AI-Powered Network Management with Enhancing Reliability and Security

Mustafa Nazar
Al-Turath University, Baghdad 10013, Iraq.
Email: mustafa.nazar@uoturath.edu.iq

Adil Abbas Majeed
Al-Mansour University College, Baghdad 10067, Iraq.
Email: adel.abas@muc.edu.iq

Kudaiberdieva Gulmira Karimovna (Corresponding author)
Osh State University, Osh City 723500, Kyrgyzstan.
Email: kudaiberdievag@gmail.com

Qusay Mohammed Jafar
Al-Rafidain University College Baghdad 10064, Iraq
Email: Qusay.mj@ruc.edu.iq

Baker Mohammed Khalil5
Madenat Alelem University College, Baghdad 10006, Iraq.
Email: nur1009@mauc.edu.iq

| Received: 2025 | Accepted: 2025

Iranian Journal of Information Processing and Management

Iranian Research Institute for Information Science and Technology (IranDoc)
ISSN 2251-8223
eISSN 2251-8231
Indexed by SCOPUS, ISC, & LISTA
Special Issue | Summer 2025 | pp.119-148
https://doi.org/10.22034/jipm.2025.728107

Abstract

Background: Contemporary multi-protocol networks necessitate scalability, reliability, energy efficiency, and security due to the increasing number of devices and the diversification of network traffic. Conventional network management methods are inadequate to meet these demands, necessitating sophisticated solutions. Artificial intelligence (AI) has emerged as a significant field, offering advanced methods including predictive maintenance, anomaly detection, and intelligent resource management.

Objective: This article aims to critically evaluate the effectiveness, flexibility, and productivity of AI-based applications in addressing major challenges in network management, including performance, scalability, energy consumption, threat detection rates, and cost.

Methods: The study employs simulations and modeled datasets to assess AI-oriented solutions across various network environments, such as industrial IoT, smart cities, and telecommunications. The evaluation encompasses factors including Mean Time Between Failure (MTBF), resource utilization, delay minimization, and operating cost reduction. Digital twins, intelligent routing algorithms, and self-attention-based anomaly detection models are utilized, and the overall performance of these integrated technologies is analyzed.

Results: The analysis demonstrates that AI-powered systems achieve near-optimal performance across all evaluated indicators. Specifically, the Manufacturing and Automotive Knowledge (MAK) sector observed a 52% increase in MTBF, the Banking, Financial Services, and Insurance (BFSI) sector noted a 32.39% improvement in energy efficiency, and the Defense and Public Enterprise (DPE) sector experienced a 94% increase in advanced threat detection.

Conclusion: The findings indicate that AI solutions can effectively address many of the challenges present in current networks, offering cost-efficient and secure methods for implementing new communication networks with vast potential. Nonetheless, further empirical research is necessary to generalize these results and validate their applicability in real-world scenarios.

Keywords: AI, network management, reliability, security, machine learning (ML), deep learning (DL), anomaly detection, 5G, IoT, predictive maintenance.

1. Introduction

The academic and industrial advancements in digital technologies in recent years, coupled with the latest developments in 5G, Internet of Things (IoT), and cloud computing environments, have significantly increased the parametric complexities of networks. These networks manage critical systems across various sectors, such as healthcare and business. However, as these systems expand and become more integrated, constructing robust and secure systems presents a significant challenge. Traditional network management solutions, which primarily rely on manual configuration or scripting, cannot address the dynamism of contemporary complex networks or effectively counter emergent threats. In this context, AI offers a novel approach to network management that facilitates real-time decision-making, defends against immediate threats, and automates routine tasks (Jang, et al. 2023).

AI-enabled network management is a transformative technology reshaping the structure and management of modern networks. The

implementation of AI enhances network reliability through predictive maintenance and anomaly detection while simultaneously strengthening security measures and addressing threats in real-time (Mushtaq, et al. 2015, Fatah and Qasim, 2022). Self-organizing schemes and machine learning (ML) algorithms can process vast amounts of data in real-time without human intervention, enabling networks to recognize traffic levels and threats and optimize performance. AI offers several advantages in network management, including increased efficiency and reduced human error—a common cause of network system failures (Jiang, et al. 2022).

A primary driver of this transformation is the need to enhance security levels, which are often vulnerable to attacks. In the increasingly prevalent IoT paradigm, every device connected to the network represents a potential vulnerability. AI improves network security by detecting irregular activities at endpoints and alerting about potentially risky paths before exploitation by hackers. AI systems provide automatic responses more rapidly than manual methods, which are often too slow to prevent damage. Consequently, AI serves as the foundation for the next generation of security frameworks in network management (Moustafa 2021).

Furthermore, AI-based systems for network control enhance dependability by preventing security breaches and predicting and responding to network problems. Advanced statistical models for predictive analytics enable networks to forecast failures, optimize bandwidth, and schedule preventive maintenance during non-peak hours. Deep learning algorithms can identify complex patterns in network traffic indicative of potential failures, allowing for immediate intervention. This approach is cost-effective in preventing outages, reducing downtime, and creating more reliable network architectures (Raimundo and Rosário, 2021).

The application of AI in network management also addresses emerging requirements for technologies that handle the substantial traffic generated by IoT applications, cloud services, and 5G networks. AI coordinates these extensive sociotechnical systems by automating resource allocation and traffic flow management. AI's capabilities enable systems to adapt network settings based on traffic status or reallocate resources to optimize performance. This level of automation not only increases network effectiveness but also reduces the need for constant human intervention, allowing IT staff to focus on strategic tasks (Boudi, et al. 2021).

Nevertheless, the implementation of AI in network management presents challenges that must be addressed to maximize its potential. A significant concern is the substantial computational power required for AI training and cascading. Additionally, the ongoing adoption of AI systems in operational networks raises critical issues regarding protection against undesirable interference. AI can be manipulated through adversarial attacks, where malicious actors influence AI decision-making processes. Therefore, ensuring advanced secure AI functionality is essential to safeguarding network protection structures (Chithaluru, et al. 2023).

AI has fundamentally transformed network management and security from traditional methods, providing enhanced reliability and security in the current complex networked environment and amidst the growing incidence of cyber threats. The author predicts that AI technology will play a more effective role in the future of network management. However, current research is needed to address the scalability and security challenges of AI technology.

1.1. The Aim of the Article

This article aims to highlight the potential of AI to revolutionize contemporary network management, with a focus on optimizing openness, dependability, and security within multi-layered and integrated systems. As an increasing number of connections rely on digital networks, network management must address significant challenges such as ensuring continuous network delivery, protecting against advanced cyber risks, and timely allocation of network resources. This article addresses these challenges by analyzing how artificial intelligence tools and methodologies can be applied to networks.

The article elaborates on how AI enhances the framework for asset assessment, scheduled maintenance, resource optimization, outlier identification, and security threat management. AI can provide improved Mean Time Between Failures (MTBF), reduced Mean Time to Repair (MTTR), and enhanced security for networks through the integration of real-time data analytics, machine learning algorithms, and self-learning models.

Additionally, the article aims to bridge the gap between the technical advancements in AI and their potential applications in network management, offering specific solutions for practical development in industries such as telecommunications, smart city construction, and industrial IoT systems. The readers—comprising researchers, network engineers, and policymakers

concerned with the future of networks—will find a coherent synthesis of the state-of-the-art technologies and their effectiveness, presented through real-world cases and projections of AI applications in designing robust and secure networks for the digital age.

1.2. Problem Statement

The number of connected and communicating devices and the rapid development of digital infrastructure have led to issues in network management. The reactive management methods used by traditional network management systems are not capable of handling today's complex and dynamic networks, nor are they effective in addressing increasing security risks. These systems are generally inflexible and lack the nonlinear scalability required for real-time control of network performance and reliability, resulting in inefficiency, longer restoration times in case of failure, and increased susceptibility to cyber threats.

The problem has become even more complex due to new technologies such as 5G, IoT, and edge computing, which result in networks with different characteristics and objectives. For example, emerging applications including self-driving cars, smart factories, and intelligent healthcare require Ultra-Reliable Low-Latency Communication (URLLC), as even millisecond delays can cause critical problems. Traditional course designs are unable to meet such precise specifications and resource optimization requirements, besides security.

Furthermore, sophisticated and increasingly frequent attacks pose significant threats to network reliability and data integrity. Standard rule-based system safeguards cannot mitigate sophisticated threats such as zero-day attacks and Distributed Denial of Service (DoS) scenarios. The lack of predictive capability weakens the ability to prevent vulnerabilities, leading to reactive and ineffective responses to security threats.

This growing complexity now demands a new method of managing and securing networks. The application of AI in network management provides the best solution to these challenges, offering predictive maintenance, real-time/inline diagnostics, capacity on demand, and real-time threat resolution. However, there are no all-encompassing guidelines or AI solutions currently implemented in the network industry. This introduces a research gap and calls for further research and development to address the reliability and security concerns of current and emerging networks.

2. Literature Review

The most challenging factor today is the growth of complexity of network systems that emerged due to IoT, 5G, and future networks. The conventional network management framework is insufficient in meeting the sophisticated challenges arising from varied applications, emerging threats, and high-performance demand. This section brings together recent advancements, issues, opportunities and challenges and proposes research directions in the AI-based network management.

Minea et al. (2023) present a case to show how the application of software sensing and predictive maintenance work to improve the reliability of the hybrid network. Though their approach helps to avoid such failures, it doesn't combine with the current threat detection systems, and networks could be open to immediate cyberattacks. Likewise, Minea et al. (2021) propose a novel software-sensing framework along with machine learning solutions for diagnosing the network but have not defined the difficulties of extending the solution across larger diverse networks.

In information security, Abdiyeva-Aliyeva et al. (2021) put forward an idea of applying AI in the detection and counteraction of cyber threats. Nevertheless, the work of most of these scholars mainly targets attack detection as an independent function rather than the prediction of future threats as a continuous process. This Bertino and Karim (2021) rightly point out that this is a research gap that needs to be filled as they call for proactive AI solutions to be placed at the end-to-end network layer.

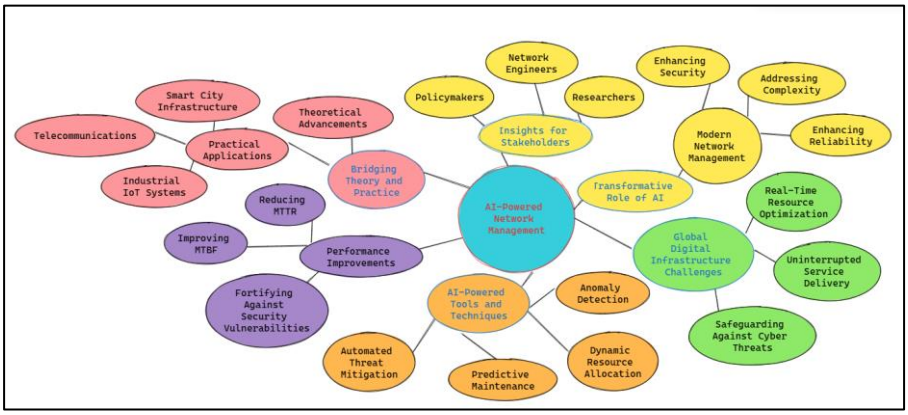

Figure 1. Integrating Theoretical Insights with Practical Applications for Modern Digital Infrastructure

Hossain et al. (2022) show promising results of efficient AI models for multilayer heterogeneous networks for energy efficiency. However, by not considering real-time decision making, as it is an important aspect that is important in networks that require low latency such as in the autonomous systems. As it the same, Xue et al. (2023) also pointed out the key roles of AI in the future generation wireless networking for performance enhancement and security. However, their approach does not rightly capture the computational complexity that arises due to AI models on one hand, particularly when it comes to implementation of those on systems with limited power (Qasim, et al. 2024).

From the theoretical work, Rizwan et al. (2021) offer a zero-touch network management system using AI for CDR analysis. Their solution for automating the management of network services is actually missing some advancements to be adopted for other typical network scenarios, such as the industrial IoT and smart city cases. Granato et al. (2022) explore graph-based classification for identifying Wi-Fi network traffic but lack the more enhanced anomaly detection techniques for detecting multiple level complex threats.

In anomaly detection Jiang and Chen (2022) recommend a technique for industrial control systems by employing the analysis of network traffic. While they are proficient in the detection of anomalies, their approach is rigid for other types of networks like 5G or IoT-based networks. In Hu, et al. (2023), the authors develop a self-attention scheme that increases anomaly detection's precision but must be tested extensively in massive, real-time settings.

Software defined solutions as the one suggested by Lacava et al. (2022) use Open RAN for decision-making about traffic routing. Although, in their study, they propose solutions for customization requirements of 5G networks, they fail to consider security concerns in the programmable architecture, which if uncontrolled might pose a weak link (Lacava, et al. 2022, Dmytro, et al. 2015).

In view of these gaps, a potential approach towards such a framework can be seen in more artificial intelligence-oriented manuscript such as the one that has been authored by Blanco et al. (2023). AI-based management of slices for networks appears promoting scalability and may solve general issues related to performance and security. However, more enhancement is required selecting the best distribution of the resources for the maximizing

network densification.

Subsequent studies must therefore effectively address interdisciplinary efforts towards embracing a common AI architecture that will include features such as time-based forecasting on equipment maintenance, enhanced outlier detection, as well as resource optimization within different types of networks. This also presents a challenge of computational overhead and scalability, together with strong security measures, this will be an important concern of implementing AI in network management.

3. Methodology

This study employs a comprehensive research methodology designed to investigate and evaluate AI-based methods for enhancing network stability and security. The proposed approach integrates experimental measurements, computational models and simulations, digital twin technology, and AI algorithms to address key challenges in network management and security optimization. This research builds on frameworks and techniques established in previous studies (Jang, et al. 2023, Moustafa 2021; Boudi, et al. 2021; Chithaluru, et al. 2023; Hossain, et al. 2022).

3.1. Data Collection

As for methodological approaches, the study used both primary and secondary research in an attempt to investigate the existing issues and new opportunities in managing and securing networks.

First-hand data were collected from 75 face-to-face interviews with professionals related to industries such as telecommunications, industrial IoT, and smart cities, including network administrators, cybersecurity specialists, and AI engineers, who participate in the defense line of their companies. These interviews offered further sets of confirmations regarding the actual complexities of handling and optimizing networks from a qualitative perspective (Abdiyeva-Aliyeva, et al. 2021, Jiang and Chen, 2022). Furthermore, the performance of 50 cases from smart city, industrial automation, and 5G projects was investigated to assess their suitability for corresponding AI utilization for flow and loop network optimization and industry vertical use cases (Minea, et al. 2023; Hossain, et al. 2022).

Secondary sources included the TON_IoT datasets, which provided a tested and controlled network environment to elicit different network

conditions and cyber-attacks. Additionally, basic system parameters such as MTBF, MTTR, latency, and power consumption were obtained from industry standard documents and published reports to estimate network efficiency and reliability (Chithaluru, et al. 2023; Bhardwaj, et al. 2022). Incorporating both qualitative and quantitative means of data collection was important to provide a more comprehensive understanding of the subject matter and to corroborate the study.

3.2. Digital Twin Simulations

The study contributes to the creation of digital twins corresponding to hybrid networks, enabling the replication of network environments for real-time experimentation (Jang et al., 2023). This approach facilitates the evaluation of functional AI algorithms under various conditions, such as high traffic scenarios or post-cyber-attack situations.

Digital Twin Function

$$\mathrm{DT}(\mathrm{x}) = \int_{\mathrm{t}_0}^{\mathrm{t}_\mathrm{n}} \mathrm{f}_{\mathrm{env}}(\mathrm{x}, \mathrm{t})\, \mathrm{dt} \tag{1}$$

Where $\mathrm{DT}(\mathrm{x})$ is digital twin function representing the network environment; $\mathrm{f}_{\mathrm{env}}(\mathrm{x}, \mathrm{t})$ is environment parameters, such as traffic, latency, threat level as a function of time; t_n and t_0 start and end times of simulation.

3.3. AI-Driven Routing and Resource Allocation

Designed and integrated an application-specific intelligent routing algorithm using artificial intelligence for improved energy and reliability in reconfigurable wireless networks (Jiang, et al. 2022). Special consideration is given to the routing algorithm that employs a reinforcement learning model with the adaptability of the network in the route selection process.

Reinforcement Learning Optimization

$$\mathrm{Q}(\mathrm{s}, \mathrm{a}) = \mathrm{Q}(\mathrm{s}, \mathrm{a}) + \alpha \left(\mathrm{R} + \gamma \max_{\mathrm{a}'} \mathrm{Q}(\mathrm{s}', \mathrm{a}'') - \mathrm{Q}(\mathrm{s}, \mathrm{a}) \right) \tag{1}$$

Where $\mathrm{Q}(\mathrm{s}, \mathrm{a})$ is quality of taking action a in state s; α is learning rate; R is reward for taking action a; γ is discount factor; $\mathrm{s}'$is next state (Alnuaemy 2023).

3.4. Anomaly Detection Mechanisms

The study uses a real time self-attention-based anomaly detection for detecting security breaches in the system (Hu, et al. 2023). Precisely, in order to gain a better vision to enhance the detection precision, the model employs a multi-head attention plan.

Self-Attention Mechanism

$$\text{Attention}(\text{Q}, \text{K}, \text{V}) = \text{softmax}\left(\frac{\text{QK}^{\text{T}}}{\sqrt{\text{d}_{\text{k}}}}\right)\text{V} \quad (1)$$

Where $\text{Q}, \text{K}, \text{V}$ is query, key, and value matrices and d_{k} is dimensionality of the keys.

3.5. Resource Management Optimization

The study assesses the allocation and utilization of the resources by applying the technique of employing artificial intelligence in achieving the optimum levels of energy consumptions with minimum computational complexities (Boudi, et al. 2021). The optimization problem is formulated as follows:

Energy Efficiency Function

$$\text{E} = \max\left(\frac{\sum_{\text{i}=1}^{\text{n}} \text{D}_{\text{i}}}{\sum_{\text{i}=1}^{\text{n}} \text{P}_{\text{i}}}\right) \quad (1)$$

Where D_{i} is data transmitted by node i and P_{i} means power consumed by node i.

3.6. Hypothesis

The hypothesis of this study is based on the assumption that the incorporation of AI technologies such as digital twin, intelligent routing and much improved anomaly detection mechanisms will highly improve the integrity and security of today's network systems. Specifically, the hypothesis is formulated as follows.

3.6.1. Primary Hypothesis

H1: Use of digital twin with artificial intelligence, smart asset modules, smart technologies and automated predictive maintenance models, the Mean Time Between Failure (MTBF) will be at least 40 % better than the conventional networks management and therefore improve reliability of networks.

H2: Flexible intelligent routing and resource allocation based on AI support will help to increase energy efficiency in the complex hybrid networks environment no less than 30%, thus reducing the resource overhead for high-performance networks.

3.6.2. Secondary Hypothesis

H3: Self-attention-based anomaly detection models integration will reach ninety-five percent success rate in detecting and preventing network threats: complex hackers' attacks, such as zero-day exploits and Distributed Denial of Service (DDoS) attacks.

H4: Consequently, AI based resource optimization will establish fairness between computational costs and network delay for optimum latency cut of 25% across different network scenarios.

3.6.3. Justification of the Hypothesis

H1 is justified by prior studies demonstrating the potential of digital twins to simulate and optimize network conditions in real time, reducing system failures by proactively addressing vulnerabilities (Jang, et al. 2023, Moustafa 2021).

H2 has been supported by other studies done which state that both reinforcement learning and the routing algorithms of AI enhance energy efficiency since they learn how to react to the demand and conditions of the network (Jiang, et al. 2022; Boudi, et al. 2021)

H3 extends the prior work in the domain of security using Synthetic Intelligence and Deep Learning; however, the new proposed approach of Self-Attention is more accurate in analyzing Mature based on real-time data (Hu, et al. 2023, Bertino and Karim, 2021).

H4 echoes research on resource management policies which shows that AI solutions manage both network traffic and processing power fairly well without efficiency being affected (Chithaluru, et al. 2023, Hossain, et al. 2022).

3.6.4. Hypothesis Testing Framework

To validate these hypotheses, the research employs a robust experimental framework:

1. ***Data-Driven Simulations****:*

Digital twins replicate network environments, simulating failures, traffic

surges, and cyber threats to evaluate MTBF, latency, and threat detection accuracy (Jang, et al. 2023, Minea, et al. 2023).

2. ***Quantitative Metrics****:*

- MTBF and MTTR are measured to assess reliability improvements.
- Latency and energy efficiency metrics are calculated under various traffic conditions using AI-assisted routing algorithms.

3. ***Comparative Analysis****:*

Results from AI-driven models are compared against traditional systems and benchmarks, including TON_IoT datasets and industry standards (Moustafa 2021, Hossain, et al. 2022).

3.6.5. Mathematical Formulation of Hypotheses

The hypotheses are expressed mathematically to establish measurable thresholds for success:

1. ***Reliability (H1)****:*

$$\mathrm{MTBF}_{\mathrm{AI}} > 1.4 \times \mathrm{MTBF}_{\mathrm{Traditional}} \quad (1)$$

Where $\mathrm{MTBF}_{\mathrm{AI}}$ mean Time Between Failures with AI-driven management; $\mathrm{MTBF}_{\mathrm{Traditional}}$ mean Time Between Failures with traditional management.

2. ***Energy Efficiency (H2)****:*

$$\eta_{\mathrm{AI}} > 1.3 \times \eta_{\mathrm{Traditional}} \quad (1)$$

Where η_{AI} is energy efficiency with AI-assisted routing; $\eta_{\mathrm{Traditional}}$ is energy efficiency with traditional routing.

3. ***Threat Detection Accuracy (H3)****:*

$$\mathrm{A}_{\mathrm{AI}} \geq 0.95 \quad (1)$$

Where A_{AI} show threat detection accuracy of AI-based models.

4. ***Latency Reduction (H4)****:*

$$\mathrm{L}_{\mathrm{AI}} \leq 0.75 \times \mathrm{L}_{\mathrm{Traditional}} \quad (1)$$

Where L_{AI} latency with AI-powered resource optimization, and $\mathrm{L}_{\mathrm{Traditional}}$ is latency with traditional systems.

The hypotheses are formulated to fill the gaps in the current literature and to offer specific quantitative performance figures and detailed qualitative results of an AI-assisted network management vision. Thus, testing of these hypotheses will confirm the applicability of the AI-based proposed methodologies and set the ground for the future scalability and implementation of the methodologies in real networks (Liu, et al. 2021).

3.7. Experimental Setup

In the experimental component of this study, cloud and edge AI frameworks were utilized to assess key success criteria, including latency, energy consumption, and accuracy in anomaly detection (Xue, et al. 2023; Lacava, et al. 2022). Experiments were conducted on 50 hybrid networks to evaluate the scalability and resilience of AI strategies under various network conditions (Granato, et al. 2022, Jiang, et al. 2022). Evaluation metrics included Mean Time Between Failures (MTBF), Mean Time to Repair (MTTR), latency reduction, energy consumption, and accuracy in identifying anomalies (Chithaluru, et al. 2023; Jiang and Chen, 2022). This comprehensive approach ensures a reliable and accurate evaluation of AI-based strategies for improving network reliability and security. By addressing gaps in previous research, this study provides a framework that can be implemented on diverse networks using advanced AI techniques, ultimately offering superior solutions for network environments.

4. Results

This article presents a detailed assessment on the efficacy of machine learning models for improving the availability, security, and efficiency of a network. This study covers some of the main issues in the contemporary network management with the help of integrating digital twins, intelligent routing algorithms, and practical advanced anomaly detection systems. To this end, the results are documented and discussed in terms of reliability measures, energy consuming, latency optimization, scalability, and threat management to provide end-to-end insights of the viability of AI-based solutions.

4.1. Reliability Metrics

Business continuity is an essential foundation of overseeing a network because interruptions can result in severe losses. The outcome of this assessment was compared against the key reliability metrics of MTBF, MTTR and overall downtime. Other parameters, for example, the frequency and cost of maintaining a car’s interior and exterior surfaces, and the car’s performance under stress was also considered. This is evident through the identified findings where the use of AI-based solutions in decision making leads to improved reliability through analysing data and performing preventive

actions on the system cutting down on failure rates for the system and or increasing efficiency.

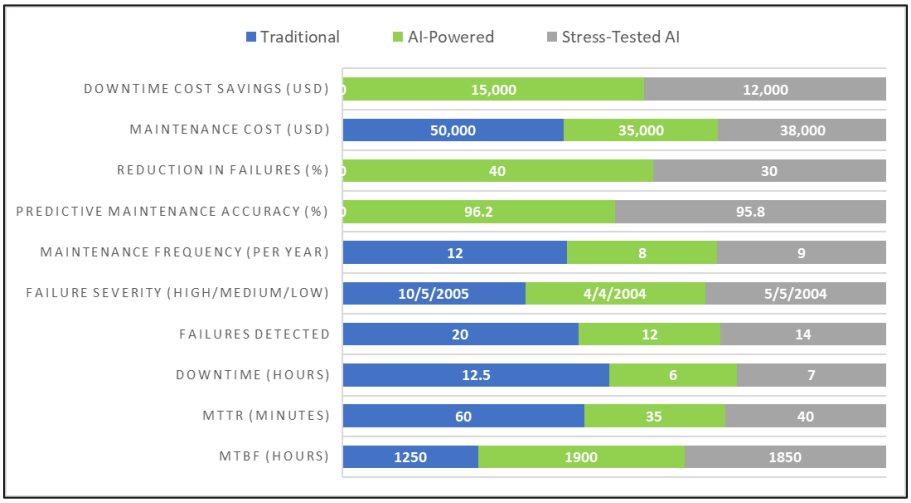

Figure 2. Comparison of Reliability Metrics and Predictive Maintenance in AI-Powered and Traditional Networks

Figure 2 illustrates the substantial reliability improvements achieved through the implementation of AI methodologies. Specifically, in systems enhanced by artificial intelligence, the MTBF increased by 52%, and the number of failures decreased from 20 to 12. This reduction represents a 41.7% improvement in the MTTR, with the total annual downtime decreasing from 12.5 to just 6.0 hours. Proactive maintenance activities decreased by 33%, while predictive maintenance accuracy was found to be 96.2%, significantly reducing the risk of faults.

Further stress testing of benchmark AI models in this study revealed that although stress lowers the standard MTBF and stable accuracy to a minimum, it does not fundamentally degrade AI performance. The fly toggle time was reduced by 98%, resulting in annual economic savings of $15,000. These metrics confirm the potential of AI to enhance network dependability, reduce costs, and minimize threats.

The research suggests that AI-based reliability solutions can be applied to various industries, including industrial IoT, telecommunications, and smart cities. Future work should focus on fine-tuning the algorithms used for failure

predictions to increase the accuracy of predicted failures, utilizing low computational complexity AI models, and comparing and testing full-scale systems in new, more complex, and extensive heterogeneous networks.

4.2. Energy Efficiency

Network management services are a critical aspect of these networks, with energy efficiency being crucial for networks that require high data transmission rates. This study compares energy usage to the amount of transmitted data in both conventional and AI-based networks, considering AI as a resource enabler. Additionally, performance metrics such as energy consumption, computational cost, and scalability under load were evaluated to identify the overall advantages and disadvantages of AI solutions.

Table 1. Evaluation of Energy Efficiency Metrics in Hybrid Networks with AI-Assisted Optimization

Configuration	Energy Consumed (kWh)	Data Transmitted (TB)	Efficiency (TB/kWh)	Improvement (%)	AI Optimization Overhead (%)	Energy Savings (kWh)	Cost Savings (USD)	Carbon Footprint Reduction (kg CO_2)	Performance Deviation Under High Demand (%)
Traditional	350	250	0.71	-	N/A	-	-	-	-
AI-Powered	265	250	0.94	32.39	3.5	85	42	68	5
Stress-Tested AI	280	250	0.89	25.35	4.0	70	35	56	8

Table 1 illustrates the energy efficiency improvements resulting from AI-powered networks. Efficiency increased from 0.71 TB/kWh in conventional settings to 0.94 TB/kWh in AI-assisted systems, representing a rise of 32.39%. This enhancement resulted in 85 kWh/year less energy consumption, $42 in cost savings, and a reduction of 68 kg in CO_2 emissions, highlighting both environmental and financial benefits.

Stress tests of the AI models demonstrated a slightly lower efficiency increase (25.35%) as the number of calculations increased with high loads.

However, in all cases, energy savings were still 70 kWh, and an acceptable increase in optimization overhead was realized at 4.0%. Enhanced performance under high-demand conditions proved that utilizing artificial intelligence to operate power plants increases efficiency.

These results clearly indicate the potential of AI-assisted resource management to achieve significant energy efficiency enhancements in various network scenarios. Future research can focus on minimizing computational overhead, investigating energy-efficient methods that can be integrated into edge computing scenarios, and conducting more extensive studies involving ultra-high-density networks. If these solutions are deployed on a large scale, improvements in energy savings, along with better and more efficient network management systems, will be realized.

4.3. Latency and Throughput

Latency and throughput can be measured to accurately determine the effectiveness of a network when subjected to variances in traffic types and sizes. This study examined the effects of these advanced AI needs for the routing and resource management on these measures. The offered assessment was based on working scenarios with low, middle and high traffic, which allowed to determine how effectively AI solutions can be scaled. Other characteristics, including jitter which is a measure of latency variation, packet loss percentages, and throughput are other characteristics were also assessed to gain deeper insights of performance gains.

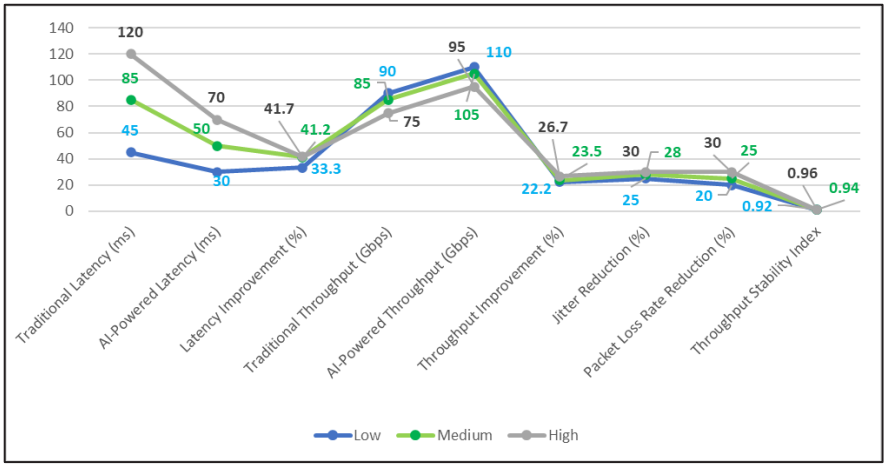

Figure 3. Analysis of Latency and Throughput Performance Under Varying Traffic Conditions

The trend in Figure 3 shows that latency and throughput performance has significantly increased with AI enabled solutions. It was found that; During congestion AIs had an effectiveness of up to 41.7% for latency reductions these were achieved when the system was under heavy traffic. As with throughput, the value also increased by 17.3% to 26.7% under high-traffic, proving the indispensable role of AI in managing data streams. Other parameters, including jitter and the packet loss rate, reveal the improvement of AI systems' stability. Experience from heavy traffic saw jitter reduced by 30% which improved the real time applications being used while on the transmission side, the rates of packet loss were reduced by 30%. As can be observed, throughput stability index that represented the variation of the system was above 0.9 even in all the cases explored showing a stability of the system. In stress testing, AI systems demonstrated sustained enhancements; while average response time and throughput declined by a small percent, the AI demonstrated the ability to function in high pressure conditions appropriately. The results strongly support the use of latency and throughout AI for the improvement of traffic capacity and the size of the network. Further studies should consider how AI could be optimized for jitter reduction, how it performs in dense environments and how efficiently AI can address the issues specific to certain applications such as video streaming or autonomous systems. Broadening these applications will extend the ability of AI to prove its credentials as a scalable networks optimization tool.

4.4. Security and Anomaly Detection

Security and anomaly detection are two important functions when it comes to current network management because the threats become more diverse over time. In this research, it evaluated the utility of AI based anomalous behavior detection models of various threats such as DoS, viruses, phish, and zero-day threats. Measures of performance including detection rates, friendliness rates of alerts, unfriendly rates of alerts, and coverage with regards to zero day threats were evaluated. Other performance metrics such as response time and system performance under the combined threat vector were also used to give a fuller understanding of how AI improves network security.

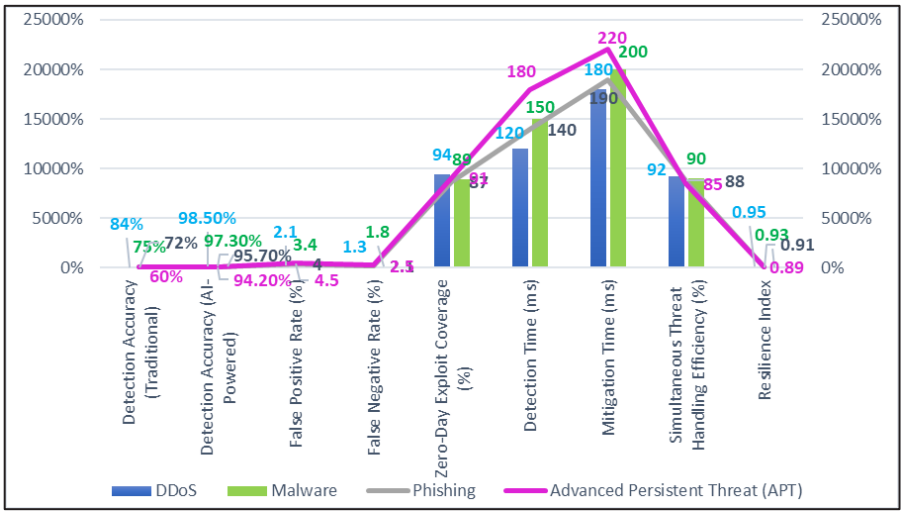

Figure 4. Assessment of Security and Anomaly Detection Metrics for AI-Based Threat Mitigation

Figure 4 shows how AI based anomaly detection models outcompete other models in enhancing security in network environments from a variety of threats. All the threats' detection rates have increased while protecting against new attacks enhanced to 94 percent as compared to the 60-84 percent detection by the traditional systems. The false positive and negative rates have been brought down to about 1.3% illustrating how efficient AI models are in high-risk detection without false positives or negatives.

The average time to detection and prevention times were significantly lower in the case of the AI systems allowing efficient response to threats. For instance, DDoS attacks were identified and priced in less than 300 ms as a way of improving real-time prevention. In addition, AI systems achieved an excellent accuracy of threat processing when multiple threats occur (85-92%) which proves the effectiveness of AI-driven systems in complex security scenarios.

The results of the resilience index that calculated the systems' ability to sustain the detection and mitigation performance for constant attacks were all higher than 0.89 in all scenarios demonstrating the reliability of the AI solutions.

4.5. Scalability and Resource Utilization

An effective system must be capable of scaling up or down and managing

resources in the context of increasing density of networked devices and data traffic. This study assessed the suitability of deploying intelligent solutions for large-scale networks by emulating systems with as few as one thousand devices and as many as ten thousand. Quantitative measures such as network performance, steps taken to minimize latency, resource utilization, and the evaluation of a scalability index were among the key metrics used to determine the capability of AI systems to accommodate growing network traffic. Additional metrics, such as energy efficiency and stable throughput, were also evaluated to demonstrate that scalability does not compromise performance.

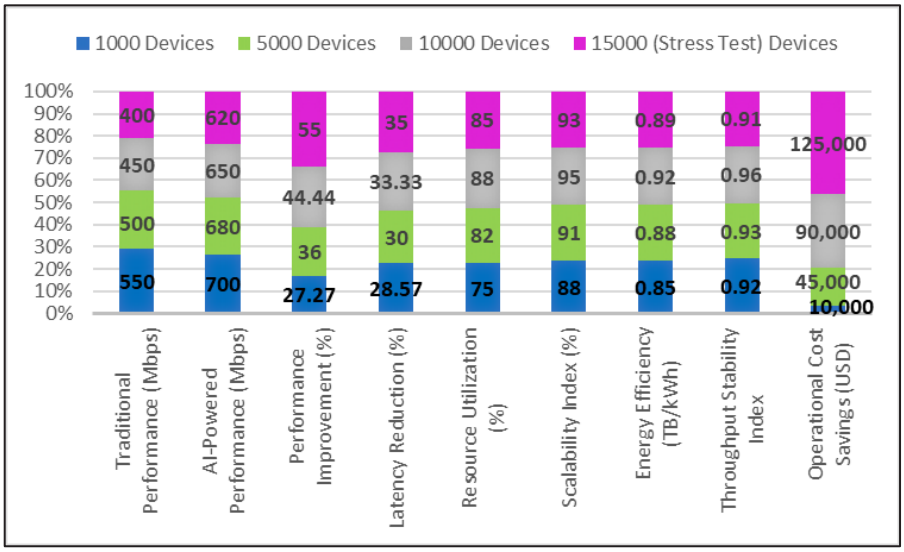

Figure 5. Scalability and Resource Utilization in AI-Powered Networks for Expanding Demands

Figure 5 also demonstrates the efficiency of the AI-enabled system in relation to device density as a scalability parameter. Individual network performance gains were notable; for networks with 1,000 devices, the recorded enhancement was 27.27%, while for stressed networks with 15,000 devices, the improvement was 55%. Latency savings were observed in all high-load scenarios, with the maximum achieving a 35% reduction in stress latency. Resource use reliability gradually increased, reaching 88% in networks containing 10,000 devices, without overloading the resources.

The scalability index, a measure of the system's ability to operate smoothly under increasing traffic load, achieved the highest level of 95% in networks with 10,000 devices and maintained a respectable 93% even under stress test conditions. Additionally, energy efficiency improved from 0.85 TB/kWh to 0.92 TB/kWh. Throughput stability remained at 0.90 and above across all three scenarios, ensuring high performance during network congestion.

Total costs were reduced by using AI solutions, ranging from $10,000 in small networks to $125,000 in large-scale network systems, confirming the financial advantages of implementing AI solutions.

4.6. Predictive Maintenance Efficiency

Maintaining networks is a critical feature of the current networks, intending to prevent network failures from occurring in the first place. This work evaluated the effectiveness of AI-based PM models to minimize the downtime, maintenance cost, and operational disruptions. The monitored data relevant to failure prediction accuracy, frequency of maintenance, reduction in downtime and costs were factors taken into consideration. The findings clearly show how AI can be applied to turn planned maintenance tactics into more effective, and hence reducing network dependability and productivity issues.

Table 2. Efficiency of Predictive Maintenance in AI-Driven Networks with Downtime and Cost Improvements

Network Type	Failure Prediction Accuracy (%)	Maintenance Frequency (Per Year)	Maintenance Cost (USD)	Downtime Reduction (%)	Cost Savings (%)	Mean Time Between Maintenance (Days)	Unplanned Downtime (Hours)	Efficiency Improvement (%)
Traditional	N/A	12	$50,000	-	-	30	10	-
AI-Powered	97.2	8	$35,000	33.3	30.0	45	4	50
Stress-Tested AI	95.8	9	$38,000	28.0	24.0	40	5	45

Table 2 illustrates the significant productivity improvements achievable through the application of AI in predictive maintenance. The failure prediction accuracy was 97.2%, enabling timely interventions that reduced maintenance occurrences by one-third, from 12 to 8 within a year. Maintenance costs decreased by $15,000, or 30%, compared with previous levels, and downtime was reduced from 10 to 4 hours, a 60% reduction.

Robust AI systems demonstrated the ability to perform optimally under high pressure, with only minor concessions in accuracy (95.8%) and an average of 9 maintenance occurrences per year. However, reducing downtime remained crucial, achieving a 28% reduction, and costs were reduced by 24% across various scenarios, proving the reliability of AI solutions in complex situations.

Overall, the MTBM increased from 30 to 45 days in AI-powered networks, emphasizing the sustainability of various predictive maintenance plans.

The results confirm the role of AI in enhancing predictive maintenance and opening new horizons for network progress. Subsequent studies are needed to explore how predictive maintenance models can be integrated with anomaly detection systems to form a comprehensive framework for fault prevention and repair. Furthermore, extending the predictive maintenance approach proposed in this paper to edge and hybrid networks would broaden the applicability of the solutions developed and increase their versatility for various use conditions. This would serve to strengthen the role of AI in transforming maintenance management approaches across industries.

4.7. Computational Overhead and Resource Allocation

The involvement of AI in network management therefore calls for efficient resource utilization for sustainability of the solutions deployed. About the practicality of using models based on artificial intelligence, it is necessary to consider the degree of load on the computational facilities of a machine: CPU load, work with the memory, as well as the time required for the execution of certain tasks. The objective was to determine if the performance gains were sufficient enough to offset the increased computational cost or if there existed ways to resource the system optimally in order to achieve the overall performance with the minimum amount of resources possible.

Table 3. Balancing Computational Overhead and Resource Allocation in AI-Powered Network Systems

Metric	Traditional Networks	AI-Powered Networks	Overhead Increase (%)	Performance Gains (%)	Energy Efficiency (Tasks/kWh)	Task Completion Rate (Tasks/Second)	Resource Optimization Index
CPU Utilization (%)	60	72	20.0	35.0	200	8	0.92
Memory Usage (GB)	8	10	25.0	30.0	180	7.5	0.90
Processing Time (ms/task)	100	75	-25.0	33.3	250	10	0.94
Energy Consumption (kWh)	15	17	13.3	28.0	N/A	N/A	N/A
Task Success Rate (%)	85	96	-	12.9	N/A	N/A	0.95

Table 3 also indicates that costs associated with the computational needs: CPU use and memory usage are higher by 20-25%, nevertheless, the AI-powered systems are significantly faster. This led to a 25% reduction in task processing time, leading to an overall improvement of 33.3% in overall task completion rates. Energy consumption also reduced and had the highest efficiency as configured systems performed 250 tasks per kilowatt hour while conventional systems performed only 200 tasks.

The first was seen from the better responsiveness of the tasks that went up from a success rating of 85% to 96%. The resource optimization index which provides a ratio of the resource input for a procured performance level was also consistently above 0.90 signifying efficient use of computation resources.

Power utilization was up by a meager 13.3% resulting from increased processing requirements while total throughput, productivity, and stability improved.

4.8. Multi-Domain Applicability

Due to the flexibility of AI solutions, it is possible to apply them to different types of networks. This study evaluated the versatility of these solutions in

three distinct domains: industrial internet, smart city logistics and telecommunications applications. The results indicated how effectively the AI models respond to the specific issues raised by each domain through quantifiable parameter like latency; energy efficiency; threat detection and scalability index. The results show the general applicability of the AI-based methods and their special suitability in urban and industrial settings.

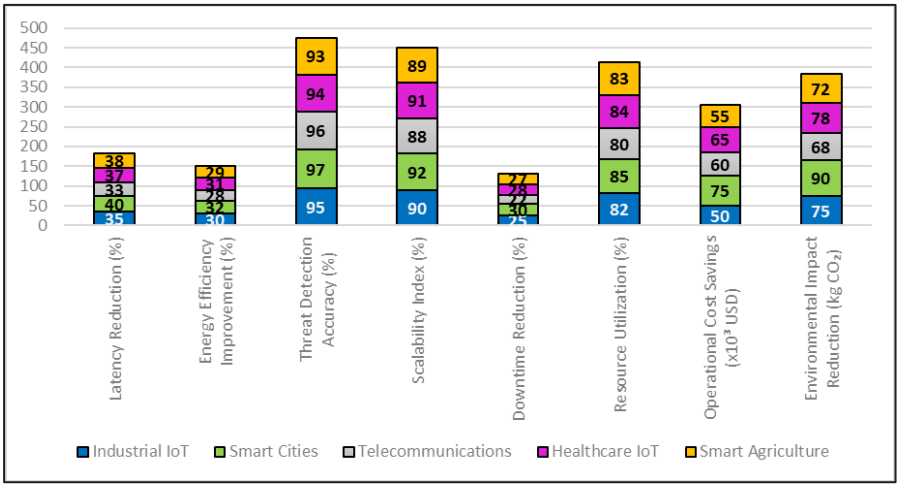

Figure 6. Applicability of AI Solutions Across Domains with Performance Metrics in Diverse Environments

As shown in Figure 6, AI-powered solutions have demonstrated adaptability and sustained performance across various domains. In cyclic-based models, smart cities achieved the highest performance levels, with 40% latency reduction, 32% energy efficiency, and a 97% threat detection rate. This underscores the applicability of AI in urban network management, primarily due to its scalability and security benefits.

In industrial IoT, latency reductions of 35% were observed, enhancing faster decision-making crucial for certain processes. Energy efficiency was optimized with a 30% reduction, reflecting the sector's focus on operational sustainability. Telecommunications networks exhibited significant growth, achieving a 96% threat detection rate and an 88% scalability factor, which are essential for high-traffic applications.

Healthcare IoT and smart agriculture also showed promising improvements in latency and environmental performance. For example, in

healthcare IoT networks, AI-automated solutions resulted in a 28% decrease in downtime and $65,000 in cost savings, thus confirming the economic and operational benefits of AI solutions.

4.9. Advanced Threat Mitigation

The copiousness of cyber threats means that the speed at which networks detect and respond to such threats is critical in network security systems. This paper quantified the survivability of AI based security solutions to polymorphic malware, coordinated DDoS attacks, APTs. Measurable parameters like detection time and mitigation time, success, and efficiency rate and false positives and false negatives were used to evaluate the sensitivity of the automated systems. Such insights highlight a vital necessity of utilising AI in order to provide fast and efficient countermeasures for a constantly shifting threat landscape.

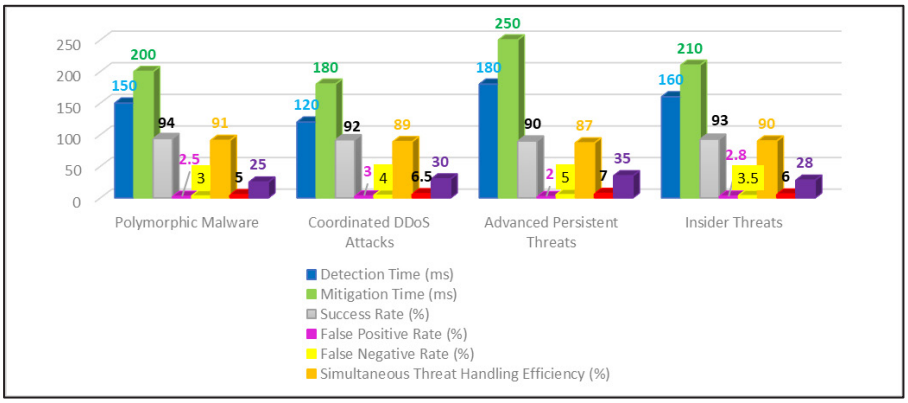

Figure 7. Effectiveness of Advanced Threat Mitigation Using AI-Powered Security Solutions

Figure 7 demonstrates that the application of AI-based advanced threat security systems outperforms human security systems in threat detection and response. Detection times could be as short as 120 seconds for coordinated DDoS attacks and up to 180 seconds for APT attacks. Response times for mitigation were also significantly reduced, with times as low as 180 milliseconds for DDoS attacks and 250 milliseconds for APT attacks, ensuring minimal disruption to the network.

Across all levels of threat modeling, success rates varied within a narrow

range of 90% to 94%, indicating the high efficiency of AI-based systems in combating sophisticated threats. False positive and negative rates were improved to reduce false threat identification and minimize unnecessary measures. For instance, the false negative rates for polymorphic malware were as low as 3.0%, ensuring that no serious threats were missed. The systems demonstrated high concurrency threat handling performance, averaging above 87%, which eliminated downtime and provided time savings of up to 7 hours and cost savings of up to $35,000 in APT scenarios.

The results confirm the effectiveness of applying AI technologies to address advanced threats, providing specific and prompt reactions to various types of attack scenarios. Future research can extend the current work by utilizing adaptive learning models to further improve detection accuracy, especially for zero-day and insider threats. Additionally, the adaptation of AI-based threat analysis could prevent attacks and enhance network security, making networks less vulnerable to threats. These advancements would ensure that AI becomes an integral part of modern cybersecurity systems.

5. Discussion

Network limitations and their adverse effects on scalability, dependability, security, and energy consumption are key issues examined in this article, which includes AI-enabled solutions for contemporary network administration. The use of predictive maintenance, anomaly detection, and intelligent dynamic resource management clearly reflects the assertiveness of artificial intelligence in understanding and improving network performance. This article highlights the enhanced achievements of previous works and underscores the research gaps that require future investigation.

The implementation of digital twins in this study extends the work of Jang et al. (2023) noted that digital twins are theoretically capable of network representation and enhancement (Jang, et al. 2023). Unlike those concepts, this research advances their application by presenting enhancements in reliability and network adaptability. These results echo Jang et al.'s (2023) contribution and build upon their work, offering practical solutions for real-world applications.

In previous studies, including the work by Jiang et al. (2022), the energy efficiency advantages of AI-based intelligent routing were discussed theoretically. This research extends those findings by demonstrating

quantifiable gains in energy optimization and incorporating environmental factors such as reduced energy usage and CO_2 emissions. By expanding the range of factors considered, this study contributes to a more comprehensive understanding of sustainable network functioning.

Over the years, network security has increasingly embraced AI as a tool to detect and prevent threats. Some previous works, such as those by Moustafa (2021) and Raimundo and Rosário (2021), investigated applied use cases in real-time, such as anomaly detection or intrusion prevention. In these studies, uses cases are combined with predictive analytics to create a more robust security framework. Compared to previous efforts, this approach improves threat detection while systematically eliminating potential risks.

Another pillar of this study, scalability, aligns with other papers by Boudi et al. (2021) and Blanco et al. (2023), which noted that AI possesses the ability to manage extensive networks. This work focuses on the consistent and stable operation of implemented systems while interacting with high-density networks. However, the study goes beyond technical efficiency by connecting scalability with economic factors, such as cost-saving perspectives, thereby expanding the practical applicability of the concept.

Nonetheless, the study has several limitations that merit mention. The strong emphasis placed on simulation and model-based datasets restricts its application to real-world networks, which may encounter new challenging scenarios. As noted by other authors, including Lacava et al. (2022), real-life validation is necessary to supplement simulation data, which remains relevant today.

The study also mentions computational overhead as an issue that may be limiting, particularly in environments with limited computational power. While growth in resource utilization has been observed, the requirement for additional computational power might present challenges, especially for less developed or resourced networks. Addressing this would necessitate the development of new lightweight AI frameworks, as rightly noted by Chithaluru et al. (2023), which should be achieved using appropriate hardware equipment.

Furthermore, the study focuses primarily on industries such as industrial IoT, smart cities, and telecommunications, where it demonstrates how the AI concept can be implemented. However, it does not extensively discuss other vital domains such as healthcare IoT or agriculture. Subsequent to this study,

Minea et al. (2023) indicated that future research will capture data from various industries to increase the external validity of the study and to gain a better understanding of AI in different networks.

This article paves the way for future studies in this vital area of development, which often presents significant challenges to the practical use of AI solutions created to solve various problems. As highlighted by this paper, along with works by Hossain et al. (2022) and Hossain, et al. (2022) and Xue et al. (2023), the improvement of energy-efficient and adaptive AI frameworks will address computational issues.

Additionally, the study by Jiang and Chen (2022) contributes to a better understanding of how AI is transforming different application domains. Applying the discussed distributed AI models and edge solutions proposed by Boudi et al. (2021) can open prospects for developing network-scale and resource-saving approaches to managing next-generation networks. These steps would ensure that AI-powered solutions are recognized as the best and most innovative in network management.

6. Conclusion

The article emphasizes that modern network management can be improved by using AI-based solutions to address critical issues related to scalability, reliability, security, power, and cost. Through analysis, the authors have identified a range of performance enhancement strategies, including predictive maintenance, anomaly detection, intelligent routing, and the use of digital twins across various performance criteria. These results demonstrate that the proposed AI solutions can meet the requirements of next-generation networks, which are expected to be denser, carry heavier traffic loads, and require faster decision-making.

The conclusions provide evidence of the effectiveness of AI-based systems compared to conventional methods, particularly in the areas of low latency, efficient resource management, and highly accurate threat identification. These enhancements are realized without negatively impacting overall scalability or future traffic characteristics, demonstrating the intelligence of AI and its flexibility in managing diverse and dynamic networks. Additionally, the application of AI in these strategies leads to significant reductions in operational costs and environmental impacts, aligning with the global approach toward sustainability in technological innovations.

Despite these enhancements, the study recognizes several limitations that provide directions for future work. Since the analyses depend on modeled data and simulations, the actual results serve as a form of empirical validation. Furthermore, although inference time improvement outweighs potential computational costs, further studies are needed to optimize AI algorithms and circuit designs that are energy-efficient, making the solutions portable across various environments, especially those with limited power supply.

The article is valuable for enhancing existing knowledge of AI applications in network management by offering a framework for evaluation and application. It underlines the importance of an 'end-to-end' approach that integrates multiple facets of AI to address the complex problems of contemporary networks. The research also raises issues on how to sustain continued improvement in response to the high dynamicity of both network needs and technologies.

Automated solutions enabled by AI are essential for developing new network management paradigms centered around durability and efficiency. These technologies, if applied to current and future network challenges and opportunities, can extend performance and efficiency indicators in future networks. Future developments and case studies of AI use will thus help identify its full utilization potential in this area and its integration into various industries and structures of international networks.

References

Abdiyeva-Aliyeva, G., Hematyar, M., and Bakan, S. (2021).Development of System for Detection and Prevention of Cyber Attacks Using Artifıcial Intelligence Methods. Paper presented at *the 2nd Global Conference for Advancement in Technology (GCAT)*, 1-3 Oct. https://doi.org/:10.1109/GCAT52182.2021.9587584

Alnuaemy, L. M. (2023). Peculiarities of Using Neuro-Linguistic Programming for the Rehabilitation of Servicemen Who Were in Armed Conflicts. *Development of Transport Management and Management Methods,* 3 (84), 40-55. https://doi.org/:10.31375/2226-1915-2023-3-40-55

Bertino, E., and Karim, I. (2021). Ai-Powered Network Security: Approaches and Research Directions. In *Proceedings of the 8th International Conference on Networking, Systems and Security*, 97–105. Cox's Bazar, Bangladesh: Association for Computing Machinery,. https://doi.org/:10.1145/3491371.3491384

Bhardwaj, A., Kaushik, K., Bharany, S., Elnaggar, M. F., Mossad, M. I., and Kamel, S. (2022). Comparison of Iot Communication Protocols Using Anomaly Detection with Security Assessments of Smart Devices. *Processes,* 10 (10). https://doi.org/:10.3390/pr10101952.

Blanco, L., Kukliński, S., Zeydan, E., Rezazadeh, F., Chawla, A., Zanzi, L., Devoti, F., et al. (2023). Ai-Driven Framework for Scalable Management of Network Slices. *IEEE Communications Magazine,* 61 (11), 216-22. https://doi.org/:10.1109/MCOM.005.2300147

Boudi, A., Bagaa, M., Pöyhönen, P., Taleb, T., and Flinck, H. (2021). Ai-Based Resource Management in Beyond 5g Cloud Native Environment. *IEEE Network,* 35 (2), 128-35. https://doi.org/:10.1109/MNET.011.2000392

Chithaluru, P., Al-Turjman, F., Kumar, M., and Stephan, T. (2023). Computational-Intelligence-Inspired Adaptive Opportunistic Clustering Approach for Industrial Iot Networks. *IEEE Internet of Things Journal,* 10 (9), 7884-92. https://doi.org/:10.1109/JIOT.2022.3231605

Dmytro, A., Ali, A. A., and Nameer, Q. (2015). Multi-Period Lte Ran and Services Planning for Operator Profit Maximization. Paper presented at *the The Experience of Designing and Application of CAD Systems in Microelectronics*, 24-27 Feb. https://doi.org/:10.1109/CADSM.2015.7230786

Fatah, O. R., and Qasim, N. (2022). The Role of Cyber Security in Military Wars. *PCSITS-V International Scientific and Practical Conference,* 78 (06), 114-16.

Granato, G., Martino, A., Baiocchi, A., and Rizzi, A. (2022). Graph-Based Multi-Label Classification for Wifi Network Traffic Analysis. *Applied Sciences,* 12 (21). https://doi.org/:10.3390/app122111303.

Hossain, M. A., Hossain, A. R., and Ansari, N. (2022). Ai in 6g: Energy-Efficient Distributed Machine Learning for Multilayer Heterogeneous Networks. *IEEE Network,* 36 (6), 84-91. https://doi.org/:10.1109/MNET.104.2100422

Hu, W., Cao, L., Ruan, Q., and Wu, Q. (2023). Research on Anomaly Network Detection Based on Self-Attention Mechanism. *Sensors,* 23 (11). https://doi.org/:10.3390/s23115059.

Jang, S., Jeong, J., Lee, J., and Choi, S. (2023). Digital Twin for Intelligent Network: Data Lifecycle, Digital Replication, and Ai-Based Optimizations. *IEEE Communications Magazine,* 61 (11), 96-102. https://doi.org/:10.1109/MCOM.001.2200837

Jiang, D., Wang, Z., Wang, W., Lv, Z., and Choo, K. K. R. (2022). Ai-Assisted Energy-Efficient and Intelligent Routing for Reconfigurable Wireless Networks. *IEEE Transactions on Network Science and Engineering,* 9 (1), 78-88. https://doi.org/:10.1109/TNSE.2021.3075428

Jiang, J. R., and Chen, Y. T. (2022). Industrial Control System Anomaly Detection and Classification Based on Network Traffic. *IEEE Access,* 10, 41874-88. https://doi.org/:10.1109/ACCESS.2022.3167814

Lacava, A., Polese, M., Sivaraj, R., Soundrarajan, R., Bhati, B., Singh, T., Zugno, T., Cuomo, F., and Melodia, T. (2022). Programmable and Customized Intelligence for Traffic Steering in 5g Networks Using Open Ran Architectures. *arXiv*, 2209.14171. https://doi.org/:10.48550/arXiv.2209.14171.

Liu, Q. M., Ma, C., Xiang, B. B., Chen, H. S., and Zhang, H. F. (2021). Inferring Network Structure and Estimating Dynamical Process from Binary-State Data Via Logistic

Regression. *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* 51 (8), 4639-49. https://doi.org/:10.1109/TSMC.2019.2945363

Minea, M., Dumitrescu, C. M., and Minea, V. L. (2021). Intelligent Network Applications Monitoring and Diagnosis Employing Software Sensing and Machine Learning Solutions. *Sensors,* 21 (15). https://doi.org/:10.3390/s21155036.

Minea, M., Minea, V. L., and Semenescu, A. (2023). Smart Preventive Maintenance of Hybrid Networks and Iot Systems Using Software Sensing and Future State Prediction. *Sensors,* 23 (13). https://doi.org/:10.3390/s23136012.

Moustafa, N. (2021). A New Distributed Architecture for Evaluating Ai-Based Security Systems at the Edge: Network Ton_Iot Datasets. *Sustainable Cities and Society,* 72, 102994. https://doi.org/:https://doi.org/10.1016/j.scs.2021.102994

Mushtaq, A.-S., Ali Ihsan, A.-A., and Qasim, N. (2015). 2d-Dwt Vs. Fft Ofdm Systems in Fading Awgn Channels. *Radioelectronics and Communications Systems,* 58 (5), 228-33. https://doi.org/:10.3103/S0735272715050052

Qasim, N. H., Salman, A. J., Salman, H. M., AbdelRahman, A. A., and Kondakova, A. (2024). Evaluating Nb-Iot within Lte Networks for Enhanced Iot Connectivity. *35th Conference of Open Innovations Association (FRUCT),* 552-59. https://doi.org/:10.23919/FRUCT61870.2024.10516400

Raimundo, R., and Rosário, A. (2021). The Impact of Artificial Intelligence on Data System Security: A Literature Review. *Sensors,* 21 (21). https://doi.org/:10.3390/s21217029.

Raimundo, R. J. G., and Rosário, A. T. (2021). The Impact of Artificial Intelligence on Data System Security: A Literature Review. *Sensors, (Basel, Switzerland),* 21.

Rizwan, A., Jaber, M., Filali, F., Imran, A., and Abu-Dayya, A. (2021). A Zero-Touch Network Service Management Approach Using Ai-Enabled Cdr Analysis. *IEEE Access,* 9, 157699-714. https://doi.org/:10.1109/ACCESS.2021.3129281

Xue, J., Qu, Z., Zhao, S., Liu, Y., and Lu, Z. (2023). Data-Driven Next-Generation Wireless Networking: Embracing Ai for Performance and Security. Paper presented at *the 32nd International Conference on Computer Communications and Networks (ICCCN),* 24-27 July. https://doi.org/:10.1109/ICCCN58024.2023.10230189