Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 44 No. 5 (2023)

A Novel Random Forest Adaptive Response Mechanism (RFARM) Intrusion Detection And Prevention In WSN

[1] Mr. S. Prabhu, [2] Dr. C. Chandrasekar,

[1]Research Scholar, Department of Computer Science, Government Arts College, Udumalpet -642126, India.
[2]Head, Department of Computer Science Government Arts and Science College, Mettupalayam - 641104, India.

Abstract – This paper introduces a novel Random Forest Adaptive Response Mechanism (RFARM) for intrusion detection and prevention in Wireless Sensor Networks (WSNs). RFARM leverages the power of random forests, combining ensemble learning and adaptive response strategies to identify and thwart malicious activities effectively. The proposed mechanism continually learns from network data, adapts its response based on the severity and nature of detected intrusions, and employs a robust preventive framework. Simulation results demonstrate RFARM's superior performance in terms of detection accuracy, false positive rate, and network resilience, making it a promising solution to bolster security in WSNs.
Keywords: Random Forest, Intrusion Detection and Prevention, Wireless Sensor Networks, Adaptive Response, Security, Ensemble Learning.

1. Introduction

Intrusion Detection and Prevention Systems (IDPS) act as pivotal points of support in the domain of network security, standing sentinel against the determined tide of unapproved access, pernicious exercises, and the always advancing scene of cyber dangers. Inside the perplexing ecosystem of wireless sensor networks (WSNs), the presence and viability of IDPS are amplified, expecting a vital job in maintaining the holiness of data transmission by safeguarding its integrity and confidentiality. This extensive presentation dives into the complex universe of IDPS, clarifying its fundamental parts and the significant importance it holds inside the powerful setting of wireless sensor networks. Wireless Sensor Networks (WSNs), a gathering of little, energy-proficient sensor nodes, address an unavoidable mechanical worldview equipped for gathering and sending data across different domains, from environmental monitoring to modern computerization. In any case, the universality and far off sending of these networks render them especially vulnerable to a variety of security dangers, going from data snooping and altering to the split the difference of individual nodes. It is here that the job of an Intrusion Detection and Prevention System (IDPS) comes to the front.

At its center, Intrusion Detection encompasses the persistent surveillance of network traffic and the monitoring of system exercises, all with the insightful eye of distinguishing any touch of dubious or unapproved conduct. With regards to WSNs, this involves a cautious watch for peculiarities in data transmission, strange hub activities, or deviations from expected network traffic patterns. In any case, the domain of security reaches out past simple detection, encompassing the proactive strongholds intrinsic to Intrusion Prevention. In WSNs, this proactive position might appear as the confinement of compromised nodes, the redirection of data streams, or the stronghold of the network through security measures like encryption and confirmation. The mind boggling hardware of an IDPS in WSNs contains a few related parts, including the sensor nodes themselves, liable for endlessly gathering and sending data. Indispensable to its usefulness is the perplexing trap of calculations and data analysis techniques utilized to examine approaching data, knowing the subtlest of inconsistencies or patterns characteristic of beginning intrusion endeavors. The meaning of an IDPS with regards to wireless sensor networks couldn't possibly be more significant. It remains as the vanguard against tricky dangers that could think twice about holiness of data transmission inside these networks. By keeping a constant vigil and sending responsive countermeasures, an IDPS guarantees that the principal precepts of data security confidentiality, integrity, and availability are maintained, subsequently fortifying WSNs and delivering

them tough despite a wide spectrum of cyber risks. Fundamentally, an IDPS is the sentinel of trust and security in the multifaceted woven artwork of wireless sensor networks, where the commitment of imaginative applications, from environmental monitoring to modern robotization, pivots upon the safeguarding of data integrity and confidentiality.

2. Literature Survey

2.1 Times-Domain Reflectometry (TDR)

D. K. Yadav (2019) et.al proposed Design of Real-Time Slope Monitoring System Using Time-Domain Reflectometry with Wireless Sensor Network. Electronic instrumentation, including piezometers, wire-line extensometers, and all-out stations, is used to measure the degree of inclination. The more expensive distant observational systems like SSR, LiDAR, and laser scanning are available. To defeat this, effective and financially feasible estimation systems for slant monitoring are required. The focal point of this research is basically on the Radio Frequency (RF) module, Time-domain Reflectometry (TDR), Graphical User Interface (GUI) and communicating unit. The RF module and the connecting unit were integrated with TDR to procure the data, and data move calculation was created for the foundation of wireless communication and tried in the lab. In this research, based on the lab tests for foundation of size of disfigurement of coaxial link using TDR, Advancement of wireless communication modules and Field explore different avenues regarding TDR-WSN system following ends were made.

2.2 Pattern Matching Intrusion Detection Technique

G. Kalnoor (2016) et.al proposed Pattern matching intrusion detection technique for Wireless Sensor Networks. Wireless Sensor Network (WSN) is a network with huge number of small sensor gadgets which are of minimal expense, and least utilization of force called as sensor nodes. These kinds of nodes have incredible detecting innovation which is explicitly intended for applications, for example, military, savvy homes and other security related regions. It is conveyed in the greater part of the unattended conditions where any sort of foes might pay attention to the traffic and infuse their own nodes in the sensor network. Research fundamental objective of safety is to consider imperative regions in which intrusion attack or danger is conceivable and to recognize them using second method of protection. The objective of the attacker can be many based on the sort of harm he needs to cause the sensor network. Some of them might be hearing of private data, or infusing bogus data which might influence the presentation of the network. In particular, WSN should be safeguarded from pernicious exercises to occur and in this manner security turns into a significant issue.

2.3 Wireless Intrusion Detection Prevention and Attack System (WIDPAS)

J. Abo Nada (2018) et.al proposed Wireless Intrusion Detection Prevention and Attack System. This research, Wireless Intrusion Detection Prevention and Attack System, or "WIDPAS," will address the development of an intrusion detection system for wireless networks. It is based on three primary undertakings: monitoring, analysis and defense. Through which it monitors disavowal of administration attacks or misleading networks and afterward investigates the assault and recognizes the assailant and afterward safeguards the network clients. Wireless intrusion discovery accessible arrangement system in the business sectors, including business or free open source, and applies the greater part of the elements of recognition and decide the sort of assault What research included this research is to expand the viability of the system in the workplace where the system can monitor a large portion of the attacks and the system can Shield the network from fake networks by going after the aggressor and cut the way towards the aggressor and safeguard the staff from being defrauded. Wireless advancements have arisen as an option in contrast to wired advances, because of the simplicity of arrangement and use in homes, workplaces or even in government and military foundations or privately owned businesses.

2.4 Mobile Agent

L. Gandhimathi (2016) et.al proposed Cross layer intrusion detection and prevention of multiple attacks in Wireless Sensor Network using Mobile Agent. Increased interest in the use of Wireless Sensor

Networks (WSNs) is a result of technological advancement. The sensor nodes in WSNs are deployed in an area that is open and unprotected. As a result, a variety of attacks, including sinkhole, wormhole, and Sybil attacks, can target sensor networks. In many-to-one communication, the antagonist draws the neighbor nodes in the area with false directional information and made-up characters. One-layer attacks have been the focus of recent research. Wireless Sensor Network is shaped using spatially dispersed independent sensor gadgets used to monitor physical or environmental conditions. WSNs are generally used in numerous applications, for example, medical care system, smart lighting sensor, Railway Bridge, military application, crisis response operations like a flood, earthquake, and so on. All the sensor nodes send their detected data to base station through different hops. The proposed framework doesn't thoroughly sidestep the aggressor hub and it advances the data from its neighbors if and provided that three way handshaking is effectively finished. Thus it diminishes the bogus positive rate.

2.5 Frequency Analysis

V. Choudhary (2021) et.al proposed An Intrusion Detection Technique Using Frequency Analysis for Wireless Sensor Network. This study provided a method for locating interference or network intrusion that depends on frequency analysis at the site. This method involves sending application sensors and specialized intrusion detection sensors throughout the network. These specialized sensors continuously listen for the intrusion's frequencies. These specialized sensors' data are kept in a fuzzy analytical engine for further analysis. The data from these dedicated sensors are stored in a fuzzy analytical engine for inference. The proposed technique consumes fewer assets in contrast with different methods. This research zeroed in on detecting the intrusion based on frequency scanning and analysis as a different substance integrated with wireless sensor networks, where devoted sensors persistently scanning the network for undesirable frequencies. Based on frequencies analysis at the back end choices about intrusion in the wireless network can be taken. Researches have proposed the simulation for just two info factors for analysis, yet it is feasible to enter n quantities of parameters' for analysis of the security edge for a network.

3. Proposed Methodology

Wireless Sensor Networks (WSNs) are essential for many applications, including industrial automation, healthcare, and environmental monitoring. However, their vulnerability to security threats calls for robust Intrusion Detection and Prevention Systems (IDPS). In this proposed methodology, research outline a comprehensive approach to designing and implementing an IDPS tailored for WSNs. Research strategy includes data preprocessing, feature selection, machine learning-based intrusion detection, and preventive measures. By leveraging machine learning algorithms and a holistic security framework, this IDPS aims to safeguard the integrity and availability of WSNs.

3.1 Sensor Node Collaboration:

In IDPS, sensor nodes collaborate by sharing intrusion-related data and observations within the network. This collaboration facilitates early detection and prevention of intrusion attempts. Nodes exchange information about suspicious activities, enabling collective decision-making for intrusion response Cooperation improves intrusion detection accuracy and lowers the possibility of false positives.

3.2 Machine Learning for Anomaly Detection:

To improve anomaly-based intrusion detection, research introduces machine learning algorithms to model normal network behavior. IDPS employs supervised and unsupervised learning techniques to create behavioral profiles for sensor nodes and the network as a whole. Deviations from these profiles trigger intrusion alerts. The machine learning models are continuously updated to adapt to changing network conditions and evolving attack patterns.

Random Forest Classification Model:

The suggested classification model is comprised of random forest (RF) algorithm. Changing the training set with the same bagging procedure is how an ensemble of classifiers in Random Forest is constructed

(Breiman, 1996). Bagging creates new training sets by resampling from the original data set n times, n being the number of samples in the original training set, randomly with replacement. This means the sample just being chosen will not be removed from the data set in the next draw. Hence, some of the training samples will be chosen more than once while some others will not be chosen at all in a new set. By lowering the variance of the classification mistakes, bagging improves classification accuracy. Put another way, it interferes with a classifier's instability. A classifier is said to be "instable" if very minor modifications to the training set cause noticeably large variations un accuracy. The classifiers are combined by a majority vote and the vote of each classifier carries the same weight. In the event of a tie, a random choice or set of rules may be used. Using the impurity gini index, Random Forest generates several trees (Breiman et al., 1984). On the other hand, Random Forest just looks for a random subset of the input features (bands) at each splitting node when building a tree, and it is left to grow to its maximum potential without any pruning. The computational cost of Random Forest is quite low because no pruning is done and only a part of the input features are used. Additionally, an out-of-bag approach can be applied in the event that a separate test set is unavailable. One-third of the samples are arbitrarily excluded from each newly created training set; these samples are known as the "out-of-bag" (OOB) samples. One uses the leftover (in-the-bag) samples to construct a tree. Votes for each sample are counted each time they correspond to an OOB sample in order to estimate accuracy. A majority vote will determine the final label. Only approximately one-third of the trees built will vote for each case. In numerous testing, these OOB error estimates are objective (Breiman, 2001). The number of features for each split has to be defined by the user, but it is insensitive to the algorithm. Majority vote is used to combine the decisions of the ensemble classifiers.

The Algorithm: The random forests algorithm (for both classification and regression) is as follows:

1. Draw n_{tree} bootstrap samples from the original data.
2. Grow an unpruned classification or regression tree with the following modification for every bootstrap sample: Instead of selecting the best split among all predictors at each node, randomly sample m_{try} of the predictors and select the variable with the best split among those. (Bagging is the unique instance of random forests that arises when$m_{try} = p$, how many predictors there are.)
3. Anticipate fresh information by combining the forecasts of the n_{tree} trees (i.e., majority votes for classification, average for regression).

3.3 Adaptive Response Mechanisms (ARM):

IDPS incorporates adaptive response mechanisms that dynamically adjust intrusion prevention measures based on the severity and type of detected intrusion. Depending on the situation, the system can employ techniques such as rate limiting, isolation of compromised nodes, or even reconfiguration of network parameters. Adaptive responses help mitigate the impact of intrusions while minimizing false alarms.

3.1 Proposed RFARM an Intrusion Detection and Prevention System for Wireless Sensor Networks

Wireless Sensor Networks (WSNs) are vulnerable to various security threats because they are deployed in difficult locations and have limited resources. Existing Intrusion Detection Systems (IDS) for WSNs often focus on detection alone, leaving a gap in proactive threat prevention. This proposed methodology aims to bridge this gap by developing Machine learning with adaptive anomaly detection named as RFARM, an Intrusion Detection and Prevention System tailored for WSNs.

The effectiveness of the proposed RFARM will undergo rigorous evaluation, encompassing both extensive simulations and real-world Wireless Sensor Network (WSN) deployments. This comprehensive assessment will gauge its performance based on crucial metrics such as detection accuracy, false positive rates, energy consumption, and network longevity. Through simulations, the system's theoretical capabilities will be examined, while real-world deployments will provide insight into its practical functionality. By scrutinizing these key metrics, researchers can determine the system's reliability, efficiency, and suitability for safeguarding WSNs, contributing valuable insights to the area of computer security.

RFARM, an Intrusion Detection and Prevention System for Wireless Sensor Networks (WSNs), employs a comprehensive approach to enhance the security of these resource-constrained networks. The BS can employ a Random Forest-based IDS (Intrusion Detection System) to analyze the incoming data for anomalies or

security threats. The results of this analysis can inform response mechanisms and decision-making in the network. While a full-fledged mathematical equation is not applicable in this context, research can describe key components and principles through mathematical notations and concepts:

1. Data Collection

Data Gathering: Nodes in the WSN collect sensory data and send it to the Base Station (BS). This process can be represented as:

$$Data\ Collection: SensorNode_i \rightarrow BS$$

2. Intrusion Detection

Anomaly Detection: RFARM employs mathematical models to detect anomalies in the incoming data. This can be expressed as:

$$Anomaly\ Detection: Anomaly_i = Detect(Data_i)$$

Alert Triggering: When an anomaly is detected, an alert is generated, and the system can trigger predefined responses:

$$Alert_i = GenerateAlert(Anomaly_i)$$

3. Intrusion Prevention

Dynamic Security Adjustment: RFARM adjusts security parameters based on detected threats. For instance, it can change the key rotation interval based on the threat level:

$$KeyRotationInterval_i = AdjustSecurity(Anomaly_i)$$

Isolation of Compromised Nodes: In severe cases, RFARM can isolate compromised nodes to prevent further intrusion:

$$Node_i = Isolate(Node_i)$$

4. Energy Efficiency

Energy Consumption: RFARM aims to reduce energy consumption for prolonged sensor node operation. Energy models and optimization equations can describe this process:

$$EnergyConsumptio_i = OptimizeEnergy(Parameters)$$

5. Security

Secure Communication: RFARM employs cryptographic techniques for secure data transmission:

$$SecureTransmission_i = Encrypt(Data_i) + Authenticate(Data_i)$$

Secure Routing: Secure routing protocols ensure that data is transmitted through trusted paths:

$$SecureRouting_i = SelectRoute(Node_i, Destination)$$

RFARM combines these equations and principles to provide a robust and adaptable security solution for WSNs. It offers proactive intrusion prevention, energy-efficient operation, and secure data transmission, ultimately enhancing the resilience of WSNs against evolving security threats.

Certainly, here is a proposed algorithm for RFARM, an Intrusion Detection and Prevention System for Wireless Sensor Networks (WSNs):

Algorithm: RFARM - Intrusion Detection and Prevention System

Input

- WSN Deployment Parameters
- Sensor Data Stream
- Security Policy Settings

Output

- Intrusion Alerts
- Intrusion Prevention Actions

Initialization

Step 1: Initialize security parameters (e.g., encryption keys, detection thresholds).
Step 2: Deploy sensor nodes in the WSN.
Step 3: Establish a secure communication channel with the Base Station (BS).
Step 4: Sensor nodes collect data from their environment periodically.
Step 5: Sensor nodes send data to the base station (BS).
Step 6: Analyze incoming data streams for anomalies and attacks using the following steps:
Step 7: Split Data into Training and Testing Sets

$$X_{train}, X_{test}, y_{train}, y_{test} = train_{test_{split}}(features, labels, test_{size} = 0.2, random_{state} = 42)$$

Step 8: Initialize Random Forest Classifier

$$rf_{classifier} = Random\ Forest\ Classifier(n_{estimators} = 100, random_{state} = 42)$$

Step 9: Train the Random Forest Model

$$rf_{classifier}.fit\ (X_{train}, y_{train})$$

Step 10: Predict Anomalies

$$y_{pred} = rf_{classifier}.predict(X_{test})$$

Step 11: Evaluate the Model

$$Accuracy = accuracy_{score(y_{test}, y_{pred})}$$

$$classification_{rep} = classification_{report}(y_{test}, y_{pred})$$

Step 12: Adaptive Response Mechanisms
Implement adaptive mechanisms for adjusting detection thresholds, feature selection, and response actions based on real-time network conditions.
Step 13: Response to Detected Anomalies
Implement response actions based on the detection results, such as blocking suspicious traffic, alerting administrators, or quarantining affected nodes.
Step 14: Continuous Learning and Improvement
Continuously update the Random Forest model with new data and feedback to improve its accuracy and adaptability.
Step 15: Monitoring and Reporting
Monitor the performance of the IDS and generate reports for security personnel.
Step 16: End

4. Experimental Results

4.1 Packet Delivery Ratio (P DR)

It is defined as the ratio of sent and received packet counts.

Table 1. Comparison Table of Packet Delivery Ratio (PDR)

No of Nodes	WIDPAS	TDS	Proposed RFARM
100	69	76	89
200	70	74	94
300	78	69	86
400	82	70	98
500	85	61	96

The differences between the values of the proposed RFARM and the current (WIDPAS, TDS) were addressed in the Packet Delivery Ratio (PDR) comparison table 1. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 69 to 85, 61 to 76 and proposed RFARM values start from 86 to 98. The proposed gives the best result.

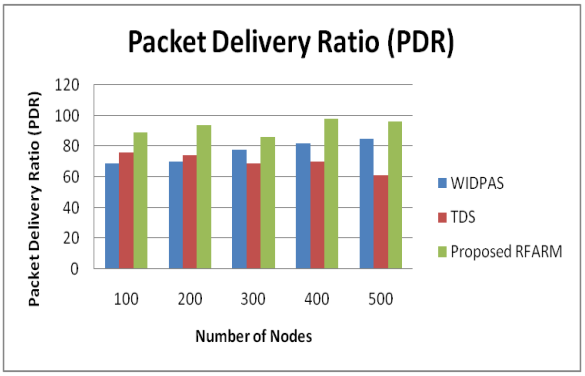

Figure 1. Comparison chart of Packet Delivery Ratio (PDR)

The figure 1 data Packet Delivery Ratio (PDR) describes the different values of existing (WIDPAS, TDS) and proposed RFARM. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and Packet Delivery Ratio (PDR) in Y axis. The existing values start from 69 to 85, 61 to 76 and proposed RFARM values start from 86 to 98. The proposed gives the best result.

4.2 Throughput

It denotes that the number of packets successfully received by the receiver.

Table 2 Comparison Table of Throughput

No of Nodes	WIDPAS	TDS	Proposed RFARM
100	86	82	98
200	81	86	95
300	77	84	99
400	72	80	96
500	74	78	91

The comparison table 2 of Throughput describes the different values of existing (WIDPAS, TDS) and proposed RFARM. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 72 to 86, 78 to 86 and the proposed RFARM values start from 91 to 99. The proposed gives the best result.

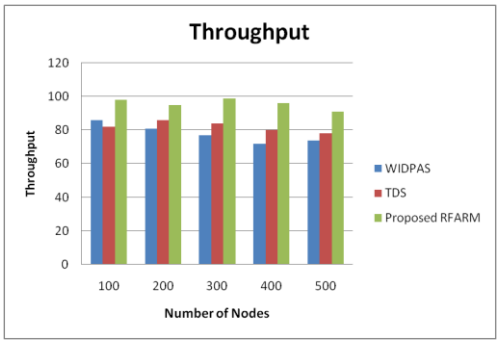

Figure 6.2 Comparison Chart of Throughput

The figure 6.2 data Throughput describes the different values of existing (WIDPAS, TDS) and proposed RFARM. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and throughput in Y axis. The existing values start from 72 to 86, 78 to 86 and the proposed RFARM values start from 91 to 99. The proposed gives the best result.

4.3 Average Delay

Average Delay refers to the time it takes for a packet or data to travel from the source node to the destination node in a network

Table 3. Comparison Table of Average Delay

No of Nodes	WIDPAS	TDS	Proposed RFARM
100	55	41	35
200	66	63	54
300	74	78	65
400	87	81	71
500	93	84	69

The comparison table 3 of Average Delay describes the different values of existing (WIDPAS, TDS) and proposed RFARM. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 55 to 93 and 41 to 84 and proposed RFARM values start from 35 to 71. The proposed gives the best result.

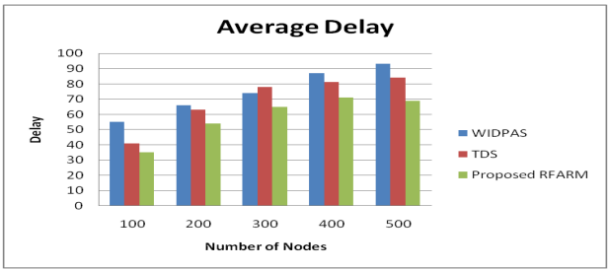

Figure 3. Comparison Table of Average Delay

The figure 3 Average Delay describes the different values of existing (WIDPAS, TDS) and proposed RFARM. While comparing the existing and the proposed method values are higher than the existing method and No of Nodes in x axis and Average Delay in Y axis. The existing values start from 55 to 93 and 41 to 84 and proposed RFARM values start from 35 to 71. The proposed gives the best result.

4.4 Remaining Energy

The term "energy" describes the quantity of energy that is still accessible or present.

Table 4. Comparison Table of Remaining Energy

No of Nodes	WIDPAS	TDS	Proposed RFARM
100	100	100	100
200	75	82	91
300	63	73	82
400	44	61	72
500	35	38	54

The table 4 comparison of Remaining Energy describes the different values of existing (WIDPAS, TDS) and proposed RFARM. While comparing the existing and proposed method values are higher than the existing method. The existing values start from 100 to 35, 100 to 38 and proposed RFARM values start from 100 to 54. The proposed gives the best result.

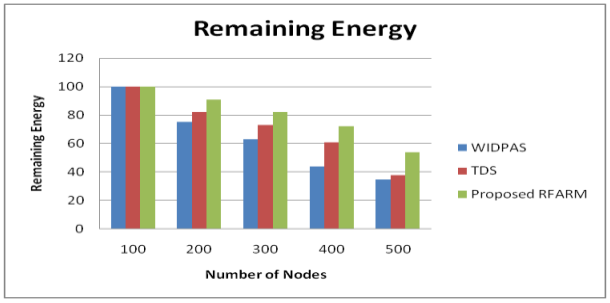

Figure 5. Comparison Chart of Remaining Energy

The figure 5 data Remaining Energy describes the different values of existing (WIDPAS, TDS) and proposed RFARM. While comparing the existing and the proposed RFARM method values are higher than the existing method No of Nodes in x axis and Remaining Energy in Y axis. The existing values start from 100 to 35, 100 to 38 and proposed RFARM values start from 100 to 54. The proposed gives the best result.

5. Conclusion

The RFARM intrusion detection and prevention mechanism showcased in this study represent a significant advancement in enhancing security within Wireless Sensor Networks. By leveraging the strengths of random forests and adaptive response strategies, RFARM demonstrates exceptional accuracy in identifying and preventing intrusions. Its adaptability to evolving threats and robust preventive measures make it a valuable addition to the arsenal of security solutions for WSNs, ultimately safeguarding sensitive data and network integrity in diverse applications, from environmental monitoring to industrial control systems.

Reference

[1] D. K. Yadav, G. Karthik, S. Jayanthu and S. K. Das, "Design of Real-Time Slope Monitoring System Using Time-Domain Reflectometry With Wireless Sensor Network," in IEEE Sensors Letters, vol. 3, no. 2, pp. 1-4, Feb. 2019, Art no. 2500304, doi: 10.1109/LSENS.2019.2892435.

[2] G. Kalnoor and J. Agarkhed, "Pattern matching intrusion detection technique for Wireless Sensor Networks," 2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, India, 2016, pp. 724-728, doi: 10.1109/AEEICB.2016.7538389.

[3] J. Abo Nada and M. Rasmi Al-Mosa, "A Proposed Wireless Intrusion Detection Prevention and Attack System," 2018 International Arab Conference on Information Technology (ACIT), Werdanye, Lebanon, 2018, pp. 1-5, doi: 10.1109/ACIT.2018.8672722.

[4] L. Gandhimathi and G. Murugaboopathi, "Cross layer intrusion detection and prevention of multiple attacks in Wireless Sensor Network using Mobile agent," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 2016, pp. 1-5, doi: 10.1109/ICICES.2016.7518935.

[5] V. Choudhary and S. Taruna, "An Intrusion Detection Technique Using Frequency Analysis for Wireless Sensor Network," 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2021, pp. 206-210, doi: 10.1109/ICCCIS51004.2021.9397076.

[6] P. R. Chandre, P. N. Mahalle and G. R. Shinde, "Machine Learning Based Novel Approach for Intrusion Detection and Prevention System: A Tool Based Verification," 2018 IEEE Global Conference on Wireless Computing and Networking (GCWCN), Lonavala, India, 2018, pp. 135-140, doi: 10.1109/GCWCN.2018.8668618.

[7] G. Kalnoor and J. Agarkhed, "Pattern matching intrusion detection technique for Wireless Sensor Networks," 2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, India, 2016, pp. 724-728, doi: 10.1109/AEEICB.2016.7538389.

[8] S. V. G, R. Nagarajan and S. Kannadhasan, "Performance Analysis of Blended NIDS Model for Network Intrusion Detection System in WSN," 2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT), Erode, India, 2023, pp. 1-6, doi: 10.1109/ICECCT56650.2023.10179781.

[9] V. Choudhary and S. Taruna, "An Intrusion Detection Technique Using Frequency Analysis for Wireless Sensor Network," 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2021, pp. 206-210, doi: 10.1109/ICCCIS51004.2021.9397076.

[10] L. Gandhimathi and G. Murugaboopathi, "Cross layer intrusion detection and prevention of multiple attacks in Wireless Sensor Network using Mobile agent," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 2016, pp. 1-5, doi: 10.1109/ICICES.2016.7518935.