Advancements in Machine Learning for Network Anomaly Detection: A Comprehensive Investigation

Weishuo Xu[a]
Information Security, Nankai University, Tianjin, China

Keywords: Network Anomaly Detection, Machine Learning, Network Traffic.

Abstract: This study examines the progress made in Machine Learning (ML) techniques for identifying network abnormalities, which is crucial for ensuring cybersecurity in the modern day. At first, anomaly detection depended on partially automated, rule-based techniques, which were restricted by the constantly changing cyber threats and the intricate nature of networks. The incorporation of artificial intelligence has completely transformed detection methods, employing machine learning to improve precision and effectiveness. The exploration focuses on supervised learning models, namely Support Vector Machines (SVMs), K-Nearest Neighbors (KNN), and Random Forests. It emphasizes that these models heavily depend on large labeled datasets. In order to overcome this obstacle, the research explores unsupervised and semi-supervised methods that can detect new attacks even without labeled data. In addition, the study focuses on deep learning and reinforcement learning due to their sophisticated abilities in recognizing patterns and adapting to new information. The review identifies specific issues such as the reliance on huge datasets, the need for significant computational resources, and the desire for models that can be easily understood. It recommends that future research should prioritize the development of machine learning models that are adaptive, efficient, and interpretable for the purpose of detecting network anomalies.

1 INTRODUCTION

As humans progressively step into the digital age, people desire to quantify the transmission of data through a specific concept, which is known as network traffic. Defined as the volume of data traversing a computer network at any given moment, this concept includes a myriad of activities from email exchanges to server-to-server data transfers. Because of its expansive nature, network traffic is susceptible to various forms of disruption. Consequently, the concept of anomalous traffic patterns has been introduced. These may signal network attacks, system failures, or unauthorized activities, posing significant threats to the integrity and continuity of network operations.

Historically, or more precisely, before the maturation of artificial intelligence, several methods were invented to address anomalies such as those mentioned, especially in the fields of network security and traffic management. Evidently, these methods have become increasingly unsuitable in the contemporary context, primarily because they are inherently low in automation and heavily reliant on predefined rules and results derived from statistical analysis (Caberera, 2000). For instance, a signature-based detection method, which identifies malicious traffic through patterns described by predefined signatures, was once explored (Bolanowski, 2015). Similarly, rule-based detection and log analysis have been widely employed. Although effective in specific scenarios, these approaches demand a significant amount of human labor and may not adapt well to the new era characterized by increasingly innovative attack methods and more complex network situations (Roy, 2014).

Fortunately, the development and advancement of artificial intelligence has led to the emergence of novel technologies that can effectively identify and detect abnormal or unusual patterns of traffic. Machine learning, which is a subset of the whole area, functions by employing algorithms to facilitate computers in acquiring knowledge from data and making judgments based on that acquired knowledge.

[a] https://orcid.org/0009-0002-1615-7232

Xu, W.
Advancements in Machine Learning for Network Anomaly Detection: A Comprehensive Investigation.
DOI: 10.5220/0012959700004508
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 1st International Conference on Engineering Management, Information Technology and Intelligence (EMITI 2024)*, pages 585-589
ISBN: 978-989-758-713-9
Proceedings Copyright © 2024 by SCITEPRESS – Science and Technology Publications, Lda.

The field of cybersecurity has seen a substantial transformation, transitioning from rule-based systems to solutions driven by machine learning. This transition allows specialists to identify abnormal traffic patterns with exceptional efficiency and accuracy.

Among the various ML paradigms, supervised learning methods such as Support Vector Machines (SVMs) (Kong, 2017; Cao, 2020; Ma, 2021), K-Nearest Neighbors (Maniriho, 2020) and Random Forest (Assiri, 2021) have been extensively utilized for network anomaly detection. These methods fundamentally utilize labeled datasets to guide models in differentiating between normal and anomalous traffic patterns. While these approaches have been proven effective, they excessively rely on large and accurately annotated datasets, which, in practical application scenarios, may incur costs that exceed expectations (Salman, 2020).

In order to overcome the constraints of supervised learning, researchers have explored the use of unsupervised and semi-supervised learning approaches. The benefit of these techniques resides in their capacity to leverage data without requiring labels, enabling the identification of new or intricate attacks that may not be recorded by current datasets (Nguyen, 2020; Vikram, 2020; Dong, 2021).

Two further promising techniques include Deep Learning (DL) and Reinforcement Learning (RL). DL, a specialized subset of ML, leverages the properties of its multi-layer neural networks to tackle intricate problems in network traffic analysis. By utilizing automatic learning algorithms to extract feature representations from data, deep learning demonstrates its superiority in capturing nuanced differences and complex patterns in high-dimensional spaces (Hwang, 2020; Qiu, 2022). RL, a promising machine learning paradigm, allows models to learn the best actions by interacting with their environment and performing anomaly detection tasks in a dynamic manner. RL models can efficiently navigate the extensive and diverse range of network behaviors by constantly adjusting to observed network traffic conditions and striving to maximize the total rewards (Dong, 2021).

This literature review examines the utilization of different machine learning paradigms in the field of network anomaly detection. This study examines recent studies and their techniques to identify the benefits, constraints, and promise of each strategy in promoting the advancement of more flexible network security measures.

2 METHODS

2.1 Supervised Learning

2.1.1 SVMs

Support Vector Machines are an assortment of supervised learning models that are frequently used for regression as well as classification analyses. They operate by identifying the most advantageous hyperplane that divides distinct categories within the feature space. SVMs use the kernel trick to handle linear and non-linear data, focusing on maximizing the margin between the nearest data points of any class (support vectors) and the hyperplane. This strategy improves the model's ability to generalize, making SVMs highly useful for a variety of applications, particularly in areas with a large number of dimensions. Consequently, numerous researchers prefer using this supervised learning strategy for detecting aberrant traffic in these tasks.

For instance, Kong et al. develop an Abnormal Traffic Identification System (ATIS) employing a SVM classifier. This system integrates four key components: data collection, flow feature extraction, data processing, and SVM classification. The methodology focuses on capturing network traffic, aggregating packets into flows based on IP and port information, extracting relevant statistical features, and then transforming these into a format suitable for SVM classification. The SVM classifier, enhanced by "one-against-all" multi-classification strategy and optimized through kernel parameter tuning and feature scaling, is utilized to distinguish between normal and various types of attack traffic, demonstrating the effectiveness of SVM in network security applications (Kong, 2017). In another study carried by Jie Cao et al., the authors introduce two principal methodological advancements for network traffic classification using SVMs. Firstly, a hybrid Filter-Wrapper feature selection technique is developed to effectively reduce feature dimensionality while capturing the optimal feature subset, addressing the limitations of traditional feature selection methods by preventing the false exclusion of significant combined features. Secondly, an improved parameter optimization algorithm based on a refined grid search approach dynamically adjusts the search area and mesh density, optimizing SVM parameters to enhance classification accuracy and prevent overfitting (Cao,2020). Qian Ma et al. also provide SVM-L, a sophisticated anomaly detection model that utilizes a combination of data transformation and a novel hyper-parameter optimization technique. This work takes a different approach from previous methods by considering URLs as natural language. It uses statistical principles and natural language processing techniques to convert raw traffic data into mathematical vectors in an effective manner. This strategy significantly decreases the number of data dimensions while still preserving important classification features. In addition, SVM-L introduces a novel optimization model for fine-tuning hyper-parameters, simplifying the intricate work into a solvable one-dimensional optimization issue. This problem can be quickly addressed using the golden section approach (Ma, 2021).

2.1.2 Other Supervised Learning Models

Aside from Support Vector Machine, various other supervised learning techniques have also attracted the interest of researchers. K-Nearest Neighbors (KNN) and Random Forest algorithms have undergone substantial advancements. K-nearest neighbors algorithm functions by identifying the 'k' nearest training examples to a given input and determines its output based on these adjacent data points. The algorithm computes the distance between the input and every point in the training set, chooses the 'k' shortest distances, and then applies a majority vote or average for classification or regression tasks, respectively. The study conducted by Pascal Maniriho et al. investigates the performance comparison between a single machine learning classifier (Lazy IBK, a K-nearest neighbors approach) and an ensemble strategy (Random Committee) for detecting intrusions in computer networks. The uniqueness of this study is the utilization of the NSL-KDD and UNSW-NB15 datasets to conduct a thorough performance analysis. Additionally, the study employs the Gain Ratio Feature Evaluator (GRFE) for the purpose of selecting the most optimal features (Maniriho, 2020).

Random Forest generates multiple decision trees during training, employing a method of random selection of features at each split in the tree-building process. For a prediction, it aggregates the results from all individual trees, taking either a majority vote (for classification) or averaging the outcomes (for regression), thus producing the final output. Adel Assiri innovatively employs a Genetic Algorithm (GA) to optimize the parameter selection of the Random Forest (RF) classifier for enhancing anomaly classification in Network Intrusion Detection Systems (NIDS). Unlike traditional methods, this approach systematically selects the optimal values for the number of trees and the minimum number of instances per split in the RF, addressing a critical challenge in RF-based anomaly classification (Assiri,2021).

2.2 Unsupervised Learning

In the realm of network security, the utilization of unsupervised machine learning presents a compelling approach for the detection of anomalous traffic, particularly in scenarios where labeled datasets are scarce or when the attack patterns are too sophisticated or novel to be captured by traditional rule-based systems. The study by Thi Quynh Nguyen et al. exemplifies the application of unsupervised learning in the context of DNS traffic analysis. The research evaluates four unsupervised algorithms—K-means, Gaussian Mixture Model (GMM), Density-Based Spatial Clustering of Applications with Noise (DBSCAN), and Local Outlier Factor (LOF)—for their effectiveness in detecting malicious DNS activities (Nguyen, 2020). Aditya-Vikram Mohana presents another noteworthy implementation of this approach through the Isolation Forest (IF) algorithm. Central to Mohana's methodology is a rigorous data preprocessing phase, including normalization and feature scaling, aimed at preparing the NSL-KDD dataset for analysis (Vikram, 2020).

2.3 Deep Learning

Deep learning is a subdivision of machine learning that use neural networks with multiple layers to gain understanding of data representations. Neural networks, which are influenced by the architectural arrangement of the human brain, consist of layers of nodes, also referred to as neurons. The incoming data undergoes transformations via various layers via operations that facilitate the model's ability to make predictions, classify data, and recognize patterns. Ren-Hung Hwang et al. introduce a novel deep learning framework named D-PACK that combines a Convolutional Neural Network (CNN) with an autoencoder to identify network traffic anomalies in their initial stages. This system distinguishes itself by giving priority to the initial bytes of the first few packets in each network flow, rather than requiring the entire flow data for analysis. This innovative approach enables the model to identify abnormalities in their initial stages, leading to a substantial decrease in the volume of data examined and facilitating the detection of anomalies in real-time (Hwang, 2020).

2.4 Reinforcement Learning

Reinforcement Learning is a sort of machine learning in which an agent acquires the ability to make decisions by doing actions in an environment with the goal of maximizing a measure of overall reward. The defining feature of this phenomenon is the presence of an entity that engages with its surroundings, obtaining feedback in the form of rewards or penalties to guide its subsequent behaviors. The study carried out by Dong et al. advances the field by introducing a semi-supervised learning model that integrates Deep Reinforcement Learning with unsupervised learning techniques. The model employs a Semi-Supervised Double Deep Q-Network (SSDDQN), which combines an Autoencoder for feature reconstruction and K-Means clustering for unsupervised label prediction with the Double Deep Q-Network (DDQN) framework for optimization. This hybrid approach enables the effective detection of abnormal network traffic with significantly reduced reliance on labeled data. The innovation lies in its semi-supervised framework that leverages unsupervised learning to alleviate the challenges associated with the high costs and scarcity of labeled datasets (Dong, 2021).

3 DISCUSSIONS

The machine learning paradigms in network anomaly detection reveal a situation that is both marked by significant progress and faced with considerable challenges. Traditional ML models, such as SVMs and KNN, while capable of addressing some basic issues of anomalous traffic detection, necessitate additional preprocessing steps for their datasets. This is because the creation and division of datasets are likely influenced by subjective biases, potentially leading to the artificial generation of poor features.

Deep learning models, despite their superior capability in feature learning and identifying complex anomaly patterns, face challenges regarding interpretability, computational intensity, and the demand for large data volumes. These challenges limit their practical application, especially in environments where computational resources are constrained, or data privacy concerns restrict the availability of training data. Additionally, the "black-box" nature of deep learning models complicates the extraction of actionable insights from their findings, a significant impediment in cybersecurity contexts where understanding the nature of an anomaly is crucial for effective response.

Reinforcement learning introduces a promising dynamic approach by adapting to new threats through interaction with the environment. However, RL's application in network anomaly detection is nascent, with issues around model convergence, reward mechanism definition, and the practical implementation in real-world scenarios still unresolved. These challenges underscore the complexity of developing ML models that can effectively navigate the constantly shifting landscape of network security threats.

Based on the discussions mentioned above, the future of anomaly detection in network traffic monitoring hinges on the development of more adaptable, efficient, and interpretable ML models. Achieving this goal involves not only technological advancements but also a nuanced understanding of the cybersecurity domain's evolving needs. As such, future research should aim to refine these ML paradigms, enhancing their resilience against novel threats while ensuring they remain grounded in practical application considerations.

4 CONCLUSIONS

This article underscores the importance of advanced network anomaly traffic monitoring in the current digital era and the transition from classical monitoring methods to those based on machine learning. The focus of the article is on introducing and evaluating different machine learning approaches within this field, including traditional models of supervised learning, as well as more complex techniques such as deep learning and reinforcement learning. While these models have shown great potential in detecting anomalous traffic, they each face difficulties in data processing, feature extraction, and the demands for interpretability. Moreover, the article itself presents certain issues, including an incomplete introduction of emerging algorithms. For the future, this paper suggests focusing efforts on balancing model accuracy with computational efficiency and seeking methods to reduce reliance on large, labelled datasets. Subsequent research will also concentrate on enhancing the interpretability of models to address the continuously evolving network security risks.

REFERENCES

Assiri, A. 2021. Anomaly classification using genetic algorithm-based random forest model for network attack detection. *Computers, Materials & Continua*, 66(1).

Bolanowski, M., & Paszkiewicz, A. 2015. The use of statistical signatures to detect anomalies in computer network. In *Analysis and Simulation of Electrical and Computer Systems* (pp.251-260). Springer International Publishing.

Caberera, J. B. D., Ravichandran, B., & Mehra, R. K. 2000, August. Statistical traffic modeling for network intrusion detection. In *Proceedings 8th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems* (Cat. No. PR00728) (pp. 466-473). IEEE.

Cao, J., Wang, D., Qu, Z., Sun, H., Li, B., & Chen, C. L. 2020. An improved network traffic classification model based on a support vector machine. *Symmetry*, 12(2), 301.

Dong, S., Xia, Y., & Peng, T. 2021. Network abnormal traffic detection model based on semi-supervised deep reinforcement learning. *IEEE Transactions on Network and Service Management*, *18*(4), 4197-4212.

Hwang, R. H., Peng, M. C., Huang, C. W., Lin, P. C., & Nguyen, V. L. 2020. An unsupervised deep learning model for early network traffic anomaly detection. *IEEE Access*, *8*, 30387-30399.

Kong, L., Huang, G., & Wu, K. 2017, December. Identification of abnormal network traffic using support vector machine. In *2017 18th international conference on parallel and distributed computing, applications and technologies (PDCAT)* (pp. 288-292). IEEE.

Ma, Q., Sun, C., Cui, B., & Jin, X. 2021. A novel model for anomaly detection in network traffic based on kernel support vector machine. *Computers & Security*, 104, 102215.

Maniriho, P., Mahoro, L. J., Niyigaba, E., Bizimana, Z., & Ahmad, T. 2020. Detecting Intrusions in Computer Network Traffic with Machine Learning Approaches. *International Journal of Intelligent Engineering & Systems*, *13*(3).

Nguyen, T. Q., Laborde, R., Benzekri, A., & Qu'hen, B. 2020, October. Detecting abnormal DNS traffic using unsupervised machine learning. In *2020 4th Cyber Security in Networking Conference (CSNet)* (pp. 1-8). IEEE.

Qiu, Y., Wang, J., Jin, Z., Chen, H., Zhang, M., & Guo, L. 2022. Pose-guided matching based on deep learning for assessing quality of action on rehabilitation training. *Biomedical Signal Processing and Control*, 72, 103323.

Roy, D. B., & Chaki, R. 2014, February. State of the art analysis of network traffic anomaly detection. In *2014 Applications and Innovations in Mobile Computing (AIMoC)* (pp. 186-192). IEEE.

Salman, O., Elhajj, I. H., Kayssi, A., & Chehab, A. 2020. A review on machine learning–based approaches for Internet traffic classification. *Annals of Telecommunications*, *75*(11), 673-710.

Vikram, A. 2020, June. Anomaly detection in network traffic using unsupervised machine learning approach. In *2020 5th International Conference on Communication and Electronics Systems (ICCES)* (pp. 476-479). IEEE.