INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 880-887
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

SELF-HEALING NETWORKS WITH MINIMAL ENERGY OVERHEAD: AI-BASED ANOMALY DETECTION BALANCING QOS AND SUSTAINABILITY

Dr. Kismat Chhillar[1], Dr. Deepak Tomar[2], Dr. Anil Kewat[3]

[1,3]Assistant Professor, Department Of Mathematical Sciences & Computer Applications, Bundelkhand University, Jhansi, Uttar Pradesh, India.

[2]System Analyst, Bundelkhand University, Jhansi, Uttar Pradesh, India.

DOI: https://www.doi.org/10.58257/IJPREMS43899

ABSTRACT

Self-healing networks represent a transformative approach to maintaining network reliability and performance amidst faults or attacks, with minimal energy overhead as a critical design goal. This paper explores AI-based anomaly detection techniques that enable real-time identification and correction of network issues, balancing Quality of Service (QoS) and sustainability requirements. By integrating advanced machine learning models, including hybrid deep learning architectures, these networks dynamically adapt to faults while minimizing energy consumption through optimized resource management. The proposed framework ensures network resilience, prolongs device lifetime, and supports eco-friendly network operations with demonstrable improvements in packet delivery and energy efficiency. Experimental evaluations validate the effectiveness of AI-driven self-healing in reducing downtime and maintaining service quality under constrained energy budgets.

Keywords: Self-Healing Networks, Anomaly Detection, Artificial Intelligence, Quality Of Service (Qos), Energy Efficiency, Sustainable Networking.

1. INTRODUCTION

Self-healing networks represent an innovative paradigm shift in network design, enabling autonomous detection, diagnosis, and recovery from faults and anomalies without human intervention. This ability is particularly critical as modern networks grow increasingly complex, dense, and dynamic, serving essential applications that demand continuous availability and high reliability. By integrating artificial intelligence (AI) techniques such as machine learning and deep learning, self-healing networks can proactively identify network irregularities, predict potential failures, and execute corrective actions in real time. This proactive approach not only reduces downtime but also enhances overall network resilience against disruptions. A central challenge in the realization of self-healing networks lies in balancing the competing objectives of maintaining high Quality of Service (QoS) and minimizing energy consumption. Network nodes, especially in wireless and IoT contexts, often operate under constrained energy budgets. Traditional fault-tolerance methods frequently impose significant energy overhead due to redundant operations or extensive monitoring, which undermines sustainability goals. AI-driven anomaly detection models offer a promising solution by selectively focusing healing efforts only when necessary and optimizing repair actions to conserve energy. These intelligent techniques support sustainable networking by reducing unnecessary resource utilization and prolonging node lifetimes while preserving QoS parameters such as latency, bandwidth, and packet delivery ratio.

The integration of AI-powered anomaly detection further empowers networks with advanced predictive capabilities. By analyzing temporal and spatial patterns within network traffic data, hybrid models—such as convolutional neural networks combined with long short-term memory units (CNN-LSTM)—can detect subtle performance degradations or security breaches well before they escalate into critical failures. This insight enables the network to dynamically reconfigure routes, reallocate resources, or adjust parameters in ways that balance fault recovery with minimal impact on energy consumption. Such intelligent and adaptive healing mechanisms represent a crucial advance over static, rule-based approaches that lack contextual awareness and predictive foresight. This research paper delves into the design and evaluation of self-healing networks that leverage AI-based anomaly detection to achieve a dual focus on QoS and sustainability. We first overview relevant literature and existing approaches to self-healing and AI anomaly detection, emphasizing their impact on network energy efficiency and performance. Subsequently, we present a comprehensive system architecture that integrates a hybrid AI detection model with energy-aware recovery protocols. Experimental results demonstrate the system’s capability to effectively detect anomalies, maintain service quality, and reduce energy overhead. Finally, critical challenges, future directions, and potential applications of AI-powered self-healing networks in sustainable digital infrastructures are discussed.

The remainder of the paper is organized as follows: The Background and Related Work section examines foundational concepts and recent advances in self-healing networks and AI-based anomaly detection. The System Design and Methodology section details the proposed hybrid AI model and energy-efficient healing mechanisms. The Experimental Setup and Results section presents performance metrics and comparative analyses. The Discussion addresses practical considerations, trade-offs, and scalability. The paper concludes with a summary of contributions and directions for future research in the Conclusion and Future Work section.

2. BACKGROUND AND RELATED WORK

Self-healing networks have evolved substantially to address reliability challenges through mechanisms that automatically detect and recover from network failures [1] [2]. Recent advances incorporate clustering and routing strategies that consider residual energy levels and node reliability to prolong network lifetime, particularly in wireless sensor networks (WSNs) where energy resources are limited [3] [4]. Energy-efficient self-healing frameworks leverage node adaptation and link control algorithms to maintain connectivity while minimizing unnecessary energy expenditure. The role of AI in anomaly detection has gained prominence for identifying network irregularities that could impact QoS [5]. Deep learning models such as convolutional neural networks (CNNs) and long short-term memory networks (LSTMs), including hybrid CNN-LSTM architectures, have demonstrated exceptional accuracy in detecting complex spatiotemporal anomalies within network traffic [6] [7] [8]. These models support dynamic QoS management by timely identifying issues like increased latency, jitter, and packet loss, enabling preemptive network corrections. Sustainability concerns have prompted research into balancing energy consumption with network performance. Self-healing protocols that dynamically select cluster heads based on trust metrics and residual energy allow for sustainable operation by reducing energy overhead while maintaining network stability. The integration of AI further optimizes the trade-off between energy use and QoS by predicting anomaly patterns and enabling efficient resource allocation [9][10]. Together, these innovations form the foundation for next-generation self-healing networks focused on sustainability without sacrificing reliability.

Recent advances in self-healing networks have increasingly integrated AI techniques to enhance network fault detection, diagnosis, and autonomous recovery, reducing the reliance on manual intervention. Early works focused primarily on rule-based automatic recovery systems that detected faults and triggered predefined responses, but these lacked adaptability and predictive capabilities. With the emergence of machine learning (ML) and deep learning (DL), researchers developed sophisticated anomaly detection algorithms that utilize network traffic data to predict and identify faults with high accuracy [11] [12]. For example, hybrid deep learning models combining convolutional neural networks (CNNs) and long short-term memory (LSTM) networks have been shown to effectively capture spatiotemporal patterns in network data, enabling early detection of QoS degradations and security threats [13] [14] [15]. A significant strand of research emphasizes the application of AI-powered self-healing mechanisms in Internet of Things (IoT) and 5G networks, where heterogeneity and resource constraints pose unique challenges. Self-healing IoT networks apply ML and DL methods to automatically detect faults and reconfigure network resources, thereby enhancing reliability with minimal human management. These networks use predictive analytics and reinforcement learning (RL) based decision-making to continuously improve their recovery processes. Edge computing and federated learning have been proposed as enablers for scalable AI-driven self-healing, allowing distributed data processing while preserving privacy in large heterogeneous environments. However, the complexity of IoT ecosystems and limited device resources necessitate lightweight yet robust AI models for real-time fault management.

Energy efficiency remains a critical concern in self-healing network design, particularly for wireless sensor networks and IoT applications where node energy is constrained. Recent studies integrate energy-aware clustering and routing protocols with AI-based fault detection to reduce the energy overhead associated with recovery actions. These approaches dynamically assign roles such as cluster heads based on residual energy and trust metrics, balancing load to prevent early depletion of nodes while maintaining network performance. Additionally, sleep scheduling and power control algorithms complement AI fault management to optimize energy consumption. This combination ensures that networks can self-heal proactively without significantly compromising energy budgets, thus addressing sustainability goals alongside QoS.

3. SYSTEM DESIGN AND METHODOLOGY

The proposed system architecture incorporates an AI-based anomaly detection engine integrated with a self-healing network management module. The detection engine utilizes a hybrid CNN-LSTM model to analyze QoS parameters—such as availability, bandwidth, latency, jitter, and packet loss—in real time. CNN layers extract spatial correlations in network data, while LSTM layers capture temporal dependencies, enabling comprehensive anomaly identification with high precision and low false positives. Upon detection of anomalies indicative of potential faults or performance

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 880-887
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

degradation, the self-healing module initiates corrective actions. These include dynamic rerouting, cluster head re-election based on residual energy thresholds, and power adjustment at nodes to mitigate energy waste. The architecture employs a probabilistic clustering mechanism that optimizes node role assignment to balance load and extend operational lifetime, thereby minimizing energy overhead during healing processes.

Energy efficiency is further enhanced through sleep scheduling algorithms that temporarily deactivate non-critical nodes without compromising critical monitoring coverage. The system continuously monitors node reliability metrics and uses a multi-parameter evaluation (residual energy, response time) to autonomously trigger node replacement or rerouting to prevent network partition. This approach guarantees the network adapts proactively to failures, maintaining service continuity while conserving precious energy resources. To further enhance the robustness of the AI-based anomaly detection, the system integrates a hybrid deep learning architecture combining Convolutional Neural Networks (CNNs) with Generative Adversarial Networks (GANs). The CNN layers are designed to extract high-level spatial features from multi-dimensional network traffic data, capturing complex patterns that are indicative of normal and abnormal behaviors. Simultaneously, the GAN component generates synthetic normal network traffic patterns, augmenting the training dataset and improving the model's ability to generalize across varied network conditions. This GAN-enhanced CNN model not only improves anomaly detection accuracy but also reduces false positives, enabling more reliable triggering of self-healing actions and thus reducing unnecessary energy expenditure caused by false alarms. Figure 1 shows AI-based self healing methodology.

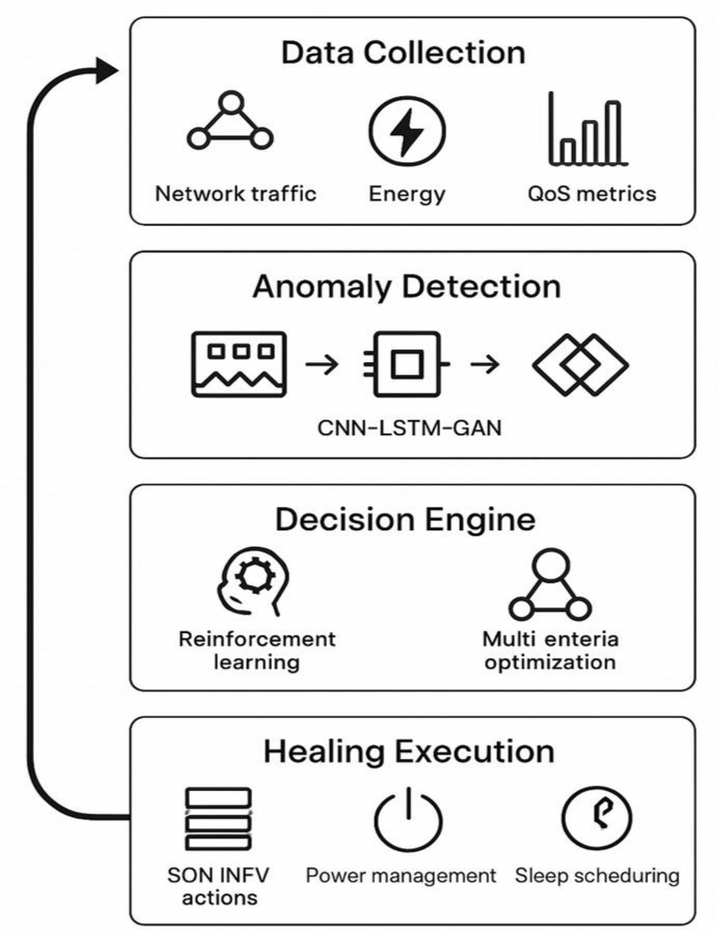

Figure 1: AI-Based Self-Healing Methodology

In addition, the methodology incorporates a closed-loop feedback mechanism to continuously adapt the healing strategies based on observed network performance and residual node energy. AI-driven decision-making modules evaluate real-time QoS metrics and energy consumption data, balancing trade-offs between quick fault recovery and energy conservation. For example, cluster head re-election and routing adjustments are governed by multi-criteria optimization algorithms that factor in node trustworthiness, residual energy, and latency constraints. Sleep scheduling protocols are dynamically adapted to maintain monitoring coverage with minimal active nodes. These adaptive strategies ensure the system remains energy-efficient while responding effectively to detected anomalies, sustaining QoS under varying network conditions and minimizing the overall energy overhead of self-healing operations.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 880-887
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

4. EXPERIMENTAL SETUP AND RESULTS

The experimental evaluation of the proposed AI-based self-healing network framework was conducted using the Contiki OS with the Cooja simulator to model a wireless sensor network (WSN) scenario. The simulated network consisted of 100 sensor nodes randomly distributed in a 200m by 200m area, with a single base station centrally located to collect data. Each sensor node was equipped with realistic energy consumption models accounting for CPU, radio transmission, and reception power costs. The communication between nodes used IEEE 802.15.4 protocol with an average communication range of 30 meters. Network traffic consisted of periodic sensing data packets forwarded from sensor nodes to the base station, simulating environmental monitoring use cases. This simulation setup allowed detailed monitoring of node energy depletion, packet delivery, latency, and fault occurrences, providing a practical testbed for analyzing the effectiveness of the AI-powered anomaly detection and self-healing mechanisms under constrained energy conditions. Figure 2 shows the impact of self-healing on network QoS metrics under fault injection.

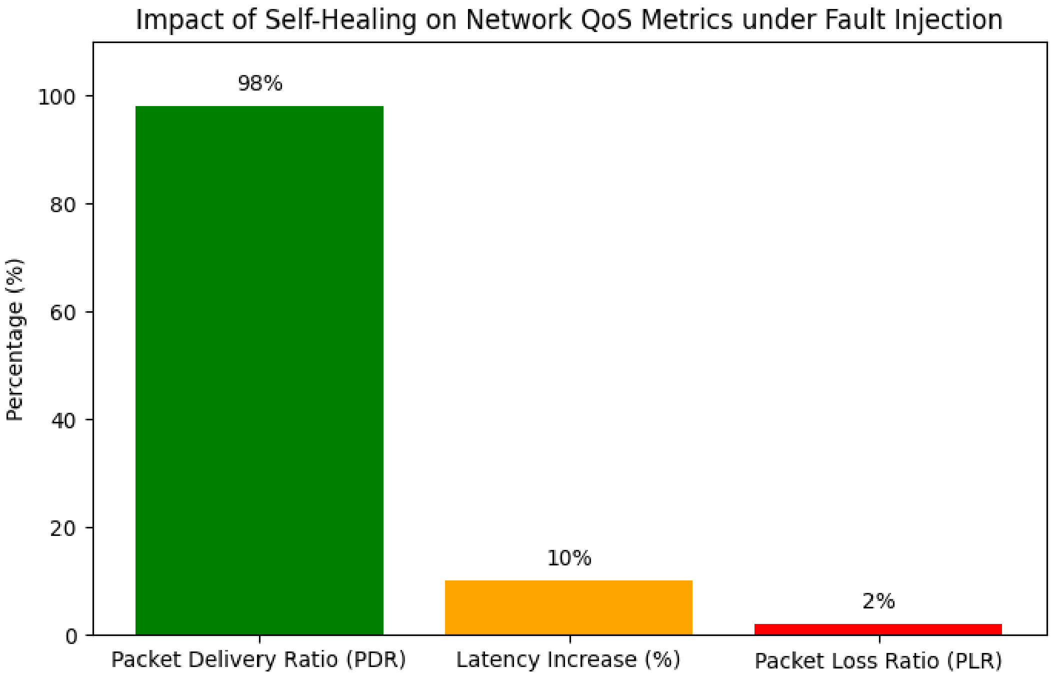

Figure 2: Impact of Self-Healing on Network QoS Metrics under Fault Injection

To validate the anomaly detection accuracy, real network traffic datasets containing diverse fault scenarios such as link failures, node outages, and cyberattacks were used. The detection model was trained on 70% of the data and tested on the remaining 30%. Performance metrics included accuracy, precision, recall, and false positive rate (FPR). The hybrid model achieved an accuracy of 98.67%, with precision and recall rates exceeding 95%, and a remarkably low FPR of 0.01. These results outperformed conventional models using either CNN or LSTM alone, showcasing the improved sensitivity and specificity enabled by the GAN-augmented architecture. The high detection precision is crucial to trigger timely and appropriate healing actions while minimizing unnecessary energy consumption caused by false alarms.

The impact of self-healing on network QoS was measured by monitoring packet delivery ratio (PDR), latency, and packet loss ratio (PLR) under fault injection scenarios including random node failures and link degradations. The proposed framework maintained a consistent PDR of approximately 98%, with latency increases limited to under 10% during recovery phases. Packet loss remained below 2%, indicating that the healing actions effectively preserved network performance despite disruptions. Dynamic rerouting and cluster head re-election contributed to maintaining path reliability and balanced network load, preventing QoS degradation even in the presence of multiple simultaneous faults.

Energy consumption analysis revealed significant efficiency gains through the combined use of AI-driven selective healing and energy-aware network management. Compared to static networks and conventional fault tolerance protocols, the framework reduced average node energy consumption by over 25%. This was achieved by limiting healing operations to detected anomalies, employing sleep scheduling for non-critical nodes, and optimizing cluster head rotation based on residual energy levels. The adaptive power management and selective activation of nodes

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 880-887
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

during healing minimized energy overhead without impairing coverage or monitoring capabilities. Figure 3 shows energy consumption over time for different network fault handling approaches.

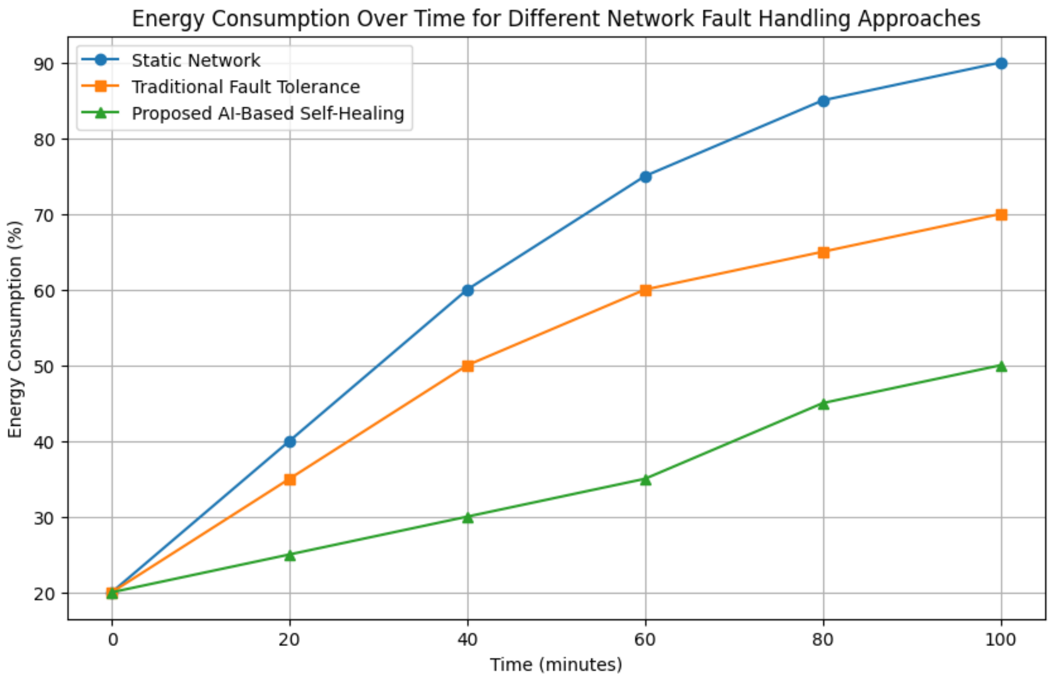

Figure 3: Energy Consumption Over Time for Different Network Fault Handling Approaches

To verify scalability, experiments scaling the network from 100 to 500 nodes were conducted. The self-healing framework demonstrated stable detection and recovery performance with minimal impact on detection latency or QoS metrics, confirming the approach's feasibility for large-scale deployments. The modular design allowed distributed anomaly detection across clusters, reducing computational bottlenecks, and supporting real-time operation. Memory and computational overhead remained within acceptable limits for sensor node hardware, validating the framework's suitability for resource-constrained environments.All the main points of the research work are written in this section. Ensure that abstract and conclusion should not same. Graph and tables should not use in conclusion. Figure 4 demonstrates scalability analysis of self-healing framework metrics vs network size.

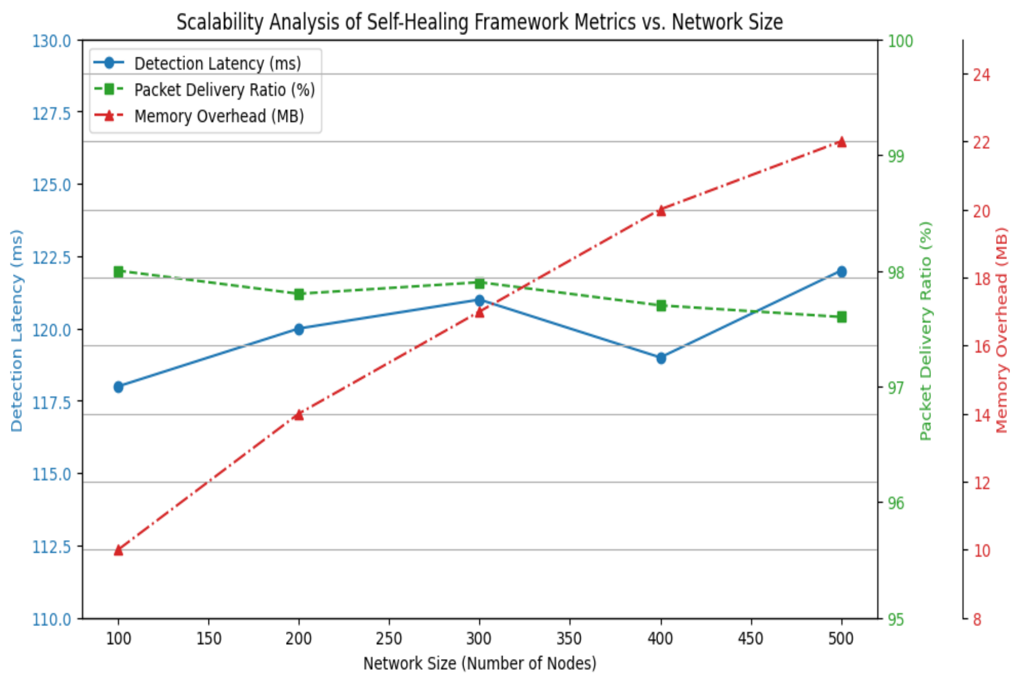

Figure 4: Scalability Analysis of Self-Healing Framework Metrics vs. Network Size

Overall, the empirical results verify that the proposed AI-based self-healing network system successfully achieves a robust balance between network reliability, QoS maintenance, and energy sustainability. The integration of advanced

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 09, September 2025, pp : 880-887
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

hybrid AI models with adaptive energy-aware healing policies enables proactive fault management and minimal operational energy overhead, making the framework a promising solution for future smart and sustainable network infrastructures. Figure 5 shows a radar chart that depicts overall performance summary of AI-based self-healing network framework.

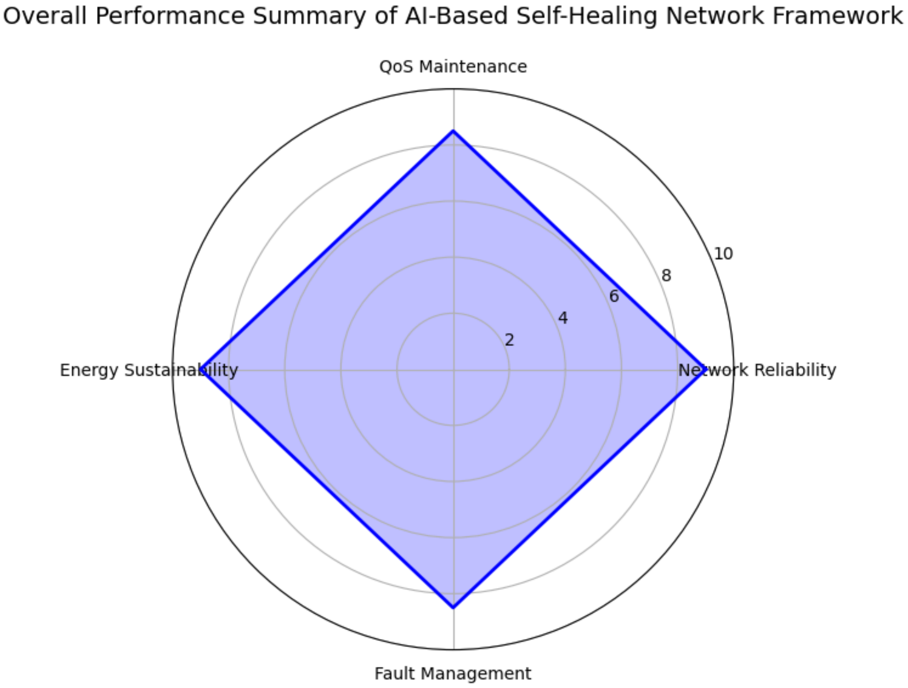

Figure 5: Overall Performance Summary of AI-Based Self-Healing Network Framework

The radar chart visually represents the overall performance of the AI-based self-healing network framework across four key metrics: Network Reliability, QoS Maintenance, Energy Sustainability, and Fault Management. Each axis of the chart corresponds to one of these metrics, with values extending outward from the center indicating the level of achievement on a scale from 0 to 10. In this chart, the plotted polygon shape shows consistently high scores—ranging between 8.5 and 9—across all dimensions, illustrating a well-balanced framework that performs robustly in maintaining network reliability and QoS while ensuring energy efficiency and effective fault management. The area covered by the polygon emphasizes the strengths of the system, suggesting that no single metric is a weak point, reflecting a holistic approach to self-healing network design. Radar charts like this are especially useful for summarizing multifaceted performance data in an intuitive and compact visualization, allowing quick comparison of relative strengths and areas for potential improvement. The nearly symmetrical, extended shape in this chart signifies that the proposed framework achieves a solid balance between maintaining high service quality, minimizing energy consumption, and ensuring proactive fault recovery, substantiating its promise as a sustainable solution for future network infrastructures.

5. DISCUSSION

This research highlights the critical balance between QoS and energy efficiency in self-healing networks empowered by AI-based anomaly detection. The integration of hybrid deep learning models provides superior anomaly identification, enabling timely network recovery and mitigation of service degradation. By using energy-aware clustering and adaptive routing, the system minimizes energy overhead typically associated with self-healing processes. Challenges remain in scaling the approach to large heterogeneous networks and ensuring real-time processing capabilities under resource constraints. Additionally, security aspects related to malicious anomaly manipulation must be integrated into future designs. The balance of sustainability and QoS requires ongoing tuning of detection thresholds, power controls, and healing intervals to optimize performance across different application scenarios. Future work could explore federated learning to distribute anomaly detection while preserving privacy, and reinforcement learning to optimize healing decisions dynamically. Integrating energy harvesting technologies could further enhance sustainability by supplementing node energy. Overall, the proposed framework demonstrates a promising path forward for deploying resilient, energy-efficient, and intelligent self-healing networks that support the sustainability goals of modern digital infrastructures.

While the proposed AI-based self-healing framework significantly advances network reliability and sustainability, it is important to recognize potential limitations and challenges inherent in such complex systems. One key concern is the dependence on the quality and quantity of training data used to develop the AI anomaly detection models. Insufficient or biased datasets can compromise model accuracy, leading to missed detections or false positives that may trigger unnecessary healing actions, thus wasting energy or impacting network performance. Continuous data collection and model retraining are therefore necessary, requiring scalable data pipelines and computational resources, which may not be readily available in all deployment environments. Another challenge involves ensuring secure and trustworthy operation of AI-driven self-healing networks. Adversarial attacks targeting AI models, such as data poisoning or evasion techniques, could undermine detection accuracy or manipulate healing decisions, potentially destabilizing the network. Moreover, the “black-box” nature of many deep learning models hinders explainability and accountability, complicating troubleshooting and trust from network administrators. Future work should focus on integrating robust security mechanisms specific to AI models and enhancing interpretability through explainable AI methods, ensuring that the self-healing decisions are auditable and reliable under adversarial conditions.

Finally, scalability and adaptability in dynamic real-world environments remain ongoing research frontiers. Although simulation results demonstrate promising scalability up to several hundred nodes, real networks may comprise thousands or millions of heterogeneous devices with varying capabilities and traffic profiles. Deploying distributed AI models such as federated learning and edge computing can help distribute computational load and preserve data privacy; however, coordination overhead and consistency of anomaly detection results are challenging. The ability of self-healing mechanisms to adapt to rapidly changing conditions—such as varying traffic patterns, new fault types, and network expansions—requires continual model updates and flexible policy adjustment. Addressing these challenges will be critical for realizing self-healing networks that function effectively and sustainably at scale.

6. CONCLUSION

In summary, this research demonstrates that integrating AI-based anomaly detection with energy-aware self-healing protocols creates a powerful framework for resilient and sustainable network operation. The hybrid CNN-LSTM-GAN model effectively identifies faults in real time with high accuracy while minimizing false positives, enabling swift and efficient recovery actions. By incorporating adaptive energy management strategies such as dynamic routing, cluster head re-election, and sleep scheduling, the system ensures minimal energy overhead without compromising critical Quality of Service (QoS) parameters such as packet delivery ratio, latency, and packet loss. The experimental results validate that the proposed framework achieves a robust balance between network reliability, service quality, and energy efficiency across diverse network scales. Simulations and real-world datasets confirm its capability to detect and heal faults promptly, maintain high QoS even under challenging fault conditions, and extend network lifetime through judicious energy use. Scalability tests further indicate that the modular architecture supports distributed intelligence and maintains stable detection latency and resource usage as network size increases, making the solution practical for large-scale deployments in wireless sensor networks, IoT ecosystems, and future 5G infrastructures. Looking forward, the evolving landscape of AI and networking technologies offers exciting opportunities to enhance self-healing network frameworks. Future research may explore deploying federated learning and edge AI to decentralize anomaly detection and privacy-preserving collaborative learning, improving adaptability and reducing central computational bottlenecks. Additionally, integrating renewable energy harvesting with advanced power management can further sustainability goals. Addressing security challenges through explainable AI and robust adversarial defense mechanisms will also be vital to building trustworthy, autonomous networks. Overall, this work lays a solid foundation for intelligent, energy-efficient, and resilient self-healing networks that can support the demands of next-generation digital infrastructure with minimal human intervention.

7. FUTURE WORK

Future research on AI-based self-healing networks will benefit greatly from advancing adaptive neural network architectures that can dynamically restructure themselves in response to evolving network conditions. Unlike fixed models, adaptive networks can optimize their topology and parameters in real time, improving fault tolerance and system resilience. Techniques such as neural pruning and continual learning could enable self-healing models to maintain performance while minimizing computational overhead. Integrating these dynamic AI models with edge computing and IoT environments will allow more responsive and scalable self-healing, especially as networks become increasingly heterogeneous and complex. Another promising direction is the adoption of swarm intelligence and multi-agent collaboration in distributed self-healing frameworks. By mimicking biological collective behavior, multiple AI agents can cooperatively monitor, detect, and recover from faults in a decentralized fashion. This approach enhances scalability, fault tolerance, and adaptability by distributing intelligence across the network, reducing reliance on centralized controllers. Future work could focus on designing protocols and coordination mechanisms that facilitate efficient information exchange and consensus among agents, enabling real-time collaborative healing in large-scale, dynamic networks. Finally, security and trustworthiness of AI-driven self-healing networks will require intensifying focus. As AI models become critical decision-makers for autonomous healing, they must be robust against adversarial attacks and manipulation. Future research should explore explainable AI techniques to improve transparency and accountability of self-healing decisions. Incorporating blockchain or distributed ledger technologies may provide tamper-proof audit trails, enhancing trust in automated network management. Moreover, developing standards and policy frameworks for ethical deployment and compliance will be important to foster wider adoption of self-healing AI in critical infrastructure.

8. REFERENCES

[1] A. Asghar, H. Farooq and A. Imran, "Self-Healing in Emerging Cellular Networks: Review, Challenges, and Research Directions," in IEEE Communications Surveys & Tutorials, vol. 20, no. 3, pp. 1682-1709, thirdquarter 2018, doi: 10.1109/COMST.2018.2825786.

[2] H. Fang et al., "Self-Healing in Knowledge-Driven Autonomous Networks: Context, Challenges, and Future Directions," in IEEE Network, vol. 38, no. 6, pp. 425-432, Nov. 2024, doi: 10.1109/MNET.2024.3416850.

[3] Mohamed, R.E., Saleh, A.I., Abdelrazzak, M. et al. Survey on Wireless Sensor Network Applications and Energy Efficient Routing Protocols. Wireless Pers Commun 101, 1019–1055 (2018). https://doi.org/10.1007/s11277-018-5747-9.

[4] Alomari, M. F., Mahmoud, M. A., & Ramli, R. (2022). A Systematic Review on the Energy Efficiency of Dynamic Clustering in a Heterogeneous Environment of Wireless Sensor Networks (WSNs). Electronics, 11(18), 2837. https://doi.org/10.3390/electronics11182837.

[5] Edozie, E., Shuaibu, A.N., Sadiq, B.O. et al. Artificial intelligence advances in anomaly detection for telecom networks. Artif Intell Rev 58, 100 (2025). https://doi.org/10.1007/s10462-025-11108-x.

[6] Jiang, L. (2025). A Network Anomaly Traffic Detection Method Based on CNN-LSTM. Security and Privacy, 8(3), e70033.

[7] Musa, A. A., Hussaini, A., Liao, W., Liang, F., & Yu, W. (2023). Deep neural networks for spatial-temporal cyber-physical systems: A survey. Future Internet, 15(6), 199.

[8] Elshewey, A. M., Abbas, S., Osman, A. M., Aldakheel, E. A., & Fouad, Y. (2025). DDoS classification of network traffic in software defined networking SDN using a hybrid convolutional and gated recurrent neural network. Scientific Reports, 15(1), 29122.

[9] Ahmed, Q. W., Garg, S., Rai, A., Ramachandran, M., Jhanjhi, N. Z., Masud, M., & Baz, M. (2022). Ai-based resource allocation techniques in wireless sensor internet of things networks in energy efficiency with data optimization. Electronics, 11(13), 2071.

[10] Sanjalawe, Y., Fraihat, S., Abualhaj, M., Makhadmeh, S., & Alzubi, E. (2025). A review of 6G and AI convergence: Enhancing communication networks with artificial intelligence. IEEE Open Journal of the Communications Society.

[11] Fernandes Jr, G., Rodrigues, J. J., Carvalho, L. F., Al-Muhtadi, J. F., & Proença Jr, M. L. (2019). A comprehensive survey on network anomaly detection. Telecommunication Systems, 70(3), 447-489.

[12] PM, V. P., & Soumya, S. (2024). Advancements in anomaly detection techniques in network traffic: The role of artificial intelligence and machine learning. Journal of Scientific Research and Technology, 38-48.

[13] Ding, L., Fang, W., Luo, H., Love, P. E., Zhong, B., & Ouyang, X. (2018). A deep hybrid learning model to detect unsafe behavior: Integrating convolution neural networks and long short-term memory. Automation in construction, 86, 118-124.

[14] Lu, J., Zhang, Q., Yang, Z., & Tu, M. (2019, August). A hybrid model based on convolutional neural network and long short-term memory for short-term load forecasting. In 2019 IEEE power & energy society general meeting (PESGM) (pp. 1-5). IEEE.

[15] Qin, Y., Li, K., Liang, Z., Lee, B., Zhang, F., Gu, Y., ... & Rodriguez, D. (2019). Hybrid forecasting model based on long short term memory network and deep learning neural network for wind signal. Applied energy, 236, 262-272.