Machine Learning for Real-Time Detection and Localization of Network Failures

CUNY School of Professional Studies

Michael Hernandez

September 12, 2025

1 Topic Description

This project develops a pragmatic system that ingests two operational signals—BGP routing updates and device logs—and applies approachable machine-learning to detect failure-induced incidents quickly and infer where they most likely originate (e.g., top-of-rack, spine/route-reflector, or edge/provider). The emphasis is operator value: fewer noisy alerts, faster first actions, and an explanation of ”what broke and where.”

2 Problem Description

Large BGP-routed environments generate many alarms but little immediate guidance about what truly matters or where to begin. Traditional SNMP/syslog thresholds alert on hard failures yet often over-page on benign edge-local events and under-explain control-plane or egress faults, leading to manual correlation and delays. In a production setting with thousands of switches and anycast/VXLAN, this increases time to detect and time to resolve. A system that correlates control-plane churn with structured log patterns and a simple role-based topology can reduce detection delay, provide a first-guess fault location, and suppress noise that is confined to a single rack or host.

3 Solution Description

The system extracts simple features from BGP updates (withdrawals, AS-path churn, next-hop shifts) and log templates (counts, severity, burstiness), then applies lightweight, well-documented methods: Matrix Profile for time-series anomaly cues on BGP streams and Isolation Forest for device-level log vectors (Scott, Johnstone, Szewczyk, & Richardson, 2024; Cheng, Li, Lv, Liu, & Wang, 2021). Scores are normalized and fused, then passed through a topology-aware localization step that uses the network's role map (server, ToR, spine/RR, edge) to propose a likely origin and to down-rank edge-local flaps (Tan, Huang, You, Su, & Lu, 2024). A small Streamlit dashboard presents the alert, the suspected location, and the top contributing signals; the goal is earlier, clearer action rather than another raw alarm. To tie the work to operator outcomes, the evaluation compares this system to manual SNMP/syslog triage and reports detection delay, event-level precision/recall/F1, localization accuracy (Hit@k), and page reduction (Mohammed, Mohammed, Côté, & Shirmohammadi, 2021).

4 Research

4.1 Coursework Foundations

My degree provided the **foundations** for this project while my work experience supplies domain depth.

- **Python, data structures, and databases** (IS 210/211, IS 361, IS 362) support streaming parsers, clean feature extraction, and simple event/metric schemas.
- **Networks and infrastructure** (IS 205, IS 260) ground the failure taxonomy and the SNMP/syslog baseline.
- **Systems analysis, enterprise architectures, and project management** (IS 320, IS 300, PROM 210) inform requirements, a layered design (ingest → features → models → localization → UI), and a semester plan.
- **Security and strategy** (IS 250, IS 350) guide secure telemetry handling, RBAC for the dashboard, and value framing.

4.2 Scholarly and Technical Resources

I will use recent papers and accessible methods: Matrix Profile for BGP time series (Scott et al., 2024), multiscale sequence models as a supervised baseline (Cheng et al., 2021), topology-aware analyses for structure (Tan et al., 2024), and an operations-oriented study tying analytics to operator decisions (Mohammed et al., 2021). For logs, approachable unsupervised techniques (e.g., Isolation Forest / One-Class SVM) provide simple, interpretable starting points. Clear UML and architecture diagrams will keep the narrative plain and direct.

4.3 Development & Evaluation Resources

A containerized **virtual lab** (FRRouting with two spines, two ToRs, two edges, and multiple ”server” peers) will generate realistic BGP updates and logs. I will inject four representative failures—**one-way loss of signal, route-reflector crash, edge/provider outage, and server crash**—then compare the system’s alerts against a **baseline of manual SNMP/syslog triage**.

Evaluation Metrics: To demonstrate the practical value of this system, I will measure three key metrics that directly address operator pain points:

- **F1 Score** — Overall alert quality that balances how many real failures are caught (recall) with how few false alarms are raised (precision). This directly addresses the over-paging problem by ensuring alerts are both comprehensive and accurate.
- **Detection Delay** — Speed of response measured as time from failure onset to first alert, compared against the SNMP/syslog baseline. This quantifies the improvement in time-to-detection for faster incident response.
- **Hit@k** — Localization accuracy determining whether the true failure origin (device or network role) appears in the top-k suspects (e.g., Hit@1, Hit@3). This addresses the under-explanation problem by providing actionable guidance on where to investigate first.

Results will be summarized in a short paper, an 18-slide presentation, and a live demo that demonstrates these metrics in real-time.

5 Writing & Formatting

The paper will use **plain, professional language** and avoid jargon where possible, defining terms when needed (e.g., ”BGP updates” as ”routing change messages”). In-text **APA citations** will be included with a reference list.

References

Cheng, M., Li, Q., Lv, J., Liu, W., & Wang, J. (2021). Multi-scale lstm model for bgp anomaly classification. *IEEE Transactions on Services Computing*, *14*(3), 765–778.

Mohammed, S. A., Mohammed, A. R., Côté, D., & Shirmohammadi, S. (2021). A machine-learning-based action recommender for network operation centers. *IEEE Transactions on Network and Service Management*, *18*(3), 2702–2713.

Scott, B., Johnstone, M. N., Szewczyk, P., & Richardson, S. (2024). Matrix profile data mining for bgp anomaly detection. *Computer Networks*, *242*, 110257.

Tan, Y., Huang, W., You, Y., Su, S., & Lu, H. (2024). Recognizing bgp communities based on graph neural network. *IEEE Network*, *38*(6), 232–238.