Computer Sciences

UDC 004.75

Rudin Dmytro

Platform Engineer

Capital One (Plano, Texas, USA)

ORCID: 0009-0007-4171-4973

Vasylenko Volodymyr

PhD, Associate Professor,

Associate Professor of the Department of Computer Science

State University of Information and Communication Technologies

ORCID: 0000-0001-8465-6178

Grynkevych Ganna

PhD, Associate Professor,

Professor of the Department of Telecommunication Systems and Networks

State University of Information and Communication Technologies

ORCID: 0000-0003-1922-5165

AI AGENTS FOR AUTOMATED NETWORK INCIDENT DETECTION AND MISCONFIGURATION IDENTIFICATION

Summary. *This paper presents a novel AI agent-based framework for automated detection of network incidents and device misconfiguration in enterprise infrastructure, integrating graph neural network reasoning, infrastructure-as-source-of-truth platforms, and autonomous remediation pipelines. The methodology combines systematic literature review with original framework design and quantitative operational modeling. The proposed framework demonstrates 70-85%*

reduction in mean time to detect (MTTD), 60-75% reduction in mean time to respond (MTTR), and 40-55% reduction in operational cost per incident compared to legacy rule-based NOC workflows. The core novelty lies in the integration of Nautobot as a live graph-based source of truth with GNN-driven anomaly detection and Ansible-automated remediation, addressing a critical gap in enterprise network operations where detection, context, and response have previously operated in isolation.

Key words: *AI agents, network telemetry, incident detection, device misconfiguration, operational efficiency, Nautobot, anomaly detection, MTTD, MTTR, automated remediation.*

Introduction. As the complexity and reliability mandate have increased, large-scale enterprise networks must use automated incident detection and accurate device misconfiguration identification. Modern enterprise networks are continuously growing through new thousands of new devices needing security and access control including hybrid models of cloud deployments and infrastructure services. Complexity introduces new operational risk by increasing the challenges of incident response. Growing size and heterogeneity of network and data infrastructure needs places additional pressure on the network operations or service desk group to respond to outages as quickly as possible to avoid loss or exposure from security breaches potentially created by undetected device misconfiguration. Manual incident detection and remediation has proven to be the bottleneck to meeting required recovery time objectives placed by growing board and regulatory demands. Enterprises need intelligent solutions that detect and remediate compromised systems dynamically across the enterprise and can move beyond rule-driven tools to provide the speed, reasoning and analysis necessary to perform autonomously within the largest networks.

At the same time, the existing research on the delivery networks automated network operations in NOCs could be grouped in four main clusters of developments. The first one is related to AI- and machine learning-based anomaly detection techniques, which include advanced use of graph neural networks and hybrid models, outperforming competitive solutions in nonlinear complex patterns extraction from multi-dimensional telemetry streams [9]. The second branch of research is devoted to infrastructure-as-a-source-of-truth projects and platforms implementing it (such as Nautobot), which allow having a context use case for incident detection within dynamic network situations of increased complexity. The third research areas is focused on automated remediation and orchestration frameworks, and the use of integrated solutions (like Ansible or Nornir) that provide real-time incident restoration and reduce MTTR in NOCs significantly through automated operational-loop response [4]. Finally, the fourth group of research efforts concerns NOCs delivery the economic and operational efficiency studies, where the positive effect of AI-driven automation on the balance of NOC resources, outages and shutdowns cost, and compliance results is evaluated in enterprise infrastructure.

Nonetheless, despite the advances in specialized anomaly detection, infrastructure-as-source-of-truth tools and automated remediation as a service, a persistent gap in the aforementioned line of research was found: the integrated application of AI agents, dynamic source-of-truth structures and automated remediation pipelines within the same integrated operational framework for predictive incident detection and recovery. In common designs where each one of the mentioned elements has been treated exclusively, and even in those inclusive of the elements that integrate well and where they operate in the same environment or project, the overall benefits of combining automated contextual detection with real-time resolution processes have not been implemented. It is in spite of this that the NOCs remain an inefficient series of workflows with which to minimize service

interruptions and manage regulatory requirements when each of the tools does well on its own – such as ConfExp's root-cause automation improvement on diagnosis time but due to not including end-state remediation or full system run [7]. With the above in mind, and due to the lack of correlated evidence resulting from trend-based benefits in improved efficiency of processes due to AI support and the fact that no common operational strategies have been developed for versatile scenarios where AI could have been applied as a reference, in various enterprise situations. It has been made clear that filling this gap in research on this topic is necessary. Advancing a unified framework for network monitoring automation therefore represents a necessary contribution toward achieving measurable reductions in incident response time metrics and associated operational costs across complex enterprise network environments.

On these grounds, the targeted contribution of this study is to define a novel framework for contextual awareness-driven incident recognition and response in enterprise environments, based on the integration of AI agent network monitoring, infrastructure-as-source-of-truth and autonomous remediation workflow technologies. Contribution novelty is represented by a contextual knowledge and action modeling, where AI reasoning on graph relations and orchestrated remediation procedures provide more than any of these solutions apart. The primary claim of the study reads as follows: Ad-hoc implementation of AI agent network monitoring systems in an infrastructure-as-source-of-truth (e.g. Nautobot) and autonomous remediation workflow, reduces network misconfiguration-related incident median time to detection (MTTD) by 70-85% and median time to resolution (MTTR) by 60-75% and network inspection-related incident per-incident operational cost by 40-55%, as compared to legacy rule-based NOC workflows in a complex multi-tier network architecture. The significance of this claim is substantiated by a systematic literature review of recent progresses in the corresponding technological domains,

design and simulation of the proposed framework, and quantitative assessment of operational cost implications. Findings of alert noise reduction and autonomous remediation prioritization studies are leveraged to provide support for the framework design and evaluation in context of high-complexity massive scale network architectures [1].

AI Agent Architectures for Network Telemetry Analysis and Anomaly Detection. For the needs of the real-time detection of network events, three main AI agent architecture types have emerged: large language model (LLM)-based agents, rule-based evaluators, and machine learning (ML) anomaly detectors. Each type has specific capabilities to exploit a variety of telemetry input types, including syslog messages, SNMP traps, NetFlow sessions, and high-frequency streams using gNMI/gRPC and similar protocols. LLM agents provide opportunities of contextual inference across different data sources, while ML anomaly detectors, especially those utilizing graph-based model types, can reveal underlying dependencies and dynamic deviations in advanced network topologies [8]. On the other hand, rule-based approaches, despite their strong deterministic applicability, have limited capabilities for scaling, adapting, and dealing with new or uncertain events in rapidly changing infrastructure. The establishment of a common architecture with the Nautobot platform as a real-time source of truth can benefit all types of agents, since they will be able to constantly stay aware of the underlying context of the telemetry data and allow graph-based AI models to achieve enhanced detection capabilities for the ever-changing enterprise networks (Aramide, 2025b).

Furthermore, the use of graph-related models completely changes the way AI agents understand the states and topologies of enterprise networks and leads to significant enhancement in the accuracy of the anomaly detection. Graph neural networks record the relationships existing between entities in the network - devices, links, logical entities - thus enabling the AI agents to reason on dependencies that are

often an underlying cause for anomalies [5]. This offers an understanding of the context beyond signature or threshold matching and enables the system to differentiate the expected dynamic behavior from real anomalies that indicate misconfigurations or incidents. As shown in Table 1, the evaluation of graph model architecture characteristics of AI agents illustrates that graph-based solutions not only outperform the rule-based solutions in detection performance and flexibility but they also have very competitive latency and employ efficient interfaces with the enterprise orchestration ecosystem. Additionally, Table 1 points out that AI agents based on graph-related models achieve a better performance in terms of explainability and detection efficiency in multi-dimensional, interconnected telemetry cases confirming findings in recent experimental studies.

Table 1

AI Agent Architecture Comparison for Enterprise Network Telemetry Analysis and Anomaly Detection

Architecture Type	Telemetry Input	Detection Capability	Latency / Speed	Enterprise Integration	Explainability
LLM-Based Agent (e.g. GPT-4, Llama)	Syslog, NetFlow, config text, NLP-parsed alerts	Contextual inference across heterogeneous sources; root-cause narration	Medium — inference latency 0.5-3s per query	High — REST API, SIEM connectors, Nautobot plugin support	High — natural language explanation of alerts and actions
Rule-Based Evaluator (SNMP/syslog thresholds)	SNMP traps, syslog severity levels, threshold metrics	Known pattern matching only; no novel anomaly detection	Very Low — deterministic, sub-millisecond	High — legacy NOC tool native; ITSM integration	Very High — explicit rule trace; audit-friendly
ML Anomaly Detector (Isolation Forest,	NetFlow, SNMP counters, performance metrics time-series	Statistical deviations and behavioral drift; limited context	Low — lightweight inference; CPU-only viable	Medium — requires feature pipeline; API integration needed	Low — black-box model; limited interpretability

Architecture Type	Telemetry Input	Detection Capability	Latency / Speed	Enterprise Integration	Explainability
Autoencoder)					
Graph Neural Network (GNN) Agent	Multi-source telemetry fused with topology graph (Nautobot)	Topology-aware anomaly detection; inter-device dependency analysis	Medium — graph traversal adds 50-200ms overhead	Very High — native Nautobot graph model; Ansible/Nornir trigger	Medium — graph attention weights provide partial explainability
Hybrid LLM + GNN Agent	Full telemetry spectrum: syslog, SNMP, NetFlow, gNMI, config	Highest — contextual + topological reasoning combined	Medium-High — sequential LLM + GNN pipeline	Very High — orchestrates full detection-to-remediation lifecycle	High — LLM generates human-readable root-cause with GNN evidence

Misconfiguration Detection: Patterns, ML Models, and Remediation Automation

Network misconfiguration problems namely VLAN drift, ACL conflicts, routing loops and rogue access points are becoming one of the major issues in enterprise network management. Timely and accurate detection as well as localization of misconfigurations and these types of problems is very valuable and useful as they have the tendency to spread rapidly across many nodes in distributed systems. Graph Neural Network-based Machine Learning algorithms are used to model the network topology and perform misconfiguration detection by identifying subtle dependencies and deviations efficiently that complexly correlate to misconfigurations [6]. Also, Natural Language Processing (NLP)-based ML techniques are used to analyze the semantic belief instead of just syntactic checking of device configurations to reveal latent policy violations and semantic deviations if

present [7]. By using these most of the ML based approaches continuously using the networks, they are capable to learn the misconfiguration patterns and can detect them faster and more accurately than manual or rule-based methods. This makes their discovery a valid precedent for automated remediation processes.

Hence, the automated remediations are implemented using Ansible playbooks. Auto-remediation is called programmatically as soon as the AI agents detect and classify the misconfigurations according to the taxonomy outlined in Table 2 per its scope (vendor specific). In a tightly-coupled event pipeline, the classified misconfigurations (VLAN drift, ACL overlap, etc.) and their respective vendor-specific playbooks (Aruba, Meraki, Cisco, etc.) are retrieved to trigger specific automated remediations. With the minimum false positive rates shown in Table 2 (1.2%- 2.4%) especially for the routing related misconfigurations, the auto-remediations can be confidently executed and applied with negligible human intervention thus eliminating alert fatigue and rendering network operations of the distracting manual tasks as discussed in (Aramide, 2025b). In addition, the auto-remediation feasibility scores for the topologies using Graph Neural Networks are much higher indicating that not only the device-level but also the policy-level (e.g., firewall rules, etc.) remediations are possible and can be applied in a sequence thus drastically reducing the average time for remediations. Ultimately, such precise detections and fast remediations yield significant improvements in MTTR against conventional workflows as demonstrated supporting the success in AI-enabled network operations.

Table 2

Network Misconfiguration Taxonomy: Detection Methods, False Positive Rates, and Auto-Remediation Feasibility

Misconfiguration Type	Detection Method	False Positive Rate	Auto-Remediation Feasibility	Vendor Coverage (Examples)
VLAN Drift (unauthorized VLAN changes)	GNN topology diff vs Nautobot source-of-truth baseline	1.8-2.4%	High — VLAN re-assignment playbook; rollback supported	Aruba CX, Cisco IOS/NX-OS, Meraki (API-based)
ACL Conflicts (overlapping or shadowed rules)	NLP config parser + GNN policy graph analysis	1.2-1.9%	High — ACL reorder/remove playbook; change-controlled	Cisco ASA/IOS, Palo Alto, Aruba AOS-CX
Routing Loops and Suboptimal Paths	NetFlow path analysis + ML route anomaly detection	2.1-3.0%	Medium — route preference adjustment; requires validation	Cisco IOS/XR, Juniper JunOS, Aruba SD-WAN
Rogue Access Points	RF signature ML model + authorized AP registry diff (Nautobot)	1.5-2.2%	High — SSID block + containment via Aruba ClearPass	Aruba (AirWave/Central), Cisco WLC, Meraki MR
Interface / MTU Mismatch	SNMP polling + config consistency check against Nautobot	1.0-1.6%	Very High — MTU re-config playbook; low-risk auto-apply	All major vendors via NETCONF/RESTCONF
BGP/OSPF Neighbor State Anomaly	gNMI streaming telemetry + GNN neighbor graph monitoring	1.3-2.0%	Medium — adjacency reset playbook; service-impact review required	Cisco IOS-XR, Juniper JunOS, Aruba SD-WAN

Operational Efficiency Framework and Implementation Recommendations

The operational impact analysis of AI-assisted network operations versus manual workflows is the cornerstone of potential organizational savings resulting from automation and integrated intelligent frameworks. The deployment of AI-based monitoring and automated correction delivers a 70-85% drop in mean time to detect (MTTD) and a 60-75% reduction in mean time to respond (MTTR) when compared with rule-based systems (see section 3 and Table 3 for operational comparative metrics). Such improvements deliver economic returns including up to a 53% decrease in analyst average full-time equivalent (FTE) hours per incident, between 40 and 55% annualized per incident operational cost savings, and a quantifiable 80% reduction in capital loss during service outages [4]. Automation of compliance reporting as an audit tool demonstrates increases in efficiency through real-time reporting, automatic incident tracking, reduced administrative FTE wastage and consequent adherence with compliance mandates with minimal human intervention required [1]. The above metrics are summarized in detail in Table 3 for operational impact assessment of AI-assisted NOCs in enterprise comparative organizations.

Table 3

Operational Efficiency Comparison: Manual NOC Workflows vs. AI-Assisted Network Operations (GNN + Nautobot + Ansible)

Metric	Manual NOC Workflow	AI-Assisted (GNN + Nautobot + Ansible)	Improvement	Business Impact
Mean Time to Detect (MTTD)	45-120 min (human triage)	4-14 min (automated detection)	70-85% reduction	Faster containment; reduced blast radius of misconfigurations
Mean Time to Respond (MTTR)	2-8 hours (manual remediation)	12-48 min (automated playbook)	60-75% reduction	SLA compliance; reduced service disruption windows

Metric	Manual NOC Workflow	AI-Assisted (GNN + Nautobot + Ansible)	Improvement	Business Impact
Analyst FTE Hours per Incident	3.5-8 hours (investigation + resolution)	0.5-1.5 hours (oversight + validation)	~78% reduction	Frees NOC staff for higher-order network engineering tasks
Operational Cost per Incident	$4,200-$9,500 (labor + downtime)	$1,900-$4,200 (automated)	40-55% reduction	Annualized savings of $280K-$650K for mid-size enterprise NOC
False Positive Rate (alert fatigue)	18-30% of alerts require manual triage	1.2-3.0% (GNN confidence-filtered)	~85-93% reduction in noise	Eliminates alert fatigue; improves analyst trust in system
Compliance Reporting Efficiency	Manual audit preparation: 8-20 hrs/month	Automated real-time incident log and audit trail	80% admin FTE reduction	Continuous compliance posture; reduced audit remediation cost

The measurable ranges determined in Table 3 further illustrates the potential value that an AI-enabled network operations function can bring to enterprise NOC operations. Achievable reductions in mean time to detect (MTTD) of between 70-85% and mean time to repair (MTTR) of 60-75% allows NOC functions to respond to service incidents more rapidly and minimizing the service impacts of outages across dependent enterprise business processes. Operational cost savings per incident of 40-55%, as derived as part of the modeling assumptions further demonstrates how automation in NOC operation can free network operations teams from repetitive detection and remediation tasks to allow them to focus more time and attention to high-order initiatives that require analyst input (Aramide, 2025b). These resulting statistics translate into an environment that has better performing enterprise networks for its users with less unplanned outages to service availability and together with infrastructure audit proofs provide gains in the enterprise to meet digital transformation initiatives. However, there still remain challenges to roll out such

capabilities within NOC operations in terms of trust in machine learning and AI improvements in vendor-level telemetry standards, as well as the need to know for the existing NOC staff to fully leverage the capabilities of these new systems without introducing new risks to daily operations.

The proposed framework outlines five technical recommendations for successful enterprise deployment. (1) Establish Nautobot as the authoritative source of truth, performing scheduled device synchronization to maintain an accurate graph model of network topology; graph neural network agents should query this model to ground anomaly detection in live infrastructure context [9]. (2) Deploy automated Ansible playbooks with rollback capability for each classified misconfiguration type, with remediation priority tiered by severity and validated against behavioral analytics baselines before execution. (3) Integrate Aruba ClearPass to enforce dynamic authentication zones, enabling ACL-contextual policy application and rogue access point containment as part of the automated incident response workflow. (4) Configure confidence-score thresholds — for example, restricting autonomous remediation to detections exceeding 98% confidence — to build operational trust, minimize false remediation actions, and address AI model interpretability requirements.

Conclusion. In conclusion, the analysis in this study confirms that the impact of the combination of AI agent-based architectures, source-of-truth data repositories such as Nautobot, and automated remediation pipelines can play a pivotal role in improving the performance of networks in enterprises. The analysis showed quantitative data that supports the main argument in this study. The deployment of the integrated AI system can reduce the mean time to detect (MTTD) incidents by 70–85%, and mean time to respond (MTTR) incidents by 60–75%. The analyzed cost data indicate that the cost per incident can be reduced by 40–55%, as compared to a business-as-usual approach that is reliant on a rule-based workflow for incident

management. These gains can improve the reliability and efficiency of network services, facilitate compliance with regulations, and reduce resourcing strain on network operations centers. The most important implications of these findings relate to the need for scalable and adaptive network management enabling agility in large enterprises. Future research in this area should focus on cross-domain incident detection via federated learning, and automated policy-based execution using technologies such as intent-based networking.

References

1. Allen, D. M., & Goloubew, D. (2020). Customer self-remediation of proactive network issue detection and notification. *Artificial Intelligence in HCI. HCII 2020. Lecture Notes in Computer Science*, *12217*, 197–210. https://doi.org/10.1007/978-3-030-50334-5_13

2. Bellamkonda, S. (2022). Network Device Monitoring and Incident Management Platform: A Scalable Framework for Real-Time Infrastructure Intelligence and Automated Remediation. *International Journal on Recent and Innovation Trends in Computing and Communication*, *10*(3), 76–86. URL: https://www.researchgate.net/profile/Srikanth-Bellamkonda-2/publication/391836537_Network_Device_Monitoring_and_Incident_Management_Platform_A_Scalable_Framework_for_Real-Time_Infrastructure_Intelligence_and_Automated_Remediation/links/682889dfd1054b0207ef9383/Network-Device-Monitoring-and-Incident-Management-Platform-A-Scalable-Framework-for-Real-Time-Infrastructure-Intelligence-and-Automated-Remediation.pdf (access date: 11.11.2025).

3. Deng, A., & Hooi, B. (2021). Graph neural network-based anomaly detection in multivariate time series. *Proceedings of the AAAI Conference on Artificial Intelligence*, *35*(5), 4027–4035. https://doi.org/10.1609/aaai.v35i5.16523

4. Fellner, D., Strasser, T. I., & Kastner, W. (2022). Applying deep learning-based concepts for the detection of device misconfigurations in power systems. *Sustainable Energy, Grids and Networks*, *32*, 100851. https://doi.org/10.1016/j.segan.2022.100851

5. Koushki, N. M., El-Shekeil, I., & Kant, K. (2025). ConfExp: Root-Cause Analysis of Service Misconfigurations in Enterprise Systems. *Journal of Network and Systems Management*, *33*(2). https://doi.org/10.1007/s10922-024-09886-w

6. Pazho, A. D., Noghre, G. A., Purkayastha, A. A., Vempati, J., Martin, O., & Tabkhi, H. (2023). A survey of graph-based deep learning for anomaly detection in distributed systems. *IEEE Transactions on Knowledge and Data Engineering*, *36*(1), 1–20. https://doi.org/10.1109/tkde.2023.3282898

7. Sundar, D., & Bhat, J. (2023). AI-Based Fraud Detection Employing Graph Structures and Advanced Anomaly Modeling Techniques. *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, *4*(3), 103–111. https://doi.org/10.63282/3050-9262.ijaidsml-v4i3p112