Journal of Electrical and Computer Engineering Innovations
(JECEI)
Journal homepage: http://www.jecei.sru.ac.ir

SRTTU

JECEI

Review Paper

A Survey Study on Intrusion Detection System in Wireless Sensor Network: Challenges and Considerations

M. Hosseini Shirvani [*]***, A. Akbarifar***

Department of Computer Engineering, Sari Branch, Islamic Azad University, Sari, Iran.

Article Info

Article History:
Received 12 February 2024
Reviewed 21 March 2024
Revised 17 May 2024
Accepted 26 May 2024

Keywords:
Intrusion detection system
Security architecture
Anomaly based detection
Misuse based detection
Specification based detection

[*]Corresponding Author's Email Address:
mirsaeid_hosseini@iausari.ac.ir

Abstract

Background and Objectives: Wireless sensor networks (WSNs) are ad-hoc technologies that have various applications in different industries such as in healthcare systems, environment and military surveillance, manufacturing, and IoT context in general. Expanding the scope of sensor network applications has led researchers to develop solutions to provide sustainable communications and networks for distributed environments, as well as how to secure these methods with limited resources.

Methods: The lack of infrastructure space and the vulnerable nature of these networks make it difficult to design security models and algorithms for them. So, to run the sensor network in safe mode, any type of attack must be detected before any security breach is materialized. According to the importance of the network and also the nature of the sensor networks along with the critical challenge of energy consumption, solutions and defensive lines such as intrusion prevention and intrusion detection systems will be selected.

Results: This paper surveys subjectively the intrusion and anomaly detection system in WSNs to determine potentials and challenges for further processing. Therefore, designing an efficient and optimal intrusion detection solution applicable to wireless sensor networks, IoT, and other ad-hoc networks has been a major challenge that will help the researcher to design or choose the best approach for their future research.

Conclusion: This research also paves the way of interested researchers to find existing challenges and shortcomings for further processing.

Introduction

Wireless sensor networks (WSNs) have more characteristic features such as limitations on energy resources, bandwidth, and storage memory [1]. Regarding the limited computation conditions, security approaches in traditional networks have not been useful in WSNs. It has been obvious that the limited features of WSN imply that it does not use IP protocol for network operations. Hereupon, the design of the novel and effective detection approach in WSN has been a big challenge for researchers. Even Though WSN has significant features in terms of operations such as low installation costs and lack of care for network operations, at the physical defensive line, there has been no gateway, router, or switch to monitor the information flows. On the other side, limitations on energy sources pose a great challenge to the security of these networks [2], [3]. Hence, the security architecture of proposed networks has been a big concern, especially for applications where non-functional requirements such as availability, integrity, confidentiality, reliability etc., have prime importance [2]. Numerous researchers have investigated security attacks as well as intrusion detection systems (IDS) in the WSN context [4]-[9]. Therefore, in order to run

Doi: 10.22061/jecei.2024.10148.683

the wireless sensor network in safe mode, any unauthorized access or manipulation of node information, traffic and transit interactions must be actually detected at the correct high rate. Along with the protection of WSN, detection and prevention mechanisms such as cryptography algorithms and IDS should be considered. It has been regarded that the other prevention systems such as intrusion prevention systems (IPS) and honeypots have the requirement to the effective algorithms in order to reduce the power source and other limited features of WSNs. Security in the highly valuable network has been a major requirement for the researchers in the sensors era. For instance, in the healthy control system usage, the patient records should not be accessed by third parties. On the other hand, it has been so important to utilize security mechanisms in military-based features such as battlefield surveillance, minefields and etc. importance of the military usage will appear when the lack of space in the network will casualties' friend armies, the importance of these networks will increase [10]-[12]. Most of the detection mechanisms in traditional networks haven't been able to be directly utilized in the WSN [13], [14]. It has been obvious that traditional approaches have been integrated for wired and IP-based networks and these solutions have not been directly applicable to the sensor networks. Hence, the researchers should consider non-functional requirements such as lack of infrastructure, dynamic topology changes, easiest physical access, extended routing protocols, and limited computation sources [15], [16]. The designing of IDS in WSN has the following requirements that researchers should consider:

- Lack of infrastructure,
- Dynamic Network topology changes,
- Physical facile access,
- Different routing protocols,
- Resources limitation.

To realize the above functional requirements, research on real-time IDS has been constantly increasing. Due to the nature of the problem and the requirement for detection, limited research on detection and meta-discovery algorithms to optimize intrusion detection systems has been presented. Limited and also valuable research has been presented on heuristic and meta-heuristic algorithms to optimize intrusion detection systems. An ant colony optimization (ACO) algorithm based on an Ad-hoc On-Demand Distance Vector (AODV) protocol has been applied for the detection of Blackhole attacks. The authors have applied Grover quantum meta-heuristic algorithms to optimize attack path detection [15]. The authors' proposed approach has been capable of improving some fundamental network parameters such as throughput, end-to-end delay, and packet delivery ratio in comparison with other approaches [15]. Binitha and Sathya have conducted extensive research on the optimization of bio-inspired algorithms [16]. They proposed an overview of evolutionary algorithms, genetic algorithms, genetic programming, evolutionary strategy, and also in the swarm intelligence (SI) category, they have also discussed on particle swarm optimization (PSO) algorithm, Ant colony optimization (ACO), bacteria foraging algorithm (BFA), Glowworm Swarm Optimization (GSO), shuffled frog-leaping algorithm (SFLA), the intelligent water drops algorithm (IWDA), Ford-Fulkerson algorithm (FFA), Feasible Solution Algorithm (FSA). In their surveyed paper, a complete and separate review of the mentioned algorithms in the form of a table with a description of operators, application areas, and control parameters has been investigated. Fu et al. have described the anomaly-based detection framework for hierarchical networks by adapting their framework to the risk theory and negotiation selection algorithm in AIS [17]. They have provided a framework for misbehavior detection utilizing the advantages of artificial intelligence and fuzzy theory to encounter the resource constraints in the typical sensor network.

They have also compared their method with the Watchdog approach. Their method has been able to detect the correct and high rate as well as the incorrect detection rate with the low rate [17]. An approach exploring the adaptability of Bio-inspired methods and their application in the field of computer networks has been published in [7]. According to this research, strategies that mimic the system as much as possible run the risk of inheriting behavioral characteristics as well as environmental constraints. This process will eventually confront the phenomenon of the evolution of nature and the limitations of the physical world [18]. As mentioned earlier concerning to the importance of several applications and industries along with regarding to the limitations of WSN, this survey study reviews published literature and proposes subjective classifications and comparisons of papers.

Then, the challenges & potentials along with research gaps are outlined to guide the future direction for improving existing schemes to bridge available gaps. Therefore, the remainder of this paper is structured as follows. Section 2 stipulates the importance of security in the WSN context. Section 3 introduces intrusion detection systems (IDSs) along with our subjective classification. Section 4 provides applications of machine learning (ML) techniques in IDS schemes. An informative example is brought in section 5 to show the effect of attacks on WSNs. Section 6 pays on intrusion detection systems in new IoT and AI technologies. Section 7 concludes the paper.

The Importance of Maintaining Security in Networks with High Information Sensitivity

Due to the cheap and simple installation capability, wireless sensor networks have been applied to various branches of science and technology. Nowadays, the increasing applications of these networks in important areas such as segmentation of information collection about human behavior and activities can be divided into health control systems, battlefield monitoring, and identification, as well as highway traffic and IoT applications. In the field of physical monitoring and environmental phenomena, it can mention areas of application, such as the ocean, wildlife, earthquake, pollution, forest fires, and water quality. In the field of monitoring industrial sites, applications such as building safety, the performance of production devices have been available. On the other hand, the security in WSN is very sensitive, important, and also very essential functional requirement parameter that the researcher should fully consider it. For example, patient health records should not be disclosed to a third party. On the other hand, securing the WSN has been very important in tactical (such as military) applications. The importance of security in the network has been multiplied when the safe space in the network leads to casualties in the friendly forces on the battlefield.

Hence, counter-attack approaches in wired and wireless networks have been included three main following components:

• Prevention (Maximum defense against attacks): this step has been intended to prevent any attack from taking place before it occurs. Therefore, the proposed technique must defend against the target of the attack.

• Detection (Awareness of the attack Presence): if the adversary devises and exploits a strategy to bypass the techniques applied by the deterrent, the defense mechanism against the attack will fail. At this time, security solutions have been immediately transferred to the attack detection phase and especially the identification phase.

• Mitigation (performing serious action against the attack): in the final step, the mitigation phase has been neutralizing any attacks before the occurrences by clearing infected groups, and then it secures the network.

In network security terminology, the intrusion has an unwanted and unauthorized activity that appears active or passive. It should be considered that in the sensor network, these attacks have been divided into the following categories:

• Active attacks (Sending the malicious packets, delete packets and worm attacks),

• Passive attacks (Eavesdropping and information gathering).

In a secure and sensitive system, if the first line of defense, i.e., intrusion prevention, has not worked properly, the second line of defense, the intrusion detection system, will play a vital role. IDS has been detected for each misbehavior and malisons activates or behavior that has been created by the members. In each security architecture plan, the IDS has been provided all of the following information for other tracking systems:

• Intruder detection,

• Intruder location detection (solitary or regional in WSN),

• Intrusion time

• Intrusion mechanism (active or passive),

• Intrusion type (Worm based attack, flooding, etc.),

• Permeable layer (physical, data link, or network vulnerable layers).

This information has been very effective in the third line of defense and clearly in the mitigation and reaction phase and compensates and corrects the results of the attacks according to the information that has been obtained from the intruder attack. Hence, IDS has very critical for network security architecture. Overall, the researchers and developers should consider IDS as the main requirement for critical systems. It has been obvious that the limited life cycle of the sensor has been playing a vital role in security decisions. These decisions have been more strategic because while achieving functional and non-functional requirements, it has been created an impact on the network platform. Therefore, the requirement to pay attention to the needs of the network has been recommended to researchers before any action in the requirements assessment phase [19]-[26].

Intrusion Detection System (IDS) and Subjective Classification

In a system or a network, each type of unauthorized and unproved activity has been referred to as intrusion. An IDS has been a set of tools, methods, and resources to help identify, access, and report intrusion. Intrusion detection has been generally part of the system's global protection that has been configured around the system and has not an individual criterion for protection. In general, the first line of defense has been the IPS which included solutions such as encryption, authentication, access control, secure routing, etc. Infiltration and compromise with a node lead them to the emergence of confidential information such as security keys for the adversary. Hence, IDS has been designed to detect secure system resources before an Intruder attack to detect intrusions. From a security point of view, the intrusion detection system has been always in the second line of defense [13]. Hence, functional requirements on WSN have been as follows:

• Low false positive rate: This rate has been estimated by calculating the percentage of normal changes that have been detected as misbehavior and abnormality.

• High True Positive Rate: This rate has been estimated by calculating the percentage of anomalies that have been detected.

Fig. 1 illustrates our subjective classification framework, derived from literature, of IDS utilization in the WSN context. In forthcoming subsections, each branch of the subjective framework is elaborated.

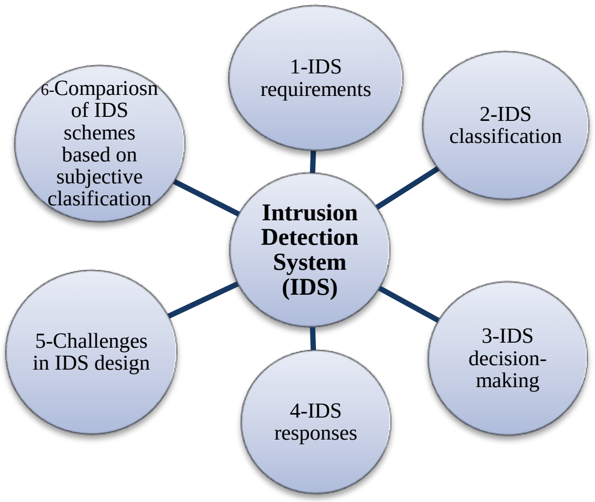

Fig. 1: The subjective classification framework for IDS in WSN context.

Intrusion Detection System Requirements

In the IDS designing process, the following non-functional requirements should be considered [14]:

• Do not add new vulnerabilities to the system,

• Limited requirements for system resources and failure to degrade system performance by introducing overheads,

• Continuous execution and transparent presence for users and the system,

• Utilizing the standards for cooperation,

• Reliability and also minimum rate of false-positive (FP) and false-negative (FN) in the detection phase.

Intrusion Detection System Classification

According to Fig. 2, IDS has been classified into the type of intruder locations, type of intrusion, detection methodology, data source examined, data collection site processing, infrastructure, and scope of application. Attempts have been made to briefly explain each of these sections based on previous research [27]-[30].

Type of Intruder Locations Placement

Generally, intruder locations placement in a network has classified as follows:

• External intruder: it has been obvious that outside the network, with various attacks, intruders have been tried to gain unauthorized access to the network.

• Internal intruder: in this category, a node has been tricked and used to place on the network.

On the other hand, on the ADHOC networks, the internal attacks have been utilized of two following nodes:

• Selfish node: This node has been utilized network resources, but it does not cooperate and has not directly damaged other nodes.

• Malicious node: This node aimed to harm and flood other nodes by creating a denial-of-service attacks (DOS) quite the same normal type of DOS attacks in IP-based networks.

An IDS has been able to detect external and internal intrusion. Researchers should consider that internal intrusion detection and also discovery have been more difficult than the external type of it. It has been obvious that internal intrusions have the key parameters that have been needed to thwart the precautionary measures taken by the authentication mechanism [36]-[38].

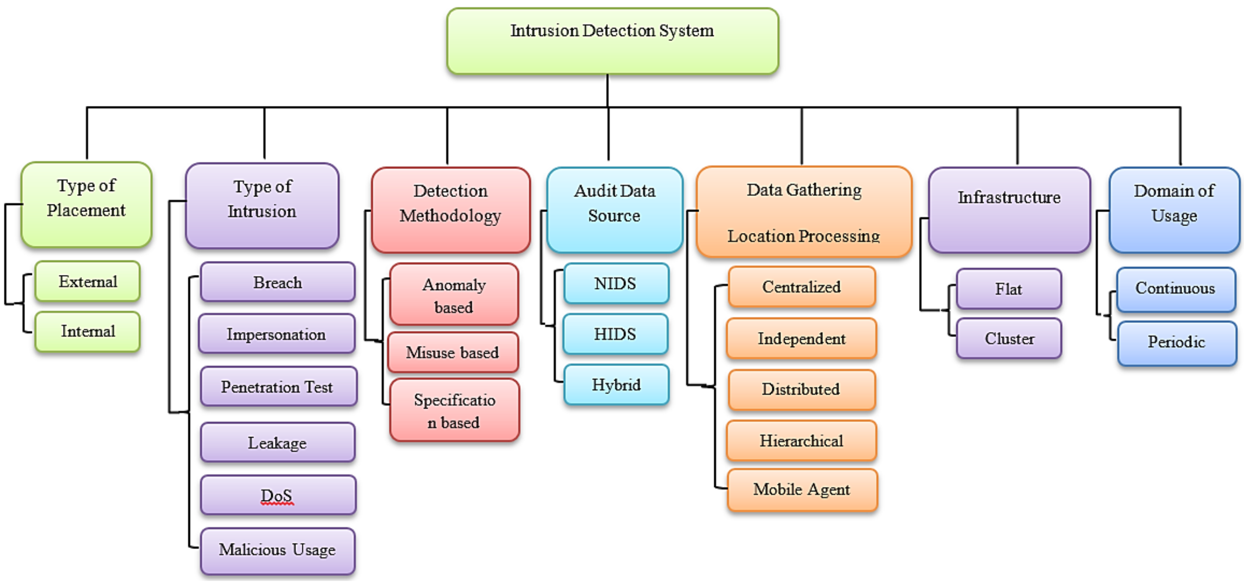

Fig. 2: Intrusion Detection System Classification based on type of intrusions.

Type of Intrusions

The intrusion in a network has been occurred in the following various forms:

- Attempted break-in: Create a search for unauthorized access to the network,
- Masquerade: Acting and using a fake identity to obtain unauthorized access to the network,
- Penetration testing: Obtaining unauthorized access to the network,
- Leakage: Unintentional information leakage from a network,
- Denial of service: flooding and blocking network resources,
- Malicious application: Aimed at intentionally hitting and damaging network resources.

Although IDS may have been provided more detailed detection solutions for the above attacks, system administrators always want a complete defensive system with the ability to detect all intrusions.

Detection Methodology

From the perspective of security architecture and critical Non-functional requirements such as performance, IDS have been classified into three following categories:

- Anomaly-based detection,
- Misuse-based detection,
- Specification-based detection.

In an anomaly-based detection strategy, the irregular solution has been based on statistical behavioral modeling.

The normal operating behavior of the members has been described for the system and the definite amount of deviation from the normal behavior has been expressed as the flag of irregularity. Disadvantages of this method included the fact that normal profiles must be updated at regular intervals due to rapid changes in network behavior. This model detects intrusion accurately and stably with small and limited values (FP, FN), under conditions where the network has been statistically considered in terms of behavioral pattern.

One of the advantages of this method has its use to detected unknown attacks or attacks encountered [13]-[15]. Based on the processing nature that has been created in the behavioral model, Anomaly detection has been divided into three following categories:

- Statistical based detection,
- knowledge-based diagnosis,
- Machine learning.

The Fig. 3 describes the classification of irregular intrusion detection systems based on their detection algorithms.

In statistically-based IDS, network traffic has been captured and a profile has been generated that represents random and sudden behavior. A reference profile has been also created when the network is in safe condition without attacks presence. After the network has been monitored, profiles have been generated at regular intervals. Hence, by comparing the reference profile, a rank has been generated. If this rating exceeds a certain threshold, the IDS assigns the flag of abuse to it.

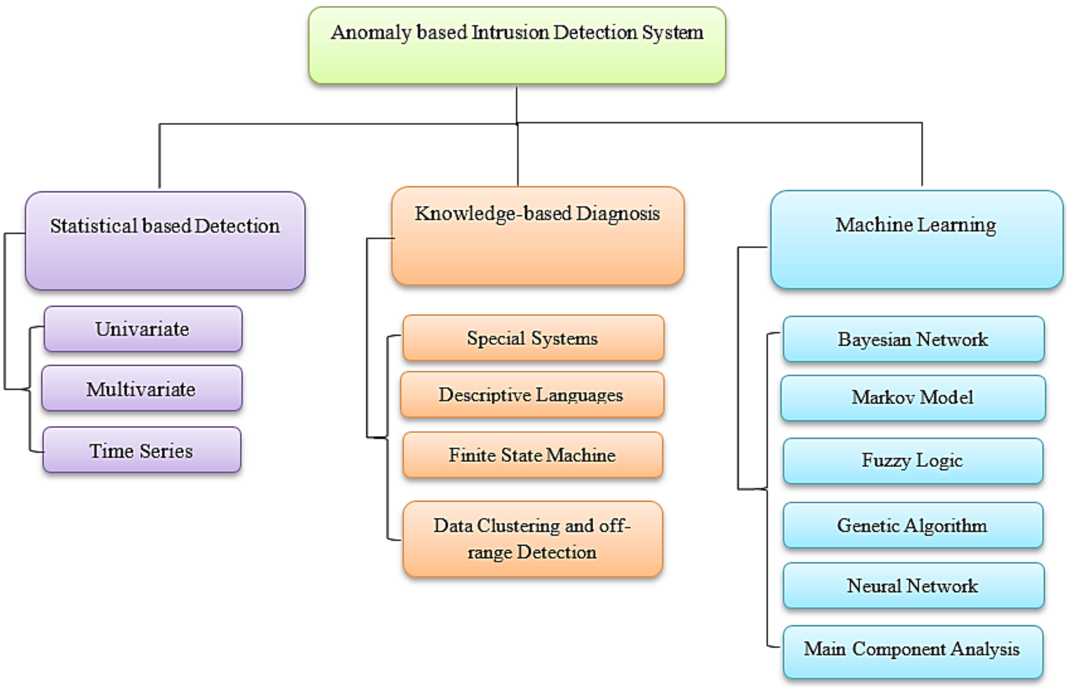

Fig. 3: Classification of Irregular Intrusion Detection System based on Detection Algorithms.

According to Fig. 3, this method has been categorized into the following sections:

- Univariate: The parameters have been modeled as separate Gaussian random variables.
- Multivariate: Correlation between two or more criteria has been considered.
- Time series model: An interrupt timer has been used during an event counter that records the order and time between the arrival of observations as well as their values in a report.

The following described an example of a detection methodology for detecting packet deletion attacks:

The percentage of FP transmissions from node m has been the rate at which packets has sent by node n among packets that sent from node M to node m with T specified time. This process has been calculated by the following equation. Table 1, Has been described the parameters that have been utilized in (1).

$$FP_m = \frac{Forwarded\ Packets}{Packets\ to\ be\ forwarded} = \frac{\#(m,M) - \#([m],M)}{\#(M,m) - \#(M,[m])} \quad (1)$$

In (1), If the Dominator that called Packets to be forwarded hasn't equaled to 0 and also if the value of the $FP_m = 0$, then the event has been recognized as "unconditional package deletion" and m has been also identified as an intruder. If the Dominator of (1), hasn't equaled to 0 and if $FP_m \leq specified\ threshold\ of\ satisfaction$ and if the condition of (2) has been met, then the event has been recognized as non-random package deletion and m has been also recognized as an intruder.

$$0 < FP_m < TF_P < 1 \quad (2)$$

Table 1: Abbreviation that utilized to detecting packet deletion attacks

Abbreviation	Parameter's role
m	Supervised node
M	Nodes to be monitored
$\#(m,M)$	The number of out-band packets from node $\boldsymbol{m}$ where $\boldsymbol{M}$ is the next step.
$\#([m],M)$	Output packets of the source node that called m where $\boldsymbol{M}$ is the next step.
$\#(M,m)$	Output packets of $\boldsymbol{M}$ where m is the next destination.
$\#(M,[m])$	Output packets of $\boldsymbol{M}$ where $\boldsymbol{m}$ is the final destination
FP_m	Percentage of sending packets from $\boldsymbol{m}$

In machine learning anomaly-based detection systems, an explicit or implicit model of the analyzed patterns has been generated. These models have been updated at regular intervals to improve IDS performance based on previous results. To optimize the IDS, the following solutions have been adopted.

- Markov model based on Markov transfer theory,
- Bayesian networks based on possible relationships between variables of interest,
- Fuzzy logic based on approximation and uncertainty,
- Genetic algorithm,
- Principal component analysis (PCA) based on dimensional technique.

In misused-based Detection, signatures, and identifiers (profiles) have been generated from previously known attacks and have been used as a reference for diagnosing future attacks. For instance, an example, of a typical ID and signature would look like the following example:

- Three unsuccessful login attempts in five minutes have been created by a brute force attack.

However, the advantage of this type of detection has been the ability to correctly and effectively detect known attacks. On the other hand, the disadvantage of this method has been that if the attack has a new type and has not already in the profiles, the misuse-based detection has not been able to detect it. These systems have been very similar to antivirus systems that often detect all or all known patterns of attacks. The researcher should be considered that the solution mentioned has been used in closed and non-public structures. Therefore, despite the high detection rate, software architects and developers have been required to utilize this method in their security architectures and networks. On the other hand, the following requirement has been proposed to monitor network anomalies:

- The requirement of interrupt: indicated a latency between the arrivals of two consecutive messages that must be within a certain range.
- The requirement of confidentiality: the passing message must be sent through the middle nodes.
- The requirement of integrity: the sender's main message should not be distracted when it reaches the recipient.
- The requirement of delay: packets must be resent after a specified waiting period.
- The requirement of iteration: Identical messages have been measured from a single node as well as a specific number.
- The requirement of radio's confidentiality rate: messages must have originated only from neighboring nodes.

- Noise rule: The number of collisions for packet transfer must be lesser than the threshold value.

In specification-based Detection, a set of specifications and constraints described the correct operation of a defined program or protocol. Then the implementation of the program has been monitored by considering the defined specifications and limitations [13]. This solution has been provided the ability to detect previously unknown attacks with low FP rates. There have been significant differences between IDS types. Anomaly-based IDS has been tried to detected anomaly behaviors, but misuse detection tried to recognize abnormal behaviors. Specification-based IDS techniques combined the benefits of abnormal detection and abuse detection through the manual development of features and constraints to determine system behaviors. Intrusion-based detection techniques have been similar to irregular detection strategies. In each, the attacks have been detected by deviating from the normal profile. Because feature-based detection techniques have been based on the extension of features and constraints manually, they have a limited false alarm rate compared to the high false alarm rate in anomaly detection. The cost of obtaining a limited false alarm is that it will take a long time to develop the details of the features and restrictions [39]-[42].

Audit Data Source

IDS has been categorized into the following parameters based on the audit data source and depending on the location of the analyzed data:

- A network-based intrusion detection system (NIDS): Actively or passively this system has listened to network communications, then records packets and evaluates packets. The mentioned system has the ability to analyze the entire packets transfer capacity and IP addresses or ports.
- A host-based intrusion detection system (HIDS): HIDS has been able to detect intrusions such as changing critical system files on the host side, repeated attempts to miss-access the host, unreasonable allocation of memory to a particular process, and input-output activities. The HIDS has been performed the detection operation by real-time monitoring of the host system or by checking the log file on the host side.
- Hybrid-based intrusion detection system: The Hybrid system has been Consist of NIDS and HIDS components in an efficient method utilizing mobile agents. Mobile agents referred to each host and check the system file log. Meanwhile, the central agent has been nationwide examining the entire network traffic for the presence of anomalies [59].

Estimation the Location of the Collected Data

Based on the location of the collected data, IDS has been divided into the following categories:

- centralized,
- Stand-alone IDS and independent,
- Cooperative and distributed,
- Hierarchical,
- Mobile agent-based IDS.

In the **centralized** IDS, a centralized computer has been observed all network activity and it has been detected intrusions by analyzing network surveillance activities and data.

In the **Stand-alone** IDS, the system has been executed separately on each node. Network members have been unaware of intrusions that have been occurred around them because a Stand-alone IDS does not allow the node to cooperate or transmit information to each other. They have only worked if they have been alone and independent.

The **Cooperative and distributed** IDS has been proposed for flat infrastructure networks. In this scenario, each node has been executed as an IDS agent which has been participated in the detection of penetration testing and the global response to the network. If a node has been detected an intrusion without evidence or without result, it has been able to independently issue a network warning regarding an attack.

The **Hierarchical** IDS has been proposed for multi-layer network infrastructure such as cluster structure. Cluster heads have been required to monitor their member nodes and also participate in global intrusion detection decision-making operations.

In the **Mobile agent-based** IDS, each mobile agent has been assigned to the selected node in order to create a specific task of the IDS and the intrusion detection has been done in cooperation with these nodes. After a specified period of time or after a specific time has elapsed for the task to be performed, agents have been moved to other predefined nodes to increased network life and also the efficiency of the IDS. Mobile agents have characteristics such as mobility, self-control, and compatibility.

In the **mobile AD-HOC networks**, IDS has been divided into the following parameters:

At the **Flat** infrastructure, all of the nodes have been considered with the same capability and have the ability to participate in routing functions. This facility has suitable for civilian applications such as a conference network or a classroom.

In the **Cluster** infrastructure, Nodes have not been considered as same. Nodes have been subdivided into clusters at a given transfer rate, and then nodes have been selected a node as a cluster head to centralize routing information for that cluster. Generally, headers have been consisted of many powerful devices with backup batteries to achieve greater transmission range. Hence, headers have been the virtual backbone of the network. Depending on the routing protocol, the middle gateway has been replayed the packets among the headers. This type of infrastructure will be very suitable for military applications with hierarchical commands [67].

Decision Making on the Intrusion Detection System

There have been two following mechanisms for decision making on an IDS:

- Stand-alone decision making,
- Cooperative decision-making.

An IDS deduces four non-zero probability decisions as a result of the decision-making process in an event.

- Intrusive and abnormal (False Negative): There has been an intrusion into the system, but the IDS has been failed to detect it and it recognizes the event as abnormal.
- Not intrusive and abnormal (False Positive): There has been no intrusion into the system, but the IDS concluded that a normal event is abnormal.
- Not intrusive and not abnormal (True Negative): There has been no intrusion in the system and the IDS has been concluded the event as abnormal.
- Intrusive and abnormal (True Positive): There has been an intrusion on the system and the IDS has been detected the event as abnormal [71], [72].

Intrusion Response

It has been obvious that the IDS has not met the prevention criteria at the time of the attack and leaves this process to the IPS section [106]. The intrusion detection system has been worked reactively in comparison to the active operation of the IPS. Whenever a production intrusion warning has been issued by an IDS, the following has been raised based on the characteristics of the system:

- Create an audition or review record
- All of the network members, system administrators, and base stations should be notified of intrusion. If possible, the location and identity of the adversary should be stated in the alert message.
- If possible, a reduction strategy should be considered to stop infiltration. For instance, a modified auto action should be generated by the collaboration activity of network members, especially the event neighbor.
- There has been no trusted source and decisions must be made by a colleague.

Challenges and Regulations of Intrusion Detection Systems Design in Sensor Networks

The proliferation of sensor networks has been leading researchers to develop and expand solutions to provide sustainable communications and networks for distributed environments, as well as how to secure these methods with limited resources. The lack of stable infrastructure space such as gates, routers, base stations, etc., makes it very difficult to design security models and algorithms for the sensor network. Limited bandwidth, throughput, battery source has scarce resources that should be considered considerably in the network architecture design phase [108]. To create an intrusion detection system in the sensor network, the system must contain the following requirements:

- Localize auditing:

The IDS in WSN must work with the main data as well as cross-sectional inspection because in WSN there has been no central point that can collect the global data examined. This is separate from the base station.

- Resource constraint:

The IDS must utilize the minimum resources for each network. Communications between two nodes should not saturate the available bandwidth to detect intrusion.

- Lack of trust in the elements:

Unlike wired networks, sensor network security has been easily compromised. Hence, the IDS should not trust every node and element in the network.

- Distributed:

Data collection and analysis must be in multiple situations. In addition, the distributed solution has been applied to implement the correlation detection and warning algorithm.

- Securely:

IDS should be resistant and withstand attacks.

A Comprehensive Comparison Among the Proposed IDS in Literature

In the hierarchical structure, cluster-based IDS, as well as clustering algorithms have been consumed significant network energy to form clusters.

Agent-based IDS has been reduced network load and latency. On the other hand, it has been led to high energy loss in the associated nodes. The cost of communication between the agents and the coordinator has been made it possible to create congestion and bottlenecks in the network.

Rule-based IDS have been Easy to configure and also executed. They have been required to constantly update the rules and regulations to counter new attacks.

Data mining-based IDS can detect new attacks. Unfortunately, these systems have been required to have high computational complexity as well as high power consumption for their data samples. There has been also a requirement for efficient analysis tools to analyze large amounts of data as well as memory space to store data.

On the Game theory-based IDS, the detection rate has been set by the network security manager utilizing changing the parameters. The disadvantage of this system has been the incompatibility as well as human intervention for sustainable operation, because a wide variety of intrusion detection algorithms have been available, selective intrusion detection solutions must be embedded for the desired features, requirements, and applications based on network hazards [114], [115].

Security has been a functional requirement that required optimal and correct detection of the adversary and satisfaction in accurately determining the exact duration of the attack. The following have been suggestions for specific applications in IDS in the sensor network architecture:

- For itinerant applications, where the sensor nodes have been in motion, it would be appropriate to utilized distributed IDS methods due to their scalability, robustness, and speed.
- For static applications, in a situation where there has been a centralized processing unit in the base station or data in the sink, the utilization of centralized solutions has been appropriate due to their robustness and ability to detection of a wide range of attacks.
- For cluster-based applications, utilizing of hierarchical intrusion detection system would be appropriate.

Various IDS for WSN have been described in Table 2, and include the required network architecture, detection technique, and features of each method.

Related Research on IDS by Incorporation Machine Learning (ML) Techniques

Since the handling of WSNs' challenges has high complexity, various researchers have proposed the utilization of machine learning (ML) on IDS [119], [120]. The ML algorithms can manage huge data with optimum speed and accuracy. These algorithms have been utilized to design the accurate models that specifically were designed for the classification, clustering, and also prediction processes. The ML techniques played a vital role in the IDS for WSNs when it has been utilized in support vector machines (SVMs), Gaussian naive Bayes, and Random Forest logic regression algorithms. The ML can be subjectively categorized as follows:

- Supervised learning,
- Unsupervised learning,
- Reinforcement learning.

It is obvious that firstly all of the ML algorithms have been labeled as training data that specify an input, output data, and some system parameters. The Fig. 4 depicts the ML classification. The supervised learning has been used as regression and also classification model. An unsupervised learning has been used to classify sample sets as well as groupings. In reinforcement learning, agents have been prepared for the learning process by interacting with the environment. It should consider that the combination of supervised learning and unsupervised learning has been considered semi-supervised and as a hybrid algorithm inherited all the main functions of the mentioned field.

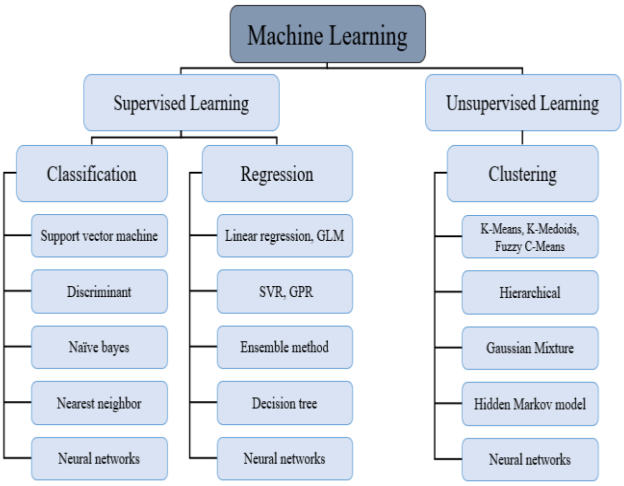

Fig. 4: Classification of ML algorithms [20].

On the other side, researchers have proposed a multi-core ML-based IDS [121].

In this structure, a prototype has been considered a hierarchical intrusion detection model. The sequence and attractiveness of multi-core functions promise to reduce detection time and high detection rates. Fig. 5 illustrates a multi Kernel-Extreme learning machine (MK-ELM) algorithm.

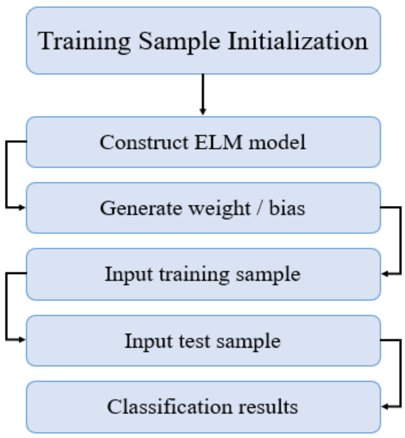

Fig. 5: MK-ELM algorithm Diagram [31].

Table 2: Comparison between researched IDS in the last 20 years

Proposed IDS	Architecture	Detection methodology	Distinctive feature
[6]	Distributed	Rule based	Scalable, powerful and accelerates detection.
[14]	Centralized	Anomaly based	Scalable and Reliable detection on black hole utilizing meta-heuristic and quantum speedup.
[8]	Hierarchical	Automatic scout	Relying on the diffusion nature of sensor node communications and the use of high node diffusion densities.
[9]	Hierarchical	Rule based	Monitor nodes and routing tables.
[22]	Hierarchical	Rule based	Energy storage, extension of network life, inability to add nodes to the network.
[23]	Hierarchical	Rule based	Combine existing solutions in order to achieve more complete solutions.
[37]	Hierarchical	Specification based	Achieve optimal performance or centralized design.
[56]	Distributed	Rule based	Detection of selective transmission attacks and black holes based on the presence of an intruder.
[60]	Centralized	Anomaly based	Only able to detect wormhole attacks.
[61]	Hierarchical	Anomaly based	Focus on collected data to maintain node or connection security.
[70]	Stand-alone	Anomaly based	Local detection, lack of node notification of attack.
[90], [91]	Hierarchical	Game theory	Monitor only at one time and one cluster.
[98]	Stand-alone	Rule based	Detection of anomalies in all network layers.
[101]	Distributed	Anomaly based	Extract sensor network stability by information from neighboring nodes.
[109]	Distributed	Rule based	Minimize processing overhead when detecting abnormalities within the network.
[112]	Centralized	Statistics based	Using heuristic ranking algorithms to determine undesirable nodes in the network.
[113]	Hierarchical	Statistics based	Use a cluster-based hierarchical secure management protocol to identify malicious and selfish nodes.
[116]	Hierarchical	Anomaly based	Efficient detection that utilizing fuzzy C-means clustering
[117]	Hierarchical	Anomaly and Misuse based	Optimal detection accuracy with the ability to Determine the type of attacks
[118]	Distributed	Anomaly based	Covering the important non-functional requirements such as reliability, efficiency, scalability, Interoperability, low overhead and etc.
[127]	Hierarchical	Anomaly based	Efficient energy consumption.
[128]	Hierarchical	Anomaly based	High accuracy in detection phase with low overhead.
[129]	Distributed	Anomaly and Misuse based	Low False Positive rate and high accuracy with low complexity.
[130]	Hierarchical	Anomaly and Misuse based	High accuracy in detection phase by a Composition between SVM classifier and signature-based approach with low overhead

Other researchers have proposed various reviews of the application of game theory in sensor network security [32]. According to the various applications of common game theory approaches for the security era, the design method has been divided into the following categories:

- Denial of service (DOS) prevention,
- Intrusion detection,
- Upgrade security level,
- Coexistence with destructive nodes.

The theory analyzes a myriad of possible scenarios before creating an operation. Hence the decision-making process has the modeling ability. The summary and also the main axes of the researches on the game theory has been described as the following categories:

First category:

- There are No-Cooperative game [33],
- Cooperative game [34],
- Repeated game to prevent DOS attack [35].

Second category:

- There has been no cooperative and also Markov games models for intrusion detection [36]-[40].
- There have been Auction theory and coalitional game theories to strengthen security [41], [42].
- There has only signaling game approach to coexist with malicious nodes [43]. In [45], an overview of IoT intrusion detection systems has been provided. They have been described the IoT architecture as shown on the Fig. 6.

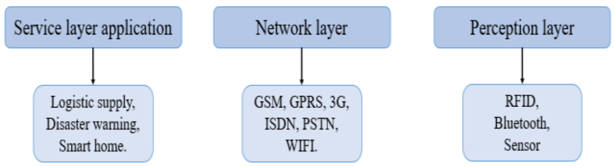

Fig. 6: IoT architecture [45].

In the same field, researchers have proposed a rule-based IDS based on the proposed event processing model (EPM) to solve the problem of real-time intrusion detection in the IoT [46]. Obviously, this model has been based on the EPM in which the rules that have been stored in the rules pattern repository (RPR) and then considered as a reference. The mentioned approach in relation to the existing IDS has consumed more CPU resources while consuming less memory and minimizing processing time. On the other side, anomaly IDS for WSN has been proposed. The steps of this IDS have been as follows:

- Local audit phase: evaluation of the packets to validate reputable neighbors.
- Rule application: this step has been worked on promiscuous mode.
- In the third step: routing attacks have been detected by validating the collected data.

It is obvious that the proposed mechanism is able to just detect routing attacks which means the weakness of this approach. From our viewpoint, this solution should not fully be considered in WSN because of its disadvantages and its weakness. In other anomaly-based IDS, a soft processing and computing system approach was proposed [47]. The main purpose of this research is to increase the performance of the system and identify any event strongly. The authors have proposed and also run famous algorithms such as PSO, LBP, LDA, PCA, SVM, and GSM. In their approach, the detection rate has been increased by decreasing the number of features. Another paper has fully described an agent-based IDS approach [48]. This approach has been used for several factors as well as classification to detect intrusion. The authors used the mobile agents to detect intrusion with below elements:

- Collector agent,
- Misuse detection,
- Anomaly detection based on SVM classification.

From the point of view of reading and criticizing their writing, it is obvious that their proposed system has fewer parameters to describe the attacks [47]. This research design could have a more useful diagnosis by creating more complex diagnostic parameters as well as using statistical anomaly detection and creating attack signatures. It is also clear that the defects have been obtained and the solution for the article under discussion at the end of this research project has been evaluated and simulated. Another important research on the IDS era has been proposed based on GA K-Means [49]. In this research, the false positive (FP) rate has been decreased and a high detection rate has been obtained. It should consider that this approach was suitable for dynamic topology changes. Clearly, this measure has been considered a critical and also non-functional requirement in IDS security architecture design. This approach has been able to detect new attacks without pattern and also allows intrusion and traffic analysis.

In a hierarchical model [50], researchers have described an IDS for blackhole attack detection in WSN based on simulation on NS2 software. In this approach, the sensor node and base station (BS) have exchanged control packets. Each control packet has consisted of a node identifier and the number of packages that have been sent to the cluster headers (CH). Obviously, the BS has been monitored to detect a black hole attack. The solution presented in [50] consumes less energy to detect intrusion. As a critique of this article, it can be acknowledged that although the effects of the attacks have been significantly reduced, there has been no guarantee that other blackhole attacks will be identified in their security architecture plan. This means that the researcher doesn't fully consider the non-functional and functional requirements in the requirement engineering and security architecture phase.

On the other side, an optimized IDS has been proposed for Sybil detection [51]. Firstly, an approach focused on sending data packet query confirmation has been implemented. It should consider that the CH has been saved from the table. This tale is used to store the identity and location of other nodes. This process is somewhat similar to the address resolution protocol (ARP). Secondly, all of the legal nodes have responded to the eclipse with their true identities and real coordinates. This has been where the Sybil node was detected. The results of their research indicated that in the mentioned system, the destructive node and specifically the Sybil attack can be accurately detected and the energy efficiency has been improved.

Another promising solution was proposed to detect wormhole attacks and flooding by simulation in NS2 [52]. In this design, the abnormal behavior of the nodes has been monitored by the energy prediction algorithm. The attack can be assessed on a scale of both real and predictable scenarios. Although the plan's approach minimizes energy consumption, the plan only detects wormhole attacks and flooding.

By reviewing on further research, a Man in the middle IDS (MITM-IDS) has been proposed to isolate attacks and reconfigure attack nodes [44]. Their simulation results show 89.147% efficiency in detecting MITM attacks. In this plan, a penetration detection system based on deep learning techniques has been introduced in order to deal with a popular attack. The strength of this model has been the rapid detection of malicious behavior due to the less complexity. Obviously, ARP spoofing and poisoning can be considered similar to the attack of inserting a malicious node in the sensor network and attacking the non-functional requirements for confidentiality, authentication, and availability, which are the most important security system design parameters such as intrusion detection.

The implementation and application of this system have led to a wide range of solutions in sensor network security. Of course, the limitations of the WSN should not be forgotten in this regard. Authors in [53] have identified various vulnerabilities and security issues across the sensor network. In this research structure, unique classes have been discussed as follows:

- Inner work style.
- Interrelated convention stack.
- Organize provisioning, oversight and transmitting issues.

In the mentioned plan, the calculations of the proposed conventions and oversight have been collected and evaluated. The current issues in the field of research and establishment of IDS in IoT and WSN have been expressed and a qualitative evaluation of approaches has been done [54].

A complete subjective classification of the research that has been done so far is depicted in Fig. 7. To make the best decision to choose the right system more than 70 papers have been studied from 2006 until 2022.

The Fig. 7 has been represented a complete classification of the research that has been conducted on the establishment of IDS.

It has been worth noting that KilerBee has a framework for exploiting ZigBee vulnerabilities. Numerous researchers have examined the challenges as well as future paths ahead for IDS in WSN [105], [115]-[120].

In [122], authors' findings on IoT IDS retrieval and attacks in different layers have been summarized in Fig. 8. Although the explanations of the researchers of the above article have been extensive, structurally, the IDS architecture, as well as the engineering of IDS requirements, have not been addressed. So, if corrected with appropriate words, the same non-functional and functional requirements have been addressed. Mentioning this point will make their research more productive, adding that functional requirements have a factor in the proper functioning of the system, and non-functional requirements, which have no tangible, will meet the unknowing needs of the user. This is the main part of the requirement engineering process and also a critical point for software architecture.

Researchers have proposed a fuzzy logic-based approach to prevent the intrusion on WSN utilizing WSN-DS dataset [123]. Their system has 3 phases:

- Feature extraction,
- Membership Computation,
- Apply fuzzy rules.

On the other side, they utilized of 3 following colors in their simulation.

- Orange: Probability of node destruction,
- Green: the node is secure in the network,
- Red: Destructive node.

Their Proposed FZMAI approach have been consist of some primary parameters as follows:

- Packet transmission rate to the base station,
- Energy Consumption,
- Signal Strength,
- Packet Delivery ratio (PDR),
- Received packet.

Their results have shown a 98.29% improvement in accuracy assessment.

Compared to other fuzzy methods, their approach has been more efficient than others. The advantage of their proposed system is that the malicious node has been prevented from entering the system and thus intrusion has been prevented. Their FZMAI model has been presented in Fig. 9.

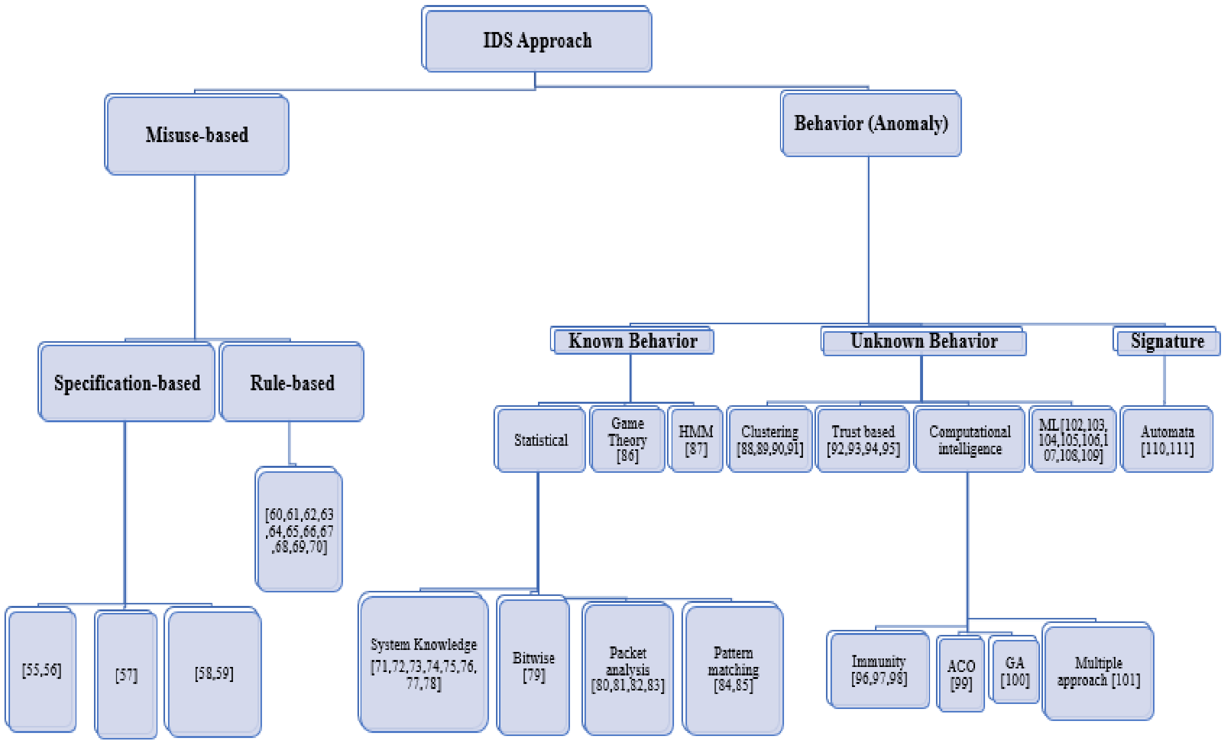

Fig. 7: The IDS classification and related researches.

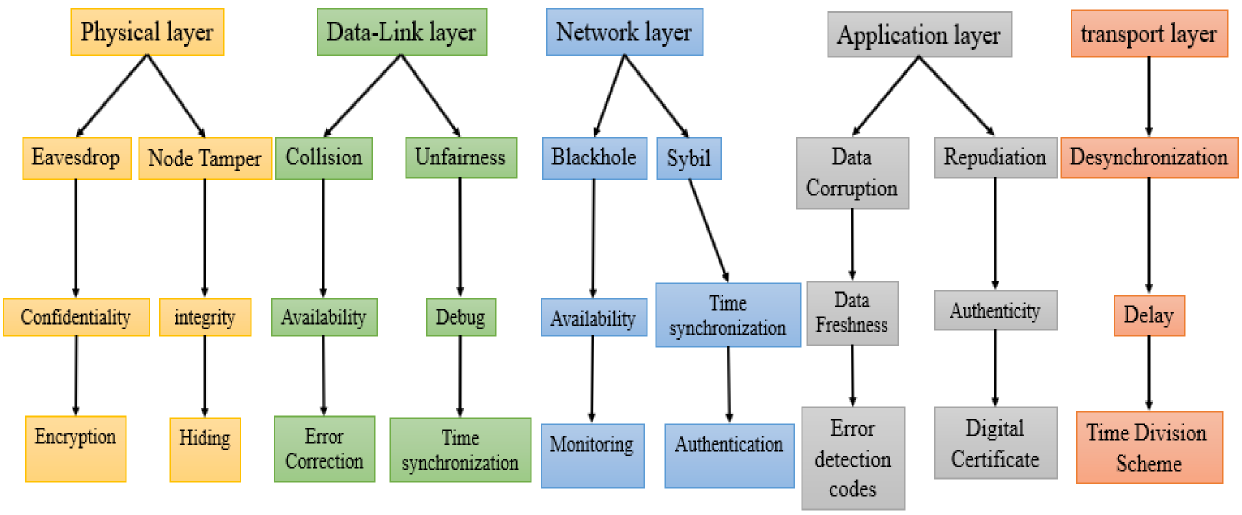

Fig. 8: Different threats in different network layers.

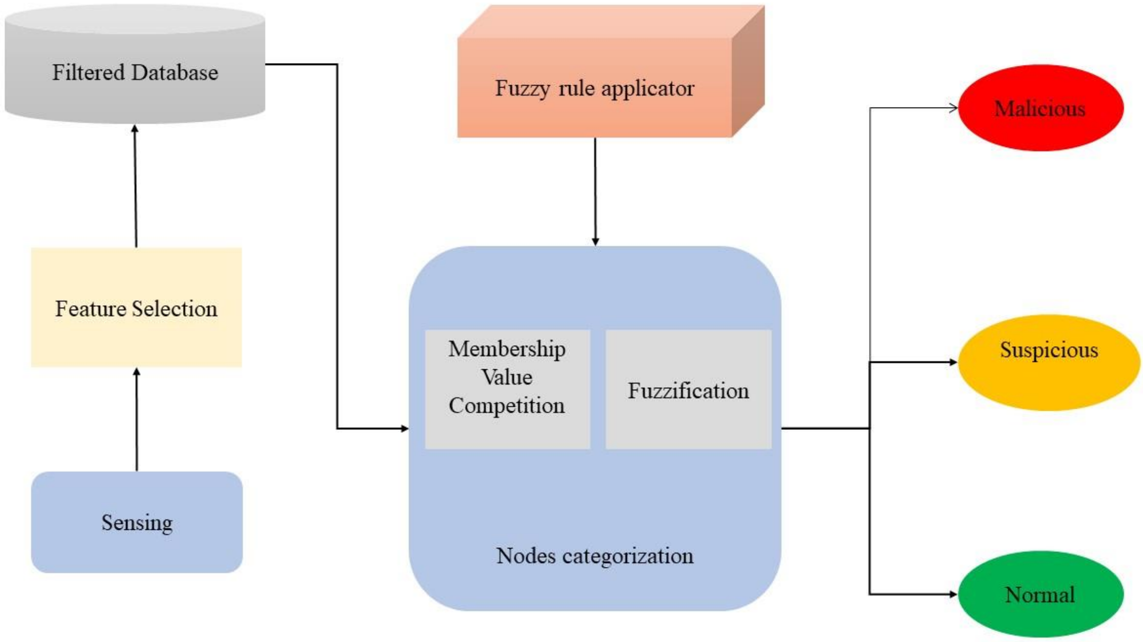

Fig. 9: The FZMAI model [123].

As a critique of their research, it should be noted that their system has not provided transparency in assessing the throughput, latency, and congestion rates in the network. Obviously, in the calculations of the membership function and fuzzy logic, the rate of FP and TP has not been given. According to the proposed algorithm, they have obtained a high FP rate due to the convergence of nodes and data volume.

In [124], researchers have proposed a mechanism for designing sink hole attack detection in the context of hierarchical networks. According to them, HWSN has been the first step in detecting 3 following attacks:

- Sink hole message modification node (SDP),
- Sink hole message delay node (SDL),
- Sink hole message dropping node (SDP).

In their approach, HWSN has been divided into several unconnected clusters, each cluster having a powerful final sensor called a cluster-head, which has been responsible for detecting malicious activity in the infrastructure of the cluster. The simulation and the results obtained from the NS2 simulator show the fact that the detection rate of this approach has been 95% and the FP rate has been 1.25%.

In [125], researchers have proposed an advanced model of IDS based on KNN utilizing the AOA optimization algorithm in WSN. This process has led to an improvement in the face of DoS attacks. to increase the accuracy of this model, a parallel strategy has been used to strengthen the relationship between the population, and also a Levy Flight strategy has been used to adjust the optimization values. The PL-AOA algorithm performs well in benchmark function testing and effectively ensures the improvement of KNN classification operations. The aforementioned model achieved 97% accuracy and almost 10% improvement over the original KNN during the DOS attack. In [126], researchers have studied the solution of secure node detection based on ANN in WSN. Their results have indicated that the optimized solution based on the biological neural network strengthens the diagnosis in WSN. On the other side, Insecure nodes negatively have affected network performance and will naturally interfere with system behavior. Regression analysis for both methods has detected changes when all nodes have been safe and also in insecure status. Diagnosis based on packet delivery ratio and energy consumption can be effectively implemented in the ANN.

Review in literature shows that more than 30% of articles have been based on detecting routing attacks. These attacks have included Blackhole, wormhole, Sybil, Sinkhole, and Selective forwarding. Table 3 has been shown the IDS that have been embedded for 15 unique scenarios. The sensor network has been less abstract than the IoT, but always has computational limitations on processing and energy consumption. On the other hand, reasoning about these systems has been much simpler because of their homogeneity and the possibility of behavioral analysis. It has been obvious that the WSN has been called an IoT system sub-category. To make the best decision to choose the right system more than 70 papers have been studied from 2006 until 2022. The papers have been collected based on how the attack structure has been positioned and the solutions used in Table 3. Table 3 through Table 8 and also Fig. 10 through Fig. 14 are dedicated for easier reference as well as classification and comparison of different areas and a comprehensive collection of previous research comparison based on prominent parameters.

Table 3: Frequency of research that has been conducted about IDS placement in WSN and IoT

Detection method	IDS placement		
	NIDS	HIDS	CIDS
Rule based	[65], [112], [113]	--	[60], [61]
Signature-based	[64]	--	[62]
Anomaly-based	[113], [84], [75], [104], [102], [103], [67]	[51], [79]	[108], [114], [109], [82], [59]
Statistical-based	[81], [73], [74]	[76], [85], [87]	[69], [94]
Stateful-based	[111]	--	--
Clustering-based	[88], [95], [89]	--	--
CI-based	[96]	[97]	[99], [101], [100], [98]
Specification-based	[55], [57]	--	[56], [83]
Trust-based	[92]-[94]	--	--
Autonomous-based	[110], [111]	--	--
Game Theory-based	[86]	--	--
Misuse-based	[66]	--	[107]

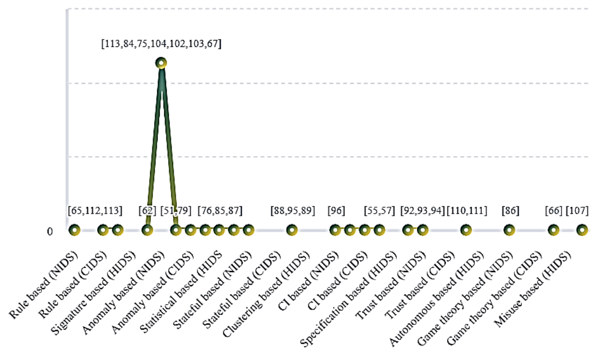

Fig. 10: The scope of research conducted in the field of deployment and type of IDS in WSN and IoT in previous years.

Table 4: Various security scenarios and IDS detection in WSN and IoT

Attack structure	IDS placement		
	NIDS	HIDS	CIDS
Scanning	[66]	--	[100]
Web exploit	--	--	[100]
Routing attack	[93]-[95], [88], [113], [55], [74], [73], [64], [67], [83]	--	[99], [58], [107], [56], [109], [59]
Rank	--	--	--
Information leakage	[66]	--	[98], [99], [101]
Replay	[57], [110]	[76]	[101], [98]
Spoofing	[57], [110]	[76]	[101], [98]
Packet Drop	[57], [110]	--	[101], [108], [98]
Flooding	[65], [75], [86], [81]	[72], [85]	[77], [101], [60], [61], [71], [78], [98]
Worm	--	[79]	--
Injection	--	[79]	--
Anomaly Behavior	[96], [103], [104]	--	[82]

Table 5: Extent of research on the spatial environmental conditions of IDS in different networks

Network Type	IDS placement		
	NIDS	HIDS	CIDS
WSN	[78], [88], [75], [104], [90], [92]	[87]	[99], [58], [107], [101], [59]
IoT	[63], [111], [97], [110], [86]	[79], [85], [97]	[108], [114], [69], [100], [71], [70]
IPV6	[73]	--	[62]
Smart grid	--	--	[92]
Smart City	[34]	--	--
Smart home	[96]	--	--
ZigBee	[102]	--	--
ICS	[84]	--	--
Bluetooth	[65], [66]	--	--
Relay Comm	--	[76]	--
RPL	[55], [74], [103], [67]	--	[49], [69], [75]
6Low pan	[81], [93]	[72]	[44], [45]
Clustered	[95]	--	--
Healthcare	[94]	--	--
BACnet	[57]	--	--

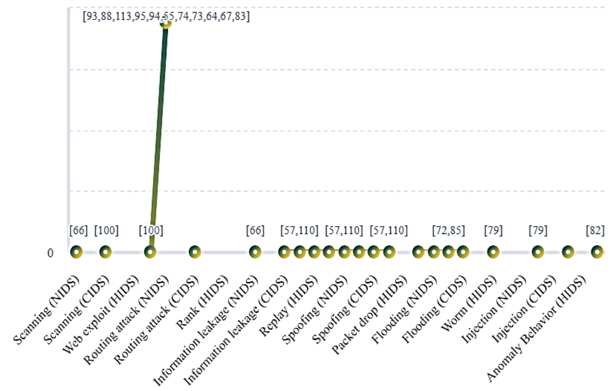

Fig. 11: The scope of research conducted in the field of Various attacks scenarios and IDS detection in WSN & IoT.

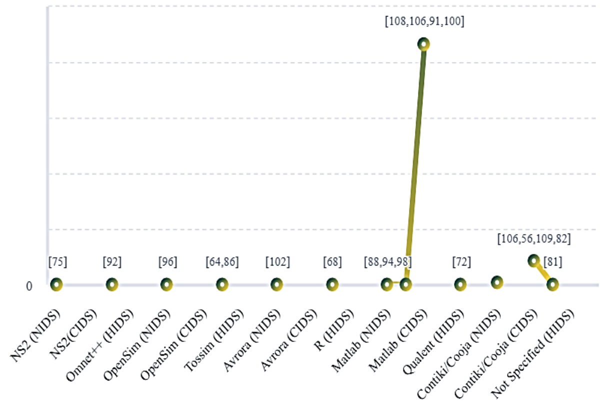

Fig. 13: The extent of the research conducted around the utilizing of various IDS simulators in WSN and IoT.

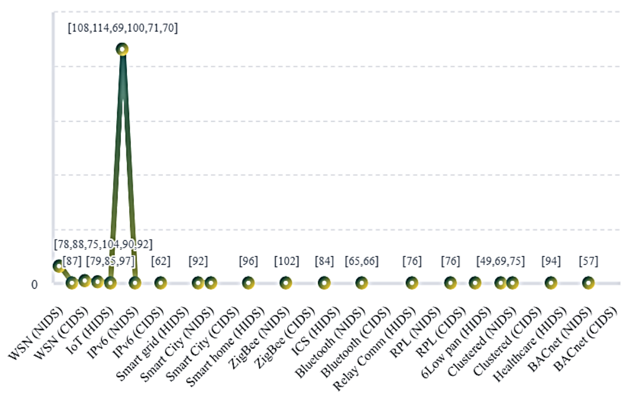

Fig. 12: The extent of the research done around the IDS in the action space and the infrastructure of various networks.

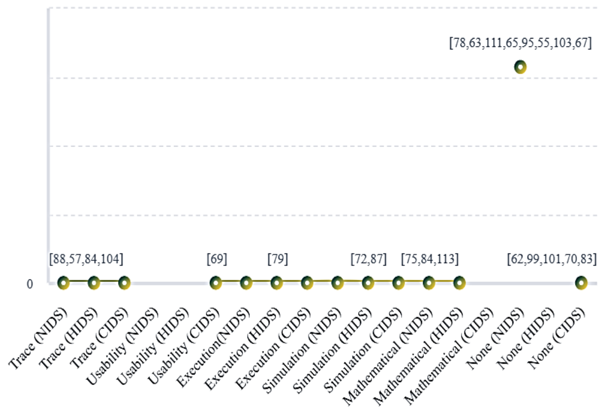

Fig. 14: The extent of previous research in the field of IoT assessment and utilizing of different types of IDS.

Table 6: IDS simulator in WSN and IoT

IDS Simulator	IDS placement		
	NIDS	HIDS	CIDS
NS2	[75]	--	--
Omnet++	[92]	--	
OpenSim	[96]	--	--
Tossim	[64], [86]	--	--
Avrora	[102]	--	--
R	[68]	--	--
Matlab	[88], [94], [98]	[87]	[108], [106], [91], [100]
Qualent	--	[72]	--
Contiki/Cooja	[93], [74], [73], [67]	--	[106], [56], [109], [82]
Not Specified	[81]	--	--

Table 7: Evaluation on IoT & IDSs

Method	IDS placement		
	NIDS	HIDS	CIDS
Trace	[88], [57], [84], [104]	[85]	[98], [107]
Usability	--	--	[69]
Execution	[57], [66], [110]	[79]	[58], [69], [100], [60], [61], [71]
Simulation	[96], [81], [88], [64], [86], [102], [92]	[72], [87]	[93], [68], [75], [94], [74], [73], [67]
Mathematical	[75], [84], [113]	[76], [85], [113]	--
None	[78], [63], [111], [65], [95], [55], [103], [67]	--	[62], [99], [101], [70], [83]

Also, Table 8 provides a summary and useful information on the NIDS in WSN and IOT that researchers have done for the last 10 years.

Table 8: Summary of research that have been conducted in NIDS on WSN and IOT

Paper	Detection Approach	IDS Placement	Envolve	Evaluation	Detection
[80]	Anomaly-based	Distributed	WSN, AD-HOC, IoT	O, Б, ж, £	$B^1, B^2, B^3, B^4, B^5, B^6$
[96]	Immune-based	Centralized	Smart-home	o	$Internal^2$
[78]	Anomaly-based	Distributed	WSN	χ	--
[81]	Statistical-based	Centralized	6Low PAN	o	DDoS
[63]	Rule-based	Centralized	Test Bed	χ	--
[88]	Cluster-based	--	WSN	0, Б	Sybil
[55]	Specification-based	Distributed	RPL	χ	Topology
[89]	Clustering-based	--	IoT	£	--
[102]	Anomaly-based	Distributed	ZigBee	o	Killer Bee
[83]	Anomaly-based	--	ICS	Б, £	--
[64]	Signature-based	Centralized	WSN	o	$Routing^3$
[86]	Game-Theory	Centralized	IoT	o	DoS
[65]	Rule-based	Centralized	Bluetooth	χ	B^4
[92]	Trust-based	Distributed	WSN	o	B^5
[66]	Misused-based	Centralized	Bluetooth	ж	B^6
[103]	Anomaly-based	Distributed	RPL	χ	$Internal^2$
[104]	Anomaly-based	Distributed	WSN	Б	$Internal^2$
[67]	Hybrid-based	Distributed	RPL	o	$Routing^3$
[73]	Statistical-based	Distributed	IPv6	o	$Routing^3$
[74]	Statistical-based	Distributed	RPL	o	$Routing^3$
[93]	Trust-based	Distributed	6Low PAN	o	Sink hole
[110]	Automata-based	Centralized	IoT	ж	DDoS
[105]	Hybrid-based	Centralized	Smart City	o	Routing
[111]	Automata-based	Centralized	HTTP	χ	$Protocol^1$
[94]	Trust-based	Distributed	Healthcare	o	$Routing^3$
[75]	Anomaly-based	Centralized	WSN	£, o	Energy-DoS
[95]	Cluster-based	Centralized	Clustered	χ	$Routing^3$
[57]	Specification-based	Centralized	BAC Net	Б, ж	$Protocol^1$
[114], [115]	Fuzzy logic-based	Distributed	WSN	--	
[111], [115]	Agent approach	Distributed	WSN	--	
[105], [115]	Rule-based	Distributed	WSN	--	
[112], [115]	ANN	Centralized	WSN	--	
[101], [115]	CVM	Centralized	WSN	WSN-DS	
[65], [115]	Fuzzy logic-based	Centralized	WSN	KDD Cup99	
[83], [115]	ANN	Distributed	WSN	--	
[75], [115]	Random forest	Centralized	WSN	KDD Cup99	
[100], [115]	K-means & SVM	Distributed	WSN	KDD Cup99	
[115], [116]	SVM	Distributed	WSN	KDD Cup99	
[115], [117]	Trust-based	Distributed	WSN	KDD Cup99	
[95], [115]	Trust-based	Distributed	WSN	--	
[115], [118]	Trust-based	Distributed	WSN	--	

Legend

Activity	Abbreviations	Operation
Detection range	B	Custom Attack List
	1	Spoofing, MITM, Drop Packet, Replay attack
	2	Unusual activity by a component in the framework
	3	Routing Attacks such as Worm, Sink & Black Holes.
	4	Resource Drain DoS, Spoofing
	5	Collision attacks, Selective forward & hello Flooding
	6	Reconnaissance, DoS, theft and leakage attacks
Evaluation style	ж	Execution evaluation performed
	Б	Trace evaluation performed
	£	Mathematical evaluation performed
	o	Simulation performed
	χ	Without any Evaluation

Attacks Against WSN (Passive & Active Attacks)

The passive attack has been limited to sniffing the exchanged traffic. This type of attack has been easier to realize and difficult to detect because they do not involve any alteration of the data. Since the attacker does not make any modification to the exchanged information. The intention of the attacker can be the find out the confidential information or the knowledge of the significant nodes in the network (cluster head node), by analyzing routing information, to prepare an active attack.

In active attacks, an attacker tries to remove or modify the messages transmitted on the network. The attacker can also inject his traffic or replay old messages to disturb the operation of the network or to cause a DOS. In WSN, among the most known active attacks, it can quote Tampering, Blackhole, Selective forwarding, Sybil, Hello flooding, Jamming, Blackmail, Exhaustion, Wormhole, and identity replication attacks [16].

A wormhole attack has been a routing scenario that will happen on the network layer. In this scenario, the attackers have been required to import at least 2 malicious nodes. These two nodes have been classified via a low latency link directly. This Direct link called tunnel caused the conflict and also aberration in routing protocols. A malicious node takes the packets in a part of the network and then will forward them via its malicious tunnel. The wormhole scenario has been running when the other node has been in the discovery phase. Note that, in this scenario, there has not been any negotiation between the sensors [15], [16]. In the Blackhole scenario, attackers have been required to import at least a malicious node into the network. On the other mean, this node will modify the routing table for malicious goals, once it takes the incoming traffic then there hasn't been any retransmission for sensed data. In the Sybil scenario, attackers can use the identities of the others nodes to take part in the distributed algorithm such as the election [18].

The traditional routing protocols faced many problems due to dynamic behavior and resource constraints. These Attacks can occur when the malicious node present in the network has been intended to attack directly the data traffic and intentionally drops, delay or alter the data traffic passing through it.

Blackhole Attack has been a very dangerous active attack on the MANETs and WSN. It has been formed during the week routing infrastructure when a malicious node joins the network this problem arises. Detection systems for ad hoc networks have been extremely difficult due to the lack of a central controller, bandwidth limitations, and dynamic topology in mobile ad hoc networks. Routing protocols have been a great guide to authors in evaluating connection quality and estimating destination info. In this paper we simulate Blackhole and Wormhole attacks in a cluster-based network with NS-2 simulator and also a safe cluster-based network for comparison phase, then we have been exploited some primary requirements such as throughput, end to end delay packet delivery ratio, normalized routing load, receive the packet with AWK language and then we have been plotted them on the following figures. To validate those results, we have been running them on Debian, Ubuntu, and Kali Linux operation systems, separately. For the network basic parameters and presents a comparison ability with another approach, we have been used other researcher measures that have been shown in Table 9, [14]-[18].

Table 9: Simulation parameters in a WSN

Parameters	Settings
Number of nodes	21
Network area	500*500 (m^2)
Routing protocol	AODV
Maximum packet in IFQ	50 (**ms**)
End time of simulation	10.0

In the following, we have been traced the primary parameters of simulation based on AGT's level trace.

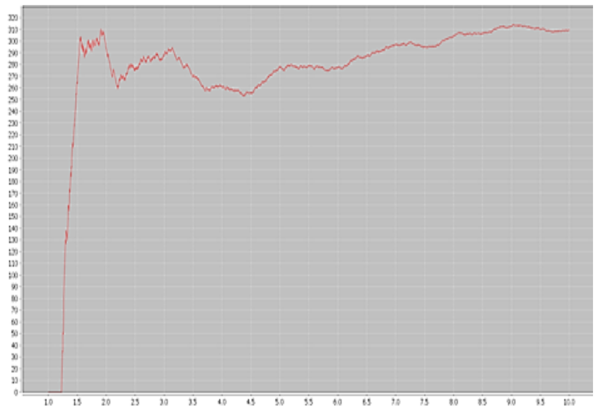

Fig. 15: Throughput in clear scenario.

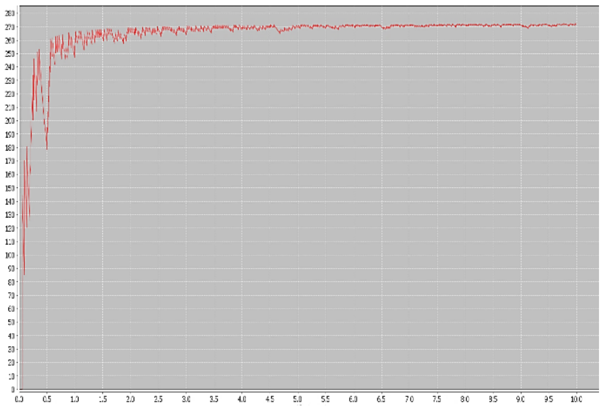

Fig. 16: Throughput in Wormhole scenario.

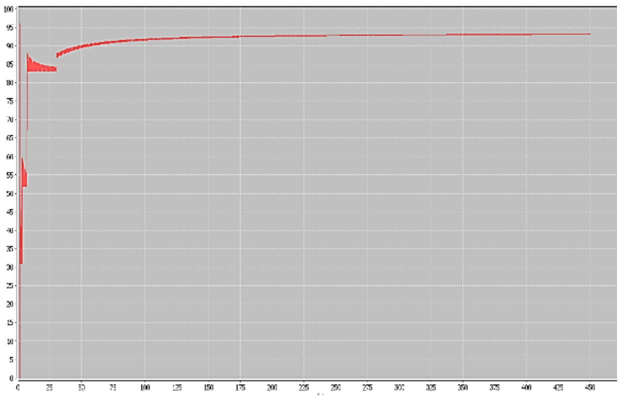

Fig. 17: Throughput in clear scenario.

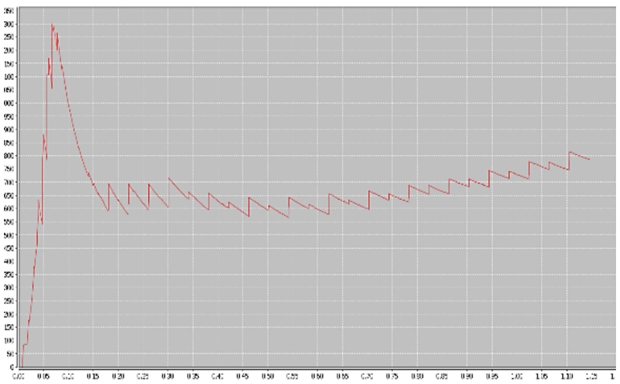

Fig. 18: Throughput in node scan scenario.

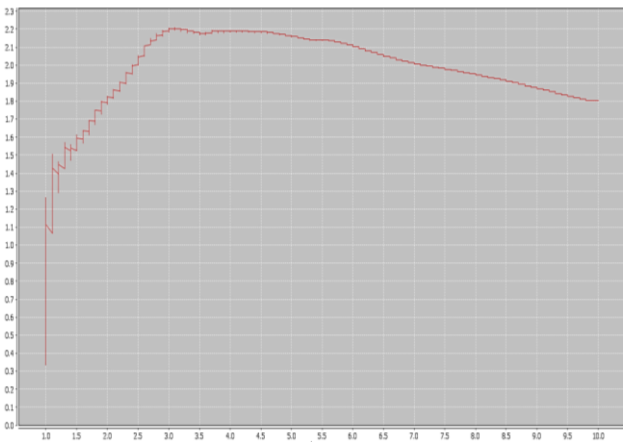

Fig. 19: End to end delay in the clear scenario.

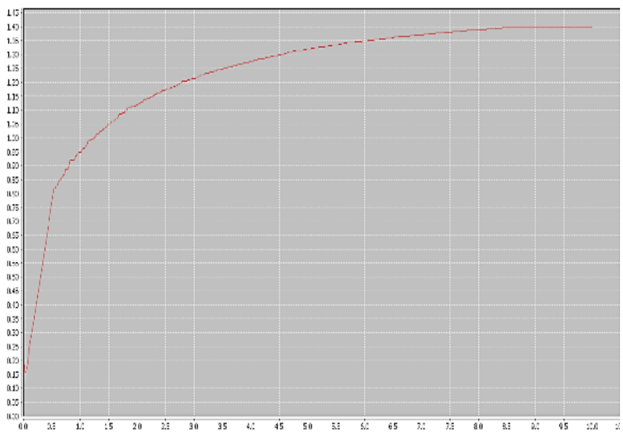

Fig. 20: End to end delay in Wormhole scenario.

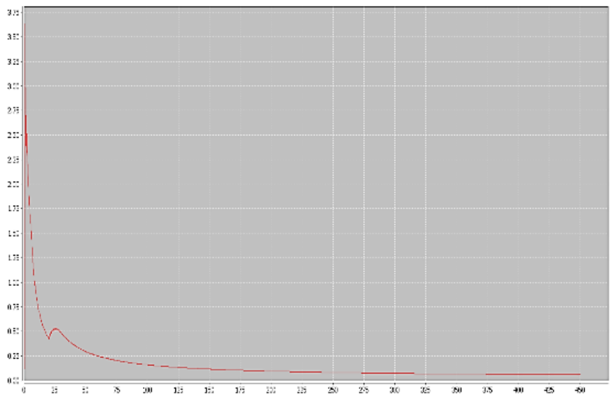

Fig. 21: End to end delay in the clear scenario.

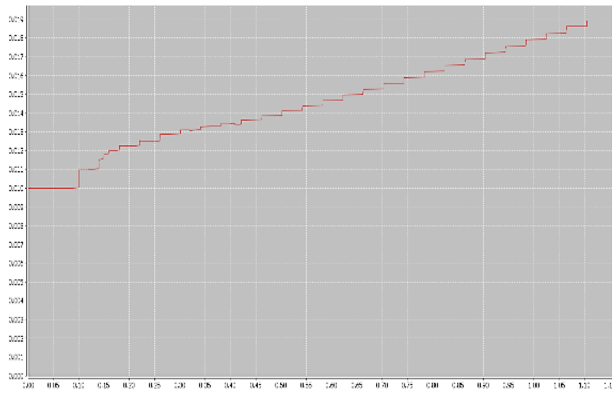

Fig. 22: End to end delay in nodes scan scenario.

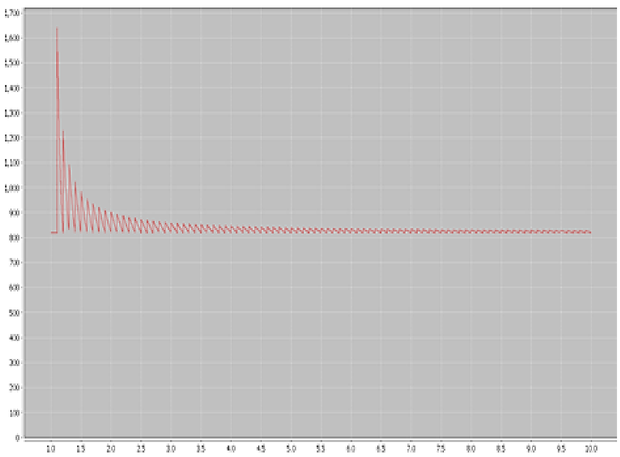

Fig. 23: Sent packet in clear scenario.

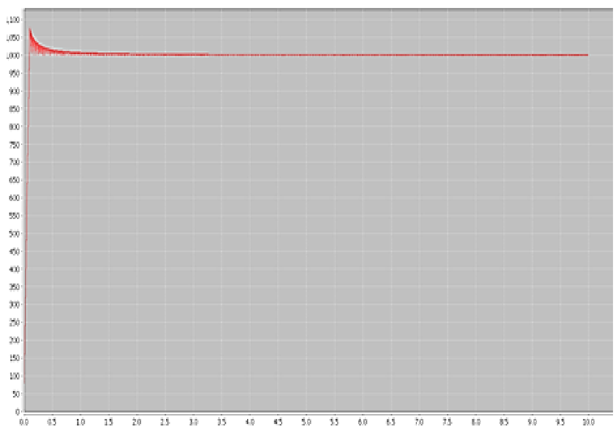

Fig. 24: Sent packet in Wormhole scenario.

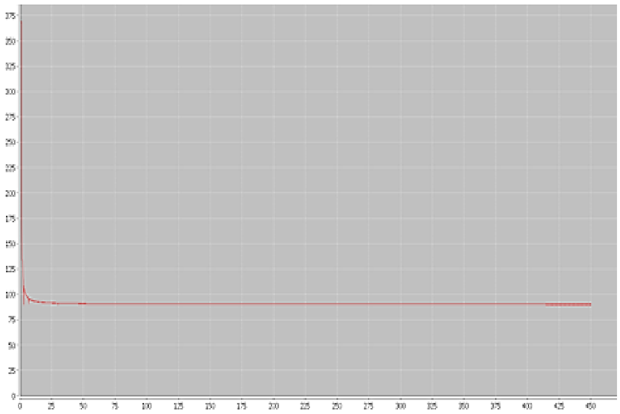

Fig. 25: Sent packet in Black hole scenario.

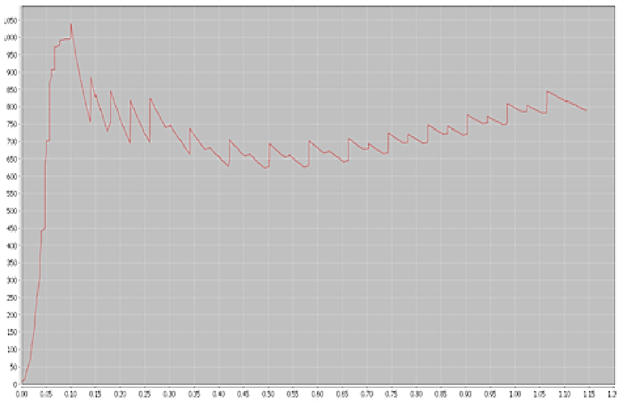

Fig. 26: Sent packet in nodes scan scenario.

Table 10: Evaluation of the simulation scenarios

Network scenario	AVG of THR	RPKT	PDR	NRL	AVG of DLY
Clear scenario	2174.19	5399	539900	0.61	8996.44
Wormhole scenario	1354.91	6489	648900	0.05	6667
Black hole scenario	2604.68	65504	6550400	0.03	308981
Malicious node scenario	680.42	32745	409312	0.03	66009.1
Scan scenario	2875.85	1375	1556.82	0.03	18.8681

According to Table 10, the average throughput in a clear scenario has been equaled to 2174.19 kbps. Figs. 15-18 described that the throughput ratio has increased in total time. On the other hand, in the wormhole attack, it showed that after 1 unit of the simulation time, we had stable traffic in the time. In the scanning scenario, the throughput has been increased. So according to the clear scenario and malicious scenarios we can predict the attacks. Table 10 and Figs. 19-22, described that the average clear scenario has been about 8996.44 kbps. After half of the simulation time, the end-to-end delay ratio has been decreased. In the wormhole scenario, this rate has been increased and in the Black hole, it has been strongly decreased. We have the same scenario with sent packet parameters. Now, based on the information of Table 10 and also Figs. 23-26, we can detect the attacks on base station units with the Splunk or other SIEM monitoring management's software.

State-of-the-Art Intrusion Detection Techniques for New Technologies

Nowadays, researchers encounter buzzwords: deep learning [131], Internet of Things (IoT) [132], [133], Safeguard in WSN, cybersecurity attacks [134], security tenets [134] etc. Unfortunately, besides developing the aforementioned technologies, cybersecurity attacks have been extended. So, different safeguard techniques were recently introduced in the literature to obviate the troubles.

In this vein, Mohamed Saied et al. [135] recently presented a survey study on how to enhance intrusion detection systems in the IoT domain by incorporating artificial intelligence approaches. To obviate problems such as blackhole and sinkhole attacks in healthcare wireless sensor networks, an efficient IDS system was recently presented by Webber et al. in 2023 [136]. This method tries to guarantee the security of sensitive data packets in the early stages of the healthcare system. One of the recently applicable technologies is Internet of Vehicles which is used in smart transportation. It is also subjected to different wireless attacks. To mitigate the problem in such networks, an intrusion detection framework was proposed by Selim Korium et al. in 2024 [137].

The authors utilized machine learning techniques such as feature selection methods to detect security attacks and have suitable countermeasures. Tseng and Change in 2023 [131] proposed a deep learning neural network-based ensemble binary detection model for recognizing the multi-level class intrusion detection attacks. A defense mechanism for intrusion detection and prevention models was proposed by incorporating the ensemble learning model [138]. A computational intelligence-based on particle swarm optimization (PSO) algorithm was recently proposed in the literature to solve intrusion detection problems in IoT/5G/Wi-Fi wireless scenarios [139].

Table 11 is dedicated to comparing state-of-the-art technologies that utilize intrusion detection methods to solve the intrusion challenges. This table compares literature based on their innovations, subject challenges, how to solve them, utilized methods, and future direction. It paves the way for further processing to obviate existing shortcomings.

Table 11: Comparison of literature in terms of prominent factors

Author(s) /Ref. /Year	Innovation	Subject Challenge	Used method/solution	Future Direction
Tseng & Change [131], 2023;	It uses data enhancement and ensemble model to improve detection accuracy.	Limited number of attack detection in distributed wireless systems	It utilizes machine learning techniques such as ensemble binary model and convert it to multi-class detection model.	Presenting a comprehensive ensemble model with the most accuracy prediction model to detect different kinds of attacks
Jayanayudu & Sudhir [133], 2023;	It engages meta-heuristic algorithm to make a balance between malicious detection and electricity consumption.	Malicious detection	It makes a safeguard against wireless attacks in IoT WSN environment.	Presenting an efficient multi-objective algorithm which make tread-off between conflicting objectives
Webber et al. [136], 2023;	Presenting an innovated intrusion detection model with high accuracy and minimum data loss	Keeping network quality of service (QoS) level along with malicious detection in early stages	It uses Minkowski K-means clustering method to define meaningful similarity.	Presenting an ensemble model which engages the advantages of existing classifiers to decrease detection error
Korium et al. [137], 2023;	It present low-execution time malicious detectors by utilizing ML methods.	Malicious detection with low time complexity	It uses different datasets and use feature selection methods to detect malic behaviors as soon as possible.	Presenting a comprehensive detection model which can efficiently works of complicated datasets
Ntizikira et al. [138], 2024;	It present a detection system framework which detects malic behaviors in different IoT applications' attacks.	Intrusion detection problem in diverse IoT applications	It utilizes different heuristic to improve detection accuracy.	Presenting a light weight deep learning algorithm which makes a trade-off between time complexity and classification accuracy
Sivagami et al. [139], 2023;	It present network intrusion detection system (NIDS) by utilizing PSO algorithm.	Identifying malicious activity	It utilizes hybridizing ML algorithm and PSO optimizer to improve presented system's performance.	Presenting an ensemble of deep learning algorithms to improve detection accuracy

Results and Discussion

Since the security tenets are a vital non-functional requirement for mission-critical applications in the WSN context, a review of the intrusion detection system in such vulnerable networks is necessary. The reason why the current survey study was conducted is to investigate solutions presented in the literature for finding existing challenges and potential solutions for further processing. The subjective classification has been done and the literatures have been analyzed based on the proposed classifications. The existing challenges and prominent considerations were proposed for improving the current schemes in the WSN context. On the other hand, since these kinds of networks have limited resources, especially in power provisions, the energy-efficient IDS systems are favorable. To this end, ML techniques are beneficial. As a result of the low energy consumption requirements in the sensor network, the use of a hierarchical model will be useful. This means that the network must be divided into clusters, and each of them will have a cluster head. Accordingly, energy consumption will be minimized by avoiding the requirement for all nodes to send data to the base station. Also, intrusion detection algorithms with high energy consumption have been implemented only on the cluster head leading to energy storage and ultimately increasing the life of the network. Intrusion detection energy consumption has been an important point from a security point of view. The WSN consumes a lot of energy by sensing events, processing the information that has been collected, and transmitting the resulting data. Therefore, an IDS has been required to use as little energy as possible to store the energy necessary for operation in the WSN. This research also paves the way of interested researchers to find existing challenges and shortcomings for further processing.

Author Contributions

Dr. Mirsaeid Hosseini Shirvani was the supervisor of the current research plan. He sketched the research framework and the roadmap. Also, he analyzed the results and tabulated the outcome derived from excerpted literatures. In this line, Amir Akbarifar searched in authentic journals to gather all relevant papers. In addition to, he prepared the blueprint of the research plan. He and his supervisor cooperatively summed up the work.

Acknowledgment

This work is completely self-supporting, thereby no any financial agency's role is available.

Conflict of Interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Abbreviation

WSN	Wireless Sensor Network
AVG	Average
DLY	Delay
THR	Throughput
PKT	Packet
PDR	Packet Delivery Ratio
RPKT	Received Packets
NRL	Normalized Routing Load

References

[1] F. Liu, J. Xu, L. Zhang et al., "DESNN algorithm for communication network intrusion detection," Wireless Pers. Commun., 126: 1705-1720, 2022.

[2] F. Junior, N. Silva, A. Guelfi, S. Takeo Kofuji, "IoT6Sec: reliability model for Internet of Things security focused on anomalous measurements identification with energy analysis," Wireless Netw., 25: 1533-1556, 2019.

[3] T. Do-Dac, K. Ho-Van, "Energy harvesting cognitive radio networks: security analysis for Nakagami-m fading," Wireless Netw., 27: 1561-1572, 2021.

[4] U. Ghugar, J. Pradhan, "NL-IDS: Trust based intrusion detection system for network layer in wireless sensor networks," in Proc. 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC): 512-516, 2018.

[5] B. J. Santhosh Kumar, S. Sinha, "An intrusion detection and prevention system against DOS attacks for internet-integrated WSN," in Proc. 2022 7th International Conference on Communication and Electronics Systems (ICCES): 793-797, 2022.

[6] A. P. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, H. C. Wong, "Decentralized intrusion detection in wireless sensor networks," in Proc. 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks (Q2SWinet '05), ACM Press: 16-23, 2005.

[7] M. Meisel, V. Pappas, L. Zhang, "A taxonomy of biologically inspired research in computer networking," Comput. Network, 54(6): 901-916, 2010.

[8] K. Chaitanya, A. Ghosh, "Analysis of Denial-of-Service attacks on Wireless Sensor networks using simulation, IT Security for the Next Generation - European Cup 2011: 1-13, 2010.

[9] R. C. Chen, C. F. Hsieh, Y. F. Huang, "A new method for intrusion detection on hierarchical wireless sensor networks", in Proc. ACM ICUIMC-09, 2009.

[10] S. Otoum, B. Kantarci, H. T. Mouftah "A novel ensemble method for advanced intrusion detection in wireless sensor networks," in Proc. 2020 IEEE International Conference on Communications (ICC 2020): 1-6, 2020.

[11] M. Aloqaily, S. Otoum, I. Al Ridhawi, Y. Jararweh, "An intrusion detection system for connected vehicles in smart cities," Ad Hoc Networks, 90: 101842, 2019.

[12] S. Otoum, B. Kantarci, H. T. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection, "IEEE Networking Lett., 1(2): 68-71, 2019.

[13] I. Butun, , S. D. Morgera, R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," IEEE Commun. Surv. Tutorials, 16(1): 266-282, 2014.

[14] M. Hosseini Shirvani, A. Akbarifar, "Anomaly-based detection of blackhole attacks in WSN and MANET utilizing quantum-metaheuristic algorithms," J.Commun. Eng., 9(1): 77-92, 2020.

[15] Y. Maleh, A. Ezzati, "A review of security attacks and intrusion detection schemes in wireless sensor networks," arXiv preprint arXiv:1401.1982, 2014.

[16] S. Binitha, S. S. Sathya, "A survey of bio inspired optimization algorithms," Int. J. Soft Comput. Eng., 2(2): 137-151, 2012.

[17] R. Fu et al., "Biologically inspired anomaly detection for hierarchical wireless sensor networks," J. Networks 7(8): 1214-1219, 2012.

[18] M. Hosseini Shirvani, A. Akbarifar, "A comparative study on anonymizing networks: TOR, I2P, and riffle networks comparison, J. Electr. Comput. Eng. Innovations (JECEI), 10(2): 259-272, 2022.

[19] E. Baraneetharan, "Role of machine learning algorithms intrusion detection in WSNs: a survey," J. Inf. Technol., 2(03): 161-173, 2020.

[20] I. Butun, S. D. Morgera, R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," IEEE Commun. Surv. Tutorials, 16(1): 266-282, 2013.

[21] X. Tan, S. Su, Z. Huang, X. Guo, Z. Zuo, X. Sun, L. Li, "Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm," Sensors, 19(1): 203, 2019.

[22] C. C. Su, K. M. Chang, Y. H. Kuo, M. F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks," in Proc. IEEE Wireless Communications and Networking Conference, 2005.

[23] A. A. Strikos, "A full approach for intrusion detection in wireless sensor networks," School of Information and Communication Technology, KTH, Stockholm, Sweden 16453, 2007.

[24] Y. Otoum, D. Liu, , A. Nayak, "DL-IDS: a deep learning–based intrusion detection framework for securing IoT," Trans. Emerg. Telecommun. Technol., 33(3): e3803, 2022.

[25] N. Moustafa, B.Turnbull, K. K. R. Choo, "An ensemble intrusion detection technique based on proposed statistical flow features

for protecting network traffic of internet of things," IEEE Internet Things J., 6(3): 4815-4830, 2018.

[26] M. Hosseini Shirvani, A. Akbarifar, A. Nazokkar, "Reliability non-functional requirement evaluation in mission-critical systems with an architectural strategy for future systems," Int. J. Comput. Appl., 46(4): 227-251, 2024.

[27] A. Aldweesh, A. Derhab, A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy, and open issues," Knowledge-Based Syst., 189: 105124 2020.

[28] G. Marín, P. Casas, G. Capdehourat, "Rawpower: Deep learning based anomaly detection from raw network traffic measurements," in Proc. the ACM SIGCOMM 2018 Conference on Posters and Demos: 75-77, 2018.

[29] R. Sharma, V. A. Athavale, "Survey of intrusion detection techniques and architectures in wireless sensor networks," Int. J. Adv. Networking Appl., 10(4): 3925-3937, 2019.

[30] K. Haseeb, I. Ud Din, A. Almogren, N. Islam, "An energy efficient and secure IoT-based WSN framework: An application to smart agriculture," Sensors, 20(7): 2081, 2020.

[31] W. Zhang, D. Han, K. C. Li, F. Massetto, "Wireless sensor network intrusion detection system based on MK-ELM," Soft Comput., 24(16): 12361-12374, 2020.

[32] S. Shen, G. Yue, Q. Cao, F. Yu, "A survey of game theory in wireless sensor networks security," J. Networks, 6(3): 521, 2011.

[33] G. Zhang, T. Wang, G. Wang, A. Liu, W. Jia, "Detection of hidden data attacks combined fog computing and trust evaluation method in sensor-cloud system," Concurrency Comput. Pract. Exper., 33(7): 1-1, 2021.

[34] A. Agah, K. Basu, , S. K. Das, "Preventing DoS attack in sensor networks: a game theoretic approach," in Proc. IEEE International Conference on Communications (ICC 2005), 5: 3218-3222, 2005.

[35] L. Yang, D. Mu, X. Cai, "Preventing dropping packets attack in sensor networks: A game theory approach," Wuhan Univ. J. Nat. Sci., 13(5): 631-635, 2008.

[36] M. A. Khan, S. U. Jan, J. Ahmad., S. S. Jamal, A. A. Shah, N. Pitropakis, W. J. Buchanan, "A Deep learning-based intrusion detection system for mqtt enabled iot," Sensors, 21: 7016, 2021.

[37] S. Rajasegarar, C. Leckie, M. Palaniswami, J. C. Bezdek, "Distributed anomaly detection in wireless sensor networks", in Proc. 10th IEEE Singapore International Conference on Communication systems, 2006.

[38] V. Kelli, V. Argyriou, T. Lagkas, G. Fragulis, E. Grigoriou, , & P. Sarigiannidis, P. IDS for industrial applications: a federated learning approach with active personalization. Sensors, 21(20), 6743 (2021)

[39] M. A Almaiah, "A new scheme for detecting malicious attacks in wireless sensor networks based on blockchain technology," in Artificial Intelligence and Blockchain for Future Cybersecurity Applications: 217-234. Springer, Cham 2021.

[40] M. Khudadad, Z. Huang, "Novel intrusion detection methods for security of wireless sensor network, "J. Fundam. Appl. Sci., 10(2S): 173-189, 2018.

[41] I. Almomani, A. Alromi, "Integrating software engineering processes in the development of efficient intrusion detection systems in wireless sensor networks," Sensors, 20(5): 1375, 2020.

[42] S. Subbiah , K. S. M. Anbananthen, S. Thangaraj, S. Kannan, D. Chelliah, "Intrusion detection technique in wireless sensor network using grid search random forest with Boruta feature selection algorithm," J. Commun. Networks, 24(2): 264-273, 2022.

[43] W. Wang, M. Chatterjee, K. Kwiat, "Coexistence with malicious nodes: A game theoretic approach," in Proc. 2009 International Conference on Game Theory for Networks: 277-286, 2009.

[44] T. Sherasiya, H. Upadhyay, H. B. Patel, "A survey: Intrusion detection system for internet of things," Int. J. Comput. Sci. Eng. (IJCSE), 5(2): 91-98, 2016.

[45] X. Jia, Q. Feng,T. Fan, Q. Lei, "Rfid Technology And Its Applications In Internet Of Things (Iot)," In Proc. IEEE 2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet): 1282-1285, 2012.

[46] C. Jun, C. Chi, "Design of complex event-processing IDS in internet of things," in Proc. IEEE 2014 sixth International Conference on Measuring Technology and Mechatronics Automation: 226-229, 2014.

[47] A. Alsadhan, N. Khan, "A proposed optimized and efficient intrusion detection system for wireless sensor network," Int. J. Comput. Inf. Eng., 7(12): 1621-1624, 2013.

[48] Y. El Mourabit, A. Toumanari, A. Bouirden, H. Zougagh, R. Latif, "Intrusion detection system in Wireless Sensor Network based on mobile agent," in Proc. Second World Conference on Complex Systems (WCCS): 248-251, 2014.

[49] G. Sandhya, A. Julian, "Intrusion detection in wireless sensor network using genetic K-means algorithm," in Proc. 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies: 1791-1794, 2014.

[50] S. Athmani, D. E. Boubiche, A. Bilami, "Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs," in Proc. 2013 World Congress on Computer and Information Technology (WCCIT): 1-5, 2013.

[51] A. B. Karuppiah, J. Dalfiah, K. Yuvashri, S. Rajaram, S. Pathan, "A novel energy-efficient sybil node detection algorithm for intrusion detection system in wireless sensor networks," in proc. 2014 3rd International Conference on Eco-friendly Computing and Communication Systems: 95-98, 2014.

[52] D. Harini, N. Balakrishnan, A. P. Renold, "Distributed detection of flooding and gray hole attacks in wireless sensor network," in Proc. 2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM): 178-184, 2015.

[53] F. Fazlic, S. A.Hashemi, A. Aletic, A. Abd Almisreb, S. M. Norzeli, N. M. Din, "A survey on security in wireless sensor network," Southeast Eur. J. Soft Comput., 8(1), 2019.

[54] L. Arnaboldi, C. Morisset, "A review of intrusion detection systems and their evaluation in the IoT," arXiv preprint arXiv:2105.08096, 2021.

[55] A. Le, J. Loo, Y. Luo, A. Lasebae, "Specification-based IDS for securing RPL from topology attacks," in Proc. 2011 IFIP Wireless Days (WD): 1-3, 2011.

[56] I. Krontiris, T. Dimitriou F. C. Freiling, "Towards intrusion detection in wireless sensor networks," in Proc. 13th European Wireless Conference, 2007.

[57] H. Esquivel-Vargas, M. Caselli, A. Peter, "Automatic deployment of specification-based intrusion detection in the BACnet protocol," in Proc. the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy: 25-36, 2017.

[58] H. Bostani, M. Sheikhan, "Hybrid of anomaly-based and specification-based ids for internet of things using unsupervised opf based on mapreduce approach," Comput. Commun., 98: 52-71 2017.

[59] Y. Otoum, D. Liu, A. Nayak, "DL-IDS: a deep learning–based intrusion detection framework for securing IoT," Trans. Emerg. Telecommun. Technol., 33(3): 3803, 2022.

[60] E. Ngai, J. Liu, M. Lyu, "On the intruder detection for sinkhole attack in wireless sensor networks," in Proc. 2006 IEEE International Conference on Communications , 2006.

[61] S. S. Doumit, D. P. Agrawal, “Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks,” in Proc. IEEE Military Communications Conference (MILCOM’03), 2003.

[62] J. P. Amaral, L. M. Oliveira, J. J. P. C. Rodrigues, G. Han, L. Shu, “Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks,” in Proc. IEEE International Conference on Communications (ICC): 1796-1801, 2014.

[63] J. M. R. Danda, C. Hota, “Attack identification framework for IoT devices,” in Advances in Intelligent Systems and Computing, 434: 505-513, Information Systems Design and Intelligent Applications, Springer, 2016.

[64] H. Sedjelmaci, S. M. Senouci, "Efficient and lightweight intrusion detection based on nodes' behaviors in wireless sensor networks," in Proc. Global Information Infrastructure Symposium - GIIS 2013: 1-6, 2013.

[65] K. M. J. Haataja, New efficient intrusion detection and prevention system for Bluetooth networks,” in Proc. the 1st International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications, 2010.

[66] T. OConnor, D. Reeves, “Bluetooth network-based misuse detection,” in Proc. Annual Computer Security Applications Conference (ACSAC): 377-391, 2008.

[67] L. Wallgren, S. Raza, T. Voigt, “Routing attacks and countermeasures in the RPL-Based internet of things,” Int. J. Distrib. Sens. Netw., 9(8), 2013.

[68] V. Garcia-Font, C. Garrigues, H. Rifà-Pous, “Attack classification schema for smart city WSNs,” Sensors, 17(4):771, 2017.

[69] T. K. Buennemeyer, T. M. Nelson, L. M. Clagett, J. P. Dunning, R. C. Marchany, J. G. Tront, "Mobile device profiling and intrusion detection using smart batteries," in Proc. 41st Annual Hawaii International Conference on System Sciences (HICSS 2008) :296-296, 2008.

[70] I. Onat, A. Miri, “A real-time node-based traffic anomaly detection algorithm for wireless sensor networks,” in Proc. 2005 Systems Communications, 2005.

[71] D. Midi, A. Rullo, A. Mudgerikar, E. Bertino, “Kalis—A system for knowledge-driven adaptable intrusion detection for the Internet of Things,” in Proc. 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS): 656-666, 2017.

[72] T. Lee, C. Wen, L. Chang, H. Chiang, M. Hsieh, “A lightweight intrusion detection schemebased on energy consumption analysis in 6LowPAN,” in Advanced Technologies, Embedded and Multimedia for Human-centric Computing, 1205-1213 2014.

[73] S. Raza, L. Wallgren, T. Voigt, “SVELTE: Real-time intrusion detection in the Internet of Things,” Ad Hoc Networks, 11(8): 2661-2674, 2013.

[74] T. Matsunaga, K. Toyoda, L. Sasase, “Low false alarm rate RPL network monitoring system by considering timing inconstancy between the rank measurements,” in Proc. 2014 11th International Symposium on Wireless Communications Systems (ISWCS): 427-431, 2014.

[75] G. Han, J. Jiang, W. Shen, L. Shu, J. Rodrigues, “IDSEP: a novel intrusion detection scheme based on energy prediction in cluster-based wireless sensor networks,” IET Inf. Secur., 7(2):97-105, 2013.

[76] S. Wu Kim, “Physical integrity check in cooperative relay communications,” IEEE Trans. Wireless Commun., 14(11): 6401-6413, 2015.

[77] R. Ahmad, I. Alsmadi, W. Alhamdani, L. Tawalbeh, “A comprehensive deep learning benchmark for IoT IDS,” Comput. Secur., 114: 102588, 2022.

[78] L. Besson, P. Leleu, "A distributed intrusion detection system for ad-hoc wireless sensor networks: The AWISSENET distributed intrusion detection system," in Proc. 2009 16th International Conference on Systems, Signals and Image Processing: 1-3, 2009.

[79] D. Summerville, K. M Zach, Y. Chen, “Ultra-lightweight deep packet anomaly detection for internet of things devices,” in Proc. 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC): 1-8, 2015.

[80] M. Talukder, S. Sharmin, S. Uddin et al., “MLSTL-WSN: machine learning-based intrusion detection using SMOTETomek in WSNs,” Int. J. Inf. Secur., 2024.

[81] E. Cho, J. Kim, C. Hong, “Attack model and detection scheme for botnet on 6LoWPAN,” in Proc. Asia-Pacific Network Operations and Management Symposium, 515-518, 2009.

[82] D. Shreenivas, S. Raza, T. Voigt, “Intrusion detection in the RPL-connected 6LoWPAN Networks,” in Proc. 3rd ACM International Workshop on IoT Privacy, Trust, and Security: 31-38 2017.

[83] Z. Banković, José M. Moya, A. Araujo, J. Goyeneche, “Intrusion detection in sensor networks using clustering and immune systems,” in Proc. 10th international conference on Intelligent data engineering and automated learning (IDEAL'09): 408-415, 2009.

[84] D. Hadžiosmanović, R. Sommer, E. Zambon, P. Hartel, “Through the eye of the PLC: semantic security monitoring for industrial processes,” in Proc. 30th Annual Computer Security Applications Conference: 126-135, 2014.

[85] D. Oh, D. Kim, W. Ro, “A malicious pattern detection engine for embedded security systems in the Internet of Things,” Sensors, 14(12): 24188-24211, 2014.

[86] H. Sedjelmaci, S. Mohammed Senouci, M. Al-Bahri, “A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology,” in Proc. 2016 IEEE International Conference on Communications (ICC): 1-6, 2016.

[87] X. Song, G. Chen, X. Li, “A weak hidden Markov Model based intrusion detection method for wireless sensor networks,” in Proc. 2010 International Conference on Intelligent Computing and Integrated Systems: 887-889, 2010.

[88] L. Deng, D. Li, X. Yao, D. Cox, H. Wang, “Mobile network intrusion detection for IoT system based on transfer learning algorithm,” Cluster Comput., 1-16, 2018.

[89] L. Liu, B. Xu, X. Zhang, X. Wu, “An intrusion detection method for internet of things based on suppressed fuzzy clustering,” EURASIP J. Wireless Commun. Networking, 113, 2018.

[90] A. Agah, S. K. Das, K. Basu, M. Asadi, “Intrusion detection in sensor networks: A non-cooperative game approach,” in Proc. 3rd IEEE International Symposium on Network Computing and Applications (NCA’04): 343-346, 2004.

[91] A. Agah, S. K. Das, “Preventing DoS attacks in wireless sensor networks: A repeated game theory approach,” Int. J. Network Secur., 5(2): 145-153, 2007.

[92] K. Yadav, A. Srinivasan, “iTrust: an integrated trust framework for wireless sensor networks,” in Proc. the 2010 ACM Symposium on Applied Computing: 1466-1471, 2010.

[93] C. Cervantes, D. Poplade, M. Nogueira, A. Santos, “Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things,” in Proc. 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM): 606-611, 2015.

[94] A. Khan, Z. Herrmann, “A trust based distributed intrusion detection mechanism for internet of things,” in Proc. 2017 IEEE 31st International Conference on Advanced Information Networking and Applications (AINA): 1169-1176, 2017.

[95] T. Jiang, G. Wang, H. Yu, "A dynamic intrusion detection scheme for cluster-based wireless sensor networks," in Proc. World Automation Congress 2012: 259-261, 2012.

[96] A. Arrington, L. Barnett, R. Rufus, A. Esterline, "Behavioral modeling intrusion detection system (bmids) using internet of things (iot) behavior-based anomaly detection via immunity-inspired algorithms," in Proc. 2016 25th International Conference on Computer Communication and Networks (ICCCN): 1-6, 2016.

[97] C. Liu, J. Yang, R. Chen, Y. Zhang, J. Zeng, "Research on immunity-based intrusion detection technology for the internet of things," in Proc. 2011 Seventh International Conference on Natural Computation, 1: 212-216, 2011.

[98] V. Bhuse, A. Gupta, "Anomaly intrusion detection in wireless sensor networks," J. High Speed Networks, 15(1): 33-51, 2006.

[99] H. Arolkar, S. Sheth, V. Tamhane, "Ant colony based approach for intrusion detection on cluster heads in WSN," in Proc. ICCCS: 523-526, 2011.

[100] A. Hassanzadeh, R. Stoleru, "Towards optimal monitoring in cooperative ids for resource constrained wireless networks," in Proc. 20th International Conference on Computer Communications and Networks (ICCCN): 1-8, 2011.

[101] I. Onat, A. Miri, "An intrusion detection system for wireless sensor networks," in Proc. IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2005.

[102] B. Stelte, G Rodosek, "Thwarting attacks on zigbee-removal of the killerbee stinger," in Proc. the 9th International Conference on Network and Service Management (CNSM): 219-226, 2013.

[103] N. Kumar, E. Nigussie, R. K. Kanth, S. Virtanen, J. Isoaho, "Distributed internal anomaly detection system for internet-of-things," in Proc. 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC): 319-320, 2016.

[104] T. Luo, S. Nagarajan, "Distributed anomaly detection using autoencoder neural networks in wsn for iot," in Proc. 2018 IEEE International Conference on Communications (ICC): 1-6, 2018.

[105] O. Can, O. K. Sahingoz, "A survey of intrusion detection systems in wireless sensor networks," in Proc. 2015 6th International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO): 1-6, 2015.

[106] A. Amouri, V. Alaparthy, S. Morgera, "Cross layer-based intrusion detection based on network behavior for IoT," in Proc. 2018 IEEE 19th Wireless and Microwave Technology Conference (WAMICON): 1-4, 2018.

[107] L. Coppolino, S. D. Antonio, A. Garofalo, L. Romano, "Applying data mining techniques to intrusion detection in wireless sensor networks," in Proc. 2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing: 247-254, 2013.

[108] N. Abhishek, T. Lim, B. Sikdar, A. Tandon, "An intrusion detection system for detecting compromised gateways in clustered IoT networks," in Proc. 2018 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR): 1-6, 2018.

[109] S. Rajasegarar, C. Leckie, M. Palaniswami, J. C. Bezdek, "Quarter sphere based distributed anomaly detection in wireless sensor networks," in Proc. IEEE ICC '07, 2007.

[110] S. Misra, P. Venkata, H. Agarwal, A. Saxena, M. S. Obaidat, "A learning automata based solution for preventing distributed denial of service in Internet of things," in Proc. 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing: 114-122, 2011.

[111] Y. Fu, Z. Yan, J. Cao, O. Koné, X. Cao, "An automata based intrusion detection method for internet of things," Mobile Inf. Syst., 2017.

[112] C. Wang, T. Feng, J. Kim, G. Wang, W. Zhang, "Catching packet droppers and modifiers in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., 23(5): 835-843, 2012.

[113] F. Bao, R. Chen, M. J. Chang, J. H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trustbased routing and intrusion detection," IEEE Trans. Netw. Serv. Manag., 9(2): 169-183, 2012.

[114] S. Etalle, "Network monitoring of industrial control systems: The lessons of security matters, in Proc. ACM Workshop on Cyber-Physical Systems Security & Privacy: 1–1, 2019.

[115] N. Kaur, P. Rattan, "A critical review of intrusion detection systems in WSN: challenges & future directions," Ann. Rom. Soc. Cell Biol., 25(4): 3020-3028, 2021.

[116] T. Wang, Z. Liang, C. Zhao, "A detection method for routing attacks of wireless sensor network based on fuzzy C-means clustering," in Proc. 6th International Conference on Fuzzy Systems and Knowledge Discovery: 445-449, 2009.

[117] K. Q. Yan, S. C. Wang, C. W. Liu, "A hybrid intrusion detection system of cluster-based wireless sensor networks," in Proc. International Multi Conference of Engineers and Computer Scientists: 1, 2009.

[118] N. Chitradevi, V. Palanisamy, K. Baskaran, S. Prabeela, "Efficient distributed clustering-based anomaly detection algorithm for sensor stream in clustered wireless sensor networks," Eur. J. Sci. Res., 54(4):484-498, 2011.

[119] M. Chauhan, M. Agarwal, "Study of various intrusion detection systems: A Survey," in Smart and Sustainable Intelligent Systems: 355-372, 2021.

[120] Z. Ahmad, A. Shahid Khan, , C. Shiang, J. Abdullah, F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Trans. Emerg. Telecommun. Technol., 32(1): e4150, 2021.

[121] A. A. Anitha, L. Arockiam, "A review on intrusion detection systems to secure IoT networks, "Int. J. Comput. Networks Appl., 9(1): 38-50, 2022.

[122] Y. Farooq, H. Beenish, M. Fahad, "Intrusion detection system in wireless sensor networks-a comprehensive survey," in Proc. 2019 Second International Conference on Latest trends in Electrical Engineering and Computing Technologies (INTELLECT): 1-6, 2019.

[123] N. Singh, D. Virmani, X. Z Gao,"A fuzzy logic-based method to avert intrusions in wireless sensor networks using WSN-DS dataset," Int. J. Comput. Intell. Appl., 19(03): 2050018, 2020.

[124] M. Wazid, A. K. Das, S. Kumari, M. K. Khan, "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks," Secur. Commun. Networks, 9(17): 4596-4614, 2016.

[125] G. Liu, H. Zhao, F. Fan, , Liu, G, Q. Xu, , S. Nazir, "An enhanced intrusion detection model based on improved kNN in WSNs," Sensors, 22(4): 1407, 2022.

[126] B. Hasan, S. Alani, M. A. Saad, "Secured node detection technique based on artificial neural network for wireless sensor network," Int. J. Electr. Comput. Eng., 11(1): 2088-8708, 2021.

[127] W. Huai-bin, Y. Zheng, W. Chun-dong, "Intrusion detection for wireless sensor networks based on multi-agent and refined clustering," in Proc. International Conference on Communications and Mobile Computing: 450-454, 2009.

[128] S. Siripanadorn, W. Hattagam, N. Teaumroong, "Anomaly detection in wireless sensor networks using self-organizing map and wavelets," Int. J. Common. 4(3):74-83, 2010.

[129] M. Sa, M. R. Nayak, A. K. Rath, "A simple agent based model for detecting abnormal event patterns in a distributed wireless sensor networks," Int. J. Comput. Sci. Secur., 4(6):580-588, 2011.

[130] H. Sedjelmaci, M. Feham, "Novel hybrid intrusion detection system for clustered wireless sensor network," Int. J. Netw. Secur. Appl., 3(4):1-14, 2011.

[131] C. Henry Tseng, Y. Chang, "EBDM: Ensemble binary detection models for multi-class wireless intrusion detection based on deep neural network," Comput. Secur., 133: 103419, 2023.

[132] M. Hosseini Shirvani, M. Masdari, "A survey study on trust-based security in internet of things: challenges and issues, Internet Things, 100640, 2022.

[133] D. Jayanayudu, A. C. Sudhir, "Shuffled frog leap and ant lion optimization for intrusion detection in iot-based WSN," in Proc. Fourth International Conference on Computer and Communication Technologies, 606, 2023.

[134] M. Hosseini Shirvani, A. M. Rahmani, A. Sahafi, "An iterative mathematical decision model for cloud migration: A cost and security risk approach," Softw. Pract. Exper., 2017: 1-37, 2017.

[135] M. Saied, S. Guirguis, M. Madbouly, "Review of artificial intelligence for enhancing intrusion detection in the internet of things," Eng. Appl. Artif. Intell., 127(A): 107231, 2024.

[136] L. Webber, A. Arafa, A. Mehbodniya, S. Karupusamy, B. Sha, A. Dahiya, P. Kanani, "An efficient intrusion detection framework for mitigating blackhole and sinkhole attacks in healthcare wireless sensor networks," Comput. Electr. Eng., 111: 108964, 2023.

[137] M. S. Korium, M. Saber, A. Beattie, A. Narayanan, S. Sahoo, P. H. J. Nardelli, "Intrusion detection system for cyberattacks in the Internet of Vehicles environment," Ad Hoc Networks, 153: 103330, 2024.

[138] E. Ntizikira, L. Wang, J. Chen, K. Saleem, "Honey-block: Edge assisted ensemble learning model for intrusion detection and prevention using defense mechanism in IoT," Comput. Commun., 214: 1-17, 2024.

[139] V. Sivagaminathan, M. Sharm, S. Henge, "Intrusion detection systems for wireless sensor networks using computational intelligence techniques," Cybersecurity, 6: 27, 2023.

Biographies

Mirsaeid Hosseini Shirvani received his B.Sc., M.Sc., and Ph.D. all in Computer Software Engineering Systems at Universities in Tehran, Iran. He has been teaching miscellaneous computer courses in several universities in Mazandaran province of IRAN since 2001. He also published several papers in authentic and worldwide well-reputed journals. Currently, he serves as a Professor in the Computer Engineering Department at IAU (Sari-Branch). He was in Stanford's top 2% of the most cited scientist across the world in two consecutive years 2021 and 2022. His research interests are in the areas of cloud computing, fog computing, IoT, distributed systems, parallel processing, machine learning, and evolutionary computation.

- Email: mirsaeid_hosseini@iausari.ac.ir & mirsaeid_hosseini@yahoo.com
- ORCID: 0000-0001-9396-5765
- Web of Science Researcher ID: NA
- Scopus Author ID: NA
- Homepage: NA

Amir Akbarifar received his B.Sc. and M.Sc. in Computer Software Engineering Systems in Islamic Azad University in IRAN. Currently, He is a Ph.D. candidate in Computer Engineering Department at IAU (Sari-Branch). He has been teaching computer courses in Gorgan Islamic Azad University in Golestan province of IRAN since 2022. He has published numerous articles in prestigious magazines. He is an information Security Analyst and his fields of study includes: Security, Software Architecture, Artificial Intelligence, Quantum Computing, and Cryptography.

- Email: Amir.Akbarifar@gmail.com
- ORCID: 0000-0003-3227-2847
- Web of Science Researcher ID: AFC-8068-2022
- Scopus Author ID: NA
- Homepage: NA

How to cite this paper:
M. Hosseini Shirvani, A. Akbarifar, "A survey study on intrusion detection system in wireless sensor network: Challenges and considerations," J. Electr. Comput. Eng. Innovations, 12(2): 449-474, 2024.

DOI: 10.22061/jecei.2024.10148.683

URL: https://jecei.sru.ac.ir/article_2116.html