Implementation of Real-time Network Function for False Base Station Detection in 5G Environments

Daehyeon Son and Ilsun You*

Kookmin University, Seoul, Republic of Korea
{sondh97, isyou}@kookmin.ac.kr

Abstract

In the context of 5G environments, the threat of attacks on false base stations(FBS) remains a critical concern. To address these threats, this paper introduces the implementation of a real-time network function for the detection of FBS through the use of the 5G RAN simulator-UERANSIM, which collects Measurement Report from base stations.

Keywords: 5G, UERANSIM, Machine Learning, Specification-based, Network Function

1 Introduction

In the 5G environment, it offers innovative mobility through enhanced mobile bandwidth and substantial support for digitalization in the corporate and industrial sectors. However, with the explosive proliferation of cost-effective IoT(Internet of Things) applications, which are often vulnerable, security threats have surged for both operators and end-users within these 5G mobile networks. Among the various potential threats in the 5G landscape, attacks on FBS, including SUCI(SUbscription Concealed Identifier)-Catchers, pose a genuine risk, potentially compromising user privacy through active or passive methods[1]. Therefore, in order to mitigate these challenges, this paper implements real-time detection of FBS using machine learning and specification-based techniques through an open-source 5G RAN simulator-UERASIM, as shown in Figure 1.

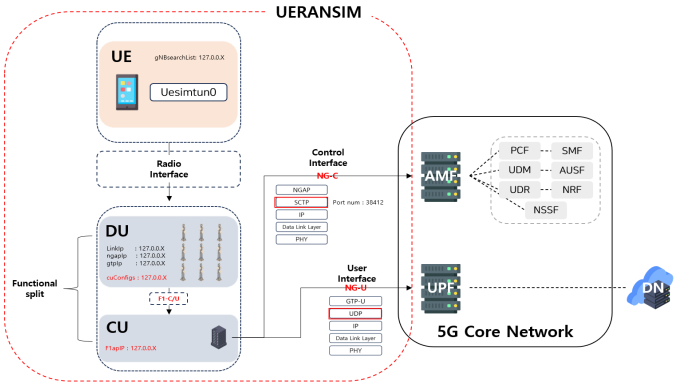

Figure 1: Modified UERANSIM Architecture

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, JAPAN, Article No. P-35
*Corresponding author: Department of Financial Information Security, Kookmin University, Seoul, 02707, Republic of Korea, Tel: +82-02-910-5127

2 Main

The newly implemented Network Function, FDF(False Base Station Detection Function), was experimentally tested in the 5G RAN environment using an enhanced UERANSIM with Functional Split and handovers. FDF communicates directly with CU(Central Unit). Messages obtained during this process, such as Measurement Report, RRC Setup, and Handovers, form the basis for the detection of FBS. There are two methods for detecting FBS. The first method, employing machine learning, detects abnormal signals through Measurement Report that include the wireless environment surrounding the device when a FBS is present. The second method, specification-based detection technique detects threats through data received from CU through a state machine indicating abnormal conditions, and then detects abnormal behavior if a FBS is detected among all data based on a certain period[2]. Figure 2 is the result of detecting FBS based on real-time incoming data as an implemented FDF.

Figure 2: Machine Learning / Specification Misbehavior Detection result

3 Conclusion

5G SA(Stand Alone) operates on an SBA(Service-Based Architecture) structure, utilizing technologies like SDN(Software-Defined Networking) and NFV(Network Function Virtualization) to virtualize and manage network functions for efficient communication. Additionally, it employs methods such as network slicing to deliver a variety of network services. One effective approach to optimizing the use of these technologies is deploying network functions tailored to each slice, ensuring optimal Network Function configuration based on QoS(quality of service) and application-specific needs for each slice. Currently CU exists in a serving network such as a DU(Distributed), but when virtualized, it is located in the core network and uses the SBI(Service-Based Interface) structure. Therefore, if the newly implemented FDF is located in the core network with the CU and communicates, it is expected that a security structure that can be organically linked to the SBA can be created after detection of FBS is made later.

Acknowledgments : This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No.2020-0-00952, Development of 5G Edge Security Technology for Ensuring 5G+ Service Stability and Availability, 100%)

References

[1] C. Popper T. Holz CM. Chlosta, D. Rupprecht. 5g suci-catchers: Still catching them all? In *Proc. of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 359–364, June 2021.

[2] H.Y. Park. *Research on False Base Station Detection Techniquesfor Secure Radio Access Networkin Next-Generation Mobile Communication Environments*. PhD thesis, Department of Information Security at Soonchunhyang University, August 2023.