Intrusion Detection Approaches for RESTful Communication in 5G Service-Based Architecture*

Youngjae Kim, Bonam Kim, and Ilsun You

Kookmin University, Seoul, Republic of Korea
{zeroash1225,kimbona,isyou}@kookmin.ac.kr

Abstract

The 5G Service-Based Architecture (SBA) enables flexible NF communication through RESTful APIs over HTTP/2 and JSON. However, web-based protocols broaden the attack surface, introducing threats such as token replay, DoS, and JSON manipulation. This study applies intrusion detection to SBA traffic, where a lightweight IDS detects abnormal API behaviors while remaining silent during normal operations, enhancing 5G core security.
Keywords: 5G, Service-Based Architecture, Intrusion Detection System

1 Introduction

The 5G Core adopts a Service-Based Architecture (SBA) where Network Functions (NFs) communicate via RESTful APIs over HTTP/2[1] As shown in Figure 1. Although TLS and OAuth 2.0 secure transport and authorization, web-based interfaces broaden the attack surface[2].

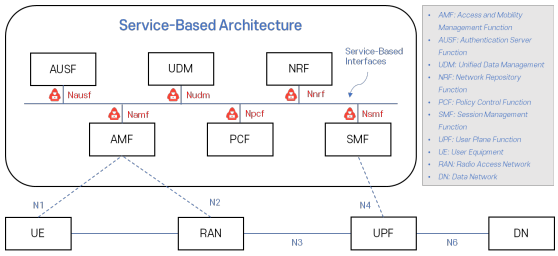

Figure 1: 5G Network Architecture and Attack Surface

Thus, 5G control-plane operations remain vulnerable to NF impersonation, token replay, and HTTP/2 or JSON-based DoS[3]. Intrusion detection techniques analyzing REST traffic and validating JSON payloads can detect abnormal API behavior and strengthen security.

2 Attack Scenario

Figure 2 illustrates three attack scenarios and their corresponding intrusion detection mechanisms. In the Token Replay and NF Impersonation scenario, a stolen OAuth 2.0 token reused from a new IP address indicates an attempt to impersonate a legitimate NF. For the HTTP/2-based Denial of Service attack, excessive stream creation or oversized headers can overload NF resources such as CPU and memory. These behaviors are detected by monitoring request rates and header sizes. Lastly, JSON Payload Manipulation involves adding or modifying fields within API messages to disrupt normal processing logic. Schema validation and payload inspection are used to detect such anomalies hidden within encrypted traffic.

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-63, December 16-18, 2025, Sapporo, Japan.

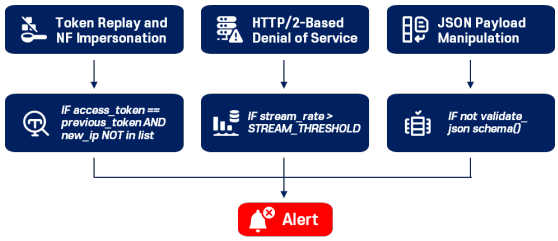

Figure 2: Netwok Function Security Threats and Detection

3 Experiment

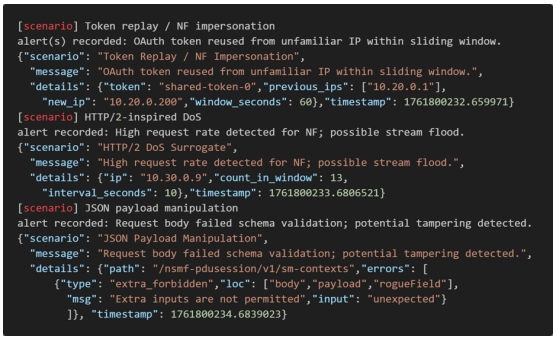

Figure 3: Attack Detection Logs

Figure 3 shows IDS outputs for three representative attack scenarios. Token reuse from 10.20.0.200 triggered impersonation alerts. HTTP/2 flood (13 requests/10 s) raised rate-limit warnings. JSON tampering with "rogueField" caused schema violation alerts. The IDS correctly flagged anomalies while ignoring normal traffic.

4 Conclusion

While TLS and OAuth 2.0 protect lower layers, they cannot prevent application-level threats. The proposed lightweight IDS effectively detects abnormal RESTful API behaviors, enhancing the security and resilience of the 5G core network.

Acknowledgement: This work was supported by Institute of Information & Communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) (No. RS-2024-00397469, Development of 5G Private Network Security Technology for Integrated Security of Specialized and Enterprise Networks).

References

[1] 3GPP. Common api framework for 3gpp northbound apis. Technical Report TS 23.222, 3rd Generation Partnership Project (3GPP), 2023. Version applicable at publication time.

[2] G. Mayer. Restful apis for the 5g service based architecture. *Journal of ICT Standardization*, 6(1-2):101–116, 2018.

[3] Q. Tang et al. A systematic analysis of 5g networks with a focus on 5g core security. *IEEE Access*, 10:18298–18319, 2022.