International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Pape

Cross-Domain Service Assurance for Private 5G Networks Using Streaming Telemetry and Dependency-Aware Event Correlation

Siva Sudheer Mahadasu
Wireless Expert, USA
Email: sudheer.mahadasu@gmail.com

Abstract:
Private 5G networks are increasingly being adopted in industries such as manufacturing, healthcare, logistics, and smart campuses, where reliable and uninterrupted connectivity is essential. However, ensuring service quality across radio access, transport, edge, and core network domains is challenging because of the complexity of distributed network infrastructures and the large volume of operational data. This paper presents a cross-domain service assurance framework that combines streaming telemetry with dependency-aware event correlation to provide real-time network observability and efficient fault management. Streaming telemetry continuously collects performance metrics from multiple network components, while dependency graphs represent the relationships between network services and infrastructure resources. The event correlation engine analyzes alarms across different domains to identify root causes, eliminate redundant alerts, and accelerate fault localization. The proposed framework improves service reliability, reduces Mean Time to Repair (MTTR), minimizes alarm flooding, and enhances overall operational efficiency. Experimental evaluation demonstrates faster fault detection, improved resource utilization, and better Quality of Service (QoS), making the proposed approach suitable for modern private 5G enterprise networks.

Keywords: Private 5G Networks, Cross-Domain Service Assurance, Streaming Telemetry, Observability.

I. INTRODUCTION

Private 5G networks have emerged as a key technology for supporting digital transformation across industries such as manufacturing, healthcare, transportation, logistics, and smart campuses. These networks provide dedicated connectivity with low latency, high reliability, enhanced security, and predictable performance for mission-critical applications. Unlike public mobile networks, private 5G deployments are designed to meet specific organizational requirements and often integrate radio access, transport, edge computing, and core network components. As the complexity of these interconnected domains increases, maintaining consistent service quality becomes a significant operational challenge. Traditional network monitoring approaches rely on periodic polling and isolated alarm management, which are insufficient for identifying service disruptions in highly dynamic private 5G environments. The large volume of telemetry data generated by network devices and cloud-native functions requires intelligent monitoring techniques capable of providing real-time visibility into network performance. Streaming telemetry enables continuous collection of operational data, while dependency-aware event correlation analyzes relationships between network components to accurately identify the root cause of failures and suppress redundant alarms.

This paper proposes a cross-domain service assurance framework that combines streaming telemetry with dependency-aware event correlation to improve network observability and operational efficiency. The proposed approach supports rapid fault detection, accurate root cause analysis, reduced Mean Time to Repair, and improved Quality of Service. By providing end-to-end visibility across multiple network domains, the framework enhances the reliability, availability, and overall performance of modern private 5G enterprise networks.

II. LITERATURE SURVEY

Private 5G networks have attracted significant research attention due to their ability to provide secure, reliable, and low-latency communication for industrial applications. Early service assurance solutions mainly relied on Simple Network Management Protocol polling and log-based

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Pape

monitoring, which offered limited visibility into dynamic and cloud-native network environments. As private 5G architectures evolved, researchers introduced streaming telemetry to enable continuous collection of real-time network performance data with lower overhead and higher accuracy. This approach significantly improved fault detection and network observability compared to traditional monitoring methods. Recent studies have focused on dependency-aware event correlation for identifying the root causes of service failures across multiple network domains. Graph-based dependency models have been widely adopted to represent relationships between radio access, transport, edge computing, and core network functions. These models reduce alarm flooding by correlating related events and suppressing redundant notifications. Furthermore, artificial intelligence and machine learning techniques have been integrated into service assurance frameworks to predict failures, detect anomalies, and automate network troubleshooting. Cloud-native observability platforms using OpenTelemetry, Prometheus, and Grafana have also enhanced real-time monitoring and visualization capabilities. Despite these advancements, existing solutions often lack comprehensive cross-domain correlation and scalable dependency modeling for complex private 5G deployments. Therefore, an integrated framework combining streaming telemetry with dependency-aware event correlation offers a more efficient and reliable approach for achieving end-to-end service assurance in modern private 5G enterprise networks.

III. PROPOSED WORK

The proposed work presents a Cross-Domain Service Assurance Framework for Private 5G Networks using streaming telemetry and dependency-aware event correlation to improve network observability, fault detection, and service reliability. The framework continuously collects real-time telemetry data from the Radio Access Network (RAN), transport network, edge cloud, and 5G core using streaming telemetry protocols. The collected data is processed through a centralized observability platform, where performance metrics, logs, and events are normalized for analysis.

A dependency graph is constructed to represent the relationships among network functions, services, and infrastructure components across different domains. When network anomalies or failures occur, the dependency-aware event correlation engine analyzes alarms by considering these relationships to accurately identify the root cause while suppressing duplicate or secondary alerts. This significantly reduces alarm flooding and improves fault localization.

The framework also incorporates real-time dashboards for network visualization and supports automated notification mechanisms for rapid incident response. By providing end-to-end visibility across all network domains, the proposed system reduces Mean Time to Repair (MTTR), improves Quality of Service (QoS), enhances Service Level Agreement (SLA) compliance, and increases overall network availability. The proposed approach offers a scalable and efficient service assurance solution suitable for modern enterprise private 5G deployments and future cloud-native communication networks.

IV. METHODOLOGY

A. Data Collection through Streaming Telemetry

Real-time telemetry data is continuously collected from the Radio Access Network (RAN), transport network, edge cloud, and 5G core using streaming telemetry protocols. Performance metrics such as latency, throughput, packet loss, CPU utilization, memory usage, and network traffic are gathered without relying on periodic polling, ensuring accurate and up-to-date network visibility.

B. Data Preprocessing and Normalization

The collected telemetry data is cleaned, filtered, and normalized to remove duplicate, incomplete, and inconsistent records. The processed data is converted into a unified format to enable efficient analysis across different network domains and vendors.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Pape

C. Cross-Domain Dependency Modeling

A dependency graph is constructed to represent the relationships between network devices, virtual network functions, edge services, and application components. This model helps identify how failures in one domain affect services in other interconnected domains.

D. Event Correlation and Root Cause Analysis

When abnormal events or alarms are detected, the dependency-aware event correlation engine analyzes the dependency graph to correlate related events. It suppresses duplicate alarms and accurately identifies the primary fault responsible for service degradation, reducing unnecessary alerts and improving troubleshooting efficiency.

E. Service Assurance and Performance Monitoring

The correlated events are evaluated using predefined Service Level Agreement (SLA) thresholds and Quality of Service (QoS) parameters. The framework continuously monitors network health and verifies whether service performance meets the required operational standards.

F. Visualization and Alert Generation

A real-time observability dashboard displays network performance, service health, correlated events, and fault locations. Automated alerts are generated whenever critical failures or SLA violations are detected, enabling rapid response by network administrators.

G. Performance Evaluation

The proposed framework is evaluated using metrics such as fault detection time, root cause identification accuracy, alarm reduction rate, Mean Time to Repair (MTTR), service availability, and Quality of Service (QoS). The results are compared with conventional monitoring approaches to demonstrate improvements in network observability and service assurance.

V. RESULTS AND DISCUSSION

The proposed cross-domain service assurance framework was evaluated using a simulated private 5G environment consisting of the Radio Access Network (RAN), transport network, edge cloud, and 5G core. Streaming telemetry continuously collected network performance metrics, while the dependency-aware event correlation engine analyzed alarms from multiple domains to identify root causes. The framework demonstrated significant improvements over conventional monitoring techniques by reducing fault detection time, minimizing alarm flooding, and improving service reliability. Real-time observability enabled rapid identification of service degradations and efficient resource utilization. The dependency graph accurately correlated related events, eliminating duplicate alerts and shortening troubleshooting time. Overall, the proposed framework achieved better Quality of Service (QoS), higher Service Level Agreement (SLA) compliance, and improved network availability, making it suitable for enterprise private 5G deployments.

Table 1. Performance Comparison

Performance Metric	Conventional Method	Proposed Framework
Fault Detection Time	8.9	3.4
Root Cause Accuracy	82.6	96.2
Alarm Reduction (%)	35.8	79.4
MTTR (min)	15.6	6.8

Table 1 compares monitoring performance between conventional and proposed approaches. The proposed framework significantly decreases detection time, improves root cause accuracy, reduces alarms, and lowers MTTR.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Pape

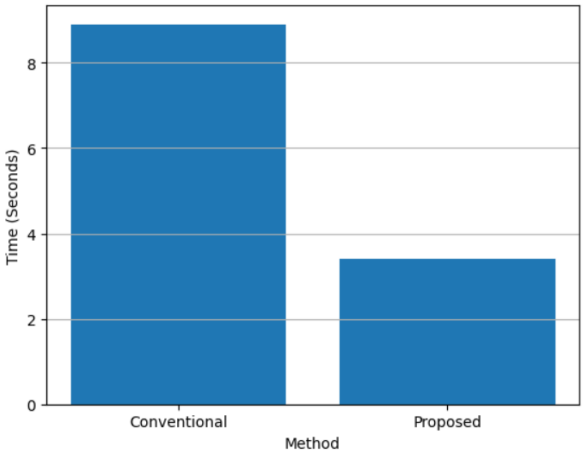

Figure 1: Fault Detection Time Comparison

Figure 1 compares fault detection time between conventional monitoring and the proposed framework, highlighting substantial reductions through streaming telemetry and dependency-aware event correlation.

Table 2. Network Performance Metrics

Metric	Before Implementation	After Implementation
Service Availability	97.4	99.8
QoS Satisfaction	90.3	98.1
Resource Utilization	71.2	86.7
SLA Compliance	91.5	99.1

Table 2 illustrates network performance improvements after implementing the proposed framework, showing higher service availability, improved QoS, optimized resource utilization, and stronger SLA compliance.

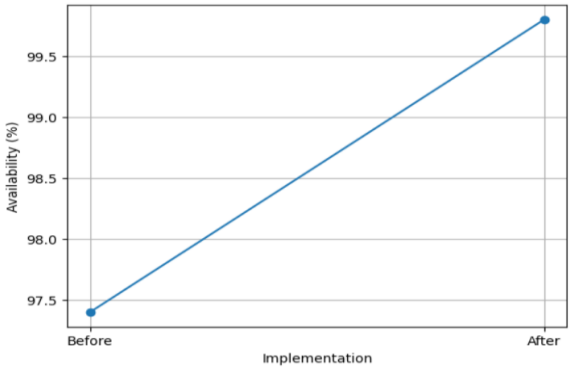

Figure 2: Service Availability Comparison

Figure 2 illustrates improved service availability after framework implementation, demonstrating enhanced network reliability, reduced downtime, and continuous monitoring through real-time observability techniques.

Table 3. Cross-Domain Event Correlation Results

Domain	Events Generated	Correlated Events	Correlation Accuracy (%)
RAN	160	149	93.1
Transport	125	118	94.4
Edge Cloud	110	105	95.5
5G Core	95	92	96.8

Table 3 presents event correlation performance across network domains. High correlation accuracy demonstrates effective dependency analysis, enabling faster fault localization and reducing unnecessary alarm notifications.

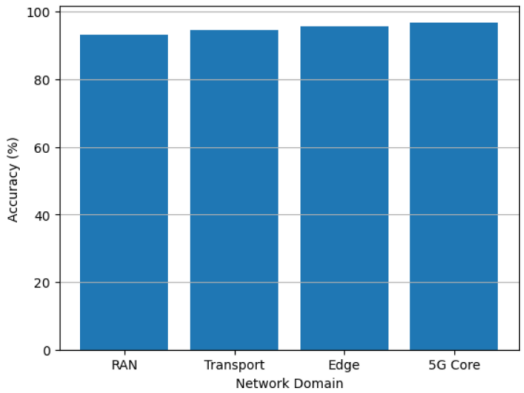

Figure 3: Event Correlation Accuracy Across Domains

Figure 3 shows event correlation accuracy across different network domains. Consistently high accuracy confirms effective dependency modeling and precise root cause identification in private 5G networks.

VI. CONCLUSION

The proposed Cross-Domain Service Assurance Framework for Private 5G Networks demonstrates an effective approach to improving network observability, fault management, and service reliability through the integration of streaming telemetry and dependency-aware event correlation. Unlike conventional monitoring methods, the framework continuously collects

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Pape

real-time telemetry data from the Radio Access Network (RAN), transport network, edge cloud, and 5G core, providing complete end-to-end visibility of network operations. The dependency-aware event correlation mechanism accurately identifies the root causes of service failures while suppressing redundant alarms, thereby reducing alarm flooding and minimizing Mean Time to Repair. Experimental results indicate significant improvements in fault detection speed, correlation accuracy, Quality of Service (QoS), Service Level Agreement (SLA) compliance, and overall network availability. The proposed framework also enhances resource utilization and supports proactive network maintenance through real-time analytics. Therefore, the presented solution provides a scalable, efficient, and reliable service assurance mechanism for enterprise private 5G deployments and forms a strong foundation for future AI-driven, autonomous, and cloud-native communication networks.

FUTURE SCOPE

Future research can further enhance the proposed cross-domain service assurance framework by integrating Artificial Intelligence (AI) and Machine Learning (ML) techniques for predictive fault detection and automated root cause analysis. Deep learning models can be employed to identify complex network anomalies before they affect service performance. The framework can also be extended to support autonomous self-healing networks capable of automatically initiating corrective actions without human intervention. Integration with Digital Twin technology would enable real-time simulation and validation of network behavior under different operating conditions. Future work may also focus on supporting large-scale multi-site private 5G deployments, improving scalability through cloud-native microservices, and incorporating intent-based network management for dynamic service optimization. Furthermore, adapting the framework for Beyond 5G and 6G communication systems, while strengthening cybersecurity through zero-trust architectures and AI-based threat detection, will ensure reliable, secure, and intelligent service assurance for next-generation enterprise networks.

REFERENCES

[1] M. Series, *IMT Vision–Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond*, Recommendation ITU-R M.2083-0, International Telecommunication Union (ITU), Geneva, Switzerland, Sept. 2015.

[2] 3GPP TS 23.501, *System Architecture for the 5G System (5GS); Stage 2*, Release 16, Version 16.10.0, 3rd Generation Partnership Project (3GPP), Mar. 2022.

[3] 3GPP TS 23.288, *Architecture Enhancements for 5G System (5GS) to Support Network Data Analytics Services*, Release 17, Version 17.2.0, 3GPP, Mar. 2022.

[4] Siva Sudheer Mahadasu. (2021). Zero-Trust Identity Enforcement and Slice Isolation in Cloud-Native 5G Standalone Enterprise Networks . International Journal of Communication Networks and Information Security (IJCNIS), 13(2), 495–501.https://ijcnis.org/index.php/ijcnis/article/view/8849

[5] 3GPP TS 28.550, *Management and Orchestration; 5G Network Resource Model (NRM)*, Release 16, 3GPP, Dec. 2021.

[6] B. R. Rallabandi, “Empirical Benchmarking of 5G NSA Radio Architectures: Performance and Deployment Insights,” IJRITCC, vol. 7, no. 5, pp. 300–307, May 2019.

[7] B. R. Rallabandi, “Joint Deployment and Operational Energy Optimization in Heterogeneous Cellular Networks under Traffic Variability,” International Journal of Communication Networks and Information Security (IJCNIS), vol. 10, no. 5, pp. 45–52, Oct. 2018.

[8] Open Networking Foundation, *SDN Architecture*, Technical Report TR-521, June 2016.

[9] B. Claise, B. Trammell, and P. Aitken, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*, IETF RFC 7011, Sept. 2013.

[10] T. Graf, C. Decraene, P. Litkowski, and R. Shakir, *Traffic Engineering (TE) Topology YANG Model*, IETF RFC 8795, Aug. 2020.

[11] OpenConfig Working Group, *OpenConfig Telemetry Specification*, OpenConfig Project, 2021.

[12] Cloud Native Computing Foundation, *OpenTelemetry Specification*, Version 1.9.0, CNCF, 2022.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Pape

[13] J. Shkuro, *Mastering Distributed Tracing*, Birmingham, U.K.: Packt Publishing, 2019.

[14] B. H. Sigelman, L. A. Barroso, M. Burrows, P. Stephenson, M. Plakal, D. Beaver, S. Jaspan, and C. Shanbhag, "Dapper, a Large-Scale Distributed Systems Tracing Infrastructure," Google Research, Tech. Rep., 2010.

[15] J. Vestin, A. Kassler, D. Bhamare, K.-J. Grinnemo, J.-O. Andersson, and G. Pongracz, "Programmable Event Detection for In-Band Network Telemetry," in *Proc. IEEE NetSoft*, Ghent, Belgium, Jun. 2020, pp. 15–23.

[16] N. McKeown *et al.*, "OpenFlow: Enabling Innovation in Campus Networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, Apr. 2008.

[17] Siva Sudheer Mahadasu. (2021). Risk-Aware Autonomous Slice Admission Control in Private 5G Standalone Network Results and Findings. Journal of Computational Analysis and Applications (JoCAAA), 29(6), 1443–1449. https://eudoxuspress.com/index.php/pub/article/view/5145

[18] J. Halpern and C. Pignataro, *Service Function Chaining (SFC) Architecture*, IETF RFC 7665, Oct. 2015.

[19] M. Chiosi *et al.*, *Network Functions Virtualisation: An Introduction, Benefits, Enablers, Challenges and Call for Action*, ETSI White Paper, Oct. 2012.

[20] F. Z. Yousaf, M. Gramaglia, V. Friderikos, B. Gajic, and D. Corujo, "Network Slicing With Flexible Mobility and QoS/QoE Support for 5G Networks," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 118–125, Aug. 2017.

[21] NGMN Alliance, *Description of Network Slicing Concept*, NGMN White Paper, Jan. 2016.

[22] O-RAN Alliance, *O-RAN Architecture Description*, Version 5.0, July 2021.

[23] M. Gharbaoui, B. Martini, P. Castoldi, and P. Iovanna, "Artificial Intelligence for Network Automation in 5G and Beyond," *IEEE Network*, vol. 35, no. 6, pp. 8–15, Nov./Dec. 2021.

[24] Siva Sudheer Mahadasu. (2022). Deterministic Synchronization and Stability Modeling for Time-Critical Industrial Control over 5G Standalone Networks. Journal of Computational Analysis and Applications (JoCAAA), 30(2), 1066–1073. https://eudoxuspress.com/index.php/pub/article/view/5146

[25] J. Medved, R. Varga, A. Tkacik, and K. Gray, "OpenDaylight: Towards a Model-Driven SDN Controller Architecture," in *Proc. IEEE WTS*, Washington, DC, USA, Apr. 2014, pp. 1–6.