A COMPREHENSIVE SURVEY OF INTRUSION DETECTION PROTOCOLS IN IOT-INTEGRATED WIRELESS SENSOR NETWORKS: EMERGING TRENDS AND FUTURE CHALLENGES

GUNUPUSALA SATYANARAYANA [1*] , KAILA SHAHU CHATRAPATHI [2]

[1*] Research Scholar, JNTU Hyderabad, India. Email: snarayana.5813@gmail.com
[2] Professor, Department of CSE, JNTU Hyderabad, India. Email: shahujntu@gmail.com.

ABSTRACT:

The rapid progress in wireless sensor networks (WSNs) and the Internet of Things (IoT) has brought about significant advancements in various sectors. However, these advancements also raise concerns regarding the security of these technologies. Real-world applications of IoT and WSN devices in sectors such as finance, healthcare, business, and industry have revealed numerous security risks. As the demand for IoT devices continues to rise worldwide, the need for enhanced security measures has become crucial. The convergence of WSNs into the IoT ecosystem is an emerging trend driven by advancements in addressing and the concept of the Internet of Everything. Although both technologies are interconnected, they exhibit notable differences in terms of application areas, connectivity, routing, and security concerns. Wireless sensor networks (WSNs) primarily emphasize resource-constrained management, while Internet of Things (IoT) systems prioritize scalability, security, quality of service, and heterogeneity. In this paper, a comprehensive examination is provided regarding the factors, prerequisites, and emerging patterns that play a vital role in the advancement of Wireless Sensor Networks (WSNs) and the Internet of Things (IoT). It delves into the intricate details of both technologies, highlighting the distinctions in their applications, connectivity issues, routing challenges, and security considerations. Additionally, it addresses the growing importance of efficient resource management in WSNs and the significance of security, scalability, and heterogeneity in IoT systems. By examining these factors and trends, this paper offers valuable insights for researchers and practitioners in the field. It emphasizes the need to address security concerns and scalability challenges while considering the unique characteristics of WSNs and IoT. Ultimately, the findings from this analysis significantly contribute to enhancing the comprehension and advancement of secure and efficient technologies in the realm of WSNs and IoT.

Keywords: Internet of Things (IoT), intrusion, security, security issues, wireless sensor networks (WSNs).

1. Introduction

The main goal of Wireless Sensor Networks (WSNs) is to efficiently collect data and transmit it to a central node in a compatible format. On the other hand, the Internet of Things (IoT) encompasses a range of technologies and protocols that facilitate the collection, processing, and transfer of data across computer networks, serving diverse applications and decision-making processes. While IoT devices directly connected to the internet can utilize conventional communication protocols, wireless networks require innovative routing techniques to enable efficient information transmission within the network. In WSNs, data is directed towards a specific node called a sink node, which plays a crucial role in the IoT infrastructure by connecting everyday objects. Both WSNs and IoT prioritize security and safety. It is essential to ensure encryption, authentication, and freshness of data originating from sensor nodes for the proper functioning of applications in both domains.

The security requirements in Wireless Sensor Networks (WSNs) differ depending on the specific application domain, and there are particularly strict security needs for military and critical infrastructure monitoring applications. On the other hand, the Internet of Things (IoT) requires the integration of multiple security policies and techniques to ensure the protection of data integrity, authenticity, and confidentiality. This complexity arises from the need to incorporate strong security measures within IoT devices. While each node in WSN does not require unique identification, IoT devices necessitate unique identification for proper communication and control, following the appropriate addressing scheme. In WSN, data processing mainly focuses on aggregation to reduce network congestion. In contrast, IoT data processing goes beyond aggregation and filtration, incorporating data analytics techniques to transform data into valuable information and knowledge across all IoT applications.

WSN functions independently of an internet connection as it relies on wireless channels to establish interconnections among its nodes. The interconnected nodes within the network send their aggregated data to the sink nodes, which subsequently transmit this data to the server. In contrast, an internet connection is an essential requirement for IoT. IoT applications typically entail additional prerequisites such as location-aware services, adaptable network configurations, and adherence to regulatory frameworks.

In an IoT system, sensors transmit their information directly to the internet. In contrast, WSN does not establish a direct connection. Instead, multiple sensors are linked to a router or central node, and data is routed accordingly. WSN involves wireless connectivity among sensor nodes for data gathering, whereas IoT encompasses WSN as well as physical objects (Things), IP addresses, the internet, applications, cloud computing, and various other components.

2. Motivation

In certain scenarios, Internet of Things (IoT) devices and Wireless Sensor Networks (WSN), including sensors, are deployed in environments that lack constant physical monitoring, making them susceptible to exploitation [3]-[6]. This vulnerability presents an opportunity for adversaries to take advantage of the situation. For instance, let's consider a scenario in which Adversary A successfully acquires unauthorized access to IoT sensor nodes deployed within a specific area. By extracting valuable information from these nodes, A gains the capability to create attacker nodes and introduce them into the established network. This malicious activity opens the door for various types of attacks, including blackhole, sinkhole, wormhole, Sybil, and flooding attacks. Such attacks significantly compromise the reliability, performance and efficiency of the network. The consequences of such attacks include reduced network throughput, decreased packet delivery ratio and increased end-to-end delay, and decreased packet delivery ratio. Therefore, it is vital for intrusion detection protocols to effectively safeguard against these attacks and ensure the integrity and security of the network.

This survey paper provides a comprehensive overview of currently available intrusion detection protocols that are specifically designed for environments involving and the Internet of Things (IoT) and Wireless Sensor Networks (WSN). Through the examination of these protocols, the survey seeks to provide valuable assistance to researchers working in the domain of intrusion detection systems for IoT and WSN. It serves as a valuable resource for understanding the current state of intrusion detection and identifying areas for further research and improvement in securing WSN and IoT networks.

3. Challenges to Security in IoT Devices

IoT devices are susceptible to various security threats that pose risks to their functionality and user privacy. This paper examines several prominent security threats encountered by IoT devices, including:

Wrong Access Control: Insufficient enforcement of access control measures allows unauthorized individuals to access IoT device functionalities. Universal usernames and passwords for hardware devices further exacerbate this problem.

Use of Outdated Software: Many IoT devices lack the capability to auto-update, leaving them vulnerable to security issues discovered after deployment. The integration of auto-update functionality is crucial to address these vulnerabilities effectively.

Bugs in Application Software: Security concerns may arise as a result of bugs or vulnerabilities present in the application software of IoT devices. Despite efforts during development, it is challenging to identify and eliminate all vulnerabilities. Continuous testing and robust software development practices are necessary to minimize such risks.

Weak Encryption: Certain IoT applications transmit data without employing encryption, while others may utilize inadequate or weak encryption methods. This leaves the data vulnerable to interception and manipulation, making it susceptible to man-in-the-middle attacks. Lightweight cryptographic algorithms[7] are needed to provide strong encryption while considering the resource constraints of IoT devices.

Weak Intrusion Detection: Numerous IoT devices suffer from the absence of logging or alerting functionalities, posing challenges for owners to detect security breaches or attacks[8]. It is crucial to implement efficient intrusion detection methods specifically designed for IoT systems in order to bolster the security stance of these devices.

4. Challenges to Security in Wireless Sensor Networks (WSN)

The integration of Wireless Sensor Networks (WSN) with advanced Internet of Things (IoT) technologies has garnered considerable interest. However, the existing implementation of these systems often lacks adequate security measures [9], making them susceptible to exploitation by malicious individuals and attackers. It is essential to address the following critical security threats in any WSN environment:

Physical Layer Attacks: Targeting the physical layer [10], attacks on wireless sensor networks encompass a range of hardware tampering methods, including node destruction and disruption of radio channels through frequency jamming. Although completely eradicating physical layer attacks is challenging, the deployment of robust encryption techniques can aid in protecting data in case of node tampering. Moreover, the implementation of efficient frequency hopping techniques can help mitigate the effects of channel jamming.

Data Link Layer Attacks: The data link layer is responsible for channel access and synchronization between nodes. It is susceptible to attacks like collisions, traffic analysis and exhaustion. Intruders engaging in eavesdropping on communication patterns can result in the leakage of sensitive information, thereby jeopardizing the integrity of the entire system. Compromised nodes that ignore Medium Access Control (MAC) protocols can cause collisions, disrupting the transmission system and enabling exhaustion attacks.

Network Layer Attacks: Network layer attacks present significant threats to the WSN environment, including denial-of-service attacks and replay attacks. These attacks specifically target the network layer in order to disrupt network operations or compromise data integrity. The inherent ad-hoc nature of WSN systems makes them particularly susceptible to these types of attacks.

Transport Layer Attacks: Attacks on the transport layer aim to disrupt connections by continuously initiating new connections. These attacks take advantage of the limited resources of sensor nodes. By manipulating the order in which nodes access shared resources, communication between sensor nodes can become desynchronized. Flooding at the transport layer disrupts legitimate requests until resources are exhausted.

Application Layer Attacks: In many WSN applications, nodes are deployed in hostile environments and managed remotely. This heightened risk increases the potential for intruders to reprogram the deployed nodes, potentially hijacking the system and gaining control over the entire network.

It is crucial to address these security threats to maintain the integrity and reliability of Wireless Sensor Network (WSN) systems integrated with Internet of Things (IoT) technologies. By implementing suitable security measures at each layer, including the data link, network, transport, physical and application layers, the risks associated with various attacks can be mitigated. This proactive approach ensures a more secure environment for wireless sensor networks.

5. Key Requirements in IoT Security

Ensuring the security of IoT devices is crucial in protecting against intrusions and safeguarding sensitive data. The following key requirements play a vital role in establishing a robust IoT security framework:

Unique Device Identification: Each connected IoT device should have a unique identification, enabling effective device management and preventing unauthorized access. Manufacturers should employ efficient cryptographic techniques to equip devices with tamper-resistant unique IDs during production.

End-to-End Encryption: Implementing strong encryption mechanisms for data and communication is essential to ensure confidentiality and integrity throughout the IoT ecosystem. A comprehensive policy for end-to-end encryption[11] should be enforced to protect sensitive information from unauthorized access.

Strong Authentication: Robust authentication procedures are necessary to establish trust between connected devices. Reliable authentication mechanisms, such as multifactor authentication, should be implemented to verify the identity of devices and prevent unauthorized entities from accessing the network.

Security Benchmarking: Regulations and standards must be in place to ensure that IoT devices meet minimum security requirements before being released into the market. A comprehensive security benchmark should be established, covering aspects like strong passwords, configuration management guidelines, and the use of Public Key Infrastructure (PKI) technology.

Consumer Awareness: Educating consumers about IoT security risks and providing guidelines on selecting secure devices is crucial. Consumers should be aware of the importance of strong passwords, avoiding default settings, and regularly updating device firmware to maintain security.

By incorporating these key requirements into IoT security practices, manufacturers, regulators, and consumers can collectively work towards establishing a more secure and trustworthy IoT environment. The Figure1 contain Key Requirements in IoT Security

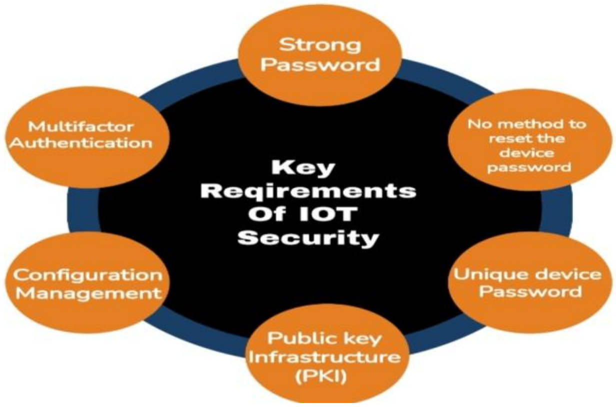

Strong Password
No method to reset the device password
Multifactor Authentication
Key Reqirements Of IOT Security
Configuration Management
Unique device Password
Public key Infrastructure (PKI)

Figure 1: Key Requirements in IoT Security

6. Key Requirements in WSN Security

Wireless Sensor Networks (WSNs) consist of low-powered devices with limited storage and processing capabilities [12]. These inherent constraints pose several security challenges and vulnerabilities within WSNs. Implementing robust security measures becomes challenging due to the resource limitations. Here are some of the security issues arising from these limitations:

Access Control: Ensuring that only authorized users or devices have access to the network and its resources. Unauthorized access can compromise the integrity and confidentiality of the data transmitted within the network.

Authentication: Verifying the identity of users or devices to prevent unauthorized access and impersonation. Strong authentication mechanisms are required to ensure that only legitimate entities can participate in the network and exchange information securely.

Data Availability: Ensuring that data is accessible and available to authorized users or applications when needed. In WSNs, where resources are scarce, mechanisms should be in place to guarantee that data is reliably collected, stored, and retrieved without loss or corruption.

Data Confidentiality: Protecting the data from unauthorized access or disclosure, ensuring that it remains confidential.

Data Freshness: Ensuring the freshness and timeliness of data by preventing replay attacks or the use of outdated information.

Data Integrity: Ensuring the integrity and trustworthiness of data, preventing unauthorized modification or tampering.

Quality of Service: Maintaining a certain level of performance, reliability, and responsiveness in the network.

Secure Localization: Ensuring the accuracy and security of location information in WSN applications.

Self-Organization: Facilitating the autonomous and secure organization of the network, including node discovery and network formation.

Time Synchronization: Achieving synchronization among nodes to coordinate their actions and enable accurate time stamping of events.

These requirements aim to address the security challenges specific to WSNs, considering their resource-constrained nature and the need for secure and reliable communication within the network. The Figure2 contain Key Requirements in WSN Security

The key security requirements in both WSN and IoT domains share similarities[1]. However, there are differences in the relevance of certain security requirements, as depicted in Table 1.

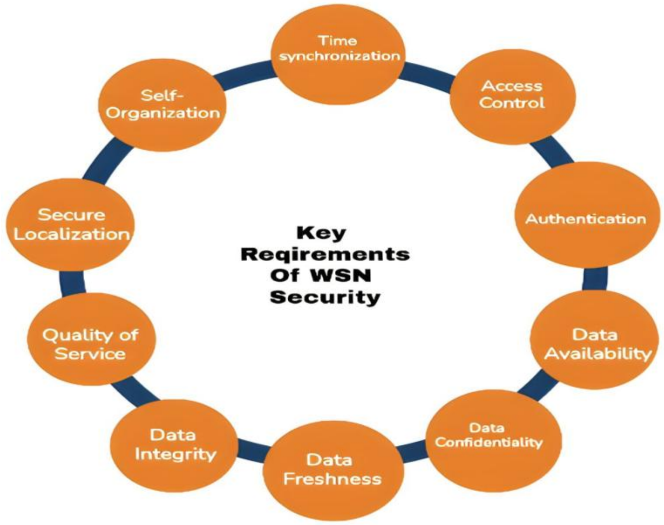
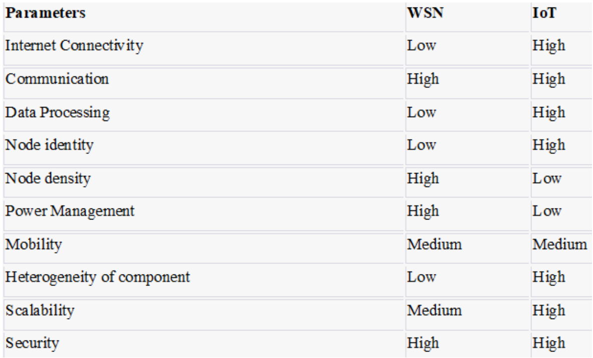


Figure 2: Key Requirements in WSN Security

Table 1: Security Requirements for WSN vs. IOT



Parameters	WSN	IoT
Internet Connectivity	Low	High
Communication	High	High
Data Processing	Low	High
Node identity	Low	High
Node density	High	Low
Power Management	High	Low
Mobility	Medium	Medium
Heterogeneity of component	Low	High
Scalability	Medium	High
Security	High	High

Internet Connectivity: IoT devices typically have high internet connectivity, allowing them to connect to a wide range of networks and services. In contrast, WSNs often have low internet connectivity due to their localized and constrained nature.

Communication: Both WSN and IoT require high levels of communication, as data exchange is a fundamental aspect of their operations.

Data Processing: IoT devices have higher data processing capabilities compared to WSNs, allowing them to handle and analyze large volumes of data. WSNs, on the other hand, have limited data processing capabilities due to their resource constraints.

Node Identity: In IoT, individual device identity and authentication are crucial due to the presence of a large number of diverse devices. WSNs typically have lower emphasis on individual node identity due to their dense deployment and homogeneous nature.

Node Density: WSNs often have high node density, with a large number of sensor nodes deployed in a small area. In contrast, IoT devices may have lower node density as they can be dispersed over a wider geographical area.

Power Management: WSNs require efficient power management techniques due to their limited power resources. IoT devices, on the other hand, may have access to a continuous power supply and may not prioritize power management as heavily.

Mobility: Both WSN and IoT devices can exhibit medium levels of mobility, depending on the specific application and use case.

Heterogeneity of Component: IoT devices often exhibit high heterogeneity, with diverse hardware and software components. WSNs tend to have lower heterogeneity, as they are typically composed of similar sensor nodes.

Scalability: IoT systems are designed to scale up to accommodate a large number of devices and users. WSNs can also scale, but the scale is often limited by the available resources and the specific application requirements.

Security: Both WSN and IoT require high levels of security to protect data, privacy, and system integrity. Security is a critical concern in both domains due to the potential risks and vulnerabilities associated with wireless and connected environments.

7. IOT Security Challenges

Utilizing IoT devices brings considerable advantages in aiding humans with tasks that are difficult to accomplish manually. Nevertheless, this convenience is accompanied by inherent risks. The rise of cyber-attacks targeting IoT applications poses a significant challenge due to the intricate nature of protocols, devices, and network topologies involved.

To ensure secure and dependable operation, IoT systems need to establish trustworthiness to mitigate various forms of security breaches and negligence attacks. The rapid proliferation of diverse IoT devices further complicates this challenge, aggravated by a scarcity of experts proficient in managing these devices. This skill gap amplifies the security concerns associated with IoT devices.

To address these issues, it is crucial to raise awareness among individuals about the security challenges associated with IoT devices. People need to be educated about the proper handling and the potential security vulnerabilities that exist. By fostering a culture of security awareness, we can empower individuals to take necessary precautions and make informed decisions when using IoT devices. The Figure3 contain IoT Security Challenges.

AI and Automation

As the number of devices in enterprise applications increases rapidly, there is a significant amount of data generated. However, handling this vast volume of data poses a challenge, particularly from a security standpoint. Detecting anomalies within this data becomes difficult, and when it is used for autonomous decision-making processes, even a single error in the code can have far-reaching consequences, potentially impacting the entire infrastructure.

Insufficient Testing and Updation

Another issue in the IoT ecosystem is the insufficient testing and updating of IoT products. With numerous players in the market, many IoT devices do not receive adequate updates or sometimes no updates at all. Even devices initially considered secure may become vulnerable when flaws are discovered in the future. Manufacturers often fail to follow robust testing procedures, leaving customers exposed to potential attacks due to outdated hardware and software.

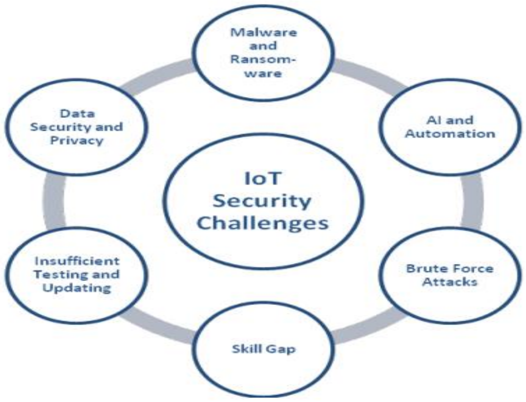


Figure 3: IoT Security Challenges

To address these concerns, it is crucial for manufacturers to prioritize regular updates and patches for their IoT devices. This includes not only addressing security vulnerabilities but also implementing enhancements and improvements based on evolving industry standards. Rigorous testing procedures should be in place during the development and manufacturing stages to ensure the reliability and security of IoT devices.

Furthermore, organizations and individuals utilizing IoT devices should prioritize ongoing monitoring, maintenance, and updates. Regular security audits and assessments can help identify and mitigate potential vulnerabilities. It is essential to stay informed about the latest security best practices and follow recommended guidelines to safeguard IoT systems.

8. WSN Security Challenges

Wireless Sensor Networks (WSNs) present various challenges related to addressing, scalability, reliability, SDN integration, and virtualization. In addition to these challenges, specific security concerns arise in WSNs that require attention. Some of these challenges include:

Wireless Connectivity: Wireless signals are more vulnerable to interception compared to wired signals, posing a security weakness. Compromised wireless channels create challenges in maintaining security and reliability. While wireless connectivity offers mobility, convenience, and remote access control, ensuring security becomes a critical concern.

Key Management and Distribution: Efficient key distribution and management play a vital role in WSNs. However, this process introduces communication overhead during authentication and searching stages. Both secret-key cryptography and public-key cryptography have their limitations, requiring a trade-off between cryptographic methods and the capabilities, power, and requirements of sensor processing.

WSN Virtualization: Virtualizing WSN hardware is a complex task. The hardware of wireless sensor networks is not easily virtualized, making it challenging to separate services and infrastructure, which otherwise provides flexibility and ease of deployment.

Integration: Integration obstacles emerge as a result of employing hardware and software components from various manufacturers in WSNs. The presence of heterogeneous nodes frequently gives rise to compatibility issues, thereby complicating synchronization, scalability and maintainability.

Programming WSN: Wireless Sensor Networks (WSNs) are comprised of diverse protocols and devices with limited resources, posing a challenge for network programming tasks. Dealing with these constraints necessitates meticulous deliberation and expertise from WSN professionals.

Intrusion Detection: Integrating an intrusion detection system into a wireless sensor network adds complexity to the network. The intrusion detection processes consume network resources and the limited energy of resource-constrained WSNs, which requires the implementation of efficient management and optimization strategies to address these challenges [15].

The Figure4 contain WSN Security Challenges.

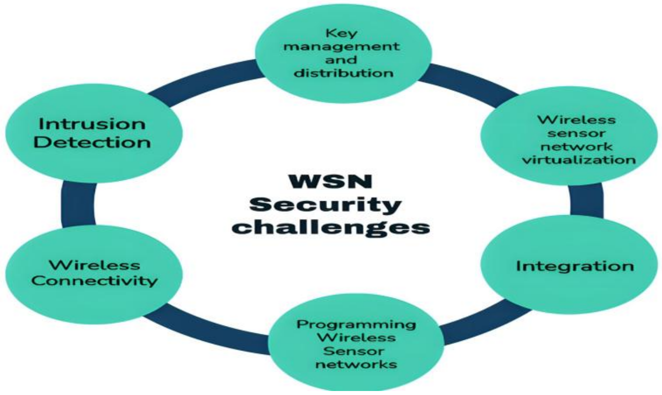

Key management and distribution
Wireless sensor network virtualization
Integration
Programming Wireless Sensor networks
Wireless Connectivity
Intrusion Detection
WSN Security challenges

Figure 4: WSN Security Challenge

Addressing these security challenges is crucial for ensuring the reliable and secure operation of WSNs in various applications and domains.

9. WSN Security Protection

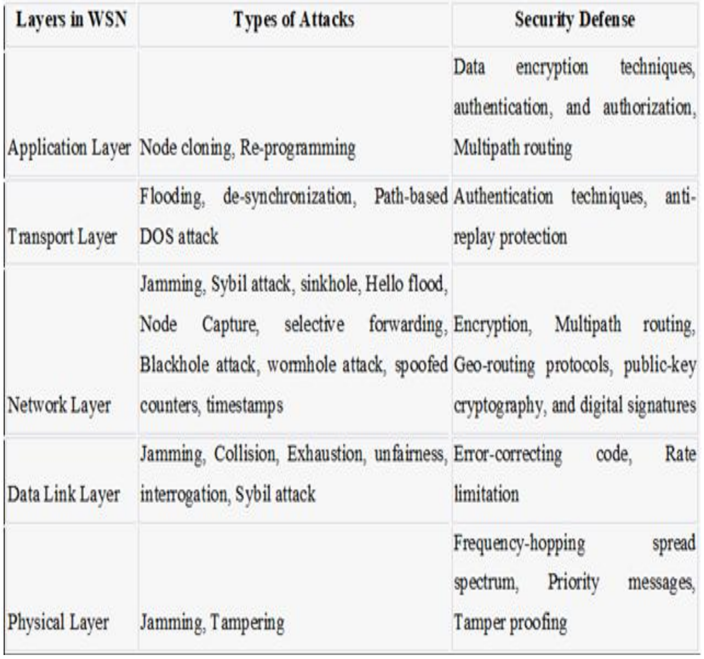
To enhance security in wireless sensor networks (WSNs), it is crucial to detect and counter various types of security attacks using appropriate protection mechanisms. To bolster security in wireless sensor networks (WSNs), it is vital to detect and mitigate different types of security attacks through suitable protection mechanisms. The design of the link layer architecture should enable swift detection of unauthorized packets injected into the network. Techniques such as code spreading and frequency hopping can be employed to prevent jamming attacks. Collision attacks can be mitigated by utilizing error-correcting codes and implementing effective media access control strategies.

To defend against spoofing and data alteration, appending message authentication codes can ensure message integrity. At the transport layer, flooding attacks like Denial of Service (DoS) can be mitigated by implementing client puzzle techniques. Sybil attacks can be addressed using identity-based encryption techniques.

Intrusion detection techniques can be implemented across the network to detect abnormal behavior and potential security breaches. Utilizing tamper-resistant hardware can effectively mitigate physical layer attacks. Lightweight encryption methods are frequently employed to ensure data protection during transmission within WSNs.

Each layer of the network should address specific key points to ensure comprehensive security. Table 2 provides an overview of the types of attacks that can occur at each layer and the corresponding security protection mechanisms used to mitigate them. For instance, at the application layer, authentication, authorization, data encryption techniques, and multipath routing can be employed to defend against node cloning and re-programming attacks. At the transport layer, anti-replay protection, authentication techniques and appropriate routing protocols can be utilized to de-synchronization, counter flooding and path-based DoS attacks. The network layer can leverage encryption, public-key cryptography, multipath routing, geo-routing protocols and digital signatures to address various attacks such as Sybil attacks, jamming and blackhole attacks. The data link layer can utilize error-correcting codes and rate limitation techniques to protect against jamming, collision, exhaustion, and Sybil attacks. Finally, the physical layer can employ frequency-hopping spread spectrum techniques, prioritize critical messages, and implement tamper-proofing measures to mitigate jamming and tampering attacks.

Table 2: Threats and Security Measures across Wireless Sensor Networks (WSN) Layers

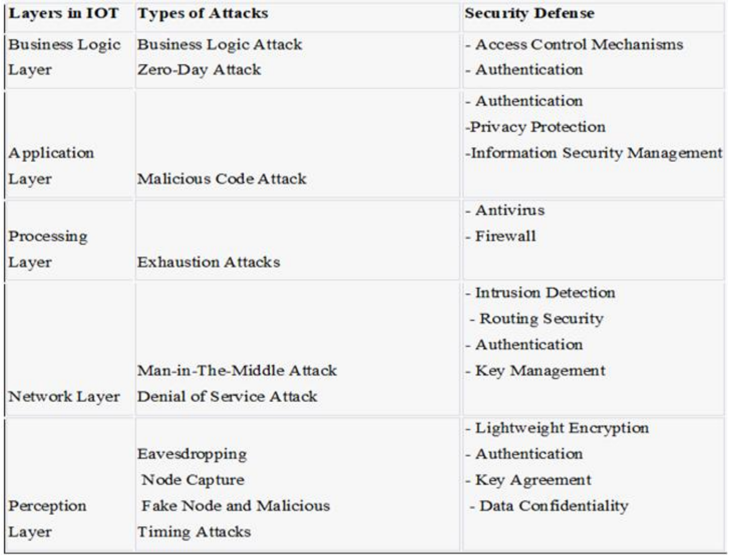


Layers in WSN	Types of Attacks	Security Defense
Application Layer	Node cloning, Re-programming	Data encryption techniques, authentication, and authorization, Multipath routing
Transport Layer	Flooding, de-synchronization, Path-based DOS attack	Authentication techniques, anti-replay protection
Network Layer	Jamming, Sybil attack, sinkhole, Hello flood, Node Capture, selective forwarding, Blackhole attack, wormhole attack, spoofed counters, timestamps	Encryption, Multipath routing, Geo-routing protocols, public-key cryptography, and digital signatures
Data Link Layer	Jamming, Collision, Exhaustion, unfairness, interrogation, Sybil attack	Error-correcting code, Rate limitation
Physical Layer	Jamming, Tampering	Frequency-hopping spread spectrum, Priority messages, Tamper proofing

10. Security Protection in IoT

In IoT, security protection measures are crucial to mitigate the various threats that arise from both the devices themselves and the wireless communication medium[18]. To ensure a secure IoT infrastructure, it is essential to implement proper cryptographic techniques. Strong authentication and encryption mechanisms must be in place for all communication entities involved. Here are some security protection techniques emphasized at each layer in the Table 3.

Table 3: Threats and Security Measures across IoT Layers



Layers in IOT	Types of Attacks	Security Defense
Business Logic Layer	Business Logic Attack Zero-Day Attack	- Access Control Mechanisms - Authentication
Application Layer	Malicious Code Attack	- Authentication -Privacy Protection -Information Security Management
Processing Layer	Exhaustion Attacks	- Antivirus - Firewall
Network Layer	Man-in-The-Middle Attack Denial of Service Attack	- Intrusion Detection - Routing Security - Authentication - Key Management
Perception Layer	Eavesdropping Node Capture Fake Node and Malicious Timing Attacks	- Lightweight Encryption - Authentication - Key Agreement - Data Confidentiality

At the business layer of the IoT architecture, which handles data analysis and modeling, a robust access control mechanism is necessary to prevent unauthorized access and ensure data integrity.

The application layer, responsible for application logic, requires strong security management protocols to protect against potential vulnerabilities and attacks.

In the network layer, secure routing protocols are crucial to ensure the secure transmission of data within the IoT network. These protocols help prevent unauthorized access, protect against data tampering, and maintain the confidentiality of sensitive information.

The perception layer, which comprises the hardware devices in the IoT ecosystem, must be designed to be temper-resistant. This involves implementing hardware-level security features that prevent physical tampering and ensure the integrity of the devices.

By addressing these security protection measures at different layers of the IoT architecture, organizations can enhance the overall security of their IoT deployments and safeguard against potential threats and attacks.

11. Existing Approaches to IDS

Numerous research papers have proposed various approaches for implementing IDS, each offering novel techniques and methodologies. Here are summaries of some of these approaches:

Farooqi and Khan [19] undertook an evaluation of intrusion detection systems (IDS) tailored for wireless sensor networks

(WSNs), with a specific emphasis on tackling security challenges and prevalent types of attacks in WSNs. Moreover, they conducted a comparative analysis of security mechanisms based on IDS that are well-suited for WSNs.

A study conducted by Dhakne and Chatur [20] focused on intrusion detection systems (IDS) specifically tailored for wireless sensor networks (WSNs). Their research delved into different detection techniques, such as anomaly-based detection, misuse-based detection, and specification-based detection. The study analyzed various IDS proposed for WSNs, assessing their advantages, drawbacks, and potential future directions. Its objective was to provide insights for selecting suitable IDS in WSN environments.

Zarpelao et al. [21] conducted a comprehensive survey on IDS in the context of the Internet of Things (IoT). They categorized IDS based on detection methods, placement strategies, security threats targeted, and validation strategies. Their study identified emerging trends, emphasized unresolved issues, and outlined potential research directions in the domain of IoT communication

Elrawy et al. [22] focused on the architecture of IoT and its security vulnerabilities. They discussed the design and implementation of IDS specifically tailored for IoT environments, taking into consideration the unique characteristics and challenges of IoT systems. The study emphasized the importance of securing IoT architectures and the need for robust intrusion detection mechanisms.

Khan and Herrmann [23] conducted a comprehensive survey on IDS for the IoT environment, covering IDS solutions for various IoT subdomains. They provided insights into IDS techniques and approaches applicable to each subdomain, discussing future research directions in IoT security.

In a study conducted by Shuai Jiang et al. [24], experiments were conducted to assess the performance of a proposed intrusion detection method using the WSN-DS dataset. The results indicated that their method achieved higher F-measure scores compared to existing detection methods when detecting various types of attacks. This suggests that their proposed method shows promise in effectively detecting and mitigating intrusions in wireless sensor networks.

Shakya, Subarna [25] proposed a machine learning-based model for intrusion detection in WSNs, demonstrating improved performance in terms of reducing false alarm rates, processing time, and enhancing detection rates and accuracy.

Gauri Kalnoor and S. Gowrishankar [26] presented a high-level security approach for IoT smart environments, integrating IoT-WSN networks and emphasizing the potential for securing network systems.

In their research, Krishnan et al. [27] presented a framework designed for wireless sensor networks (WSNs) that aims to guarantee the reliability and security of sensory data. Their framework utilizes a (k, n) threshold-based Shamir secret sharing scheme. This scheme helps in distributing and reconstructing the secret key among multiple sensor nodes in a way that requires at least k out of n nodes to collaborate in order to recover the original key. By employing this approach, the framework enhances both the reliability and security aspects of sensory data transmission and storage in WSNs.

Aljebreen et al. [28] proposed a BCOA-MLID technique for intrusion detection in IoT-WSNs, showcasing promising results and outperforming existing models in terms of accuracy.

Wang et al. [29] developed single and multiple node detection models based on network parameters and computed the probability of detecting malicious nodes with respect to their distance in the network.

Wang et al. [30] proposed an intelligent hybrid intrusion detection system (IHIDS) using three different IDS models at different positions in the network. They utilized self-learning and rule-based modules to detect abnormal and predefined attacks.

Salehi et al. [31] developed an IDS to detect sinkhole intruders by identifying suspicious nodes through data inconsistency and analyzing network traffic information flow.

Wazid et al. [32] designed a hierarchical IDS to detect sinkhole attacks, performing detection in two phases based on network performance values and specific types of sinkhole attacker nodes.

Selvakumar et al. [33] proposed an intelligent intrusion detection system (IDS) that incorporates temporal reasoning using a fuzzy and rough set-based nearest neighborhood algorithm (FRNN). Their approach aims to reduce complexity by eliminating redundant attributes and leveraging Allen's interval algebra operators. By integrating temporal reasoning techniques, the IDS can effectively analyze and detect intrusions in a more intelligent and efficient manner. The utilization of FRNN in the system enables accurate intrusion detection by considering both fuzzy and rough set-based reasoning, providing improved performance and reliability.

Alaparthy and Morgera [34] developed a multilevel intrusion detection system (IDS) inspired by the immune system. Their design incorporated factors like battery life, message size, and data transfer rate to facilitate detection. In this system, nodes in proximity to the sink formed a network and conducted pathogen-associated molecular pattern (PAMP) analysis.

Sun et al. [35] introduced a multilevel intrusion detection system (IDS) that employed the negative selection algorithm (NSA) and an enhanced V-detector algorithm. To reduce dimensionality, they incorporated principal component analysis (PCA) into their system. The effectiveness of their IDS relies on the assumption that the deployed sensor nodes follow a Gaussian distribution. By leveraging these techniques, their multilevel IDS offers enhanced intrusion detection capabilities, improving the overall security of the wireless sensor network.

Wang et al. [36] performed an analysis of intrusion detection in wireless sensor networks (WSNs) that exhibit a Gaussian distribution, comparing it with WSNs characterized by a uniform distribution. Their analysis encompassed both single sensing and multiple-sensing detection scenarios. By investigating these different distribution patterns, the study aimed to gain insights into the performance and effectiveness of intrusion detection techniques in WSNs, considering the impact of the underlying distribution characteristics on detection accuracy and reliability.

Wazid and Das [37], [38] proposed an intrusion detection scheme specifically tailored to identify blackhole attacker nodes and hybrid anomalies in wireless sensor networks (WSNs). Their scheme involved a hierarchical network structure where resource-rich cluster head nodes took on the responsibility of conducting the detection process. These cluster head nodes were equipped with sufficient resources to perform advanced detection techniques and efficiently identify malicious activities, enhancing the security of the WSN by effectively detecting and mitigating potential threats.

In their research, Jan et al. [39] implemented a lightweight intrusion detection system (IDS) to mitigate common Denial-of-Service (DoS) attacks in IoT networks that have limited resources. Their approach utilized the packet transmission rate as a basis for detection and extracted a reduced set of features to improve classification efficiency. They employed Support Vector Machines (SVM) for classification and mitigation. However, it is important to consider that this approach may not be as effective in networks that experience a steady flow of traffic, as it is primarily designed to address DoS attacks in resource-constrained IoT networks.

Sharma et al. [40] implemented a lightweight mechanism called behavior rule specification-based misbehavior detection for IoT-embedded cyber-physical systems. They detected intruders through the misbehavior of existing nodes. However, the use of rule-based systems can be easily bypassed by smart attackers. The proposed technique included a profiler and a fuzzy analysis module to validate behavior rules using the hierarchical context-aware aspect-oriented Petri net (HCAPN) model.

Pajouh et al. [41] introduced an intrusion detection system (IDS) specifically designed for identifying different types of malicious attacks in IoT environments. To enhance the efficiency of the detection process, they utilized dimensionality reduction techniques, such as principal component analysis (PCA) and linear discriminant analysis (LDA), to reduce the number of features involved. The IDS leveraged K-nearest neighbors (KNN) and naive Bayes classification techniques to effectively detect and classify malicious activities. By combining these approaches, their IDS offers improved accuracy and reliability in identifying and mitigating security threats in IoT environments.

Li et al. [42] developed a collaborative signature-based intrusion detection system (IDS) called CBSigIDS, utilizing blockchain technology specifically for IoT environments. The collaborative IDS employed rules or signatures to identify and detect malicious activities, with the capability to share this information with other nodes and update their respective databases. To address insider attacks and ensure data integrity, a blockchain-based approach was implemented. This approach ensures that the shared data remains tamper-proof and trustworthy, enhancing the overall security and effectiveness of the intrusion detection system in IoT environments.

Breitenbacher et al. [43] presented HADES-IoT, a lightweight host-based anomaly detection system specifically designed for IoT environments. HADES-IoT adopted a proactive approach to detect anomalies and was specifically designed to be implemented on Linux-based end devices. One notable feature of HADES-IoT is its ability to be loaded directly into the kernel of the operating system, which makes it highly suitable for deployment in Linux-based end devices commonly found in IoT environments. This integration allows for efficient and effective anomaly detection, enhancing the security of IoT systems at the host level.

Mudgerikar et al. [44] introduced E-Spion, an intrusion detection system (IDS) that operated at the client system level and relied on anomaly detection techniques to identify intruders. E-Spion was designed with three security layers, each providing increasing levels of security. However, it is important to consider that higher security levels also introduced higher overhead. In the first module, E-Spion employed a whitelist approach to compare ongoing processes and their associated IDs. The second module utilized machine learning classifiers that were trained using logs generated during the learning phase. These classifiers enabled the system to effectively detect and mitigate intrusions based on learned patterns and behaviors.

Saeed et al. [45] proposed a two-phase intrusion detection system (IDS) aimed at improving system security. The first phase of the IDS involved implementing an anomaly-based detection approach using a random neural network model. This approach enabled the system to identify deviations from normal behavior patterns. In the second phase, a tag system was introduced, associating tags with memory locations. This tag-based system facilitated the detection of anomalies by utilizing tag-checking methods. By combining these two phases, the IDS offered enhanced detection capabilities, allowing for the identification and mitigation of potential security threats in the system.

Wazid et al. [46] presented intrusion detection schemes specifically designed to detect routing attacks in edge-based IoT (EIoT) environments. These schemes were developed to address the unique security challenges associated with EIoT, where edge devices play a critical role in data processing and communication. The intrusion detection schemes proposed by Wazid et al. focused on identifying and mitigating routing attacks that could compromise the integrity and reliability of data transmission within the EIoT system. By specifically targeting routing attacks in EIoT environments, their schemes aim to enhance the overall security and resilience of edge-based IoT systems.

12. Future Research Challenges and Directions in Wireless Sensor Networks (WSN) and the Internet of Things (IoT)

Wireless Sensor Networks (WSNs) and Internet of Things (IoT)-based communication environments have a diverse range of applications, spanning smart healthcare ,smart homes, smart transportation and smart cities. These environments possess distinct requirements, including real-time data processing and access, facilitating immediate monitoring of patients or environmental conditions in industrial plants, among various other use cases.The data generated by IoT sensors is voluminous, necessitating the utilization of big data analytics to extract meaningful patterns, such as future health predictions for patients. However, being part of the Internet, these communication environments are also subject to traditional security, privacy, and other challenges.

Intrusion detection in WSNs and IoT has emerged as a crucial problem, attracting significant attention from researchers. This research area faces unique challenges due to the characteristics of WSNs and IoT, including resource-constrained devices, dynamic network topology, heterogeneous communication protocols, and the sheer scale of deployed devices. Intrusion detection plays a vital role in identifying and mitigating malicious activities, ensuring the integrity, confidentiality, and availability of the systems and data.

Addressing these challenges requires the development of effective intrusion detection mechanisms tailored to the specific characteristics of WSNs and IoT. Researchers are actively exploring innovative approaches to improve intrusion detection accuracy, reduce false positives and false negatives, minimize computational and communication overhead, and adapt to dynamic network conditions. Machine learning, data mining, and artificial intelligence techniques are being leveraged to enhance intrusion detection capabilities. Furthermore, the integration of anomaly-based and signature-based detection methods, as well as the utilization of hybrid approaches, holds promise for more robust and comprehensive intrusion detection in WSNs and IoT environments.

Looking ahead, the future of intrusion detection in WSNs and IoT environments is expected to focus on several key aspects. First, advancements in machine learning algorithms, deep learning models, and anomaly detection techniques will contribute to more accurate and efficient intrusion detection. Second, the development of lightweight and energy-efficient intrusion detection mechanisms will address the resource constraints of WSNs and IoT devices. Third, the integration of intrusion detection with secure communication protocols, encryption, and authentication mechanisms will enhance the overall security of WSNs and IoT systems. Finally, the adoption of standardization and interoperability frameworks will promote compatibility and collaboration among different intrusion detection solutions, enabling seamless integration and unified management in diverse WSN and IoT deployments.

12.1. Ensuring the Security of Intrusion Detection Techniques in WSN and IoT Environments

Many existing intrusion detection techniques proposed for Internet of Things (IoT) and Wireless Sensor Networks (WSN) environments have limitations when it comes to providing comprehensive security. These techniques often fall short in offering foolproof protection against a wide range of attacks, and some may only focus on addressing specific attack types, making them ineffective in detecting multiple attacks simultaneously. Indeed, the development of robust and secure intrusion detection techniques is crucial in addressing the ever-evolving landscape of cyber threats. With the increasing sophistication of attacks and the growing complexity of systems and networks, it is essential to have intrusion detection techniques that can effectively detect and mitigate various attack scenarios. These techniques should be capable of identifying both known and unknown attacks, adapt to new attack patterns, and provide timely response to mitigate potential damages. Furthermore, the techniques should be able to handle diverse environments, such as IoT networks, wireless sensor networks, and edge-based systems, while considering the resource constraints and scalability requirements. By focusing on the development of such intrusion detection techniques, we can enhance the security posture and protect critical systems and networks from malicious activities.

However, the design of such techniques is inherently challenging due to the resource limitations of sensors and IoT devices. These resource constraints impose restrictions on computational power and storage capacity, making it difficult to deploy complex intrusion detection mechanisms. Consequently, striking a balance between the effectiveness and efficiency of intrusion detection becomes a crucial consideration in WSN and IoT environments. It is essential to develop techniques that can accurately detect multiple attack types while minimizing the computational and storage overhead imposed on the constrained devices.

12.2. Enhancing the Efficiency of Intrusion Detection Techniques in WSN and IoT Environments:

In the communication environment of Wireless Sensor Networks (WSN) and Internet of Things (IoT), both WSN sensors and IoT sensors encounter resource limitations, such as restricted computation power, short battery life and short battery life. These constraints hinder the ability of these devices to handle computationally intensive tasks, transmit and receive large amounts of data, and store extensive information. Therefore, it is recommended to adopt a strategy that employs small-sized messages during the intrusion detection process. This approach conserves device resources, preventing rapid battery depletion caused by the transmission and reception of bulky messages.

To tackle these challenges, intrusion detection techniques should be designed to minimize computation costs, communication costs, and storage requirements, all while maintaining the overall security of the system [47], [48], [49]. Achieving the right balance between resource efficiency and effective intrusion detection is critical for ensuring optimal performance of WSN and IoT devices. By optimizing resource utilization without compromising security, these techniques can effectively mitigate the limitations imposed by resource-constrained environments, enabling reliable intrusion detection in IoT and WSN settings.

12.3. Addressing the Scalability of Intrusion Detection Techniques in WSN and IoT Environments

The integration of Wireless Sensor Networks (WSN) with the Internet of Things (IoT) results in the formation of a large-scale and heterogeneous network that encompasses a diverse range of communication paradigms and applications. Each component within this network possesses unique capabilities and requirements, thereby adding complexity to intrusion detection efforts. For instance, in healthcare scenarios, Electronic Health Records (EHRs) may be stored in an IoT-enabled cloud server, while various devices within the Body Area Network (BAN) generate data that is transmitted to the cloud. Consequently, this setup forms a heterogeneous network comprising various types of communicating devices.

To ensure the security of such a diverse communication environment, it is essential to develop intrusion detection techniques specifically tailored to protect all types of devices involved. This requires further comprehensive investigation and research in this area. It is crucial to develop effective intrusion detection mechanisms that can address the unique characteristics and requirements of WSN integrated IoT networks. By doing so, the integrity and security of the overall system can be effectively maintained, ensuring the protection of sensitive data and the reliable operation of the network.

12.4. Safeguarding Data Privacy in Cloud Server Environments

Data privacy is of utmost importance in maintaining the confidentiality and integrity of information within various resources. The integration of Wireless Sensor Networks (WSNs) with IoT-based communication is extensively employed in applications that require high levels of privacy, such as smart healthcare. In such scenarios, smart health sensors are strategically positioned to collect health data, which is then transmitted to cloud servers for storage and processing. However, these communication environments are vulnerable to various types of intrusions, which can disrupt data transmission and lead to data leakage [50], [51].

To address these concerns, it is crucial to prioritize the privacy of data both during transit and at rest. Innovative and effective schemes need to be developed to safeguard the privacy of stored data as well as data in transit. These schemes should comprehensively address potential vulnerabilities and threats in the communication environment. Additionally, the design of privacy-aware intrusion detection schemes should be tailored specifically to IoT environments, where the privacy of devices and users is a critical concern. By placing a strong emphasis on data privacy and implementing robust intrusion detection mechanisms, the confidentiality and security of sensitive information can be effectively maintained in WSN-integrated IoT environments.

12.5. Understanding the Heterogeneous Nature of WSN and IoT Communication Environments

The WSN and IoT communication environment is characterized by significant heterogeneity, encompassing a wide variety of devices including laptops, desktops, personal digital assistants, low-end RFID tags, and low-powered sensing devices. These devices operate on diverse communication protocols and possess varying communication ranges, storage capacities, computation powers, and operating systems. When designing an intrusion detection technique, it is crucial to recognize and accommodate these differences in order to ensure its effectiveness across the heterogeneous landscape.

To ensure comprehensive protection, the intrusion detection technique must be capable of safeguarding all types of devices and associated technologies within the heterogeneous WSN and IoT communication environment. By taking into consideration the diverse characteristics and requirements of these devices, the intrusion detection mechanism can be customized to address the unique challenges posed by each device type. This approach will facilitate the detection and prevention of intrusions across the entire spectrum of devices, fostering a secure and robust communication environment [52].

12.6. Cross-Platform Intrusion Detection

The presence of heterogeneity in the wireless sensor network (WSN) and Internet of Things (IoT) environment poses significant challenges when it comes to deploying effective intrusion detection techniques. While this heterogeneity allows for the interconnection of diverse application domains, it also introduces complexities in designing efficient intrusion detection processes. For example, in scenarios where a smart home application needs to access data from a healthcare sensing device, the intrusion detection mechanism must be resilient and compatible to ensure seamless data retrieval from the targeted network. Moreover, since data is often stored in the cloud, distinct intrusion detection mechanisms may be required to secure cloud-based data storage.

To tackle these challenges, it is necessary to develop efficient and robust intrusion detection techniques that ensure smooth connectivity across diverse IoT platforms. These techniques should be capable of detecting and mitigating intrusions across different application domains, safeguarding the security and integrity of the transmitted and stored data within the IoT ecosystem. By considering the unique requirements and characteristics of each platform, these intrusion detection techniques can facilitate seamless data access and secure communication throughout the diverse IoT landscape [52], [53].

13. Conclusion

In this survey paper, we have conducted an extensive examination of the security requirements and potential attacks in communication environments based on wireless sensor networks (WSN) and the Internet of Things (IoT). Our coverage includes an overview of the integration of WSNs into IoT, highlighting emerging projects and the diverse architectures employed in WSN and IoT systems. Furthermore, we have provided a taxonomy of existing intrusion detection schemes specifically designed for WSN and IoT-based communication environments. Through comparative analyses of these schemes, considering factors such as detection rate, false positive rate, and the applicability of state-of-the-art approaches, we aim to offer valuable insights to researchers and practitioners for selecting and implementing suitable intrusion detection mechanisms. Additionally, we have identified and discussed future research challenges involved in developing intrusion detection schemes and other security protocols for WSN and IoT-based communication environments. By addressing these challenges, our objective is to inspire further advancements and improvements in the design of intrusion detection mechanisms and security protocols within this domain. Overall, this survey article offers a comprehensive understanding of the current security landscape in WSN and IoT-based communication environments. It provides insights into existing intrusion detection schemes, their strengths, limitations, and outlines future directions to enhance the security of these environments. We believe that this work serves as a valuable resource for researchers, practitioners, and stakeholders interested in the security aspects of WSN and IoT-based systems.

References

[1] Choudhary, V., & Taruna, S. (2018). A Distributed Key Management Protocol for Wireless Sensor Network. Communications in Computer and Information Science, 243–256. https://doi. org/10.1007/978-981-13-3143-5_21

[2] Kavak, A., & Kucuk, K. (2009). On connectivity analysis of smart antenna capable wireless sensor networks. 2009 6th International Symposium on Wireless Communication Systems. https://doi.org/10.1109/iswcs.2009.5285278

[3] S. Chatterjee and A. K. Das, ''An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks,'' Secur. Commun. Netw., vol. 8, no. 9, pp. 1752–1771, Jun. 2015.

[4] A. K. Das, ''A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks,'' Peer-to-Peer Netw. Appl., vol. 9, no. 1, pp. 223–244, Jan. 2016.

[5] A. K. Das, ''A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor,'' Int. J. Commun. Syst., vol. 30, no. 1, Jan. 2017, Art. no. e2933.

[6] A. K. Das, ''A secure and efficient user anonymity–preserving three– factor authentication protocol for large–scale distributed wireless sensor networks,'' Wireless Pers. Commun., vol. 82, no. 3, pp. 1377–1404, Jun. 2015

[7] Li, Y. X., Qin, L., & Liang, Q. (2010). Research on Wireless Sensor Network Security. 2010 International Conference on Computational Intelligence and Security. https://doi.org/10.1109/ cis.2010.113

[8] Choudhary, V., & Taruna, S. (2021). An Intrusion Detection Technique Using Frequency Analysis for Wireless Sensor Network. 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS).https://doi. org/10.1109/icccis51004.2021.9397076

[9] Gupta, S., Bharti, P. K., & Choudhary, V. (2011). Fuzzy Logic Based Routing Algorithm for Mobile Ad Hoc Networks. High Performance Architecture and Grid Computing, 574–579. https:// doi.org/10.1007/978-3-642-22577-2_76

[10] Choudhary, V. (2017). Fuzzy Analysis for Nodes Deployment Strategies in Wireless Sensor Network. International Journal on Recent and Innovation Trends in Computing and Communication, 5(6), 852–855. https://doi.org/10.17762/ijritcc. v5i6.866

[11] Manrique, J. A., Rueda-Rueda, J. S., & Portocarrero, J. M. (2016). Contrasting Internet of Things and Wireless Sensor Network from a Conceptual Overview. 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). https://

doi.org/10.1109/ithings-greencom-cpscom-smartdata.2016.66

[12] Choudhary, V., & Taruna, S. (2020). The highly secure polynomial pool-based key pre-distribution scheme for wireless sensor network. Journal of Discrete Mathematical Sciences and Cryptography, 23(1), 95–114. https://doi.org/10.1080/0972052 9.2020.1721880

[13] Zahra, S. R., & Ahsan Chishti, M. (2019). RansomWare and Internet of Things: A New Security Nightmare. 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). https://doi.org/10.1109/confluence.2019.8776926

[14] Mohammed, A. F., & Qyser, A. A. M. (2020). A Survey on Security Mechanisms in IoT. 2020 International Conference on Emerging Trends in Information Technology and Engineering (Ic-ETITE). https://doi.org/10.1109/ic-etite47903.2020.172

[15] Choudhary, V., & Taruna, S. (2021). An Intrusion Detection Technique Using Frequency Analysis for Wireless Sensor Network. 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS). https://doi. org/10.1109/icccis51004.2021.9397076

[16] Sun, Y., Guo, S., Cheung, S. C., & Tang, Y. (2019). Analyzing and Disentangling Interleaved Interrupt-Driven IoT Programs. IEEE Internet of Things Journal, 6(3), 5376–5386. https://doi. org/10.1109/jiot.2019.2900769

[17] Mohammed, S., & Al-Jammas, M. H. (2020). Data Security System for IoT Applications. 2020 International Conference on Advanced Science and Engineering (ICOASE). https://doi.org/10.1109/ icoase51841.2020.9436579

[18] Alharbi, R., & Aspinall, D. (2018). An IoT Analysis Framework: An Investigation of IoT Smart Cameras' Vulnerabilities. Living in the Internet of Things: Cybersecurity of the IoT - 2018. https://doi. org/10.1049/cp.2018.0047

[19] A. H. Farooqi and F. A. Khan, ''A survey of intrusion detection systems for wireless sensor networks,'' Int. J. Ad Hoc Ubiquitous Comput., vol. 9, no. 2, pp. 69–83, 2012

[20] A. R. Dhakne and P. N. Chatur, ''A comprehensive survey on intrusion detection systems in wireless sensor network,'' in Smart Trends in Information Technology and Computer Communications, vol. 628. Singapore: Springer, 2016, pp. 541–549

[21] B. B. Zarpelao, R. S Miani, C. T. Kawakani, and S. C. de Alvarenga, ¯ ''A survey of intrusion detection in Internet of Things,'' J. Netw. Comput. Appl., vol. 84, pp. 25–37, Apr. 2017.

[22] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, ''Intrusion detection systems for IoT-based smart environments: A survey,'' J. Cloud Comput., vol. 7, no. 1, p. 21, Dec. 2018.

[23] Z. A. Khan and P. Herrmann, ''Recent advancements in intrusion detection systems for the Internet of Things,'' Secur. Commun. Netw., vol. 2019, pp. 1–19, Jul. 2019, doi: 10.1155/2019/4301409.

[24] S. Jiang, J. Zhao and X. Xu, "SLGBM: An Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments," in *IEEE Access*, vol. 8, pp. 169548-169558, 2020, doi: 10.1109/ACCESS.2020.3024219.

[25] Shakya, Subarna. "Modified gray wolf feature selection and machine learning classification for wireless sensor network intrusion detection." *IRO Journal on Sustainable Wireless Systems* 3.2 (2021): 118-127.

[26] Kalnoor, G., Gowrishankar, S. IoT-based smart environment using intelligent intrusion detection system. *Soft Comput* **25**, 11573–11588 (2021). https://doi.org/10.1007/s00500-021-06028-1

[27] Krishnan, R., Krishnan, R.S., Robinson, Y.H. *et al.* An Intrusion Detection and Prevention Protocol for Internet of Things Based Wireless Sensor Networks. *Wireless Pers Commun* **124**, 3461–3483 (2022). https://doi.org/10.1007/s11277-022-09521-4

[28] Aljebreen, M.; Alohali, M.A.; Saeed, M.K.; Mohsen, H.; Al Duhayyim, M.; Abdelmageed, A.A.; Drar, S.; Abdelbagi, S. Binary Chimp Optimization Algorithm with ML Based Intrusion Detection for Secure IoT-Assisted Wireless Sensor Networks. *Sensors* **2023**, *23*, 4073. https://doi.org/10.3390/s23084073.

[29] Y. Wang, X. Wang, B. Xie, D. Wang, and D. Agrawal, ''Intrusion detection in homogeneous and heterogeneous wireless sensor networks,'' IEEE Trans. Mobile Comput., vol. 7, no. 6, pp. 698–711, Jun. 2008.

[30] S.-S. Wang, K.-Q. Yan, S.-C. Wang, and C.-W. Liu, ''An integrated intrusion detection system for cluster-based wireless sensor networks,'' Expert Syst. Appl., vol. 38, no. 12, pp. 15234–15243, Nov. 2011.

[31] S. A. Salehi, M. A. Razzaque, P. Naraei, and A. Farrokhtala, ''Detection of sinkhole attack in wireless sensor networks,'' in Proc. IEEE Int. Conf. Space Sci. Commun. (IconSpace), Malacca, Malaysia, Jul. 2013, pp. 361–365

[32] M. Wazid, A. K. Das, S. Kumari, and M. K. Khan, ''Design of sinkhole node detection mechanism for hierarchical wireless sensor networks,'' Secur. Commun. Netw., vol. 9, no. 17, pp. 4596–4614, Nov. 2016.

[33] K. Selvakumar, M. Karuppiah, L. Sairamesh, S. H. Islam, M. M. Hassan, G. Fortino, and K.-K.-R. Choo, ''Intelligent temporal classification and fuzzy rough set-based feature selection algorithm for intrusion detection system in WSNs,'' Inf. Sci., vol. 497, pp. 77–90, Sep. 2019.

[34] V. T. Alaparthy and S. D. Morgera, ''A multi–level intrusion detection system for wireless sensor networks based on immune theory,'' IEEE Access, vol. 6, pp. 47364–47373, 2018

[35] Z. Sun, Y. Xu, G. Liang, and Z. Zhou, ''An intrusion detection model for wireless sensor networks with an improved V–detector algorithm,'' IEEE Sensors J., vol. 18, no. 5, pp. 1971–1984, Mar. 2018.

[36] Y. Wang, W. Fu, and D. P. Agrawal, ''Gaussian versus uniform distribution for intrusion detection in wireless

sensor networks,'' IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 2, pp. 342–355, Feb. 2013.

[37] M. Wazid and A. K. Das, ''A secure group–based blackhole node detection scheme for hierarchical wireless sensor networks,'' Wireless Pers. Commun., vol. 94, no. 3, pp. 1165–1191, Jun. 2017.

[38] W. Stallings, Cryptography and Network Security: Principles and Practice, 5th ed. Upper Saddle River, NJ, USA: Prentice-Hall, 2010.

[39] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, ''Toward a lightweight intrusion detection system for the Internet of Things,'' IEEE Access, vol. 7, pp. 42450–42471, 2019.

[40] V. Sharma, I. You, K. Yim, I.-R. Chen, and J.-H. Cho, ''BRIoT: Behavior rule specification–based misbehavior detection for IoT–embedded cyber– physical systems,'' IEEE Access, vol. 7, pp. 118556–118580, 2019.

[41] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K.-K.-R. Choo, ''A two–layer dimension reduction and two–tier classification model for anomaly–based intrusion detection in IoT backbone networks,'' IEEE Trans. Emerg. Topics Comput., vol. 7, no. 2, pp. 314–323, Apr. 2019.

[42] W. Li, S. Tug, W. Meng, and Y. Wang, ''Designing collaborative blockchained signature-based intrusion detection in IoT environments,'' Future Gener. Comput. Syst., vol. 96, pp. 481–489, Jul. 2019.

[43] D. Breitenbacher, I. Homoliak, Y. L. Aung, N. O. Tippenhauer, and Y. Elovici, ''HADES-IoT: A practical host-based anomaly detection system for IoT devices,'' in Proc. ACM Asia Conf. Comput. Commun. Secur., Auckland, New Zealand, 2019, pp. 479–484.

[44] A. Mudgerikar, P. Sharma, and E. Bertino, ''E-spion: A system-level intrusion detection system for iot devices,'' in Proc. ACM Asia Conf. Comput. Commun. Secur., Auckland, New Zealand, 2019, pp. 493–500.

[45] A. Saeed, A. Ahmadinia, A. Javed, and H. Larijani, ''Intelligent Intrusion Detection in Low–Power IoTs,'' ACM Trans. Internet Technol., vol. 16, no. 4, pp. 1–25, Dec. 2016.

[46] M. Wazid, P. Reshma Dsouza, A. K. Das, V. Bhat K, N. Kumar, and J. J. P. C. Rodrigues, ''RAD–EI: A routing attack detection scheme for edge-based Internet of Things environment,'' Int. J. Commun. Syst., vol. 32, no. 15, p. e4024, Oct. 2019, doi: 10.1002/dac.4024.

[47] M. Wazid, A. K. Das, S. Kumari, and M. K. Khan, ''Design of sinkhole node detection mechanism for hierarchical wireless sensor networks,'' Secur. Commun. Netw., vol. 9, no. 17, pp. 4596–4614, Nov. 2016.

[48] M. Wazid and A. K. Das, ''A secure group–based blackhole node detection scheme for hierarchical wireless sensor networks,'' Wireless Pers. Commun., vol. 94, no. 3, pp. 1165–1191, Jun. 2017.

[49] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues, ''Authentication in cloud-driven IoT-based big data environment: Survey and outlook,'' J. Syst. Archit., vol. 97, pp. 185–196, Aug. 2019

[50] M. Wazid and A. K. Das, ''An efficient hybrid anomaly detection scheme using k–means clustering for wireless sensor networks,'' Wireless Pers. Commun., vol. 90, no. 4, pp. 1971–2000, Oct. 2016.

[51] M. Wazid and A. K. Das, ''A secure group–based blackhole node detection scheme for hierarchical wireless sensor networks,'' Wireless Pers. Commun., vol. 94, no. 3, pp. 1165–1191, Jun. 2017

[52] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. Rodrigues, ''Authentication in cloud-driven IoT-based big data environment: Survey and outlook,'' J. Syst. Archit., vol. 97, pp. 185–196, Aug. 2019.

[53] EBU Tech. Cross-Platform Authentication. Accessed: Oct. 2019. [Online]. Available: https://tech.ebu.ch/groups/CPA.