Wireless Sensor Networks: Vulnerabilities, challenges and Security Solutions

Hajar FARES[1*]

[1]Faculty of sciences, Abdelmalek Essaadi University, Tetouan, Morocco

*{professeurhajar@gmail.com}

Abstract. The use of wireless sensor networks (WSN) has increased recently with its various and real-time applications, which make them vulnerable for various types of attacks, considering their limited resources we need an automatic system which will be able to detect, alert and react as fast as possible against any abnormal behaviors. The traditional protocols of security like cryptography, key management, routing protocols is no longer useful. A system based on artificial intelligence, specifically learning models present additional value and can help to increase security in wireless networks performed by their high accuracy and provide a good model for reducing the computational cost. In this paper, we provide an overview on wireless sensor networks; we highlight their vulnerabilities, constraints and the current solutions of security.

Keywords: wireless sensor network, cryptography, key management, routing protocols, learning model, dataset, accuracy

1. Introduction

Wireless sensor networks (WSN) is a new technology consists of a large number of a small components deployed and distributed randomly. The basic architecture for wireless sensor networks is shown in figure.1. Sensors in the network allow a physical quantity to be transformed into an electrical signal. WSNs are used for various real-time applications and deployed in hostile area which make them vulnerable for attacks [1]

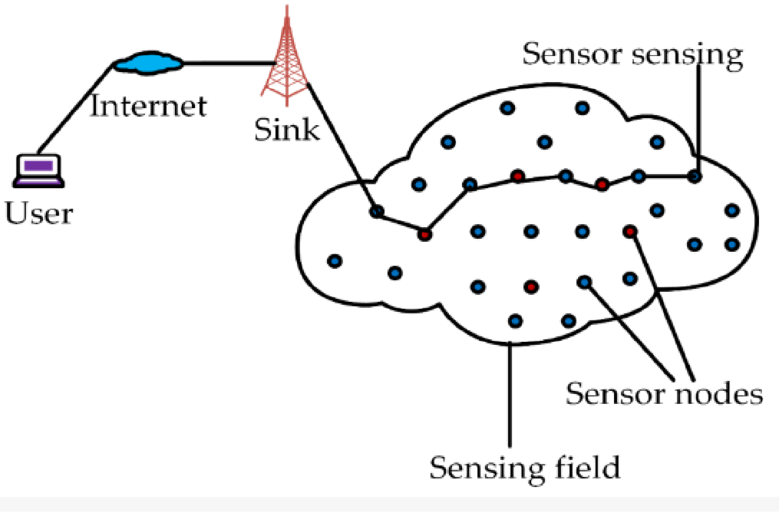

Figure.1: wireless sensor networks architecture [2]

The areas of application of WSN are shown in figure.2. They have been used in the medical industry to monitor patients continuously without the need for surgery. They may also be used to monitor heart rate and help identify cancer. They may be used to monitor the weather, identify natural disasters to aid with things like fighting fires, and can be deployed independently to support military objectives.

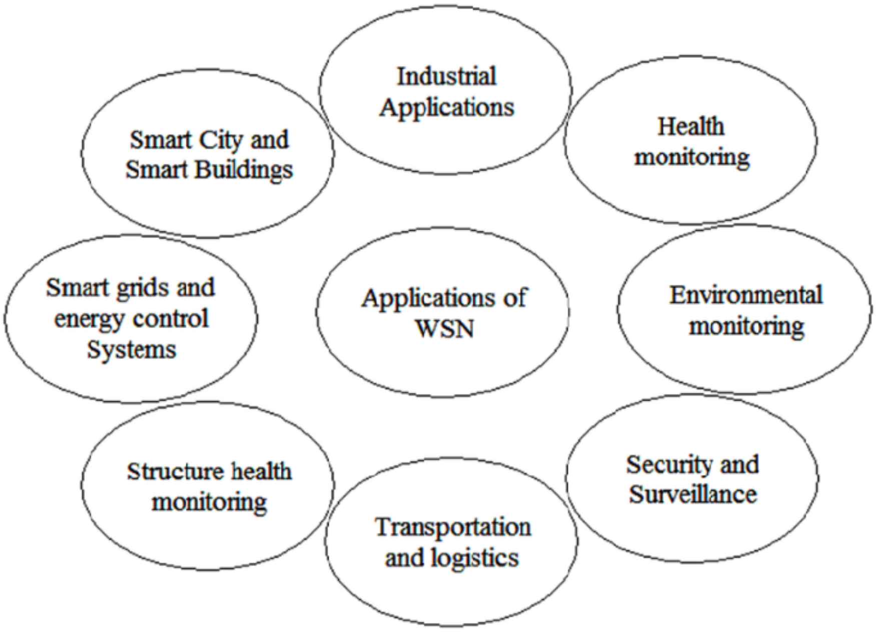
Industrial Applications
Smart City and Smart Buildings
Health monitoring
Smart grids and energy control Systems
Applications of WSN
Environmental monitoring
Structure health monitoring
Security and Surveillance
Transportation and logistics

Figure.2: Area of application of WSNs [3]

Unfortunately sensor nodes have limited resources (CPU, Memory, Battery…) which make the application of classical solutions of security wasteful. Recently machine learning plays an important role in security filed; it can control the continuous behaviors of sensors during the communication. Machine learning, which is a branch of artificial intelligence; have provided several low cost security solutions, adequate for wireless sensor networks.

Despite the importance of machine learning to protect WSN from vulnerabilities, attack soft unenhanced their behaviors. The accuracy of prediction depend on one hand of : the learning model used and the appropriate dataset used to obtain highest rate and the approximation of the precision in the classification of attacks.

In this paper, we provide an overview on wireless sensor networks, we highlight their vulnerabilities, constraints and the current solutions of security.

The rest of this study is structured as follows:

Section 1, present a general introduction about wireless sensor networks, followed by section 2, which provide the different types of attacks related to WSNs, while in section 3, we cite the constraints and challenges of WSNs, subsequently, section 4 provide the different solutions of security. Finally, we conclude our paper by a detailed conclusion.

2. Types of Attacks in WSNs:

An attack could be a malicious node of unauthorized access, which can listen, update and even destroy data in the network.

Generally, we can specify attacks: as interne or extern and active or passive [4].

Internal attacker: When the attacker poses as an authorized network entity with the ability to access system resources. Thus, every component of the network authenticates and recognizes the attacker.

External attacker: in which the attacker is seen as a "foreigner" on the network. Passing from outside the network security perimeter, this user is not permitted.

Active Attacker: Attackers that try to alter data or fabricate a message are said to be engaging in active attacks. They may have an impact on data availability and integrity in addition to confidentiality.

Passive attacker: It is usually a concealed attack, with its primary function being the collection or listening of network information, which gives the attacker the ability to manipulate and monitor data between nodes. These attacks are simple to execute but also challenging to identify.

According to many research studies, Denial of Service (Dos) attack is considered one of the most common and dangerous attacks that threaten the security of WSNs, which share all layers. There are a various types of attacks such as: Flooding, Grayhole, Blackhole and TDMA.

Flooding: Flood attacks are also known as Denial of Service (DoS) attacks. In a flood attack, attackers send a very high volume of traffic to a system so that it cannot examine and allow permitted network traffic. The flooding attack scenario is shown in figure.3.

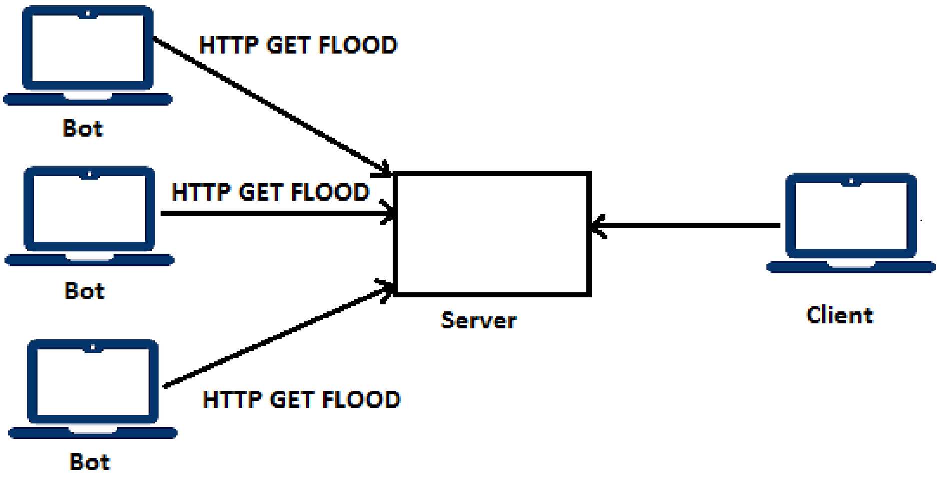

Figure.3: Flooding attack [5]

Blackhole: the attacker drops packets selectively, or all control and data packets that are routed through him. Therefore, any packet routed through this intermediate malicious node will suffer from partial or total data loss. The blackhole attack scenario is shown in figure.4.

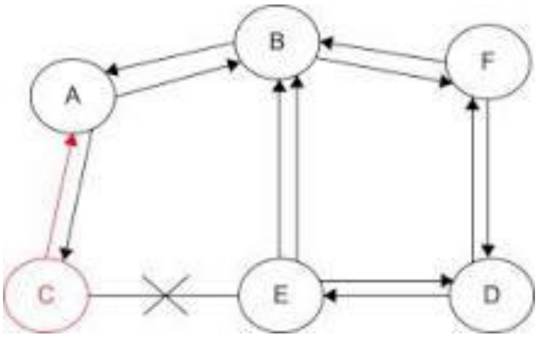

Figure 4: Blackhole attack [5]

Grayhole: It is an advanced transformation of blackhole attack. Both of them are a common type of attack in Wireless Sensor Network (WSN). Malicious nodes may constantly or randomly drop packets and therefore reduce the efficiency of the networking system. The garyhole scenario is shown in figure.5.

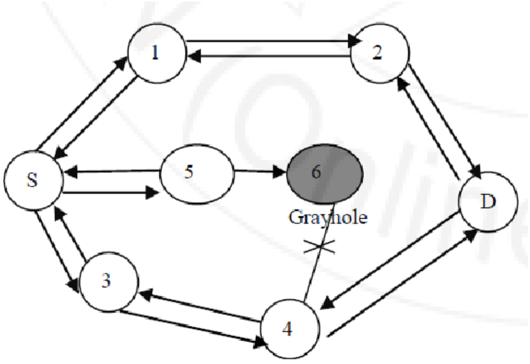

Figure 5: Grayhole attack [5]

TDMA: Such attacks typically rely on the use of periodic sampling or a low-precision clock to measure CPU usage; like a train passenger hiding whenever the conductor checks tickets, an attacking process ensures it is never scheduled

3. Wireless Sensor Networks Challenges

Despite the usefulness of sensor networks in various fields, they are characterized by several constraints [6] such as:

Limited resources: Sensors have RAM and some storage space, but they are not designed to store large databases. The information collected must be sent to the base station, not stored long-term by the sensors themselves. Sensors are equipped with batteries with limited energy.

In addition, wireless sensor networks the sensor batteries are a short life time, which make them easy to destroy.

Dynamic topology: The topology of a sensor network changes over time. Network dynamism is caused by node failures due to physical damage or the expiration of its energy.

Fault tolerance: Sensors may not work properly because they are entities sensitive to state alterations such as climatic phenomena (humidity, heat, electro magnetism) or due to a low battery. Therefore, the network must be able to detect this type of error and remedy it.

4. Security Solutions for WSNs

To protect a Network from malicious attacks, defense methods are essential. Sophisticated techniques and tools are used to strengthen the security of sensitive data and information within a complex system [7].

Authentication:

It's the process of access controlling for users or systems. It frequently makes use of tools like biometric technologies, authentication keys, and passwords. In order to improve the security of sensitive data and system access, strong authentication is becoming more and more popular. Indeed, putting in place sufficient security measures is crucial in a society that is becoming more interconnected and vulnerable to cyber attacks [8-9].

Cryptography:

This process involves transforming data into a format that can only be read by those without the necessary decryption keys. Exchanges are protected by encryption and decryption protocols, allowing for the effective and dependable assurance of data confidentiality and integrity. There are various cryptographic algorithms including, symmetric and asymmetric.

However, despite the various advantages of cryptographic system, it stays inadequate for wireless sensor networks, according to the constraints and challenges of sensors nodes already cited [10-11].

Artificial Intelligence

Artificial intelligence (AI), have grown rapidly in the recent years. AI excels at analyzing large volumes of data and extracting trends or anomalies. Machine Learning and Deep learning as branches of artificial intelligence provide robust security solutions based on automatic learning from a dataset. Various learning models have proven their efficiency, such as Decision Tree, Random Forest, Support Vector Machine and so on.

While AI has significant promise and potential benefits, it can also be insufficient, while attackers enhance their behaviors continuously [12].

5. Conclusion

Wireless sensor networks (WSN) are the technology which has been integrated increasingly in various applications in the recent years, especially with the big advancement of Smart Cities. The areas where the sensors are deployed are often random and no secured, which make the network vulnerable of various types of attacks. However, Sensors nodes have several constraints, which make the robust and standard solutions of security almost impossible.

In this paper, we provide an overview on wireless sensor networks; we highlight their vulnerabilities, constraints and the current solutions of security.

References

[1]. Sahar, G.; Bakar, K.A.; Rahim, S.; Khani, N.A.K.K.; Bibi, T. Recent Advancement of Data-Driven Models in Wireless Sensor Networks: A Survey. *Technologies* **2021**, *9*, 76. https://doi.org/10.3390/technologies9040076

[2]. pachlor, Rohit&Shrimankar, Deepti. (2019). Post-Deployment Energy- Efficient Schemes in Wireless Sensor Networks: A Study on Three Well-Known Energy-Efficient Approaches Post-Deployment Energy-Efficient Schemes in Wireless Sensor Networks. 10.4018/978-1-5225-7335-7.ch014.

[3]. yetgin, Halil& Cheung, Kent &El-Hajjar, Mohammed & Hanzo, L.. (2017). A Survey of Network Lifetime Maximization Techniques in Wireless Sensor Networks. IEEE Communications Surveys &Tutorials. 19. 828 -. 10.1109/COMST.2017.2650979.

[4]. Tournier, Jonathan. *Modélisation de réseaux IoT hétérogènes à des fins d'évaluation de sécurité*. Diss. Université de Lyon, 2021.

[5]. Dener, M., Okur, C., Al, S. and Orman, A., 2023. WSN-BFSF: A new dataset for attacks detection in wireless sensor networks. IEEE Internet of Things Journal.

[6]. G. Anastasi, M. Conti, M. Di Francesco, A. Passarella, Energy conservation in wireless sensor networks: A survey, 7(3) (2009) 537- 568 doi: http://dx.doi.org/10.1016/j.adhoc.2008.06.003

[7]. Jain, A.K. and Nandakumar, K., 2012. Biometric authentication: System security and user privacy. Computer, 45(11), pp.87-92.

[8]. Van Tilborg, H.C. and Jajodia, S. eds., 2014. Encyclopedia of cryptography and security. Springer Science & Business Media.

[9]. Matlou, O.G. and Abu-Mahfouz, A.M., 2017, October. Utilizing artificial intelligence in software defined wireless sensor network. In IECON 2017-43rd annual conference of the IEEE industrial electronics society (pp. 6131-6136). IEEE.

[10]. Olakanmi, Oladayo Olufemi, and Adedamola Dada. "Wireless sensor networks (WSNs): Security and privacy issues and solutions." *Wireless mesh networks-security, architectures and protocols* 13 (2020): 1-16.

[11]. Boubiche, Djallel Eddine, et al. "Cybersecurity issues in wireless sensor networks: current challenges and solutions." *Wireless Personal Communications* 117 (2021): 177-213.

[12]. Bhasin, Vandana, et al. "Security architectures in wireless sensor network." *International Journal of Information Technology* 12.1 (2020): 261-272.