Review Article

INTERNATIONAL JOURNAL OF ENGINEERING BUSINESS MANAGEMENT

International Journal of Engineering Business Management
Volume 15: 1–29

DOI: 10.1177/18479790231157220
journals.sagepub.com/home/enb
SAGE

Wireless sensor network security: A recent review based on state-of-the-art works

Mohammed Faris[1], Mohd Nazri Mahmud[1], Mohd Fadzli Mohd Salleh[1], and Alhamzah Alnoor[2]

Abstract

Wireless sensor networks (WSNs) are a major part of the telecommunications sector. WSN is applied in many aspects, including surveillance battlefields, patient medical monitoring, building automation, traffic control, environmental monitoring, and building intrusion monitoring. The WSN is made up of a vast number of sensor nodes, which are interconnected through a network. However, despite the growing usage of applications that rely on WSNs, they continue to suffer from restrictions, such as security issues and limited characteristics due to low memory and calculation power. Security issues lead to a lack of communication between sensors, wasting more energy. The need for efficient solutions has increased, especially with the rise of the Internet of Things, which relies on the effectiveness of WSNs. This review focuses on security issues by reviewing and addressing diverse types of WSN assaults that happened on each layer of the WSN that were published in security issues in the previous 3 years. As a consequence, this paper gives a taxonomy of security threats for each layer and different algorithmic solutions that numerous researchers who seek to counter this attack have explored. This study also presents a framework for constructing an intrusion detection system in the WSN by emphasising the drawbacks of each approach suggested by researchers to defend against specific forms of assault. In order to diminish the impact of this attack, this summary shows which attacks the majority of researchers have dealt with as well as which ones they have not yet addressed in their academic work.

Keywords

Wireless sensor network, architecture, attack types, security, networks

Date received: 11 August 2022; accepted: 28 January 2023

Introduction

Wireless sensor networks (WSNs) is an increasingly valuable foundational technology for the Internet of Things (IoT).[1] WSN is considered an increasingly important fundamental component of the IoT. The WSN market was worth the US $46.76 billion in 2020 and is predicted to be worth US $126.93 billion by 2026, growing at a CAGR of 17.64% between 2021 and 2026.[2–5] As a result, the use of WSNs is increasing significantly with each passing day. Wireless sensor networks are applied for a variety of purposes, including monitoring systems, transportation tracking, health care checking, home automation, protection and surveillance, object tracking, and farming techniques.[6–9] According to how sensor nodes are deployed, WSNs are categorised into five groups: terrestrial, underground, multimedia, underwater, and mobile.[7] Base stations and sensor nodes produce WSNs (BS).[10–12]

[1]School of Electrical and Electronic Engineering, Universiti Sains Malaysia, Malaysia
[2]Management Technical College, Southern Technical University, Basrah, Iraq

Corresponding author:
Alhamzah Alnoor, Management Technical College, Southern Technical University, Basrah, Iraq.
Email: Alhamzah.malik@stu.edu.iq

Although the BS can be protected through security measures, sensor nodes are usually implemented without a predetermined wireless architecture and are normally left unsupervised without having sufficient network security measures. These characteristics increase WSNs vulnerability to cyberattacks, the rise of which has been exponentially in recent years. However, their implementation is still essential for tracking variables like humidity, heat, electricity, light, pressure, and soil composition as well as for sending sense data to the BS through the wireless link. Processing speed, memory capacity, battery capacity, transmission range, throughput, and data security are all frequent limitations of sensor nodes. Inhospitable, unfriendly, and unprotected locations are where sensor nodes are deployed. As a result of resource-constrained nodes, wireless connection routes, and the deployment of unfriendly nodes, WSN security is essential.[13–15]

In WSN, adversaries can easily compromise sensor nodes and launch assaults. The adversary can launch assaults on the network at various levels. Wireless sensor network security is provided on two levels.[16] On the first level, encryption methods and firewalls are utilised to protect the network from outside attackers. Intrusion detection systems (IDS) are employed to defend against internal intruders at the second level. However, IDS has been used largely for intrusion detection only rather than for initiative-taking intrusion prevention. As a result, unauthorized access to information, altering the information, dropping some packets, and forwarding them to subsequent nodes in the network are all examples of intrusion that are still prevalent despite the widespread implementation of IDS. A method called intrusion detection watches for suspicious behaviour on a network and alerts the user when one is found. On the other hand, an intrusion prevention system (IPS) provides a mechanism that detects anomalous activities and immediately stops them, thereby preventing potential intrusion. However, intrusion prevention has severe limitations, such as causing false-positive results that erroneously classify legitimate users as attackers.[17] Such classification errors would reduce performance in terms of system capacity. Moreover, IPS needs high bandwidth, reduces network performance, and is more expensive than IDS.[18–20] Another factor affecting WSN security is that the environment where these sensors are deployed plays a crucial role in determining the network size, deployment system, and network topology. Offering precise, authenticated, and controlled physical access to a sensor node is the most significant step in providing security. Because sensors are located in remote and difficult-to-reach locations and are deployed in open environments, many WSNs are left unattended.[18,21–23] Therefore, maintaining constant monitoring and physical protection of a sensor node is difficult, leaving it vulnerable to unauthorised physical access. Physically tempered nodes that are compromised can result in several security breaches in the future.[24–28] The basis of WSN dissemination is gathering pertinent data for the monitoring region. Sensor distribution is done in two ways: ad-hoc (i.e., sensors are distributed randomly to cover as many areas as possible), called an unstructured WSN, and pre-planned (i.e., sensor distribution in an array), called a structured WSN. When the sensors are distributed for coverage in an ad-hoc manner, network maintenance, such as security management and intrusion detection/prevention, is complicated as many nodes exist and the connections between them and the BS are not continuous. Hence, it makes sense that information sent, such as information on security management, is lost.

The core element of a WSN is the sensor node, which is exposed to radio frequency (RF) interference, vibration, a highly corrosive environment, high humidity, and dirt or dust, all of `which degrade its performance.[29–33] Sensors may malfunction as a result of these environments harsh conditions, providing inaccurate information to other nodes.[34,35] Therefore, environmental obstructions may also restrict connection within nodes, which has an impact on network connectivity and results in some data loss sensed by nodes, including information related to security.

There have been many review papers on WSN security and mechanisms for the detection of attacks investigated recently, such as Pragadeswaran, 2021,[36,37] Panwar et al., 2021,[38] Kaur and Rattan, 2021,[39] Ahmad et al., 2022,[40] Singh et al., 2022[41] and Temene et al., 2022.[42,43] Pragadeswaran[36] present a review of security concerns in WSNs in this article. They elaborate on these concerns by specifying the constraints, security requirements, and attacks on WSNs. However, no study conducted an in-depth and comprehensive review of the IDS that would discover these types of attacks on WSNs. Hence, several previous studies provided a brief description of security specifications regarding WSN techniques.[38,44] Besides, the types of detection mechanisms without mentioning the type of attack detection have been described.[39]

On other hand, Ahmad et al., 2022[40,45] Concentrate on energy and security as key challenges, as infection of communication and data networks occurs due to WSN's limited power. Machine learning algorithms are suggested in the study as a way to help detect threats, assaults, dangers, and malicious nodes by decreasing security costs and improving the ability of sensors to learn and evolve on their own. While Singh et al., 2022[41,46] discuss WSN protocols and applications in the military, industrial, and health sectors. Moreover, Temene et al., 2022[42,47] present an extensive review in the area of WSN mobility and discuss the intriguing algorithms in this area that were divided into sink and node methods depending on the kind of node that has the mobility feature.

Demands for high-quality medical care have grown in this digital age. The traditional medical system is facing new challenges as the number of patients keeps rising. Gaurav

et al., 2022[48] proposed a hybrid system that combines traditional healthcare practices with IoT technologies developing MIoT. IoMT seeks to improve patients' ability to respond to their therapy in a timely and effective manner. The protection of user privacy, however, is a crucial concern when it comes to gathering and managing extremely sensitive personal health data. IoMTs can only use a limited number of security measures because of their low computing capabilities. Patient data is therefore vulnerable to data leakage during the transfer of health data via MIoT. According to the authors, this publication stresses the importance of putting in place sufficient security measures to strengthen the IoMT's resistance to cyberattacks. The authors also offer an overview of current methodologies and examine the primary security and privacy concerns related to IoMT in this publication.

Consequently, there is a lack of an in-depth review of WSN we find that there are two aspects to the survey research; one with minimal information about assaults and other studies that explore network security and its impact on energy dissipation, using our understanding of the security difficulties in WSN. Therefore, a novel taxonomy to classify the reviewed literature based on WSN is needed. By analyzing all attacks in WSN in-depth and presenting additional information to identify these assaults according to the layer for WSN with new algorithms and strategies for fending off these assaults, we want to rectify that out-of-date survey in our study. To this end, the objective of this paper is to present an in-depth analysis of the attack types for each layer on WSN. Accordingly, the critical question needs to be answered: "How can they design appropriate IDS schemes in WSN to detect several types of attacks? "To speed up the process of developing a new algorithm to address the security problems in WSN, we highlight the gaps in this survey so that the researchers may work to fix them.

Methodology for research

The following are the criteria for the conduct of research and the scientific mapping procedure. First, to carry out this scientific mapping, we have selected the Web of Science, IEEE, and Scopus databases. The term was used for the period between 2002 and 2022. Papers were examined and explored using the keywords: "WSNs", "WSNs", "WSNs surveys", "WSNs technologies", "WSNs security", "WSNs toward IoTs", "IoT based on WSNs", "WSNs applications" and "WSN security and attack types." We chose only articles and reviews specifically; we excluded the studies which were published in a language other than English and proposed a new algorithm and methods that enhance the ability to detect diverse types of attacks on the WSN layers as a document filter. We used the RStudio software to conduct all key elements of the science maps for this bibliometric analysis. After a pre-processing step had been taken to ensure quality results, excluding duplication of documents, 540 documents were exported from the Web of Science, IEEE, and Scopus. Furthermore, a selection criterion was defined for the identified studies shown in Figure 1. We limited our literature search by using useful keys through mind mapping, as shown in Figure 1. The studies which did not meet the predefined criteria were excluded. These analyses of WSN security, attack types, and applications were then identified into a generic coarse-grained taxonomy that was generated from an earlier literature review. The following was among the exclusion criteria: The article is written as an overview of WSNs as well as real-world applications of WSNs and different WSN layer attack types. This survey resulted in the compilation of a number of WSN security risks and defence mechanisms. The reader would then see which attacks have been made, how they have been addressed, and which threats still persist. Because there are so many different WSN applications, these dangers must be addressed immediately and pro-actively by the industry and academic research groups as well as by manufacturers.

Figure 2 was created with the RStudio program, which depicts the Annual Scientific Output curve in the WSN security publication, implying that researchers have become more focused on this field in recent years.

China leads research and publication on WSN security, followed by India, as shown in Figures 3 and 4 show the most used keywords in research, such as energy usage, network protocol, security and privacy concerns.

Figure 5 show how countries worldwide collaborated to address the challenge and implement a solution to the problems of WSN. Through data analysis, we can see that the locations with dark blue have a strong interest in resolving these security issues in WSN, while the locations with light blue have already begun working to address these issues, and the locations with dark grey have not yet made any attempts to identify or address these issues.

Figure 6 displays the correlation between the most important WSN security themes, including node hostility, energy usage, security concerns, and security measures.

WSN applications

The WSN is used in a wide variety of applications due to its attributes, including its inexpensive cost and ability to be quickly installed in any environment. It is used at a place that is hard for viewers to approach from below or underwater. The WSN application is covered in the following subsections as shown in Figure 7.

Military applications

The military sector was the first human activity to deploy WSNs, and it is also said to have sparked interest in sensor network research.[49] These early research projects, which were

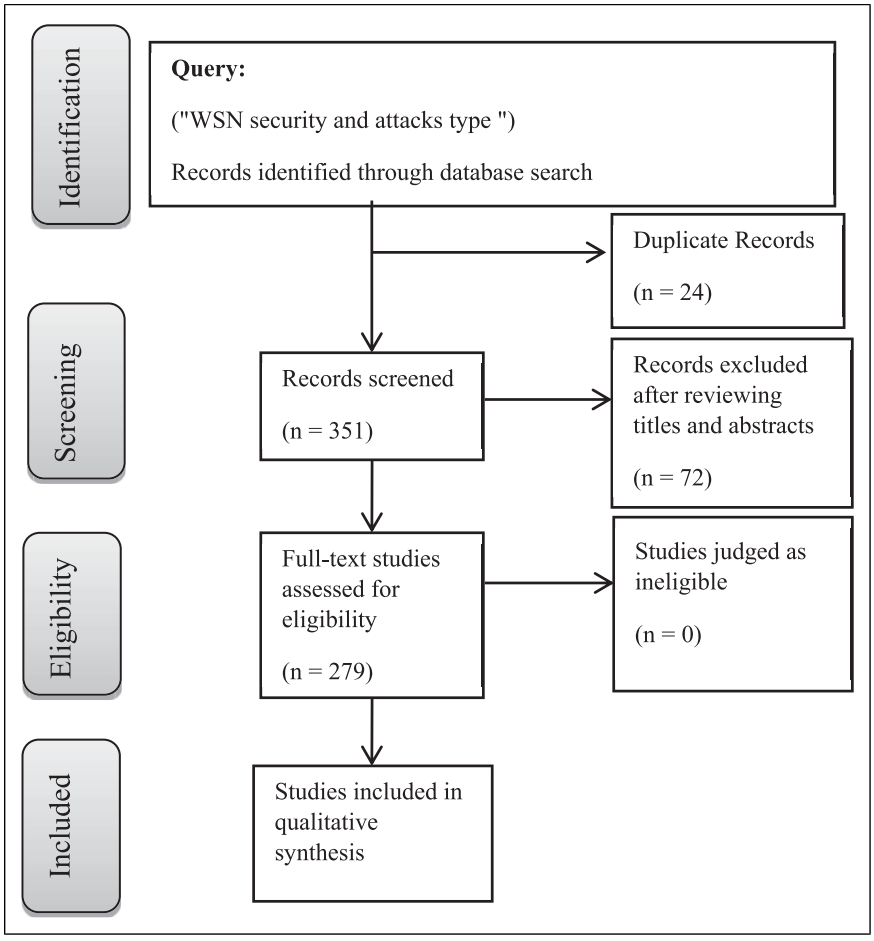

Figure 1. Systematic review.

conducted in the late 1990s to create sensor nodes capable of performing espionage operations despite their incredibly small size, are best exemplified by Smart Dust.[50–52] Due to recent technology advancements,[53] WSNs may now handle a variety of operations. The three primary subcategories of the military uses of WSNs, such as battlefield surveillance, combat monitoring, and intruder detection, as well as the most typical sensor types utilised in each, are depicted.[49,54]

Health applications

Wireless sensor networks are used in the healthcare industry to track patients' vital indicators, including temperature, blood pressure, and heart rate.[55] Using wearable electronics, healthcare providers may provide real-time monitoring of patients' vitals both inside and outside of healthcare facilities, such as hospitals and nursing homes.[56] Patient wearable monitoring,[57,58] home assistance systems and hospital patient surveillance[59] are the three primary subcategories of health applications of WSNs that are presented together with the types of sensors that are most frequently employed in them.

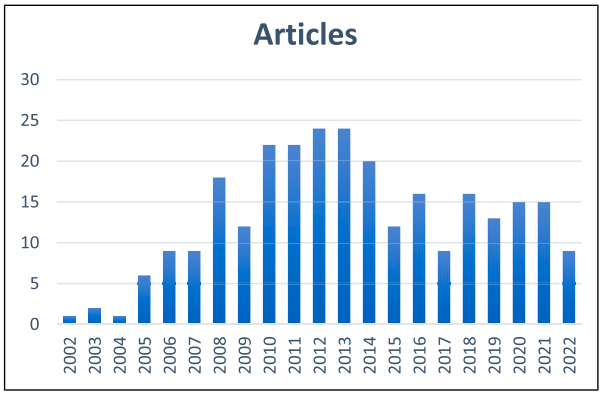

Figure 2. Annual scientific production.

Environmental applications

Wireless sensor networks can be used to enhance environmental applications that seek continuous surveillance of ambient conditions in dangerous and distant locations.[60] The primary environmental applications of WSNs

are water checking, air checking, recognising floods, earthquakes, volcanic eruptions, air pollution and emergency alerting.[61]

Wildlife and plants applications

Every nation needs its wildlife and plants.[62] The primary subcategories of wildlife and plant applications of WSNs, namely greenhouse monitoring, crop monitoring, and livestock husbandry, are presented together with the most typical sensor types utilised in them.[63]

Industrial applications

Wireless sensor networks may be used in a variety of industrial applications to address a wide range of connected issues.[64] The three primary industrial uses of WSNs are machinery health surveillance,[64] robots, and logistical.[65]

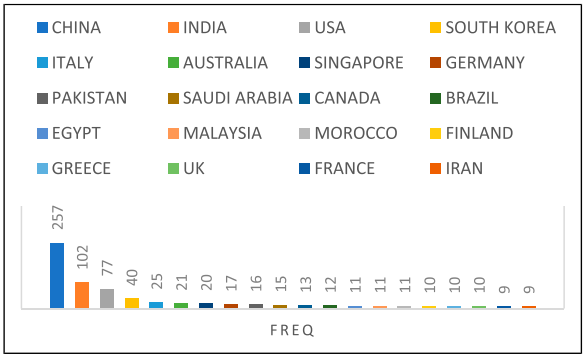

Figure 3. Country scientific production.

Urban applications

Wireless sensor networks' wide range of sensing capabilities also provides users with the chance to learn an unparalleled amount of data about a target region, whether it be inside or outside of a structure or apartment.[66] There are various uses for WSNs, which are a tool for measuring the spatial and temporal characteristics of any phenomenon in an urban setting. Smart homes, smart cities, transportation systems, and structural health monitoring are the most widely used WSN applications in the urban setting.[63]

Critical analysis for WSN security research

On wireless networks, the issue of security is a major source of anxiety. Due to their distinctive features, wireless networks are prime candidates for physical and network manipulation. Resource limitations further make it difficult to differentiate security breaches such as node failures, intrusions, and malfunctions in sensor networks since sensor nodes are moved to remote locations where people cannot travel and leave these sensors unattended to run without charging facilities. Due to resource limitations, conventional security mechanisms are unsuitable for WSNs. The main objective of this work is to present the most recent theories on the difficulties facing WSNs. By reviewing earlier research on the subject, this paper analyses WSNs. To aid future academics in their exploration of this topic, we offer an assault taxonomy. There are various benefits to the proposed taxonomy. The taxonomy, for instance, organized the publications at different levels. Many academics that are interested in WSN security think that a lot of research lacks healthy organization, which causes unsuitable research activities. The proposed taxonomy offers a precise research

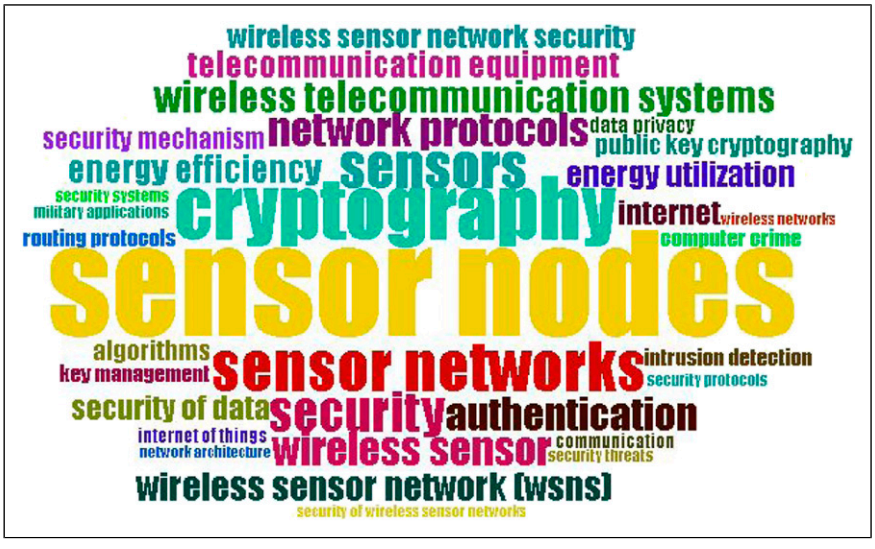

Figure 4. Word cloud.

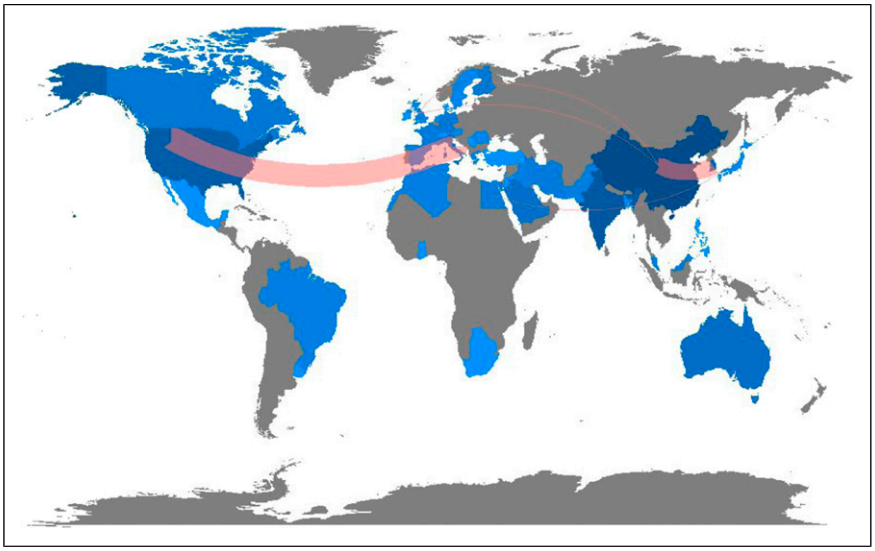

Figure 5. Collaboration world map.

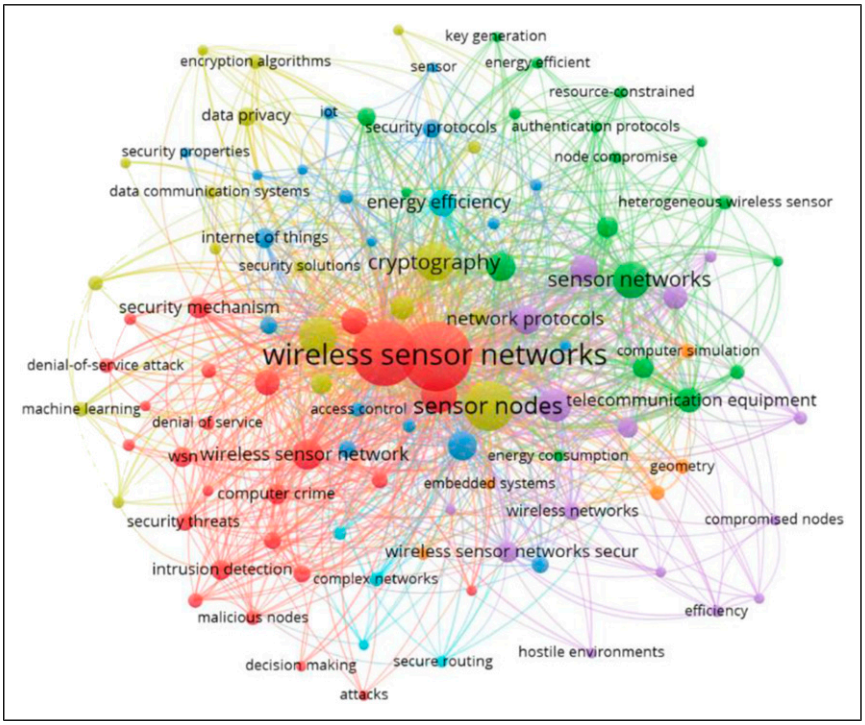

Figure 6. Co-occurrence.

framework, which gives researchers key research ideas about the most significant issues and solutions in the WSN security sector. The taxonomy offers academics and students numerous guidelines for selecting a subject linked to the security of WSNs. This study classifies WSN security attacks according to each layer and discusses the most popular algorithms proposed by researchers that introduce solutions for solving these attacks with their drawbacks in order to encourage and assist researchers in identifying gaps and weaknesses in the existing body of knowledge for the most significant directions to adopt a new strategy or modify this algorithm.

Figure 7. Wireless sensor network applications.

WSN attack types

Traditional wired network security methods require a lot of computation. The resource limitations of WSNs prevented certain approaches from being implemented directly for WSNs. Confidentiality, integrity, and availability (CIA)[67] together form the basis for WSN information security. Confidentiality guarantees authorised access by applying encryption algorithms to information. Integrity defends against unauthorised data change and fraud with cycle and message authentication codes (MAC). The presence of particular data means the information is available at the right time to the right user. In WSN resource-restricted communication, it is not easy to provide information and resources. Due to the restricted resources, an attacker may quickly penetrate a node in the WSN and launch a number of assaults on it to deplete its resources. WSN security attacks may be categorised under two categories:[68] passive and active assaults. The opponent observes the connection to access the data during a passive attack. Passive assault examples are camouflage adversaries, traffic analysis, homing attacks and eavesdropping. In eavesdropping attacks, the attacker intercepts the message with the malicious node to spy on data to discover the transmission path and compromise network privacy. An attacker investigates communication patterns in traffic analysis. Instead of modifying or altering the packets, the attacker in a home assault looks for the network's insight resources, which are then exploited to execute any assault. To prevent this kind of assault, cluster chiefs, also known as encryption key managers, use data structure analysis and payload cryptography to detect and identify nodes. In camouflage adversaries, attackers hide the required number of nodes and imitate them as regular nodes, causing packets to be misrouted. The attacker in a homing attack does not change or edit the packets; instead, the attacker is seeking network perception resources, which are then exploited to conduct any active assault.[69] When attacking actively, an attacker monitors the communication connection and modifies or drops the data packet in the middle of the communication. Compared to passive attacks, active attacks are more dangerous. Active assaults have been undertaken on various WSN stages. The following sections discussed active attacks based on diverse types of WSN layers.

Physical layer attacks

The physical layer implements various functions in WSNs, like producing carrier signals, signal identification, modulation, and information cryptography to transmit the information across the wireless link.[70] The sensor node broadcasts its information over a wireless channel. The services of sensor nodes are disrupted when radio signals are jammed or intercepted. WSN networks are placed in hostile, isolated, and unguarded areas. As a result, it is a possibility that sensor nodes could gain physical access to sensitive data. Jamming and node tampering are the two most common physical layer attacks. In the next section, the state-of-art approach to countering these attacks are also reviewed.

Jamming attacks. The radiofrequency of an attacker node interferes with the other legitimate nodes when the former launches a successful jamming attack on the latter.[71] The primary purpose of the jamming assault is to prevent valid nodes from communicating with low energy. Jamming assaults take advantage of the common structure of wireless networks to interfere with transmission by dropping the Signal to Noise Ratio (SNR). Santoro et al., 2017[72] had made

a distinction between two aspects of jamming assaults: physical jamming and virtual jamming. Physical jamming is typically attempted through the use of radio signals, whereas virtual jamming is usually executed and carried out by using request to send (RTS) and clear to send (CTS) signals. Del-Valle-Soto et al., 2019[73] propose Connected Mechanism and Extended Mechanism as two novel jamming detection techniques that can detect reactive jamming. The first is based on data from performance metrics obtained from nodes that are directly linked. While the second technique, a collector node has access to all of the network's performance characteristics and can compare them. The results demonstrate that when using a proactive protocol such as MPH (Multi-Parent Hierarchical) in comparison to well-known reactive protocols such as AODV (ad hoc distance vector) and DSR, the first method has enhanced performance by 78% and the second method has enhanced performance by 86% in identifying the region impacted by an intervention node (dynamic origin routing).

Bengag et al., 2020[74] developed a new IDS method to identify jamming assaults in WBAN based on four critical metrics of the network: packet delivery ratio (PDR), energy consumption (ECA), signal strength indication received (RSSI) and bad packet ratios (BPR). As a first step, they presume that the WBAN system is in good working order, with no jamming or other issues. The network thresholds are then established for each sensor medical based on the parameters PDRth, ECAth, BPRth, and RSSIth. The starting parameters (PDRth, ECAth, BPRth, and RSSIth) are then contrasted with the present values to see whether there are any abnormalities in the WBAN. One of the parameters crossing the network threshold will trigger an alert for declaring the presence of a jammer node. Three forms of jamming assaults namely constant, deceptive, and reactionary are classified. The simulation for the suggested technique was carried out in two primary situations: one with jamming and the other without jamming, using the prominent WBAN simulator tools OMNET++ and Castalia. The result inductees that the utilized parameters have favourable benefits in detecting the existence of jamming with lower false alarms. However, this technology requires more development to make it more robust, as well as to optimize performance for detection and minimize false alarms.

Dell Valle Soto al., 2021[75] proposed a simple jamming detection system technique that uses a strategy to find sections of damaged nodes where energy is limited. The detection technique is evaluated by using four known clusters of protocols: PEGASIS (Power-Efficient Gathering in Sensor Information Systems), TEEN (Threshold-sensitive Energy Efficient), LEACH (Low Energy Adaptive Clustering Hierarchy), and HPAR (Hierarchical Power-aware Routing). These protocols are evaluated in Zigbee and LoRa, two well-known and widely used wireless technologies. Experiments are conducted on an actual network in a section of a college in Guadalajara, Mexico, and the identification method used is examined. The findings demonstrated the method's ability to identify nodes displaying unusual activity. In these regions, PEGASIS has a 92% accuracy, TEEN has an 86% accuracy, LEACH has a 70% accuracy, and HPAR has a 61% accuracy. This accuracy aids in the identification of a potential jamming assault. For each wireless technology, they employ six sensors, as well as a controller node and a Cluster Head. According to findings, implementing the detection techniques in LoRa consumes 16% more electricity than in Zigbee. This is probably primarily caused by the fact that LoRa requires 7% more operations and updates to the nodes' route tables. The performance assessments of the nodes allow LoRa to send an indicator of a potential area of the damaged node more quickly.

Node tampering attack. In a tampering attack, the attacker can reconfigure a valid node to make it a compromised node. The adversary has access to sensitive data from the sensor node, such as security keys and data. Da-Wen Huang et al., 2021[76] propose an algorithm for hybrid diagnosis to detect attacks on dynamic WSNs. The suggested hybrid diagnostic method involves three stages: data comparison, distributed diagnosis, and global diagnosis. In the phase of distributed diagnostics, a general polling mechanism and a multi-round diagnosis technique are implemented. The authors offer a global diagnostic phase to alleviate the problem of the phase, which may result in inconsistent diagnosis outcomes across various sensor nodes. When used for the diagnosis of sparse networks, the technique suggested in this study, like many defects diagnostic systems have a high rate of false alarm (0.2–0.8). By appropriately setting the threshold values, the suggested method may achieve high accuracy [96% ± 0.02] since maintaining a low false alarm rate by raising the fraction of affected sensor nodes p and reducing the mean node grade of the WSN. The algorithm suggested in this paper is the high rate of false alarms when used to diagnose small networks. The method should be modified to operate with several types of networks, like mobile WSNs and mobile ad hoc networks. Several ways of improving the predictive efficiency of sparse networks must be provided.

Data link layer attacks

The WSN link layer is used as a frame, to control errors, detect and access data frames. Data link layer attacks are collisions, sleep denial, exhaustion of resources and unequal channel allocation.[70]

Collision attacks. A collision assault occurs when two nodes broadcast data simultaneously and at the same frequency. It retransmits the collided packets after a packet collision.[70]

An attacker purposefully collides with certain packets, such as control packets, resulting in a massive back-off exponential. By violating the limitations of the network protocols and delivering messages indefinitely, an attacker induces a conflict.

Denial of sleep attack. An assault known as "denial of sleep" restricts the node's ability to rest and increases the power required for data transmission and reception by sensor nodes. Wireless sensor networks's MAC protocols keep the node in sleep mode if there is no data to send. The attacker trying to prevent sleep is transmitting messages to the genuine node all the time. Therefore, increasing node ECA. Fotohi et al., 2020[77] suggested two methods proposed ASDARSA (Abnormal Sensor Detection Accuracy) schema to safeguard the network from denial of sleep attacks and for decreasing energy usage by defeating denial of sleep. In ASDARSA, in order to reduce power consumption and improve network lifetime, a clustering technique based on power and range is used to choose the ideal cluster head. According to simulation studies, ASDARSA was incredibly resilient to attacks that denied sleep. In terms of average throughput (more than 29.5%), PDR (more than 16.33%), network lifetime (more than 27.16%), detection accuracy (more than 18.5%), and mean residual power (more than 16.5%), it outperforms current methods. In this work, they developed a solution for decreasing energy usage by preventing denial of sleep assaults using encryption and authentication. All sinks were fixed in the suggested technique, and that causes nodes to be near the sink to operate as the cluster head or as a middleman for the flow of data from other nodes to the source. As a result, the energy of these nodes is rapidly depleted, resulting in a shorter network lifetime.

Mohd et al., 2020[78] implement IDS to detect denial of sleep attacks via support vector machine learning in WSN. In this method, feature rating and cutting are important. The SVM performance analysis parameters include Overall Classification Accuracy (OCA), Overall Training Time (OTT), and Overall Testing Time (OTST). Following that, each feature may be classified as "significant (S)," "moderate (M)," and "trivial (T)." After utilising the Feature Selection method, a set of 19 features has been executed, and a secondary feature set of seven expressive features is chosen. Those extracted features are further examined by applying a supplied set of rules in an approach for the identification of sleep assaults in WSN. The result for Linear Kernel function OCA (87.30%), PPV(89.40%) and TPR(91.40%), while for radial Kernel function OCA (90.80%), PPV(89.50%) and TPR(97.49%) and finally for Sigmoid Kernel function OCA (65.23%), PPV(65.23%) and TPR(97.21%).

Fotohi and Firoozi, 2020[79] a hybrid strategy involving the mobility sink and the Firefly approach depending on LEACH and the Hopfield neural network was suggested in this research WSN-FAHN (WSN firefly algorithm Hopfield neural networks). Mobile sinks are utilised to decrease power consumption and increase network lifespan. To prevent sleep deprivation assaults, the Firefly approach was created, which clusters nodes and uses two levels of authentication. In order to give CH data, the Hopfield neural network also recognises the sink movement's straight path. While all nodes that broadcast synchronisation messages should be checked before the messages are accepted if they are not already, the suggested technique successfully prevents DoSL attacks (it is a type of denial-of-service attack that prevents sensor nodes operated by batteries from entering into the sleep state). Their results showed that the WSN-FAHN model can provide excellent rates of safety and detection rate (93.92%). Furthermore, when compared to the other ways already in use, the suggested model has a higher PDR (over 91.52%), higher throughput (over 90.75%), higher average residual power (over 91.125%), and a high network lifespan (over 89.95%). It is recommended to use several mobile sinks to minimise energy usage in WSNs.

Exhaustion attack. An exhaustion assault repeats collision attacks until all of the nodes' energy is depleted. In other words, resource exhaustion attacks require establishing routing loops and extending the route during packet transfers to deplete the energy of the nodes.[80] Hussain et al., 2019[81] developed an IDS to recognize many forms of intruder assaults on WSN MAC protocols. A soft decision method has been built to identify Exhaustion and intrusions assaults. In addition, a preventive mechanism has been included to assist a node in avoiding these invasive attacks. In the intrusion detection section, they picked the following statistics as intrusion indicators: Collision Ratio (Rc) is specified as the measurement of a node's collision duration in seconds. The probability that an information packet will be successfully transmitted is determined by the proportion of successful data packet transmissions to all information packets communicated. RTS packet arrival ratio (RRTS) is a measure of how many RTS packets are safely received by a node per second. They gathered all of the data and calculated the chance of an intrusion. After that, input the values of the RTS counts information packet arriving rate into the soft function to get the value of exhaustion. The threshold is divided by the probability of failure, multiplied by the probability of depletion. The assault has been found if the quantity surpasses the cutoff; else, there was no attack. They set the bar for their results higher than the likelihood of success. Individually, the likelihood of success is added to the probability of contact. The likelihood of success is multiplied by the probability of collision detection, and the outcome is contrasted with the threshold. After that, a threshold is determined, and summation results are compared to it.

Hristozov et al., 2020[82–84] presented a system that combines rate limiting and lightweight authentication with the help of a trustworthy backend. They use the rate limiting to fix the problems of battery fatigue assaults by obtaining capabilities at low levels within normally less active operating hours. They presented two rate techniques limiting – Leaky Bucket and EWMA (Exponentially Weighted Moving Average). They also suggest and formalize two authentication methods that are suited for a variety of frequently used IoT network topologies. Even if providers are experiencing battery fatigue, the mechanisms ensure that service is available to innocent requesters.

They used the ProVerif verifier Blanchet et al., 2019[85–87] for formal verification and made their verification models accessible online. Their solution may be applied in a battery-powered limited device in an energy-efficient manner, significantly lowering the attack surface for battery exhaustion. The simulation demonstrates that the accuracy rate varies from 86 to 99%, with an average false alert rate of 15%, while the percentage of attackers is between 5 and 15%. Additionally, it requires some time to get a ratio of 100% accuracy and a 0% false-positive ratio.

Premkumar and Sundararajan, 2020[88] suggested DLDM frame structure protects the network from DoS attacks in this article. An attacker is detected on a homogenous network based on clusters using a Deep Learning-based Defense Mechanism (DLDM). In light of the requirements for received signal intensity, packets processed per second, packet reception latency, the information modified, the information forwarded, and decreasing ratios for node activity, they are categorised as being benign or malicious by their DLDM method. If the node is determined to be malicious, it is going to be placed on the block table. The creation of a reliable network can lower the amount of power used by computer resources, such as bandwidth, processing speed, and battery. The key advantage of the approaches proposed is the right selection of routing protocols will generally extend the sensor's lifespan. During interventions, the CH and base station include an impact on the sensor node's power usage. By blocking various forms of assaults on CHs and base stations, the network may be improved over time.

Noorwali et al., 2021[89] proposed an adversary detection technique for the IEEE 802.15.4 standard, which is a central medium access protocol utilized in WSN-based IoT applications. A soft-decision-based method is employed to detect collisions and fatigue attacks by determining collisions and effectively transmitting probabilities using the soft function scale. The scaled values are compared to the threshold value. An assault is detected if the total value exceeds the threshold value; otherwise, no attack is detected. The chance of exhaustion and the probability of successful transmission is used to identify malicious exhaustion attempts. If the amount exceeds the threshold, an assault is detected; otherwise, no attack is detected. If the intruder detection method fails to identify the adversary's involvement and the system still perceives a breach of QoS, the coordinator's duty cycle must be changed to achieve the QoS specifications. Using this technique, the administrator can alter their duty schedule to meet QoS requirements. The active period grows as the node count rises and more data requests are needed. According to this, the active period has to be shortened when a network has less data. The IEEE 802.15.4 standard does not address duty cycle modification in response to QoS requirements. This method enables the coordinator to modify its duty cycle to suit the network's QoS requirements. The technique increases data transfer by increasing performance and decreasing collisions. The technique enables the coordinator to evaluate QoS during the previous and make necessary modifications in the subsequent. The data that the coordinator will need to receive is projected to be half of its full capacity.

Unfairness attack. Unfairness is a vulnerable type of DoS attack.[70] This attack leads to the needless delay of WSN effectiveness using MAC protocols.

Network layer attacks

The WSN network layer is responsible for routers and transfers data from the source node to the destination sensor node. The routing protocols decide on the best path for packet transfer. In order to shorten the life of the network, the adversary manipulates the routing protocols to offer less-than-ideal channels for network layer assaults. Blackhole attacks, misdirection attacks, selective forwarding attacks, wormhole attacks, and Sybil attacks are some of the more frequent network layer assaults.[90]

Blackhole attack. The adversary node in a blackhole assault reveals the smallest pathway between the source and destination nodes. As a result, the source node is tricked into sending data to the target node through the attacker node. Instead of sending the packets, the attacker node receives from the source node to the target node, it drops them.

Kalkha et al., 2019[91] has devised a Black Hole attack and offered a protection mechanism for the AODV (Adhoc On-demand Distance Vector) routing protocol via WSN. They employ a preventative strategy that takes the fastest routes between a sender and a recipient. The suggested approach presupposes that neither the supplier nor the destination is malicious or hacked, and then it suggests that the process of identifying a malicious pathway be included in the path development step of AODV routing protocols. The use of a tree main stage can ensure the prevention of a black hole assault. The topology of the network is marked in the first stage by the deployment of nodes. Then, in the second step, the system

uses Yen's algorithm[92] to determine the four direct routes between the two points. The value of every path is considered as the HMM (Hidden Markov Model) state of their method as the black hole attack uses the fastest path among supplier and recipient as a parameter in its network assault. A Viterbi algorithm[93] is employed in the decisive step to finding the path with the greatest risk of being harmful. This algorithm's packet data ratio (PDR) is approximately 19% under assault, whereas end-to-end delivery is between 80–85%. All packets of data are taken by the black hole nodes, which purposefully drop packets. As a result, all nodes along the defined path are packet dropped and examined to identify the hostile node, preventing any further routing pathways from avoiding it.

Clement et al., 2020[94] proposed an algorithm to detect a Black-Holes Attack on the healthcare network of wireless sensors utilising a powerful machine learning method called PICA (Projected Independent Component Analysis). The PICA is a technology that has been successfully implemented in WSN to improve intrusion detection. The PICA method optimises memory as well as ECA. As the scale of the black hole attack increases, the WSN's performance significantly degrades. As a consequence, principal component analysis is performed to discover the black hole node based on their behaviour analysis. Mutual information, according to the independence assumption, is a measure of the inherent reliance manifested in the mutual distribution of sensor nodes. Mutual information (MI) is a measurement of the mutual reliance between node behaviours in a WSN, such as packet reception capabilities, collaboration, and trust level, among other things. When compared to the current Channel-aware Reputation System with adaptive detection threshold (CRS-A) and Hybrid Intrusion Detection System (HIDS), the suggested PICA approach enhances BHADR (Black Hole Attack Detection Rate) by 7% and 18%, respectively. As a result, the suggested PICA approach reduces BHADT (Black Hole Attack Detection Time) by 29% in WSN when compared to CRS-A and 38% in the HIDS model. The PICA methodology improves the previous CRS-A and HIDS model methods, with FPR (False Positive Rate) decreasing by 37% and 27%, respectively. The PDR has been enhanced by 12 and 22%, respectively, over the prior CRS-A and HIDS versions.

Ifzarne et al., 2021[95] aim to create an intrusion detection model that is consistent with WSN's properties. The IDS was developed as a machine learning technique which successfully classifies real-time detection data from several devices by utilising a trainable algorithm. Crammer et al., 2006[96] introduced the Online Passive-Aggressive Algorithm (PA), which is a category of algorithms for online education (for both classification and regression). It may be viewed as the online equivalent of a support vector machine classifier. The idea is straightforward, and they have outperformed several different approaches, such as the Online Perceptron and the Margin-infused Relaxed Algorithm (MIRA) method. The PA classifier searches for hyper-planes which will divide the instance in half while learning from streaming input. A WSN intrusion identification methodology called ID-GOPA is based on an online passive-aggressive methodology and information gain rate. The main goal of the proposed methodology is to utilise online classifiers for network streaming data. The online categorizer PA trains the model to be more familiar with and learnable about current network actions, while filtered and labelled knowledge recordings are provided to construct a trainable model that can be assessed online. In the online phase, the same superior engine is utilised to choose just the suitable characteristic using the data gain rate approach and identify every packet as likely normal or attacked in real-time detection. The suggested model, ID-GOPA, has a 96% detection accuracy in assessing if the network is stable or under assault. The detection accuracy for scheduled, grayhole, flooding, and blackhole assaults is 86%, 68%, 63%, and 46%, correspondingly, as compared to 99% of normal traffic. Their findings imply how an online learning strategy can offer robust anomaly detection for the WSN.

Alruhaily and Ibrahim, 2021[97] offer a multi-layer architecture for intrusion detection in WSNs which improve network security. The sensors are placed in the initial layer, which is at the periphery of the network, and the next layer is at the centre of the network. They used the Naive Bayes method, which is straightforward and efficient in terms of computing, as the classifier's core. The initial layer will categorise observed data as being either normal or harmful, which has no further details on attack patterns. However, because the intermediate detection layer is located in the cloud and exclusively processes anomalous activity, it will have fewer resource constraints, allowing further complicated techniques and in-depth examination. As a consequence, harmful traffic was confirmed using the Random Forest (RF) with a multi-class classifier. The classification model was utilised to determine the type of attempted assault and provide recommendations for choosing an appropriate defence mechanism. The findings demonstrate that their suggested multi-layer protection approach increased TPR, TNR, FPR, and FNR values while also attaining a high accuracy rate, with values of 100%, 90.4%, 99.5%, 97%, and 99.9% for the normal, flooding, scheduling, grayhole, and blackhole assaults, correspondingly. In previous work, the values for normal, flooding, scheduling, grayhole, and blackhole attacks were 99.8%, 90.4%, 99.5%, 91.1%, and 73%, accordingly.

Suma and Harsoor, 2022[98] suggest solution combines an on-demand link and an energy-aware dynamic multipath (O-LEADM) routing system for MANETs to identify blackhole nodes using the baiting approach and distinguish between packet loss caused by congestion and malicious

nodes. The suggested technique can readily distinguish between packet drops caused by link failure and malicious nodes. The findings are compared to the existing AODV-Blackhole routing system and analysed. Concerning packet delivery ratio, the suggested O-LEADM Black-hole identification approach outperforms the current AODV-Blackhole strategy, which has 84% of nodes moving at 20 m/s and decreases to 83% when mobility velocity grows, while the OLEADM-Blackhole has 87% at 20 m/s. In order to minimise congestion and preserve route reliability, OLEADM-Blackhole achieves a % delivery ratio as speed increases by accounting for connectivity faults and channel accessibility. In the inclusion of a black-hole node in the network, the average delay graph reveals that AODV-Blackhole has an average delay of 0.083 ms at higher mobility speeds, but O-LEADM Blackhole has an average delay of 0.050 ms. The ECA of the AODV Blackhole and the O-LEADM Blackhole In the presence of an adversary, the OLEADM-Blackhole expends an average of 6.0 J of energy while travelling at a higher speed. As a result, at greater mobility speeds, AODV-Blackhole consumes 11.2 J of energy. The overhead of the O-LeadM Blackhole is between 4.1 and 11.1, whereas the overhead of the AODV-Blackhole is between 5.9 and 16.6. When a blackhole is identified, O-LEADM Blackhole improves significantly with great movement and at a low expense in identifying other channels. On the other hand, route identification in AODV-Blackhole had a higher expense in terms of detecting other routes to the destination.

Misdirection attack. One form of DoS assault that can happen at the network layer is a misdirection assault. In a misdirection attack, the attackers change the route of the packet delivery to a node different from the target node.[99] Sensor nodes along the path experience resource loss as a result of traffic being redirected in a particular way.

Mustafa et al., 2020[100] suggests an RL algorithm (Reinforcement Learning) for Misdirection Attack Detection and Prevention (RLMADP) in WSNs. In addition to the level architecture arrangement for WSN, the MDP (Markov Decision Process) from RL is estimated in their proposed approach. This strategy provides load distribution with more significant residual power to enhance the life of the network using an online technique with cheap computing costs. Their network is an RL or MDP process in which each node has an operator installed, and a Cluster Head (CH) has been tasked with maintaining surveillance on the network utilising criteria that are common to all of the nodes: Environment, Agent, Action, State, Policy, Value Function, and Reward Function. Air, sea, and cyber-physical are just a few of the realms in which this protocol functions. The random separation of clusters, which results in an unequal distribution and, in certain cases, an increase in ECA, is one of the disadvantages of the recommended protocols. The experimental outcomes demonstrate that the proposed method can efficiently identify the impacted node while simultaneously enhancing throughput and lowering delay. The proposed technique has not been utilised in real-time applications.

Singh et al., 2020[101,102] propose a unique approach for detecting misdirection attacks in WSN that does not employ cluster heads. The suggested detection method was evaluated using Omnetpp 5.4.1 on four diverse network sizes (10, 20, 30, and 40 nodes) with varying amounts of malicious nodes. The suggested method assigns a fixed unit of time (time slice) for nodes to send data to their next neighbouring node along a given path, along with a route for data transmission in a WSN. The experiment outcomes demonstrate that the proposed technique has greater detection accuracy and lower end-to-end latency (22.61 ms) than the cluster head detection method. The observations show that the suggested approach outperforms the frequently used cluster-based techniques in detecting misdirection attacks in WSN by using a smaller end-to-end delay parameter.

Selective forwarding attack. Selective forwarding is also known as a grayhole attack. A selective forwarding attack is a subtype of blackhole assault. In a black hole attack, the attacking node announces that it has the fastest route to the target over that node and discards every packet that passes through it. However, in selective forwarding, a hacked sensor node selectively denies data. Most studies assume that an attacker node ignores data based on the protocol being used, the sender or destination of the packets, or both (drops all UDP packets or drops all TCP (transmission control protocol) protocol).[103–105] There are several mechanisms to detect a selective forwarding attack in WSN. Mehetre et al., 2019[106] a twin security approach with a double assurance system was offered, along with two techniques for the data packet's secure networking. In addition, this study identified the untrustworthy route and offered secure routing paths using the CS (Cuckoo search) method and active trustworthiness in cluster sensor nodes. The presented secure routing strategy would avoid black holes and selective forwarding attacks by maximising the packet delivery ratio. The offered secured route approach prevents black holes and selective forwarding attacks while optimising packet delivery rates. The proposed system features optimum accuracy, minimal power loss, simplicity, privacy, and durability. The experimental findings suggest that the proposed system exhibits these characteristics in terms of power usage, latency, route length, network lifespan in homogenous and heterogeneous networks, throughput, and packet drop (Network size 16, ECA 160 J, Latency 20,000 ms, Throughput 85, and Packet drop ratio 18%). The findings show that at the maximum network capacity, the suggested system performs better, with 20,000 ms of delay power and 85% throughput. As a result, the data flow for this method must be increased.

Zhang and Zhang, 2019[107] aim to improve selective forwarding attack detection accuracy using an e-watchdog system. Misbehaving can be detected by employing detective agents closer to the attacker, improving the detection rate and effectively reducing the fake alert rate. The fundamental disadvantage of the watchdog is that it relies on a quiet communication paradigm instead of paying attention to the initiator's and receiver's signal-to-noise ratios. When the initiator's signal-to-noise ratio is higher than the receiver's, detection accuracy is significantly increased since the false alarm rate is decreased. The enhanced watchdog (E-watchdog) presented in this article encourages one or more of the initiator's nearby nodes that are closer to the target to identify SFA, resulting in accurate detection of the SFA node. In addition, E-watchdog uses reports from more than one detection agent to avoid collaborative selective transmission attacks. An elector algorithm filters fake reports from attackers. The false alarm rate of the E-watchdog is 25% lower than that of the Watchdog, and the network throughput is 10% higher.

Hao Fu et al., 2019[108] proposes a Data Clustering Algorithm (DCA) for identifying Selective Forwarding assaults (DCA-SF). The DCA-SF approach has been upgraded by adaptively changing the variables Epsilon and Minimum Points (Eps, Minpts). The simulation results show that the DCA-SF uses little energy with a low loss detection accuracy of 1.04% and a low false alarm rate of 0.42%. To confirm that the detection approach is precise, and analyses dispersed WSNs, this technique has to be assessed on the WSN platform. They want to cluster the information collected in the sensor node using DPC and SNN-DPC in order to assess their effects.

UmaRani and Somasundaram, 2020[109] developed Beta Distribution Reputation Model (BDRM) based on the beta distribution in this research to defend networks from selective forwarders. It detects selective forwarding attacks rapidly by using the sensor node's packet forwarding and packet dropping behaviour. By evaluating reputation BDRM discovers the shifting behaviour of selective forwarders. As a result, the network's throughput and message delivery rate are increased through the routing process. The connection delay and storage requirements for the BDRM paradigm are modest. To enhance security collaboration in WSNs, the BDRM model will be used in the future to assist cluster head selection.

Singh and Saini, 2021[110] suggested a technique for detecting selective forwarding assaults through the WSN. A node may ignore some or all of the data packets after being subjected to a selective forwarding attack. The node may even discard the entire data packet. To group the nodes collectively, the LEACH method is utilised. The suggested method splits the total number of cluster nodes into Investigator nodes (IN), Member nodes (MN), and Cluster Heads (CH) depending on the functioning of the nodes. A CH is the main controller that manages all transmissions. When the CH is assaulted, the entire cluster turns malicious over all communications. The IN is intended to observe communications between CH and MNs that a training module is under consideration and the IN is intended to keep a check out for CH behaviour that might be damaging. The entire proposed process is modelled utilizing NS2 for ECA (21 mj), and there is a variation in energy use of roughly 40%. The same number of nodes has shown a substantial variance in delay duration using the LBST technique. The suggested solution has a comparatively short delay duration (7000 ms). In the proposed method, there are 8% more packet drops.

Wormhole attack. A wormhole assault compromises two sensor nodes in distinct sections of the WSN. To access the sensor node packets, the attacker establishes a high-bandwidth channel between two compromised nodes.[111] Sensor nodes tend to choose this compromised channel for routing data packets and thus are exposed to wormhole attacks in this channel. Patel et al., 2019[112] proposed an alternative path length calculation based on neighbourhood information with two assumptions. The first assumption they make is that all of the sensor nodes are stationary. The second assumption is that malicious nodes are not present in the network at some initial interval at the time of deployment. All genuine sensor nodes securely establish their neighbour's information during the first period. Two malicious nodes launch a high-speed tunnel. The packet delivery ratio in a normal scenario is 99.88%, 36% in an assault scenario, and 98.10% after using the suggested technique. Similarly, throughput is 86 kbps in the normal situation, 34 kbps in the assault scenario, and 84.70 kbps after using the proposed technique. Packet delivery ratio and throughput both drop dramatically in the event of an assault. The suggested method dramatically increased both the packet delivery rate and throughput. The possibility of a false positive is eliminated. A wormhole that is propelled for a brief distance might provide a wrong result. The detection accuracy is very close to 100% if a wormhole is deployed across a significant distance. The bulk of the methods needs hardware, which increases the cost of manufacturing the sensor node. Present identification methods are usually resource-intensive and have limitations in terms of efficiency. The challenge of detecting secure neighbours in a mobile WSN is tough to solve. This approach will not identify attacks if the nodes are moving.

Tamilarasi and Santhi, 2020[113] proposed a technique for the detection of wormhole attacks using PSO (Particle Swarm Optimization). The suggested method is being implemented using the Network Simulator NS2. Several intermediate nodes in the route pathways between the various paths may provide fake routes that are shorter than the actual paths throughout the transmission. Wormhole pathways are the paths that have been assaulted. The DP

(Detection Packet) is used to detect the wormhole attack. An origin node must select the optimum route among the route table's assaulter paths for safe routing. Moreover, AD (Attack Detection)-time PSO is reduced by 50% compared to TESRP (Trust and Energy aware Secure Routing Protocol) by recognising and avoiding wormhole attacked pathways. The delivery ratios of AD-PSO and TESRP are compared. The suggested AD-delivery PSO ratio is raised by 33% over the present strategy due to optimum path selection employing PSO. The sent data is retrieved from misbehaviour by picking the secure path from the attacker-free pathways. As a result, the suggested AD-throughput of PSO is 66% higher than TESRP. The suggested PSO is utilised to choose the optimal route from the assaulter paths, cutting the consumption of the proposed AD-energy PSO by 10% and the proposed AD-drop PSO by 16% compared to TESRP. Assaulter paths between the source and the destination are constructed by identifying the wormhole-attacked pathways. Using the PSO method, the best path for threat data transmission is selected among the assaulter paths. The network's lifetime is increased by 32% as a consequence, in comparison to the old approach.

Singh et al., 2021[114] provide a method for identifying wormhole assaults in WSNs by employing artificial neural networks (ANNs), with connection data serving as the detection component. The suggested method detects any two sensor nodes using connection information. The suggested approach was used in the WSN area with the following probability distributions: uniform, Poisson, gaussian, exponential, gamma, and beta. Train the ANN by using the data calculated from the network before evaluating it. A wormhole attack exists if the output is 0.8. Otherwise, wormhole attacks do not exist if the training output is less than 0.8. When the train has finished uploading for continued ANN training, replace the training data with testing data. The experiment results for each applied method show high detection accuracies, such as uniform (90%), Poisson (90%), gaussian (100%), exponential (96%), gamma (97%) and beta (99%).

Singh and Saini, 2022[115] new routing approach Intelligent Ad-Hoc-On-Demand Multipath Distance Vector (I-AOMDV) is given which aims to ensure a secure way for data transfer in the Underwater WSN. The suggested technique is validated using Measures of WSN performance including power consumption, end-to-end latency, throughput, and packet delivery ratios. It proposes a wormhole detection approach that involves forming a cluster in the WSN. Many paths have begun with a network connecting the sender and receiver. It creates several paths using the AOMDV routing protocol (Ad-Hoc-On Demand Multipath Distance Vector). Cluster formation is considered during the initial phase of node deployment, for which the LNCA (Local Negotiated Clustering Algorithm) technique is used in the research methodology, which groups the nodes into clusters head and sensors node. Every node in the cluster should have RTT (Round Trip Time), ETD (Estimated Time of Departure), Th (Threshold value), PSent (packet sent), PReceived (packet received), DP (Detection Packet), and FP (Feedback packet) information stored in the routing table, which is determined by the number of hops and several initializations. The approach used NS2 and its performance to calculate associated measures such as energy efficiency (21 mj), packet delivery ratio (96%), throughput (65 kbps), and end-to-end latency (7 ms). This approach gives high results for avoiding wormhole attacks by increasing the packet delivery ratio. However, the throughput ratio must still be increased.

Alajlan, 2022[116] introduces a novel multi-step detection (MSD) technique for WSNs that can efficiently identify wormhole attacks. The MSD uses three techniques to identify and prevent simplex (where two nodes in the network which has tunnels between them but in different places of the network) and duplex (three nodes are in different locations and thus are not one-hop neighbours) wormhole attacks: the neighbour node validation process (NNVP), the fake link reduction process (FLRP), and wormhole separation. The Poisson distribution was used to distribute data throughout the network. Furthermore, the suggested MSD may be used to remove any false connections. Finally, the effectiveness of the separation module's performance guarantees highly successful identification and recuperation, effectively cutting off the wormhole from the network. Research should take into account the limitations of assessing after reconfiguring and rescheduling actual traffic control for the identification framework. Unconventional methods must be used to study distributed network scenarios in order to discover the most effective means of protecting the WSN from wormhole assaults. The recommended MSD displays fewer false detection and false toleration rates, as shown by simulation data acquired in OMNET++. Additionally, as shown by the simulation findings, the proposed MSD can effectively identify wormhole attacks in a genuinely scattered network setting with a 99.944% accuracy rate.

Sybil attack. The Sybil assault is often referred to as a spoofing attack. In a Sybil assault, an adversary hacks a network node, and the compromised node pretends to be numerous nodes using false identities.[100] The effect of the Sybil attack on the performance of IDS in WSN was considered by Jamshidi et al., 2019[117] a novel Sybil attack model for cluster based WSNs such as LEACH is suggested. The given method is built on cluster head node collaboration and RSSI (Received Signal Strength Indicator). Numerous experiments were carried out to assess the effectiveness of the suggested method in terms of real DR (detection rate), FDR (false detection rate), and communication latency. Studies show that the proposed method can detect 99.8% of Sybil nodes with a false identification ratio of 0.008%. The ECA of the proposed method for sensor

networks is a major factor in considering the energy constraints of sensor nodes. The number of transferred packets is an important parameter for evaluating the algorithm's performance since transmitting packets uses more power than analysing or receiving information. The new attack strategy is built for cluster networks. However, the suggested method is executed after clustering, thus it does not increase the communication cost of the clustering phase.

Angappan et al., 2021[118] present a new Sybil attack detection methodology known as (NoSad) for detecting and isolating Sybil attacks in WSN. This technique is based on intercommunication and RSSI measurement as a localised method of locating the Sybil node. The proposed protocol has undergone extensive simulation with different topologies, and the results demonstrate that the protocol is extremely effective in terms of detecting rates, power use, storage use, processing, and communication requirements (the TDR of the NoSad algorithm is over 99.85%). This protocol may be used in any infrastructure WSN to get decent results. This study proposes a solution for various Sybil node location circumstances to mitigate the Sybil attack in WSN.

Mounica et al., 2021[119] Design a machine learning technique that is designed to assess the effectiveness and accuracy of machine learning methods in order to identify Sybil and other vulnerabilities. On the basis of unprocessed Internet traffic information, a machine learning technique is intended to recognise a Sybil assault. By applying the NSL-KDD dataset, they trained the technique in their machine learning model. Four distinct models were used to identify various Sybil assaults. The first model used was Random Forest had a 79% average efficiency rate (This method combines decision trees with all of the features available in each decision tree. It could be used for both classification and regression.). The second model devised was logistic regression, which had an average efficiency of 84%. The third support vector machine model had a precision of 93%, whereas the fourth decision tree model had an accuracy of 83%. As a result, 93% of users are expected to use the support vector machine model with the highest accuracy and strongest occurrence indicators (DDOs, R2L, Probe, Sybil, and Normal) in the supplied data from the various evaluation graphs. By creating a real-time Web site where nodes pass through identification and reject clear network information, it is easy to prevent anything from occurring till it alters the current state of nodes in networks, allowing for the achievement of a prediction strategy for various attacks under examination.

Sinkhole attack. In a sinkhole assault, an attacker hacks any nodes around the sink node or the sink node itself to capture all the information in the WSN.[120] Nadeem and Alghamdi, 2019[121] suggest a sinkhole attack detection system that uses data aggregation, approach distance, and energy-related information to identify sinkhole attacks in Wireless Body Area Sensors Networks (WBASN). The attack by the sinkhole might significantly harm the network's functionality in terms of low throughput, higher delay, and message breakage. In simulations, their detection technique works effectively, with a great detection rate and a lower false alarm rate. Researchers must investigate the security and privacy issues with the multi-BAN scenario being implemented in a real-world hospital ward. This feature, which makes use of the multi BAN and wearable shimmer sensors, allows all of the patients in the award to be monitored autonomously. Then investigate, identify, and provide solutions to privacy and security concerns.

Nwankwo, 2019[122] provide a structure for enhancing sinkhole detection mechanisms by using Ant Colony Optimization with a swarm intelligence method using the network emulator NS3. There are two parts to the suggested framework. The first step entails issue conception and planning, as well as dataset specification and architecture. The second stage entails implementation, which includes EACO detection (Enhanced Ant Colony Optimization) on the NS-3.29 simulator, as well as flowcharts and pseudocode. Before comparing it to another accepted technique, they must increase the effect of the detecting ratio and false alarm reducing ratio. Dhivya et al., 2021[123] proposed solution presented a novel way of identifying and avoiding sinkhole attacks in WSN. The large number of terminals may be handled using the AODV (Ad hoc On-Demand Distance Vector) routing protocol. An Armstrong number and the GAN network are used to lessen the impact of sinkhole attacks. To identify and isolate sinkhole attacks no further communication is used for that. The proposed method may also be used if sinkhole nodes promote a high-quality link with high transmitted power. They must employ other strategies to cut energy usage even more, as well as concentrate on evaluating and understanding sinkhole attacks in the context of other routing protocols.

Byzantine attack. The network layer is exposed to the risk of the byzantine attack. Byzantine attacks are defined as actions taken randomly to disrupt a network by attackers who have total control over a collection of authorised devices.[124] A Byzantine threat entails one or more affected nodes working together to carry out a variety of attacks, such as sending packets down inefficient paths, establishing routing loops, or picking and choosing which packets to drop. All of these actions impair network performance, interfere with network routing services, and consume network component resources.[125] Once attackers have yielded the active group of insider nodes in the network hostile, the entire network will be under their control, and further safe data transfer will be impossible.

Subhashini et al., 2019[126] present a viable approach for identifying information insertion and Byzantine attacks utilising the proposed unpredictable network coding scheme. These attackers are in complete control of some of the authorised nodes and are capable of acting irregularly to cause systemic disruption. Through the use of network coding, neighbouring intermediary nodes in a network can encrypt data packets that are sent to them. The priority scheduling approach is then employed as an improvisation tactic to successfully schedule data transmission. The Priority Algorithm includes changing the threshold to achieve the optimal false alarm, fault detection, or error rate. By aspects of packet delivery rate, throughput, and delay, simulated findings in the NS2 scenario show that using the priority scheduling strategy produces successful outcomes. Furthermore, when the priority scheduling approach is utilised, attack identification measures such as the false positive ratio and detection ratio improve. A novel priority technique for an uplink scheduler in a WSN has been created in order to increase efficiency and detection measures.

Routing attacks. Routing assaults are one of the most successful network layer attacks because they target the network's routing capabilities. There are various forms of routing attacks, including Routing Table Poisoning, Route Cache Poisoning, Routing Table Overflow, Packet Replication, and Rushing assaults.[127] The attacker node transmits a fake route or tries to modify the route data in the packet in routing table poisoning. A routing table attack aims to clog up networks, degrade functionality, or severely damage route functions. Reactive routing techniques employ caches to store freshly discovered routes for faster processing, whereas initiative-taking routing approaches rely on routing tables. The adversary may try to flood the cache with fake routes in order to stop the creation of new genuine entries. Caches are used by routing protocols to save the newly discovered routes for better execution. On the other hand, proactive routing protocols seek to implement routing access in the absence of dependent route discovery. This implementation gives the malicious node the way to send massive fake routing advertisements to nodes to overcome the routing table, which leads to the implementation stops. The adversary node uses packet replication to repeatedly send the same message, confusing the routing process and using up all available bandwidth and energy. The request RREQ packet will be received by the adversary node in a rushed assault that is situated along the route path of the source node. With "PUSH," this node attempts to transfer the packet quickly to the target node. The repeated RREQ from the origin node will be dumped by the target node because it is mistaken for a duplicate packet. However, these security procedures can only detect pathways that are less than two jumps away and are only useful against rushing assaults.[127]

Packet replay attack. In the packet replay assault, the adversary attempts to intercept the packet being sent from the source node and, if successful, delays the packet transmission before sending it to the receiving node. The delay will result in receiving an erroneous location due to the wrong time and fluctuating transmission power provide a more advanced deep learning system for identifying and blocking replay attacks.[128] On the dataset, decision trees are used with the help of a support vector machine (SVM) to demonstrate their effectiveness. Many studies have shown that SVM has a success rate of over 98% in identifying and blocking WSN assaults. During a replay assault, the whole route from the sensing node to the basis station is filled with bogus packets. As a consequence, on the receiver side, a fictitious distance and a fictitious location are estimated depending on the signal's arrival time, resulting in a simulated time of propagation and false signal strength.

Transport layer attacks

The transportation layer allows for the logical connection of two different sensor nodes between applications. The transportation layer protocol is vulnerable to attacks from various sources, such as flood attacks, TCP SYN, and Desynchronisation attacks.[17]

TCP SYN flooding attack. Transmission control protocol SYN flooding is a kind of denial-of-service assault. Transmission control protocol is a transport layer protocol that employs a handshake to communicate between two nodes. During the handshake, three messages (SYN, SYN-ACK, and ACK) are transmitted between sensor nodes to assess whether the nodes are suitable for communication and to transmit data using serial codes. The malicious node will send an increased number of SYN packets to start an SYN attack. Once the flood of SYN packets was received, the victim node has to reply with the SYN + ACK packet and waited for the corresponding ACK packets. As a result, the victim node has half-open connections. The victim node can only begin to communicate again with other nodes after a TCP half-open connection is timed out, with much time already wasted for unnecessary waiting.[129]

Burmaka et al., 2019[130] proposed a method for detecting DDoS attacks (TCP SYN Flood, HTTP Flood), as well as several types of system resource usage, including miner scripts, botnet scripts, and malware. A proposed approach involves tracking system resources, extracting traits, and spotting abnormalities through critical selection detection. Accurate detection relies on the immune mechanism technique, in which any sample of parameters that is "nonself" causes an alarm. This method also enables to detection of unknown threats or system resource abuses. This approach has a few advantages, including minimal platform resource use since it checks a small amount of data

and continuous system resource usage that is independent of the load on the monitored system. The second advantage is portability; this technique may be applied to a variety of devices, such as central servers, routers, and switches, as well as desktops and integrated ones. This approach has the limitation that it can only find problems that affect CPU and memory use. As a result, it cannot replace a typical IDS, but it can be a helpful addition to an IDS that uses signatures. Finding the optimal set of parameters for spotting anomalies and minimising the effects of a variety of factors is the key issue that still has to be resolved. It may accelerate the search for that match. Making an unsupervised machine learning method that can calculate the optimal range of system resource utilisation for a typical system state is an additional option. This will assist in lowering the number of false positives. Additionally, this method has to be examined for various DDoS excesses and assaults on diverse structures.

Session hijacking. Another name for an impersonated assault is a session hijacking assault. The assailant assumes the identity of the victim's sensor node's IP address, ascertains the pattern of packets that the receiver sensor node anticipates, and executes a denial-of-service attack.[131,132] Hu et al., 2019[133] analyse the ability to launch the PHY-UIR hijacking attack to enable an aggressor to control the common key. They also suggest that when devices exchange information simultaneously on the shared keys established, they can detect whether a third party agrees to different keys. Through human interactions, the hijacking session attack manipulates the key agreement and compels genuine devices to carry out the attacker's PHY UIR protocol. Conclusions from simulation and testing validate the attack and provide excellent attack performance for the key produced.

Singh, 2020[134] Token and Session ID Reset strategies were created and put into use to avoid session hijacking brought on by cookie duplication. The suggested approach makes use of session-id, tokens, IP, and browser fingerprinting to authenticate the user on the web server. This method saves the token in local storage on the client's side, rather than in cookies. With this strategy, Man-in-the-middle (MITM), Cross-Site Scripting (XSS), Session fixation, Cookie-stealing malware, Predictable token and session id, Physical data theft, and Cookie Cloning attacks are all less likely. The suggested method takes around 6 milliseconds longer than the OTC method. The attacker can impersonate the user before the token and session ID expire. To solve this problem, establish a brief period for the token and session id to be renewed.

Prapty et al., 2020[135] provide a novel approach to protect cookie privacy, authenticity, and integrity and to guard against replaying and cookie toxin assaults that can hijack sessions. To produce and verify one-time session cookies, they employed reverse proxy servers. To handle the encryption one-time cookies, they built a custom cryptographic procedure system. They performed a security analysis to validate their proposed system. By utilising OTC rather than pricey HTTPS connections, they may avoid cookie toxicity threats and replay attacks that hijack sessions.

Desynchronisation attack. Desynchronization is the breakdown of established connectivity among network elements. An attacker will provide false communication with false sequence numbers and control flags to disrupt normal communication between nodes, forcing the nodes to request retransmission of the lost packets.[17] Once the assault is executed properly, it may prevent the nodes continue transferring files, consuming additional power while the transmission is being resynchronized and errors are fixed. Desynchronization assaults may be extremely harmful when combined with other attacks like wormholes, Sybil, or replay, which affect the round duration among nodes and hence break the duration integration.

Trinh et al., 2020[136] suggested that LBCbAP (Lightweight Block Cipher-Based Mutual Authentication Protocol) is a unique security protocol relying on lightweight block cyphers. The primary security primitive in this protocol is CRAFT. CRAFT is a tweakable block cypher that was recently proposed, and its security has been proven by an independent security study. Their in-depth security examination of LBCbAP, conducted both covertly and overtly utilising a GNY concept and the Scyther program, shows that it is protected against several assaults, including dangers from interruptions and secret exposure. An expense examination of the designed protocol and contrast to similar lightweight protocols shows that LBCbAP is cost-effective. Designing a multiple-reader RIFD system based on LBCbAP is also an intriguing area for future research. In that study, it may be possible to solve the concerns of how the viewer initialises its dataset if communication could be retrieved if the writer's dataset is destroyed and the way the label interacts among many readers while being private and synchronous. Before the proposed protocol can be implemented in any operational environment, it must first undergo extensive community study and evaluation (it has not yet been used in a practical context).

Application layer attacks

HTTP, TELNET, SMTP, and FTP are application layer protocols used to send user data. Because it directly includes user information, the attacker finds application layer information particularly appealing. Application layer assaults use additional throughput and refill the battery energy of sensor nodes. DoS and Deluge attacks are application layer attacks on the WSN.[137]

DoS attack. A DoS (Denial of Service) occurs when an adversary interferes with the legal node's ability to provide functions by transmitting additional meaningless signals to the recipient sensor node in an attempt to use up broadband and power.[41] Al-issa et al., 2019[138] proposed to use decision trees and support vector machines to identify assault behaviours for a certain dataset. The dataset was developed to distinguish between Blackhole, Grayhole, Flooding, and Scheduling, four types of DoS assaults. Using machine learning techniques, decision trees and support vector algorithms were used to evaluate the effectiveness of DoS identification on the WSN dataset. The floods and grayhole assaults were assessed, with the whole dataset being used first. SVM performed worse than decision trees in terms of classification. On the other hand, their approach failed to detect various forms of DoS attack scenarios. According to the experimental results, decision trees outperformed Support Vector Machines in terms of both true-positive rates and false-positive rates, with 99.86% vs. 99.62% and 0.05% vs. 0.09%, correspondingly.

Nagamuthu, 2019[139] presented a hierarchical clustering technique to detect node compromise in a WSN related to DoS assaults. The strategy makes use of multiple representation sites (nodes) by selecting nodes that are widely dispersed and then centring them by a fractional amount to enable efficient DoS assault identification and spread. The clusters thus come in a variety of geometrical forms. For a larger number of nodes, segmentation and irregular sampling are used more quickly to detect attacks. Outliers were successfully filtered using irregular sampling. The main advantage of the clustering algorithm-based identification approach is its scalability for high numbers of nodes without sacrificing cluster quality. The authors have to think about utilising a different clustering strategy which enhances the spread and dispersion of nodes in a network to speed up attack identification and prevention.

Prabakaran et al., 2020[140] introduced an SVM-based ID approach. They use a feature vector to characterise nodes in the ID algorithm. The SVM parameter vectors and feature values are generated using the optimal feature subset. By examining the vector with the best features and characteristic weights, as well as the one with the highest classification precision, the most perfect chromosome may be identified. Limit value and score are two crucial factors that they used. The sum value of the closest neighbouring nodes is used to calculate the score. The limit value is the limit or threshold that separates aberrant nodes from the base station. As a result, the SVM detection algorithm distinguishes between irregular nodes that broadcast RREQ signals more frequently than normal nodes. In this case, the Ant Colony Optimization (ACO) method employs to choose the best path for sending data from the origin to the receiving node. A proposed method increases network lifetime and WSN intrusion node detection. Uneven nodes will be shown as a result. The evaluation's results led to the recommended technique having a higher accuracy rate.

Deluge attack. Deluge assaults are another name for reprogramming attacks. Applications and software platforms used by the adversary's sensor node are infected with malicious software (viruses, spyware, Trojan horses, and worms). The sensor node's harmful malware propagates throughout the network, slowing it down or even damaging it.[41]

Conclusion and future research

The requirement for security procedures becomes crucial as WSN develops and is often employed in several high impact applications. Many limitations, including those on processor speed, memory, ECA, unsupervised activities, and inconsistent connectivity, among others, severely hurt WSNs. Secure communication is vulnerable to several assaults. The lifetime of the node network is shortened due to energy depletion. The attack forms depending on the layer WSN architecture were explored in this work, and Figure 8 provides a taxonomy for this attack type.

Machine learning methods were primarily used to implement an IDS in the WSN to detect several types of attacks. The majority of the attack types detected by these proposed algorithms were examined in Table 1, along with summaries of the relevant research articles. The disadvantage of those algorithms is that the deployment of a model to a sensor node takes additional memory, and the development and evaluation of the data set for WSN take longer for a machine learning algorithm. To decrease the amount of memory needed to implement a strategy, it may be possible to create a hybrid machine learning prototype for conducting intrusion detection in the WSN.

We identified several issues and challenges in the literature review that we believe should be addressed in future research. The researcher must pay closer attention to the privacy area because it is a significant factor in making wireless networks risky. Three categories can be used to identify privacy: consciousness of privacy dangers faced by smart objects and assistance around the data matter; independent restriction over the gathering and handling of confidential data by those smart objects; and consciousness and regulation of the subsequent usage and dispersal of confidential data by those entities to any entity outside the subject's personal control sphere.[141] An ambiguous understanding of personal information results from the tendency for privacy to alter depending on the individual's perspective and needs. Because of this, it is important to carefully evaluate the user requirements and the sensitivity of the data involved when creating new systems and services. There are several types of privacy threats, such as Identification, Localization and Tracking, Profiling, Privacy violating interaction and presentation. Lifecycle transitions.

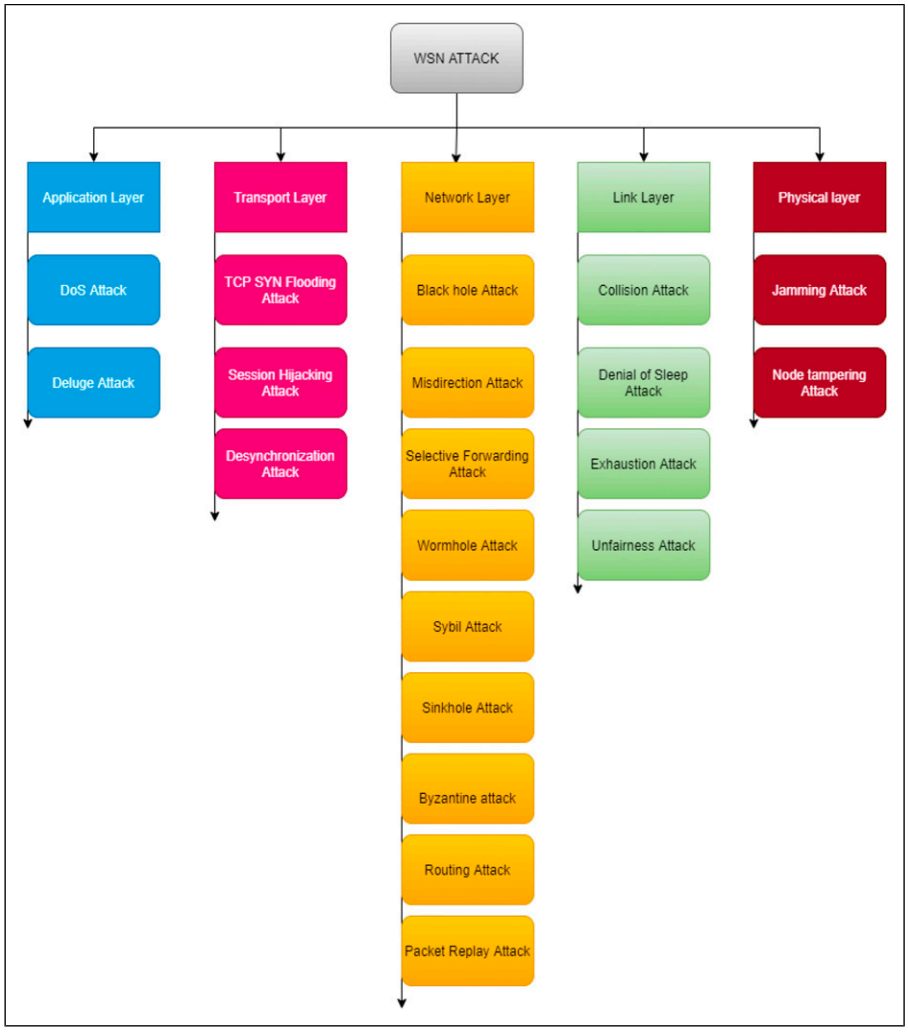

Figure 8. Taxonomy for attack types.

Some solutions are used to combat privacy threats. Although many sensors cannot provide acceptable security procedures owing to a lack of storage and computing power, cryptography is still the most prevalent technology in virtually all of the existing solutions that have been offered.[142]

Another critical area of study and research in WSN is resilience, which can improve its abilities because it is dependent on long-term environments. Resilience was initially used to describe the ability of damaged tissue to repair itself. Later, the idea was broadened to include natural ecosystems, material science, a human-centred system, or a sociological system. One of the earliest scholars to explore the robustness of data systems.[143] They described derived data in their work for a data recovery service. Instead of redundant physical equipment, strategies like a visualised network and mobility control were employed.

Some papers review security and privacy, such as Lin et al., 2021,[144] Gupta and Dharma 2021.[145] Lin et al[144] discussed the linkages between resilience in security and privacy in security. For thorough privacy safeguards, a collection of mobile apps with a solid system design foundation is suggested. Additionally, a mobile healthcare app is created to show how the design principles may be used to cut down on patient wait times while maintaining their privacy. The current study has certain limitations in the literature in that it does not cover all articles related to privacy protection and security, as well as resilience design. Furthermore, the proof is required for the design principles that are suggested in this paper. While Gupta and Dharma[145] discuss the efficacy of security and privacy in Enterprise Information Systems (EIS) and recommend further research to determine the best approach to overcoming these issues.

Finally, its import provides WSN with a labelled dataset on which to train and evaluate the assaults. We notice most currently used strategies only pay attention to one kind of assault on one layer of the WSN, ignoring attacks on other layers.

Table 1. Detection method for attacks.

Authors	Year	Attack type	Type of layer	Technique used	Limitations
Del-Valle-Soto et al	2019	Jamming attack	Physical layer	Have proposed a combined mechanism and extended mechanism to detect reactive jamming attacks	Work on one type of jamming attack only
Bengag, et al	2020	Jamming attack	Physical layer	A detection technique was developed relying on four essential network metrics: packet delivery ratio (PDR), energy consumption (ECA), signal strength indication received (RSSI), and lousy packet ratios (BPR)	This method must improve the detection rate while decreasing false alarms
Dell Valle Soto al	2021	Jamming attack	Physical layer	The technique uses to find sections of damaged knots where energy is limited. Detection is evaluated on four common protocol clusters: PEGASIS, TEEN, LEACH, and HPAR.	This algorithm is dependent on pack loss and energy consumption for detecting the abnormal node
Da-Wen Huang et al	2021	Node tampering attack	Physical layer	a hybrid algorithm for detecting attacks on dynamic WSNs	This mechanism consumes more energy and also does not deal with the dynamics of WSN security
Fotohi et al	2020	Denial of sleep attack	Link layer	A multi-stage method called ASDA-RSA is proposed	Energy consumption must be reduced more for the network lifetime will be increased
Mohd, et al	2020	Denial of sleep attack	Link layer	Using various Kernel functions to achieve better results	This algorithm does not work in actual network sensors. The denial of attack is the only attack that can detect it
Fotohi and Firoozi	2020	Denial of sleep attack	Link layer	A hybrid solution relies on Hopfield's neural network, the mobile sink algorithm, and the leach firefly method (WSN-FAHN)	To decrease energy consumption in WSN, many mobile sinks must be used
Hussain et al	2019	Exhaustion attack	Link layer	A soft decision technique was built to identify collision and depletion assaults. A preventative method is used to assist a node in avoiding these invasive attacks	Another kind of assault cannot be detected using this strategy
Hristozov et al	2020	Exhaustion attack	Link layer	Offer a technique that integrates blocking and attacking with the light authentication process, performed by a trustworthy third party	This strategy does not provide a complete answer for increasing the device's power efficiency
Premkumar and. Sundararajan	2020	Exhaustion attack	Link layer	The deep learning-based defense mechanism (DLDM) proposes detecting and isolating attacks during the data forwarding phase (DFP)	Need to apply an improvement to their technique so can detect all types of DOS attacks
Noorwali et al	2021	Exhaustion attack	Link layer	Detection method for assaults on the IEEE 802.15.4 standard. In the suggested protocol, the IEEE 802.15.4 switching frequency is adaptively changed	When attackers target IoT nodes unfairly, it does not function
Kalkha et al	2019	Blackhole attack	Network layer	It has conducted a blackhole assault and uses WSNs to implement its AODV routing protocol prophylactic method	This algorithm does not work in actual network sensors
Clement Sunder, et al	2020	Blackhole attack	Network layer	An efficient machine learning technique has been developed to detect a black-holes attack on the healthcare network of wireless sensors	This algorithm does not work in actual network sensors. Daley's time needs to reduce more

(continued)

Table 1. (continued)

Authors	Year	Attack type	Type of layer	Technique used	Limitations
Ifzarne et al	2021	Blackhole attack	Network layer	The model was developed using the data gain ratio and the online condescending classification. The appropriate sensor data properties are initially selected using the information gain ratio. Second, different DDoS attacks are recognised and categorised by the online passive aggressive algorithm	Cannot recognise other forms of assaults
Alruhaily and Ibrahim	2021	Blackhole attack	Network layer	present a defence-in-depth security strategy that uses two levels of detection as the foundation for a multi-layer intrusion identification architecture for WSN. A Naive Bayes classifier is used in the first layer, which is installed on the network edge sensors, to make judgements about the analysed packets in real time. A cloud-based random Forest multi-class classifier is used in the second layer's in-depth analysis of the packets under scrutiny	Cannot recognise other forms of assaults
Suma and Harsoor	2022	Blackhole attack	Network layer	When utilising the on-demand link and the energy-aware dynamic multipath (O-LEADM) routing scheme for MANETs to identify black-hole nodes by combining the bait method, the performance of nodes is analysed using influence packets containing destination-sequence (des-Seq) and reply-sequence (rep-Seq) information	This algorithm does not work in actual network sensors. Energy consumption must be reduced
Mustafa et al	2020	Misdirection attack	Network layer	They used a reinforcement learning-based approach	This algorithm does not work in actual network sensors. Energy consumption must be reduced
Singh et al	2020	Misdirection attack	Network layer	Proposed algorithm without using cluster heads to spot misdirection attacks	Reduce energy consumption in wireless sensor networks. Daley's time needs to reduce more
Mehetre et al	2019	Selective forwarding attack	Network layer	Two schemes for secure networking of the data packet were proposed, naming it a two-stage security technique with a dual assurance scheme	This algorithm does not work in real network sensors. Energy consumption must be reduced more in order for the network lifetime will be increased
Zhang and Zhang	2019	Selective forwarding attack	Network layer	Misbehaving can be detected by utilising detective agents closer to the attacker	Not able to detect another type of attack
Hao fu et al	2020	Selective forwarding attack	Network layer	An algorithm data clustering (DCA) to detect a selective transmission attack (DCA-SF)	This algorithm does not deploy for distribution WSN its works on centralised WSN only
UmaRani, and Somasundaram	2020	Selective forwarding attack	Network layer	a distributed BDRM is developed to protect the network against Selex transmitters based on the beta distribution	Not apply on centralized network
Singh and Saini	2021	Selective forwarding attack	Network layer	According to their functions, the complete collection of nodes is divided into three categories: Inspector node (IN), cluster head (CH), and Member node (MN). The cluster head (CH) is the strongest susceptible node in the overall cluster, and if the CH is assaulted, the entire cluster stops functioning on the network. As a result, it is claimed that the newly recognised node as IN may see all of the actions of the CH.	The energy consumption is not solved by this algorithm

(continued)

Table 1. (continued)

Authors	Year	Attack type	Type of layer	Technique used	Limitations
Patel et al	2019	Wormhole attack	Network layer	They proposed an alternative path length calculation based on neighbourhood information	The accuracy's restrictions. A difficult research problem is security neighbourhood detection in mobile wireless sensor networks
Tamilarasi, and Santhi	2020	Wormhole attack	Network layer	The detection of wormhole attacks with optimum path selection by PSO(Particle swarm optimization)	The parameter for this algorithm does not depend on the false rate and detection accuracy
Singh et al	2020	Wormhole attack	Network layer	They employ ANN, which uses connectivity data as a detection mechanism, to spot wormhole assaults in WSNs	Detection accuracy needs to be enhanced
Singh and Saini	2022	Wormhole attack	Network layer	Introduces a new routing approach that aims to ensure a safe data transmission channel. The suggested technique is validated using WSN performance measures such as packet delivery rate, end-to-end delay, bandwidth, and power consumption	The algorithm cannot detect another attack
Alajlan, A. M	2022	Wormhole attack	Network layer	A novel multi-step detection (MSD) approach for detecting wormhole attacks on WSN is introduced. The MSD is made up of three algorithms that identify and thwart simplex and duplex wormhole attacks	This algorithm does not deploy for distribution in the real network
Jamshidi et al	2019	Sybil attack	Network layer	Model is being proposed for cluster-based sensor networks	This algorithm does not work in real network sensors
Angappan et al	2021	Sybil attack	Network layer	It proposes a new protocol for Sybil attack detection, which is a mechanism used in W SN to recognise and separate Sybil attacks	The NoSad cannot cope if there are lower than or equivalent to two Sybil nodes
Mounica et al	2021	Sybil attack	Network layer	They presented a method to employ a machine learning model developed to identify accuracy and efficiency via machine learning methods to recognise Sybil and other vulnerabilities	Energy compulsion and lifetime do not discuss
Nadeem and Alghamdi	2019	Sinkhole attack	Network layer	They use data aggregation technology to detect a sinkhole attack in BAN for information on distance and energy	Needs to increase the accuracy of detection and reduce the false rate
Nwankwo	2019	Sinkhole attack	Network layer	Propose an ant-colony optimisation sinkhole detection programmed to increase sinkhole detection employing packet drops, parcel delivery rates, and energy exchange	They need to apply this algorithm in simulation NS3 and a wireless sensor network to discuss its accuracy detection and false error rate. All the results it has been initiated
Dhivya et al	2021	Sinkhole attack	Network layer	Presented a novel approach to the proposed method for detecting and preventing sinkhole assaults on WSN. The AODV (ad hoc on-demand distance vector) routing protocol can be extended to a wide range of terminals	Concentrate on decreasing power use while evaluating and researching sinkhole threats concerning many different route protocols
Subhashini et al	2019	Byzantine attack	Network layer	The suggested method of random network coding is used to conduct a realistic approach to detecting data injection and byzantine assaults	They cannot detect the attack in the multi-network (heterogeneous). Its works in one type of network

(continued)

Table 1. (continued)

Authors	Year	Attack type	Type of layer	Technique used	Limitations
Rajaram et al	2020	Packet replay attack	Network layer	Provide a better deep learning strategy for identifying and blocking replay attacks. The dataset is used to demonstrate the efficiency of decision trees with the help of an SVM support vector machine (support vector machine)	This approach does not work in real network sensors
Burmaka et al	2019	TCP SYN flooding attack	Transport layer	A method is proposed to efficiently identify DDoS (TCP SYN Flood, HTTP Flood) assaults and other network abnormalities, such as botnet assaults, mining abuse, and ransom abuse	They should create an unsupervised machine learning strategy to forecast the best range of system resource utilisation for a steady state of the system and choose a group of ideal criteria to reduce the vector of attributes for identifying abnormalities. The rate of false-positive errors may decline as a result. Additionally, this technique must be evaluated against various DDoS assault forms and excesses on various infrastructures
Hu et al	2019	Session hijacking	Transport layer	They analyse the ability to launch the PHY-UIR hijacking attack to enable an aggressor to control the standard key	This algorithm does not work in real network sensors
Singh, T	2020	Session hijacking	Transport layer	To prevent session hijacking by cookie duplication, a token and session ID reset method were suggested and put into practice. The suggested method uses the session id, token, IP, and browser fingerprints to verify the user's identity on the web server	Cannot detect other attack types
Prapty et al	2020	Session hijacking	Transport layer	Presented a cookie protection mechanism that is both secure and efficient. They encrypted critical information in the cookie to preserve cookie integrity and secrecy to prevent an attacker from injecting cookies	When more requests are being made at once, it takes longer to encrypt cookie information at first, but after a specific point, it takes less duration even if there are more attempts. They are unable to recognise other forms of assault
Trinh et al	2020	Desynchronization attack	Transport layer	Proposed a new lightweight block cypher-based security protocol called LBCbAP	This algorithm does not work in real network sensors
Al-issa et al	2019	DoS attack	Application layer	Two machine learning systems are proposed to detect signatures on a data set. Decision trees and vector support machines	This method must account for more circumstances and procedures for DoS assaults. It is also possible to experiment with various classifications and data mining approaches
Nagamuthu Krishnan, S. S	2019	DoS attack	Application layer	It is suggested to use clustering techniques to find WSN nodes that have been compromised by DoS assaults	It is necessary to speed up the process of detecting assaults and reducing their duration
Prabakaran et al	2020	DoS attack	Application layer	Developed a method for employing vector machine support in infiltration detecting (ID) (SVM)	Need to reduce an energy consumption

However, it is crucial to create a cross-layer IDS that can identify multiple assaults on various WSN levels. When we looked at the academics' recent concentration on each form of assault, we discovered the graphs indicate the number of articles published each year for each sort of assault. Some researchers concentrate on a variety of attacks, while others receive little attention or study. Researchers may focus more on this sort of assault in the future to avoid it and enhance network performance.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Alhamzah Alnoor https://orcid.org/0000-0003-2873-2054

References

1. Lee I and Lee K. The internet of things (IoT): applications, investments, and challenges for enterprises. *Bus Horiz* 2015; 58(4): 431–440.
2. WIRELESS SENSORS NETWORK MARKET - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS. 2021 - 2026. Access on 29/9/2021. https://www.mordorintelligence.com/industry-reports/wireless-sensor-networks-market#faqs
3. Hamid RA, Albahri AS, Alwan JK, et al. How smart is e-tourism? A systematic review of smart tourism recommendation system applying data management. *Comput Sci Rev* 2021; 39: 100337.
4. Albahri AS, Alnoor A, Zaidan AA, et al. Based on the multi-assessment model: towards a new context of combining the artificial neural network and structural equation modelling: a review. *Chaos, Solitons Fractals* 2021; 153: 111445.
5. Eneizan B, Mohammed AG, Alnoor A, et al. Customer acceptance of mobile marketing in Jordan: an extended UTAUT2 model with trust and risk factors. *Int J Eng Bus Manag* 2019; 11: 1847979019889484.
6. Balakrishnan SM and Sangaiah AK. MIFIM—Middleware solution for service centric anomaly in future internet models. *Future Gener Comput Sys* 2017; 74: 349–365.
7. Carvalho LF, Abrão T, de Souza Mendes L, et al. An ecosystem for anomaly detection and mitigation in software-defined networking. *Expert Sys Appl* 2018; 104: 121–133.
8. Al-Abrrow H, Fayez AS, Abdullah H, et al. Effect of open-mindedness and humble behavior on innovation: mediator role of learning. *Int J Emerg Mark* 2021.
9. Alsalem MA, Mohammed R, Albahri OS, et al. Rise of multiattribute decision-making in combating COVID-19: a systematic review of the state-of-the-art literature. *Int J Intell Syst* 2022; 37(6): 3514–3624.
10. Wang W, Zhang S, Duan G, et al. *Security in wireless sensor networks. InWireless network security.* Berlin, Heidelberg: Springer, 2013, pp. 129–177.
11. Abdulaali AR, Alnoor A and Eneizan B. A multi-level study of influence financial knowledge management small and medium enterprises. *Polish J Manag Stud* 2019; 19: 21–31.
12. Khaw KW, Alnoor A, Al-Abrrow H, et al. Modelling and evaluating trust in mobile commerce: a hybrid three stage Fuzzy Delphi, structural equation modeling, and neural network approach. *Int J Hum Comput Interact* 2022; 38: 1–7.
13. Fadhil SS, Ismail R and Alnoor A. The influence of soft skills on employability: a case study on technology industry sector in Malaysia. *Interdiscip J Inf Knowl Manag* 2021; 16: 255–283.
14. Hadi AA, Alnoor A and Abdullah HO. Socio-technical approach, decision-making environment, and sustainable performance: role of ERP systems. *Interdiscip J Inf Knowl Manag* 2018; 13: 397–415.
15. Khaw KW, Thurasamy R, Al-Abrrow H, et al. Influence of generational status on immigrants' entrepreneurial intentions to start new ventures: a framework based on structural equation modeling and multicriteria decision-making. *J Entrepreneurship Emerg Economies* 2021.
16. Bamakan SM, Wang H and Shi Y. Ramp loss K-support vector classification-regression; a robust and sparse multi-class approach to the intrusion detection problem. *Knowl-Based Sys* 2017; 126: 113–126.
17. Löf A and Nelson R. Annotating network trace data for anomaly detection research. In: 39th annual IEEE conference on local computer networks workshops, Edmonton, AB, Canada, 8 September 2014. IEEE, pp. 679–684.
18. Ghafir I, Husak M and Prenosil V. A survey on intrusion detection and prevention systems. In: Proceedings of student conference Zvule, IEEE/UREL, Aug 2014. Brno University of Technology, Vol. 1014.
19. AL-Abrrow H, Al-Maatoq M, Alharbi RK, et al. Understanding employees' responses to the COVID-19 pandemic: the attractiveness of healthcare jobs. *Glob Bus Organ Excell* 2021; 40(2): 19–33.
20. Al-Abrrow H, Alnoor A, Ismail E, et al. Psychological contract and organizational misbehavior: exploring the moderating and mediating effects of organizational health and psychological contract breach in Iraqi oil tanks company. *Cogent Bus Manag* 2019; 6(1): 1683123.
21. Abbas S, Al-Abrrow H, Abdullah HO, et al. Encountering Covid-19 and perceived stress and the role of a health climate among medical workers. *Curr Psychol* 2022; 41(12): 9109–9122.
22. Alnoor A, Zaidan AA, Qahtan S, et al. Toward a sustainable transportation industry: oil company benchmarking based on the extension of linear Diophantine fuzzy rough sets and

multicriteria decision-making methods. *IEEE Trans Fuzzy Syst* 2022; 31: 1–11.
23. Al-Abrrow H, Alnoor A and Abbas S. The effect of organizational resilience and CEO's narcissism on project success: organizational risk as mediating variable. *Organ Manag J* 2019; 16(1): 1–13.
24. Bala T, Bhatia V, Kumawat S, et al. A survey: issues and challenges in wireless sensor network. *Int J Eng Technol* 2018; 7(2): 53–55.
25. Alnoor AM, Al-Abrrow H, Abdullah H, et al. The impact of self-efficacy on employees' ability to accept new technology in an Iraqi university. *Glob Bus Organ Excell* 2020; 39(2): 41–50.
26. Sandberg H, Alnoor A and Tiberius V. Environmental, social, and governance ratings and financial performance: evidence from the European food industry. *Bus Strategy Environ* 2022.
27. Abdullah H, Ismail I, Alnoor A, et al. Effect of perceived support on employee's voice behaviour through the work engagement: a moderator role of locus of control. *Int J Process Manag Benchmarking* 2021; 11(1): 60–79.
28. Alnoor A. Human capital dimensions and firm performance, mediating role of knowledge management. *Int J Bus Excellence* 2020; 20(2): 149–168.
29. Amutha J, Sharma S and Nagar J. WSN strategies based on sensors, deployment, sensing models, coverage and energy efficiency: review, approaches and open issues. *Wirel Pers Commun* 2020; 111(2): 1089–1115.
30. Alharbi R and Alnoor A. The influence of emotional intelligence and personal styles of dealing with conflict on strategic decisions. *PSU Res Rev* 2022 (ahead-of-print).
31. Albahri AS, Alnoor A, Zaidan AA, et al. Hybrid artificial neural network and structural equation modelling techniques: a survey. *Complex Intell Sys* 2022; 8(2): 1781–1801.
32. Alnoor A, Tiberius V, Atiyah AG, et al. How positive and negative electronic word of mouth (eWOM) affects customers' intention to use social commerce? A dual-stage multi group-SEM and ANN analysis. *Int J Hum Comput Interact* 2022; In press: 1–30.
33. Alnoor A, Abdullah HO, AL-Abrrow H, et al. A Fuzzy Delphi analytic job demands-resources model to rank factors influencing open innovation. *Transnatl Corp Rev* 2021; 14: 1–5.
34. Mallick C and Satpathy S. Challenges and design goals of wireless sensor networks: a state-of-the-art review. *Int J Comput Appl* 2018; 179(28): 42–47.
35. Alnoor A, Eneizan B, Makhamreh HZ, et al. The effect of reverse logistics on sustainable manufacturing. *Int J Acad Res Account Finan Manag Sci* 2018; 9(1): 71–79.
36. Pragadeswaran S. Wireless sensor networks security issues, security needs and different types of attacks based on layers: a survey. *Int J Adv Eng Sci Inf Technol* 2021; 5(5): 1–23.
37. Atshan NA, Al-Abrrow H, Abdullah HO, et al. The effect of perceived organizational politics on responses to job dissatisfaction: the moderating roles of self-efficacy and political skill. *Glob Bus Org Exc* 2022; 41(2): 43–54.
38. Panwar P, Verma R, Rauthan MM, et al. An overview on security issues, attacks, challenges and protocols in WSN. In: Proceedings of integrated intelligence enable networks and computing, 2021, pp. 269–278.
39. Kaur N and Rattan P. A critical review of intrusion detection systems in WSN: challenges and future directions. *Ann Romanian Soc Cell Biol* 2021; 25: 3020–3028.
40. Ahmad R, Wazirali R and Abu-Ain T. Machine learning for wireless sensor networks security: an overview of challenges and issues. *Sensors* 2022; 22(13): 4730.
41. Singh MT, Shrivtastav N and Tripathi HP. Survey paper of wireless sensor network, 2022.
42. Temene N, Sergiou C, Georgiou C, et al. A survey on mobility in wireless sensor networks. *Ad Hoc Networks* 2022; 125: 102726.
43. Al-Abrrow H, Ali J and Alnoor A. Multilevel influence of routine redesigning, legitimacy and functional affordance on sustainability accounting: mediating role of organizational sense-making. *Glob Bus Rev* 2022; 23(2): 287–312.
44. Alnoor A, Al-Abrrow H, Al Halbusi H, et al. Uncovering the antecedents of trust in social commerce: an application of the non-linear artificial neural network approach. *Compet Rev: An Int Bus J* 2022; 32: 492–523.
45. Eneizan BM, abdelqader Alsakarneh AA, AL-kharabsheh KA, et al. An investigation into the relationship between emotional labor and customer satisfaction. *Cent Eur Manag J* 2019; 27(4): 23–47.
46. Alhamdi M, Noor RM, Abdulla M, et al. How does financial analysis influence the firm's failure of Iraqi private sector? *J Soc Sci Res* 2019; 5(9): 1321–1328.
47. Ferasso M and Alnoor A. Artificial neural network and structural equation modeling in the future. In: *Artificial neural networks and structural equation modeling*. Singapore: Springer, 2022, pp. 327–341.
48. Gaurav A, Psannis K and Peraković D. Security of cloud-based medical internet of things (miots): a survey. *Int J Software Sci Comput Intell* 2022; 14(1): 1–6.
49. Pragadeswaran S, Madhumitha S and Gopinath S. Certain investigation on military applications of wireless sensor network. *Int J Adv Res Sci Commun Technol* 2021; 3(1): 14–19.
50. Fourniol M, Gies V, Barchasz V, et al. Applications of an ultra low-power analog wake-up detector for environmental iot networks and military smart dust. In: 2018 IEEE international conference on internet of things and intelligence system (IOTAIS), Bali, Indonesia, 1 November 2018. IEEE, pp. 16–22.
51. Alnoor A, Khaw KW, Al-Abrrow H, et al. The hybrid strategy on the basis of miles and snow and porter's strategies: an

overview of the current state-of-the-art of research. *Int J Eng Bus Manag* 2022; 14: 18479790221080214.
52. Abdullah HO, Atshan N, Al-Abrrow H, et al. Leadership styles and sustainable organizational energy in family business: modeling non-compensatory and nonlinear relationships. *J Fam Bus Manag* 2022 (ahead-of-print).
53. Đurišić MP, Tafa Z, Dimić G, et al. A survey of military applications of wireless sensor networks. In: 2012 Mediterranean conference on embedded computing (MECO), Bar, Montenegro, 19 June 2012. IEEE, pp. 196–199.
54. Jabbar Ak, Almayyahi Ar, Ali Im, et al. Mitigating uncertainty in the boardroom: analysis to financial reporting for financial risk COVID-19. *J Asian Finan Econ Bus* 2020; 7(12): 233–243.
55. Hii PC and Chung WY. A comprehensive ubiquitous healthcare solution on an Android™ mobile device. *Sensors* 2011; 11(7): 6799–6815.
56. Hariharan U, Rajkumar K and Ponmalar A. WBAN for e-healthcare application: systematic review, challenges, and counter measures. In: 2021 international conference on computer communication and informatics (ICCCI), Coimbatore, India, 27 January 2021. IEEE, pp. 1–7.
57. Adeniyi EA, Ogundokun RO and Awotunde JB. IoMT-based wearable body sensors network healthcare monitoring system. In: *IoT in healthcare and ambient assisted living 2021*. Singapore: Springer, pp. 103–121.
58. Alnoor A, Khaw KW, Chew X, et al. The influence of the barriers of hybrid strategy on strategic competitive priorities: evidence from oil companies. *Glob J Flex Syst Manag* 2023; In press: 1–20.
59. Al Ameen M, Liu J and Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications. *J Med Syst* 2012; 36(1): 93–101.
60. Khan MN, Haque H, Labeeb K, et al. Internet of things and wireless sensor network solution in smart environmental. In: 6th international conference on communication and electronics systems (ICCES), Coimbatre, India, 8 July 2021. IEEE, pp. 1–5.
61. Al-Ani K, Abdalkafor A and Nassar A. An overview of wireless sensor network and its applications. *Indones J Electr Eng Comput Sci* 2020; 17(3): 1480–1486.
62. Nadzri MM. Design issues and considerations for hardware implementation of wildlife surveillance system: a review. *J Tomogr Sys Sens Appl* 2021; 4(2): 82–94.
63. Kandris D, Nakas C, Vomvas D, et al. Applications of wireless sensor networks: an up-to-date survey. *Appl Syst Innov* 2020; 3(1): 14.
64. Majid M, Habib S, Javed AR, et al. Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: a systematic literature review. *Sensors* 2022; 22(6): 2087.
65. Radivojević G and Milosavljević L. The concept of logistics 4.0. In: 4th logistics international conference, May 2019: 283–292.
66. Bravo-Arrabal J, Fernandez-Lozano JJ, Serón J, et al. Development and implementation of a hybrid wireless sensor network of low power and long range for urban environments. *Sensors* 2021; 21(2): 567.
67. Uzougbo OI, Ajibade SS and Taiwo F. *An overview of wireless sensor network security attacks: mode of operation, severity and mitigation techniques*. arXiv preprint arXiv: 2011.06779. 2020.
68. Butun I, Morgera SD and Sankar R. A survey of intrusion detection systems in wireless sensor networks. *IEEE Commun Surv Tutorials* 2013; 16(1): 266–282.
69. Vikas N, Sagar BB and Munjul M. Security issues in wireless sensor network–a survey. *J Discrete Math Sci Cryptogr* 2021; 24(5): 1415–1427.
70. Al Dhabooni SR, Jassim HS, Sharef ZT, et al. Survey: security attacks in wireless sensor networks. *Int Adv Res J Sci Eng Technol* 2017; 4: 1–7.
71. Shanthi S and Rajan EG. Comprehensive analysis of security attacks and intrusion detection system in wireless sensor networks. In: 2016 2nd international conference on next generation computing technologies (NGCT), Dehradun, India, 14 October 2016. IEEE, pp. 426–431.
72. Santoro D, Escudero-Andreu G, Kyriakopoulos KG, et al. A hybrid intrusion detection system for virtual jamming attacks on wireless networks. *Measurement* 2017; 109: 79–87.
73. Del-Valle-Soto C, Valdivia LJ and Rosas-Caro JC. Novel detection methods for securing wireless sensor network performance under intrusion jamming. In: 2019 international conference on electronics, communications and computers (CONIELECOMP), Cholula, Mexico, 27 February 2019. IEEE, pp. 1–8.
74. Bengag A, Bengag A and Moussaoui O. Attacks classification and a novel IDS for detecting jamming attack in WBAN. *Adv Sci Technol Eng Syst J* 2020; 5(2): 80–86.
75. Del-Valle-Soto C, Mex-Perera C, Nolazco-Flores JA, et al. A low-cost jamming detection approach using performance metrics in cluster-based wireless sensor networks. *Sensors* 2021; 21(4): 1179.
76. Huang DW, Liu W and Bi J. Data tampering attacks diagnosis in dynamic wireless sensor networks. *Comput Commun* 2021; 172: 84–92.
77. Fotohi R, Firoozi Bari S and Yusefi M. Securing wireless sensor networks against denial-of-sleep attacks using RSA cryptography algorithm and interlock protocol. *Int J Commun Syst* 2020; 33(4): e4234.
78. Mohd N, Singh A and Bhadauria HS. A novel SVM based IDS for distributed denial of sleep strike in wireless sensor networks. *Wirel Pers Commun* 2020; 111(3): 1999–2022.
79. Fotohi R and Firoozi Bari S. A novel countermeasure technique to protect WSN against denial-of-sleep attacks using firefly and Hopfield neural network (HNN) algorithms. *J Supercomput* 2020; 76(9): 6860–6886.
80. Diaz A and Sanchez P. Simulation of attacks for security in wireless sensor network. *Sensors* 2016; 16(11): 1932.

81. Hussain I, Zahra S, Hussain A, et al. Intruder attacks on wireless sensor networks: a soft decision and prevention mechanism. *Int J Adv Comput Sci Appl* 2019; 10(5): 1–21.
82. Hristozov S, Huber M and Sigl G. Protecting restful IoT devices from battery exhaustion DoS attacks. In: 2020 IEEE international symposium on hardware oriented security and trust (HOST), San Jose, CA, USA, 7 December 2020. IEEE, pp. 316–327.
83. Zaidan AS, Khaw KW and Alnoor A. The influence of crisis management, risk taking, and innovation in sustainability practices: empirical evidence from Iraq. *Interdiscip J Inf Knowl Manag* 2022; 17: 413–442.
84. Sadaa AM, Ganesan Y, Khaw KW, et al. Based on the perception of ethics in social commerce platforms: adopting SEM and MCDM approaches for benchmarking customers in rural communities. *Curr Psychol* 2022; In press: 1–35.
85. Blanchet B, Cheval V, Allamigeon X, et al. *ProVerif: cryptographic protocol verifier in the formal model*, 2012.
86. Hadi AA, Alnoor A, Abdullah H, et al. How does socio-technical approach influence sustainability? Considering the roles of decision making environment. *Appl Decis Sci Bus Manag* 2019; In press: 55.
87. Wah KK, Omar AZ, Alnoor A, et al. Technology application in tourism in Asia: comprehensive science mapping analysis. In: *Technology application in tourism in asia 2022*. Singapore: Springer, pp. 53–66.
88. Premkumar M and Sundararajan TV. DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks. *Microprocess Microsyst* 2020; 79: 103278.
89. Noorwali A, Alvi AN, Khan MZ, et al. A novel QoS-oriented intrusion detection mechanism for IoT applications. *Wirel Commun Mob Comput* 2021; 2021: 2021–2110.
90. Tomić I and McCann JA. A survey of potential security issues in existing wireless sensor network protocols. *IEEE Internet Things J* 2017; 4(6): 1910–1923.
91. Kalkha H, Satori H and Satori K. Preventing black hole attack in wireless sensor network using HMM. *Procedia Comput Sci* 2019; 148: 552–561.
92. Yen JY. Finding the k shortest loopless paths in a network. *Manag Sci* 1971; 17(11): 712–716.
93. Chandy KM and Misra J. Distributed computation on graphs: shortest path algorithms. *Commun ACM* 1982; 25(11): 833–837.
94. Clement Sunder AJ and Shanmugam A. Black hole attack detection in healthcare wireless sensor networks using independent component analysis machine learning technique. *Curr Signal Transduct Ther* 2020; 15(1): 56–64.
95. Ifzarne S, Tabbaa H, Hafidi I, et al. Anomaly detection using machine learning techniques in wireless sensor networks. *J Phy Conf Ser* 2021, 1743(1): 012021.
96. Crammer K, Dekel O, Keshet J, et al. Online passive aggressive algorithms, 2006.
97. Alruhaily NM and Ibrahim DM. A multi-layer machine learning-based intrusion detection system for wireless sensor networks. *Int J Adv Comput Sci Appl* 2021; 12(4): 281–288.
98. Suma S and Harsoor B. An approach to detect black hole attack for congestion control utilizing mobile nodes in wireless sensor network. *Mater Today Proc* 2022; 56: 2256–2260.
99. Kardi A and Zagrouba R. Attacks classification and security mechanisms in wireless sensor networks. *Adv Sci Technol Eng Syst J* 2019; 4(6): 229–243.
100. Mustafa I, Aslam S, Qureshi MB, et al. Reinforcement learning-based misdirection attack prevention technique for WSN. In: 2020 international wireless communications and mobile computing (IWCMC), Limassol, Cyprus, 15 June 2020. IEEE, pp. 721–726.
101. Singh MM, Barthakur SK and Singh TR. Misdirection attack detection in wireless sensor network, 2020.
102. Abdullah H, Thajil K, Alnoor A, et al. Predicting determinants of use mobile commerce through modeling non-linear relationships. *Cent Eur Bus Rev* 2022.
103. Wang W, Zhang S, Duan G, et al. Security in wireless sensor networks. In: *Wireless network security*. Berlin, Heidelberg: Springer, 2013, pp. 129–177.
104. Khaw KW, Alnoor A, Al-Abrrow H, et al. Reactions towards organizational change: a systematic literature review. *Curr Psychol* 2022; In press: 1–24.
105. Alnoor A, Wah KK and Hassan A. Artificial neural networks and structural equation modeling: marketing and consumer research applications.
106. Mehetre DC, Roslin SE and Wagh SJ. Detection and prevention of black hole and selective forwarding attack in clustered WSN with active trust. *Cluster Comput* 2019; 22(1): 1313–1328.
107. Zhang Q and Zhang W. Accurate detection of selective forwarding attack in wireless sensor networks. *Int J Distrib Sens Netw* 2019; 15(1): 1550147718824008.
108. Fu H, Liu Y, Dong Z, et al. A data clustering algorithm for detecting selective forwarding attack in cluster-based wireless sensor networks. *Sensors* 2019; 20(1): 23.
109. UmaRani V and Somasundaram K. Detection of selective forwarding attack using BDRM in wireless sensor network. *AIP Conf Proc* 2020; 2271(1): 030029.
110. Singh S and Saini HS. Learning-based security technique for selective forwarding attack in clustered WSN. *Wirel Pers Commun* 2021; 118(1): 789–814.
111. Siddiqui A, Karami A and Johnson MO. A wormhole attack detection and prevention technique in wireless sensor networks. *Int J Comput Appl* 2017; 174: 1–8.
112. Patel M, Aggarwal A and Chaubey N. Detection of wormhole attack in static wireless sensor networks. In: *Advances in computer communication and computational sciences*. Singapore: Springer, 2019, pp. 463–471.

113. Tamilarasi N and Santhi SG. Detection of wormhole attack and secure path selection in wireless sensor network. *Wirel Pers Commun* 2020; 114(1): 329–345.
114. Singh MM, Dutta N, Singh TR, et al. A technique to detect wormhole attack in wireless sensor network using artificial neural network. In: *Evolutionary computing and mobile sustainable networks 2021*. Singapore: Springer, pp. 297–307.
115. Singh S and Saini HS. Intelligent ad-hoc-on demand multipath distance vector for wormhole attack in clustered WSN. *Wirel Pers Commun* 2022; 122(2): 1305–1327.
116. Alajlan AM. Multi-step detection of simplex and duplex wormhole attacks over wireless sensor networks. *Comput Mater Contin* 2022; 70(3): 4241–4259.
117. Jamshidi M, Zangeneh E, Esnaashari M, et al. A novel model of sybil attack in cluster-based wireless sensor networks and propose a distributed algorithm to defend it. *Wirel Pers Commun* 2019; 105(1): 145–173.
118. Angappan A, Saravanabava TP, Sakthivel P, et al. Novel Sybil attack detection using RSSI and neighbour information to ensure secure communication in WSN. *J Ambient Intell Humaniz Comput* 2021; 12(6): 6567–6578.
119. Mounica M, Vijayasaraswathi R and Vasavi R. Detecting sybil attack in wireless sensor networks using machine learning algorithms. *IOP Conf Ser: Mater Sci Eng* 2021; 1042(1): 012029.
120. Nithiyanandam N, Parthiban PL, Rajalingam B, et al. Effectively suppress the attack of sinkhole in wireless sensor network using enhanced particle swarm optimization technique. *Int J Pure Appl Math* 2018; 118(9): 313–329.
121. Nadeem A and Alghamdi TG. Detection algorithm for Sinkhole attack in body area sensor networks using local information. *Int J Netw Secur* 2019; 21(4): 670–679.
122. Nwankwo KE. Sinkhole attack detection in a wireless sensor networks using enhanced ant colony optimization to improve detection rate. In: 2019 2nd international conference of the IEEE Nigeria computer chapter (NigeriaComputConf), Zaria, Nigeria, 14 October 2019. IEEE, pp. 1–6.
123. Dhivya M, AP SR and Sneha KV. Detection and prevention of Sinkhole attack in wireless sensor network using Armstrong 16-digit key identity and GAN Network. *Int J Progressive Res Sci Eng* 2021; 2(3): 58–61.
124. Xian J, Wu H, Mei X, et al. NMTLAT: a new robust mobile multi-target localization and tracking scheme in marine search and rescue wireless sensor networks under Byzantine attack. *Comput Commun* 2020; 160: 623–635.
125. Yang Y, Xiong P, Wang Q, et al. Analysis of Byzantine attacks for target tracking in wireless sensor networks. *Sensors* 2019; 19(15): 3436.
126. Subhashini SJ, Stalin B and Vairamuthu J. Improvising reliability and security in multiple relay network using optimal scheduling, 2019.
127. Karthigha M, Latha L and Sripriyan K. A comprehensive survey of routing attacks in wireless mobile ad hoc networks. In: 2020 international conference on inventive computation technologies (ICICT), Coimbatore, India, 26 February 2020. IEEE, pp. 396–402.
128. Rajaram P, Sathishkumar A and Khadirkumar N. An enhanced deep learning approach for preventing replay attacks in wireless sensor network. *Solid State Technol* 2020; 63(4): 8010–8023.
129. Lupu TG. Main types of attacks in wireless sensor networks. In: Proceedings of the 9th WSEAS international conference on signal, speech and image processing, and 9th WSEAS international conference on multimedia, internet and video technologies, 3 September 2009, pp. 180–185.
130. Burmaka I, Zlobin S, Lytvyn S, et al. Detecting flood attacks and abnormal system usage with artificial immune system. In: *International scientific-practical conference*. Cham: Springer, 2019, pp. 131–143.
131. Ibrahim MH. OCTOPUS: an edge-fog mutual authentication scheme. *Int J Netw Secur* 2016; 18(6): 1089–1101.
132. Park N and Kang N. Mutual authentication scheme in secure internet of things technology for comfortable lifestyle. *Sensors* 2015; 16(1): 20.
133. Hu Q, Du B, Markantonakis K, et al. A session hijacking attack against a device-assisted physical-layer key agreement. *IEEE Trans Industr Inform* 2019; 16(1): 691–702.
134. Singh T. Prevention of session hijacking using token and session id reset approach. *Int J Inf Technol* 2020; 12(3): 781–788.
135. Prapty RT, Md SA, Hossain S, et al. Preventing session hijacking using encrypted one-time-cookies. In: 2020 wireless telecommunications symposium (WTS), Washington, DC, 22 April 2020. IEEE, pp. 1–6.
136. Trinh C, Huynh B, Lansky J, et al. A novel lightweight block cipher-based mutual authentication protocol for constrained environments. *IEEE Access* 2020; 8: 165536–165550.
137. Gavric Z and Simic D. Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks. *Ing Inv* 2018; 38(1): 130–138.
138. Al-issa AI, Al-Akhras M, ALsahli MS, et al. Using machine learning to detect DoS attacks in wireless sensor networks. In: 2019 IEEE Jordan international joint conference on electrical engineering and information technology (JEEIT), Amman, Jordan, 9 April 2019. IEEE, pp. 107–112.
139. Nagamuthu Krishnan SS. Denial of service (DoS) detection in wireless sensor networks applying geometrically varying clusters. In: *International conference on computer networks and communication technologies*. Singapore: Springer, 2019, pp. 1023–1030.
140. Prabakaran K, Kumaratharan N, Suresh G, et al. An Evaluation of Effective Intrusion DoS Detection and Prevention System Based on SVM Classifier for WSN. *IOP Conf Ser: Mater Sci Eng* 2020; 925(1): 012068.

141. Ziegeldoorf JH, Morcon OG and Wehrle K. Privacy in the internet of things: threats and challenges. *J Comput Mach* 2017; 7(1): 110.
142. Feng H and Fu W. Study of recent development about privacy and security of the internet of things. In: 2010 international conference on web information systems and mining, Sanya, China, 23 October 2010. IEEE, pp. 91–95.
143. Zhang WJ and Lin Y. On the principle of design of resilient systems–application to enterprise information systems. *Enterp Inf Sys* 2010; 4(2): 99–110.
144. Lin W, Xu M, He J, et al. Privacy, security and resilience in mobile healthcare applications. *Enterp Inf Sys* 2021; In press: 1–5.
145. Gupta BB and Agrawal DP. Security, privacy and forensics in the enterprise information systems. *Enterp Inf Sys* 2021; 15(4): 445–447.