Advances in IT and Electrical Engineering

vol. 30, 2024, 49-59
https://doi.org/10.7862/re.2023.x

THE FACULTY OF ELECTRICAL AND COMPUTER ENGINEERING
RZESZOW UNIVERSITY OF TECHNOLOGY

Original Research/Review

Impact of Artificial Intelligence on Computer Networks

Kacper Zdrojewski [1*]

[1] Department of Information Technology Networks, Regional Information Technology Center Warsaw, 00-909 Warsaw, Poland.

* Corresponding author. kacper.zdrojewski.1997@gmail.com

Received: 24 October 2024 / Accepted: 23 December 2024 / Published online: 31 December 2024

Abstract

The integration of artificial intelligence (AI) into computer networks has rapidly evolved, influencing network architecture, security measures, and traffic management. This paper explores AI's transformative impact on these areas, focusing on advancements in machine learning (ML), deep learning (DL), and reinforcement learning. These innovations are reshaping network security by improving threat detection and anomaly identification, as well as enhancing traffic management through predictive and adaptive routing. AI-driven systems are also making strides in automating network management tasks, allowing for more efficient resource allocation and self-healing networks. Despite these advancements, challenges remain, particularly concerning the integration of AI with legacy infrastructures and the ethical implications of AI decision-making processes.

Keywords: artificial intelligence, machine learning, network security, deep learning

1. Introduction

In recent years, the integration of artificial intelligence into various domains has revolutionized industries, with computer networks being a notable beneficiary of these advancements. As global internet traffic grows exponentially, driven by the proliferation of Internet of Things (IoT) devices, cloud computing, 5G technology, and the ever-increasing demand for bandwidth, the complexity of managing and securing networks has become a critical challenge. Traditional network management techniques, often based on manual configuration and rule-based systems, struggle to cope with this increasing complexity and the dynamic nature of modern networks.

Simultaneously, the number and sophistication of cyber threats continue to grow. Traditional intrusion detection systems (IDS) rely heavily on predefined signatures or rules to detect known threats. While effective against previously encountered attacks, these systems often fail to identify novel or evolving threats, such as zero-day vulnerabilities or advanced persistent threats (APTs) [2]. This has led to a paradigm shift towards more adaptive, AI-driven approaches.

AI, particularly machine learning and deep learning, offers promising solutions to these challenges. By leveraging vast amounts of historical and real-time data, AI models can learn traffic patterns, detect anomalies, and make decisions autonomously. For instance, AI-driven systems can automatically adjust traffic routing based on real-time congestion data, ensuring optimal performance and minimizing packet loss. In terms of security, AI systems can detect and mitigate threats more efficiently by identifying anomalous behavior that might indicate the presence of malicious activity [2, 3].

Moreover, reinforcement learning (RL) has enabled networks to adapt in real-time by optimizing routing paths and network configurations dynamically. These RL-based systems learn by continuously interacting with the network environment, making them ideal for highly dynamic network scenarios, such as mobile ad hoc networks (MANETs) or multi-cloud architectures.

However, the deployment of AI in network environments also presents unique challenges. The integration of AI systems with legacy network infrastructure is often difficult due to hardware limitations or the lack of necessary computational resources. Additionally, the growing reliance on AI for critical network functions raises concerns regarding accountability, transparency, and the potential for bias in AI decision-making processes [1]. Despite these challenges, the potential benefits of AI integration into computer networks - such as enhanced security, more efficient traffic management, and autonomous network operations - are vast and continue to drive research and development in this area.

This paper delves into the multifaceted impact of AI on computer networks, examining how AI can address current networking challenges and predict future trends. Artificial intelligence refers to the simulation of human intelligence by machines, encompassing a broad range of techniques and approaches. These include machine learning, where systems learn from data to make predictions or decisions, and deep learning, a subset of ML that uses neural networks to model complex patterns in data. Computer networks refer to interconnected systems of devices and communication technologies that enable data exchange. These networks can be viewed from different perspectives, including physical infrastructure (e.g., wired or wireless networks), logical architecture (e.g., client-server or peer-to-peer models), and functional layers such as transport, application, or network layers in the OSI model. This article focuses on how AI can enhance the management and optimization of such networks across various layers, particularly in areas like traffic management, security, and resource allocation.

2. AI in Network Security

AI has become indispensable in securing modern computer networks, where the volume and complexity of cyberattacks are constantly growing. Traditional network security methods, such as firewalls and signature-based intrusion detection systems, are increasingly insufficient in the face of sophisticated threats. AI enhances network security by enabling dynamic threat detection and rapid response to anomalies. ML-based IDS can analyze historical network traffic data to identify malicious patterns, while DL systems improve this capability by learning from unstructured data and detecting novel attacks.

2.1. Machine Learning in Intrusion Detection

Intrusion detection focuses on identifying unauthorized access and abnormal activities within network environments. The primary challenge lies in distinguishing between legitimate and malicious traffic in real-time, a task complicated by the diversity and scale of modern networks. The effectiveness of an IDS is typically measured using metrics such as detection rate, false positive rate, precision, recall, and F1 score [12, 13]. Traditional methods, relying on predefined signatures (such as Snort[1] or AIDE[2]), struggle to detect novel threats such as zero-day attacks, highlighting the need for adaptive, intelligent systems. Zero-day attacks are cyber exploits targeting unknown vulnerabilities in software or hardware, leaving no time for defensive measures.

Machine learning has revolutionized intrusion detection by providing more accurate and scalable solutions compared to rule-based systems. Supervised learning algorithms, such as Support Vector Machines (SVM) and Random Forests, are trained on labeled datasets to distinguish between legitimate and malicious traffic. However, one limitation is their reliance on large datasets for training, which can result in performance issues when faced with zero-day attacks. On the other hand, unsupervised learning, including anomaly detection, enables the identification of previously unknown threats by analyzing deviations from normal traffic behavior.

Detecting malicious traffic can be achieved by analyzing its behavior, such as deviations in packet flow, unusual connection frequencies, or irregular user activity patterns, a principle employed by behavioral Intrusion Detection Systems [14]. The authors of [14] designed a multi-level intrusion detection method for identifying abnormal network behaviors using machine learning techniques. Their approach integrates multiple classifiers to detect anomalies at various levels of analysis, starting with broad detection of unusual traffic patterns and proceeding to detailed evaluation of specific threats, such as Distributed Denial of Service (DDoS) attacks or port scans. The method demonstrated improved accuracy in identifying zero-day attacks while significantly reducing false positives, showcasing the effectiveness of hierarchical analysis in intrusion detection systems.

[1] https://www.snort.org

[2] https://aide.github.io

Building on this solution, the authors of [12] developed a specialized IoT crawler integrated into the fog layer (network layer), designed to prioritize critical nodes for inspection based on their significance within the network. The IoT crawler utilizes a behavioral analyzer with a machine learning core to differentiate between malicious and legitimate nodes based on data streams collected from IoT devices. The proponents of this idea evaluated this system using machine learning algorithms like Random Forest, AdaBoost, and Extra Tree, achieving a remarkable 98.3% accuracy with the Extra Tree classifier. This result highlights the system's ability to process IoT-specific data streams efficiently, adapting dynamically to threats without overwhelming resource-constrained IoT nodes. This work demonstrates the potential of integrating multi-level machine learning frameworks within IoT ecosystems to enhance real-time intrusion detection. By leveraging fog computing for reduced latency and prioritizing critical nodes, the IoT crawler exemplifies the practical application of advanced machine learning in securing modern, heterogeneous networks.

Mukkamala [6] described approaches to intrusion detection and audit data reduction using support vector machines and Neural Networks, highlighting their effectiveness in analyzing high-dimensional datasets. The primary goal was to create classifiers capable of distinguishing normal network traffic from various types of attacks. The researchers compared the performance of SVM with a radial kernel to Neural Networks with two intermediate layers. The results demonstrated that SVM with a radial kernel outperformed Neural Networks in terms of hit ratio and processing time for both model training and prediction tasks. This research underscores the potential of SVM in efficiently processing and classifying network traffic, making it a robust solution for real-time intrusion detection in environments characterized by large-scale, complex datasets.

Similarly, Kim [7] introduced a hybrid intrusion detection model that integrates decision trees (DT) with one-class SVM to combine the strengths of anomaly detection and misuse detection. This approach addresses the limitations of standalone methods by leveraging the high accuracy of misuse detection for known attack patterns and the adaptability of anomaly detection to identify previously unknown threats. The researchers proposed a two-stage framework. In the first stage, DT, as a supervised learning algorithm, are employed to quickly and effectively classify known attack patterns. This ensures reliable identification of previously encountered threats. In the second stage, a one-class SVM is used to analyze the residual data (traffic not classified in the first stage) for potential anomalies. This step enhances the system's ability to detect zero-day attacks and other novel intrusions. The study evaluated the hybrid method using benchmark datasets, demonstrating that the integration of these techniques improves both detection accuracy and processing efficiency. Specifically, the model achieved a significant reduction in false positives while maintaining high detection rates, particularly for mixed traffic scenarios.

The article [16] categorizes various IDS based on deep learning techniques. The authors explore how models like autoencoders and Long Short-Term Memory (LSTM) networks can detect anomalies in network traffic more effectively than traditional signature-based systems. Autoencoders, as unsupervised learning models, excel at detecting anomalies in network traffic by reconstructing input data and identifying deviations that signify potential threats. LSTM networks, on the other hand, are particularly effective in modeling sequential data, such as network logs or traffic flows, enabling the detection of complex temporal patterns associated with sophisticated attacks. The study showcases that deep learning enables real-time analysis and reduces false positives significantly, addressing a key limitation of conventional IDS.

2.2. Deep Learning for Enhanced Security

Deep learning models, particularly Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), offer superior performance in threat detection by analyzing more complex features. For example, RNNs, with their ability to capture temporal dependencies, are effective in detecting attacks like Distributed Denial of Service, where the timing of events is crucial. Furthermore, DL-based systems can operate autonomously, learning from new attack patterns without requiring frequent human intervention.

Kou in [4] proposed a network security situational element recognition method combining a deep-stacked encoder with the backpropagation (BP) neural network algorithm. The method leverages unsupervised learning algorithms to train each layer of the network individually, allowing for a hierarchical representation of the data. By stacking the encoders, the method creates a deep-stacked network capable of extracting high-dimensional features from raw network data. In the initial stage, unsupervised training

is conducted using the stacked encoders to learn meaningful features from unlabeled data. These encoders utilize reconstruction-based loss functions to ensure that the most relevant information is retained during feature extraction. Once the unsupervised training phase is complete, the BP algorithm is applied to fine-tune the network using labeled data, optimizing it for classification tasks. The authors conducted simulation studies to evaluate the effectiveness of this method in enhancing situational awareness in network security. The results indicated that the deep-stacked encoder significantly outperformed traditional models in terms of precision and recall when recognizing situational elements such as potential threats, vulnerabilities, and network states. Moreover, the method demonstrated resilience against noisy and incomplete data, which are common in real-world network environments.

In addition, Fu in [5] proposed to use an adaptive genetic algorithm to effectively optimize the traditional APT attack prediction model, thereby improving prediction accuracy. This model's ability to accurately predict risk nodes that may be present in the network system as well as to track the progress of APT attacks in real time and determine the attack path through sequence attacks greatly enhances the network system's security [1].

In 2018, Radford [17] presented an anomaly detection model using a LSTM network to analyze network traffic logs for cybersecurity applications. The model was designed to leverage the temporal sequence learning capabilities of LSTM networks, enabling it to identify anomalies in network behavior that might indicate potential security threats.

In [18] authors introduced RawPower, a DL architecture designed to analyze raw bytestream data for network anomaly detection. This approach eliminates the need for extensive feature engineering by directly processing raw traffic measurements. The experimental results demonstrate that RawPower achieves exceptional performance, surpassing traditional anomaly detection systems in terms of detection accuracy, robustness, and scalability. Specifically, it excels in scenarios involving high-speed networks, where traditional methods struggle to keep up with the sheer volume and diversity of data.

The studies [19, 20] investigate the application of deep learning techniques for identifying various types of malicious network activities, such as malware communication. By utilizing CNNs to analyze packet-level features, the method achieves superior performance in detecting previously unseen threats. The authors compare the results with conventional techniques and highlight significant improvements in precision and recall metrics.

The authors of [15] provides a thorough review of how deep learning techniques are applied to various domains of network security, highlighting their significant advantages over traditional, rule-based systems. The authors analyze several deep learning architectures, including CNNs and RNNs, demonstrating their ability to automatically extract and learn meaningful patterns from raw network data without the need for extensive manual feature engineering. The survey emphasizes the limitations of rule-based systems, which rely on predefined rules or signatures, making them ineffective against zero-day attacks and adaptive threats. In contrast, deep learning models are dynamic and capable of generalizing to unseen attack scenarios. By analyzing both known and novel attack patterns, these methods significantly enhance detection rates and reduce false positives, which are common drawbacks of conventional systems.

The article [21] highlights the transformative role of deep learning in securing 5G networks. The authors discuss how the high complexity and dynamic nature of 5G architectures, including virtualization, software-defined networking (SDN), and network slicing, demand advanced security mechanisms capable of real-time threat detection and mitigation. The study concludes that integrating deep learning into 5G security frameworks significantly enhances the adaptability, precision, and scalability of network defenses, making them more resilient to evolving threats. However, it also underscores the need for addressing challenges such as computational overhead and the interpretability of deep learning models to ensure their effective deployment in real-world 5G applications.

3. Traffic Optimization with AI

Efficient traffic management is critical in maintaining network performance, particularly as the number of connected devices and the amount of data traffic continue to grow. AI's ability to predict traffic patterns and optimize routing decisions in real-time has significantly improved the efficiency of networks. AI-based systems analyze historical and real-time data to dynamically adjust traffic routes and manage bandwidth, thereby reducing congestion and packet loss.

3.1. Predictive Traffic Routing

AI can predict network traffic fluctuations by analyzing historical data and recognizing patterns that suggest future behavior. By leveraging ML models, networks can proactively re-route data to avoid congestion before it occurs, improving Quality of Service (QoS) for end-users. QoS refers to the ability of a network to provide predictable performance levels, typically measured by parameters such as bandwidth, latency and packet loss. It ensures that network resources are allocated efficiently to maintain the reliability and quality of specific applications or services, such as video streaming or VoIP. Predictive routing is particularly beneficial in large-scale networks, such as data centers or cloud infrastructures, where traffic load balancing is essential for maintaining optimal performance.

The study presented in [30] focus on predicting the network traffic by using the different prediction regression models such as K-Nearest Neighbors, Random Forest, Gradient Boosting and DT with different sub-parameters. Using real-world network traffic data, the authors train and test the models to predict key traffic parameters, such as bandwidth demand and packet flow rates. The results demonstrate that Gradient Boosting outperforms the other algorithms in terms of accuracy and error metrics, such as Mean Absolute Error (MAE) and Root Mean Square Error (RMSE).

One notable study [8] presents a framework for traffic flow classification based on deep learning models. The authors train deep neural networks (DNNs) on real-world network traffic data to predict characteristics such as flow throughput and duration. Their approach moves beyond binary classifications like "mice" (small) and "elephant" (large) flows [23], opting instead for a multi-class quantization strategy. This methodology classifies flows into a range of categories based on their characteristics (flow throughput, duration, or packet interarrival times), rather than relying on rigid binary distinctions. The proposed system is intended to enhance network traffic management by predicting flow behaviors, ultimately improving routing decisions in real time.

The authors of [9, 31] explored the application of AI in predicting network traffic patterns to enhance routing efficiency in smart networks. It reviews various AI methodologies, including machine learning techniques, and discusses their roles in optimizing resource allocation and reducing latency. Techniques such as RNNs and LSTM networks are discussed for their ability to analyze temporal traffic data and accurately forecast future traffic demands. These predictions enable dynamic adjustments to routing protocols, reducing congestion and enhancing QoS across diverse network environments, including 5G, IoT, and edge computing. Despite the advancements, the article identifies several challenges associated with AI integration in network traffic management, such as scalability in large-scale networks, maintaining prediction accuracy in highly dynamic environments, and computational overhead. The authors suggest that future research should focus on lightweight AI models, federated learning to address data privacy concerns, and explainable AI (XAI) to improve the interpretability and trustworthiness of predictive systems.

3.2. Reinforcement Learning for Dynamic Traffic Management

Reinforcement learning, a type of machine learning where agents learn by interacting with their environment, has been applied to dynamic traffic management. RL agents learn optimal routing strategies through trial and error, adjusting decisions based on rewards, such as reduced latency or higher throughput. This approach allows networks to adapt in real-time, adjusting to changing conditions without the need for human intervention.

The article [10] explores the application of reinforcement learning for adaptive routing in networks subject to dynamic changes. The authors present an RL framework that dynamically learns optimal routing policies by interacting with the network environment, thereby facilitating efficient traffic management and minimizing delays, even under unpredictable traffic fluctuations and varying network topologies. The study highlights the potential of RL to enhance routing performance in scenarios where traditional algorithms may struggle due to variability in network conditions.

Abrol in [22] presents a framework leveraging deep reinforcement learning (DRL) to optimize network traffic management dynamically. The authors propose a model that integrates a deep graph convolutional neural network with a reinforcement learning agent to predict and adapt to real-time traffic demands. This approach is particularly suited for next-generation networks, which face challenges such as high data volumes, dynamic topologies, and diverse service requirements. By modeling the network as a graph, the DRL agent learns optimal routing policies by interacting with the network environment and receiving feedback through reward signals. These signals are designed to reflect key performance

metrics, such as throughput, latency, and packet loss. Over time, the model identifies patterns in traffic behavior and dynamically adjusts routing decisions to prevent congestion and maximize resource utilization. The approach minimizes packet delays and reduces congestion, leading to improved QoS for users and applications.

Q-Learning [24] (QL) uses unsupervised RL to determine optimal behaviour to maximise performance when interacting with its environment. The method has also found its way into network traffic management and optimization in SDN. The authors of [25] addressed network congestion in SDN by reselecting flow paths and changing flow table using predefined threshold. The researchers in [26] introduced fairness function in SDN for load-balancing in peak traffic conditions. Harewood-Gill [27] proposed three Q-routing algorithms [28] with distinct performance metrics to enhance traffic management in SDN environments and conducted a comparative analysis of their effectiveness against the K-Shortest Path algorithm. A more detailed description of these articles, along with additional examples of QL applications in SDN, is provided by the authors in [29].

4. AI in Network Management

AI has also revolutionized network management by automating routine tasks such as configuration management, fault detection, and network monitoring. AI-driven network management systems can identify and resolve issues autonomously, reducing human workload and minimizing downtime.

In traditional networks, configuration management is a labor-intensive process prone to human error. AI tools automate the configuration process, ensuring consistency and reducing the risk of misconfigurations. By analyzing network requirements, AI systems can automatically apply optimal settings and adjust them as network demands evolve.

Moreover, AI systems excel at detecting anomalies in network performance, which can be indicators of hardware failure, security breaches, or performance degradation. By using ML models, these systems can predict failures before they occur and take preventive action, such as rerouting traffic or initiating backup systems. Some AI-driven networks even exhibit self-healing capabilities, where the system automatically corrects issues without human intervention. Examples of the use of AI solutions in network management are described in [8, 9, 11, 32, 39].

The article [33] discusses the integration of machine learning techniques into cognitive network management systems to enhance decision-making processes and automate network operations. The authors emphasize the segmentation of network management into distinct areas - Fault, Configuration, Accounting, Performance, and Security (FCAPS) - and the assignment of specific ML algorithms to address challenges in each domain. Furthermore, they underscore that developing an integrated network management system is a highly complex yet indispensable task, particularly in light of the rapid expansion of computer networks in recent years.

Li in [34] explores the transformative role of AI and ML in enhancing the management of data center networks. It provides a detailed analysis of how ML techniques are being employed to address the growing complexity of modern data centers by enabling adaptive, automated, and efficient network management solutions. A notable contribution of the survey is the introduction of a quality assessment criterion called REBEL-3S, designed to impartially evaluate the strengths and weaknesses of the proposed research approaches.

Kadiyala in [38] examines the groundbreaking potential of AI in network automation, emphasizing its ability to predict and prevent network issues, optimize resources, and enable self-healing capabilities. It presents real-world case studies demonstrating AI's effectiveness in enhancing network reliability and reducing downtime.

An existing technological solution utilizing AI for network infrastructure management is Cisco AI Network Analytics[3]. This application is designed to enhance network management by leveraging AI and ML to provide proactive insights and automated solutions [35]. The platform collects and analyzes vast amounts of telemetry data from network devices, enabling it to identify anomalies, predict potential performance issues, and optimize network configurations in real time. A key advantage of Cisco AI Network Analytics is its ability to automate routine tasks, such as identifying misconfigurations or reallocating bandwidth, reducing the need for manual intervention and minimizing operational costs.

[3] https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/2-3-7/b_cisco_dna_assurance_2_3_7_ug/b_cisco_dna_assurance_2_3_6_ug_chapter_010.pdf

Similarly, Juniper Networks' AI-driven network management solution, Marvis, employs ML to proactively predict network issues and deliver actionable insights [36]. By analyzing data from various sources - including network devices, applications, and user behavior - Marvis identifies patterns and anomalies with high accuracy. In a customer deployment, Marvis successfully predicted 90% of network issues, reducing the mean time to resolution (MTTR) by 70% and increasing network uptime by 25% [37], showcasing its impact on operational efficiency and reliability.

5. Challenges and Future Directions

Despite the numerous advantages of integrating AI into computer networks, there are several challenges that must be addressed. One key issue is the difficulty of integrating AI into existing legacy network infrastructure, which often lacks the computational power or flexibility required for AI systems. Additionally, the deployment of AI in critical networks raises ethical concerns, including questions of accountability, transparency, and bias in decision-making processes.

5.1. Ethical and Accountability Concerns

As AI systems become more autonomous, determining accountability in the event of network failures or security breaches becomes increasingly complex. The opaque nature of some AI algorithms, particularly deep learning models or decision trees, makes it difficult to understand how decisions are made. This is why many AI systems operate as "black boxes", making it difficult for users and stakeholders to understand how decisions are made. This lack of transparency raises accountability issues, particularly in scenarios where AI decisions impact user safety or privacy. Establishing clear accountability frameworks is essential; organizations must define who is responsible for AI-driven decisions, whether it be the developers, the companies that deploy these systems, or designated administrators. This clarity can help foster trust and facilitate ethical governance of AI technologies.

The findings reported in [40] highlight practical issues of developing and operating ML-based solutions in real networks. The authors discuss concerns related to data quality and availability, emphasizing that the effectiveness of AI systems heavily relies on large, high-quality datasets, which are often difficult to obtain or maintain due to privacy regulations and dynamic network environments. It is worth mentioning that gathering sufficient data from diverse network environments is often hindered by logistical limitations, such as incompatible data formats, the high cost of data acquisition, and varying network configurations. One more significant challenge lies in data labelling. Supervised learning algorithms, which are commonly used in network management tasks like traffic classification and anomaly detection, require labeled datasets for training. Labeling network data is both time-consuming and resource-intensive, often requiring expert knowledge to correctly identify patterns or categorize flows. This bottleneck can slow down the development cycle of AI-driven solutions and limit the scope of their applicability.

Another major issue is algorithmic bias, which can emerge from the data sets used to train AI systems. If these data sets reflect historical biases or imbalances, the resulting AI algorithms may reinforce or exacerbate these biases in decision-making processes. For example, an AI system employed for network traffic management might unintentionally prioritize data flows from certain applications or user groups, leading to unequal access to bandwidth and resources. Addressing this concern requires ongoing scrutiny of training data and the implementation of measures that ensure fairness and inclusivity in AI applications, promoting equitable service distribution across all users.

Furthermore, the ethical implications of data privacy in computer networks cannot be overlooked. AI systems often require vast amounts of network traffic data to function effectively, raising concerns about how this data is collected, stored, and used. Users may be unaware of the extent to which their online activities are being monitored and analyzed, leading to potential violations of privacy rights. Organizations must prioritize ethical data management practices, ensuring that users are informed about data usage and that consent is obtained for data collection. Establishing regulatory frameworks that protect user privacy while allowing for innovation in AI technologies will be a crucial step forward in fostering trust and accountability within network systems.

5.2. The Future of AI-Driven Networks

The future of AI-driven networks is set to revolutionize the way we manage and interact with digital infrastructures. One of the most promising advancements lies in the development of self-optimizing networks. These networks will leverage AI algorithms to analyze real-time data, enabling them to dynamically adjust their performance based on current conditions. This capability could significantly enhance efficiency, as networks become adept at reallocating resources and bandwidth in response to changing demands. As a result, users can expect faster, more reliable connections, improving overall user experiences across various applications.

Moreover, AI-driven networks are likely to play a pivotal role in enhancing security measures. The integration of AI in cybersecurity can enable proactive threat detection and response, as systems learn to identify and mitigate potential vulnerabilities before they can be exploited. By analyzing patterns in network traffic, AI can differentiate between legitimate user behavior and suspicious activities, significantly reducing the risk of cyberattacks. However, this increased reliance on AI also necessitates the development of robust safeguards to ensure that these systems themselves do not become targets for manipulation or exploitation.

When discussing the future of computer networks, it is impossible to overlook the transformative role of generative AI. This technology is set to revolutionize network optimization, security, and automation through its innovative applications. One such use case is synthetic data generation, where models like Generative Adversarial Networks (GANs) [41] and diffusion models create realistic network traffic patterns. These synthetic datasets address the challenges of limited or biased real-world data, enhancing the robustness and adaptability of AI systems in managing network operations.

In the area of network security, generative AI has proven its utility in simulating complex cyberattacks, such as DDoS or phishing scenarios [42]. By proactively testing security systems against these simulated threats, networks can better anticipate and counter emerging vulnerabilities. However, this dual-use potential also introduces risks, as attackers might exploit generative AI to craft more sophisticated and hard-to-detect malicious traffic, necessitating effective protections and ethical guidelines.

6. Conclusion

The impact of artificial intelligence on computer networks is profound and multifaceted, offering both significant benefits and challenges. AI technologies have the potential to revolutionize network management, enhancing efficiency, reliability, and security. Through the use of advanced algorithms, networks can achieve greater self-optimization and self-healing capabilities, leading to improved performance and reduced downtime. This transformation is particularly crucial in an era where demand for bandwidth and responsiveness continues to grow, necessitating innovative solutions to manage complex network environments. Table 1 provides a summary of artificial intelligence applications and their transformative impact on key areas of computer networks.

Table 1. AI Applications and Their Impact on Key Network Areas

Computer Network Area	Traditional Challenges	AI Approaches	Impact of AI
Traffic Management	Network congestion, inefficient routing	Predictive analytics, reinforcement learning	Improved routing, reduced latency, dynamic traffic optimization
Network Security	Threat detection delays, zero-day attack detection, advanced persistent threats	Anomaly detection, generative AI, ML classifiers, neural networks	Faster threat detection, adaptive defense mechanisms, reduced false positives, effective prediction of APT and zero-day attacks
Resource Allocation	Static resource distribution, underutilization	AI-based optimization models, deep learning	Efficient bandwidth management, adaptive resource distribution
Fault Detection	Manual monitoring, delayed detection of hardware or software failures, delayed troubleshooting	Predictive maintenance, neural networks	Early failure detection, minimized downtime, automated troubleshooting
Quality of Service	Packet loss, inconsistent service quality	AI-driven traffic prioritization, reinforcement learning	Enhanced user experience, optimized service delivery

Network Design and Planning	Complex manual configurations, Complexity in multi-cloud or MANET scenarios	Generative models (e.g., GANs), optimization techniques	Automated network topology design, scalability, reduced human error

However, the integration of AI into computer networks is not without its drawbacks. Ethical considerations, particularly around data privacy and algorithmic bias, pose serious challenges that must be addressed to foster trust among users and stakeholders. As AI systems become increasingly autonomous in their decision-making processes, ensuring accountability becomes critical. Organizations must implement transparent practices and ethical guidelines that govern AI usage, ensuring that user data is handled responsibly and equitably. A groundbreaking step toward the responsible and ethical development of this technology is the EU Artificial Intelligence Act[4], which represents the world's first comprehensive legal regulation for artificial intelligence systems and models.

Looking ahead, the future of AI-driven networks necessitates a collaborative approach that integrates the insights of technologists, ethicists, and policymakers. This interdisciplinary cooperation is crucial for establishing standards that promote technological advancement while safeguarding users' rights and classified information. By balancing innovation with ethical considerations, the full potential of artificial intelligence can be harnessed for applications in computer networks, ensuring that these technologies enhance their integrity, accessibility, and security.

Literature

[1] Wang M., Song G., Zhang Y.: The Current Research Status of AI-Based Network Security Situational Awareness. Electronics (2023), 12, 2309. https://doi.org/10.3390/electronics12102309.

[2] Amrollahi M., Hadayeghparast S., Karimipour H., Derakhshan F., Srivastava G.: Enhancing Network Security Via Machine Learning: Opportunities and Challenges, (2020), In: Choo, KK., Dehghantanha, A. (eds) Handbook of Big Data Privacy. Springer, Cham. https://doi.org/10.1007/978-3-030-38557-6_8.

[3] De Lucia, M.J., Srinivasan, A.: Artificial Intelligence and Machine Learning for Network Security: Quo Vadis?, (2024), In: Chen, Y., Wu, J., Yu, P., Wang, X. (eds) Network Security Empowered by Artificial Intelligence. Advances in Information Security, vol 107. Springer, Cham. https://doi.org/10.1007/978-3-031-53510-9_3.

[4] Kou G., Wang S., Zhang D.: Recognition of network security situation elements based on depth stack encoder and back propagation algorithm. J. Electron. Inf. Technol. 2019, 41, 2187–2193.

[5] Fu T., Lu Y., Zhen W.: APT attack situation assessment model based on optimized BP neural network. In Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (IT-NEC), IEEE, Chengdu, China, 15–17 March 2017; pp. 2108–2111.

[6] Mukkamala S., Janoski G., Sung A.: Intrusion detection using neural networks and support vector machines. Proceedings of the 2002 International Joint Conference on Neural Networks. IJCNN'02 (Cat. No.02CH37290), Honolulu, HI, USA, 2002, pp. 1702-1707.

[7] Kim G., Lee S., Kim S.: A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection With Misuse Detection. Expert Systems with Applications, vol. 41, no. 4, pp. 1690–1700, 2014.

[8] Hardegen C., Pfülb B., Rieger S., Gepperth A.: Predicting Network Flow Characteristics Using Deep Learning and Real-World Network Traffic. IEEE Transactions on Network and Service Management, vol. 17, no. 4, pp. 2662-2676, (2020).

[9] Chen A., Law J., Aibin M.: A Survey on Traffic Prediction Techniques Using Artificial Intelligence for Communication Networks. Telecom 2021.

[10] Khodayari S., Yazdanpanah M.: Network routing based on reinforcement learning in dynamically changing networks. 17th IEEE International Conference on Tools with Artificial Intelligence (ICTAI'05), 2005.

[11] Sivalingam K.: Applications of Artificial Intelligence, Machine Learning and related techniques for Computer Networking Systems. (2021).

[12] Albdour L., Manaseer S., Sharieh A.: IoT Crawler with Behavior Analyzer at Fog layer for Detecting Malicious Nodes. International Journal of Communication Networks and Information Security, vol. 12, pp. 83-94. https://doi.org/10.17762/ijcnis.v12i1.4459, (2020).

[13] Deng X., Liu Q., Deng Y., Mahadevan S.: An improved method to construct basic probability assignment based on the confusion matrix for classification problem. Information Sciences, vol. 340–341, pp. 250–261, May 2016.

[4] https://artificialintelligenceact.eu/

[14] Ji S.-Y., Jeong B.-K., Choi S., Jeong D.: A multilevel intrusion detection method for abnormal network behaviors. J. Netw. Comput. Appl., vol. 62, pp. 9–17, February 2016. https://doi.org/10.1016/j.jnca.2015.12.004.
[15] Berman D. S., Buczak A. L., Chavis J. S., Corbett C. L.: A Survey of Deep Learning Methods for Cyber Security. Information (2019), vol. 10(4), 122. https://doi.org/10.3390/info10040122.
[16] Lansky J. et al.: Deep Learning-Based Intrusion Detection Systems: A Systematic Review. IEEE Access, vol. 9, pp. 101574-101599, 2021, doi: 10.1109/ACCESS.2021.3097247.
[17] Radford B., Apolonio L., Trias A., Simpson J.: Network Traffic Anomaly Detection Using Recurrent Neural Networks. (2018), 10.48550/arXiv.1803.10769.
[18] Marín G., Casas P., Capdehourat G.: RawPower: Deep Learning based Anomaly Detection from Raw Network Traffic Measurements. In Proceedings of the ACM SIGCOMM 2018 Conference on Posters and Demos (SIGCOMM '18). Association for Computing Machinery, New York, NY, USA, pp. 75–77. https://doi.org/10.1145/3234200.3234238.
[19] Marín G., Casas P., Capdehourat G.: Deep in the Dark - Deep Learning-Based Malware Traffic Detection Without Expert Knowledge. IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 2019, pp. 36-42, doi: 10.1109/SPW.2019.00019.
[20] Marín G., Casas P., Capdehourat G.: DeepMAL - Deep Learning Models for Malware Traffic Detection and Classification. (2021), doi: 10.1007/978-3-658-32182-6_16.
[21] Haider N., Baig M. Z., Imran M.: Artificial Intelligence and Machine Learning in 5G Network Security: Opportunities, advantages, and future research trends. (2020), doi: 10.48550/arXiv.2007.04490.
[22] Abrol A., Mohan P. M., Truong-Huu T.: A Deep Reinforcement Learning Approach for Adaptive Traffic Routing in Next-gen Networks. (2024), https://doi.org/10.48550/arXiv.2402.04515.
[23] Mori T., Uchida M., Kawahara R., Pan J., Goto S.: Identifying elephant flows through periodically sampled packets. Proc. 4th ACM SIGCOMM Conf. Internet Meas., 2004, pp. 115–120.
[24] Watkins C.: Learning From Delayed Rewards. Ph.D. dissertation, King's College, Cambridge, UK, (1989).
[25] Kim S., Son J., Talukder A., Hong C. S.: Congestion prevention mechanism based on Q-leaning for efficient routing in SDN. 2016 International Conference on Information Networking (ICOIN), Kota Kinabalu, Malaysia, pp. 124-128, doi: 10.1109/ICOIN.2016.7427100.
[26] Tennakoon D., Karunarathna S., Udugama B.: Q-learning Approach for Load-balancing in Software Defined Networks. 2018 Moratuwa Engineering Research Conference (MERCon), Moratuwa, Sri Lanka, pp. 1-6, doi: 10.1109/MERCon.2018.8421895.
[27] Harewood-Gill D., Martin T., Nejabati R.: The Performance of Q-Learning within SDN Controlled Static and Dynamic Mesh Networks. (2020), pp. 185-189, doi: 10.1109/NetSoft48620.2020.9165530.
[28] Boyan J., Littman M.: Packet Routing in Dynamically Changing Networks: A Reinforcement Learning Approach. Advances in Neural Information Processing Systems, vol. 6, (1999).
[29] Dake D., Gadze D., Klogo G., Nunoo-Mensah H.: Traffic Engineering in Software-defined Networks using Reinforcement Learning: A Review. International Journal of Advanced Computer Science and Applications, vol. 12, (2021), doi: 10.14569/IJACSA.2021.0120541.
[30] P S., Kamboj A., Shete V., R H.: Machine Learning Based Network Traffic Predictive Analysis. Review of Computer Engineering Research, vol. 9(2), pp. 96–108, (2022). https://doi.org/10.18488/76.v9i2.3065.
[31] Vashishth T., Sharma V., Kumar B., Chaudhary S., Panwar R., Sharma S.: ARTIFICIAL INTELLIGENCE-ENABLED NETWORK TRAFFIC OPTIMIZATION: A COMPREHENSIVE SURVEY. Journal of Industrial Engineering, vol. 52, pp. 26-34, (2023).
[32] Sivalingam K.: Applications of Artificial Intelligence, Machine Learning and related techniques for Computer Networking Systems. (2021), https://arxiv.org/abs/2105.15103.
[33] Ayoubi S., Limam N., Salahuddin M., Shahriar N., Boutaba R., Estrada-Solano F., Caicedo M.: Machine Learning for Cognitive Network Management. IEEE Communications Magazine, vol. 56, (2018), doi: 10.1109/MCOM.2018.1700560.
[34] Li B., Wang T., Yang P., Chen M., Yu S., Hamdi M.: Machine Learning Empowered Intelligent Data Center Networking: A Survey. (2022), https://doi.org/10.48550/arXiv.2202.13549.
[35] Cisco: Cisco DNA Center: Intent-Based Networking for the Enterprise. Solution Overview, 2020.
[36] Juniper Networks: Marvis: AI-Driven Virtual Network Assistant. Datasheet, 2021.
[37] Juniper Networks: Global Retailer Achieves Network Efficiency and Uptime with Juniper Marvis. Case Study, 2021.
[38] Kadiyala C., Chilukoori S., Gangarapu S.: AI-Powered Network Automation: The Next Frontier in Network Management. Journal of Advanced Research Engineering and Technology, vol. 3, pp. 223-233, (2024).

[39] Ge J., Li T., Wu Y.: AI and Machine Learning for Network and Security Management. Wiley-IEEE Press, (2022).
[40] Liu Q., Zhang T., Hemmatpour M., Qiu H., Zhang D., Chen C. S., Mellia M., Aghasaryan A.: Operationalizing AI in Future Networks: A Bird's Eye View from the System Perspective. (2024), https://doi.org/10.48550/arXiv.2303.04073.
[41] Nukavarapu S. K., Ayyat M., Nadeem T.: MirageNet - Towards a GAN-based Framework for Synthetic Network Traffic Generation. GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 3089-3095, doi: 10.1109/GLOBECOM48099.2022.10001494.
[42] Sai S., Yashvardhan U., Chamola V., Sikdar B.: Generative AI for Cyber Security: Analyzing the Potential of ChatGPT, DALL-E and Other Models for Enhancing the Security Space. IEEE Access, (2024), vol. 12, pp. 53497-53516, doi: 10.1109/ACCESS.2024.3385107.