ISSN: 2093-5374 / E-ISSN: 2093-5382

# A Study on the Implementation of a Network Function for Real-time False Base Station Detection for the Next Generation Mobile Communication Environment

Daehyeon Son[1], Youngshin Park[2], Bonam Kim[3], and Ilsun You[4*]

[1]Kookmin University, Seoul, Republic of Korea, South Korea. sondh97@kookmin.ac.kr, https://orcid.org/0000-0003-0722-4851

[2]Kookmin University, Seoul, Republic of Korea, South Korea. p17030508@kookmin.ac.kr, https://orcid.org/0009-0004-0787-4779

[3]Kookmin University, Seoul, Republic of Korea, South Korea. kimbona9@kookmin.ac.kr, https://orcid.org/0000-0002-8074-4899

[4*]Kookmin University, Seoul, Republic of Korea, South Korea. isyou@kookmin.ac.kr, https://orcid.org/0000-0002-0604-3445

Received: September 15, 2023; Revised: November 20, 2023; Accepted: January 19, 2024; Published: March 30, 2024

## Abstract

The threat posed by false base stations remains pertinent across the 4G, 5G, and forthcoming 6G generations of mobile communication. In response, this paper introduces a real-time detection method for false base stations employing two approaches: machine learning and specification-based. Utilizing the UERANSIM open 5G RAN (Radio-Access Network) test platform, we assess the feasibility and practicality of applying these techniques within a 5G network environment. Emulating real-world 5G conditions, we implement a functional split in the 5G base station and deploy the False Base Station Detection Function (FDF) as a 5G NF (Network Function) within the CU (Central Unit). This setup enables real-time detection seamlessly integrated into the network. Experimental results indicate that specification-based detection outperforms machine learning, achieving a detection accuracy of 99.6% compared to 96.75% for the highest-performing machine learning model XGBoost. Furthermore, specification-based detection demonstrates superior efficiency, with CPU usage of 1.2% and memory usage of 16.12MB, compared to 1.6% CPU usage and 182.4MB memory usage for machine learning on average. Consequently, the implementation of specification-based detection using the proposed method emerges as the most effective technique in the 5G environment.

**Keywords:** 5G, False Base Station, Network Function, Security, Abnormal Behavior Detection.

## 1 Introduction

5G (5G, Fifth generation technology standard) is a fifth-generation mobile communication network based on the official designation IMT-2020 (International Mobile Telecommunications-2020), significantly improving bandwidth, latency, terminal connection capacity, and other aspects compared to previous generations, enabling services that were previously impossible (Fruhlinger et al., 2023; Yan

*Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, volume: 15, number: 1 (March), pp. 184-201. DOI: *10.58346/JOWUA.2024.I1.013*

*Corresponding author: Kookmin University, Seoul, Republic of Korea, South Korea.

2010). Through these advancements, 5G networks, coupled with state-of-the-art terminal and sensor technologies, as well as AI (Artificial Intelligence) and Machine Learning technologies, are driving innovation and advancement in various fields such as smart cities, smart factories, smart grids, and autonomous vehicles, contributing to the establishment of future-generation mobile communication-based industrial infrastructure. However, despite these developments, threats persist. One of the continuously mentioned threats is the false base station attack. Malicious actors deploy false base stations by impersonating legitimate base stations, allowing them to steal important resources such as user's personal information or exhaust resources through DoS attacks (Khan et al., 2022). The primary objective of threats originating from false base stations is often to compromise user availability. Therefore, ongoing research efforts to mitigate the aforementioned threats are essential to ensure users receive the highest quality of service. In this paper, we aim to validate the feasibility of addressing false base stations based on abnormal behavior detection by implementing machine learning-based detection and rule-based specification of false base station attack detection techniques in the form of NF, using real-time RSRP (Received Signal Reference Power) values received through UERANSIM. Ultimately, this ensures the reliability and sustainability of services provided in the 5G environment.

## 2 Background and Security Threats

### 1) 5G System Architecture

The structure of the 5G system is as depicted in Figure 1. The composition of the 5G service network consists of UE (User Equipment), NG-RAN (New Generation – Radio Access Network), and the core network responsible for service connection control and UE authentication. Here, UE refers to user terminals, which connect to the RAN via the wireless interface (Air-Interface). The RAN provides the wireless interface to UE, allocates wireless resources, and controls UE mobility (Abdullah 2020). The core network is comprised of multiple NFs and connects UE to the data network through the UPF (User Plane Function), which handles the user plane (Manipriya et al., 2020).

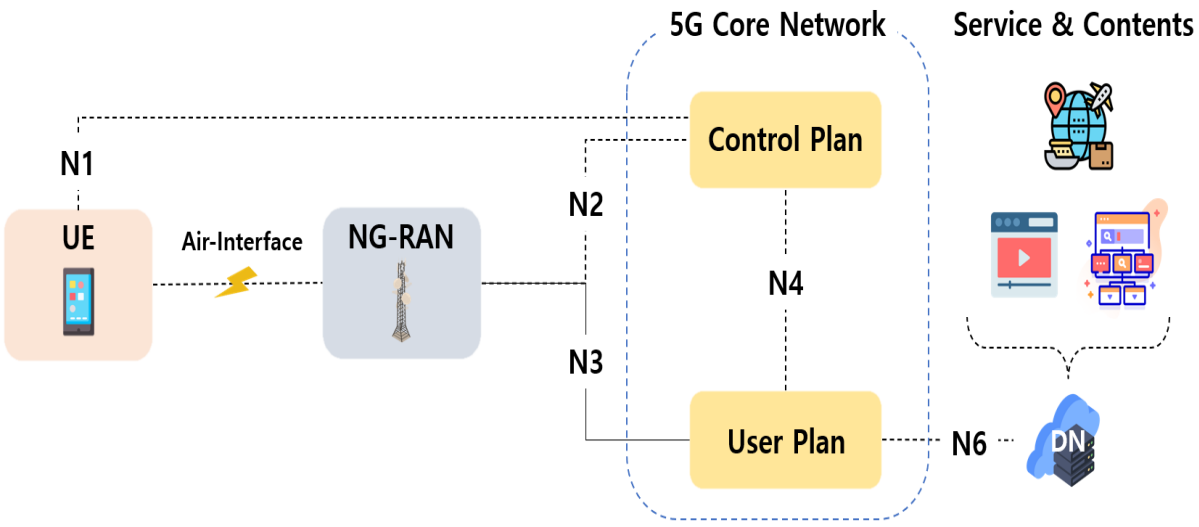


Figure 1: 5G System Architecture

The 5G system provides services based on the interaction of NFs. Basic NFs were defined in 3GPP Release 15, with additional NFs such as SCP (Service Communication Proxy) and NSSAAF (Network Slice Specific Authentication and Authorization Function) defined in Release 16, and further NFs like EASDF (Edge Application. Server Discovery Function) and NSACF (Network Slice Admission Control Function) defined in Release 17 (Krisztian et al., 2024).

Compared to the previous 4G, the 5G system undergoes structural changes due to the broadening of RAN bandwidth, core separation, and unit reassignment. The broadening of RAN bandwidth allows for the utilization of higher bandwidth due to wider frequency bands (Panek et al., 2022). In terms of core separation and unit reassignment, 5G employs server virtualization based on MEC (Multiple-Access Edge Computing), distinguishing it from previous generations. This allows for forward deployment of the core to provide user data services from locations close to the user. UP (User Plane) is deployed forward, while CP (Control-Plane) is positioned at the core site, facilitating core separation and forward deployment.

### 2) Service Based Architecture

As an innovative architecture in 5G, SBA (Service-Based Architecture) has been introduced (Brown 2017). In 5G SBA, each network device is software-defined into NFs, and through the SBI (Service-Based Interface) based on SDN (Software Defined Networking) and NFV (Network Function Virtualization), they are organically interconnected (Shin 2022; Shin 2019). With the introduction of SDN/NFV concepts, various NFs in the core network have been software-defined and can operate in a virtualized environment. This led to the definition of separate Peer to Peer interfaces required for adding NFs and entities in mobile communication systems (Rudolph et al., 2019). By adopting the SBA structure in the 5G system, each NF can provide independent and reusable services. While this structure may be less efficient for introducing new features quickly, with the transition to the 5G system, introducing the SBA structure to NFs handling the control plane allows each NF to serve as a service provider, offering specific services through a single SBI, thereby retaining independence and reusability advantages (Wanshi & Puneet 2023).

In SBA, each NF exposes implemented services through the HTTP/2 protocol and REST method, provided via the SBI. This structure allows new NFs to easily access other NF functionalities once permission is granted, enabling efficient network management in virtualized and cloud environments. The SBI in SBA supports interaction between service providers and service users, implemented using JSON and the HTTP/2 protocol. Additionally, all 3GPP NFs communicate via Transport Layer Security (TLS) encrypted channels to ensure the security of the transport layer (Brown 2017).

Currently, NFs handling the CP in the 5G structure are all based on the SBA structure, and in the 5G-Advanced network structure based on 3GPP (3rd Generation Partnership Project) Release-18 specifications, some event processing of the UPF is also planned to be expanded into the SBA structure (Wanshi & Puneet 2023). Figure 2 illustrates the 5G SBA structure, and Table 1 summarizes the innovations of the 5G SBA structure.

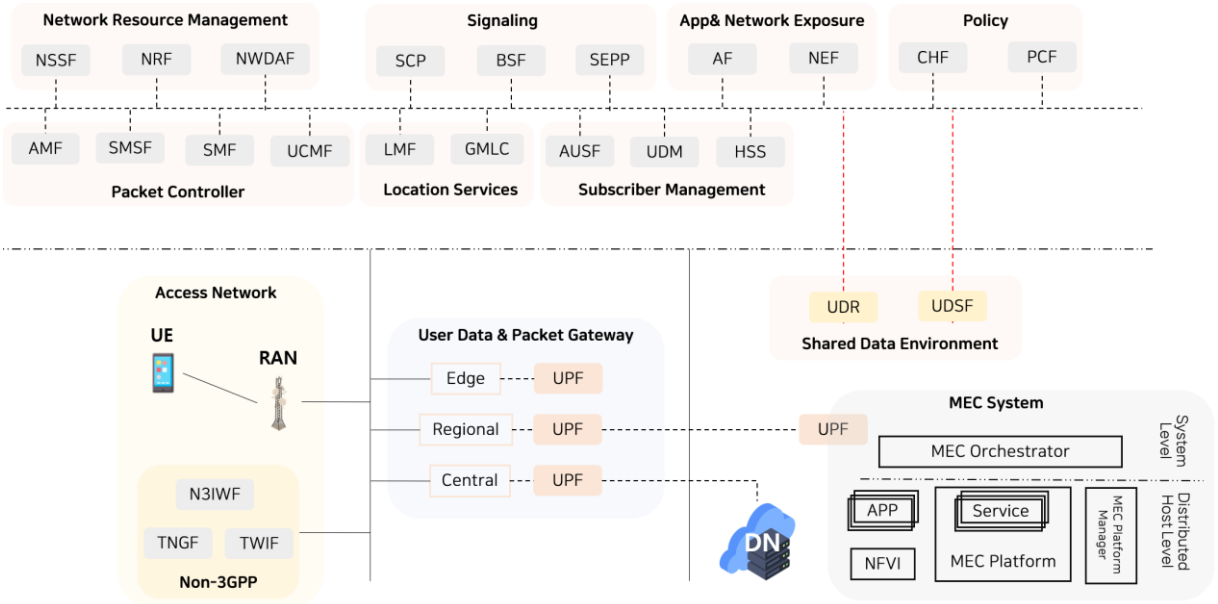


Figure 2: 5G Service Based Architecture Structure

Table 1: 5G SBA structure innovation

| Flexible Structural features | Common Core Structure |
|---|---|
| Functional Split between UP and CP | In addition to 3GPP access, non-3GPP access networks such as Wi-Fi can connect to the core NF with the same N1/N2 interface as the access network. |
| Functional Split of AMF (Access and Mobility Management Function) and SMF (Session Management Function) | |
| Modularization of NEF (Network Exposure Functions) and NFs facilitates deployment of 5G cores in a variety of optional infrastructure environments | An integrated authentication framework for authentication and access authorization is designed to provide integrated services for a variety of wired and wireless access technologies with a common core structure that is independent of access technology. |
| Integration with MEC (Multi Access Edge Computing) and combination with IT applications | |
| Network slicing can be implemented | |

### 3) Security Threats from False Base Station

The NG-RAN, the wireless access network of 5G, plays a crucial role in determining the performance and service quality of mobile communication networks. 5G is associated with various security threats, among which false base station attacks stand out as one of the most threatening attacks that have persisted from previous generations. These attacks exploit the characteristics of terminals attempting to connect to base stations receiving stronger signals, enabling malicious activities such as IMSI (International Mobile Subscriber Identity) theft, DoS (Denial of Service), and Device Bidding Down. Among these, IMSI theft attacks, which pose a risk of personal information theft, persist as a threat despite 5G encrypting the standard subscriber unique identifier, SUPI (Subscription Permanent Identifier), and sending it in the form of SUCI (Subscription Concealed Identifier). Recently, a new attack technique called SUCI-Catcher has been introduced, further highlighting the ongoing threats (Chlosta et al., 2021).

Additionally, in the 5G environment, attacks exist that compromise SON (Self-Organizing Networks), which support network self-configuration, optimization, and recovery. These attacks exploit the insufficient ability of UEs to distinguish between wireless signals transmitted by false base stations

and those from legitimate base stations, thereby disrupting SON functionality and providing malicious users with opportunities to manipulate UE location information. Furthermore, additional security threats associated with false base stations are outlined in Table 2 (3GPP 2023).

Table 2: Security threats related to false base stations

| Type of Attacks | Description |
|---|---|
| Passive attack | The false base station detects nearby radio signals and stores parameters and messages from nearby cells. |
| Active attack | An attack in which a false base station disguises itself as a normal base station and receives a handover mobility management procedure message from the user. |
| Downgrade attack | An attack that lowers the quality of use by downgrading the user's device to a previous generation network. |
| location-tracking attack | An attack that tracks the detailed location of a user within the range of a false base station based on the collected user information. |
| Injection attack | An attack in which an attacker inserts a random message into a user's message. |
| Information leakage | An attack that collects IMSI when a user connects to a false base station by leveraging the user's device's ability to select stronger signals. |
| Spoofing attack | Since UEs that follow the LTE standard believe in the authenticity of messages received before EPS-AKA, it is possible for attackers to spoof information sent to the user. |
| Relay attack | The attacker uses a false base station and a malicious UE to induce the victim UE to connect and relays the communication by transmitting the message sent by the victim UE to a distant normal base station through the malicious UE. |

# 3 Related Work

To address the threat of false base stations, various methods utilizing physical information have been proposed as primary efforts for identification. Ali et al. proposed a method for detecting false base stations using UE's RF (Radio Frequency) fingerprinting of legitimate base stations (Ali & Fischer 2019). Shin et al. proposed a whitelist detection approach utilizing the ANR (Automatic Neighbor Relation) procedure to verify the PCI (Physical Cell Identifier) values of legitimate base stations and detect PCI duplicates to prevent forgery of legitimate base station information (Shin et al., 2022). However, these studies lack experimental results in various scenarios, and their applicability in 5G systems is limited due to being simulated in previous-generation environments.

P.K. Nakarmi et al. were the first to detect false base stations by applying machine learning techniques to RSRP values included in the MR (Measurement Report) in a 5G environment (Nakarmi et al., 2022). However, this method is limited to NSA (Non-Stand Alone) 5G environments and cannot address threats that may arise in current SA (Stand Alone) 5G networks.

In response, Park introduced research on false base station detection applying machine learning and specification-based techniques in 2023 (Park 2023). However, previous studies have not reached the level of considering the feasibility of applying them in actual 5G network environments. Therefore, this paper implements real NFs in a UERANSIM environment similar to the 5G network environment and validates their feasibility.

# 4 False Base Station Detection Function

### 1) Overview

The NF known as the FDF (False base station Detection Function) operates using the open-source program UERANSIM as a 5G RAN simulator. The conventional UERANSIM supports the NAS layer for communication between RRC and UE and AMF, but lacks support for wireless environment simulation, leading to the inability of UE to generate MRs and inadequate support for handovers

(Docomo 2016). To address these issues, a testbed is constructed using UERANSIM with functional separation as DU (Distributed Unit)-CU (Central Unit) applied in the 5G wireless environment to measure wireless signals from multiple base stations and collect data. The system architecture of UERANSIM with functional separation is illustrated in Figure 3.

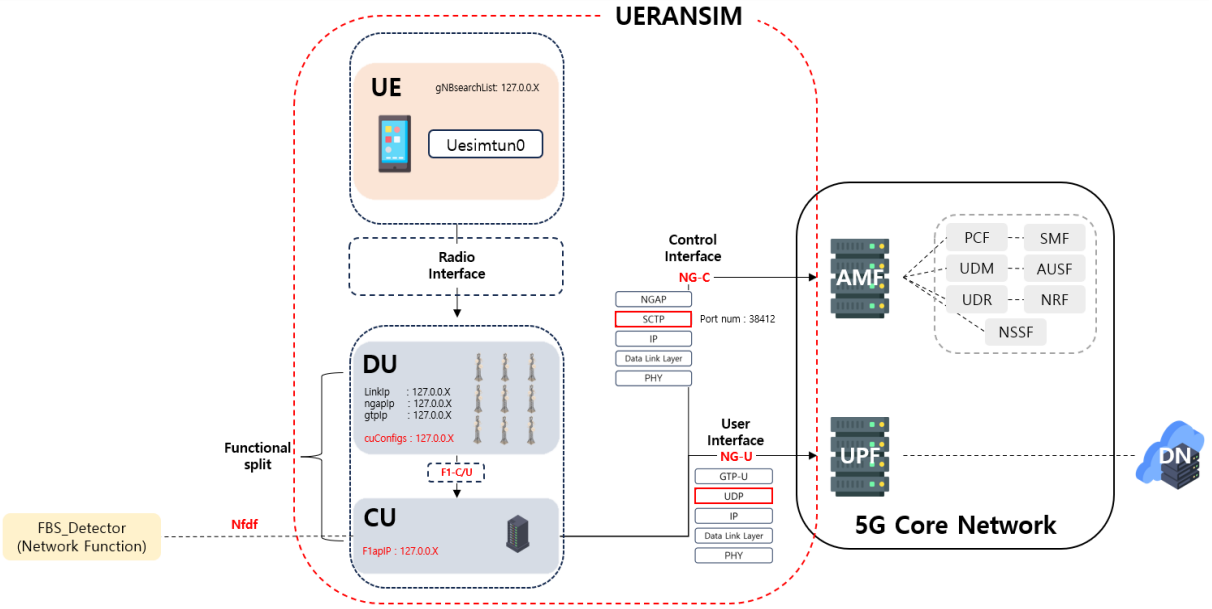


Figure 3: UERANSIM Architecture with Functional Split

Communication within the UERANSIM architecture revolves around the interface between NG-RAN and the 5G core, while the connection between DU and CU is established via the F1 interface. Within NG-RAN, two interfaces, NG-U and NG-C, handle the user plane and control plane, respectively. The NG-C utilizes SCTP (Stream Control Transmission Protocol) for reliable message-based communication, and its multi-homing capability enables the management of multiple IP addresses (3GPP 2023). This structure plays a crucial role in 5G communication, enabling efficient and stable communication.

### 2) System Model

The FDF follows the basic structure of the 5G core network, known as SBA. Such third-party NFs can seamlessly operate with other NFs in 5G networks or beyond, enabling organic integration. They exist within serving networks like CU, monitoring the data transmitted from DU to CU in real-time and detecting data generated from false base stations using machine learning and specification-based detection techniques. In this process, the FDF analyzes the MRs it receives in real-time to identify data from false base stations. Machine learning techniques utilize trained models to validate the data, while specification-based detection identifies abnormal behavior according to predefined behavioral rules. The results are stored in the FDF's database, and the system model and operational process are depicted in Figure 4 and Figure 5, respectively.

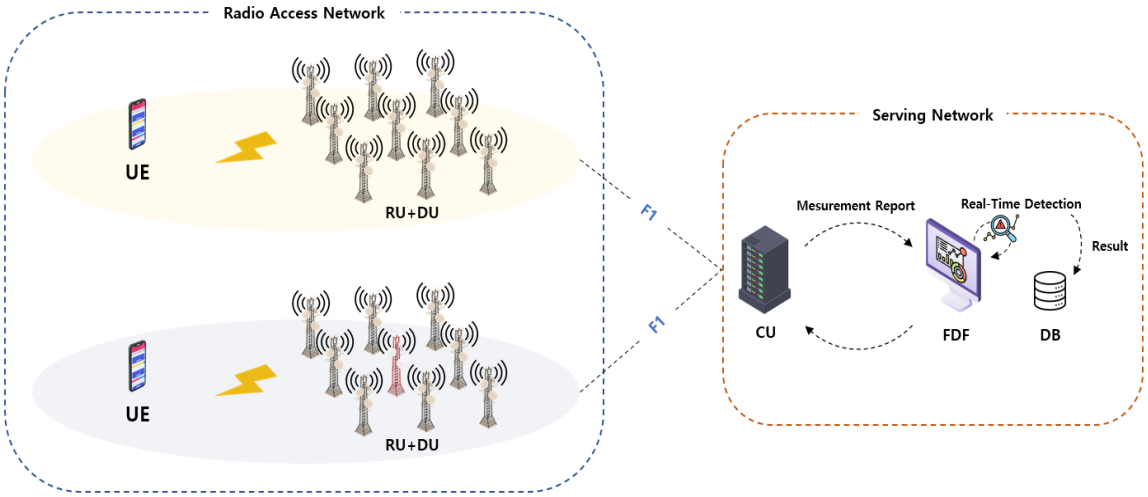


Figure 4: FDF System Mode

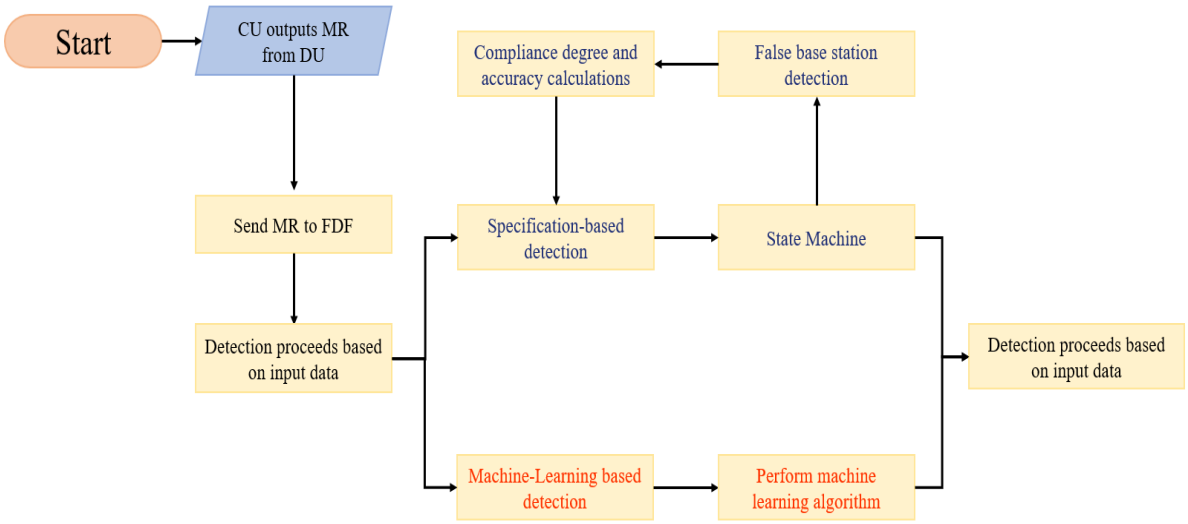


Figure 5: FDF Operation Flow Chart

### 3) Operation Process

The FDF processes real-time received data through interactions between DU, CU, and itself. This is illustrated in the sequence diagram shown in Figure 6, depicting the communication between DU and CU and the interaction with FDF. In this diagram, DU sends the ID of the currently connected UE to CU, which receives it and adds a Client_ID. Then, CU transmits messages related to data communication along with buffer, data length, and the stream using the SCTP protocol to CU. This process repeats iteratively through SCTP communication. Subsequently, CU generates MR, stores logs in its own database, and sends messages including MR with Client_ID and signal strength values, as well as RRC_Setup, Handover Procedure, UE Capability, etc., to FDF. Upon receiving this, FDF detects and processes abnormal messages through machine learning and specification-based detection, thus handling the real-time received data and detecting security threats.

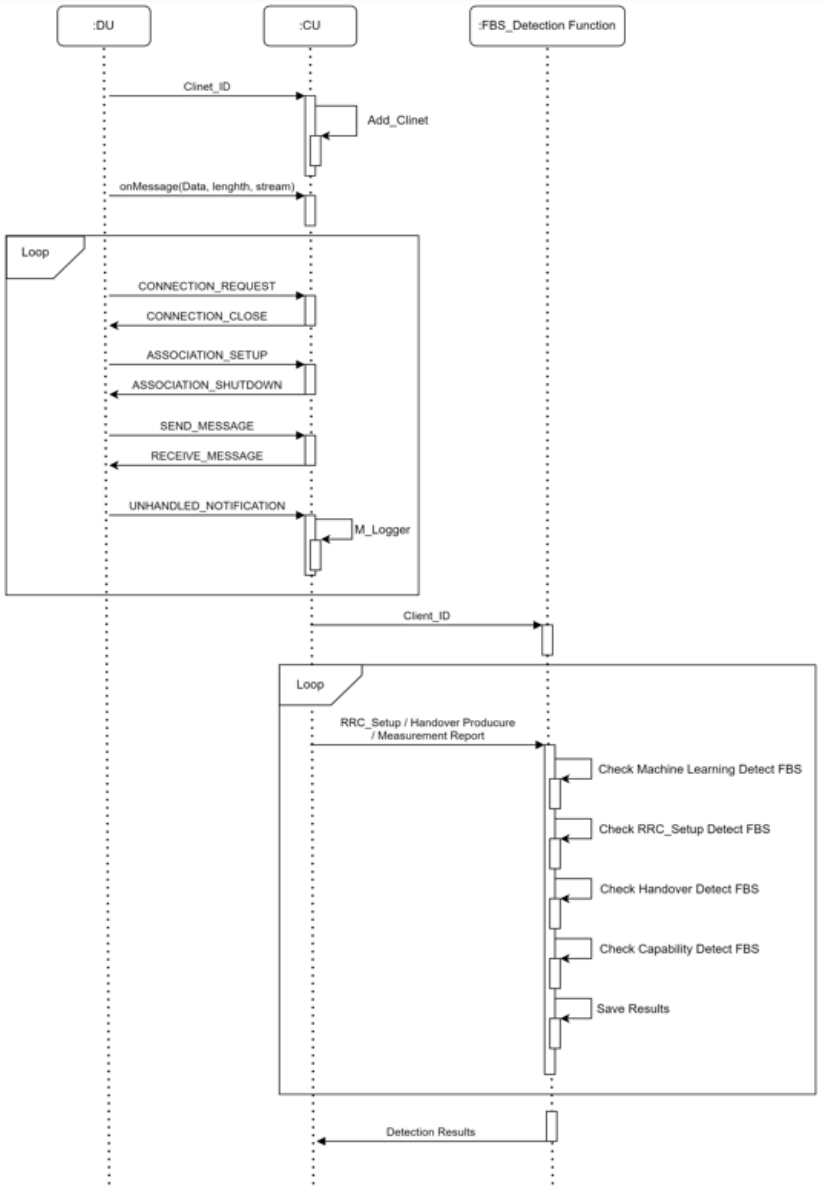


Figure 6: FDF Sequence diagram

Figure 7 illustrates the overall operational flow of FDF. It connects to a CU, collects real-time accumulated MR and other data, and mirrors received messages. Then, it preprocesses signal strength data accumulated in CU for detection through machine learning, preprocesses it into a form suitable for learning, and trains each model in advance. Subsequently, real-time input data is checked for abnormal patterns in MR transmitted by the terminal through the trained classification model. For detection through specification-based techniques, it analyzes data collected in real-time from CU, such as RRC_Setup, Handover, etc., using a state machine representing abnormal states, detects threats, and reports them as abnormal if suspicious behavior indicating false base stations is detected in the entire data at regular intervals. Through this process, FDF efficiently detects false base stations and mitigates security threats.

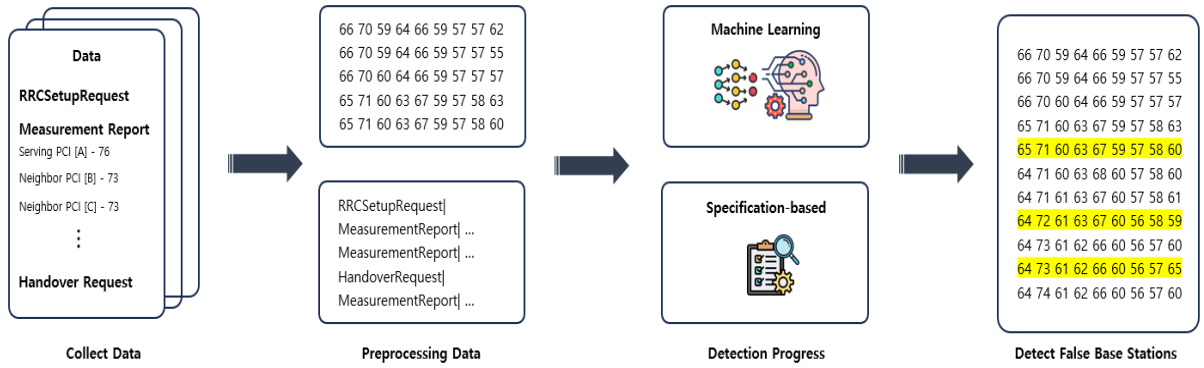


Figure 7: FDF operating procedure

#### 4) Feature of FDF

Based on the MR, RRC messages, Handover messages, and Capability messages received from CU, FDF performs machine learning and specification-based detection. It resides on the network along with CU and establishes organic communication with CU through the Nfdf service-based interface. Through this, FDF offers various services for CU, and the end-to-end interaction between NF service consumers within the NF service framework occurs in a request/response manner, as shown in Figure 8.

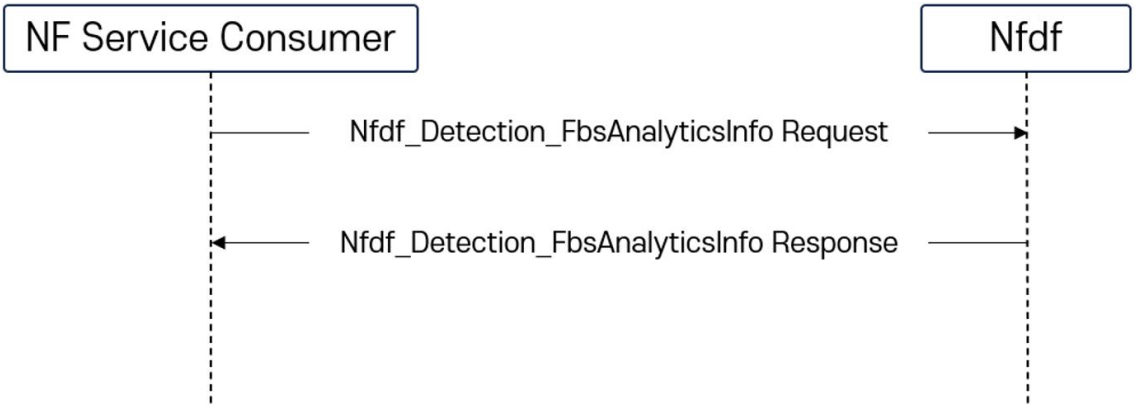


Figure 8: Nfdf Services “Response-Requests”

In this setup, NF service consumers can discover FDF and request false base station detection analysis services, thus receiving analyzed information. Communication in the request/response mechanism takes place between the two NFs in a 1:1 manner, with one-time responses being provided.

The designed Nfdf interface, depicted in Figure 9, includes the Nfdf_FbsDetection service, which provides information regarding false base station detection. For this purpose, it analyzes the data received from CU through MsgAnalyticsInfo and exchanges information in a request/response manner. The request includes information such as MachineLearningDetection, RrcSetupDetection, HandoverDetection, CapabilityDetection.

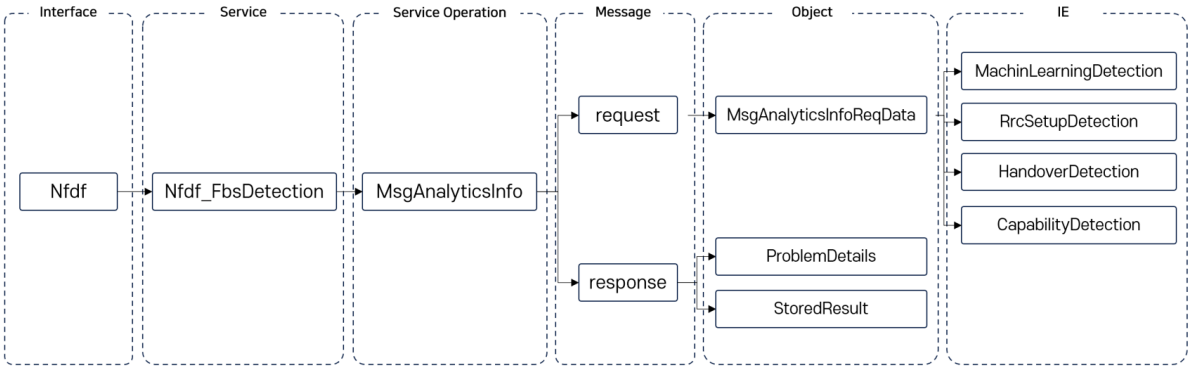


Figure 9: Description of the services provided by the Nfdf interface

# 5 Experiment and Implementation Results

### 1) Experiment Environment

The experiment detects false base station attacks using machine learning and specification-based techniques. For machine learning, six supervised learning algorithms (SVM, KNN, Decision Tree, Gaussian NB, Random Forest, XGBoost) are employed to measure detection accuracy. The training data for supervised learning is categorized into normal and abnormal data, based on a dataset generated using the improved UERANSIM. Normal data is labeled as 0, while abnormal data is labeled as 1. The experiments are conducted in Python using Scikit-Learn and XGBoost libraries. Information contained in the MR transmitted from UE to base stations includes PCI and RSRP values of serving and neighboring cells. This data serves as the training dataset for machine learning detection methods, consisting of 9 base station PCIs and their corresponding RSRP values. Table 3 illustrates an example of the data included in MR.

Table 3: Data Set Example

| PCI | 1(S) | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| RSRP | 67 | 60 | 54 | 73 | 61 | 54 | 60 | 57 | 54 |
| | 68 | 60 | 54 | 74 | 61 | 55 | 61 | 57 | 53 |
| | 66 | 60 | 54 | 75 | 62 | 55 | 60 | 58 | 52 |
| | 65 | 60 | 54 | 76 | 62 | 56 | 61 | 59 | 53 |
| | 66 | 60 | 54 | 77 | 62 | 54 | 62 | 58 | 52 |

Machine learning requires essential training data, and the type and format of data required vary depending on the learning model being utilized. Hence, specialized data collection and preprocessing must be carried out for each specific environment. In contrast, specification-based detection identifies false base stations based on predefined rules. This method relies on human-made behavioral rules to achieve accurate and reliable detection, providing faster and more lightweight benefits compared to machine learning. Figure 10 applies a security context to system requirements from the perspective of false base station detection agents based on 3GPP standard specifications (Park 2023; 3GPP 2023).

Specification-based detection offers the advantage of effectively detecting new types of zero-day attacks and predefined attack patterns, even when false base stations exhibit patterns similar to normal

base stations. Thus, FDF can swiftly and effectively detect false base stations by collecting and preprocessing diverse data tailored to the environment.

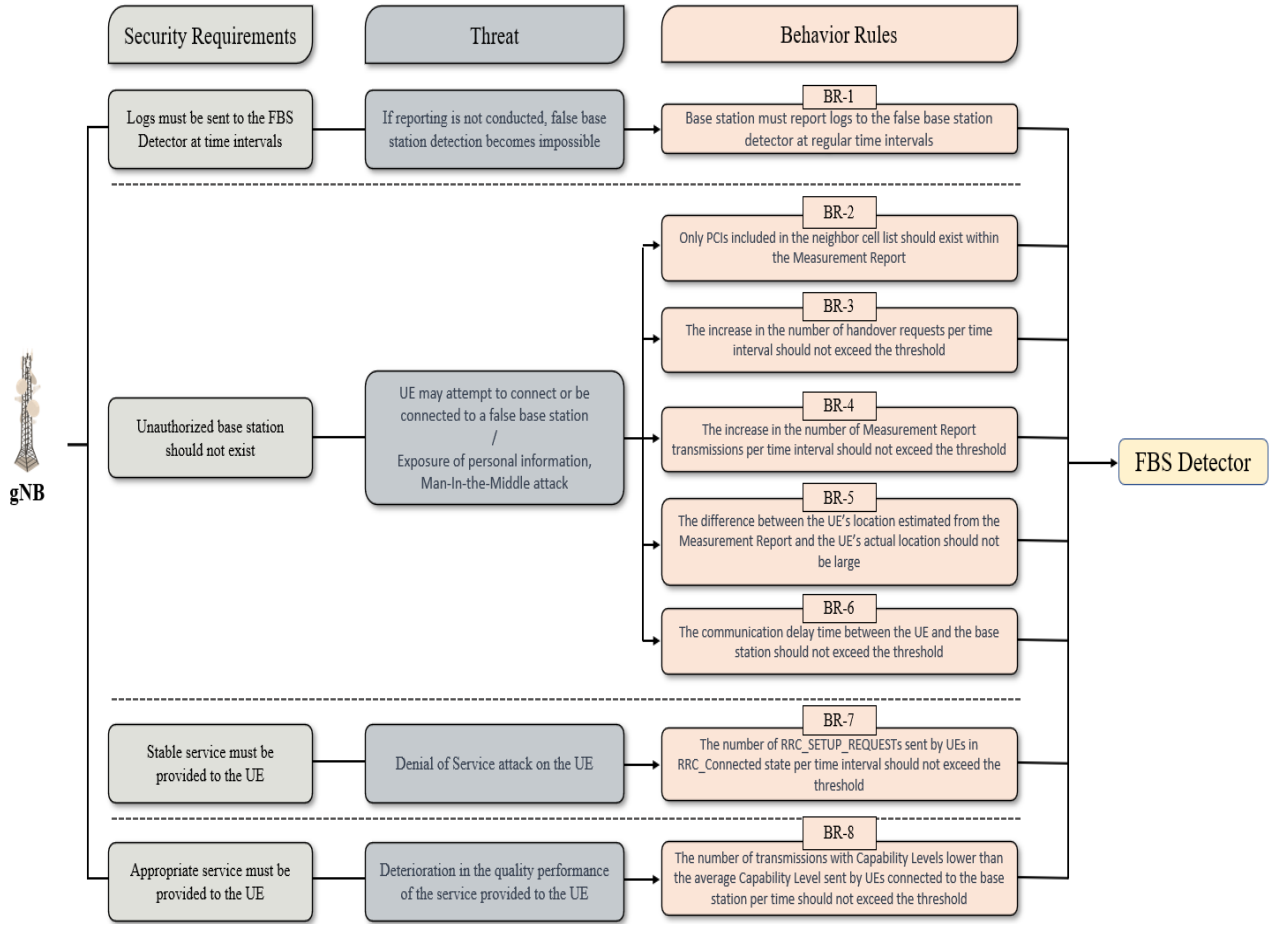


Figure 10: Workflow for deriving behavior rules for false base station detection

### 2) Implementation Results

The implementation results of real-time machine learning detection through FDF are shown in Figure 11. Using the pre-trained machine learning model, detection is performed based on the received data's signal strength values from the MRs transmitted in real-time by the CU. The output results include the predicted values of normal or abnormal detection and the probability that the predicted result is true.

```
Received from CU : MeasurementReport|1|5|76|8|8|62|9|58|7|60|6|61|4|66|3|58|2|63|1|61
[SVM : normal 99%] [KNN : normal 100%] [DT : normal 100%] [RF : normal 98%] [XGB : normal 99%] [NB : normal 50%]
Received from CU : MeasurementReport|1|5|76|8|8|62|9|58|7|60|6|61|4|66|3|58|2|63|1|61
[SVM : normal 99%] [KNN : normal 100%] [DT : normal 100%] [RF : normal 98%] [XGB : normal 99%] [NB : normal 50%]
Received from CU : MeasurementReport|1|5|78|8|8|62|9|58|7|60|6|61|4|65|3|58|2|63|1|61
[SVM : normal 99%] [KNN : normal 100%] [DT : normal 100%] [RF : normal 97%] [XGB : normal 99%] [NB : normal 50%]
```

Figure 11: Workflow for deriving behavior rules for false base station detection

To detect false base station-related attack types as suggested by 3GPP, in the case of specification-based detection, false base station detection state machine is employed every minute, as shown in Figure 12, to detect abnormal behavior indicators ranging from 1 to 8. After detection is conducted for each abnormal behavior indicator, the results are outputted. In the case of specification-based false base

station detection, detection of abnormal behaviors ranging from 1 to 8 is carried out through a false base station detection state machine at intervals of 1 minute.

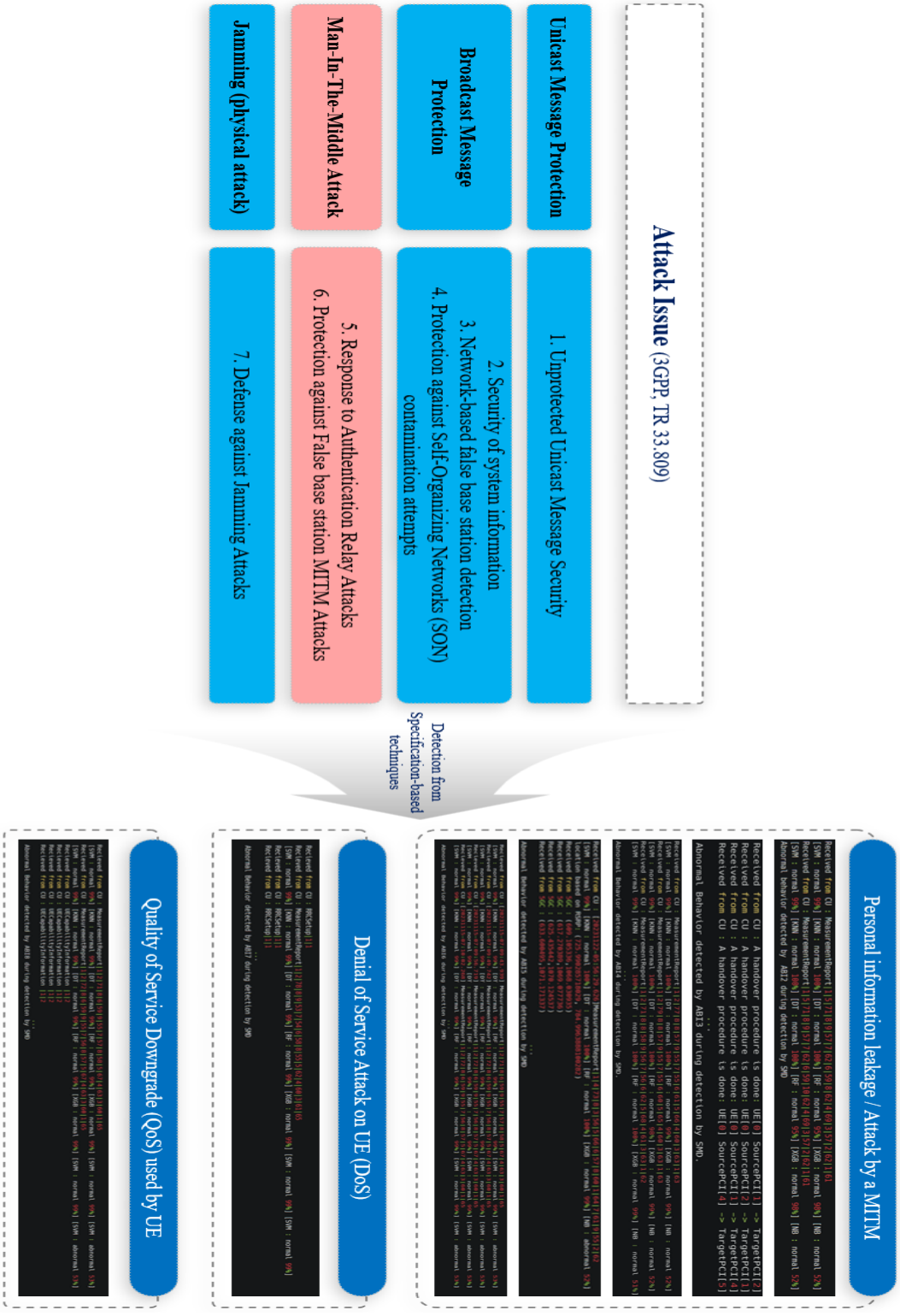


Figure 12: Detection results of attack types related to false base stations

After detection for 1 minute, if the system detects normal behavior, the result is as shown in Figure 13.

```
Received from CU : MeasurementReport|1|2|81|8|8|56|9|55|7|55|6|60|5|65|4|60|3|63|1|63
[SVM : normal 99%] [KNN : normal 100%] [DT : normal 100%] [RF : normal 98%] [XGB : normal 99%] [NB : normal 54%]
Received from CU : MeasurementReport|1|2|80|8|8|56|9|55|7|55|6|60|5|65|4|61|3|62|1|64
[SVM : normal 99%] [KNN : normal 100%] [DT : normal 100%] [RF : normal 98%] [XGB : normal 99%] [NB : normal 54%]
Received from CU : MeasurementReport|1|2|80|8|8|56|9|55|7|55|6|60|5|65|4|61|3|62|1|64
[SVM : normal 99%] [KNN : normal 100%] [DT : normal 100%] [RF : normal 98%] [XGB : normal 99%] [NB : normal 54%]
The detection result through SMDFbs is Normal Behavior.
```

Figure 13: FDF Implementation - Results through Specification-Based Detection (Normal)

If no report is received from the FDF at 1-minute intervals, it is considered abnormal behavior, and the detection result is outputted as abnormal behavior as shown in Figure 14.

```
Received from CU : RRCSetup|1|1
Received from CU : UECapabilityEnquiry|1|2
Received from CU : A handover procedure is done: UE[0] SourcePCI[1] -> TargetPCI[2]
Received from CU : A handover procedure is done: UE[0] SourcePCI[2] -> TargetPCI[1]
Received from CU : A handover procedure is done: UE[0] SourcePCI[1] -> TargetPCI[4]
Abnormal Behavior detected by ABI1 during detection by SMD.
```

Figure 14: FDF Implementation - Results through Specification-Based Detection (Abnormal - ABI1)

The FDF detects false base stations by analyzing the MRs transmitted from the base stations. In this process, the base station receives MRs from the terminals it serves, which should only contain PCIs corresponding to the neighbor cell list of the serving base station. If an MR contains PCIs that are not in the neighbor cell list of the serving base station, it is considered abnormal and detected by the FDF as shown in Figure 15.

```
Received from CU : MeasurementReport|1|5|71|8|9|57|7|62|6|59|8|62|4|69|3|57|2|62|1|61
[SVM : normal 99%] [KNN : normal 100%] [DT : normal 100%] [RF : normal 95%] [XGB : normal 98%] [NB : normal 52%]
Received from CU : MeasurementReport|1|5|71|8|9|57|7|62|6|59|10|62|4|69|3|57|2|62|1|61
[SVM : normal 99%] [KNN : normal 100%] [DT : normal 100%] [RF : normal 95%] [XGB : normal 98%] [NB : normal 52%]
Abnormal behavior detected by  ABI2 during detection by SMD
```

Figure 15: FDF Implementation - Results through Specification-Based Detection (Abnormal – ABI2)

The FDF detects the presence of false base stations by monitoring the process of handover of mobile terminals to base stations that send stronger signals according to MR trigger conditions while in motion. In this scenario, if a terminal sends a handover request to a false base station, the handover request count increases. The increase in such request counts is considered abnormal in the presence of false base stations and is detected by the FDF, as illustrated in Figure 16.

```
Received from CU : A handover procedure is done: UE[0] SourcePCI[1] -> TargetPCI[2]
Received from CU : A handover procedure is done: UE[0] SourcePCI[2] -> TargetPCI[1]
Received from CU : A handover procedure is done: UE[0] SourcePCI[1] -> TargetPCI[4]
Received from CU : A handover procedure is done: UE[0] SourcePCI[4] -> TargetPCI[5]
                                ...
Abnormal Behavior detected by ABI3 during detection by SMD.
```

Figure 16: FDF Implementation - Results through Specification-Based Detection (Abnormal – ABI3)

If the number of MR transmissions in the presence of false base stations exceeds a predetermined threshold per unit time, it can be considered abnormal and detected as such, as illustrated in Figure 17.


Figure 17: FDF Implementation - Results through Specification-Based Detection (Abnormal – ABI4)

In the process of estimating the distance between base stations and terminals using the triangulation technique based on the RSRP values included in the MRs, it is possible to calculate the distances between each base station and terminal. This allows for the estimation of the terminal's position, and by using the estimated position along with the signal strength values of the serving cell, the distance to the serving cell can be calculated, thereby determining the coordinates of the two points. Consequently, by calculating the difference between the two position coordinates, the difference between the RSRP value and the estimated position can be obtained. If this difference exceeds a predefined threshold, it is considered abnormal and detected by the FDF, as illustrated in Figure 18.

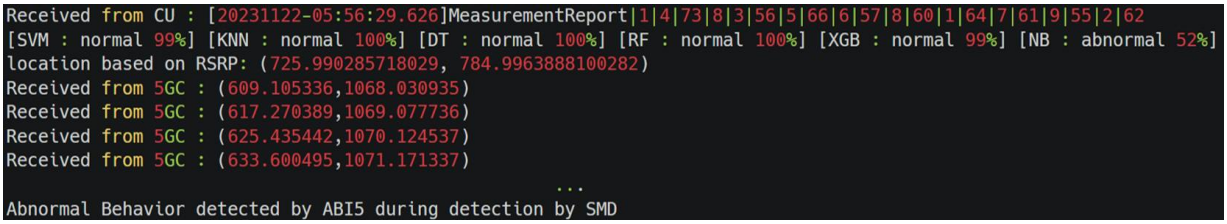


Figure 18: FDF Implementation - Results through Specification-Based Detection (Abnormal – ABI5)

If an attacker is positioned in between and acting as a relay, it results in increased communication latency. Therefore, if this communication latency exceeds a threshold, as depicted in Figure 19, it is detected as abnormal.

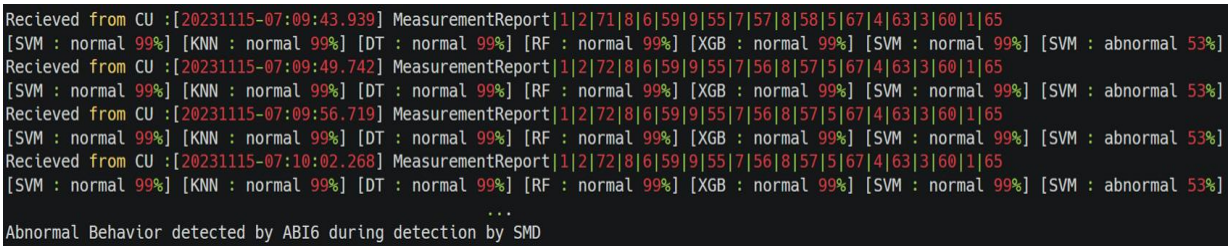


Figure 19: FDF Implementation - Results through Specification-Based Detection (Abnormal – ABI6)

After the terminal is powered on, an RRC_setup_request message is sent to establish a connection with the base station. However, if an attacker exists, they can intercept this message and send it to the base station instead. The base station, upon receiving this message, may terminate the connection with the already connected legitimate terminal, leading to a denial-of-service attack. If such an attack is suspected, as it can affect multiple affected terminals, exceeding the threshold of RRC_setup_request message transmissions is considered abnormal and detected by the FDF, as shown in Figure 20.

```
Recieved from CU : RRCSetup|1|1
Recieved from CU : MeasurementReport|1|2|78|8|9|53|7|54|6|58|8|55|5|62|4|60|3|61|65
[SVM : normal 99%] [KNN : normal 99%] [DT : normal 99%] [RF : normal 99%] [XGB : normal 99%] [SVM : normal 99%] [SVM : normal 99%]
Recieved from CU : RRCSetup|1|1
Recieved from CU : RRCSetup|1|1
                              ...
Abnormal Behavior detected by ABI7 during detection by SMD
```

Figure 20: FDF Implementation - Results through Specification-Based Detection (Abnormal – ABI7)

Detecting abnormal behavior related to UE Capability messages is crucial. UE Capability Information messages can be transmitted before AS (Access Stratum) security is activated. However, if these messages are tampered with through a man-in-the-middle attack, it may degrade the quality of service experienced by users. Therefore, if the number of transmissions of Capability messages with a level lower than the average Capability Level sent by the UE exceeds a threshold, it is considered abnormal and detected by the FDF, as depicted in Figure 21.

```
Recieved from CU : MeasurementReport|1|2|71|8|6|59|9|55|7|57|8|58|5|67|4|63|3|60|1|65
[SVM : normal 99%] [KNN : normal 99%] [DT : normal 99%] [RF : normal 99%] [XGB : normal 99%] [SVM : normal 99%] [SVM : abnormal 53%]
Recieved from CU : MeasurementReport|1|2|72|8|6|59|9|55|7|56|8|57|5|67|4|63|3|60|1|65
[SVM : normal 99%] [KNN : normal 99%] [DT : normal 99%] [RF : normal 99%] [XGB : normal 99%] [SVM : normal 99%] [SVM : abnormal 53%]
Recieved from CU : UECapabilityInformation |1|2
Recieved from CU : UECapabilityInformation |1|2
Recieved from CU : UECapabilityInformation |1|2
Recieved from CU : UECapabilityInformation |1|2
                                        ...
Abnormal Behavior detected by ABI8 during detection by SMD
```

Figure 21: FDF Implementation - Results through Specification-Based Detection (Abnormal – ABI8)

### 3) Implementation Results

In this section, we compare and evaluate the performance of machine learning techniques and specification-based methods used to detect false base stations. As depicted in Figure 22, the false base station detection method based on specification outperforms other machine learning algorithms in terms of accuracy. Furthermore, as shown in Figure 23, the efficiency aspect, including CPU usage, memory usage, and network latency, also demonstrates the superiority of specification-based methods. Additionally, we verify that the specification-based method effectively detects complex attack types outlined in the 3GPP technical documents addressing critical security issues in 5G environments, as illustrated in Figure 12. This underscores the significance of employing specification-based techniques for false base station detection, expecting them to play a crucial role in mitigating threats from false base stations in future-generation network environments.

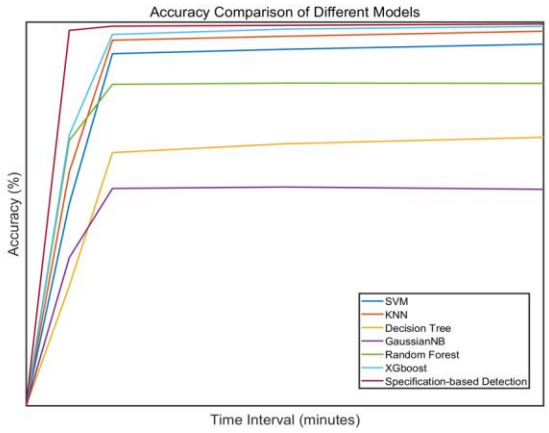


Figure 22: Comparison of detection accuracy performance by hour

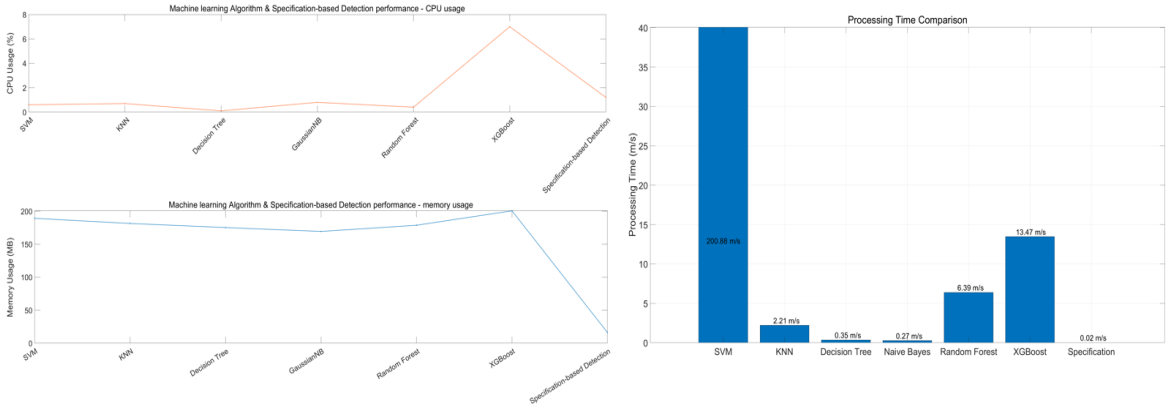


Figure 23: Comparison of Machine Learning and Specification-Based false base station memory usage & processing time

# 6 Conclusion

With the advancement of mobile communication networks, new types of threats continue to emerge, and solutions to address them are being continuously researched. One of the prominent threats in 5G networks is the proliferation of false base station attacks, where malicious actors disguise them selves as legitimate base stations to collect user information or conduct denial-of-service attacks. In response to these false base station threats, this study implemented FDF, a false base station detection system in the form of an NF. FDF was implemented based on the SBI following the SBA for seamless communication with the CU. The feasibility of applying FDF in real 5G environments was validated through simulations using the 5G RAN test platform UERANSIM, which incorporates functional separation and handover capabilities.

FDF utilizes both machine learning and specification-based detection techniques to analyze incoming MRs in real-time and detect abnormal behavior. Experimental results comparing the accuracy of the two implemented techniques revealed that while the XGBoost machine learning algorithm exhibited the highest accuracy at 96.75%, the accuracy of the specification-based false base station detection technique was superior at 99.6%. Efficiency measurements indicated that the CPU usage was on average 1.6% for machine learning and 1.2% for specification-based detection, while memory usage was 182.4MB for machine learning and 16.12MB for specification-based detection. Overall, specification-based false base station detection demonstrated superior performance. Additionally, when comparing the processing times of machine learning and specification-based techniques within FDF, it was evident that specification-based detection achieved significantly lower processing times.

While specification-based detection proved superior, combating highly sophisticated, unknown attacks beyond specifications necessitates the combined application of machine learning and deep learning techniques for detection.

Traditional intrusion detection systems like firewalls operate independently and are not seamlessly integrated with 5G networks. Therefore, implementing NFs like FDF and invoking them through interfaces enable organic integration with serving networks such as CU, facilitating real-time detection by receiving CU data, thus offering speed advantages.

In conclusion, while specification-based detection techniques excel, to effectively counter advanced, unknown attacks beyond specifications, it is desirable to apply a combination of machine learning and deep learning techniques for detection.

## References

[1] 3GPP. F1 interface – f1 signalling transport, 2023.
[2] 3GPP. Service requirements for the 5g system, 2023.
[3] 3GPP. Study on 5g security enhancements against false base stations, 2023.
[4] Abdullah, D. (2020). A Linear Antenna Array for Wireless Communications. *National Journal of Antennas and Propagation (NJAP), 2*(1), 19-24.
[5] Ali, A., & Fischer, G. (2019). Enabling fake base station detection through sample-based higher order noise statistics. *In 42nd International Conference on Telecommunications and Signal Processing (TSP)*, 695-700.
[6] Brown, G. (2017). Service-based architecture for 5g core networks. *Huawei White Paper, 1*.
[7] Chlosta, M., Rupprecht, D., Pöpper, C., & Holz, T. (2021). 5G SUCI-Catchers: Still catching them all?. *In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 359-364.
[8] Docomo, N.T.T. (2016). *5G Channel Model for bands up to100 GHz*. Technical report, 1-56.
[9] Fruhlinger, J. How different definition of 5g core technologies and differences from 4g, 2023.
[10] Khan, M.S., Farzaneh, B., Shahriar, N., Saha, N., & Boutaba, R. (2022). Slice Secure: Impact and Detection of DoS/DDoS Attacks on 5G Network Slices. *In IEEE Future Networks World Forum (FNWF)*, 639-642.
[11] Krisztian, P., Pradeep, P., Sridhar, V.K.V., & Nirlesh, K. (2024). Network slice specific authentication and authorization (nssaa) 5g new radio (nr) procedures. US Patent 11,877,234.
[12] Manipriya, S., Mala, C., & Mathew, S. (2020). A collaborative framework for traffic information in vehicular adhoc network applications. *Journal of Internet Services and Information Security (JISIS), 10*(3), 93-109.
[13] Nakarmi, P.K., Sternby, J., & Ullah, I. (2022). Applying machine learning on rsrp-based features for false base station detection. *In Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1-7.
[14] Panek, G., Fajjari, I., Tarasiuk, H., Bousselmi, A., & Toukabri, T. (2022). Application relocation in an edge-enabled 5G system: Use cases, architecture, and challenges. *IEEE Communications Magazine, 60*(8), 28-34.
[15] Park, H.Y. (2023). *Research on False Base Station Detection Techniques for Secure Radio Access Network in Next Generation Mobile Communication Environments*. PhD thesis, Department of Information Security at Soonchunhyang University.
[16] Rudolph, H.C., Kunz, A., Iacono, L.L., & Nguyen, H.V. (2019). Security challenges of the 3gpp 5g service based architecture. *IEEE Communications Standards Magazine*, *3*(1), 60-65.
[17] Shin, J., Shin, Y., & Park, J.G. (2022). Network Detection of Fake Base Station using Automatic Neighbour Relation in Self-Organizing Networks. *In 13th International Conference on Information and Communication Technology Convergence (ICTC)*, 968-970.
[18] Shin, M.K. (2019). 5g network/system (5gs) standard technology trends.
[19] Shin, M.K. (2022). 5g to 6g: Architecture evolution.
[20] Wanshi, C., & Puneet, J. (2023). 3gpp release 18 overview: A world of 5g-advanced.
[21] Yan, Z.W. (2010). N-NEMO: a comprehensive network mobility solution in proxy mobile IPv6 network. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications (JOWUA), 1*(2/3), 52-70.

## Authors Biography

**Daehyeon Son** graduated from Soon Chun Hyang University with a bachelor's degree in information Security and earned a master's degree in financial information security at Kookmin University. His research interests are IoT, Protocol analysis and research on false base station detection in 5G/6G security.

**Youngshin Park** graduated in Information Security, Cryptology, and Mathematics from Kookmin University, South Korea. Her research interests are 5G/6G security based on machine learning.

**Bonam Kim** is a research professor, Department of financial information security, Kookmin University, South Korea. She received Ph.D. degree in the department of Computer Science and Software Engineering from Auburn University, USA in 2006. Her main research interests include wireless sensor networks, IoT security, and 5G/6G security.

**Ilsun You** received the MS and PhD degrees from Dankook University, Seoul, Korea, in 1997 and 2002, respectively. He received the second PhD degree from Kyushu University, Japan, in 2012. Now, he is a full professor at Department of Information Security, Cryptology, and Mathematics, Kookmin University. His research interests include 5/6G security, security for wireless networks & mobile internet, IoT/CPS security, and security protocol design/formal verification. He is included in Stanford-Elsevier's list of the world's top 2% scientists from 2020 to present while achieving 50 H-index based on the google scholar. He is a Fellow of the IET and a Senior member of the IEEE.