STAP
Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Assessment of cybersecurity threats and defense mechanisms in wireless sensor networks

Elham Alotaibi[1], Rejwan Bin Sulaiman[2] Mohammed Almaiah[3]

[1] *Department of Computer Networks and Communications, King Faisal University, Al-Ahsa 31982, Saudi Arabia*
[2] *Rejwan Bin Sulaiman, School of Computer science and Technology, Northumbria University, Newcastle Upon Tyne, UK*
[3] *King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan*

ARTICLE INFO

Article History

Received 07 Jan 2025
Accepted 23 Jan 2025
Published 20 Feb 2025

Academic Editor:

Youakim Badr

Vol.2025, No.1

DOI:

https://doi.org/10.63180/jcsra.thestap.2025.1.5

ABSTRACT

Wireless sensor networks (WSNs) are a rapidly advancing technology and serve as a foundational component for the Internet of Things (IoT) and various other domains, including healthcare, education, surveillance, military applications, and more. These networks possess unique characteristics such as limited memory, battery life, and processing power, as well as the ability to be deployed in remote or inaccessible areas. While these features enable their widespread use, they also impose significant constraints, making the implementation of robust security and protection mechanisms a complex challenge. This research paper examines a collection of recent scientific studies and proposals aimed at enhancing the security of wireless sensor networks against diverse types of attacks. The primary objective of this study is to explore the common challenges faced by WSNs as an emerging technology. Through a comprehensive review of existing research and practical implementations, it identifies potential risks and threats, evaluates current security measures, and analyzes the outcomes of these studies to provide insights for future advancements in the field.

Keywords: Wireless Sensor Networks; Cybersecurity; Threat; DOS; Sybil; Wormhole, Sinkhole.

How to cite the article

Alotaibi, E., Bin Sulaiman, R., & Almaiah, M. (2025). Assessment of cybersecurity threats and defense mechanisms in wireless sensor networks. Journal of Cyber Security and Risk Auditing, 2025(1), 47–59. https://doi.org/10.63180/jcsra.thestap.2025.1.5

1. Introduction

Many applications, systems and innovations have appeared in our lives. With the emergence of these technologies, many threats and security risks will appear, which must be analyzed and evaluated. Risk assessment is a mature system based on the discovery and analysis of risks, determining their causes, describing them, and determining their effect [1]. One of the main challenges of wireless sensor networks is the safe transmission of data, and some networks have been exposed to many breaches and threats for example Dos, Sybil, Sinkhole and wormhole that will be mentioned in this project [1] [2].

Security risk analysis and management can be defined as: a set of practices and management tools used to analyze risks, which include, identifying threats and weaknesses to which the system is exposed, evaluating the possibility of risks and their impact, reviewing the results of monitoring and taking the necessary action in the event of a threat to the system. One of the most important systems that need to analyze and manage risks is wireless sensor networks, which are the most widespread type of networks and contain sensitive data. Wireless sensor networks can be defined as an emerging technology, which is a self-sufficient network that includes a large amount of sensor nodes. Examples of the uses of current applications

such as commercial applications, military, traffic control, and in surveillance systems. These networks and sensor nodes are used to transmit data and information obtained by monitoring the surrounding environment by means of sensors. The data is transmitted and transmitted securely to the main center of the network [2].

Risk management, analysis and security guidance in wireless sensor networks is an difficult steps due to the nature of the environments in which the sensor nodes are located and the nature of the resources of the sensor network, Because it is a new technology. The network is exhausted, and due to the weaknesses in the network, it is vulnerable to many threats that harm and cause the network to be unreliable to communicate and work [3]. There have been many attacks on the wireless sensor network examples of this, Sinkhole ,Dos, wormhole, sinkhole, selective forwarding, hello flood, false routing attacks and acknowledgement flooding have recently attracted considerable attention [3]. The hijacking of sensors is one of the most common threats and attacks in wireless sensor networks environment.

According to previous studies and research reviews [4] [5] [6] wireless sensor networks can be exploited from many attacks and different types and on different layers in wireless sensor networks, these attacks may cause network penetration, stealing information and destruction of data and damage network resources as shown in Figure 1 [7] [8]. This research addresses the common challenges faced by wireless sensor networks as an emerging technology. It involves a thorough review of numerous research and practical studies to identify potential risks and threats, evaluate the security measures implemented, and analyze the outcomes derived from these scientific works. Therefore, the main objective of this research paper is to review and analyze the most important security threats on wireless sensor networks, review the most important technicians of cybersecurity in wireless sensor networks for protection and monitoring and identifying threats and finally what is the most important measures for each network.

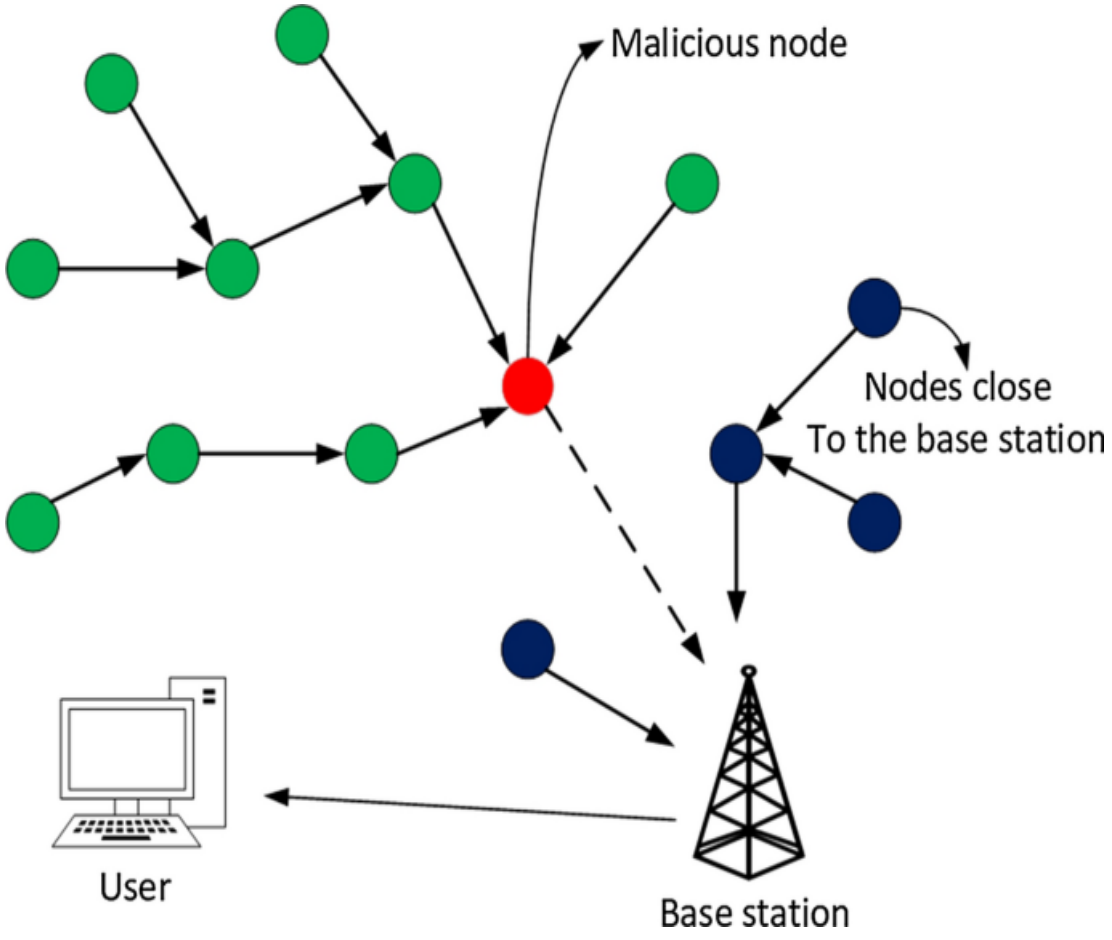


Figure 1. Wireless sensor network threat.

2. Related Works

This section presents a summarize and review of related works in Table 1, that outline the objectives of each selected research paper, along with proposed improvements and strategies to enhance the safety and security measures discussed in each study. This analysis aims to provide a deeper understanding of the previous researches contributions through offering actionable recommendations to strengthen the protection mechanisms for wireless sensor networks. For instance, Zhang Huanan, Xing Suping, Wang Jiannan [6] aimed in their study to provide a new method for enhancing the security of wireless sensor network. This new method based on self-organizing by using different types of key distribution helps to complete secure routing and improve resistance to attacks on wireless sensor networks. Tin yang et al., [7] aimed to increase the efficiency of networks and the possibility of multi-user and a high level of security, outcomes The results of the research paper showed that the multi-gateway three-factor authentication protocol is characterized by high levels of privacy, effectiveness and security. Shariq Aziz Butt [8] discussed the most important attacks on wireless sensor networks in smart health systems and their impact on monitoring systems, and suggest some necessary measures to prevent these attacks. The findings recommend to build a smart health monitoring system, security guidelines must be followed to prevent attacks by applying some security strategies.

Waleed in the study [9] presented a discussion on the most important threats on wireless sensor networks and describe them and propose the intelligent guidance of the network. This study developed an effective algorithm to detect and identify gaps and vulnerabilities on wireless sensor networks and improve system performance. Reza et al., [10] focused on studying the denial-of-sleep attack and proposed an algorithm that may help to counter these threats. The research study showed that one of the effective ways to counter denial-of-sleep attacks is ASDA-RSA. Subrato et al., [11] studies the application of Road safety control and traffic management is an application on wireless sensor networks that is faced with many threats in this review and various threats and ways to protect them have been discussed. The results of the research review need to focus on cybersecurity in VANET networks and provide algorithms and techniques designed to provide security and attack-free communication. Mohammad [12] describe different types of denial-of-service attacks in different layers of the network. The study recommended that defense systems against denial-of-service attacks must be reconsidered and focus on ensuring the lowest overhead cost of resource consumption in wireless sensor networks. Babaeer et al., [13] focused on studying and describing a Sinkhole attack and proposing a protocol improve network performance. The proposed algorithm and scheme enhances security and ensures the integrity and validity of the sensor data during transmission and reception.

Aliady et al., [14] found that the wormhole attack is one of the most dangerous attacks on wireless sensor networks, harmful and easy to spread and targets the routing layer. This paper focuses on this attack and defines a way to identify and treat it focuses on this attack and defines a way to identify and treat. The results proved that the protocol used is effective in terms of power, throughput, packet delivery rates and safety. David and George [15] recommended that proof and verification is one of the most important requirements for wireless sensor networks. Identity fraud is one of the threats that threaten networks, the most famous of which is a Sybil attack that will be studied and a technique proposed to try to mitigate it. The proposed attack detector is powerful and effective for detecting attacks launched by enemies from different levels and transmitting energy. Ding et al., [16] studied the selective forwarding attack, they display its damage and propose a model to counter this attack. The findings found that NB-DPC algorithm can identify and block malicious nodes. Safaldin et al., [17] aims to increase the accuracy of intrusion detection. The results discovered that an e GWOSVM-IDS technology performs the performance of the original GWO-IDS and PSO-IDS techniques in terms of detection and error rate, alert rate, number of specified features, execution time, in addition to high accuracy. Kumar et al., [18] found that time synchronization is a requirement of wireless sensor networks, which may be lost due to some attacks such as node destruction and denial of service. This problem was studied and a solution was proposed Modern CTS, MMAR-CTS Algorithms. The simulation results show that it is more effective compared to other algorithms. Akashah et al., [19] indicated that wireless sensor networks are one of the most widespread networks on IoT applications, and one of the most common threats to IoT is the Sybil attack. The paper discussed many techniques used to prevent Celia's attack, but it turns out that there are no effective measures against it so far.

Julie et al., [20] the study aimed to identify a DDOS attack and suggest a technique that may help reduce its damage. The results are a modus operandi FBDR that works far better than other proposed schemes. Pramod et al., [21] aimed to identify the threats and the most important security concerns that threaten technologies 5G Mobile Wireless Network. It is necessary to focus on security in these networks and to provide effective protection techniques. Wang et al., [22] in their research aimed to increase network security in internet technologies by using algorithm that depends on the state of the channel (CSI). The proposed technique can be implemented in specific areas such as army battlefields and critical events. Osanaiye

et al., [23] aimed to study the nature of wireless sensor networks and the possibility of placing them in remote areas, vulnerable to many threats, the most important of which is dos jamming attack. The proposed technique can be implemented in specific areas such as army battlefields and critical events. Yang et al., [24] aimed to provide a comprehensive overview of the attacks, challenges, privacy and limitations of underwater wireless sensor networks. The results found that underwater WSN in the first stage of theoretical and experimental research are rare and it is necessary to focus on them and intensify studies in this field. Adil et al., [25] aimed to study and propose a solution scheme for the jamming attack, which is one of the most common types of security vulnerabilities. The results indicated that proposed scheme is an effective against spoofing attacks and is intended for heterogeneous networks. Fattah et al., [26] indicated that the rapid development of WSN underwater needs strength and flexibility in solutions that meet the basic requirements of network security. The results found that the networks have received many improvements, but there are still technologies that need to be studied and to provide better solutions and better security for the underwater WSN. Ali [27] focused in his study to detect and analyze the sinkhole attack and suggest a solution to try to prevent this attack. The proposed method is considered effective in isolating and detecting this attack, as it helps reduce network power consumption and increase throughput.

Huan et al., [28] propose a method to prevent and mitigate the impact of the spoofing attack. The results found that this method can effectively detect and accurately identify the node and detect the attack. Yuan et al., [29] aimed to detect and prevent Sybil attack by using (SF)-APIT algorithm. The results indicated that (SF)-APIT algorithm was an effective technique in preventing attack with high detection rate. Ahutt [30] aimed to Identify and detect a wormhole attack by using MCRP protocol. The findings confirmed that Central steering protocol is effective for preventing wormhole attacks. Numan et al., [31] aimed to study the replication attack and suggest ways to mitigate it. Systematic review of the threats and characteristics of cloning and detection techniques. Liu et al., [32] proposed a SILRD Propagation Model for detection. The results indicated that an effective model, but it will be more effective and accurate when more practical conditions are considered. Mohapatra et al., [33] aimed to study of man-in-the-middle attack and development of IDS technology. Outcomes showed that the model is effective in detecting harmful behavior in record time compared to its complexity. Bhatt et al., [34] aimed to Introduce and study a node capture attack and discover a proposal to prevent this attack. The outcomes indicated that FFOA Maximize the efficiency of attack detection. Liu et al., [35] aimed to determine the impact of malware on the wireless sensor network and suggest a model to prevent these programs. The simulation results, SILRD has clear advantages in increasing the amount of sensor nodes and has proven its effectiveness with solar charging. Alotaibi et al., [36] suggested a new technology that contributes to preventing DOS attacks by using HWSN based on the K-means clustering algorithm. The proposed system is effective and highly efficient to detect and identify the attack.

Bangashand others [37] focused on how to ensure wireless sensor networks is secured. The results provided an important recommendations aiming to provide high security systems, authentication and encryption systems effective. Periyanayagi et al., [38] aimed to identify physical layer attacks in WSN by using Swarm Based Trusted Node for Tampering and Cheating Attack (SBTN-TC) model. The model has proven effective through the results of the remaining package and power delivery ratio. Huang et al., [39] aimed to identify the data tampering attacks and how do we protect networks from them. The proposed hybrid diagnosis algorithm is effective for this type of attack and its performance is ideal. Kibirige et al., [40] indicated that characteristics of wireless sensor networks are low memory and low computational power, which may expose them to many attacks such as wormholes and others. The study recommended that security in WSN networks must be further studied and restrictions that prevent their application should be further investigated. Boni et al., [1] classified the main attacks in WSN as shown in Figure 2.

Table 1. Related works.

Ref	*Objectives*	*Problem statement*	*methodology*
[6]	Studying the security and privacy of WSN.	Multiple attack methods on WSN	Key distribution algorithm
[7]	increase the efficiency of networks and the possibility of multi-user	Simultaneous access protocols by multiple users that do not.	A new connection to WSN based on three-factor authentication protocols.
[8]	most important	Smart health rely on WSN to send patient data, and are vulnerable to threats.	A comparison of the most

Ref	*Objectives*	*Problem statement*	*methodology*
	attacks on WSN used in smart health systems		important types of attacks
[9]	discuss the intelligent guidance of the WSN	safety in WSN	Routing protocol
[10]	Study DOS attacks	Dos loss and depletion of power in sensors.	RSA encryption algorithm
[11]	threats of the Road safety control and traffic management	technique VANET faced by many threats such as a man in the middle	Discuss importan t threats on the VANET
[12]	Study of DOS	DOS , used to disrupt access to network, cannot respond to request	(Co-FAIS)
[13]	Studying a Sinkhole attack	sinkhole attack, an announce itself as the best path to the base station	TSEESN protocol
[14]	Wormhole attack, harmful, easy to spread and targets the routing layer.	it is an untrusted shortcut, where an intruder sensor establishes a wired or wireless connection	AODV protocol.
[15]	Identity fraud is one of the threats , the most famous of is Sybil attack	The attacker can forge his identity and enter from another device.	RSS
[16]	Study the Selective Forwarding attack	Harmful attack sends forwarding attacks causing amal function in the provision of service.	NB-DPC
[17]	aims to increase the accuracy of intrusion detection	Infiltration is a threat to WSN	NSL KDD’99
[18]	Time synchronizatio n lost due to some attacks such as Dos	Dos threat contribute to poor network	Modern CTS Algorithms.

Ref	*Objectives*	*Problem statement*	*methodology*
[19]	WSN are one of the most widespread networks on IoT applications	Sybil attack announces his false identity	Encryption Rssi
[20]	Identify a DDOS attack	attacker will flood the target node so that the node cannot respond and accept other requests	fuzzy logic mechanism
[21]	Study the threats for 5G mwn.	intrusion threats more danger to this type of network	Encryption
[22]	Increase security WSN	Sybil attack that relies on forgery	Detection by state of the channel (CSI)
[23]	jamming attack The most famous threats to WSN	Dos jamming that disrupts the functions of the sensor by sending many radio frequency signals	step-wise approach
[24]	Providing a comprehensive overview of the attacks underwater WSN	nature of Underwater WSN are vulnerable to many threats nature of Underwater WSN are vulnerable to many threats	signature,
[25]	Study and solution scheme for the jamming	The attacker jams network traffic by sending frequencies	three-edge scheme

Ref	*Objectives*	*Problem statement*	*methodology*
[26]	WSN underwater needs strength and flexibility in solutions that meet the basic requirements	One of the challenges for networks is the delay variation	Access control and authentication
[27]	analyze an sinkhole attack and suggest a solution	in which the attacker spoofs the identity of the node and behaves in the same way as the node	Simulator (NS2)
[28]	Make a proposal to prevent impact of the Spoofing attack	Spoofing is a cyber-attack that occurs when a scammer is disguised as a trusted source to gain access to data	(NISA)
[29]	Detect and prevent Sybil attack.	Sybil, who relies on fake identities	(SF)-APIT algorithm
[30]	identify worm hole attack	Wormhole is one of the most harmful attacks	MCRP protocol
[31]	Study the replication attack and suggest ways to mitigate it	attacker is able to capture the target node and use the credential information	distributed based detection
[32]	Study Malware and suggested model for detection	Malware is considered one of the threats to WSN	SILRD Propagation Model

Ref	*Objectives*	*Problem statement*	*methodology*
[33]	Study of man in the middle attack	third party tries to obtain Data from the connection of the two nodes	IDS
[34]	Introduce and study a node capture attack	attacker captures the node and can he read, view the node	FFoA Algorithm
[35]	Determine the impact of malware on the WSN	Information leakage, network paralysis	SILRD with solar energy harvesters and the SILRD
[36]	Suggesting a new technology to preventing DOS attacks	DOS networks, which means denial of service.	HWSN based on the K-means clustering algorithm
[37]	security in WSN	The nature of SN and their locations may expose them to many risks such as hijacking	Literature survey
[38]	Identify physical layer attacks for WSN	Data tampering is a set of deliberate actions that are applied to data.	Cheating Attack (SBTN-TC) mode
[39]	data tampering attacks and how do we protect networks	tampering attack the change and tampering with data	hybrid diagnosis algorithm
[40]	The characteristic of WSN are low memory may expose to many attacks	An attack on WSN may cause other multiple attacks	A model for analyzing the solutions used for detection

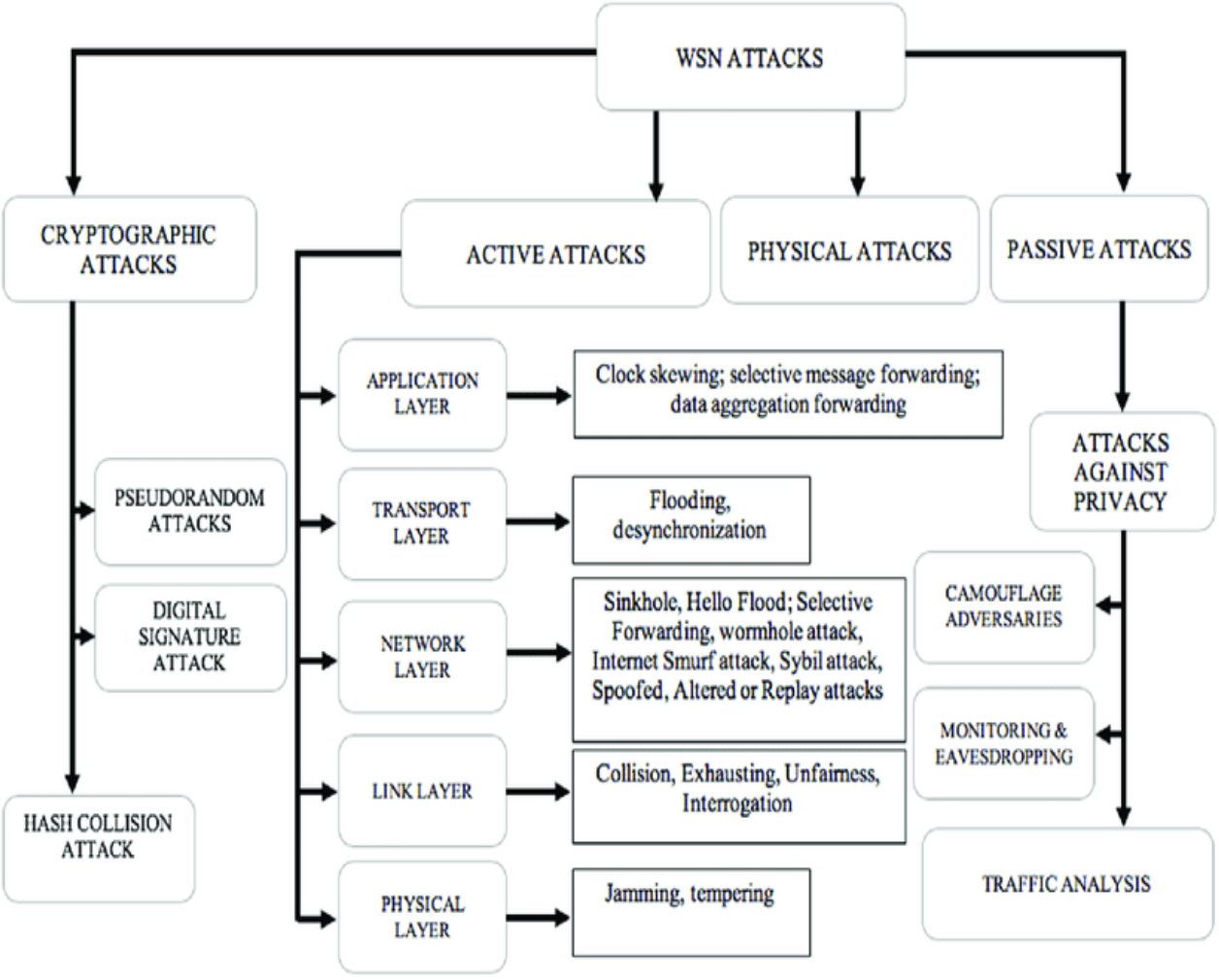


Figure 2. The common attacks in WSN.

3. Research Methodology

This systematic review followed four main stages as outlined by PRISMA. The search terms used were: (Wireless sensor networks OR sensor networks) AND (security OR protection) AND (threats OR risks). The research was based on a collection of studies retrieved from the Saudi Digital Library and Google Scholar, with a focus on the following criteria: publication year and relevance to the cybersecurity of wireless networks. In the identification phase, 50 research papers were initially collected. During the sorting phase, duplicates and redundant studies were removed, reducing the count to 45. Additionally, five older papers published in 2015 or earlier were excluded, leaving a total of 40 research papers for the final review, as illustrated in Figure 3.

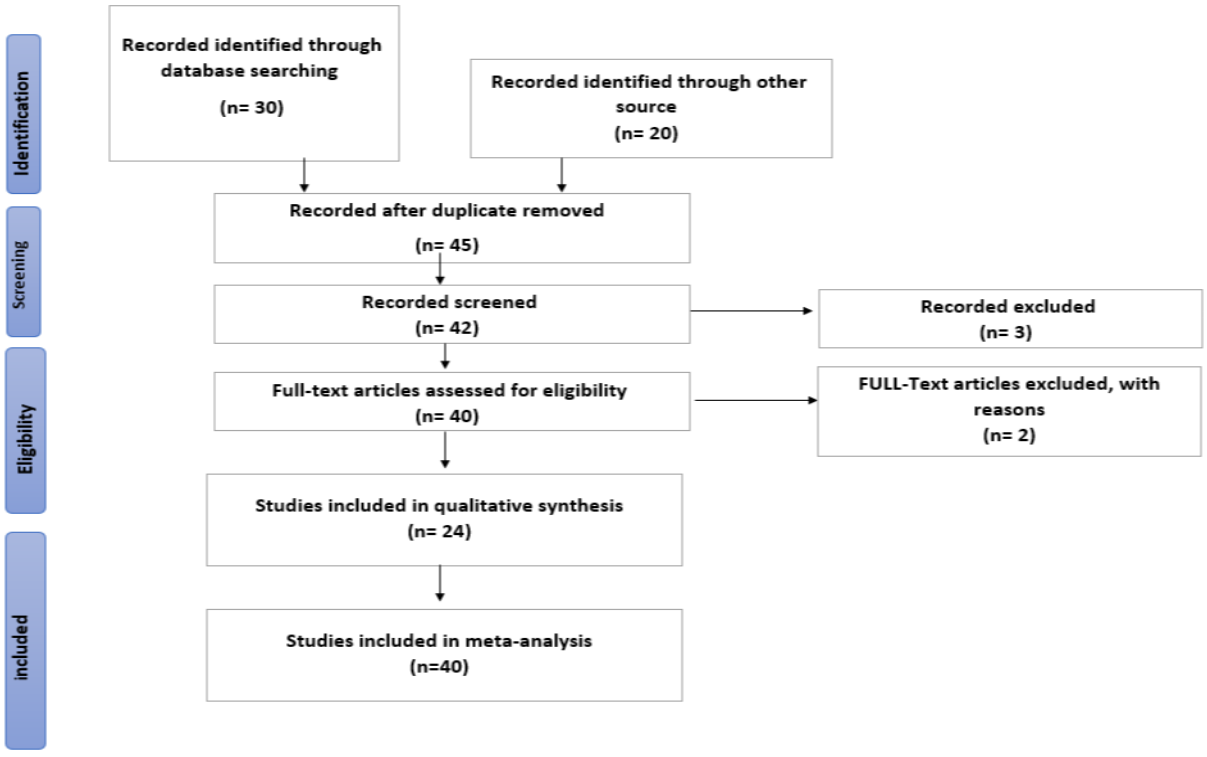


Figure 3. PRMISA methodology.

4. Analysis and Findings

The findings of this study indicated that wireless sensor networks face numerous threats and risks. However, these threats can be classified based on their severity and impact. According to the reviewed studies, Denial of Service (DoS) attacks pose the highest risk, accounting for 30% of the total threat impact. Sinkhole attacks follow at 23%, while Sybil attacks contribute 19%. The remaining attack types are considered less severe, as illustrated in Figure 4.

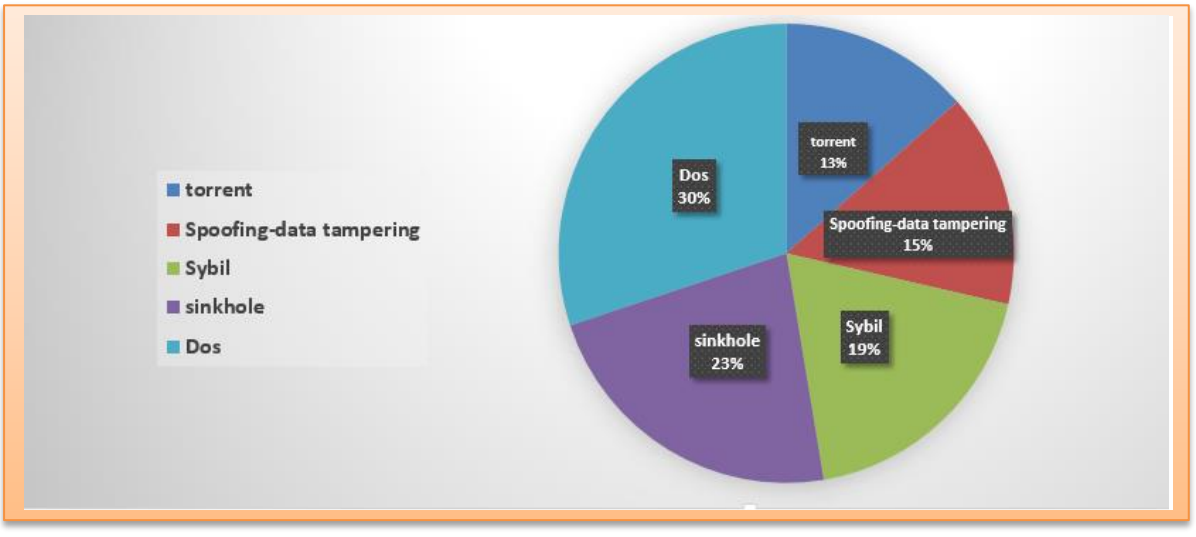


Figure 4. Classification of cyber-attacks in WSN.

The results of this study indicate that proposed security controls and protection techniques rely heavily on encryption, access control, asymmetric encryption, hashing functions, and key distribution algorithms, as illustrated in Figure 5. A key recommendation is to focus on the security of underwater wireless sensor networks, a technology that remains largely unexplored in terms of protection mechanisms. Theoretical and experimental research in this area is scarce, highlighting the need for further investigation. Additionally, we recommend exploring blockchain technologies, as they have the potential to enhance the security of wireless sensor networks.

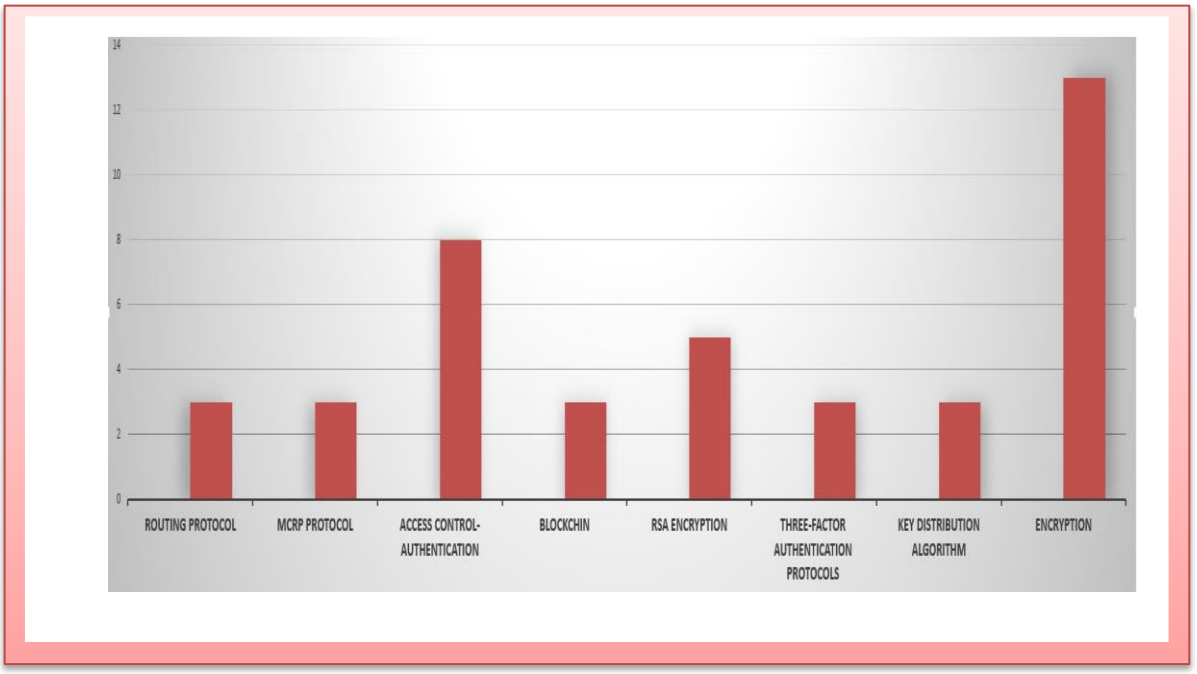


Figure 5. Classification of security controls for WSN.

5. Conclusion

Advancements in wireless sensor networks, security measures, and sensor placement strategies have significantly influenced their usability. However, one of the key challenges facing these networks is ensuring seamless deployment and operation, both indoors and outdoors, as environmental factors can impact communication and data transmission. Our findings indicate that the most critical threats to these networks include Denial of Service (DoS) attacks, downstream attacks, sleep deprivation attacks, hijacking, and other security vulnerabilities. While various protection techniques have been proposed, their effectiveness varies in terms of strength and resilience. There remains a need for the development of newer and more robust security measures to better prevent these attacks.

Conflicts Of Interest

The authors declare no conflicts of interest.

Funding

No funding.

Acknowledgment

References

[1] Boni, K. R. C., Xu, L., Chen, Z., & Baddoo, T. D. (2020). A security concept based on scaler distribution of a novel intrusion detection device for wireless sensor networks in a smart environment. *Sensors*, *20*(17), 4717.

[2] London School of Economics and Political Science, Dept. of Accounting and Finance and ESRC, Centre for Analysis of Risk and Reg.,2019 The risk management of nothing q Michael Power, www.elsevier.com/locate/aos.

[3] Subrato Bharati1, Prajoy Podder2, M. Rubaiyat Hossain Mondal3, Md. Robiul Alam Robel4 (11.jun, 2020) Threats and Countermeasures of Cyber Security in Direct and Remote Vehicle Communication Systems.(arxiv.org)

[4] Balasem Al-Isawi, University of Babylon(oct,2021) wireless sensor network performance analysis under sinkhole attacks.(https://www.researchgate.net/publication/355615212)

[5] Reza Fotohi1 Somayyeh Firoozi Bari2 Mehdi Yusefi3 (27.nov,2020) Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol (arxiv.org).

[6] Zhang Huanan*, Xing Suping, Wang Jiannan (2020) Security and application of wireless sensor network, at www.sciencedirect.com.

[7] Tin yang and outhers (19 nov 2021) Design of a secure and efficient authentication protocol for real-time accesses of multiple users in PIoT-oriented multi-gateway WSNs , https://www.sciencedirect.com/.

[8] Shariq Aziz Butt (19 th 2019) IoT Smart Health Security Threats, www.researchgate.net

[9] Waleed Kh. Alzubaidi (2018) Methods of Secure Routing Protocol in Wireless Sensor Networks, http://qu.edu.iq/.

[10] Reza Fotohi and outhrers (2020) Securing Wireless Sensor Networks Against Denial-of-Sleep Attacks Using RSA Cryptography Algorithm and Interlock Protocol, arxiv.org.

[11] Subrato Bharati and others (2020) Threats and Countermeasures of Cyber Security in Direct and Remote Vehicle Communication Systems, arxiv.org.

[12] Mohammad Nafis Ul Islam (2021) Denial-of-Service Attacks on Wireless Sensor Network and Defense Techniques, arxiv.org

[13] HUDA A. BABAEER and others(29 may 2020) Efficient and Secure Data Transmission and Sinkhole Detection in a Multi-Clustering Wireless Sensor Network Based on Homomorphic Encryption and Watermarking, https://ieeexplore.ieee.org/

[14] WATEEN A. ALIADY and others(July 12 ,2019) Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Networks, https://ieeexplore.ieee.org/.

[15] Stalin David and 2 T. Joseph George (2020) Identity-Based Sybil Attack Detection and Localization, Artech Journals.

[16] JINGZE DING and others (February 5,2021) The DPC-Based Scheme for Detecting Selective Forwarding in Clustered Wireless Sensor Networks, https://ieeexplore.ieee.org/.

[17] Mukaram Safaldin and others (13 june ,2020) Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks, https://doi.org/10.1007/s12652-020-02228-z.

[18] Suresh Kumar Jha and others (13 august2021) Security Threat Analysis and Countermeasures on Consensus-Based Time Synchronization Algorithms for Wireless Sensor Network, https://link.springer.com/

[19] Akashah Arshad and others (September 22,2021) A survey of Sybil attack countermeasures in IoT-based wireless sensor networks, arxiv.org.

[20] Golden Julie and others (march 25 ,2021) FBDR-Fuzzy based DDoS attack Detection and Recovery mechanism for wireless sensor networks, https://orcid.org/0000-0002-3905-2460

[21] Shailesh Pramod Bendale and others (2018) Security Threats and Challenges in Future Mobile Wireless Networks , https://ieeexplore.ieee.org/

[22] Chundong Wang and others (march 15, 2018) Accurate Sybil Attack Detection Based on Fine-Grained Physical Channel Information, mdpi.com

[23] Opeyemi Osanaiye anf others (24 may 2018) A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks

[24] Guang Yang and others (13 Nov 2018) Challenges, Threats, Security Issues and New Trends of Underwater Wireless Sensor Networks, mdpi.com

[25] Muhammad Adil and others (18 Apr 2018) An Anonymous Channel Categorization Scheme of Edge Nodes to Detect Jamming Attacks in Wireless Sensor Networks

[26] Salmah Fattah and others (21 September 2020) A Survey on Underwater Wireless Sensor Networks: Requirements, Taxonomy, Recent Advances, and Open Research Challenges, ; https://doi.org/10.3390/s20185393.

[27] Mubashir Ali (2020) Detection and Isolation Technique for Sinkhole Attack in WSN, , arxiv.org.

[28] Xintao Huan and others(2021) NISA: Node Identification and Spoofing Attack Detection Based on Clock Features and Radio Information for Wireless Sensor Networks, https://ieeexplore.ieee.org/.

[29] YALI YUAN and others (June 5, 2018) Secure APIT Localization Scheme Against Sybil Attacks in Distributed Wireless Sensor Networks, https://ieeexplore.ieee.org/.

[30] OHIDA RUFAI AHUTU (April 15,2020) Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks, https://ieeexplore.ieee.org/

[31] MUHAMMAD NUMAN and others (march 1,2020) A Systematic Review on Clone Node Detection in Static Wireless Sensor Networks, , https://ieeexplore.ieee.org/

[32] Guiyun Liu and others (3 jul 2020) Differential Games of Rechargeable Wireless Sensor Networks against Malicious Programs Based on SILRD Propagation Mode, https://doi.org/10.1155/2020/5686413.

[33] Hitesh Mohapatra and others (5 may , 2020) Handling of Man-In-The-Middle Attack in WSN Through Intrusion Detection System, http://www.warse.org/IJETER/static/pdf/file/ijeter05852020.pdf

[34] Ruby Bhatt and others(5 september 2019) implementation of Fruit Fly Optimization Algorithm (FFOA) to escalate the attacking efficiency of node capture attack in Wireless Sensor Networks (WSN), https://doi.org/10.1016/j.comcom.2019.09.007.

[35] Guiyun Liu and others (14 sep 2020) Attack-Defense Game between Malicious Programs and Energy-Harvesting Wireless Sensor Networks Based on Epidemic Modeling, https://doi.org/10.1155/2020/3680518.

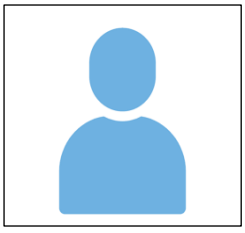
[36] Elham alotaibi and others (2019) Securing Cyber-Physical Systems,psu.edu.sa

[37] Bangashand others (2017) Security Issues and Challenges in Wireless Sensor Network,

[38] Periyanayagi and others (2018) Swarm-based defense technique for tampering and cheating attack in WSN using CPHS , https://link.springer.com/

[39] Da-WenHuang (2021) Data tampering attacks diagnosis in dynamic wireless sensor networks, https://www.sciencedirect.com.

[40] George William Kibirige and others (2020) Attacks in Wireless Sensor Networks, arxiv.org.



Elham Alotaibi received his M.Sc. degree in Cybersecurity from the King Faisal University (KFU), Saudi Arabia. She has published several papers in well reputed journals and conferences. Her research interests include cybersecurity, cybersecurity risk assessment and cryptographic .

Dr. Rejwan Bin Sulaiman is a highly skilled researcher in the field of artificial intelligence and cybersecurity. Currently serving as a lecturer and module leader at Northumbria University London. His teaching approach combines theoretical foundations with practical applications, fostering an interactive and engaging learning environment. Rejwan believes in equipping students with both conceptual understanding and hands-on skills, enabling them to excel in their academic pursuits and future careers. Rejwan specializes in the areas of cybersecurity, machine learning, and artificial intelligence. He has actively contributed to the field through his research, attending conferences and seminars to present his work and staying up to date with the latest advancements in his domain.

Dr. Mohammed Almaiah is an Associate Professor in the Department of Computer Science at University of Jordan. Almaiah is among the top 2% scientists in the world from 2020 up to now. He is working as Editor in Chief for the International Journal of Cybersecurity and Risk Assessment. He has published over 115 research papers in highly reputed journals such as the Engineering and Science Technology, an International Journal, Education and Information Technologies, IEEE Access and others. Most of his publications were indexed under the ISI Web of Science and Scopus. His current research interests include Cybersecurity, Cybersecurity-Risk Assessment and Blockchain.