Cross-layer based Intrusion Detection System for Wireless Sensor Networks: Challenges, Solutions, and Future Directions

Noradila Nordin[1,2][0000−0002−5354−9780] and Muhammad Syafiq Mohd Pozi[2][0000-0001-9379-7351]

[1] School of Games and Creative Technology, University for the Creative Arts, Farnham, GU9 7DS, England, United Kingdom
[2] School of Computing, University Utara Malaysia, Sintok 06010, Kedah, Malaysia
adila.nordin@uca.ac.uk

Abstract. Wireless Sensor Networks (WSNs) consist of numerous affordable, energy-efficient, compact wireless sensors. These sensors are designed to collect, process, and communicate data from their surrounding environment. Several energy-efficient protocols have been created specifically for WSNs to optimize data transfer rates and prolong network lifespan. Multi-channel protocols in WSN are one of the ways to optimize efficiency and enable seamless communication between nodes, thereby reducing interference and minimizing packet loss through multiple channels. Despite their numerous advantages in data sensing and monitoring, various attacks can pose a threat to a WSN. There are several types of attacks that a WSN may encounter, including spoofing, eavesdropping, jamming, sinkhole attacks, wormhole attacks, black hole attacks, Sybil attacks, and DoS attacks. One of the strategies for enhancing security in WSNs is implementing a cross-layer intrusion detection system (IDS) that can detect initial indicators of attacks that target vulnerabilities across multiple WSN layers. This paper reviews the existing IDS at each layer and the challenges in an energy-efficient cross-layer IDS for WSN in terms of the attacks and IDS approaches.

Keywords: Cross-layer IDS, Wireless Sensor Network, Multi-channel protocol.

1 Introduction

A Wireless Sensor Network (WSN) is a dispersed sensor system made up of small nodes called sensor nodes. These nodes are frequently used for monitoring and detecting different occurrences or events. WSNs are also utilized for target tracking, environment monitoring, and event detection. WSNs are easily deployable in a variety of situations because of their compact size and low power consumption. In WSNs, the sensor nodes often employ low-power radios like IEEE 802.15.4, a 2.4 GHz band radio transmission standard radio technology with a relatively small range of operation. Within this band, the standard permits broadcast on several various channels. Unfortunately, the channels used by this technology, such as Wi-Fi (IEEE 802.11) and Bluetooth

(IEEE 802.15.1), frequently experience interference. In wireless networks, multi-channel communication can lessen the impacts of interference, enhancing network effectiveness, stability, and link dependability, minimizing latency, and reducing total energy usage. This, however, creates another issue.

A wireless sensor network is susceptible to several various attacks. Due to several flaws and, most crucially, the data involved, wireless sensor networks are continually vulnerable to serious attacks. Typically, the nodes in a WSN are tiny, battery-operated gadgets containing sensors, microcontrollers, and communication transcribers. Due to the node's limited resources, wireless sensor networks are susceptible to various threats that may jeopardize the security and integrity of the data. Nevertheless, WSNs are susceptible to risks despite the various benefits they offer regarding data sensing and monitoring. These risk factors include those caused by memory limitations, unreliable communication, higher communication latency, unattended network operation, deployment in an environment prone to attacks and scalability. Some of these attacks, such as random multi-channel jamming attacks that interfere with radio frequencies on wireless communication channels and cause channel congestion, are intended to take down the network. The challenge may be that random multi-channel jamming attacks are difficult to detect and eliminate due to their random jamming behaviours. Attackers have complete discretion over the time and the specific channels to jam. Other attacks aim to eavesdrop on communications. Others are made to introduce erroneous data into the network. This poses a danger to real-time, reliable WSNs. Security in WSNs is, therefore a difficult problem since it depends on the way to evaluate the reliability of sensor data.

Numerous studies on intrusion detection in WSNs have been done in recent years [1, 2, 3, 4, 5]. Intrusion detection is used to detect unauthorized activity in a system. It works well as a security measure to defend WSNs against intrusion. There have been a few studies on the security of WSNs. However, they have mostly emphasized attack prevention instead of attack detection. This is an important study area since an attacker who can go undetected might cause significant damage or disruption. Although several intrusion detection systems have been developed to support WSNs, the majority of these systems only work at one layer of the Open Systems Interconnection (OSI) model. Several proposed intrusion detection systems are based on a cross-layer approach. They comprise the physical, data link, and network layers that contribute to cross-layer intrusion detection systems (IDS) design. By detecting the attackers across multiple layers, cross-layer IDS secures the WSN.

The rest of the paper is organized as follows. Section 2 highlights various attacks and challenges associated with WSN at each layer. Section 3 presents and compares recent existing work in cross-layer IDS in WSN. Section 4 discusses the challenges and future directions on cross-layer IDS, and section 5 concludes the paper.

2 Related Work

2.1 Wireless Sensor Network Cross-layer Protocols

WSNs are networks of many inexpensive, low-power, small wireless sensors. The sensors can gather, analyse, and transmit data from their environment. WSNs have gotten a lot of attention from several application sectors because of their capabilities, including military surveillance, industrial monitoring, target tracking, and environment monitoring. Numerous energy-efficient protocols have been developed for WSNs to maximize throughputs while extending the lifetime of the networks through the Medium Access Control (MAC) and routing protocols, power consumption, and energy harvesting. The protocols are a vital aspect of WSN communication. The protocols determine the allocation of channel resources among the network's nodes in a way that maximizes efficiency, manages channel constraint, and ensures that nodes communicate simultaneously in single or multiple channels effectively to reduce interference which leads to packet drop. The WSNs are susceptible to attacks due to the extensive nature of node dispersion and the hardware limitation of the nodes.

Numerous studies on single-channel WSN protocols such as LEACH [6], RPL [7] and multi-channel protocols such as Chrysso [8] and MiCMAC [9] that interface to the MAC and the network layers, as well as MCRP [10], that interfaces to the MAC, network, and application layers, have been conducted. The real-time nature of MCRP's multi-channel processing enables it to adjust to any location's local interference. MCRP is a cross-layer protocol that is decentralized and centrally controlled to reduce interference without knowing where the channels are occupied in advance. In order to effectively use the spectrum, MCRP considers all channels that are accessible and transmits on a number of them. This generality makes it possible for better channels to be selected based on the location the sensor nodes are deployed. As a result, the protocol reduces the impact of interference, improving network efficiency, stability, and link reliability. While MCRP exhibits promising results in terms of improved resilience to interference, significantly higher throughput, and link stability, extending the lifetime of WSNs, it is vulnerable to numerous attacks because security was not considered. The protocol is more susceptible to attacks due to the cross-layer attributes and usage of several channels which are necessary for proper data transmission and reception. Thus, the intrusion detection system is a potential approach to detect attacks.

2.2 Intrusion Detection Systems

The limitations of sensor nodes in WSNs prevent traditional IDSs from being directly implemented in WSNs. To resolve this issue, various IDSs have been proposed for WSNs. Due to its IDS mechanism and the high processing demands of the algorithms of the IDs, several extended protocols have negatively impacted the network's energy. An IDS tracks traffic data that may be used to spot and prevent intrusions that compromise the privacy, integrity, and accessibility of an information system. An IDS is a term for software or hardware devices that monitor networks for cyberattacks from inside or outside and trigger an alert.

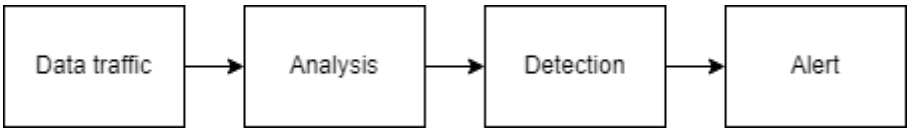

Fig. 1. Fundamental IDS architecture

The fundamental architecture of IDS as shown in Fig. 1, comprises four phases. The first phase is monitoring the captured data traffic, which will then be analysed for any feature extraction or pattern identification in the second phase. The data that has been analysed is examined in the third phase, the detection stage. Any possible harmful data is detected using IDS. The four types of intrusion detection techniques are signature-based, anomaly-based, specification-based, and hybrid-based IDS. These categories are based on the capability of detection algorithms. All these methods can be used to distinguish between trustworthy and malicious traffic. When a match is discovered, the IDS generates an alert.

Signature-based IDS

The signature-based IDS is also called knowledge-based, misuse-based or rule-based IDS. This method depends on a database containing historical attack signatures and known system vulnerabilities. The signature-based IDS only detects known attacks and issues an alert for any matching signature patterns that have been recorded in the signature database. However, as sensor nodes in WSN have limited storage capacity, they could not store all the attack patterns. An example of a signature-based IDS is as proposed by Kurniawan & Yazid (2020)[11]. The IDS implements a blocking approach on the Denial-of-Service (DoS) attack node. It blocks all packets coming from the attacker's node until the attacker runs out of energy.

Anomaly-based IDS

The anomaly-based IDS is also called behaviour-based IDS. This method detects attacks based on the attack patterns which model the user, network, and host system behaviour. An alert will be generated when the detected behaviour deviates from the usual behaviour. In contrast to the signature-based IDS, the anomaly-based IDS can identify known and unknown threats without prior knowledge of the attack. Based on their functions, anomaly-based detection approaches are divided into four categories: statistical, data mining, machine learning, and artificial intelligence.

Mohd et al. (2020) implemented IDS to detect Denial-of-Sleep (DoSL) attacks using support vector machine (SVM) learning in WSN [12]. Mehbodniya et al. (2021) suggested utilizing machine learning techniques like Naive Bayes, random forest, and logistic regression to calculate node packet delivery rates and detect assaults that use false identities, such as the Sybil attack [13]. Mounica et al. (2021) also suggested using machine learning to detect Sybil attacks that distinguish between authorized and illegal access points using the network's raw traffic data to evaluate the efficacy and accuracy of the machine learning approaches [14].

Specification-based IDS

The advantages of signature-based and anomaly-based intrusion detection methods are combined in specification-based IDS. It learns the fundamental traits of attacks, identifies known attacks like a signature-based IDS, and also has the ability of anomaly-based IDSs to identify new attacks that do not fit into the system's normal conduct. Intrusion rules are manually developed in specification-based IDS to detect known and unknown attacks. The manual depiction of specification-based IDS produces few false positives. However, it is a lengthy process to establish the rules. Specification-based IDS can be utilized without the need for training after the rules have been established. Specification-based IDS is ineffective if the manually defined rules do not correspond with the real environment.

The forged rank and routing metric detector (FORCE) proposed by Althubaity et al. (2020) is a specification-based IDS. It makes use of the parent-child relationship in the RPL topology, where the type of node is an essential part of detection [15]. Each node in FORCE examines the control messages it has received from its neighbours, performs local threat detection using the information supplied, and notifies other nodes when it finds threats in the neighbourhood. Gothawal & Nagaraj (2019) suggested an IDS that utilizes the RPL's specifications, such as rank and DODAG version [16]. It monitors the network traffic to record normal network behaviour and compares it with possible attacks.

Hybrid-based IDS

The hybrid-based IDS is a combination of anomaly-based, signature-based or specification-based intrusion detection techniques. Most of the IDSs use any one of the intrusion detections. It is possible to utilize hybrid-based IDS since each intrusion detection technique has its own benefits and drawbacks. In order to increase accuracy and detection rates and reduce false alarm rates, hybrid-based IDS perform the detection by integrating signature-based, anomaly-based, or specification-based intrusion detection methods.

Bhushan & Sahoo (2019) proposed an Integrated IDS scheme (IIS), a hybrid IDS that combines clustering and digital signature [17], while Huang et al. (2022) suggested using multi-hop clustering. In their proposed IDS, to monitor the network and detect the intrusion, the cluster heads and the sink operate collaboratively as IDS agents [18]. Gandhimathi & Murugaboopathi (2020) proposed a two stages hybrid IDS that combines packet-based IDS using a cross-layer approach and flow-based IDS [19]. In the first stage, the sensor network's flow-based IDS differentiates malicious and normal flows. In the second stage, the entire packet's content is validated using cross-layer features by performing packet payload analysis. This increases the detection process’s accuracy.

3 Wireless Sensor Network Intrusion Detection Systems

WSNs are vulnerable to various cyberattacks that might jeopardize the network's availability, privacy, control, and reliability. The nodes are usually deployed in hazardous and remote environments. Thus, they are frequently left unattended and unable to physically safeguard the information flow, which raises the risk of node compromise and lowers network security and protection. Therefore, securing such networks from breaches and assaults is vital where effective security measures are necessary. A possible approach to safeguard WSNs against cyberattacks is the cross-layer intrusion detection system, which protects multiple WSN layers.

3.1 Wireless Sensor Network Attacks

A WSN can be subjected to a variety of attacks, including spoofing, eavesdropping, jamming, sinkhole attack, wormhole attack, black hole attack, Sybil attack and DoS attack [1, 2, 3, 4, 5, 20]. Attacks that cause packet loss are among the most destructive and disruptive threats to WSNs. When such an attack occurs, normal network operations are disrupted because the received data packets or control messages are discarded instead of forwarded to other nodes. Attacks against WSNs can be grouped according to their OSI layers since each layer is vulnerable to multiple attacks.

Physical Layer

The physical layer in WSNs performs various operations, including the production of carrier signals, signal identification, modulation, and information cryptography to transfer data from the sensor nodes across wireless channels. The functions of sensor nodes are compromised when radio transmissions are obstructed or intercepted. A node might be the target of a DoS attack by jamming the physical channel. In this attack, an attacker constantly jams the communication frequencies by sending out unnecessary signals. A legitimate node becomes unavailable to the other nodes as it is occupied with receiving the signals from the malicious node, which jams the network [21].

Bengag et al. (2019) proposed a novel IDS approach based on the packet delivery ratio, energy consumption, signal strength indication received and bad packet ratios as the indicators for detecting jamming attacks in WBAN [22]. An alert is triggered when one of the indicators crosses the network threshold to indicate the presence of a jammer node. Bengag et al. (2023) improved their work by using a fuzzy logic system to identify jamming attacks in different network cases [23]. Savva et al. (2022) also proposed to detect jamming attacks through the use of fuzzy logic [24].

Data Link Layer

The link layer in WSNs, consisting of the MAC layer, is used to control errors and detect and access data frames. The MAC layer is vulnerable to several attack types, including back-off manipulation, denial of sleep and exhaustion attacks. A back-off manipulation attack is used to shorten the back-off time to get the channel priority.

Ghugar & Pradhan (2020) proposed a MAC layer trust-based intrusion detection system, ML-IDS, based on the concept of a weighting method to detect back-off manipulation attacks [25].

A node subjected to a denial of service (DoS) attack, leading to a denial of sleep attack (DoSL) has its ability to sleep restricted. This raises the power needed for node data transmission and reception. It is also called an exhaustion attack. If no data has to be sent, the MAC protocols retain the node in sleep mode. The attacker attempts to keep the node awake by sending messages constantly, which results in an unnecessary transmission and increases energy consumption until all the node's energy is depleted.

Mohd et al. (2020) proposed an IDS using support vector machine learning in WSN to detect denial of sleep attacks [12]. It uses feature ranking and pruning based on performance analysing parameters. Yaghoubi et al. (2022) on the other hand, proposed a Trust Value Based Intrusion Detection System (TIDS) that uses a genetic algorithm framework in WBAN to identify and prevent denial of sleep [26]. Hussain et al. (2019) proposed an IDS using a soft decision mechanism to identify, prevent and avoid exhaustion attacks [27].

Network Layer

In WSNs, the network layer manages the routes and data transmission using routing protocols to determine the best path from the source node to the destination node. At the network layer, the attacker attacks by gaining control of the data and interfering with its route. Attacks on the network layer can be severe because they compromise the entire network operation, particularly the routing part. Examples of attacks on this layer are Sybil, blackhole, and wormhole attacks.

Sybil attacks target fault-tolerance techniques, and as a result, they manifest in networks that utilize multiple paths for routing. In a Sybil attack, a malicious node assumes the identities of several other nodes to disguise its true identity. Sybil refers to these false identities that appear to be multiple nodes. These Sybil may develop their own identities or take on the identities of authorized nodes. Mehbodniya et al. (2021) proposed the use of machine learning approaches such as Naïve Bayes, Random Forest, and Logistic Regression to detect fake identity and Sybil attacks using the node's packet delivery rates [13]. Mounica et al. (2021) proposed a machine-learning model to evaluate the efficacy and precision of machine-learning techniques for identifying authorized and unauthorized access points in networks where raw internet traffic data has been gathered to detect Sybil attacks [14]. Arshad et al. (2022) proposed a Trust-based Hybrid cooperative RPL protocol (THC-RPL) that observes the directly connected neighbour node's behaviour and calculates the trust value in detecting Sybil nodes [28].

Distance vector routing protocols are vulnerable to blackhole attacks where a malicious node claims a short routing distance from the source and the destination nodes. As a result, the attacker node is used to deceive the source node into passing data to the target node through it. The attacker node gets packets from the source node, but it drops them instead of delivering them to the destination node. Soni & Sudhakar (2020) proposed the Link Hop Value-based Intrusion Detection System (L-IDS) against the blackhole attack by establishing a wireless link between the nodes, exchanging data packets,

and identifying the link hop value as the presence of the attacker by incorporating the data delivery in each hop [29]. On the other hand, Kumar et al. (2023) suggested anomaly-based hierarchical intrusion detection that uses a trust model and data routing with data type verification as the time of route to detect and prevent blackhole attacks [30].

Wormhole attacks are particularly common in WSNs, occurring on a low-latency bandwidth. The wormhole attack occurs within two independent network nodes containing distinctive portions of a message. The attacker uses a laptop or other wireless device to tunnel the packet to another area of the WSN over a low-latency link, where they are replayed. Deshmukh-Bhosale & Sonavane (2019) proposed an IDS for wormholes using RSSI to identify the attack and attacker node [31]. Bhosale & Sonavane (2021) further proposed an innovative intrusion detection system that detects wormhole attacks by analysing the location information of any node and its neighbours, as well as the Received Signal Strength Indicator (RSSI) values and the hop count [32].

Transport Layer

WSNs' simplified or omitted transport layer protocols make this layer less vulnerable to attacks than the network layer. The transportation layer enables logical connections between two different sensor nodes. Examples of transport layer attacks are flood attacks, desynchronization attacks, and session hijacking attacks. The purpose of flooding is to drain a sensor node's memory by delivering a large number of connection setup requests. Desynchronization can be used to request retransmissions by transmitting packets with a different sequence number. Session hijacking occurs when an unsecured or inadequately protected session is hijacked at the start. When the right sequence number is discovered, the attacker spoofs the target node's IP address and launches a DoS attack. The attacker's goal is to get private information such as identities, passwords, and secret keys.

Application Layer

Protocols on the application layer are more vulnerable to DoS attacks. This layer holds user applications and data and is compatible with HTTP, Telnet, SMTP, and FTP protocols. The attacker is particularly interested in application layer information as it directly contains data about the user. At the application layer, a Man-in-the-Middle attack (MITM) is a type of eavesdropping which is also called a sniffing or snooping attack. It occurs when an outsider eavesdrops on the conversations of two or more exchange parties. Maniriho et al. (2020) presented an anomaly-based IDS approach that uses a hybrid feature selection engine. It chooses the most important information and uses the Random Forest algorithm to classify traffic as normal or abnormal [33]. The IDS can detect DoS and MITM attacks.

Table 1. Attacks in WSN based on the layers.

Layer	Attacks
Physical	Jamming, DoS, tampering, Sybil attack, interception, eavesdropping, active interference

Data link	Back-off manipulation, replay attack, interception, DoS, exhaustion attack, Sybil attack, collision, unfairness, traffic analysis and monitoring, spoofing and altering routing attack, selfish misbehaviour, malicious misbehaviour, Denial of sleep attack
Network	Selective forwarding attack, sinkhole attack, wormhole attack, black hole attack, Sybil attack, DoS, hello flood attack, Homing, spoofing attack, neglect and greed, grey-hole attack, misdirection attack, Internet smurf attack, rushing attack, replay attack, Byzantine attack
Transport	SYN flooding attack, desynchronization, session hijacking
Application	Eavesdropping, false data injection, spoofing and altering routing attack, malicious code attack, repudiation attack, DoS attack

Other attacks on all the layers are listed in Table 1 [1, 2, 3, 4, 5]. These cyber-attacks have a variety of objectives, including stealing, altering, hacking, and flooding the targeted nodes with excessive packets to deplete the sensors' battery power and disconnect them from the network, making them unusable and hindering them from sensing or routing traffic. The performance, effectiveness, and reliability of communication may suffer as a result of these attacks. To overcome these problems, effective security mechanisms, such as well-defined detection and mitigation procedures, must be put in place. As a result, intrusion detection methods to protect against such attacks are becoming increasingly important. An intrusion detection system (IDS) is a promising solution to identify intrusions in WSNs. However, the IDSs in WSNs face new challenges due to the characteristics of WSNs, thus, there is a need for an IDS to work interoperability across the layers.

3.2 Cross-layer Intrusion Detection Systems

Due to the numerous characteristics of sensor networks, such as their limited battery power supply, poor bandwidth support, self-organizing nature, and dependence on other nodes, there is a significant risk of security attacks in all OSI model layers. A single or a series of attacks may be made. Several specific attacks occur at regular intervals, such as blackhole attacks, rushing attacks, and flooding attacks. It has been noticed that circumstances may result in several attacks rather than a single attack. As a result, it is preferable to develop an effective Intrusion Detection System (IDS) capable of handling many attacks. Several proposed intrusion detection schemes are proposed based on a cross-layer approach, including the physical, data link and network layers that contribute towards the design of a cross-layer intrusion detection system. Cross-layer IDS secures WSNs by detecting various malicious activities and attackers at different layers.

Amouri et al. (2018) proposed an IDS that has a two-stage detection process that happens locally and globally [34]. The IDS system is for data collecting that works in situations that prohibit direct access to data on specific nodes. It uses dedicated sniffers to capture packets and generate correctly classified instances. The system establishes a detection threshold based on these instances. By analysing the variation of correctly classified instances from different sniffers using a sliding window approach, the IDS

detects malicious nodes in the network. Alharthi & Abdullah (2019) developed XLID, a cross-layer intrusion detection system between the network and MAC layers [35]. XLID detects intruders trying to communicate with network nodes by analysing packet data and signal strength. It combines information from the MAC, network, and physical layers to identify potential attacks. XLID offers a unified system for detecting various intrusions at both layers, using cross-layer concepts.

Canbalaban & Sen (2020) proposed a novel intrusion detection system for RPL using neural networks [36]. It combines features from the link and network layers to detect specific attacks on RPL, such as version number, worst parent, and hello flood attacks. By analysing packet drops at the link layer, the system distinguishes between natural losses and those caused by attacks. The system aims to process large amounts of data generated by RPL and accurately predict the type of attack, not just its presence. Ghugar et al. (2019) proposed LB-IDS, a layered-based intrusion detection system for Wireless Sensor Networks (WSNs) [21]. LB-IDS aims to detect various types of attacks, including jamming, back-off manipulation, sinkhole, and cross-layer attacks, occurring at different network protocol stack layers. The system calculates the trust value of a sensor node by analysing the trust metrics' deviation at the physical, MAC, and network layers, considering trustworthiness in each layer individually. By utilizing this layered approach, LB-IDS provides a comprehensive means of identifying and mitigating attacks at multiple levels within the WSN.

Gandhimathi & Murugaboopathi (2020) proposed a hybrid IDS for WSN that consists of two stages [19]. The first stage utilizes cross-layer features, considering both the network and MAC layers. The network layer analyses packet routing, while the MAC layer considers medium access duration. If a compromised node is detected based on high MAC duration and packet drop rates, it is declared as an attacker. The second stage correlates the MAC and network layers to analyse IP flow records to detect network traffic attacks accurately.

Table 2. Existing IDS in WSN based on the layers.

Authors	Intrusion Detection Approaches	Layers				
		P	D	N	T	A
Amouri et al. (2018)[34]	Traces packets	√	√	√		
Ghugar et al. (2019)[21]	Trust value	√	√	√		
Alharthi & Abdullah (2019)[35]	Combines information from layers		√	√		
Gandhimathi & Murugaboopathi (2020)[19]	Packet routing, medium access duration		√	√		
Canbalaban & Sen (2020)[36]	Neural networks		√	√		
Bengag et al. (2019)[22]	Packet delivery ratio, energy consumption, RSSI, bad packet ratios	√				
Bengag et al. (2023)[23]	Fuzzy logic system	√				
Hussain et al. (2019)[27]	Soft decision mechanism		√			
Ghugar & Pradhan (2020)[25]	Weighting method		√			

Mohd et al. (2020)[12]	Support vector machine learning	√		
Yaghoubi et al. (2022)[26]	Trust value	√		
Deshmukh-Bhosale & Sonavane (2019)[31]	RSSI		√	
Soni & Sudhakar (2020)[29]	Hop count		√	
Mehbodniya et al. (2021)[13]	Machine learning approaches		√	
Mounica et al. (2021)[14]	Machine learning approach		√	
Bhosale & Sonavane (2021)[32]	Location information, RSSI, hop count		√	
Arshad et al. (2022)[28]	Trust value		√	
Kumar et al. (2023)[30]	Trust model and verification		√	
Maniriho et al. (2020)[33]	Random Forest algorithm			√

**P is physical, D is data link, N is network, T is transport and A is application*

Each of these proposed IDS in Table 2 showed to detect various types of attacks in WSN. Further improvements are required to enable these IDS to adapt to any changes in WSN, such as the limitations on the nodes and the attacks.

4 Challenges and Future Directions

The IDS schemes presently in use usually consider a few of the attacks. Attacks on other layers of the WSN are disregarded mainly by most currently employed techniques, which exclusively focus on one or more types of attacks on one layer of the WSN. In order to identify numerous attacks on distinct WSN layers, a cross-layer IDS needs to be devised. Future expansion of the types of attacks across the layers that an IDS must take into consideration when doing detection is intriguing. Additionally, multi-channel cross-layer protocols like MCRP were created to lengthen the lifespan of WSNs, but security was not a consideration. In order to safeguard the multi-channel cross-layer routing mechanism and make it resistant to both insider and external attackers, it might be expanded to add security features such as with an IDS.

WSNs use energy to gather information about their surroundings, process it, and send the resulting data. The IDSs must therefore use the least amount of energy feasible to leave enough for the WSN's vital operations. IDSs are crucial for the security of WSNs, and those created for them need to have specific features like low power usage. The success of an IDS in a WSN depends on the way it affects the network's energy usage as a WSN is resource constrained. Maintaining a network over its lifespan is one of the biggest issues in WSNs, so energy efficiency in IDSs is equally important. WSN sensor nodes have limited storage capacity. Therefore, it is challenging to meet the need to store attack signatures in sensor nodes.

In order to create an IDS in the WSN to identify various sorts of attacks, machine learning techniques were mostly utilised. The drawback of those techniques is that they require more memory to deploy a model to a sensor node and take longer for machine

learning algorithms to build and evaluate data sets for WSN. It could be conceivable to develop a hybrid or cloud-based machine learning prototype for carrying out intrusion detection in the WSN to reduce the amount of memory required in the detection techniques. Another point to consider is many of the IDS schemes available do not provide self-defence. It is crucial because certain attackers may frequently generate false alarms by flooding the IDS host with irrelevant traffic. The host can run out of resources as a result, leaving the system open to intrusions. IDS's ability to protect itself is thus desirable.

5 Conclusions

WSNs face numerous cyberattacks that pose risks to the network's availability, privacy, control, and reliability. These attacks exploit the vulnerable nature of nodes deployed in hazardous and remote environments, where they often remain unattended, unable to protect the information flow physically. As a result, there is an increased likelihood of node compromise, leading to decreased network security and protection. It is crucial to implement robust security measures to safeguard these networks against breaches and assaults. One effective approach is the adoption of a cross-layer intrusion detection system, which provides comprehensive protection across multiple WSN layers. This paper reviews the existing IDS at each of the layers and cross-layers for WSN in terms of the attacks and approaches. Cross-layer IDS can detect early signs of advanced attacks exploiting multiple layers' vulnerabilities. They reduce evasion techniques by analysing data from multiple layers, making it harder for attackers to evade detection. However, it's important to consider WSN's limited resources and constraints when designing and implementing cross-layer IDS. Thus, a more energy-efficient cross-layer IDS for WSN needs to be developed and improved from the existing IDS.

References

1. Khan, K., Mehmood, A., Khan, S., Khan, M. A., Iqbal, Z., & Mashwani, W. K.: A survey on intrusion detection and prevention in wireless ad-hoc networks. Journal of Systems Architecture, 105, 101701 (2020).
2. Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J., & Park, Y.: Intrusion detection protocols in wireless sensor networks integrated to Internet of Things deployment: Survey and future challenges. IEEE Access, 8, 3343-3363 (2019).
3. Elsaid, S. A., & Albatati, N. S.: An optimized collaborative intrusion detection system for wireless sensor networks. Soft Computing, 24(16), 12553-12567 (2020).
4. Faris, M., Mahmud, M. N., Salleh, M. F. M., & Alnoor, A.: Wireless sensor network security: A recent review based on state-of-the-art works. International Journal of Engineering Business Management, 15 (2023).
5. Godala, S., & Vaddella, R. P. V.: A study on intrusion detection system in wireless sensor networks. International Journal of Communication Networks and Information Security, 12(1), 127-141 (2020).
6. Kong, H. Y.: Energy efficient cooperative LEACH protocol for wireless sensor networks. Journal of Communications and Networks, 12(4), 358-365 (2010).

7. Winter, T., Thubert, P., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, J. & Alexander, R.: RPL: IPv6 routing protocol for low-power and lossy networks (No. RFC6550) (2012).
8. Iyer, V., Woehrle, M., & Langendoen, K.: Chrysso—A multi-channel approach to mitigate external interference. In 2011 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks pp. 449-457. IEEE (2011).
9. Al Nahas, B., Duquennoy, S., Iyer, V., & Voigt, T.: Low-power listening goes multi-channel. In 2014 IEEE International Conference on Distributed Computing in Sensor Systems pp. 2-9. IEEE (2014).
10. Nordin, N., Clegg, R. G., & Rio, M.: Multi-channel cross-layer routing for sensor networks. In 2016 23rd International Conference on Telecommunications (ICT) pp. 1-6. IEEE (2016).
11. Kurniawan, M. T., & Yazid, S.: Mitigation and detection strategy of dos attack on wireless sensor network using blocking approach and intrusion detection system. In 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE) pp. 1-5. IEEE (2020).
12. Mohd, N., Singh, A., & Bhadauria, H. S.: A novel SVM based IDS for distributed denial of sleep strike in wireless sensor networks. Wireless Personal Communications, 111(3), 1999-2022 (2020).
13. Mehbodniya, A., Webber, J. L., Shabaz, M., Mohafez, H., & Yadav, K.: Machine learning technique to detect Sybil attack on IoT based sensor network. IETE Journal of Research, 1-9 (2021).
14. Mounica, M., Vijayasaraswathi, R., & Vasavi, R.: Detecting Sybil attack in wireless sensor networks using machine learning algorithms. In IOP Conference Series. Materials Science and Engineering 1042(1). IOP Publishing (2021).
15. Althubaity, A., Gong, T., Raymond, K. K., Nixon, M., Ammar, R., & Han, S.: Specification-based distributed detection of rank-related attacks in rpl-based resource-constrained real-time wireless networks. In 2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS) 1, pp. 168-175. IEEE (2020).
16. Gothawal, D. B., & Nagaraj, S. V.: Intrusion detection for enhancing RPL security. Procedia Computer Science, 165, 565-572 (2019).
17. Bhushan, B., & Sahoo, G.: A hybrid secure and energy efficient cluster based intrusion detection system for wireless sensing environment. In 2019 2nd International Conference on Signal Processing and Communication (ICSPC) pp. 325-329. IEEE (2019).
18. Huang, D. W., Luo, F., Bi, J., & Sun, M.: An Efficient Hybrid IDS Deployment Architecture for Multi-Hop Clustered Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security, 17, 2688-2702 (2022).
19. Gandhimathi, L., & Murugaboopathi, G.: A Novel Hybrid Intrusion Detection Using Flow-Based Anomaly Detection and Cross-Layer Features in Wireless Sensor Network. Automatic Control and Computer Sciences, 54, 62-69 (2020).
20. Jilani, S. A., Koner, C., & Nandi, S.: Security in wireless sensor networks: attacks and evasion. In 2020 National conference on emerging trends on sustainable technology and engineering applications (NCETSTEA) pp. 1-5. IEEE (2020).
21. Ghugar, U., Pradhan, J., Bhoi, S. K., & Sahoo, R. R.: LB-IDS: Securing wireless sensor network using protocol layer trust-based intrusion detection system. Journal of Computer Networks and Communications (2019).
22. Bengag, A., Moussaoui, O., & Moussaoui, M.: A new IDS for detecting jamming attacks in WBAN. In 2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS) pp. 1-5. IEEE (2019).

23. Bengag, A., Bengag, A., Moussaoui, O., & Mohamed, B.: A Fuzzy Logic-Based Intrusion Detection System for WBAN Against Jamming Attacks. In Proceedings of the 3rd International Conference on Electronic Engineering and Renewable Energy Systems: ICEERE 2022, 20-22 May 2022, Saidia, Morocco pp. 3-11. Singapore: Springer Nature Singapore (2023).
24. Savva, M., Ioannou, I., & Vassiliou, V.: Fuzzy-Logic Based IDS for Detecting Jamming Attacks in Wireless Mesh IoT Networks. In 2022 20th Mediterranean Communication and Computer Networking Conference (MedComNet) pp. 54-63. IEEE (2022).
25. Ghugar, U., & Pradhan, J.: ML-IDS: MAC layer trust-based intrusion detection system for wireless sensor networks. In Computational Intelligence in Data Mining: Proceedings of the International Conference on ICCIDM 2018 pp. 427-434. Springer Singapore (2020).
26. Yaghoubi, M., Ahmed, K., & Miao, Y.: TIDS: Trust Value-Based IDS Framework for Wireless Body Area Network. In 2022 32nd International Telecommunication Networks and Applications Conference (ITNAC) pp. 142-148. IEEE (2022).
27. Hussain, I., Zahra, S., Hussain, A., Bedru, H. D., Haider, S., & Gumzhacheva, D.: Intruder attacks on wireless sensor networks: A soft decision and prevention mechanism. International Journal of Advanced Computer Science and Applications, 10(5) (2019).
28. Arshad, D., Asim, M., Tariq, N., Baker, T., Tawfik, H., & Al-Jumeily OBE, D. THC-RPL: A lightweight Trust-enabled routing in RPL-based IoT networks against Sybil attack. PloS one, 17(7) (2022).
29. Soni, G., & Sudhakar, R.: A L-IDS against dropping attack to secure and improve RPL performance in WSN aided IoT. In 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN) pp. 377-383. IEEE (2020).
30. Kumar, V. N., Srisuma, V., Mubeen, S., Mahwish, A., Afrin, N., Jagannadham, D. B. V., & Narasimharao, J.: Anomaly-Based Hierarchical Intrusion Detection for Black Hole Attack Detection and Prevention in WSN. In Proceedings of Fourth International Conference on Computer and Communication Technologies pp. 319-327. Springer, Singapore (2023).
31. Deshmukh-Bhosale, S., & Sonavane, S. S.: A real-time intrusion detection system for wormhole attack in the RPL based Internet of Things. Procedia Manufacturing, 32, 840-847 (2019).
32. Bhosale, S. A., & Sonavane, S. S.: Wormhole attack detection system for IoT network: A hybrid approach. Wireless Personal Communications, 124(2), 1081-1108 (2022).
33. Maniriho, P., Niyigaba, E., Bizimana, Z., Twiringiyimana, V., Mahoro, L. J., & Ahmad, T.: Anomaly-based intrusion detection approach for IoT networks using machine learning. In 2020 international conference on computer engineering, network, and intelligent multimedia (CENIM) pp. 303-308. IEEE (2020).
34. Amouri, A., D. Morgera, S., A. Bencherif, M., & Manthena, R.: A cross-layer, anomaly-based IDS for WSN and MANET. Sensors, 18(2), 651 (2018).
35. Alharthi, M., & Abdullah, M.: XLID: Cross-Layer Intrusion Detection System for Wireless Sensor Networks. Indian Journal of Science and Technology, 12, 3 (2019).
36. Canbalaban, E., & Sen, S.: A cross-layer intrusion detection system for RPL-based Internet of Things. In Ad-Hoc, Mobile, and Wireless Networks: 19th International Conference on Ad-Hoc Networks and Wireless, ADHOC-NOW 2020, Bari, Italy, October 19–21, 2020, Proceedings 19 pp. 214-227. Springer International Publishing (2020).