A Hybrid Network Management approach: integrating Traditional Protocols and Intelligent Monitoring System for Effective Fault Detection and performance optimization.

Piyush Pardesi
Department of Computing Technologies
SRM Institute of Science and Technology
Chennai, India
pp3055@srmist.edu.in

Maddali Manikanta
Department of Computing Technologies
SRM Institute of Science and Technology
Chennai, India
mm0684@srmist.edu.in

Dr. Rajasekaran P
Department of Computing Technologies
SRM Institute of Science and Technology
Chennai, India
rajasekp2@srmist.edu.in

Abstract*—Network management is one of the essential factors which maintain the overall performance, scalability and relia-bility of present communication infrastructures. Traditionally, Simple Network Management protocol (SNMP) and Remote Monitoring (RMON) protocols have been used for the purpose of monitoring of a network since they have standard defined mechanisms. These protocols were inherently limited to reactive network performance monitoring as they were mostly poll-based. With increase in size and complexity of networks, modern protocols such as streaming telemetry, SDN (Software defined networks), and machine learning-based monitoring techniques have come up for gaining higher real-time visibility and predict-ing faults. However, the significant issue lies in the complexity they pose and their incapability to integrate into the legacy environments without drastic changes. In this paper we provide a comprehensive study of these architectures, discuss their pros and cons. Based on the discussed analysis, a three-layered hybrid architecture has been proposed which combines both the conventional protocol mechanisms and the intelligence provided by modern telemetry and AI-based analytics, thereby leading to improvement in fault detection rates and optimization of the network performance. Also, the study discusses a migration path toward such a hybrid network management system and the open research issues.

***Index Terms*—Network Management, SNMP, RMON, Streaming Telemetry, Machine Learning, Hybrid Architecture, Fault Detection, SDN, Performance optimization, Anomaly detection.**

I. Introduction

The networks have now evolved to such a vastness and heterogeneous nature due to rise of distributed computing, cloud computing and enterprise network deployments that an effective network management system is of critical importance for maintainability, scalability and continuous operation. Net-work management is an ongoing process that encompasses: monitoring the behavior of devices and traffic, the ability to detect, identify and localize faults rapidly, performance evaluation, and the execution of remedial actions.

Traditional protocols such as SNMP and RMON, the two pillars of network management, have been developed for the task of collecting statistical information on network devices through a poll-based mechanism with exception-handling using traps, since the overhead associated with it was lower and it was easily implementable across a variety of devices from different vendors. However, their reactive, poll-driven nature means that faults in such architectures are detected only after they occur, thus delaying troubleshooting and potentially leading to significant service disruptions.

Modern telemetry protocols such as streaming telemetry have a push-based mechanism to send continuous data, while SDN has enabled centralized network control for efficient management and automation. Furthermore, machine learning and AI have been widely adopted for performing various tasks such as: traffic classification, anomaly detection and fault prediction from network data streams. The above-mentioned modern approaches have not been effectively adapted for organizations operating legacy networks due to significant changes needed in the infrastructure, specialized skillset, and high computing costs.

To bridge this gap between the legacy systems and modern approaches to monitoring, a hybrid architecture can be adopted which attempts to incorporate modern techniques with the al-ready established ones in a gradual manner, without discarding the current infrastructure entirely. A structured overview of both the approaches, the respective benefits and drawbacks, and the proposed hybrid architecture are discussed herein. The major research challenge here is to design a consolidated system to manage the conventional protocols in an intelligent

manner, and the architecture proposed herein achieves exactly that in a layered fashion, providing the means for faster fault detection and performance optimization.

II. Background

A. Network Management and the FCAPS Model

Network management encompasses the suite of tools, proce-dures, and protocols designed to monitor, manage, and main-tain network infrastructure. It is typically partitioned into five functional domains, as established by the FCAPS taxonomy: Fault Management, Configuration Management, Accounting Management, Performance Management, and Security Man-agement [1]. Fault and Performance management are directly responsible for the effective delivery of services and ensuring a reliable experience for network users.

B. Simple Network Management Protocol (SNMP)

The SNMP employs a client-server architecture with an NMS (Network Management Station) and SNMP agents re-siding on various devices on the network. All network infor-mation is presented in the form of Management Information Bases (MIBs) – hierarchies of typed variables which provide an abstract representation of the state of the device. The two methods used in SNMP to access MIB information are by a managed entity periodically polling agents at certain time intervals, and by the SNMP agent sending trap messages upon triggering an event [2].

Though, SNMP has proven to be cost-effective, widely supported, and is relatively simple to deploy, the polling nature of SNMP induces latencies that are directly proportional to the polling interval and also consumes substantial bandwidth of the network when deployed at a larger scale, lacking any mechanisms for prediction and self-adaptation.

C. Remote Monitoring (RMON)

RMON is an extension of SNMP, where a monitoring device (probe) that resides at a network segment performs local mon-itoring of the traffic in the particular segment. RMON1 (data-link layer probe) analyzes MAC address, error counts, packet types, collisions etc., whereas RMON2 (network layer probe) is a more advanced monitoring system which also collects IP related statistics such as packet sizes, packet flow etc. This approach reduce the polling traffic to the NMS, though retaining its inherent characteristics of limited intelligibility and reactive monitoring [3].

TABLE I
Comparison of Traditional Network Management Protocols

Feature	SNMP	RMON
Monitoring Type	Device-level	Network-level
Data Collection	Polling + Traps	Distributed Probes
Scalability	Limited	Moderate
Intelligence	Low	Low
Complexity	Low	Medium
Real-time Capability	Limited	Moderate
Fault Prediction	Not supported	Not supported

III. Literature Review

A. Traditional monitoring and Fault Detection

One of the earliest works in the domain of fault localization in network systems was by Steinder and Sethi [1], which gave a taxonomy based on rules, models and inferences for fault diagnosis and management. These techniques still hold significance for troubleshooting modern network systems, though they lacked the capability of real-time analysis and static rule sets had limitations of becoming obsolete.

B. The Evolution to Modern Monitoring Architectures

The transition towards modern and efficient network man-agement architectures has been highlighted by various re-searchers in their surveys of network monitoring protocols. Lee et al. [3] traced the evolution from centralized, poll based management systems to event-driven and distributed network monitoring solutions and attributed the failure of SNMP to scalability issues for cloud deployments. Further with the emergence of SDN, there was a transformation of traditional network monitoring with centralized, dynamic network control provided through decoupling the control and data plane as explained by Kreutz et al. [4] and also a detailed review on programmable network architectures was given by Nunes et al. [5]. Though modern techniques possess enhanced visibility and flexibility, issues such as security concerns and complexity remained.

C. Machine Learning based Intelligent Monitoring

The use of Machine Learning has greatly improved the performance of network feature measurement, with accurate anomaly detection rates over threshold-based methods [9]. Follow-up work in this direction include the development of an AI driven telemetry network [10] for in-network anomaly detection, intent based networking architectures [7] which can abstract high level network behavior and translate it to actual device configurations, and an ML based control charts for real-time network monitoring with reduced anomaly detection false-alarm rates [12].

D. Hybrid/Transition Approaches

Hybrid SDN architectures which allow legacy systems to function along-side programmable network elements were considered most feasible for large network operators [6], while other works survey standards and protocols related to intent based network architectures and highlight the benefits of integration of traditional methods into these infrastruc-tures [8]. From these literature sources, a clear research gap emerges which has been addressed in the subsequent sections, by proposing a hierarchical three-layer network management model.

IV. Comparative Analysis

To set the groundwork for a hybrid network management system, a detailed comparison of traditional, modern, and hybrid network management strategies must be performed. Six

important operational parameters have been considered for the evaluation.

Traditional SNMP and RMON-based monitoring systems are low-complexity, low-cost and backed by years of tools and vendors. However, their polling nature results in high network overhead as the device count increases, and their simple thresholding is insufficient to detect fine-grained or novel fault patterns before impacting service. Modern, ML-based telemetry and SDN systems can address these shortcomings with high-fidelity, continuous telemetry and adaptive detection, but come with increased deployment complexity and cost and require significant, well-labeled datasets to train on.

The hybrid approach takes a middle path that organizations can find to be highly productive. It leverages SNMP/RMON for inventory and basic alerting, but utilizes telemetry and ML over that infrastructure for fast and predictive alerting. It thus offers both fast detection and predictive capability without the full cost of replacing its existing network monitoring infrastructure. As can be seen from the results cited across this work, network management performance increases with more timeliness data-polling based monitoring delays MTTD, while continuous telemetry combined with ML shortens MTTD and hence MTTR.

TABLE II
COMPARATIVE ANALYSIS OF NETWORK MANAGEMENT APPROACHES

Parameter	**Traditional (SNMP/RMON)**	**Modern (Telemetry/ SDN/AI)**	**Proposed Hybrid**
Scalability	Low	High	Medium–High
Detection Speed	Slow	Fast	Fast
Network Overhead	High (polling)	Moderate–High	Optimized
Implementation Complexity	Low	High	Medium
Intelligence Level	Low	High	Medium–High
Cost	Low	High	Moderate
Real-time Monitoring	Limited	Strong	Strong
Fault Prediction	Not supported	Supported	Partially supported

Note: Scores are qualitative representations derived from literature analysis.

V. PROPOSED HYBRID MODEL

A. System Overview

The proposed system is implemented using a three-layer architecture where each layer provides unique and complementary functionality and communicates using well-defined interfaces so that layers are easily modifiable and replaceable.

Layer 1 – Legacy monitoring infrastructure: SNMP agents, monitoring network devices for metrics such as interface statistics, CPU usage, error counters, and RMON probes for network traffic aggregates. This data is stored in a local or central database where it is used for defining alerting thresholds and configuration inventory.

Metric	Traditional	Modern	Hybrid
Scalability	3	9	8
Detection Speed	3	9	8
Intelligence	2	9	7
Cost Efficiency	9	4	7

TABLE III
PERFORMANCE COMPARISON: TRADITIONAL VS. MODERN VS. HYBRID (QUALITATIVE SCORES, SCALE 1–10)

Layer 2 – Streaming telemetry: agents push high-granularity, real-time network telemetry to a data collection bus (e.g. Apache Kafka or gRPC based streaming interfaces) which provide data for the upper analytics layers that have a much finer temporal resolution than SNMP polling interval.

Layer 3 – Intelligence Analytics: Machine learning models are trained on the telemetry data collected over time, historical fault data, for real-time anomaly detection, traffic characteriza-tion, and predictive failure analysis. Results of the ML models are either presented as actionable alerts to the operator or translated to commands sent back to the network elements (if SDN integration is possible).

B. How It Works

Both the data from layer 1 and 2 streams to the analytics pipeline after appropriate normalization. Supervised learning techniques are employed to recognize known patterns of failures while unsupervised techniques identify emerging anomalies in traffic. Alerts are shown to the operator as they are determined with appropriate weighting, with critical alerts triggering automated response and human-in-the-loop action taken on other events.

C. Advantages of the Proposed System

The benefits of the hybrid architecture over both pure traditional and pure modern networks include. Detection time for faults is drastically reduced because the telemetry layer continuously streams data to the analytics engine rather than polling for information. Throughput requirements can be handled by the distributed telemetry bus and the intelligence does not grow linearly with the device count. The system does not require a high level of initial investment as the legacy infrastructure does not need to be discarded and the modern

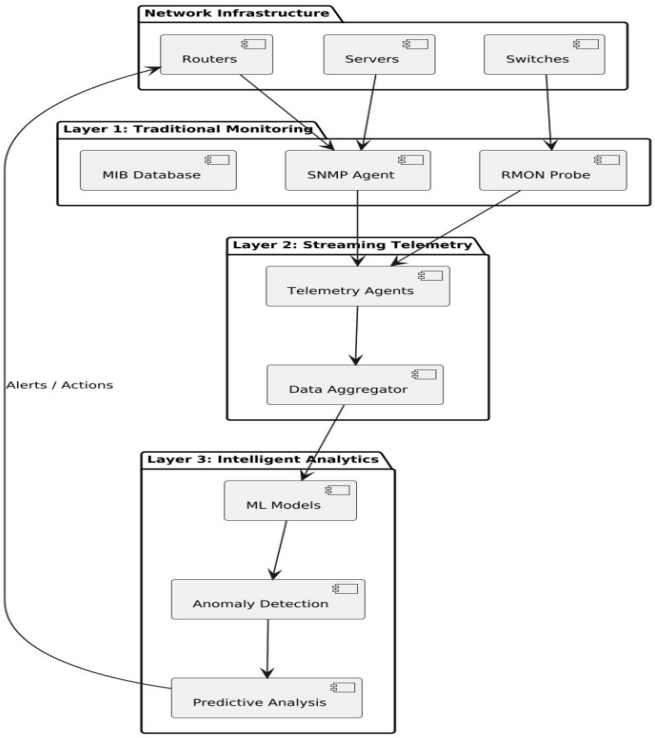


Fig. 1. Proposed Three-Layer Hybrid Network Management Architecture.

systems are implemented on top of the existing ones and this enables migration path – organizations can use Layer 1 only first and later add Layer 2 and Layer 3.

TABLE IV
FEATURE COMPARISON: TRADITIONAL VS. MODERN VS. PROPOSED HYBRID

Feature	Traditional	Modern	Proposed Hybrid
Reliability	High	Medium	High
Scalability	Low	High	High
Intelligence	Low	High	Medium–High
Deployment Cost	Low	High	Moderate
Deployment Ease	Easy	Difficult	Moderate
Fault Detection Speed	Slow	Fast	Fast
Legacy Compatibility	Full	Partial	Full

VI. CHALLENGES AND FUTURE SCOPE

A. Implementation Challenges

A significant challenge that would be encountered when deploying such a hybrid system is integration. Polled based SNMP relies on static and structured communication, but streaming telemetry involves transmitting large streams of data of varying sizes with different communication semantics; hence careful designing of ingestion pipelines, normalization layers and data schemas is critical. Many network elements in the network infrastructure have differing level of capabilities, varying firmware, vendor-specific MIBs; thereby requiring development of adaptable parsers.

Significant amount of data will be generated by the layer 2 so data compression, filtering and sampling will be required to prevent storage and computation limits being reached. Machine learning layer will impose computation requirement in line with the models and it can be offloaded to the cloud or to the network edges. Security is also a factor since older SNMP versions lack secure mechanisms for encryption or authentication [2], telemetric data may expose sensitive topology information and the machine learning models are vulnerable to adversarial attacks.

B. Research Directions

Further research is required to develop models capable of detecting faults on a new 5G and even 6G network with extremely tight deadlines and vast number of connected devices; to be implemented on edge infrastructure for minimal detection delay; to embed zero trust security principles into the management plane, and to develop common management APIs with a standardized schema, similar to what exists for SNMP with NETCONF/YANG.

VII. CONCLUSION

This paper analyzes the evolution of network management from traditional SNMP/RMON based solutions to modern telemetry-based AI powered solutions, highlighting limitations with both approaches. A three-layered hybrid model utilizing legacy monitoring features along with modern, real-time and predictive intelligence is presented. Comparison reveals that the hybrid model is scalable and dramatically faster than traditional monitoring systems and yet significantly less expensive and less complex than modern monitoring systems.

The presented approach offers a practical path toward the management of heterogeneous infrastructure and ensures existing infrastructure is well utilized, while also being capable of accommodating newer technologies as required. Such issues as integration complexity, data volume management, computational burden, and security are all challenging areas that require much more research.

In summary, the future of network management involves neither one solution but an integrated set of approaches working together. A hybrid model like that of the paper provides a foundation toward networks that are scalable, intelligent and also reliable.

APPENDIX: DIAGRAM AND GRAPH

Fig. 2: Evolution of Network Management

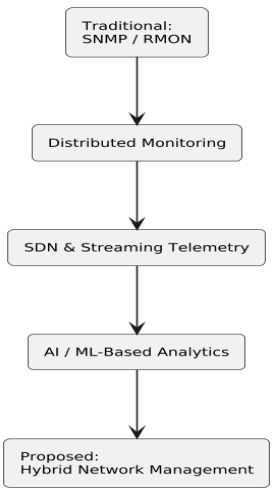
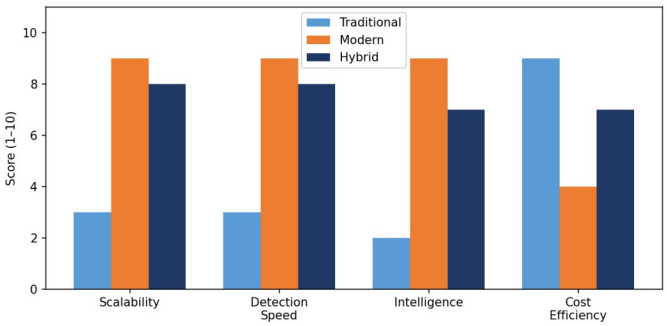


Fig. 3: Performance Comparison Graph



REFERENCES

[1] M. Steinder and A. S. Sethi, "A survey of fault localization techniques in computer networks," *Science of Computer Programming*, vol. 53, no. 2, pp. 165–194, 2004. DOI: 10.1016/j.scico.2004.01.010

[2] D. R. Kuhn, B. J. Walsh, and S. Fries, "Security considerations for SNMPv3," *NIST Special Publication 800-78*, 2013.

[3] T. Lee, H. Levanti, and H. Kim, "Network monitoring: Present and future," *Computer Networks*, vol. 65, pp. 84–98, 2014. DOI: 10.1016/j.comnet.2014.03.007

[4] D. Kreutz et al., "Software-defined networking: A comprehensive sur-vey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, Jan. 2015.
DOI: 10.1109/JPROC.2014.2371999

[5] B. A. Nunes et al., "A survey of software-defined networking: Past, present, and future of programmable networks," *Journal of Net-work and Computer Applications*, vol. 67, pp. 1–25, 2016. DOI: 10.1016/j.jnca.2016.03.016

[6] S. Khorsandroo et al., "Hybrid SDN evolution: A compre-hensive survey," *Computer Networks*, vol. 192, 2021. DOI: 10.1016/j.comnet.2021.107981

[7] E. Zeydan and Y. Turk, "Recent advances in intent-based networking: A survey," in *Proc, IEEE 91st Veh. Technical. Conf. (VTC2020-Spring),* 2020. DOI: 10.1109/VTC2020-Spring48590.2020.9128422

[8] A. Leivadeas and N. Falkner, "A survey on intent-based networking," *IEEE Communications Surveys & Tutorials,* vol. 25, no. 1, pp. 625-655, 2022. DOI: 10.1109/CMST.2022.3215919

[9] Y. Sun et al., "A survey: Network features measurement based on machine learning," *Applied Sciences,* vol. 13, no. 4, 2023. DOI: 10.3390/app13042551

[10] M. Foroughi, F. Brockners, and J. Rougier, "AI-driven network telemetry processing on routers," *Computer Networks,* vol. 221, 2023. DOI: 10.1016/j.comnet.2022.109474

[11] S. Harsh et al., "Flock: Accurate network fault localization at cloud scale," in *Proc. ACM SIGCOMM,* 2023. DOI: 10.1145/3595289

[12] H. Hao et al., "A network surveillance approach using machine learning-based control charts," *Experts Systems with Applications,* vol. 213, 2023. DOI: 10.1016/j.eswa.2023.119660