

Machine Learning for Network Anomaly and Failure Detection

CUNY School of Professional Studies

Michael Hernandez

IS 499 Information Systems Capstone

Professor John Bouma

October 11, 2025

Contents

1	Introduction	2
2	Topic Description	2
2.1	In-depth Description of the Chosen Topic	2
2.2	Why This Topic Was Chosen	2
3	Problem Description	2
3.1	The Problem I am Trying to Solve	2
3.2	Why Current Monitoring Systems are Insufficient	3
4	Solution Discussion	3
5	Analysis	3
6	Research	4
7	References	5

1 Introduction

This paper examines machine learning techniques for detecting and localizing network anomalies and failures in large-scale environments, using data from BGP routing updates and SNMP metrics. Traditional monitoring approaches based on static thresholds produce excessive false positives and lack the ability to correlate anomalies across multiple data sources (Wang, 2020; Manna & Alkassabeh, 2019). By integrating unsupervised learning techniques such as Matrix Profile analysis (Mueen & Keogh, 2017; Scott et al., 2024) for routing data and Isolation Forest (Liu et al., 2008) for hardware telemetry, this project explores whether multi-modal correlation can provide incremental improvements in accuracy and operational relevance. The implementation emphasizes practical feasibility, scalability, and modest but meaningful reductions in alert fatigue.

2 Topic Description

2.1 In-depth Description of the Chosen Topic

Large networks contain thousands of devices, where failures can cascade rapidly. Operations teams must determine not only that a failure occurred, but where it originated and how much impact it has (Mohammed et al., 2021). Two key monitoring streams are BGP routing updates, which reflect how traffic paths change, and SNMP metrics, which reveal the state of individual devices (Rekhter et al., 2006; Cisco, 2006). Under normal conditions these follow predictable statistical patterns, but failures produce deviations such as route flapping (Scott et al., 2024) or sharp increases in error counters. Identifying and correlating these deviations provides a basis for anomaly detection.

Machine learning offers techniques to highlight unusual sequences and outliers in this data. Matrix Profile identifies anomalous subsequences, called discords, in BGP updates without requiring labeled data (Mueen & Keogh, 2017). Isolation Forest isolates outliers in multi-dimensional SNMP data (Liu et al., 2008), flagging hardware degradation or environmental instability. By combining evidence from both sources and incorporating topology awareness, the system aims to provide stronger confidence in genuine failure detection compared to single-source methods.

2.2 Why This Topic Was Chosen

The motivation comes from operational challenges: excessive alerts, lack of prioritization, and the manual effort required to correlate failures across systems (Skazin, 2021). In real environments, operators face hundreds of notifications when a single fault occurs, slowing response time. Research shows that correlating multiple telemetry sources can improve detection quality and reduce false positives (Feltin et al., 2023). This project does not attempt to create entirely new algorithms, but instead tests whether an integrated, topology-aware multi-modal system can provide measurable operational benefits.

3 Problem Description

3.1 The Problem I am Trying to Solve

The primary issue is that monitoring systems operate in silos. BGP and SNMP anomalies are tracked independently, threshold-based alerts lack contextual prioritization, and topology is ignored. Operators therefore must manually align logs, metrics, and routing updates to determine scope

and root cause. This project attempts to reduce that manual burden by aligning multiple anomaly streams automatically.

3.2 Why Current Monitoring Systems are Insufficient

Threshold monitoring provides a coarse tool for complex, dynamic environments. It cannot distinguish benign variation from genuine faults, and cannot prioritize failures by criticality. As a result, false positives remain high, while subtle but meaningful anomalies may be missed. Multi-source detection offers the potential to address these weaknesses by combining time-series analysis for routing, outlier detection for hardware, and topology-aware prioritization.

4 Solution Discussion

The implemented system processes data from two simulators—one generating BGP routing updates, the other generating SNMP device metrics—and analyzes them through dedicated pipelines before correlating results.

The **BGP pipeline** applies Matrix Profile on streaming updates using a sliding window architecture (Mueen & Keogh, 2017). As updates arrive, subsequences are compared, and anomalous discords are flagged when deviations exceed a threshold. This allows detection of novel routing instability without labeled training data.

The **SNMP pipeline** applies Isolation Forest, an ensemble method where anomalies are isolated with fewer decision tree splits (Liu et al., 2008). Metrics such as CPU, memory, temperature, and interface error counters are modeled against baseline behavior, and unusual deviations are flagged. A layered variant (Liu et al., 2024) was also tested for scalability on large datasets.

The **correlation agent** integrates both pipelines. Implemented in Python (`multimodal_correlator.py`), it ingests anomaly signals from BGP and SNMP, aligns them in time windows, and applies severity scoring based on topology. Failures in core devices receive higher priority than edge devices. This triage step reduces noise and emphasizes alerts most likely to impact critical systems.

A **real-time dashboard**, built with Streamlit, visualizes anomalies from both pipelines and their correlations. Panels display BGP message rates, SNMP metrics, and anomaly scores. Operators can inspect subsequence discord plots and feature-space outliers. The dashboard enables quick assessment of network health and provides contextualized alerts enriched with confidence scores and likely impact.

Testing relied on simulators producing realistic traffic with 98% baseline data and 2% anomalies. Failures included cable disconnects, route flaps, thermal overload, and combined routing-hardware problems. The system ran on a 20-device simulated topology with core, distribution, and access layers, supporting controlled evaluation while approximating real-world conditions.

Overall, the solution demonstrates a practical architecture for multi-modal anomaly detection and impact triage. It provides incremental operational value through correlation and visualization, without claiming to fully replace existing monitoring systems.

5 Analysis

System analysis focused on scalability, detection effectiveness, and trade-offs.

Scalability. Isolation Forest models trained on historical SNMP data (500,000 samples) scaled linearly with device count, requiring 1 KB overhead per additional device. Matrix Profile computa-

tions maintained $O(n \log n)$ complexity, processing multiple streams in parallel. At 1,000 simulated devices, throughput reached 921 samples per second, confirming feasibility for larger networks.

Detection performance. Controlled evaluation achieved perfect precision and recall (1.0) on known failure patterns due to tuned parameters and enriched features (see Figure ??). However, results on novel patterns were weaker, reflecting the limits of unsupervised detection. Mean detection delay was 29.4 seconds, below the 60-second operational target (see Figure ??).

Trade-offs. Aggregating features across devices supports scalability but sacrifices device-level attribution. The system detects anomalies but requires correlation to identify specific failing devices. Similarly, sliding window aggregation balances false positive reduction with latency: smaller windows increase sensitivity but raise noise, larger windows delay detection.

Operational impact. While modest, the improvements are meaningful. Multi-modal correlation reduces false positives and provides prioritization, lowering operator burden during incidents. Topology-aware triage highlights high-impact failures, assisting in resource allocation. The gains are incremental rather than revolutionary, but align with goals of reducing mean time to resolution (MTTR).

Limitations. All testing used simulators rather than production traffic, limiting generalizability. The system currently processes only BGP and SNMP data, leaving other modalities such as syslog or flow records for future work. Classifier performance is sensitive to parameter tuning, and additional validation on real-world data is needed.

6 Research

The project builds on established work in machine learning for anomaly detection. Mueen and Keogh (2017) introduced Matrix Profile as a universal time-series tool, later validated for BGP by Scott et al. (2024). Liu et al. (2008) proposed Isolation Forest for high-dimensional outlier detection, with layered variants showing improved performance on imbalanced data (Liu et al., 2024). Manna and Alkasassbeh (2019) demonstrated that SNMP-MIB groups carry predictive power for equipment failures, while Mohammed et al. (2021) highlighted the value of topology-aware ML in reducing operator burden. Feltin et al. (2023) emphasized feature selection as critical for fault diagnosis, supporting this project’s design of cross-modal correlation features.

Additional research provides context for future extensions. Cheng et al. (2021) achieved high accuracy in classifying BGP anomalies with LSTMs, showing potential for applying deep learning in this domain. Tan et al. (2024) demonstrated that graph neural networks can model BGP communities, suggesting possible future incorporation of topology learning. Benzekki et al. (2017) surveyed software-defined networking, linking anomaly detection to broader automation trends.

This capstone project contributes not by advancing algorithmic novelty, but by integrating proven methods into a practical architecture for multi-modal anomaly detection. Its significance lies in testing feasibility, scalability, and operational utility, showing how academic research can be translated into working tools for network operations. The approach demonstrates that modest improvements—reducing noise, adding prioritization, and enabling real-time visualization—can meaningfully support operators in complex environments.

7 References

References

- [1] 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. Available at: <https://doi.org/10.1109/TSC.2018.2824809>
- [2] 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. Available at: <https://doi.org/10.1109/TNSM.2021.3095463>
- [3] Mueen, A., & Keogh, E. (2017). Matrix Profile I: All Pairs Similarity Joins for Time Series. *ICDM 2016*, 1317–1322. Available at: <https://doi.org/10.1109/ICDM.2016.0179>
- [4] Scott, B., Johnstone, M. N., Szewczyk, P., & Richardson, S. (2024). Matrix Profile data mining for BGP anomaly detection. *Computer Networks*, 242, 110257.
- [5] 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. Available at: <https://doi.org/10.1109/MNET.2024.3414113>
- [6] Allagi, S., & Rachh, R. (2019). Analysis of Network log data using Machine Learning. *I2CT 2019*, 1–3. Available at: <https://doi.org/10.1109/I2CT45611.2019.9033528>
- [7] Skazin, A. (2021). Detection of network anomalies in log files. *IOP Conference Series: Materials Science and Engineering*, 1069(1), 012021. Available at: <https://doi.org/10.1088/1757-899X/1069/1/012021>
- [8] Feltin, T., Cordero Fuertes, J. A., Brockners, F., & Clausen, T. H. (2023). Understanding Semantics in Feature Selection for Fault Diagnosis. *NOMS 2023*, 1–9. Available at: <https://doi.org/10.1109/NOMS56928.2023.10154455>
- [9] Wang, H. (2020). Improvement and implementation of Wireless Network Topology System. *Computer Communications*, 151, 10–18. Available at: <https://doi.org/10.1016/j.comcom.2020.01.001>
- [10] Manna, A., & Alkasassbeh, M. (2019). Detecting network anomalies using machine learning and SNMP-MIB dataset with IP group. *arXiv preprint arXiv:1906.00863*. Available at: <https://arxiv.org/abs/1906.00863>
- [11] Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation Forest. *ICDM 2008*, 413–422. Available at: <https://doi.org/10.1109/ICDM.2008.17>
- [12] Liu, T., Zhu, Y., Xu, Q., Kong, X., & Yu, P. S. (2024). A layered isolation forest algorithm for outlier detection. *Neurocomputing*, 578, 127381. Available at: <https://doi.org/10.1016/j.neucom.2024.127381>
- [13] Zhou, J., Qian, Y., Zou, Q., Liu, P., & Xiang, J. (2022). DeepSyslog: Deep Anomaly Detection on Syslog Using Sentence Embedding. *IEEE TIFS*, 17, 3051–3066. Available at: <https://doi.org/10.1109/TIFS.2022.3198188>

- [14] Powers, D. M. W. (2011). Evaluation: From Precision, Recall and F-Measure to ROC, Informedness, Markedness & Correlation. *Journal of Machine Learning Technologies*, 2(1), 37–63.
- [15] Järvelin, K., & Kekäläinen, J. (2002). Cumulated Gain-Based Evaluation of IR Techniques. *ACM TOIS*, 20(4), 422–446. Available at: <https://doi.org/10.1145/582415.582418>
- [16] Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2017). Software-Defined Networking (SDN): A Survey. *Security and Communication Networks*, 2017, 9739131. Available at: <https://doi.org/10.1155/2017/9739131>
- [17] Cisco Systems. (2006). Understanding Simple Network Management Protocol (SNMP) Traps. Cisco Technical Documentation. Available at: <https://www.cisco.com/c/en/us/support/docs/ip/simple-network-management-protocol-snmp/7244-snmp-trap.html>
- [18] Sommerville, I. (2016). *Software Engineering* (10th ed.). Pearson Education Limited.
- [19] Rekhter, Y., Li, T., & Hares, S. (2006). A Border Gateway Protocol 4 (BGP-4). RFC 4271, IETF. Available at: <https://www.rfc-editor.org/rfc/rfc4271>