International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

A Review of Deep Learning Techniques for Optimizing Accuracy in Network Attack Detection

Arshad Husain
Department of Computer Science and Engineering
Research Scholar, Rajshree Institute of Management and Technology, Bareilly
Dr Ruchin Jain (HOD)
Department of Computer Science and Engineering
Guide, Rajshree Institute of Management and Technology, Bareilly

Abstract
As cyber threats grow in complexity and volume, traditional network security approaches are increasingly unable to provide effective and timely protection. Deep learning has emerged as a transformative solution for detecting network attacks with improved precision and adaptability. This review presents a comprehensive analysis of current deep learning techniques applied to network intrusion detection systems (NIDS). It explores how models like CNNs, RNNs, LSTMs, and Autoencoders can learn from vast, high-dimensional network data to detect both known and unknown threats. The study also examines hybrid architectures and ensemble models that enhance detection accuracy by integrating multiple learning methods. Emphasis is placed on the role of data preprocessing, feature selection, and evaluation metrics in optimizing model performance. Moreover, key challenges such as limited labeled data, real-time detection constraints, interpretability issues, and resilience against adversarial attacks are critically discussed. The review concludes by highlighting emerging trends, including the use of federated learning, lightweight DL models for edge deployment, and explainable AI for transparent threat analysis. Overall, the paper provides valuable insights into how deep learning continues to shape the future of intelligent and efficient network attack detection systems.

Keywords: Deep Learning, Network Intrusion Detection, Cyber Threats, Neural Networks, Attack Detection Accuracy

Introduction

Internet connected systems and digital infrastructure to new heights, cybersecurity threats are becoming complex and pervasive than ever. However, traditional security mechanisms, especially IDS based on signatures, often lack the capability of detecting new, emerging attack patterns and lose their efficacy in real time threat detection. Specifically, deep learning (DL)

has been demonstrated as a very promising tool for improving accuracy and adaptability of network attack detection systems in this context. DL models can uncover subtle patterns and anomalies from large volumes of data and large number of features using hierarchical feature learning. Nowadays, we have techniques that deal with network traffic for malicious behavior classification, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory networks (LSTMs), and Deep Belief Networks (DBNs) which can analyse the traffic with high precision.

In this paper, this review talks about the different deep learning-based approaches which can be used to make the optimization of the detection accuracy for network security. It compares the performance of different DL architectures in handling structured and unstructured network data as well as handling class imbalance and working in real-time IR environment. Additionally, the enhancement in performance by combining DL with other machine learning algorithms or feature engineering techniques is shown to help in extracting complex threat signatures and reducing false positives. Further discussion is provided regarding the benchmark datasets used such as NSL-KDD, CICIDS2017 and UNSW-NB15, and their usage in the practical evaluation of DL models. Ultimately, this paper argues that deep learning is key to the next generation of intelligent IDS solutions, and determines undercurrent research topics, such as interpretability of deep models, deep learning robustness, and scalability for real time deployment.

Background of network security and intrusion detection

With the increase of connections being made in the world through the internet, network security has now become a very important issue for both individuals, organizations and governments. Is the practice of network security in which the policies, technologies, and practices are aimed at protecting data confidentiality, data integrity, and the availability of data from cyber threat. Digital transformation has brought greater sophistication and numbers of cyberattacks to light such as Denial of Service (DoS), phishing, malware, ransomware and zero-day attacks. These threats lead to financial loss, data breaches and critical service disruption. For this reason, there is a growing need of threat identifying, analyzing and mitigating intelligent systems, which can prevent threats from effectively inflicting large damage.

Monitoring network traffic to find any signs of malicious activity is the main job where Intrusion Detection Systems (IDS) plays a major role. There are two major categories of IDS techniques from the traditional point of view: the signature based and the anomaly based. For

known threats, signature-based detection compares activities observed to a database of known patterns and has high accuracy, but it does not detect new or unknown attack. On the other hand, anomaly-based systems use statistical methods or machine learning to find the difference between normal behavior and unusual behavior and can detect novel threats but at a price of higher false positive rates. Thus, these traditional methods have had difficulties keeping up to this pace over time as cyber threats evolve. With this, there has been the need to explore more advanced approaches like deep learning that are able to automatically capture features and learn complex patterns in the network traffic data. Promising capabilities of the deep learning models in detecting known and unknown attacks at higher accuracy and adaptability serve as a basis for the next generation of intelligent and proactive network security solutions.

Motivation for using deep learning

This has been because intrusion detection strategies have been limited by the growing complexity and frequency of cyberattacks. As deep learning is able to automatically learn hierarchical representations of data with little manual feature engineering, deep learning presents a highly promising alternative. Deep learning architectures like Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) or Autoencoders can process raw network traffic raw data and extract subtle or complex features to detect malicious behavior without any kind of domain specific knowledge. As such, deep learning is extremely efficient in discovering both known and unknown (zero day) attacks. Moreover, deep learning models can accommodate huge and high dimensional datasets which are the norm in most modern networks with massive amount of data generated in such networks. In addition, they are very adaptive to continuously changing environments where attack strategy changes over time. Furthermore, along with improvements in GPU computing and the existence of big labeled datasets eg NSL-KDD and CICIDS2017, the deep learning-based protection tools development and deployment in cybersecurity are also skyrocketed. Deep learning in network intrusion detection has been integrated to improve the accuracy of detection and also decrease the false positive errors and false negative errors, the disadvantages of conventional IDS. Deep learning is powerful and future ready technique for securing network infrastructures against sophisticated cyber threats. The combination of capabilities makes deep learning a compelling way to defend network structures against advanced cyberattacks.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

Overview of Network Attack Detection

Current network security systems emphasise on the detection of network attacks that violate the confidentiality, integrity, and availability of network systems. As we continue to incorporate digital communication and exchange of data into everyday life, networks become almost constant targets of attackers that use various techniques. There are certain common types of Network Attacks such as Denial of Service (DoS), Distributed Denial of Service (DDoS), phishing, man in the middle attack, malware injection, port scan, and trying to unauthorized access. Such attacks compromise sensitive information, disrupt services, and wreak large financial and reputational damage. Network intrusion detection systems (IDS) are used to monitor suspicious traffic patterns and attempt to respond to those threats. IDS solutions occur at different network layers and can be installed endpoints, gateways, or cloud infrastructures.

The intrusions are broadly classified into two categories, i.e., signature based and anomaly-based detection methods. An IDS by using signature method detects attacks since it compares observed traffic with a set of known hazard patterns, or "signatures," in a database. Though this technique is effective in picking up known attack classes, it overlooks changes and/or new attacks. On the other hand, the anomaly-based detection operates using a model that characterizes normal network traffic and raising the flag when a deviation from baseline is observed. Because of this, it is suitable for detecting zero-day attacks but also contributes to a higher rate of false positives. With the attack vectors growing more sophisticated and with the amount of network data increasing, traditional detection techniques are difficult to maintain speed, accuracy and reliability. As a result, modern approaches have been increasingly turning to machine learning and even more so to deep learning. Accumulating many complex relationships in high dimension network traffic data, these technologies can provide an improved detection capability. Deep learning models thus constitute a huge progress in network attack detection since they allow feature extraction to be automated and adapted to changing attack patterns.

Literature review

Afreen Bhumgara and Anand Pitale (2019) A detection of network intrusion through a hybrid intelligent system is the integration of numerous techniques of machine learning and artificial intelligence to boost the accuracy and efficiency of detection of the presence of unauthorized access or abnormal behavior in the network. This approach combines different

models like neural networks, decision trees and fuzzy logic to exploit the power of the strengths of each one of them. Hybrid systems can detect subtle patterns that indicate intrusions by processing huge amounts of network data that might normally be missed by traditional methods. Pattern recognition can be done by Neural networks and decision trees helps in classification of data based on set rules. The fuzzy logic enables system to manage uncertainty and deciding with uncertain, incomplete or ambiguous information. The hybrid intelligent system is more adaptive and can detect a larger number of intrusions including new and zero days attacks by combining these techniques. The intrusion detection mechanism becomes more robust, reliable, and in a real time, what is needed for a network security.

Ritumbhira Uikey and Dr. Manari Cyanchandani (2019) This paper has explored a survey on classification techniques applied to intrusion detection systems (IDS) and their applications to classify various attacks on network using machine learning. Supervised learning algorithms such as decision trees, support vector machines (SVM), k nearest neighbor (KNN), and neural networks which have their own advantages in terms of accuracy and processing power are amongst these techniques. Clustering algorithms, as one of unsupervised learning methods, are also used to detect unknown or novel attacks without data in hand. A comparative analysis of these techniques is then made on how they behave in terms of their detection rate, false alarm rate, scalability, and capability to adapt to new attack patterns. SVM is known to be highly accurate, and some times more accurate than decision trees, especially for binary classification, which runs by a high of accuracy of 99%. Although complex, they are very good at detecting complex patterns. The technique strengths and limitations for real time intrusion detection and system security are pointed out by the survey.

Aditya Phadke et al (2019) In this article a review of machine learning methodologies for the network intrusion detection is presented which applies different learning algorithms to detect and solve possible security threats in computer networks. Though there are different methodologies, which includes supervised, unsupervised and semi supervised learning for finding out the malicious activities. These techniques involve supervised learning, where some of the data is labeled as normal or intrusive, and the other methods are trained to learn how to classify network traffic as normal or intrusive. Using unsupervised methods, such as clustering and anomaly detection algorithms, to find patterns of previously unknown or novel attacks from a typical pattern. In addition, utilizing both labeled and unlabeled data helps to detect rare or changing threats, which is called as semi supervised learning. It also points out critical

challenges like feature selection, dealing with imbalanced datasets and real time performance requirement. In general, machine learning methodologies offer a compelling paradigm for improving the accuracy and productivity of a network intrusion detection system.

S. Sivantham et al (2019) In this sense, comparison of anomaly based intrusion detection systems (IDS) on networks can be viewed as investigation of several ways of detecting abnormal deviations from normal network behavior, which can be a result of malicious activity. Anomaly based systems constantly monitor network traffic versus a baseline of normal behavior. Any large deviation of the model is immediately flagged as a potential intrusion. Establish and update baseline using various techniques, such as using statistical methods, machine learning models, clustering algorithms, etc. Outliers detection is done via statistical methods with predefined thresholds and distributions, or from the machine learning model that utilizes the network traffic patterns to detect anomalous behavior (i.e. neural network and support vector machines). Data points are clustered together, outliers are found in these clusters, using clustering algorithms. However, managing false positives is a key challenge with an anomaly-based IDS because sometimes benign activities are anomalous. Yet, these systems are very effective in detecting zero-day attacks and intrusions that were not previously known, hence contributing lots to the current network security systems.

Azar Abid Salih and Maiwan Bahjat Abdulrazaq (2019) But combining the best feature selection technique with three classifiers in a system of intrusion detection (IDS), improves its ability to accurately and efficiently detect network intrusions. This step constitutes the reduction in dimensionality of the data, which is critical in IDS since it enhances the performance as well as the interpretability of the model. The system reduces the number of features selected such that the most relevant features are chosen, therefore, the system concentrates on the key patterns that differentiate normal from malicious network behavior. In this approach, we use the combination of three classifiers namely decision trees, SVM, and KNN to test and classify network traffic using the selected feature set. The strengths of each classifier are exploited, as the outputs of the classifiers are combined and the accuracy and redundant false positives are minimized. Using multiple classifiers improve robustness to various attack types, so that the IDS is still capable of detecting both known and unknown threats.

Lukman Hakim and Rahilla Fatma Novriandi (2019) Clearly, feature selection has a significant effect on the performance of a network intrusion detection system (NIDS) in terms

of detection accuracy, and also with respect to system overhead. As such, in this analysis, we use the NSL-KDD dataset, a widely recognized benchmark for the intrusion detection problem, to determine how choosing the most relevant features affects the effectiveness of NIDS. Several feature selection methods, including mutual information, chi-square, and correlation-based methods, are applied in order to select the most discriminative attributes that separate normal from malicious network traffic. The study demonstrates that if a smaller, more relevant set of features can be chosen, the classification performance of the system improves dramatically, significantly elevating detection rates and decreasing false positive rates. The system will be less likely to overfit by eliminating the redundant or irrelevant features. Feature selection has proven to be critical to the construction of NIDS, and this analysis illustrates the effect of it on performance and on the consumption of computational resources, and perhaps, emphasizes the importance of feature selection as the central step in the building of intrusion detection models.

Lan Liu et al (2020) Intrusion detection in imbalanced network traffic using machine learning and deep learning techniques is solving the problem of intrusion detection from datasets where the number of normal instances is several magnitudes than that of malicious instances. Sometimes Imbalanced datasets lead to a high rate of false negatives, where attacks are not detected too due to very obtrusive benign traffic. This is solved using machine learning algorithms such as decision tree, support vector machine (SVM) as well as ensemble methods, which use information of both the classes to balance the detection process and focus on minority classes (intrusions) for detection. Moreover, convolutional neural networks and recurrent neural networks are also utilized to automatically extract useful features of raw network data and address complicated patter of traffic behavior. These models use oversampling, undersampling, and cost sensitive learning techniques to improve detection performance, and such that even rarely occurring and sophisticated attacks are detected properly. Combining the machine and deep learning techniques, with improvements of the detection accuracy and robustness in imbalanced environment.

A. Raghavan et al (2019) Two advanced techniques, that of hidden Markov models (HMMs) with random restarts and boosting, are used for malware detection with each technique having its own advantages in identifying malicious software. Marecar model the behaviour of malware over time as sequential patterns with system activities, using HMMs which are a statistical model representing system consisting of hidden states. To avoid local minima in the

optimization process, HMMs can incorporate random restarts and be further enhanced in finding more accurate patterns of such malicious behavior. In contrast, boosting is an ensemble learning that produces stronger (stronger) classifier by combining multiple weak classifiers. Working iteratively, it focuses on misclassified instances and increases the detection accuracy by focusing on harder to detect malware samples. Therefore, HMMs excel in sequential modeling, whereas boosting is very efficient in boosting performance of simple classifiers. To compare theses methods, we conduct a comparative analysis and find that boosting usually outperforms HMMs in terms of accuracy of classification, but HMMs may have the advantage in representation of the dynamics of malware behavior over time."

Zhiyou Zhang and Peishang Pan (2019) A hybrid network intrusion detection method based on improved fuzzy C-means (FCM) clustering and support vector machine (SVM) integrates the merits of unsupervised and supervised classification to improve the network security. For clustering of network traffic data, the fuzzy C-means algorithm is used to cluster the data points into a number of fuzzy clusters each of which is characterized by the degrees of memberships, that helps identify both the patterns in the traffic and outliers. For the FCM technique, the improvement is mostly on its parameters or couplings with other methods, like feature selection, to improve the clustering accuracy. Having clustered the data, an SVM classifier is used to differentiate normal from malicious traffic. SVM is successful in high dimensional spaces and can accommodate any sort of nonlinear data. This hybrid method is an improvement over FCM and SVM by combining adaptability of FCM with precise classification ability of SVM, that is, it overwhelms others in detecting various types of network intrusions, reduce false positives, and enhance overall system efficiency.

Kezhou Ren et al (2022) Deep reinforcement learning (DRL) based unmanned network intrusion detection model is an original approach to the automated network security threats detection and response. This model employs DRL for the agent over the network environment where this agent learns from his actions continuously in order to detect malicious activities. Different from traditional IDSs which need prior rules or labeled data, the DRL agent learns the optimal detection strategies by trial and error, and gets better in making decisions as more trials. The model works with a reward based model where the agent is rewarded with positive points upon correctly classifying intrusions and negative or zero points for false positives or negatives. Due to its ability to adapt and evolve, the system can detect new or unknown attack patterns, thus, being better suited to detect unknown (zero-day) threats. The main features of

this approach include scalability, real-time detection, as well as the level of its autonomous, dynamic and efficient intrusion prevention in complex network environments.

Deep Learning Techniques for Network Attack Detection

Due to its capability to process large amount of dataset and discover subtle patterns which are otherwise very difficult to capture using classical approaches, Deep learning (DL) has become a transformative approach for network security. Convolutional Neural Networks (CNNs) are the most widely used deep learning techniques for network attack detection, because they are particularly good at identifying spatial features in structured input data such as traffic flow matrices. Feature engineering for packet header or flow data is no longer required because CNNs can extract relevant features automatically. This is due to the fact that their layered architecture helps them to capture both low level and high-level features, which enables them to detect various type of attacks including DoS, probe and infiltration attempts.

Another attractive choice in intrusion detection is Recurrent Neural Networks (RNNs), and especially Long Short-Term Memory (LSTM) networks due to their skill in processing sequential data. Given this fact, LSTMs can learn time dependent patterns and relationships in traffic streams. Because of this, they are well suited for detecting attacks that happen over time, for example, botnet communications, or data exfiltration. Moreover, RNN based models hold context over longer input sequences making them suitable for real time monitoring and detection of delayed or subtle attacks which may not be identified by other means.

Network intrusion detection is also carried out using Autoencoders and hybrid deep learning models. Unsupervised learning models known as autoencoders learn how to reproduce input data and can effectively identify anomalies (faults) because they compute the reconstruction error. Anomalies or attacks usually result in higher reconstruction error. As a result, more and more hybrid models are utilized to enhance detection accuracy at the expense of generating false positives, which comprise of combining various deep learning architectures (e.g., CNN + LSTM) or traditional machine learning algorithms. The combinations of models allow for utilizing the advantages of other methods such as spatial feature extraction, sequential learning, and anomaly detection into a single framework. With cyber threats progressing, the employment of various deep learning models strengthens the immunity, expandability, as well as the adaptability of intrusion detection systems, therefore indicating the direction towards more intelligent and precautionary network security solutions.

Challenges and Future Directions

Although there have been promising results of deep learning in network attack detection, there exist many challenges that impede its integration into real–world systems. Interpretability of deep learning models is one of the main troubles. The majority of the DL models run as the black box, leaving the cybersecurity analysts clueless about why a certain traffic pattern is labelled as malicious. However, the absence of transparency makes it difficult to build trust and to make decision in such critical environments. Moreover, deep learning models usually demand batches of large quantities of high quality and labelled data to train well, and it is not always possible to obtain such data, particularly for rare or novel attack types. A second major drawback is dataset imbalance, i.e., benign traffic largely dwarfs the number of malicious samples causally resulting in biased models with a poor detection rate of minority classes. These models are also computationally intensive, requiring a large amount of training and inference resources and are difficult to deploy in near real time, or constrained resource environments such as IoT networks.

Future research in deep learning focuses on creating more efficient, interpretable, and resilient deep learning models. There is a trend of research on explainable AI (XAI) which demands explanations of model decisions in a manner that is intelligible to and justifiable for the human users. There are also being explored lightweight and energy efficient DL architectures, which will facilitate faster inference and real time processing on edge devices. Another important direction is that of adversarial robustness since DL models are vulnerable to specially crafted input that may be able to evade detection. Reliability can only be maintained with the integration of defense mechanisms against such attacks. In addition, unsupervised and semi supervised learning methods are proposed to reduce the dependence on labeled data and enhance the model generalization to unseen threats. Lastly, deep learning is being combined with federated learning and blockchain technologies to better protect data privacy and secure model training in a peer-to-peer system. They indicate the need for more flexible, translucent and secure deep learning solutions for the emerging networks attack detection landscape.

Conclusion

In recent times, there has been an increasing adoption of deep learning making it one very effective and a relatively young avenue to improve the accuracy and intelligence of network attack detection systems. These models make use of advanced architectures like Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), or Long Short-Term Memory (LSTM) networks, and Autoencoders, which automatically extract high level complex features

in massive volumes of network traffic data, allowing for detection of known, as well as previously unseen cyber threats. Deep learning is capable of learning from raw data, able to dynamically adapt to adversaries changing the strategy, and reduces reliance on manual feature engineering, making it a great advancement in contrast with conventional intrusion detection methods. Nevertheless, deep learning techniques suffer a number of challenges, such as data imbalance, model interpretability, computational complexity, and vulnerability to adversarial attacks, yet promise to tackle them in the near future. To avoid conducting research on toy problems, and to guarantee the reliable incorporation into real-time, large-scale network environments, these challenges must be addressed. Future research will aim to build more transparent, less computationally expensive, and more robust models, by increasing use of unsupervised learning, federated learning, and adversarial defences. The goal is to make these advancements in scalability, trustworthiness, and adaptability of deep learning systems in cyber threat landscapes becoming more and more complex. All in all, the deep learning in network attack detection seems to be a bright future for developing more secure and intelligent cyber security frameworks, and it is a key research and innovative field to be developed in the face of increasing digital threats.

References

[1] Kezhou Ren, Maohuan Wang, Yifan Zeng and Yingchao Zhang, *"*An Unmanned Network Intrusion Detection Model Based on Deep Reinforcement Learning*",* IEEE International Conference on Unmanned Systems (ICUS), IEEE 2022.

[2] R. Ahsan, W. Shi, X. Ma, and W. L. Croft, "A comparative analysis of CGAN-based oversampling for anomaly detection," *IET* Cyberphysical Systems: Theory & Applications, vol. 7, no. 1, pp. 40–50, Mar. 2022.

[3] S. Dong, Y. Xia, and T. Peng, "Network Abnormal Traffic Detection Model Based on Semi-Supervised Deep Reinforcement Learning," IEEE Transactions On Network And Service Management, vol. 18, no. 4, pp. 4197–4212, Dec. 2021.

[4] Lan Liu, Pengcheng Wang , Jun Lin, and Langzhou Liu, "Intrusion Detection of Imbalanced Network Traffic Based on Machine Learning and Deep Learning", IEEE Access 2020.

[5] A. Raghavan, F. D. Troia, and M. Stamp, ``Hidden Markov models with random restarts versus boosting for malware detection," *J. Comput. Virol. Hacking Techn.*, vol. 15, no. 2, pp. 97107, Jun. 2019.

[6] Zhiyou Zhang and Peishang Pan "A hybrid intrusion detection method based on improved fuzzy C-Means and SVM", IEEE International Conference on Communication Information System and Computer Engineer (CISCE), pp. no. 210-214, Haikou, China 2019.

[7] Afreen Bhumgara and Anand Pitale, "Detection of Network Intrusion Using Hybrid Intelligent System", IEEE International Conferences on Advances in Information Technology, pp. no. 167-172, Chikmagalur, India 2019.

[8] Ritumbhira Uikey and Dr. Manari Cyanchandani "Survey on Classification Techniques Applied to Intrusion Detection System and its Comparative Analysis", IEEE 4th International Conference on Communication $ Electronics System (ICCES), pp. no. 459-466, Coimbatore, India 2019.

[9] Aditya Phadke, Mohit Kulkarni, Pranav Bhawalkar and Rashmi Bhattad "A Review of Machine Learning Methodologies for Network Intrusion Detection", IEEE 3rd National Conference on Computing Methodologies and Communication (ICCMC), pp. no. 703-709, Erode, India 2019.

[10] S. Sivantham, R.Abirami and R.Gowsalya "Comapring in Anomaly Based Intrusion Detection System for Networks", IEEE International conference on Vision towards Emerging Trends in Communication and Networking (ViTECon), pp. no. 289-293, Coimbatore, India 2019.

[11] Azar Abid Salih and Maiwan Bahjat Abdulrazaq "Combining Best Features selection Using Three Classifiers in Intrusion Detection System", IEEE International Conference on Advanced science and Engineering (ICOASE), pp. no. 453-459, Zakho - Duhok, Iraq 2019.

[12] Lukman Hakim and Rahilla Fatma Novriandi "Influence Analysis of Feature Selection to Network Intrusion Detection System Performance Using NSL-KDD Dataset", IEEE International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE), pp. no. 330-336, Jember, Indonesia 2019.