

REVIEW OF THE ARTICLE

«AI AGENTS FOR AUTOMATED NETWORK INCIDENT DETECTION AND MISCONFIGURATION IDENTIFICATION»

The submitted article is devoted to a highly relevant problem in the field of computer science and enterprise infrastructure management — the application of artificial intelligence agents to the automated detection of network incidents and identification of infrastructure misconfigurations. The growing scale, heterogeneity, and complexity of modern enterprise networks make traditional monitoring and manually driven incident response increasingly demanding, which determines the practical importance of the research presented in the article.

A notable feature of the study is its integrated approach to the problem. Rather than considering anomaly detection, infrastructure modeling, and incident remediation as separate technological tasks, the authors propose combining them into a unified operational framework. The integration of graph neural networks, Nautobot as a source of infrastructure truth, and Ansible-based automated remediation creates a coherent technological chain extending from telemetry analysis and contextual incident recognition to automated response.

The theoretical part of the article provides a useful classification of AI-agent architectures applicable to network telemetry analysis. The comparison of LLM-based agents, rule-based evaluators, conventional machine-learning anomaly detectors, graph neural networks, and hybrid LLM-GNN architectures allows the reader to assess the respective capabilities of these approaches in terms of detection, latency, enterprise integration, and explainability. This comparative perspective strengthens the analytical value of the research and clearly demonstrates the advantages of combining complementary AI techniques.

Particular scientific interest is associated with the use of graph-based reasoning for network anomaly detection. Enterprise infrastructure is inherently characterized by numerous relationships between devices, interfaces, services, policies, and communication paths. The proposed use of graph neural networks

makes it possible to account for these dependencies rather than relying exclusively on isolated telemetry values or predefined thresholds. This provides a more context-aware approach to identifying abnormal behavior and infrastructure inconsistencies.

The section addressing network misconfigurations further develops this approach by examining several practically significant categories, including VLAN drift, ACL conflicts, routing anomalies, rogue access points, interface and MTU mismatches, and BGP/OSPF neighbor anomalies. The correlation of detection techniques with false-positive rates, remediation feasibility, and vendor coverage gives the proposed framework a pronounced applied character. It demonstrates that the authors consider not only the detection of an abnormal event but also the feasibility of subsequent automated action.

Another important contribution of the article is the quantitative assessment of operational effects. The comparison between conventional NOC workflows and the proposed AI-assisted model addresses such practically important indicators as mean time to detect, mean time to respond, analyst workload, operational cost per incident, alert noise, and compliance reporting efficiency. The presented modeling indicates substantial potential improvements across these dimensions and provides an understandable basis for assessing the organizational value of intelligent network operations.

The proposed framework is also noteworthy from the perspective of automation maturity. The use of confidence thresholds, rollback-enabled remediation procedures, infrastructure source-of-truth principles, and continuous audit trails reflects an understanding that enterprise AI systems must operate within controlled and traceable processes. This makes the research relevant not only to the technical design of network monitoring systems but also to broader questions of operational reliability, governance, and enterprise digital transformation.

The practical significance of the research is particularly high for large organizations operating complex and distributed network infrastructures. The

proposed architecture can contribute to reducing the amount of routine manual work performed by network operations teams, accelerating incident localization and response, reducing alert fatigue, and improving the consistency of remediation procedures. The framework also creates opportunities for further integration of intelligent network management with security, compliance, and infrastructure automation processes.

The article is logically structured and presents a consistent progression from identification of the research gap and analysis of existing technological approaches to the development of an integrated framework and assessment of its operational implications. The conclusions correspond to the stated objectives and emphasize the potential of AI-agent architectures as an important component of scalable and adaptive enterprise network management.

Overall, the article makes a meaningful contribution to the discussion of intelligent network operations by bringing together several technological directions that are often examined independently. Its combination of AI-agent reasoning, graph-based network modeling, infrastructure-as-source-of-truth principles, and automated remediation provides the study with clear scientific and practical relevance.

A potential area for further improvement is the inclusion of additional empirical validation under diverse network conditions, particularly to assess the reliability of automated remediation and the framework’s resilience to false-positive detections.

The article “AI Agents for Automated Network Incident Detection and Misconfiguration Identification” possesses scientific and practical significance and recommended for publication in a scientific journal.

Reviewer:

Lev Kazarnovskiy

*Expert in Software Test Automation
and Quality Engineering*