Phoenix: International Multidisciplinary Research Journal
Vol 3, No. 3, July-Sep, 2025
ISSN: 2583-6897

WIRELESS SENSOR NETWORK BASED INTRUSION DETECTION SYSTEM'S: A REVIEW

Dr Syed Umar
Professor, Department of Computer Science & Engineering, Malla Reddy (MR) deemed to be University, Hyderabad, syedumar@mrec.ac.in
Goli Madhuri
Assistant Professor, Department of computer science and engineering, Malla Reddy (MR) Deemed to be University, Hyderabad, golimadhurireddy120@gmail.com
Dikshendra Daulat Sarpate
Professor, Department of Artificial Intelligence & Data Science, ZEAL College of Engineering & Research, Pune, Email id -dikshendra@gmail.com
Gopala Soujanya
Assistant Professor, Department of computer science and engineering, Malla Reddy (MR) Deemed to be University, Hyderabad, Soujanyachiluka52@gmail.com
B.Rani
Assistant Professor, Department of computer science and engineering, Malla Reddy (MR) Deemed to be University, Hyderabad, rani@mrec.ac.in

Abstract— **A Wireless Sensor Network (WSN) based Intrusion Detection System's (IDS) primary goals are to increase network security and integrity via the effective utilisation of sensor nodes' limited resources.**

An IDS is to identify intrusions into a wireless sensor network (WSN). It has to be able to spot out-of-the-ordinary actions or patterns that may point to intrusion, data manipulation, or hostile assaults on the network. The IDS should offer prompt reactions to detected intrusions in order to lessen the severity of any security lapses. It should warn the central control system or administrators so they may take corrective action as soon as possible. The IDS should aim for high detection accuracy to minimize the false positives (FP) and false negatives (FN) rate. For effective intrusion detection, a middle ground must be found between sensitivity and specificity. The IDS has to be scalable so that it can work with WSNs of different sizes and in different deployment settings. It has to precede a growing number of sensor nodes without slowing down or otherwise degrading its ability to detect or react.

When these goals are met, the network's security posture is greatly improved, and the network's dependable and secure operation across a wide range of application domains is ensured.

Index Terms— Intrusion Detection Systems, Security, Wireless Sensor Network

I. INTRODUCTION

Wireless sensor networks (WSNs) have become more popular in recent years, as a critical technology in numerous fields, ranging from environmental monitoring to industrial automation and healthcare. These networks consist of small, autonomous sensor nodes capable of sensing, processing, and transmitting data, making them ideal for monitoring and gathering information in various environments. But there are also serious security issues that have arisen as a result of the widespread use of WSNs[1].

As WSNs are often deployed in remote or hostile environments, they are susceptible to a wide range of security risks, such as denial-of-service attacks, data manipulation, unauthorized access, and node compromise. Traditional security mechanisms, such as firewalls and encryption, are not sufficient to adequately protect these resource-constrained and distributed networks. Therefore, specialised security solutions are required to effectively identify and reduce possible intrusion occurrences.

The IntrusionDetection System (IDS) is a critical component in securing WSNs. An IDS is developed to detect suspicious and malicious activities within a network, ensuring timely detection and response to potential security breaches. Conventional IDS approaches developed for traditional the special features and limitations of WSNs may not be immediately applicable to wired networks, like limited computational power, communication bandwidth, and energy resources.

The research presents a thorough study on the development and execution of the Wireless Sensor Network-Based IntrusionDetection System (WSN-IDS). The primary objective of WSN-IDS is to detect and respond to various types of intrusion attempts and security violations in WSNs [2]. The system leverages the inherent advantages of distributed sensor nodes to collectively monitor the network and collaboratively analyse the data collected from the surrounding environment.

The following are the main attributes and contributions of the suggested WSN-IDS:

1. Distributed Monitoring: The WSN-IDS takes advantage of the spatial distribution of sensor nodes to monitor the network's physical environment comprehensively. Each sensor node is responsible for capturing local data and sharing relevant information with neighbouring nodes, enabling the system to maintain a global view of the network's health.

2. Machine Leaming and Data Fusion: To handle the enormous volume of data produced by sensor nodes efficiently, the WSN-IDS employs machine learning techniques and data fusion techniques. By analysing patterns and anomalies in the data, the system can identify potential intrusion events and differentiate them from normal network behaviour.

3. Self-Adaptation and Learning: The WSN-IDS is designed to adapt and learn from new data, enabling it to stay updated with emerging threats and attack patterns. This self- learning capability ensures that the system remains effective and accurate in detecting intrusion events, even in dynamic and evolving WSN environments.

4. Resource Optimisation: Given the resource constraints of WSNs, the WSN-IDS prioritises resource optimisation and energy efficiency. The system implements lightweight cryptography and adaptive sampling strategies to reduce data redundancy and communication overhead, thereby conserving valuable resources.

The evaluation of the WSN-IDS involves both simulation-based testing and real-world experimentation. Through rigorous testing, we assess the system's performance in terms of false positive rates, accuracy, resource utilisation, and responsiveness to different types of intrusion scenarios [3].

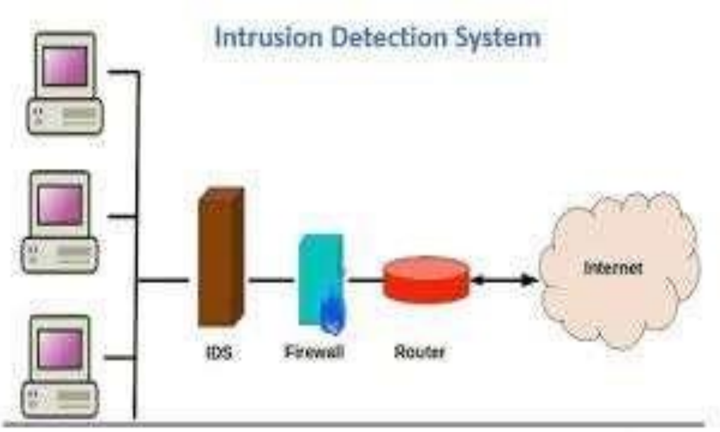

Figure 1 Intrusion Detection System's (IDS) based WSN [4]

The development of a reliable and efficient Intrusion Detection System for Wireless Sensor Networks is imperative to make sure the security and integrity of these pervasive networks. By leveraging the distributed nature of sensor nodes and employing machine learning techniques, the proposed WSN-IDS presents a promising solution to mitigate security threats and protect sensitive data in diverse WSN applications.

1. Cloud Computing: The word "cloud computing" is utilized to explain the process of offering computer services and resources through the internet rather than on the user's local machine or server. Cloud computing makes use of distant servers located on the internet to do different activities, rather than local PCs or servers.

Some of the cloud computing's most distinguishing features are Computing resources (such as processing time, storage space, and network connections) may be made available to users on demand, without the need for interaction from the service provider's staff.

2. Widespread network availability: Users may access cloud services from any internet- connected computer or mobile device.
3. To reduce costs and maximise efficiency, providers use a multi-tenant model in which numerous tenants share the same pool of computing and storage resources [5].
4. The cloud's scalability to meet fluctuating demands means that it can better accommodate businesses of various sizes.
5. Metered service: Customers only pay for resources they really use, on a metered or "pay as you go" basis. This maximises efficiency and helps put off costly infrastructure expenditures.

Cloud services may be broken down further according to the degree of abstraction and management they provide.

Provides virtualized computing resources such virtual computers, storage, and networking via the internet; sometimes abbreviated as "laaS." When using virtualized resources, users have more freedom in selecting which operating systems and programmes to run.

In contrast, PaaS allows developers to focus on creating, deploying, and managing apps rather than the underlying infrastructure. To facilitate this, PaaS furnishes resources like as tools, databases, and development frameworks.

SaaS (Software as a Service) is a model for delivering software to users without requiring them to download, install, and maintain the software locally. Software as a service (SaaS) programmes are those that may be accessed online and often include fees for subscription [6].

AmazonWeb Services (AWS), Microsoft Azure, GoogleCloud Platform (GCP), IBM Cloud, and others are all well-known sky service companies. These companies provide anything from simple data storage to advanced machine learning and AI services, meeting the demands of a broad variety of customers.

II. Overview of WSN

The wireless sensor network is the abbreviated form. Small, self-sufficient devices called wireless metres have sensors, computing power, and connected modules to form this sort of network. Together, these sensors may create a dispersed network to collect and share data about the conditions in which they are placed [7].

Among the most distinguishing features of WSNs are:
1. Wi-Fi, Bluetooth, and Zigbee are among the wireless communication protocols used by WSNs, and LoRa to relay information from sensors to a centralised control system.
2. Each WSN sensor node often has its own power supply and processing capabilities, making it independent and simple to install in a wide variety of settings.
3. The network's sensors are able to sense environmental conditions by using a wide range of sensors (temperature, humidity, motion, light, etc.).
4. WSNs are generally created to self-organize, which means the nodes may dynamically construct a network and adapt to changes in the network architecture to make it more robust and scalable.
5. Limited in power, memory, and computing capacity Sensor nodes in WSNs often have limited resources. As a consequence, developing WSNs with minimal energy consumption and maximum data optimization in mind is essential [8].

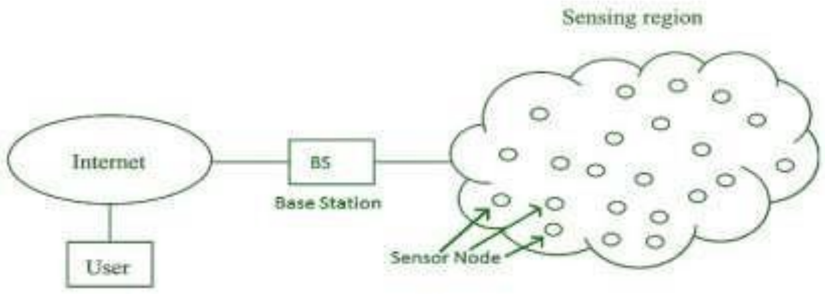

Figure 2 Wireless Sensor Networks [8]

Wireless sensor networks and their uses:
1. In distant or extreme locations, WSNs are used to keep tabs on things like temperature, humidity, air quality, and water quality.
2. WSNs may be used for condition monitoring of machinery and equipment in manufacturing and industrial environments, allowing for predictive maintenance and process optimization.
3. WSNs are used in agriculture to keep track of soil moisture, temperature, and crop health, which allows for more precise watering and better use of available resources.
4. WSNs may be utilized for home automation, allowing for the intelligent regulation of things like lighting, temperature, and appliances.
5. WSNs may be utilize for real-time data collecting, patient monitoring, and tracking of medical equipment.
6. WSNs may be installed in buildings and bridges to keep tabs on their condition and spot problems before they become major.

Because of their low initial investment, adaptability, and scalability, wireless sensor networks may be used in many situations where wired networks would be unfeasible or too costly.

Energy economy, data security, and communication dependability are just a few of the aspects that need to be considered while designing and deploying these systems.

III. Intrusion Detection System

The concept of an intrusion detection system (IDS) in the context of Wireless Sensor Networks (WSNs) includes a wide range of approaches to monitoring for and reacting to security breaches and other network irregularities. The concept of IDS by WSN is based on the idea that by learning about and accounting for the specifics of WSNs, effective intrusion detection systems may be developed. Key elements of IDS theory in WSNs are outlined here.

Methods of Intrusion Detection:

a. Detection based on Anomalies: Modelling the WSN's typical behaviour and then looking for variations to identify probable intrusions is what anomaly-based detection is all about. Methods like data mining, machine learning, and statistical analysis are used to build norms and spot outliers [9]. Attacks or other irregular occurrences could be indicated by suspicious behaviour.

b. Signature-based Detection: This method compares incoming data to a database of known attack patterns (signature). An attack is flagged when a match is made. While this method excels at spotting common assaults, it may have trouble with novel dangers.

Combining anomaly-based and signature-based detection improves the detection accuracy of hybrid intrusion detection systems. Hybrid IDS uses the advantages of both methods to improve attack detection while simultaneously decreasing false positives (FP) and false negatives (FN) [10].

The second part of the idea is picking the right sensor nodes to use as intruder alarms. For this aim, nodes are selected that have enough computational and sensory resources. The coverage of the network as a whole is taken into account throughout the choosing process.

Data preprocessing is crucial in IDS theory since it cleans up the raw sensor data before it can be analysed. To improve intrusion detection's precision and speed, it is necessary to clean, filter, and extract characteristics from the available data.

For deciding which traits to extract for use in intrusion detection is especially important in WSNs owing to limited resources. The aim of feature selection methods is to maintain the most useful characteristics for precise identification while reducing the complexity of the data. A reliable and effective protocol for transferring information about intrusions between sensor nodes and the control system is a must, according to the IDS idea [11]. This standard protects the privacy, security, and veracity of transmitted data.

The idea calls for the generation of an intrusion response system to efficiently deal with any identified incursions. In the case of an intrusion, the system may take one of many actions, such as isolating the affected nodes, adjusting the network's settings, or alerting the system administrators.

IDS theory for WSNs places a premium on energy efficiency as a primary design factor. Data aggregation, duty cycling, and localized processing are just a few of the methods used for intrusion detection that help save power.

Evaluation of Intrusion Detection System Performance is an Important Part of IDS Theory. The IDS's achievements is computed and improved focused on a *number of metrics, including its detection accuracy, false positive rate (FPR), false negative rate (FNR), and reaction time [12].

Security and privacy are cornerstones of IDS theory, which brings us to point number nine. The theory includes safeguards to prevent assaults on the IDS infrastructure and to keep private any sensitive information gathered by the WSN [13].

To sum up, the essential ideas underlying Intrusion Detection System through WSN are the refinement of intrusion detection methods, the enhancement of resource utilisation, and the protection of user privacy and data. The aim of IDS theory is to create a resilient and efficient security solution for many applications in our linked world through knowledge of the specific features and restrictions of WSNs.

IV. Challenges and Future Directions in IDS

Evasion Techniques and Defense Strategies

Intrusion Detection Systems (IDS) face a substantial obstacle in the form of evasion strategies since attackers are always looking for new ways to avoid being detected. In order to conceal harmful payloads and sidestep signature-based detection, attackers may fragment assaults, modify the packet headers of sent data, or utilise encryption. This section investigates a variety of evasion approaches and proposes defence measures that IDS may use to help offset the effects of these difficulties. Increasing detection capabilities may be accomplished via the use of techniques such as protocol normalisation, payload inspection, and traffic reassembly [14]. Additionally, adopting a mix of signature, anomaly, and behavior-based detection approaches may lower the efficacy of evasion efforts and increase the overall resilience of the intrusion detection system (IDS).

Privacy and Legal Considerations

As IDS track network traffic or the activity of hosts, privacy and legal problems become more important. The possible effect on user privacy, data protection rules, and compliance requirements is discussed in this section. It investigates the difficulties that arise when attempting to strike a symmetry between the requirements of efficient intrusion detection and the maintenance of user confidentiality. In addition, the section addresses issues over users' privacy by discussing various methods of data reduction and anonymization, as well as the need of open and honest communication with users. When adopting IDS, ensuring legal compliance and fostering confidence in the system may be accomplished by compliance with applicable rules pertaining to data protection and the formulation of detailed data use rules [15].

Scalability and Resource Constraints

Scalability issues and resource restrictions are two factors that might reduce the efficacy of intrusion detection systems (IDS), especially in large-scale networks or situations with limited resources. In this part, the difficulties of scaling intrusion detection systems (IDS) to handle high-volume traffic and the computational overhead associated with advanced detection approaches, like deep learning, are investigated and discussed. In order to improve scalability and make the most use of available resources, this study investigates several methods for deploying distributed IDS systems, including load balancing, the use of specialised hardware accelerators, and load balancing. In addition, adaptive sampling and traffic filtering algorithms are able to assist in relieving resource restrictions without affecting detection accuracy.

Advancements and Research Opportunities

In this part, we take a look at some of the fascinating recent developments and potential for study in the subject of IDS. Emerging technologies like quantum computing and edge computing are discussed, along with the potential influence these technologies might have on IDS capabilities [16,17]. In addition, it sheds light on the necessity of integrating threat intelligence feeds and machine learning approaches into IDS systems in order to increase detection accuracy and boost proactive defence. Opportunities for research may be found in the investigation of zero-trust architectures, sophisticated threat hunting methods, and the incorporation of artificial intelligence in order to develop IDS systems that are more resilient and autonomous.

V. Conclusion.

Although WirelessSensor Networks (WSNs) perform a crucial role in many applications, they are susceptible to security attacks due to their decentralised and limited nature. WSN's IntrusionDetection System (IDS) is built to safeguard these networks by monitoring for and reacting to security threats, keeping data secure and upholding network dependability.

Anomaly-basedDetection, signature-basedDetection, and hybrid methods are only some of the intrusion detection techniques used by the IDS to spot possible security breaches. The detection method based on signatures compares incoming data to a database of recognized attack types, whereas detection based on anomaly's uses a model of typical behaviour to identify outliers.

Sensor node selection, feature selection, and data preprocessing are important tenets of IDS theory for maximising detection precision while minimising resource consumption. Information shared about intrusions may be kept private and unaltered with the use of a secure communication protocol. In order to deal with discovered threats, the IDS employs an intrusion response mechanism. Depending on the severity of the intrusion, it may shut down the affected nodes, send an alert to the administrators, or take other preventative measures. The optimisation of IDS operations to minimize energy usage and enhance the lifespan of the network places a premium on energy efficiency. Metrics like as detection accuracy and reaction time may be utilized to compute an IDS's performance and reveal where it might be strengthened. In conclusion, the main goals of IDS using WSN theory are the improvement of detection methods, the maximisation of resource efficiency, and the protection of user confidentiality. IDS improves the trustworthiness and safety of WSNs in a variety of contexts by catering to their particular difficulties

Reference

[1] D. E. Baraneetharan, “Role of machine learning algorithms intrusion detection in WSNs: A survey,” Journal of Information Technology and Digital World, vol. 2, no. 3, pp. 161–173, 2020.

[2] Ferran Mohamed Amine et al. 2020, ‘Deep learning for cyber security intrusion detection: approaches, datasets & comparative study’, J Information Secure Appl., vol. 50, 102419.

[3] R. Vinayakumar, K.P. Soman, P. Poornachandran, Applying convolutional neural network for network intrusion detection, in: 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 1222–1228.

[4] Umar, Syed, Bommina Naveen Sai, Nagineni Sai Lasya,Doppalapudi Asutosh, and LohithaRani. "Machine Learning based Sentiment Analysis of Product Reviews Using DeepEmbedding." Journal of Optoelectronics Laser 41, no. 6(2022): 108-113.

[5] Saheed, YK 2022, ‘Performance improvement of intrusion detection system for detecting attacks on Internet of things and edge of things. In: Misra S, TKA, Piuri V, Garg L, editors, Artificial intelligence for cloud and edge computing’. Internet of things (technology, communications and computing). Cham: Springer; pp. 321-39.

[6] Kasongo, SM & Sun, Y 2021, ‘A Deep Gated Recurrent Unit based model for wireless intrusion detection system. ICT Express, vol. 7, no. 1, pp. 81-87.

[7] Nagalalli, G & Ravi, G 2022, ‘A Novel Megabat Optimized Intelligent Intrusion Detection System In Wireless Sensor Networks’, Journal of Intelligent Automation and Soft Computing, Tech Science Press, vol. 35, no. 1, pp. 475-490.

[8] S. Jiang, J. Zhao and X. Xu, “SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments,” IEEE Access, vol. 8, pp. 169548–169558, 2020.

[9] Habeeb, M. S., & Babu, T. R. (2022). Network intrusion detection system: a survey on artificial intelligence-based techniques. Expert Systems, 39(9), e13066.

[10] Naveen Sai Bommina, Nandipati Sai Akash, Uppu Lokesh, Dr. Hussain Syed, Dr. Syed Umar, "A Hybrid Optimization Framework for Enhancing IoT Security via AI-based Anomaly Detection",

International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169 Volume: 11 Issue: 3.

[11] Uppu Lokesh , Naveen Sai Bommina , Nandipati Sai Akash , Dr. Hussain Syed , Dr. Syed Umar. (2021). Deep Reinforcement Learning with Genetic Algorithm Tuning for Intrusion Detection in IoT Systems. International Journal of Communication Networks and Information Security (IJCNIS), 13(3), 582–595.

[12] Nandipati Sai Akash, Uppu Lokesh, Naveen Sai Bommina, Hussain Syed, Syed Umar, "Swarm Intelligence-Based Hyperparameter Optimization for AI-Powered IoT Threat Detection", International Journal of Intelligent Systems and Applications in Engineering, (2024), 12(17s), 941.

[13] Uppu Lokesh, Naveen Sai Bommina, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Designing Energy-Efficient and Secure IoT Architectures Using Evolutionary Optimization Algorithms", International Journal of Applied Engineering & Technology, Vol. 4 No.2, September, 2022.

[14] Habeeb, M. S. (2024). Predictive analytics and cybersecurity. Intelligent Techniques for Predictive Data Analytics, 151-169.

[15] hakre N, Nimma D, Turukmane AV, Singh AK, Rohatgi D, Bangaru B (2024) Dynamic path planning for autonomous robots in forest fire scenarios using hybrid deep reinforcement learning and particle swarm optimization. Int J Adv Comput Sci Appl 15(9).

[16] M. Mukhedkar, D. Rohatgi, V.A. Vuyyuru, K.V.S.S. Ramakrishna, Y.A. Baker El-Ebiary, V.A. Asir Daniel, "Feline wolf net: A hybrid lion-grey wolf optimization deep learning model for ovarian cancer detection", Int. J. Adv. Comput. Sci. Appl., 14 (9) (2023)

[17] Naveen Sai Bommina, Uppu Lokesh, Nandipati Sai Akash, Dr. Hussain Syed, Dr. Syed Umar, "Optimizing AI-Driven Security Protocols in IoT Networks Using Metaheuristic Algorithms", International Journal of Intelligent Systems and Applications in Engineering, IJISAE, 2024, 12(23s), 3339–3347.

[18]