International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 01 | Jan - 2025 SJIF Rating: 8.448 ISSN: 2582-3930

Machine Learning Algorithms for Intrusion Detection in WSNs

Arunendar Kumar Soni

Dr. Akhilesh a waoo

Abstract: Machine learning (ML) has emerged as a potent tool for optimizing network performance and extending network lifespans. By automating complex data processing tasks, ML algorithms enable real-time solutions that optimize resource allocation and utilization. ML's ability to process vast, intricate datasets with speed and precision empowers networks to adapt dynamically to evolving demands. [13]. Wireless Sensor Networks (WSNs), composed of interconnected sensor and sink nodes, exemplify the transformative potential of ML. These distributed, decentralized networks inherently possess self-organization and self-healing capabilities. By integrating ML techniques, WSNs can significantly enhance their efficiency, reliability, and scalability, enabling a wide array of applications, from environmental monitoring to military operations. As advancements in electronics and wireless communication continue to drive WSN evolution, the fusion of ML and WSNs promises to unlock new horizons in network intelligence and performance. However, WSNs face several challenges, including resource constraints such as limited memory, processing power, and energy. Additionally, the physical infrastructure of WSNs must be secured to protect sensitive data, especially in privacy-critical applications. To address these challenges, the integration of machine learning offers a promising solution. By leveraging ML techniques, WSNs can adapt to dynamic environments, optimize energy consumption, and detect and mitigate potential security threats. This enables the deployment of WSNs in diverse applications, from environmental monitoring to smart cities, while ensuring data privacy and system security.

Keywords: Intrusion Detection System (IDS), Security, Wireless Sensor Network (WSN), Attacks, Reinforcement Learning (RL), Denial-of-Service (DoS), Networks, Machine Learning (ML)

Introduction:

Wireless Sensor Networks (WSNs) are low-power devices that are widely used to collect data on human activities, environmental conditions, and other phenomena. Despite their numerous benefits, WSNs are susceptible to various security threats. There are two primary categories of attacks on WSNs: Passive and Active. Passive attacks involve eavesdropping on network traffic to steal sensitive information or degrade network performance. Active attacks, on the other hand, directly target the network infrastructure to disrupt its operation or compromise its security.

Wireless sensor networks (WSNs), comprising numerous autonomous sensors dispersed across a region and interconnected via wireless channels, are tasked with monitoring environmental and physical parameters such as temperature, sound, and pressure. WSNs typically exhibit two primary traffic patterns: many-to-one upstream traffic (from sensors to a central sink) and one-to-many downstream traffic (from the sink to the sensors). As data traffic within a WSN increases, congestion becomes a significant concern. To address this challenge, various implementation strategies and crucial requirements for effective WSN operation must be considered throughout the network lifecycle [29].

Common types of active attacks include jamming, which interferes with wireless communication, and denial-of-service (DoS) attacks, which overload the network. Other threats include Sybil attacks, where malicious nodes impersonate legitimate nodes, and wormhole attacks, which create shortcuts in the network. To mitigate these security challenges, a multi-layered approach is necessary. Intrusion Prevention Systems (IPS) can be deployed to prevent attacks by implementing measures like access control and encryption. Intrusion Detection Systems (IDS) can monitor network traffic for malicious activity and alert administrators to potential threats. By combining IPS and IDS technologies,

WSNs can significantly enhance their security. Timely detection and response to attacks are crucial to protect the integrity and confidentiality of the data collected by WSNs.

Wireless Sensor Networks (WSNs) present a complex challenge in terms of performance optimization. These networks are tasked with a diverse range of functions, from data collection and transmission to network security. To address these challenges, game theory can be employed in WSN design to mitigate various network intrusions, as illustrated in Figure 1.

WSN nodes are constrained by limited power resources, necessitating efficient energy management. To ensure reliable data transmission, WSNs must communicate with a

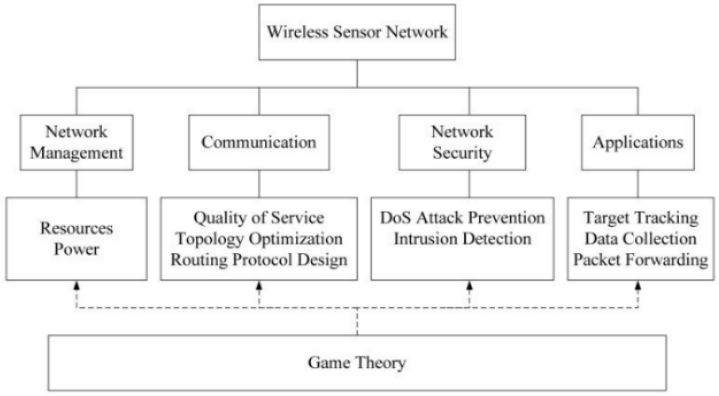


Fig.1 Design of WSN with Game Theory

remote base station within a specific timeframe. Key priorities for WSNs include robust security measures to prevent attacks like denial-of-service (DoS), as well as maintaining high quality of service (QoS). Additionally, WSNs play a crucial role in applications such as target tracking, data collection, and packet forwarding.

WSNs have some common security goals [16]. Added to this, they have

(1) Forward secrecy: preventing leak of secret messages when it leaves the internet.

(2) Backward secrecy: prevent decryption of already transmitted messages.

(3) Survivability: Services of some level are in lack of failure.

(4) Freshness: Making sure that the data are new and no one can repeat the old/previous messages. (5) Scalability: Handling a greater number of nodes.

(6) Efficiency: on sensor nodes like storage, communication border, and processing should not be measured.

Intrusions, unauthorized activities within a network or system, pose significant security risks. Intrusion Detection Systems (IDS) are tools designed to identify and differentiate these malicious actions. A robust network security strategy requires a comprehensive approach to safeguard against various threats, extending beyond the capabilities of a single IDS.

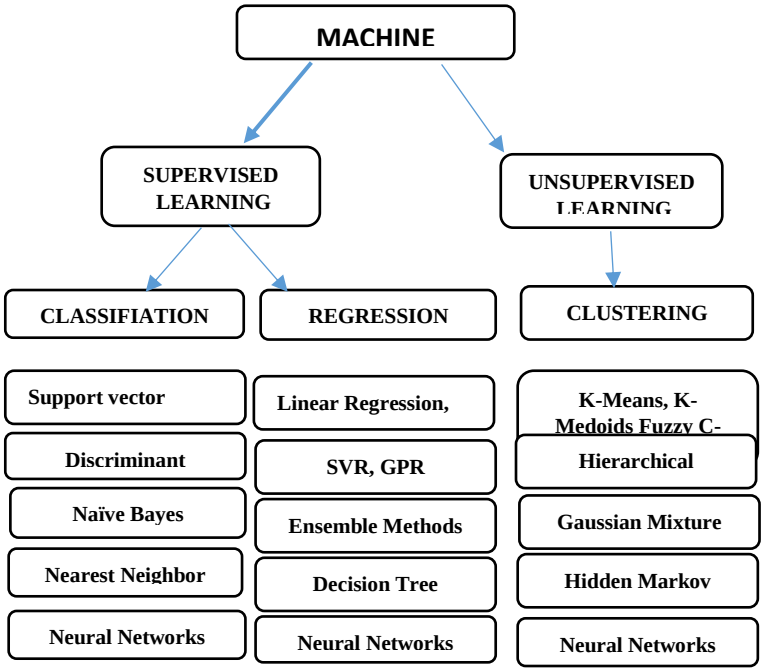
Intrusions can be categorized into two primary types:

1. External Intrusions: Unauthorized access originating from outside the network.
2. Internal Intrusions: Malicious activities initiated from within the network, often by compromised devices or insiders.

While IDS can effectively detect both external and internal intrusions, identifying internal threats can be more challenging due to the potential use of legitimate credentials. To ensure comprehensive security, it is crucial to deploy IDS on every device within the network [20].

Although IDS can partially respond to attacks, a proactive and layered security approach is necessary to mitigate risks and protect sensitive information. Intrusion Detection Systems (IDS) can be categorized into three types based on their deployment:

1. **Host-Based IDS (HIDS):** A HIDS is a software solution installed on individual hosts to monitor system activity and detect potential intrusions. It analyzes system logs and system calls to identify anomalies such as unauthorized access



Machine Learning (ML) provides a powerful toolkit for extracting valuable insights from WSN data. ML algorithms, classified into Supervised, Unsupervised, and Reinforcement Learning, can analyze labeled, unlabeled, or interactive data to identify patterns and make accurate predictions [28].

Supervised Learning models, such as classification and regression, are trained on labeled datasets to make precise predictions. Unsupervised Learning algorithms, on the other hand, delve into unlabeled data to uncover hidden patterns and relationships. Reinforcement Learning involves agents learning through interaction with an environment to optimize rewards.

By combining these ML techniques, we can unlock the full potential of WSN data, leading to innovative applications and improved decision-making processes.

2. Attempts, malicious code execution, and data breaches.
3. **Network-Based IDS (NIDS):** A NIDS monitors network traffic to identify suspicious patterns that may indicate an attack. It analyzes network packets to detect anomalies such as port scans, denial-of-service attacks, and unauthorized access attempts.

Hybrid IDS: A Hybrid IDS combines the features of both HIDS and NIDS to provide a more comprehensive security solution. It can monitor both host and network traffic to identify and respond to threats more effectively. Machine learning algorithms excel at creating precise models for prediction, classification, and clustering. This study leverages machine learning techniques such as Support Vector Machines and Logistic Regression to detect intrusions in wireless sensor networks (WSNs). [25]Additionally, Gaussian Naive Bayes, Random Forest, and Regression are employed to identify network threats.

Machine learning is indispensable for WSN applications due to the following reasons:

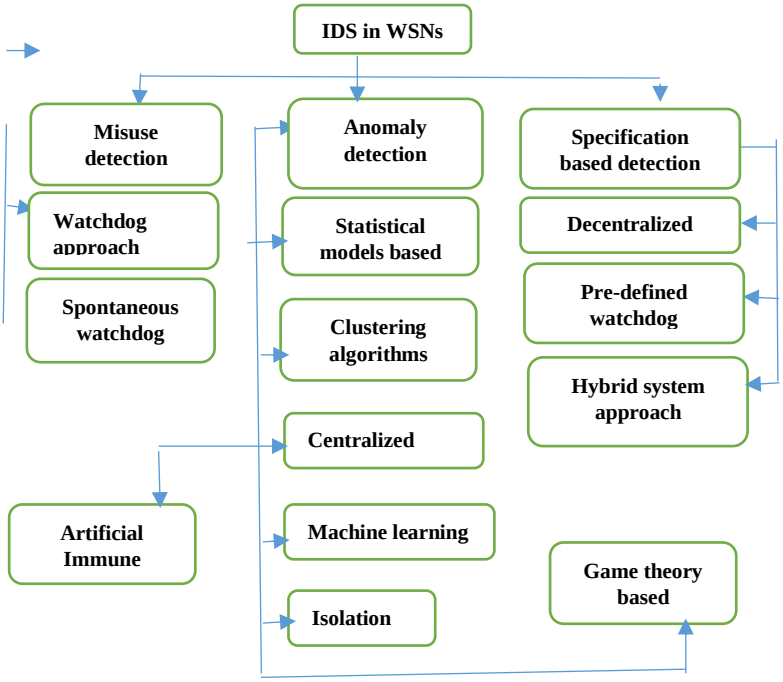
1. **Dynamic Environments:** Sensor networks monitor dynamic environments that are subject to rapid change.
2. **Complex Settings:** WSNs operate in complex scenarios that cannot be easily represented by simple mathematical models.

Noureddine Assad et al. present a model that guarantees coverage and synchronization in wireless K-sensing sensor networks. This model leverages geometric analysis and probabilistic models to optimize sensor deployment [24].

Sensor deployment quality, a critical factor influencing network performance and cost, necessitates careful consideration prior to implementation is not that easy. The proposed intrusion detection paradigm focuses on single-sensing/multi-sensing and k-sensing detection connectivity within WSNs. To realize this, measurements of total system node density, transmission range, and sensing range are essential. The findings reveal that the authors have developed and analyzed a novel WSN, enabling the selection of optimal internet parameters to fulfill WSN specifications.

Related Works

Machine learning is being used to develop intelligent intrusion detection systems (IDS) for wireless sensor networks (WSNs). These systems address inherent



Vulnerabilities and threats like unauthorized access, data breaches, and denial-of-service attacks. By analyzing network traffic patterns and detecting anomalies, these systems can employ sophisticated algorithms to proactively mitigate security risks [27]. In WSN, intrusion is considered as stealing data and creating false data by altering the system, which leads to gaining access to the system using an energy-efficient method. In this source, data is considered to be categorized into Network-Based Intrusion Detection, Hybrid-Based Intrusion Detection, and Host-Based Intrusion Detection techniques. Figure 3 explains the IDS in WSN. Based on the location of data, it is classified into two divisions: distributed and centralized IDS. Some of the machine learning approaches used in WSN are discussed below.

2.1 Anomaly Based Detection Approaches in WSN

Since WSNs are susceptible to various anomalies, they are categorized into network, node, data, and other anomalies. Network anomalies primarily relate to connection issues, such as signal loss, while node anomalies stem from hardware or software failures, often due to power supply or solar panel issues [26]. Data anomalies arise from inconsistencies within datasets or environmental factors affecting sensor readings. Other anomalies encompass those that do not fit into the aforementioned categories. Table 1 provides a comprehensive overview of several IDS detection methods employed in WSNs.

It is employed as a game-theoretic framework for WSN security and intrusion detection troubleshooting. This gaming feature is regarded as WSN's primary feature. Next, it utilizes Ultra Wide Band technology, which offers wireless communication with low battery consumption. The comparison of different detection methods is covered in Table 1. Incursions are detected using a rule-based method and a round-based algorithm. Both anomaly and misuse detection strategies are used in Wireless Sensor Networks (WSNs), from data mining techniques to intrusion detection systems. Then, IDS is composed of a central agent and a number of local agents. It is installed on the sensors to detect intrusion detection operations.

Table 1. Comparison of various Detection Techniques [11] [14] [15] [19]

IDS	Statistical models based	Clustering algorithm based	Artificial Immune System	Isolation table	Game Theory based	Machine Learning
Accuracy	Medium	High	High/Medium	Low	High/Medium	High
Energy efficiency	No detail	Yes	No	No detail	No	Yes
Memory Requirement	No detail	High	No detail	Medium	Medium	High
Network Structure	Normal	Clustered	Normal	Clustered	Normal/Distributed	Normal

2.2 Misuse Based Detection Approaches in WSN

Abuse detection, a signature-based intrusion detection system, is used to identify known attacks. However, its reliance on predefined signatures limits its ability to detect novel threats due to the lack of established standards. This approach is particularly challenging and less effective in WSNs [21].

WSNs utilize the Watchdog Based Clonal Selection Algorithm to identify intrusions. This algorithm examines nodes during data forwarding to detect anomalous behavior. It is responsible for providing information to nodes and monitoring their activity within the WSN. However, this constant surveillance can negatively impact WSN

performance. This approach is used to identify whether a WSN node is selfish or malicious. Then, it also utilizes the distance-vector routing protocol, or DSDV protocol, for DoS detection and replay attacks. This is predicated not only on accuracy but also on robustness and non-degradation of network performance. The DSDV protocol regularly updates the routing table, which not only saves energy on the nodes but also utilizes some of that energy as valuable bandwidth.

2.3 Hybrid Based Detection Approaches in WSN

The administrator manually defines each of WSN's security protocols. The hybrid approach combines methods for detecting anomalies and misuse. With the creation of protocol requirements, humans create hybrid detection approaches. It may or may not be applied as a combination technique. In order to create an accurate intrusion detection system, this method is also used for clustered wireless sensor networks. Additionally, it solves the two-class problem for anomaly detection and trains the SVM algorithm using a distributed learning approach. This strategy's primary goal is to reduce the network's energy consumption.

2.4 Clustering Based IDS in WSN

This method's primary application is in global decision-making and response. By allocating the subordinates that fall under the clustering, the approach aims to save energy for the majority of the nodes. Another name for it is Hierarchical-based IDS. As a single layer of promiscuous monitors, clustering is considered. These are employed in statistical anomaly detection to identify the misbehavior route. Using intrusion detection as a monitoring agent within each cluster, the cluster technique is utilized to protect the resources it continuously monitors [23]. Thus, this is installed on every node to keep an eye on local intrusions and investigate the causes of intrusions and responses. As a centralized and collaborative intrusion detection technique for the cluster method, this system also makes use of MANET. For WSN, this clustering-based IDS is far more advantageous. Because more batteries must be installed on the clusters for a longer lifespan, it has more energy than other nodes. The node with the highest energy among the other nodes is chosen on a regular basis to be the clustering node.

2.5 Trust Based IDS in WSN

The trust-based, or reputation-based, IDS fosters node cooperation by monitoring and evaluating their performance. The primary goal of this reputation system is to assess each node's contribution to the network. Nodes with higher reputations are more likely to be selected for communication by other nodes. This incentivizes nodes to improve their behavior to enhance their reputation and increase their opportunities for network interaction. Additionally, it includes three different kinds of reputations: subjective, indirect, and functional. Subjective reputations assess the direct interactions between a subject and their respective neighbors. Indirect reputations are determined by assessing the community's non-neighbors.

Functional Reputations consider subjective and indirect reputations, using a reputation table for data structure on nodes. DoS attacks are a drawback, so cooperation is enforced. Reputation mechanisms can prevent selfish nodes from executing DoS attacks. A DSR protocol rates nodes based on malicious behavior, with a Watchdog mechanism for suspicious activity and alarm messages from trusted nodes. This system updates reputation nodes only when messages arrive.

2.6 Zone-Based IDS in WSN

Zone-based IDS is divided into Gateway Zones and non-overlapping Zones, where agents broadcast alerts within these zones. Gateway Zones correlate local alerts and aggregate them for detection. Global aggregation and correlation engines aggregate and correlate local detection results. The aggregation algorithm achieves lower false positives but is not as efficient for Wireless Sensor Networks (WSNs).

2.8 Existing methods used in WSN

In WSN, other techniques are also employed, such as the watchdog mechanism, which is applied on top of the DSR

protocol to verify if the node is forwarding the packet to the subsequent node. This approach is more effective when used in WSNs. Next is Hybrid IDS, which may be applied to wired and ad hoc networks [22]. The performance is contrasted with that of the other nodes. WSN does not provide the end-to-end encrypted communication channels that this IDS requires in order to broadcast.

For managing some tactical networks, such infantry units and vehicle convoys, MANET is quite helpful. Additionally, it seeks to provide a MANET intrusion detection solution. The traffic in the network is then predicted using a traffic model based on the Auto Regressive Moving Average (ARMA) and time series data. It requires a centralized unit for processing traffic data, which is not present in WSN, because of the high volume of traffic data and the continuous monitoring of data packets in the network.

3. Wireless sensor network intrusion detection system based on MK-ELM

Weinjie Zhang et al. proposed a Multi-Kernel Extreme Learning Machine-based solution for WSN intrusion detection [5]. This hierarchical intrusion detection model utilizes a Mercer property-based algorithm to combine multiple kernel functions. By optimizing linear combinations, the multi-kernel extreme learning machine enhances the WSN intrusion detection system. After evaluating the performance of multi-kernel functions, the proposed solution demonstrated improved detection rates and reduced detection times. This approach is particularly suitable for resource-constrained wireless sensor networks.

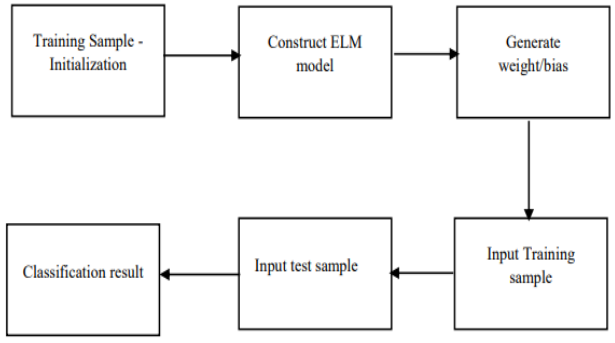


Fig.4 Flowchart of MK-ELM Algorithm

The extreme learning machine (ELM) is a solution that combines machine learning theory and quality optimization methods. It consists of neural networks with single-hidden-layer feedforward, enabling fast resolution speed. The MK-ELM algorithm uses kernel functions with various traits to advance multi-kernel functions. The structure of the MK-ELM can be influenced by kernel functions, and kernel parameter selection and type function are influenced by performance classification [26].

The MK-ELM ID algorithm is proposed for WSN infrastructure, integrating distinct functions of a single kernel, optimal kernel function selection, and parameter values. The system consists of nodes like sensors, cluster heads, sinks, and management. The wireless sensor network is congregated for undemanding management processes, and information is sent to the sink node via relay technique. The algorithm uses a hierarchical model, incorporating the KELM algorithm and multi-function kernel theory. The proposed algorithm aims to improve network operation stability.

4. Machine learning algorithms for wireless sensor networks

D. Praveen Kumar et al. proposed a comprehensive survey of Machine Learning methodologies for Wireless Sensor Networks (WSNs). The survey presents several ML-based algorithms, detailing their advantages, limitations, and parameter considerations [2]. It concludes with a statistical analysis and a discussion of ML techniques.

Supervised learning establishes a mapping between input and output sets during training. Upon completion, the model predicts primary outputs for given inputs. Regression, a supervised learning technique, predicts numerical values based on input features. It is a straightforward approach often yielding accurate results. Decision trees, another supervised learning method, construct models to classify data into categories based on decision rules [20]. The Random Forest methodology is a supervised machine learning method that uses all of the trees in the forest to classify data. It works effectively with large datasets and even modifies the values that are overlooked.

The findings regarding the performance of various machine learning algorithms, such as K-Nearest Neighbor (KNN), Logistic Regression (LR), Support Vector Machine (SVM),

Gboost, Decision Tree (DT), Naïve Bayes, Long Short Term Memory (LSTM), and Multi-Layer Perceptron (MLP), on different performance metrics are significant [19]. Singleton value decomposition is a factorization method that does not decrease dimensionality with matrix product. Principle and independent component analyses combine information and multivariate estimations. Semi-supervised learning aims to predict unlabeled labels from data. Reinforcement learning accumulates information to control actions by interconnecting with the environment.

5. Investigation of Computational Intelligence techniques for IDS in WSNs

Focused on using machine learning algorithms for detecting Denial of Service (DoS) attacks in Wireless Sensor Networks (WSNs) addresses a critical issue in network security. The experiment using WEKA to evaluate the efficiency of five machine learning algorithms for detecting various types of DoS attacks (flooding, grayhole, blackhole, and scheduling) is a valuable contribution to the field.

The finding that the random forest classifier outperforms the other classifiers with an accuracy of 99.72% is significant, demonstrating the effectiveness of machine learning in DoS attack detection in WSNs. This result could have important implications for improving the security of WSNs against such attacks [8].

Cyberattacks in Wireless Sensor Networks (WSNs) are categorized into active and passive attacks. Passive attacks involve monitoring vulnerabilities and information gathering, while active attacks entail data manipulation, targeted routing disruptions, or unauthorized network access.

Focused on using machine learning algorithms for detecting Denial of Service (DoS) attacks in Wireless Sensor Networks (WSNs) addresses a critical issue in network security. The experiment using WEKA to evaluate the efficiency of five machine learning algorithms for detecting various types of DoS attacks (flooding, grayhole, blackhole, and scheduling) is a valuable contribution to the field [18]. Signature-based and anomaly-based ID methods, such as artificial neural networks, are used for anomaly detection. Feedforward and Feedback networks are two ANN architectures. SVM supervised machine learning algorithms are used for complex problems and classification and regression tasks.

6. Machine Learning in WSN

Machine Learning addresses issues in Wireless Sensor Networks (WSNs) by evaluating pros and cons against the problems. Supervised learning includes various algorithms, such as K-nearest neighbors, decision trees, and neural networks. K-nearest neighbors categorize sample data based on output values, while decision trees classify input values and compare properties to decision conditions. Neural networks are built by surging bonds of decision elements and are composite and non-linear.[1] An approach for detecting malicious actions of nodes is used to estimate secular and structural data collections.

Proposed an IDS leveraging a variety of prominent machine learning classifiers, including Random Tree, Bayesian Network, Artificial Neural Network, Decision Tree, Decision Table, Random Decision Forest, and Naive Bayes classifier. The KDD’99 dataset was used for training and testing. Various performance indicators, such as recall, precision, F1-score, and overall accuracy, were assessed to evaluate the model's performance [15]. These challenges require both functional and non-functional approaches to ensure successful WSN design

7. ML techniques to solve WSN issues

Machine Learning techniques are used to solve twelve issues in Wireless Sensor Networks (WSNs), including localization, routing, mobile sink, event detection, congestion control, MAC, coverage and connectivity, data aggregation, energy harvesting, target tracking, anomaly and fault detection, and synchronization. Localization is solved using Reinforcement Learning and k-NN, while routing uses Decision trees, Evolutionary computation, and Random forest to predict optimal paths for data traffic control. Mobile sink uses Evolutionary computation, Random forest, and Reinforcement Learning to select optimal sink paths between sensor nodes. Event detection uses PCA, Deep Learning, and

ICA for efficient duty cycling management and event detection from sensor data [2].

The fifth issue involves congestion control using Random Forest, Decision Tree, SVM, PCA, ICA, Evolutionary computation, and Reinforcement Learning. It predicts congestion locations and finds alternate routing paths. The sixth issue uses MAC, Decision Tree, Deep Learning, and SVM for reconfiguring sensor nodes and channel assignment. The seventh issue deals with coverage and connectivity, using Decision Tree and Deep Learning for classification and minimum sensor number. The eighth issue deals with data aggregation using SVM, Reinforcement Learning, and k-means.[17]

Addresses a critical issue in wireless sensor networks (WSNs) regarding the trade-off between energy consumption and security. It's interesting that you're proposing machine learning algorithms as a solution to improve security while considering the energy constraints of WSNs [14].This research aims to accurately predict energy harvesting potential and allocate it efficiently within specific time slots.

The tenth issue explores the realm of target tracking, leveraging the power of Deep Learning, Decision Trees, and SVM. These advanced algorithms enable precise tracking of targets, even in complex and dynamic environments.

The eleventh issue focuses on the critical task of anomaly and fault detection in various systems. By employing Principal Component Analysis (PCA), Independent Component Analysis (ICA), Random Forest, and Deep Learning, this research seeks to identify and address potential issues proactively.

The final issue addresses the synchronization challenge in communication networks. Deep Learning-based approaches are employed to optimize channel allocation and dynamically resynchronize the network, ensuring efficient and reliable communication.

These cutting-edge techniques are indispensable for optimizing energy harvesting systems, enhancing target tracking accuracy, detecting anomalies and faults promptly, and ensuring seamless network synchronization.

8. Energy-efficient learning solution for intrusion detection in wireless sensor networks

The protocol is a simple, low-energy approach that leverages learning automata to sample packets and create an energy-aware Intrusion Detection System (IDS). Its self-learning and decentralized nature allows compromised nodes to be bypassed, making it a robust solution for addressing vulnerabilities in wireless sensor networks.[9] By filtering malicious packets at individual nodes, this protocol offers a more granular and efficient security approach.

The primary objective is to detect and mitigate malicious data while optimizing network power consumption. A learning system is employed to identify and eliminate harmful packets [11]. A learning automata-based intrusion detection model is utilized within wireless networks. The S-LAID system monitors packets transmitted by attackers and employs rate control mechanisms. Reward and penalty functions regulate sampling rates. System performance is evaluated based on the false positive rate and the number of detected packets.

9. Performance evaluation of supervised machine learning for Intrusion Detection

Intrusion Detection Systems (IDS) are predictive network security systems that utilize machine learning algorithms such as Logistic Regression, Gaussian Naive Bayes, Support Vector Machine, and Random Forest. By monitoring network traffic, IDS can identify potential security breaches, making it a valuable tool for advanced network technologies like wireless devices [10]. Machine Learning-based IDS can be categorized into anomaly-based and misuse-based systems. Misuse-based IDS detect known attack patterns, while anomaly-based IDS identify novel and previously unseen attacks. Integrated IDS approaches, combining techniques like Artificial Neural Networks, Support Vector Machine, and Naive Bayes, offer a comprehensive and robust solution for network security.

Proposes an innovative approach to enhance the security of Wireless Sensor Networks (WSNs) by leveraging machine learning and artificial intelligence techniques. The study focuses on identifying and preventing cyberattacks through a series of steps:

Feature Reduction: The study uses Singular Value Decomposition (SVD) and Principal Component Analysis (PCA) for feature reduction, which helps in reducing the dimensionality of the dataset and improving the efficiency of the model.

Feature Extraction: The K-means clustering model enhanced with information gain (KMC-IG) is employed for feature extraction, which helps in selecting the most relevant features for intrusion detection [12].while the standard KDDCUP99 intrusion detection dataset did not yield satisfactory results, an advanced version incorporating 42 features and simulating 4 attack types demonstrated improved performance.

This information can be exploited to compromise system vulnerabilities and gain unauthorized access, such as elevated privileges (e.g., Perl, xterm). Probe-response attacks typically target specific or small groups of clients, leaving distinct signatures in system or network intrusion alerts. Remote-to-local (r2l) attacks aim to gain unauthorized access to a target machine within a network. Similarly, user-to-root (u2r) attacks involve escalating privileges to gain root access on a locally accessed machine without authorization.

Categorical data is converted into numerical form, divided into testing and training data. Different models predict test data labels, and true and false rates are calculated. Supervised machine learning classifiers are used for intrusion detection, with random forest classifiers showing promising results based on observation.

10. Future Applications of Machine Learning in WSN

Machine Learning techniques have been applied to many research areas [1]. Some of the future applications of Machine Learning in WSN are:

1) Compressive Sensing and Sparse Coding

2) Distributed and Adaptive Machine Learning Techniques for WSN

3) Resource Management Technique using Machine Learning

4) Detecting Data Spatial and Temporal Correlations using Hierarchical Clustering.

1) Compressive Sensing and Sparse Coding

Measurements from the sensor are necessary to keep the detection accuracy high. Eighty percent of energy is reportedly used for data transmission and reception. Data compression and dimensionality reduction techniques are two methods used to decrease transmission and increase the network's lifetime

2) Distributed and Adaptive Machine Learning Techniques for WSN

WSNs and other devices with limited resources are a good fit for machine learning techniques. Despite this, processing the data requires less processing power [5]. The nodes can anticipate and adjust to future behavior in the current environment thanks to these decentralized learning mechanisms. For instance, "Adaptive Regularization of Weights."

3) Resource Management Technique using Machine Learning

Energy conservation in WSN is the primary concern. Two methods are used: the first addresses the OSI layers (physical, MAC, and network layer), and the second focuses on reducing the amount of energy used for small and non-functional requirements.

4) Detecting Data Spatial and Temporal Correlations using Hierarchical Clustering

To establish a hierarchical cluster structure, Hierarchical Clustering, an unsupervised learning algorithm, is employed. This approach involves partitioning the set of sensor nodes into smaller, more manageable clusters. Clustering criteria such as temporal data correlations and geographical proximity are leveraged in this novel WSN approach.

Hierarchical Clustering offers energy-efficient strategies by activating only a single node from each cluster at a specific time, ensuring comprehensive coverage and monitoring of the entire network area.

References

1. Alsheikh, M. A., Lin, S., Niyato, D., & Tan, H. P. (2014). Machine learning in wireless sensor networks: Algorithms, strategies, and applications. IEEE Communications Surveys & Tutorials, 16(4), 1996-2018.
2. Kumar, D. P., Amgoth, T., & Annavarapu, C. S. R. (2019). Machine learning algorithms for wireless sensor networks: A survey. Information Fusion, 49, 1-25
3. Maleh, Y., Ezzati, A., Qasmaoui, Y., & Mbida, M. (2015). A global hybrid intrusion detection system for wireless sensor networks. Procedia Computer Science, 52, 1047-1052.
4. Zhang, W., Han, D., Li, K. C., & Massetto, F. I. (2020). Wireless sensor network intrusion detection system based on MK-ELM. Soft Computing, 1-14.
5. Alrajeh, N. A., Khan, S., & Shams, B. (2013). Intrusion detection systems in wireless sensor networks: a review. International Journal of Distributed Sensor Networks, 9(5), 167575.
6. Butun, I., Morgera, S. D., & Sankar, R. (2013). A survey of intrusion detection systems in wireless sensor networks. IEEE communications surveys & tutorials, 16(1), 266-282.
7. McDermott, C. D., & Petrovski, A. (2017). Investigation of computational intelligence techniques for intrusion detection in wireless sensor networks. International journal of computer networks and communications, 9(4).
8. Aliady, Wateen A., and Saad A. Al-Ahmadi. "Energy preserving secure measure against wormhole attack in wireless sensor networks." *IEEE Access* 7 (2019): 84132-84141.
9. Belavagi, M. C., & Muniyal, B. (2016). Performance evaluation of supervised machine learning algorithms for intrusion detection. Procedia Computer Science, 89(2016), 117-123. 11. Tan, X., Su, S., Huang, Z., Guo, X., Zuo, Z., Sun, X., & Li, L. (2019). Wireless sensor networks intrusion detection based on SMOTE and the random forest algorithm. Sensors, 19(1), 203.
10. Amouri, A., Alaparthy, V. T., & Morgera, S. D. (2020). A Machine Learning Based Intrusion Detection System for Mobile Internet of Things. Sensors, 20(2), 461.
11. Yu, Z., & Tsai, J. J. (2008, June). A framework of machine learning based intrusion detection for wireless sensor networks. In 2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008) (pp. 272-279). IEEE.
12. Behiry, Mohamed H., and Mohammed Aly. "Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods." *Journal of Big Data* 11.1 (2024): 16.
13. Soliman, H. H., Hikal, N. A., & Sakr, N. A. (2012). A comparative performance evaluation of intrusion detection techniques for hierarchical wireless sensor networks. Egyptian Informatics Journal, 13(3), 225- 238.
14. Ahmad, Rami, Raniyah Wazirali, and Tarik Abu-Ain. "Machine learning for wireless sensor networks security: An overview of challenges and issues." *Sensors* 22.13 (2022): 4730.
15. Kumar, Gulshan, and Hamed Alqahtani. "Machine Learning Techniques for Intrusion Detection Systems in SDN-Recent Advances, Challenges and Future Directions." *CMES-Computer Modeling in Engineering & Sciences* 134.1 (2023).
16. Li, G., He, J., & Fu, Y. (2008). Group-based intrusion detection system in wireless sensor networks. Computer Communications, 31(18), 4324-4332.
17. Chen, R. C., Hsieh, C. F., & Huang, Y. F. (2009, February). A new method for intrusion detection on hierarchical wireless sensor networks. In

Proceedings of the 3rd International Conference on Ubiquitous Information Management and Communication (pp. 238-245).

18. Al-Ahmadi, Saad. "Secured Aodv to protect WSN against malicious intrusion." *International Journal of Network Security & Its Applications (IJNSA) Vol* 12 (2020).
19. Wazirali, Raniyah, and Rami Ahmad. "Machine Learning Approaches to Detect DoS and Their Effect on WSNs Lifetime." *Computers, Materials & Continua* 70.3 (2022).
20. Hai, T. H., Khan, F., & Huh, E. N. (2007, August). Hybrid intrusion detection system for wireless sensor networks. In International Conference on Computational Science and Its Applications (pp. 383-396). Springer, Berlin, Heidelberg.
21. Yan, K. Q., Wang, S. C., & Liu, C. W. (2009, March). A hybrid intrusion detection system of clusterbased wireless sensor networks. In Proceedings of the International MultiConference of Engineers and Computer Scientists (Vol. 1, pp. 18-20).
22. Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks.
23. Raymond, D. R., & Midkiff, S. F. (2008). Denial-of-service in wireless sensor networks: Attacks and defenses. IEEE Pervasive Computing, 7(1), 74-81
24. Mubarak, T. M., Sattar, S. A., Rao, G. A., & Sajitha, M. (2011, March). Intrusion detection: An energy efficient approach in heterogeneous WSN. In 2011 International Conference on Emerging Trends in Electrical and Computer Technology (pp. 1092-1096). IEEE.
25. Islam, M. S., & Rahman, S. A. (2011). Anomaly intrusion detection system in wireless sensor networks: security threats and existing approaches. International Journal of Advanced Science and Technology, 36(1), 1-8.
26. Singh, S. K., Singh, M. P., & Singh, D. K. (2011). Intrusion detection- based security solution for clusterbased wireless sensor networks. International Journal of Advanced Science and Technology, 30(83).
27. Jadidoleslamy, H. (2011). A high-level architecture for intrusion detection on heterogeneous wireless sensor networks: hierarchical, scalable and dynamic reconfigurable. Wireless Sensor Network, 3(07), 241.
28. Zhang, Y., Meratnia, N., & Havinga, P. (2010). Outlier detection techniques for wireless sensor networks: A survey. IEEE communications surveys & tutorials, 12(2), 159-170
29. Akhilesh A. Waoo, Varsha Tiwari , Review of Congestion Control Techniques in Wireless Sensor Network , International Journal of Research Publication (Volume: 3, Issue: 1), http://ijrp.org/paper_detail/86