Towards robust security in WSN: a comprehensive analytical review and future research directions

Tamara Zhukabayeva[1,2,3], Lazzat Zholshiyeva[1,6], Khu Ven-Tsen[1,4], Yerik Mardenov[1], Aigul Adamova[1,3], Nurdaulet Karabayev[1,3], Assel Abdildayeva[1,5], Dilaram Baumuratova[1]
[1]International Science Complex "Astana", Astana, Kazakhstan
[2]Department of Information Systems, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
[3]Departtment of Computer Sciences, Astana IT University, Astana, Kazakhstan
[4]Higher School of Information Technologies and Energy, Mukhtar Auezov South Kazakhstan University, Shymkent, Kazakhstan
[5]Department of Artificial Intelligence and Big Data, Al-Farabi Kazakh National University, Almaty, Kazakhstan
[6]Astana IT College, Astana, Kazakhstan

Article Info

Article history:

Received Feb 22, 2024
Revised May 21, 2024
Accepted Jun 5, 2024

Keywords:

Intrusion detection methods
Intrusion detection systems
Wireless sensor networks
WSN
WSN attacks
WSN security

ABSTRACT

One of the most important aspects of the effective functioning of wireless sensor network (WSN) is their security. Despite significant progress in WSN security, there are still several unresolved issues. Many review studies have been published on the problems of possible attacks on WSN and their identification. However, due to the lack of their systematic analysis, it is not possible to fully substantiate practical recommendations for the effective application of the proposed solutions in the field of WSN security. In particular, the creation of methods that provide a high degree of security while minimizing computational effort and costs, and the development of effective methods for detecting and preventing attacks on WSN. The purpose of this document is to fill this gap. The article presents the results of the study in the form of a systematic analysis of the literature with a targeted selection of sources to identify the most effective methods for detecting and preventing attacks on WSN. By identifying the security of WSN, which has not yet been addressed in research works, the review aims to reduce its impact. As a result, our extended taxonomy is presented, including attack types, datasets, effective WSN attack detection methods, countermeasures, and intrusion detection systems (IDS).

Corresponding Author:

Lazzat Zholshiyeva
International Science Complex "Astana"
010000 Astana, Kazakhstan
Email: Lazzat_Zholshiyeva@astanait.edu.kz

1. INTRODUCTION

Wireless sensor networks (WSNs)are used for many purposes, primarily as the communication backbone of the internet of things (IoT). A sensor network also creates access to the physical world. WSN are networks that embed a large number of sensor nodes in the environment. The use of WSN is increasing significantly day by day [1], [2]. The rapid development of WSN and the IoT is responsible for generating huge amounts of data in various forms that require careful authentication and security. At the same time, there continue to be limitations in the form of security issues and limited performance due to insufficient memory resources or computational power. These circumstances are risk factors that reduce the positive effects of WSN and IoT technologies. In this regard, the challenges of effectively addressing these issues are significantly actualized.

Application areas of WSN include medical, industrial, agricultural, military applications, monitoring systems, transportation tracking, home automation, security and surveillance [3]-[5] as shown in Figure 1. Depending on how sensor nodes are deployed, WSN are categorized into five groups: terrestrial, underground, multimedia, underwater and mobile [6]. However, this diversity of usage poses serious limitations to address specific security and reliability challenges in WSN, which may face a multitude of failure and failure-related problems. The consequences of security breaches and attacks on WSN can be particularly severe in government, military, medical or industrial organizations, where important information can be damaged or stolen [7]. One of the main risks is the possibility of unauthorized access to the WSN system [8]. In addition, WSN can be the target of a denial-of-service (DoS) attack [5]. Attackers can overload the network with a large number of requests or create a botnet to attack the system. This can lead to network resource overload, DoS and disruption of facilities. To protect WSN from such threats, WSN security measures should be implemented. This may include encrypting data transmitted, installing authentication and access control mechanisms, and monitoring the network for anomalies. In addition, regular software updates and training of personnel on WSN security measures are also important aspects [9]. Understanding these risks and applying appropriate security measures are integral to the successful operation of WSN. In this regard, it is relevant to solve the problem of identifying attacks on WSN.

Figure 1. WSN applications

Cybersecurity attacks have increased rapidly in various fields such as building management, healthcare, energy, agriculture, automation and industrial processes [10]. Different techniques and protocols are used to achieve authentication, encryption and data integrity [11]. The application of various techniques to detect WSN attacks is gaining popularity [12]-[14]. The security challenges of WSN include:

- Lack of security standards and uniform data protection principles for WSN can lead to incorrect or incomplete implementation of security measures, and make it difficult to assess the security level of the overall system. Different devices may have different levels of security, and their dynamic nature, such as relocation or addition and removal from the network, can create difficulties in establishing and maintaining data protection. WSN are at risk of cyberattacks due to the deployment of sensor nodes without a defined wireless communication structure and the lack of robust network security protocols.
- Limited computing resources, memory and energy efficiency of sensor nodes do not allow for the implementation of high-performance data processing algorithms and sophisticated analytics, complex data protection and encryption mechanisms. Due to inadequate cybersecurity and the failure to apply appropriate data protection measures both directly in the sensor nodes and in the wireless network infrastructure, there is the potential for cyber threats such as data interception, spoofing, or discrediting, as well as attacks on communication protocols or the network infrastructure. Sensor nodes in WSN are limited by their computational capabilities, memory capacity, battery life, communication range, bandwidth and security. These limitations make them vulnerable to various threats and compromises.

- Intrusion detection problem is very important in the case of WSN. Traditional approaches that analyze network anomalies at multiple points of concentration are costly in terms of network memory and power consumption. Therefore, there is a need for decentralized intrusion detection.
- Traditional security protocols are not well suited for WSN due to the limited network resources and the isolated, uncontrolled nature of sensor node placement. Different devices may have different levels of security, and their dynamic nature, such as moving or adding and removing them from the network, can create difficulties in establishing and maintaining data protection. WSN may be vulnerable to attacks on the physical parameters of the environment in which they operate.

The current state of research in approaches, methods, techniques and models, algorithms for attack identification and security assessment of WSN is an actively developing field. This paper analyzes recent research and advances with the identification of WSN security gaps. Solutions to these identified gaps are detailed in section 3, and recommendations of security measures are proposed, and recommendations of security measures are proposed for WSN.

The study aims to develop a systematic literature review on WSN insecurity and to identify the most effective methods for detecting attacks on WSN, and to analyze effective methods and tools for preventing such attacks. The main contribution of this research is:
- Performing a systematized literature review to assess the current state of the problem of WSN safety and security in the last 5 years.
- Categorizing the research, according to the types of algorithms used methods of attack identification, IDS and types of threats.
- Analyzing known methods, models, algorithms for identifying attacks on WSN in order to identify their effectiveness.
- Compilation of a comprehensive taxonomy on classifications of attack types, datasets, controllers, recommendations, effective methods for detecting attacks on WSN and on intrusion detection system (IDS) architectures in the context of WSN.

Figure 2 shows how the article is organized, which consists of four sections. The introduction is described in section 1, which includes the main problems and relevance of the study, the purpose and main contribution of the article. Section 2 is devoted to the research methodology, which includes research questions and strategies for finding related work. Section 3 describes the result, which compiles the empirical analysis and proposes our extended WSN security taxonomy and discussion. Finally, section 4 describes the conclusion.

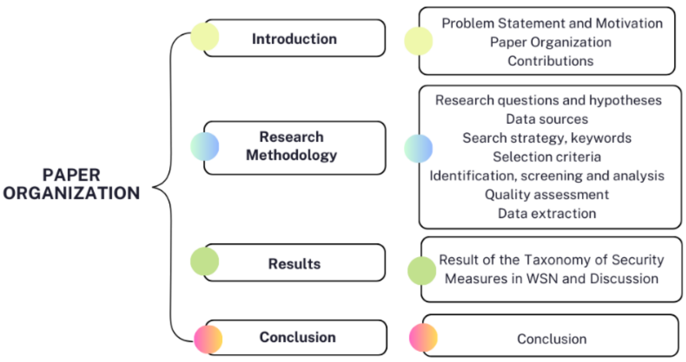


Figure 2. Paper organization

2. RESEARCH METHOD

This section demonstrates the methodology for conducting a systematic review of the article. The focus was on research related to WSN security. This section is composed of the following parts: research questions and hypotheses, search strategy, keywords and paper selection criteria.

2.1. Research questions and hypotheses

These research questions and hypotheses in Table 1 can guide further investigation into the security measures of WSN, contributing to the development of more secure and resilient WSN systems. This paragraph consists of research questions and hypotheses aimed at improving the security of WSNs. Additionally, the study compares various IDS, examines different attack datasets, and reviews vulnerability databases to develop robust security models for WSNs.

Table 1. Research questions and hypotheses

No	Research questions	Hypotheses
1	How effective are machine learning (ML) and deep learning techniques in detecting intrusions in WSN?	ML, deep learning and artificial intelligence techniques significantly improve the accuracy of intrusion detection in WSN compared to traditional methods.
2	What are the comparative advantages and disadvantages of anomaly-based IDS versus signature-based IDS in the context of WSN security?	Anomaly-based IDS are more effective in detecting novel attacks in WSN, whereas signature-based IDS are faster and more efficient in identifying known attacks.
3	How do different attack datasets contribute to the development of more robust security measures in WSN?	Utilizing a combination of different attack datasets for training IDS models leads to a more comprehensive and adaptable security system in WSN.
4	What role do vulnerabilities datasets play in enhancing the security framework of WSN?	Regular updates and integration of vulnerabilities databases into WSN security frameworks significantly reduce the risk of successful cyber-attacks.
5	How can the principles of confidentiality, integrity, and availability be best implemented in WSN to ensure maximum security?	Implementing a multi-layered security approach that addresses confidentiality, integrity, and availability can significantly enhance the overall security of WSN.
6	What are the most significant privacy concerns in WSN, and how can they be addressed effectively?	Addressing privacy concerns such as identification, localization, and profiling through advanced encryption and anonymization techniques can significantly enhance user trust in WSN applications.
7	Which types of attacks on WSN are most prevalent at each layer of the network, and what are the most effective countermeasures?	Layer-specific security measures tailored to the unique vulnerabilities of each network layer are the most effective strategy for mitigating attacks on WSN.

2.2. Search strategy, keywords

A search strategy was developed for this study to search and identify relevant literature sources. The selected keywords searched include “WSN”, “wireless sensor networks”, “WSN security”, “WSN attacks”, “intrusion detection systems”, “intrusion detection methods”. They were linked using the logical operators “AND”, “OR” as shown in Table 2. Relationships in the form of: (TITLE (“WSN”) OR TITLE-ABS-KEY (“Wireless Sensor Networks”) AND TITLE-ABS-KEY (“WSN security”) OR TITLE-ABS-KEY (“Wireless Sensor Networks security”) AND TITLE-ABS- KEY (“attack”) OR TITLE-ABS-KEY (“cyberattacks”) OR TITLE-ABS-KEY (“IDS”) OR TITLE-ABS-KEY (“Intrusion Detection Systems”) OR TITLE-ABS-KEY (“Intrusion Detection Methods”)).

SCOPUS, Google scholar, Crossref, Semantic scholar databases are selected for this research study using the study of the last five years from 2019-2023 as shown in Table 3. Scientific databases from the sources listed above, are summarized in Table 3, and keywords are summarized in Table 2. Specific search strategies were also used. In particular, research articles were analyzed for inclusion and exclusion criteria as shown in Figure 3.

Table 2. List of keywords

Strings	Watchwords
WSN	OR
Wireless sensor networks	AND
WSN security	OR
WSN attacks	OR
Intrusion detection systems	OR
Intrusion detection methods	OR

Table 3. Databases

Publisher	URL
Scopus	https//www.scopus.com
Web of Science	https://www.webofscience.com
Google Scholar	https://scholar.google.com
Crossref	https://www.crossref.org
Semantic Scholar	https://www.semanticscholar.org

The criterion for selecting articles for further review and analysis was defined, i.e., the method of searching and selecting articles using specialized keys and PRISMA meta-analysis [15], [16], as shown in Figure 3. The PRISMA flowchart, describes the process of identifying studies in scientific databases for systematic review. The flowchart is divided into four main steps: identification, screening, selection and inclusion. The algorithm results in the selection of 100 articles according to given requirements for further research.

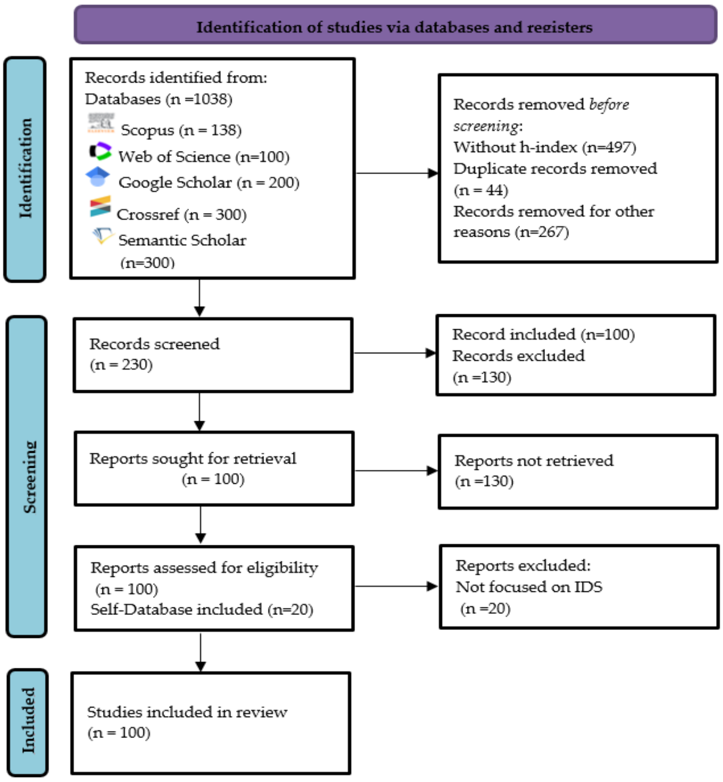
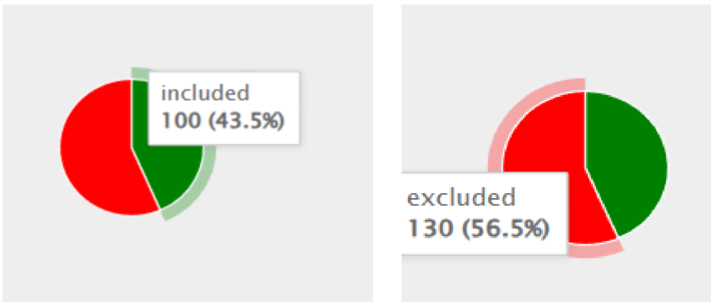


Figure 3. PRISMA flow diagram on selection and screening of the papers

2.3. Paper selection criteria

The selection criterion was based on the PRISMA flow diagram. The search first focused on existing research on WSN attack detection methods and algorithms, WSN security, and WSN attack detection methods. The search covered the period from 2019 to 2023. First, all articles published before 2019 were excluded from the search. Then, all articles written in languages other than English were excluded. The search was mainly focused on matching research on the defense of wireless sensor networks. In order to identify studies through scientific databases using PRISMA scheme, first, 1,038 articles from different database from Table 3 were effectively collected and imported. After importing the collected studies, a screening process follows. In the screening process, firstly, duplicates are removed and then 230 articles are selected for further screening. Articles in the field of computer science, engineering were selected. The duplicate 44 articles were eliminated. Next, articles with high h index were selected. After screening, another 20 articles from own database were added to the study list. Screening result of included and excluded articles is shown in Figure 4. After that, 100 articles were selected and included as shown in Figure 4(a) for further analysis of papers. 130 articles were excluded as shown in Figure 4(b). Table 4 shows the inclusion and exclusion criteria for research articles.



(a) (b)

Figure 4. Screening result of (a) included and (b) excluded articles

Table 4. Criteria for inclusion and exclusion of research articles

Parameters	Inclusion	Exclusion
Source	Published works in different journals or conferences	-
Year of publication	2019-2023	to 2019
Language	English	Other languages
Field of science	Computer science, engineering	Other fields
Citation and Index	More citations	Less citation
	High h index	Without h index
Duplication	-	Duplicates
Own database	+ 20 databases	-

The study involved extensive data collection, which was stored in a spreadsheet with the addition of an in-house database. This data included information on the title of the articles, authors, year of publication, dataset, IDS, algorithm or method used, model performance, types of attacks on WSN, annotations, and data sources. This approach allowed us to organize and organize the information, which further facilitated the work. Several interesting findings emerged from this study. First, it was found that the use of different types of artificial intelligence algorithms can significantly affect the performance of models.

2.4. Quality assessment

Articles, review articles and conference proceedings were used in the quality assessment process of this review. To ensure the quality of the review, all repeated entries were carefully checked. Each study was carefully evaluated. Article abstracts were screened in depth to analyze and clean the articles to ensure the quality and relevance of the research article included in the review process.

The study selection criteria showed high relevance and reliability of information. It is important to note that this assessment is a result of the analysis, thus giving credence to the findings and recommendations. This review is a reliable and relevant source of information on the topic.

Our study emphasized the need for an extended study of this topic. The findings suggest that the complexities inherent in this topic are far-reaching and require more in-depth study. We can hope to show the intricacies of the field, thereby contributing to a more complete understanding that can potentially inform future academic discussions and practical applications. It is important to note that this assessment results from an analysis, which allows you to trust the conclusions and recommendations obtained. This review provides a reliable and up-to-date source of information on the topic.

3. RESULTS

This section presents a comprehensive analytical review and empirical analysis of WSN security, covering classifications by attack type, IDSs, attack identification techniques, algorithms, models, and existing security taxonomies. The proposed extended taxonomy of WSN security measures reflects the evolving landscape of cybersecurity threats and defense mechanisms, offering a forward-looking perspective on WSN security. This section has provided a comprehensive analytical review and empirical analysis of WSN security, covering classifications based on attack types, IDSs, attack identification methods, algorithms, models, and existing security taxonomies. The proposed extended taxonomy of WSN security measures reflects the evolving landscape of cybersecurity threats and defense mechanisms, offering a forward-looking perspective on securing wireless sensor networks.

3.1. Analysis of selected articles by publisher and by year

Figure 5 shows the structured number of articles that were selected for analysis from those published by reputed scientific publishers between 2019 and 2023. Including ‘IEEE Xplore’ with 17.9%, ‘Springer’ with 20.2%, sources include ‘Elsevier’ with 13.1%, ‘Other’ with 10.7% and ‘Academia.edu’ with 6.0%. Smaller segments are represented by sources such as ‘Wiley Online Library’ with 4.8%, ‘Taylor and Francis’ with 2.1%, ‘ACM’ with 2.4%, ‘Science Direct’ and ‘Scholar.archive.org’ with 2.4%, 'ResearchGate' with 7.1%, ‘MDPI’ with 6.0%, and ‘IJETT’ with 1.2%.

Figure 5 provides a visualization of the variety of sources used to access research papers and shows that there is a range of preferred sources on the research topic within the research community. Figure 6 shows the annual distribution of research from 2019 to 2023. It has been observed that the number of studies has not decreased over the years, which means that the areas of attack identification and security assessment of WSN are gaining popularity and attracting more attention from various scholars as the security of WSN is relevant.

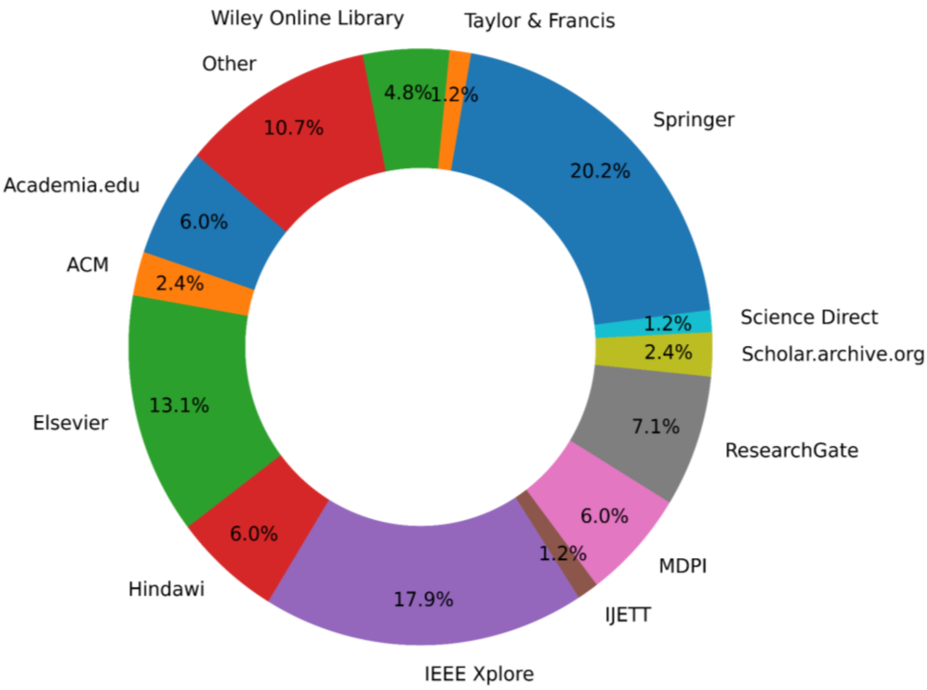


Figure 5. Articles selected for review publisher

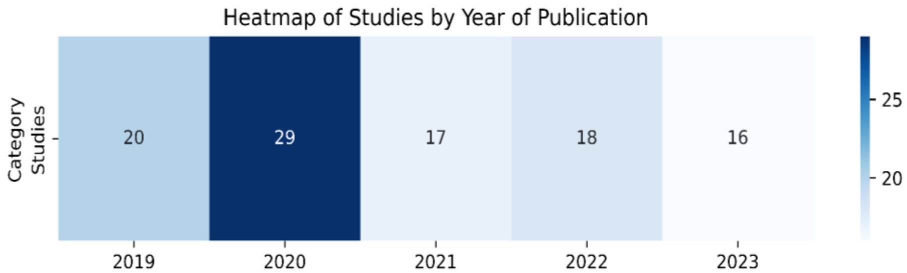


Figure 6. Distribution of studies by year of publication

3.2. Classification of studies on types of WSN attacks

Attacks on WSN can be classified based on their purpose, type and methods used. By purpose, attacks can target data availability, integrity or confidentiality. By type, attacks can be passive or active. Passive attacks involve intercepting and analyzing traffic, while active attacks involve altering or destroying data [17]. According to the methods used, attacks can be based on physical vulnerabilities, software vulnerabilities or protocol vulnerabilities.

When WSN are used in different domains, a variety of attack scenarios are possible. The articles [18] classify attacks into 6 main categories: physical attacks, network attacks, software attacks, encryption attacks, data privacy attacks, encryption attacks. And common attacks on wireless sensor networks include:

- Network availability attacks, such as DoS attacks, which can overload a network and make it unavailable to legitimate users [19].
- Data integrity attacks, such as message spoofing attacks, which can alter or delete data on the network [20].
- Data privacy attacks, such as traffic hijacking attacks, which could lead to the disclosure of sensitive data [21].
- Software attacks, such as buffer overflow attacks, which can lead to the execution of arbitrary code on the network.
- Protocol attacks such as routing attacks that can lead to network disruption or traffic redirection.

The classification of WSN attacks is presented in Figure 7 and the types of attacks and defense techniques are described in Table 5.

Table 5. Comprehensive analysis of classification by attack type

Authors	Year	Threat/attack types
Chen *et al.* [17]	2023	DoS, GPU side channel
Chen *et al.* [18]	2019	LDoS
Godala *et al.* [19]	2020	DoS
Subbiah *et.al.* [20]	2022	DDoS, black hole, wormhole, and gray hole
Faris *et.al.* [1]	2023	Dos, black hole, wormhole, sinkhole, sybil, jamming, node tampering, collision, exhaustion, unfairness, routing, flooding, deluge, selective forwarding, misdirection, byzantine, packet replay, TCP SYN flooding, session hijacking, and deluge
Chauhan and Sharma [21]	2019	DoS
Gupta *et al.* [22]	2023	DoS
Otoum *et al.* [23]	2019	Wormhole
Xie *et al.* [24]	2019	Wormhole
Boubiche *et al.* [25]	2020	Sinkhole
Dener *et al.* [26]	2023	Black hole, flooding, and selective forwarding
Hanif *et al.* [27]	2022	Wormhole
Alqahtani *et al.* [28]	2019	Black hole, flooding, scheduling, and gray hole
Angappan *et al.* [29]	2021	Sybil
Hajiheidari *et al.* [30]	2019	DoS, wormhole, sinkhole, sybil, replay, selective forwarding, jamming, and black hole
Bel and Sabeen [31]	2021	Black hole, wormhole, sinkhole, sybil, hello flooding, selective forwarding, and fragmentation
Liang and Kim [32]	2021	ARP

Figure 7 presents the different types of network attacks, which can be useful for analyzing cybersecurity and prioritizing defense strategies. Attacks involving the software layer are among the most common. This type of attacks can exploit vulnerabilities in WSN software to gain control over the network [32]. To protect WSN from attacks, various security measures such as: i) data encryption: encryption protects the data from unauthorized access; ii) authentication and authorization: authentication and authorization make sure that only authorized users can access the network and its resources; and iii) attack detection and response: attack detection and response systems can help detect and remediate attacks in real time. Following these security measures can help protect the WSN from attacks and ensure safe and secure network operations. Figure 8 illustrates the variety of attacks that can occur in WSN and the different strategies used to control measures WSN from these threats.

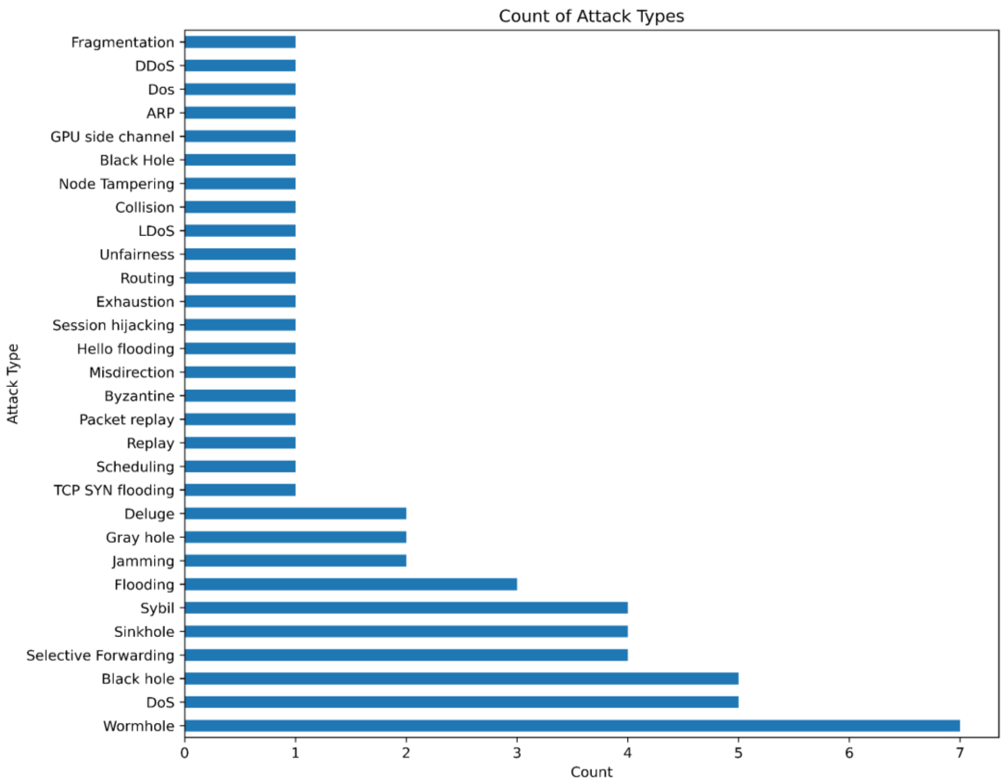


Figure 7. Classification of studies by attack type

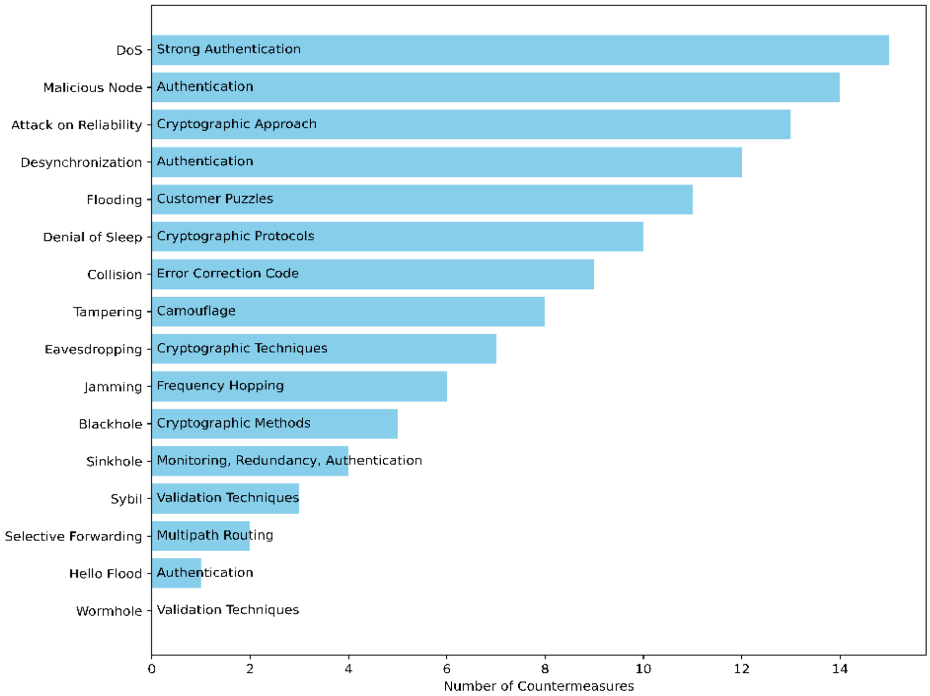


Figure 8. WSN attacks and countermeasures

3.3. Classification of IDS-based studies

The section is dedicated on the classification of research on IDS-based WSN IDS. An IDS sometimes known as an intrusion prevention system (IPS) is an active defense mechanism deployed by the IoT that can recognize intrusion activity and initiate alerts [33]. However, as the number of hazards increases, questions arise about the long-term viability and practicality of current methods. These considerations are particularly relevant in light of the increasing level of adaptive performance and the lack of detection accuracy. Intrusion detection capabilities include: monitoring and analyzing user and system activities; analyzing system configuration and vulnerabilities; assessing system and file integrity; the ability to identify attack patterns; analyzing anomalous activity patterns; and tracking users for policy violations [34].

Research analysis has shown that there are four main methods to build an IDS: signature-based and data-based, behavior analysis-based IDS, and artificial intelligence-based IDS. Each type of IDS has its own advantages and disadvantages [35]. The selection of the most appropriate system depends on the specific requirements of a particular organization. In some cases, it may be necessary to deploy multiple IDS types to ensure comprehensive coverage [36]. Table 6 shows the classification of selected studies on IDS, detection categories and detection methods, attacks and threats [37]. According to the selected studies, most of the researchers used WSN based IDS, distribution-based IDS, anomaly-based IDS, DL based IDS, and ML based IDS and that the proposed IDS improves security, detection accuracy.

Existing IDSs for WSN have several shortcomings. First, they often do not take into account the specific characteristics of WSN, such as limited computational resources and low bandwidth. Second, they are often unable to detect sophisticated attacks that can be disguised as legitimate traffic. Figure 9 shows that the application efficiency is more in WSN-based IDSs, ML-based IDSs, and DL-based IDSs. The literature review of IDS for WSN identified the following problems that need to be addressed:

– Lack of attention to privacy. Most existing IDSs do not consider privacy issues that may arise when using WSN.
– Lack of comprehensive approach. Most existing IDSs focus on detecting attacks on one layer of WSN while ignoring attacks on other layers. This leads to the fact that IDSs cannot provide a complete defense of WSN against all possible attacks.
– Insufficient research on some types of attacks. Some types of attacks, such as attacks on the physical layer of WSN, are not sufficiently studied. This makes it difficult to develop effective methods to defend against such attacks.

It is necessary to develop new IDSs that will take into account the specific characteristics of WSN, provide a comprehensive approach to attack detection and will be able to detect complex attacks.

Table 6. Comprehensive analysis of classification by IDS

Authors	Year	Detection category	Detection method/algorithm
Salmi and Oughdir [34]	2023	Efficient and lightweight IDSs	DNN, CNN, RNN и CNN + RNN
Albelwi [35]	2022	Anomaly-based IDS	Multi-task learning (MTL) model for
Smys *et al.* [36]	2020	Anomaly-based IDS	Network attack
Almiani *et al.* [37]	2020	Fog computing-based IDS	DoS, Probe, R2L, U2R
Larriva-Novo *et al.* [38]	2021	Anomaly-based IDS	Network traffic categorization
Lyu *et al.* [39]	2019	Anomaly-based IDS	Distributed DNS attacks
Shafiq *et al.* [40]	2020	IoT anomaly and intrusion traffic identification system	Bot-IoT attacks
Korzhuk *et al.* [41]	2019	IDS	DL
Kilincer *et al.* [42]	2023	SPA-IDS: an intelligent IDS	KNN, SVM, DT, and BT classifiers
Yang *et al.* [43]	2023	Anomaly-based IDS	ML models
Selvakumar *et al.* [44]	2022	Intelligent IDS	
Elsayed *et al.* [45]	2022	IoT and SDN systems	DL
Safaldin *et al.* [46]	2020	GWOSVM-IDS	GWOSVM-ID
Almomani and Alromi [47]	2020	IDS: scheduling, broadcast и watchdog	
Umarani and Kannan [48]	2020	Artificial immune system	Hybrid tissue growing algorithm
Sinha and Paul [49]	2022	Anomaly-based IDS	NN
Gite *et al.* [50]	2023	ML-based intrusion detection scheme	C4.5 and CART classifiers
Otoum *et al.* [51]	2019	DL-based IDS	Restricted boltzmann machine-based clustered IDS (RBC-IDS)
Sinha and Tripathi [52]	2023	ML and DL based IDS	ML/DL
Rajasoundaran *et al.* [53]	2022	DPFES, DCNN, DL-MCDS	DL
Zhang *et al.* [54]	2020	WSN IDS	
Karthikeyan *et al.* [55]	2023	QoS based hybrid swarm intelligent IDS	Artificial bee colony (ABC) with the genetic algorithm (GA)
Asharf *et al.* [56]	2020	Machine and deep learning-based IDS	ML/DL
Zhao *et al.* [57]	2019	An effective exponential-based trust and reputation evaluation system	ETRES
Yang and Wang [58]	2019	ICNN	Stochastic gradient descent algorithm LeNet-5 and DBN, LeNet-5, and RNN
Davahli *et al.* [59]	2020	IoTIDS	GA–GWO
Subramani and Selvi [60]	2023	Classification algorithms-based IDS	Proposed fuzzy CNN
Abhale and Reddy [61]	2023	Network IDS (NIDS)	DL
Raveendranadh and Tamilselvan [62]	2023	WSN based IDS	EPK-DNN
Li *et al.* [63]	2023	WSN based IDS	ESVM
Gupta and Gupta [64]	2023	MWSN	SDFA
Hemanand *et al.* [65]	2022	CSGO	CSGO и LSVM
Godala and Vaddella [19]	2020	Suitable IDS	CSGO-LSVM model

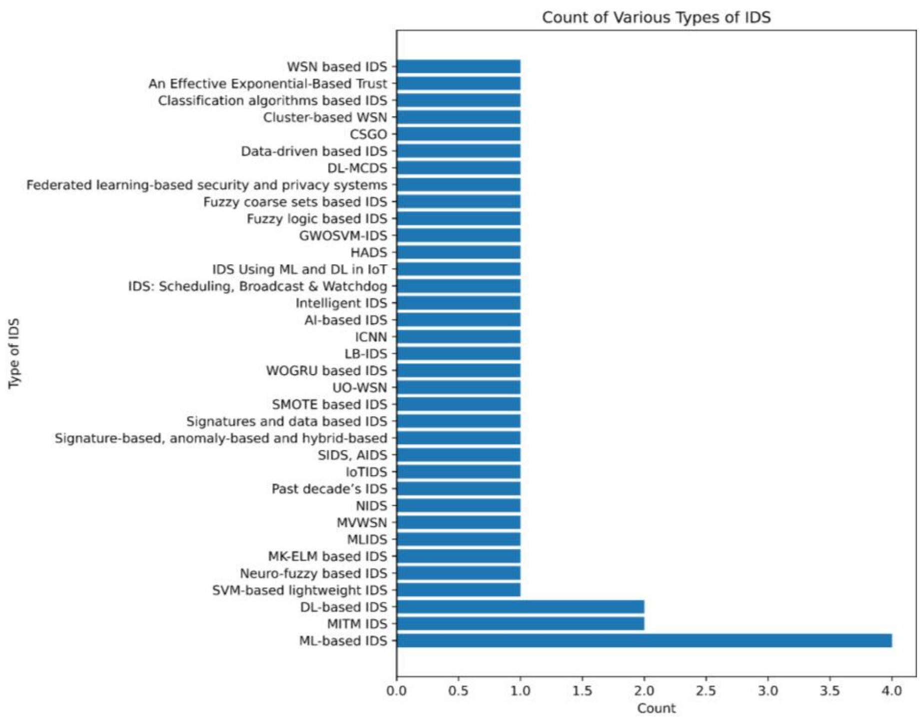


Figure 9. Distribution of studies by IDS

3.4. Classification of studies based on attack identification methods, algorithms and models

This section describes studies based on attack identification methods and algorithms. Some studies [66]-[75] use data-driven approach because signature-based methods cannot detect zero-day attack. To identify WSN attacks, several data-driven approaches based on ML or DL methods have been proposed in the articles. The fundamental limitations of these approaches include the use of raw features to build an intrusion detection model, which may result in low detection accuracy. There are studies that implement entity embedding for the sake of transforming raw features, to provide accurate detection. Table 7 in Appendix shows the studies classified based on attack identification methods and algorithms.

Figure 10 shows the categorization of studies on attack detection methods, algorithms, and technologies that have investigated the implementation of various AI algorithms. These algorithms include XGBoost, extreme learning machine (ELM) algorithm, Naive Bayes (NB), decision tree (DT), random forest (RF), support vector machine (SVM), probability support vector machine (LSVM), long short term memory (LSTM), recurrent neural network (RNN), convolutional neural network (CNN) deep neural network (DNN), K-nearest neighbors (K-NN) algorithm, fuzzy pattern tree (FPT), fuzzy logic algorithm, C-means, logistic regression (LR), deep learning (DL), and artificial neural network (ANN), CNN+RNN. The results of the analysis show that most of the studies utilized DL algorithms and various ML algorithms, while other studies focused on current issues related to WSN and IoT security.

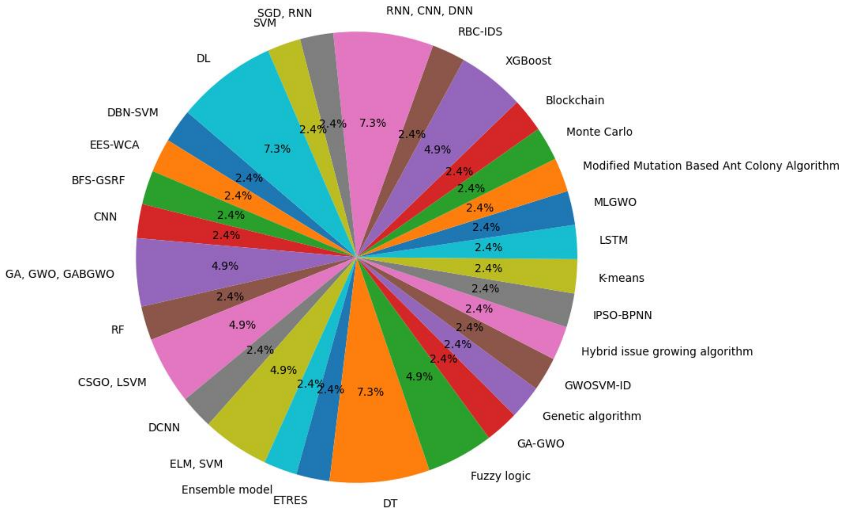


Figure 10. Classification of research by methods, algorithms and technologies for detecting attacks

3.5. Taxonomy classification of studies

This section presents the taxonomy of security attacks, different IDS mechanisms to detect the attacks and performance metrics used to evaluate the IDS algorithm for WSN. The taxonomy of security threats for each layer and different algorithmic solutions that have been studied by numerous researchers aim to counter this attack and will allow more accurate reflection of network threats in new datasets. According to the presented taxonomies of modern IDSs, a comprehensive review of recent works, it can be concluded that WSN are becoming more secure. Table 8 and Figure 10 summarize the studies classified by taxonomy.

Table 8. Comprehensive analysis of classification by taxonomy

Authors	Year	Taxonomy
Farooq *et al.* [110]	2020	A taxonomy of advanced IDSs, a comprehensive litany of popular recent cases, and a litany of datasets typically used for evaluation
Sasi *et al.* [111]	2023	IoT attack taxonomy
Hassija *et al.* [112]	2019	A taxonomy of security threats at different layers of an IoT application
Kavitha *et al.* [113]	2023	Taxonomy of security threats for each layer and ML algorithmic solutions
Krishna *et al.* [114]	2021	The comprehensive taxonomy of security and threats within the IoT paradigm
Amanullah *et al.* [115]	2020	Taxonomy of IoT attacks
Liang and Kim [32]	2021	Taxonomy of IoT attacks
Atzori *et al.* [33]	2021	Taxonomy of IoT attacks
Shah and Sengupta [116]	2020	Taxonomy of cyber-attacks on IoT and IoT devices
Makhdoom *et al.* [117]	2018	Taxonomy of threats to the IoT
Adamova *et al.* [2]	2023	Taxonomy of different types of failures in WSN

From Table 8, we can summarize that improving anomaly detection techniques is of great importance in combating cyberattacks. It can identify typical attacks and detect potential threats at early stages, which helps to better protect information systems and reduce risks and for better performance evaluation [115], [116]. ML and DL are becoming more and more widely used in the field of WSN and IoT security. This is due to its ability to analyze large amounts of data and detect anomalies in the performance of systems. ML algorithms learn from the data provided to them and can predict possible vulnerabilities and attacks. Thus, they can be an effective tool in combating cyber threats related to WSN and IoT [117], [118]. All these aspects are widely discussed in academia and practitioners to develop more reliable and secure WSN and IoT systems. However, it is necessary to continuously develop technical tools and strategies to maximize the effectiveness and protection against possible cyber threats in WSN and IoT.

3.6. Result of the taxonomy of security measures in WSN and discussion

Thus, our extended taxonomy of security measures in WSN is proposed based on the results of the study. This taxonomy can be characterized as containing elements of a systematic approach to analyzing and addressing WSN security issues. Our extended taxonomy is presented in Figure 11, which includes attack types, datasets, effective methods for detecting attacks on WSN, countermeasures, and IDS. In addition, the presented taxonomy exhausts the gaps in building an IDS in WSN, and the shortcomings of the approaches proposed by researchers are identified. The detailed taxonomy of security measures in WSN aligns well with the initial hypotheses, providing a comprehensive framework that supports the effectiveness of ML, DL, and AI, the importance of IDS types, the role of attack and vulnerabilities databases, the implementation of security principles, the need to address privacy concerns, and the efficacy of layer-specific security measures. This comparison highlights the depth and relevance of the taxonomy in guiding research and development efforts in securing WSN.

Figure 12 illustrates future WSN security research directions and their relative importance based on a hypothetical assessment. These areas include advanced encryption techniques, AI and ML for threat detection, energy-efficient security protocols, blockchain applications, and more. Each area is critical to improving the security and efficiency of WSN. Future WSN security research directions can make a meaningful contribution to the development of more secure, efficient, and resilient WSN that can meet the cybersecurity challenges of the future.

Security in WSN and IoT is a challenging task not only due to the limited resources of end devices along with link losses but also due to new communication and networking technologies. Analyzing recent research studies on different types of attacks shows varying levels of attention and study. Some attacks attract significant research interest while others are relatively ignored. Researchers need to focus on understanding and mitigating all forms of attacks to improve network performance and security in the future.

Currently, many strategies only consider specific types of attacks on individual layers of WSN, ignoring attacks on other layers. However, there is a need to develop a cross-layer IDS capable of detecting multiple attacks at different layers of WSN. In conclusion, securing WSN is a multifaceted task that requires an integrated approach. The proposed recommendations and our taxonomy together form a sound framework for enhancing WSN security. By applying these measures in real-world applications, WSN can significantly reduce the risks associated with cyber threats, unauthorized access, and data leakage in the WSN environment.

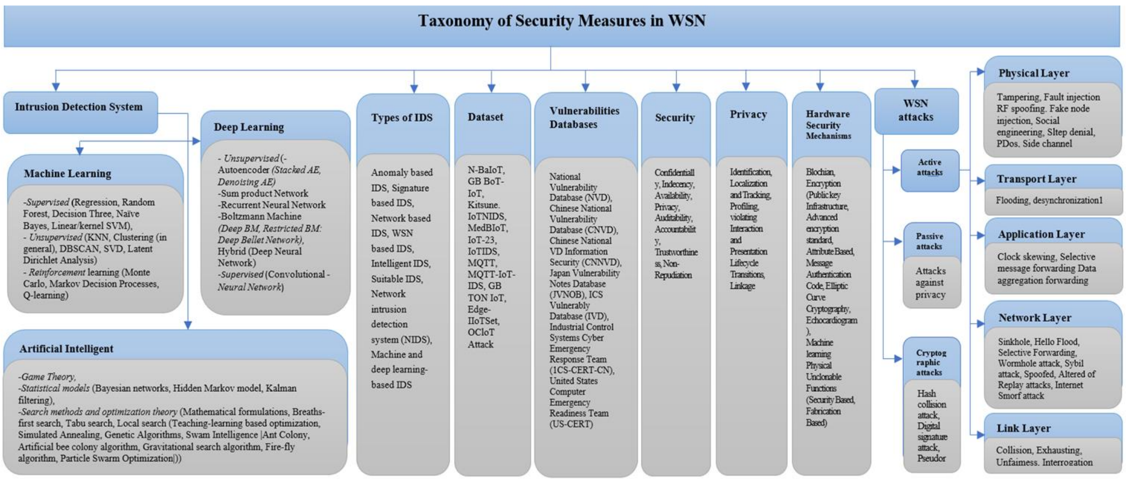


Figure 11. Taxonomy of WSN security

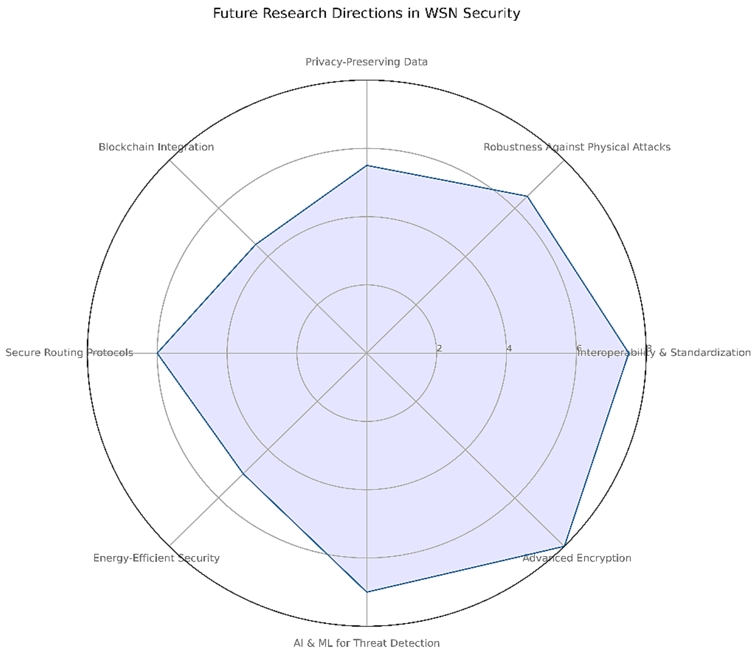


Figure 12. Future research directions

4. CONCLUSION

In this paper, we performed an analytical review of WSN security article selected using specialized procedures to highlight the most informative and relevant scientific publications. As a result, we found a lack of comprehensive reviews on WSN. Existing reviews either provide minimal information on attacks or focus on network security and its impact on energy dissipation. To address this gap, we propose a new taxonomy to categorize WSN security measures.

Based on the results of this study, we performed a systematic literature review to assess the current state of the WSN security and protection problem in the last 5 years. We categorized the research, according to the types of algorithms and methods used to identify attacks, and types of threats and the results of the classification revealed that the improvement of anomaly detection methods is of great importance in the fight against cyberattacks. We analyzed the IDS identification of attacks on WSN to identify their effectiveness. Furthermore, Research on ML, DL, and AI techniques for effective detection of different types of attacks, which are key actions in combating cyberattacks and securing WSN and IoT, is categorized. Lastly, a taxonomy of WSN security measures is proposed, based on analytical and empirical analysis.

To successfully deploy and operate fault-tolerant and fault-tolerant WSN, several challenges related to their reliability, energy efficiency, management and security need to be addressed. Implementing modern authentication and authorization mechanisms, using data encryption, monitoring and detecting incidents, and regular security testing, creating standards and using new technologies such as blockchain, creating a security culture can significantly improve the security of WSN and ensure their safe and secure operation. Further research and development in this area is essential to ensure the resilience and security of WSN. Further work is also needed to improve the accuracy of attack detection with real applications and on real datasets to detect new types of threats.

APPENDIX

Table 7. Comprehensive analysis of classification by type of methods and algorithms of identification attacks

Authors	Year	Dataset	Threat/attack types	Detection method/algorithm/model
Alzahrani and Alzahrani [66]	2020	CICDDoS2019	DDoS	K-nearest neighbors, and decision tree
Nedeljković and Jakovljević [67]	2021	SWaT	Cyber-attack	CNN
Kumari and Mrunalini [68]	2022	CAIDA 2007	DoS attack	ML
Su *et al.* [69]	2020	NSL-KDD		BLSTM (bidirectional long short-term memory)

Table 7. Comprehensive analysis of classification by type of methods and algorithms of identification attacks *(Continued)*

Authors	Year	Dataset	Threat/attack types	Detection method/algorithm/model
Dasari and Devarakonda [70]	2022	CICDDoS2019	DDoS	Logistic regression, decision tree, random forest, Adaboost KNN и Naive Bayes
Alsahli *et al.* [71]	2021	KDD99	IPS	Random forest, Naïve Bayes, IBK
Kovač *et al.* [72]	2022		phishing attacks and spam	Regression and classification algorithms
Singh *et al.* [73]	2020	WSN-DS	Malicious attacks	Fuzzified method
Avcı and Koca [74]	2023	CIC IoT dataset 2022	DDoS	KNN, ANN, and SVM
Almiani *et al.* [37]	2020	NSL-KDD	Cyber-attack	RNN
Zhang *et al.* [75]	2023	DBN	SF attack	DBN
Alotaibi [76]	2019		Malicious attacks	Hamming residue method (HRM)
Nancy *et al.* [77]	2020	KDD cup data set and network trace data set	Known type of attacks	Dynamic recursive feature selection algorithm
Jahromi *et al.* [78]	2021	ICS datasets	Known type of attacks	DNN
Doiba *et al.* [79]	2023	NSL-KDD, IoT-23, BoT-IoT, and Edge-IIoT	IDS	Gradient boosting, decision tree
Mounica *et al.* [80]	2021	Datasets of DDOs, R2L, Probe, Sybil, and Norma	Sybil attack	SVM
Lakshmi *et al.* [81]	2019		RREQ flooding DOS attacks	NS2-based WSN model
Asad *et al.* [82]	2023	CIC IDS 2017	DDOS attack	DNN
Pan *et al.* [83]	2021	NSL-KDD and UNSW-NB15 data sets	Cyber-attack	kNN, PM-CSCA algorithms
Devi *et al.* [84]	2023	CIC-IDS2017	DDoS attack	RF
Chinnaraju and Nithyanandam [85]	2022		GHA	Neighbor based
Wazirali and Ahmad [86]	2022	WSN-dataset in different sizes	DOS attack, DDOS attack	LSTM, MLP, KNN, LR, SVM, DT, and Naïve Bayes
Elsaid and N. S. lbatati [87]	2020			ML algorithm BS
Al-Tashi *et al.* [88]	2020	15 standard benchmark datasets from the UCI repository		BMOGWO-S
Jiang *et al.* [89]	2020	WSN-DS	Blackhole, grayhole, flooding, and scheduling TDMA attack	SLGBM
Otoum *et al.* [90]	2021		DoS, user-to-root (U2R) attack, probe attack, and remote-to-local (R2L) attack	Restricted boltzmann machine-based clustered IDS (RBC-IDS)
Rajasoundaran *et al.* [53]	2022		Sinkhole	DL
Karthikeyan *et al.* [55]	2023			ABC with the GA
Asharf *et al.* [56]	2020			ML/DL
Ferrag *et al.* [91]	2019	Bot-IoT, MQTTset, TON_IoT	Cyber-attacks	RNN, CNN и DNN.
Yang and Wang [58]	2019	KDDTest		Stochastic gradient descent algorithm LeNet-5 and DBN, LeNet-5, and RNN
Davahli *et al.* [92]	2020			GA–GWO
Lutfi and Ahmed [93]	2020			HNF--ACA
Kumar *et al.* [94]	2021		Malicious nodes	IDCNN
Zhang *et al.* [54]	2020		FDI attacks	DL
Raveendranadh and Tamilselvan [62]	2023	BC, MC dataset		EPK-DNN, DL
Amaran and Mohan [95]	2023	NSL KDDCup 99		OSVM
Shelar *et al.* [96]	2023			EBB84
Li *et al.* [63]	2023			SDFA
Saif *et al.* [97]	2022		Blackhole, grayhole, flooding attacks	RF, kNN, SVM, J48, and NB
Hemanand *et al.* [65]	2022	CSGO		CSGO и LSVM
Godala and Vaddella [19]	2020			CSGO-LSVM model
Embarak and Abu Zitar [98]	2023		DoS attack	ML

Table 7. Comprehensive analysis of classification by type of methods and algorithms of identification attacks *(Continued)*

Authors	Year	Dataset	Threat/attack types	Detection method/algorithm/model
Dener *et al.* [26]	2023	WSN-BFSF	Blackhole, flooding, and selective forwarding attacks	ML: RF, DT, NB, LR, and DL
Sadineni *et al.* [99]	2022			Fuzzy-related feature selection technique
Kushwaha and Pandey [100]	2023			SACC-AHP
Jing *et al.* [101]	2019	Open-source datasets	DDoS flooding attacks	Modified multi-chart cumulative sum
Cai *et al.* [102]	2020		types of network attacks in CPSs	ADA, AGV
Khraisat *et al.* [103]	2019	DARPA, KDD98 datasets		ML
Shakya [104]	2021	NSL KDD’99		MLGWO
Selvakumar *et al.* [105]	2019			FRNN
Tekerek [106]	2021		Web attack	CNN
Farooq *et al.* [107]	2020	IDS		Four common evasion techniques IDSs
Tahsien *et al.* [108]	2020			ML
Kumari and Jain [109]	2023		DDoS attack	DDoS defense methodologies

ACKNOWLEDGEMENTS

Author thanks to the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan (Grant No. AP19680345).

REFERENCES

[1] M. Faris, M. N. Mahmud, M. F. M. Salleh, and A. Alnoor, “Wireless sensor network security: a recent review based on state-of-the-art works,” *International Journal of Engineering Business Management*, vol. 15, p. 184797902311572, Jan. 2023, doi: 10.1177/18479790231157220.

[2] A. Adamova, T. Zhukabayeva, and Y. Mardenov, “Machine learning in action: an analysis of its application for fault detection in wireless sensor networks,” in *2023 IEEE International Conference on Smart Information Systems and Technologies (SIST)*, May 2023, pp. 506–511, doi: 10.1109/SIST58284.2023.10223548.

[3] P. Zeng, B. Pan, K.-K. R. Choo, and H. Liu, “MMDA: multidimensional and multidirectional data aggregation for edge computing-enhanced IoT,” *Journal of Systems Architecture*, vol. 106, p. 101713, Jun. 2020, doi: 10.1016/j.sysarc.2020.101713.

[4] A. A. Diro and N. Chilamkurti, “Distributed attack detection scheme using deep learning approach for internet of things,” *Future Generation Computer Systems*, vol. 82, pp. 761–768, May 2018, doi: 10.1016/j.future.2017.08.043.

[5] F. Farivar, M. S. Haghighi, A. Jolfaei, and M. Alazab, “Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial IoT,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2716–2725, Apr. 2020, doi: 10.1109/TII.2019.2956474.

[6] L. F. Carvalho, T. Abrão, L. de S. Mendes, and M. L. Proença, “An ecosystem for anomaly detection and mitigation in software-defined networking,” *Expert Systems with Applications*, vol. 104, pp. 121–133, Aug. 2018, doi: 10.1016/j.eswa.2018.03.027.

[7] S. Ali, T. Al Balushi, Z. Nadir, and O. K. Hussain, “Improving the resilience of wireless sensor networks against security threats: a survey and open research issues,” *International Journal of Technology*, vol. 9, no. 4, p. 828, Jul. 2018, doi: 10.14716/ijtech.v9i4.1526.

[8] A. K. Nuristani and J. Thakur, “Security issues and comparative analysis of security protocols in wireless sensor networks a review,” *International Journal of Computer Sciences and Engineering*, vol. 6, no. 10, pp. 436–444, Oct. 2018, doi: 10.26438/ijcse/v6i10.436444.

[9] I. Nadir *et al.*, “An auditing framework for vulnerability analysis of IoT system,” in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, Jun. 2019, pp. 39–47, doi: 10.1109/EuroSPW.2019.00011.

[10] S. Singh, Q. Z. Sheng, E. Benkhelifa, and J. Lloret, “Guest editorial: energy management, protocols, and security for the next-generation networks and internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3515–3520, 2020, doi: 10.1109/TII.2020.2964591.

[11] I. F. Parreño and D. F. Avila, “Analysis of the cybersecurity in wireless sensor networks (WSN): A Review Literature,” *Smart Innovation, Systems and Technologies*, vol. 255, pp. 83–102, 2022, doi: 10.1007/978-981-16-4884-7_8.

[12] M. Abdullahi *et al.*, “Detecting cybersecurity attacks in internet of things using artificial intelligence methods: a systematic literature review,” *Electronics*, vol. 11, no. 2, p. 198, Jan. 2022, doi: 10.3390/electronics11020198.

[13] R. Ahmad, R. Wazirali, and T. Abu-Ain, “Machine learning for wireless sensor networks security: an overview of challenges and issues,” *Sensors*, vol. 22, no. 13, 2022, doi: 10.3390/s22134730.

[14] J. Luo, Z. Zhang, C. Liu, and H. Luo, “Reliable and cooperative target tracking based on WSN and WiFi in indoor wireless networks,” *IEEE Access*, vol. 6, pp. 24846–24855, 2018, doi: 10.1109/ACCESS.2018.2830762.

[15] D. Moher, A. Liberati, J. Tetzlaff, and D. G. Altman, “Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement,” *Annals of Internal Medicine*, vol. 151, no. 4, pp. 264–269, Aug. 2009, doi: 10.7326/0003-4819-151-4-200908180-00135.

[16] M. D. J. Peters, C. M. Godfrey, H. Khalil, P. McInerney, D. Parker, and C. B. Soares, “Guidance for conducting systematic scoping reviews,” *International Journal of Evidence-Based Healthcare*, vol. 13, no. 3, pp. 141–146, 2015, doi: 10.1097/XEB.0000000000000050.

[17] H. Chen, Y. Zhang, Y. Cao, and J. Xie, "Security issues and defensive approaches in deep learning frameworks," *Tsinghua Science and Technology*, vol. 26, no. 6, pp. 894–905, Dec. 2021, doi: 10.26599/TST.2020.9010050.
[18] H. Chen, C. Meng, Z. Shan, Z. Fu, and B. K. Bhargava, "A novel low-rate denial of service attack detection approach in zigbee wireless sensor network by combining hilbert-huang transformation and trust evaluation," *IEEE Access*, vol. 7, pp. 32853–32866, 2019, doi: 10.1109/ACCESS.2019.2903816.
[19] S. Godala and R. P. V. Vaddella, "A study on intrusion detection system in wireless sensor networks," *International Journal of Communication Networks and Information Security*, vol. 12, no. 1, pp. 127–141, 2020, doi: 10.17762/ijcnis.v12i1.4429.
[20] S. Subbiah, K. S. M. Anbananthen, S. Thangaraj, S. Kannan, and D. Chelliah, "Intrusion detection technique in wireless sensor network using grid search random forest with boruta feature selection algorithm," *Journal of Communications and Networks*, vol. 24, no. 2, pp. 264–273, 2022, doi: 10.23919/JCN.2022.000002.
[21] A. Chauhan and K. Sharma, "A review of IoT security solutions using machine learning and deep learning," in *Lecture Notes in Networks and Systems*, vol. 787 LNNS, 2023, pp. 115–132.
[22] N. Gupta, S. K. Jain, V. Sagar, and S. G. Karale, "Enhanced SVM-based novel detection of intrusions for wireless sensor networks (WSNS)," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 8s, pp. 79–85, 2023.
[23] S. Otoum, B. Kantarci, and H. T. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," *IEEE Networking Letters*, vol. 1, no. 2, pp. 68–71, Jun. 2019, doi: 10.1109/LNET.2019.2901792.
[24] H. Xie, Z. Yan, Z. Yao, and M. Atiquzzaman, "Data collection for security measurement in wireless sensor networks: a survey," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2205–2224, Apr. 2019, doi: 10.1109/JIOT.2018.2883403.
[25] D. E. Boubiche, S. Athmani, S. Boubiche, and H. Toral-Cruz, "Cybersecurity issues in wireless sensor networks: current challenges and solutions," *Wireless Personal Communications*, vol. 117, no. 1, pp. 177–213, 2021, doi: 10.1007/s11277-020-07213-5.
[26] M. Dener, C. Okur, S. Al, and A. Orman, "WSN-BFSF: a new data set for attacks detection in wireless sensor networks," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 2109–2125, Jan. 2024, doi: 10.1109/JIOT.2023.3292209.
[27] M. Hanif *et al.*, "AI-based wormhole attack detection techniques in wireless sensor networks," *Electronics*, vol. 11, no. 15, p. 2324, Jul. 2022, doi: 10.3390/electronics11152324.
[28] M. Alqahtani, A. Gumaei, H. Mathkour, and M. M. Ben Ismail, "A genetic-based extreme gradient boosting model for detecting intrusions in wireless sensor networks," *Sensors*, vol. 19, no. 20, p. 4383, Oct. 2019, doi: 10.3390/s19204383.
[29] A. Angappan, T. P. Saravanabava, P. Sakthivel, and K. S. Vishvaksenan, "Novel Sybil attack detection using RSSI and neighbour information to ensure secure communication in WSN," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 6567–6578, 2021, doi: 10.1007/s12652-020-02276-5.
[30] S. Hajiheidari, K. Wakil, M. Badri, and N. J. Navimipour, "Intrusion detection systems in the Internet of things: a comprehensive investigation," *Computer Networks*, vol. 160, pp. 165–191, Sep. 2019, doi: 10.1016/j.comnet.2019.05.014.
[31] H. F. Bel and S. Sabeen, "A survey on IoT security: attacks, challenges and countermeasures," *Webology*, vol. 19, no. 1, pp. 3741–3763, 2022.
[32] X. Liang and Y. Kim, "A survey on security attacks and solutions in the IoT network," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan. 2021, pp. 0853–0859, doi: 10.1109/CCWC51732.2021.9376174.
[33] L. Atzori, A. Iera, and G. Morabito, "The internet of things: a survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010, doi: 10.1016/j.comnet.2010.05.010.
[34] S. Salmi and L. Oughdir, "Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network," *Journal of Big Data*, vol. 10, no. 1, p. 17, Feb. 2023, doi: 10.1186/s40537-023-00692-w.
[35] S. A. Albelwi, "An intrusion detection system for identifying simultaneous attacks using multi-task learning and deep learning," in *2022 2nd International Conference on Computing and Information Technology (ICCIT)*, Jan. 2022, pp. 349–353, doi: 10.1109/ICCIT52419.2022.9711630.
[36] Dr. S. Smys, Dr. Abul Basar, and Dr. H. Wang, "Hybrid intrusion detection system for internet of things (IoT)," *Journal of ISMAC*, vol. 2, no. 4, pp. 190–199, Sep. 2020, doi: 10.36548/jismac.2020.4.002.
[37] M. Almiani, A. AbuGhazleh, A. Al-Rahayfeh, S. Atiewi, and A. Razaque, "Deep recurrent neural network for IoT intrusion detection system," *Simulation Modelling Practice and Theory*, vol. 101, p. 102031, May 2020, doi: 10.1016/j.simpat.2019.102031.
[38] X. Larriva-Novo, V. A. Villagrá, M. Vega-Barbas, D. Rivera, and M. Sanz Rodrigo, "An IoT-focused intrusion detection system approach based on preprocessing characterization for cybersecurity datasets," *Sensors*, vol. 21, no. 2, p. 656, Jan. 2021, doi: 10.3390/s21020656.
[39] M. Lyu, H. H. Gharakheili, C. Russell, and V. Sivaraman, "Hierarchical anomaly-based detection of distributed DNS attacks on enterprise networks," *IEEE Transactions on Network and Service Management*, vol. 18, no. 1, pp. 1031–1048, Mar. 2021, doi: 10.1109/TNSM.2021.3050091.
[40] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Future Generation Computer Systems*, vol. 107, pp. 433–442, Jun. 2020, doi: 10.1016/j.future.2020.02.017.
[41] V. Korzhuk, A. Groznykh, A. Menshikov, and M. Strecker, "Identification of attacks against wireless sensor networks based on behaviour analysis," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 10, no. 2, pp. 1–21, 2019, doi: 10.22667/JOWUA.2019.06.30.001.
[42] I. F. Kilincer, T. Tuncer, F. Ertam, and A. Sengur, "SPA-IDS: an intelligent intrusion detection system based on vertical mode decomposition and iterative feature selection in computer networks," *Microprocessors and Microsystems*, vol. 96, p. 104752, Feb. 2023, doi: 10.1016/j.micpro.2022.104752.
[43] Y. Yang, S. Tu, R. H. Ali, H. Alasmary, M. Waqas, and M. N. Amjad, "Intrusion detection based on bidirectional long short-term memory with attention mechanism," *Computers, Materials & Continua*, vol. 74, no. 1, pp. 801–815, 2023, doi: 10.32604/cmc.2023.031907.
[44] K. Selvakumar *et al.*, "Intelligent temporal classification and fuzzy rough set-based feature selection algorithm for intrusion detection system in WSNs," *Information Sciences*, vol. 497, pp. 77–90, Feb. 2019, doi: 10.1016/j.ins.2019.05.040.
[45] R. A. Elsayed, R. A. Hamada, M. I. Abdalla, and S. A. Elsaid, "Securing IoT and SDN systems using deep-learning based automatic intrusion detection," *Ain Shams Engineering Journal*, vol. 14, no. 10, p. 102211, Oct. 2023, doi: 10.1016/j.asej.2023.102211.
[46] M. Safaldin, M. Otair, and L. Abualigah, "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 2, pp. 1559–1576, Feb. 2021, doi: 10.1007/s12652-020-02228-z.
[47] I. Almomani and A. Alromi, "Integrating software engineering processes in the development of efficient intrusion detection systems in wireless sensor networks," *Sensors*, vol. 20, no. 5, p. 1375, Mar. 2020, doi: 10.3390/s20051375.

[48] C. Umarani and S. Kannan, "Intrusion detection system using hybrid tissue growing algorithm for wireless sensor network," *Peer-to-Peer Networking and Applications*, vol. 13, no. 3, pp. 752–761, May 2020, doi: 10.1007/s12083-019-00781-9.

[49] S. Sinha and A. Paul, "Neuro-fuzzy based intrusion detection system for wireless sensor network," *Wireless Personal Communications*, vol. 114, no. 1, pp. 835–851, Sep. 2020, doi: 10.1007/s11277-020-07395-y.

[50] P. Gite, K. Chouhan, K. M. Krishna, C. K. Nayak, M. Soni, and A. Shrivastava, "ML based intrusion detection scheme for various types of attacks in a WSN using C4.5 and CART classifiers," *Materials Today: Proceedings*, vol. 80, pp. 3769–3776, 2023, doi: 10.1016/j.matpr.2021.07.378.

[51] S. Subbiah, K. S. M. Anbananthen, S. Thangaraj, S. Kannan, and D. Chelliah, "Intrusion detection technique in wireless sensor network using grid search random forest with boruta feature selection algorithm," *Journal of Communications and Networks*, vol. 24, no. 2, pp. 264–273, 2022, doi: 10.23919/JCN.2022.000002.

[52] H. Sinha and R. Tripathi, "Internet of vehicles: a study and comparison of machine learning and deep learning-based intrusion detection approaches," in *AIP Conference Proceedings*, 2023, vol. 2705, p. 030002, doi: 10.1063/5.0133284.

[53] S. Rajasoundaran *et al.*, "Secure routing with multi-watchdog construction using deep particle convolutional model for IoT based 5G wireless sensor networks," *Computer Communications*, vol. 187, pp. 71–82, Apr. 2022, doi: 10.1016/j.comcom.2022.02.004.

[54] W. Zhang, D. Han, K.-C. Li, and F. I. Massetto, "Wireless sensor network intrusion detection system based on MK-ELM," *Soft Computing*, vol. 24, no. 16, pp. 12361–12374, Aug. 2020, doi: 10.1007/s00500-020-04678-1.

[55] N. Karthikeyan, J. Bhargav, M. S. Kavitha, and S. Karthik, "QoS based hybrid swarm intelligent intrusion detection system for network security," in *2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Jul. 2023, pp. 1–8, doi: 10.1109/ICCCNT56998.2023.10307865.

[56] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, and A. Wahab, "A review of intrusion detection systems using machine and deep learning in internet of things: challenges, solutions and future directions," *Electronics*, vol. 9, no. 7, p. 1177, Jul. 2020, doi: 10.3390/electronics9071177.

[57] J. Zhao, J. Huang, and N. Xiong, "An effective exponential-based trust and reputation evaluation system in wireless sensor networks," *IEEE Access*, vol. 7, pp. 33859–33869, 2019, doi: 10.1109/ACCESS.2019.2904544.

[58] H. Yang and F. Wang, "Wireless network intrusion detection based on improved convolutional neural network," *IEEE Access*, vol. 7, pp. 64366–64374, 2019, doi: 10.1109/ACCESS.2019.2917299.

[59] A. Davahli, M. Shamsi, and G. Abaei, "Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 11, pp. 5581–5609, Nov. 2020, doi: 10.1007/s12652-020-01919-x.

[60] S. Subramani and M. Selvi, "Intelligent IDS in wireless sensor networks using deep fuzzy convolutional neural network," *Neural Computing and Applications*, vol. 35, no. 20, pp. 15201–15220, Jul. 2023, doi: 10.1007/s00521-023-08511-2.

[61] A. B. Abhale and A. Jayaram Reddy, "Deep learning perspectives to detecting intrusions in wireless sensor networks," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 2s, pp. 18–26, 2023.

[62] B. Raveendranadh and S. Tamilselvan, "An accurate attack detection framework based on exponential polynomial kernel-centered deep neural networks in the wireless sensor network," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 3, 2023, doi: 10.1002/ett.4726.

[63] W. Li, C. Liu, D. Gu, J. Gao, and W. Sun, "Statistical differential fault analysis of the saturnin lightweight cryptosystem in the mobile wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1487–1496, 2023, doi: 10.1109/TIFS.2023.3244083.

[64] I. Gupta and K. Gupta, "Evaluation of intrusion detection schemes in wireless sensor network," *International Organization Of Scientific Research Journal of Computer Engineering (IOSR-JCE)*, vol. 18, no. 2, pp. 60–63, 2016.

[65] D. Hemanand, G. V. Reddy, S. S. Babu, K. R. Balmuri, T. Chitra, and S. Gopalakrishnan, "An intelligent intrusion detection and classification system using CSGO-LSVM model for wireless sensor networks (WSNs)," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 10, no. 3, pp. 285–293, 2022.

[66] R. J. Alzahrani and A. Alzahrani, "Security analysis of DDoS attacks using machine learning algorithms in networks traffic," *Electronics*, vol. 10, no. 23, p. 2919, Nov. 2021, doi: 10.3390/electronics10232919.

[67] D. Nedeljković and Ž. Jakovljević, "Implementation of CNN based algorithm for cyber-attacks detection on a real-world control system," in *Proceedings of the 14th International Scientific Conference MMA 2021-Flexible Technologies, Novi Sad, september 2021*, 2021, pp. 119–122.

[68] K. Kumari and M. Mrunalini, "Detecting denial of service attacks using machine learning algorithms," *Journal of Big Data*, vol. 9, no. 1, p. 56, Dec. 2022, doi: 10.1186/s40537-022-00616-0.

[69] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "BAT: deep learning methods on network intrusion detection using NSL-KDD dataset," *IEEE Access*, vol. 8, pp. 29575–29585, 2020, doi: 10.1109/ACCESS.2020.2972627.

[70] K. B. Dasari and N. Devarakonda, "Detection of DDoS attacks using machine learning classification algorithms," *International Journal of Computer Network and Information Security*, vol. 14, no. 6, pp. 89–97, Dec. 2022, doi: 10.5815/ijcnis.2022.06.07.

[71] M. S. Alsahli, M. M. Almasri, M. Al-Akhras, A. I. Al-Issa, and M. Alawairdhi, "Evaluation of machine learning algorithms for intrusion detection system in WSN," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 5, 2021, doi: 10.14569/IJACSA.2021.0120574.

[72] A. Kovac, I. Dunder, and S. Seljan, "An overview of machine learning algorithms for detecting phishing attacks on electronic messaging services," in *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, May 2022, pp. 954–961, doi: 10.23919/MIPRO55190.2022.9803517.

[73] N. Singh, D. Virmani, and X.-Z. Gao, "A fuzzy logic-based method to avert intrusions in wireless sensor networks using WSN-DS dataset," *International Journal of Computational Intelligence and Applications*, vol. 19, no. 03, Sep. 2020, doi: 10.1142/S1469026820500182.

[74] İ. Avcı and M. Koca, "Predicting DDoS attacks using machine learning algorithms in building management systems," *Electronics*, vol. 12, no. 19, p. 4142, Oct. 2023, doi: 10.3390/electronics12194142.

[75] S. Zhang, H. Wang, X. Zhang, and Y. Wu, "Detecting selective forwarding attacks in WSN based on deep belief network," in *International Conference on Cloud Computing, Performance Computing, and Deep Learning (CCPCDL 2023)*, May 2023, p. 49, doi: 10.1117/12.2679074.

[76] M. Alotaibi, "Security to wireless sensor networks against malicious attacks using Hamming residue method," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, p. 8, Dec. 2019, doi: 10.1186/s13638-018-1337-5.

[77] P. Nancy, S. Muthurajkumar, S. Ganapathy, S. V. N. S. Kumar, M. Selvi, and K. Arputharaj, "Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks," *IET Communications*, vol. 14, no. 5, pp. 888–895, Mar. 2020, doi: 10.1049/iet-com.2019.0172.

[78] A. N. Jahromi, H. Karimipour, and A. Dehghantanha, "Deep federated learning-based cyber-attack detection in industrial control systems," in *2021 18th International Conference on Privacy, Security and Trust (PST)*, Dec. 2021, pp. 1–6, doi: 10.1109/PST52912.2021.9647838.
[79] M. Douiba, S. Benkirane, A. Guezzaz, and M. Azrour, "An improved anomaly detection model for IoT security using decision tree and gradient boosting," *The Journal of Supercomputing*, vol. 79, no. 3, pp. 3392–3411, Feb. 2023, doi: 10.1007/s11227-022-04783-y.
[80] M. Mounica, R. Vijayasaraswathi, and R. Vasavi, "RETRACTED: detecting sybil attack in wireless sensor networks using machine learning algorithms," *IOP Conference Series: Materials Science and Engineering*, vol. 1042, no. 1, p. 012029, Jan. 2021, doi: 10.1088/1757-899X/1042/1/012029.
[81] H. N. Lakshmi, S. Anand, and S. Sinha, "Flooding attack in wireless sensor network-analysis and prevention," *International Journal of Engineering and Advanced Technology*, vol. 8, no. 5, pp. 1792–1796, 2019.
[82] M. Asad, M. Asim, T. Javed, M. O. Beg, H. Mujtaba, and S. Abbas, "DeepDetect: detection of distributed denial of service attacks using deep learning," *The Computer Journal*, vol. 63, no. 7, pp. 983–994, Jul. 2020, doi: 10.1093/comjnl/bxz064.
[83] J.-S. Pan, F. Fan, S.-C. Chu, H.-Q. Zhao, and G.-Y. Liu, "A lightweight intelligent intrusion detection model for wireless sensor networks," *Security and Communication Networks*, vol. 2021, pp. 1–15, Apr. 2021, doi: 10.1155/2021/5540895.
[84] M. Devi, P. Nandal, and H. Sehrawat, "DDOS attack in WSN using machine learning," in *Lecture Notes in Networks and Systems*, vol. 703 LNNS, 2023, pp. 859–872.
[85] G. Chinnaraju and S. Nithyanandam, "Grey hole attack detection and prevention methods in wireless sensor networks," *Computer Systems Science and Engineering*, vol. 42, no. 1, pp. 373–386, 2022, doi: 10.32604/csse.2022.020993.
[86] R. Wazirali and R. Ahmad, "Machine learning approaches to detect dos and their effect on wsns lifetime," *Computers, Materials & Continua*, vol. 70, no. 3, pp. 4922–4946, 2022, doi: 10.32604/cmc.2022.020044.
[87] S. A. Elsaid and N. S. Albatati, "An optimized collaborative intrusion detection system for wireless sensor networks," *Soft Computing*, vol. 24, no. 16, pp. 12553–12567, Aug. 2020, doi: 10.1007/s00500-020-04695-0.
[88] Q. Al-Tashi *et al.*, "Binary multi-objective grey wolf optimizer for feature selection in classification," *IEEE Access*, vol. 8, pp. 106247–106263, 2020, doi: 10.1109/ACCESS.2020.3000040.
[89] S. Jiang, J. Zhao, and X. Xu, "SLGBM: an intrusion detection mechanism for wireless sensor networks in smart environments," *IEEE Access*, vol. 8, pp. 169548–169558, 2020, doi: 10.1109/ACCESS.2020.3024219.
[90] Y. Otoum, D. Liu, and A. Nayak, "DL-IDS: a deep learning–based intrusion detection framework for securing IoT," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, 2022, doi: 10.1002/ett.3803.
[91] M. A. Ferrag, O. Friha, L. Maglaras, H. Janicke, and L. Shu, "Federated deep learning for cyber security in the internet of things: concepts, applications, and experimental analysis," *IEEE Access*, vol. 9, pp. 138509–138542, 2021, doi: 10.1109/ACCESS.2021.3118642.
[92] A. Davahli, M. Shamsi, and G. Abaei, "A lightweight anomaly detection model using SVM for WSNs in IoT through a hybrid feature selection algorithm based on GA and GWO," *Journal of Computing and Security*, vol. 7, no. 1, pp. 63–79, 2020, [Online]. Available: https://jcomsec.ui.ac.ir/article_24558.html.
[93] S. S. Lutfi and M. L. Ahmed, "A novel intrusion detection system in WSN using hybrid neuro-fuzzy filter with ant colony algorithm," *Journal of Computational Science and Intelligent Technologies*, vol. 1, no. 1, pp. 1–8, 2020, doi: 10.53409/mnaa.jcsit1101.
[94] M. Kumar, P. Mukherjee, K. Verma, S. Verma, and D. B. Rawat, "Improved deep convolutional neural network based malicious node detection and energy-efficient data transmission in wireless sensor networks," *IEEE Transactions on Network Science and Engineering*, vol. 9, no. 5, pp. 3272–3281, Sep. 2022, doi: 10.1109/TNSE.2021.3098011.
[95] S. Amaran and R. M. Mohan, "Intrusion detection system using optimal support vector machine for wireless sensor networks," in *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)*, Mar. 2021, pp. 1100–1104, doi: 10.1109/ICAIS50930.2021.9395919.
[96] P. A. Shelar, P. N. Mahalle, G. R. Shinde, and N. N. Wasatkar, "Enhanced quantum key distribution algorithm for underwater optical wireless sensor network," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 7s, pp. 392–407, Jul. 2023, doi: 10.17762/ijritcc.v11i7s.7015.
[97] S. Saif, K. Karmakar, S. Biswas, and S. Neogy, "MLIDS: machine learning enabled intrusion detection system for health monitoring framework using BA-WSN," *International Journal of Wireless Information Networks*, vol. 29, no. 4, pp. 491–502, Dec. 2022, doi: 10.1007/s10776-022-00574-7.
[98] O. H. Embarak and R. Abu Zitar, "Securing wireless sensor networks against DoS attacks in Industrial 4.0," *Journal of Intelligent Systems and Internet of Things*, vol. 8, no. 1, pp. 66–74, 2023, doi: 10.54216/JISIoT.080106.
[99] G. Sadineni, M. Archana, and R. C. Tanguturi, "Intrusion detection in wireless sensor networks using fuzzy related feature selection technique with optimized classification," *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 19, pp. 5648–5657, 2022.
[100] V. Kushwaha and D. Pandey, "Security aware congestion management using fuzzy analytical hierarchal process for wireless sensor networks," *National Academy Science Letters*, Jun. 2023, doi: 10.1007/s40009-023-01290-3.
[101] X. Jing, Z. Yan, X. Jiang, and W. Pedrycz, "Network traffic fusion and analysis against DDoS flooding attacks with a novel reversible sketch," *Information Fusion*, vol. 51, pp. 100–113, Nov. 2019, doi: 10.1016/j.inffus.2018.10.013.
[102] X. Cai, K. Shi, K. She, S. Zhong, Y. Soh, and Y. Yu, "Performance degradation estimation mechanisms for networked control systems under DoS attacks and its application to autonomous ground vehicle," *IEEE Transactions on Cybernetics*, vol. 54, no. 5, pp. 2992–3002, May 2024, doi: 10.1109/TCYB.2023.3286878.
[103] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, p. 20, Dec. 2019, doi: 10.1186/s42400-019-0038-7.
[104] S. Shakya, "Modified gray wolf feature selection and machine learning classification for wireless sensor network intrusion detection," *IRO Journal on Sustainable Wireless Systems*, vol. 3, no. 2, pp. 118–127, Jun. 2021, doi: 10.36548/jsws.2021.2.006.
[105] K. Selvakumar *et al.*, "Intelligent temporal classification and fuzzy rough set-based feature selection algorithm for intrusion detection system in WSNs," *Information Sciences*, vol. 497, pp. 77–90, Sep. 2019, doi: 10.1016/j.ins.2019.05.040.
[106] A. Tekerek, "A novel architecture for web-based attack detection using convolutional neural network," *Computers & Security*, vol. 100, p. 102096, Jan. 2021, doi: 10.1016/j.cose.2020.102096.
[107] M. S. Farooq, S. Riaz, A. Abid, T. Umer, and Y. Bin Zikria, "Role of IoT technology in agriculture: a systematic literature review," *Electronics*, vol. 9, no. 2, p. 319, Feb. 2020, doi: 10.3390/electronics9020319.
[108] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of internet of things (IoT): a survey," *Journal of Network and Computer Applications*, vol. 161, p. 102630, Jul. 2020, doi: 10.1016/j.jnca.2020.102630.

[109] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," *Computers & Security*, vol. 127, p. 103096, Apr. 2023, doi: 10.1016/j.cose.2023.103096.

[110] M. S. Farooq *et al.*, "A survey on the role of industrial IoT in manufacturing for implementation of smart industry," *Sensors*, vol. 23, no. 21, p. 8958, Nov. 2023, doi: 10.3390/s23218958.

[111] T. Sasi, A. H. Lashkari, R. Lu, P. Xiong, and S. Iqbal, "A Comprehensive survey on IoT attacks: taxonomy, detection mechanisms and challenges," *Journal of Information and Intelligence*, Dec. 2023, doi: 10.1016/j.jiixd.2023.12.001.

[112] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.

[113] S. Kavitha, N. U. Maheswari, and R. Venkatesh, "Intelligent intrusion detection system using enhanced arithmetic optimization algorithm with deep learning model," *Tehnicki Vjesnik*, vol. 30, no. 4, pp. 1217–1224, Aug. 2023, doi: 10.17559/TV-20221128071759.

[114] R. R. Krishna, A. Priyadarshini, A. V. Jha, B. Appasani, A. Srinivasulu, and N. Bizon, "State-of-the-art review on IoT threats and attacks: taxonomy, challenges and solutions," *Sustainability*, vol. 13, no. 16, p. 9463, Aug. 2021, doi: 10.3390/su13169463.

[115] M. A. Amanullah *et al.*, "Deep learning and big data technologies for IoT security," *Computer Communications*, vol. 151, pp. 495–517, Feb. 2020, doi: 10.1016/j.comcom.2020.01.016.

[116] Y. Shah and S. Sengupta, "A survey on classification of cyber-attacks on IoT and IIoT devices," in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, Oct. 2020, pp. 0406–0413, doi: 10.1109/UEMCON51285.2020.9298138.

[117] I. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu, and W. Ni, "Anatomy of threats to the internet of things," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1636–1675, 2019, doi: 10.1109/COMST.2018.2874978.

[118] Y. Mardenov, A. Adamova, T. Zhukabayeva, and M. Othman, "Enhancing fault detection in wireless sensor networks through support vector machines: a comprehensive study," *Journal of Robotics and Control (JRC)*, vol. 4, no. 6, pp. 868–877, Dec. 2023, doi: 10.18196/jrc.v4i6.20216.

BIOGRAPHIES OF AUTHORS

Tamara Zhukabayeva is currently an Associate Professor in informatics, computer engineering and management with L. N. Gumilyov Eurasian National University, Astana, Kazakhstan. She is also an Associate Member of the Universal Association of Computer and Electronics Engineers and has membership in scientific societies in the society of digital information and wireless communications (SDIWC) and the Universal Association of Computer and Electronics Engineers. She has published over 70 scientific and educational-methodical works: in the Republic of Kazakhstan and countries far and near abroad, including a foreign edition from the clarivate analytics database, Scopus. She is the author and co-author of educational publications and scientific monographs and has innovative patent and copyright certificates for intellectual property rights. She can be contacted at email: tamara_kokenovna@mail.ru.

Lazzat Zholshiyeva in 2003, she graduated from the Taraz State University named after M. Kh. Dulati with a degree in mathematics and computer sciences. In 2012, she received a Master's degree in mechanical engineering. In 2020, she graduated from the doctoral program "Astana International University", specialty 8D06101- "Computing and software". Her research interests include computer vision, machine learning, IoT. Researcher at the international science complex "Astana". She can be contacted at email: lazzat.zhol.81@gmai.com.

Khu Ven-Tsen is Doctor of Technical Sciences, Professor, Higher School of Information Technologies and Energy, M. Auezov South Kazakhstan State University, Shymkent, Kazakhstan. Scientific direction - Automation of technological processes and production, automated optimal control of complex technological systems. He can be contacted at email: qbcba@bk.ru.

Yerik Mardenov graduate of OP 6D070400 Computer technologies and software, Eurasian National University named after L. N. Gumilyov. The topic of the dissertation is “Development and research of algorithms and models for analyzing the security of software and hardware components of wireless sensor networks”. Director of the Information Technology Department at Astana International University. He can be contacted at email: emardenov@gmail.com.

Aigul Adamova received the Ph.D. degree in computing and software from L. N. Gumilyov Eurasian National University, Kazakhstan, in 2016. She is currently the Head of the Career and Employment Center, Astana IT University. She has about 40 published papers in refereed journals and conferences. Her teaching interests include operation systems, algorithms, embedded systems, programming languages, cybersecurity, computer vision, information security, and mobile robotics. She can be contacted at email: aigul.adamova@astanait.edu.kz.

Nurdaulet Karabayev master’s student at Astana IT University, junior researcher at the International Science Complex “Astana”. He has published more than 5 scientific and educational works: in the Republic of Kazakhstan, countries far and near abroad. He can be contacted at email: 222240@astanait.edu.kz.

Assel Abdildayeva received her Ph.D. International University of Information Technologies, Kazakhstan. Currently, she is an associate professor at the Department of Artificial Intelligence and Big Data, KazNU named after. Al-Farabi, Almaty, Kazakhstan. She has published more than 40 scientific and educational works: in the Republic of Kazakhstan, countries far and near abroad. She can be contacted at email: abass_81@mail.ru.

Dilaram Baumuratova Ph.D., senior lecturer at the Pedagogical Institute of Astana International University. She has published more than 20 scientific and educational works: in the Republic of Kazakhstan, countries far and near abroad. She can be contacted at email: Baumuratova.d@gmail.com.