International Journal of Safety and Security Engineering
Vol. 14, No. 2, April, 2024, pp. 373-386
Journal homepage: http://iieta.org/journals/ijsse

A Comprehensive Analysis of Security Challenges and Countermeasures in Wireless Sensor Networks Enhanced by Machine Learning and Deep Learning Technologies

Hadeel M. Saleh[1,2*], Hend Marouane[1], Ahmed Fakhfakh[3]

[1] National School of Electronics and Telecommunications (ENET'COM), NTS'COM Laboratory, Safax University, Sfax 3029, Tunisia
[2] Continuing Education Center, University of Anbar, Ramadi 31006, Iraq
[3] Laboratory of Signals, Systems, Artificial Intelligence and Networks (SM@RTS), Digital Research Center of Sfax (CRNS), National School of Electronics and Telecommunications of Sfax (ENET'com), University of Sfax, Sfax 1163, Tunisia

Corresponding Author Email: hadealms89@gmail.com

https://doi.org/10.18280/ijsse.140206

Received: 15 November 2023
Revised: 22 March 2024
Accepted: 1 April 2024
Available online: 26 April 2024

Keywords:
wireless sensor network, deep learning, network attack detection, the Internet of Medical Things (IOMT), cloud, Internet of Things (IoT)

ABSTRACT

Wireless sensor networks (WSNs) play a crucial role in monitoring and capturing information in various domains, including the Internet of Medical Things (IOMT). However, WSNs face significant security challenges, such as intrusion and potential malicious activities, due to their distributed and resource-constrained nature. This research provides a comprehensive analysis of the security challenges in WSNs enhanced by machine learning and deep learning technologies within the context of the IOMT. The research addresses these challenges by proposing practical countermeasures to mitigate security concerns in WSNs. It discusses the complexities, critical security issues, and vulnerabilities within WSNs, offering insights into potential fixes based on various approaches and theories. Furthermore, the integration of machine learning and deep learning in WSNs enables efficient communication, data analysis, and control, supporting areas like the IOMT, which includes monitoring prescription orders, tracking patients' movements, and remotely managing patients with chronic illnesses. By addressing the security challenges specific to WSNs in the IOMT environment, this research contributes to the advancement of secure and reliable wireless sensing systems in critical domains. The utilization of machine learning and deep learning technologies facilitates the development of robust methods for detecting and mitigating network attacks. The practical implications of the research findings are demonstrated through tangible examples within the IOMT context, emphasizing the potential impact on improving the security and reliability of wireless sensing systems.

1. INTRODUCTION

In today's interconnected world, network attacks pose significant threats to the security and integrity of various systems. The Internet of Medical Things (IOMT) is no exception, as it relies on machine-to-machine communication and the integration of medical devices to enhance healthcare services. However, the IOMT environment is particularly vulnerable to attacks due to its unique characteristics, such as the reliance on wireless sensor networks (WSNs) and the sensitive nature of medical data [1].

WSNs play a crucial role in the IOMT environment by enabling the monitoring of vital signs, tracking patient movements, and remotely managing patients with chronic illnesses. These networks consist of numerous sensor nodes that collect and transmit data wirelessly. However, the distributed and resource-constrained nature of WSNs introduces security challenges, including intrusion and potential malicious activities. Without proper countermeasures, these vulnerabilities can compromise the confidentiality, integrity, and availability of sensitive medical information [2]. Therefore, there is a pressing need to address security challenges and develop effective countermeasures specifically tailored to the IOMT environment. This research aims to provide a comprehensive analysis of the security challenges faced by wireless sensor networks in the context of the IOMT. By identifying and understanding these challenges, the research seeks to propose practical solutions and countermeasures to mitigate security concerns. To achieve these objectives, the research will employ a combination of machine learning and deep learning technologies. Machine learning algorithms can analyze large datasets and detect anomalous behavior or patterns indicative of attacks in real-time. Deep learning techniques, on the other hand, can extract complex features and enhance the accuracy of attack detection systems. By leveraging these advanced technologies, the research aims to develop robust and efficient methods for detecting and mitigating network attacks in the IOMT environment.

To provide clarity and demonstrate the relevance of the research, tangible examples, and scenarios within the IOMT context will be presented. For instance, the system could be applied to monitor prescription orders, where anomalous activities could indicate unauthorized access or tampering. Furthermore, tracking hospitalized patients' movements using wearable health equipment can benefit from the proposed security mechanisms to ensure the integrity and privacy of patients' data. These examples highlight the practical implications of the research findings and the potential impact on improving the security and reliability of wireless sensing systems in critical medical domains. This research aims to address the security challenges in wireless sensor networks enhanced by machine learning and deep learning technologies in the IOMT environment. By providing a comprehensive analysis of these challenges, proposing effective countermeasures, and utilizing advanced methodologies, the research seeks to contribute to the advancement of secure and reliable wireless sensing systems in critical medical domains. The real-world examples within the IOMT context further emphasize the significance and applicability of the research findings.

The rapid advancement of the IoT has revolutionized various industries, including healthcare. holds tremendous potential for improving patient care, enabling remote monitoring, and enhancing healthcare delivery [3]. However, with this increased connectivity comes a pressing concern: the security of the IOMT environment. The IOMT environment presents unique security challenges due to the critical nature of healthcare data, the diverse range of interconnected medical devices, and the potential consequences of security breaches. Attacks on the IOMT network can lead to disastrous outcomes, including unauthorized access to patient records, manipulation of medical device functionality, or disruption of healthcare services. It is imperative to address these security challenges and develop robust systems to safeguard the integrity, confidentiality, and availability of healthcare data and services. The problem is to detect and classify attacks within the IOMT environment accurately. Various approaches have been proposed to tackle this challenge, including anomaly detection, signature-based detection, and machine learning techniques. Each approach has its strengths and weaknesses, and their applicability varies depending on the specific IOMT scenario. Anomaly detection techniques aim to identify deviations from normal network behavior. They establish a baseline of expected behavior and flag any anomalies that deviate significantly from it [4]. While anomaly detection can be effective in detecting previously unknown attacks, it can also generate a high number of false positives and may struggle with detecting sophisticated attacks that closely mimic normal behavior. Signature-based detection relies on pre-defined attack signatures or patterns to identify known attacks. This approach is effective in detecting attacks with well-defined signatures, but it may struggle with detecting new or evolving attack patterns that have not been previously identified. Machine learning techniques, particularly deep learning models, have gained significant attention in recent years due to their ability to automatically learn patterns and detect complex attacks. These models can analyze vast amounts of network traffic data, identify subtle patterns, and adapt to new attack variations. However, deep learning models typically require substantial computational resources and extensive training datasets to achieve optimal performance [5].

The choice of approach depends on the specific requirements and constraints of the IOMT environment. For example, in scenarios where real-time detection is critical, signature-based or anomaly detection techniques may be more suitable due to their low computational overhead. On the other hand, in scenarios with a large volume of network traffic and a need for detecting sophisticated attacks, machine learning techniques can provide better accuracy and adaptability. In the subsequent sections, we will provide a critical analysis and comparison of these approaches, highlighting their strengths, weaknesses, and applicability in different IOMT scenarios. Additionally, we will explore the potential of combining these approaches or leveraging hybrid models to enhance the detection and classification of attacks in the IOMT environment. By critically evaluating these techniques, we aim to identify the most effective and practical approaches for addressing the security challenges in the IOMT context. Through this research, we seek to not only advance the understanding of IOMT security challenges but also provide valuable insights for developing effective countermeasures and enhancing the overall security of interconnected medical devices and healthcare systems.

The article starts with an introduction that highlights the vulnerabilities of the IOMT environment and the importance of developing effective countermeasures. It then discusses the background of WSNs and their role in the IOMT environment. The article further explores the integration of machine learning and deep learning technologies in WSNs for improved security. It presents methodologies for attack detection and prevention in the IOMT environment. The article also provides case studies and practical examples to demonstrate the practical implications of the research findings. Finally, it concludes by emphasizing the significance of the research and presents the overall structure of the article, including sections on security challenges, machine learning integration, attack detection methodologies, case studies, and the conclusion.

2. BACKGROUND

A wireless sensor network is a collection of specialized transducers that are linked together through a communications system to monitor and record conditions in a wide variety of settings [6, 7]. Humidity, temperature, wind speed, pressure, direction, vibration, light, sound, power-line voltage, chemical concentrations, pollution levels, and critical physiological processes are just some of the factors that are tracked in real-time. A sensor network is made up of numerous small sensor nodes, and lightweight, and transportable detecting stations. Each sensor node comes with transducers, microprocessors, transceivers, and a power supply [8]. Based on audible physical activities and processes, the transducer generates electrical signals. The sensor output is processed by the CPU and then stored. A central computer issues orders to the transceiver, which then transmits data to it. Each sensor node is powered by its battery, as shown in Figure 1 [9].

After receiving instructions from the hub, the sensor nodes collaborate to finish the job. Upon collecting the necessary information, the sensor nodes transmit it back to the hub [10]. Connections to other networks may be made online from a base station. Once the base station receives an update from the sensor nodes, it sends the data to the user via the Internet. A single-hop network design is used when each sensor node is linked to the base station. Long-distance transmission will require a lot more energy than data collection and calculation, although it is technically feasible [11].

In wireless sensor networks, there are two different kinds of architectures, which include the following: layered network architecture, as shown in Figure 2, and clustered network architecture [12].

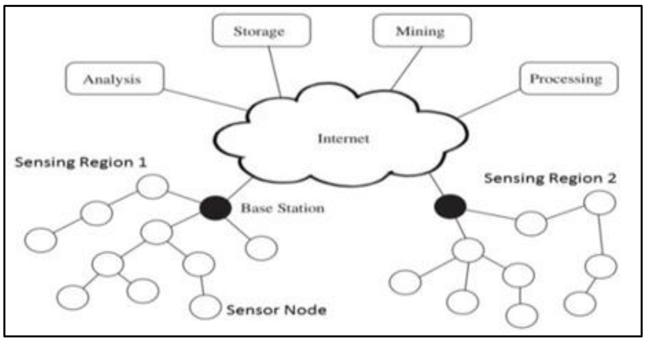

Figure 1. Architecture for wireless sensors

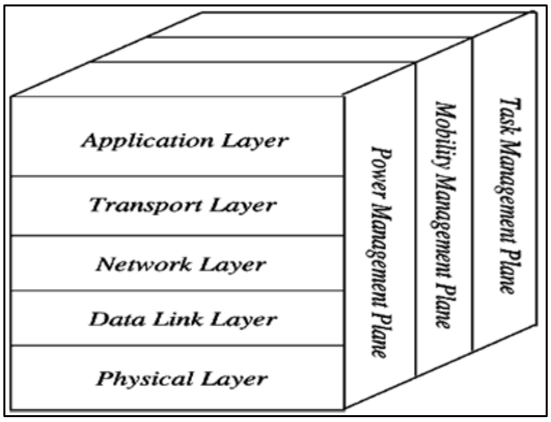

Figure 2. The IP model for WSN

The Layered Network Architecture has five main layers: The Application Layer provides software for various applications that turn data into a form that can be comprehended to discover crucial information in addition to controlling traffic [13]. The transport layer on the upstream, numerous approaches may be used to achieve this goal, but the transport layer's function is to offer dependability and congestion avoidance. These strategies employ several methods for loss detection and loss recovery.

The fact that Transmission Control Protocol (TCP) uses more energy than other protocols to provide trustworthy loss recovery is one of the primary reasons it is inappropriate for WSNs. The classifications of packet-driven and event-driven transport layers are frequently distinguishable. On the transport layer, there are several well-known protocols, such as Pump-Slowly, Fetch-Quickly (PSFQ), and Stream Control Transmission Protocol (STCP).

The Network Layer Routing is the main task, but it also performs a variety of additional tasks, the most crucial of which are power management, partial memory management, buffer management, and the self-organization of sensors without a common Internet address (ID)

The Data Link is in charge of point-to-point (or point-to-multipoint) dependability, multiplexing data stream detection, error management, and Media Access Control address MAC.

Physical Layer The physical layer can be used as an edge to send a stream of bits above the physical medium. This layer is in charge of carrier frequency generation, signal detection, modulation, and frequency selection.

Centralized network management and sensor aggregation are two main purposes of this architecture's cross-layers, the Power Management Plane, Mobility Management Plane, and Task Management Plane.

In the Clustered Network Architecture, various sensor nodes aggregate into clusters in this architecture, which is dependent on the "Leach Protocol" since it employs clusters. The following are the primary characteristics of this architectural Figure 3 [14].

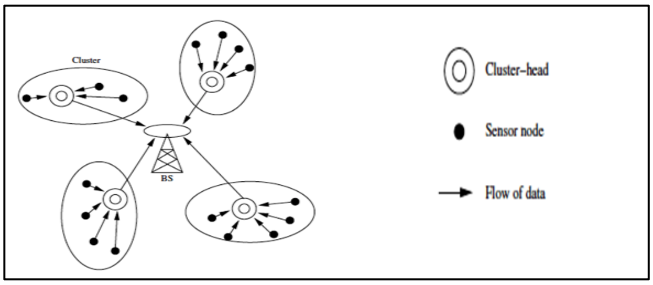

Figure 3. Clustered network architecture

A cluster's nodes may all talk to the master node. All the information collected by the clusters will be sent to the base station. A cluster is formed, and the head of each cluster is chosen using an independent, autonomously distributed approach [15].

3. THE TOPOLOGIES OF WIRELESS SENSOR NETWORKS

The major components of a WSN's structure include several radio communication network topologies including a star, mesh, and hybrid star [16]. These topologies are briefly explained below [17].

3.1 Star network

In situations where only the base station can send or receive messages to distant nodes, a communication architecture similar to a star network is utilized. There are several nodes accessible, but they are prohibited from communicating with one another. The key advantages of this network are its simplicity and its ability to minimize the power consumption of distant nodes. Additionally, it enables communication between a distant node and the base station with minimal delay. This network's fundamental flaw is that every node has to be within the radio range of the base station. Since just one node is required to run the network, it is less reliable than the other one [18].

3.2 Mesh network

A node can use another sensor as an intermediary to convey a message to a destination node if it needs to communicate with another node that is beyond its radio communication range. The main benefits of a mesh network are its scalability and reliability. After a failure of a single node, the message may be sent by a faraway node interacting with any other kind of node within range [19]. The primary drawback of such a network is the excessive amount of energy it consumes, which rapidly depletes the batteries of network nodes engaged in multi-hop conversations. The time it takes to deliver a message grows in proportion to the number of communication hops necessary to reach its destination if the nodes' low-power approach is needed.

3.3 Hybrid star–mesh network

Combining networks like Star and Mesh offers a dependable and adaptable communications system while also decreasing the power requirements of wireless sensor nodes. In this network design, weaker sensor nodes are prohibited from sending data. This makes it possible to maintain minimal power use. But by enabling them to send messages from one network node to another, additional nodes are given the power to multi-hop. The multi-hop nodes often have high power and are regularly connected to the main line. This architecture has been developed using the forthcoming ZigBee mesh networking standard [20].

4. WIRELESS SENSOR NETWORK TYPES

When using wireless sensor nodes to properly link base stations, they may be spread in either an ad hoc or planned fashion on land. The sensor nodes are dropped from a preset plane at random locations over the target area. The battery in WSNs contains solar cells as a backup power source despite the battery's low capability. By adopting low-duty cycles, optimum routing, minimizing delays, and other techniques, WSNs can conserve energy [21].

4.1 Underground wireless sensor networks

Compared to terrestrial WSNs, underground wireless sensor networks are more expensive to construct, maintain, buy the necessary hardware for, and properly design. Numerous sensor nodes are buried to create underground wireless sensor networks, or UWSNs, which are used to monitor conditions underneath. Additional sink nodes are positioned above the surface to transfer data from the sensor nodes to the base station because it is challenging to recharge these earth-buried WSNs. It is challenging to recharge the sensor battery nodes due to their low battery power. Due to the considerable attenuation and signal loss levels in the subterranean environment, wireless communication is particularly difficult [22].

4.2 Underwater wireless sensor networks

More than 70% of the surface of the earth is covered by water. These networks include numerous underwater vehicles and sensor nodes. Data from these sensor nodes is acquired by unmanned underwater vehicles and equipment. Underwater communication may be difficult due to the high propagation latency, limited bandwidth, and sensor failures. WSN batteries are constrained and are not capable of underwater replacement or recharge. The development of underwater networking and communication solutions is required to address the issue of the necessity for energy conservation in underwater WSNs [23].

4.3 Wireless sensor networks for multimedia

It is proposed that multimedia wireless sensor networks be used for the tracking and monitoring of multimedia occurrences. These networks include cheap sensor nodes equipped with cameras and microphones. Multimedia WSN sensory nodes are linked through the wireless network to facilitate data retrieval, compression, and correlation. High bandwidth needs, high energy consumption, processing, and compression methods are some of the difficulties with multimedia WSNs [24].

4.4 Mobile wireless sensor networks MWSNs

Mobile WSN networks are made up of many sensor nodes that may move around autonomously and communicate with the outside world. The mobile nodes feature computational, sensing, and communication capabilities. Compared to static sensor networks, mobile wireless sensor networks are far more flexible. Because of their better and expanded coverage, higher channel capacity, increased energy efficiency, and other advantages, mobile WSNs are preferable to static WSNs [25].

5. WIRELESS SENSOR NETWORK SECURITY CONSIDERATIONS AND REQUIREMENTS

WSNs are susceptible to assault because wireless communications use a broadcast transmission channel and have minimal tamper resistance. As a result, a hacker may eavesdrop on any conversation, send malicious packets, re-establish a connection, or even take over a sensor node. In most cases, the most important aspects of WSN security are privacy protection and node authentication. Secure network connections, particularly between sensor nodes and the management station, are made possible thanks to the attainment of privacy. WSNs are vulnerable to fraud and data theft, however, a secure authentication procedure may prevent these attacks [26].

One challenge WSNs is achieving optimal resource utilization while yet meeting stringent security requirements. Some of the criteria for WSN security include authenticating nodes, keeping data private, protecting against breaches, and not being easily analyzed by traffic researchers. With proper authentication from their respective management nodes or cluster heads, the deployment sensors can identify both dependable and malicious nodes [27]. WSNs may filter out unwanted nodes throughout the authentication process. All packets sent between a management node and a sensor must remain unaltered to prevent eavesdroppers from modifying or decoding them and gaining access to potentially helpful information in WSNs [28]. In addition to the characteristics and elements previously addressed, concerns about and the implementation of security are also critical for a variety of sensor network applications. In recent years, many issues related to the safety of WSNs have been brought to light. In this part, we will go through the various threats and requirements for WSN security [29].

5.1 Passive attacks

Passive attacks (such as eavesdropping assaults) allow snoopers to listen in on a conversation between two parties without really interfering with the transmission [30].

5.2 Active attacks

There are two kinds of aggressive assaults: those from the outside and those from the inside. A few examples of such assaults include node replication attacks, Sybil attacks, wormhole attacks, and compromised nodes. During an external attack like a Sybil attack or wormhole attack, a nonparticipating node can first listen in on packets sent or received by regular participating nodes to maliciously tamper with, interfere with, guess, or spam the data and then inject invalid packets to obstruct the network's operations [31].

A sensor node might falsely claim several IDs for Sybil attacks by either directly creating bogus IDs or by imitating authentic IDs. Distributed storage, routing techniques, and data aggregation may be seriously threatened by this destructive attack [32]. In wormhole attacks [33], the malicious node could be located close to legal nodes, and the malicious entity can use fictional connections that it truly controls to tunnel traffic between legitimate nodes. As a last resort, the rogue node may discard the tunneled packet or attack the routing protocols. Internal assaults are harder to defend against than external ones because compromised members of the target sensor network generally begin them (such as node replication attacks and node-compromised ones) [34]. When a sensor is taken over by an attacker, they may immediately set up several copies of this taken-over node at various locations around the networks. This is known as a node replication assault. By leveraging these compromised nodes, attackers may attempt to compromise the network's operation by, for example, injecting false data [35]. Sensor networks must contend with a variety of passive and active assaults because of their previously identified inherent weaknesses. These attacks might easily obstruct their operation and eliminate the advantages of using their services. Although they can obtain data from the network, passive assaults do not affect how it behaves [36]. Active assaults, on the other hand, obstruct the provision of services directly. The next paragraphs will go into depth about the many risks that affect sensor networks and may be classified into the following categories:

5.3 Common attacks

The wireless medium is very vulnerable to a wide variety of assaults, both passive (eavesdropping) and offensive (hacking). It acts as the WSN's main transmission channel (data injection) [37].

5.4 Denial of service attacks (DoS)

These assaults inhibit any aspect of WSN from operating properly or quickly. Such assaults may aim to block the communication channel or endanger the nodes' lives (e.g. power exhaustion) [38].

5.5 Contamination of a node

After the embedded device has been launched into the wild, it has been compromised if an attacker gains control of it or gains access to it in some other way. These kinds of assaults are often the precursor to far more severe ones [39].

5.6 Side-channel attacks

When performing a cryptographic operation, an attacker can keep track of certain node physical characteristics, such as electromagnetic radiation. The enemy can discover information about the secret key if it affects the recorded physical values [40].

5.7 Impersonation attacks

A rogue sensor node can produce copies with the same identification and various false identities (Sybil attack) (replication attack). The attacker can carry out a variety of malicious assaults by starting with these kinds of attacks [41].

5.8 Protocol-specific attacks

Table 1. Type of attack on WSN layers and defense

Layers	Attacks	Defence
Physical Layer	Jamming Tampering Eavesdropping Interception Radio Interference Node Capturing	Spread Spectrum Priority Messaging Tamper-proofing. Hiding Low Duty Cycle Region Mapping Mode Change Adaptive Antennas
Data link Layer	Jamming Collision Exhaustion Sybil Unfairness Traffic Analysis Monitoring Disruption WEP Weakness Interrogation	Small Frames Rate Limit Error Correcting Code Link Layer Encryption
Network Layer	Black hole, Flooding Sinkhole Homing Wormhole Sybil Selective Forwarding Spoofing Node Capture Resource Exhaustion Denial of Service (DoS) Byzantine Looping	Authentication Monitoring Probing Secure Routing Packet Leashes Authorization Monitoring Egress Filtering Key Management Redundancy Verification
Transport Layer	Flooding DE synchronization False Data Injection Session Hijacking	Client Puzzles Rate Limitation Authentication
Application Layer	Subversion Malicious Nodes	Isolation Malicious Node Detection

Specific attacks that seek to affect the core functions of the network target some crucial WSN protocols, including routing, aggregation, and time synchronization [42].

-As a result of the sensor nodes' poor tamper resistance, attackers may use compromised nodes to establish communication channels with healthy nodes and launch further, more damaging attacks on the sensor network.

- Based on the aforementioned threats, we have determined the following requirements for a safe sensor network:

-Node Authentication: To fulfill this condition, a deployed sensor node must demonstrate its dependability to the other nodes in its local neighborhood and to the supervisor node. By doing so, the supervisor node may verify that the data it got came from a trusted sensor node and not an unauthorized one, preventing the introduction of dangerous data into the networks. In addition, it indicates that the sensor node's authenticity has been confirmed and it has been allowed access to the WSN [43].

-Availability: Even if sensors can only give a minimal amount of processing power, energy, and storage, this shouldn't have any impact on the network's availability.

Therefore, a sensor needs to include a mechanism that controls its sleep cycles if it is to survive for an extended period [44].

-Situational awareness: There is no way for an intruder to spread malware from the compromised sensor node to the remainder of the network. So, to lessen the damage that may be done by unapproved users of a secure communication system, the location awareness method is used [45]. Moreover, the type of Attack on WSN Layers and Defense is presented in Table 1.

6. THE INTERNET OF MEDICAL THINGS APPLICATIONS

In healthcare specifically, IoMT has led to a dramatic increase in treatment quality and positive patient outcomes. Data collected by these apps is often stored in the cloud, making it readily available to doctors who may use it to make instantaneous diagnoses and treatments. This information is also used for medical research and analysis. Some examples of IoT/IoMT communication environment applications such as emergency assistance and management of patient information [46, 47].

Emergency assistance can be challenging to get in touch with a patient's family in the event of an accident or a natural disaster. In these situations, the patient's emergency contact information that is maintained online via IoMT can assist in automatically taking the necessary action [48]. Moreover, in healthcare, patient information management is another area where the IoT shows potential. With the use of the medical Internet of things, sensitive information about the patient, such as their medical history and family medical history, may be safely saved in the cloud (age, sex, allergies, emergency contact information, insurance details, blood group, etc.) When using cloud-based storage [49]. One of the most significant uses of the Internet of things in healthcare is Remote medical help and real-time monitoring. This phenomenon has been made possible by the increase in wearable sensors that patients can wear. These sensors give healthcare professionals real-time data regarding patients' vital signs. Doctors or nurses are immediately informed of any changes in blood pressure, blood glucose levels, and heart rate so they can offer urgent aid. Numerous lives are saved because of this [50]. It can be used to automate every step of the inventory process for medical supplies, including storage, use, requisitions, orders, and inspections. This assures efficient resource use while reducing effort, time, and paperwork.

During emergencies, it can help maintain a tight eye on supplies and guarantee the availability of medications and medical equipment. The medical Internet of things aids in inventory management and equipment located on hospital grounds. Finding supplies like IV drips, wheelchairs, and stretchers is simple and improves healthcare staff productivity [51].

7. WSN IN IOT/IOMT

A network of several monitoring sensors situated in a homogeneous or heterogeneous environment tracks the physiological state of a patient in real-time. Numerous IOT applications for medical equipment, like blood pressure and heart rate monitors, are currently in use and have the potential to completely transform how the healthcare sector operates. There are growing fears that the connection of these medical devices may negatively impact clinical treatment and patient safety since it exposes them to security breaches [52].

8. THE COMMON NETWORK ATTACKS AGAINST IOMT

8.1 Attack on the service

The goal of this attack is to compromise the accessibility of a system, in this case, one that handles medical data or is part of the IoMT (Internet of Medical Things). IoMT gadgets often have poor specs, such as limited memory, bandwidth, battery life, and storage capacity. Because of this, they are very vulnerable to denial-of-service (DoS) attacks. It is common for hackers to launch denial of service (DoS) attacks on hospital networks to disrupt patient care. Once these assaults are underway, they prevent deserving patients from obtaining proper treatment, including potentially lifesaving drugs. Moreover, the attacks make it difficult or impossible for clinicians to access patient records [53].

8.2 Hole attacks

Attack of the Sinkholes: The attacking nodes (noted SHA: sinkhole attacker) start their activity by luring other trustworthy nodes in search of the quickest route to the target. As the legitimate nodes begin the process of sending their packets along the same route (i.e., via SHA), the attacking nodes begin to obstruct network traffic in one of four ways: either by refusing to drop any packets (hoping to avoid detection by the IDS), by failing to deliver the information that the destination stations require, or by delivering incomplete or modified data. Consequences include a decline in the performance of the network and a deterioration in the effectiveness and dependability of communication [54].

8.3 Attack by a blackhole

In this attack, the malicious node discards every packet that it gets from its neighbors, and that is meant to be sent to other nodes. When the blackhole node is also a sinkhole, this assault is more dangerous. As a result, all data flow surrounding the black hole stops. This assault is also known as "selfishness" in the literature [55].

8.4 Greyhole attack

This Blackhole attack variation is also known as "selected forwarding" or "select and forwarding." In this instance, the rogue node only drops a portion of the packets it receives. The IDS has a difficult time identifying this assault. Packet forwarding is a key duty of a routing node in multi-hop networks. However, in a selective forwarding attack, the adversarial nodes can prevent some messages from being forwarded by simply discarding them and making sure that such packets are no longer given to the neighbors. The blackhole attack exposes the attacker to the possibility that the surrounding nodes may opt to look for an alternative route after concluding that they have failed. In the Greyhole assault, the attacker reduces the likelihood that his nefarious deeds will be suspected by sending some of the traffic to nearby neighbors [56, 57]. Moreover, a wormhole Attack is carried out when a network node that is maliciously connected to by an attacker is given connections that allow it to send packets more quickly than is typical for data transport. As a result, a wormhole develops in the network [58].

8.5 Replay attack

Through the use of redirection, the attacker in this attack can either steal or intercept delivered information. Medical systems are only one type of system that might suffer harm. Before being "played back" later the receiving device, the intercepted packets are first recorded. This assault might have two outcomes: theft and the revealing of private information to get access to a specific medical system. The attack's basic strategy is to trick the recipient by having data saved by a hostile node without any permission and then retransmitted to it [59]. To connect with the receiver while posing as the original sender, the malicious sensor first records network traffic. It is mostly used to prevent authentication, especially when certificates are involved. Even if the communications are encrypted in this situation, the attacker can still access the network by retransmitting legitimate connection messages without knowing the genuine keys or passwords [60].

8.6 Sybil attack

A node attempts to gain many identities unlawfully, which causes redundancy in the routing protocol. Attacks via Sybil compromise data security, resource utilization, and integrity. The Sybil node uses the identity of the regular node to contact nearby nodes. The Sybil node can create a new identity or act following an accepted and legitimate one. The network becomes disorganized as a result and eventually collapses [61]. A sensor can fail at any time in a typical network scenario owing to a lack of power. In this situation, a cunning attacker can quickly change the sensor and carry out harmful operations. Patient data can be modified by the attacker, and fake information can be added [62].

9. LITERATURE REVIEW

Wireless sensor networks suffer from harmful impacts and data loss. The introduction of new, demanding technologies has prompted an investigation into the security and privacy issues of networking.

In 2022, the researchers created a deep learning model for wireless sensor networks' approach to detecting cyber-attacks [61]. Based on deep learning technology, a cyber-attack detection approach for wireless sensor networks (WSN) is suggested. This approach utilizes the Message Queuing Telemetry Transport (MQTT) protocol-dependent data transfer as well as the node behavior of the WSN.

The approach is built using a combination of convolutional neural networks (CNN) and long-term memory (LSTM) deep learning algorithms. It was used to categorize the different sorts of attacks that were found in the MQTT2020 dataset that was used for adoption. When comparing this hybrid model to the conventional CNN or LSTM-alone deep learning models, the predictive performance is greater than the CNN-LSTM model, where characteristics are picked out and fed into the shown architecture. The initial convolution with the kernel is constructed using the ReLU function, with the dimensions (3×1×128) and bias (128). The bias and size of the second kernel convolution are 128 and (3×128×128). So far, the stage's output has been routed into the Maxpooling layer 1D. The last two convolution layers are built with biases of 64 and 32, and dimensions of 3×128×64 and 3×64×32. The Tanh function is used to generate a weight matrix from the LSTM layer, and the matrix's dimensions are (32, 128). As part of the batch normalization, we use parameters of gamma =32, beta =32, moving mean =32, and moving variance =32. In Dropout, the 6 is fully connected to the 1x1 matrix, rounding out the notion. The method will be used to classify the various forms of attack included in the MQTT2020 dataset. The results of deep learning are 96.02 for CNN LSTM Techniques for the training stage and 95.08 for the validation stage. The machine learning models are 87% and 91%. The limitations of this study are We need more information about cyber security attacks by providing examples of attacks and improving data accuracy. This study only applied to one data set and not to more than one data set. In 2022, Gulganwa and Jain [62], the researchers developed a data-driven, machine learning-based weighted clustering algorithm that is secure and energy-efficient (EES-WCA). The EES-WCA combines the EE-WCA and a centralized intrusion detection system that uses machine learning (IDS). Instead of disrupting the usual operations of WSN, this technique begins by constructing network clusters and then collects traffic samples at the base station. The base station utilizes many machine learning models, such as Support Vector Machine (SVM) and Multi-Layer Perceptron, to categorize traffic data and detect malicious nodes in the network (MLP). Both simulated traffic generated in the NS2.35 simulator and traffic generated in real-world scenarios are utilized to verify the strategy's success.

In 2022, Almomani et al. [63], the authors of this paper created a unique hybrid deep learning framework for intrusion detection systems in WSN-IoT networks. Multiple hybrid deep learning models, such as spotted hyena optimization (SHO), long short-term memory (LSTM), and multi-tiered intrusion detection (MITID), have been studied to create an effective IDS (MDIT). The suggested system's real-time data layer consists of two parts. In the first phase, wireless nodes are deployed in real-time to capture data, and energy-efficient hierarchical clustering is applied. Many attacks were made on the system during phase two. In the second stage, several features are extracted from the cleaned and prepared data to train the proposed model. Third layer shole networks were built to classify attacks into their respective categories. In this study, we provide a procedure for identifying the attacker and the specific type of malicious node. The Node's Multi-Core Processing Unit (MCU) The CIDDS-001, UNSWNB15, and KDD++ datasets, as well as other conventional and cutting-edge learning models, have been used in extensive field testing of our embedded boards and industry-standard benchmarks. The single data set used in this research is one of its main flaws.

In 2021, Maheswari and Karthika [64], the researchers developed DRNDC (Deep Radial Basis Network Defense Countermeasures) for WSNs. This paper suggests using radial basis networks for attack detection and isolation that are based on deep learning. The DRBN algorithm is provided for efficient detection of DoS assaults such as depletion, jamming, flooding, and others. After comprehensive modeling studies are carried out to precisely distinguish them, the malevolent nodes are demonstrated to be more resistant to DoS attacks. The DRBN framework's important module for attack detection employs the available sub-modules to identify various forms of assault. Almost all of the modules in this detecting unit are independent of one another, and the communication module is the only one that converts data. In a real-time setting, the detecting modules dynamically acquire the parameters. The flag number for each mobile or continuous sub-module is determined by the defensive unit. As a result, the communication module gets the detected information. apply on one data set.

In 2021, Gowdhaman and Dhanapal [65], the team developed a method of intrusion detection for WSNs using a deep neural network. This study introduces a deep neural network-based intrusion detection system (DNN). With the help of a cross-correlation technique, we extract the most relevant characteristics from the dataset and utilize them as the building blocks for a deep neural network architecture that keeps an eye out for security breaches.

There are two states in the proposed intrusion detection system. The first stage involves choosing the best traits, while the second stage includes categorization. Cross-correlation methodology is used in the first step to choose the best features, and a deep neural network is employed in the second stage to identify network intrusion. The suggested work uses a deep learning technique rather than a typical machine learning-based categorization procedure since it offers additional benefits. Through effective computing, the deep learning-based technique not only effectively identifies the intrusion but also lowers the network's energy usage. The normalization procedure first reduces the data to numerical values before choosing the best characteristics.

The NSLKDD dataset and experiments that structure the suggested design are used to assess the model. The limitation of this study is the need to increase the precession and accuracy. Moreover, the need for effective cyber-attack detection inspired the adoption of deep recurrent neural networks and machine learning methods in The Internet of Medical Things [66]. A Smart Environment. The primary objective is to demonstrate how supervised machine learning models such as a random forest, decision tree, KNN, and ridge classifier may be used to build an efficient and effective IDS in the IoMT environment for classifying and predicting unknown cyber threats. Networked data cleaning and standardization. They employed a particle swarm technique, which has its roots in biology, to improve the characteristics. We do comprehensive assessments of DRNN and other SML studies using data from regular intrusion detection systems. DoS assaults, probing attacks, remote-to-local attacks, and user-to-root attacks are the primary targets of this technique's detection. After being collected by various medical sensors within the patient's body, the data is sent via a gateway and a router before finally reaching servers. During transmission from the gateway to the servers, a potential eavesdropper may make unauthorized changes or even employ denial-of-service attacks to prevent the therapeutic data from being shown. This system uses data filtering to provide information in a logical, usable format. Inconsistent string attributes were converted to numerical variables, and the data was cleaned up as a result. At the same time, a faulty part is taken out of the equation. This research has limitations due to its reliance on a single data collection.

In 2020, Saheed and Arowolo [67], they suggested using an intrusion detection system as the backbone for a man-in-the-middle attack approach for WSNs. Outline the concept of a Man-in-the-Middle Attack Detection System (MITM-IDS) for identifying intruders and isolating compromised nodes so that they may be re-configured. Intruder Detection System Method aids nodes in preparing for future assaults. The simulation's productivity rate for conducting MITM attacks is 89.14%. The goal of this research is to develop an IDS that can withstand attacks. The limitations of this study are applied to one data set and given low accuracy. In 2019, Mohapatra et al. [68] proposed a distributed algorithm to defend it and a model of Sybil's attack in cluster-based WSN. The first step is the proposal of a unique Sybil attack model for cluster-based sensor networks. According to the suggested attack paradigm, a malicious node joins each cluster in the network using a different Sybil identity. As a result, the rogue node concurrently joins several network clusters. Additionally, a distributed technique based on placement with three points and the Received Signal Strength Indicator is suggested to counter the unique assault paradigm and the limitation is Less input.

In 2018, Jamshidi et al. [69] offered a thorough empirical research target aimed at analyzing several data mining methods (DMTs) utilizing a fresh, public dataset specifically designed for WSN networks (named WSN-DS). To effectively identify major Denial of Service (DoS) assaults, which harm the services offered by WSNs, an effective IDS must be made available. In this study, eight DMTs are considered. They were initially attempted, utilizing all the WSN characteristics and DS's, and their detection precision and time complexity were assessed. The limitation of this study is that it uses one dataset. In 2017, Almomani and Alenezi [70], they presented a method to boost the effectiveness of cloud-based systems that use wireless sensor networks. To prevent sinkholes, black holes, and selective forwarding attacks, WSNs may be equipped with intrusion detection features by modifying the low-energy adaptive clustering hierarchy (LEACH) protocol. LEACH++ is the name given to the modified protocol.

During the literature review, several research studies were examined to gain insights into existing approaches and techniques for addressing security challenges in the Internet of Medical Things (IOMT) environment. While these studies have contributed to the understanding of IOMT security. Many studies rely on synthetic or limited datasets, which may not fully capture the complexity and diversity of network traffic patterns and attack scenarios encountered in actual IOMT environments. Future research should aim to collect and utilize more diverse and realistic datasets to evaluate the effectiveness and generalizability of proposed security approaches. Another limitation is the focus on specific types of attacks or attack scenarios, neglecting the broader spectrum of potential threats in the IOMT environment. For instance, some studies primarily address network-level attacks, while others focus on device-level attacks. Future research should strive for a more holistic approach that considers the entire attack surface of the IOMT ecosystem, including attacks targeting devices, communication channels, and data storage and processing systems. This comprehensive approach will enable the development of robust security mechanisms that can address a wide range of threats. Furthermore, several studies rely on assumptions that may not hold in practical IOMT deployments. These assumptions can include ideal network conditions, homogeneous device populations, or trusted communication channels. To enhance the applicability of research findings, future studies should consider real-world deployment scenarios, accounting for the inherent heterogeneity, dynamic network conditions, and potential vulnerabilities of the IOMT environment. This will ensure that proposed security measures are effective and viable in real-world settings. Additionally, many existing studies focus predominantly on the detection aspect of security, neglecting the importance of preventive measures and mitigation strategies. While detection is crucial, future research should emphasize the development of proactive security mechanisms that can prevent attacks, identify vulnerabilities, and establish robust defenses against emerging threats in the IOMT environment. This shift towards a more proactive security approach will significantly enhance the resilience and overall security posture of the IOMT ecosystem. To address these limitations in future research, several approaches can be adopted. First, researchers should collaborate with healthcare providers, device manufacturers, and other stakeholders to gain access to real-world datasets that accurately reflect the complexities of the IOMT environment. This collaboration will enable the evaluation of proposed security mechanisms under realistic conditions and facilitate the development of more effective and practical solutions. Second, future research should adopt a multidisciplinary approach by integrating expertise from various fields, such as cybersecurity, healthcare, and data science. This collaboration will enable a more holistic understanding of the IOMT environment and the diverse security challenges it presents. By leveraging interdisciplinary knowledge, researchers can develop comprehensive and context-aware security solutions that address the unique requirements of the IOMT ecosystem. Finally, researchers should actively engage in testing and validating proposed security measures in real-world IOMT deployments. Conducting pilot studies or collaborating with healthcare institutions to conduct field trials will provide valuable insights into the feasibility, scalability, and effectiveness of proposed security mechanisms. Additionally, feedback from healthcare professionals and end-users should be solicited to ensure that the developed solutions align with their practical needs and requirements. By addressing these limitations and incorporating the suggested approaches, future research in the field of IOMT security can make significant strides toward developing robust and practical security measures that effectively safeguard the integrity, confidentiality, and availability of interconnected medical devices and healthcare systems. Table 2 summarizes the literature review.

Table 2. Summary of literature review

Reference	Environment	Type of Attack	Approaches	Data Set	Limitations	Aims
[61]	WSN	Cyber attacks	Efficient classification of cyber-attacks was presented.	MQTT2020 data set	Need more information about the cyber security attack by giving some examples about the attacks	Improve accuracy by maximizing the utilization of a variety of deep learning approaches.
[62]	WSN	the malicious nodes in the network	Energy-efficient and secure weighted clustering algorithm that is data-driven and machine learning-based (EES-WCA).	The dataset for training, the dataset contains six meaningful attributes or characteristics, additionally seven .classes	Low accuracy	Identifying the malicious node and attack type
[63]	IOT	malicious node different attacks	LSTM network was included in the Spotted Hyena Optimizer.	The real-time datasets were collected using the embedded CPU interfaced with esp8266 transceivers The real-time datasets were collected using the embedded CPU interfaced with esp8266 transceivers The real-time datasets were collected using the embedded CPU interfaced with the esp8266 transceiver	Apply on one data set	Identifying the malicious node and attack type
[64]	WSN	DoS such as depletion, jamming flooding	DoS such as depletion, jamming flooding.	Public data set with DoS attack	Apply on one data set	Identifying and segregating the DoS assaults and improving deep learning via the use of various optimization techniques has led to a decrease in node energy consumption and an improvement in node longevity.
[65]	WSN		The deep learning-based technique The normalization procedure.	NSLKDD	Need to increase the precession and accuracy	Lowers the network's energy usage. reduces the data to numerical values before choosing the best characteristics.

[66]	IOMT	DoS, probing attacks, and remote to local and user to root attacks	(DRNN) and supervised machine learning models.	Data is sent from the patient's body through a number of medical sensors	Applied on one data set	The paper shows how to build an efficient and successful model using a deep recurrent neural network (DRNN) and supervised machine learning models (such as a random forest, decision tree, KNN, and ridge classifier). IDS in the IoMT environment for categorizing and foretelling unexpected cyber threats.
[67]	WSN	Man-in-the-Middle Attack Handling	Focuses on MITM intrusion detection system (MITM-IDS) based on neural network, genetic algorithm, fuzzy logic.	Centralized database network	Applied on one data set and given low accuracy	Develop an IDS that can withstand attacks.
[68]	WSN	Sybil Attack	Sybil attack model is suggested, and a distributive method based on RSSI and participation of cluster head nodes is proposed to counter it.	Sybil nodes	Less number of input	Distributed algorithm based on Received Signal Strength Indicator and positioning using three points to defend against the novel attack model.
[69]	WSN	Denial of Service (DoS)	Eight DMTs are considered firstly using all existing features and evaluated in terms of detection accuracy and time complexity. Moreover, a feature selection algorithm has been applied to reduce around 53% of overall features.	WSN data set	Applied on one data set	Examining several Data mining techniques (DMTs) using a new specialized, published dataset for WSN networks.
[70]	WSN	Protect Wireless Sensor Networks (WSNs) Against Attacks Like Sinkholes, Black Holes, and Selective Forwarding	Run simulations in Network Simulator-2 (NS-2) to back up the findings of the numerical analysis and assess the influence on throughput and energy consumption.	WSN-DS	Applied on one data set	Provide intrusion detection capabilities to the low-energy adaptive clustering hierarchy (LEACH) protocol for wireless sensor networks.

The above table exhibits the literature survey of WSN attack detection using different techniques of a deep learning model from 2017 to 2022. Moreover, the size of the dataset is another important consideration. Larger datasets generally provide more representative samples of network traffic and attack patterns, leading to more accurate and reliable results. However, collecting extensive real-world datasets can be challenging due to privacy concerns and logistical constraints. Researchers should strive to strike a balance between dataset size and practicality, ensuring that the collected data is large enough to capture the essential characteristics of the IOMT environment while being feasible to obtain and process. In addition to using real-world datasets, it is crucial to consider using more than one dataset to enhance the robustness and generalizability of the proposed approaches. Multiple datasets offer a broader perspective on network behaviors and attack patterns, allowing for a comprehensive evaluation of the proposed security mechanisms. Different datasets may exhibit variations in terms of network traffic volume, device types, communication protocols, and attack scenarios. By incorporating multiple datasets, researchers can assess the performance and effectiveness of their approaches across diverse IOMT environments, validating the robustness and generalizability of their findings. Furthermore, the relevance of the datasets to the research objectives should be carefully considered. The datasets should cover a wide range of network traffic patterns, including normal behavior, known attack types, and potentially new or emerging attack patterns. This ensures that the proposed approaches are capable of detecting both known and unknown attacks within the IOMT environment. The datasets should also reflect the specific characteristics and challenges of the IOMT ecosystem, such as resource-constrained devices, wireless communication, and the criticality of healthcare data. By utilizing real-world datasets that accurately reflect the characteristics of the IOMT environment and incorporating multiple datasets to ensure robustness and generalizability, future research can enhance the validity and effectiveness of proposed security approaches. This approach will provide more confidence in the performance and applicability of the proposed mechanisms, leading to improved security measures for interconnected medical devices and healthcare systems.

Moreover, the evaluation of attack detection techniques in research studies involves the use of various performance evaluation metrics to measure the effectiveness of the proposed models. These metrics provide quantitative measures of how well the detection techniques perform in terms of accuracy, efficiency, and robustness. These metrics include Precision, Recall, and F1 Score 1. The significance of these performance evaluation metrics lies in their ability to provide an objective assessment of the attack detection techniques. They help researchers compare different models, identify strengths and weaknesses, and validate the effectiveness of the proposed approaches. By considering multiple metrics, researchers can gain a comprehensive understanding of the models' performance characteristics, ensuring that the selected techniques meet the specific requirements of the IOMT security context. It is important to note that the choice of performance evaluation metrics should align with the research objectives and the specific characteristics of the IOMT environment. For example, in a healthcare setting, where false negatives (missed detections) can have severe consequences, recall and F1 Score may be of particular importance. Additionally, the selection of metrics should consider any class imbalance in the dataset to ensure a fair assessment of the models' performance.

10. CHALLENGES AND OPEN RESEARCH ISSUES

Significant strides have been made in WSN attack detection, yet numerous challenges and research gaps persist, necessitating a concerted effort to bolster WSN security. The critical challenges encompass energy efficiency, given the resource-constrained nature of WSN environments, urging the development of energy-conscious detection methods to prolong sensor node lifetimes. Scalability is paramount, with the burgeoning volume of network traffic and nodes demanding scalable detection techniques capable of handling large-scale WSNs without compromising accuracy. Real-time detection is imperative for prompt response, but maintaining low false positive rates remains elusive. Adaptive and resilient detection mechanisms are essential to counteract evolving attack strategies, necessitating exploration into AI-driven approaches. Ensuring secure communication is pivotal, calling for robust protocols to safeguard data integrity and confidentiality. Intrusion-tolerant techniques are vital to maintaining network functionality despite compromised nodes, while privacy preservation measures are imperative to protect sensitive data. Cross-layer approaches integrating information from multiple layers promise enhanced detection accuracy. Real-world evaluation remains a challenge, demanding extensive field experiments for validation. Standardization efforts are crucial for fair comparisons and reproducibility. Addressing these challenges through interdisciplinary collaboration and innovative methodologies will fortify WSN security, enabling their widespread and secure deployment in critical applications.

11. CONCLUSION

This research has provided a comprehensive analysis of the security challenges faced by wireless sensor networks (WSNs) in the context of the Internet of Medical Things (IOMT). The distributed and resource-constrained nature of WSNs introduces vulnerabilities and potentially malicious activities, posing significant risks to the integrity and availability of sensitive medical information. However, by leveraging machine learning and deep learning technologies, effective countermeasures can be developed to mitigate these security concerns. The integration of machine learning algorithms and deep learning techniques enables real-time analysis of large datasets and the detection of anomalous behavior or patterns indicative of network attacks. This research has emphasized the practical implications of these technologies within the IOMT context, such as monitoring prescription orders and tracking patients' movements. By employing advanced methodologies, robust and efficient methods for attack detection and prevention can be developed, enhancing the security and reliability of wireless sensing systems in critical medical domains. The findings of this research contribute to the advancement of secure and reliable wireless sensing systems in the IOMT environment. By addressing the security challenges specific to WSNs enhanced by machine learning and deep learning, this research provides insights into potential fixes based on various approaches and theories. The practical examples and scenarios presented demonstrate the relevance and applicability of the research findings in real-world settings.

In summary, this research emphasizes the importance of addressing security challenges in WSNs within the IOMT environment and proposes practical solutions and countermeasures. By leveraging machine learning and deep learning technologies, the research contributes to the development of robust methods for detecting and mitigating network attacks.

REFERENCES

[1] Abdulkarem, M., Samsudin, K., Rokhani, F.Z., A Rasid, M.F. (2020). Wireless sensor network for structural health monitoring: A contemporary review of technologies, challenges, and future direction. Structural Health Monitoring, 19(3): 693-735. https://doi.org/10.1177/1475921719854528

[2] Kumar Gupta, D. (2013). Network and Complex Systems A Review on Wireless Sensor Networks, 3(1): 2013

[3] Alani, S., Zakaria, Z., Saiedi, T., Ahmad, A., Mahmood, S.N., Saad, M.A., Ma'ath Abdulla, A. (2020). A review on UWB antenna sensor for wireless body area networks. In 2020 4th International Symposium on

Multidisciplinary Studies and Innovative Technologies (ISMSIT), Istanbul, Turkey, pp. 1-10. https://doi.org/10.1109/ISMSIT50672.2020.9254219

[4] Lykov, S., Asakura, Y., Hanaoka, S. (2017). Positioning in wireless sensor network for human sensing problem. Transportation Research Procedia, 21: 56-64. https://doi.org/10.1016/j.trpro.2017.03.077

[5] Manickam, P., Mariappan, S.A., Murugesan, S.M., Hansda, S., Kaushik, A., Shinde, R., Thipperudraswamy, S.P. (2022). Artificial intelligence (AI) and internet of medical things (IoMT) assisted biomedical systems for intelligent healthcare. Biosensors, 12(8): 562. https://doi.org/10.3390/bios12080562

[6] Niranjan, S. (2015). Wireless sensor networks. International Journal of Engineering Research & Technology (IJERT).

[7] Saad, M.A., Alhamdane, H.J., Ali, S.A.H., Hashim, M.M., Hasan, B. (2020). Total energy consumption analysis in wireless mobile ad hoc network with varying mobile nodes. Indonesian Journal of Electrical Engineering and Computer Science, 14(2): ab-cd.

[8] Widhalm, D., Goeschka, K.M., Kastner, W. (2021). An open-source wireless sensor node platform with active node-level reliability for monitoring applications. Sensors, 21(22): 7613. https://doi.org/10.3390/s21227613

[9] Rashid, S.A., Hamdi, M.M., Alani, S. (2020). An overview on quality of service and data dissemination in VANETs. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Ankara, Turkey, pp. 1-5. https://doi.org/10.1109/HORA49412.2020.9152828

[10] Zhao, J. (2022). Application of wireless sensor network technology in multipoint control in music performance management system. Computational Intelligence and Neuroscience, 2022: 2783944. https://doi.org/10.1155/2022/2783944

[11] Hosseini, S.A., Abd Ali, D.M., Mohammed, M.Q. (2018). Efficient routing protocol algorithm for wireless sensor networks. Iraqi Journal for Computers & Informatics.

[12] Singh, A.P., Luhach, A.K., Gao, X.Z., Kumar, S., Roy, D.S. (2020). Evolution of wireless sensor network design from technology centric to user centric: an architectural perspective. International Journal of Distributed Sensor Networks, 16(8): 1550147720949138. https://doi.org/10.1177/1550147720949138

[13] Ranganathan, D. (2021). Cross-layer design in sensor networks: Issues and possible solutions. 1-9.

[14] Behera, T.M., Samal, U.C., Mohapatra, S.K., Khan, M.S., Appasani, B., Bizon, N., Thounthong, P. (2022). Energy-efficient routing protocols for wireless sensor networks: Architectures, strategies, and performance. Electronics, 11(15): 2282. https://doi.org/10.3390/electronics11152282

[15] Gielow, F., Jakllari, G., Nogueira, M., Santos, A. (2015). Data similarity aware dynamic node clustering in wireless sensor networks. Ad Hoc Networks, 24: 29-45. https://doi.org/10.1016/j.adhoc.2014.07.008

[16] Verma, S. (2013). Network topologies in wireless sensor networks: A review 1. International Journal of Electronics & Communication Technology, 4(3): 1-5.

[17] Ibrahim, D.S. Zaidan, F.K. Kadum, J. Saleh, H.H., Rasheed, L.T., Nsaif, W.S. (2021). Routing Protocols - based Clustering in WSNs. in 4th International Iraqi Conference on Engineering Technology and Their Applications, IICETA, pp. 201–205. https://doi.org/10.1109/IICETA51758.2021.9717419.

[18] Raza, S., Faheem, M., Guenes, M. (2019). Industrial wireless sensor and actuator networks in industry 4.0: Exploring requirements, protocols, and challenges—A MAC survey. International Journal of Communication Systems, 32(15): e4074. https://doi.org/10.1002/dac.4074

[19] Dettmann, C.P., Georgiou, O., Pratt, P. (2018). Spatial networks with wireless applications. Comptes Rendus Physique, 19(4): 187-204. https://doi.org/10.1016/j.crhy.2018.10.001

[20] Majid, M., Habib, S., Javed, A.R., Rizwan, M., Srivastava, G., Gadekallu, T.R., Lin, J.C.W. (2022). Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review. Sensors, 22(6): 2087. https://doi.org/10.3390/s22062087

[21] Karim, S., Shaikh, F.K., Aurangzeb, K., Chowdhry, B.S., Alhussein, M. (2021). Anchor nodes assisted cluster-based routing protocol for reliable data transfer in underwater wireless sensor networks. IEEE Access, 9: 36730-36747. https://doi.org/10.1109/ACCESS.2021.3063295

[22] Sharma, P., Singh, R.P., Mohammed, M.A., Shah, R., Nedoma, J. (2021). A survey on holes problem in wireless underground sensor networks. IEEE Access, 10: 7852-7880. https://doi.org/10.1109/ACCESS.2021.3140038

[23] Wei, X., Guo, H., Wang, X., Wang, X., Qiu, M. (2021). Reliable data collection techniques in underwater wireless sensor networks: A survey. IEEE Communications Surveys & Tutorials, 24(1): 404-431. https://doi.org/10.1109/COMST.2021.3134955

[24] Kadiravan, G., Sujatha, P., Asvany, T., Punithavathi, R., Elhoseny, M., Pustokhina, I.V., Shankar, K. (2021). Metaheuristic clustering protocol for healthcare data collection in mobile wireless multimedia sensor networks. Computers, Materials & Continua, 66(3): 3215-3231. https://doi.org/10.32604/cmc.2021.013034

[25] Fahad, A.M., Alani, S., Mahmood, S.N., Fahad, N.M. (2019). Ns2 based performance comparison study between DSR and AODV protocols. International Journal of Advanced Trends in Computer Science and Engineering, 8(1): 379-393.

[26] Ganesh, D.E. (2022). Analysis of wireless sensor networks through secure routing protocols using directed diffusion methods. International Journal of Wireless Network Security, 7(2): 28-32. https://doi.org/10.37591/IJWNS

[27] Vaseghi, B., Pourmina, M.A., Mobayen, S. (2017). Secure communication in wireless sensor networks based on chaos synchronization using adaptive sliding mode control. Nonlinear Dynamics, 89(3): 1689-1704. https://doi.org/10.1007/s11071-017-3543-9

[28] Rhim, H., Sauveron, D., Abassi, R., Tamine, K., Guemara, S. (2021). A secure protocol against selfish and pollution attacker misbehavior in clustered WSNs. Electronics, 10(11): 1244. https://doi.org/10.3390/electronics10111244

[29] Pathan, A.S.K., Lee, H.W., Hong, C.S. (2006). Security in wireless sensor networks: issues and challenges. In 2006 8th International Conference Advanced

Communication Technology, Phoenix Park, pp. 6. https://doi.org/10.1109/ICACT.2006.206151

[30] Yang, G., Dai, L., Wei, Z. (2018). Challenges, threats, security issues and new trends of underwater wireless sensor networks. Sensors, 18(11): 3907. https://doi.org/10.3390/s18113907

[31] Singh, R., Singh, J., Singh, R. (2016). TBSD: a defend against sybil attack in wireless sensor networks. International Journal of Computer Science and Network Security, 16(11): 90-99.

[32] Dhamodharan, U.S.R.K., Vayanaperumal, R. (2015). Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method. The Scientific World Journal, 2015: 841267. https://doi.org/10.1155/2015/841267

[33] Ghugar, U., Pradhan, J. (2021). Survey of wormhole attack in wireless sensor networks. Computer Science and Information Technologies, 2(1): 33-42. https://doi.org/10.11591/csit.v2i1.p33-42

[34] Ding, C., Yang, L., Wu, M. (2017). Localization-free detection of replica node attacks in wireless sensor networks using similarity estimation with group deployment knowledge. Sensors, 17(1): 160. https://doi.org/10.3390/s17010160

[35] Sharma, G., Vidalis, S., Anand, N., Menon, C., Kumar, S. (2021). A survey on layer-wise security attacks in IoT: Attacks, countermeasures, and open-issues. Electronics, 10(19): 2365. https://doi.org/10.3390/electronics10192365

[36] Kalnoor, G., Agarkhed, J. (2018). Intrusion threats and security solutions in wireless sensor networks. International Robotics & Automation Journal, 4(1): 00093. https://doi.org/10.15406/iratj.2018.04.00093

[37] Keerthika, M., Shanmugapriya, D. (2021). Wireless sensor networks: Active and passive attacks-vulnerabilities and countermeasures. Global Transitions Proceedings, 2(2): 362-367. https://doi.org/10.1016/j.gltp.2021.08.045

[38] 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. https://doi.org/10.1007/s11277-020-07776-3

[39] 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. https://doi.org/10.1016/j.jnca.2021.103118

[40] Cao, Y., Zhao, X., Ye, W., Han, Q., Pan, X. (2018). A compact and low power RO PUF with high resilience to the EM side-channel attack and the SVM modelling attack of wireless sensor networks. Sensors, 18(2): 322. https://doi.org/10.3390/s18020322

[41] Darbandeh, F.G., Safkhani, M. (2020). A new lightweight user authentication and key agreement scheme for WSN. Wireless Personal Communications, 114(4): 3247-3269. https://doi.org/10.1007/s11277-020-07527-4

[42] O'Mahony, G.D., Harris, P.J., Murphy, C.C. (2018). Analyzing the vulnerability of wireless sensor networks to a malicious matched protocol attack. In 2018 International Carnahan Conference on Security Technology (ICCST), Montreal, QC, Canada, pp. 1-5. https://doi.org/10.1109/CCST.2018.8585681.

[43] Jawad, K., Mansoor, K., Baig, A.F., Ghani, A., Naseem, A. (2019). An improved three-factor anonymous authentication protocol for WSN s based iot system using symmetric cryptography. In 2019 International Conference on Communication Technologies (ComTech), Rawalpindi, Pakistan, pp. 53-59. https://doi.org/10.1109/COMTECH.2019.8737799

[44] Gulati, K., Boddu, R.S.K., Kapila, D., Bangare, S.L., Chandnani, N., Saravanan, G. (2022). A review paper on wireless sensor network techniques in Internet of Things (IoT). Materials Today: Proceedings, 51: 161-165. https://doi.org/10.1016/j.matpr.2021.05.067

[45] Loh, T.H., Lin, H. (2020). On the improvement of positioning accuracy in wireless sensor network using smart antennas. In 2020 IEEE Eighth International Conference on Communications and Networking (ComNet), Hammamet, Tunisia, pp. 1-4. https://doi.org/10.1109/ComNet47917.2020.9306083

[46] Kurda, R.M.S., Haje, U.A., Abdulla, M.H., Khalid, Z.M. (2021). A review on security and privacy issues in IoT devices. Academic Journal of Nawroz University, 10(4): 192-205. https://doi.org/10.25007/ajnu.v10n4a1245

[47] Mohammadzadeh, N., Gholamzadeh, M., Saeedi, S., Rezayi, S. (2023). The application of wearable smart sensors for monitoring the vital signs of patients in epidemics: A systematic literature review. Journal of ambient Intelligence and Humanized Computing, 14: 6027-6041. https://doi.org/10.1007/s12652-020-02656-x

[48] Dias, D., Paulo Silva Cunha, J. (2018). Wearable health devices-vital sign monitoring, systems and technologies. Sensors, 18(8): 2414. https://doi.org/10.3390/s18082414

[49] Vishnu, S., Ramson, S.J., Jegan, R. (2020, March). Internet of medical things (IoMT)-An overview. In 2020 5th international conference on devices, circuits and systems (ICDCS), Coimbatore, India, pp. 101-104. https://doi.org/10.1109/ICDCS48716.2020.243558

[50] Dwivedi, R., Mehrotra, D., Chandra, S. (2022). Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. Journal of Oral Biology and Craniofacial Research, 12(2): 302-318. https://doi.org/10.1016/j.jobcr.2021.11.010

[51] Aledhari, M., Razzak, R., Qolomany, B., Al-Fuqaha, A., & Saeed, F. (2022). Biomedical IoT: enabling technologies, architectural elements, challenges, and future directions. IEEE Access, 10: 31306-31339. https://doi.org/10.1109/ACCESS.2022.3159235

[52] Qureshi, F., Krishnan, S. (2018). Wearable hardware design for the internet of medical things (IoMT). Sensors, 18(11): 3812. https://doi.org/10.3390/s18113812

[53] Sadhu, P.K., Yanambaka, V.P., Abdelgawad, A., Yelamarthi, K. (2022). Prospect of internet of medical things: A review on security requirements and solutions. Sensors, 22(15): 5517. https://doi.org/10.3390/s22155517

[54] Pundir, S., Wazid, M., Singh, D.P., Das, A.K., Rodrigues, J.J., Park, Y. (2020). Designing efficient sinkhole attack detection mechanism in edge-based IoT deployment. Sensors, 20(5): 1300. https://doi.org/10.3390/s20051300

[55] Roy, S.D., Singh, S.A., Choudhury, S., Debnath, N.C. (2008). Countering sinkhole and black hole attacks on sensor networks using dynamic trust management. In 2008 IEEE Symposium on Computers and

Communications, Marrakech, Morocco, pp. 537-542. https://doi.org/10.1109/ISCC.2008.4625768

[56] Kaur, R., Singh, P. (2014). Review of black hole and grey hole attack. The International Journal of Multimedia & Its Applications, 6(6): 35. https://doi.org/10.5121/ijma.2014.6603

[57] Shree, R., Khan, R.A. (2014). Wormhole Attack in Wireless Sensor Network. International Journal of Computer Networks and Communications Security, 2(1): 22-26.

[58] Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., Douligeris, C. (2020). Security in IoMT communications: A survey. Sensors, 20(17): 4828. https://doi.org/10.3390/s20174828

[59] Ghildiyal, S., Gupta, A., Tomar, N., Semwal, A. (2014). Analysis of sybil attack in wireless sensor networks. International Journal of Engineering Research & Technology (IJERT), 3(5): 845–848.

[60] Mushtaq, M., Shah, M.A., Ghafoor, A. (2021). The internet of medical things (IOMT): Security threats and issues affecting digital economy. in IET Conference Publications, 2021: CP786. https://doi.org/10.1049/icp.2021.2420

[61] Naser, S.M., Ali, Y.H., OBE, D.A.J. (2022). Deep learning model for cyber-attacks detection method in wireless sensor networks. Periodicals of Engineering and Natural Sciences, 10(2): 251-259.

[62] Gulganwa, P., Jain, S. (2022). EES-WCA: energy efficient and secure weighted clustering for WSN using machine learning approach. International Journal of Information Technology, 14(1): 135-144. https://doi.org/10.1007/s41870-021-00744-5

[63] Almomani, I., Al-Kasasbeh, B., Al-Akhras, M. (2016). WSN-DS: A dataset for intrusion detection systems in wireless sensor networks. Journal of Sensors, 2016: 4731953. https://doi.org/10.1155/2016/4731953

[64] Maheswari, M., Karthika, R.A. (2022). A Novel hybrid deep learning framework for intrusion detection systems in WSN-IoT networks. Intelligent Automation & Soft Computing, 33(1): 365-382. https://doi.org/10.32604/iasc.2022.022259

[65] Premkumar, M., Sundararajan, T.V.P. (2021). Defense countermeasures for DoS attacks in WSNs using deep radial basis networks. Wireless Personal Communications, 120(4): 2545-2560. https://doi.org/10.1007/s11277-021-08545-6

[66] Gowdhaman, V., Dhanapal, R. (2022). An intrusion detection system for wireless sensor networks using deep neural network. Soft Computing, 26(23): 13059-13067. https://doi.org/10.1007/s00500-021-06473-y

[67] Saheed, Y.K., Arowolo, M.O. (2021). Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms. IEEE Access, 9: 161546-161554. https://doi.org/10.1109/ACCESS.2021.3128837

[68] Mohapatra, H., Rath, S., Panda, S., Kumar, R. (2020). Handling of man-in-the-middle attack in WSN through intrusion detection system. International Journal, 8(5): 1503-1510. https://doi.org/10.30534/ijeter/2020/05852020

[69] Jamshidi, M., Zangeneh, E., Esnaashari, M., Darwesh, A. M., Meybodi, M.R. (2019). A novel model of sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it. Wireless Personal Communications, 105: 145-173. https://doi.org/10.1007/s11277-018-6107-5

[70] Almomani, I.M., Alenezi, M. (2018). Efficient denial of service attacks detection in wireless sensor networks. Journal of Information Science and Engineering, 34(4): 977-1000. https://doi.org/10.6688/JISE.201807_34(4).0011