SECURITY IN WIRELESS SENSOR NETWORKS: COMPARATIVE STUDY

Fatimah Khalil Aljwari, Hajer Abdullah Alwadei and Aseel Abdullah Alfaidi

Advanced Computer Network, Jeddah University, Jeddah, Saudi Arabia

ABSTRACT

The security in wireless sensor networks (WSNS) is a very important issue. These networks may be exposed it different attacks. With this in mind, researchers propose in this area variety of security techniques for this purpose, and this article describes security in wireless sensor networks. Discussed threats and attacks of wireless sensor networks. The article also aims to provide the basic information related to determining essential requirements for the protection WSNs. Lastly, we mention some security mechanisms against these threats and attacks in Wireless Sensor Network.

KEYWORDS

Wireless Sensor Networks, Security Requirements, Attacks, Security Mechanisms.

1. INTRODUCTION

A wireless sensor network is the most important emerging technology trend in the coming years because sensing technologies and processing power, and wireless communication make it beneficial for use in the soon future. wireless sensor setworks (WSNs) are used to collect data from the physical environment; wireless sensor networks can work in any environment other than conventional networks, especially if they are not wired connections in that environments [1].

The sensor nodes used in WSNs deploy efficiently more than the conventional wired sensor network; the sensor nodes consist of several components such as sensing, data processing, and wireless communication technology, which monitor the environment without connection with the wired network. Therefore, WSNs more advantages than the conventional wired sensor network [2].

Security is quite a challenging issue in WSNs. It is used in many practical applications, in military applications, disaster management in remote areas, traffic monitoring, and monitoring intelligent houses and cities. The WSNs can be prone to different security threats and attacks or hackers to disrupt the entire network. From challenges and Issues face in WSN today is security.
Therefore, security for WSNs becomes most important. This paper's purpose and requirements security in WSNs then mention some of the security mechanisms used to handle those security issues in WSNs.

2. BACKGROUND

In this section, we will cover in general the concept of both Wireless Sensor Networks (WSNs), attack, security and provide some of the prominent areas of applications of WSNs.

DOI: 10.5121/ijcsit.2022.14305

2.1. Wireless Sensor Networks (WSNs)

Wireless Sensor Networks are self-configured and infrastructure-free wireless networks that track physical or environmental conditions such as temperature, sound, vibration, friction, motion, or pollutants and cooperatively transfer their data through the network to a central position or sink where it can be viewed and analyzed. Sensing and computing instruments, radio transceivers, and control components are all used in a wireless sensor node. A wireless sensor network's individual node is resource restricted by design: they have minimal processing power, storage space, and connectivity bandwidth. The sensor nodes can operate in either a continuous or event-driven mode. The architecture of a WSN is shown in Fig.1. The WSN uses a gateway known as a sink to connect a wired network and the distributed wireless sensors. The sensors collect the data sent to the gateway, which sends it to the user through a network or internet.

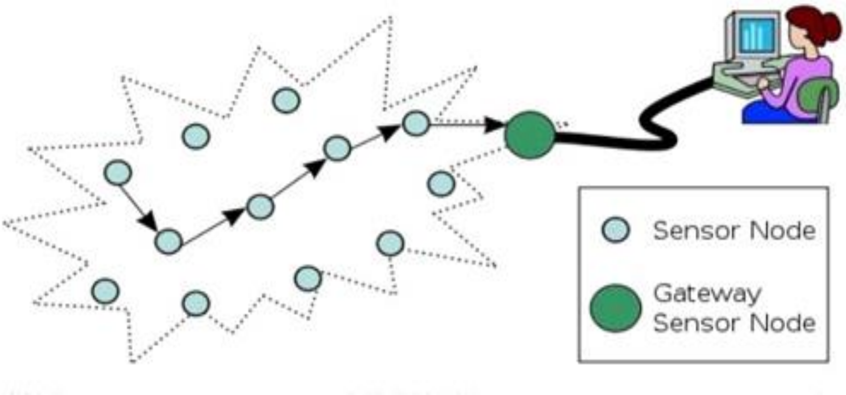

Figure 1. Architecture of WSNs

2.2. Attack

Attacks are the techniques that attackers use to find and exploit program flaws. An attack can attempt to gain unauthorized access to a service or information. These WSNs are subject to numerous attacks. Because the nodes can be in a dangerous environment. once a node has been hacked, the attacker can steal the node's key materials. On these networks, there are various attacks that can be categorized as routing attacks, data traffic attacks and on various points of view can be outsider vs insider, passive vs active, node capture attack and attacks on layers.

2.3. Security

One of the difficulties of WSNs is meeting high-security standards when working with limited capital. Node protection, user confidentiality, anti-compromise, and resilience against traffic manipulation are all security standards in WSNs. The implementation sensors must pass a node authentication review by their respective manager nodes or cluster heads to distinguish both trustworthy and incompetent nodes from a security standpoint, and unauthorized nodes may be separated from WSNs during the node authentication process. Similarly, all packets sent between a sensor and the manager node must be kept secret to prevent eavesdroppers from intercepting, modifying, and analyzing WSN data and discovering sensitive information.

2.4. Application of WSNs

The potential applications of WSNs to any field in the world are virtually limitless, ranging from environmental monitoring and control to medical and healthcare systems, as well as other areas such as positioning and tracking, localization, and logistics. It is important to stress that the advantages and applications influence the preference of wireless machinery to be used. If the application's specifications have been established, network designers must pick and choose the machinery that will enable these requirements to be met. WSNs have received a lot of acclaim for their versatility in addressing problems in many application areas, and they have what it takes to transform the environment in a variety of respects, such as military applications, applications in area monitoring, transportation applications, medical/health applications, environmental applications, structural applications, industrial applications, and agricultural applications.

2.4.1. Security requirement of wireless sensor network:

The objective of security services in WSNs is to protect and preserve the information and resources from attacks and manipulation. In this section, we discuss different types of security requirements for wireless sensor networks.

Yan-Xiao Li et al. (2010) mentioned the security services in WSNs are usually centered around cryptography. Security requirements in WSNs include (availability, authorization, authentication, confidentiality, integrity, nonrepudiation). and they suggested it should also be considered to (1) forward secrecy it is sensor should not be able to read any future messages after it leaves the network. (2) backward secrecy, it is joining sensor should not be able to read any previously transmitted message [3].

Muazzam A. Khan et al. (2011) explained the requirements by considering the importance. In each of the (data integrity, confidentiality, and data freshness). Also mentioned, any compromise on these requirements could cause huge destruction in the network. Other than what was said (Yan-Xiao Li et al.), two new requirements were added it is. (1) Flexibility it is external conditions as well as demands of the user changes rapidly example in emergency scenarios and battlefield. So according to the nature of mission or changing conditions the sensor nodes may have flexibility to adopt these changes. (2) Secure localization it is accurate location of a sensor node is very important for data or warding as well as trust management[4].

Discussed Mahsa Teymourzadeh et al. (2013) [2].The requirements and how would the attacker have worked If the requirement is not present in WSNs and confidentiality is a fundamental security service.

Compared to what others have said, Vikash Kumar et al. (2014) security goals are classified as primary and secondary. The primary goals are known as standard security goals such as confidentiality, integrity, authentication, and availability. The secondary goals are data freshness, self-organization, time synchronization and secure localization. finally, vikash kumar et al. (2014). add new requirement secure localization from secondary goals. and explain most sensor network applications rely on some form of time synchronization [1].

We summarize the security requirements in Fig.2 that have been put forward by the researchers and we emphasize the importance of requirements for the WSNs.

- Confidentiality: Is a fundamental security service Commonly, is required in sensor networks to protect information traveling between the sensor nodes of the network or between the sensors and the base station.

- Integrity: Data integrity is very significant in such networks, mostly used for security purposes. That further guarantee the message sent from one node to another is not modified by malicious intermediate nodes.
- Availability: This ensures that the required network services are accessible even in the presence of attacks. The most harmful danger to network availability is a denial of service [2].
- Data Freshness: It means that the information is recent and ensures that no opponent can replay old messages.
- Self-Organization: The harm resulting from an attack or even the risky environment can be devastating if sensor network lacking self -organization.

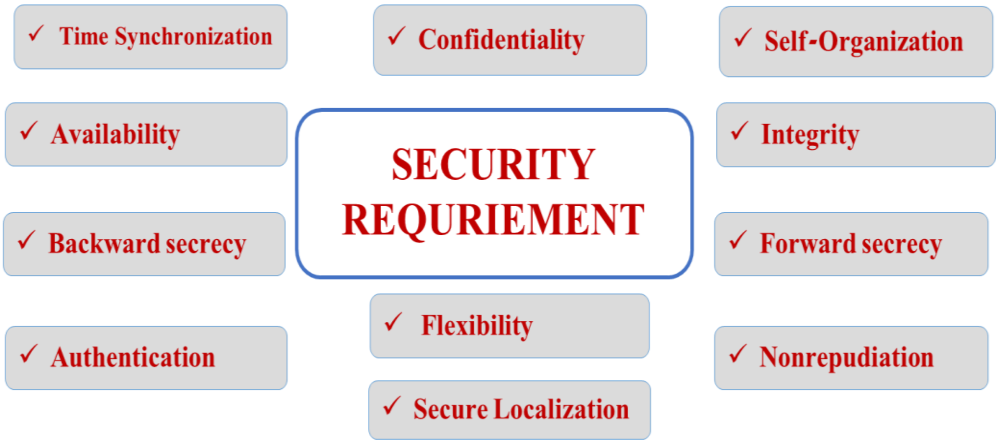

Figure 2. Security Requirements

2.4.2. Related word:

This section provides a review of some works on security in wireless sensor networks. It covers different papers from all aspects that relate to threats in WSNs and security solutions for that.

Clarified Kumar et al. [1]challenges and issues in sensor networks. As they mentioned, ad-hoc wireless sensor networks pose major challenges when it comes to developing protection chimes. Also, proposed some security solutions to protect the WSN from this threat. Presented also Mahsa Teymourzadeh et al. [2]issues and challenges in WSNs, but from different perspectives examined the state of the art in analyzing network and sensor security, and discusses some potential future research directions.

Discussed Rani and Kumar [5] survey about security in wireless sensor networks in 2017. And mentioned WSNs are vulnerable to several threats if they are not adequately protected. Various aspects of security have been examined, including cryptography, key management, and stable routing protocols to improves and enhances the security mechanism in the WSNs. According to Yan-Xiao Li et al. [3]components without security can easily be exploited and they become vulnerable to attacks, Incorporate security into every part to pervade security and privacy into every element of the design. And mentioned each of the security solutions may be used to help secure a WSN.

Muawia A. Elsadig [6]et al discussed Security in WSNs is challenging and critical to the functionality of this type of network. Therefore, a combining effort to represent a common model that takes into consideration the security issues concerning each layer still a challenge. Cryptography is an adequate security solution for many scenarios of WSNs but still needs more enhancements to reduce the overheads to an acceptable rate that fit WSNs particularities and constraints. Moreover, introduced Modares et al. [7].The challenges in WSN include routing, QoS provisioning, energy efficiency, stability, and multicasting. Since security is a mechanism rather than a product, the developer of the system can keep up with the latest trends in embedded system attacks. Important devices' protection should be re-evaluated on a daily basis to prepare for new detections. The application's level of protection is needed.

Muazzam A. Khan et al [4].Discussed security requirements for wireless sensor networks, and sensor that works without a battery Since networks have inherent limits, they said physical protection is required in addition to communications security. and in this kind of network, the most frequent attack is for a node to compromise and accept tempered data before forwarding it onward. As a result, cryptography alone is insufficient to keep such networks stable. It may be possible for sensor nodes to authenticate and encrypt data. David Martins et al [8]. Clarified science strategies to fight attacks in wireless sensor networks have been suggested, but they do not resolve all attacks. and Sensors' low processing capacity and, more significantly, their limited energy are impediments to the introduction of advanced techniques, and we are still looking for solutions that can handle security, while still combining lifetime and sensor latency.

Anuj Kumar and Patro [9]explained in their paper WSNs have two significant security aspects. The first is a taxonomy of WSN security specifications, followed by a taxonomy of WSN attacks. They also gave a snapshot of possible countermeasures to various WSN attacks. Kalpana Sharma et al [10]mentioned in their paper both vulnerability attacks, such as the hello flood attack, wormhole attack, sybil attack, and sinkhole attack, have the same goal in mind: to breach the network's credibility. They concentrated on the security risks in WSN in their report. They summarized the challenges to WSNs that impact various levels, as well as their defensive mechanisms.

3. ATTACKS IN WIRELESS SENSOR NETWORKS

The attacks pose a major threat to the security of wireless sensor networks where they destabilize the security. The network layers are divided in to: physical layer, data link layer, network layer, and transport layer. Each layer is vulnerable to different types of attacks. Here comes the role of security attacks so that the interaction between layers can be exploited. In this section, we make a list of the latest attacks on wireless sensor networks.

Yan-Xiao Li et al. in (2010) suggest attacks in sensor networks can be classified into the following categories mote-class versus laptop-class attacks, outsider versus insider attacks and passive versus active attacks. finally, mentioned classify according to the security requirements in WSNs such as attacks on secrecy and authentication, attacks on network availability and stealthy attacks against service integrity [3].Discuss also, Khan et al. in (2011), different types of attacks and their affects in WSN. And the comparison between active attacks is easily identifiable and passive attacks are more dangerous as compared to active attacks because in passive attacks you are unable to recognize your attacker [4].

Mahsa et al. (2013) explain to us there are many reasons for importance of security in WSN of which, exist the nodes are in a dangerous or hazardous setting. Their physical protection is jeopardized in this environment. WSNs could be more vulnerable to denial-of-service attacks Also, many kinds of DoS attacks in various layers in wireless sensor networks [2]. Mentioned Vikash et al. (2014) about wireless sensor networks it will be vulnerable to attacks because of the due to the broadcast nature of the transmission medium. Identify two categories is active attacks and passive attacks [1].

According to Aditi &Sanjeet (2017), WSNs are vulnerable to several attacks. Attacks in WSNs can be categorized on the basis of different layers physical layer, link layer, network layer, and transport layer. Mentioned some attacks such as selective forwarding (SF), sinkhole, sybil, acknowledgment spoofing (AS), and collision [5]. According to singh & Patro (2019), WSNs work in harsh and hostile areas it is vulnerable to different threats and attacks, and the attacks section on WSNs in five categories based on, layers, authentication, privacy [9]. Elsadig et al. Focused (2019) on mentioning two subsections to two types of WSN attack as layered-based classification and the internal\external classification [6].The attacks be classified in terms of:

- Active attacks are when data flow into the communication channel is tracked, listened to, and updated by unauthorized attackers, and passive are attacks transmission of information or data files to an attacker without the user's permission or awareness,
- In an external attack, an additional sensor node is installed in the WSN to be targeted. This remote node lacks access to the WSN's security parameters and cryptographic keys. In an internal attack, the security of an internal sensor node is breached in order to undermine the network's security. In Fig.3, shows the classification for most of the attacks.

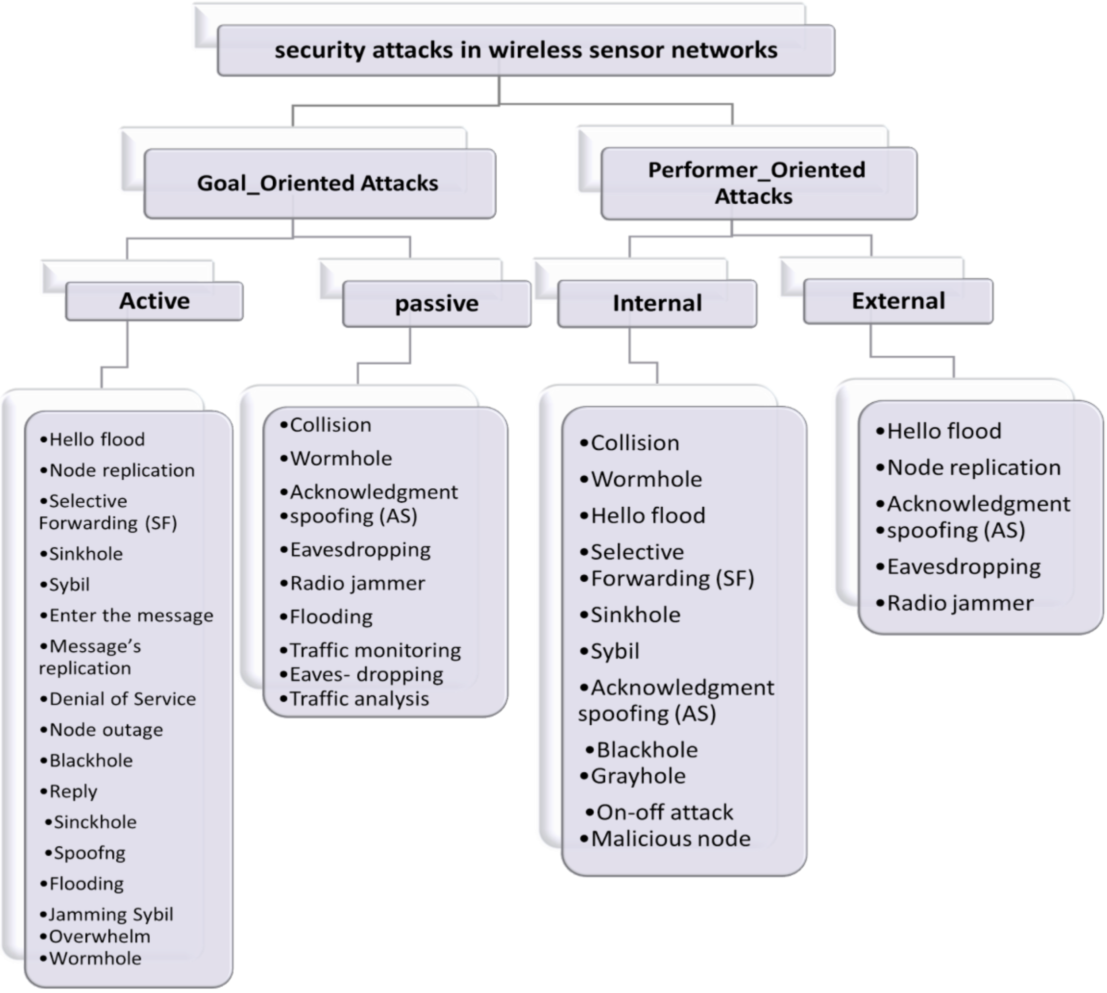

Figure 3. Active / passive attacks and external / internal attacks

Wireless sensor networks are layered in organized. Because of their architecture, these networks are vulnerable to a variety of attacks. It is one of the classifications for attacks, layer-based classification [5][9]. Based on the Fig.4, when compared layers, the number of network layer attacks is obviously the most prevalent followed by data link layer and physical layer finally application and transport in approximately same number attacks.

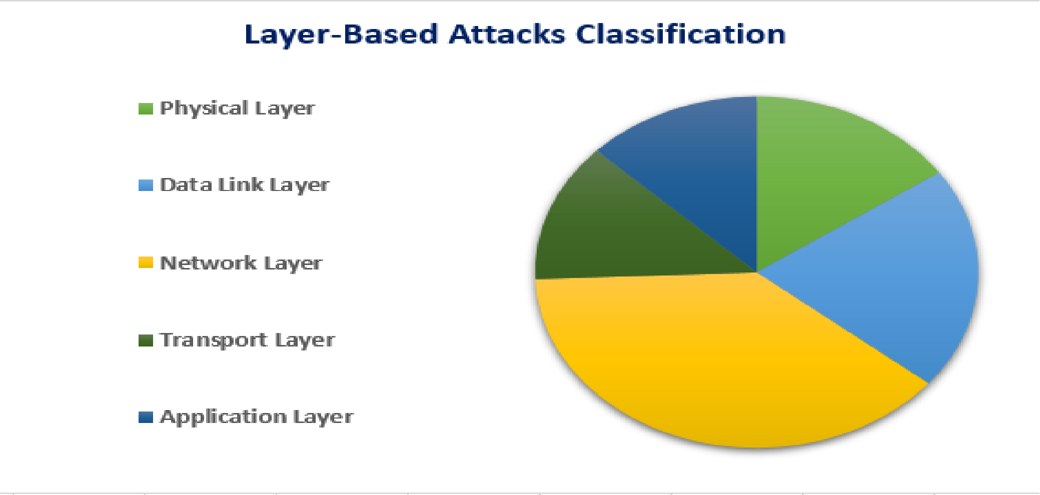

Figure 4. network layer attacks

4. SECURITY MECHANISMS IN WSNS

To counter these attacks that threaten wireless sensor networks. We have to find simple solutions that allow securing the network. These solutions are to prevent and detect different security attacks in wireless sensor networks. In this section, we discuss a list of solutions.

David Martins &Hervé Guyennet (2010) discuss a list from the mechanisms. And they mentioned we must simple solutions that enable us to secure the network while using as little energy as possible. such as the data partitioning, cryptography, trust management and steganography [8]. Kalpana Sharma &Ghose (2010) mentioned to other methods to defense some threats in WSNs. And summarized of defense mechanisms. DOS prevention can use priority messages, and encryption. Selective Forwarding attack prevention can use routing dawwsen proactive and detection by signal strength. Identity certificates can defense Sybil attack [10] .

Aditi &Sanjeet (2017) ,WSNs play an important role in providing protection at the nodal and network levels. Explained of the various security aspects like cryptography, secure routing protocols. Mentioned by considering at node level is used cryptography and network levels is used Secure Routing Protocol and Key management [5].Vikash Kumar (2014) mentioned to counter malicious attacks, a wide range of protection schemes can be devised, and these can be classified as high-level and low-level as secure routing , key establishment and trust Setup and secrecy and authentication[1].

We explain some of the security mechanisms that have been suggested by researchers, and we want to emphasize in our view, Its importance for WSNs.

4.1. Data Partitioning

One of the solutions to prevent information capture in wireless sensor networks by data partitioning. The aim is to divide the information into several parts. If a sensor tries to send information, it cuts the data into several packets of fixed size. Each packet is sent on a different route from another route. And Packets pass in different nodes. Packets are eventually received, which could then bring packets together to reproduce information. An attacker has to catch all packets of a message if it wants to know the information. And To do it, it has to be able to listen to the entire network. It is more complicated for an attacker to have the information, but this solution increases energy consumption and needs to use many nodes more essential to communicate.

4.1.1. Key management

For solutions of key management, we find four types that can be used in security mechanisms against attacks:

Table 1. Key management types in security mechanisms

Key Type	Definition	Role in security
Global key	The entire network shares one key the sender sends a message and information encrypted with this key. Once it receives the message, it can be decrypted with the same key.	The solution with limited security because: If an attacker could find the key, he can hear the entire network that communicates with this unique key, then to know this key allows the possibility to insert a malicious node in the network.
Pair-wise key node	Each node has a different key to communicate with a neighboring node that shares this key. a node that sends a message must encrypt the message with a key neighbor who receives the information. The neighboring decrypts information to re-encrypt with the key corresponding to the following receiver.	This solution increases the network's security because if an attacker discovers a key, this key can communicate with two nodes. The attacker has to find all pair-wise keys to listen to the entire network
Pair-wise key group	Each group or cluster has a key to communicating between nodes in the cluster. Cluster-heads use a single key for all cluster-heads to communicate between two cluster heads.	The solution increases the work of cluster heads, which have to decrypt and encrypt the information.
Individual key	Each node has its own key to encrypt data. The sink only knows this key. the message sent by this node goes around hidden on the network until it reaches the sink.	This solution secures only communication between a node and the sink.

4.2. Trust management

Another solution is to use trust and reputation mechanisms that Exist in peer-to-peer networks, community networks, or even market websites like eBay. In this kind of network, as in wireless sensor networks, it is hard, because of the large number of nodes, to know which node can be a malicious node. To detect and protect the network's integrity, each node of the network monitors its neighboring nodes and their actions over time. Depending on its neighboring nodes' actions, a node will increase these nodes' trust based on its reputation. When a node does not carry out a request, its level of trust falls. If this node always sends correct data, its level of trust increases. With these levels of trust, a node will then choose the most secure route for sending data. Instead of going through the fastest path (geographical distance), the node will transmit its data via nodes with the highest trust level (the safest route). These techniques make it possible to eliminate potentially dangerous nodes and protect data from going through these nodes. Solutions based on trust management are energy efficient.

Many different classification methods have been used in literature. In this paper we collect the attacks and classify each attack according to what was mentioned in terms of classification types on different perspectives [3] [4] [2] [1] [5][9][6]. Several studies are being conducted in order to find suitable solutions to attacks wireless sensor networks. We identify defenses for all attacks and according to what was mentioned in [8][10][5][4]. We explain in the table 2.

Table 2. WSNs Attacks Classification & Defense mechanisms.

Attacks	**Definition**	**Layer-based Classification**	**Internal/External Classification**	**active /passive Classification**	**Defenses**
Collision	There is this type in the link layer when two nodes try to transmit at the same time on the same frequency where there is a collision due to the collision of the packets with each other	Data Link layer	Internal	passive	Error-correcting code[9]
Wormhole	is a serious attack, an attacker records packets at one location in the network and tunnels them to another location. This attack needs to insert in the network at least two [Short Survey].	Network Layer	Internal	passive	An efficient monitoring system[3].
Hello flood	An adversary node broadcasts hello packets with high transmission capacity, allowing the majority of the network's nodes to choose it as the cluster head.	Network Layer	Internal /External	Active	Suspicious node detection by signal strength[10].
Node replication	In this attack, the attacker creates a new sensor node in the network by copying an existing sensor node's node ID.	Network Layer	External	Active	Line selected multicast[4]
Selective Forwarding (SF)	It is the attacker creating a corrupt node in the network so that it can intentionally drop some important messages while forwarding only a few of them	Network Layer	Internal	Active	Multipath routing[5]
Sinkhole	In this type, the attacker is keen to make the defected node be very attractive compared to the rest, in order to be able to reach his goal, which is for the surrounding nodes to send data to that defected node	Network Layer	Internal	Active	Geographic routing protocols[10]
Sybil	It is also known as clone attack, In this type, attackers rely on placing copies of each node in order to be able to leak data or be able to place false data	Network Layer	Internal	Active	utilize identity certificates[10]
Acknowledgment spoofing (AS)	Attacking nodes that provide false information to other nodes, such as claiming that a dead node is still alive but actually dead	Data Link Layer	Internal /External	Passive	○Authentication mechanism[5]
Eavesdropping	Is the attacker listening to listen the network to intercept information on the network so that he can steal it when sent without encryption. This attack is difficult to detect because there is no modification to the data, so it is difficult to detect	physical layer	External	passive	Encryption of data and messages[9]
Radio jammer	The attacker uses radio waves to disturb the communication between the nodes by sending the waves to the same frequency so that they cannot communicate	physical layer	External	passive	Spread spectrum, priority messages[10].
Denial of Service	In a conventional network, this is an intentional intrusion like denial of service. The assault disrupts the wireless sensor network, and the influx of data causes sensors to run, wasting their resources.	Physical layers	Internal /External	Active	payment for network resources, Priority messages, monitoring, authorization, encryption[10]
Flooding	Flooding occurs when an attacker attacks a source node in such a way that it receives a large number of requests frequently and its memory becomes complete.	Transport Layer	Internal	Passive	Strong authentication mechanism[9]

5. CONCLUSION

Wireless sensor networks have become more commonly used as a result of recent technical developments. It is, however, also vulnerable to a variety of attacks, for example like sinkhole, Sybil, selective forwarding. They are used for many important applications. As a result, the protection of WSNs is a major concern for researchers. In this paper we discussed security requirement for wireless sensor networks. We mentioned various security threats and potential attacks as well as current security methods suggested by various studies.

REFERENCES

[1] V. Kumar, A. Jain, and P. N. Barwal, “Wireless Sensor Networks: Security Issues, Challenges and Solutions,” Int. J. Inf. Comput. Technol., vol. 4, no. 8, pp. 859–868, 2014, [Online]. Available: http://www.irphouse.com.

[2] M. Teymourzadeh, R. Vahed, S. Alibeygi, and N. Dastanpor, “Security in Wireless Sensor Networks: Issues and Challenges,” arXiv, 2020, doi: 10.47277/ijcncs/1(7)7.

[3] Y. X. Li, Lian-Qin, and Qian-Liang, “Research on wireless sensor network security,” Proc. - 2010 Int. Conf. Comput. Intell. Secur. CIS 2010, pp. 493–496, 2010, doi: 10.1109/CIS.2010.113.

[4] M. A. Khan, G. A. Shah, and M. Sher, “Challenges for security in Wireless sensor networks (WSNs),” World Acad. Sci. Eng. Technol., vol. 80, no. 8, pp. 390–396, 2011, doi: 10.5281/zenodo.1334423.

[5] A. Rani and S. Kumar, “A survey of security in wireless sensor networks,” 3rd IEEE Int. Conf. , pp. 3–7, 2017, doi: 10.1109/CIACT.2017.7977334.

[6] M. A. Elsadig, A. Altigani, and M. A. A. Baraka, “Security issues and challenges on wireless sensor networks,” Int. J. Adv. Trends Comput. Sci. Eng., vol. 8, no. 4, pp. 1551–1559, 2019, doi: 10.30534/ijatcse/2019/78842019.

[7] H. Modares, R. Salleh, and A. Moravejosharieh, “Overview of security issues in wireless sensor networks,” Proc. - CIMSim 2011 3rd Int. Conf. Comput. Intell. Model. Simul., pp. 308–311, 2011, doi: 10.1109/CIMSim.2011.62.

[8] D. Martins and H. Guyennet, “Wireless sensor network attacks and security mechanisms: A short survey,” Proc. - 13th Int. Conf. Network-Based Inf. Syst. NBiS 2010, pp. 313–320, 2010, doi: 10.1109/NBiS.2010.11.

[9] M. Al and K. Yoshigoe, “Security and attacks in wireless sensor networks,” Netw. Secur. Adm. Manag. Adv. Technol. Pract., vol. 14, no. 2, pp. 183–216, 2011, doi: 10.4018/978-1-60960-777-7.ch010.

[10] A. Nelli and S. Mangasuli, “Wireless Sensor Networks: An Overview on Security Issues and Challenges,” Int. J. Adv. Eng. Manag. Sci., vol. 3, no. 3, pp. 209–214, 2017, doi: 10.24001/ijaems.3.3.10.