IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

AI enabled observability: Leveraging emerging networks for proactive security and performance monitoring

Omoniyi David Olufemi[1*], Adedeji Ojo Oladejo[2], Vincent Anyah[3], Kamaldeen Oladipo[4], Friday Ogochukwu Ikwuogu[5]

[1]*Computer Science & Engineering University of Fairfax, Virginia, USA.*
[2]*J. Warren McClure School of Emerging Communication Technologies, Ohio University, USA.*
[3]*Computer Science, New Mexico highlands University, USA.*
[4]*Nokia Technologies, Mexico.*
[5]*Dept of Computer Science, University of Texas, Permian Basin, USA.*

Corresponding author: Omoniyi David Olufemi (*Email: do585819@ohio.edu*)

Abstract

The emergence of advanced networks is transforming the digital landscape, driving unprecedented complexity, decentralization, and service requirements across industries. As networks evolve towards increasingly dynamic, software-defined, and virtualized architectures, traditional monitoring techniques prove insufficient in managing the scale and complexity of next-generation infrastructures. This paper introduces observability as a proactive, intelligent, and security-aware framework for gaining real-time insights into the internal states of future networks. By integrating AI-driven analytics and leveraging open-source technologies alongside standards from globally recognized institutions such as 3GPP, ETSI, 5GPPP, Linux Foundation, ISACA, and ISC2, we propose a robust approach to managing the complexities of network slicing, smart cities, edge computing, and beyond. The framework emphasizes intelligent decision-making, autonomous network management, and predictive analytics to enhance performance monitoring, incident detection, and regulatory compliance in increasingly autonomous, interconnected environments. Detailed architectures, code examples, and tooling references are provided to support implementation in diverse real-world use cases. This paper envisions a future of secure, resilient, and adaptive networks, driven by AI and observability, capable of meeting the demands of digital transformation and evolving cybersecurity challenges.

Keywords: 3GPP, 5G, 5GPPP, AI for Networks, AI, Compliance, Deep Learning, eBPF, Edge Computing, ETSI, In-Band Telemetry, ML, Network Automation, Network Slicing, Network Telemetry, NFV, Observability, ONAP, OpenTelemetry, Proactive Monitoring, Prometheus, SDN, Security Monitoring, Smart Cities.

DOI: 10.53894/ijirss.v8i3.7054
Funding: This study received no specific financial support.
History: Received: 18 March 2025 / **Revised:** 22 April 2025 / **Accepted:** 24 April 2025 / **Published:** 15 May 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.

Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction to Observability in Modern Networks

1.1. The Evolution of Network Complexity

The architecture of telecommunication networks has undergone a transformative evolution over the past decade, driven by the adoption of cloud-native principles, network virtualization, and the proliferation of smart devices. With the advent of 5G, the network landscape has become increasingly complex, comprising thousands of virtualized functions, decentralized edge deployments, and real-time service orchestration [1]. Unlike traditional static and centralized networks, modern infrastructures are dynamic and distributed, which introduces new challenges in maintaining performance, reliability, and security.

As network complexity scales, so too does the need for intelligent, contextual visibility across every layer. Traditional monitoring tools, which primarily focus on binary metrics such as uptime and CPU utilization, fall short in revealing how and why system behaviors change under varying conditions [2]. This growing demand has led to the emergence of observability as a core architectural principle for future networks.

1.2. From Monitoring to Observability

Monitoring has historically been essential for IT and network operations, providing basic indicators such as latency, availability, and throughput. However, in software-defined and cloud-native environments, it becomes insufficient to simply track whether a service is “up” or “down.” Observability, by contrast, refers to the ability to infer the internal state of a system from its external outputs—such as logs, metrics, traces, and events [3]. It offers deeper insights, helping engineers understand why the system is behaving a certain way, not just what is happening.

This paradigm shift is especially critical in 5G networks, where service chains are composed of loosely coupled microservices and virtual functions distributed across edge and core locations [4]. Observability empowers operators to trace packet flows across slices, correlate telemetry from disaggregated nodes, and proactively detect issues before they impact users.

1.3. Drivers Behind Observability in 5G

One of the key enablers of observability is Multi-access Edge Computing (MEC), which relocates computing and storage closer to the user to meet low latency demands [4]. While MEC offers performance benefits, it also decentralizes infrastructure, making centralized monitoring ineffective. Observability provides a distributed telemetry framework that adapts to dynamic workloads and environments.

The rise of massive IoT deployments further compounds the problem. With billions of devices transmitting telemetry across constrained and unstable links, traditional polling-based monitoring becomes impractical. Observability enables the real-time ingestion and analysis of device-level signals to detect failures, optimize connectivity, and maintain SLA compliance [2].

Additionally, Ultra-Reliable Low-Latency Communication (URLLC) applications, such as remote surgery and autonomous vehicles, demand stringent latency guarantees. Any delay, jitter, or packet loss could have critical consequences. Observability provides operators with predictive insights into latency hotspots and failure conditions, enabling timely remediation and fault tolerance [2].

Another powerful feature introduced by 5G is network slicing, which allows operators to provision isolated virtual networks over shared infrastructure. Each slice is configured with its own QoS, latency, and bandwidth parameters. Without observability, it is nearly impossible to maintain slice isolation, detect cross-slice interference, or ensure SLA guarantees in multi-tenant environments [1].

1.4. Observability and Proactive Security

The dynamic and programmable nature of 5G networks creates a larger attack surface and increases the complexity of threat detection. Traditional perimeter-based security models are inadequate in this new environment. Observability enhances security posture by embedding telemetry and deep visibility throughout the stack—from infrastructure to workloads and services.

By integrating logs, flow records, and contextual metadata into centralized analytics engines, observability enables anomaly detection, behavioral analytics, and root cause correlation [5]. Techniques such as eBPF, XDP, and in-band telemetry (INT) are now leveraged to capture granular traffic patterns and enforce Zero Trust architectures [6].

Security compliance standards such as ISACA's COBIT and ISC²'s CISSP Common Body of Knowledge (CBK) emphasize the need for real-time detection, continuous monitoring, and auditability—principles that align directly with observability [7, 8]. In essence, observability serves as a proactive security layer that enhances detection capabilities while supporting regulatory compliance.

1.5. Standards Bodies and Open-Source Ecosystems

The push toward full-spectrum observability is being actively shaped by leading standards organizations and open-source communities. 3GPP, the main standardization body for mobile communication systems, has introduced the Network Data Analytics Function (NWDAF) to provide native support for real-time data collection, aggregation, and analytics within the 5G core [1]. NWDAF enables operators to make intelligent decisions based on contextual and predictive analyses of network events.

In parallel, ETSI plays a critical role in defining the observability aspects of NFV (Network Function Virtualization) and MEC frameworks. Their work ensures that virtualized network functions expose telemetry through standardized APIs, which can be consumed by analytics platforms for real-time insights [4].

The 5G Infrastructure Public-Private Partnership (5GPPP), funded by the European Commission, sponsors a range of research projects focused on enabling intelligent orchestration, intent-based networking, and self-healing architectures. These efforts prioritize observability as a central enabler for closed-loop automation and SLA assurance [1].

From the open-source side, the Linux Foundation serves as a hub for observability innovation through initiatives like LF Networking, ONAP, and OpenTelemetry. These projects provide vendor-neutral frameworks, telemetry collectors, and orchestration engines that support observability across SDN, NFV, and 5G-native infrastructures [6].

Cybersecurity organizations like ISACA and (ISC)² contribute to the ecosystem by offering frameworks, guidelines, and certifications that emphasize continuous visibility and risk mitigation. Their principles reinforce the need for observability not just as a tool for reliability, but also as a cornerstone of modern cyber resilience strategies.

1.6. Laying the Groundwork for Resilient 5G

As networks become more agile, programmable, and service-oriented, observability has emerged as a foundational requirement. It is no longer sufficient to rely on traditional monitoring to guarantee performance, ensure SLA compliance, or detect security anomalies in time. Observability—when integrated across the entire 5G lifecycle—empowers operators with contextual intelligence, enabling self-optimization, anomaly prediction, and closed-loop automation.

The following chapters in this paper will examine in greater detail how observability is implemented across the layers of the 5G stack. We will explore the tools, open-source frameworks, standards, and real-world use cases that demonstrate the value of observability in enhancing both performance and security in future networks.

2. 5G Architecture and the Need for Observability

2.1. Core Components of the 5G Architecture

2.1.1. Radio Access Network (RAN)

The 5G RAN, composed primarily of the gNB (Next-Generation Node B), provides wireless connectivity between the user equipment (UE) and the 5G Core. The RAN is responsible for radio resource management, beamforming, and cell handovers. Unlike its 4G predecessor, the 5G RAN supports multiple deployment modes, including Non-Standalone (NSA) and Standalone (SA), and operates across diverse spectrum bands—from sub-6 GHz to mmWave (above 24 GHz).

The challenge with observability at the RAN layer lies in the volatility of radio frequency environments and the mobility of users. Rapid fluctuations in RSRP (Reference Signal Received Power) and RSRQ (Reference Signal Received Quality) impact user experience in real time. Additionally, handovers between gNBs can fail due to interference, resource exhaustion, or backhaul issues.

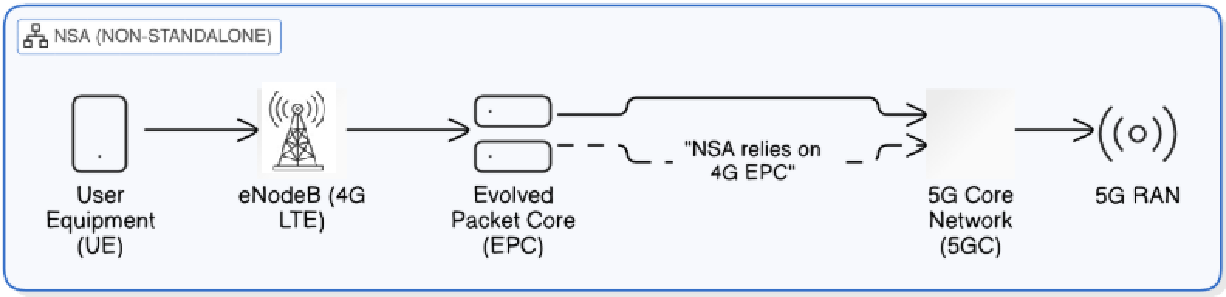


Figure 1.
5G End-to-End NSA.

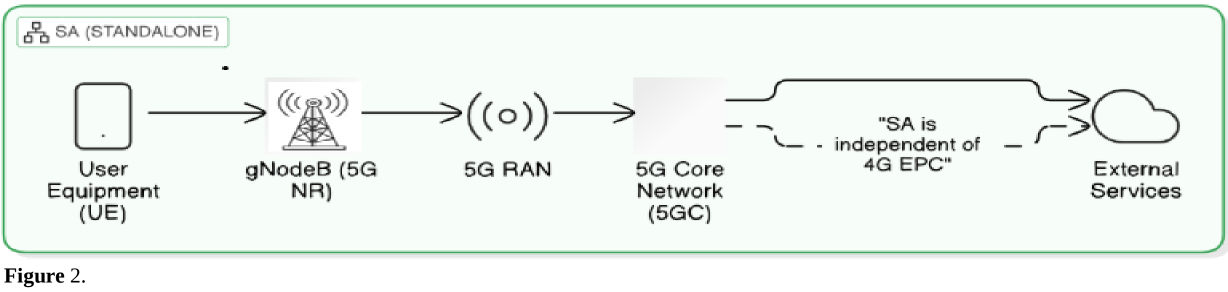


Figure 2.
5G End-to-End SA.

RAN Observability KPIs:

- Handover Success Rate (HSR)
- Radio Link Failure (RLF) events per user
- Spectral Efficiency (bps/Hz/cell)
- Uplink/Downlink Throughput
- Signal-to-Interference-plus-Noise Ratio (SINR)

Handover Success Rate (HSR):

$$HSR = \left(\frac{\text{Number of Successful Handovers}}{\text{Total Number of Handovers}}\right) \times 100$$

Measures the percentage of successful handovers out of all attempted handovers.

Radio Link Failure (RLF) Events per User:

$$RLFperUser = \frac{\text{Number of RLF Events}}{\text{Total Number of Active Users}}$$

Measures the average number of radio link failures per user.

Spectral Efficiency (bps/Hz/cell):

$$Spectral\ Efficiency = \frac{\text{Total Throughput (bps)}}{\text{Bandwidth (Hz)}}$$

Measures how efficiently the available bandwidth is utilized in the network.

Uplink/Downlink Throughput:

- Uplink Throughput:

$$Uplink\ Throughput = \frac{\text{Total Data Transferred from User to Network}}{\text{Measurement Time}}$$

- Downlink Throughput:

$$Downlink\ Throughput = \frac{\text{Total Data Transferred from Network to User}}{\text{Measurement Time}}$$

Measures the data rate of the uplink (from user to network) and downlink (from network to user) respectively.

Signal-to-Interference-plus-Noise Ratio (SINR):

$$SINR = \frac{\text{Signal Power}}{\text{Interference Power} + \text{Noise Power}}$$

Modern RAN observability leverages O-RAN Alliance standards, where telemetry from distributed units (DUs) and centralized units (CUs) is collected and analyzed in near-real time. The RAN Intelligent Controller (RIC) is often used to apply closed-loop automation based on this telemetry [9].

2.1.2. 5G Core Network (5GC)

The 5G Core (5GC) represents a shift from traditional monolithic cores to a service-based architecture (SBA), where each network function (NF) is a microservice accessible via standard APIs.

Table 1.
Key 5G Core Network Functions and Their Descriptions.

Network Function	Description
AMF	Handles registration, connection, and mobility management
SMF	Session management and dynamic IP address assignment
UPF	User plane packet processing and forwarding
PCF	Policy decision function
UDM/AUSF	Authentication and subscriber profile management

These functions communicate using HTTP/2-based APIs defined in 3GPP TS 29.500. Observability challenges in the core include inter-service API latency, context loss across microservices, and failure propagation across control and user planes.

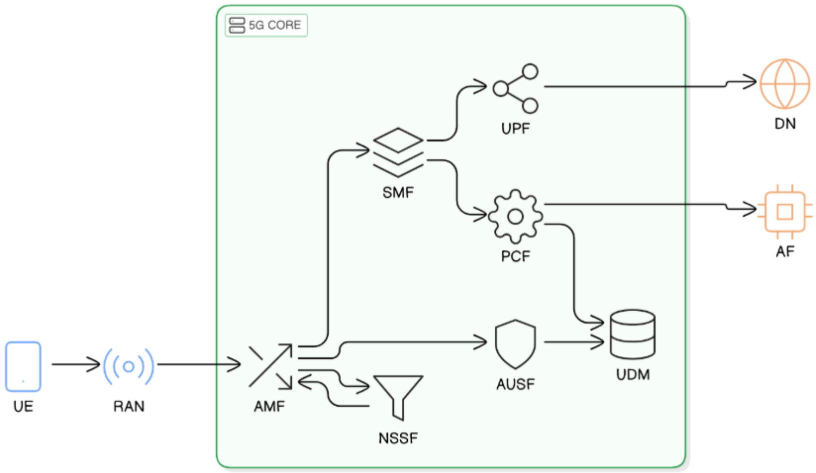


Figure 3.
Basic SA 5G Core Architecture Overview.

5GC Observability KPIs:

- AMF Registration Delay (ms)
- UPF Round-Trip Latency (ms)
- Service Instance CPU and Memory Usage
- Inter-NF Call Failure Rate
- Packet Loss in User Plane Forwarding

Modern observability in 5GC includes distributed tracing (e.g., using OpenTelemetry or Jaeger) and streaming analytics through NWDAF (Network Data Analytics Function). NWDAF, standardized by 3GPP TR 23.288, enables real-time analytics consumption by NFs to trigger QoS adaptations or scaling actions [1].

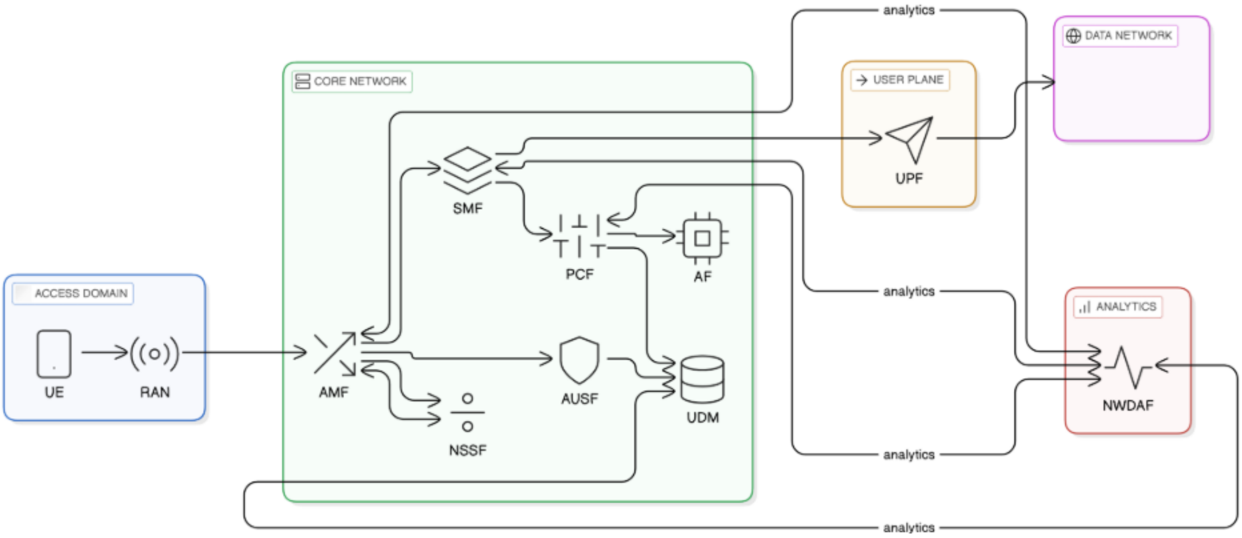


Figure 4.
SA 5G Core Architecture with NWDAF.

2.1.3. Network Slicing

Network slicing allows the same physical network infrastructure to be logically partitioned into multiple independent virtual networks. Each slice is tailored for different requirements:

- eMBB (Enhanced Mobile Broadband): High bandwidth for video streaming and VR/AR.
- URLLC (Ultra-Reliable Low-Latency Communication): Use cases like remote surgery, smart grid control.
- mMTC (Massive Machine-Type Communication): For IoT devices and smart cities.

The complexity of observability in network slicing lies in ensuring strict isolation, monitoring slice-specific KPIs, and maintaining dynamic resource allocation without breaching SLAs.

Slice-Level KPIs:

- End-to-End Slice Latency (per QoS class)
- Slice Availability (%)
- Slice Resource Utilization (vCPU, vRAM, bandwidth)
- SLA Violation Rate
- Interference Leakage Across Slices

Operators must have multi-tenant observability and policy-aware metrics pipelines to ensure that tenant A's failure or overload does not impact tenant B. Observability tools must also allow operators to trace issues within a slice—from RAN to core to MEC—and enforce governance rules automatically.

2.1.4. Multi-access Edge Computing (MEC)

MEC decentralizes computing and storage by moving workloads closer to the user. The purpose is to support latency-sensitive applications and offload traffic from the central data plane.

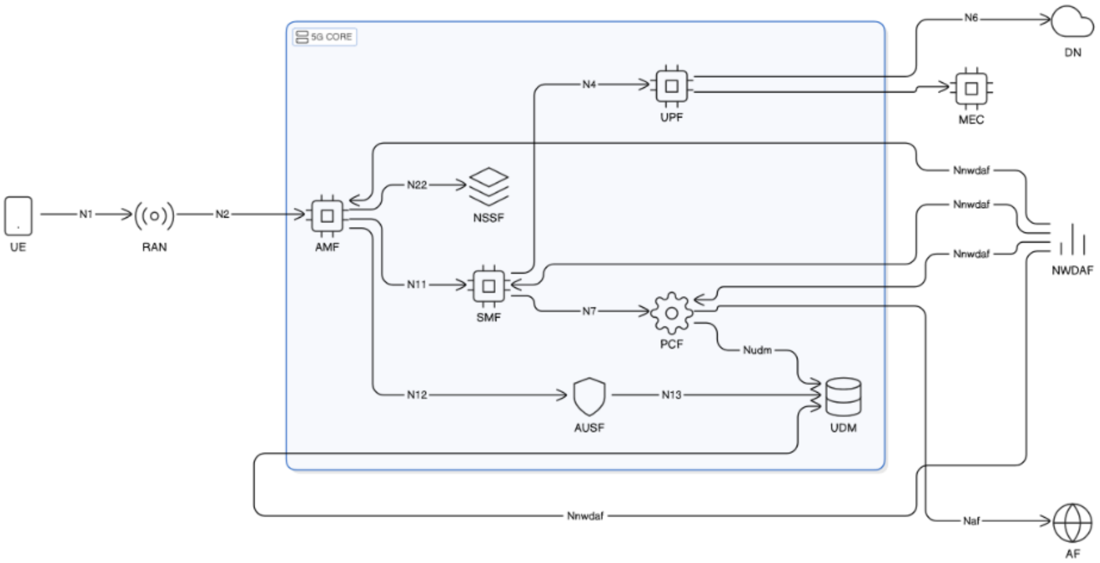
Edge observability is essential because:

- Faults at the edge are harder to detect centrally.
- Workload migration across edge nodes is dynamic.
- Resource constraints are more severe than in centralized clouds.

MEC Observability KPIs:

- Edge Node CPU/GPU Utilization
- Container Startup Time (for microservices)
- Average Service Response Time (per application)
- Local Traffic Offload Ratio
- Latency to UE (RTT in ms)

MEC observability is often achieved through lightweight collectors such as Prometheus node exporters, eBPF tracing, and Kubernetes-native tools (e.g., Kube-state-metrics, Kiali for service mesh visibility).



Figure

2.2. Observability Gaps in 5G Networks

Despite being designed for flexibility and agility, 5G networks introduce observability gaps due to the **virtualized,** disaggregated, and multi-vendor nature of deployments. The major gaps can be categorized as follows:

Table 2.
Observability Gaps in 5G Network Layers.

Layer	Observability Gap
RAN	Lack of real-time, fine-grained radio metrics; limited correlation between cell handovers and UE QoS degradation
5GC	Siloed logs; no unified tracing across control plane and user plane; difficulty diagnosing API-level failures
MEC	Inadequate container-level observability at scale; poor visibility into service-to-service communication
Network Slices	Absence of per-slice SLA dashboards; difficulty ensuring tenant isolation and policy enforcement

Moreover, telemetry data silos make root cause analysis time-consuming. For example, a degraded video stream may appear as a content delivery issue when, in fact, it is rooted in a failed RAN handover, a congested UPF instance, or resource starvation at a MEC node. Without cross-layer correlation, proactive resolution becomes nearly impossible.

2.3. Observability Points in 5G: Architectural View

The following diagram illustrates major observability injection points within a simplified 5G deployment:

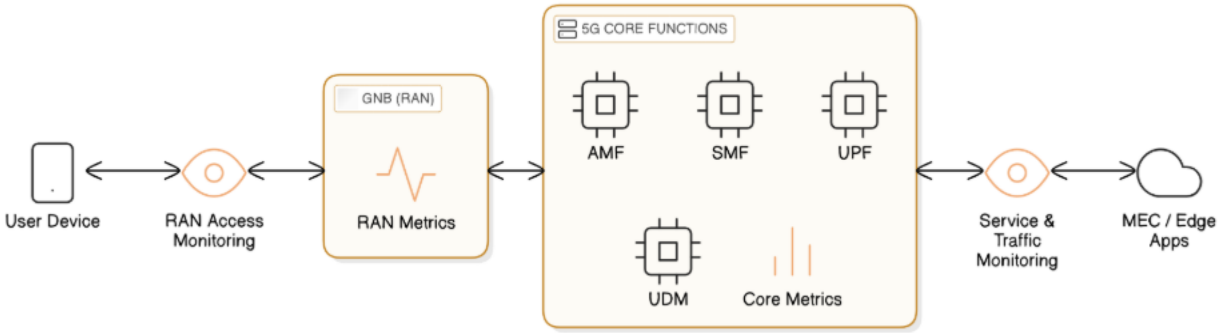


Figure 5.
Observability injection points in simplified Deployments.

Each layer (RAN, 5GC, MEC) must be instrumented with telemetry collectors and trace injectors. For example:

- RAN: Use O-RAN E2 interface telemetry
- 5GC: Enable HTTP/2 API tracing and NWDAF
- MEC: Deploy OpenTelemetry SDKs in edge applications

These observability signals must be exported to a central observability control plane that provides real-time analytics and alerts.

2.4. Code: Exporting UPF Metrics with Prometheus

A simple telemetry exporter can be written for the User Plane Function (UPF) in Python, showing how to collect latency metrics:

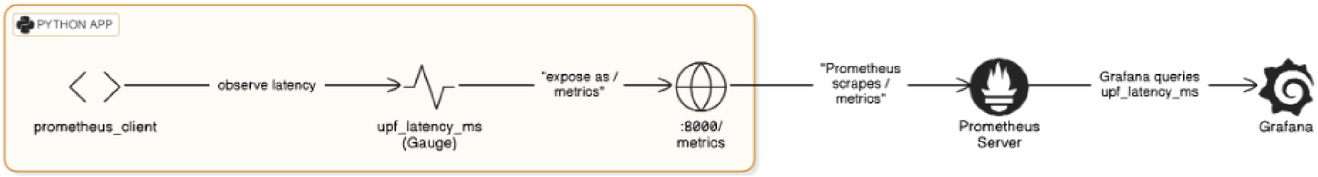


Figure 6:
Prometheus Metrics Export for UPF latency.

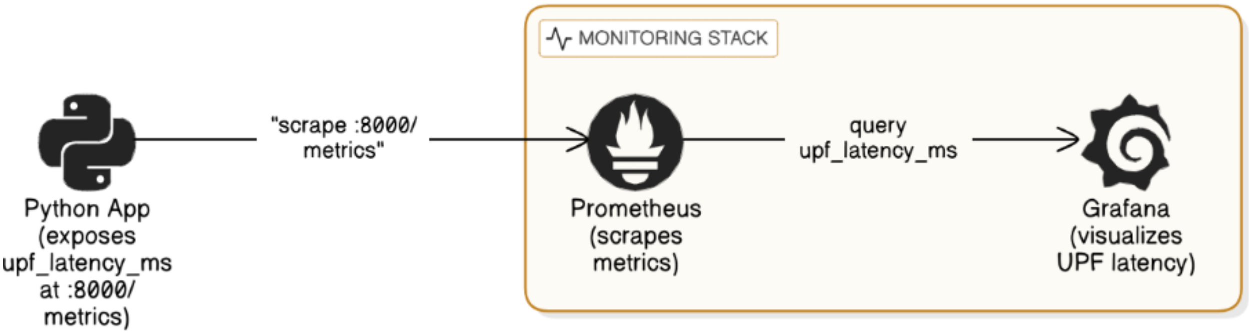

MONITORING STACK
Python App (exposes upf_latency_ms at :8000/ metrics)
"scrape :8000/ metrics"
Prometheus (scrapes metrics)
query upf_latency_ms
Grafana (visualizes UPF latency)

Figure 7.
UPF Latency Metrics Flow.

This exporter can be scraped every 5 seconds by Prometheus, and metrics visualized via Grafana dashboards to monitor real-time performance of the UPF.

2.5. Integrating NWDAF and AI for Observability

The Network Data Analytics Function (NWDAF) defined by 3GPP is a central component for observability in the 5G core. NWDAF gathers data from network functions and provides insights to optimize operations (e.g., scaling up SMF instances during congestion). It supports AI/ML plugins to predict:

- Load forecasts
- UE mobility patterns
- QoS degradation risks

The NWDAF APIs (3GPP TS 29.520) allow integration with external analytics engines such as Grafana Mimir, Apache Kafka, or TensorFlow Serving for model inference.

Example NWDAF Use Case:

- Predict latency spikes in UPF based on input throughput trends and trigger dynamic scale-out before SLA violation.

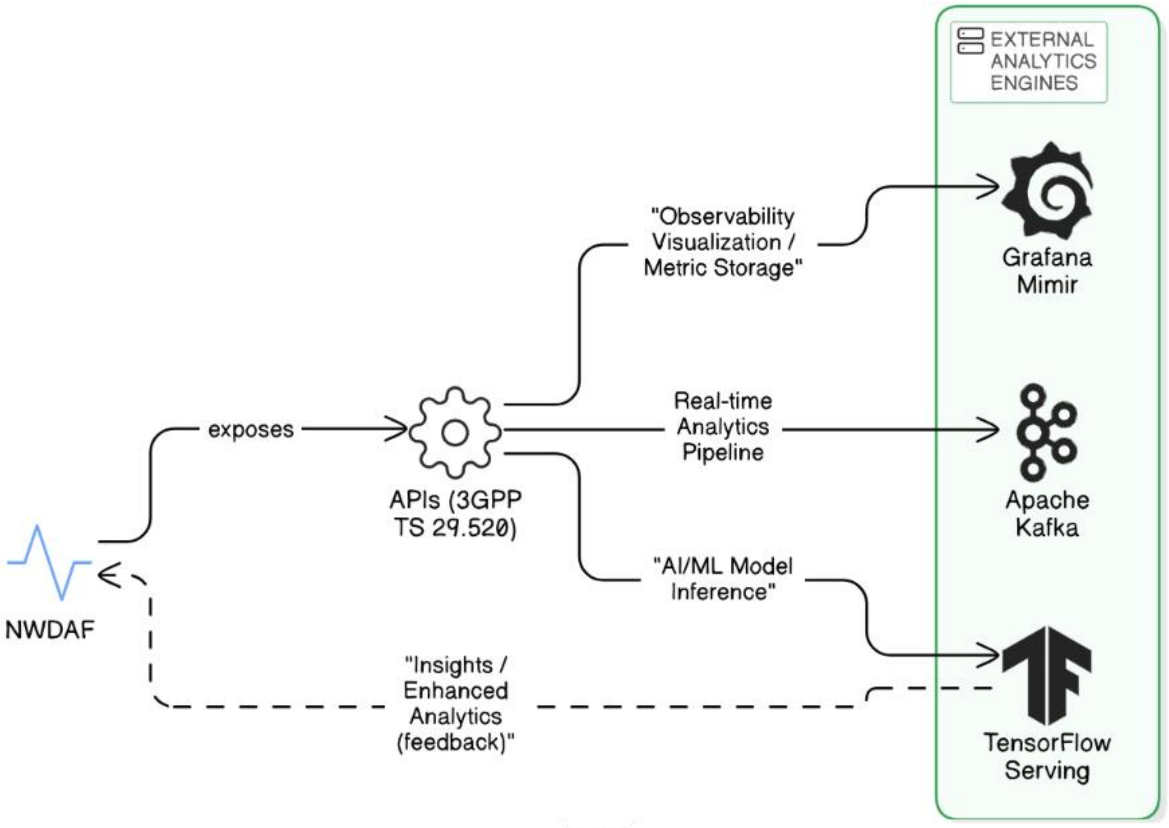

EXTERNAL ANALYTICS ENGINES
"Observability Visualization / Metric Storage"
Grafana Mimir
exposes
APIs (3GPP TS 29.520)
Real-time Analytics Pipeline
Apache Kafka
"AI/ML Model Inference"
NWDAF
"Insights / Enhanced Analytics (feedback)"
TensorFlow Serving

Figure 8.
NWDAF and AI for Observability – Component Diagram.

3. Open-Source Observability Tools for 5G Networks

The observability requirements of 5G networks demand a multi-layered, interoperable approach that cannot be met by monolithic or proprietary monitoring systems alone. Open-source tools have emerged as vital components of the observability fabric in 5G, allowing for seamless integration, standardized telemetry collection, and vendor-neutral automation. This chapter explores the most prominent open-source solutions, their architectural roles, deployment strategies, and performance indicators in the context of 5G networks.

3.1. The Case for Open-Source Observability in 5G

3.1.1. Open Standards for a Disaggregated Ecosystem

5G architectures are fundamentally disaggregated, consisting of virtualized network functions (VNFs), containerized workloads, edge components, and cloud-native cores [1]. This complexity makes vendor lock-in impractical. Open-source observability solutions ensure transparency, extensibility, and alignment with frameworks such as the 3GPP's Network Data Analytics Function (NWDAF) and ETSI’s NFV and MEC standards.

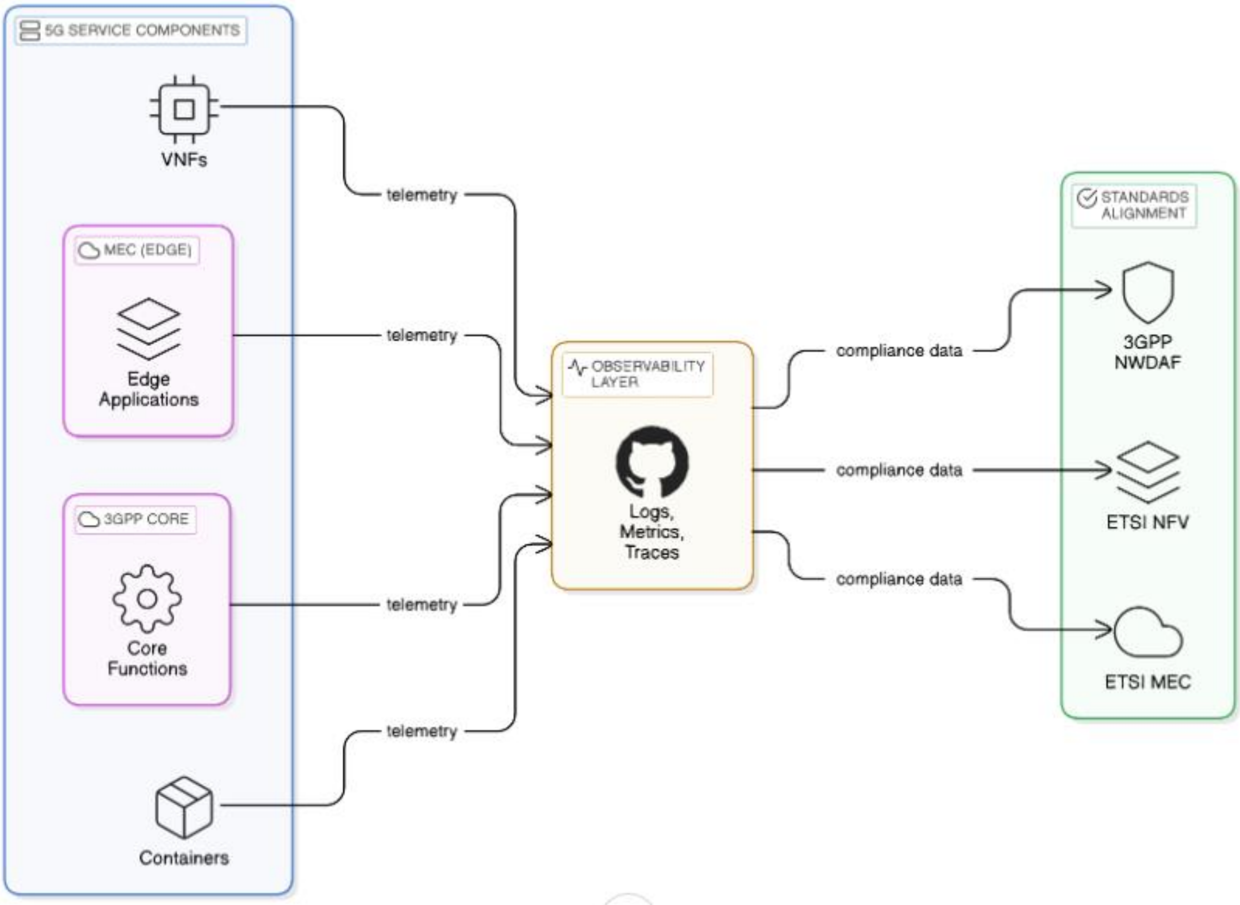


Figure 9.
Disaggregated 5G Architecture with Observability and Standard Alignment.

3.1.2. Community-Driven Innovation and Modularity

Open-source projects governed by the Cloud Native Computing Foundation (CNCF) and the Linux Foundation Networking (LFN) evolve rapidly to meet new demands. Projects like OpenTelemetry, Prometheus, and ONAP offer modularity, allowing operators to select components tailored to specific layers [6].

3.2. OpenTelemetry: Unified Telemetry Collection Framework

3.2.1. Architecture and Scope

OpenTelemetry (OTel) is a CNCF project that provides an SDK and APIs for capturing logs, metrics, and traces from distributed systems. It supports multi-language instrumentation, including Go, Python, Java, C++, and offers exporters for Prometheus, Jaeger, Zipkin, and OTLP (OpenTelemetry Protocol) [10].

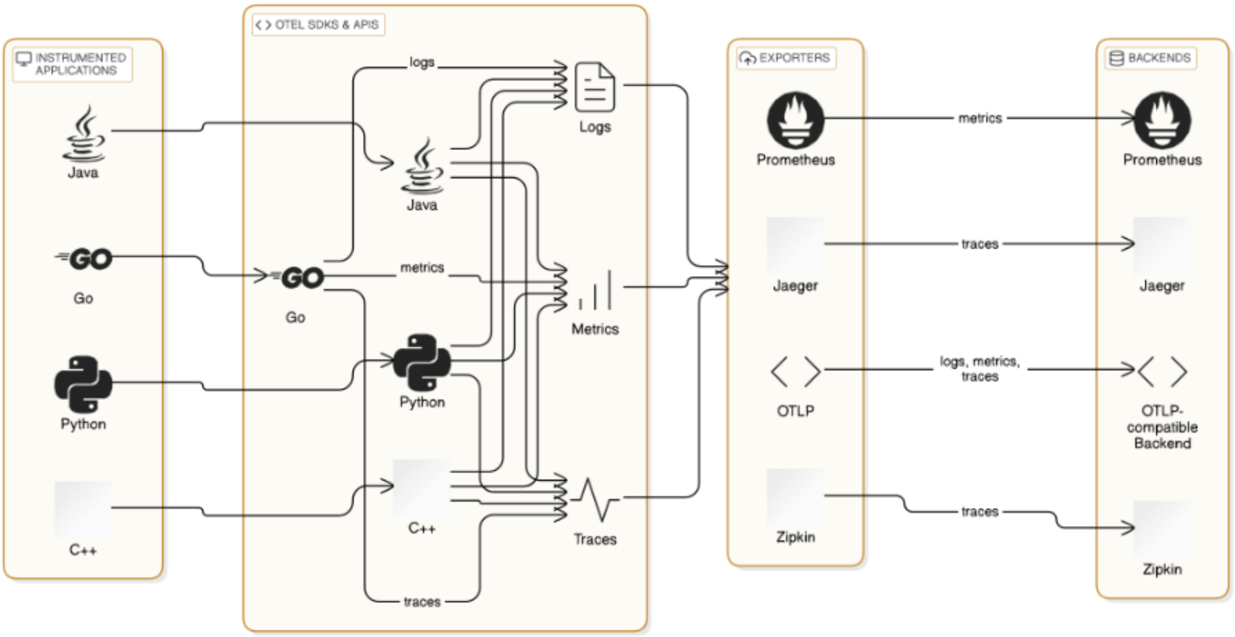


Figure 10.
OpenTelemetry (OTel) Observability Architecture.

3.2.2. Implementation in 5G Core

In 5G, OpenTelemetry can be integrated directly into the microservices making up the Service-Based Architecture (SBA) of the 5G core. For example, Access and Mobility Management Function (AMF) and Session Management Function (SMF) can be instrumented to emit spans for user registration and session setup, respectively.

3.2.3. Key Benefits

- Enables end-to-end traceability of user sessions
- Supports auto-instrumentation for Kubernetes workloads
- Allows custom attributes such as slice_id, qos_profile, or ue_ip for richer telemetry

3.2.4. SMF Tracing with OpenTelemetry

A Python script can be set up to achieve distributed tracing using OpenTelemetry by initializing a tracer provider, configuring an OTLP (OpenTelemetry Protocol) HTTP exporter to send trace data to a collector (such as Jaeger), and registering a batch span processor to handle the export of spans. It then starts a span named "smf_session_allocation" to represent a specific operation—here, the allocation of session resources—and prints a log message during that span. The trace data generated would be visualized as part of a broader trace in tools like Jaeger or any backend that supports the OpenTelemetry protocol.

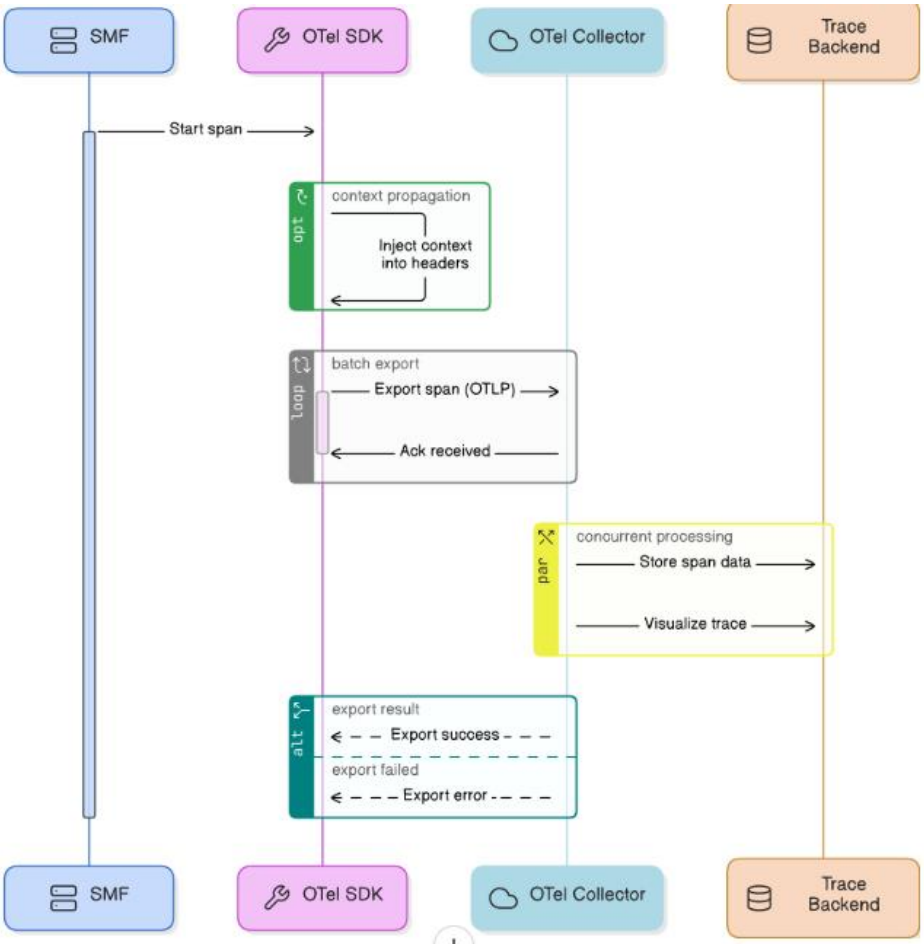


Figure 11.
SMF Tracing with OpenTelemetry.

3.3. Prometheus and Grafana: Metrics Collection and Visualization

3.3.1. Overview of Prometheus

Prometheus is a pull-based time-series database and monitoring system that collects metrics via HTTP endpoints. It is ideal for cloud-native infrastructures, including Kubernetes-hosted 5G components [10].

3.3.2. Integration in 5G Deployments

Prometheus can scrape metrics from exporters attached to:

- 5GC NFs like UPF, AMF, SMF
- Edge containers running MEC apps
- Slice management entities

A Prometheus Operator can be deployed to automate scraping, alerting, and metric storage within Kubernetes-based 5G stacks [11].

3.3.3. Grafana for SLA Dashboards

Grafana complements Prometheus by providing powerful visualization capabilities for the metrics collected during network operations. It allows operators to build real-time dashboards that monitor key performance indicators such as RAN signal quality trends, UPF throughput and latency, and adherence to service level agreements (SLAs) at the network slice level. By integrating Grafana with Prometheus, network teams can track metrics like upf_latency_seconds to measure User Plane Function latency, smf_cpu_usage_percent to monitor the CPU usage of the Session Management Function, and slice_packet_drop_ratio (slice_id="eMBB") to observe packet drop ratios specifically within the eMBB (enhanced Mobile Broadband) slice. This integration enhances observability and supports proactive network management.

Example Metrics:

- upf_latency_seconds
- smf_cpu_usage_percent
- slice_packet_drop_ratio (slice_id="eMBB")

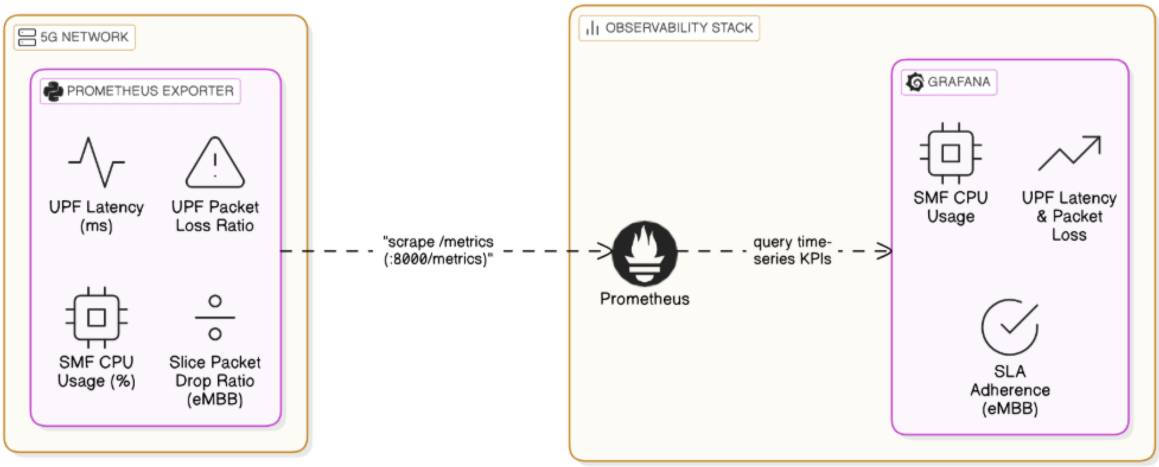


Figure 12.
Grafana and Prometheus Observability in 5G Network.

3.4. Jaeger: Distributed Tracing in 5G Microservices

3.4.1. Tracing for Root Cause Analysis

Jaeger allows tracing of transactions across services, which is critical for identifying bottlenecks in session setup, policy enforcement, and user authentication. When integrated with OpenTelemetry, Jaeger can display trace trees of 5G user flows [12].

3.4.2. Real-World Use Case in 5G

In a scenario where UE registration fails, Jaeger traces help determine whether the issue lies in:

- gNB to AMF signaling
- AMF to UDM query
- SMF allocation timeout

Such root cause analysis drastically reduces the Mean Time To Resolution (MTTR) and supports automated incident classification.

3.5. ONAP: Closed-Loop Telemetry and Automation

3.5.1. Architecture and Modules

ONAP (Open Network Automation Platform) is an open-source project under the Linux Foundation Networking (LFN) initiative, created to provide a comprehensive platform for orchestrating and automating the entire lifecycle of both Virtual Network Functions (VNFs) and Cloud-native Network Functions (CNFs). It enables service providers to design, deploy, monitor, and manage network services more efficiently and at scale. Key components of ONAP include DCAE (Data Collection, Analytics, and Events), which is responsible for gathering telemetry data, performing real-time analytics, and triggering events; the Policy Engine, which allows for the dynamic creation and enforcement of rules and policies across the network; and CLAMP (Closed Loop Automation Management Platform), which facilitates closed-loop automation by enabling feedback-driven control loops for self-healing and optimization of network services. Together, these components support agile, automated, and intelligent network management in modern, software-defined environments.

3.5.2. Observability-Oriented Features

- DCAE can ingest metrics/logs from Prometheus and Fluentd
- Policy Engine triggers alerts or reconfigurations
- AI/ML modules can train on historical observability data

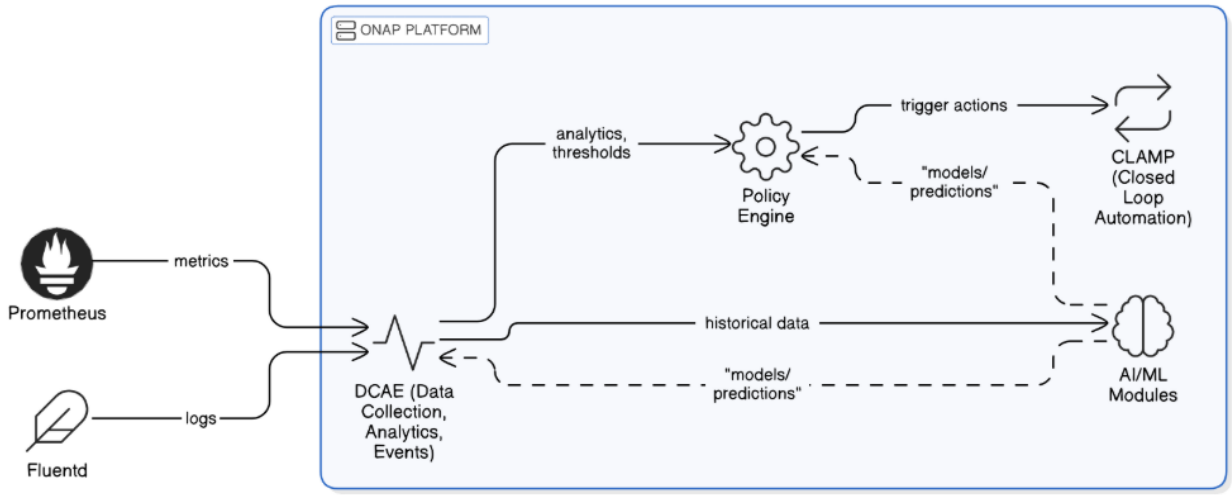


Figure 13.
ONAP Observability-Oriented Architecture.

3.5.3. Closed-Loop Example: UPF Auto-Scaling

1. DCAE detects rising packet loss via Prometheus.
2. Policy engine decides on scale-out.
3. SDN-C configures routing to a new UPF instance.
4. Logs and metrics confirm mitigation.

This pipeline enables self-healing, a core principle in intent-based and autonomous networks [1].

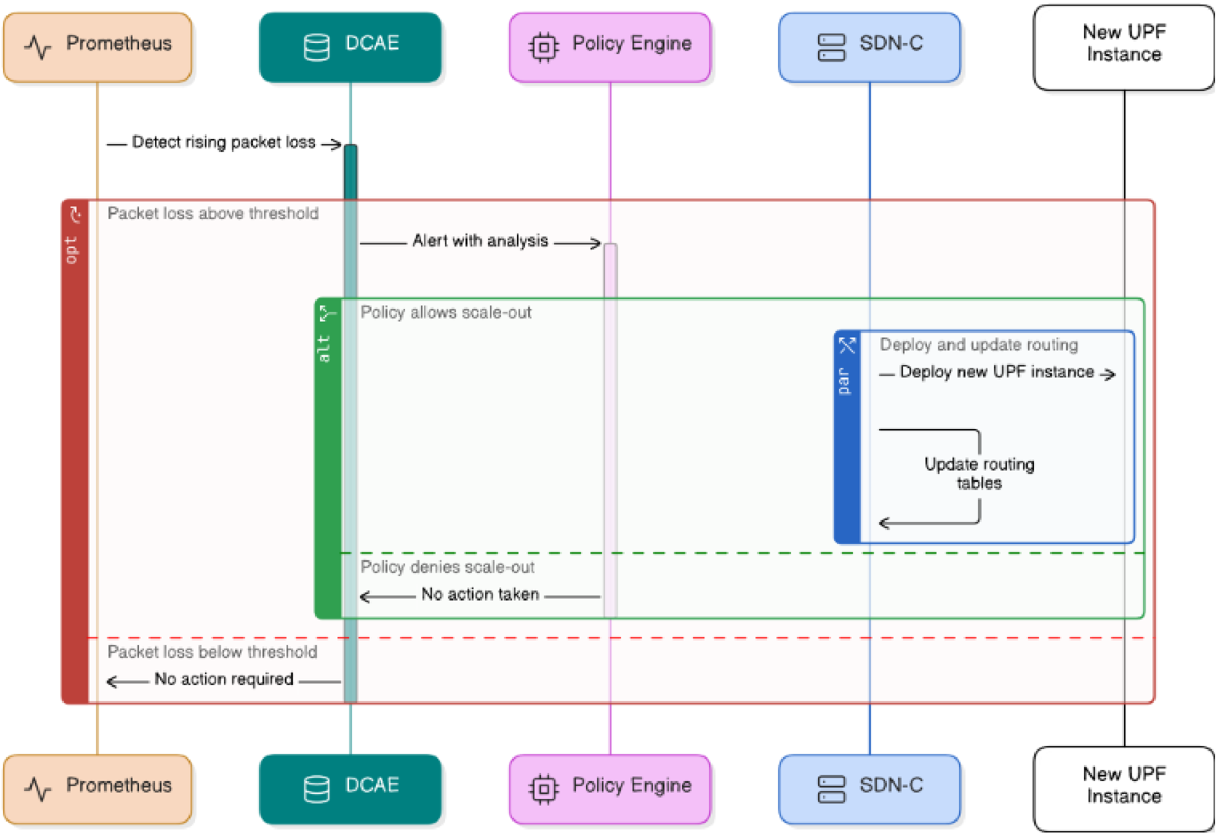


Figure 14.
Closed-Loop Example – UPF Auto-Scaling.

3.6. Telemetry Pipelines: Combining Open Tools

3.6.1. Full Stack Architecture

This full-stack architecture illustrates the end-to-end flow of data and control across a 5G core network integrated with observability and automation tools. The diagram begins with the gNB (Next Generation Node B), which connects to the AMF (Access and Mobility Management Function)—responsible for handling registration, mobility, and connection management. The AMF forwards control signaling to the SMF (Session Management Function), which manages session establishment and interacts with the UPF (User Plane Function) for data routing and forwarding. From the UPF, data reaches the EdgeApp (Edge Application), enabling ultra-low-latency services at the network edge.

Observability is embedded throughout the stack. The AMF emits real-time metrics that are collected by Prometheus for monitoring. SMF and EdgeApp generate distributed traces via OpenTelemetry, which are visualized in Jaeger to track request flows and detect bottlenecks. The UPF outputs logs that are gathered by Fluentd, then indexed and stored in Elasticsearch for powerful search and log analytics capabilities.

In the analytics and automation plane, the NWDAF (Network Data Analytics Function) streams events and insights through Kafka, a distributed message broker. These messages are consumed by ONAP (Open Network Automation Platform), which interprets the data and applies policies via its Policy Engine, enabling intelligent, closed-loop automation and real-time decision-making based on network conditions. This architecture brings together 5G functions, observability tools, and AI-driven automation into a cohesive, scalable, and self-optimizing system.

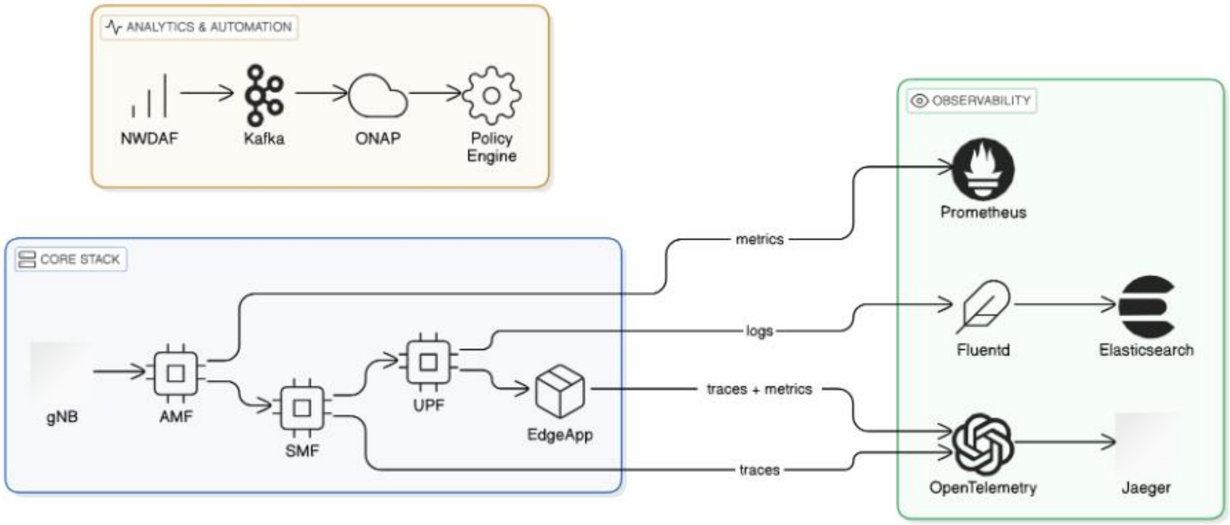


Figure 15:
Full Stack 5G Observability Architecture.

3.6.2. Benefits of Modular Observability Stack

- Vendor Interoperability: Works across heterogeneous infrastructure
- Horizontal Scalability: Components can be scaled independently
- Analytics-Driven Actions: Data from observability stack feeds automation logic

3.7. Observability KPIs Across the Stack

Table 3.
Critical 5G Metrics for RAN, Core, Slicing & Edge.

Component	Metric	Description
UPF	upf_latency_ms	End-to-end user traffic delay
SMF	smf_session_failures_total	Failed session initiations
RAN	handover_failure_rate	Handover errors due to poor signal
Slice Manager	slice_sla_violations_total	QoS or latency violations per slice
Edge App	service_response_latency_ms	User-facing latency from edge workloads

These KPIs are essential for real-time visibility and SLA enforcement.

3.8. Summary

This chapter examines how open-source observability tools form the backbone of modern 5G operations. Projects like OpenTelemetry, Prometheus, Grafana, Jaeger, and ONAP provide an integrated observability fabric that spans metrics, logs, traces, and automation. By combining these tools, operators can build real-time, intelligent, and self-healing 5G infrastructures that align with ETSI, 3GPP, and Linux Foundation standards.

4. SDN, Telemetry, and AI for Proactive Security in 5G Networks

The advent of 5G networks has introduced unprecedented capabilities, including enhanced bandwidth, ultra-low latency, and massive device connectivity. However, these advancements also bring forth complex security challenges. To address these, integrating Software-Defined Networking (SDN), advanced telemetry, and Artificial Intelligence (AI) has emerged as a strategic approach to bolster proactive security measures in 5G networks. This chapter explores the synergy among these technologies and their collective role in fortifying 5G network security.

4.1. The Role of Software-Defined Networking (SDN) in 5G Security

4.1.1. Decoupling Control and Data Planes

Software-Defined Networking (SDN) is a paradigm that separates the network's control plane from the data plane, enabling centralized control and programmability of network behavior. This separation allows for dynamic management of network resources, facilitating rapid responses to security threats and efficient traffic engineering [9].

4.1.2. Centralized Network Control for Enhanced Security

The centralized nature of SDN provides a holistic view of the network, which is instrumental in detecting and mitigating security threats. By leveraging global network visibility, SDN controllers can implement consistent security policies across the network, identify anomalous traffic patterns, and respond to incidents in real time [13].

4.1.3. Dynamic Policy Enforcement

SDN enables dynamic policy enforcement by allowing the network to adapt its behavior based on real-time conditions. For instance, if a potential Distributed Denial of Service (DDoS) attack is detected, the SDN controller can reroute or block malicious traffic flows, thereby mitigating the attack's impact [5].

4.2. Advanced Telemetry for Real-Time Network Monitoring

4.2.1. In-Band Network Telemetry (INT)

In-Band Network Telemetry (INT) embeds telemetry data within the actual data packets, allowing for real-time monitoring of network conditions such as latency, jitter, and packet loss. This approach provides granular visibility into the network's performance and health, facilitating prompt detection of anomalies [14].

4.2.2. eBPF and XDP for Kernel-Level Observability

Extended Berkeley Packet Filter (eBPF) and Express Data Path (XDP) are technologies that enable the execution of sandboxed programs within the Linux kernel. They allow for high-performance packet filtering and monitoring, which is crucial for detecting and mitigating security threats at the kernel level [15].

4.2.3. Integration with SDN for Comprehensive Monitoring

Integrating advanced telemetry with SDN enhances the network's observability by providing detailed insights into traffic flows and network behavior. This integration enables the SDN controller to make informed decisions based on real-time data, improving the network's ability to respond to security incidents proactively [16].

4.3. Leveraging Artificial Intelligence (AI) for Threat Detection

4.3.1. Machine Learning Models for Anomaly Detection

Machine Learning (ML) models can be trained to detect anomalies in network traffic that may indicate security threats. Techniques such as Isolation Forests, Support Vector Machines (SVM), and Deep Neural Networks (DNN) have been employed to identify patterns associated with malicious activities [17].

4.3.2. Real-Time Threat Prediction and Mitigation

By analyzing telemetry data, AI models can predict potential security incidents before they fully manifest. This predictive capability allows for proactive mitigation strategies, such as adjusting network configurations or isolating affected segments to prevent the spread of an attack [6].

4.3.3. Challenges in AI-Driven Security

While AI offers significant advantages in threat detection, challenges remain, including the need for large datasets for training, the potential for adversarial attacks against AI models, and the interpretability of AI-driven decisions. Addressing these challenges is crucial for the effective deployment of AI in network security [17].

4.4. Integration of SDN, Telemetry, and AI for Proactive Security

4.4.1. Architectural Framework

The integration of SDN, telemetry, and AI forms a cohesive framework for proactive security in 5G networks. In this architecture:

- SDN Controllers manage and enforce security policies across the network.
- Telemetry Systems provide real-time data on network performance and anomalies.
- AI Engines analyze telemetry data to detect and predict security threats.

This collaborative approach enables dynamic and automated responses to security incidents, enhancing the resilience of the network [18].

4.4.2. Use Case: DDoS Attack Mitigation

Consider a scenario where a 5G network is targeted by a DDoS attack:

1. Detection: Telemetry data reveals abnormal traffic patterns indicative of a DDoS attack.
2. Analysis: The AI engine analyzes the data to confirm the attack and identify its characteristics.

3. Response: The SDN controller dynamically reconfigures the network to mitigate the attack, such as by rerouting traffic or implementing rate limiting.

This integrated response minimizes the attack's impact and maintains service availability [19].

4.4.3. Integrated Security Framework

The architecture outlined below integrates telemetry systems, AI engines, SDN (Software-Defined Networking) controllers, and network infrastructure to create a real-time, adaptive network management system. Telemetry data from the network is continuously sent to the AI engine, where advanced anomaly detection algorithms analyze the data and generate alerts when abnormal network behavior is detected. These alerts inform the SDN controller, which can adjust network configurations accordingly. The SDN controller sends policy updates and configuration commands back to the network infrastructure, ensuring that the network reacts dynamically to changing conditions and optimizes its performance in real-time. This seamless flow of data and feedback creates a self-healing and automated network capable of responding to anomalies and ensuring optimal performance without manual intervention.

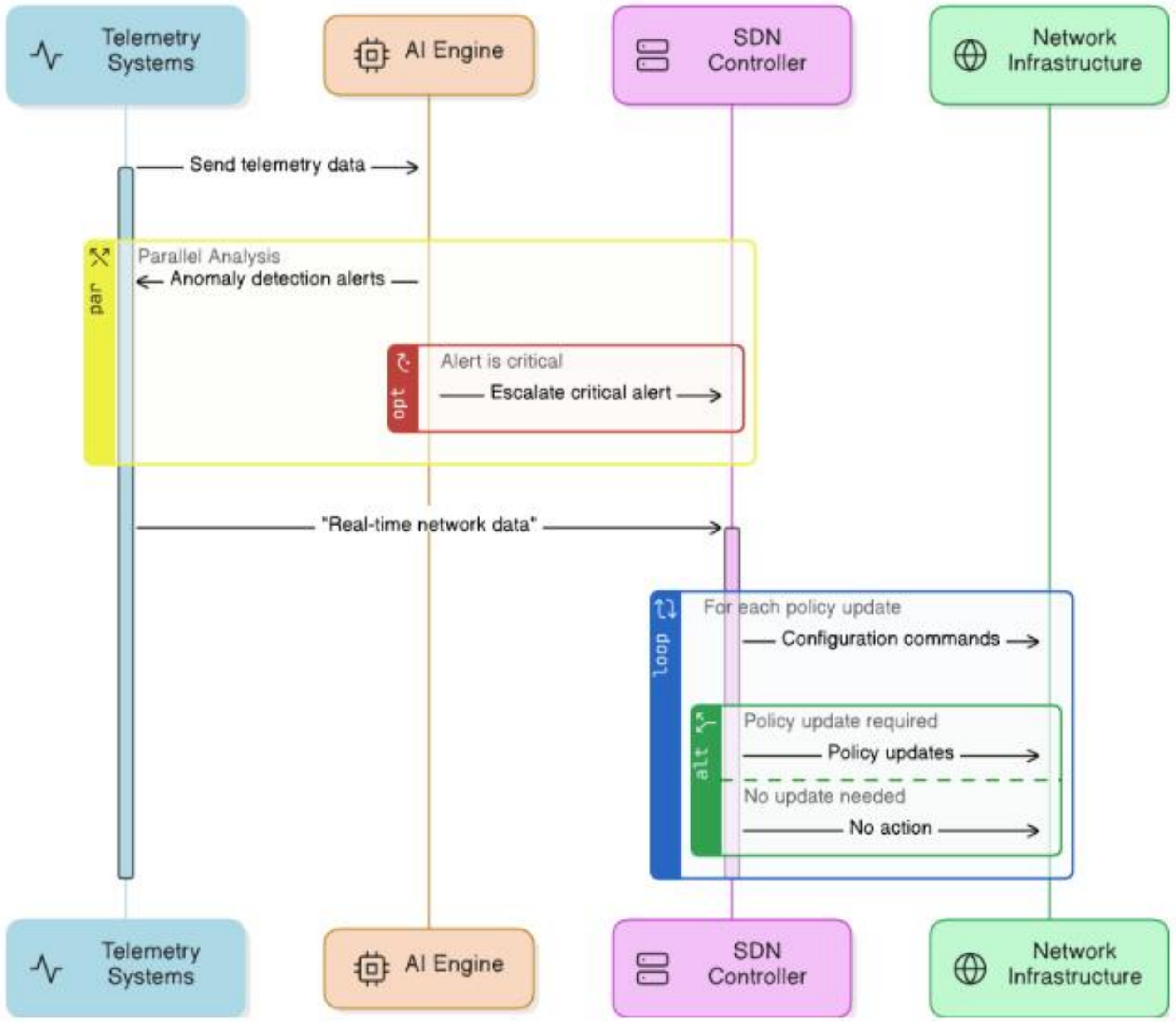


Figure 15.
Integrated Security Framework Sequence.

4.5. Key Performance Indicators (KPIs) for Security Observability

To evaluate the effectiveness of the integrated security framework, the following KPIs are considered:

- Detection Accuracy: The proportion of correctly identified security incidents.
- Response Time: The time taken from detection to mitigation of a security threat.
- False Positive Rate: The frequency of benign activities incorrectly identified as threats.
- Network Performance Impact: The effect of security measures on overall network performance.

Monitoring these KPIs ensures that security measures are both effective and efficient, maintaining the balance between protection and performance [6].

5. Observability-Driven Security Compliance Frameworks in 5G Networks

The integration of observability into modern security compliance frameworks is vital in addressing the complex challenges introduced by 5G networks. With the proliferation of distributed network functions, network slicing, and multi-access edge computing (MEC), the traditional methods of compliance auditing, anomaly detection, and risk mitigation fall short. Observability offers the ability to monitor, analyze, and infer internal states of a network based on external outputs, thereby enhancing both real-time compliance enforcement and proactive security. This chapter explores how observability enhances security compliance in 5G and aligns with emerging global standards.

5.1. The Imperative for Security Compliance in 5G Networks

5.1.1. Growing Threat Landscape in 5G

5G introduces an exponentially larger threat surface compared to previous generations due to its cloud-native architecture, software-defined networking, network slicing, and virtualized infrastructure. As a result, compliance with stringent security standards is not just a regulatory necessity but a functional requirement to ensure network integrity [19].

5.1.2. Global Compliance Standards and Bodies

Several international organizations provide frameworks and guidelines to ensure that 5G networks are secure, resilient, and compliant with best practices.

- 3GPP TS 33.501 defines the security architecture for 5G systems, including authentication, integrity protection, confidentiality, and subscriber privacy [1].
- ETSI NFV SEC outlines guidelines for secure virtualization of network functions, emphasizing trusted execution environments and isolation [4].
- NIST SP 800-207 introduces the Zero Trust Architecture, which has strong applicability in securing multi-tenant and multi-slice 5G environments [8].
- ENISA’s 5G Security Controls Matrix provides actionable controls based on the EU’s 5G cybersecurity toolbox, emphasizing monitoring, isolation, and policy compliance [11].
- GSMA FS.40 and FS.50 serve as operator-oriented security guidelines focusing on risk mitigation, architecture protection, and vendor compliance [2].

These standards collectively shape the compliance landscape that observability must support.

5.2. Observability as a Foundation for Security Compliance

5.2.1. Definition and Scope of Observability

Observability in network systems refers to the capability to infer the internal states of components based on telemetry data such as logs, traces, and metrics. Unlike traditional monitoring, observability enables proactive insights and root cause analysis [3].

In a 5G compliance context, observability plays three primary roles:

1. Monitoring Compliance State in Real Time
2. Automating Evidence Collection for Audits
3. Triggering Policy Enforcement Based on Detected Deviations

5.2.2. Visibility for Auditable Assurance

Effective compliance requires visibility into network configurations, access controls, API transactions, and authentication flows. Observability tools such as Prometheus, Elasticsearch, Jaeger, and OpenTelemetry can be deployed to continuously collect evidence aligned with 3GPP and NIST recommendations for network function behavior and service access patterns [20].

5.3. Frameworks that Enable Observability-Driven Compliance

5.3.1. ENISA 5G Security Controls Matrix

The ENISA controls matrix addresses domain-specific risks in 5G, including virtualization risks, supply chain security, and inter-slice isolation. Observability supports ENISA's control recommendations through real-time telemetry pipelines that validate control effectiveness [11]. For example, real-time detection of unauthorized cross-slice traffic via Jaeger traces directly aligns with ENISA's isolation controls.

5.3.2. GSMA Security Guidelines

GSMA's security guidelines emphasize baseline controls for 5G architecture protection. Observability tools support these controls by ensuring continuous validation of SLAs, user policy enforcement, and cryptographic integrity [2]. An example is the monitoring of UPF latency and throughput using Prometheus, which supports GSMA's requirement for data plane visibility and congestion prevention.

5.3.3. NIST Zero Trust Framework Integration

NIST’s Zero Trust model recommends continuous monitoring of trust signals and behavioral verification before granting access to any service [8]. Observability makes this possible by integrating signals from identity management, telemetry, and policy systems—enabling adaptive trust decisions in 5G environments.

5.4. Automation and Real-Time Policy Compliance

5.4.1. Closed-Loop Policy Enforcement

Observability enables closed-loop security operations, wherein telemetry inputs are analyzed and acted upon in real-time by automation frameworks like ONAP, SDN controllers, or policy engines [21]. For instance, a spike in anomalous API calls in the SMF (Session Management Function) can trigger ONAP to quarantine affected services and scale replicas in secure zones.

5.4.2. AI-Driven Compliance Monitoring

Machine learning models can be trained on observability data to detect policy violations, usage anomalies, or misconfigurations. Predictive compliance monitoring using AI enables early detection of SLA violations, security drift, or resource overuse, ensuring dynamic compliance enforcement [17].

5.5. Implementation Challenges and Considerations

5.5.1. Data Privacy and Ethics

While observability is critical for security and compliance, it must be balanced with privacy obligations such as GDPR. Collected telemetry should be anonymized, encrypted, and access-controlled to prevent misuse or overreach [20].

5.5.2. Toolchain Fragmentation

The variety of open-source and commercial observability tools can result in fragmented visibility and integration difficulties. Standards such as OpenTelemetry and ETSI ZSM aim to address this by offering unified schemas and APIs for observability [3].

5.6. KPIs for Observability-Driven Compliance

To measure the effectiveness of observability in enabling compliance, the following Key Performance Indicators (KPIs) are used:

Table 4.
AI-Driven Compliance Monitoring Performance Indicators.

KPI	Description
Compliance Drift Detection Rate	Frequency of detected deviations from policy configurations
Mean Time to Detect Policy Violation	Average time between a breach and its detection
Percentage of Automated Remediations	Ratio of compliance breaches resolved through automation
Audit Readiness Score	Availability of evidence required for compliance audits
SLA Violation Predictive Accuracy	Accuracy of AI models in forecasting potential SLA/security violations

5.7. Summary

The integration of observability into compliance frameworks represents a pivotal advancement for securing 5G networks. By aligning with globally recognized standards such as 3GPP TS 33.501, ENISA's control matrix, and NIST's Zero Trust architecture, observability tools enable continuous, auditable, and automated assurance. As 5G systems grow in complexity and exposure, real-time observability will be indispensable for sustained regulatory compliance, policy enforcement, and resilient network operations.

6. Proactive Observability in a 5G Smart City Deployment

The integration of 5G technology into urban environments is a significant driver of the smart city revolution. Smart cities utilize 5G's ultra-reliable, low-latency communication (URLLC) capabilities to support a broad spectrum of applications, including traffic management, autonomous vehicles, environmental monitoring, and public safety. Given the complexity of these systems, proactive observability becomes essential in ensuring both operational efficiency and security. This chapter explores how observability can enhance performance, security, and regulatory compliance in a 5G-powered smart city.

6.1. The Role of 5G in Smart Cities

6.1.1. Enabling Smart City Services with 5G

5G's high throughput, ultra-low latency, and massive machine-type communication (mMTC) capabilities provide a foundational infrastructure for smart city applications. These applications rely heavily on real-time data, where delays in processing can lead to significant risks—particularly in mission-critical services like emergency response, autonomous driving, and environmental monitoring [22].

For example, autonomous vehicles require seamless connectivity to exchange data about road conditions, traffic signals, and obstacles. Any disruption in this connectivity could lead to accidents or operational inefficiencies. Similarly, smart grids that rely on 5G must ensure that sensors communicate instantly to balance electricity loads across the grid in real time.

6.1.2. Observability as the Backbone of 5G Smart Cities

Proactive observability enables real-time monitoring of network conditions, device health, and application performance. By integrating observability tools such as Prometheus, OpenTelemetry, and Jaeger into the smart city's 5G architecture, network operators and city planners can identify issues before they escalate into serious disruptions [23].

Observability provides transparency into the performance of both network functions (e.g., UPF, SMF) and application services running at the edge. This transparency is critical for ensuring that smart city applications remain responsive and meet the required service level agreements (SLAs).

6.2. Use Case: Smart Traffic Management System

6.2.1. Overview of the Smart Traffic Management System

One of the flagship applications in a 5G-powered smart city is smart traffic management, which leverages real-time data from traffic cameras, vehicle sensors, and other connected infrastructure. Using this data, a central traffic control system can optimize traffic lights, reroute vehicles, and adjust speed limits in real time to reduce congestion and improve safety [24].

In a 5G deployment, observability systems are crucial for monitoring the real-time performance of the entire traffic management infrastructure. Any failure or latency in sensor data transmission, traffic light adjustments, or vehicle communication could lead to traffic accidents, gridlocks, or inefficient traffic flow.

6.2.2. Observability in Smart Traffic Management

To monitor and maintain high-performance levels, the following observability tools are deployed:

- Prometheus collects metrics from traffic sensors, cameras, and traffic lights. These metrics include response times, signal synchronization, and sensor uptime.
- OpenTelemetry is used for distributed tracing of vehicle data as it moves through the smart city infrastructure. This helps monitor the latency of traffic signal changes and the accuracy of vehicle position reporting.
- Jaeger is employed to trace requests between vehicles, traffic management systems, and cloud-based controllers.

By using these tools in tandem, the smart city's traffic management system can ensure that performance bottlenecks or connectivity issues are identified and resolved proactively.

6.2.3. Monitoring Traffic Signal Health with Prometheus

The Prometheus client library can monitor the health status of traffic signals. It can be defined to **Gauge** metric named traffic_signal_health that tracks whether a traffic signal is functioning properly (1 for healthy, 0 for malfunctioning). The simulate_traffic_signal_health function continuously generates random health statuses for traffic signals every 10 seconds, simulating either a healthy or malfunctioning signal. A Python script can be created to start an HTTP server on port 8000, where Prometheus can scrape the health data by periodically querying this endpoint. This setup allows Prometheus to monitor the state of traffic signals in real-time, enabling proactive maintenance or alerting when signals are malfunctioning. This code, if created, can establish a simple Prometheus exporter that tracks the health of traffic signals, with 1 indicating a healthy signal and 0 indicating a malfunction.

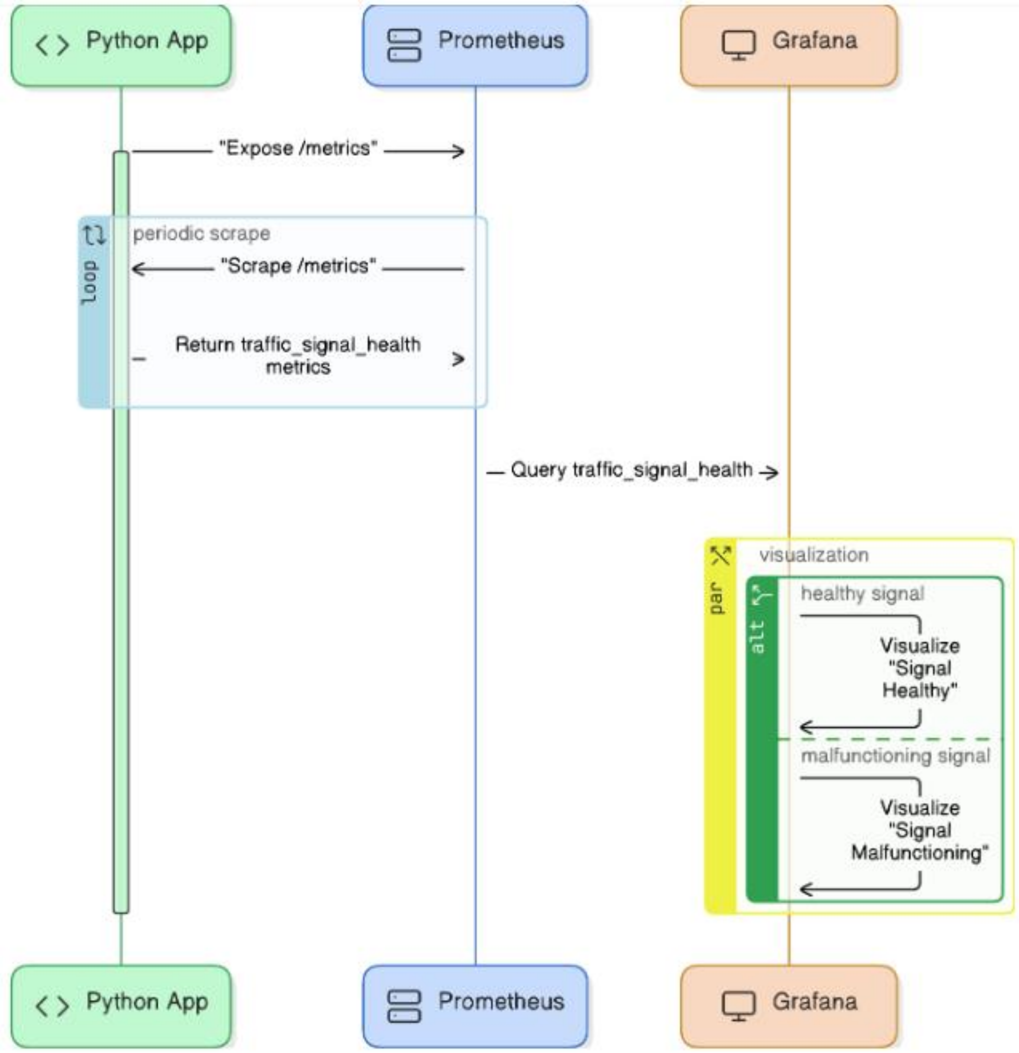


Figure 16.
Prometheus Monitoring of Traffic Signal Health.

6.3. Use Case: Environmental Monitoring and Waste Management

6.3.1. Overview of Environmental Monitoring

Another critical component of smart cities is environmental monitoring, which uses a combination of sensors to measure air quality, noise levels, water contamination, and temperature across the urban environment. These sensors collect real-time data that can trigger alerts or inform city planners about potential pollution hotspots or environmental hazards [25].

In a 5G deployment, environmental sensors are connected via 5G NR (New Radio) to ensure low-latency data collection and fast feedback loops. However, ensuring the health and accuracy of these sensors is paramount to maintaining accurate readings.

6.3.2. Observability in Environmental Monitoring

Proactive observability in this context involves tracking:

- Sensor health metrics: Are the sensors functioning correctly, or are they offline or malfunctioning?
- Data integrity: Is the data received from sensors accurate and within the expected thresholds?

Tools such as Prometheus and Grafana are used to collect and visualize environmental data, ensuring that city planners have access to up-to-date information about the city's environmental status.

6.3.3. Prometheus Exporter for Environmental Sensors

A Prometheus Exporter for Environmental Sensors is a tool that integrates environmental monitoring systems, such as pollution or air quality sensors, with Prometheus, a powerful open-source monitoring system. This exporter collects data from various environmental sensors and exposes the status of these sensors as metrics that Prometheus can scrape at regular intervals. Typically, the exporter tracks the operational status of the sensors, such as whether they are active or malfunctioning, using a metric like a Gauge, which is updated periodically. In practice, the exporter simulates or retrieves the status of environmental sensors (e.g., air pollution sensors) and provides this data to Prometheus for monitoring. Once the data is collected, it can be used to track sensor health, generate alerts if a sensor is malfunctioning, and visualize sensor performance over time. This integration is crucial for ensuring the reliability of environmental monitoring infrastructure, enabling timely responses to sensor failures, and helping organizations maintain accurate environmental data for decision-making and regulatory compliance.

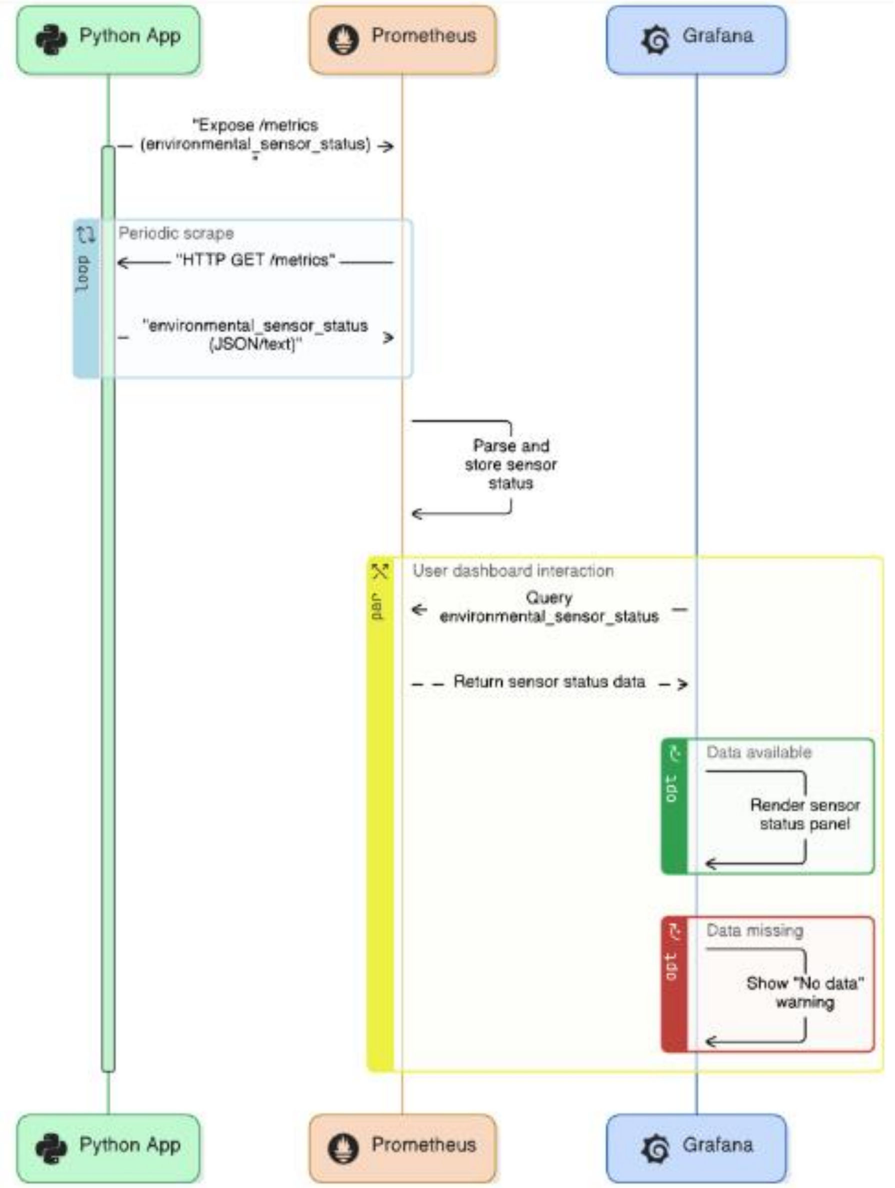

Python App
Prometheus
Grafana
"Expose /metrics (environmental_sensor_status)
loop
Periodic scrape
"HTTP GET /metrics"
"environmental_sensor_status (JSON/text)"
Parse and store sensor status
par
User dashboard interaction
Query environmental_sensor_status
Return sensor status data
opt
Data available
Render sensor status panel
opt
Data missing
Show "No data" warning
Python App
Prometheus
Grafana

Figure 17.
Prometheus Exporter for Environmental Sensors.

6.4. Use Case: Public Safety and Emergency Response

6.4.1. Enhancing Public Safety with 5G

In a smart city, public safety systems such as emergency response teams, surveillance cameras, and alert systems must be highly responsive to ensure timely interventions in critical situations. 5G's ultra-low latency and massive IoT capabilities support the rapid transmission of data from connected devices and cameras, enabling emergency responders to make real-time decisions.

6.4.2. Observability for Emergency Response

To ensure system readiness, observability tools are utilized to track the performance and availability of public safety infrastructure. For example:

- Jaeger traces can monitor the sequence of actions in emergency call centers and the dispatch of first responders.
- Prometheus can monitor the health of emergency response equipment, ensuring that communication systems are always functional.

6.5. Challenges in Implementing Observability for 5G Smart Cities

6.5.1. Data Privacy Concerns

While observability enables real-time monitoring, it also raises concerns about the privacy and security of citizen data. 5G smart cities must comply with data protection regulations like the General Data Protection Regulation (GDPR) in the European Union, ensuring that data used for observability does not infringe on personal privacy rights [1].

6.5.2. Integration Complexity

Integrating observability tools across multiple 5G systems—spanning both core and edge environments—can be complex. The dynamic nature of 5G networks, with its mix of virtualized network functions and physical infrastructure, demands seamless tool integration and standardization [26].

6.6. Future of Observability in Smart Cities

6.6.1. AI-Driven Insights

As smart city applications grow in sophistication, the integration of Artificial Intelligence (AI) into observability systems will enable predictive insights, automated decision-making, and self-healing networks. AI will be pivotal in enhancing anomaly detection and traffic forecasting [23].

6.6.2. Full Automation and Self-Healing Systems

Future smart cities will leverage observability data to automate network adjustments and security protocols. Automated scaling of network functions, rerouting of traffic during congestion, and real-time responses to environmental disasters will be a reality as observability systems evolve [22].

6.7. Summary

Proactive observability in 5G-powered smart cities is crucial for ensuring the continuous performance, security, and compliance of essential services. Through the use of observability tools like Prometheus, Jaeger, and OpenTelemetry, smart cities can achieve real-time insights into their infrastructure, mitigate risks, and optimize operations. The future of urban living will be shaped by the integration of observability systems, which will evolve to incorporate AI, automation, and self-healing networks.

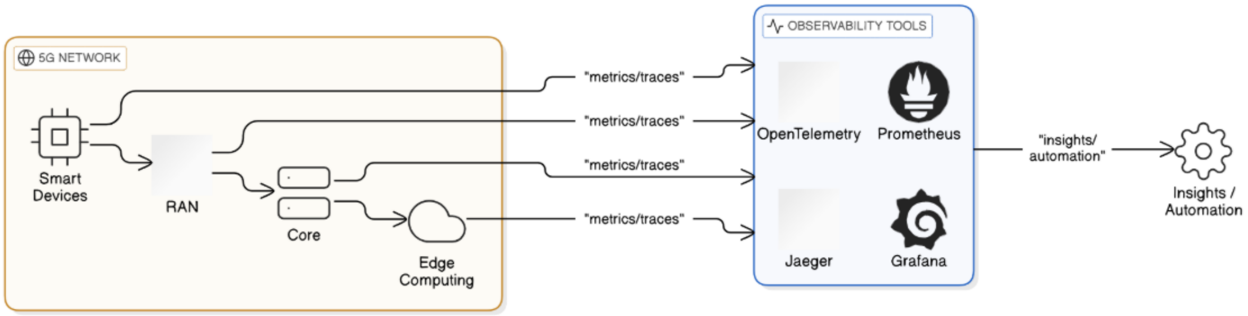


Figure 18:
Observability Stack for 5G Smart City Applications.

This diagram outlines the integration of observability tools in various 5G smart city applications. It shows how Prometheus, OpenTelemetry, Jaeger, and Grafana fit into the smart city ecosystem, monitoring different network layers and applications. The architecture emphasizes the importance of end-to-end monitoring in smart city services, with key observability components such as Prometheus, OpenTelemetry, and Jaeger providing visibility across the 5G RAN, core network, and edge computing layers.

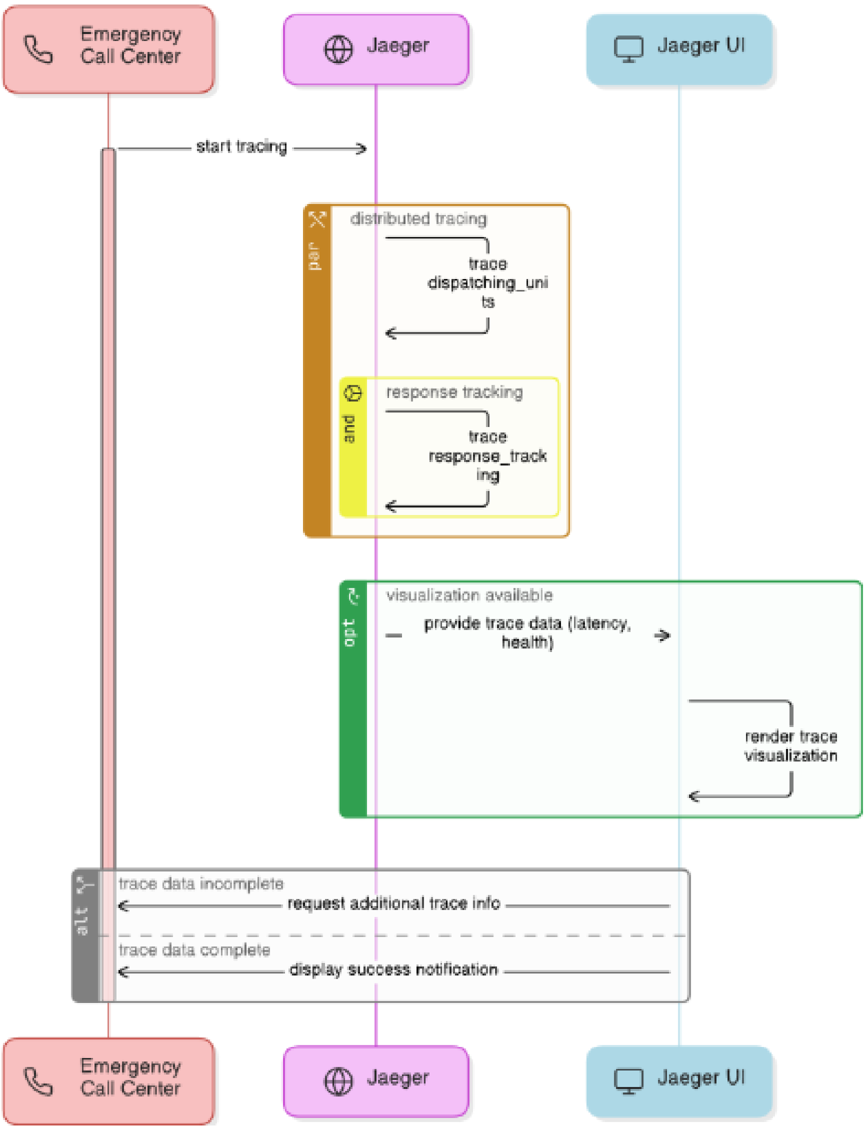


Figure 19:
Jaeger Distributed Tracing for Emergency Response.

In a public safety scenario, distributed tracing with Jaeger can be used to track the sequence of actions during an emergency response. In this example, Jaeger traces each step in the emergency response process, from the initial call to the dispatching of units and tracking their progress. These traces can be visualized in Jaeger's UI, showing the latency and health of the entire incident-handling process.

- Traffic sensors and autonomous vehicles collect real-time data, which is transmitted via 5G RAN and processed in the 5G core.
- OpenTelemetry collects distributed traces for network performance and latency tracking across the system, helping to identify delays or failures.
- Prometheus collects real-time metrics (e.g., signal health, response times) for traffic lights and sensor status.
- AI/ML models predict congestion and accident risks, triggering traffic signal adjustments based on real-time data.

7. Summary and Future Directions for Observability in 5G Networks

7.1. Summary of Key Findings

Throughout this paper, we have explored the crucial role of observability in securing, optimizing, and ensuring the compliance of 5G networks, particularly in the context of smart cities and emerging applications. The integration of observability tools with 5G networks is essential for real-time performance monitoring, security incident detection, and proactive management of critical systems. Below are the key takeaways from the paper:

7.1.1. The Growing Importance of Observability in 5G Networks

As 5G networks evolve and become more complex, the traditional methods of network monitoring and security management become insufficient. With the introduction of network slicing, virtualized network functions (VNFs), edge computing, and distributed services, new observability challenges emerge. Observability enables operators to track the health and performance of network functions and applications in real time, offering insights into network behavior and potential vulnerabilities.

Key tools like Prometheus, Grafana, OpenTelemetry, Jaeger, and ONAP form the backbone of modern observability in 5G environments. These tools facilitate continuous monitoring, distributed tracing, real-time metrics collection, and automated incident responses, ensuring that 5G networks operate efficiently and securely.

7.1.2. Observability and Security Compliance in 5G

In a highly distributed 5G architecture, observability also plays a pivotal role in ensuring compliance with security standards. Global regulatory bodies, including 3GPP, ETSI, NIST, and ENISA, have developed comprehensive frameworks for securing 5G networks. By integrating observability into these frameworks, network operators can continuously monitor their infrastructure for compliance with data protection regulations, service availability, and security protocols. Tools like Prometheus and Jaeger can be used to track metrics related to session management, encryption, and data integrity, ensuring that security measures are continuously enforced.

7.1.3. AI-Driven Observability for Proactive Security

The integration of Artificial Intelligence (AI) and Machine Learning (ML) with observability tools enhances the ability to predict network anomalies and security incidents before they occur. AI models, when combined with real-time telemetry data, enable operators to detect emerging threats, performance degradation, and compliance violations proactively. This predictive capability helps reduce mean time to resolution (MTTR) and enhances the network's overall resilience.

7.1.4. Key Use Cases of Observability in 5G Smart Cities

The application of observability tools in real-world use cases, such as smart traffic management, environmental monitoring, and public safety, underscores the importance of these technologies in supporting urban infrastructure. In these scenarios, observability tools collect real-time data from sensors, vehicles, and communication networks to ensure high performance, reliability, and security. The ability to proactively identify and address issues before they impact city services enhances the safety and efficiency of smart cities.

7.2. Future Directions and Challenges for Observability in 5G

While significant progress has been made in integrating observability into 5G networks, several challenges and opportunities lie ahead. The following section outlines key areas of focus for the future of observability in 5G networks.

7.2.1. Evolving Towards Autonomous Networks

As 5G networks mature, the demand for autonomous operations will increase. The ability of networks to self-optimize, self-heal, and self-scale will depend heavily on observability data. Tools like ONAP, SDN controllers, and AI-driven analytics will play a central role in enabling closed-loop automation, where network events trigger automated actions (e.g., traffic rerouting, fault isolation, or scaling of resources).

Observability-driven automation can significantly reduce manual intervention and improve service availability, especially in complex 5G environments such as network slicing and edge computing. This will be critical as 5G networks evolve to support more diverse use cases, including autonomous vehicles, smart cities, and industrial IoT.

7.2.2. Real-Time Security and Privacy Considerations

While observability provides critical insights into network performance and security, it also raises significant privacy concerns, especially in environments like smart cities where sensitive personal data is continuously generated by connected devices. Future observability solutions must ensure that privacy regulations (e.g., GDPR) are adhered to while still providing the required visibility into network health and security.

Furthermore, as 5G networks become the backbone of a wide array of critical infrastructure, including healthcare, finance, and public safety, ensuring secure telemetry becomes increasingly important. Future systems will need to integrate advanced encryption and anomaly detection mechanisms to safeguard both the data being collected and the systems involved in the observability process [27].

7.2.3. Standardization and Interoperability Challenges

One of the major challenges in achieving effective observability in 5G networks is the lack of standardization across different vendors and technologies. As 5G ecosystems expand, with multiple vendors offering network functions, components, and tools, achieving interoperability between different observability systems will be crucial.

Standardization efforts, such as those led by 3GPP, ETSI, and the Linux Foundation, are essential for creating frameworks that enable seamless data exchange and integration across different observability tools. Future work should focus on improving interoperability to ensure that observability systems function effectively across various environments and network configurations [22].

7.2.4. AI-Enhanced Predictive Analytics and Automation

AI-powered predictive analytics will play a key role in the future of observability, enabling anticipatory actions in the network. By analyzing vast amounts of telemetry data, AI models will be able to forecast potential network failures, security breaches, or performance issues before they manifest, allowing for timely interventions. Predictive maintenance, load balancing, and traffic optimization will become increasingly common as AI models are integrated into observability systems to drive proactive network management [25].

Furthermore, the evolution of AI-driven network automation will enable self-healing networks, where the network can automatically adjust its behavior based on detected anomalies or performance dips. These systems will rely heavily on real-time observability data to maintain the health and stability of the network autonomously.

7.3. Conclusion

Observability is a foundational element in the design, deployment, and operation of 5G networks. As the complexity of these networks grows, observability tools will be critical in ensuring performance, security, and compliance in real time. By integrating observability into smart city systems, autonomous networks, and security protocols, 5G operators can address both current and future challenges effectively. The AI-driven, automation-enabled, and compliance-centric nature of future observability systems will enable self-healing and resilient networks that are capable of adapting to an ever-evolving technological landscape.

References

[1] GSM Association, "5G security guidelines," *GSMA*, 2020.

[2] GSM Association, "5G security guidelines: Fs.40 and fs.50," *GSMA*, 2023.

[3] Cloud Native Computing Foundation, "Open telemetry project documentation," cloud native computing foundation," Retrieved: https://opentelemetry.io/docs/, 2022.

[4] European Telecommunications Standards Institute, "NFV-SEC 012: Security management and monitoring for virtualized network functions," *ETSI*, 2020.

[5] S. Scott-Hayward, "Software-defined networking: The new norm for networks," *IEEE Communications Magazine*, vol. 51, no. 6, pp. 14–23, 2013. https://doi.org/10.1109/MCOM.2013.6553663

[6] X. Lin, "Artificial Intelligence in 5G networks: Security applications and challenges," *Journal of Cyber Security and Privacy*, vol. 4, no. 3, pp. 19–37, 2020.

[7] S. Sonchack and M. Hossain, "High-performance in-band telemetry for 5G: Frameworks and applications," *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2417–2430, 2020. https://doi.org/10.1109/TNSM.2020.3029355

[8] V. Stafford, "Zero trust architecture," *NIST special publication*, vol. 800, no. 207, pp. 800-207, 2020. https://doi.org/10.6028/NIST.SP.800-207

[9] O. F. Ogunjinmi, "Optimizing network reliability: Strategies for resilient telecommunications infrastructure in emerging economies," *Global Journal of Engineering and Technology Advances*, vol. 22, no. 3, pp. 236–258, 2025. https://doi.org/10.30574/gjeta.2025.22.3.0065

[10] J. Castoldi, "Proactive security in SDN and 5G systems: Use cases and challenges," *Journal of Security and Privacy*, vol. 3, no. 4, pp. 20–35, 2021. https://doi.org/10.1007/s40940-021-00128-9

[11] European Union Agency for Cybersecurity, "5G security controls matrix," enisa," Retrieved: https://www.enisa.europa.eu/publications/5g-security-controls-matrix, 2021.

[12] A. O. Oladejo, M. Adebayo, D. Olufemi, E. Kamau, D. Bobie-Ansah, and D. Williams, "Privacy-aware AI in cloud-telecom convergence: A federated learning framework for secure data sharing," *International Journal of Science and Research Archive*, vol. 21, no. 3, pp. 144-167, 2025. https://doi.org/10.30574/gjeta.2024.21.3.0235

[13] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14-76, 2014. https://doi.org/10.1109/JPROC.2014.2370092

[14] T. Kim, "In-band network telemetry: From packet-level traces to network-wide insights," *ACM SIGCOMM Computer Communication Review*, vol. 45, no. 4, pp. 55–64, 2015. https://doi.org/10.1145/2815677.2815682

[15] D. Borkmann, "The eBPF revolution: Leveraging eBPF for high-performance observability," *ACM SIGCOMM Computer Communication Review*, vol. 47, no. 1, pp. 54–60, 2017. https://doi.org/10.1145/3051321.3051331

[16] S. Sonchack, "Real-time anomaly detection using in-band network telemetry: A case study," *ACM SIGCOMM Conference*, vol. 28, no. 3, pp. 76–88, 2018. https://doi.org/10.1145/3230795.3230800

[17] K. Kaur, V. Kumar, and M. Singh, "Artificial Intelligence techniques for intrusion detection in 5G networks: A survey," *Computer Communications*, vol. 2023, pp. 73–88, 2023. https://doi.org/10.1016/j.comcom.2023.02.026

[18] J. Castoldi, "Future of 5G network automation: From configuration to monitoring," *Future Networks and Services*, vol. 2, no. 3, pp. 128–145, 2025.

[19] S. Alshahrani, O. Bamasak, and A. Abuzneid, "Security and privacy in 5G networks: A survey," *IEEE Access*, vol. 10, pp. 19807–19833, 2022. https://doi.org/10.1109/ACCESS.2022.3149937

[20] K. O'Hara and G. Baldini, "Ethics and privacy in 5G technology: A framework for governance," *Telecommunications Policy*, vol. 45, no. 2, p. 102102, 2021. https://doi.org/10.1016/j.telpol.2020.102102

[21] P. Bertin, "Intent-based security automation for 5G: Challenges and research directions," *Journal of Network and Systems Management*, vol. 29, no. 2, pp. 1–27, 2021.

[22] S. Belli, R. Caffarelli, and G. Bassi, "5G-enabled smart city applications: Opportunities and challenges," *Journal of Network and Systems Management*, vol. 29, no. 3, pp. 1–23, 2021. https://doi.org/10.1007/s10922-021-09684-w

[23] L. Zhang, X. Lin, and Y. Zhao, "5G-enabled smart cities: Challenges and opportunities," *Future Generation Computer Systems*, vol. 108, pp. 93–99, 2020. https://doi.org/10.1016/j.future.2020.02.038

[24] Y. Zhang and Y. Luo, "Real-time security monitoring in 5G networks using AI and SDN," *IEEE Security & Privacy*, vol. 19, no. 6, pp. 45–56, 2021. https://doi.org/10.1109/MSP.2021.3087228

[25] M. S. Hossain and S. Islam, "Real-time environmental monitoring and management in smart cities: A 5G perspective," *IEEE Access*, vol. 8, pp. 131314–131325, 2020. https://doi.org/10.1109/ACCESS.2020.3012122

[26] K. Pahlavan and X. Li, "Smart city 5G architectures and challenges," *Wireless Personal Communications*, vol. 113, no. 3, pp. 1617–1631, 2020. https://doi.org/10.1007/s11277-020-07277-w

[27] Z. Zhang, "End-to-end performance monitoring of mobile networks: Challenges and future directions," *IEEE Communications Surveys & Tutorials*, vol. 32, no. 3, pp. 1879–1905, 2020. https://doi.org/10.1109/COMST.2020.2986374