., & Agrawal, D. P. (2008). Coverage and lifetime optimization of wireless sensor networks with gaussian distribution. *IEEE Transactions on Mobile Computing*, 7(12), 1444-1458.
- [12] Bourenane, W. (2013). Étude et conception d'un système de télésurveillance et de détection de situations critiques par suivi actimétrique des personnes à risques en milieu indoor et outdoor (Doctoral dissertation).
- [13] Benazzouz, M. (2013). Surveillance de tout point d'une zone d'intérêt à l'aide d'un réseau de capteur multimédia sans fil. *Rapport de recherche. Ecole nationale supérieure d'informatique, Oued-Smar, Alger, Algérie*.
- [14] Chafik, A. (2014). Architecture de réseau de capteurs pour la surveillance de grands systèmes physiques à mobilité cyclique (Doctoral dissertation).
- [15] Roux, J. (2020). Détection d'intrusion dans des environnements connectés sans-fil par l'analyse des activités radio (Doctoral dissertation, Université Toulouse 3 Paul Sabatier (UT3 Paul Sabatier)).
- [16] Puccinelli, D., & Haenggi, M. (2005). Wireless sensor networks: applications and challenges of ubiquitous sensing. *IEEE Circuits and systems magazine*, 5(3), 19-31.

[17] Romoozi, M., & Ebrahimpour-Komleh, H. (2012). A positioning method in wireless sensor networks using genetic algorithms. *Physics Procedia*, 33, 1042-1049.

[18] Wang, X., Dai, H., Wang, Z., & Sun, Y. (2006). A mathematical model for energy-efficient coverage and detection in wireless sensor networks. In *Intelligent Control and Automation* (pp. 130-137). Springer, Berlin, Heidelberg.

[19] Singh, V. P., Ukey, A. S. A., & Jain, S. (2013). Signal strength based hello flood attack detection and prevention in wireless sensor networks. *International Journal of Computer Applications*, 62(15).

[20] Raghavendra, C. S., Sivalingam, K. M., & Znati, T. (Eds.). (2006). *Wireless sensor networks*. Springer.

IntechOpen