http://dx.doi.org/10.18623/rvd.v22.n3.3445

DEPLOYMENT OF NODES IN WSNs

IMPLANTAÇÃO DE NÓS EM WSNs

Article received on: 6/30/2025
Article accepted on: 9/29/2025

Sana AKOURMIS*
*LRIT, Research Unit Associated with the CNRST (URAC29), Faculty of Sciences - University Mohammed V-Agdal,
Rabat, Morocco
Orcid: https://orcid.org/0000-0001-7940-534X
sakourmis@gmail.com

Youssef Fakhri*
*LaRIT LAboratory - Faculty of Sciences, University Ibn Tofail
Kenitra, Morocco
Orcid: https://orcid.org/0000-0002-5647-303X
fakhri@uit.ac.ma

The authors declare that there is no conflict of interest

Abstract
The Internet of Things (IoT) facilitates widespread automation, simplifying human life by deploying sensors in interconnected environments. Recent developments in Micro Electro Mechanical Systems (MEMS) with technical advancements in terms of performance and miniaturization, wireless communications, and digital electronics have made it possible to produce small, inexpensive, and "smart" devices, including smartphones, PDAs, RFID systems, Wireless Sensor Networks (WSNs), and many other technologies to offer economically viable solutions for remote monitoring and data processing in complex and distributed environments. Strategy of communication and architecture of node, the model within the operation of the system monitoring assisted by sensor nodes in WSNs, their basic concepts, and manner of communication, also the way in which data is transmitted over a wireless link will be presented in this chapter to unite the necessities of a specific application.

Keywords: WSN Technology. System Monitoring. Sensor Node. Advanced Sensing Functionalities. Routing Protocol. Path Selection.

Resumo
A Internet das Coisas (IoT) facilita a automação generalizada, simplificando a vida humana por meio da implantação de sensores em ambientes interconectados. Desenvolvimentos recentes em Sistemas Microeletromecânicos (MEMS), com avanços técnicos em termos de desempenho e miniaturização, comunicações sem fio e eletrônica digital, tornaram possível a produção de dispositivos pequenos, baratos e "inteligentes", incluindo smartphones, PDAs, sistemas RFID, Redes de Sensores Sem Fio (RSSFs) e muitas outras tecnologias, oferecendo soluções economicamente viáveis para monitoramento remoto e processamento de dados em ambientes complexos e distribuídos. A estratégia de comunicação e a arquitetura do nó, o modelo de operação do sistema de monitoramento assistido por nós sensores em RSSFs, seus conceitos básicos e a forma de comunicação, bem como a maneira como os dados são transmitidos por um link sem fio, serão apresentados neste capítulo para atender às necessidades de uma aplicação específica.

Palavras-chave: *Tecnologia WSN. Monitoramento de Sistema. Nó Sensor. Funcionalidades Avançadas de Detecção. Protocolo de Roteamento. Seleção de Caminho.*

1 INTRODUCTION

The rise of wireless technologies today offers new perspectives in the field of telecommunications. Compared to the wired environment, the wireless environment allows users flexibility in access and ease of handling information through mobile computing units (laptops, PDAs, sensors, etc.). The phrase "wireless" makes the first differentiating factor clear. In fact, motes no longer use wires to communicate; instead, they use wireless communication modules. Recent technological advances reinforce the presence of computing and electronics at the heart of the real world. More and more objects are thus equipped with processors and mobile communication means, allowing them to process information and also transmit it. Wireless sensor networks fall into this category. Indeed, they consist of a set of small devices, or sensors, with particularly limited resources, which nevertheless enable them to acquire data about their immediate environment, process it, and communicate it.

They are considered a special type of ad hoc network, consisting of many physically small sensors, typically placed in inaccessible or hostile environments. Integrated sensors transform physical quantities collected by a sensing unit into digital quantities, with a computing processing unit, data storage, and a wireless transmission module.

It is with its various advantages that this technology has established itself as an essential element in network architectures. The radio medium offers unique properties, for example, the ease and reduced cost of deployment, as well as the ubiquity of information. What forms a wireless sensor network is the establishment of several sensor nodes autonomously, aiming to collect and transmit environmental data to a collection point, called a sink node.

These sensors can collect, process, and rout environmental data from the monitored region autonomously to collection stations called sink nodes or base stations (see Figure1). They share several common properties with ad hoc networks, such as the absence of infrastructure and wireless communication. However, one key difference between the two architectures is the application domain.

With the rapid advancement of wireless communication and sensor technologies, the use of Wireless Sensor Networks (WSNs) has gained traction in various sectors such as aviation, industry, and environmental monitoring, overcoming the constraints of

traditional data collection methods in challenging environments. They are characterized by their deployments in hostile environments, their infrastructure-less architectures, as well as the constraints imposed by the sensor nodes that constitute them, such as their limitations in terms of energy and storage capacity. In the realm of wireless sensor network research, a key concern revolves around minimizing the energy consumption of sensor nodes. These networks are susceptible to a number of attacks due to the deployment space's openness and hostility as well as its resource limitations.

This chapter focuses on the monitoring of sensor nodes in WSNs, the communication strategy, the network model, and the distribution manner of wireless nodes. It is organized as follows: Section 2 gives an overview of the modeling process in WSNs; the communication strategy in WSNs is shown in Section 3; Section 4 explains the components of nodes in WSNs; Section 5 presents the sources of vulnerabilities in WSNs; and lastly, the conclusion is provided in Section 6.

2 MODELING PROCESS in WSNs

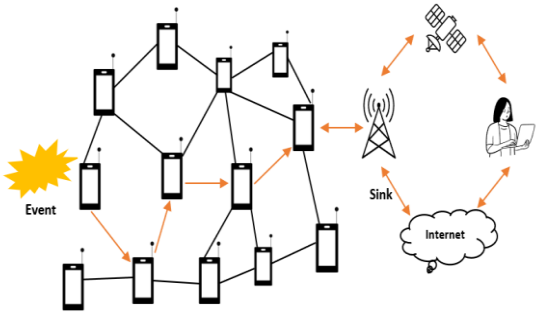
A wireless network is created by grouping individual devices or entities called sensor nodes in accordance with a certain routing algorithm. It is an essential part of a WSN, or wireless sensor network. They possess characteristics such as multihop communication, self-organization, self-healing, and distributed architecture. These sensors detect the surroundings and activate the control system without requiring human intervention. The wireless sensor network's sensor nodes broadcast data to the sink via the routing algorithm and use a coverage algorithm to detect it. For this reason, routing protocols are systems that allow routers to communicate routing data in order to make routing decisions. Sensor networks use many of these sensors to form an infrastructure-less network. A sensor analyzes its environment and propagates the collected data to the sensors within its coverage area. The data captured by the nodes is routed through a multi-hop routing to a node considered as a "collection point" called a sink node as shown in Figure 1. This sink node can be connected to the network user via the Internet, a satellite, or another system. The user can send requests to other nodes in the network, specifying the type of data required to collect the environmental data captured through the sink node.

With each sensor relaying information over its coverage area, the network is fully covered (see Figure1). A key concern in their operation is the efficient management of

energy consumption, which has spurred significant efforts towards developing power-saving techniques. Reducing energy consumption is crucial for extending the lifetime of sensor nodes in Wireless Sensor Networks (WSNs). This can be accomplished in a number of ways, such as routing protocols, energy harvesting techniques, and efficient data aggregation. Both academia and industry have shown a growing interest in wireless sensor networks, leading to a notable rise in their real-world deployments in recent years. However, their inherent vulnerabilities to external intrusion have emphasized the critical importance of ensuring security within WSNs. With their ad hoc network nature, sensor nodes are exposed to various security threats, necessitating the development of new security techniques to safeguard the transmitted information.

Figure 1

Diagram of a Wireless Sensor Network.



Source: Adapted from I.F. Akyildiz et al. / Computer Networks 38 (2002).

Why, the basis for creating wireless sensor networks is the types of sensors which is supplemented by base stations, or sink and data collectors, among other things as shown in the figure above. A different kind of network node called a data collector connects numerous motes together and serves as a gateway to external networks like the Internet, observed data will therefore move across the network from one sensor to another until it, for example, reaches the base station. In exchange, a base station might ask a particular sensor to carry out a particular task. These networks are utilized in a variety of industries where collecting environmental data is necessary.

A vast number of tiny devices, referred to as "sensor nodes," are used in wireless sensor networks to construct a network in the absence of an existing infrastructure. Each node in these networks is capable of detecting its surroundings, processing data locally, and transmitting it wirelessly to one or more collection sites. Sensor networks are densely

populated, heterogeneous environments with thousands of nodes spread across a very small area (about 3 meters). Furthermore, every node in the network has a limited energy reserve (such as a battery) that may not be able to be replaced.

Sensor nodes can join or leave the network at any time due to the limited transmission range. In such a network, communication and connectivity are achieved by nodes forwarding packets to one another, which requires support from routing protocols like AODV (Ad-hoc On-Demand Distance Vector) and DSR (Dynamic Source Routing). This connectivity is maintained in a distributed manner. The coverage algorithm must consider constraints like connectivity to ensure that the data sensed can be successfully transmitted to the base station.

Long-range transmissions are rarely necessary with multihop networking because signal route loss grows exponentially with distance. Every node in a sensor network has the ability to repeat, which lowers the required link range and, as a result, the transmission power.

3 COMMUNICATION STRATEGY IN WSNs

Sensors are extremely small devices with very limited resources, autonomous, capable of processing information and transmitting it, via radio waves, to another entity (sensors, processing unit, etc.) over a distance limited to a few meters.

It is a device that transforms the state of an observed physical quantity into a usable quantity, for example, an electrical voltage, a mercury height. Sensors are components of a few cubic millimeters in volume. This product is the result of extensive research and also thanks to the progress made recently in the fields of microelectronics, micromechanics, and wireless communication technologies.

Low-power sensor devices often face unstable radio connectivity, making it difficult to model real-world radio communication channels accurately. In mobile ad hoc networks, wireless nodes act as routers, enabling communication between nodes outside direct range. These networks are ideal for critical applications, such as military use, and need strong security to ensure availability, confidentiality, and integrity. Wireless sensors, which are low-cost and short-range, use multiple paths to transmit data to a central sink (see Figure 2). They rely on other nodes to relay packets, enabling communication beyond their range. The nodes can join or leave the network as needed, enhancing flexibility and

adaptability to different communication conditions.

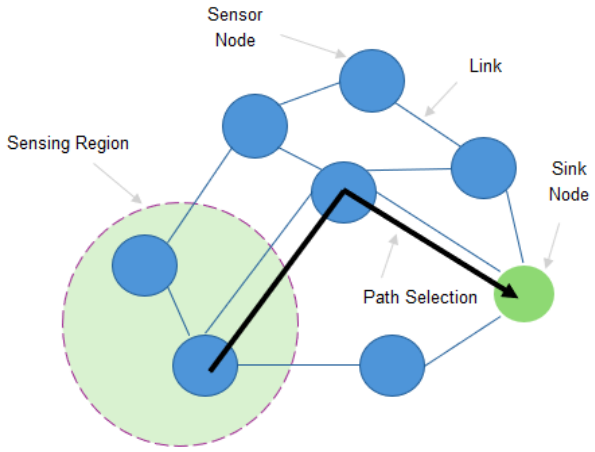
Routers can choose paths between nodes by exchanging information with each other, which is facilitated by a routing protocol.

Many sensor nodes connected by wireless links make up a Wireless Sensor Network (WSN), they have become integral for monitoring the physical state of environments and rely on limited framework resources, including battery power, communication range, and processing capacity.

To send environmental data, such as humidity, temperature, and pressure, to a central sink node, the sensor nodes use routing protocols for transmitting data into the network. However, their susceptibility to diverse network assaults stems from low processing power and vulnerable wireless connectivity. As a result, the observed data will flow from one sensor to another throughout the network until they, for instance, arrive at the base station or sink node as shown in the Figure below.

Figure 2

WSN Elements considered into the network.



Source: Adapted from Dâmaso, A., Rosa, N., & Maciel, P. (2014). Reliability of wireless sensor networks. *Sensors*, *14*(9), 15760-15785.

The communicating nodes use short-range communication to provide vital services. However, the maximum distance that may be covered by sensors and the base station may be limited due to their limited power supply.

Direct connection between a sensor and its base station is frequently rendered impracticable by this constraint, especially in difficult radio settings with high attenuation. Multi-hop networks with dispersed nodes are used to enhance

communication range and solve this problem.

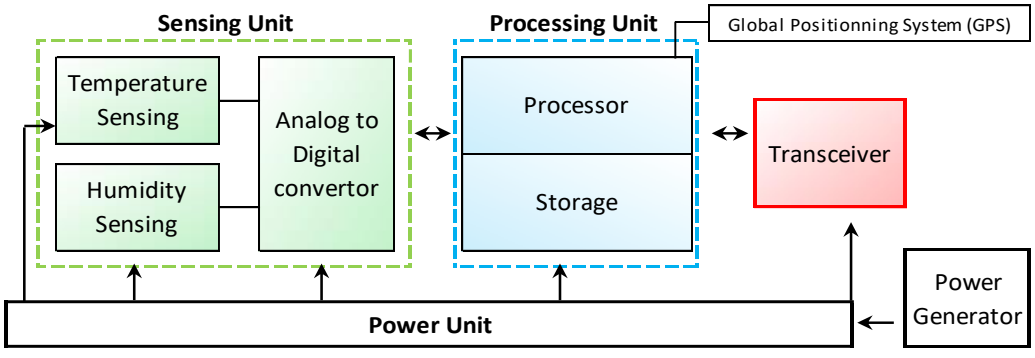
Multihop activities can take place in these systems between sensor nodes that are the same or between sensor nodes and the base station. By constantly reconfiguring around obstructed pathways, the network maintains ongoing connectivity by enabling the signal to hop between nodes until it successfully reaches the base station.

4 THE COMPONENTS OF NODES IN WSN

A wireless sensor is a device that uses a physical sensor to gather data, processes it, and then wirelessly sends the information. A sensor, a micro-controller, a wireless transceiver, and a power and power management module are the four primary components that make up a sensor node's hardware (see Figure 3). It is a specific kind of ad-hoc network composed of nodes that is made up of several sensors joined together within the same wireless network. To send data to an end user, these nodes use routing protocols, usually in star or hybrid arrangements. Sensing and communication need a lot of energy; therefore, sensor nodes have less computing power and battery life than ad-hoc nodes. A 16-bit, 8 MHz RISC CPU, for instance, is used in the TelosB sensor node. It also has 10 KB of RAM, 1024 KB of flash storage, and 48 KB of program memory. The software architecture of the sensor network is shown in Figure 3.

Figure 3

Sensor node's components.



Source: Adapted from I.F. Akyildiz et al. / Computer Networks 38 (2002).

Within a wireless network, the sensor node is an autonomous device that is organized into a group based on a particular routing algorithm. They also represent a distinct type of ad hoc network, where the nodes are equipped with advanced sensing

functionalities, a small processor, and a short-range wireless transceiver. It is an essential part of WSNs, or wireless sensor networks. A sensor, a micro-controller, a wireless transceiver, and a power and power management module are the four basic components that make up a sensor node's hardware.

The system's consistent power supply is guaranteed by the power module. The sensor collects environmental and equipment status data and is an essential part of WSN nodes. Light, vibration, and chemical signals are among the signals it gathers and transforms into electrical impulses, which are then sent to the micro-controller. The received data is processed appropriately by the micro-controller. The Wireless Transceiver (RF module) thus makes data transmission easier, allowing for network communication. A typical WSN configuration is shown in the schematic in Figure 2.

This ability to combine several modules into compact sensors has been made possible by advancements in miniaturisation. Usually, these sensors are made up of four major parts:

1. A collection unit
2. A processing unit
3. A transmission unit
4. A unit for energy management

In Figure 3, we can see the different components that make up a sensor. To be more precise, each group of components has its own role.

In addition to these, a localisation unit, a movement unit, and occasionally an energy-producing unit made possible by tiny solar panels can be found, depending on the sensor network's field of application. All of these various modules are shown in the schematic in Figure 3. Let's focus on each of these modules individually in our situation. Wireless sensors have been created for the captive unit, which is the module in question. It disassembles into two smaller components. The event that the "sensor" or receiver is supposed to monitor will be identified by it. It will then detect the analogue signals that the receiver is emitting and convert them into a digital signal that the processing unit can comprehend.

The Processing Unit, which consists of a processor and occasionally even a small amount of RAM for storage, runs an operating system made specifically for this kind of media (such as the open-source TinyOS). This component enables the node to cooperate

with the rest of the network in order to carry out communication protocols. In certain cases, the processing unit might lessen the task at the well node by analysing the observed data.

The Transceiver Unit is responsible for handling data transmission and reception operations. Either optical or radio-frequency radiation is present in this. The main limitation of this technology was the power unit, hence a module that allowed for sparse energy management inside the sensor had to be inserted. Consequently, it will be in charge of allocating the sensor's energy as efficiently as possible, perhaps by placing inactive parts on standby. In addition, it will oversee the energy replenishment system, although a dedicated module has been supplied for this function.

Location Finding System, which provides the location information necessary for certain routing protocols, typically using a Global Positioning System (GPS).

One important design limitation that needs to be carefully taken into account is power usage. The main energy consumers in most situations are the antennas and communication circuitry. Both passive and active sensors are possible. Devices that monitor strain, temperature, humidity, acoustics, and seismic activity are examples of passive sensors. Passive sensors can measure optical (visible, infrared at 1 micron, and infrared at 10 microns) and biological data when they are organized in arrays. In general, these passive sensors use less power. Conversely, active sensors, like sonar and radar, usually use more energy. The physical size of the battery utilized as a power source is restricted by the tiny size of a sensor node.

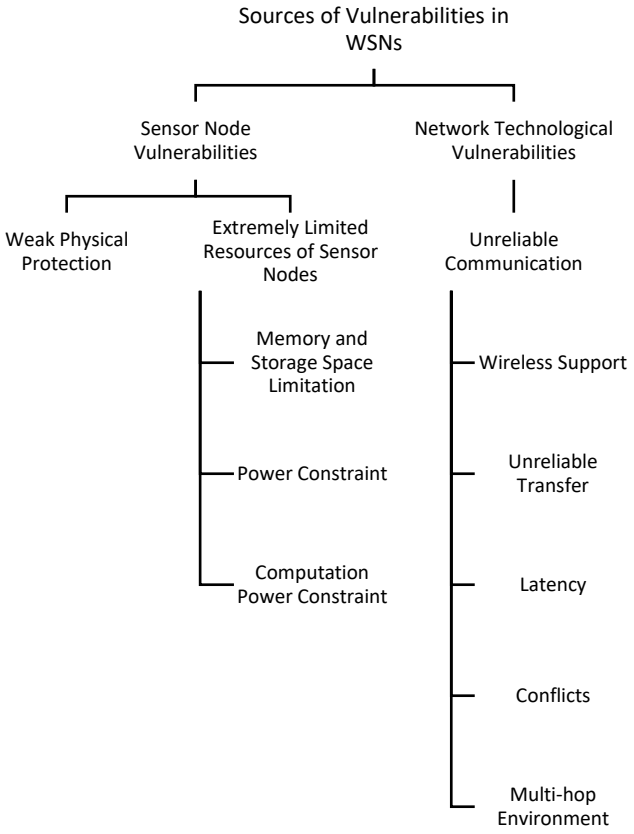
Because they can be widely placed in harsh and pervasive situations, sensor nodes, when arranged to form a wireless sensor network run by a central authority at the base station, can provide useful applications. But there are serious security issues with this deployment for these networks. Because wireless sensor networks are limited in terms of processing power, memory size, battery life, and computing resources, as well as non-tamper-proof packaging, they are susceptible to a wide range of external and internal attacks. However, the quantity and types of sensors differ depending on the specific needs of the application. A diverse range of sensors is available in the market, including common types like temperature, humidity, light, pressure, vibration, sound, as well as specialized ones such as CO-sensors for chemicals, and body sensors like heart rate monitors and accelerometers.

5 SOURCES OF VULNERABILITIES IN WSNs

Due to the technological features of the nodes and the benefits this kind of network offers, WSNs pose more security difficulties than traditional and Ad-hoc networks. Wireless communication, widespread deployment, and other WSN advantages create new security limitations as well as potential sources of risk. As a result, any security solution is severely constrained by the downsizing and low cost of sensor nodes, leading us to think about security that is more appropriate than that of wired and Ad-hoc networks. WSNs have tight and inherent limitations despite having intriguing features. These limitations result from two different sorts of vulnerabilities: those caused by sensor nodes and those caused by wireless network technology as shown in Figure 4.

Figure 4

Differents sorts of vulnerabilities in WSNs.



Source: Adapted from Challal, Y. (2008). Réseaux de capteurs sans fils. Université de Technologie de Compiègne, France, 17.

5.1 Sensor node vulnerabilities

To increase the lifetime of the node and the network, any security strategy must not be resource-intensive due to the sensor's limited resources. The design of an efficient security mechanism for WSNs must adhere to tight guidelines due to the sensors' limited resources.

Sensor nodes must be able to be installed in unsecured environments and left unattended for extended periods of time due to the specific mode of operation of the sensor network, raising new security risks for unattended sensor nodes.

5.1.1 Weak physical PR

Sensors can be used in vulnerable locations (forests, battlefields, mountains, etc.) because of their low cost. As a result, they infrequently use tamper-proof electronic components. As a result, these networks are susceptible to physical attacks (such as the irreversible destruction of sensors, which renders losses irrecoverable), interceptions, and corruption during natural disasters (such as earthquakes, tornadoes, or floods). Although it is obvious that no security protocol can withstand this kind of physical attack, security measures can be created to give networks the ability to self-repair.

5.1.2 Extremely limited resources of sensor nodes

Any security strategy that is put into practice needs a certain amount of resources, such as data memory, code space, computer power, and energy to power the sensor. These resources are severely constrained in this kind of wireless sensor nodes, though, because of their cheap cost and compactness. The following are the key restrictions as a result of sensor node characteristics:

5.1.2.1 Memory and storage space limitation

A sensor is a small device with limited memory capacity and storage space for code. For instance, the Atmel ATMEGA103 4 MHz CPU in a Mica mote-type sensor contains 128 KB of instruction memory, 512 KB of flash memory, and just 4 KB of RAM

for data. To create an efficient security mechanism given these constraints, the amount of the security algorithm code must be constrained.

5.1.2.2 Power constraint

Another issue with WSNs is energy, which is seen to be the biggest barrier to the potential of wireless sensors. It is one of the main causes of nodes failing when their batteries run out of power. Once installed in a sensor network, the sensor nodes are difficult to replace (high operational cost) or recharge.

A sensor node must activate its radio antenna in order to transmit data, which uses a lot of energy (transmission is particularly power-intensive). Strategic and vital nodes can run out of batteries if they are subjected to a sleep deprivation attack; or if the attacker sends the target node pointless packets to keep its radio on. As a result, the sensor node is unable to take part in communication, drastically impairing the performance of the network. To increase the sensor's lifetime, energy consumption must be kept to a minimum, which calls on both hardware energy efficiency and the effectiveness of security and other routing protocols.

5.1.2.3 Computation power constraint

Sensor nodes are small and inexpensive, and as a result, their microcontrollers have a limited amount of storage space. Telos B-type sensors, for instance, have an 8 MHz, 16-bit RISC CPU. A computer power limit of this magnitude necessitates highly computationally sophisticated security techniques. This consequently restricts the viability of some efficient encryption methods.

5.2 Network technological vulnerabilities

Despite recent advancements in WSN hardware and software, the features of the network that make it effective and desirable cause the biggest security issues in WSNs:

5.2.1 Unreliable communication

Unreliable communication is another source of vulnerability for the security of WSNs. The network's security heavily depends on a well-defined protocol, which in turn relies on communication. The key parameters influencing communication security in WSNs are defined in.

5.2.1.1 Wireless support

One of the main security risks to WSNs originate from the very nature of wireless communication support. Wireless communication support is open and available to everyone, unlike wired networks where a device must be physically attached to the medium.

As a result, WSN security is increasingly threatened, making this one of the main challenges to sensor security. An intruder who enters the coverage area can easily record, forge, or repeat all messages that are transmitted.

By creating noise on the channel, an intrusive party with a potent transmitter can prevent sensor nodes from transmitting packets. As a result, the medium may appear to be constantly busy. Wireless technologies make it simple for hackers to intercept, disable, and insert malicious or corrupted packets.

5.2.1.2 Unreliabe transfer

In WSNs, packet routing is connectionless, which is inherently unreliable. In the case of a channel error or highly congested nodes, packets can be corrupted, and as a result, critical security packets can be damaged or lost.

5.2.1.3 Latency

Valid synchronization between nodes is essential for any security mechanism that relies on the distribution of cryptographic keys and event reporting. Proper synchronization between sensor nodes in WSNs is almost impossible due to network

congestion, multi-hop routing, and node processing, which introduces significant latency into the network.

5.2.1.4 Conflicts

The broadcast nature of WSNs makes it impossible to guarantee reliable communication. Conflicts can arise during packet transmission as a result of packet collisions, which can cause transfer failure. By creating interference inside the coverage region, a strong intruder can readily take advantage of this weakness to disrupt the network.

5.2.1.5 Muti-hop environment

To reduce deployment costs and enable easy and rapid deployment, a multi-hop architecture is essential for WSNs, wherein nodes have the ability for self-healing, self-configuration, and self-adjustment. Such architectures enable adversaries to threaten security by exploiting attacks such as the black hole attack, selective forwarding attack, Sybil attack, as well as attacks that allow the creation of erroneous or non-existent paths between the source and the destination.

6 CONCLUSION

In this chapter, we have first described the different elements of the WSNs composed by the communicating nodes as well as their specific characteristics and functionality to unite the necessities of a specific application. After that, we go into more detail about the vulnerabilities and restrictions. These restrictions significantly restrict the use of advanced techniques to achieve security goals. As a result, attackers with varying degrees of its impact on performance can quickly create a variety of attacks. The most critical threat to wireless sensor networks primarily focuses on attacks that exploit node batteries by excessively forwarding packets. The next chapter will be devoted to outlining the various security attacks and threats that have occurred in general within the WSN.

REFERENCES

Akyildiz, I. F. (2002). Wireless sensor networks: a survey. *Computer Networks (Elsevier) google schola*, *2*, 6-14.

ATHMANI, Samir. *Protocole de sécurité Pour les Réseaux de capteurs Sans Fil*. 2010. Thèse de doctorat. Université de Batna 2.

EDDINE, Boubiche Djallel. Protocole de routage pour les réseaux de Capteurs Sans fil» mémoire de Magistère en Informatique. *Université de l'Hadj Lakhdar-Batna Faculté des sciences de l'ingénieur*, 2008.

KAMEL, Beydoun. *Conception d'un protocole de routage hiérarchique pour les réseaux de capteurs*. 2009. Thèse de doctorat. Thèse de Doctorat, Universite de franche-comte.

BELUCH, Thomas. *High precision synchronized mac-phy cross-layer designed wireless sensor networks*. 2013. Thèse de doctorat. Toulouse, INSA.

Boujaada, S., Qaraai, Y., Agoujil, S., & Hajar, M. (2016). Protector Control PC-AODV-BH in The Ad Hoc Networks. *arXiv preprint arXiv:1606.02534*.

Belfkih, A., Sadeg, B., Duvallet, C., & Amanton, L. (2014). Les bases de données dans les réseaux de capteurs sans fil. *Tech. Sci. Informatiques*, *33*(9-10), 739-776.

Shebli, F. (2008). *Réseaux de capteurs sans fil : minimisation de la consommation d'énergie et application à la localisation de cibles* (Doctoral dissertation, Valenciennes).

Jingjing, Z., Tongyu, Y., Jilin, Z., Guohao, Z., Xuefeng, L., & Xiang, P. (2022). Intrusion Detection Model for Wireless Sensor Networks Based on MC-GRU. *Wireless Communications and Mobile Computing*, *2022*(1), 2448010.

Boubiche, D. E. (2013). *Une approche Inter-Couches (cross-layer) pour la Sécurité dans les RCSF* (Doctoral dissertation, Université de Batna 2).

Hanane, F., & Sabrina, C. (2011). *Le routage dans les réseaux de capteurs sans fil* (Doctoral dissertation, Université Mouloud Mammeri).

Uzougbo, O. I., Ajibade, S. S. M., & Taiwo, F. (2020). An overview of wireless sensor network security attacks: mode of operation, severity and mitigation techniques. *arXiv preprint arXiv:2011.06779*.

Akourmis, S., Fakhri, Y., & Rahmani, M. D. (2020). Design Model and Deployment Fashion of Wireless Sensor Networks. In *Wireless Sensor Networks-Design, Deployment and Applications*. IntechOpen.

FELLAH, K. S., & BEHIH, M. (2021). *Analyse les performances d'un routage aléatoire sur les réseaux de capteurs sans fil* (Doctoral dissertation, Université Ibn Khaldoun-Tiaret-).

Dâmaso, A., Rosa, N., & Maciel, P. (2014). Reliability of wireless sensor networks. *Sensors*, *14*(9), 15760-15785.

Makhoul, A. (2008). *Réseaux de capteurs : localisation, couverture et fusion de données* (Doctoral dissertation, Besançon).

Challal, Y. (2008). Réseaux de capteurs sans fils. Cours, Systèmes Intelligents pour le Transport, Université de Technologie de Compiègne, France, 17.

Abdulwahhab, A. R., Salleh, M. F. M., Akb, M. F., & Abdullah, M. N. (2025). Intelligent Intrusion Detection in Clustered Wireless Sensor Networks: A Dynamic Clustering and Machine Learning-Based Approach. Iraqi Journal for Computer Science and Mathematics, 6(2), 30.

Zadeh, M. V., Fadayie, F., & Mirzaei, A. A comprehensive analysis of security in wireless sensor networks, including an examination of lightweight cryptography, artificial intelligence-based cryptography, and machine learning solutions.

Yaras, S., & Dener, M. (2024). IoT-based intrusion detection system using new hybrid deep learning algorithm. *Electronics*, *13*(6), 1053.

Authors' Contribution

Both authors contributed equally to the development of this article.

Data availability

All datasets relevant to this study's findings are fully available within the article.

How to cite this article (APA):
Fakhri, Y., & Rahmani, M. D. DEPLOYMENT OF NODES IN WSNs. Veredas Do Direito, 223445. https://doi.org/10.18623/rvd.v22.n3.3445