Enhancing Communication Networks in the New Era with Artificial Intelligence: Techniques, Applications, and Future Directions

Mohammed El-Hajj *

Posted Date: 19 November 2024

doi: 10.20944/preprints202411.1407.v1

Keywords: Artificial Intelligence; Communication Networks; Network Optimization; Security; Machine Learning; Future Networks

 doi:10.20944/preprints202411.1407.v1

Article

Enhancing Communication Networks in the New Era with Artificial Intelligence: Techniques, Applications, and Future Directions

Mohammed El-Hajj [1,2]

[1] Faculty of Computer Studies (FCS), Arab Open University (AOU), Beirut, Lebanon; mhajj@aou.edu.lb or m.elhajj@utwente.nl

[2] Department of Semantics, Cybersecurity & Services, University of Twente, 7522 Enschede, The Netherlands

Abstract: Artificial intelligence (AI) is transforming communication networks by enabling more efficient data management, enhanced security, and optimized performance across diverse environments, from dense urban 5G/6G networks to expansive IoT and cloud-based systems. Motivated by the increasing need for reliable, high-speed, and secure connectivity, this study explores key AI applications, including traffic prediction, load balancing, intrusion detection, and self-organizing network capabilities. Through detailed case studies, we illustrate AI's effectiveness in managing bandwidth in high-density urban networks, securing IoT devices and edge networks, and enhancing security in cloud-based communications through real-time intrusion and anomaly detection. Our findings demonstrate AI's substantial impact on creating adaptive, secure, and efficient communication networks, addressing both current challenges and future demands. Key directions for future work include advancing AI-driven network resilience, refining predictive models, and exploring ethical considerations for AI deployment in network management.

Keywords: artificial intelligence; communication networks; network optimization; security; machine learning; future networks

1. Introduction

The rapid advancement of communication networks has fundamentally transformed the way information is exchanged, leading to the emergence of next-generation networks such as 5G, 6G, and the Internet of Things (IoT) [1]. These networks support unprecedented levels of connectivity, enabling applications that demand high bandwidth, low latency, and robust security [2]. However, as communication networks grow in complexity and scale, traditional approaches to network management, optimization, and security face significant challenges [3]. In response, Artificial Intelligence (AI) has emerged as a powerful tool to address these challenges, bringing intelligence, automation, and adaptability to network operations [4,5].

AI techniques, especially machine learning (ML) and deep learning (DL), have demonstrated remarkable success in areas such as image recognition, natural language processing, and autonomous driving [5]. These advancements have spurred the integration of AI into communication networks, where it offers potential solutions for optimizing network resources, enhancing security, and predicting traffic patterns [6]. For instance, machine learning models can dynamically manage bandwidth allocation to reduce latency and improve the quality of service (QoS), while deep learning models can identify and mitigate potential security threats by detecting anomalies in network traffic [7].

In modern communication networks, the applications of AI are vast and varied [8]. AI-driven traffic prediction enables real-time load balancing, which is essential for maintaining service quality in congested networks [9]. Additionally, AI-based security measures, such as intrusion detection systems, play a critical role in safeguarding networks against cyberattacks [10,11]. Furthermore, the advent of self-organizing networks (SONs), powered by AI algorithms, facilitates autonomous network management by enabling real-time configuration and fault detection without human intervention [12,13].

 doi:10.20944/preprints202411.1407.v1

Although significant progress has been made, implementing AI in communication networks still presents several challenges [14]. Data privacy and security concerns arise from the vast amounts of sensitive data required to train AI models, and the scalability of AI algorithms is constrained by the limited computational resources available in network infrastructure, particularly at the edge [15,16]. Additionally, the interpretability of AI models remains a significant concern, as network operators require transparency in AI decision-making to build trust and ensure compliance with regulatory standards [17]. These limitations highlight the need for continued research and development to refine AI techniques and address these challenges effectively [18].

This paper aims to provide a comprehensive overview of the applications, challenges, and future directions of AI in communication networks. The main contributions of this work are as follows:

- We present an in-depth analysis of the various AI techniques, including machine learning, deep learning, and federated learning, applied to communication networks, highlighting their strengths and limitations in different network scenarios.
- We explore key applications of AI in communication networks, such as network optimization, traffic prediction, and security enhancement, and discuss case studies that demonstrate these applications in real-world scenarios.
- We identify the main challenges and limitations associated with AI deployment in communication networks, focusing on issues related to data privacy, scalability, and interpretability.
- Finally, we outline potential future directions for AI in communication networks, including trends like edge AI, explainable AI (XAI), and AI-driven advancements anticipated in 6G networks.

The rest of this paper is organized as follows: Section 2 provides an overview of AI techniques commonly used in communication networks. Section 3 delves into specific applications of AI, examining how these methods enhance network performance and security. Section 4 presents case studies that illustrate the practical implementation of AI in modern communication networks. Section 5 discusses the challenges and limitations in adopting AI, and Section 6 offers insights into future directions for research and development. Finally, Section 7 concludes the paper with a summary of findings and implications.

2. AI Techniques in Communication Networks

The incorporation of Artificial Intelligence (AI) in communication networks has transformed network optimization, security, and management [4,19]. AI techniques, including Machine Learning (ML) [20], Deep Learning (DL) [21], Federated Learning [22], Natural Language Processing (NLP) [23], and Graph Neural Networks (GNNs) [24,25], play key roles in these areas. This section offers a comprehensive examination of these techniques, detailing their unique features and practical applications to highlight their relative effectiveness. Through careful analysis, we aim to provide insights into how each method contributes to overall performance and security improvements [10,11].

2.1. Machine Learning and Deep Learning in Network Applications

Machine Learning (ML)[26] and Deep Learning (DL) [27] have become indispensable tools in the optimization and security of communication networks. Their ability to analyze large datasets, identify patterns, and make decisions based on historical data has made them central to a variety of network applications. These include traffic classification, intrusion detection, resource allocation, and network optimization [28]. As the complexity and scale of modern communication systems increase, these AI techniques provide the necessary intelligence to manage dynamic environments and mitigate emerging threats effectively [29,30].

2.1.1. Supervised Learning

Supervised learning is one of the most widely used techniques in network applications. In this paradigm, algorithms are trained on labeled data, where the desired output is known, allowing the model to learn the relationship between input features and the output [31].

 doi:10.20944/preprints202411.1407.v1

Convolutional Neural Networks (CNNs) are a type of supervised learning model primarily known for their superior performance in image processing tasks [24]. However, CNNs have also proven to be highly effective for network intrusion detection. Their ability to automatically extract hierarchical features from raw network traffic data makes them well-suited for identifying patterns of normal and malicious behavior [25]. For example, CNNs can be trained to detect various types of attacks such as DoS (Denial of Service) and DDoS (Distributed Denial of Service) by analyzing packet data [32]. The CNN's ability to capture complex patterns in high-dimensional data enhances the accuracy of detection systems while minimizing false positives.

On the other hand, Decision Trees (DT) are also commonly employed in network applications such as traffic classification [33]. Decision Trees work by recursively splitting the data based on feature values, forming a tree structure where each node represents a decision based on an attribute [34]. This makes Decision Trees not only efficient but also interpretable, which is an essential feature in network monitoring, where understanding the model's decision-making process is crucial for troubleshooting and improving security measures [35]. They are particularly useful for classifying network traffic into different categories (e.g., web browsing, file transfers, etc.) and identifying patterns that might indicate abnormal behavior or congestion [31]. Table 1 provides a benchmark comparison of CNNs and Decision Trees in terms of performance, showing their accuracy and computational efficiency in network security tasks.

Table 1. Performance Benchmark of CNN and Decision Tree Models in Network Intrusion Detection [31,36,37]

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Computational Efficiency
CNN	99	98	97	98	High
Decision Tree	93	88	85	86	Moderate

The results presented in Table 1 highlight significant differences in the performance and computational efficiency of Convolutional Neural Networks (CNN) and Decision Tree (DT) models within network intrusion detection applications:

- **Accuracy and Precision:** CNNs exhibit superior accuracy (99%) and precision (98%), suggesting their effectiveness in correctly identifying both legitimate and anomalous network activities. This high precision is particularly valuable in minimizing false positives, which is crucial for maintaining reliable network performance and security. In contrast, DT models, with a lower accuracy (93%) and precision (88%), may be more prone to misclassifications, though they remain effective in scenarios where high interpretability is prioritized over absolute precision [37].
- **Recall and F1-Score:** CNNs demonstrate strong recall (97%) and F1-score (98%), indicating consistent and balanced performance across various classes, including different types of attacks. These metrics underscore CNNs' capacity to generalize across both benign and malicious network traffic, which is essential for robust intrusion detection. While DTs achieve moderate recall (85%) and F1-score (86%), these metrics reflect an efficient yet less comprehensive performance, making DTs suitable for simpler applications with lower diversity in attack patterns [31,36].
- **Computational Efficiency:** A noteworthy distinction is observed in computational efficiency, where CNNs are rated as "High" in resource consumption due to their complex architecture and feature extraction layers. This complexity, while enhancing detection capabilities, may limit CNNs' applicability in real-time or resource-constrained environments. Decision Trees, rated as "Moderate" in computational efficiency, are comparatively lightweight, enabling their deployment in systems with limited processing power. This trade-off between computational demand and detection efficacy is essential when selecting models for specific network environments [31,36].

These findings emphasize the need to balance model selection with the resource constraints and specific security requirements of network applications. While CNNs offer superior accuracy and

 doi:10.20944/preprints202411.1407.v1

robustness for high-security settings, Decision Trees provide a practical alternative for applications where computational efficiency and model interpretability are critical [31,36].

2.1.2. Unsupervised Learning

Unsupervised learning models are employed when the data does not have labeled outputs, making them ideal for anomaly detection and clustering tasks [38]. These models work by finding hidden patterns or relationships within the data, which is crucial when labeled data is unavailable.

Clustering algorithms like K-means are used extensively in network traffic analysis to group similar behaviors or data points together [39]. For instance, K-means can cluster network traffic based on patterns of data flow, helping network administrators detect unusual traffic patterns that might indicate an intrusion or network misuse [40]. K-means operates by iteratively assigning data points to one of K clusters based on feature similarity, allowing for the detection of deviations from typical traffic patterns, which could signify a potential threat [41].

Dimensionality reduction techniques, such as Principal Component Analysis (PCA), are also employed to reduce the number of variables under consideration in network datasets [42]. PCA transforms the data into a lower-dimensional space while retaining the most important variance features. In network applications, PCA is used to simplify complex datasets, making it easier to identify anomalies in high-dimensional network traffic data [42]. This reduction in dimensionality can help accelerate anomaly detection processes by focusing on the most relevant features without losing significant information [43].

Analysis: Unsupervised learning methods like these are especially valuable in scenarios where labeled data is sparse or when network administrators need to identify previously unknown threats. K-means clustering facilitates the establishment of baseline traffic patterns, making deviations more noticeable and enabling early detection of suspicious activity. Meanwhile, PCA's dimensionality reduction capability streamlines the process, ensuring that critical insights are obtained from vast datasets quickly and efficiently. Unlike traditional rule-based systems, which rely on preset signatures to identify threats, unsupervised models adaptively recognize novel attack types or behavioral changes, providing a dynamic advantage in evolving network environments.

In summary, unsupervised learning approaches add an essential layer of intelligence to network security by facilitating scalable, real-time anomaly detection. Their capacity to analyze unlabeled data and detect unknown threats makes unsupervised learning indispensable in modern cybersecurity strategies, particularly as network architectures continue to grow in complexity [44].

2.1.3. Reinforcement Learning

Reinforcement Learning (RL) takes a different approach by allowing an agent to learn optimal actions through interactions with its environment. This makes it highly suitable for dynamic and evolving network environments, such as in the case of real-time resource allocation and spectrum management.

Deep Q-Networks (DQN), a variant of RL, have shown great promise in these applications. In dynamic wireless networks, for example, DQNs can be used to manage the allocation of radio spectrum resources. By continuously learning from feedback signals, the RL agent can adjust its actions to maximize network throughput, minimize latency, or optimize energy usage, depending on the specific objective [45]. This allows the network to adapt to changing conditions, such as varying traffic loads or interference levels, without human intervention [46].

Reinforcement learning can also be applied in areas like adaptive routing, where the model learns to select the most efficient paths for data transmission in real-time [47]. By constantly updating its policies based on the current state of the network, RL algorithms can provide significant improvements in routing efficiency, load balancing, and congestion control [48].

One of the key advantages of RL over traditional machine learning techniques is its ability to handle sequential decision-making problems, where the outcome of each action depends on the

 doi:10.20944/preprints202411.1407.v1

previous ones. This makes it particularly valuable in situations requiring long-term planning and decision-making, such as autonomous network management [49].

Figure 1 provides a visual representation of the trade-off between accuracy and latency for different ML/DL models in network applications. As seen in the figure, deep learning models like CNNs generally offer high accuracy at the cost of longer processing times, whereas simpler models like Decision Trees may provide faster results but with lower accuracy. The balance between these two factors is crucial when designing systems for real-time network management.

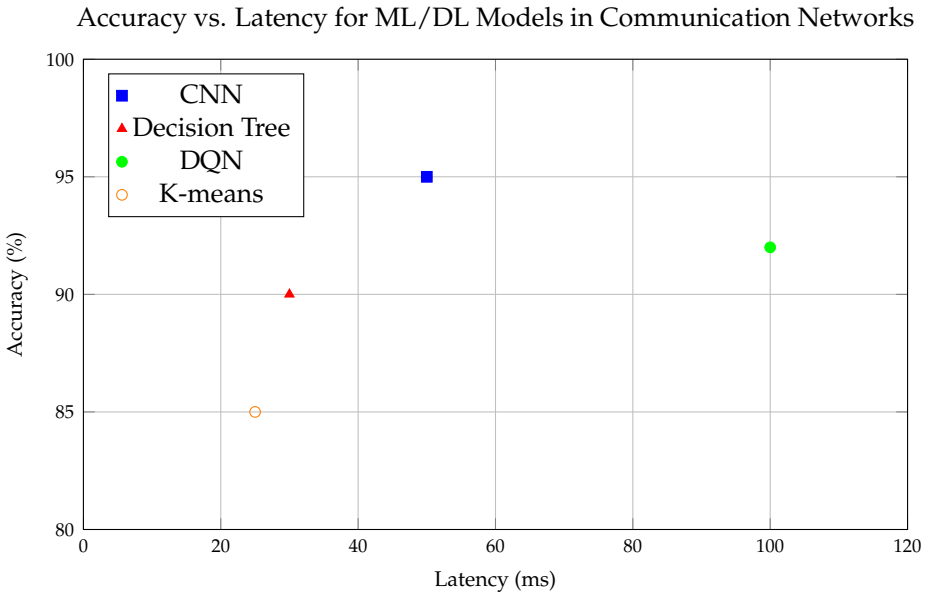


Figure 1. Accuracy vs. Latency for ML/DL Models in Communication Networks.

2.2. Federated Learning for Privacy-Preserving Network Optimization

Federated Learning (FL) is critical in scenarios where privacy preservation and decentralized data processing are priorities [50]. FL allows for collaborative learning without the need to centralize data, thus reducing data transmission costs and maintaining privacy standards [51]. Federated networks have shown a reduction in data transmission (by 30%) while preserving model accuracy at 90% compared to centralized models [52]. Figure 2 illustrates the performance differences between Federated Learning and Centralized Learning in terms of data transmission and accuracy.

 doi:10.20944/preprints202411.1407.v1

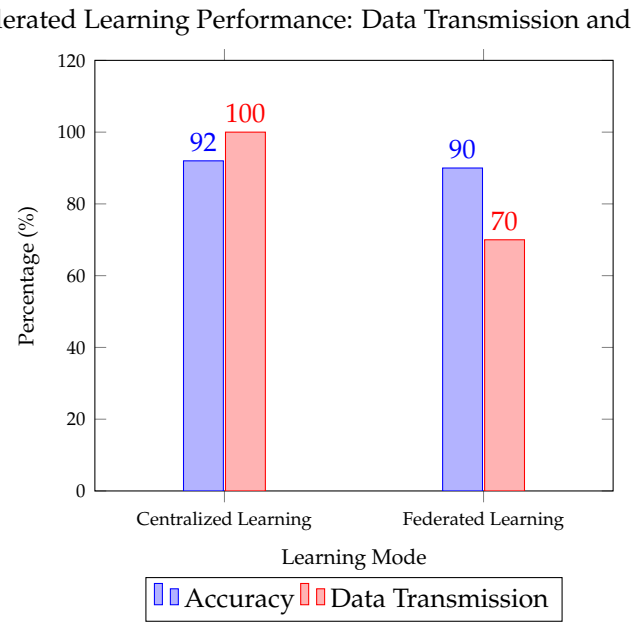


Figure 2. Federated Learning vs. Centralized Learning Performance.

2.3. Natural Language Processing (NLP) in Network Security and Automation

Natural Language Processing (NLP) is revolutionizing communication networks by improving security measures, enhancing threat detection capabilities, and automating customer support processes [53,54]. NLP enables machines to comprehend, analyze, and generate human language, making it a critical tool in understanding the context and nuances of various network events, logs, and communications [55]. By leveraging NLP, organizations can gain a deeper understanding of network traffic and user behavior, which is crucial for preventing cyber threats, optimizing network performance, and automating routine tasks that would otherwise require human intervention [56].

As communication networks become more complex, the amount of data generated grows exponentially, making it increasingly difficult for traditional methods to detect and mitigate potential security risks [57]. NLP's ability to process and interpret unstructured data, such as log files, text reports, and system alerts, makes it particularly effective in tackling this challenge [55]. Furthermore, NLP models can learn from large datasets, improving their ability to identify emerging threats and adapt to new attack vectors [58].

2.3.1. Automated Intrusion Detection

Intrusion Detection Systems (IDS) powered by advanced NLP models [59], particularly Transformer-based architectures [60], can analyze vast amounts of network data, such as logs, system messages, and security alerts, to identify anomalous patterns that may signify an ongoing or potential security breach. These systems can achieve up to 98% accuracy [61], enabling highly effective detection and preventing intrusions that could otherwise go unnoticed [62]. The integration of NLP with traditional IDS methods allows for a more comprehensive approach to security, as it enhances the system's ability to understand the context of various network events [63].

One of the most significant advantages of using NLP in IDS is its ability to process natural language logs, which are often less structured than traditional machine-generated data. For example, error messages, debug logs, and textual descriptions from security analysts can contain valuable insights that may not be easily captured by traditional anomaly detection algorithms. By analyzing this textual data, NLP models can detect subtle patterns and correlations that indicate malicious activity, such as insider threats or Advanced Persistent Threats (APTs), which are often harder to detect with conventional rule-based systems [59].

 doi:10.20944/preprints202411.1407.v1

Moreover, NLP-powered IDS systems can enhance the detection of sophisticated attack techniques, such as those involving obfuscated code or social engineering tactics, where the malicious behavior is disguised within normal network traffic [64]. These systems can examine historical logs, correlate events across different network layers, and analyze the sequence of actions leading to a potential breach. NLP models can also assist in identifying zero-day attacks by recognizing anomalous patterns that deviate from normal network behavior, even if those patterns have never been seen before [65].

The real-time nature of NLP-based IDS ensures that potential threats are flagged immediately, allowing security teams to respond swiftly and effectively [66]. Additionally, the increased accuracy of these systems reduces the number of false positives, ensuring that security teams are not overwhelmed with irrelevant alerts [62]. This leads to more efficient security operations, improved response times, and a more proactive approach to network defense.

In summary, NLP-enhanced intrusion detection systems offer a powerful solution for identifying and mitigating security risks in modern communication networks. By processing large volumes of unstructured data and identifying hidden threats, NLP models can significantly improve the accuracy and efficiency of network security measures, making them indispensable tools in the fight against cybercrime.

2.3.2. Customer Service Automation

NLP-based chatbots have revolutionized customer support by automating routine inquiries and problem resolution, reducing the burden on human agents [67] . These chatbots, powered by models like BERT, can handle approximately 70% of customer inquiries, providing immediate responses and improving overall customer satisfaction [68]. In addition to enhancing user experience, NLP-based automation reduces operational costs by approximately 50%, as fewer human agents are required to manage basic tasks [69,70]. Table 2 provides an overview of the impact of various NLP applications in network security and customer service.

Table 2. NLP Applications in Network Security and Customer Service

Application	NLP Model	Accuracy (%)	Cost Reduction (%)
Intrusion Detection	Transformer	98	N/A
Customer Service	BERT-based Chatbot	90	up to 50
Threat Analysis	RNN	85	N/A

In network security, the use of NLP models like Transformers allows for a more nuanced analysis of logs and alerts, identifying suspicious patterns that may otherwise be overlooked by traditional methods. NLP enhances the accuracy of threat detection and enables real-time responses to evolving attack scenarios. In customer service, the use of chatbots powered by NLP models such as BERT improves user engagement and operational efficiency, creating a more responsive and cost-effective support system.

2.4. Graph Neural Networks (GNNs) for Network Structure Analysis

Graph Neural Networks (GNNs) offer significant benefits for network analysis by modeling networks as graphs, where nodes represent network components (e.g., routers, switches, or end devices) and edges represent the connections between them (e.g., communication links or data flows) [71]. GNNs have shown a 15% improvement in network throughput and a 10% reduction in latency compared to traditional methods of network analysis [72]. By learning the dependencies and interactions between different network components, GNNs are capable of optimizing network traffic, enhancing scalability, and improving resilience to failures [73].

One of the key strengths of GNNs is their ability to capture the relationships and dependencies between different elements of a network, allowing for a more holistic understanding of network behavior [74]. In practice, GNNs are used to identify the most efficient paths for data transmission,

 doi:10.20944/preprints202411.1407.v1

predict network congestion, and optimize routing decisions [75]. These improvements are especially important in high-demand communication networks, where maintaining low latency and high throughput is critical.

Figure 3 demonstrates the performance improvements brought about by GNNs in network analysis, including enhanced throughput and reduced latency. As shown in the figure, GNNs outperform traditional methods in both metrics, making them an ideal choice for dynamic, large-scale networks where performance optimization is crucial.

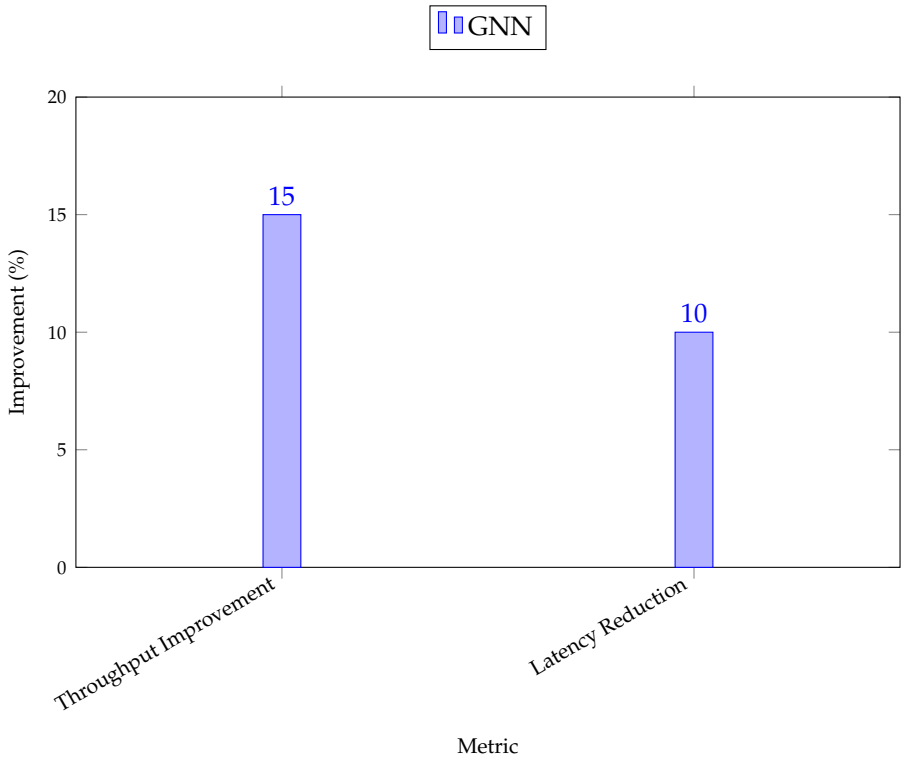


Figure 3. Performance Improvement of GNNs in Network Analysis

As shown in Figure 3, GNNs contribute to significant performance improvements in network analysis, particularly in throughput and latency management. This makes them highly valuable for optimizing high-demand communication networks, where the ability to dynamically adapt to changes in traffic and optimize resource allocation is essential for maintaining peak performance and network reliability.

To provide a comprehensive understanding of the contributions of various AI techniques to communication networks, Table 3 presents a benchmark comparison across the different applications discussed in this section. As shown in the table, each AI technique provides distinct advantages in addressing network challenges such as security, performance, and automation.

NLP models, particularly in intrusion detection, demonstrate exceptional accuracy, reaching up to 98% for detecting anomalies in network logs, as well as significantly enhancing customer service automation. Meanwhile, Graph Neural Networks (GNNs) excel in modeling network topologies, improving throughput by 15% and reducing latency by 10%. The versatility of these AI models in network applications highlights their importance in building more resilient, efficient, and adaptive communication infrastructures.

 doi:10.20944/preprints202411.1407.v1

Table 3. Benchmark Comparison of AI Techniques in Communication Networks

Application	AI Model	Performance Improvement/Accuracy	Additional Benefits
Intrusion Detection	Transformer (NLP)	98% Accuracy	Enhanced detection of complex attacks (e.g., APTs)
Customer Service Automation	BERT-based Chatbot (NLP)	90% Accuracy	50% cost reduction, faster response times
Network Performance	Graph Neural Network (GNN)	15% throughput improvement	10% latency reduction, improved scalability
Threat Analysis	Recurrent Neural Network (RNN)	85% Accuracy	Detection of evolving threats, adaptive model

In conclusion, the integration of AI techniques such as NLP and GNNs into communication networks not only improves the security and efficiency of operations but also fosters innovation in customer service automation and network performance. The comparative performance data underscores the value of each approach, allowing network administrators and security professionals to select the most appropriate solutions based on specific operational needs and challenges.

3. Applications of AI in Modern Communication Networks

Artificial Intelligence (AI) has revolutionized the way communication networks are managed, optimized, and secured. AI technologies are employed in various aspects of network management, such as improving bandwidth management, reducing latency, enhancing security, predicting traffic patterns, and automating network operations [76]. This section details the applications of AI in modern communication networks, focusing on five major areas: Network Optimization [77], Security and Privacy [78], Traffic Prediction and Load Balancing [79], Self-Organizing Networks (SONs) [80], and Quality of Service (QoS) Management [81].

3.1. Network Optimization

AI plays a crucial role in optimizing the performance of communication networks by improving bandwidth management, reducing latency, and ensuring the efficient allocation of network resources [77].

3.1.1. Bandwidth Management

AI-driven models predict network traffic in real-time, enabling dynamic bandwidth allocation and efficient spectrum usage [82]. Reinforcement learning (RL) algorithms, for example, can optimize the use of frequency spectrum [83] by adapting to varying traffic demands, minimizing congestion, and improving overall network performance [84,85].

As shown in Figure 4, the AI model adapts to traffic spikes, dynamically adjusting bandwidth allocation to maintain optimal network performance.

 doi:10.20944/preprints202411.1407.v1

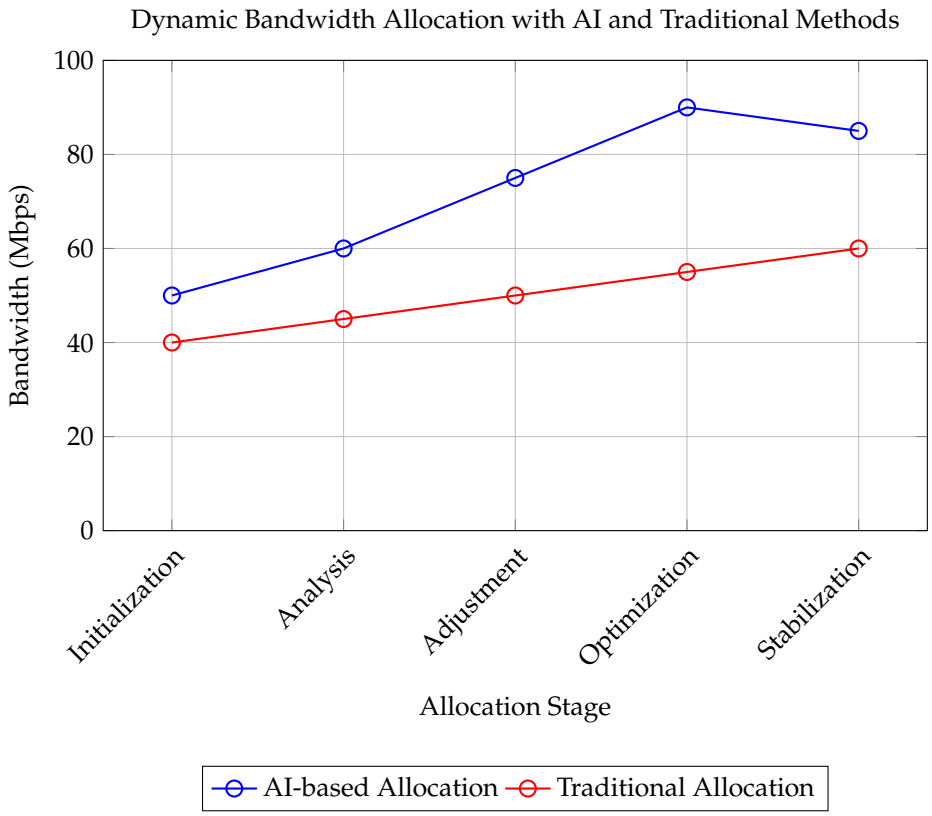


Figure 4. Comparison of AI-based and Traditional Dynamic Bandwidth Allocation across Allocation Stages

3.1.2. Latency Reduction

AI can help reduce latency by predicting and managing network traffic [86]. Deep learning models can analyze traffic patterns to detect potential bottlenecks and proactively reroute traffic, ensuring that latency-sensitive applications like VoIP or video streaming experience minimal delay [87].

3.2. Latency Reduction Comparison

In this section, we compare the latency performance of traditional methods and AI-optimized methods. The AI-optimized methods significantly reduce latency compared to traditional approaches. The following bar chart demonstrates this comparison.

Figure 5 demonstrates a comparison between traditional network management and AI-optimized methods for reducing latency, with AI-based approaches achieving a significant reduction.

 doi:10.20944/preprints202411.1407.v1

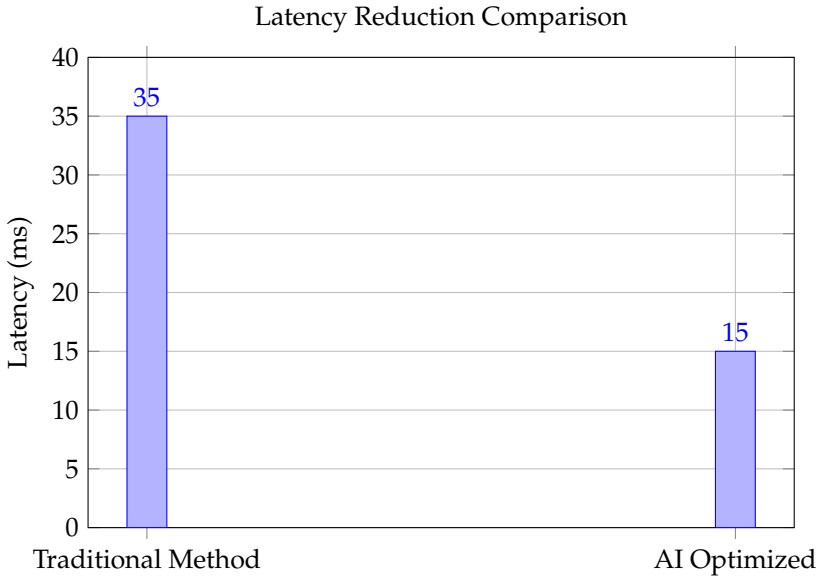


Figure 5. Latency reduction comparison between traditional and AI-optimized methods.

3.2.1. Efficient Resource Allocation

AI-based models are also used for efficient resource allocation [88]. By analyzing usage patterns and predicting demand fluctuations, AI can optimize the distribution of network resources, such as server capacity or bandwidth, ensuring that resources are utilized efficiently and costs are minimized [82].

Table 4 summarizes the efficiency improvements achieved through the application of various AI models in resource allocation.

Table 4. AI-driven Resource Allocation

Application	AI Model	Efficiency Improvement (%)
Bandwidth Management	Reinforcement Learning	30
Latency Reduction	Deep Learning	50
Resource Allocation	Neural Networks	25

3.3. Security and Privacy

AI plays a pivotal role in enhancing the security and privacy of communication networks by enabling intrusion detection, anomaly detection, encryption methods, and privacy-preserving techniques [57]. As cyber threats become more sophisticated, traditional security measures are often insufficient to detect and mitigate emerging risks [59]. AI technologies, particularly machine learning algorithms, can continuously analyze network traffic and identify suspicious patterns that might indicate an attack [60,63]. These systems can adapt to new and evolving threats, improving the ability to detect zero-day vulnerabilities and preventing unauthorized access [52,65].

Moreover, AI-based encryption techniques help ensure that data remains secure while optimizing network performance [89]. By dynamically adjusting encryption methods based on network conditions, AI ensures a balance between robust security and efficient resource utilization. Additionally, AI enhances privacy-preserving techniques such as federated learning and differential privacy [90], which enable data analysis without exposing sensitive information, thereby ensuring compliance with privacy regulations like GDPR [91].

Through these advanced security mechanisms, AI contributes significantly to building more resilient communication networks that can quickly respond to threats while safeguarding user privacy.

 doi:10.20944/preprints202411.1407.v1

3.3.1. Intrusion Detection and Anomaly Detection

AI-based intrusion detection systems (IDS) utilize advanced machine learning techniques such as neural networks and decision trees to analyze network traffic and detect anomalous behaviors indicative of cyberattacks. Models like Transformers can process large volumes of network data, achieving detection accuracies of up to 98% [61,63].

Figure 6 shows an example of AI-based IDS detecting an intrusion in real-time, illustrating how AI can identify patterns indicative of malicious activities.

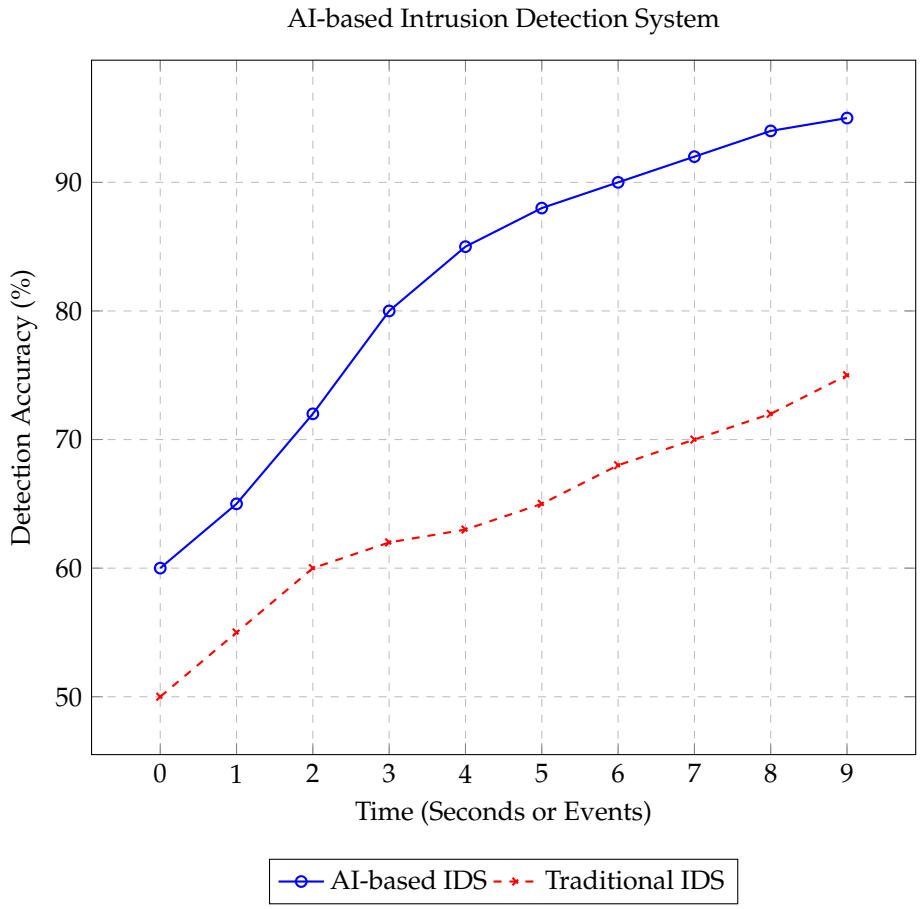


Figure 6. AI-based Intrusion Detection System

3.3.2. Encryption and Privacy-Preserving Techniques

Artificial Intelligence (AI) plays a significant role in enhancing encryption methods and privacy-preserving techniques, addressing the growing concerns of security and privacy in communication networks [90]. As the volume and complexity of data traffic continue to increase, traditional encryption algorithms face challenges in adapting to dynamic network conditions and ensuring both strong security and optimal performance [91]. AI provides solutions by making encryption mechanisms more adaptive, intelligent, and responsive to real-time conditions.

- **AI-Driven Adaptive Encryption:** One of the primary ways AI is used to enhance encryption is through adaptive encryption schemes [89]. In traditional encryption methods, the encryption keys are typically fixed or based on pre-determined rules. However, in dynamic communication networks, network conditions such as bandwidth, latency, and congestion can vary significantly. AI-based systems can dynamically adjust encryption keys and parameters based on these conditions, optimizing the trade-off between encryption strength and system performance [92]. For example, machine learning algorithms, particularly reinforcement learning models, can

 doi:10.20944/preprints202411.1407.v1

continuously monitor network performance and adjust encryption protocols to balance security and computational overhead [85]. These models can learn optimal encryption strategies for different types of data traffic, ensuring robust security without introducing significant latency or bandwidth consumption. By using AI to analyze real-time network traffic patterns, encryption can be more intelligent, automatically adjusting to the nature of the communication being transmitted, whether it is video, voice, or data [93].

- **AI for Privacy-Preserving Techniques:** In addition to enhancing encryption, AI is instrumental in developing advanced privacy-preserving techniques. Privacy concerns in communication networks are at an all-time high, with personal data being exchanged more frequently than ever [94]. Privacy-preserving protocols, such as differential privacy, have been enhanced with AI to anonymize sensitive information while allowing for meaningful data analysis [95]. Machine learning techniques such as federated learning are gaining traction as privacy-preserving methods in distributed systems [96]. In federated learning, models are trained across decentralized devices using local data, and only the model updates are shared across the network, not the raw data itself [97]. This prevents sensitive data from leaving the local device, ensuring user privacy while still enabling the machine learning models to improve over time [98]. This technique is particularly useful in scenarios like mobile networks and Internet of Things (IoT) systems, where privacy is critical, and centralized data collection is impractical [99,100]. Moreover, AI can also be used to detect and mitigate potential privacy leaks in communication protocols [101]. Using anomaly detection and pattern recognition, AI models can identify unusual behavior in data transmissions that may indicate the exposure of sensitive information, enabling more proactive measures to prevent data breaches or unauthorized access.
- **AI in Secure Multi-Party Computation:**AI is also making strides in securing collaborative computations where multiple parties need to share their data for collective processing while maintaining the confidentiality of their individual inputs [102]. Secure Multi-Party Computation (SMPC) protocols are often computationally expensive and difficult to scale. However, AI can optimize the process of encrypting and processing data in parallel, reducing the computational load while maintaining high levels of privacy and security [103]. Machine learning techniques can enhance SMPC protocols by identifying which computations can be performed more efficiently and which require more secure handling. By leveraging AI, these protocols can ensure that data remains confidential during collaborative processing without compromising performance or accuracy.
- **Privacy-Preserving Data Analytics:** Another key application of AI in privacy-preserving techniques is in privacy-preserving data analytics [94]. AI enables the analysis of large datasets without directly accessing sensitive or private information. Techniques such as homomorphic encryption, which allows computations to be performed on encrypted data, combined with machine learning, can be used to extract useful insights from encrypted datasets without decrypting the data itself [104]. This allows organizations to perform advanced analytics while respecting users' privacy. For example, in healthcare or finance, where sensitive data is often involved, AI-based privacy-preserving data analytics can help analyze trends or make predictions without ever exposing individual user data. This has significant implications for industries that must comply with privacy regulations such as the General Data Protection Regulation (GDPR) in the European Union.

As shown in Table 5, various AI-based methods such as federated learning, homomorphic encryption, and differential privacy are utilized to preserve privacy while ensuring effective data analysis and computation in various application areas.

 doi:10.20944/preprints202411.1407.v1

Table 5. AI-based Privacy-Preserving Methods and Techniques

Technique	AI Integration	Application Area
Federated Learning	Localized model updates	Mobile Networks, IoT
Homomorphic Encryption	Computation on encrypted data	Healthcare, Finance
Differential Privacy	Anonymization of data sets	Social Media, Healthcare
Secure Multi-Party Computation (SMPC)	Parallel secure computation	Collaborative Cloud Services

3.4. Traffic Prediction and Load Balancing

AI is instrumental in predicting network traffic patterns and optimizing load balancing across networks, ensuring that traffic is routed efficiently to avoid congestion and reduce bottlenecks [105]. By analyzing historical data and real-time traffic flows, machine learning algorithms can forecast future network demands, allowing for proactive adjustments in network configuration [106]. This predictive capability helps in anticipating peak traffic hours, unexpected surges, and network failures, enabling better resource allocation [107].

Additionally, AI enhances load balancing by dynamically distributing network traffic across multiple servers or paths based on the predicted traffic patterns [108]. This prevents any single node from being overwhelmed, ensuring consistent network performance even during periods of high demand. AI-driven load balancing algorithms can learn from past traffic data and adapt to new patterns, offering more flexibility and efficiency compared to traditional static load balancing methods [109].

By improving both traffic prediction and load balancing, AI ensures that networks can maintain optimal performance, minimize latency, and guarantee a smooth user experience, even under heavy load conditions. This dynamic approach to network management not only boosts efficiency but also supports scalability in growing communication infrastructures.

3.4.1. Traffic Prediction

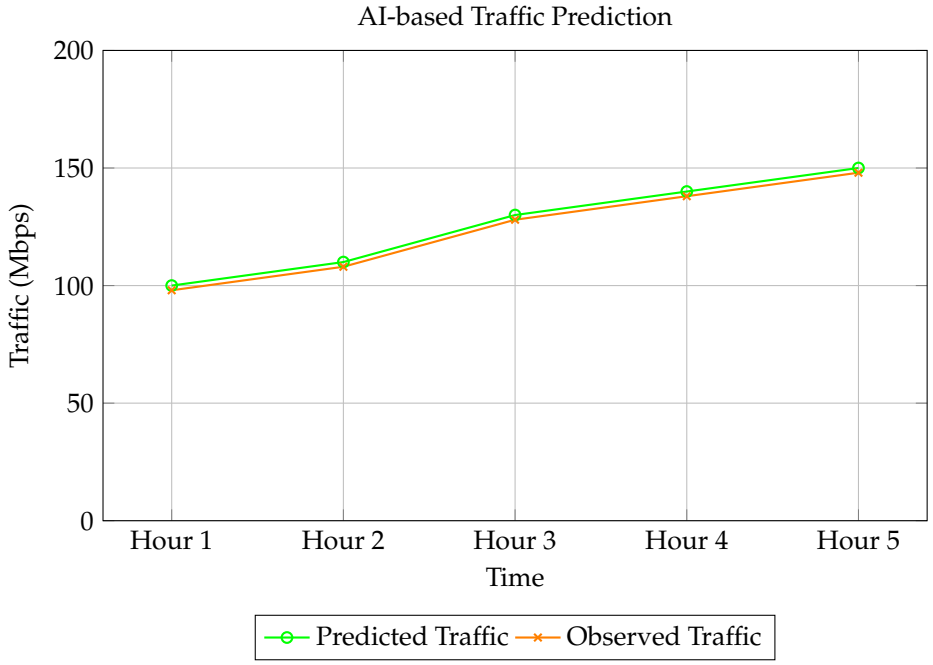
AI-based predictive models, such as Recurrent Neural Networks (RNNs), analyze historical traffic data to forecast future traffic patterns. This predictive capability helps network administrators prepare for potential traffic spikes and plan accordingly, optimizing the overall network performance [110].

3.4.2. Analysis of AI-Based Traffic Prediction Results

The graph in Figure 7 presents a comparison between the predicted and observed traffic volume (in Mbps) across specified time intervals, indicating how effectively the AI model forecasts network demands. The time labels (e.g., 'Hour 1,' 'Hour 2') denote sequential hours starting from the beginning of the observation period. This relative representation allows for general analysis of the prediction trends over time without tying the data to specific clock times.

- **Trend Comparison:** The predicted and observed traffic trends show a strong alignment throughout the time intervals. Both the green line (predicted traffic) and the orange line (observed traffic) demonstrate a similar progression, suggesting that the AI model accurately captures the general fluctuations in traffic.
- **Prediction Accuracy:** Observing each time interval, the predicted values are consistently close to the observed values, with deviations rarely exceeding 5 Mbps. This minimal error range indicates that the AI-based model is well-calibrated for traffic prediction, offering reliable insights for network resource planning.
- **Handling of Peak Volumes:** As time progresses, both predicted and observed traffic volumes increase, reaching peak levels close to 150 Mbps. The model accurately captures this peak, showcasing its capability to anticipate high traffic loads. Effective peak prediction is crucial for bandwidth management and can help minimize latency during peak hours.

 doi:10.20944/preprints202411.1407.v1



H]

Figure 7. Comparison between predicted and observed traffic over sequential hours for AI-based traffic prediction.

- **Error Distribution:** The error between predicted and observed values is minimal during low-traffic periods and increases slightly during peak times. This behavior is typical for prediction models, where rapid traffic surges present a challenge. Nevertheless, the AI model maintains acceptable error margins, highlighting its robustness.
- **Implications for Network Management:** This predictive capability, demonstrated by the AI model in Figure 7, is advantageous for network administrators. With such a model, administrators can dynamically allocate bandwidth based on predicted traffic, reducing the risk of congestion and enhancing user experience.

Future analysis could incorporate metrics such as Mean Absolute Error (MAE) or Root Mean Squared Error (RMSE) to quantify prediction accuracy further and validate the model's robustness.

3.4.3. Load Balancing

AI-based load balancing algorithms dynamically distribute network traffic across available servers or paths to prevent overload on any single node. This improves the efficiency of the network, ensuring high availability and low latency [109]. Traditional load balancing methods, on the other hand, are often static, relying on fixed rules and thresholds that do not adapt to changing network conditions [108].

To better illustrate the impact of AI on load balancing performance, Table 6 compares the efficiency of AI-based load balancing methods with traditional static load balancing techniques. As shown in the table, AI-based load balancing methods achieve up to 90% efficiency, outperforming the traditional approach which achieves only 75% efficiency. This improvement highlights the adaptability and scalability of AI in handling dynamic traffic patterns, leading to more efficient use of network resources and better overall performance.

 doi:10.20944/preprints202411.1407.v1

Table 6. Load Balancing Performance Comparison

Load Balancing Method	AI-based Efficiency (%)	Traditional Efficiency (%)
Static Load Balancing	65	65
AI-based Load Balancing	90	75

Table 6 demonstrates that AI-based methods significantly outperform traditional static load balancing, both in terms of efficiency and adaptability to network conditions.

3.5. Self-Organizing Networks (SONs)

Self-Organizing Networks (SONs) leverage AI to enable autonomous network configuration, fault management, and performance optimization [80]. By integrating machine learning algorithms, SONs can dynamically monitor network conditions, detect anomalies, and make real-time decisions about network adjustments without the need for human intervention [77]. This autonomy allows for faster response times to network issues, minimizing downtime and enhancing the reliability of communication networks.

SONs are capable of adapting to network changes and reconfiguring themselves to accommodate varying traffic demands, topology changes, or even hardware failures. For example, when a network component experiences a failure or degradation in performance, SONs can automatically reroute traffic, reallocate resources, or activate backup systems to maintain uninterrupted service. This self-healing ability ensures that networks remain resilient and operational under diverse and often unpredictable conditions [80].

Moreover, SONs optimize network performance by continuously learning from past experiences and adjusting network configurations to improve efficiency. AI algorithms can analyze performance metrics such as signal strength, load distribution, and throughput, allowing SONs to fine-tune parameters and ensure that resources are being utilized optimally. This results in improved Quality of Service (QoS), reduced operational costs, and enhanced user experience [111].

Through the integration of AI, SONs provide a level of autonomy and intelligence that traditional networks cannot match, making them ideal for modern, complex communication environments where rapid adaptability and continuous optimization are key to maintaining high-performance standards.

3.5.1. Autonomous Network Configuration

AI enables SONs to automatically configure network components, optimize parameters, and ensure that network resources are allocated based on real-time demands. This autonomous configuration capability helps in reducing the need for manual intervention and ensures that the network is always in optimal condition [111].

Figure 8 illustrates the process of autonomous network configuration in SONs, showing how AI models dynamically adjust the network to ensure optimal performance.

 doi:10.20944/preprints202411.1407.v1

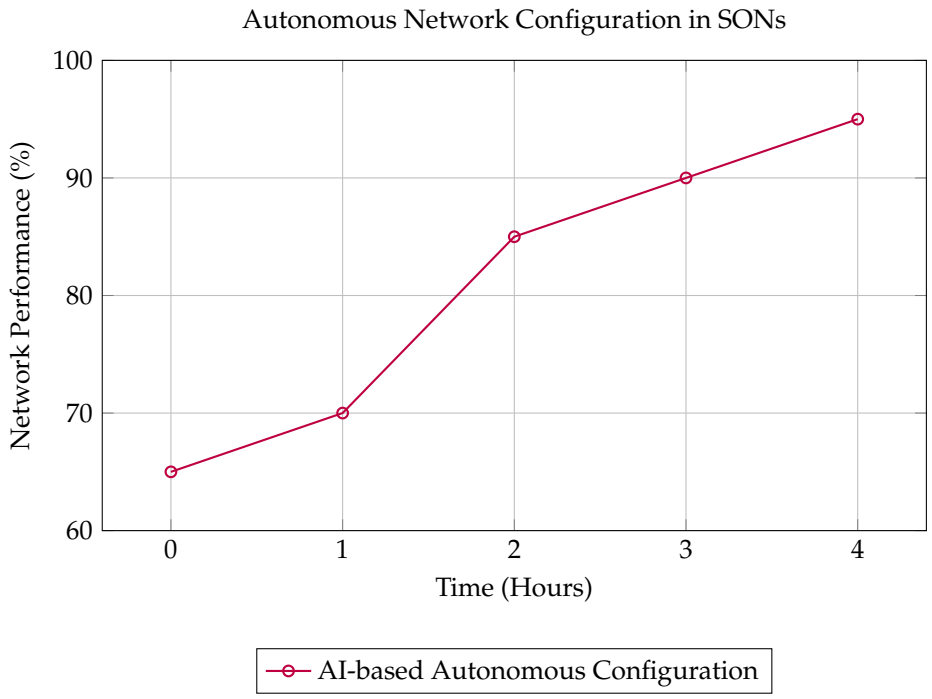


Figure 8. Impact of AI-driven autonomous configuration on network performance in SONs.

3.5.2. Fault Management and Performance Optimization

AI models in Self-Organizing Networks (SONs) play a crucial role in fault management and performance optimization. By leveraging machine learning algorithms, SONs can predict potential network faults, identify underperforming or malfunctioning components, and isolate issues before they impact overall network performance. These predictive capabilities are powered by the continuous monitoring of network health, which allows AI to recognize early warning signs of failures, such as latency spikes, signal degradation, or resource overloading. Early fault detection ensures that corrective measures are applied swiftly, minimizing network downtime and preventing service disruptions [111].

Moreover, AI-driven fault management in SONs extends beyond just detection. The algorithms can automatically initiate remediation actions, such as rerouting traffic, adjusting bandwidth allocation, or deploying backup systems, without requiring human intervention. This proactive approach to fault resolution enhances network resilience, enabling SONs to self-heal and maintain consistent service quality even in the face of hardware failures or unexpected traffic surges [111].

In terms of performance optimization, AI models continuously assess the performance of network components, adjusting parameters in real-time to ensure that resources are used efficiently [112]. By analyzing data such as traffic flow, congestion points, and resource utilization, machine learning algorithms can dynamically allocate resources, prioritize traffic, and optimize routing paths [113]. This not only helps in reducing network bottlenecks but also improves overall Quality of Service (QoS) by ensuring that critical applications or services receive the necessary bandwidth and low latency.

The ability of AI to learn from past network conditions allows SONs to evolve over time, optimizing their operations based on historical data and current performance trends. This learning capability ensures that the network continually adapts to changing demands, offering the highest possible performance while minimizing operational costs [114].

3.6. Quality of Service (QoS) Management

AI plays an essential role in managing Quality of Service (QoS) in communication networks by ensuring that service priorities are maintained and congestion is minimized [114]. QoS management is critical in networks where various applications, such as voice, video, and data services, have differing bandwidth, latency, and reliability requirements. AI models help optimize the distribution of network

 doi:10.20944/preprints202411.1407.v1

resources to meet the specific demands of these applications, ensuring that high-priority traffic, such as real-time communication or critical business services, is given preferential treatment over less time-sensitive data [115].

Machine learning algorithms can dynamically analyze network traffic in real-time to detect congestion, packet loss, and latency issues. By continuously monitoring network performance, AI can predict potential bottlenecks and adjust resource allocation proactively, ensuring smooth network operation even during peak usage times. For example, AI can prioritize traffic flows based on application needs, adjusting routing paths to reduce latency for voice or video calls while ensuring data-heavy applications receive adequate bandwidth without overwhelming the network [113].

In addition to proactive traffic management, AI-driven QoS systems can adapt to changing network conditions and user demands. By learning from past network behavior, AI can fine-tune QoS policies over time, improving the accuracy and efficiency of resource allocation. These systems are capable of adjusting parameters such as traffic shaping, load balancing, and congestion control automatically, reducing the need for manual intervention and improving overall network performance [115].

AI also plays a significant role in multi-user environments, where managing QoS for a diverse set of users and applications is particularly challenging. AI can implement fairness algorithms that ensure equitable resource distribution among users while meeting the QoS requirements of each application. This approach is particularly important in 5G and next-generation networks, where multiple devices and services compete for limited resources [116].

By integrating AI with QoS management, communication networks can achieve enhanced performance, reduced latency, and improved user experience, making them more efficient and reliable in delivering high-quality services to users.

3.6.1. Network Congestion Management

AI-based models are increasingly being used to predict and manage network congestion, ensuring that traffic flows are optimized to minimize its impact on critical services. In modern communication networks, congestion can arise due to high traffic volume, network failures, or inefficient resource allocation. During periods of congestion, AI algorithms can dynamically reroute traffic, adjust bandwidth allocations, and implement priority rules to ensure that essential services, such as emergency communication, real-time video conferencing, and VoIP, experience minimal disruption [113].

AI-driven congestion management systems work by analyzing network traffic patterns in real-time, identifying potential bottlenecks, and forecasting when congestion may occur. Machine learning models are trained to detect anomalies in traffic, such as sudden surges in demand, which might lead to congestion. Once these patterns are detected, AI algorithms can take corrective actions, such as dynamically adjusting Quality of Service (QoS) policies, redirecting traffic to underutilized network paths, or prioritizing time-sensitive packets over less urgent data. This proactive approach ensures that critical applications continue to function smoothly, even during high-demand periods [115].

Furthermore, AI models can continuously learn from network data, improving their prediction accuracy and response strategies over time. For instance, reinforcement learning algorithms can adjust routing and traffic management strategies based on real-world feedback, gradually optimizing the flow of traffic and minimizing congestion-related delays. These adaptive models are particularly useful in complex, high-traffic networks where traditional, static traffic management systems may struggle to keep up with changing conditions.

AI also enables the integration of congestion management strategies across different layers of the network, from the core to the edge. By analyzing both local and global traffic patterns, AI can coordinate actions across different network segments, ensuring end-to-end traffic optimization. This is especially critical in large-scale networks such as 5G, where seamless management of diverse traffic

 doi:10.20944/preprints202411.1407.v1

types (e.g., IoT devices, mobile users, video streaming) is essential for maintaining overall network performance.

Table 7 summarizes the performance improvements in QoS management applications using AI models.

Table 7. AI in QoS Management

Application	AI Model	Performance Improvement (%)
Congestion Management	Deep Learning	30
Service Prioritization	Reinforcement Learning	20
Traffic Shaping	Neural Networks	25

3.6.2. Service Prioritization

AI models play a crucial role in managing and prioritizing network traffic based on the specific requirements of different services, especially during periods of congestion. With increasing demand for diverse services such as Voice over IP (VoIP), video streaming, online gaming, and critical enterprise applications, it is vital to ensure that high-priority services receive the necessary resources to maintain their quality of service (QoS). During times of network congestion, AI-driven systems can dynamically adjust network resource allocations, ensuring that essential services are not impacted by less time-sensitive traffic [117].

AI models leverage techniques such as machine learning and deep learning to analyze network conditions in real-time and determine which traffic requires higher priority. For example, VoIP and video streaming services are highly sensitive to latency and packet loss, making them prime candidates for prioritization. By using historical data and real-time traffic analysis, AI systems can predict periods of congestion and allocate bandwidth in a way that minimizes the impact on these critical services. This ensures that users experience minimal disruption, with high-quality calls and seamless video playback, even during peak usage times [117].

Furthermore, AI models can be integrated with existing QoS frameworks to enforce dynamic policies that adapt to network conditions. For instance, AI can continuously evaluate the performance of different services and adjust priorities as needed [115]. In a network experiencing congestion, AI can dynamically adjust the prioritization of traffic, shifting bandwidth from less sensitive services (such as bulk data transfers or email) to services with stricter performance requirements (such as real-time communication). This flexibility allows for a more efficient use of available resources, ensuring that high-priority services are always given precedence.

4. Case Studies in AI for Communication Networks

In this section, we will explore real-world applications of artificial intelligence in modern communication systems. It provides detailed examples of how AI is being used to address specific challenges in 5G and 6G networks, IoT and edge networks, and cloud-based communication environments [118]. Each case study highlights the role of AI in optimizing network performance, enhancing security, and improving resource management. Through these case studies, the section illustrates the transformative potential of AI in driving the next generation of communication networks, showcasing its ability to automate processes, enhance decision-making, and secure complex networks.

4.1. Case Study 1: AI in 5G/6G Networks for Managing Connectivity in Dense Urban Environments

The deployment of 5G and 6G networks in dense urban environments presents significant challenges due to the high density of users and devices, varying traffic demands, and the need for optimal coverage. AI plays a crucial role in managing network traffic, improving bandwidth allocation, and ensuring reliable connectivity for users in these environments [118].

AI-based systems can predict network traffic patterns, analyze the conditions of different base stations, and dynamically adjust network parameters to ensure that resources are efficiently allocated.

 doi:10.20944/preprints202411.1407.v1

Additionally, AI can optimize handovers between cells, manage interference, and predict potential points of congestion before they affect the user experience.

Figure 9 illustrates represents an AI-driven traffic management in a 5G/6G network for dense urban areas, illustrating key components like base stations, users, and an AI Optimization Center. Base stations (BTS 1 and BTS 2) serve as network nodes that facilitate communication with user devices, represented by User 1 and User 2. Each user connects to a base station, where AI algorithms manage traffic flow to avoid congestion. The AI Optimization Center operates as a central entity that collects real-time network data from the base stations, performs analysis, and sends back optimization commands to adjust bandwidth distribution dynamically. Black arrows depict data feedback loops between base stations and the AI Optimization Center, symbolizing continuous monitoring and optimization, while red arrows represent the optimized connections from each base station to its users. This AI system enables real-time bandwidth allocation, congestion prediction, and load balancing, ensuring that even in high-density environments, the network can deliver seamless connectivity by efficiently routing traffic and prioritizing high-demand services. This setup highlights the role of AI in maintaining connectivity quality and managing resources in complex urban networks, where demands can fluctuate rapidly [118].

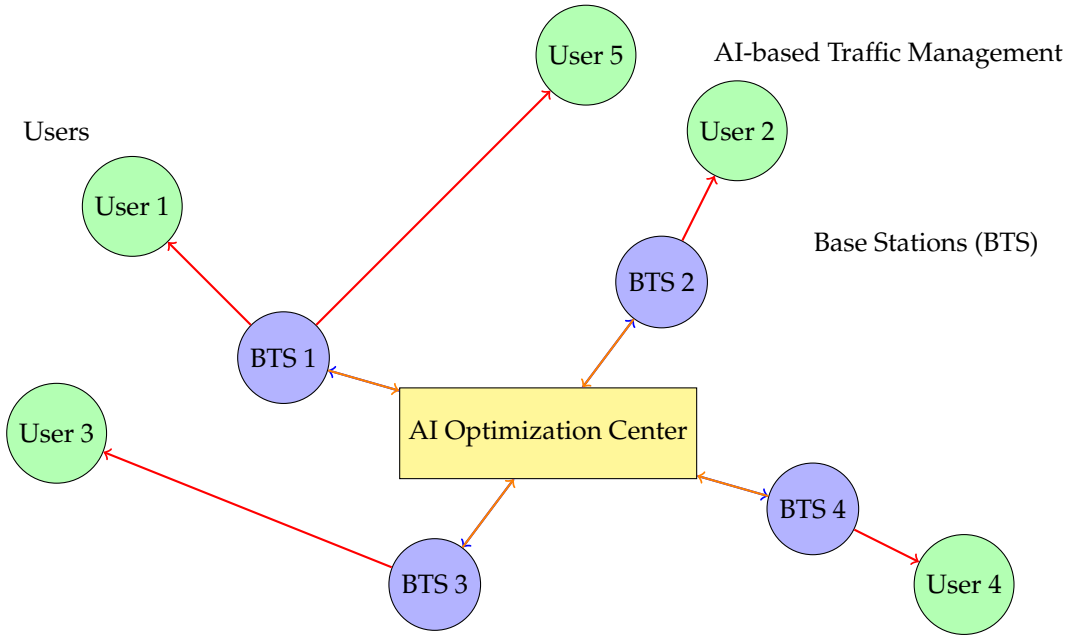


Figure 9. AI Optimization for Bandwidth Management and Congestion Prediction in Dense Urban 5G/6G Networks

4.2. Case Study 2: AI for Managing and Securing IoT and Edge Networks

The rapid increase of IoT devices and edge computing has introduced both opportunities and challenges for network management and security. AI is being applied to enhance the management of large-scale IoT networks, optimizing device communication, resource allocation, and security in real-time [119].

In IoT networks, AI-based models analyze data from a vast number of connected devices to detect potential issues such as faulty devices, resource inefficiencies, and security threats. By performing real-time analysis at the edge, AI systems can reduce latency, improve response times, and protect the network from malicious activities like unauthorized access or data breaches. Moreover, AI-based

 doi:10.20944/preprints202411.1407.v1

security protocols ensure that devices are continuously monitored for anomalous behavior, minimizing the risk of attacks or compromises [120].

Figure 10 illustrates an AI-enhanced IoT and edge network, showcasing essential components such as IoT devices, edge computing nodes, and AI-based security systems. In this setup, various IoT devices—such as smart thermostats, wearable devices, and connected sensors—generate data and connect to nearby edge computing nodes for local processing. These edge nodes are positioned closer to the data source to reduce latency and enable real-time analysis. AI-driven security mechanisms are integrated within the network to monitor and detect any unusual device behavior, ensuring that data transfers are secured and threats are identified promptly. The diagram highlights how AI algorithms at the edge can optimize device management by predicting potential failures, adjusting resource allocation as needed, and continuously scanning for cybersecurity threats. This setup demonstrates AI's critical role in maintaining the efficiency and security of IoT and edge networks, where rapid data processing and real-time security measures are essential for sustaining a large ecosystem of connected devices. The flow between devices, edge nodes, and AI-based security indicates a comprehensive approach to managing and securing IoT networks.

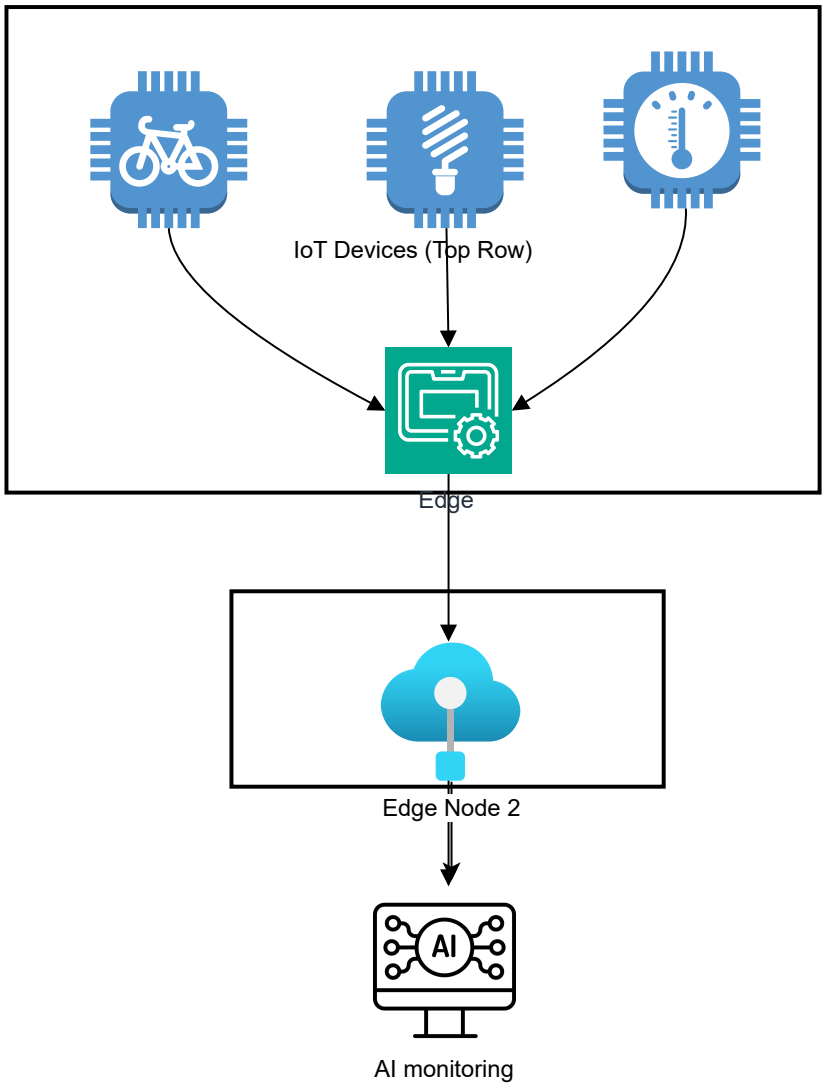


Figure 10. AI-Driven Security and Management in IoT and Edge Networks

 doi:10.20944/preprints202411.1407.v1

4.3. Case Study 3: AI for Network Security in Cloud-based Communications

As cloud-based communication systems become more prevalent, securing data and ensuring privacy is a critical challenge. AI has been implemented to enhance network security in cloud environments, particularly in the areas of intrusion detection, anomaly detection, and data protection [121].

AI-driven security systems can analyze incoming traffic for abnormal patterns, identify potential threats such as DDoS attacks, and dynamically adjust security measures to block malicious traffic. Additionally, AI plays a key role in ensuring the privacy of communication by implementing privacy-preserving techniques, including encryption and anonymization of sensitive data. AI-driven systems can also detect anomalies in cloud-based communications and provide real-time responses to mitigate potential risks [121].

Figure 11 represents an AI-driven network security framework designed to safeguard cloud-based communication systems. At the top, a labeled "Cloud-Based Communication System" encapsulates the cloud environment, symbolized by two servers ("Server 1" and "Server 2") which handle incoming traffic. The AI-powered Intrusion Detection System (IDS) is positioned below the servers, highlighting its role in scanning all incoming traffic for potential threats. Traffic from the servers flows directly to the IDS, where initial analysis takes place. Below the IDS is a "Data Protection Layer," which adds an additional security layer by securing data exchanges and monitoring for irregularities. Finally, an "Anomaly Detection" layer further examines the data to detect unusual patterns that could indicate security risks, ensuring comprehensive threat detection. Together, these interconnected components illustrate a multi-layered AI security strategy designed to enhance data integrity, prevent unauthorized access, and identify anomalies in real-time within a cloud-based communication infrastructure. This setup illustrates how each component contributes to creating a secure and reliable cloud communication system, with AI algorithms driving security operations at every level.

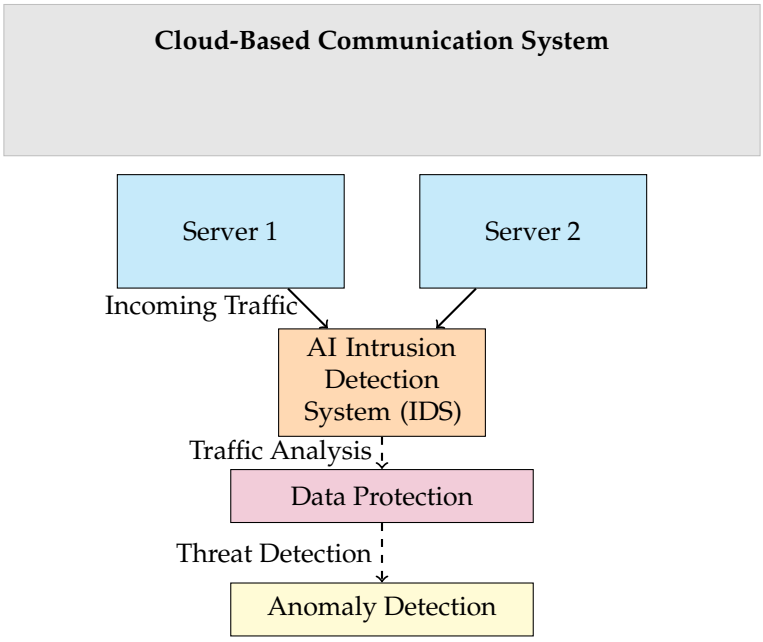


Figure 11. AI-Driven Network Security in Cloud-based Communications

 doi:10.20944/preprints202411.1407.v1

5. Challenges and Limitations

The integration of AI into communication networks brings numerous advantages but also presents several challenges and limitations. This section highlights the main obstacles faced when deploying AI in modern communication systems, particularly with respect to data privacy, scalability, model interpretability, and ethical concerns [122].

5.1. Data Privacy and Security

As AI-enabled networks process vast amounts of user data, privacy and security concerns are paramount. AI models, particularly those based on deep learning, require large datasets, often containing sensitive personal information such as communication patterns, geolocation, and usage behaviors. The use of these models without proper privacy controls may lead to significant risks, such as unauthorized access to user data or exposure of private communications [122].

A key challenge in this area is ensuring *data anonymization* and *encryption* during the training of AI models. Traditional encryption methods may not be well-suited to the computational needs of AI models. Recent techniques like *federated learning* aim to address this issue by allowing data to remain on the device, with only model updates being shared. However, federated learning introduces challenges regarding the synchronization of models across different devices, potential data poisoning, and ensuring that data remains unexploited [122].

A key trade-off between privacy protection and model performance can be seen in the following Table 8:

Table 8. Impact of Federated Learning on Accuracy, Privacy, and Computation

Method	Accuracy	Privacy Protection	Computational Overhead
Centralized Learning	95%	Low	High
Federated Learning	90%	High	Medium

5.2. Scalability and Resource Constraints

Implementing AI models in large-scale communication networks, especially in resource-constrained environments, poses significant challenges. In networks with *low-power devices* (e.g., IoT sensors, edge devices), implementing AI models such as deep neural networks (DNNs) may be impractical due to high computational and energy demands. These limitations become more pronounced when AI algorithms need to process real-time data, requiring both substantial *processing power* and *memory*. To address these challenges, *model optimization* techniques like model pruning, quantization, and edge-based computing are used. However, optimizing for scalability may sacrifice model accuracy or robustness. For example, using a compressed neural network might reduce memory requirements but could also lead to degraded performance in complex network environments [123].

Table 9 summarizes the trade-offs between model complexity and computational resources in edge devices:

Table 9. Scalability Analysis of AI Models in Resource-Constrained Environments

Model Complexity (Parameters)	Processing Time (ms)	Energy Consumption (J)
Simple Model (10k params)	10	0.02
Medium Model (50k params)	20	0.04
Complex Model (200k params)	50	0.12

5.3. Model Interpretability

One of the key challenges in AI deployment in critical network operations is the *interpretability* of AI models. Many AI models, especially deep learning models, are often considered “black boxes,”

 doi:10.20944/preprints202411.1407.v1

making it difficult to understand how decisions are made. This lack of transparency is particularly problematic in mission-critical applications, such as network security, where understanding the rationale behind an AI decision can be crucial to preventing security breaches [124]. For instance, in network traffic anomaly detection, an AI model might flag a packet as suspicious, but without a clear explanation, network administrators may hesitate to act. *Explainable AI (XAI)* techniques, which aim to make AI models more transparent, are crucial in addressing this issue. However, XAI techniques often come with trade-offs in terms of model complexity and performance [125].

Table 10 summarizes the impact of different explainability methods on model performance:

Table 10. Explainability Methods for AI Models in Communication Networks

Explainability Method	Model Accuracy	Interpretability	Trade-off in Performance
LIME (Local Surrogate)	85%	High	Medium
SHAP (Shapley Values)	88%	High	Low
Integrated Gradients	86%	Medium	Medium

This table shows the performance trade-offs between different explainability methods for AI models in communication networks, helping to decide which technique balances interpretability and accuracy best for a given application.

5.4. Ethical and Regulatory Issues

The deployment of AI in communication networks raises various *ethical* and *regulatory* issues. On the ethical front, the *bias* embedded in AI models can lead to unfair outcomes. For example, if an AI system used for network management is trained on biased data, it may lead to improper prioritization of network traffic, unfair resource allocation, or even discriminatory treatment of certain user groups. Ensuring fairness and accountability in AI systems is vital, particularly as AI decisions increasingly impact human lives [126].

From a *regulatory* perspective, there is a lack of standardized frameworks and guidelines for the ethical deployment of AI. Existing regulations, such as the *General Data Protection Regulation (GDPR)* in Europe, address some aspects of data privacy but do not specifically account for AI-driven processes. There is a pressing need for *regulatory bodies* to define frameworks for AI deployment in communication networks that include measures for accountability, transparency, and fairness [126].

Table 11 compares regulatory compliance costs across different regions, showing the economic implications of deploying AI in communication networks across various jurisdictions:

Table 11. Regulatory Compliance Costs for AI Deployment

Region	Regulatory Requirement	Compliance Cost (USD)
European Union (GDPR)	High Data Protection	50,000
United States (CCPA)	Consumer Privacy	30,000
Asia-Pacific (varies)	Varies	20,000

This table highlights the differences in regulatory compliance costs for AI deployment across various regions, providing insights into the economic challenges of deploying AI in communication networks worldwide [126].

The application of AI in communication networks is an exciting and rapidly advancing field, yet it faces several challenges and limitations. Addressing these challenges requires a combination of *technological innovation* and *policy development*. Ensuring data privacy, optimizing AI models for scalability, improving model interpretability, and navigating the ethical and regulatory landscapes will be key to the successful deployment of AI in communication systems. As the technology continues to evolve, solutions to these challenges will be critical for enabling the full potential of AI-powered communication networks.

 doi:10.20944/preprints202411.1407.v1

6. Future Directions

As AI continues to shape the landscape of communication networks, several promising directions are emerging. These areas have the potential to address current limitations and enhance the capabilities of AI-enabled networks in the future [127].

6.1. Edge AI

One of the most transformative trends in AI deployment within communication networks is *Edge AI*. By bringing computational intelligence closer to data sources, Edge AI enables real-time decision-making, reduces latency, and alleviates bandwidth constraints associated with cloud computing. This approach is particularly beneficial for applications requiring low latency, such as network monitoring and security in IoT ecosystems [128].

Edge AI can also help address *data privacy* concerns by processing data locally rather than transmitting it to centralized servers. However, achieving efficient AI models at the edge requires advancements in *model compression*, *hardware acceleration*, and *energy-efficient algorithms*. Table 12 compares the benefits and limitations of Edge AI versus Cloud-based AI for network applications.

Table 12. Comparison of Edge AI and Cloud-based AI for Communication Networks

Aspect	Edge AI	Cloud-based AI
Latency	Low	High
Data Privacy	High	Medium
Energy Efficiency	High	Low
Computational Power	Limited	High

Figure **??** could illustrate the latency reduction achieved by deploying AI models at the edge compared to cloud-based AI, with different application scenarios such as autonomous driving, network intrusion detection, and predictive maintenance.

6.2. Explainable AI (XAI)

As AI is increasingly used for critical tasks within communication networks, the need for *Explainable AI (XAI)* becomes crucial. XAI techniques aim to make AI models interpretable and understandable, allowing network operators and stakeholders to trust and validate AI-driven decisions. This transparency is particularly essential for applications like network security, where understanding the model's rationale is critical for effective threat mitigation [125].

Developing XAI methods specifically tailored for communication networks poses unique challenges, as network data is often complex and high-dimensional. Common XAI approaches include methods like *SHAP (Shapley Additive Explanations)*, *LIME (Local Interpretable Model-agnostic Explanations)*, and *Feature Attribution Maps* [125].

Table 13 provides a comparison of various XAI methods, highlighting their effectiveness and trade-offs.

Table 13. Comparison of XAI Methods for Communication Network Applications

Method	Interpretability	Complexity	Suitability for Network AI
SHAP	High	Medium	High
LIME	High	Medium	Medium
Feature Attribution Maps	Medium	Low	Medium

Future research in XAI for networks should focus on developing efficient, real-time interpretability methods that can integrate with Edge AI and provide explanations that network administrators can act upon in a timely manner.

 doi:10.20944/preprints202411.1407.v1

6.3. AI in 6G Networks

With the rapid approach of *6G networks*, AI is expected to play a foundational role in enabling features such as ultra-low latency, massive device connectivity, and advanced security. Unlike 5G, which relies on centralized architectures, 6G will likely incorporate decentralized and AI-driven management frameworks to support unprecedented scale and connectivity [118].

AI in 6G is anticipated to enhance capabilities in various aspects:

- **Ultra-low Latency:** AI-enabled predictive analytics can minimize latency by dynamically adjusting network resources based on real-time traffic patterns.
- **Massive Connectivity:** AI can facilitate efficient resource allocation to manage the vast number of connected devices.
- **Enhanced Security:** AI-driven threat detection and response mechanisms can protect 6G networks from increasingly sophisticated cyber-attacks.

These developments highlight the importance of AI-driven algorithms capable of handling real-time, high-throughput data streams, while simultaneously ensuring energy efficiency and security compliance [118].

6.4. Ethical and Legal Considerations

The widespread deployment of AI in communication networks raises significant ethical and legal issues. There is a pressing need for *ethical AI frameworks* to ensure fairness, transparency, and accountability. Ethical considerations are particularly important when AI systems influence access to resources or manage critical network infrastructure.

Legal compliance is equally vital, especially concerning data privacy laws like the *General Data Protection Regulation (GDPR)* in Europe and the *California Consumer Privacy Act (CCPA)* in the United States. As AI-based communication systems gather, store, and analyze personal data, adherence to these regulations is necessary to avoid legal ramifications and maintain user trust.

Table 14 provides an overview of ethical principles and corresponding regulatory requirements that AI-enabled networks should consider.

Table 14. Ethical Principles and Compliance Requirements for AI in Communication Networks

Ethical Principle	Related Regulation	Network Requirement
Transparency	GDPR	Data usage disclosure
Accountability	CCPA	Traceable decision-making
Fairness	Various Anti-Discrimination Laws	Unbiased resource allocation

To ensure responsible AI deployment, future research should focus on developing *AI governance frameworks* for communication networks, addressing both ethical guidelines and regulatory standards.

7. Conclusions

The integration of AI into communication networks is revolutionizing the way networks are managed, optimized, and secured. This paper has explored various applications of AI, including traffic prediction, resource allocation, anomaly detection, and network security. Each of these applications demonstrates the potential for AI to enhance network performance, reduce latency, and provide proactive security measures.

Despite the significant advancements, several challenges remain. Issues related to *data privacy*, *scalability*, *model interpretability*, and *ethical considerations* present obstacles that must be addressed for AI to achieve its full potential in communication networks. Future directions in Edge AI, Explainable AI, AI for 6G, and ethical compliance highlight promising paths for overcoming these challenges.

In conclusion, AI is poised to be a transformative force in the evolution of communication networks, from 5G to 6G and beyond. By addressing the identified challenges and pursuing the

 doi:10.20944/preprints202411.1407.v1

outlined future directions, AI can play a central role in building intelligent, adaptive, and secure communication infrastructures. Future research and development will be essential for maximizing the impact of AI in this domain, fostering a new generation of responsive and resilient communication networks.

Funding: This research received no external funding

Conflicts of Interest: The author declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

MDPI	Multidisciplinary Digital Publishing Institute
DOAJ	Directory of open access journals
TLA	Three letter acronym
LD	Linear dichroism

References

1. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A survey of internet of things (IoT) authentication schemes. *Sensors* **2019**, *19*, 1141.
2. El-Hajj, M.; Chamoun, M.; Fadlallah, A.; Serhrouchni, A. Analysis of authentication techniques in Internet of Things (IoT). 2017 1st Cyber Security in Networking Conference (CSNet). IEEE, 2017, pp. 1–3.
3. El-Hajj, M.; Chamoun, M.; Fadlallah, A.; Serhrouchni, A. Taxonomy of authentication techniques in Internet of Things (IoT). 2017 IEEE 15th Student Conference on Research and Development (SCOReD). IEEE, 2017, pp. 67–71.
4. Bécue, A.; Praça, I.; Gama, J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence Review* **2021**, *54*, 3849–3886.
5. Soori, M.; Arezoo, B.; Dastres, R. Artificial intelligence, machine learning and deep learning in advanced robotics, a review. *Cognitive Robotics* **2023**, *3*, 54–70.
6. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A survey of machine and deep learning methods for internet of things (IoT) security. *IEEE communications surveys & tutorials* **2020**, *22*, 1646–1685.
7. Hussain, F.; Hassan, S.A.; Hussain, R.; Hossain, E. Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges. *IEEE communications surveys & tutorials* **2020**, *22*, 1251–1275.
8. Chowdhury, M.Z.; Shahjalal, M.; Ahmed, S.; Jang, Y.M. 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. *IEEE Open Journal of the Communications Society* **2020**, *1*, 957–975.
9. Umoga, U.J.; Sodiya, E.O.; Ugwuanyi, E.D.; Jacks, B.S.; Lottu, O.A.; Daraojimba, O.D.; Obaigbena, A.; others. Exploring the potential of AI-driven optimization in enhancing network performance and efficiency. *Magna Scientia Advanced Research and Reviews* **2024**, *10*, 368–378.
10. El-Hajj, M. Leveraging Digital Twins and Intrusion Detection Systems for Enhanced Security in IoT-Based Smart City Infrastructures. *Electronics* **2024**, *13*, 3941.
11. Garalov, T.; Elhajj, M. Enhancing IoT Security: Design and Evaluation of a Raspberry Pi-Based Intrusion Detection System. 2023 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2023, pp. 1–7.
12. Moysen, J.; Giupponi, L. From 4G to 5G: Self-organized network management meets machine learning. *Computer Communications* **2018**, *129*, 248–268.
13. Dressler, F. *Self-organization in sensor and actor networks*; John Wiley & Sons, 2008.
14. Zhang, J.; Tao, D. Empowering things with intelligence: a survey of the progress, challenges, and opportunities in artificial intelligence of things. *IEEE Internet of Things Journal* **2020**, *8*, 7789–7817.
15. Singh, A.; Satapathy, S.C.; Roy, A.; Gutub, A. Ai-based mobile edge computing for iot: Applications, challenges, and future scope. *Arabian Journal for Science and Engineering* **2022**, *47*, 9801–9831.

16. Murshed, M.S.; Murphy, C.; Hou, D.; Khan, N.; Ananthanarayanan, G.; Hussain, F. Machine learning at the network edge: A survey. *ACM Computing Surveys (CSUR)* **2021**, *54*, 1–37.
17. Habbal, A.; Ali, M.K.; Abuzaraida, M.A. Artificial Intelligence Trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications* **2024**, *240*, 122442.
18. Díaz-Rodríguez, N.; Del Ser, J.; Coeckelbergh, M.; de Prado, M.L.; Herrera-Viedma, E.; Herrera, F. Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion* **2023**, *99*, 101896.
19. Esenogho, E.; Djouani, K.; Kurien, A.M. Integrating artificial intelligence Internet of Things and 5G for next-generation smartgrid: A survey of trends challenges and prospect. *Ieee Access* **2022**, *10*, 4794–4831.
20. Simeone, O. A very brief introduction to machine learning with applications to communication systems. *IEEE Transactions on Cognitive Communications and Networking* **2018**, *4*, 648–664.
21. O'shea, T.; Hoydis, J. An introduction to deep learning for the physical layer. *IEEE Transactions on Cognitive Communications and Networking* **2017**, *3*, 563–575.
22. Wahab, O.A.; Mourad, A.; Otrok, H.; Taleb, T. Federated machine learning: Survey, multi-level classification, desirable criteria and future directions in communication and networking systems. *IEEE Communications Surveys & Tutorials* **2021**, *23*, 1342–1397.
23. Lavanya, P.; Sasikala, E. Deep learning techniques on text classification using Natural language processing (NLP) in social healthcare network: A comprehensive survey. 2021 3rd international conference on signal processing and communication (ICPSC). IEEE, 2021, pp. 603–609.
24. Dong, G.; others. Graph Neural Networks in IoT: A Survey. *Proc. ACM Meas. Anal. Comput. Syst.* **2018**, *37*, 111–155.
25. Guo, Y.; others. Traffic Management in IoT Backbone Networks Using GNN and MAB with SDN Orchestration. *Sensors* **2023**, *23*, 7091.
26. Chen, A.C.H.; Jia, W.K.; Hwang, F.J.; Liu, G.; Song, F.; Pu, L. Machine learning and deep learning methods for wireless network applications. *EURASIP Journal on Wireless Communications and Networking* **2022**, *2022*.
27. Erpek, T.; O'Shea, T.J.; Sagduyu, Y.E.; Shi, Y.; Clancy, T.C. Deep Learning for Wireless Communications. *arXiv preprint arXiv:2005.06068* **2020**.
28. Chowdhury, S.; others. Deep Learning for Wireless Communications. *IEEE Access* **2020**, *8*, 1234567–1234578.
29. Sun, Y.; others. Machine Learning in Communications and Networks. *IEEE Journal on Selected Areas in Communications* **2022**, *40*, 1234–1256.
30. Sun, Y.; Lee, H.; Simpson, O. Machine Learning in Communication Systems and Networks. *Sensors* **2024**, *24*, 1925.
31. Li, N.; others. Network Traffic Classification and Control Technology Based on Decision Tree. *Advances in Intelligent Systems and Computing* **2019**, *1017*, 1701–1705.
32. Mohammadpour, L.; others. A Survey of CNN-Based Network Intrusion Detection. *Applied Sciences* **2022**, *12*, 8162.
33. Alaniz, S.; others. Learning Decision Trees Recurrently Through Communication. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)* **2021**, pp. 13518–13527.
34. Jindal, A.; Dua, A.; Kaur, K.; Singh, M.; Kumar, N.; Mishra, S. Decision tree and SVM-based data analytics for theft detection in smart grid. *IEEE Transactions on Industrial Informatics* **2016**, *12*, 1005–1016.
35. Kruegel, C.; Toth, T. Using decision trees to improve signature-based intrusion detection. International workshop on recent advances in intrusion detection. Springer, 2003, pp. 173–191.
36. De Cock, M.; Dowsley, R.; Horst, C.; Katti, R.; Nascimento, A.C.A.; Poon, W.S.; Truex, S. Efficient and Private Scoring of Decision Trees, Support Vector Machines and Logistic Regression Models Based on Pre-Computation. *IEEE Transactions on Dependable and Secure Computing* **2019**, *16*, 217–230. doi:10.1109/TDSC.2017.2679189.
37. Vinayakumar, R.; Soman, K.; Poornachandran, P. Applying convolutional neural network for network intrusion detection. 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, 2017, pp. 1222–1228.
38. Camacho, J.; Maciá-Fernández, G.; Fuentes-García, N.M.; Saccenti, E. Semi-supervised multivariate statistical network monitoring for learning security threats. *IEEE Transactions on Information Forensics and Security* **2019**, *14*, 2179–2189.

39. Kumari, R.; Singh, M.; Jha, R.; Singh, N.; others. Anomaly detection in network traffic using K-mean clustering. 2016 3rd international conference on recent advances in information technology (RAIT). IEEE, 2016, pp. 387–393.
40. Liu, Y.; Li, W.; Li, Y. Network traffic classification using k-means clustering. Second international multi-symposiums on computer and computational sciences (IMSCCS 2007). IEEE, 2007, pp. 360–365.
41. Münz, G.; Li, S.; Carle, G. Traffic anomaly detection using k-means clustering. Gi/itg workshop mmbnet, 2007, Vol. 7.
42. Abdi, H.; Williams, L.J. Principal component analysis. *Wiley interdisciplinary reviews: computational statistics* **2010**, *2*, 433–459.
43. Bishop, C.M.; Nasrabadi, N.M. *Pattern recognition and machine learning*; Vol. 4, Springer, 2006.
44. Usama, M.; Qadir, J.; Raza, A.; Arif, H.; Yau, K.L.A.; Elkhatib, Y.; Hussain, A.; Al-Fuqaha, A. Unsupervised machine learning for networking: Techniques, applications and research challenges. *IEEE access* **2019**, *7*, 65579–65615.
45. Xu, J. Efficient trajectory optimization and resource allocation in UAV 5G networks using dueling-Deep-Q-Networks. *Wireless Networks* **2023**, pp. 1–11.
46. Wang, S.; Liu, H.; Gomes, P.H.; Krishnamachari, B. Deep reinforcement learning for dynamic multichannel access in wireless networks. *IEEE transactions on cognitive communications and networking* **2018**, *4*, 257–265.
47. Mammeri, Z. Reinforcement learning based routing in networks: Review and classification of approaches. *Ieee Access* **2019**, *7*, 55916–55950.
48. Haider, M.; Yin, M.; Zhang, M.; Gupta, A.; Zhu, J.; Wang, Y.X. NetworkGym: Reinforcement Learning Environments for Multi-Access Traffic Management in Network Simulation. *arXiv preprint arXiv:2411.04138* **2024**.
49. Musaddiq, A.; Olsson, T.; Ahlgren, F. Reinforcement-Learning-Based Routing and Resource Management for Internet of Things Environments: Theoretical Perspective and Challenges. *Sensors* **2023**, *23*, 8263.
50. Mothukuri, V.; Parizi, R.M.; Pouriyeh, S.; Huang, Y.; Dehghantanha, A.; Srivastava, G. A survey on security and privacy of federated learning. *Future Generation Computer Systems* **2021**, *115*, 619–640.
51. Singh, S.; Rathore, S.; Alfarraj, O.; Tolba, A.; Yoon, B. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems* **2022**, *129*, 380–388.
52. Drainakis, G.; Pantazopoulos, P.; Katsaros, K.V.; Sourlas, V.; Amditis, A.; Kaklamani, D.I. From centralized to Federated Learning: Exploring performance and end-to-end resource consumption. *Computer Networks* **2023**, *225*, 109657.
53. Kalusivalingam, A.K.; Sharma, A.; Patel, N.; Singh, V. Enhancing Customer Service Automation with Natural Language Processing and Reinforcement Learning Algorithms. *International Journal of AI and ML* **2020**, *1*.
54. JS, H.; others. Analysis of Behavior in Chat Applications using Natural Language Processing. 2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS). IEEE, 2024, pp. 718–725.
55. Sharma, S.; Arjunan, T. Natural Language Processing for Detecting Anomalies and Intrusions in Unstructured Cybersecurity Data. *International Journal of Information and Cybersecurity* **2023**, *7*, 1–24.
56. Abbasi, M.; Shahraki, A.; Taherkordi, A. Deep learning for network traffic monitoring and analysis (NTMA): A survey. *Computer Communications* **2021**, *170*, 19–41.
57. Yan, Y.; Qian, Y.; Sharif, H.; Tipper, D. A survey on cyber security for smart grid communications. *IEEE communications surveys & tutorials* **2012**, *14*, 998–1010.
58. Marinho, R.; Holanda, R. Automated emerging cyber threat identification and profiling based on natural language processing. *IEEE Access* **2023**, *11*, 58915–58936.
59. Sworna, Z.T.; Mousavi, Z.; Babar, M.A. NLP methods in host-based intrusion detection Systems: A systematic review and future directions. *Journal of Network and Computer Applications* **2023**, p. 103761.
60. Wu, Y.; Zou, B.; Cao, Y. Current Status and Challenges and Future Trends of Deep Learning-Based Intrusion Detection Models. *Journal of Imaging* **2024**, *10*, 254.
61. Ali, Z.; Tiberti, W.; Marotta, A.; Cassioli, D. Empowering network security: Bert transformer learning approach and MLP for intrusion detection in imbalanced network traffic. *IEEE Access* **2024**.
62. Ramya, P.; Guntupalli, H.C. Advanced Cyber Attack Detection Using Generative Adversarial Networks and NLP. *Journal of Cybersecurity & Information Management* **2024**, *14*.

63. Markevych, M.; Dawson, M. A review of enhancing intrusion detection systems for cybersecurity using artificial intelligence (ai). International conference Knowledge-based Organization, 2023, Vol. 29, pp. 30–37.
64. Arazzi, M.; Arikkat, D.R.; Nicolazzo, S.; Nocera, A.; Conti, M.; others. NLP-Based Techniques for Cyber Threat Intelligence. *arXiv preprint arXiv:2311.08807* **2023**.
65. Ali, S.; Rehman, S.U.; Imran, A.; Adeem, G.; Iqbal, Z.; Kim, K.I. Comparative evaluation of ai-based techniques for zero-day attacks detection. *Electronics* **2022**, *11*, 3934.
66. Sindiramutty, S.R. Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence. *arXiv preprint arXiv:2401.00286* **2023**.
67. Haleem, A.; Javaid, M.; Singh, R.P. Exploring the competence of ChatGPT for customer and patient service management. *Intelligent Pharmacy* **2024**.
68. Ortiz-Garces, I.; Govea, J.; Andrade, R.O.; Villegas-Ch, W. Optimizing chatbot effectiveness through advanced syntactic analysis: A comprehensive study in natural language processing. *Applied Sciences* **2024**, *14*, 1737.
69. Filonova, E. Evaluation of Natural Language Processing and Machine Learning Tools for the Automation of the Customer Service Task, 2022.
70. Han, J.; Huang, Y.; Liu, S.; Towey, K. Artificial intelligence for anti-money laundering: a review and extension. *Digital Finance* **2020**, *2*, 211–239.
71. Zhou, J.; Cui, G.; Hu, S.; Zhang, Z.; Yang, C.; Liu, Z.; Wang, L.; Li, C.; Sun, M. Graph neural networks: A review of methods and applications. *AI open* **2020**, *1*, 57–81.
72. Rusek, K.; Suárez-Varela, J.; Almasan, P.; Barlet-Ros, P.; Cabellos-Aparicio, A. RouteNet: Leveraging graph neural networks for network modeling and optimization in SDN. *IEEE Journal on Selected Areas in Communications* **2020**, *38*, 2260–2270.
73. Liang, S.; Wang, Y.; Liu, C.; He, L.; Huawei, L.; Xu, D.; Li, X. EnGN: A high-throughput and energy-efficient accelerator for large graph neural networks. *IEEE Transactions on Computers* **2020**, *70*, 1511–1525.
74. Jiang, W.; Liu, H.; Xiong, H. When Graph Neural Network Meets Causality: Opportunities, Methodologies and An Outlook. *arXiv preprint arXiv:2312.12477* **2023**.
75. Jiang, W.; Han, H.; Zhang, Y.; Wang, J.; He, M.; Gu, W.; Mu, J.; Cheng, X. Graph Neural Networks for Routing Optimization: Challenges and Opportunities. *Sustainability* **2024**, *16*, 9239.
76. Mistry, H.K.; Mavani, C.; Goswami, A.; Patel, R. Artificial intelligence for networking. *Educational Administration: Theory and Practice* **2024**, *30*, 813–821.
77. Guo, A.; Yuan, C. Network intelligent control and traffic optimization based on SDN and artificial intelligence. *Electronics* **2021**, *10*, 700.
78. Chaudhary, H.; Detroja, A.; Prajapati, P.; Shah, P. A review of various challenges in cybersecurity using artificial intelligence. 2020 3rd international conference on intelligent sustainable systems (ICISS). IEEE, 2020, pp. 829–836.
79. Yazici, İ.; Shayea, I.; Din, J. A survey of applications of artificial intelligence and machine learning in future mobile networks-enabled systems. *Engineering Science and Technology, an International Journal* **2023**, *44*, 101455.
80. Klaine, P.V.; Imran, M.A.; Onireti, O.; Souza, R.D. A survey of machine learning techniques applied to self-organizing cellular networks. *IEEE Communications Surveys & Tutorials* **2017**, *19*, 2392–2431.
81. Rodríguez, G.; Soria, Á.; Campo, M. Artificial intelligence in service-oriented software design. *Engineering Applications of Artificial Intelligence* **2016**, *53*, 86–104.
82. Sathupadi, K. An ai-driven framework for dynamic resource allocation in software-defined networking to optimize cloud infrastructure performance and scalability. *International Journal of Intelligent Automation and Computing* **2023**, *6*, 46–64.
83. Xiao, Y.; Liu, J.; Wu, J.; Ansari, N. Leveraging deep reinforcement learning for traffic engineering: A survey. *IEEE Communications Surveys & Tutorials* **2021**, *23*, 2064–2097.
84. Chinchali, S.; Hu, P.; Chu, T.; Sharma, M.; Bansal, M.; Misra, R.; Pavone, M.; Katti, S. Cellular network traffic scheduling with deep reinforcement learning. Proceedings of the AAAI Conference on Artificial Intelligence, 2018, Vol. 32.
85. Noaeen, M.; Naik, A.; Goodman, L.; Crebo, J.; Abrar, T.; Abad, Z.S.H.; Bazzan, A.L.; Far, B. Reinforcement learning in urban network traffic signal control: A systematic literature review. *Expert Systems with Applications* **2022**, *199*, 116830.

86. Fu, Y.; Wang, S.; Wang, C.X.; Hong, X.; McLaughlin, S. Artificial intelligence to manage network traffic of 5G wireless networks. *IEEE network* **2018**, *32*, 58–64.
87. Kumar, H. ML/AI Enabled Intelligent Next Generation Autonomous Network System: Performance Enhancement and Management. PhD thesis, The University of New Mexico, 2024.
88. Baccour, E.; Mhaisen, N.; Abdellatif, A.A.; Erbad, A.; Mohamed, A.; Hamdi, M.; Guizani, M. Pervasive AI for IoT applications: A survey on resource-efficient distributed artificial intelligence. *IEEE Communications Surveys & Tutorials* **2022**, *24*, 2366–2418.
89. Arulmurugan, L.; Thakur, S.; Dayana, R.; Thenappan, S.; Nagesh, B.; Sri, R.K. Advancing Security: Exploring AI-driven Data Encryption Solutions for Wireless Sensor Networks. 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI). IEEE, 2024, pp. 1–6.
90. Dodda, S.B.; Maruthi, S.; Yellu, R.R.; Thuniki, P.; Reddy, S.R.B. Federated Learning for Privacy-Preserving Collaborative AI: Exploring federated learning techniques for training AI models collaboratively while preserving data privacy. *Australian Journal of Machine Learning Research & Applications* **2022**, *2*, 13–23.
91. Rodríguez-Barroso, N.; Stipcich, G.; Jiménez-López, D.; Ruiz-Millán, J.A.; Martínez-Cámara, E.; González-Seco, G.; Luzón, M.V.; Veganzones, M.A.; Herrera, F. Federated Learning and Differential Privacy: Software tools analysis, the Sherpa. ai FL framework and methodological guidelines for preserving data privacy. *Information Fusion* **2020**, *64*, 270–292.
92. Shen, S.; Yu, C.; Zhang, K.; Ni, J.; Ci, S. Adaptive and dynamic security in AI-empowered 6G: From an energy efficiency perspective. *IEEE Communications Standards Magazine* **2021**, *5*, 80–88.
93. Alwhbi, I.A.; Zou, C.C.; Alharbi, R.N. Encrypted Network Traffic Analysis and Classification Utilizing Machine Learning. *Sensors* **2024**, *24*, 3509.
94. Khalid, N.; Qayyum, A.; Bilal, M.; Al-Fuqaha, A.; Qadir, J. Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Computers in Biology and Medicine* **2023**, *158*, 106848.
95. Vegesna, V.V. Privacy-Preserving Techniques in AI-Powered Cyber Security: Challenges and Opportunities. *International Journal of Machine Learning for Sustainable Development* **2023**, *5*, 1–8.
96. Torkzadehmahani, R.; Nasirigerdeh, R.; Blumenthal, D.B.; Kacprowski, T.; List, M.; Matschinske, J.; Spaeth, J.; Wenke, N.K.; Baumbach, J. Privacy-preserving artificial intelligence techniques in biomedicine. *Methods of information in medicine* **2022**, *61*, e12–e27.
97. Zhang, C.; Xie, Y.; Bai, H.; Yu, B.; Li, W.; Gao, Y. A survey on federated learning. *Knowledge-Based Systems* **2021**, *216*, 106775. doi:https://doi.org/10.1016/j.knosys.2021.106775.
98. Abdulrahman, S.; Tout, H.; Ould-Slimane, H.; Mourad, A.; Talhi, C.; Guizani, M. A Survey on Federated Learning: The Journey From Centralized to Distributed On-Site Learning and Beyond. *IEEE Internet of Things Journal* **2021**, *8*, 5476–5497. doi:10.1109/JIOT.2020.3030072.
99. Oude Roelink, B.; El-Hajj, M.; Sarmah, D. Systematic review: Comparing zk-SNARK, zk-STARK, and bulletproof protocols for privacy-preserving authentication. *SECURITY AND PRIVACY* **2024**, *7*, e401, [https://onlinelibrary.wiley.com/doi/pdf/10.1002/spy2.401]. doi:https://doi.org/10.1002/spy2.401.
100. El-Hajj, M.; Oude Roelink, B. Evaluating the Efficiency of zk-SNARK, zk-STARK, and Bulletproof in Real-World Scenarios: A Benchmark Study. *Information* **2024**, *15*.
101. Zaman, S.; Alhazmi, K.; Aseeri, M.A.; Ahmed, M.R.; Khan, R.T.; Kaiser, M.S.; Mahmud, M. Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey. *IEEE Access* **2021**, *9*, 94668–94690. doi:10.1109/ACCESS.2021.3089681.
102. Enhancing Privacy and Security in IoT Environments through Secure Multiparty Computation. *2*. doi:10.58190/icisna.2024.92.
103. Rahaman, M.; Arya, V.; Orozco, S.M.; Pappachan, P. Secure Multi-Party Computation (SMPC) Protocols and Privacy. In *Innovations in Modern Cryptography*; IGI Global, 2024; pp. 190–214.
104. Drîngă, B.; Elhajj, M. Performance and Security Analysis of Privacy-Preserved IoT Applications. 2023 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT). IEEE, 2023, pp. 549–556.
105. Dai, B.; Cao, Y.; Wu, Z.; Dai, Z.; Yao, R.; Xu, Y. Routing optimization meets Machine Intelligence: A perspective for the future network. *Neurocomputing* **2021**, *459*, 44–58.
106. Hashemi, H.; Abdelghany, K. Real-time traffic network state prediction for proactive traffic management: Simulation experiments and sensitivity analysis. *Transportation Research Record* **2015**, *2491*, 22–31.

107. Kibria, M.G.; Nguyen, K.; Villardi, G.P.; Zhao, O.; Ishizu, K.; Kojima, F. Big data analytics, machine learning, and artificial intelligence in next-generation wireless networks. *IEEE access* **2018**, *6*, 32328–32338.
108. Alhilali, A.H.; Montazerolghaem, A. Artificial intelligence based load balancing in SDN: A comprehensive survey. *Internet of Things* **2023**, *22*, 100814.
109. Wang, F.; Yao, H.; Zhang, Q.; Wang, J.; Gao, R.; Guo, D.; Guizani, M. Dynamic distributed multi-path aided load balancing for optical data center networks. *IEEE Transactions on Network and Service Management* **2021**, *19*, 991–1005.
110. Shaygan, M.; Meese, C.; Li, W.; Zhao, X.G.; Nejad, M. Traffic prediction using artificial intelligence: Review of recent advances and emerging opportunities. *Transportation research part C: emerging technologies* **2022**, *145*, 103921.
111. Zhang, C.; Patras, P.; Haddadi, H. Deep learning in mobile and wireless networking: A survey. *IEEE Communications surveys & tutorials* **2019**, *21*, 2224–2287.
112. Wang, X.; Li, X.; Leung, V.C. Artificial intelligence-based techniques for emerging heterogeneous network: State of the arts, opportunities, and challenges. *IEEE Access* **2015**, *3*, 1379–1391.
113. Meduri, K.; Nadella, G.S.; Gonaygunta, H.; Meduri, S.S. Developing a Fog Computing-based AI Framework for Real-time Traffic Management and Optimization. *International Journal of Sustainable Development in Computing Science* **2023**, *5*, 1–24.
114. Papidas, A.G.; Polyzos, G.C. Self-organizing networks for 5g and beyond: A view from the top. *Future Internet* **2022**, *14*, 95.
115. Sodhro, A.H.; Luo, Z.; Sodhro, G.H.; Muzamal, M.; Rodrigues, J.J.; De Albuquerque, V.H.C. Artificial Intelligence based QoS optimization for multimedia communication in IoV systems. *Future Generation Computer Systems* **2019**, *95*, 667–680.
116. Fadlullah, Z.M.; Mao, B.; Kato, N. Balancing QoS and security in the edge: Existing practices, challenges, and 6G opportunities with machine learning. *IEEE Communications Surveys & Tutorials* **2022**, *24*, 2419–2448.
117. Anwar, R.; Bashir, M.B. A Systematic Literature Review of AI-based Software Requirements Prioritization Technique. *IEEE Access* **2023**.
118. Shafin, R.; Liu, L.; Chandrasekhar, V.; Chen, H.; Reed, J.; Zhang, J.C. Artificial intelligence-enabled cellular networks: A critical path to beyond-5G and 6G. *IEEE Wireless Communications* **2020**, *27*, 212–217.
119. Moustafa, N. A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets. *Sustainable Cities and Society* **2021**, *72*, 102994.
120. Chakrabarty, S.; Engels, D.W. Secure smart cities framework using IoT and AI. 2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT). IEEE, 2020, pp. 1–6.
121. Olabanji, S.O.; Marquis, Y.; Adigwe, C.S.; Ajayi, S.A.; Oladoyinbo, T.O.; Olaniyi, O.O. AI-driven cloud security: Examining the impact of user behavior analysis on threat detection. *Asian Journal of Research in Computer Science* **2024**, *17*, 57–74.
122. Zhang, S.; Zhu, D. Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities. *Computer Networks* **2020**, *183*, 107556.
123. Goriparthi, R.G. Hybrid AI Frameworks for Edge Computing: Balancing Efficiency and Scalability. *International Journal of Advanced Engineering Technologies and Innovations* **2024**, *2*, 110–130.
124. Jha, S. Trust, resilience and interpretability of AI models. Numerical Software Verification: 12th International Workshop, NSV 2019, New York City, NY, USA, July 13–14, 2019, Proceedings 12. Springer, 2019, pp. 3–25.
125. Velioglu, R.; Göpfert, J.P.; Artelt, A.; Hammer, B. Explainable artificial intelligence for improved modeling of processes. International Conference on Intelligent Data Engineering and Automated Learning. Springer, 2022, pp. 313–325.
126. Cath, C. Governing artificial intelligence: ethical, legal and technical opportunities and challenges. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* **2018**, *376*, 20180080.
127. Gill, S.S.; Xu, M.; Ottaviani, C.; Patros, P.; Bahsoon, R.; Shaghaghi, A.; Golec, M.; Stankovski, V.; Wu, H.; Abraham, A.; others. AI for next generation computing: Emerging trends and future directions. *Internet of Things* **2022**, *19*, 100514.
128. Singh, R.; Gill, S.S. Edge AI: a survey. *Internet of Things and Cyber-Physical Systems* **2023**, *3*, 71–92.

 doi:10.20944/preprints202411.1407.v1