Detection for Malicious Network Traffic Based on Convolutional Neural Networks

Yueyang Li
Information and Computing Science, Beijing Jiaotong University, Beijing, 10004, China

Keywords: Machine, Network Security, Malicious Network Traffic Detection, Convolutional Neural Network.

Abstract: This research underscores the paramount significance of network security in our modern, interconnected digital landscape. It sheds light on the escalating threat posed by malicious network traffic, which poses risks to both sensitive information and critical infrastructure. Effectively detecting and mitigating these malicious flows is crucial for safeguarding our digital ecosystem. In response to this pressing concern, the study delves into the potential of deep learning, specifically Convolutional Neural Networks (CNNs), as a means to address the issue. It introduces a method for conducting multi-class classification on network traffic using deep learning techniques, leveraging the UNSW-NB15 dataset. The research highlights the remarkable superiority of the proposed 1D deep CNN architecture when compared to traditional methods. Moreover, this study looks ahead to the future, discussing the potential and challenges of implementing Artificial Intelligence (AI)-based detection systems in governmental and business settings. It underscores the necessity of collaboration and the adoption of explainable AI to ensure effective network security solutions in our rapidly evolving digital landscape.

1 INTRODUCTION

In the contemporary globally connected digital landscape, ensuring network security is crucial for protecting vital infrastructure and sensitive data. As the reliance on computer networks continues to grow, so does the threat of cyberattacks. One of the most prevalent and damaging forms of cyber threats is malicious network traffic. Malicious network flows encompass a variety of activities, including intrusion attempts, malware propagation, and denial-of-service attacks (Li et al 2021). Detecting these malicious flows is essential to maintaining the integrity and availability of network resources. The importance of research in the field of malicious network flow detection cannot be overstated. Malicious activities can lead to data breaches, financial losses, and even threats to national security. Traditional methods of detecting malicious network flows often rely on signature-based approaches, which are limited in their ability to adapt to evolving threats. Therefore, the development of innovative and robust detection techniques is crucial to stay ahead of cyber adversaries.

Previous research in the domain of network security has focused on various aspects of malicious flow detection. Signature-based methods have been widely employed (Shone et al 2018), but they struggle to detect zero-day attacks and new attack patterns. Anomalies-based approaches have also been explored, but they often suffer from high false-positive rates. Machine learning techniques, including deep learning, have shown promise in improving the accuracy of detection, but there remains a gap in developing specialized models tailored to the unique characteristics of malicious network flows. Prior studies have contributed valuable insights into the general field of network security and machine learning. They have highlighted the potential of deep learning models, such as Convolutional Neural Networks (CNNs), in capturing intricate patterns in network traffic data. However, these studies have primarily focused on broader applications of deep learning in network security rather than specializing in the specific challenges posed by malicious network flow detection.

Deep learning, particularly CNNs, has made a substantial impact on network security, specifically within the realm of network intrusion detection. A pivotal study conducted by N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi. presented a deep learning approach that harnessed the power of CNNs to enhance Network Intrusion Detection Systems

Li, Y.
Detection for Malicious Network Traffic Based on Convolutional Neural Networks.
DOI: 10.5220/0012805400003885

In *Proceedings of the 1st International Conference on Data Analysis and Machine Learning (DAML 2023)*, pages 321-325
ISBN: 978-989-758-705-4

(NIDS). Their approach proved highly efficient, utilizing CNNs to automatically learn and detect intrusions in network traffic data, showcasing promising results in terms of both accuracy and efficiency (Radhika and Shah 2019).

In the broader landscape of network security, a comprehensive survey by Kwon, D., Kim, H., Kim, J et al. provides valuable insights into the extensive application of deep learning, encompassing CNNs, in this domain. The survey outlines a plethora of approaches that leverage deep learning for network anomaly detection, shedding light on the advancements and challenges within this area. Notably, CNNs emerge as a prominent technique, demonstrating their effectiveness in learning intricate patterns from network data and aiding in anomaly detection (Kwon et al 2019).

Moreover, the application of CNNs for intrusion detection extends to emerging domains, such as the Internet of Things (IoT). An insightful review by LMN et al. Delves into the utilization of deep learning, including CNNs, for securing IoT networks. The review provides a comprehensive overview of state-of-the-art techniques and discusses how CNNs have displayed promise in effectively detecting intrusions within the IoT network context (Kaushik 2023).

The rest of this chapter is organised as follows. First, this review will outline two specific approaches of CNNs for malicious stream detection in Section 2. Then, in Section 3, this review will discuss the application and development of CNNs for malicious stream detection Finally, Section 4 concludes the paper.

2 METHOD

2.1 Multi-Class Classification of Network Traffic Using Deep Learning on UNSW-NB15 Dataset

This research explores the approach to address the multi-class classification challenge of differentiating normal from malicious network traffic. It leverages deep learning models and focuses on the demanding UNSW-NB15 dataset (shown in figure 1) (Moustafa and Slay 2015). The primary focus is on explaining dataset specifics and pre-processing steps. Subsequently, visualization methods such as t-SNE and Andrews curve were employed. The outlined approaches include a fully connected feed-forward neural network with multiple layers, as well as both shallow and deep 1D CNN architectures.

The selection of the UNSW-NB15 dataset, curated by the Australian Center for Cyber Security, was preferred over the traditional NSL-KDD dataset due to its unique benefits. This dataset presents a diverse range of contemporary network attack scenarios grouped into nine categories. The decision to utilize this dataset was motivated by its accurate representation of real-world enterprise-level network traffic and its comprehensive coverage of modern attacks listed in the Common Vulnerabilities and Exposures (CVE) website (Chapaneri and Shah 2019). The dataset consists of two simulation scenarios: one spanning 16 hours at an attack rate of 1/sec, and another lasting 15 hours with an attack rate of 10/sec. Various features are extracted from network traces using Argus and BRO-IDS tools, encompassing flow, basic, content, time, and additional features. The target variable includes nine attack categories as well as the normal class.

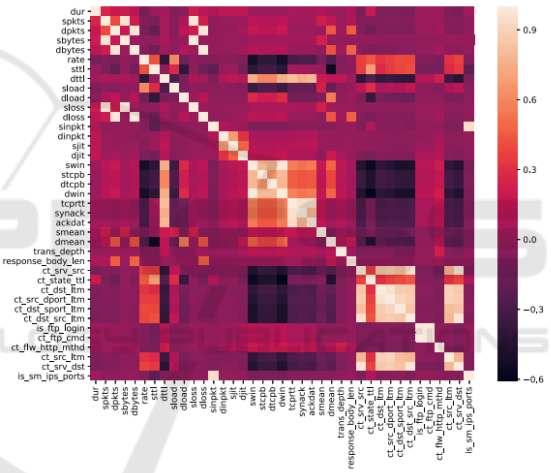

Figure 1: UNSW-NB15 dataset.

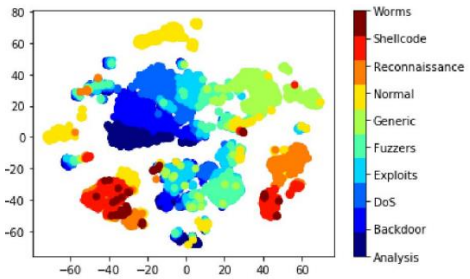

Figure 2: Visualization of the UNSW-NB15 dataset with t-SNE plot.

The distribution of the ten classes in the training and testing sets reveals an imbalanced class distribution, notably with the "Worms" category having the fewest data samples. Moreover, a Pearson

correlation scatter plot of the dataset shows that not all features have a high degree of cross-correlation. This suggests the potential benefit of using a deep learning model to capture nonlinear patterns in the data (Chapaneri and Shah 2019).

In this study, two deep learning architectures, a fully-connected feed-forward neural network and a convolutional neural network, were proposed and evaluated using the recent UNSW-NB15 dataset. Visualization techniques, specifically t-SNE and Andrews curve, demonstrated a high degree of non-linearity in the dataset. This insight motivated the exploration of deep learning models, which are well-known for their ability to effectively capture non-linear data patterns.

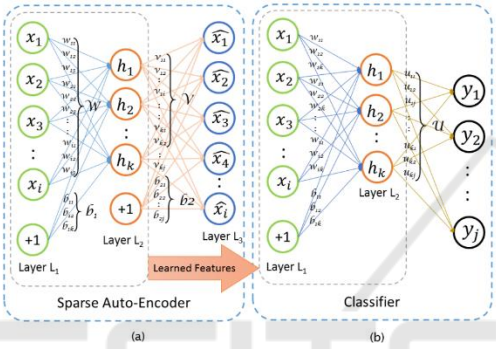

Figure 3: The two-stage process of self-taught learning: a) Unsupervised Feature Learning (UFL) on unlabeled data. b) Classification on labeled data.

The results highlighted the effectiveness of the proposed 1D deep CNN (D-CNN) architecture in comparison to conventional machine learning classifiers and dense neural networks. The F-score comparison illustrates the superior performance of the D-CNN architecture, especially for challenging attack categories such as Analysis, Shellcode, and Worms, with an approximate 20% increase in F-score compared to the existing 2D CNN approach (Chapaneri and Shah 2019).

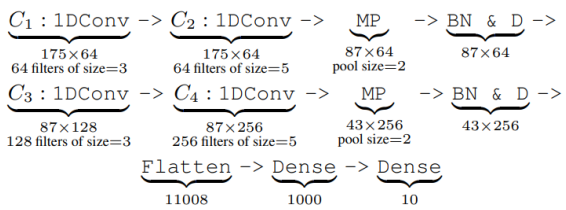

Figure 4: The two-stage process of self-taught learning: a) Unsupervised Feature Learning (UFL) on unlabeled data. b) Classification on labeled data (Shone et al 2018).

2.2 Deep Learning-Based Approach Network Intrusion Detection System

A deep learning-based approach for an efficient and adaptable Network Intrusion Detection System (NIDS) (Shone et al 2018). The approach involves employing a sparse autoencoder and soft-max regression for NIDS implementation, evaluated on the NSL-KDD benchmark dataset. The NIDS exhibited superior performance in normal/anomaly detection during evaluation on test data compared to previous NIDS implementations (Shone et al 2018). The potential for further performance enhancement exists through advanced techniques such as Stacked Autoencoder and appropriate classification algorithms like NB-Tree, Random Tree, or J48. The future focus involves implementing a real-time NIDS for practical network usage utilizing deep learning. Additionally, exploring on-the-fly feature learning directly from raw network traffic headers, rather than pre-derived features, holds promise for significant advancements in this domain. The study emphasizes the effectiveness of deep learning in enhancing NIDS capabilities and sets the stage for further research in real-world network security applications (Shone et al 2018).

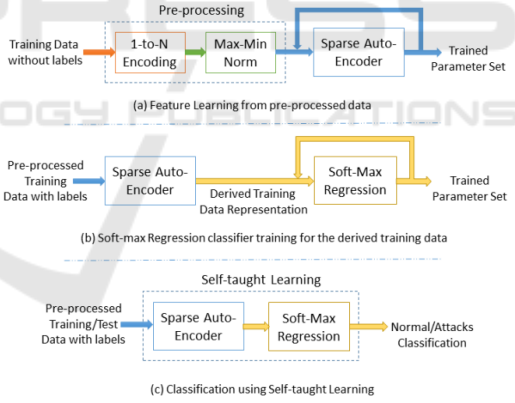

Figure 5: Various steps involved in our NIDS implementation.

2.3 Government

It is crucial for governments and public infrastructure to use AI-based detection to identify and prevent harmful network traffic. Networked systems are vital for critical operations, like defense, national security, public services, and healthcare, and governments worldwide rely on them more and more. These networks are vulnerable to cyber threats, which is why strong security measures are essential.

AI-based detection systems can defend against cyber threats by analyzing network traffic, identifying anomalies, detecting potential intrusions, and predicting attack patterns through deep learning. This proactive and adaptive mechanism empowers governments to protect sensitive information with enhanced efficiency. Still, challenges must be addressed. The rapidly changing cyber threat environment requires AI models to be continuously updated and improved. It is also essential to safeguard citizens' data privacy and security when using AI-based detection. Achieving the correct balance between security and privacy remains an ongoing issue.

AI-based detection holds great promise for the future. As AI systems continue to advance and gain the capacity to learn from vast datasets, they will acquire the capability to detect cyber threats that are growing in complexity. Collaborative work between governments, research institutions and the private sector will be crucial to effectively utilise AI's full potential in securing vital networks and infrastructure.

2.4 Company

In the business world, using AI to detect harmful network activity is a significant development that helps to maintain the smooth running of operations, safeguard important data, and keep customers confident in the company. All kinds of organisations, from those in finance to healthcare, handle huge quantities of valuable information, making them potential targets for cyber criminals.

AI-driven detection programmes give businesses the means to tighten their defences against these threats and improve their overall cybersecurity. These systems can quickly spot and address dangers, reducing the risk of harm. Furthermore, AI can help to evaluate and anticipate risks, allowing people to take anticipatory measures to manage risks proficiently.

Nevertheless, establishments are grappling with difficulties implementing AI-based answers, primarily investing in AI tech, assimilating the solutions with current cyber protection installations, and addressing the lack of adept AI professionals. Overcoming these challenges is crucial to reap the rewards of AI in boosting network security.

In the future, AI will advance and provide even more advanced detection techniques. This will enable firms to outsmart cyber attackers. Collaborations between companies and cybersecurity firms will also fuel innovation and hasten the growth of AI-powered solutions for network security.

2.5 Challenges and Future Prospects

Despite progress with AI-driven identification of harmful network traffic, there are still challenges to be tackled. Attackers are always altering their strategies, creating difficulties in devising AI systems that can precisely detect innovative and unknown attack approaches. Moreover, an unequal distribution of datasets (with few harmful occurrences compared to harmless ones) presents a challenge in training AI models effectively. Therefore, more advanced AI models that have been widely applied in other domains can be also considered in this field for further improving the performance (Yu et al 2020 & Malhotra et al 2022).

3 CONCLUSION

This work acknowledges that addressing future challenges will necessitate collaboration between the research community and industry. Techniques such as transfer learning and continual learning will play a crucial role in adapting AI models to effectively tackle evolving threats. Furthermore, integrating AI with human expertise to develop AI-powered collaborative defense systems is likely to be the future approach. Highlighting the importance of explainable AI in network security will be paramount. AI models need to be comprehensible and interpretable to establish trust and enhance their effectiveness. Maintaining a harmonious equilibrium between AI autonomy and human supervision is vital for the development of future AI-driven detection systems.

REFERENCES

Y. Li et al. 2021 Robust Online Learning against Malicious Manipulation and Feedback Delay With Application to Network Flow Classification.

N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, 2018. A Deep Learning Approach to Network Intrusion Detection, in IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp.4150.

C. Radhika, and S. Shah. Detection of malicious network traffic using convolutional neural networks. 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE (2019).

D. Kwon et al. A survey of deep learning-based network anomaly detection. Cluster Comput 22 (Suppl 1), 949–961 (2019).

P. Kaushik. Unleashing the Power of Multi-Agent Deep Learning: Cyber-Attack Detection in IoT.

International Journal for Global Academic & Scientific Research, 2(2), 23–45 (2023).

N. Moustafa and J. Slay, UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set), 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, pp. 1-6, doi: 10.1109/MilCIS.2015.7348942 (2015).

R. Chapaneri and S. Shah, Detection of Malicious Network Traffic using Convolutional Neural Networks, 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, pp. 1-6, doi: 10.1109/ICCCNT45670.2019.8944814 (2019).

N. Shone, T. N. Ngoc, V. D. Phai and Q. Shi, A Deep Learning Approach to Network Intrusion Detection, in IEEE Transactions on Emerging Topics in Computational Intelligence, vol. 2, no. 1, pp. 41-50, Feb. (2018), doi: 10.1109/TETCI.2017.2772792.

Q. Yu et al. Improved denoising autoencoder for maritime image denoising and semantic segmentation of USV. China Communications, 17(3): 46-57 (2020).

P. Malhotra et al. Deep neural networks for medical image segmentation. Journal of Healthcare Engineering (2022).