Structure-Aware NGAP Fuzzer Design for Procedural and State Anomaly Analysis*

Nakyung Lee[1], Young Seo Nam[2], Jinha Kim[2] and Hwankuk Kim[2†]
[1] Sangmyung University, Cheonan, South Korea
[2] Kookmin University, Seoul, South Korea
nakyeoungl0123@gmail.com, rinyfeel@kookmin.ac.kr

Abstract

This paper presents a structure-aware NGAP-based fuzzing framework for assessing vulnerabilities in Network Functions in 5G network environments. Owing to architectural features of cellular cores that hinder effective fuzzing, prior work has predominantly focused on a single protocol layer (e.g., NAS). In response, this study presents a fuzzing tool design that targets NGAP and performs structure-aware mutations at the IE-level within stateful scenarios that reproduce 3GPP procedures.

Keywords: *Access and Mobility Management Function (AMF), NG Application Protocol (NGAP), Structure-Aware Fuzzing, 5G Core (5GC)*

1 Introduction & Methodology

The 5G Core (5GC) adopts a service-based architecture (SBA) in which Network Functions (NFs) — such as Access and Mobility Management Function (AMF), Session Management Function (SMF), and User Plane Function (UPF) — are composed via service interfaces. This forms a standardized mobile-communications infrastructure that encompasses both public and non-public networks (NPN), and provides the basis for configuring and operating logically isolated network slices on a common physical infrastructure according to service-level requirements [1]. Control-plane signaling between NG-RAN and the 5GC is primarily conveyed via the Non-Access Stratum (NAS) and the NG Application Protocol (NGAP). NAS handles authentication, security, and session management between the User Equipment (UE) and the core, whereas NGAP coordinates registration, resource control, and other state transitions between the gNodeB (gNB) and the AMF [2]. While many prior fuzzing studies have focused on a single protocol layer (for example, NAS or Radio Resource Control (RRC)), and although research targeting NGAP has recently increased, systematic structure-aware verification of NGAP remains relatively scarce [3, 4].

To address this gap, we propose a structure-aware fuzzing framework for NGAP. The framework mutates diverse NGAP message formats exchanged with 5G Core Network Functions and monitors the target system for abnormal behavior to uncover potential vulnerabilities. It models 3GPP procedures as a state machine to select signaling sequences, and it combines per-IE, ASN.1-based generation and mutation with structure-aware transformations of signaling sequences. By focusing on NGAP over the Stream Control Transmission Protocol (SCTP), the framework increases the proportion of syntactically and semantically valid inputs. This is achieved by exercising both request-transmission and response-

* Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-22, December 16-18, 2025, Sapporo, Japan.
† Corresponding author: Hwankuk Kim, Kookmin University, Seoul, South Korea, rinyfeel@kookmin.ac.kr

handling paths, which enables deeper protocol logic exploration and comprehensive detection of procedural vulnerabilities. Each processing stage reproduces AMF state transitions according to the procedures defined in 3GPP TS 38.413 (see Figure 1). By performing semantic IE modifications rather than naive bit-level mutations, the framework generates inputs that remain acceptable within legitimate sessions while probing protocol edge cases. Consequently, the framework is capable of detecting a wide range of faults, including procedural state inconsistencies in NGAP and logical vulnerabilities arising during authentication and session-management phases.

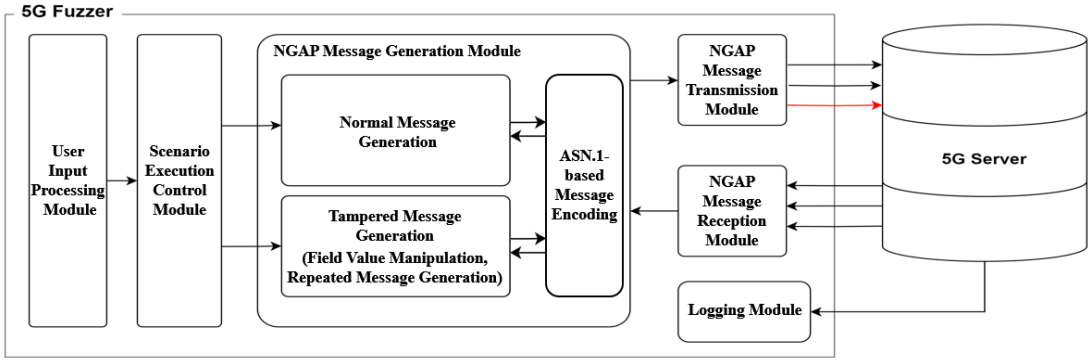

Figure 1

2 Conclusion

In this work, we presented the design of a prototype NGAP-based fuzzing framework targeting NFs. For future work, we will verify compliance with the NGAP standard and characterize AMF behavior by generating legitimate NGAP messages and simulating Denial-of-Service (DoS) scenarios. We also plan to extend the framework to support NGAP field-level mutations and to add coverage for other NFs, such as the UPF, thereby progressing toward a comprehensive 5G security testing framework.

Acknowledgement

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MIST) (No.RS-2024-00438156, Development of security resilience technology based on network slicing service in the 5G specialized Network)

References

[1] 3GPP TS 23.501, 5G; System architecture for the 5G System (5GS)

[2] 3GPP TS 38.413, NG-RAN; NG Application Protocol (NGAP)

[3] N. Bennett, W. Zhu, B. Simon, R. Kennedy, W. Enck, and K. R. B. Butler. (2024). RANsacked: A Domain-Informed Approach for Fuzzing LTE and 5G RAN-Core Interfaces. In *Proc. ACM Conf. Comput. Common Security (CCS)*

[4] Y. Sun, X. Liu, Q. Sun, J. Wang, L. Tian, and J. Liu. (2025). 5GC-Fuzz: Finding Deep Stateful Vulnerabilities in 5G Core Network with Black-box Fuzzing. In *Proc. IEEE*