International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Predictive Configuration Governance for AI-Assisted Network Automation in Hyperscale MPLS/IP Backbone Networks

Vasantha Kumar Hosahalli Seenappa

Submitted: 01/11/2025 **Revised**: 18/12/2025 **Accepted**: 25/12/2025

Abstract: Hyperscale MPLS/IP backbone networks require high levels of availability and operational reliability to support the interconnection of distributed Points of Presence across geographic regions. Despite this requirement, most existing frameworks for automating network management execute configuration changes based on a "fire and forget" principle with reactive failure recovery mechanisms that will often lead to service disruptions due to lengthy rollback time frames post-failure. The research proposes a framework for the autonomous management of hyperscale MPLS/IP backbone network called the Predictive Configuration Governance (PCG) framework. The focus of the research is to proactively predict deployment risk based on operator intent, OpenConfig/NETCONF (Network Configuration Protocol) configurations, topology, telemetry data, configurations change and previous incidents history. A Configuration Risk Score will allow automated deployment of low-risk changes while routing high-risk configurations to be manually approved. In addition, the PCG framework will continuously refine the model prediction accuracy via a refined closed-loop feedback process as post-deployment telemetry continues to be ingested. The conceptual framework we present enhances prediction intelligence with policy guardrails that can be applied to automated deployments in a core network environment to ensure that the deployment is done safely. Conceptual evaluations have shown that the proposed framework has the capacity to greatly improve the success rates of configurations, reduce the mean time to recover and lower the rollback rate when compared to traditional, non-governed automation pipelines in a production system. Ultimately, the research presented here offers a scalable way to improve the stability and robustness of next-generation IP backbones.

Keywords: *Predictive Configuration Governance, Artificial Intelligence for IT Operations (AIOps), MPLS/IP Backbone, Intent-Based Networking*

1. Introduction

Backbone networks now have a geometric increase in size, performance capability and use due to Cloud-based services, Content Delivery Network (CDN) and Distributed Applications. They physically interconnect Point of Presence (POP) located worldwide within highly complex MPLS and IP backbone networks with reliability demands of 99.999% uptime or greater. The operational complexity of effectively managing such large globally distributed networks consists of thousands of routers, millions of changes in router states and multiple paths for transporting traffic based on dynamic engineering techniques. As a result, operators are moving away from using manual commands to access their networks, i.e., command line interface (CLI)-based operations, to implementing a Zero-Touch Networking (ZTN) architecture that allows for the automation of standard network policy, provisioning and change management processes [1]. Leading organizations in the industry are promoting the use of structured programmability using vendor-neutral OpenConfig Yet Another Next Generation (YANG) models and the use of NETCONF protocol as a replacement for unstructured and error-prone CLI-based legacy scripting [2]. Additionally, AIOps (Artificial Intelligence for IT Operations) is being utilized for autonomous fault resolution, telemetry-based anomaly detection and immediate incident response in large scale WANs [3].

Modern observability platforms enable autonomous operation of networks by streaming telemetry data in real time to AIOps engines for automated incident remediation and security of complex network infrastructures [4]. These technologies greatly reduce manual effort and change operational workflows from a reactive firefighting mode to an automated monitoring and recovery mode [5]. The original research to provide service continuity was to create self-healing control loops using Deep Q-Networks (DQNs) for adapting virtual network function (VNFs) [6] and Cognitive Autonomous Networking (CAN) architectures for core internet backbones [7]. These self-healing paradigms use high-frequency streaming telemetry, including using In-band Network Telemetry (INTs) provisioned as a service, to online learn and track packet-level stats, queue depths and path changes [8]. Additionally, the physical data plane has implemented hardware acceleration of MPLS network actions directly on high-speed switching ASICs using Programming Protocol-Independent Packet Processors (P4) programmable languages [9]. By combining distributed hybrid frameworks with passive-active telemetry for lightweight localized failure detection [10], modern networks can identify and isolate data plane errors within milliseconds.

Automation currently relies on humans or algorithms to automatically configure routers after verifying they are working properly. These automated configuration pipelines produce and implement new configurations with no knowledge of their risk and rely on monitoring devices to scoop up errors and begin the roll-back procedure after the configuration has been implemented. A

Senior Network Engineer/Architect

Maximum Transmission Unit (MTU) mismatch or incorrect Border Gateway Protocol (BGP) export policy for example can propagate across hyperscale backbone networks in a matter of milliseconds, at which point it will be impossible to roll everything back and the routing protocols may have already converged into a state that could cause packets to be lost and lead to blackhole traffic, as well as violating a Service Level Agreement (SLA). In a hyperscale WAN, a single misconfigured routing or traffic-engineering policy can impact an entire region's connectivity. This further reinforces the need for a mechanism to assess the risk of configuration prior to implementing it into production.

This paper proposes a new framework for addressing an identified gap in the way that organizations manage Predictive Configuration Governance (PCG) for large-scale MPLS/IP backbone networks. The previously described models have been developed to transform network automation from a reactive approach to one that proactively prevents configuration risk. PCG uses the intent expressed by the operator to create candidate configurations via standardized OpenConfig YANG models, extracting a multitude of features and generating a multitude of different candidate configurations before predicting deployment risks via a machine learning classifier. By computing a numerical estimated Configuration Risk Score (CRS) prior to configuration deployment, PCG enables organizations to automatically deploy configurations that have been predicted to be low-risk through the use of NETCONF, while also blocking configurations that have been predicted to be high-risk, creating an automatic routing path for manual approval of these configurations. Additionally, by validating configurations against live operational data and previous configuration failure records, PCG increases compliance and improves the overall governance of configuration changes, while also reducing the potential for unplanned service interruptions. The rest of this paper will include a review of the most related work in Section 2, provide a description of the PCG architecture in Section 3, describe how the system will be evaluated and the anticipated benefits of using the PCG architecture in Section 4, discuss the limitations of implementing the PCG framework and suggest future lines of research in Section 5 and finally, provide a conclusion in Section 6.

2. Literature Review

In this section, we provide a thorough review of the literature that covers the fundamental technologies needed to support autonomous networks. We will discuss the current state of agentic artificial intelligence for managing networks, autonomous control loops, in-band telemetry and architectures based on intent. For each of the studies covered, we will analyze the methodology, the contributions, the strengths and the limitations described in the literature so we may form the baseline for current research. Finally, we will explain the research gap that drives our development of a predictive configuration governance framework.

2.1. Zero-Touch Networking and AIOps Frameworks

Zero-touch network automation has received extensive research into how to reduce human error and operational costs associated with managing complex backbones. One author has proposed an incident resolution framework for hyperscale networks using agentic artificial intelligence for network operations [11]. Their approach uses autonomous agents communicating with each other for issue resolution and executing remediation scripts. The primary strength of this research is that it was designed to manage very complex and unpredictable operational tasks. Its primary advantage is that it is flexible when using cognitive resources as well as having excellent orchestration capabilities. Its primary disadvantage is that it cannot fulfill real-time pre-configuration validation or confirmation for high-speed backbone networks due to its high latency and unpredictable execution times because of the non-deterministic nature of the underlying large language model (LLM).

An adaptable AI Assistant for managing networks is provided, based on LLM techniques for converting natural language queries from users into diagnostic commands and device status checks [12]. This user-friendly conversational assistant provides a simple way for operations teams to interact with the Assistant. However, the primary limitation of this Assistant is its inability to conduct quantitative risk prediction or provide assurance that policies will be enforced in deterministic ways. In addition, although this assistant will check the syntax of the configuration files, it does not have access to operational context to determine if any configuration change will create an outage in a production network.

2.2. Telemetry, Self-Healing and Control Plane Programmability

Closed-loop control systems provide the core resilience of the Internet backbone. These autonomous self-healing architectures leverage real-time alarm systems to trigger dynamic routing adjustments [13] to recover from line cuts and node outages, their main advantage is the speed of restoring traffic after a failure they provide a reactive response to service disruption and do not validate configuration changes. More frequent and accurate monitoring of state by using optimal in-band telemetry orchestration allows for collection of high-resolution telemetry data and reduces telemetry overhead [14]. However, there is no consideration for validating whether the risk associated with changing configurations will result in a transition between states. The surveys on generative AI for network management [15] and zero-touch management orchestration for 5G and 6G [16] show that AI technology is capable of providing automated deployment and operational systems through open Application Programming Interface (API) interfaces but do not provide predictive deployment validation mechanisms. Although existing network resilience and failure analysis models provide a comprehensive taxonomy of failure types [17], they do not offer an automated prevention framework. Meanwhile, AI-driven autonomous control planes dynamically optimize routing parameters [18] while link weight optimization based on machine learning principles reduces congestion [19]. However, neither of these solutions validate changes to configuration policies prior to deployment. Finally, the decentralized architecture approach to WAN controller architecture improves scalability [20], but it continues to permit misconfigured routing policies to escape into the environment and thus demonstrates the need for proactive governance of all configuration activities.

2.3. Intent-Based Networking and Language Models

Intent-Based Networking (IBN) is a technique that creates an indirect relationship between high-level business policies and low-level device configuration. The study conducted for policy mapping purposes involved intent-based management research the smart grid [21]. They have developed a structured intent translation pipeline. This research results have several benefits, yet it is primarily focused on the utility grid. Unified telemetry platform has been built to provide optical network intelligence [22]. The

intent-based systems of Artificial Intelligence have introduced syntax verification to the intent-based architectures [23]. Their approach takes natural language intent and converts it into configuration, guaranteeing that configuration will contain no syntax errors. Unfortunately, the syntax verification approach does not have the capability to identify semantic errors such as BGP export rule configurations that allow individual routers to send routing tables incorrectly. LLM-centric approaches have also been proposed for parsing user intent into commands [24]. LLMs can be used to demonstrate how to translate a user's intent into Command Line Interface (CLI) commands. Similarly, intent-based orchestration architectures have been developed for telecommunications and enterprise infrastructures [25]. Although IBN architectures excel in automating the translation of high-level business policy into low-level device configuration, they do not provide a formal risk assessment of the pre-deployment configuration activity. Therefore, they are a major impediment to reliable configuration.

2.4. Research Gap Analysis

A thorough examination of the literature points to a significant gap in research. The presently available network automation systems place emphasis solely on automated deployment [2], optimization of telemetry paths [14], self-healing capability post-failure [13] and intent realization [24,25] without offering or demonstrably testing a pre-deployment configuration governance model which checks the correctness of configuration changes prior to their configuration in a network. In other words, past pipelines merely perform configuration without thinking and are overly reliant on rollback that happens after the fact [26,27]. When a wrong configuration is deployed, it invariably leads to a failure resulting in downtime before the system can be restored which takes only a few minutes before the system is back to normal [28].

Accordingly, this paper proposes a new framework entitled Predictive Configuration Governance (PCG). In contrast to traditional ZTN and AIOps systems, PCG incorporates a new concept of a pre-deployment validation stage into the network automation process wherein a multi-dimensional set of attributes, the configuration diffs and the network's topology, the actual network's telemetry and the past incidents, will be extracted and included [29,30]. It applies the machine learning principles in order to make predictions about the danger level of a potential change. Through banning risky changes, one can prevent any possible failure from taking place in advance. The researched studies are reviewed in Table 1 presenting their peculiarities and weaknesses.

Table 1. Comparative Literature Review

Author	Year	Methodology	Dataset / Testbed	Key Contribution	Limitation
Ihle [9]	**2024**	P4 Hardware Actions	Switching ASIC Testbed	Proposed hardware-accelerated MPLS network actions using P4-programmable switching ASICs for high-speed backbone packet forwarding.	Limited to data-plane programmability without predictive configuration governance.
Manias et al. [11]	**2024**	LLM-Based Intent Extraction	5G Core Network	Proposed an LLM-based approach for extracting network intents from natural-language requirements to support intent-based network management.	Focuses primarily on intent extraction and does not provide complete predictive deployment or configuration governance.
Fang et al. [17]	**2024**	Knowledge-Driven Self-Healing	Autonomous Network Environment	Presented a comprehensive discussion of self-healing mechanisms, challenges, and future directions for knowledge-driven autonomous networks.	Primarily provides a conceptual/review perspective rather than a complete automated predictive deployment framework.
Zeng et al. [22]	**2024**	Matrix-Completion-Based Network Telemetry	Network-Wide Telemetry Environment	Proposed a low-overhead in-band network-wide telemetry approach using matrix completion to reduce monitoring overhead while maintaining network visibility.	Focuses on telemetry overhead reduction rather than predictive configuration and deployment governance.
Habib et al. [25]	**2024**	LLM-Based Intent Processing + Hierarchical Reinforcement Learning	Network Optimization Environment	Proposed an LLM-based framework for processing network intents and using attention-based hierarchical reinforcement learning for network optimization.	Primarily focuses on intent processing and optimization rather than complete predictive deployment-risk assessment.
Van Tu et al. [26]	**2024**	LLM-Based Intent Configuration	NFV / Network Function Configuration	Proposed using in-context learning with large language models to translate network intents into configurations for network functions.	Focuses on intent-to-configuration generation but does not comprehensively address predictive deployment risk and governance.
Li et al. [27]	**2024**	Intent-Driven Autonomous Network Management	Intent-Driven Network Prototype	Proposed a decoupled architecture and intent-driven management scheme for autonomous network management and control across the network lifecycle.	Focuses on autonomous management architecture and control rather than predictive deployment-risk assessment and configuration governance.
Gowtham et al. [28]	**2023**	Intent-Based Network Management Framework	5G / Beyond-5G Network Environment	Proposed NEMI, a standardized approach for intent-based networking to support automated network and service management.	Focuses on standardization and intent-based management rather than predictive configuration validation.
Ahn & Jeong [29]	**2024**	Intent-Driven Management Automation	5G Mobile Networks	Proposed an intent-driven management automation approach for 5G mobile networks to translate high-level requirements into network-management actions.	Focuses on management automation but provides limited emphasis on predictive deployment-risk assessment.

Mekrache et al. [30]	**2023**	NWDAF + Machine Learning	Beyond-5G Network	Combined the Network Data Analytics Function with machine learning for abnormal traffic detection and intelligent network analytics in beyond-5G networks.	Focuses on traffic anomaly detection rather than intent-based configuration and predictive deployment governance.

3. Proposed Methodology

This part of the paper deals with the technological architecture of the proposed Predictive Configuration Governance (PCG) framework. It provides the basis for preventing configuration

failures in enormous MPLS/IP backbone networks by verifying the changes before they are made. The essential elements of the framework are explored, starting from operator's intent processing and going through feature extraction, machine learning risk prediction and closed-loop feedback learning to enable safe and automated implementation process.

3.1. Overall Framework Architecture

The presented Predictive Configuration Governance (PCG) model has been developed to ensure proactive and smart automating processes of configuration management within big MPLS/IP networks. This framework is quite different from existing mechanisms and technologies, which implement configuration changes without making any evaluation of the operational impact. The system provides risk evaluation in case of configuration deployment before the configurations are applied to network devices. The framework consists of different components with functions like processing operator intention, automatic configuration generation, multi-dimensional feature extraction, machine learning-based risk estimation, decision making, etc. Using all the information from real-time telemetry, network topology, configuration differences and past incidents, it is possible to build a complete operational level, ensuring the risk assessment accuracy.

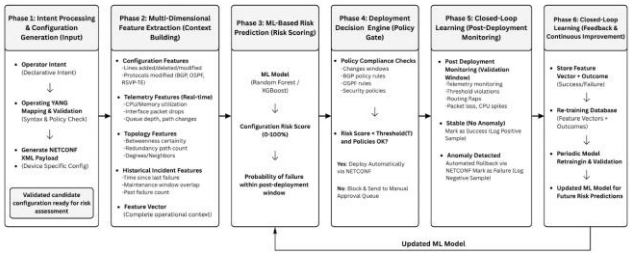

Fig. 1. Overall Predictive Configuration Governance Framework

The uniqueness of the proposed PCG framework is found in the fact that there is a proactive pre-deployment validation gate before the programs can be executed, this is highly different from the existing autonomous network management methods. Already established ZTN and AIOps approaches are concerned with automation of implementation processes and failure detection, while self-healing systems just respond to failures after there is an issue. IBN appears to be very good in converting intents to sentences, but the existing technologies do not provide quantitative risk estimation. The PCG system offers a unique opportunity of combining intents processing, collecting multidimensional features that consist of different configurations, topological parameters, current telemetry and some other novel techniques to forecast deployment risks in advance.

3.2. Intent Processing and Configuration Generation

The Configuration Generation Plane ensures that the intent of high-level instructions is converted into standardized configurations that fall in line with OpenConfig YANG. OpenConfig YANG models define the network state independent of the vendor. The modeling coverage includes parameters related to all the components of the network such as interfaces, BGP and OSPF (Open Shortest Path First). The configuration engine interprets the intent from the user and converts it into corresponding YANG schema with appropriate validation. This way the configurations are guaranteed to comply with policies and be syntactically correct.

3.3 Streaming Telemetry Collection

Simultaneously, the module for streaming telemetry uses gNMI (gRPC Network Management Interface) in order to obtain live performance data from the various backbone routers. Subscriptions are made to capture various statistics with frequent updates, such as Central Processing Unit (CPU) loads, memory usage, packet drop rates, queue size and path changes. As opposed to using traditional polling methods, such as SNMP, gNMI is capable of sending this telemetry data at short intervals. The capabilities of gNMI allow it to combine telemetric data together with information about the network topology and the historical logs of incidents, which help to create a comprehensive operating context for the target node.

3.4. Operational Feature Extraction

The Feature Extraction Engine builds a multidimensional feature vector from the candidate configuration, topology and telemetry stream. In particular, it extracts configuration features which refer to the number of lines that have been added, deleted, or changed in the NETCONF Extensible Markup Language (XML) payload together with flags helping to identify which protocols have been affected including BGP, Resource Reservation Protocol - Traffic Engineering (RSVP-TE), OSPF. Telemetry features refer to the information regarding the current CPU operation of the target router and the number of dropped packets on the active interfaces. Topology features include the position of the router in the network including its betweenness centrality which shows the number of shortest routes involving this node and redundancy path count showing how many redundant routes could be used in case of a failure. As a result, the historical incident features help to get the information about the time of last failure on that router node as well as its correlation with the scheduled downtime. Therefore, the feature extraction engine outputs the complete feature vector needed for the ML risk predictor which shows the current network configuration change and the operational status of the selected router node.

3.5. Configuration Risk Prediction

The ML Risk Prediction Plane assesses the combination of characteristics with an educated classifier in order to foresee the risks associated with the installation. The classifier has been trained by dissimilar configuration log entries, streams of

telemetry and incident logs to identify intricate patterns responsible for potential failures. In the case of a router change, for example, updating a BGP protocol in a router that has high CPU utilization and low path redundancy would trigger an actual failure. The outcome of the model is a continuous degree of failure probability, which will be changed into a Configuration Risk Level from 0% to 100%.

3.6. Deployment Decision Engine

The Deployment Decision Engine applies a policy-based mechanism to decide if a candidate configuration should be deployed. It compares the calculated Configuration Risk Score with the threshold (T) defined by the operator. When the configuration risk score is below T and the results of all static compliance policies comply, e.g., no BGP peering changes during the peak traffic hours and mandatory passive-interface commands for OSPF, the configuration gets deployed automatically through NETCONF. When the risk score exceeds T, or the violation of any of the policies occurs, in this case, the deployment will be denied and the configuration diff, risk score and telemetry functions will be sent to the manual approval queue for review by the engineer.

3.7. Closed-Loop Learning

After the deployment, the closed-loop learning engine tracks all operational telemetry for the router being validated. If everything stays stable, meaning if there are no violations concerning the telemetry threshold and the routing is stable, then we can call that deployment a success as the feature vector will be saved as a positive case. If an anomaly occurs, NETCONF rollback is activated here followed by reverting back to the previous state. Those logs are preserved in the re-training database in order to be strictly examined so that the machine learning model is regularly upgraded. This closed-loop method allows the model to update itself with recent topology and traffic profile changes, ensuring the accuracy of the results in the long-term perspective.

4. Result Analysis

This part discusses the evaluation framework conceptualized to evaluate the performance, practicality, as well as operational advantages of the proposed Predictive Configuration Governance (PCG) framework. In this context, since applying untested models in production hyperscale infrastructures entails significant operational risks, we provide a concept of evaluation including simulated WAN topologies and traffic generators. We consider some key performance indicators (KPIs) and perform a qualitative comparison of the PCG framework with traditional automation pipelines being non-governed.

4.1. Evaluation Methodology and Metrics

The Predictive Configuration Governance (PCG) framework put forward in this study is analyzed conceptually in simulated WANs, mimicking real life activities and conditions on a backbone network. Testing and simulation environments and virtual router configurations have been used to determine the PCG ability to detect configuration faults. Various errors in configuration have been simulated including routing policy, MTU and routing loops, with the help of which an assessment of the machine learning risk prediction ability has been carried out. The most important parameters of the performance evaluation include deployment stability, prediction quality, operational efficiency and network performance of PCG framework. The metrics used for evaluation or practical significances are presented in Table 2.

Table 2. Evaluation Metrics for Assessing the Proposed Framework

Metric	*Description*	*Importance*
Configuration Success Rate	The percentage of deployed configuration changes that do not trigger any operational anomalies or performance degradations.	Indicates the effectiveness of the framework in ensuring backbone stability and policy compliance.
Deployment Validation Latency	The time required to parse operator intent, extract operational features, generate the risk score and validate policies.	Ensures the pre-deployment screening does not introduce significant delays in automated provisioning pipelines.
Deployment Rollback Rate	The percentage of configurations that must be rolled back due to post-deployment telemetry anomalies or routing issues.	Measures the framework's ability to prevent faulty changes from reaching the active network configuration.
Mean Time to Recovery (MTTR)	The average duration of service degradation when an anomalous configuration change is deployed and requires rollback.	Shows how the automated rollback module minimizes downtime compared to manual intervention.
Network Availability	The proportion of total operation time that the core network remains fully functional and accessible.	Represents the ultimate operational goal of backbone management, directly impacting SLA agreements.
Risk Prediction Precision	The ratio of true configuration anomalies blocked to the total number of deployments flagged as high-risk by the model.	Critical for operator trust, high precision prevents alert fatigue and unnecessary manual approval delays.

4.2 Comparative Analysis: PCG vs. Traditional Pipelines

It is obvious that the methodology employed by PCG differs from that of the traditional approach in several aspects which lead to a need for the revision of the concept of configuration deployment. The traditional automation pipeline provides for the implementation of configuration at the level of the functioning of configuration devices without testing it beforehand, whereas PCG proposes to make use of the pre-deployment validation process before the application of configuration. The testing phase suggests that there should be represented configuration analysis, real-time telemetry, topology information and estimation of confidence in

the configuration via machine learning. Such an approach allows one to define the riskiest way of implementation of configuration and make it safer in the future since there will be an opportunity to eliminate high-risk levels in advance rather than checking the reached performance after the functions of configuration are implemented

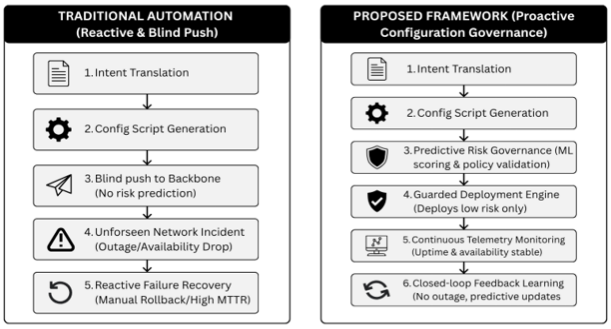

Fig. 2. Comparison Between Traditional Configuration Deployment and Predictive Configuration Governance

4.3. Practical Significance and Operational Impact

The operational benefits foreseen from the implemented PCG framework include increase in configuration success and decrease in incidents associated with the deployment. The PCG framework makes sure that any candidate configuration cannot be implemented when the node which is going to be configured is either congested or degraded. It uses telemetry data like CPU load and link drops and identifies the correct type of configuration in accordance with flawless compliance. The engine of policy verification provides an opportunity to implement the compliance and keep any unauthorized changes from taking place at top traffic periods. As a result, a significant reduction in similar incidents is achieved with the framework being able to shield the operator.

5. Challenges and Future Work

In this section, we will tackle the practical challenges regarding implementation, limitations and future research in Predictive Configuration Governance framework. The deployment of predictive validation gates in global backbone networks raises issues such as data size, model interpretability, compatibility with old technologies and adjustable threshold values. We will discuss these issues as well as suggest your paths.

5.1. Practical Deployment Challenges

In order to deploy a functioning system in a real-world situation a number of challenges need to be resolved. One of the most serious obstacles is the availability of the data as configuration fails become a rarity in real-world cases and thus the dataset is bound to be biased. Such conditions may lead to too many false negatives with the application of machine learning. In addition, it is also complicated to build a model which would work across different networks and vendor platforms. Building a classifier for one network architecture does not mean that the model will work for another topology unless it is trained again in terms of all peculiarities of the new mesh. To make matters worse, it is difficult to integrate the solution with old equipment which does not have a support for YANG and gNMI and thus requires some telemetry adapters or equipment for command interface conversion at a higher price and with delays and lower level of detail.

5.2. Future Research Opportunities

Future research will explore several paths to address these challenges. The first involves using Explainable AI (XAI) solutions like SHapley Additive exPlanations (SHAP) or Local Interpretable Model-agnostic Explanations (LIME), which provide natural language interpretations of the decisions made by a risk prediction engine, so that operators can understand the reasons behind high-risk decisions. The second path concerns the use of reinforcement learning (RL) strategies in order to modify the threshold of risk for the prediction engine. The third option is built on the research of the possibility to use different types of Agentic AI systems in which autonomous agents would resolve conflicting situations based on the policy set by the operator. Finally, validating the framework in multi-vendor hardware testbeds will verify its interoperability and performance.

6. Conclusion

High operational reliability and safe network automation are crucial when it comes to the need for modern hyperscale MPLS/IP backbone networks. There is the use of reactive framework of network automation, wherein configuration of networks is done without prior assessment. Meaning that switching or failure of networks because of wrong configuration occurs before the problem is rectified by the use of telemetry to track any occurrences of issue. The paper proposes a new technique known as Predictive Configuration Governance (PCG) technology that enables predictive automation of changing the networks without failure of automation frameworks that are utilized in network automation. PCG allows parsing the intentions of the users and processing them to generate the OpenConfig/NETCONF data formats. From the data formats, PCG can process and assess operational features that are defined using some methods and techniques. Techniques used by PCG to determine the operational features of a network are the separate models, rules encompassing complex sets that comprehensively gives the network information. The presentation of the intended, processed results encompasses points to be analyzed by the readers.

References

[1] M. El Rajab, L. Yang, and A. Shami, “Zero-touch networks: Towards next-generation network automation,” *Computer Networks*, vol. 243, p. 110294, 2024.

[2] Amlou et al., “Automated network programmability using OpenConfig YANG models and NETCONF protocol,” in *2023 20th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA)*, IEEE, 2023.

[3] M. Bajpai, “Autonomous Network Troubleshooting with AIOps and Machine Learning: A Data-Driven Architecture for Correlation, Prediction, and Remediation,” *The Eastasouth Journal of Information System and Computer Science*, vol. 2, no. 02, pp. 275–283, 2024.

[4] M. Bajpai, “From Observability to Closed-Loop AIOps: Data-Driven Automation for Secure and Resilient Network Operations,” *The Eastasouth Journal of Information System and Computer Science*, vol. 1, no. 02, pp. 260–267, 2023.

[5] M. Bajpai, “The transformative impact of AI Ops/ML and observability in automating networking operations and network

security," *International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences*, vol. 11, no. 4, pp. 1–4, 2023.

[6] Arulappan et al., "Dqn approach for adaptive self-healing of vnfs in cloud-native network," *IEEE Access*, vol. 12, pp. 34489–34504, 2024.

[7] S. K. Balakrishnan, "Cognitive Autonomous Networking (CAN): Self-Learning and Self-Healing Framework for the Global Internet Backbone," *Journal of Computational Analysis & Applications*, vol. 31, no. 3, p. 713, 2023.

[8] M. Ji et al., "INTaaS: Provisioning in-band network telemetry as a service via online learning," *Computer Networks*, vol. 241, p. 110211, 2024.

[9] Ihle, Fabian, and Michael Menth. "MPLS Network Actions: Technological overview and P4-based implementation on a high-speed switching ASIC." *arXiv preprint arXiv:2410.20400* (2024).

[10] J. Xiao et al., "Themis: A passive-active hybrid framework with in-network intelligence for lightweight failure localization," Computer Networks, vol. 255, p. 110836, 2024.

[11] Manias, Dimitrios Michael, Ali Chouman, and Abdallah Shami. "Towards intent-based network management: Large language models for intent extraction in 5g core networks." *2024 20th International Conference on the Design of Reliable Communication Networks (DRCN)*. IEEE, 2024.

[12] Abane, A. Battou, and M. Merzouki, "An adaptable AI assistant for network management," in NOMS 2024 - 2024 IEEE Network Operations and Management Symposium, IEEE, 2024.

[13] Bayazeed, Adnan, Khaldoun Khorzom, and Mohamad Aljnidi. "Towards coordinating self-healing instances: Policy-based and non-cooperative game theory-based approaches with location awareness." *Computer Networks* 254 (2024): 110827.

[14] Xu, Zichen, Ziye Lu, and Zuqing Zhu. "Information-sensitive in-band network telemetry in P4-based programmable data plane." IEEE/ACM Transactions on Networking 32.6 (2024): 5081-5096.

[15] Dzeparoska, Kristina, Ali Tizghadam, and Alberto Leon-Garcia. "Intent assurance using LLMs guided by intent drift." *NOMS 2024-2024 IEEE Network Operations and Management Symposium*. IEEE, 2024.

[16] E. Coronado et al., "Zero touch management: A survey of network automation solutions for 5G and 6G networks," IEEE Communications Surveys & Tutorials, vol. 24, no. 4, pp. 2535–2578, 2022.

[17] Fang, Honglin, et al. "Self-healing in knowledge-driven autonomous networks: Context, challenges, and future directions." *IEEE Network* 38.6 (2024): 425-432.

[18] Mata, Luís, et al. "A machine learning driven methodology for alarm prediction towards self-healing in wireless networks." *2024 Wireless Telecommunications Symposium (WTS)*. IEEE, 2024.

[19] U. J. Umoga et al., "Exploring the potential of AI-driven optimization in enhancing network performance and efficiency," Magna Scientia Advanced Research and Reviews, vol. 10, no. 1, pp. 368–378, 2024.

[20] Krentsel et al., "A decentralized sdn architecture for the wan," in Proceedings of the ACM SIGCOMM 2024 Conference, 2024.

[21] Q. Han et al., "Intent-Based Network Management and Its Application Prospects in Smart Grids," in 2024 3rd International Conference on Cloud Computing, Big Data Application and Software Engineering (CBASE), IEEE, 2024.

[22] Zeng, Xin, et al. "INT-MC: Low-overhead in-band network-wide telemetry based on matrix completion." *Proceedings of the ACM on Measurement and Analysis of Computing Systems* 8.3 (2024): 1-30.

[23] Y. Njah, A. Leivadeas, and M. Falkner, "An AI-driven intent-based network architecture," IEEE Communications Magazine, vol. 63, no. 4, pp. 146–153, 2024.

[24] Mekrache, A. Ksentini, and C. Verikoukis, "Intent-based management of next-generation networks: An LLM-centric approach," IEEE Network, vol. 38, no. 5, pp. 29–36, 2024.

[25] Arafat Habib, Md, et al. "LLM-Based Intent Processing and Network Optimization Using Attention-Based Hierarchical Reinforcement Learning." *arXiv e-prints* (2024): arXiv-2406.

[26] Van Tu, Nguyen, Jae-Hyoung Yoo, and James Won-Ki Hong. "Towards intent-based configuration for network function virtualization using in-context learning in large language models." *NOMS 2024-2024 IEEE Network Operations and Management Symposium*. IEEE, 2024.

[27] Li, Tong, et al. "Architecting autonomous network management and control via intent-driven decoupled network." *IEEE Network* 38.6 (2024): 361-369.

[28] Gowtham, Varun, et al. "Nemi: A standardized approach to intent based networking." *2023 IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 2023.

[29] Ahn, Yoseop, and Jaehoon Paul Jeong. "An intent-driven management automation for 5g mobile networks." *2024 International Conference on Information Networking (ICOIN)*. IEEE, 2024.

[30] Mekrache, Abdelkader, Karim Boutiba, and Adlen Ksentini. "Combining network data analytics function and machine learning for abnormal traffic detection in beyond 5g." *GLOBECOM 2023-2023 IEEE Global Communications Conference*. IEEE, 2023.