A Detection Framework for Identity Protection in Cloud-Based 5G Core Networks*

Mirae Kim[1], Mijin Shin[1], Hyunji Lee[1], and Seongmin Kim[1]

Sungshin Women's University, Seoul, Republic of Korea
{20231066, 220256037, 20231105, sm.kim}@sungshin.ac.kr

Abstract

This study proposes a cloud-based anomaly detection framework for CSPs to identify abnormal states in virtualized 5G core networks. The framework focuses on enhancing trust and log integrity during the subscriber identity verification process.
Keywords– 5G Security · Privacy · Mobile Security.

1 Introduction

The new 5G standalone (SA) mobile network architecture virtualizes functions that were previously implemented on physical network equipment, enabling flexible, cloud-based infrastructure. This evolution enhances interoperability between mobile network operators (MNOs) and cloud service providers (CSPs) but simultaneously introduces new security challenges related to trust boundaries and log integrity within the virtualization layer. In particular, CSPs must oversee security management and event logging associated with personally identifiable information (PII) within the virtualized core network.

However, network functions operating on virtualized servers remain vulnerable to interference or infiltration by third-party applications. If a malicious network function gains access through such interactions, subscriber data may be exposed due to insufficient CSP-level management. To address this issue, we propose a cloud-based anomaly detection framework that enables CSPs to identify abnormal states in virtualized 5G core networks during the identity verification process.

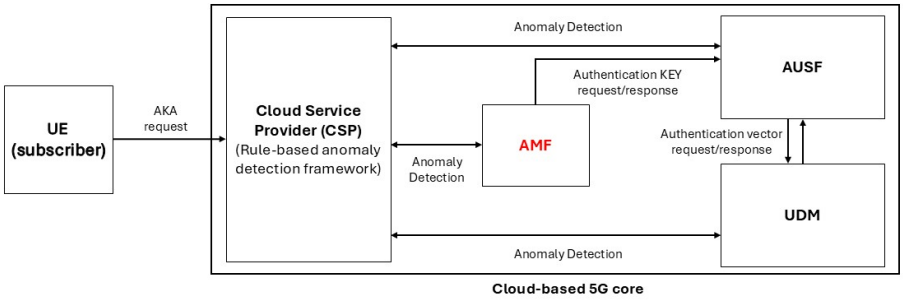

Figure 1: Cloud-Based Framework for AKA-protocol Leak Detection

2 Threat Model and Log–Based AMF Anomaly Detection

The identity verification process in 5G networks is performed through the Authentication and Key Agreement (AKA) protocol, where authentication vectors and key generation parameters

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-3, December 16-18, 2025, Sapporo, Japan.

are exchanged among the Access and Mobility Management Function (AMF), Authentication Server Function (AUSF), and Unified Data Management (UDM) [1]. In this process, the AUSF and UDM collaboratively verify authentication responses and generate corresponding vectors for the AMF. However, if the AMF is compromised or manipulated by a third-party application, the AUSF and UDM may continue producing authentication vectors as if the procedure were legitimate, remaining unaware of the compromised AMF state [2]. This can lead to a control plane operating on forged or replayed messages while maintaining seemingly valid authentication results. As shown in Figure 1, to address this blind spot, we design a rule-based anomaly detection framework that analyzes AMF logs to identify abnormal behavior during the identity authentication phase. The feasibility of the proposed framework is validated through an analysis of the log characteristics and abnormal patterns observed in AMF operations [2].

Table 1: AMF Log Features for Anomaly Detection

Feature	**Description**	**Detection Objective**
Timestamp	Event occurrence time	Validation of repetition or timing anomalies based on temporal patterns
UE_ID	Device or session identifier	Detection of abnormal repetitive events or frequent reconnection attempts
Message Type	NAS/NGAP message type classification	Identification of abnormal message sequences compared with normal routines
Security Context ID	Unique security session identifier	Detection of repeated use of the same context ID within different sessions
State Event	NAS state transition messages	Detection of abnormal state transition violations
Warning/Error Event	Warning or error messages recorded	Logging of tampered or abnormal packet events

As shown Table 1, detection rules are defined based on the authentication event logs requested and generated by the AMF during the identity authentication procedure.

1. Repeated NAS sequence numbers or Security Context IDs within a short interval indicate possible brute-force or replay attempts to infer the UE sequence number.
2. A SecurityModeComplete message observed without a preceding SecurityModeCommand implies potential exposure of the UE's security parameters or identity information.
3. Excessive or repeated authentication requests originating from a single UE suggest replay attempts to exfiltrate subscriber identity data.
4. Significant deviation in the inter-arrival time of NAS or NGAP messages from the standard mean indicates possible intermediate manipulation or delay injection.

These rules are constructed by detecting deviations from legitimate NAS/NGAP message sequences, emphasizing the AMF's role in maintaining security context integrity. When abnormal log patterns are detected during inter-NF interactions, it becomes crucial to preserve the continuity and integrity of the identity authentication process. The proposed rule-based framework adopts AMF-centric monitoring to identify such anomalies and establish a foundation for secure fallback and recovery in cloud-based 5G core networks.

References

[1] Sudip Maitra, Tolga O. Atalay, Angelos Stavrou, and Haining Wang. Towards shielding 5g control plane functions. In *2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 302–315, 2024.

[2] Zujany Salazar, Huu Nghia Nguyen, Wissam Mallouli, Ana R. Cavalli, and Edgardo Montes de Oca. 5greplay: a 5g network traffic fuzzer - application to attack injection. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ARES 2021, page 1–8, 2021.