Journal of Theoretical and Applied Information Technology

15th October 2023. Vol.101. No 19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE COUNTERMEASURES OF WIRELESS SENSOR NETWORK THREATS IN IOT SYSTEM

JAWAHER ALSHEHRI[1] , ALMAHA ALHAMED[2], MOUNIR FRIKHA[3]

[1,2,3] Department of Computer Networks & Communications.

King Faisal University, CCSIT , Al Hofuf, Al Hassa 31982, Saudi Arabia,

E-mail: [1] 223001719@student.kfu.edu.sa , [2] 223000349@student.kfu.edu.sa, , [3] mmfrikha@kfu.edu.sa

ABSTRACT

Wireless sensor networks (WSNs) are a critical component in Internet of Things (IoT) systems, playing a crucial role in collecting and transmitting data. Wireless sensor networks (WSNs) often transmit sensitive data, such as personal information or industrial data. Without any proper protection, this transmitted data can be intercepted and exploited by malicious actors that use threats and attacks to achieve their goals. This paper explores the different types of threats faced by WSNs and proposes countermeasures to mitigate these threats. Through the implementation of these countermeasures, the security of WSNs in IoT systems can be strengthened, ensuring the safe and reliable transmission of data.

Keywords: *Wireless Sensor Networks, Threats, Attacks , Countermeasures, WSN Security, Iot Security*

1. INTRODUCTION

The Internet of Things (IoT) has revolutionized the way we interact with technology, leading to the development of a wide range of IoT systems that rely on wireless sensor networks to collect and transmit data. However, these networks are vulnerable to a range of threats, including eavesdropping, jamming, and denial-of-service attacks, which can compromise the security and integrity of the system. To address these threats, a number of countermeasures have been proposed and implemented, with varying degrees of success. However, the threats faced by wireless sensor networks in IoT systems continue to evolve and become more sophisticated. This research paper aims to provide an in-depth analysis of the various types of threats that can be faced by wireless sensor networks in IoT systems, and the countermeasures that can be taken to mitigate these threats. The paper will begin by providing an overview of wireless sensor networks and their role in IoT systems, before examining the various types of threats that these networks can face. The paper will then analyze the effectiveness of different countermeasures, including cryptographic techniques and physical security measures, in preventing or mitigating these threats.

1.1 WSN Overview

Wireless network sensors are small, low-power devices used to gather and transmit data in an Internet of Things (IoT) system. These sensors are designed to be energy-efficient and long-lasting, allowing them to operate for extended periods without requiring frequent battery replacement or recharging. They use a variety of wireless communication protocols, such as Wi-Fi, Bluetooth, Zigbee, or LoRaWAN, to transmit data to a gateway or a central server. Wireless network sensors are often used in various applications, such as smart homes, industrial automation, healthcare monitoring, and environmental monitoring. In smart homes, sensors can be used to detect motion, temperature, and humidity to control heating, ventilation, and air conditioning (HVAC) systems. In industrial automation, sensors can monitor machine performance, energy consumption, and inventory levels. In healthcare, sensors can be used to track patients' vital signs and medication intake, and in environmental monitoring, sensors can measure air quality, water quality, and soil moisture. For this reason, wireless network sensors are one of the most basic and dangerous methods that intruders use to access unauthorized information. This information may be for several reasons, including stealing personal data, disrupting sensor systems, and other risks that affect a negative and huge effect on IOT systems. Wherefore, wireless network sensors play a crucial role in IoT systems, providing real-time data that enables informed decision-making and increased efficiency across a broad range of industries and use cases.

1.2 Requirement for Security

The four security goals that are important for wireless sensor networks [19] include:

1. Confidentiality: Ensuring that data transmitted through the network can only be accessed by authorized entities, preventing eavesdropping or data theft.

2. Integrity: ensuring that data transmitted through the network is not altered or modified without the sender's knowledge, ensuring the authenticity and reliability of the data.

3. Availability: ensuring that the network and its data are accessible to authorized entities, preventing hackers from causing disruptions or denying access to the network.

4. Authentication: ensuring that only authorized entities can access the network, preventing unauthorized entities from gaining access, tampering with data, or conducting attacks on the network.

2. PRISMA METHODOLOGY

PRISMA is one of the research strategies used in the current article. It assists in the identification and reduction of duplicate research on countermeasures for wireless sensor network threats in IOT systems. PRISMA is used to define research investigations and articles in a few steps. The first step is to conduct a Google Researcher and Saudi Digital Library search using the keywords " wireless sensor network security AND IOT system," OR "WSN threats " AND "WSN attacks", "WSN countermeasure for threats " AND "IOT security". In the second step, some criteria are defined, with a particular emphasis on studies on the significance of countermeasures of wireless sensor network threats in IOT System and papers published between 2015 until 2023 Figure 1.

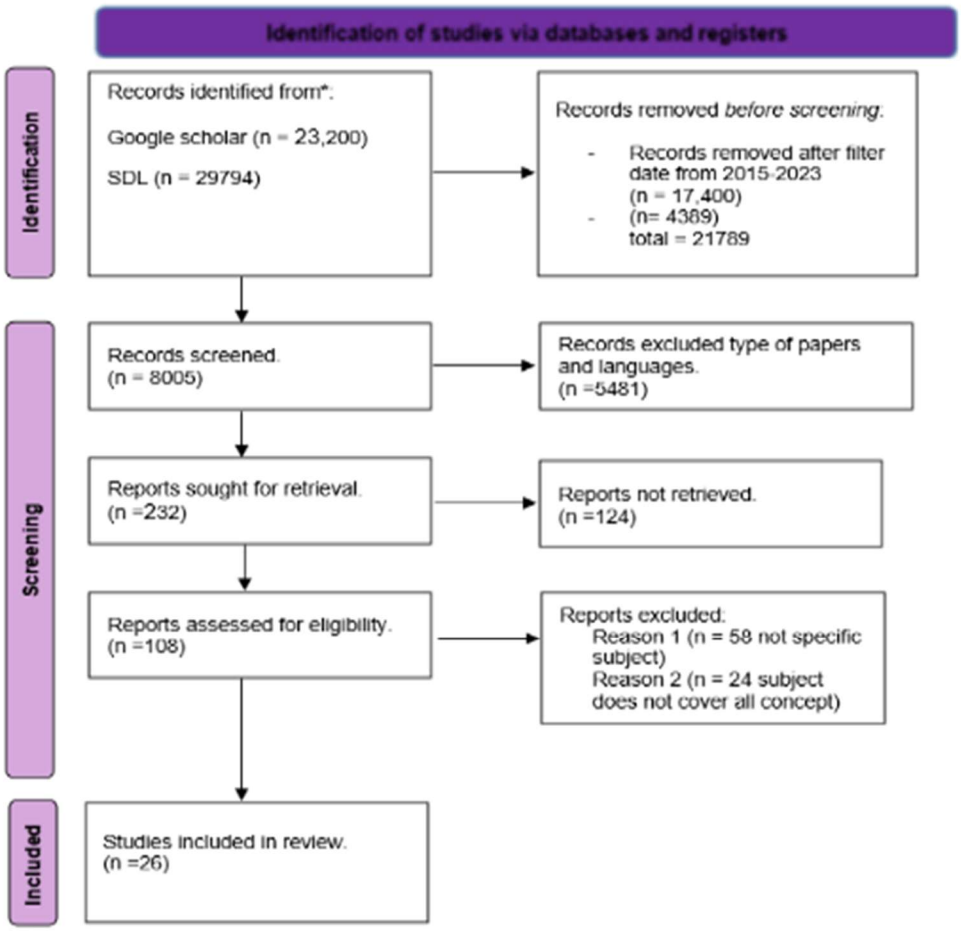

Figure 1: PRISMA Methodology

Figure 1: shows the Prisma diagram of the countermeasures of the wireless sensor network in IOT. The initial outcome was that the Saudi Digital Library and Google Scholar databases were able to identify 29,794 papers. In detail, the Saudi Digital Library's result is 6,794 papers, and Google Scholar's result is 23,200 papers. Papers were removed before the screening, and 17,400 Google Scholar papers and 4,389 Saudi Digital Library papers were excluded after a filtering date of 2015 to 2023. The total number of papers after screening is 8,005. Moreover, after filtering papers' types, 5,481 duplicate papers were removed. 124 of the 232 remaining papers were eliminated because they did not meet our research objectives. Furthermore, the total is 108 papers. However, there are 58 papers that are excluded because they are outside of our research's subject, and 24 papers are also excluded because their subject does not cover all the concepts. In the end, 26 papers were included and approved to study and review for our paper.

3. LITERATURE REVIEW

Abirami, et al. [1] covered the most attacks affected in OSI layers and addressed some countermeasures. In the physical layer, the attacks are malicious code attacks and reliability attacks, and the countermeasures are malicious node detection and isolation. In the data link layer, attacks are on data integrity, synchronization issues, and energy consumption. Using hashing, two-way authentication, and data encryption are the best practices for avoiding these attacks. In network layer attacks, wormholes, sinkholes, hello flood attacks, acknowledgement spoofing, node replication, sybil, black holes, and selective forwarding are the most common, and the countermeasures suggest using authentication methods, key management, active trust, and multi-path routing. Colloison and intelligent jamming are the most common attacks in the transport layer, and for countermeasures using mechinsim for error control, collision avoidance techniques, and flow control techniques, The last layer application layer attacks are basic jammers, eavesdropping, and DOS attacks, and the best practices for securing this layer are adaptive antennas and spread spectrum.

Shahzad,et al. [2] conducted a survey of threats and countermeasures for WSN. The authors defined four basic areas for the attack, which included threats to confidentiality, integrity, availability, and non-repudiation. Additionally, the attacks are divided into two types: active attacks and passive attacks. A passive attack is an attack on privacy that involves listening to communications silently without changing them. An active attack intercepts the connection and attempts to modify the message's content. The authors compared the most common attacks in WSN with the best corresponding countermeasures.

Arshad, et al.[3] conducted a survey of Sybil attacks with countermeasures in an IoT-based WSN. It explores some strategies for defensive ways against Sybil attacks, which can be exploited. The Sybil attack sends incorrect data using fake identities. Moreover, the Sybil attack can participate in the selection process by listening and sending its fake location during protocol handshakes. The suggested methods to prevent Sybil attacks are cryptographic methods, radio resource testing, RSSI localization, neighboring node information, trust, watchdog, RFID, clustering, time difference of arrival (TDOA) localization technique, random key pre-distribution, and geographic routing. The authors defined the open issues and obtained knowledge from WSN security analysis. The majority of current research focuses on encryption and RSSI methods, which account for 29\% of Sybil countermeasure solutions. The remaining solutions accounted for 14\%, 14\%, and 7\% of the total for trust, artificial intelligence, and encryption hybrid, respectively. Finally, 3\% and 4\% are allocated to rule-based anomalies and multi-kernel, respectively.

Najmi,et al.[4] reviewed the issues of privacy and security in IoT systems, including the crucial requirements, possible dangers, and tools to defend against risks. IoT architectures and protocols consist of four layers, such as the application layer, transport layer, network layer, and physical layer. The application layer is represented as an interface that provides services for users or applications. It is responsible for data formatting and depends on the HTTP protocol as well as MQTT and CoAP protocols that are able to deal with IoT environments. The transport layer is responsible for the data floods in terms of managing the services layer and storing the information flow from different layers in the database. The network layer is responsible for communication between smart devices, network devices, and servers, which allows data to pass between sensors. It's working with 3G, 4G, Wi-Fi infrared, and WiMAX. Moreover, a protocol of routing called RPL has been developed for lost networks and low power. The physical layer is considered a nursery for sensors that sense and

collect information about their surroundings, using WSNs and RFID to send and receive data. Despite the differences between each layer's attacks and countermeasures, As a result, they explained the details of the protocols used, the work based on them, the threats and security measures needed for the Internet of Things, and the tools and techniques needed to build a safe environment.

Ganesh et al. [5] defined the routing protocol, which is one of the protocols used for analyzing the WSN threats. It's responsible for removing potential threats and attacks from the routing structure and analyzing them in terms of security issues. Direct diffusion is considered a routing protocol for communication between sink and source nodes with random and mesh topologies. The main three attacks discussed in this paper are DoS attacks, data dropping or selective forwarding, and modifying routing information spoofing. A DoS attack starts with the attacker sending malicious code to the node or base station that affects three units such as the sensing unit, processing unit, and communication unit, which is to make it down. Modification and spoofing of routing information is done through directed diffusion routing, which is done on the basis of interest dissemination and the corresponding gradient institution. Malicious nodes can influence opposite nodes to route information through them by spoofing positive and negative reinforcements and false information events. An example is when a malicious node receives interest from the bottom station or a sink node. Dropping or selective forwarding of data is a malicious node that can influence the opposite nodes to route information through it by spoofing positive and negative reinforcements and false information events. The authors suggest countermeasures to avoid these attacks, including the fact that the directed diffusion protocol does not specify the identity of the sink node that generated the interest, making spoofing interests difficult. This could be addressed by specifying the identity of the sink node within the interest packet, and the data packets received from supply nodes would contain no information about the identity of the supply node, preventing malicious nodes from spoofing high data rates to the bottom station.

Farjamnia, et al.[6] reviewing and evaluating the techniques that are used to avoid wormhole attacks in WSN. The wormhole is an attack that can steal information and disrupt network performance. Discuss the most common attacks in WSN, such as selective forwarding attacks [21], black holes [22], Hello Flood [23], Sybil [23], and denial of service [24]. Additionally, she explained other attacks, such as the external and internal attacks in WSN, passive and active attacks, and mobile class versus laptop class attacks. External attack External attacks originate from nodes outside of a WSN. Moreover, external attacks could result in bogus data being injected into the network to take up network resources and launch denial-of-service (DOS) attacks, which could result in passive eavesdropping on data transactions [25]. Internal attacks occur when legitimate nodes of a WSN behave in unplanned or unauthorized ways, and an internal attacker is a licensed participant who seeks to disrupt operations or exploit organizational assets. Passive attacks involve eavesdropping on or observing packets exchanged within a WSN, while active attacks involve modifications to the data stream or creating a false stream. In mote-class (sensor-class) attacks, a few nodes with capabilities similar to those of network nodes are used by an adversary to attack a WSN. In laptop-class attacks, an adversary may cause far more damage to a network than a malicious sensor node by using more powerful devices like laptops, etc. This paper analyzes the advantages and disadvantages of various proposed models for detecting wormhole attacks. Concluded that each model is suitable for diagnosis, but there are disadvantages, such as waste of energy. The researcher proposed a suitable and efficient model for detecting wormhole attacks based on the proposed models. A wormhole attack poses a serious challenge for designing routing protocols, and it is unlikely that defense mechanisms can completely resist it. In the future, we aim to provide a recovery method to detect wormhole attacks in WSNs.

Kardi et al. [7] designed and implemented secure routing protocols for the researchers. The authors proposed a new classification for the potential attacks, which includes four categories of attacks: \\

- Based on the protocol stack
- Based on the capability of the attacker
- Based on the attack's impacts
- Based on the attack target,

The protocol stack covered five layers in WSN, such as the physical, data link, transport, and application layers. The capabilities of the attack include location and attacking device capabilities. For the attack based on impacts such as interruption, interception, modification, fabrication, reloading packets, and resource depletion. The targets of the attack include users, hardware, software, and information. In this paper, the authors

used the NS3 simulator as a simulation tool for effecting jamming and hello flood attacks in WSN by using the LEACH protocol [26]. The LEACH protocol is utilized by WSN to reduce energy usage. It enables nodes to create clusters and choose cluster leaders in a self-organizing way; data collection from the cluster heads' member nodes and transmission to the base station are their responsibilities [27]. The evaluation has depended on measures in terms of network lifetime, like alive nodes versus rounds, dead nodes versus rounds, stability and instability periods, and remaining energy versus rounds. According to simulation data, a jamming assault can cause the network lifetime to drop by more than 45%. This paper proposes a new taxonomy to categorize and analyze attacks on WSNs. It classifies and analyzes the most known attacks based on the proposed model and using the NS3 simulator. Future work will propose a new security method to counter these attacks.

Yang et al. [8] discuss the challenges and threats of underwater wireless sensor networks (UWSN). In addition, analyze the constraints and particularities of UWSN and the underwater environment. Defined the vulnerability of UWSNs to a wide class of threats and malicious attacks that affected communication and introduced the security requirements of UWSNs. Moreover, they discussed some specific security technologies and schemes. Concluding, future research should consider the energy consumption of excessive security schemes when designing security schemes to reduce energy consumption.

Islam, et al.[9] due to their simple construction, low computational requirements, and security flaws, wireless sensor networks (WSNs) have been applied in a variety of real-world applications. The characteristics, restrictions, DoS assaults, and defense mechanisms of WSNs have all been covered in this study. Most DoS defense measures concentrate on techniques like acknowledgments, encryption, and authentication, although these are resource intensive. The authors are urged to emphasize that instead of defending while under attack, researchers should concentrate on creating stronger preventative criteria at design time. Recently, a technology called Co-FAIS was put forth to protect the WSN from DoS attacks. The authors proposed to create fresh protection strategies that put less emphasis on limiting wireless sensor networks' ability to use resources.

Pundir, et al. [10] The survey includes specifics of the threat model applicable to the security of WSN and IoT-based communications. explains the security needs and many types of threats that could be used in WSN and IoT-based communication settings. It also presents a critical literature overview of recent intrusion detection algorithms for IoT and WSN contexts, as well as a taxonomy of security and privacy-preservation protocols.

Yousefpoor, et al.[11] explained Data aggregation methods are an appropriate way to decrease the consumption of energy in wireless networks, which face a lot of attacks because of their wireless links, which put them in danger every time from threats and attacks. So, it's so important to secure these data in the data aggregation process by providing some secure data aggregation systems depending on the network model, network topology, cryptography techniques, authentication mechanism, data recovery ability, and others that are effective in determining the problems and solutions in wireless networks.

Poornima et al. [12] proposed providing security systems in the IoT to prevent unauthorized access to information or other objects by protecting them from alterations or destruction. On the other hand, privacy systems have the right to control the collected information's usage. Some examples of IoT systems are healthcare, building a smart city with an advanced construction management system, and public and defense surveillance.

Chelli, et al.[13] expressed the wireless sensor network suffers from many difficulties such as limited energy, storage capacity, and unreliable communication which covered major aspects of wireless sensor network security, including problems, objectives, and attacks, as well as particular threats.

Butun et al. [14] explained that understanding passive and active attacks and CIA (confidentiality, integrity, and availability) associated defense mechanisms by inserting Internet access capability in sensor nodes will help pave a secure path toward the proliferation and public acceptance of IoT technology.

Sinha et al. [15] reviewed IoT cybersecurity technologies and cyber risk management frameworks. A four-layer IoT cyber risk management framework was developed. The IoT

cyber risk assessment layer identifies, quantifies, and prioritizes IoT cyber risks. Also, the authors introduced an optimal linear programming method and an illustration of the IoT cyber risk assessment with an LP model.

Elsadig et al. [16] provided a full description of WSN's constraints, vulnerabilities, and security attacks. Moreover, the countermeasures used to face the WSN attacks are still facing researchers as they try to find effective solutions to secure WSN applications.

Keerthika et al. [17] focused on the different types of active and passive security attacks in wireless sensor networks to design effective countermeasures for secured communication and identify the most vulnerable attacks in the communication and defensive mechanisms to encounter the attacks in WSN.

Vikhyath et al. [18] mentioned addressing the security issues and challenges of WSNs and identifying the threats and security mechanisms of wireless sensor networks.

Inayat et al. [19] covered the key security objectives, threats, and threats that are related to the layers of WSNs, along with their countermeasures, which are the sensor nodes set up to solve problems that cause the weak on WSNs to face complex threats or destruction.

Singh et al. [20] proposed applying the security of wireless sensor networks by analyzing in-depth threats to wireless sensor networks and some countermeasures against these threat.

4. METHODOLOGY

Wireless sensor networks (WSNs) are susceptible to various types of security threats and attacks due to their distributed nature and limited resources. Wireless sensor networks typically have limited resources in terms of processing power, memory, and energy. This is why wireless sensor network threats continue to be a real problem. This makes it challenging to implement complex security mechanisms and protocols, leaving these networks more susceptible to attacks. Some wireless sensor network vulnerabilities allow attackers to gain unauthorized access to the network, compromise the integrity of data and disrupt the network's normal operation, wireless signals can be easily intercepted by attackers who are within range, making it easier for them to launch attacks on the network. Attackers can use several methodologies to launch attacks on WSNs. The attacks depend on three types that the attacker exploits to launch the attack which are the type of layers [1], and if the attack is passive or active attacks [2], lastly an attacker's capability, impact, and target [7].

In this section, we will highlight deeply the most attacks and threats that affected WSN and the countermeasures for preventing and avoiding these attacks. For each attack, there are some countermeasure techniques to protect from the attacks. Here are a few common methods used in WSN attacks depending on attack type:

4.1 Attacks & Threats Types

As mentioned earlier, the attacks are categorized according to their type, the type of attacker, and the network layer. Before reviewing some wireless network sensor attacks on the Internet of Things, the types of attacks will be explained clearly.

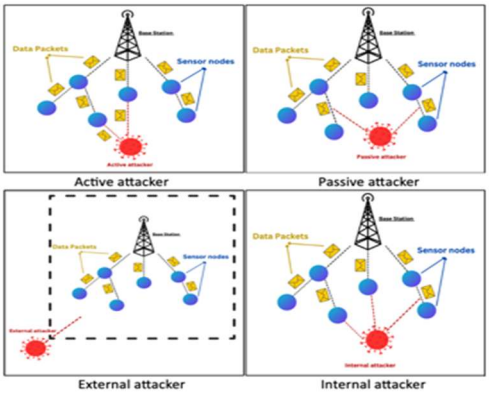

Figure 2: Types Of Attacks

4.1.1 Goal-Oriented Attacks

Points to active and passive attacks. Fig. 2 represents active and passive attacks; passive attacks monitor unencrypted traffic and look for sensitive information that can be used in other types of attacks without knowing the victim, which sneaks into the data packet transmission path. Unlike passive attacks, active attacks represent attacks that are no longer passive but take active actions to achieve control over the network by sneaking to the sensor node. [13]

4.1.2 Internal/External-Oriented Attacks

Categorized attacks on wireless sensor networks can be internal or external. Fig. 2 represents the external and internal attacks. The external attacks are attacks that occur outside the scope of the network or path. Also, it causes dangerous eavesdropping and consumes network resources for outside data transmission processes. Unlike external attacks, internal attacks are launched within the network. Internal attackers launch different types of attacks, such as modification or eavesdropping, that prevent data transmission to the main station.

4.1.3 Layer-Oriented Attacks

The wireless sensor network is organized in layers. Fig. 3 represents each layer with its attacks and countermeasures, which are [1] Physical Layer Attacks: An attacker can continuously transmit radio signals on a wireless channel, which causes denial-of-service attacks at this layer. Data Link Layer Attacks: At this layer, coordinating neighboring nodes to access shared wireless channels and providing link abstraction to upper layers. Network Layer Attacks: focusing on the complete disruption of routing information and therefore the whole operation of an ad-hoc network, like DoS attacks at the network layers of WSNs Transport Layer Attacks: making new connection requests until the resources required by each connection are exhausted repeatedly or reach a maximum limit. Application Layer Attacks: overwhelming the network nodes, which causes the network to forward large volumes of traffic to a main station.

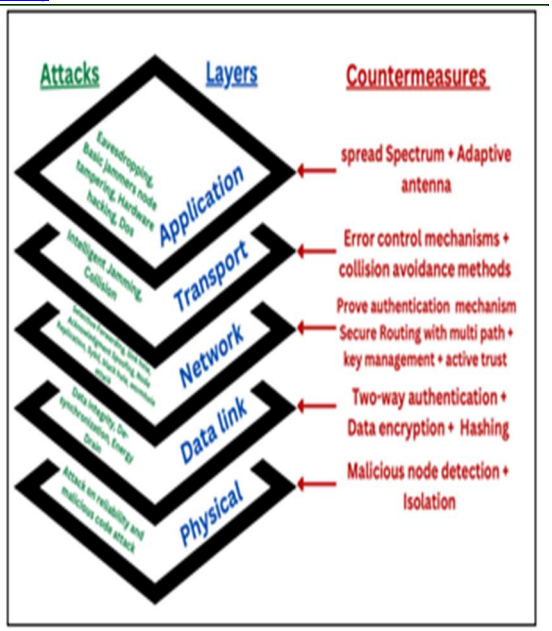

Figure 3: Layers-Oriented attacks

4.2 Common WSN attacks

The wireless sensor network on the Internet of Things refers to a group of dispersed and dedicated sensors for monitoring the physical conditions of the environment and recording it. After that, it passes these data in a collective way via a wireless network. So, when the base station discovers un-normal passing between sensor nodes, it tries to record and discover what is it. Mostly, these are attacks trying to steal, alter or destroy the sensor nodes. And that's what will be highlighted. In this section, some attacks that highly affect the sensor nodes and their countermeasures are explained. Wireless sensor network attacks will be divided depending on the type of attack, whether it was an active or passive attack, or whether the attack was external or internal. Also, in any of the layers that affect by the attack negatively.

The following attacks are active external attacks and threaten availability requirements in a physical layer:

1-Jamming attacks: Fig (4) represents a jamming attack is a kind of Denial-of-Service (DoS) attack. It disrupts the WSN functions and generates wireless frequency signals in physical channels to jam legitimate signals and cause a denial of Service by blocking any communication in the same physical channel within its transmission range [16].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

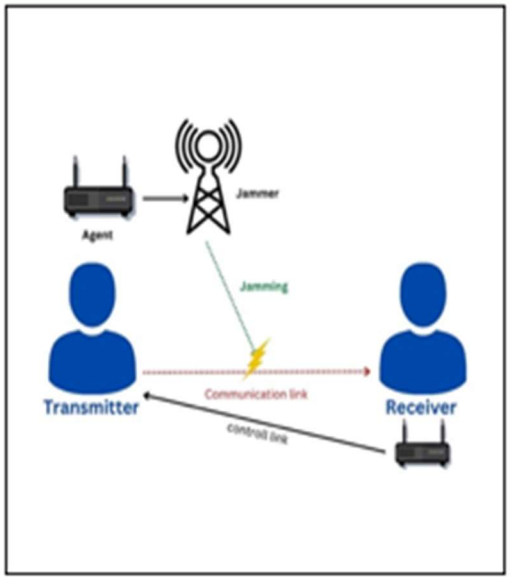

Figure 4: Jamming Attacks

The following attacks are considered active external attacks and threaten availability requirements in a network layer:

2-Black Hole attack: Fig(5-A) represents the black hole encourages the other nodes to send their own data packets through these malicious nodes. In this case, the black hole arrives at all the data packets that are received from other sensor nodes and delete them. [11]

3-Sink Hole attack: Fig(5-B) represents this attack as a kind of black hole attack which is active and external. The difference is that the attacker knows the position of the sink nod. It is more dangerous and destructive than a black hole attack because the malicious node tries to convince all sensor nodes to select it as the next hop to reach the sink node. The sinkhole node shows this fake route has optimal parameters such as a shorter distance to the sink node, less traffic, and the best link quality. [11]

4-Wormhole attack: in the wormhole attack case in Fig (5-C), sharing two malicious nodes establishes a wormhole channel between themselves and demonstrates a wormhole attack. Inside the worm tunnels, there are two far nodes and establish between them a tunnel to attract other nodes by saying that is an optimal route to another part of the network. The attacker can intercept the communications between sensor nodes, copy data packets, and manipulate network traffic.

5-Selective forwarding: also called the gray hole. The gray hole node removes some received data packets and forwards other data packets. This attack is implemented in two ways: removing a special type of data packet or removing data packets that have a specific destination as shown in Fig (5-D).[11]

6-Sybil attack [3]: as shown in Fig (5-E), the Sybil attack is to send fake data packets and disable the entire network. Malicious nodes are arranged in a specific area. Also, the malicious nodes are dispersed throughout the network, so it is more difficult to detect this attack.[11]

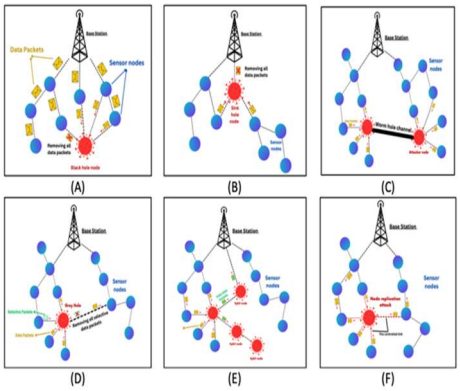

Figure 5: Active External Attacks – Availability

The following attacks are considered active external attacks and threaten integrity requirements in a network layer:

7-Node replication attack: as shown in Fig (4-F), This attack targets data integrity, which is the attacker copies the memory of a sensor node. After that, the attacker can inject fake data packets into the network, remove data packets, and send modified data packets.

8-Packet injection: the attacker can inject fake data packets into the network to interrupt the data transmission process. Fig (6-G) represents the attacker forges valid messages on the network which cannot be easily distinguished from valid data packets by injecting fake data packets.

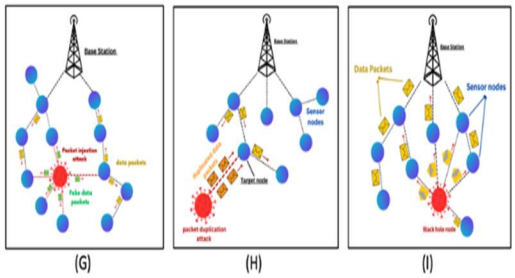

Figure 6: Active external attacks- Integrity

9-Packet duplication: the malicious node duplicates a valid data packet and forwards it continuously to the target node to drain its resources and interrupt the network performance. As shown in Fig (6-H).

10-Packet alteration: in Fig (6-I), the attacker changes the data packets exchanged between the sensor nodes and sends the modified data packets on the network.

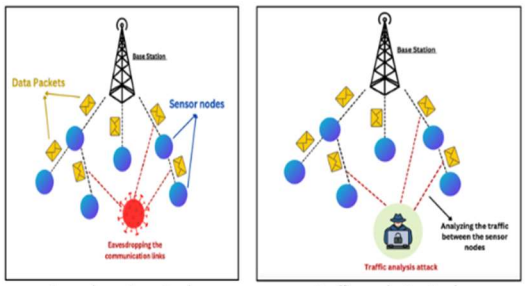

Figure 7: Eavesdropping Attack & Traffic Analysis Attack

The following attacks are passive, and external attacks, and threaten data confidentiality and privacy requirements in the physical and application layer:

11- Eavesdropping attack: the attacker tries to figure out the confidential data of sensor nodes by eavesdropping on wireless communication links. As shown in Fig (7).

The following attacks are passive, and external attacks, and threaten data confidentiality and privacy requirements in a network layer:

12- Traffic analysis attack: the attacker analyzes the activities of a sensor node and seeks to explore traffic information, network topology, transferred message pattern, message length, message waiting time in the buffer, and so on. As shown in Fig (7).

4.3 Contributions of countermeasures

Due to WSN vulnerabilities, WSNs may become targets of various attacks, including node compromise, eavesdropping, message tampering, and denial-of-service attacks. Therefore, countermeasures must be applied to ensure the security and privacy of WSNs. Contributions to wireless sensor network countermeasures include the development of encryption algorithms, authentication protocols, and intrusion detection systems. These countermeasures can help secure the transmission of data between nodes, authenticate nodes, and detect and prevent malicious activities. Here are some common countermeasures:

4.3.1 Spread Spectrum Technologies

Spread spectrum refers to the system developed originally for military applications to provide secure communications by spreading the signal over a large frequency band. Any other signal easily jams these narrow signals in the same band. Spread-spectrum technologies can be used to protect against jamming attacks. [15]

4.3.2 Sign-Share

The black hole and sinkhole can be detected using two techniques, which are the data-slicing process and the digital signature. In this countermeasure, each sensor node divides its data into several slices, then encrypts and signs each slice, and finally transfers them to different aggregator nodes in the cluster.

4.3.3 Authentication Mechanisms

Authenticating the user with a specific authentication technology, such as a username and password or one-time password, Wormholes and selective forwarding attacks can be detected by using authentication mechanisms. [17]

4.3.4 A REWARD Scheme

Proposed as a countermeasure to detect blackhole attacks against WSNs, in which the detected black holes are avoided. Also, using the honeypots to attract and catch black-hole attack performers by creating dummy Route-Request (RREQ) packets.

4.3.5 Efficient healthcare data aggregation (EHDA)

A scheme is presented for homogeneous WSNs and sensor nodes that are arranged in a hierarchical topology in which the sensor nodes transmit the data packets to aggregator nodes and then to the base station Fog server. The EHDA method uses a symmetric key cryptography technique to secure communication links between sensor nodes. The EHDA scheme has three phases, which are: the local data transmission phase, the data packet receipt phase, and the data extraction phase. There are some attacks that EHDA can detect and prevent, such as eavesdropping, traffic analysis, Sybil, packet alteration, and packet injection. Eavesdropping If an attacker eavesdrops on communication links, it cannot find out the contents of data packets. The same is true with traffic

analysis; if an attacker analyzes network traffic, it cannot threaten privacy or data confidentiality. But the attacker may obtain information such as node ID, location of nodes, and FoG server location. Moreover, to counteract the Sybil attack, each sensor node must insert a hash value in the data packet so that the nodes can detect fake data packets in the network. If a fake data packet is detected, the node rejects it. In a flooding attack, when nodes receive a data packet, they first check the timestamp inserted into it to determine whether it is a duplicate or not. If the data packets are duplicates, then the nodes reject them. In packet alteration and packet injection, each node can detect fake data packets or modified data packets by checking the hash value inserted into the data packet [11].

4.3.6 The Multi-Functional Secure Data Aggregation Scheme (MODA)

MODA uses as a countermeasure encryption technology to provide the security of messages exchanged between sensor nodes. For implementing MODA, a homogeneous WSN is applied by arranging the sensor nodes in a tree topology to transmit the aggregated data to the sink node. The MODA passes five phases to prevent the attack which are mapping, encoding, encryption, aggregation, and decryption [11].

4.3.7 IETF

Pproposed a protocol named 6TiSCH that used time-slotted channel hopping (TSCH) MAC with IPv6 addressing. The IETF contains secure communication of MAC layer frames, which has no benefit from any kind of eavesdropping, packet capturing, or desynchronise attack [14]. In addition, there are some general countermeasures that must be ensured during data transmission to prevent attackers from achieving their goals. This may reduce the attack through such as countermeasures.

4.3.8 Key Management

Cryptography and key management are key management mechanisms that enable sensitive information to be stored or delivered in unsecured networks such as the underwater acoustic channel. Unfortunately, existing cryptography and key management mechanisms are suffering from problems such as cipher text expansion and computational complexity. Digital signatures are usually used for message authentication, which increases the length of messages and causes energy consumption on transmission and computation.

4.3.9 Synchronization Security

Synchronization is essential for underwater applications and scheduling MAC protocols, but security protocols proposed for WSNs are unsuitable for UWSNs. To defend against time synchronization attacks, cryptographic techniques can be used, but countermeasures against delay attacks proposed for WSNs are not applicable to UWSNs.

4.3.10 Routing Security

Routing security consists of basic transport and connectivity security mechanisms applied to routing protocols and individual nodes. It involves two aspects: secure routing and secure data forwarding. Secure routing requires nodes to cooperate to share the correct routing information, while secure data forwarding requires data packets to be protected from tampering. Recent research has been presented to provide routing security for UWSNs [18]. Countermeasures can also help mitigate power consumption in all forms, which is a major concern for WSNs operating in resource-constrained environments. In conclusion, WSN countermeasures have made significant contributions to the development of secure and reliable wireless sensor networks, enabling deployment of WSNs for critical applications and providing a secure communication platform for the Internet of Things (IoT).

5. DISCUSSION & IDEA PROPOSAL

As many attacks and threats affect the WSN's performance, we suggest to creating a platform that is responsible for monitoring, managing, tracking and taking action against the attacks on all sensors on the platform. All sensors that are used in the platform will be added by IP, and then they will appear on the main view, which shows the performance of sensors and all details that are needed, such as date, time, alert, etc. The platform will use configuration techniques to know the attack type and block attempts from the attacker. For example, if the platform protects sensors from DoS attacks, it will add configuration to ICMP request. Also, if there is any change in behaviors, it should be alerted in the view and the device temporarily turned off until verification. The advantage of this

platform is that it can add other features. For example, by extracting a daily report or at any time showing the general performance of these sensors and whether they were subjected to any type of attack, this feature helps information security specialists take more preventive measures and make better decisions for improved security. Adding configurations to take the action without the need for user intervention to control it is necessary to ensure that the action is taken in the shortest possible period and to avoid damage. Through this proposal, we expect the speed of taking the appropriate action and the ease of remote control and monitoring, thus preserving the work of these sensor networks for a longer period and in a healthy way. Additionally, this proposal is useful in managing, reducing, and preventing some threats, but with rapid technical development, more threats and attacks will appear as well, so It will need to innovate and develop the work of platforms or the hardware of software that is used in security protection for the WSN. This point needs more research and investigation to be able to improve performance for WSN protection.

Due to the significance and widespread usage of wireless sensor networks in the present and the development of new technologies, this study examines the most prevalent security risks that influence them. The dangers rank among the most noticeable dangers that are present in all sorts of networks, not only sensor networks. All of the information that has been collected demonstrates the safeguards against these dangers and how to lessen and avoid them. It facilitates information access via an integrated search for the researcher and the user. From our individual perspectives, we see the start of limiting and preventing these threats and intrusions by developing a platform to manage this kind of network, which will significantly reduce these threats. This platform should include all addresses of sensor networks used in the organization or the specified area, making it easier to monitor, analyze, and take appropriate action. A thorough security team is needed to identify and program this platform in order to take the proper action depending on the circumstances. This entails analyzing the majority of threats in order to identify all kinds, determine which layer will be affected, and manage the configuration of each breach that may be revealed for examples [27] [28] depends on one technique as cryptography for secure WSN.
In [27], they use cryptography techniques for secure communication in WSN. Its simulations tested the implementation of AES and RSA algorithms on an IT-SDN platform, resulting in AES being more efficient in resource usage and energy consumption. However, the AES algorithm's security is not guaranteed, so PKC methods like RSA and ECC may offer a better trade-off. New platforms, considering SDWSN's nature, could combine symmetric and asymmetric solutions for a clear cryptography solution. Cryptography For WSN security services to be effective, the proper cryptography mechanism for sensor nodes must be chosen. Public-key cryptosystems are thought to be too complex for sensor nodes with limited resources. However, several studies have demonstrated that it is doable to use the correct selection of algorithms and associated parameters, optimization, and low-power techniques to apply public key cryptography to sensor networks. These cryptographic techniques were developed to overcome the limitations of symmetric-based methods and improve performance. Small sensor nodes can use RSA and Diffie-Hellman based on elliptic curve cryptography, and the results demonstrate that good outcomes can be obtained with fewer keys. The amount of data communicated and stored is decreased, as is the computation time. Elliptic curve cryptography, a particular asymmetric technique using public-key cryptosystems, shows promise for addressing security needs in WSNs [28]. It's play role for protect but still need a new platform including countermeasures for most of threats.

6. CONCLUSIONS

This research paper has provided an in-depth analysis of the various types of threats that can be faced by wireless sensor networks in IoT systems. Threats such as data tampering or injection can lead to incorrect data analysis, potentially causing serious consequences in critical applications. Also, protecting WSNs from threats prevents unauthorized entities from accessing the network which can result in unauthorized control or manipulation of the sensors, leading to compromised data and potential misuse. The findings have highlighted the importance of developing and implementing effective countermeasures to protect wireless sensor networks in IoT systems. To address these threats, several countermeasures have been proposed and analyzed. The effectiveness of these countermeasures has been evaluated in terms of their ability to prevent or mitigate the various types of threats that wireless sensor networks face. The research conducted in this paper has also

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

highlighted the need for continued efforts in developing and implementing effective countermeasures to protect wireless sensor networks in IoT systems. The findings of this research paper emphasize the importance of developing and implementing effective countermeasures to protect wireless sensor networks in IoT systems, as the threats faced by these systems can have serious consequences if left unchecked. By implementing the countermeasures outlined that enhance more security of WSNs in this research paper, organizations can help to ensure the security and integrity of their wireless sensor networks and safeguard sensitive data and critical systems.

Based on the analysis of attacks and countermeasures in wireless sensor networks (WSNs), the paper presented a comprehensive argument regarding the security challenges and potential solutions in this domain. The main argument of the paper revolves around the critical need for enhanced security in WSNs due to their vulnerability to sophisticated attacks. It highlights the potential consequences of successful attacks, including unauthorized data access, network disruption, and manipulation of sensor readings. Moreover, it emphasizes the significance of enhanced security to ensure the integrity and reliability of the collected data. The paper outlines several countermeasures to mitigate the identified attacks, such as encryption algorithms, authentication protocols, intrusion detection systems, and secure routing protocols. But, Numerous issues and challenges in WSNs are still open and wide. Such as:

- To what extent do the socio-cultural and political contexts of different regions influence the motivations behind attacks on wireless sensor networks, and how might this impact the efficacy of countermeasures designed based on specific regional contexts?
- What are the potential ethical implications of deploying wireless sensor networks for surveillance purposes, considering their potential vulnerabilities to attacks?
- How might emerging technologies and advancements, such as quantum computing, impact the effectiveness of current countermeasures against attacks on wireless sensor networks?
- How can the role of human decision-making and human error in deploying and managing wireless sensor networks impact their effectiveness against attacks?

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Type of attack	Performance-Oriented Attacks	Layers	Some Common Attacks	Target	Countermeasures
Active	External	Physical	Jamming attack [15]	Availability	Spread spectrum techniques such as FHSS,DSSS[15]
		Network	Black Hole Sink Hole Wormhole Gray hole Sybil	Availability	Sign-share Authentication mechanisms Efficient Healthcare data aggregation (EHDA) [11] Geographic routing protocol [2]
			Node replication	Integrity	Authentication through BS[2] Location confirmation by the witness nodes [2]
		Application	Malware attack		Firewalls and anti-virus
	Internal-External	Physical	Malicious code attack [16] DDoS Attack [16]	Availability	Spread spectrum techniques
		Network	Packet injection Packet duplication Packet alteration	Integrity	Efficient Healthcare data aggregation (EHDA) [11]
		Transport	Desynchrony attack [18]		IETF
Passive	External	Physical	Eavesdropping	Confidentiality	Cryptographic technique Efficient Healthcare data aggregation (EHDA) [11]
		Data Link	MAC spoofing Network injection [15]	Integrity	Use ARP packets. Reprogramming network devices
		Network	Traffic analysis	Confidentiality and privacy	Efficient Healthcare data aggregation (EHDA) [11]
		Transport	TCP or UDP flood [15]	Availability	Increasing the TCP backlog and reducing the SYN timer. Reducing the UDP packets response rate.
		Application	Eavesdropping SMTP attack [15]	Confidentiality	Firewalls and anti-virus
	Internal	Physical	Node tampering	Confidentiality	Tamper proof packing Effective key management schemes
		Data Link	Collision	Confidentiality	Error correction code
		Application	SQL injection [15]	Integrity	Firewalls and anti-virus

FIGURE 7: Summary Of Countermeasure

Table 1: Papers Contributions

Author	Title	Attack	Countermeasure	Contribution
Abirami, et al. [1]	A Complete Study on the Security Aspects of Wireless Sensor Networks	Malicious code attack reliability attack, data integrity, synchronization issues, energy consumption, wormhole, Sink Hole, Hello Flood Attack, Acknowledgement Spoofing, Node Replication, Sybil, Black Hole, Selective Forwarding, collision, intelligent jamming, basic jammers, eavesdropping tampering with nodes, hardware, and Dos.	Malicious node detection and isolation, data encryption, two-way authentication, hashing, authentication method must be proven secure, key management, active trust, and multi-path routing, mechanisms for error control, collision avoidance techniques, and flow control techniques, adaptive antenna, and spread spectrum.	Discussed in detail the attack and countermeasure that related to OSI layers such as physical, data link, network, transport, transport and application layers, and the suggestion to use intrusion detection and prevention systems as prevention methods for these attacks.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Shahzad ,et al. [2]	A Survey of active attacks on wireless sensor networks and their Counter measures	Passive attacks include: eavesdropping , traffic analysis. Active attacks include: DoS attack , masquerade attack, replay Attack , selective forwarding , node replication , wormhole attack, sybil attack, sink hole attack, rushing attack and modification of messages	For the countermeasure of DOS attack , prevent network broadcasts from sensor nodes . Masquerade attacks use solid authentication for prevention. The replay attack uses spending session tokens as countermeasures. Selective Forwarding countermeasures such as multi-path routing and local monitoring Node replications depend on authentication through the base station and a location-oriented key. Sinkhole attack: perform geographic routing protocol as a countermeasure. Modifications to messages utilize link layer authentication.	Provided a summary of the most significant attacks that affected confidentiality, integrity, availability and non-repudiation, with an overview of the best practices to avoid active attacks.
Arshad, et al.[3]	A survey of Sybil attack counterm easures in IoT-based wireless sensor networks	Sybil attack	There are some countermeasures for Sybil attacks, such as cryptographic methods, radio resource testing, RSSI localization, neighboring node information, trust, watchdog, RFID, clustering, time difference of arrival (TDOA) localization technique, random key pre-distribution, and geographic routing.	The survey addressed many defense strategies for preventing the Sybil attack conducted from various application domains against the IoT-based WSN. The working principles, advantages, and limitations of each countermeasure category have been increased.
Najmi,e t al.[4]	A survey on security threats and counterm easures	Jamming in WSN , Physical damages, social engineering , node tempering , traffic analysis attack, RFID spoofing , RFID cloning, sinkhole	Secure booting , secure physical design , device authentication , risk assessment , routing security , routing protocol , hello flood	Discusses processes, risks security measures, and tools that provide protection while developing a secure environment as they relate to security and privacy issues in IOT.

	in IoT to achieve users confidentiality and reliability	attack, malicious code injection , sleep deprivation attack , data security third party relationships ,virtualization threats, DOS , malicious script , viruses, trojan , phishing and cryptanalysis attack.	detection , data privacy , web application scanner , fragmentation redundancy, data security , access control list , firewall and anti-viruses.	
Ganesh, et al.[5]	Analysis of Wireless Sensor Networks Through Secure Routing Protocols Using Directed Diffusion Methods	Denial of Service attacks , Modification and spoofing of routing data and Dropping or selective forwarding of knowledge & Utilizing encoding at the link layer is one of the useful actions that may be made to thwart a number of the attacks.	Utilizing encoding at the link layer is one of the useful actions that may be made to thwart a number of the attacks.	Identifying a new method, the directed diffusion protocol, as a countermeasure that is used for analyzing attacks that affect WSN.
Farjamnia, et al.[6]	Review of the Techniques Against the Wormhole Attacks on Wireless Sensor Networks	Wormhole attack	Locating of sensor nodes , trust-based security mechanisms and RSSI	Clarify WSN works, and how can detect an attack node, and how to link with the other node. Moreover, the authors explain some of the challenges such as affected on the database, timeliness and lack of reliability. The some of solutions suggested for detection of the attacker's node are positioning, geographic distance, validation via ID, and food signaling.
Kardi, et al.[7]	Attacks classification and security mechanisms in Wireless Sensor Networks	The attacks have been categorized into four parts, including: attack based on the impact, target, stack and capability of the attacker	Symmetric and asymmetric cryptography in WSNs , hybrid cryptography in WSNs , elliptic curve cryptography in WSN , management of encryption keys in WSNs, symmetric patterns, asymmetric patterns and encryption key in hybrid patterns	This paper proposes a new taxonomy to categorize and analyze attacks on WSNs. It classifies and analyzes the most known attacks and presents security methods and protocols to manage and distribute encryption keys. Future work aims to propose a new security method to counter these attacks.

Yang, et al.[8]	Challenges and Security Issues in Underwater Wireless Sensor Networks.	Compromise attacks , repudiation attacks , routing attacks and DoS attacks	Key management, intrusion detection, trust management , localization security, synchronization security and routing security	UWSNs are vulnerable to a wide class of security threats and malicious attacks, so security requirements are introduced and security technologies and schemes discussed.
Islam, et al.[9]	Denial of Service Attacks on Wireless Sensor Network and Defense Techniques	Node tampering , interrogation attacks, spoofng attack , synchronization flood attacks , de synchronization attacks , content attacks overwhelming the sensors and path-based-dos attack	Spread spectrum communication, error correcting codes, mac layer authentication, packet authentication , collaborative hierarchical model, multi-path routing, geo-location and energy aware protocol, reducing connections , client puzzle , full packet authentication, • sensor modification and one way hash chain	Wireless sensor networks are easy to implement and effective due to their simple construction and low computational resources. However, they are also vulnerable to DoS attacks due to their limiting factors. This paper discusses different types of DoS attacks and their prevention techniques, which are resource consuming. Future research should focus on developing stronger prevention criteria in design time, such as Co-FAIS, to defend against DoS attacks on the WSN.
Pundir, et al. [10]	Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges	Eavesdropping, traffic analysis, replay attack, man-in-the-middle attack, impersonation attack	Some of security protocols used in WSN include : User authentication/device authentication, access control/user access control , privacy-preservation, and intrusion detection	This survey article discusses the security requirements and attacks possible in WSN and IoT based communication environments. It provides a taxonomy of existing intrusion detection schemes and comparisons of them, including detection rate, false positive rate, and applicability. It also identified future research challenges in the design of intrusion detection schemes and other security protocols.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Yousefpoor, et al.[11]	Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review	Black hole attack, Sinkhole attack, Wormhole attack, Selective forwarding attack, Sybil attack, Flooding attack, Node replication attack, Packet injection attack, Packet duplication attack, Packet alteration attack, Eavesdropping attack, Traffic analysis attack.	The multi-functional secure data aggregation scheme (MODA), the efficient healthcare data aggregation (EHDA), Sign-share.	Data aggregation methods were explained as an appropriate way to decrease energy consumption in wireless networks, which face a lot of attacks because of their wireless links.
Poornima et al.[12]	Security and Privacy in IoT: A Survey	Depend on confidently, integrity and availability attacks	An object authentication method, an access control system, Checksum, and Cyclic Redundancy Check (CRC) mechanisms.	Providing security systems in the IoT to prevent unauthorized access to information or other objects by protecting them from alterations or destruction was proposed.
Chelli, et al.[13]	Security Issues in Wireless Sensor Networks: Attacks and Counter measures	Depend on Goal-Oriented, Performer-Oriented, and Layer-Oriented Attacks	Apply public key cryptography in sensor networks by using the appropriate algorithms and techniques like RSA and Diffie-Hellman based on the elliptic curve cryptography.	The wireless sensor network suffers from many difficulties such as limited energy, storage capacity, and unreliable communication. Major aspects of wireless sensor network security, including objectives, attacks, and threats, were covered.
Butun, et al.[14]	Security of the Internet of Things: Vulnerabilities, Attacks and Counter measures	Eavesdropping Node Destruction Node Malfunctioning Node Outage Traffic Analysis	Link-layer encryption, authentication using shared keys, SNEP (Secure Network Encryption Protocol), A sensor Ware communication multicast model in which 3 different levels of link-layer encryption are provided by using the RC6 algorithm was proposed.	The dependence on passive and active attacks and CIA (confidentiality, integrity, and availability)-associated defense mechanisms by inserting Internet access capability in sensor nodes was explained.

Sinha, et al.[15]	Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A Survey	Physical layer, Network layer, Mac layer, Transport layer, and Application layer attacks	Cryptographic techniques, spread spectrum techniques, VPNs, Firewalls, Anti-viruses.	A four-layer IoT cyber risk management framework was developed. The authors introduced an optimal linear programming method and an illustration of the IoT cyber risk assessment with an LP model.
Elsadig, et al.[16]	Security Issues and Challenges on Wireless Sensor Networks	WSN Internal/External attacks and layers based attacks classification like eavesdropping, node tampering, n ode replication, black hole, sybil attack, worm attack, sinkhole.	SET-IBS and SET-IBOOS are two protocol can achieve the security requirements in Cluster WSN in better than current protocols, statistical detection approach to detect WSNs' DoS jamming attack, A pre-key distribution scheme for public key cryptography to be applicable, An Agent-based Trust Model (ATSN) for WSNs were proposed.	The countermeasures used to face the WSN attacks, which are still facing researchers trying to find effective solutions to secure WSN applications, were introduced.
Keerthika, et al.[17]	Wireless Sensor Networks: Active and Passive attacks - Vulnerabilities and Countermeasures.	Depend on active/ passive attacks; Dos, jamming, physical, tampering, routing attacks, eavesdropping, traffic analysis.	Cryptographic techniques, spread spectrum, jamming techniques, authentication mechanisms, privacy analysis.	The different types of active and passive security attacks in wireless sensor networks were focused on to design effective countermeasures for secured communication and identify the most vulnerable attacks in the communication and defensive mechanisms to encounter the attacks in WSN.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Vikhyath, et al.[18]	Wireless sensor networks security issues and challenges: A survey	Jamming, Node tampering, collision, selective forwarding, sinkhole, wormhole, hello flood, sybil attacks	Spread spectrum techniques, cryptography-based authentication, key management, SYN cookies, Data aggregation.	Addressing the security issues and challenges of WSNs and identifying the threats and security mechanisms of wireless sensor networks were mentioned.
Inayat, et al.[19]	Wireless Sensor Networks: Security, Threats, and Solutions	Physical layer; jamming attack, tampering attack, sybil attack. Link layer; collision, exhaustion, interrogation attack. Network layer; blockhole, sybil attack, wormhole attack. Transport layer; flooding, desynchronization. Application layer; SQL injection, SMTP attack, and malware attack.	Spread spectrum techniques, authentication, and encryption mechanisms, anti-viruses and firewalls.	The key security objectives and threats that are related to the layers of WSNs, along with their countermeasures on WSNs to face complex threats or destruction, were covered.
Singh, et al.[20]	Wireless sensor network: attacks and countermeasures	Physical layer; jamming attack, tampering attack, sybil attack. Data Link layer; collision, exhaustion, spoofing, desynchronization. Network layer; Dos, sybil attack, wormhole attack. Transport layer; flooding.	Channel hopping and blacklisting, CRC, sending of dummy packet, two-way authentication, three-way handshake.	Applying the security of wireless sensor networks by analyzing in-depth threats to wireless sensor networks was proposed.

FUNDING

This work was funded by King Faisal University, Saudi Arabia [Project No. GRANT4036].

ACKNOWLEDGMENTS

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No. GRANT4036].

CONFLICTS OF INTEREST

All authors declare no conflict of interest.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCES

[1] Abirami, S. (2019). A complete study on the security aspects of wireless sensor networks. In International Conference on Innovative Computing and Communications: Proceedings of ICICC 2018, Volume 1 (pp. 223-230). Springer Singapore.

[2] Shahzad, F., Pasha, M., & Ahmad, A. (2017). A survey of active attacks on wireless sensor networks and their countermeasures. Arxiv preprint arxiv:1702.07136.

[3] Arshad, A., Hanapi, Z. M., Subramaniam, S., & Latip, R. (2021). A survey of Sybil attack countermeasures in iot-based wireless sensor networks. Peerj Computer Science, 7, e673.

[4] Najmi, K. Y., alzain, M. A., Masud, M., Jhanjhi, N. Z., Al-Amri, J., & Baz, M. (2021). A survey on security threats and countermeasures in iot to achieve users confidentiality and reliability. Materials Today: Proceedings.

[5] Ganesh, D. E. (2022). Analysis of Wireless Sensor Networks Through Secure Routing Protocols Using Directed Diffusion Methods. International Journal of Wireless Network Security, 7(1), 28-35.

[6] Farjamnia, G., Gasimov, Y., & Kazimov, C. (2019). Review of the techniques against the wormhole attacks on wireless sensor networks. Wireless Personal Communications, 105, 1561-1584.

[7] Kardi, A., & Zagrouba, R. (2019). Attacks classification and security mechanisms in Wireless Sensor Networks. Advances in Science, Technology and Engineering Systems Journal, 4(6), 229-243.

[8] Yang, G., Dai, L., Si, G., Wang, S., & Wang, S. (2019). Challenges and security issues in underwater wireless sensor networks. Procedia Computer Science, 147, 210-216.

[9] Islam, M. N. U., Fahmin, A., Hossain, M. S., & Atiquzzaman, M. (2021). Denial-of-service attacks on wireless sensor network and defense techniques. Wireless Personal Communications, 116, 1993-2021.

[10] Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J., & Park, Y. (2019). Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges. IEEE Access, 8, 3343-3363.

[11] Yousefpoor, M. S., Yousefpoor, E., Barati, H., Barati, A., Movaghar, A., & Hosseinzadeh, M. (2021). Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: A comprehensive review. Journal of Network and Computer Applications, 190, 103118.

[12] Chanal, P. M., & Kakkasageri, M. S. (2020). Security and privacy in IOT: a survey. Wireless Personal Communications, 115, 1667-1693.

[13] Chelli, K. (2015, July). Security issues in wireless sensor networks: Attacks and countermeasures. In Proceedings of the world congress on engineering (Vol. 1, No. 20, pp. 876-3423).

[14] Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644.

[15] Sinha, P., Jha, V. K., Rai, A. K., & Bhushan, B. (2017, July). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. In 2017 International Conference on Signal Processing and Communication (ICSPC)(pp.288-293). IEEE.[16] Elsadig, M. A., Altigani, A.& Baraka, M. A. A. (2019). Security issues and challenges on wireless sensor networks. Int. J.Adv. Trends Comput. Sci. Eng, 8, 1551-1559

[17] Keerthika, M., & Shanmugapriya, D. (2021). Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures. Global Transitions Proceedings, 2(2), 362-367 \bibitem:Vikhyath, K. B., & Brahmanand, S. H.: Wireless sensor networks security issues and challenges: A survey. Int. J. Eng. Technol, 7(2), 89-94 (2018)

[18] Inayat, U., Ali, F., Khan, H. M. A., Ali, S. M., Ilyas, K., & Habib, H. (2021). wireless sensor networks: security, threats, and solutions. in 2021 international conference on innovative computing (icic) (pp. 1-6). ieee

[20] Goyal, Gourav & Singh, Yudhvir & Dhwaj, Dheer & Malik, dr. (2022).wireless sensor network: attacks and countermeasures

[21] mahajan, m., reddy, K. T. V., & Rajput, M. (2016). Design and simulation of a blacklisting technique for detection of hello food attack on LEACH protocol. Procedia Computer Science, 79, 675–682

[22] Vasudeva, A., & Sood, M. (2018) . Survey on sybil attack defense mechanisms in wireless ad hoc networks. Journal of Network and Computer Applications, 120, 78–118

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[23] Patil, A., & Gaikwad, R. (2015) .Comparative analysis of the prevention techniques of denial of service attacks wireless sensor network. Procedia Computer Science, 48, 387–393

[24] Anand, C., & Gnanamurthy, R. K. (2016).Localized dos attack detection architecture for reliable data transmission over Wireless Sensor Network. Wireless Personal Communications, 90(2), 847–859

[25] ZHENSHAN, Bao, BO, Xue, et WENBO, Zhang. (2013).HT-LEACH: An improved energy efficient algorithm based on LEACH. In : Mechatronic Sciences, Electric Engineering and Computer (MEC), Proceedings 2013 International Conference on. IEEE, 2013. P. 715-718

[26] Palan, N. G., Barbadekar, B. V., & Patil, S. (2017). Low energy adaptive clustering hierarchy (LEACH) protocol: A retrospective analysis. In 2017 International conference on inventive systems and control (ICISC) (pp. 1-12). IEEE.

[27] Pritchard, S. W., Hancke, G. P., & Abu-Mahfouz, A. M. (2018, June). Cryptography methods for software-defined wireless sensor networks. In 2018 IEEE 27th international symposium on industrial electronics (ISIE) (pp. 1257-1262). IEEE.

[28] Chelli, K. (2015, July). Security issues in wireless sensor networks: Attacks and countermeasures. In Proceedings of the world congress on engineering (Vol. 1, No. 20, pp. 876-3423)