Transforming Network Security by Including Convolutional Neural Networks for Improved Automated Attack Classification and Real-Time Intrusion Detection

Manish K [*1], Dr. Rachana P [*2], Chandan M N [*3], Laya R [*4], Prashanth Kumar B C[*5]

[1] *Student, Information Science & Engineering, Alva's institute of engineering and technology, Karnataka, India*
[2] *Assistant Professor, Information Science & Engineering, Alva's institute of engineering and technology, Karnataka, India*
[3] *Student, Information Science & Engineering, Alva's institute of engineering and technology, Karnataka, India*
[4] *Student, Information Science & Engineering, Alva's institute of engineering and technology, Karnataka, India*
[5] *Student, Information Science & Engineering, Alva's institute of engineering and technology, Karnataka, India*

ABSTRACT

Network intrusion detection systems (NIDS) have been greatly enhanced by developments in machine learning (ML) and deep learning (DL), which have made it possible to analyze network traffic more effectively for anomaly identification. However, the sequential pattern of network transmission is frequently overlooked by current packet-based NIDS, increasing the number of false positives and negatives. Additionally, they usually ignore important header information, which makes it more difficult to identify assaults like denial-of-service (DoS). This research proposes a unique artificial intelligence-enabled paradigm for packet-based NIDS in order to overcome these constraints. By converting sequential packets into two-dimensional images, our technique records temporal linkages in addition to header and payload information. Malicious behavior is successfully identified by the suggested model using convolutional neural networks (CNN). Experiments on publicly accessible datasets show remarkable durability against adversarial instances and high detection rates (97.7%–99%) across a range of attack modes. These outcomes demonstrate our method's potential for precise, real-time intrusion detection in a variety of settings.

INTRODUCTION

By spotting malicious activity and defending vital infrastructure, intrusion detection systems, or IDS, are essential to the protection of organizational networks. The latter of the two main categories of intrusion detection systems (IDS)—host-based (HIDS) and network-based (NIDS)—is especially well-suited for traffic monitoring over extensive networks. Due to their dependence on preset rules, traditional signature-based NIDS techniques are becoming less and less effective as network traffic volume and complexity increase. Alternatively, anomaly-based NIDS use big data analysis and machine learning (ML) and deep learning (DL) approaches to identify malicious activity patterns.

Existing ML/DL-enabled NIDS techniques have a number of drawbacks despite their potential. Although flow- based NIDS are useful for offline traffic analysis, they are unable to detect in real time and ignore the functional and sequential behavior of individual packets. However, packet-based NIDS, which are more appropriate for real- time situations, frequently disregard temporal linkages within a flow and treat packets as separate entities. Additionally, the majority of packet-based systems only pay attention to the payload data, ignoring important information in packet headers that is necessary for identifying complex attacks like port scans and denial-of- service (DoS) attacks.

This research suggests a unique approach to tackle these issues by converting sequential network packets into two-dimensional images that capture the temporal-spatial interactions between packets as well as header and payload data. This method greatly lowers false negatives and false positives while also improving real-time attack

detection capabilities by utilizing a convolutional neural network (CNN)-based model. Our approach is a viable solution for dynamic and changing network settings since it exhibits high accuracy across a variety of attack types and robustness against adversarial perturbations, as demonstrated by extensive testing with publically available datasets.

LITERATURE SURVEY

In anomaly-based Network Intrusion Detection Systems (NIDS), machine learning (ML) and deep learning (DL) techniques have become more popular within the past ten years. These systems can be roughly divided into two categories: packet-based and flow-based. This section examines previous research in both fields, stressing its advantages, disadvantages, and unsolved issues.

Flow-based NIDS

Flow-based NIDS examine aggregated network flow characteristics such flow direction, packet size, and duration. Usually, programs such CIC FlowMeter or Zeek (Bro) are used to extract these features from packet headers. Although flow-based NIDS perform well for offline analysis, their reliance on full network flows makes it difficult for them to provide real-time detection.

In this field, deep neural networks (DNNs) have been used extensively to simulate intricate traffic patterns. For example, an RNN-based model for flow-based NIDS was proposed by Yin et al., and it showed better detection rates than traditional ML techniques. However, because feature sets vary across network settings, flow-based algorithms have limited domain flexibility and frequently miss application-layer assaults like SQL injection. Additionally, when it comes to detecting minority attack classes, they have high false-positive rates.

Packet-based NIDS

By examining individual packets rather than waiting for a full flow, packet-based NIDS provide real-time detection. Deep learning approaches have the potential to enhance packet-based intrusion detection, according to recent studies. RNNs with attention mechanisms are used in techniques like ATPAD to identify irregularities in packet payloads. Similarly, Zhang et al. used convolutional neural networks (CNNs) to create grayscale visual representations of packets for classification. But the majority of current works have serious drawbacks:

The independence assumption disregards the temporal correlations within a flow and treats packets as independent units.
Payload-centric Analysis: A lot of methods just look at the payloads of packets, ignoring important header data that is necessary to identify attacks like denial-of-service (DoS). Static Packet

Representations: These models are biased and have lesser accuracy in real-world deployments because they ignore the sequential nature of network traffic.

Hybrid Approaches

To overcome these constraints, some research has looked into hybrid strategies that blend flow and packet characteristics. For instance, PBCNN uses several packets in a flow to produce session-level images. These techniques work well for offline detection, but because they depend on capturing a set quantity of packets, they are inappropriate for real-time situations. Moreover, environment-specific header elements like IP addresses and port numbers can inject biases into these methods.

Research Gaps

The following significant issues restrict the efficacy of current approaches in practical applications:

1.The absence of temporal-spatial modeling in many packet-based systems results in erroneous detection of sequential traffic.

2. The capacity to detect a variety of attack methods is diminished when header-level characteristics are either disregarded or insufficiently implemented.

There are still problems with high false-positive rates and subpar performance in detecting minority attack types. By putting forth a unique AI-enabled system that preserves the temporal linkages between packet sequences while capturing both header and payload data, this article fills these gaps. Our method enables CNN-based detection with low false positive rates and excellent accuracy by introducing a sequential packet picture representation.

METHODOLOGY

We suggest a unique AI-enabled architecture called Sequential Packets Image-based Network Intrusion Detection System (SPIN-IDS) to overcome the shortcomings of current NIDS techniques. In order to record header and payload information as well as the temporal relationships between packets, the framework converts sequential packets into two-dimensional image representations. Convolutional neural networks (CNNs) are used to detect harmful patterns in network data in real time. There are three main parts to the methodology:

1. **Parser for packets**
   In order to extract packet-based information, the packet parser analyzes raw network data, either in real- time or from pcap files.

   Feature Extraction: To reduce bias, important details like source and destination IP addresses, ports, and protocol are eliminated. To record the time difference between successive packets in a flow, a temporal correlation characteristic called delta time is added.
   Converting Hexadecimal to Decimal: Hexadecimal packet data is transformed into decimal numbers (0– 255) that can be used to describe images.
   Alignment and Padding: With a fixed feature vector of 1486 bytes per packet, zero-padding is used to ensure consistency among packets of different lengths. For picture construction, auxiliary features like packet direction and delta time are added.

2. **Picture Constructing**

Using a network flow's sequential packets, this component creates 2D graphics while maintaining temporal-spatial linkages.

The structure of the images is as follows: P is the number of sequential packets (picture height), Q is the packet feature length (1486), and 3 is the number of RGB channels. The images are formed with dimensions of P×Q×3.

The red channel (R) is used for forward packet encoding, the green channel (G) for backward packet encoding, and the blue channel (B) is zero-padded for uniformity. The flow of communication between sender and recipient is captured in this design.

Temporal Representation: To produce a static representation of their features, packets are stacked one after the other. To encode the temporal interactions between packets, delta time is utilized.

3. **Detector of Network Intrusion**

Images are categorized as either benign or malicious by the CNN-based network intrusion detector.

Model Architecture: The CNN is made up of batch normalization and max-pooling layers after convolutional layers with same-padding. The purpose of dropout layers is to avoid overfitting. The last dense layer produces binary classifications (malicious or benign) using a Sigmoid activation function. Training and Validation: The model is trained and validated using historical datasets (such as CIC- IDS2017). KerasTuner optimizes hyperparameters like learning rate, number of filters, and kernel size. Evaluation Metrics: Accuracy, precision, recall, F1-score, false positive rate (FPR), and false negative rate (FNR) are used to assess performance.

Benefits of the Suggested Approach

1Temporal-Spatial Awareness: The framework recognizes important patterns in the packet header and payload by turning successive packets into images.

2Real-Time Detection: SPIN-IDS considerably shortens response times by detecting attacks within the first nine packets of a flow, in contrast to flow-based techniques.

3Robustness: CNNs sustain excellent detection rates across a variety of datasets and contexts by providing robustness against adversarial attacks.

This creative method provides a scalable and efficient answer to contemporary cybersecurity issues by bridging the gap between the requirements for real-time detection and the constraints of conventional packet-based NIDS.

Overview of Workflow

Three essential components—Packet Parser, Image Builder, and Network Intrusion Detector—are integrated into the workflow of the suggested Sequential Packets Image-based Network Intrusion Detection System (SPIN-IDS) in order to effectively identify malicious activity in network traffic. A detailed description of the procedure is provided below:

1. Raw input Source of Network Traffic: Pcap files or real-time network traffic capture are both available. Content: In addition to header and payload information, each packet also contains extra

metadata, such as timestamps.

2. Packet Parsing: The goal of packet parsing is to eliminate duplicate and environment-specific information from raw network data while extracting pertinent features. Actions to take: Retrieve the payload and packet header information. Eliminate information that can cause prejudice, such as protocol identities, ports, and IP addresses. Use a delta time feature (the time difference between consecutive packets) to encode temporal relationships. For image appropriateness, convert hexadecimal values to decimal values (range: 0–255). To standardize feature vectors to a predetermined size (1486 bytes), use zero-padding.

3. Image Building: The goal of image building is to collect both spatial and temporal information by converting sequential packet data into two-dimensional RGB images. Actions to take: Sort packets according to flow and recognize them by shared characteristics (e.g., source/destination IPs, ports). Create pictures with the following dimensions: $P \times Q \times 3$, where P is the number of consecutive packets, $Q = 1486$ is the packet feature length, and 3 stands for RGB channels. Backward packets should be encoded into the green (G) channel and forward packets into the red (R) channel. For homogeneity, the blue (B) channel is zero-padded. To maintain order and capture the temporal-spatial linkages in the image representation, stack packets one after the other.

4. CNN-Based Intrusion Detection Goal: Determine whether the produced photos are malicious or benign. Steps: Run a Convolutional Neural Network (CNN) model that is tuned for binary classification over the photos. Using convolutional layers to extract features, pooling layers to lower dimensionality, and dropout layers to avoid overfitting, the CNN learns patterns from training data. In the last layer, apply a Sigmoid activation function to provide a likelihood score that indicates the maliciousness of the traffic.

5. Real-time detection and action output: Determine whether an image is harmful or benign. Timing: By detecting malicious behavior in the first nine packets of a network flow, the system accomplishes early detection.
Integration: For real-time warnings and mitigation, detection results can be incorporated into larger security systems.

Important Workflow Features
1.Efficiency in Real Time: Rapid processing and detection inside a flow's first packets are made possible by the image-based representation.
2.Thorough Analysis: Robust detection of a variety of attack types is ensured by simultaneously taking into account both header and payload data.
3.Scalability: Without requiring a lot of retraining, the modular design allows deployment in a variety of scenarios.

A highly accurate and effective intrusion detection system is produced by this organized approach, which skillfully blends data preprocessing, creative feature representation, and cutting-edge machine learning techniques.

RESULTS

The performance of the suggested Sequential Packets Image-based Network Intrusion Detection System (SPIN- IDS) is assessed in this section. Early attack detection, accuracy across attack types, resilience to adversarial attacks, and adaptation to various network settings are some of the factors that are examined in the analysis of the results.

1. Early Malicious Traffic Identification:
Early in a network flow, the SPIN-IDS architecture shows that it can identify malicious traffic.

Key Finding: After analyzing the first nine consecutive packets in a flow, the detection reaches a high accuracy of 98.77 percent. Compared to flow-based NIDS, which normally need to handle an average of 80 packets per flow, this is a major gain.
Observation: During TCP three-way handshakes, for example, malicious intent is frequently not visible in the first packets. However, the system successfully detects malicious activity early by utilizing temporal-spatial patterns.

2. Performance for All Types of Attacks:
A wide range of attack types from the CIC-IDS2017 dataset, such as DoS, DDoS, penetration, and online attacks, were used to test the framework.

Average Rates of Detection:
Accuracy: 98.5% for every kind of strike.
When the True Positive Rate (TPR) is more than 98.5%, malicious traffic is reliably identified.
Particular Examples of Attacks:
Because of clear and dependable patterns in the packet sequences, SSH and FTP patators were able to achieve 100% detection accuracy.
DoS Attacks (such as Slowloris and Slowhttptest): Showed TPR values above 97%, indicating that the model can manage a variety of traffic patterns.

3. Resilience in the Face of Adversarial Attacks:
Resilience against adversarial perturbations introduced to avoid detection is demonstrated via the SPIN-IDS architecture.

Adversarial Experimentation: Carefully constructed packet perturbations in both header and payload data were used to test the framework.
Result: In spite of noise or small disturbances, the CNN-based detector demonstrated resilience in detecting underlying harmful patterns, maintaining high detection rates (97.5%–99%).

4. Flexibility in Various Network Environments:
The CIC-IDS2018 dataset, which includes a variety of network environments and attack methods, was used to test the model's adaptability.

Performance: Without the need for retraining, the model achieved an accuracy of over 97%, demonstrating transferability.
Implication: Domain adaptability is improved by using sequential packet image representation and eliminating bias-inducing elements (such as IP addresses and ports).

5. Examining Detection Patterns Statistically:
The peak signal-to-noise ratio (PSNR) was used for statistical analysis in order to analyze the similarity between attack and benign traffic.

Observation: Following the transmission of 4–9 packets, there were notable departures from benign patterns that were consistent with the detection accuracy trends of the system.

Implication: The system provides a proactive approach to intrusion detection by effectively detecting anomalies in the early phases of communication.

DISCUSSION

The outcomes of the SPIN-IDS framework highlight its promise as a dependable and expandable real-time intrusion detection system:

1:Rapid mitigation of network threats is made possible by early detection capability, which shortens response times.
2:Broad Attack Coverage: Detects a variety of attack types, such as DoS, DDoS, and infiltration, with accuracy. 3.Robustness and Scalability: Shows excellent performance in a variety of network environments and under hostile circumstances without requiring a lot of retraining.
Notwithstanding its benefits, the method might not work well in situations involving highly encrypted communication or obfuscated packet headers, in which case further preprocessing or decryption would be required. By combining sophisticated feature extraction methods with hybrid approaches, future research can overcome these obstacles.

CONCLUSION

In order to overcome the shortcomings of the current network intrusion detection systems (NIDS), this study suggested a unique framework called the Sequential Packets Image-based Network Intrusion Detection System (SPIN-IDS). The system efficiently captures header and payload information as well as temporal-spatial correlations between packets by converting sequential packets into two-dimensional images. This allows for the early and precise detection of network threats.High detection rates (97.7%–99%) were achieved by the framework in the testing findings for a variety of attack types, such as distributed denial-of-service (DDoS), denial-of-service (DoS), and penetration attacks. With over 97% accuracy on previously untested datasets, the SPIN-IDS system has demonstrated resilience to adversarial perturbations and flexibility in various network contexts. Compared to conventional methods, the system's ability to detect malicious activity early in a communication flow—within the first nine packets—significantly speeds up detection and reaction times.

This work's main contributions are as follows:

1. a method for transforming packets into images that improves detection capabilities by extracting important elements from both header and payload data.

2. using convolutional neural networks (CNNs) to analyze representations based on images, which improves detection accuracy and lowers false positives and negatives.

3. The framework's scalability and adaptability allow for deployment in a variety of real-world settings without requiring a great deal of retraining.

Even if the framework tackles a lot of issues, some still exist, like the inability to handle encrypted traffic and identify highly obfuscated attacks. Advanced feature extraction methods, hybrid detection strategies, and performance optimization for high-throughput settings will be the main topics of future research.

In summary, the SPIN-IDS architecture is a useful component of contemporary cybersecurity systems since it provides a strong, scalable, and effective real-time intrusion detection solution.

REFERENCES

1. Ghadermazi, J., Shah, A., & Bastian, N. D. (2024). Towards Real-time Network Intrusion Detection with Image-based Sequential Packets Representation. *IEEE Transactions on Big Data*.

DOI: 10.1109/TBDATA.2024.3403394

2. Canadian Institute for Cybersecurity (CIC). CIC-IDS2017 Dataset. Retrieved from: https://www.unb.ca/cic/datasets/ids-2017.html
3. Canadian Institute for Cybersecurity (CIC). CIC-IDS2018 Dataset. Retrieved from: https://www.unb.ca/cic/datasets/ids-2018.html
4. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks (RNNs). *IEEE Access*, 5, 21954–21961. DOI: 10.1109/ACCESS.2017.2762418
5. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A Deep Learning Approach to Network Intrusion Detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, 2(1), 41–50. DOI: 10.1109/TETCI.2017.2772792
6. Chai, Z., Li, X., Zhang, Y., & Guan, X. (2021). Few-shot Learning for Malware Detection Using Dynamic Prototype Networks. *Computers & Security*, 106, 102263. DOI: 10.1016/j.cose.2021.102263
7. Zhang, Y., Wang, G., Sun, Y., & Zhou, D. (2020). Packet2Image: A Deep Learning Approach for Network Packet Classification. *Computers & Security*, 89, 101684. DOI: 10.1016/j.cose.2020.101684
8. Yu, Y., Zhuang, L., Wang, W., & Zhang, X. (2020). PBCNN: Packet-Based Convolutional Neural Networks for Network Intrusion Detection. *Computers & Security*, 92, 101745. DOI: 10.1016/j.cose.2020.101745
9. Zeek (Bro) Network Monitoring Tool. Retrieved from: https://zeek.org
10. Wireshark: The World's Foremost Network Protocol Analyzer. Retrieved from: https://www.wireshark.org
11. Naseer, M. A., Iqbal, A., & Khokhar, R. H. (2019). A Comparative Study of Machine Learning Algorithms for Network Intrusion Detection Systems. *Journal of Network and Computer Applications*, 137, 19–29. DOI: 10.1016/j.jnca.2019.04.012
12. Xu, B., Zhang, W., & Liu, Y. (2018). Intrusion Detection with a Deep Neural Network: A Review of Methods and Applications. *Future Generation Computer Systems*, 87, 704–717. DOI: 10.1016/j.future.2018.05.018
13. Zhou, Y., & Zhuang, F. (2020). Deep Learning for Cyber Security: A Survey. *IEEE Access*, 8, 115473– 115491. DOI: 10.1109/ACCESS.2020.3001989
14. Zhang, J., & Wang, S. (2019). A Deep Learning Approach for Intrusion Detection Using Network Traffic Data. *Computers & Security*, 84, 1–10. DOI: 10.1016/j.cose.2019.03.001
15. Naseem, M., & Qureshi, H. (2021). A Comprehensive Survey on Deep Learning Approaches for Intrusion Detection Systems: Challenges and Solutions. *Computers & Security*, 103, 102144. DOI: 10.1016/j.cose.2020.102144