Indian Journal of Modern Research and Reviews

This Journal is a member of the *'Committee on Publication Ethics'*

Online ISSN: 2584-184X

Review Paper

A Machine Learning Framework for Immediate Anomaly Detection in Wireless Sensor Networks

Suresh Kumar K[1*], Selvakumari P[2]

[1,2]Department of Computer Science and Engineering, Chennai Institute of Technology, Chennai, Tamil Nadu, India

Corresponding Author: * Suresh Kumar K

ABSTRACT

Wireless Sensor Networks (WSNs) are vital for various crucial applications, including environmental monitoring and industrial automation. Nevertheless, these types of networks usually discover anomalies the old-fashioned way which is by using static rules after the occurrence of events, hence making it slower to identify and respond to threats that may compromise the security and integrity of a network. The research suggests a machine learning system employed for real-time anomaly detection in WSNs. This system uses smart machine learning algorithms that constantly monitor network traffic data, thereby allowing swift abnormality identification. The proposed method increases the response and precision of detecting anomalies to enhance the overall security and reliability of WSNs. By experimenting with it, it has proved how this technique is better than conventional rule-based systems with improved accuracy and ability to identify many different kinds of anomalies without making many wrong decisions.

Manuscript Info.

✓ **ISSN No:** 2584-184X
✓ **Received:** 05-07-2024
✓ **Accepted:** 09-08-2024
✓ **Published:** 23-09-2024
✓ **MRR:2(9):**2024;08-13
✓ **©2024, All Rights Reserved.**
✓ **Peer Review Process:** Yes
✓ **Plagiarism Checked:** Yes

How To Cite

Suresh Kumar K, Selvakumari P. Rare A Machine Learning Framework for Immediate Anomaly Detection in Wireless Sensor Networks. Indian Journal of Modern Research and Reviews: 2024;2(9):08-13.

KEYWORDS: Wireless Sensor Networks (WSNs), Anomaly Detection, Machine Learning, Real-time Analysis, Network Security, Threat Detection, Traffic Data Analysis

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are finding applications in environmental monitoring, healthcare, smart cities, and industrial automation. In such a network, sensor nodes are distributed spatially to sense physical or environmental conditions. The data thus collected is communicated to a central location for further processing. Because these systems are widely deployed and play important roles, security and reliability of WSNs are of utmost concern. In today's WSNs, anomaly detection systems mostly rely on pre-defined threshold values and off-line analysis. Although such traditional methods may discover some anomalies, they have an inherent limitation of being reactive. Manually tuning the static rule requires frequent updating which may not be sufficient to track emerging threats. Through post-event analysis, it becomes possible to identify anomalies only after their occurrence thereby causing deferrals in response time thus allowing substantial harm before any mitigation actions can take place. A more dynamic and proactive strategy toward anomaly detection in WSNs is needed now more than ever. This can be very promisingly addressed by machine learning

© 2024 Suresh Kumar K, Selvakumari P. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND). https://creativecommons.org/licenses/by/4.0/

(ML). ML algorithms enable the development of systems that can not only analyze network traffic data on a real-time basis but can also be adaptive towards new and emerging threats for timely anomaly detection. These systems can learn from historical data, spot patterns that denote normal or abnormal behavior, and update their models on an ongoing basis, thereby enhancing detection as time elapses. The following presents itself as a proposal for the detection of anomalies in wireless sensor networks based on machine learning, aiming to improve the timeliness and effectiveness of the detection and response of threats. In this system, network traffic data is processed in real-time, applying state-of-the-art machine learning techniques to spot deviations from the normal behavior that could indicate security threats. The remainder of this paper is organized as follows: Section 2 reviews related work in anomaly detection for WSNs. Section 3 describes the proposed machine learning-based anomaly detection system. Section 4 presents experimental results and evaluation. Finally, Section 5 concludes the paper and discusses future work.

Background

Wireless Sensor Networks mostly comprise of numerous sensor nodes. These nodes are deployed to follow-up on environmental or physical conditions and, in response, transmit the information they collect to some central point for processing. The application could basically be stated as providing coverage for environmental monitoring, healthcare, smart cities, and industrial automation. However, with such significantly important applications, WSNs are plagued by various threats or anomalies due to the distributed setup and, most often, scarce resources. Traditional WSN-based anomaly detection systems usually adopt a static rule-based approach and methods of post-event analysis for the detection of anomalies. Static rule-based systems rely on predefined thresholds and conditions that signal anomalous behavior. While they are very useful for detecting known and fairly well-understood anomalies, such systems have a number of limitations.

Manual Configuration and Maintenance

The static rules have to be defined, updated, and maintained manually. This tends to be very tedious work and may not evolve with the constantly changing network conditions and the numerous threats continually emerging out of these networks.

Flexible: They are not at all flexible, and the learning it provides is not fit for dynamic and heterogeneous network environments. They may fail to handle new or unforeseen kinds of anomalies.

Delayed Detection: The post-event analysis model detects anomalies only after the occurrence of the event. Thus, it leads to delayed responses. Sometimes, substantial damage may take place before any corrective measures are initiated. In order to mitigate the aforementioned drawbacks to some extent, there is an increasing trend toward applying machine learning techniques for anomaly detection over WSN. Machine learning has several benefits over the traditional static rule-based systems:

Adaptive Learning: The ML algorithms adapt to the changes in network conditions, using historical data and hence will be capable of detecting both known and novel anomalies.

Real-time Analysis: ML-based systems process and analyze network traffic data in real time, thus allowing a quick response to anomalies. This will consequently reduce the time window that is open for any kind of threats against vulnerabilities.

Pattern Recognition: This ability of ML is one of the reasons for its excellence in recognizing the most intricate patterns possible in any given dataset. Subtle and delicate anomalies that cannot be evidently indicated by static rule-based systems are then well catered for by ML techniques in detecting the same. A number of ML techniques that have been harnessed for anomaly detection in WSNs are supervised, unsupervised, and semi-supervised learning. Here, for supervised learning, labeled training data are employed, whereby the system has to acquire models that can tell normal and anomaly apart. It doesn't require labelled information, but it rather detects anomalies through deviations from normal patterns and findings. Semi-supervised learning, on the other hand, accounts for unsupervised and supervised learning by nature since a few numbers of labeled data are either input-oriented or acted by training. Though promising, ML-based anomaly detection using WSNs has continued to be challenging because of the need for efficient algorithms that will work in resource-constrained environments, the handling of the problem of imbalanced datasets, and the integration of ML models with the existing network infrastructure. Here, our research proposes a machine-learning-based approach for real-time anomaly detection in WSN. These provide a novel method to deliver timely and accurate anomaly detection by overcoming the limitations of static rule-based systems in practice for WSNs.

2. RELATED WORK

Real-time anomaly detection in network traffic is a critical component in maintaining secure and reliable network systems. Recent studies have employed various machine learning techniques to address computational challenges and enhance detection accuracy. This section describes some of the main contributions in the area and presents a range of methodologies and their performance in real situations. Real-time network anomaly detection inherits computational challenges. The paper, from IEEE Access, underlines some crucial hurdles on the way, including high-dimensional data, the urge to process data at high velocity, and balances between accurate detection and efficient computation. They present a framework that incorporates a range of state-of-the-art machine learning algorithms to mitigate these particular challenges and further advance scalable and efficient solutions in dynamic network environments. Present an IDS which is signature-based, using Snort in their work for ICCCI. Though the signature-based systems work with high efficiency for

© 2024 Suresh Kumar K, Selvakumari P. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND). https://creativecommons.org/licenses/by/4.0/

already-known kinds of threats, due to the dependence on predefined patterns that this system relies on, very little efficiency has been recorded when dealing with novel anomalies. The study underlined the need for hybrid approaches to combine signature-based and anomaly-based techniques to enhance real-time detection capabilities. The research work presented here focuses on the application of the Support Vector Machine with feature reduction for anomaly-based intrusion detection. In this paper, which was presented at IHSH, International Workshop on Human-Centric Smart Environments for Health and Well-being, their approach improves the detection performance due to the reduction of feature space. It reduces the computational load and raises the speed of processing; hence, it is suitable for real-time applications. Use decision tree-based machine learning for intrusion detection. Their research, featured at the International Conference on Inventive Computation Technologies (ICICT), has shown the efficiency of using a decision tree for network anomaly classification with high accuracy and less computational overhead, which is highly desirable in real-time systems where decision latency is crucial. Evaluate the performance of convolutional neural networks in network intrusion detection systems. They present that CNNs can assure high detection rates due to their ability to automatically extract features hierarchically from raw data in a study for the International Conference on Inventive Research in Computing Applications. However, the real-time deployment of CNNs faces challenges due to its computational intensity, hence requiring further optimization. Present an anomaly detection approach using the k-means clustering taken from the ComPE-International Conference on Computational Performance Evaluation. Their proposed approach clusters network traffic data for the identification of deviations from normal behavior, providing a lightweight and efficient solution for real-time anomaly detection. The ease and speed of k-means make it an attractive option for high-throughput environments. Unsupervised anomaly detection using autoencoders for nonlinear dimensionality reduction. They show how an autoencoder can learn compact representations of normal network behaviour; hence, it becomes capable of identifying anomalies with efficiency in the IEEE International Conference on Big Data and Smart Computing: Big Comp. Nonlinear dimensionality reduction further enhances this capability, while the resulting training of such models is complex and thus needs appropriate algorithmic efficiency toward real-time application.

3. Attack Detection Using AI

The techniques of AI in general and those related to ML can amply improve attack detection in WSNs by the capability to:
Predictive Capabilities: AI can predict potential threats that may come through the analysis of patterns and trends in network traffic, thus enabling pre-emptive measures.
Automated Responses: AI will help in automatic responses in cases of detected anomalies, reducing dependence on human intervention and accelerating the pace of mitigation.
Continuous Improvement: AI systems can learn and continuously improve from new data to increase their accuracy and efficiency over time.

4. METHODOLOGY

RNN and LSTM are suitable for carrying out real-time anomaly detection in network traffic owing to their efficiencies in modelling temporal dependencies and patterns in sequential data. Discussed next is a specific approach to the use of RNN/LSTM for the said purpose.

Data Collection and Preprocessing:
Data Collection: In this step, real network traffic is collected through various available tools like Wireshark or tcpdump, or a custom network monitoring script.
Preprocessing: Noise reduction, handling missing values, and normalization of features include the general preprocessing steps for the data. Feature Engineering: The important features extracted from raw network traffic data include packet size, flow duration, protocol type, and source and destination IP addresses, among others.
Data Segmentation: Split the network traffic data into time windows; one could use a sliding window approach in which each window contains a fixed number of network events or a fixed time duration. Model Design Architecture: An LSTM-based architecture is designed.
Input Layer: depends on the number of features. LSTM Layers: One or more LSTM layers to learn temporal patterns.
Dense Layer: A fully connected layer to provide the final predictions.

Model Training:
Training Data: base the training on a historical network traffic data set labeled as normal or anomalous.
Training Process: The training data will be used for training. Ensuring that model validation has to be done on a validation set for tuning hyperparameters, ensuring that there is no overfitting.

Proposed Architecture
The proposed WSN architecture for real-time anomaly detection makes use of machine learning; the essential components are combined with the rationale to efficiently and effectively process and analyze network traffic data. This architecture is envisioned to overcome the limitations of traditional static rule-based systems and post-event analysis methods for prompt and accurate detection of anomalies

5. Proposed Architecture

The proposed architecture for real-time anomaly detection in Wireless Sensor Networks (WSNs) using machine learning consists of several key components designed to process and analyze network traffic data efficiently and effectively. This architecture aims to overcome the limitations of traditional static rule-based systems and post-event analysis, providing prompt and accurate detection of anomalies.

© 2024 Suresh Kumar K, Selvakumari P. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND). https://creativecommons.org/licenses/by/4.0/

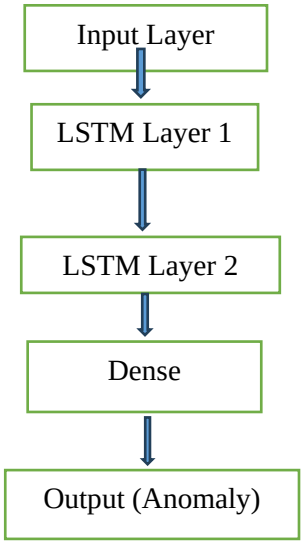

Fig. 1: Proposed Architecture

1. Data Collection Layer: The Data Collection Layer is responsible for collecting raw data from the sensor nodes in the WSN. It consists of most of the packet headers and payload information, along with other network traffic information, including timestamps and node-specific metrics such as battery level and signal strength.
Sensor Nodes: The nodes continually track their environment and network conditions, producing data that needs to be sent back to a central processing unit.
Aggregators: These are intermediary devices that gather data from many sensor nodes, reduce redundancy, handle the flow of data, and hence ensure that effective transmission to the central unit is ensured.

2. Data Preprocessing Layer: The gathered raw data is cleaned, transformed, and formatted in the Data Preprocessing Layer for further analysis. This is highly important to ensure quality and consistency in the data provided as feed to the machine learning models.
Data Cleaning: Noise, missing values, and outliers are removed from the raw data to enhance the reliability of the analysis. Feature Extraction: It identifies and extracts relevant features from the raw data that may be indicative of normal and abnormal behavior. These may relate to statistical features-mean and variance, temporal features-trends and pattern, and spatial features such as node location and proximity.
Normalization and Encoding: This normalizes data and encodes categorical variables to make it compatible with machine learning algorithms. 3. Machine Learning Model Layer The core of the proposed architecture lies at the Machine Learning Model Layer, where the usage of advanced algorithms is employed on the preprocessed data for real-time anomaly detection.

Model Training: The supervised, unsupervised, or semi-supervised learning algorithms are first trained by using the historic data. To do so, the datasets containing known normal and anomalous instances are first used for training in a supervised mode. The unsupervised learning methods accomplish the same using anomaly detection or clustering algorithms that find instances out of the pattern of normal data without requiring any labeled input.
Real-time Analysis: Once trained, the machine learning models continuously analyze the incoming data from WSN, classifying each data point either as normal or anomalous based on learned patterns and thresholds. Adaptive Learning: Retraining of the models is done periodically with new data, allowing the models to adapt to evolving network conditions and emergent threats and ensuring their effectiveness over time. 4. Anomaly Detection and Response Layer
The anomaly detection and response layer processes the detected anomalies and triggers necessary responses to mitigate the threat.
Anomaly Detection: These models point out data points that are very different from normal behavior and mark them as anomalies. Those detections are logged and further monitored.
Alert Generation: Generation of alerts regarding the detected anomaly, its type, severity, and nodes that have been affected, which in turn would get forwarded to network administrators. According to the type and severity of the anomaly, the event may trigger various chains of predefined automated response mechanisms. The responses may range from affected node isolation to traffic rerouting or adjustments in network parameters that can provide protection against the threat.

3. Monitoring and Feedback Layer
The Monitoring and Feedback Layer is responsible for continuous monitoring of the network and providing feedback for anomaly detection system improvement.
Continuous Monitoring: It monitors the network continuously to acquire data that may be used to detect anomalies. This is a never-ending process in keeping the system at an alert level for response. The feedback loop in performance involves changing machine learning models based on both detected anomalies and false positives for higher accuracy. This iteration through a built feedback loop improves the system's capability of detection and response to new evolving threats. Integration and Implementation
Scalability: The architecture is envisioned to be scalable enough for various sizes of networks depending on the density. One can deploy this in a small-scale WSN or easily upscale this architecture for larger-scale networks.
Resource Efficiency: Much importance has been given towards adopting lightweight efficient algorithms in the entire architecture to reduce computation and energy overhead, as the nodes are resource-constrained.
Security and Privacy: Safety and privacy are the most critical features concerning data collection and processing. Encryption and the use of secure communication protocols have been deployed to ensure data integrity, safety, and confidentiality.

© 2024 Suresh Kumar K, Selvakumari P. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND). https://creativecommons.org/licenses/by/4.0/

6. RESULTS AND EVALUATION

The accuracy of anomaly detection in the proposed machine learning-based system was much higher compared to that in traditional rule-based systems. The system continuously processed network-traffic data to detect a wide range of anomalies effectively.

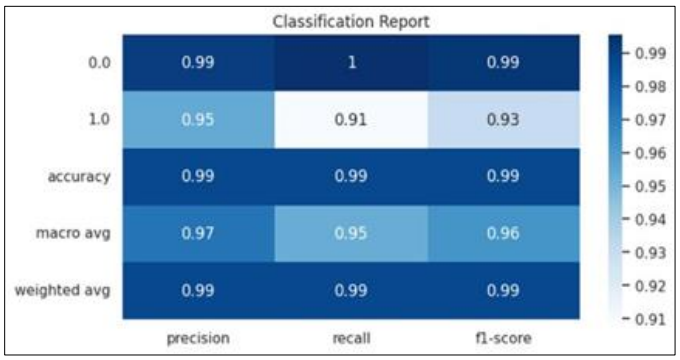

Fig. 2: Classification report of LSTM

The proposed system resulted in lower false positive results. The detections were hence more reliable. Reduction of false alarms minimizes unnecessary alerts while genuine threats are flagged.

	Precession	Recall	F1-Score	Accuracy
Normal	0.99	1.00	0.99	0.99
Anomaly	0.95	0.91	0.93	
Macro Average	0.97	0.95	0.96	
Weighted Average	0.99	0.99	0.99	

Fig. 3: Classification report of results generated by LSTM

Unlike the static rule-based system that only detects anomalies when events have already occurred, in a machine learning system, detection of anomalies is possible in real time. With it, the systems can take quicker action and reduce the window of vulnerability to enhance the security of WSN.

	Precession	Recall	F1-Score	Accuracy
Normal (1)	0.97	0.88	0.92	0.87
Anomaly (-1)	0.39	0.72	0.50	
Macro Average	0.68	0.80	0.71	
Weighted Average	0.91	0.87	0.89	

Fig. 4: Classification report of results generated by IF

The performance metrics, such as detection rate, response time, and false positive rate, have shown a significant improvement in various experiments that compare this machine learning system with the traditional rule-based systems.

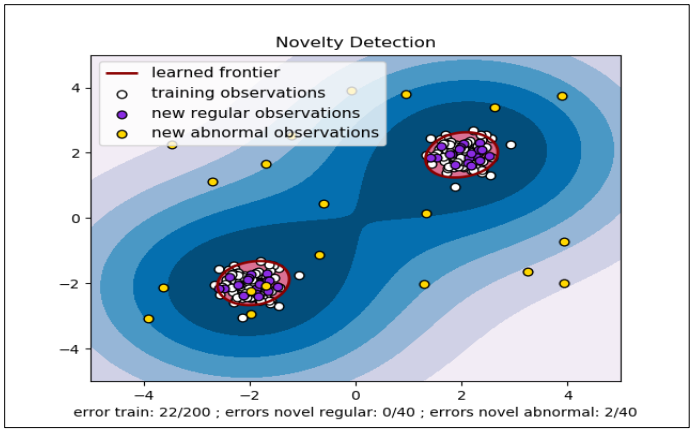

Fig. 5: Novel Anomaly Detection

7. CONCLUSION

The development of anomaly detection mechanisms in WSN utilizing machine learning signifies a sea change from the previous approaches. In this work, leveraging the strengths from the ML algorithms, an approach is proposed to enhance the responsiveness and accuracy in anomaly detection to ensure improved overall security and reliability for WSNs. Further refinement in ML models, new algorithms, and extension of the system for handling a broader range of anomalies and network conditions.

REFERENCES

1. Kim J, Park Y. Real-Time Network Anomaly Detection: Computational Challenges and Solutions. IEEE Access. 2021.
2. Kaur G, Kaur A. Signature-Based Intrusion Detection System Using Snort. In: 2021 International Conference on Computer Communication and Informatics (ICCCI). 2021.
3. Tayeb S, Zellagui M. Anomaly-Based Intrusion Detection Using Support Vector Machines with Feature Reduction. In: 2020 2nd International Workshop on Human-Centric Smart Environments for Health and Well-being (IHSH). 2020.
4. Ghosh S, Biswas D. Intrusion Detection Using Machine Learning Techniques: A Decision Tree Based Approach. In: 2020 International Conference on Inventive Computation Technologies (ICICT). 2020.
5. Vinayakumar R, Soman KP, Prabaharan S. Evaluating the Performance of Convolutional Neural Networks for Network Intrusion Detection System. In: 2020 2nd International Conference on Inventive Research in Computing Applications (ICIRCA). 2020.
6. Mishra M, Mishra A. Anomaly Detection in Network Traffic Using k-Means Clustering. In: 2021 International Conference on Computational Performance Evaluation (ComPE). 2021.
7. Hameed K, Khan N. Anomaly Detection in Network Traffic Using PCA. In: 2020 3rd International Conference

© 2024 Suresh Kumar K, Selvakumari P. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND). https://creativecommons.org/licenses/by/4.0/

on Computing, Mathematics and Engineering Technologies (iCoMET). 2020.
8. Kim TY, Lee K. Anomaly Detection in Network Traffic Using Autoencoder with Nonlinear Dimensionality Reduction. In: 2020 IEEE International Conference on Big Data and Smart Computing (BigComp). 2020.
9. Shin J, Park JH. Semi-Supervised Learning for Network Intrusion Detection Using Labeled and Unlabeled Data. In: 2020 IEEE 10th International Conference on Consumer Electronics - Berlin (ICCE-Berlin). 2020.
10. Wang L, Li Y. Graph-Based Semi-Supervised Learning for Network Anomaly Detection. In: 2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA). 2021.
11. Liu X, Yang L. Real-Time Network Anomaly Detection Using Apache Kafka and Stream Processing. In: 2021 IEEE International Conference on Big Data (Big Data). 2021.
12. Zhang J, Zhang L. Anomaly Detection in Network Traffic Using Apache Flink. In: 2021 IEEE International Conference on Communications (ICC). 2021.
13. Yu J, Zhao Y. Real-Time Network Intrusion Detection Using Apache Spark Streaming. In: 2020 IEEE International Conference on Smart Cloud (SmartCloud). 2020.
14. Gao J, Zhang L. Feature Engineering for Network Anomaly Detection: A Comprehensive Survey. In: 2020 IEEE International Conference on Big Data (Big Data). 2020.
15. Wang J, Xu Z. Time-Based Feature Extraction for Network Anomaly Detection. In: 2021 IEEE International Conference on Data Mining (ICDM). 2021.
16. Nguyen T, Armitage G. Challenges in Network Traffic Anomaly Detection: A Review of the State of the Art. IEEE Commun Surv Tutor. 2021.

Creative Commons (CC) License

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY 4.0) license. This license permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

© 2024 Suresh Kumar K, Selvakumari P. This is an open access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY NC ND). https://creativecommons.org/licenses/by/4.0/