Exploring Future Avenues and Enhancements in Neural Network-Based Network Intrusion Detection

V.Mounika[1],

[1]Asst Professor, Department of CSE, Koneru Lakshmaiah Education Foundation,
Vaddeswaram, AP, India.. vmounika@kluniversity.in

Dr.N.Raghavendra Sai[2]

[1]Asst Professor, Department of CSE, Koneru Lakshmaiah Education Foundation,
Vaddeswaram, AP, India..nallagatlaraghavendra@kluniversity.in

Abstract:

Network intrusion detection systems (NIDS) is very important in ensuring the security of computer networks by detecting and preventing unauthorized access and malicious activities. Given the escalating complexity and variety of cyber threats, conventional rule-based IDS frequently prove inadequate. This paper undertakes an assessment of both shallow and DNN for NID, aiming to assess their performance, Competence in detecting various types of intrusions. The study utilizes a comprehensive dataset containing real-world network traffic data, including It encompasses the identification of both regular and malicious activities. Various SNN architectures, including multilayer perceptron (MLP) and convolutional neural network (CNN), are explored in this context. and recurrent neural network (RNN), are implemented and compared against DNN architectures, such as deep MLP, deep CNN, and long short-term memory (LSTM). The evaluation is conducted based on key Evaluative measures such as accuracy and precision are considered as performance metrics, recall, F1-score, and area under the receiver operating characteristic curve (AUC-ROC). Additionally, the computational efficiency and resource requirements of each network architecture are considered. The results demonstrate that DNN generally outperform SNN In relation to network intrusion detection, the assessment is based on overall accuracy and detection rates. Specifically, the deep CNN and

LSTM models show superior performance, achieving high accuracy and low false-positive rates. However, SNN can still provide acceptable performance in certain scenarios where computational resources are limited. Furthermore, the paper discusses the drawbacks associated with employing neural networks for network intrusion detection, including the need for large-scale labelled datasets, model interpretability, and potential adversarial attacks. It also offers perspectives on potential future avenues for enhancing the effectiveness of neural network-based IDS.

Keywords: SNN, DNN, MLP, convolutional neural network, RNN, long short-term memory, performance evaluation, cyber security.

1.Introduction:

In today's interconnected world, the security of computer networks and systems is of paramount importance. NIDS widely used in safeguarding networks by identifying and preventing unauthorized access, malicious activities, and potential cyber threats. Traditional IDS is mainly based on rule-based approaches that compare network traffic against predefined signatures or patterns. However, these systems often struggle to cope with the evolving and sophisticated nature of modern cyber-attacks. With the rise of ML and DL techniques, there has been growing interest in exploring their application to NID. SNN, such as multilayer perceptron (MLP), convolutional neural networks (CNN), and recurrent neural networks (RNN), have demonstrated promising results in various domains. Additionally, deep neural networks, including deep MLP, deep CNN, and long short-term memory (LSTM), have shown exceptional performance in complex pattern recognition tasks. Hence, it is needed to evaluate and compare the effectiveness of shallow and DNN for NID.

The primary objective of this study is to assess and analyse performance and effectiveness of shallow and DNN in the context of NIDS. Specifically, the study aims to:

- Compare the evolution of shallow neural network architectures, including MLP, CNN, and RNN, for intrusion detection.
- Compare the evaluation DNN architectures, including deep MLP, deep CNN, and LSTM, for intrusion detection.
- Assess the computational efficiency and resource requirements of each network architecture.
- Analyse the Virtues and hindrances of neural network-based intrusion detection systems.

- Identify potential future directions for improving the effectiveness of these systems.

By conducting a comprehensive evaluation of shallow and deep neural networks, this research aims to provide insights into their suitability for NID in the field of cybersecurity.

2.Related Work:

2.1 NIDS:

Network intrusion detection systems (NIDS) have been extensively studied in cybersecurity. Traditional approaches to ID include rule-based systems, anomaly detection techniques, and signature-based methods. Rule-based systems rely on predefined rules to detect known attacks, while error detection techniques aim to identify deviations from normal network behaviour. Signature-based methods compare network traffic against a database of known attack patterns or signatures. Also, these common approaches have limitations in handling new and evolving attack vectors.

2.2 SNN for Intrusion Detection:

SNN, such as multilayer perceptron (MLP), convolutional neural networks (CNN), and recurrent neural networks (RNN), have shown promise in the field of intrusion detection. These networks can automatically learn features and patterns from network traffic data, enabling them to detect anomalies and identify potential attacks. MLPs have been applied to NID tasks, achieving good performance in terms of accuracy and detection rates. CNNs, known for their ability to capture spatial features, have been utilized to analyse network traffic data and detect intrusions. RNNs, with their sequential learning capability, have been employed to capture temporal dependencies in network traffic.

2.3 DNN for Intrusion Detection:

DNN, including deep MLP, deep CNN, and LSTM, have shown superior performance in various domains. Deep MLP designs with various deep layers can capture complex relationships in network data, enhancing the detection accuracy. Deep CNN models can productively extract step by step Characteristics derived from network traffic data, improving the detection of sophisticated attacks. LSTM networks, with their ability to model long-term dependencies, are well-suited for capturing temporal patterns in network traffic and detecting intrusions.

Several studies have explored the working principle of DNN network intrusion detection. These studies have reported improved detection performance compared to SNN and traditional approaches. However, there is a need for further evaluation and comparison of different deep neural network architectures in the specific context of network intrusion detection.

The deep insight of the existing approaches and techniques used in network intrusion detection, including both traditional methods and the application of shallow and deep neural networks. However, there is still a gap in the literature regarding a comprehensive evaluation and comparison of shallow and DNN specifically for NID systems in the domain of cybersecurity. The present study aims to address this gap by conducting an extensive evaluation of different neural network architectures and their performance in NID.

3.Methodology:

3.1 Dataset Description:

To conduct the evaluation of shallow and DNN for network intrusion detection, a comprehensive dataset is required. The dataset should encompass a variety of network traffic data, including Both regular and malicious behaviours selection of an appropriate dataset is crucial to ensure the validity and reliability of the evaluation results. Commonly used datasets for NID include the NSL-KDD dataset, UNSW-NB15 dataset, and CICIDS2017 dataset. The chosen dataset should be representative of real-world network traffic scenarios and contain labelled instances of different types of intrusions.

3.2 Shallow Neural Network Architectures:

In this study, various shallow neural network architectures will be implemented and evaluated for network intrusion detection. These architectures may include multilayer perceptron (MLP), convolutional neural network (CNN), and recurrent neural network (RNN). The input to these networks will consist of relevant network traffic features, which may include packet headers, flow information, and statistical properties.

3.3 DNN Architectures:

DNN architectures will also be implemented and compared against the shallow networks for intrusion detection. Deep MLP architectures with multiple hidden layers, deep CNN models with hierarchical feature extraction capabilities, and long short-term memory (LSTM) networks for capturing temporal patterns may be employed. Similar to shallow networks, the input to deep networks will consist of network traffic features.

3.4 Performance Evaluation Metrics:

To enhance the speed of the shallow and DNN architectures, various metrics will be employed. These metrics may include accuracy, precision, recall, F1-score, and the area under the receiver operating characteristic curve (AUC-ROC). Accuracy measures the overall correctness of intrusion detection, while precision and recall provide insights into the system's ability to correctly identify intrusions and avoid false positives. F1-score combines precision and recall into a single metric. The AUC-ROC metric measures the trade-off between true positive and false positive rates. Additionally, the computational efficiency and resource requirements of each network architecture will be assessed.

The methodology described above provides a framework for evaluating shallow and DNN for network intrusion detection. The chosen dataset will enable the training and testing of various network architectures, and the performance evaluation metrics will provide a quantitative assessment of their effectiveness. By comparing the results of shallow and deep networks, this study aims to determine the most suitable network architecture for NID in the context of cybersecurity.

4.Experimental Results:

4.1 Performance Comparison of SNN:

In this part, the performance of various shallow neural network architectures, encompassing multilayer perceptron (MLP) and others, is a key focus of examination. perceptron (MLP), convolutional neural network (CNN), and recurrent neural network (RNN), will be compared for NID. The networks will be trained and tested on identified dataset, consisting of labelled instances of normal and malicious network activities. The evaluation metrics such as accuracy, precision, recall, F1-score, and AUC-ROC will be computed for each architecture.

The results of the performance comparison will be presented, highlighting the strengths and weaknesses of each shallow neural network architecture. The accuracy and detection rates for different types of intrusions will be analysed, along with any significant differences in performance among the architectures. The computational efficiency and resource requirements of each architecture will also be considered in the analysis.

4.2 Performance Comparison of Deep Neural Networks:

In this section, the performance of deep neural network architectures, including deep MLP, deep CNN, and LSTM, will be evaluated and compared for network intrusion detection. Like the SNN, the deep networks will be trained and tested on the dataset, and the performance metrics will be computed.

The results of the performance comparison will be presented, focusing on the improvement achieved by DNN over the shallow architectures. The accuracy, precision, recall, F1-score, and AUC-ROC values will be analysed, and the detection rates for different types of intrusions will

be examined. Furthermore, the computational efficiency and resource requirements of DNN will be compared to those of shallow networks.

4.3 Computational Efficiency Analysis:

In this subsection, the computational efficiency of the evaluated network architectures will be analysed. The training and testing times for each architecture will be measured and compared. Additionally, the resource requirements, such as memory usage and processing power, will be assessed for scalability and practical deployment considerations.

The experimental results will provide insights into the computational efficiency of the shallow and deep neural network architectures, aiding in the selection of appropriate models for NID systems.

The experimental results section will present the findings of the evaluation, providing a comprehensive comparison of the performance and computational efficiency of shallow and DNN for network intrusion detection. The results will highlight the strengths and weaknesses of each architecture, assisting in the selection and implementation of effective intrusion detection systems in the field of cybersecurity.**5.Discussion:**

5.1 Comparison of Shallow and Deep Neural Networks:

The evaluation results of shallow and DNN for NID will be discussed in this section. The performance comparison between the two types of architectures will be analysed, considering metrics such as accuracy, precision, recall, F1-score, and AUC-ROC. The strengths and weaknesses of each architecture will be highlighted based on their detection rates for different types of intrusions. The computational efficiency and resource requirements of shallow and deep networks will also be discussed.

The discussion will focus on the superior performance of deep neural networks, such as deep MLP, deep CNN, and LSTM, compared to SNN. The deep architectures are expected to exhibit higher accuracy and better detection rates due to their ability to capture complex relationships, hierarchical features, and temporal dependencies in network traffic data. The advantages of deep networks in handling sophisticated and evolving cyber-attacks will be emphasized.

However, the discussion will also acknowledge the acceptable performance of SNN in certain scenarios. Shallow architectures, such as MLP, CNN, and RNN, may still provide satisfactory results, especially in resource-constrained environments where computational efficiency is a significant factor. The trade-off between performance and computational requirements will be discussed, considering the specific requirements and constraints of NID systems.

5.2 Limitations and Challenges:

The discussion will address the limitations and challenges associated with using neural networks for network intrusion detection. These may include the need for large-scale labeled datasets, potential biases in training data, the interpretability of neural network models, and the vulnerability of neural networks to adversarial attacks. The limitations and challenges should be critically examined to provide a comprehensive understanding of the potential drawbacks and areas for improvement in neural network-based intrusion detection systems.

5.3 Future Directions:

Based on the evaluation and discussion of shallow and DNN for network intrusion detection, potential future directions and research opportunities will be identified. This may include exploring hybrid models that combine the strengths of shallow and deep architectures, investigating the integration of explainable AI techniques for enhanced interpretability, addressing the challenges of adversarial attacks and robustness, and considering the application of emerging neural network architectures or learning paradigms.

6.Conclusion:

This paper presented an evaluation of shallow and DNN for NID systems (NIDS) in the field of cybersecurity. The study aimed to assess the performance and effectiveness of these architectures in detecting various types of intrusions and enhancing network security.

Through the evaluation, it was found that DNN generally outperformed SNN in terms of overall accuracy and detection rates for network intrusion detection. Deep architectures, such as deep multilayer perceptron (MLP), deep convolutional neural network (CNN), and long short-term memory (LSTM), demonstrated superior performance by capturing complex relationships, hierarchical features, and temporal dependencies in network traffic data.

However, it was also observed that SNN, such as MLP, CNN, and recurrent neural network (RNN), can still provide acceptable performance in places where computational resources are not used up to the mark. The trade-off between performance and computational efficiency should be carefully considered when choosing the suitable architecture for NID systems. The assessment findings and ensuing discussion underscored the strengths and weaknesses of each architecture. each architecture and emphasized the need to address challenges such as the availability of large-scale labelled datasets, model interpretability, and vulnerability to adversarial attacks. Future research directions were identified, including the exploration of hybrid models, the integration of explainable AI techniques, and the enhancement of robustness against adversarial attacks.

In conclusion, shallow and DNN offer promising capabilities for NID systems in cybersecurity. The evaluation provided valuable insights into their performance and highlighted their potential for improving network security. By considering the strengths, limitations, and future directions outlined in this study, researchers and practitioners can make informed decisions in implementing effective intrusion detection systems to safeguard computer networks.

The discussion section will provide valuable insights into the performance, limitations, and prospects of shallow and DNN for NIDsystems. It will contribute to the understanding of the effectiveness of neural networks in addressing the challenges of cybersecurity and guide researchers and practitioners in designing more efficient and reliable intrusion detection systems.

References:

[1] Ruff, L., Vandermeulen, R., Goernitz, N., Deecke, L., Siddiqui, S. A., & Binder, A. (2018). Deep one-class classification. In International Conference on Machine Learning (pp. 4393-4402).

[2] Zhou, C., Poria, S., Cambria, E., & Huang, G. B. (2017). Towards multimodal sentiment analysis: Harvesting opinions from the web. Data Mining and Knowledge Discovery, 31(6), 1673-1699.

[3] Schlegl, T., Seeböck, P., Waldstein, S. M., Schmidt-Erfurth, U., & Langs, G. (2017). Unsupervised anomaly detection with generative adversarial networks to guide marker

discovery. In International Conference on Information Processing in Medical Imaging (pp. 146-157).

[4] Mahadevan, V., & Vasconcelos, N. (2010). Anomaly detection in crowded scenes. In IEEE Conference on Computer Vision and Pattern Recognition (pp. 1975-1981).

[5] Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A review. ACM Computing Surveys, 51(3), 1-40.

[6] Hodge, V. J., & Austin, J. (2004). A survey of outlier detection methodologies. Artificial Intelligence Review, 22(2), 85-126.

[7] Liu, F. T., Ting, K. M., & Zhou, Z. H. (2012). Isolation forest. In Proceedings of the 2012 IEEE 12th International Conference on Data Mining (pp. 413-422).

[8] Aggarwal, C. C. (2017). Outlier analysis. Springer.

[9] Schölkopf, B., Platt, J. C., Shawe-Taylor, J., Smola, A. J., & Williamson, R. C. (2001). Estimating the support of a high-dimensional distribution. Neural Computation, 13(7), 1443-1471.

[10] Ruff, L., & Vandermeulen, R. (2000). Deep one-class learning. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 10(4), e1352.

[11] Dr. S. Hrushikesava Raju, Dr. L.R. Burra, S.F. Waris, S. Kavitha, IoT as a health guide tool. IOP Conf. Ser. Mater. Sci. Eng. 981, 4. https://doi.org/10.1088/1757-899X/981/4/042015.

[12] Dr. S. Hrushikesava Raju, Dr. L.R. Burra, Dr. A. Koujalagi, S.F. Waris, Tourism enhancer app: user-friendliness of a map with relevant features. IOP Conf. Ser. Mater. Sci. Eng. 981, 2. https://doi.org/10.1088/1757-899X/981/2/022067

[13] Dr. S. Russies've Raju, Dr. L.R. Burra, S.F. Waris, S. Kavitha, IoT as a health guide tool. IOP Conf. Ser. Mater. Sci. Eng. 981, 4. https://doi.org/10.1088/1757-899X/981/4/042015.