5G SECURITY TEST BED™

Securing 5G:

5G Security Test Bed Assesses 5G Network Resiliency Against False Base Station Attacks

Q3 2025 Technical Report

Table of Contents

Introduction

This document presents test results based on the false base station (FBS) use case derived from the 5G Security Test Bed (5G STB) primary use cases focusing on network security. An unauthorized user can utilize a false base station to attempt to perform Denial-of-Service attacks, circumvent 5G authentication procedures, and force a legitimate user to lose network connectivity.

The objective of this FBS testing was to perform a real-world assessment of such possibilities in existing 5G networks. By simulating these threats in a controlled lab environment, the test team observed that 5G networks and devices are resilient to FBS attacks. This testing helped ensure that authentication, encryption, and network integrity mechanisms such as 5G's mutual authentication and Non-Access Stratum (NAS) security enforcement are functioning effectively. To conduct this assessment, the 5G STB Technical Advisory Committee (TAC) developed a set of false base station test cases grouped within four high-level categories:

- User Equipment Radio Resource Control (RRC) Connection Scenarios
- Invalid Authentication Handshake Scenarios
- Denial-of-Service (DoS) Attacks
- False Public Warning System (PWS) Messages

Test Cases

The 5G Security Test Bed established and executed ten test cases to assess user equipment (UE) behaviors in response to false base stations impersonating legitimate 5G networks. Each test case progressively addressed a range of potential scenarios to assess whether the false base station is able to capture UE identifiers, or inhibit the UE from successfully connecting to its valid home network during and after the attack. The test cases were executed as follows:

Table 1: False Base Station Test Cases

Test Case ID	Test Case Title	Description
TC 1	Establishing UE RRC Connection	This test case is designed to observe a successful RRC connection between the UE and false base station when the UE is not attached to its home network. The UE initiates NAS registration procedures, but subsequent registration and authentication procedures fail between the UE and false base station. The goal of this test is to ensure the 5G UE does not fully connect and register to the false base station.
TC 2	Establishing UE RRC Connection After Forced Disconnect from Home Radio Base Station	This test case is designed to observe a successful RRC connection between the UE and a high-powered false base station when the UE is attached to its home network. The UE initiates NAS registration procedures, but subsequent registration and authentication procedures fail between the UE and the FBS. The goal of this test is to confirm that the UE will be released without authenticating, and the false base station will collect any identifiers (GUTI) that the UE sends to build the RRC connection.

Table 1: False Base Station Test Cases (continued)

Test Case ID	Test Case Title	Description
TC 3	Attempting Registration After Omitting Authentication Handshake	This test case is designed to observe false base station attempts to force the UE to accept NAS registration without performing the authentication procedure. The FBS replies to the UE's NAS registration request with a "Registration Accept" message without sending an authentication request. The goal of this test is to confirm that the UE will respond by rejecting the authentication request and disconnecting from the false base station.
TC 4	Attempting Authentication Handshake Using Random Identifiers	This test case is designed to observe false base station attempts to authenticate the UE using fabricated authentication credentials. After establishing an RRC connection with the UE, the false base station attempts NAS authentication with the UE using random authentication vectors. The goal of this test is to confirm that the UE will respond by rejecting the authentication request and disconnecting from the false base station.
TC 5	Attempting Authentication Handshake Using Replayed Credentials	This test case is designed to observe false base station attempts to authenticate the UE using replayed authentication credentials. After establishing an RRC connection with the UE, the false base station attempts NAS authentication with the UE using authentication credentials captured from a previous authentication between the UE and the home gNB. The goal of this test is to confirm that the UE will respond by rejecting the authentication request and disconnecting from the false base station.
TC 6	Conducting DoS Attack Using "5GS Services Not Allowed" Message	This test case is designed to observe false base station attempts to conduct a Denial-of-Service (DoS) attack against the UE by using a "5GS Services Not Allowed" registration reject message. The goal of this test is to confirm that the UE will respond by ignoring the RRMU reject message and reconnecting to its own home radio base station.
TC 7	Conducting DoS Attack Using "Cell Barred" Message	This test case is designed to observe false base station attempts to conduct a DoS attack against the UE by cloning the UE's home radio base station and using the cell-identifier's "Cell Barred" field to prevent the UE from connecting with its home network. The goal of this test is to confirm that the UE will store the value and not connect even when the false base station is no longer transmitting on a stronger signal than the home radio base station.
TC 8	Conducting DoS Attack Using "PLMN Not Allowed" Message	This test case is designed to observe false base station attempts to conduct a DoS attack against the UE by using a "PLMN Not Allowed" registration reject message. The goal of this test is to confirm that the UE will respond by ignoring the false base station's message and reconnecting to its own home radio base station.
TC 9	Attempting Authentication with Spoofed Public Warning System Message	This test case is designed to observe the UE's behavior when the false base station sends a spoofed Public Warning System (PWS) message with the Commercial Mobile Alert System (CMAS). The primary goal of this test is to confirm that the UE will ignore the spoofed PWS messages and maintain its connection with its home radio base station.
TC 10	Attempting Authentication with Spoofed Public Warning System Message Followed by "PLMN Not Allowed" Message	This test case is designed to observe the UE's behavior when the false base station first sends a spoofed Public Warning System message, then rejects the UE's NAS registration by using a "PLMN Not Allowed" message. The goal of this test is to confirm that the UE will ignore the messages and maintain its connection with its home radio base station.

Test Setup

The configuration used for these tests was comprised of a false base station radio access network (RAN), 5G Core network, and Ericsson RAN equipment hosted at the Virginia Tech Applied Research Corporation (VT-ARC), as well as a 5G Standalone (SA) Core that provided 5G functionality hosted at the MITRE Corporation.

The 5G Security Test Bed lab components utilized for false base station testing are listed in Table 2. Tests were run with band N71 on the Ericsson RAN and on the false base station with a 5G test device (user equipment, or UE).

Table 2: Test Bed Components

Test Bed Component	Type	Hardware/Software	Location
Home Network	Radio Unit	Ericsson 4478 N71 (600 MHz)	VT-ARC
	gNodeB	Ericsson Baseband Unit 6648	VT-ARC
	Switch	Mikrotik CCRA2216	VT-ARC
	5G SA Core	Ericsson	MITRE
	Router	Ericsson 6672	VT-ARC and MITRE
FBS	Radio Unit	Universal Software Radio Peripheral (USRP) X310	VT-ARC
	gNodeB	srsRAN	VT-ARC
	5G SA Core	Open5GS	VT-ARC
Device	5G UE	5G Test Device	VT-ARC
Tools	5G UE Trace	Qualcomm eXtensible Diagnostic Monitor (QXDM)	VT-ARC
	Home Network and FBS RAN-Core Trace	Wireshark	VT-ARC

As shown in the detailed test configuration diagram in Figure 1 below, the false base station equipment (i.e., USRP and FBS NUC (Next Unit of Computing)) was inside VT-ARC's Faraday cage along with the test UE. The FBS and UE were operated remotely along with the Ericsson RAN to conduct testing and collect logs. Wireshark packets were captured at the FBS NUC and Mikrotik switch, whereas UE traces were captured at the test device laptop.

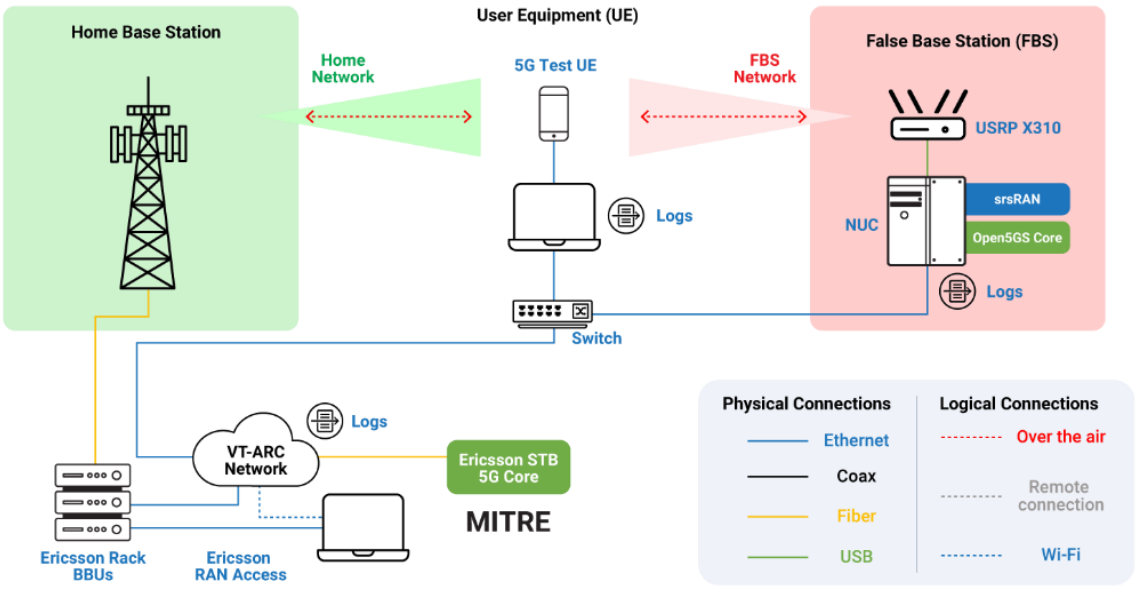


Figure 1: 5G Security Test Bed False Base Station Test Configuration

Test Process

As a prerequisite prior to executing each of the tests, the test team configured the false base station laptop with open-source software and the Wireshark packet analyzer tool. The functionality of these software components was verified and tested, confirming the software components were operational. The 5G test UE used two different Subscriber Identity Module (SIM) cards provisioned to work with the Ericsson 5G Core network, with the goal of testing SIMs with and without authentication protocols: 1) a 5G Authentication and Key Agreement (5G AKA) algorithm-encoded SIM card hereby described as Profile B and 2) a 5G Null encryption SIM card hereby described as Profile N. It is important to note that, although some tests are done with Null encryption, the Null scheme is never used on U.S. networks except during emergency services (e.g. when the user calls 911), as per CSRIC recommendations.[i]

As illustrated in Figure 2, each SIM card was used separately in the UE for every test case to determine the differences in UE and false base station behavior due to different SIM encryption. The combination of the USRP X310, FBS software components, and 5G UE worked as an end-to-end 5G Standalone false base station configuration. Apart from the false base station, the test team ensured the 5G home network consisting of the Ericsson RAN and Core network were functional to perform the tests.

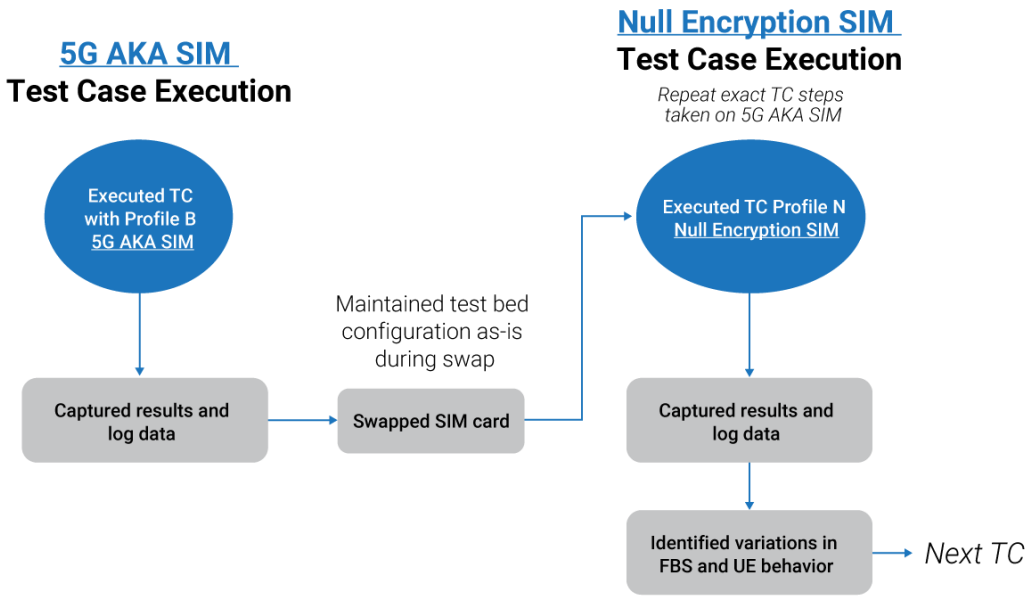


Figure 2: Test Process with 5G AKA and Null Encryption SIMs

The sections below list each false base station test case with its description, objectives, success criteria, expected results, and detailed test results. It is important to note that for each conducted test case, its associated section provides test results collected while running the test separately for each SIM card: first with the aforementioned 5G AKA SIM and then again with the Null encryption SIM.

Some test cases are further classified into two sub-categories: (a) where the test International Mobile Subscriber Identity (IMSI) is not registered in the FBS Core, with the objective to harvest user information for future targeted attacks or for Denial-of-Service purposes, and (b) where the test IMSI is registered in the FBS Core, with the objective to capture more information in targeted attacks. In the real world, the adversary is expected to register their target IMSI in their FBS Core.

Test Case 1 – Establishing UE RRC Connection

Test Case ID: TC-FBS-1

Test Case Name: Establishing UE RRC Connection

Description:
This test case is designed to observe a successful RRC connection between the UE and false base station when the UE is not attached to the home network. The UE initiates NAS registration procedures, but subsequent registration and authentication procedures fail between the UE and the FBS. The primary goal is to ensure the 5G UE does not fully connect and register to the false base station.

Objectives:

- Demonstrate that the UE initiates an RRC connection to the FBS.
- Demonstrate that registration is rejected between the UE and the FBS for the Profile B 5G AKA SIM and release the RRC connection with the FBS.
- Demonstrate that authentication is rejected between the UE and the FBS for Profile N Null encryption SIM, and the UE releases the RRC connection with the FBS.

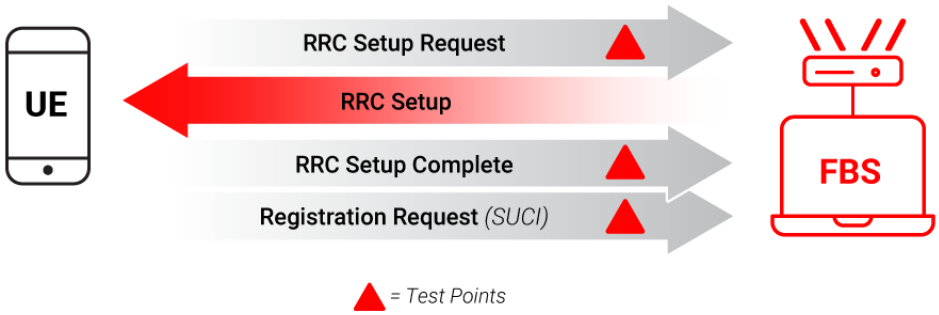


Figure 3: Basic UE RRC Request to FBS

1.1 5G AKA Protocol Test Results

For Test Case 1, the test team initially set the SIB parameters for the false base station's srsRAN gNB—frequency band, channel bandwidth, Physical Cell Identity (PCI), and Tracking Area Code values. The test team initially enabled protocol message capture on a Wireshark packet analyzer on the false base station laptop. The test UE device was also initially powered ON but left with Airplane Mode ON. The test team then initialized the docker container services for the FBS 5G Core as shown in Figure 4, ensuring all services were up and functional.

```
vt-arc@vtarc-NUC10i7FNK:~/docker_open5gs$ docker-compose -f docker-compose-fbs-v3.yaml up
Starting scp     ... done
Starting mongo   ... done
Starting metrics ... done
Starting nrf     ... done
Starting webui   ... done
Starting udr     ... done
Starting ausf    ... done
Starting udm     ... done
Starting nssf    ... done
Starting bsf     ... done
Starting pcf     ... done
Starting amf     ... done
Starting smf     ... done
Starting upf     ... done
Attaching to nrf, metrics, mongo, scp, webui, udr, udm, ausf, pcf, bsf, nssf, amf, smf, upf
```

Figure 4: FBS 5G Core Services Initialized

Once the FBS Core network was operational, the FBS gNB was initialized, enabling broadcasting of Master Information Block (MIB) and System Information Block (SIB) messages using the false base station's USRP X310 software-defined radio (SDR), as shown in Figure 5. The protocol message capture data was observed to record the NAS message exchange between the FBS gNB and the FBS Core. Figure 6 shows the Next Generation Application Protocol (NGAP) and NAS protocol messages between the FBS gNB (IP address 172.22.0.1) and the FBS Core (IP address 172.22.0.10), which contains the initial NG Setup Request and NG Setup Response message exchanges.

The test team began capturing the UE trace logs using the QXDM software on the laptop connected to the 5G test UE. The UE was then turned ON (Airplane Mode OFF), enabling the UE to listen to false base station broadcast signaling messages. The uplink's initial UE message, "RRC Connection Request," was then transmitted. The FBS gNB responded with an "RRC Connection Complete" message to the UE. Once the RRC connection was established, the UE sent a registration request to register to the FBS Core network with registration type "Initial Registration," as shown in Figure 7. As part of the initial registration request, the UE sends the encrypted identity (the Subscription Concealed Identifier, or SUCI), including the concealed Mobile Country Code (MCC) and Mobile Network Code (MNC).

```
vt-arc@vtarc-NUC10i7FNK:~/srsRAN_Project$ sudo docker-compose -f fbs-srs-host-network-docker-compose.yml up
WARNING: Some networks were defined but are not used by any service: host
Starting srsran_gnb ... done
Attaching to srsran_gnb
srsran_gnb | [INFO] [UHD] linux; GNU C++ version 13.2.0; Boost_108300; UHD_4.6.0.0+ds1-5.1build4
srsran_gnb | [INFO] [LOGGING] Fastpath logging disabled at runtime.
srsran_gnb | [INFO] [X300] X300 initialization sequence...
srsran_gnb | [INFO] [X300] Maximum frame size: 1472 bytes.
srsran_gnb | [INFO] [GPS] Found an internal GPSDO: LC_XO, Firmware Rev 0.932
srsran_gnb | [INFO] [X300] Radio 1x clock: 184.32 MHz
srsran_gnb | [WARNING] [0/Radio#0] Attempting to set tick rate to 0. Skipping.
```

Figure 5: False Base Station srsRAN gNB Service Initialized

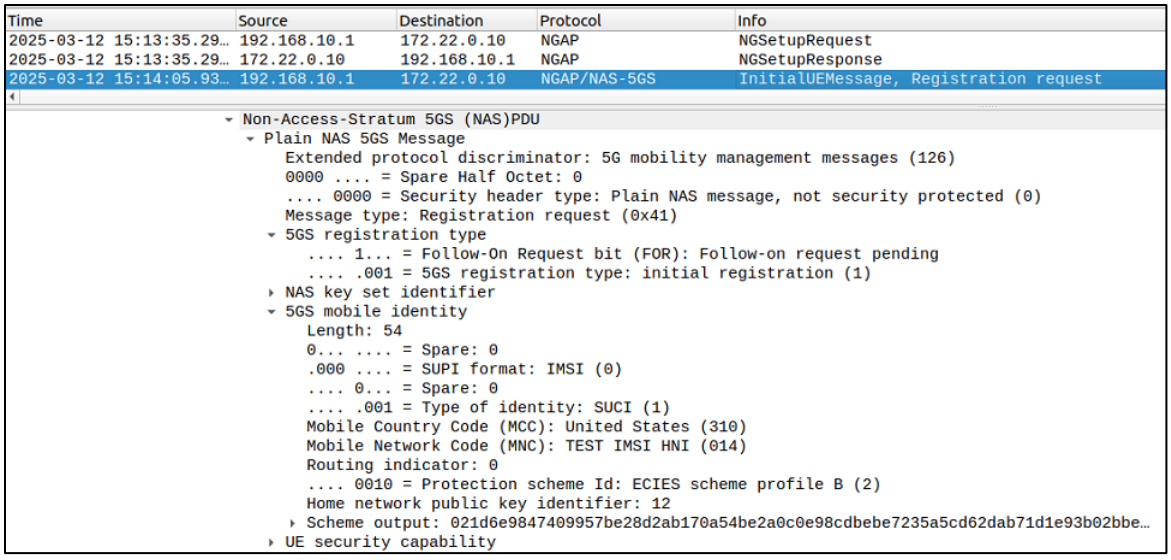


Figure 6: UE NAS Initial Registration Request

The FBS Core network immediately rejected the registration with 5GMM (5G Mobility Management) cause code #9 – "UE identity cannot be derived by the network," as the FBS Core network could not derive the UE's identity from the SUCI due to no matching identity/context stored in the network as shown in Figure 7 and Figure 8. As a result, the UE registration was rejected, and the network sent the context release message to the UE. The UE was then turned OFF (Airplane Mode ON) and the test team captured logs for each of the interfaces demonstrating the test case behavior as shown in the series of figures below from the FBS RAN, FBS Core, and UE QXDM.

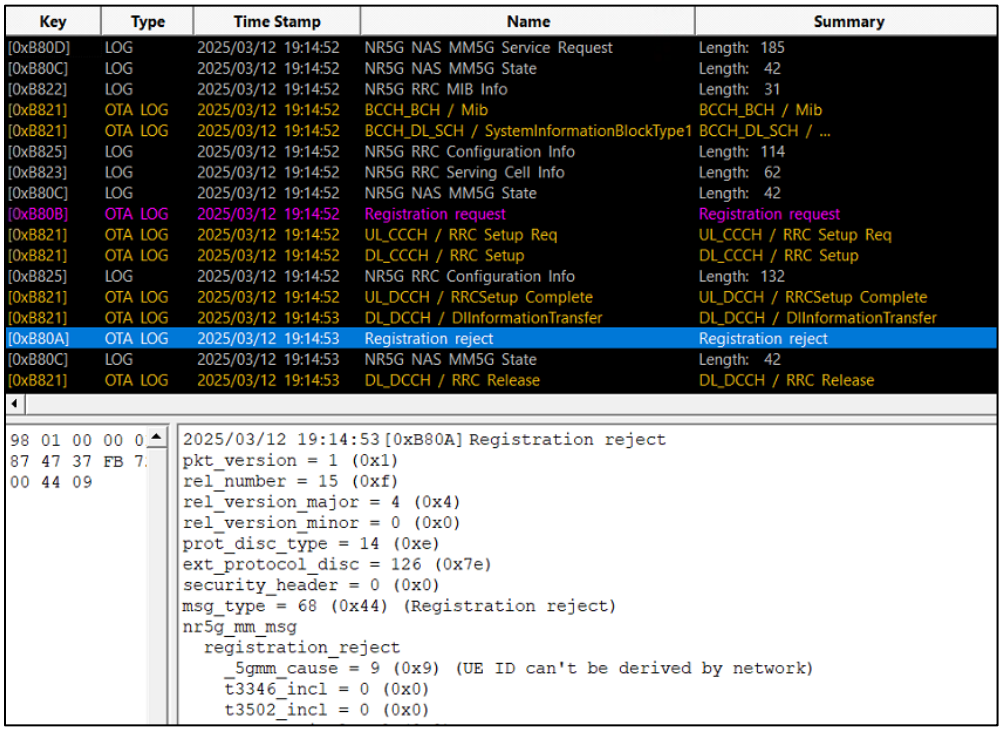


Figure 7: False Base Station NAS Registration Rejection (UE QXDM Log)

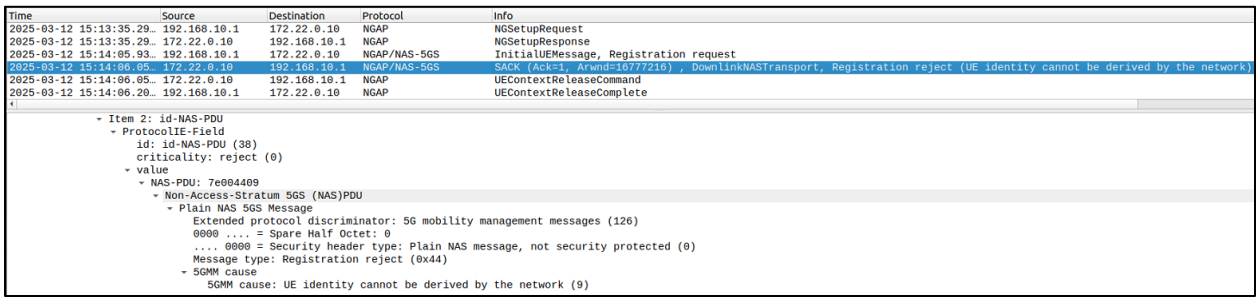


Figure 8: UE Registration Rejection (FBS Wireshark Trace)

Figure 9: False Base Station NAS Registration Rejection (FBS Core Log)

1.2 Null Encryption Test Results

To demonstrate the behavior of a 5G Null encryption SIM in the presence of a false base station, the steps from the test above were repeated with the unencrypted SIM card. To begin, the false base station's gNB and Core docker services were initialized and confirmed as online and operational. The test UE was then turned ON (Airplane Mode OFF), enabling the UE to listen to false base station broadcast signaling messages. The uplink initial UE message "RRC Connection Request" was transmitted. The false base station's gNB responded with an "RRC Connection Complete" message to the UE. Once the RRC connection was established, the UE sent a registration request to register to the FBS Core network with registration type "Initial Registration," as shown in Figure 10.

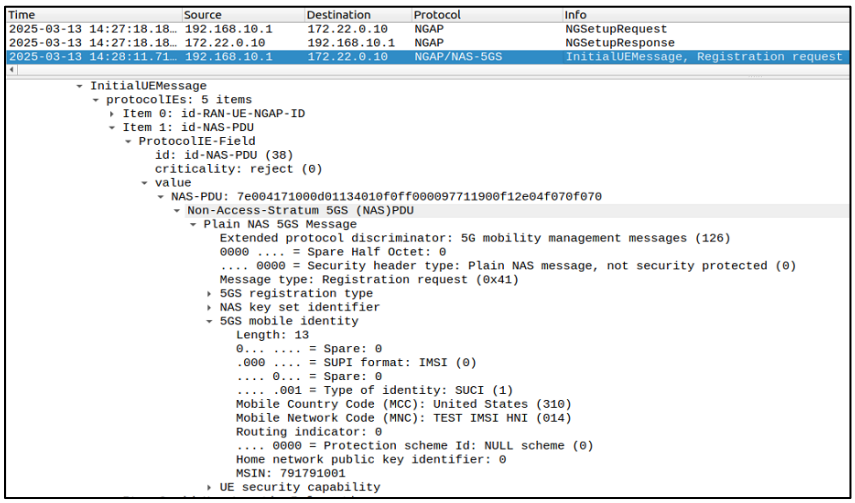


Figure 10: UE NAS Initial Registration

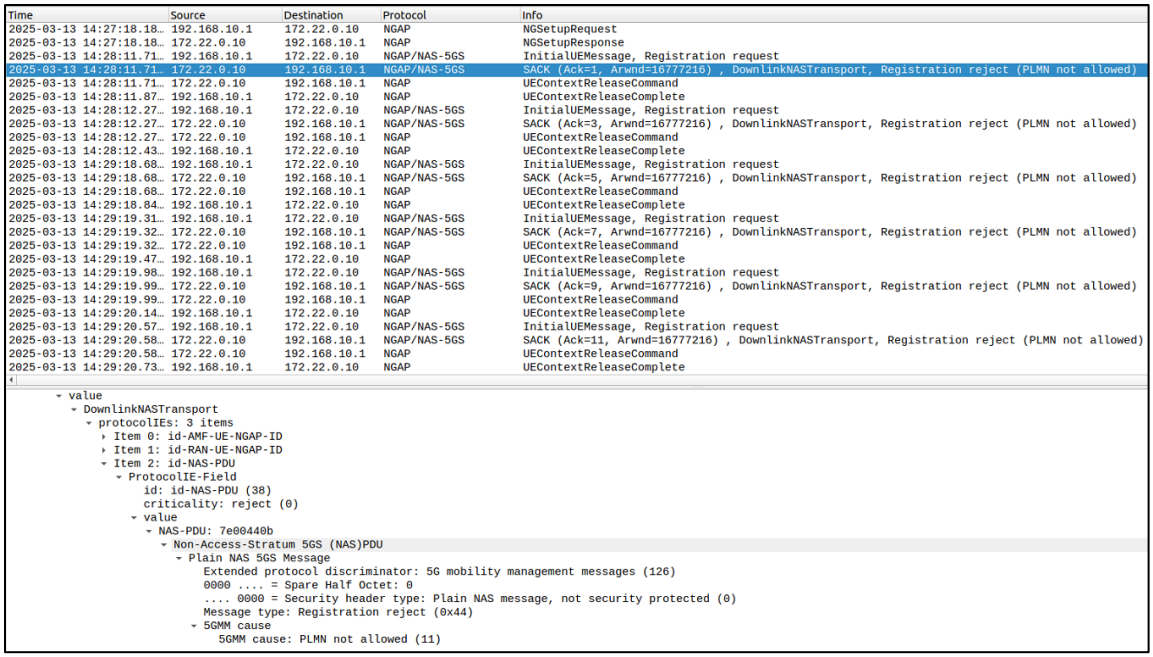
As part of the initial registration request, and in contrast to the 5G AKA SIM, the UE sends the Subscription Permanent Identifier (SUPI) in plain text, which contains the MCC, MNC, and Mobile Subscriber Identification Number (MSIN) in the clear, as shown in Figure 11. This was the expected behavior since the 5G SIM in this test was provisioned to operate without encryption for authenticating users in a 5G network.

```
[amf] INFO: InitialUEMessage (../src/amf/ngap-handler.c:372)
[amf] INFO: [Added] Number of gNB-UEs is now 1 (../src/amf/context.c:2527)
[amf] INFO:     RAN_UE_NGAP_ID[0] AMF_UE_NGAP_ID[1] TAC[1] CellID[0x66c000] (../src/amf/ngap-handler.c:533)
[amf] INFO: [suci-0-310-014-0-0-0-791791001] Unknown UE by SUCI (../src/amf/context.c:1793)
[amf] INFO: [Added] Number of AMF-UEs is now 1 (../src/amf/context.c:1580)
[gmm] INFO: Registration request (../src/amf/gmm-sm.c:1061)
[gmm] INFO: [suci-0-310-014-0-0-0-791791001]    SUCI (../src/amf/gmm-handler.c:231)
[sbi] WARNING: [284e4d6c-0038-41f0-b9ce-e7ab664cc357] (NF-discover) NF has already been added (../lib/sbi/nnrf-handler.c:833)
[sbi] WARNING: NF EndPoint updated [172.22.0.11:80] (../lib/sbi/context.c:1623)
[sbi] WARNING: NF EndPoint updated [172.22.0.11:7777] (../lib/sbi/context.c:1532)
[sbi] INFO: [284e4d6c-0038-41f0-b9ce-e7ab664cc357] (NF-discover) NF Profile updated (../lib/sbi/nnrf-handler.c:856)
[dbi] INFO: [imsi-310014791791001] Cannot find IMSI in DB (../lib/dbi/subscription.c:56)
[udr] WARNING: [imsi-310014791791001] Cannot find SUPI in DB (../src/udr/nudr-handler.c:68)
[udm] WARNING: [suci-0-310-014-0-0-0-791791001] HTTP response error [404] (../src/udm/nudr-handler.c:86)
[ausf] WARNING: [suci-0-310-014-0-0-0-791791001] Cannot find SUPI [404] (../src/ausf/ue-sm.c:155)
[gmm] WARNING: [suci-0-310-014-0-0-0-791791001] Cannot find SUCI [404] (../src/amf/gmm-sm.c:1572)
[amf] WARNING: [suci-0-310-014-0-0-0-791791001] Registration reject [11] (../src/amf/nas-path.c:219)
[amf] INFO: UE Context Release [Action:3] (../src/amf/ngap-handler.c:1648)
```

Figure 11: False Base Station NAS Registration Rejection (FBS Core Log)

Note that the test IMSI was not added to the FBS Core network subscriber profile during this test case execution. As a result, the FBS Core network immediately sent a registration reject message to the UE with cause code #11 – "PLMN Not Allowed." This 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, in a Public Land Mobile Network (PLMN) where the UE, by subscription or due to operator determined barring, is not allowed to operate.

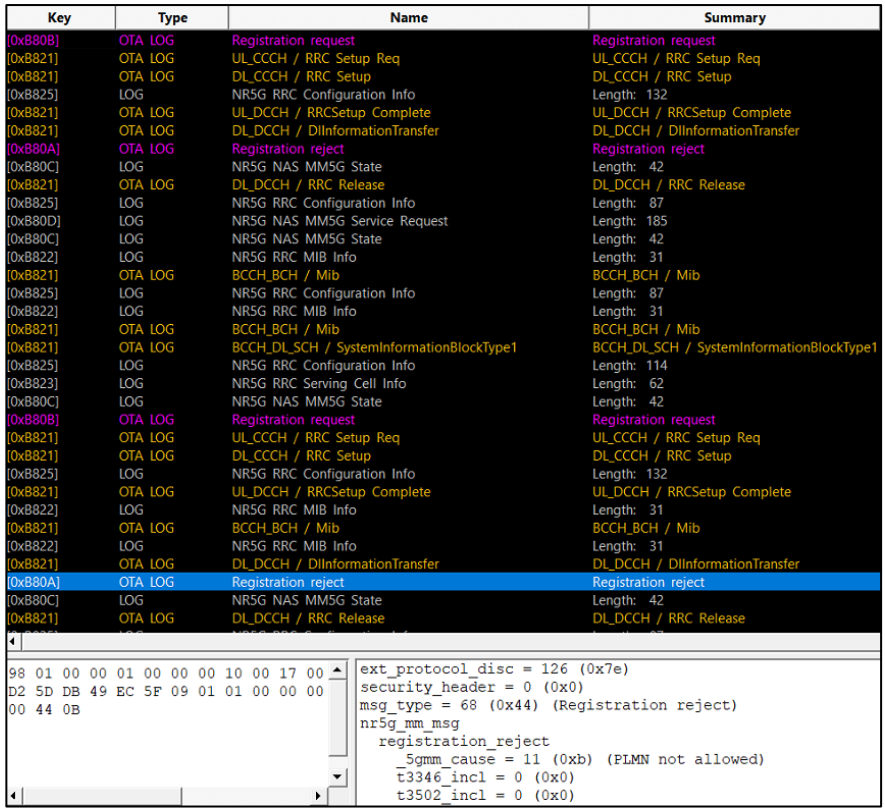
The false base station then sent a UE context release message to the UE, and the registration process was terminated. The UE sent another registration request to the FBS, which rejected the registration, again with cause code #11, sending the UE into a repetitive loop whereby it is unable to connect to false base station, as shown in Figure 12 and Figure 13. It is important to note that here, the FBS network did not have the SIM's IMSI and SUPI information in its database, and the NAS registration procedure is expected to be rejected. The 5G UE was then turned OFF, and the test team captured logs for each of the interfaces demonstrating the test case behavior.



Time	Source	Destination	Protocol	Info
2025-03-13 14:27:18.18…	192.168.10.1	172.22.0.10	NGAP	NGSetupRequest
2025-03-13 14:27:18.18…	172.22.0.10	192.168.10.1	NGAP	NGSetupResponse
2025-03-13 14:28:11.71…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-03-13 14:28:11.71…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-03-13 14:28:11.71…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-03-13 14:28:11.87…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-03-13 14:28:12.27…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-03-13 14:28:12.27…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=3, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-03-13 14:28:12.27…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-03-13 14:28:12.43…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-03-13 14:29:18.68…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-03-13 14:29:18.68…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=5, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-03-13 14:29:18.68…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-03-13 14:29:18.84…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-03-13 14:29:19.31…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-03-13 14:29:19.32…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=7, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-03-13 14:29:19.32…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-03-13 14:29:19.47…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-03-13 14:29:19.98…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-03-13 14:29:19.99…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=9, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-03-13 14:29:19.99…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-03-13 14:29:20.14…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-03-13 14:29:20.57…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-03-13 14:29:20.58…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=11, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-03-13 14:29:20.58…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-03-13 14:29:20.73…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete

```
value
  DownlinkNASTransport
    protocolIEs: 3 items
      Item 0: id-AMF-UE-NGAP-ID
      Item 1: id-RAN-UE-NGAP-ID
      Item 2: id-NAS-PDU
        ProtocolIE-Field
            id: id-NAS-PDU (38)
            criticality: reject (0)
          value
            NAS-PDU: 7e00440b
              Non-Access-Stratum 5GS (NAS)PDU
                Plain NAS 5GS Message
                    Extended protocol discriminator: 5G mobility management messages (126)
                    0000 .... = Spare Half Octet: 0
                    .... 0000 = Security header type: Plain NAS message, not security protected (0)
                    Message type: Registration reject (0x44)
                  5GMM cause
                     5GMM cause: PLMN not allowed (11)
```

Figure 12: False Base Station NAS Registration Rejection (FBS Wireshark Trace)



Key	Type	Name	Summary
[0xB80B]	OTA LOG	Registration request	Registration request
[0xB821]	OTA LOG	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	Registration reject	Registration reject
[0xB80C]	LOG	NR5G NAS MM5G State	Length: 42
[0xB821]	OTA LOG	DL_DCCH / RRC Release	DL_DCCH / RRC Release
[0xB825]	LOG	NR5G RRC Configuration Info	Length: 87
[0xB80D]	LOG	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	NR5G NAS MM5G State	Length: 42
[0xB822]	LOG	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB825]	LOG	NR5G RRC Configuration Info	Length: 87
[0xB822]	LOG	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	NR5G NAS MM5G State	Length: 42
[0xB80B]	OTA LOG	Registration request	Registration request
[0xB821]	OTA LOG	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB822]	LOG	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB822]	LOG	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	Registration reject	Registration reject
[0xB80C]	LOG	NR5G NAS MM5G State	Length: 42
[0xB821]	OTA LOG	DL_DCCH / RRC Release	DL_DCCH / RRC Release

```
98 01 00 00 01 00 00 00 10 00 17 00
D2 5D DB 49 EC 5F 09 01 01 00 00 00
00 44 0B
```

```
ext_protocol_disc = 126 (0x7e)
security_header = 0 (0x0)
msg_type = 68 (0x44) (Registration reject)
nr5g_mm_msg
  registration_reject
    _5gmm_cause = 11 (0xb) (PLMN not allowed)
    t3346_incl = 0 (0x0)
    t3502_incl = 0 (0x0)
```

Figure 13: False Base Station NAS Registration Rejection (UE QXDM Log)

1.3 Outcomes for Both 5G AKA and Null Encryption Tests

Expected Results:
The UE establishes an RF RRC channel with the false base station but waits for authentication before proceeding. The UE drops the false base station connection.

Success Criteria:
The UE establishes an RF RRC channel with the false base station but waits for authentication before proceeding. The UE drops the false base station connection.

Test Results:
As per the observed test results, the UE was able to establish a successful RRC connection with both SIM profiles and requested registration with the false base station. As per the expected results, the registration was rejected by the false base station for the 5G AKA SIM profile due to missing UE context in the FBS Core network. For the Null encryption SIM, the false base station rejected the registration with "PLMN not allowed" due to missing subscriber information in the FBS Core network, as expected. In both cases, the UE was unable to complete registration and released the RRC connection, as expected.

Condition	Status
UE establishes RF RRC channel with FBS but waits for authentication before proceeding. UE drops FBS connection.	
Overall Test	Success

Test Case 2 – Establishing UE RRC Connection After Forced Disconnect from Home Network

Test Case ID: TC-FBS-2

Test Case Name: Establishing UE RRC Connection After Forced Disconnect from Home Radio Base Station

Description:
This test case is designed to observe a successful RRC connection between the UE and a high-powered false base station when the UE is attached to its home network. The UE initiates NAS registration procedures, but subsequent registration and authentication procedures fail between the UE and the FBS. The primary goal of the test is to confirm that the UE will be released without authenticating, and the false base station will collect any identifiers (GUTI) that the UE sends to build the RRC connection.

Objectives:

- Demonstrate that false base station is able to attract the UE attached to its home network by using higher power than the home network. The UE is forced to disconnect from its home network and establish an RRC connection with the FBS.
- Demonstrate that UE then attempts to register to the false base station without success (for both SIM profiles) and releases the RRC connection with the FBS.

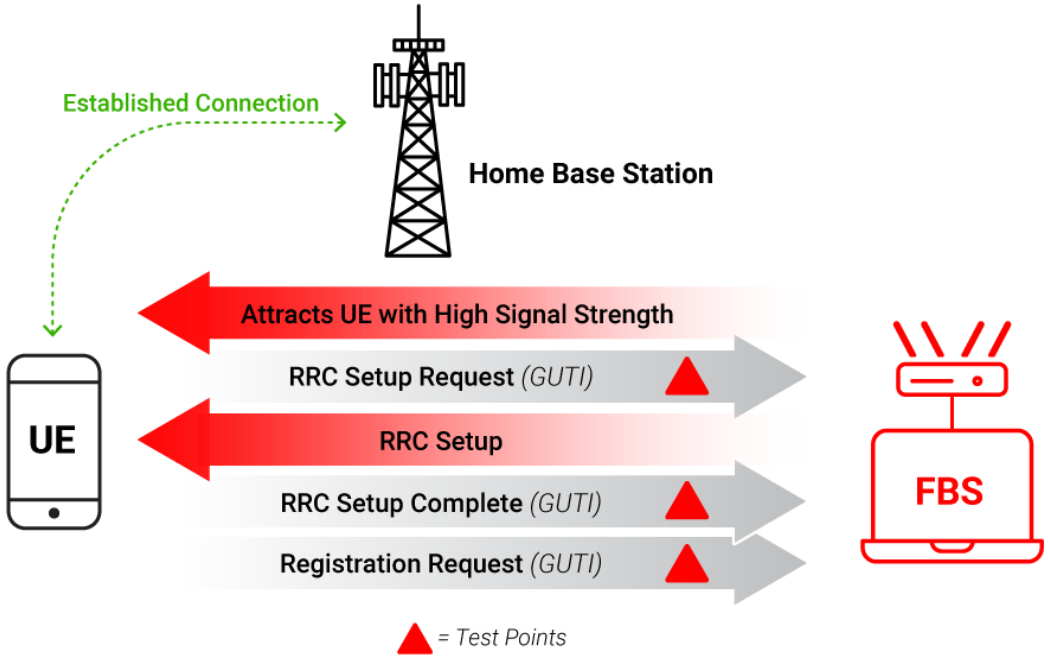


Figure 14: Basic UE RRC Request to False Base Station After Home Radio Base Station (RBS) Disconnect

2.1 5G AKA Test Results

For TC 2, the test team powered ON the home gNodeB and ensured the 5G cells were unlocked and broadcasting as per Figure 15.

```
MUMDO2AVW> st cell

250218-13:27:57-0500 169.254.2.2 23.0k MSRBS_NODE_MODEL_22.Q2_566.28125.116_3317 stopfile=/tmp/1857
================================================================================
Proxy   Adm State       Op. State       MO
================================================================================
   44   0 (LOCKED)      0 (DISABLED)   ENodeBFunction=1,EUtranCellFDD=LUMDO2AVW11
  499   0 (LOCKED)      0 (DISABLED)   GNBDUFunction=1,NRCellDU=AUMDO2AVW11
  501   1 (UNLOCKED)    1 (ENABLED)    GNBDUFunction=1,NRCellDU=KUMDO2AVW11
================================================================================
Total: 3 MOs
```

Figure 15: ECell Unlocked

The test team also enabled the protocol message capture on a Wireshark packet analyzer to capture the NAS messages exchanged between the Ericsson home gNB and the 5G SA Core network. Upon turning ON the 5G test UE, the UE immediately performed a successful RRC connection and NAS registration with the home gNB and the 5G SA Core network as shown in Figure 16. At this time, the UE successfully completed registration and established a PDU session with the home radio base station.

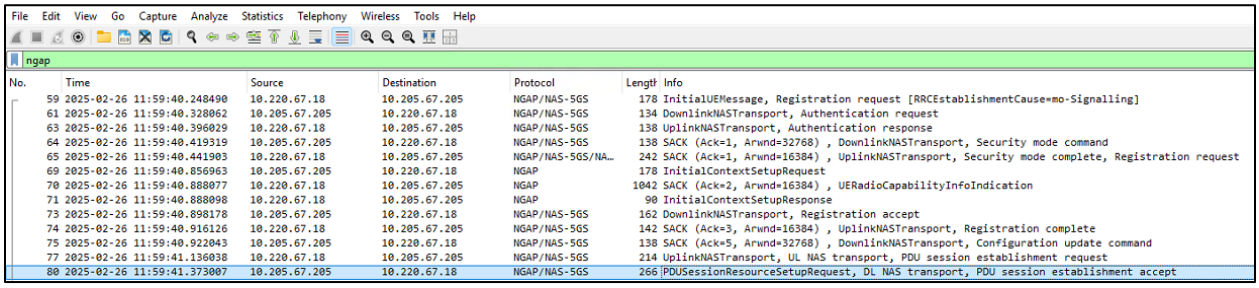


Figure 16: Successful UE NAS Registration with Home Radio Base Station

To observe the behavior of a 5G UE attached to a home network in the presence of a false base station network, the test team used a similar configuration as in TC 1 for the FBS using srsRAN. The test team enabled protocol message capture on a Wireshark packet analyzer on the false base station laptop. To ensure the false base station was able to attract the 5G UE, the FBS output power was set to a maximum allowable value. The test team then initialized the docker container services for the FBS Core, ensuring all services were up and functional. Once the FBS Core network was operational, the FBS gNB was initialized, enabling broadcasting of MIB and SIB messages using the FBS radio. The protocol message capture data was observed to record the NAS message exchange between the FBS gNB and the FBS Core.

To coerce the UE to connect to the false base station, the output power of home gNB was decreased gradually to reduce the influence of the 5G signal propagating from the UE's home network. Once the power values were optimized and the false base station was broadcasting a stronger signal than the home gNB, the UE immediately released its RRC connection to the home

gNB, as shown in Figure 17, and performed a PLMN search, as shown per UE traces in Figure 18: *RRC Connection Setup with FBS*. As the false base station was broadcasting MIB and SIB messages with the same PLMN as the UE's home network, the UE proceeded to perform an RRC connection with the FBS, as shown in Figure 19.

Key	Type	Time Stamp	Name	Summary
[0xB800]	OTA LOG	2025/02/26 16:59:41	PDU session establishment accept	PDU session establishment accept
[0xB821]	OTA LOG	2025/02/26 16:59:51	DL_DCCH / RRC Release	DL_DCCH / RRC Release
[0xB825]	LOG	2025/02/26 16:59:51	NR5G RRC Configuration Info	Length: 87
[0xB822]	LOG	2025/02/26 16:59:51	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 16:59:51	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB825]	LOG	2025/02/26 16:59:51	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/26 16:59:51	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/26 16:59:51	NR5G NAS MM5G State	Length: 42
[0xB80D]	LOG	2025/02/26 17:03:08	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/26 17:03:08	NR5G NAS MM5G State	Length: 42
[0xB825]	LOG	2025/02/26 17:03:08	NR5G RRC Configuration Info	Length: 87
[0xB822]	LOG	2025/02/26 17:03:08	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 17:03:08	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/26 17:03:09	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1

Figure 17: UE Releasing RRC Connection with Home Network and Detecting FBS gNB

```
2025/02/26 17:03:08 [0xB80C] NR5G NAS MM5G State
Version = 1
Version 1 {
   MM5G State = REGISTERED
   Mm5g Registered Substate = PLMN_SEARCH
   PLMN ID {
      Identity = { 0xFF, 0xFF, 0xFF }
```

Figure 18: UE Performing PLMN Search

```
2025/02/26 17:03:09 [0xB821] UL_CCCH / RRC Setup Req
Pkt Version = 14
RRC Release Number.Major.minor = 16.3.1
Radio Bearer ID = 0, Physical Cell ID = 1
NR Cell Global Id = N/A
Freq = 126990
Sfn = N/A, SubFrameNum = N/A
slot = 0
PDU Number = UL_CCCH Message,    Msg Length = 6
SIB Mask in SI =  0x00
```

Figure 19: RRC Connection Setup with FBS

Once the UE successfully established an RRC connection with the false base station, the UE sent a mobility update registration request to register with the false base station network using the 5G-GUTI identifier allocated during the initial registration in a previous session by the home radio base station. Note that the 5G registration type was "mobility registration updating" as the UE switched between two networks having different tracking areas (TA) as shown in Figure 20.

The false base station network then attempted to authenticate the 5G UE and initiated further security procedures by sending an "Identity Request" message. As the UE's stored 5G-GUTI was unknown to the FBS Core network, the false base station requested the UE to provide its SUCI identifier. Upon receiving the mobility update registration request, the UE responded with the Identity Response message containing the encrypted SUPI (SUCI), as shown in Figure 21. However, the FBS network was unable to authenticate the 5G UE as the false base station could not derive the UE's identity from the SUCI due to no matching identity/context stored in the network. As seen in Figure 21 below, the 5G UE sent the MCC MNC in clear, but the MSIN was encrypted containing the public key. As a result, the UE registration was rejected with 5GMM

cause #9 – "UE identity cannot be derived by the network," and the false base station sent the context release message to the UE. Note that here the FBS network considers the 5G UE SIM to be a foreign SIM, and the NAS registration procedure is expected to be rejected. The UE was then turned OFF, and the test team captured logs for each of the interfaces demonstrating the test case behavior.

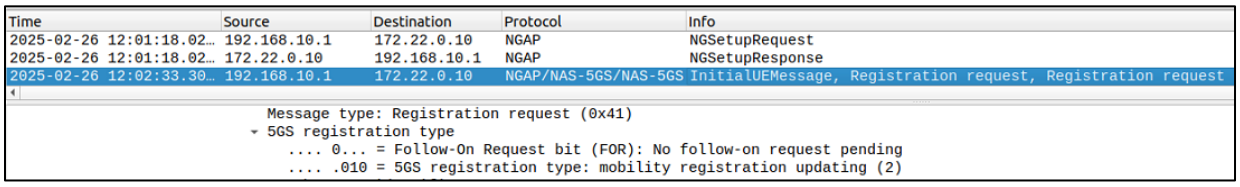


Figure 20: UE NAS Mobility Update Registration Request

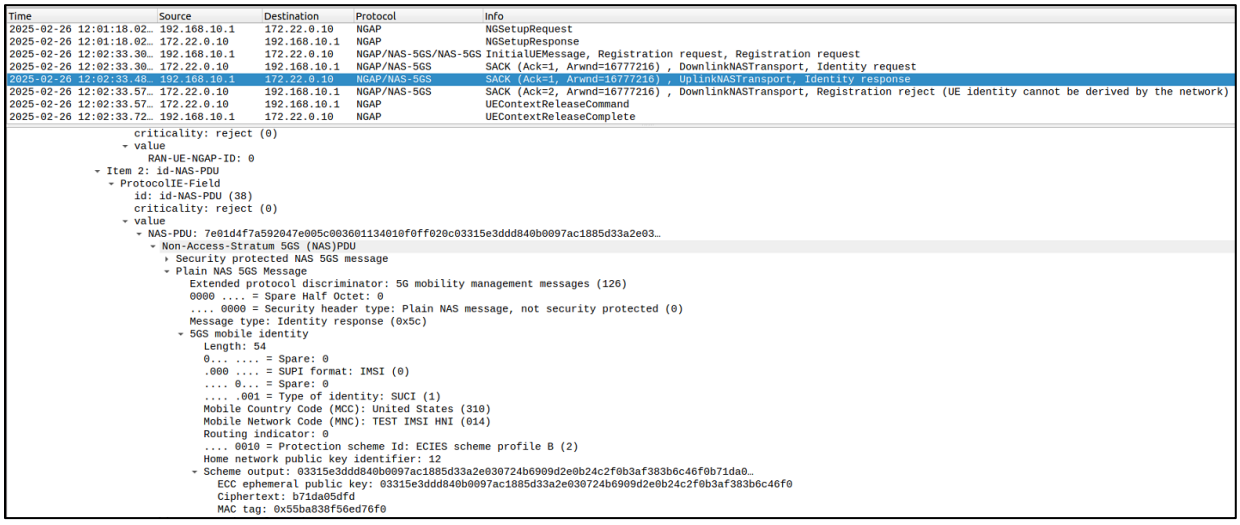


Figure 21: NAS Identity Request and Response Procedure

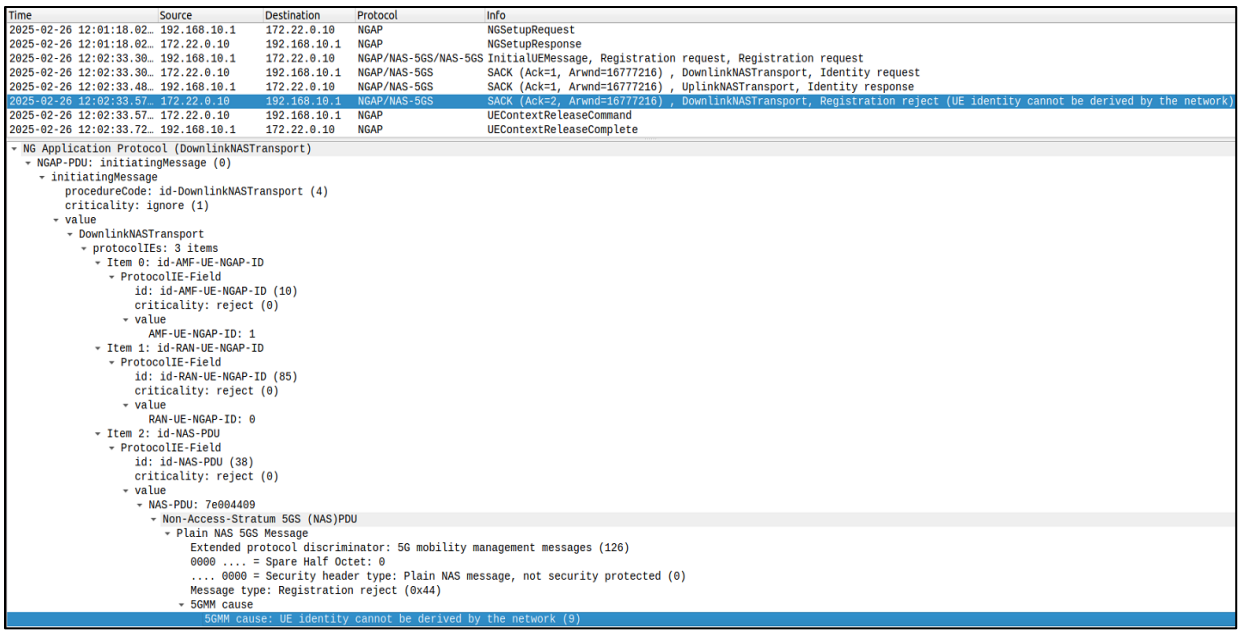


Figure 22: False Base Station NAS Registration Rejection (FBS Wireshark Trace)

2.2 Null Encryption Test Results

To demonstrate the behavior of a 5G Null encryption SIM in the presence of a false base station, the test team turned ON the 5G UE and ensured the UE was connected and attached successfully to the home network, as per the UE traces shown in Figure 23.

Key	Type	Time Stamp	Name	Summary
[0xB814]	OTA LOG	2025/02/27 19:23:04	NR5G NAS Plain Message Container	Length: 71
[0xB80B]	OTA LOG	2025/02/27 19:23:04	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/27 19:23:04	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 102
[0xB821]	OTA LOG	2025/02/27 19:23:04	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/27 19:23:04	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/27 19:23:04	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 19:23:04	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/27 19:23:04	DL_DCCH / securityModeCommand	DL_DCCH / securityModeCommand
[0xB825]	LOG	2025/02/27 19:23:04	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 19:23:04	UL_DCCH / SecurityMode Complete	UL_DCCH / SecurityMode Complete
[0xB821]	OTA LOG	2025/02/27 19:23:04	DL_DCCH / UeCapabilityEnquiry	DL_DCCH / UeCapabilityEnquiry
[0xB821]	OTA LOG	2025/02/27 19:23:04	UL_DCCH / UeCapabilityInformation	UL_DCCH / UeCapabilityInformation
[0xB821]	OTA LOG	2025/02/27 19:23:04	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB808]	OTA LOG	2025/02/27 19:23:04	NR5G NAS MM5G Security Protected OTA Incoming Msg	Length: 79
[0xB80A]	OTA LOG	2025/02/27 19:23:04	Registration accept	Registration accept
[0xB80B]	OTA LOG	2025/02/27 19:23:04	Registration complete	Registration complete
[0xB809]	OTA LOG	2025/02/27 19:23:04	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 33
[0xB821]	OTA LOG	2025/02/27 19:23:04	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB80C]	LOG	2025/02/27 19:23:04	NR5G NAS MM5G State	Length: 42
[0xB821]	OTA LOG	2025/02/27 19:23:04	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB808]	OTA LOG	2025/02/27 19:23:05	NR5G NAS MM5G Security Protected OTA Incoming Msg	Length: 52
[0xB80A]	OTA LOG	2025/02/27 19:23:05	Config update command	Config update command
[0xB801]	OTA LOG	2025/02/27 19:23:05	PDU session establishment req	PDU session establishment req
[0xB80B]	OTA LOG	2025/02/27 19:23:05	UL NAS transport	UL NAS transport
[0xB809]	OTA LOG	2025/02/27 19:23:05	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 119
[0xB821]	OTA LOG	2025/02/27 19:23:05	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/27 19:23:05	DL_DCCH / RRCReconfiguration	DL_DCCH / RRCReconfiguration
[0xB825]	LOG	2025/02/27 19:23:05	NR5G RRC Configuration Info	Length: 168
[0xB821]	OTA LOG	2025/02/27 19:23:05	UL_DCCH / RRCConfiguration Complete	UL_DCCH / RRCConfiguration Complete
[0xB808]	OTA LOG	2025/02/27 19:23:05	NR5G NAS MM5G Security Protected OTA Incoming Msg	Length: 118
[0xB80A]	OTA LOG	2025/02/27 19:23:05	DL NAS transport	DL NAS transport
[0xB800]	OTA LOG	2025/02/27 19:23:05	PDU session establishment accept	PDU session establishment accept

Figure 23: Successful UE NAS Registration with the Home Radio Base Station

The protocol capture was enabled for both the home network and the false base station. The FBS Core and gNB docker container services were initialized and ensured the services were up and operational. For this test case, the FBS Core network is unaware of any UE credentials and does not have any information on the UE subscriber SIM profile. With the false base station configured to transmit at maximum output power, and with signal strength stronger than the home network, the UE was able to successfully release the connection to the home network and perform an RF connection with the FBS using the RRC connection procedure as shown in Figure 24. Once the RRC connection was established, the UE sent a mobility update registration request to register to the FBS Core network.

Key	Type	Time Stamp	Name	Summary
[0xB821]	OTA LOG	2025/02/27 19:26:02	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/27 19:26:02	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/27 19:26:02	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/27 19:26:02	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/27 19:26:02	NR5G NAS MM5G State	Length: 42
[0xB814]	OTA LOG	2025/02/27 19:26:02	NR5G NAS Plain Message Container	Length: 75
[0xB80B]	OTA LOG	2025/02/27 19:26:02	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/27 19:26:02	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 106
[0xB821]	OTA LOG	2025/02/27 19:26:02	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/27 19:26:02	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/27 19:26:02	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 19:26:02	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/27 19:26:02	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/27 19:26:02	Identity request	Identity request
[0xB80B]	OTA LOG	2025/02/27 19:26:02	Identity response	Identity response
[0xB809]	OTA LOG	2025/02/27 19:26:02	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 48
[0xB821]	OTA LOG	2025/02/27 19:26:02	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/27 19:26:02	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/27 19:26:02	Registration reject	Registration reject
[0xB821]	OTA LOG	2025/02/27 19:26:02	DL_DCCH / RRC Release	DL_DCCH / RRC Release
[0xB80C]	LOG	2025/02/27 19:26:02	NR5G NAS MM5G State	Length: 42
[0xB825]	LOG	2025/02/27 19:26:02	NR5G RRC Configuration Info	Length: 87
[0xB80D]	LOG	2025/02/27 19:26:02	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/27 19:26:02	NR5G NAS MM5G State	Length: 42

```
98 01 00 00 0
AB 65 BF 36 E
00 0E F0 01 0
05 8D CF D4 8
```

```
2025/02/27 19:26:02 [0xB821] UL_CCCH / RRC Setup Req
Pkt Version = 14
RRC Release Number.Major.minor = 16.3.1
Radio Bearer ID = 0, Physical Cell ID = 1
NR Cell Global Id = N/A
Freq = 126990
Sfn = N/A, SubFrameNum = N/A
slot = 0
PDU Number = UL_CCCH Message,    Msg Length = 6
SIB Mask in SI =  0x00
```

Figure 24: RRC Connection Setup with the False Base Station

Similar to the procedure described with the 5G AKA SIM in Section 2.1 above, the false base station then attempted to authenticate the 5G UE and initiated further security procedures by sending an "Identity Request" message. Upon receiving the mobility update registration request, 5G UE responded back with an "Identity Response" message containing the SUPI, as shown in Figure 25. In this case, since the SIM is non-encrypted, the 5G UE sent the MCC, MNC, and MSIN in clear as part of the SUPI identity.

Time	Source	Destination	Protocol	Info
2025-02-27 14:23:51.40…	192.168.10.1	172.22.0.10	NGAP	NGSetupRequest
2025-02-27 14:23:51.40…	172.22.0.10	192.168.10.1	NGAP	NGSetupResponse
2025-02-27 14:25:26.43…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS/NAS-5GS	InitialUEMessage, Registration request, Registration request
2025-02-27 14:25:26.43…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , DownlinkNASTransport, Identity request
2025-02-27 14:25:26.47…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , UplinkNASTransport, Identity response
2025-02-27 14:25:26.48…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-02-27 14:25:26.48…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-27 14:25:26.63…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete

```
            criticality: reject (0)
          ▾ value
              RAN-UE-NGAP-ID: 0
        ▾ Item 2: id-NAS-PDU
          ▾ ProtocolIE-Field
              id: id-NAS-PDU (38)
              criticality: reject (0)
            ▾ value
              ▾ NAS-PDU: 7e01abf01fec0b7e005c000d01134010f0ff000097711900f1
                ▾ Non-Access-Stratum 5GS (NAS)PDU
                  ▸ Security protected NAS 5GS message
                  ▾ Plain NAS 5GS Message
                      Extended protocol discriminator: 5G mobility management messages (126)
                      0000 .... = Spare Half Octet: 0
                      .... 0000 = Security header type: Plain NAS message, not security protected (0)
                      Message type: Identity response (0x5c)
                    ▾ 5GS mobile identity
                        Length: 13
                        0... .... = Spare: 0
                        .000 .... = SUPI format: IMSI (0)
                        .... 0... = Spare: 0
                        .... .001 = Type of identity: SUCI (1)
                        Mobile Country Code (MCC): United States (310)
                        Mobile Network Code (MNC): TEST IMSI HNI (014)
                        Routing indicator: 0
                        .... 0000 = Protection scheme Id: NULL scheme (0)
                        Home network public key identifier: 0
                        MSIN: 791791001
```

Figure 25: NAS Identity Response Containing SUCI Values in the Clear

However, the FBS Core network immediately sent a registration reject message to the UE with the cause code value #11 – "PLMN Not Allowed," as shown in Figure 26. This 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, in a PLMN where the UE, by subscription or due to operator determined barring, is not allowed to operate.

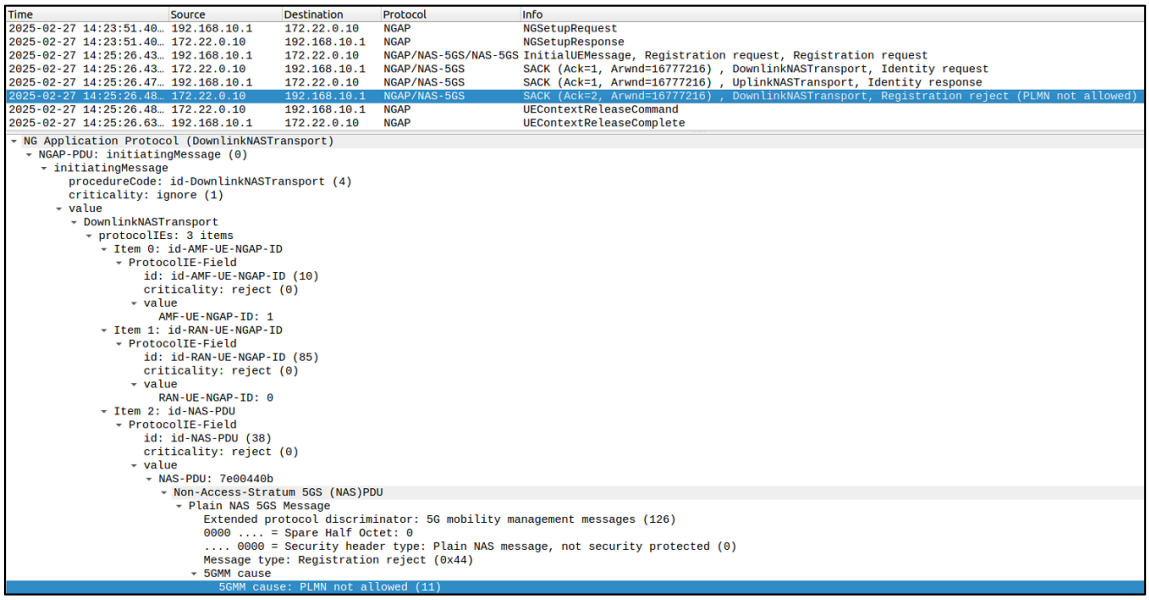


Figure 26: False Base Station NAS Registration Rejection (FBS Wireshark Trace)

The FBS then sent the UE a context release message, and the registration process was terminated. The UE again sent a registration request to the FBS, and the FBS rejected the registration with the same cause code value and went into a repetitive loop whereby it was unable to connect to the false base station, as shown in Figure 27. Note that from this registration attempt onward, the UE sent a registration request with the 5GS registration type "Initial Registration" instead of "Mobility Registration Update." It should also be noted that here the FBS network considers the 5G UE SIM to be a foreign SIM, and the NAS registration procedure is expected to be rejected. The 5G UE was then turned OFF, and the test team captured logs for each of the interfaces demonstrating the test case behavior.

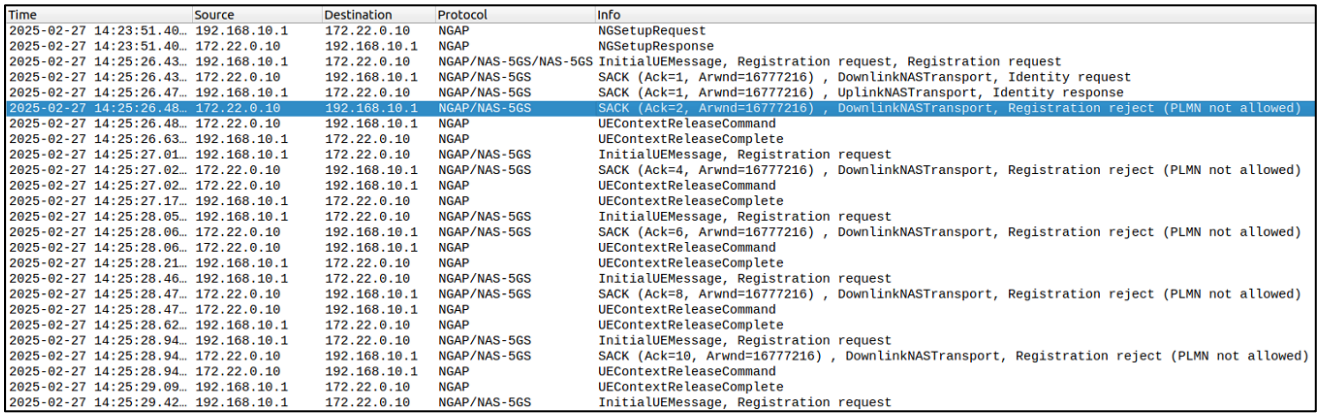


Figure 27: Multiple NAS Registration Rejections (FBS Wireshark Trace)

2.3 Outcomes for Both 5G AKA and Null Encryption Tests

Expected Results:
The UE cannot be coerced off the home gNB. The UE establishes an RF RRC channel with the false base station but waits for authentication before proceeding. The UE drops the false base station connection.

Success Criteria:
The UE cannot be coerced off the home gNB. The UE establishes an RF RRC channel with the false base station but waits for authentication before proceeding. The UE drops the false base station connection.

Test Results:
As per the observed test results and success criteria, the false base station was able to attract the 5G UE attached to its home network and establish a successful RRC connection. The 5G UE initiated NAS registration procedures (i.e., identity verification) with FBS, but was unable to complete the registration and released the RRC connection as expected. Note that for the 5G Null encryption SIM, the UE goes into a repetitive loop whereby the false base station continues rejecting registration on the same PLMN as the home network, and the UE is unable to connect to either network.

Condition	Status
UE cannot be coerced off the home gNB. UE established RF RRC channel with FBS but waits for Authentication before proceeding. UE drops the FBS connection.	
Overall Test	Success

Test Case 3 – Attempting Registration After Omitting Authentication Handshake

---

Test Case ID: TC-FBS-3

Test Case Name: Attempting Registration After Omitting Authentication Handshake

Description:
This test case is designed to prompt the false base station to accept UE registration without authentication by replying to UE with a "Registration Accept" NAS message without sending an authentication request. The primary goal of this test is to confirm that the UE will respond by rejecting the authentication request and disconnecting from the FBS.

Objectives:

- Demonstrate whether a UE attached to its home network is forced to disconnect, establish an RRC connection to a false base station with higher power levels than the home gNodeB, and accept the NAS registration message sent by the false base station without performing identity transfer or authentication procedures.

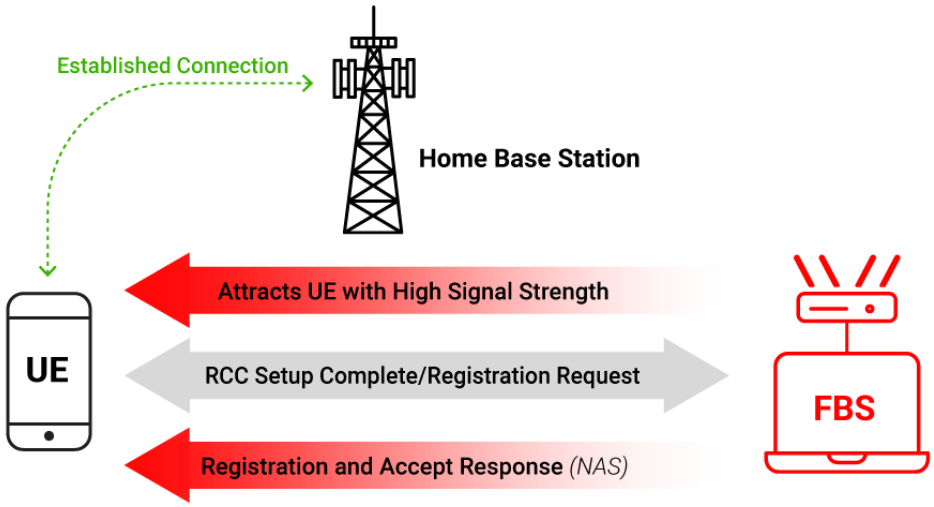


Figure 28: UE Registration Attempt Without FBS Authentication Request

3.1 5G AKA Test Results

As described and performed in Test Case 2, the 5G test UE initially established a connection and properly authenticated with the home network. For this Test Case 3, the FBS Core configuration was modified prior to the test to prompt the FBS to respond to the UE with a 'Registration Accept' NAS message and skip the authentication handshake. The FBS Core and gNB docker container services were initialized and the services were up and operational. The UE was then prompted by the higher-powered FBS to release its connection with the home network. The UE, upon seeing a stronger signal being emitted from the FBS, attempted to connect to the FBS and an RRC connection was successfully established. Once the RRC connection was established, the UE sent a mobility update registration request to register to the FBS Core network using the 5G-GUTI previously assigned by the 5G home network as shown in Figure 29.

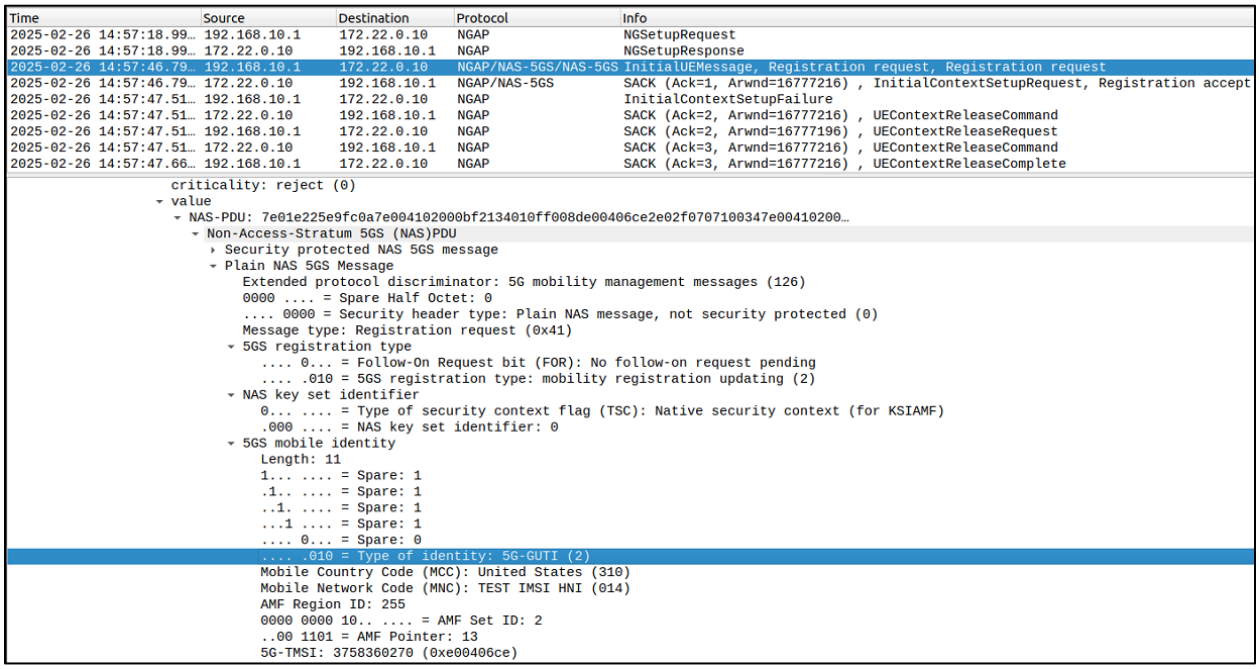


Figure 29 UE NAS Mobility update Registration request

Upon receiving the mobility update registration request from the UE, the FBS Core network attempted to perform an initial context setup with the UE and responded directly with the NAS 'registration accept' message bypassing the authentication procedure step ideally required for the NAS registration process as shown in Figure 30.

```
Time                        Source          Destination     Protocol                Info
2025-02-26 14:57:18.99…  192.168.10.1    172.22.0.10     NGAP                    NGSetupRequest
2025-02-26 14:57:18.99…  172.22.0.10     192.168.10.1    NGAP                    NGSetupResponse
2025-02-26 14:57:46.79…  192.168.10.1    172.22.0.10     NGAP/NAS-5GS/NAS-5GS    InitialUEMessage, Registration request, Registration request
2025-02-26 14:57:46.79…  172.22.0.10     192.168.10.1    NGAP/NAS-5GS            SACK (Ack=1, Arwnd=16777216) , InitialContextSetupRequest, Registration accept
2025-02-26 14:57:47.51…  192.168.10.1    172.22.0.10     NGAP                    InitialContextSetupFailure
2025-02-26 14:57:47.51…  172.22.0.10     192.168.10.1    NGAP                    SACK (Ack=2, Arwnd=16777216) , UEContextReleaseCommand
2025-02-26 14:57:47.51…  192.168.10.1    172.22.0.10     NGAP                    SACK (Ack=2, Arwnd=16777196) , UEContextReleaseRequest
2025-02-26 14:57:47.51…  172.22.0.10     192.168.10.1    NGAP                    SACK (Ack=3, Arwnd=16777216) , UEContextReleaseCommand
2025-02-26 14:57:47.66…  192.168.10.1    172.22.0.10     NGAP                    SACK (Ack=3, Arwnd=16777216) , UEContextReleaseComplete

        id: id-NAS-PDU (38)
        criticality: ignore (1)
      ▾ value
        ▾ NAS-PDU: 7e0200000000007e0042010177000bf2134010020040c00003d0540740134010000001150…
          ▾ Non-Access-Stratum 5GS (NAS)PDU
            ▾ Security protected NAS 5GS message
                Extended protocol discriminator: 5G mobility management messages (126)
                0000 .... = Spare Half Octet: 0
                .... 0010 = Security header type: Integrity protected and ciphered (2)
                Message authentication code: 0x00000000
                Sequence number: 0
            ▾ Plain NAS 5GS Message
                Extended protocol discriminator: 5G mobility management messages (126)
                0000 .... = Spare Half Octet: 0
                .... 0000 = Security header type: Plain NAS message, not security protected (0)
                Message type: Registration accept (0x42)
              ▸ 5GS registration result
              ▾ 5GS mobile identity - 5G-GUTI
                  Element ID: 0x77
                  Length: 11
                  1... .... = Spare: 1
                  .1.. .... = Spare: 1
                  ..1. .... = Spare: 1
                  ...1 .... = Spare: 1
                  .... 0... = Spare: 0
                  .... .010 = Type of identity: 5G-GUTI (2)
                  Mobile Country Code (MCC): United States (310)
                  Mobile Network Code (MNC): TEST IMSI HNI (014)
                  AMF Region ID: 2
                  0000 0000 01.. .... = AMF Set ID: 1
                  ..00 0000 = AMF Pointer: 0
                  5G-TMSI: 3221226448 (0xc00003d0)
```

Figure 30 FBS sending NAS 'Registration accept' message to UE

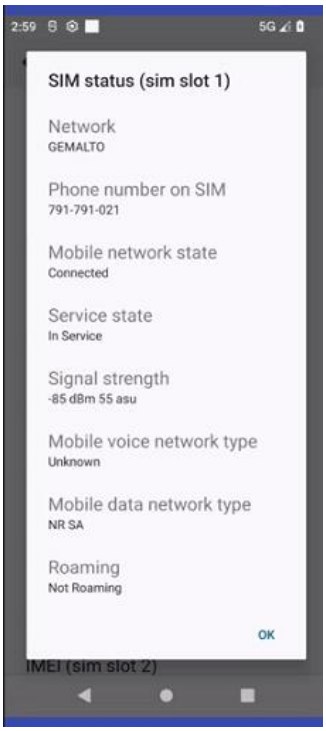


Figure 31: UE connected to FBS

As the FBS Core network did not have the NAS security context from the UE, the FBS sent the security mode command message to the UE as part of the initial context set up request along with the registration accept message. However, the UE upon receiving this security mode command message was unable to validate the network and sent the 'Security Mode Failure' message informing the network that the UE could not successfully establish the new security context due to invalid security parameters as shown in UE traces in Figure 32. As a result, the FBS network immediately terminated the initial context setup process and released the RRC connection. The UE was then turned OFF and the test team captured logs for each of the interfaces demonstrating the test case behavior.

Figure 31 shows the snapshot of the 5G UE when the UE was connected to the FBS network with an RSRP level of -85 dBm as the FBS attempted to force UE to accept the NAS registration without authentication.

Key	Type	Time Stamp	Name	Summary
[0xB823]	LOG	2025/02/26 19:58:22	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/26 19:58:22	NR5G NAS MM5G State	Length: 42
[0xB814]	OTA LOG	2025/02/26 19:58:22	NR5G NAS Plain Message Container	Length: 75
[0xB80B]	OTA LOG	2025/02/26 19:58:22	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/26 19:58:22	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 106
[0xB821]	OTA LOG	2025/02/26 19:58:22	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/26 19:58:22	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/26 19:58:22	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/26 19:58:22	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/26 19:58:22	DL_DCCH / securityModeCommand	DL_DCCH / securityModeCommand
[0xB821]	OTA LOG	2025/02/26 19:58:22	UL_DCCH / SecurityMode Failure	UL_DCCH / SecurityMode Failure
[0xB821]	OTA LOG	2025/02/26 19:58:23	DL_DCCH / RRC Release	DL_DCCH / RRC Release

Figure 32: NAS Security Mode Failure During UE Registration

3.2 Null Encryption Test Results

The test results for the Null encryption SIM were similar to the results demonstrated in Section 3.1 above with the 5G AKA SIM. As described and performed in TC 2, the 5G test UE initially established a connection and properly authenticated with the home network. The FBS Core configuration was modified prior to the test to prompt FBS to respond to UE with a 'Registration Accept' NAS message and skip the authentication handshake. The FBS Core and gNB docker container services were initialized and ensured the services were up and operational. The UE was then prompted by the higher-powered FBS to release its connection to the home network. The UE upon seeing a stronger signal being emitted from the FBS, attempted to connect to the FBS and an RRC connection was successfully established. Once the RRC connection was established, the UE sent a mobility update registration request to register to the FBS Core network using the 5G-GUTI previously assigned by the 5G home network.

Upon receiving the mobility update registration request from the UE, the FBS Core network attempted to perform an initial context setup with the UE and responded directly with the NAS "registration accept" message bypassing the authentication procedure step ideally required for the NAS registration process as shown in Figure 33.

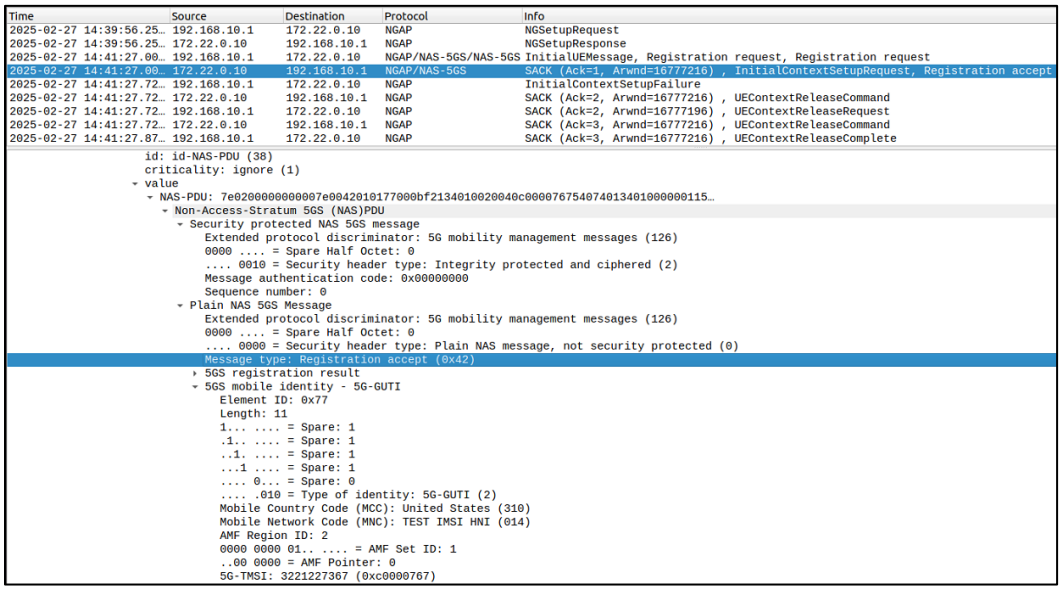


Figure 33: FBS Sending NAS "Registration Accept" Message to the UE

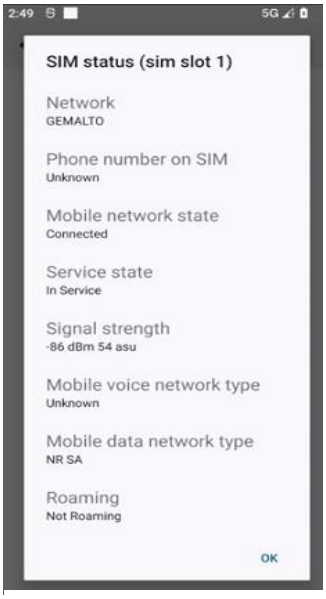


Figure 34: UE Connected to FBS

As the FBS Core network did not have the NAS security context from the UE, the false base station sent the security mode command message to the UE as part of the initial context set up request along with the registration accept message. However, the UE upon receiving this security mode command message was unable to validate the network and sent the "Security Mode Failure" message informing the network that the UE could not successfully establish the new security context due to invalid security parameters, as shown in UE traces in Figure 35. As a result, the FBS network immediately terminated the initial context setup process and released the RRC connection. The UE was then turned OFF, and the test team captured logs for each of the interfaces demonstrating the test case behavior.

Figure 35 shows the snapshot of the 5G UE when the UE was connected to false base station network with an RSRP (Reference Signal Received Power) level of -86 dBm as the FBS attempted to force UE to accept the NAS registration without authentication.

Key	Type	Time Stamp	Name	Summary
[0xB825]	LOG	2025/02/27 19:42:02	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/27 19:42:02	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/27 19:42:02	NR5G NAS MM5G State	Length: 42
[0xB814]	OTA LOG	2025/02/27 19:42:02	NR5G NAS Plain Message Container	Length: 75
[0xB80B]	OTA LOG	2025/02/27 19:42:02	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/27 19:42:02	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 106
[0xB821]	OTA LOG	2025/02/27 19:42:02	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/27 19:42:02	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/27 19:42:03	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 19:42:03	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB822]	LOG	2025/02/27 19:42:03	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 19:42:03	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB822]	LOG	2025/02/27 19:42:03	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 19:42:03	DL_DCCH / securityModeCommand	DL_DCCH / securityModeCommand
[0xB821]	OTA LOG	2025/02/27 19:42:03	UL_DCCH / SecurityMode Failure	UL_DCCH / SecurityMode Failure
[0xB821]	OTA LOG	2025/02/27 19:42:03	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB821]	OTA LOG	2025/02/27 19:42:03	DL_DCCH / RRC Release	DL_DCCH / RRC Release

Figure 35: NAS Security Mode Failure During UE Registration

3.3 Outcomes for Both 5G AKA and Null Encryption Tests

Expected Results:
The UE does not connect with the false base station. If the UE does connect with the FBS, the UE disconnects from the FBS when it receives the Registration Accept NAS message without an Authentication Request message.

Success Criteria:
The UE does not connect with the false base station. If the UE does connect with FBS, the UE disconnects from the FBS when it receives a Registration Accept NAS message without an Authentication Request message.

Test Results:
The test results were successfully validated by observing that UE disconnects from the false base station as expected when the FBS attempts to force the UE to accept the NAS registration instead of performing the identity request and response steps as part of the authentication procedure.

Condition	Status
The UE does not connect with the FBS. If the UE does connect, the UE disconnects from the FBS when it receives a Registration Accept NAS message without first receiving an Authentication Request message.	
Overall Test	Success

Test Case 4 – Attempting Authentication Handshake Using Random Identifiers

Test Case ID: TC-FBS-4

Test Case Name: Attempting Authentication Handshake Using Random Identifiers

Description:
This test case is designed to observe the UE's behavior when the false base station attempts to authenticate the UE using fabricated authentication credentials. The primary goal of this test is to confirm that the UE will respond by rejecting the authentication request and disconnecting from the FBS.

Objectives:

- Demonstrate that when a UE attached to its home network is forced to disconnect from the network and establish an RRC connection to a higher-powered false base station, the UE will reject NAS authentication to an FBS network that is using random authentication vectors.

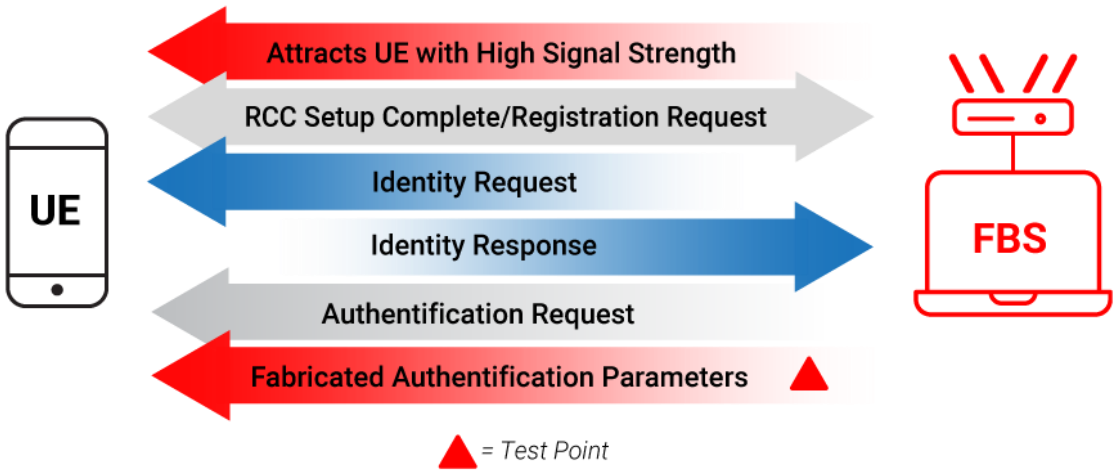


Figure 36: False Base Station Authentication Request with UE Using Fabricated Credentials

4.1 5G AKA Test Results

As described and performed in Test Case 2, the 5G test UE initially established a connection and properly authenticated with the home network. For this TC 4, the test IMSI was added to the FBS Core network subscriber profile with random subscription key "K" and Operator code "OPc" values. Note that an FBS operator is typically unaware of the true authentication identifiers provisioned for a legitimate 5G IMSI being used with its home network and hence random values were utilized to mimic the real-world operational scenario. The FBS Core and gNB docker

container services were initialized and ensured the services were up and operational. The UE was then prompted by the higher-powered FBS to release its connection with the home network. The UE, upon seeing a stronger signal being emitted from the FBS, attempted to connect to the FBS. The RRC connection to the FBS was successful, and the protocol capture was recorded using the Wireshark tool.

The FBS Core configuration was also modified prior to test execution to include the test IMSI into the unified data management to allow the FBS to perform authentication. This additional modification in the FBS network configuration allowed the UE to proceed with the 5G UE authentication step after identity procedures and to observe the behavior of a 5G AKA encoded IMSI in the presence of random authentication vectors assigned by the FBS. As a result of these changes, the FBS 5G Core network then initiated authentication procedures to authenticate the UE, and the FBS network proceeded to send an authentication request using a 5G authentication challenge, as shown in Figure 37.

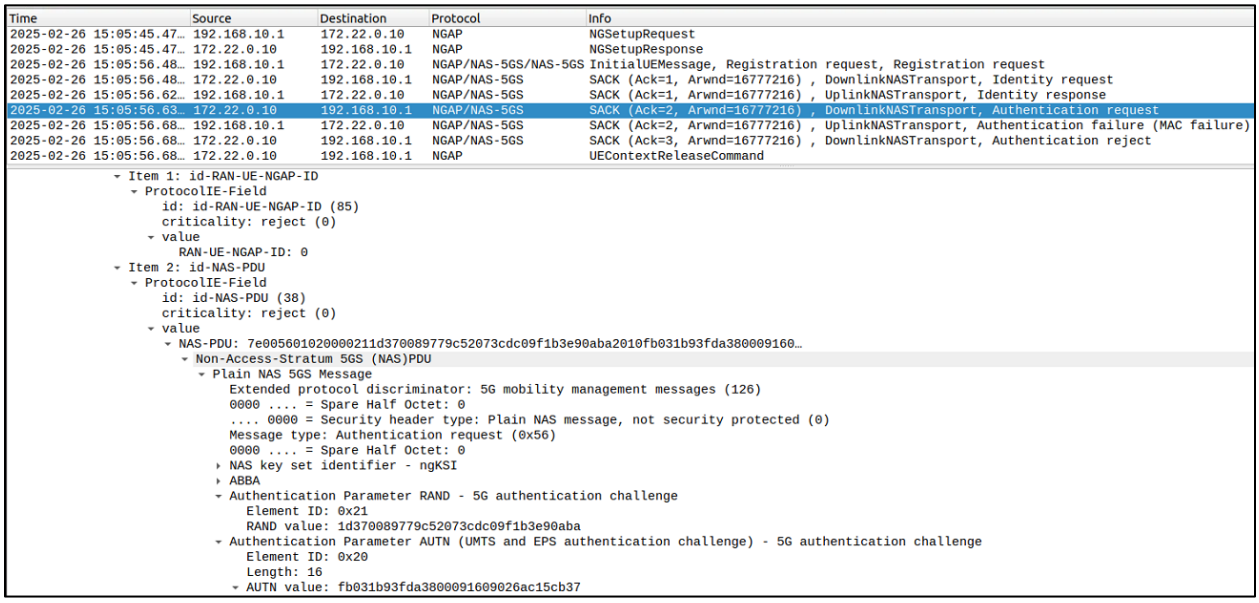


Figure 37: FBS 5G Core NAS Authentication Challenge

However, the 5G UE could not decode the authentication parameters, Random Number “RAND” and Authentication Token “AUTN” sent by the FBS network due to mismatched “K” and “OPc” values, resulting in a 5G authentication failure with 5GMM cause code #20 – “MAC Failure,” as shown in Figure 38. This 5GMM cause is sent to the network if the SIM detects that the Message Authentication Code (MAC) in the authentication request message is not fresh.

Key	Type	Time Stamp	Name	Summary
[0xB821]	OTA LOG	2025/02/26 20:06:32	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/26 20:06:32	NR5G RRC Configuration Info	Length: 168
[0xB823]	LOG	2025/02/26 20:06:32	NR5G RRC Serving Cell Info	Length: 62
[0xB821]	OTA LOG	2025/02/26 20:06:32	UL_CCCH / RRC Reestablishment Req	UL_CCCH / RRC Reestablishment Req
[0xB821]	OTA LOG	2025/02/26 20:06:32	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB80C]	LOG	2025/02/26 20:06:32	NR5G NAS MM5G State	Length: 42
[0xB80B]	OTA LOG	2025/02/26 20:06:32	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/26 20:06:32	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 82
[0xB825]	LOG	2025/02/26 20:06:32	NR5G RRC Configuration Info	Length: 132
[0xB80C]	LOG	2025/02/26 20:06:32	NR5G NAS MM5G State	Length: 42
[0xB814]	OTA LOG	2025/02/26 20:06:32	NR5G NAS Plain Message Container	Length: 79
[0xB80B]	OTA LOG	2025/02/26 20:06:32	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/26 20:06:32	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 110
[0xB821]	OTA LOG	2025/02/26 20:06:32	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/26 20:06:32	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/26 20:06:32	Identity request	Identity request
[0xB80B]	OTA LOG	2025/02/26 20:06:32	Identity response	Identity response
[0xB809]	OTA LOG	2025/02/26 20:06:32	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 89
[0xB821]	OTA LOG	2025/02/26 20:06:32	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/26 20:06:32	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/26 20:06:32	Authentication req	Authentication req
[0xB80B]	OTA LOG	2025/02/26 20:06:32	Authentication failure	Authentication failure
[0xB809]	OTA LOG	2025/02/26 20:06:32	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 34
[0xB821]	OTA LOG	2025/02/26 20:06:32	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/26 20:06:32	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/26 20:06:32	Authentication reject	Authentication reject
[0xB821]	OTA LOG	2025/02/26 20:06:32	DL_DCCH / RRC Release	DL_DCCH / RRC Release

```
98 01 00 00 01 (
BE 18 1F 31 EB 9
00 59 14
```

```
20:06:32.038911 [0xB80B] Authentication failure
pkt_version = 1 (0x1)
rel_number = 15 (0xf)
rel_version_major = 4 (0x4)
rel_version_minor = 0 (0x0)
prot_disc_type = 14 (0xe)
ext_protocol_disc = 126 (0x7e)
security_header = 0 (0x0)
msg_type = 89 (0x59) (authentication failure)
nr5g_mm_msg
  auth_failure
    5gmm_cause = 20 (0x14) (MAC failure)
```

Figure 38: UE NAS Authentication Failure (UE QXDM Log)

The authentication procedure was rejected by the FBS network, as expected (Figure 39), followed by the context release message. The UE was then turned OFF, and logs were captured for each of the interfaces demonstrating the test case behavior.

Time	Source	Destination	Protocol	Info
2025-02-26 15:05:45.47…	192.168.10.1	172.22.0.10	NGAP	NGSetupRequest
2025-02-26 15:05:45.47…	172.22.0.10	192.168.10.1	NGAP	NGSetupResponse
2025-02-26 15:05:56.48…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS/NAS-5GS	InitialUEMessage, Registration request, Registration request
2025-02-26 15:05:56.48…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , DownlinkNASTransport, Identity request
2025-02-26 15:05:56.62…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , UplinkNASTransport, Identity response
2025-02-26 15:05:56.63…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=16777216) , DownlinkNASTransport, Authentication request
2025-02-26 15:05:56.68…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=16777216) , UplinkNASTransport, Authentication failure (MAC failure)
2025-02-26 15:05:56.68…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=3, Arwnd=16777216) , DownlinkNASTransport, Authentication reject
2025-02-26 15:05:56.68…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand

```
▾ value
    AMF-UE-NGAP-ID: 1
▾ Item 1: id-RAN-UE-NGAP-ID
  ▾ ProtocolIE-Field
      id: id-RAN-UE-NGAP-ID (85)
      criticality: reject (0)
    ▾ value
        RAN-UE-NGAP-ID: 0
▾ Item 2: id-NAS-PDU
  ▾ ProtocolIE-Field
      id: id-NAS-PDU (38)
      criticality: reject (0)
    ▾ value
      ▾ NAS-PDU: 7e0058
        ▾ Non-Access-Stratum 5GS (NAS)PDU
          ▾ Plain NAS 5GS Message
              Extended protocol discriminator: 5G mobility management messages (126)
              0000 .... = Spare Half Octet: 0
              .... 0000 = Security header type: Plain NAS message, not security protected (0)
              Message type: Authentication reject (0x58)
```

Figure 39: UE NAS Authentication Rejection (FBS Wireshark Trace)

4.2 Null Encryption Test Results

The test results for the Null encryption SIM were similar to the results demonstrated in Section 4.1 above with the 5G AKA SIM. As described and performed in TC 2, the 5G test UE initially established a connection and properly authenticated with the home network. For this TC 4, the test IMSI was added to the FBS Core network subscriber profile with random subscription key "K" and Operator code "OPc" values. Note that as the Null encryption SIM does not use any encryption for subscriber identity, there was no modification required on the FBS Core network to modify the SUPI encryption. The UE was then prompted by the higher-powered FBS to release its connection to home network. The UE, upon seeing a stronger signal being emitted from the FBS, attempted to connect to the FBS. The RRC connection to the FBS was successful, and the protocol capture was recorded using the Wireshark tool.

As per the NAS registration process, the FBS and UE performed identity request and identity response procedures, respectively. The FBS then initiated authentication procedures to authenticate the UE, and the FBS network proceeded to send an 'authentication request' using 5G authentication challenge as shown in Figure 40.

However, the 5G UE could not decode the authentication parameters "RAND" and "AUTN" sent by the FBS network due to mismatched "K" and "OPc" values resulting in 5G authentication failure with 5GMM cause code #20 – "MAC Failure" as shown in Figure 41. As discussed in Section 4.1, this 5GMM cause is sent to the network if the SIM detects that the MAC in the authentication request message is not fresh.

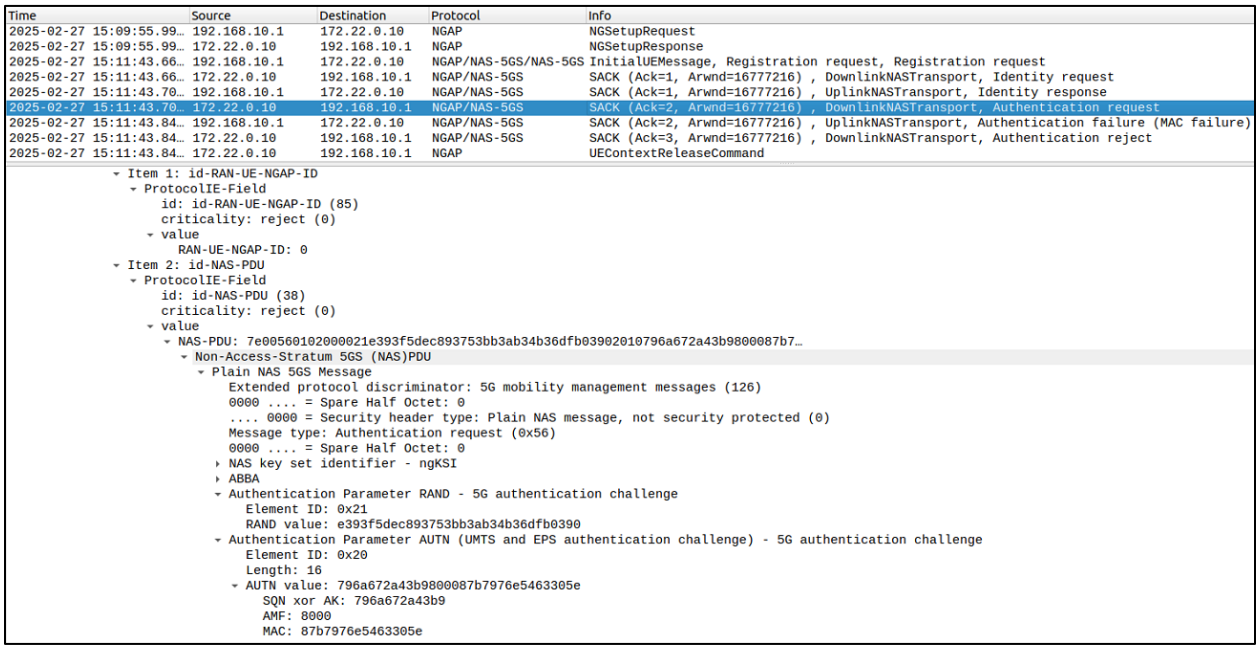


Figure 40: FBS 5G Core NAS Authentication Challenge

Key	Type	Time Stamp	Name	Summary
[0xB821]	OTA LOG	2025/02/27 20:12:19	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/27 20:12:19	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/27 20:12:19	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/27 20:12:19	NR5G NAS MM5G State	Length: 42
[0xB814]	OTA LOG	2025/02/27 20:12:19	NR5G NAS Plain Message Container	Length: 75
[0xB80B]	OTA LOG	2025/02/27 20:12:19	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/27 20:12:19	NR5G NAS MM5G Security Protected OTA ...	Length: 106
[0xB821]	OTA LOG	2025/02/27 20:12:19	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/27 20:12:19	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/27 20:12:19	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 20:12:19	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/27 20:12:19	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/27 20:12:19	Identity request	Identity request
[0xB80B]	OTA LOG	2025/02/27 20:12:19	Identity response	Identity response
[0xB809]	OTA LOG	2025/02/27 20:12:19	NR5G NAS MM5G Security Protected OTA ...	Length: 48
[0xB821]	OTA LOG	2025/02/27 20:12:19	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/27 20:12:19	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/27 20:12:19	Authentication req	Authentication req
[0xB80B]	OTA LOG	2025/02/27 20:12:19	Authentication failure	Authentication failure
[0xB809]	OTA LOG	2025/02/27 20:12:19	NR5G NAS MM5G Security Protected OTA ...	Length: 34
[0xB821]	OTA LOG	2025/02/27 20:12:19	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/27 20:12:19	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/27 20:12:19	Authentication reject	Authentication reject
[0xB821]	OTA LOG	2025/02/27 20:12:19	DL_DCCH / RRC Release	DL_DCCH / RRC Release

```
98 01 00 00 01 00 00 00 10 00 17 00 17
A7 69 70 1E 0E 60 09 01 01 00 00 00 0F
00 59 14
```

```
2025/02/27 20:12:19 [0xB80B] Authentication failure
pkt_version = 1 (0x1)
rel_number = 15 (0xf)
rel_version_major = 4 (0x4)
rel_version_minor = 0 (0x0)
prot_disc_type = 14 (0xe)
ext_protocol_disc = 126 (0x7e)
security_header = 0 (0x0)
msg_type = 89 (0x59) (authentication failure)
nr5g_mm_msg
  auth_failure
    _5gmm_cause = 20 (0x14) (MAC failure)
    auth_fail_param_incl = 0 (0x0)
```

Figure 41: UE NAS Authentication Failure (UE QXDM Log)

The authentication procedure was rejected by the FBS network as expected (Figure 42), followed by the context release message. The UE was then turned OFF, and logs were captured for each of the interfaces demonstrating the test case behavior.

Time	Source	Destination	Protocol	Info
2025-02-27 15:09:55.99…	192.168.10.1	172.22.0.10	NGAP	NGSetupRequest
2025-02-27 15:09:55.99…	172.22.0.10	192.168.10.1	NGAP	NGSetupResponse
2025-02-27 15:11:43.66…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS/NAS-5GS	InitialUEMessage, Registration request, Registration request
2025-02-27 15:11:43.66…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , DownlinkNASTransport, Identity request
2025-02-27 15:11:43.70…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , UplinkNASTransport, Identity response
2025-02-27 15:11:43.70…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=16777216) , DownlinkNASTransport, Authentication request
2025-02-27 15:11:43.84…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=16777216) , UplinkNASTransport, Authentication failure (MAC failure)
2025-02-27 15:11:43.84…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=3, Arwnd=16777216) , DownlinkNASTransport, Authentication reject
2025-02-27 15:11:43.84…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand

```
▾ ProtocolIE-Field
    id: id-AMF-UE-NGAP-ID (10)
    criticality: reject (0)
  ▾ value
      AMF-UE-NGAP-ID: 1
▾ Item 1: id-RAN-UE-NGAP-ID
  ▾ ProtocolIE-Field
    id: id-RAN-UE-NGAP-ID (85)
    criticality: reject (0)
  ▾ value
      RAN-UE-NGAP-ID: 0
▾ Item 2: id-NAS-PDU
  ▾ ProtocolIE-Field
    id: id-NAS-PDU (38)
    criticality: reject (0)
  ▾ value
    ▾ NAS-PDU: 7e0058
      ▾ Non-Access-Stratum 5GS (NAS)PDU
        ▾ Plain NAS 5GS Message
            Extended protocol discriminator: 5G mobility management messages (126)
            0000 .... = Spare Half Octet: 0
            .... 0000 = Security header type: Plain NAS message, not security protected (0)
            Message type: Authentication reject (0x58)
```

Figure 42: UE NAS Authentication Rejection (FBS Wireshark Trace)

4.3 Outcomes for Both 5G AKA and Null Encryption Tests

Expected Results:
The UE does not connect with the false base station. If the UE does connect, the UE rejects the authentication request.

Success Criteria:
The UE does not connect with the false base station. If the UE does connect, the UE rejects the authentication request.

Test Results:
The test results were successfully validated by observing that the UE rejects the authentication request and disconnects from the false base station as expected when the FBS attempts to authenticate UE using random authentication parameters.

Condition	Status
The UE does not connect with the false base station. If the UE does connect, the UE rejects the authentication request.	
Overall Test	Success

Test Case 5 – Attempting Authentication Handshake Using Replayed Credentials

Test Case ID: TC-FBS-5

Test Case Name: Attempting Authentication Handshake Using Replayed Credentials

Description:
This test case is designed to observe the UE's behavior when the false base station attempts to authenticate the UE using authentication credentials captured from a previous authentication between the UE and the home gNB. The primary goal of this test is to confirm that the UE will respond by rejecting the authentication request and disconnecting from the false base station.

Objectives:

- Demonstrate that a UE attached to its home network is forced to disconnect home network, establishes an RRC connection to a higher-powered FBS, and rejects NAS authentication to an FBS network configured with the same authentication credentials as used by the home network.

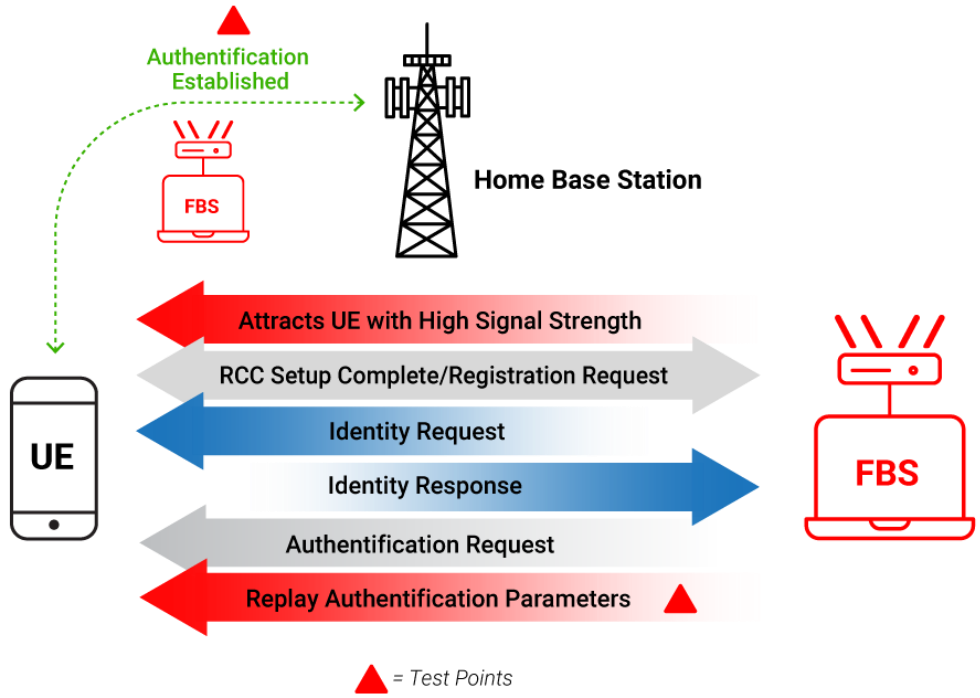


Figure 43: FBS Authentication Request with UE Using Replayed Credentials with Home Radio Base Station

5.1 5G AKA Test Results

As described and performed in TC 2, the 5G test UE initially established a connection and properly authenticated with the home network. As a prerequisite to conduct TC 5, during this process, the test team initially used the Wireshark tool to record the authentication parameters “AUTN” and “RAND” between the UE and the home network as shown in Figure 44.

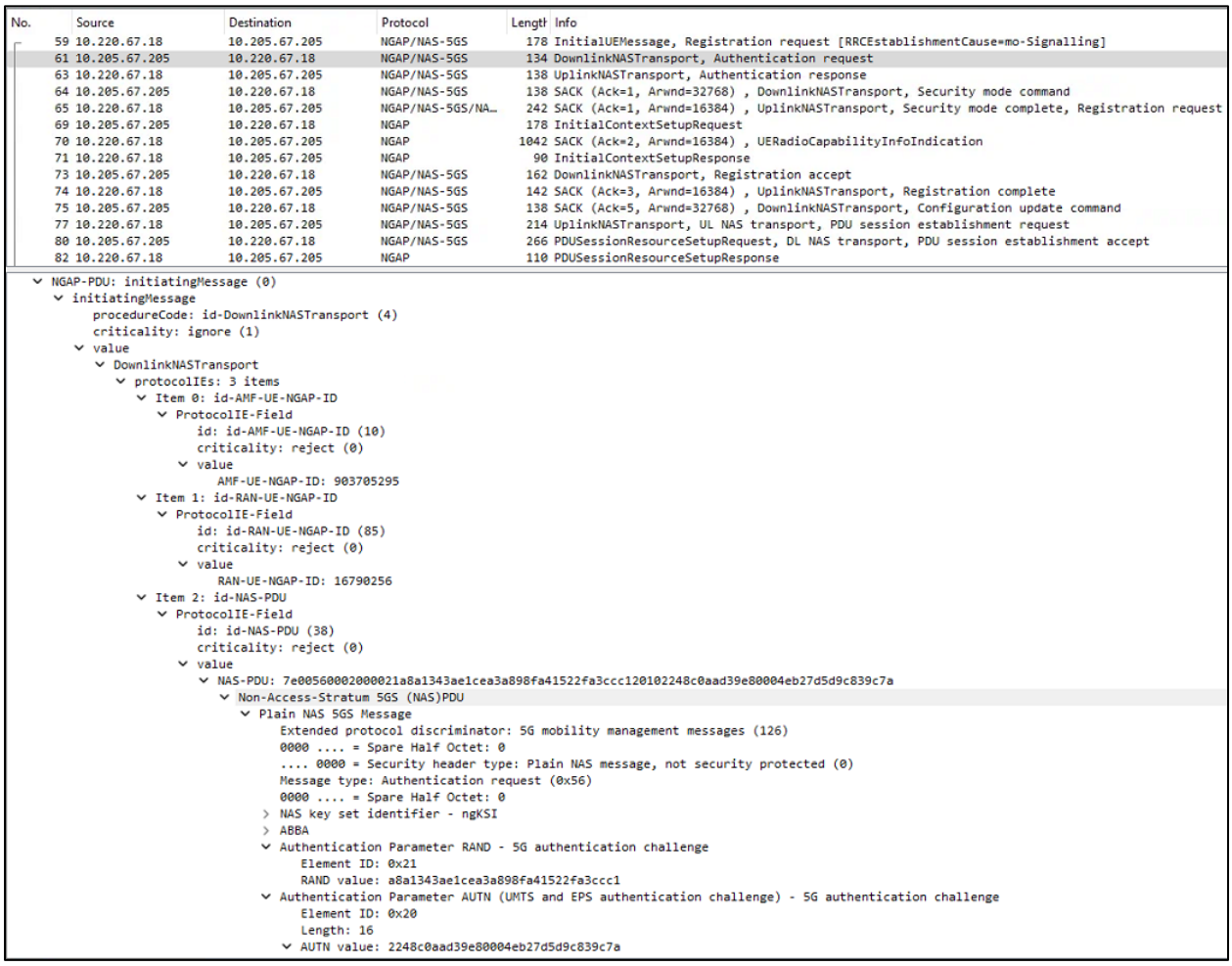


Figure 44: NAS Authentication Parameters “RAND” and “AUTN” Values Recorded During UE Registration with 5G Home Network

Similar to Test Case 4, the test 5G AKA IMSI was added to the FBS Core network subscriber profile with random subscription key “K” and Operator code “OPc” values. For this TC 5, the previously observed and recorded authentication parameters “AUTN” and “RAND” between the UE and home network were then used to update the FBS Core network’s unified data management (UDM) configuration as custom parameters. The FBS Core and gNB docker container services were initialized and the services were up and operational. The UE was then prompted by the higher-powered FBS to release its connection with the home gNB. The UE upon seeing a stronger signal being emitted from the FBS, attempted to connect to the FBS. The RRC connection to the FBS was successful, and the protocol capture was recorded using the Wireshark tool.

The FBS Core configuration was also modified prior to test execution to include the test IMSI into the unified data management to allow the FBS to perform authentication. This additional modification in the FBS network configuration allowed the UE to proceed with the 5G UE authentication step after identity procedures and to observe the behavior of a 5G AKA encoded IMSI in the presence of replayed authentication vectors assigned by the FBS. As a result of these changes, the FBS 5G Core network then initiated authentication procedures to authenticate the UE and replayed the recorded "RAND" and "AUTN" values to perform 5G authentication challenge as shown in Figure 45. Note the "RAND" and "AUTN" values used by FBS in Figure 45 are same as "RAND" and "AUTN" values shown in Figure 44.

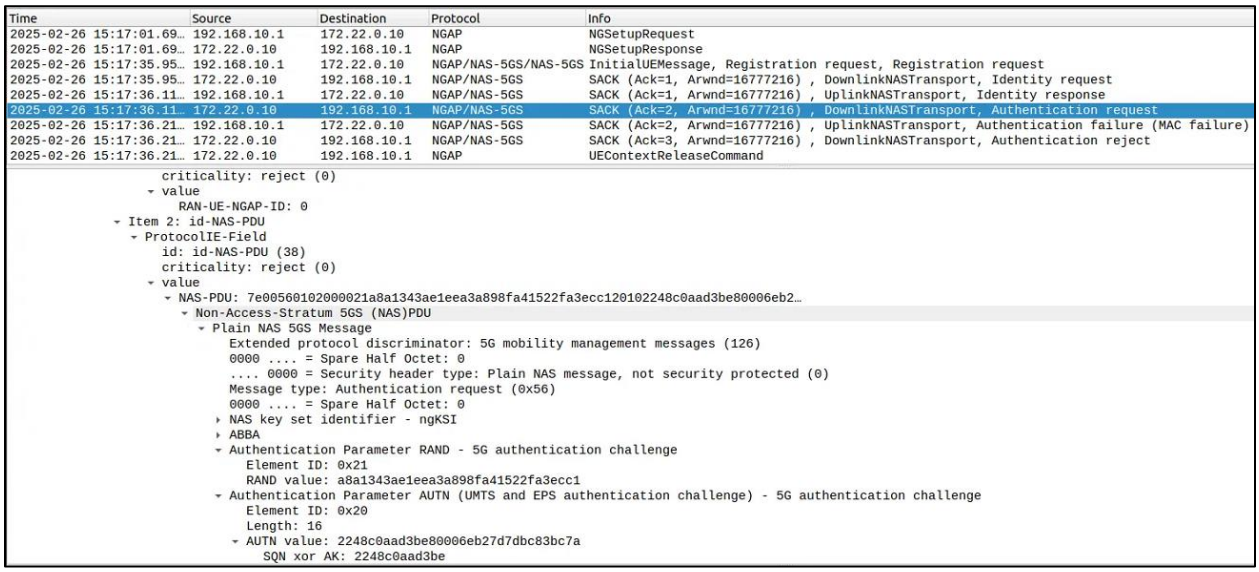


Figure 45: FBS 5G Core NAS Authentication Challenge Using Replayed Authentication Vectors

However, the 5G UE could not decode the authentication parameters "RAND" and "AUTN" sent by the FBS network due to mismatched "K" and "OPc" values resulting in 5G authentication failure with 5GMM cause code #20 – "MAC Failure," as shown in Figure 45.

The authentication procedure was rejected by the FBS network as expected (Figure 47), followed by the context release message. The UE was then turned OFF, and the test team captured logs for each of the interfaces demonstrating the test case behavior.

Key	Type	Time Stamp	Name	Summary
[0xB821]	OTA LOG	2025/02/26 20:18:11	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/26 20:18:11	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/26 20:18:11	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/26 20:18:11	NR5G NAS MM5G State	Length: 42
[0xB814]	OTA LOG	2025/02/26 20:18:11	NR5G NAS Plain Message Container	Length: 75
[0xB80B]	OTA LOG	2025/02/26 20:18:11	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/26 20:18:11	NR5G NAS MM5G Security Protected OTA ...	Length: 106
[0xB821]	OTA LOG	2025/02/26 20:18:11	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/26 20:18:11	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/26 20:18:11	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/26 20:18:11	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/26 20:18:11	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/26 20:18:11	Identity request	Identity request
[0xB80B]	OTA LOG	2025/02/26 20:18:11	Identity response	Identity response
[0xB809]	OTA LOG	2025/02/26 20:18:11	NR5G NAS MM5G Security Protected OTA ...	Length: 89
[0xB821]	OTA LOG	2025/02/26 20:18:11	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB822]	LOG	2025/02/26 20:18:11	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 20:18:11	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB822]	LOG	2025/02/26 20:18:11	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 20:18:11	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/26 20:18:11	Authentication req	Authentication req
[0xB80B]	OTA LOG	2025/02/26 20:18:12	Authentication failure	Authentication failure
[0xB809]	OTA LOG	2025/02/26 20:18:12	NR5G NAS MM5G Security Protected OTA ...	Length: 34
[0xB821]	OTA LOG	2025/02/26 20:18:12	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/26 20:18:12	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/26 20:18:12	Authentication reject	Authentication reject
[0xB821]	OTA LOG	2025/02/26 20:18:12	DL_DCCH / RRC Release	DL_DCCH / RRC Release

```
98 01 00 0C
8B 52 03 BE
00 59 14
```

```
2025/02/26 20:18:12 [0xB80B] Authentication failure
pkt_version = 1 (0x1)
rel_number = 15 (0xf)
rel_version_major = 4 (0x4)
rel_version_minor = 0 (0x0)
prot_disc_type = 14 (0xe)
ext_protocol_disc = 126 (0x7e)
security_header = 0 (0x0)
msg_type = 89 (0x59) (authentication failure)
nr5g_mm_msg
  auth_failure
    _5gmm_cause = 20 (0x14) (MAC failure)
```

Figure 46: UE NAS Authentication Failure (UE QXDM Log)

Time	Source	Destination	Protocol	Info
2025-02-26 15:17:01.69…	192.168.10.1	172.22.0.10	NGAP	NGSetupRequest
2025-02-26 15:17:01.69…	172.22.0.10	192.168.10.1	NGAP	NGSetupResponse
2025-02-26 15:17:35.95…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS/NAS-5GS	InitialUEMessage, Registration request, Registration request
2025-02-26 15:17:35.95…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , DownlinkNASTransport, Identity request
2025-02-26 15:17:36.11…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , UplinkNASTransport, Identity response
2025-02-26 15:17:36.11…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=16777216) , DownlinkNASTransport, Authentication request
2025-02-26 15:17:36.21…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=16777216) , UplinkNASTransport, Authentication failure (MAC failure)
2025-02-26 15:17:36.21…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=3, Arwnd=16777216) , DownlinkNASTransport, Authentication reject
2025-02-26 15:17:36.21…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand

```
▾ protocolIEs: 3 items
  ▾ Item 0: id-AMF-UE-NGAP-ID
    ▾ ProtocolIE-Field
        id: id-AMF-UE-NGAP-ID (10)
        criticality: reject (0)
      ▾ value
          AMF-UE-NGAP-ID: 1
  ▾ Item 1: id-RAN-UE-NGAP-ID
    ▾ ProtocolIE-Field
        id: id-RAN-UE-NGAP-ID (85)
        criticality: reject (0)
      ▾ value
          RAN-UE-NGAP-ID: 0
  ▾ Item 2: id-NAS-PDU
    ▾ ProtocolIE-Field
        id: id-NAS-PDU (38)
        criticality: reject (0)
      ▾ value
        ▾ NAS-PDU: 7e0058
          ▾ Non-Access-Stratum 5GS (NAS)PDU
            ▾ Plain NAS 5GS Message
                Extended protocol discriminator: 5G mobility management messages (126)
                0000 .... = Spare Half Octet: 0
                .... 0000 = Security header type: Plain NAS message, not security protected (0)
                Message type: Authentication reject (0x58)
```

Figure 47: UE NAS Authentication Rejection (FBS Wireshark Trace)

5.2 Null Encryption Test Results

The test results for Null encryption SIM were similar to the results demonstrated above in Section 5.1 with the 5G AKA SIM. As described and performed in TC 2, the 5G test UE initially established a connection and properly authenticated with the home network. As a prerequisite to conduct Test Case 5, during this process, the test team used the Wireshark tool to record the authentication parameters “AUTN” and “RAND” between the UE and the home network as shown in Figure 48.

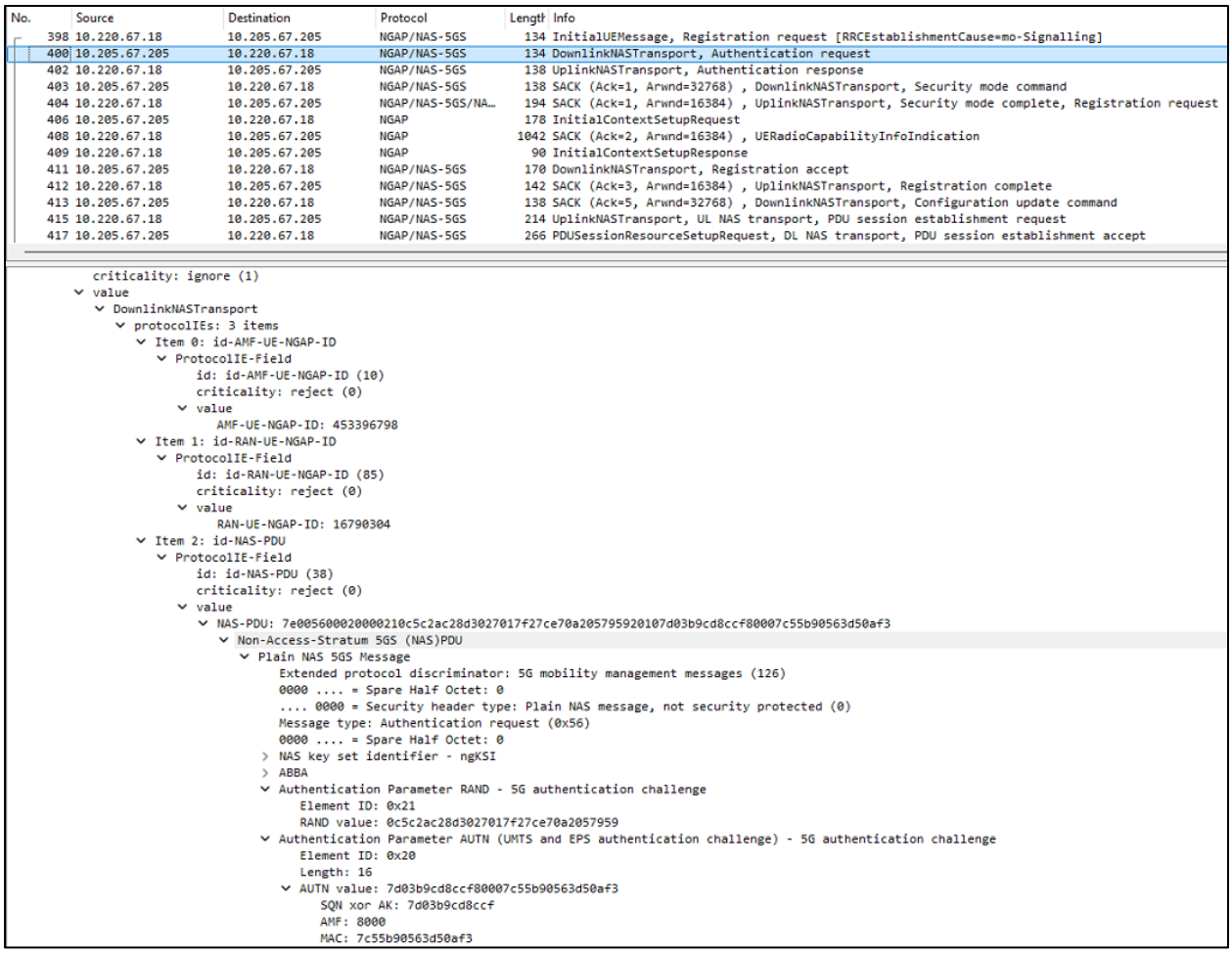


Figure 48: NAS Authentication Parameters “RAND” and “AUTN” Values Recorded During UE Registration with 5G Home Network

For Test Case 5, the test 5G Null IMSI was added to the FBS Core network subscriber profile with random subscription key “K” and Operator code “OPc” values. Note that as the null encryption SIM does not use any encryption for subscriber identity, there was no modification required on the FBS Core network to modify the SUPI encryption. Again, the previously observed and recorded authentication parameters “AUTN” and “RAND” between the UE and home network were then used to update the FBS Core network’s unified data management (UDM) configuration as custom parameters. The FBS Core and gNB docker container services were initialized, and the services were up and operational. The UE was then prompted by the higher-powered FBS to

release its connection with the home network. The UE upon seeing a stronger signal being emitted from the FBS, attempted to connect to the FBS. The RRC connection to the FBS was successful, and the protocol capture was recorded using the Wireshark tool.

As per the NAS registration process, the FBS and UE performed identity request and identity response procedures, respectively. The FBS 5G Core network then initiated authentication procedures to authenticate the UE and replayed the recorded “RAND” and “AUTN” values to perform 5G authentication challenge as shown in Figure 49. Note the “RAND” and “AUTN” values used by FBS in Figure 45 are same as “RAND” and “AUTN” values shown in Figure 48.

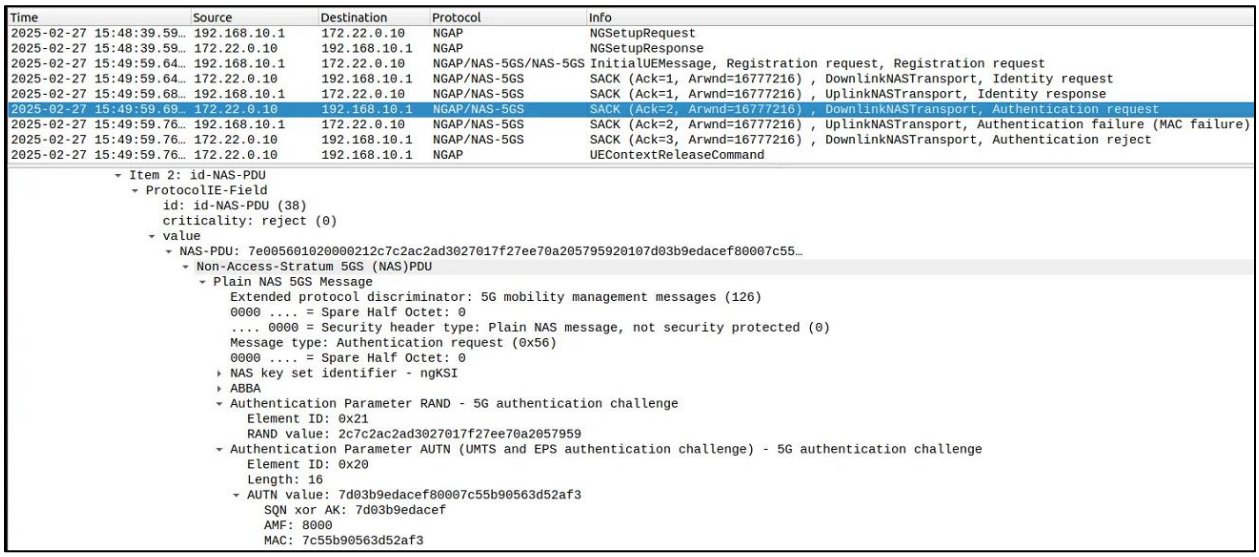


Figure 49: FBS 5G Core NAS Authentication Challenge Using Replayed Authentication Vectors

However, the UE could not decode the authentication parameters “RAND” and “AUTN” sent by the FBS network due to mismatched “K” and “OPc” values resulting in 5G authentication failure with 5GMM cause code #20 – “MAC Failure” as shown in Figure 50.

Key	Type	Time Stamp	Name	Summary
[0xB821]	OTA LOG	2025/02/27 20:50:35	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/27 20:50:35	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/27 20:50:35	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/27 20:50:35	NR5G NAS MM5G State	Length: 42
[0xB814]	OTA LOG	2025/02/27 20:50:35	NR5G NAS Plain Message Container	Length: 75
[0xB80B]	OTA LOG	2025/02/27 20:50:35	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/27 20:50:35	NR5G NAS MM5G Security Protected OTA Outgoing ...	Length: 106
[0xB821]	OTA LOG	2025/02/27 20:50:35	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/27 20:50:35	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/27 20:50:35	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 20:50:35	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/27 20:50:35	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/27 20:50:35	Identity request	Identity request
[0xB80B]	OTA LOG	2025/02/27 20:50:35	Identity response	Identity response
[0xB809]	OTA LOG	2025/02/27 20:50:35	NR5G NAS MM5G Security Protected OTA Outgoing ...	Length: 48
[0xB821]	OTA LOG	2025/02/27 20:50:35	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/27 20:50:35	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/27 20:50:35	Authentication req	Authentication req
[0xB80B]	OTA LOG	2025/02/27 20:50:35	Authentication failure	Authentication failure
[0xB809]	OTA LOG	2025/02/27 20:50:35	NR5G NAS MM5G Security Protected OTA Outgoing ...	Length: 34
[0xB821]	OTA LOG	2025/02/27 20:50:35	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/27 20:50:35	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/27 20:50:35	Authentication reject	Authentication reject

```
98 01 00 00
E7 96 61 25
00 59 14
```

```
2025/02/27 20:50:35 [0xB80B] Authentication failure
pkt_version = 1 (0x1)
rel_number = 15 (0xf)
rel_version_major = 4 (0x4)
rel_version_minor = 0 (0x0)
prot_disc_type = 14 (0xe)
ext_protocol_disc = 126 (0x7e)
security_header = 0 (0x0)
msg_type = 89 (0x59) (authentication failure)
nr5g_mm_msg
  auth_failure
    _5gmm_cause = 20 (0x14) (MAC failure)
    auth_fail_param_incl = 0 (0x0)
```

Figure 50: UE NAS Authentication Failure (UE QXDM Log)

The authentication procedure was rejected as expected (Figure 51), and the network sent the context release message to the UE. The UE was then turned OFF, and logs were captured for each of the interfaces demonstrating the test case behavior.

Time	Source	Destination	Protocol	Info
2025-02-27 15:48:39.59…	192.168.10.1	172.22.0.10	NGAP	NGSetupRequest
2025-02-27 15:48:39.59…	172.22.0.10	192.168.10.1	NGAP	NGSetupResponse
2025-02-27 15:49:59.64…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS/NAS-5GS	InitialUEMessage, Registration request, Registration request
2025-02-27 15:49:59.64…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , DownlinkNASTransport, Identity request
2025-02-27 15:49:59.68…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , UplinkNASTransport, Identity response
2025-02-27 15:49:59.69…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=16777216) , DownlinkNASTransport, Authentication request
2025-02-27 15:49:59.76…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	SACK (Ack=2, Arwnd=16777216) , UplinkNASTransport, Authentication failure (MAC failure)
2025-02-27 15:49:59.76…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=3, Arwnd=16777216) , DownlinkNASTransport, Authentication reject
2025-02-27 15:49:59.76…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand

```
▾ protocolIEs: 3 items
  ▾ Item 0: id-AMF-UE-NGAP-ID
    ▾ ProtocolIE-Field
        id: id-AMF-UE-NGAP-ID (10)
        criticality: reject (0)
      ▾ value
          AMF-UE-NGAP-ID: 1
  ▾ Item 1: id-RAN-UE-NGAP-ID
    ▾ ProtocolIE-Field
        id: id-RAN-UE-NGAP-ID (85)
        criticality: reject (0)
      ▾ value
          RAN-UE-NGAP-ID: 0
  ▾ Item 2: id-NAS-PDU
    ▾ ProtocolIE-Field
        id: id-NAS-PDU (38)
        criticality: reject (0)
      ▾ value
        ▾ NAS-PDU: 7e0058
          ▾ Non-Access-Stratum 5GS (NAS)PDU
            ▾ Plain NAS 5GS Message
                Extended protocol discriminator: 5G mobility management messages (126)
                0000 .... = Spare Half Octet: 0
                .... 0000 = Security header type: Plain NAS message, not security protected (0)
                Message type: Authentication reject (0x58)
```

Figure 51: UE NAS Authentication Rejection (FBS Wireshark Trace)

5.3 Outcomes for Both 5G AKA and Null Encryption Tests

Expected Results:
UE does not connect with FBS. If UE does connect, UE rejects authentication request.

Success Criteria:
UE does not connect with FBS. If UE does connect, UE rejects authentication request.

Test Results:
The test results were successfully validated by observing that the UE rejects the authentication request and disconnects from the FBS as expected when the FBS attempts to authenticate the UE using replayed authentication credentials (previously recorded authentication parameters between the UE and the home network).

Condition	Status
The UE does not connect with FBS. If the UE does connect, the UE rejects the authentication request.	
Overall Test	Success

Test Case 6 – Conducting DoS Attack Using a "5GS Services Not Allowed" Message

Test Case ID: TC-FBS-6

Test Case Name: Conducting DoS Attack Using "5GS Services Not Allowed" Message

Description:
This test case is designed to observe false base station attempts to prevent the UE from reconnecting with its home radio base station by rejecting the UE's RRMU (Registration Request of type "Mobility Update") NAS message with a "5GS Services Not Allowed" message.[ii] The primary goal of this test is to confirm that the UE will respond by ignoring the RRMU reject message and reconnecting to its home radio base station.

Objectives:

- Configure the false base station to send a registration reject NAS message to the UE with NAS reject cause "5GS Services Not Allowed."
- Observe the UE behavior and see if the UE ignores the FBS message and reconnects to the home radio base station.
- Verify if any at any stage the UE is vulnerable to the Denial-of-Service attack.

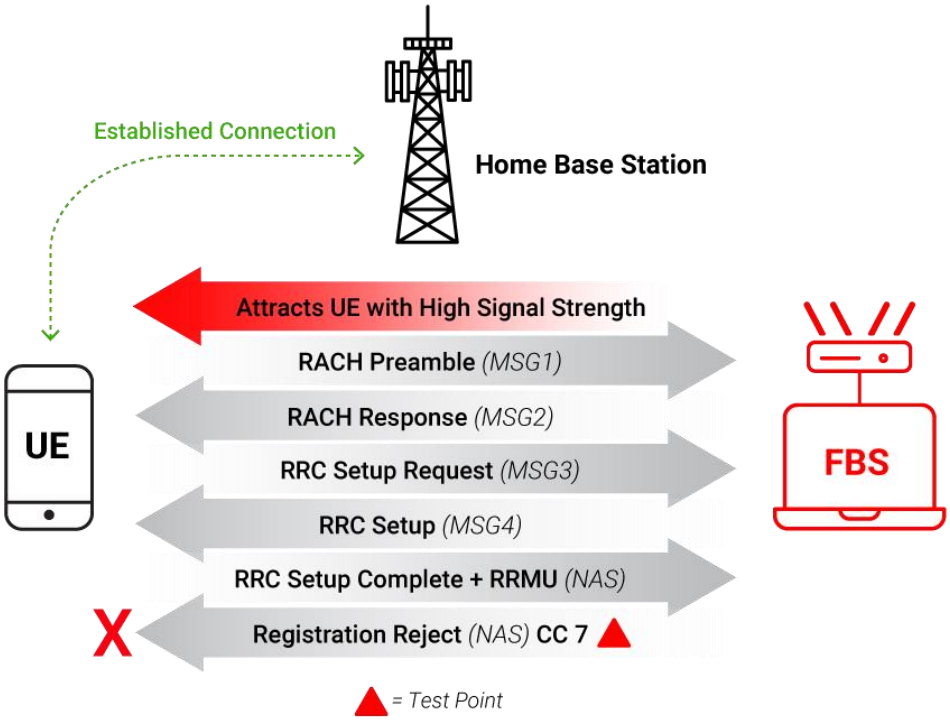


Figure 52: FBS with Different TA Sends NAS Registration Reject to Deny UE of Any 5G Service

6.1 5G AKA Test Results

As described and performed in Test Case 2, the 5G test UE initially established a connection and properly authenticated with the home network. The test IMSI remained added to the FBS Core network subscriber profile with random subscription key "K" and Operator code "OPc" values. For this Test Case 6, the FBS Core configuration was modified to include the NAS registration reject message with cause value #7 – "5GS Services Not Allowed." The FBS Core and gNB docker container services were initialized and ensured the services were up and operational. The UE was then prompted by the higher-powered FBS to release its connection with the home network. The UE, upon seeing a stronger signal being emitted from the FBS, attempted to connect to the FBS. The RRC connection to the FBS was successful, and the protocol capture was recorded using the Wireshark tool.

Once the RRC connection was established, the UE sent a mobility update registration request to register to the FBS Core network using the 5G-GUTI previously assigned by the 5G home network. Upon receiving the mobility update registration request from the UE, the FBS Core network immediately sent a registration reject message to the UE with the cause code value #7 – "5GS Services Not Allowed," as shown in Figure 53 and Figure 54. This 5GMM cause is sent to the UE when it is not allowed to operate 5GS services.

Key	Type	Time Stamp	Name	Summary
[0xB822]	LOG	2025/02/26 18:50:16	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 18:50:16	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/26 18:50:16	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/26 18:50:16	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/26 18:50:16	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/26 18:50:16	NR5G NAS MM5G State	Length: 42
[0xB814]	OTA LOG	2025/02/26 18:50:16	NR5G NAS Plain Message Container	Length: 75
[0xB80B]	OTA LOG	2025/02/26 18:50:16	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/26 18:50:16	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 106
[0xB821]	OTA LOG	2025/02/26 18:50:16	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/26 18:50:16	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/26 18:50:16	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/26 18:50:16	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/26 18:50:16	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/26 18:50:16	Registration reject	Registration reject
[0xB821]	OTA LOG	2025/02/26 18:50:16	DL_DCCH / RRC Release	DL_DCCH / RRC Release

```
98 01 00 00 01 00 0
48 38 1A 56 B3 5B 0
00 44 07
```

```
2025/02/26 18:50:16 [0xB80A] Registration reject
pkt_version = 1 (0x1)
rel_number = 15 (0xf)
rel_version_major = 4 (0x4)
rel_version_minor = 0 (0x0)
prot_disc_type = 14 (0xe)
ext_protocol_disc = 126 (0x7e)
security_header = 0 (0x0)
msg_type = 68 (0x44) (Registration reject)
nr5g_mm_msg
  registration_reject
    _5gmm_cause = 7 (0x7) (5GS Service not allowed)
    t3346_incl = 0 (0x0)
```

Figure 53: FBS NAS Registration Rejection (UE QXDM Log)

```
Time                        Source          Destination     Protocol                Info
2025-02-26 13:46:55.86…     192.168.10.1    172.22.0.10     NGAP                    NGSetupRequest
2025-02-26 13:46:55.86…     172.22.0.10     192.168.10.1    NGAP                    NGSetupResponse
2025-02-26 13:49:40.96…     192.168.10.1    172.22.0.10     NGAP/NAS-5GS/NAS-5GS    InitialUEMessage, Registration request, Registration request
2025-02-26 13:49:40.96…     172.22.0.10     192.168.10.1    NGAP/NAS-5GS            SACK (Ack=1, Arwnd=16777216) , DownlinkNASTransport, Registration reject (5GS services not allowed)
2025-02-26 13:49:40.96…     172.22.0.10     192.168.10.1    NGAP                    UEContextReleaseCommand
2025-02-26 13:49:41.12…     192.168.10.1    172.22.0.10     NGAP                    UEContextReleaseComplete

        ▾ ProtocolIE-Field
            id: id-AMF-UE-NGAP-ID (10)
            criticality: reject (0)
          ▾ value
              AMF-UE-NGAP-ID: 1
      ▾ Item 1: id-RAN-UE-NGAP-ID
        ▾ ProtocolIE-Field
            id: id-RAN-UE-NGAP-ID (85)
            criticality: reject (0)
          ▾ value
              RAN-UE-NGAP-ID: 0
      ▾ Item 2: id-NAS-PDU
        ▾ ProtocolIE-Field
            id: id-NAS-PDU (38)
            criticality: reject (0)
          ▾ value
            ▾ NAS-PDU: 7e004407
              ▾ Non-Access-Stratum 5GS (NAS)PDU
                ▾ Plain NAS 5GS Message
                    Extended protocol discriminator: 5G mobility management messages (126)
                    0000 .... = Spare Half Octet: 0
                    .... 0000 = Security header type: Plain NAS message, not security protected (0)
                    Message type: Registration reject (0x44)
                  ▾ 5GMM cause
                      5GMM cause: 5GS services not allowed (7)
```

Figure 54: FBS NAS Registration Rejection (FBS Wireshark Trace)

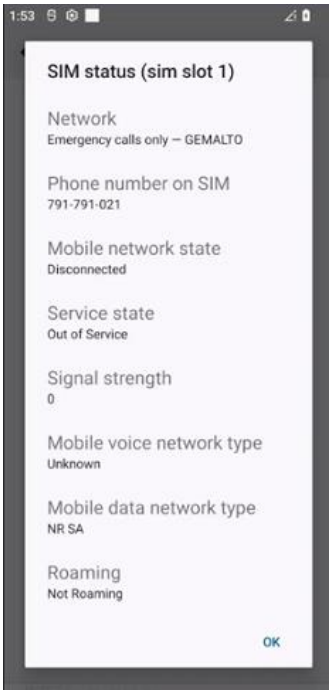


Figure 55: UE in "Out of Service" State

The FBS then sent a UE context release message to the UE and the registration process was terminated. The FBS Core and RAN services was then turned OFF. Upon disconnecting from the FBS network, the UE received SIB 1 message from the 5G home network and attempted to reconnect to the home network, however, the UE failed to connect to its 5G home RAN network as shown in Figure 56. As per snapshot shown in Figure 55, UE entered an "Out of Service" state and remained deregistered from any network.

This test case's results demonstrate that a UE is vulnerable to a DoS attack if a false base station attempts to attract a UE and then force it to reject registration by preventing access to 5GS services. Due to this behavior, the test team toggled the UE into Airplane Mode, after which it was able to register properly with its home radio base station. The test team captured logs for each of the interfaces demonstrating the test case behavior.

Key	Type	Time Stamp	Name	Summary
[0xB80A]	OTA LOG	2025/02/26 18:50:16	Registration reject	Registration reject
[0xB821]	OTA LOG	2025/02/26 18:50:16	DL_DCCH / RRC Release	DL_DCCH / RRC Release
[0xB80C]	LOG	2025/02/26 18:50:16	NR5G NAS MM5G State	Length: 42
[0xB825]	LOG	2025/02/26 18:50:16	NR5G RRC Configuration Info	Length: 87
[0xB80D]	LOG	2025/02/26 18:50:16	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/26 18:50:16	NR5G NAS MM5G State	Length: 42
[0xB822]	LOG	2025/02/26 18:50:16	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 18:50:16	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB825]	LOG	2025/02/26 18:50:16	NR5G RRC Configuration Info	Length: 87
[0xB822]	LOG	2025/02/26 18:50:17	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 18:50:17	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/26 18:50:17	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/26 18:50:17	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/26 18:50:17	NR5G RRC Serving Cell Info	Length: 62
[0xB801]	OTA LOG	2025/02/26 18:50:17	PDU session establishment req	PDU session establishment req
[0xB80D]	LOG	2025/02/26 18:50:37	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/26 18:50:37	NR5G NAS MM5G State	Length: 42
[0xB825]	LOG	2025/02/26 18:50:37	NR5G RRC Configuration Info	Length: 87
[0xB822]	LOG	2025/02/26 18:50:38	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 18:50:38	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/26 18:50:38	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/26 18:50:38	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/26 18:50:38	NR5G RRC Serving Cell Info	Length: 62
[0xB825]	LOG	2025/02/26 18:54:42	NR5G RRC Configuration Info	Length: 87
[0xB80C]	LOG	2025/02/26 18:54:42	NR5G NAS MM5G State	Length: 42

Figure 56: UE Unable to Connect to 5G Home Network After RRC Release from FBS (UE QXDM Log)

6.2 Null Encryption Test Results

The test results for the Null encryption SIM were similar to the results demonstrated in Section 6.1 above with the 5G AKA SIM. As described and performed in Test Case 2, the 5G test UE initially established a connection and properly authenticated with the home network. The test IMSI remained added to the FBS Core network subscriber profile with random subscription key "K" and Operator code "OPc" values. Similar to Section 6.1, the FBS Core configuration was modified to include the NAS registration reject message with cause value #7 – "5GS Services Not Allowed." The FBS Core and gNB docker container services were initialized and ensured the services were up and operational. The UE was then prompted by the higher-powered FBS to release its connection with the home network. The UE upon seeing a stronger signal being emitted from the FBS, attempted to connect to FBS. The RRC connection to FBS was successful, and the protocol capture was recorded using the Wireshark tool.

Once the RRC connection was established, the UE sent a mobility update registration request to register to the FBS Core network using the 5G-GUTI previously assigned by the 5G home network. Upon receiving the mobility update registration request from the UE, the FBS Core network immediately sent a registration reject message to the UE with the cause code value #7 – "5GS services not allowed," as shown in Figure 57 and Figure 58. This 5GMM cause is sent to the UE when it is not allowed to operate 5GS services.

Key	Type	Time Stamp	Name	Summary
[0xB821]	OTA LOG	2025/02/27 21:00:34	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/27 21:00:34	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/27 21:00:34	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/27 21:00:34	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/27 21:00:34	NR5G NAS MM5G State	Length: 42
[0xB814]	OTA LOG	2025/02/27 21:00:34	NR5G NAS Plain Message Container	Length: 75
[0xB808]	OTA LOG	2025/02/27 21:00:34	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/27 21:00:34	NR5G NAS MM5G Security Protected OTA ...	Length: 106
[0xB821]	OTA LOG	2025/02/27 21:00:34	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/27 21:00:34	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/27 21:00:34	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 21:00:34	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/27 21:00:34	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/27 21:00:34	Registration reject	Registration reject
[0xB821]	OTA LOG	2025/02/27 21:00:34	DL_DCCH / RRC Release	DL_DCCH / RRC Release

```
98 01 00 00 01 00 00 0
CE 82 85 74 31 60 09 0
00 44 07
```

```
2025/02/27 21:00:34 [0xB80A] Registration reject
pkt_version = 1 (0x1)
rel_number = 15 (0xf)
rel_version_major = 4 (0x4)
rel_version_minor = 0 (0x0)
prot_disc_type = 14 (0xe)
ext_protocol_disc = 126 (0x7e)
security_header = 0 (0x0)
msg_type = 68 (0x44) (Registration reject)
nr5g_mm_msg
  registration_reject
    _5gmm_cause = 7 (0x7) (5GS Service not allowed)
    t3346 incl = 0 (0x0)
```

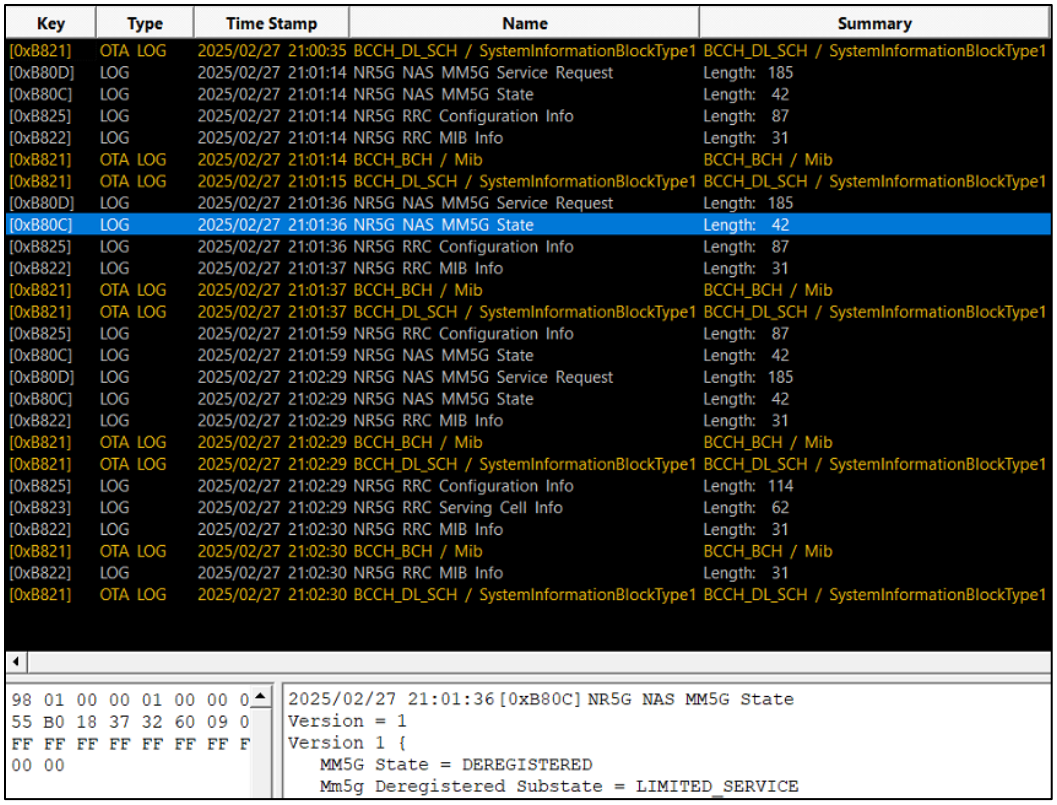
Figure 57: FBS NAS Registration Rejection (UE QXDM Log)

Time	Source	Destination	Protocol	Info
2025-02-27 15:58:54.53…	192.168.10.1	172.22.0.10	NGAP	NGSetupRequest
2025-02-27 15:58:54.53…	172.22.0.10	192.168.10.1	NGAP	NGSetupResponse
2025-02-27 15:59:58.49…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS/NAS-5GS	InitialUEMessage, Registration request, Registration request
2025-02-27 15:59:58.49…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , DownlinkNASTransport, Registration reject (5GS services not allowed)
2025-02-27 15:59:58.49…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-27 15:59:58.65…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete

```
▾ ProtocolIE-Field
    id: id-AMF-UE-NGAP-ID (10)
    criticality: reject (0)
  ▾ value
      AMF-UE-NGAP-ID: 1
▾ Item 1: id-RAN-UE-NGAP-ID
  ▾ ProtocolIE-Field
    id: id-RAN-UE-NGAP-ID (85)
    criticality: reject (0)
  ▾ value
      RAN-UE-NGAP-ID: 0
▾ Item 2: id-NAS-PDU
  ▾ ProtocolIE-Field
    id: id-NAS-PDU (38)
    criticality: reject (0)
  ▾ value
    ▾ NAS-PDU: 7e004407
      ▾ Non-Access-Stratum 5GS (NAS)PDU
        ▾ Plain NAS 5GS Message
            Extended protocol discriminator: 5G mobility management messages (126)
            0000 .... = Spare Half Octet: 0
            .... 0000 = Security header type: Plain NAS message, not security protected (0)
            Message type: Registration reject (0x44)
          ▾ 5GMM cause
              5GMM cause: 5GS services not allowed (7)
```

Figure 58: FBS NAS Registration Rejection (FBS Wireshark Trace)

The FBS then sent a UE context release message to the UE, and the registration process was terminated. The FBS Core and RAN services were then turned OFF. Upon disconnecting from the FBS network, the UE received SIB 1 message from the 5G home network and attempted to reconnect to the home network; however, the UE failed to connect to its 5G home RAN network, as shown in Figure 59. The UE entered an “Out of Service” state and remained deregistered from any network.



Key	Type	Time Stamp	Name	Summary
[0xB821]	OTA LOG	2025/02/27 21:00:35	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB80D]	LOG	2025/02/27 21:01:14	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/27 21:01:14	NR5G NAS MM5G State	Length: 42
[0xB825]	LOG	2025/02/27 21:01:14	NR5G RRC Configuration Info	Length: 87
[0xB822]	LOG	2025/02/27 21:01:14	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 21:01:14	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/27 21:01:15	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB80D]	LOG	2025/02/27 21:01:36	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/27 21:01:36	NR5G NAS MM5G State	Length: 42
[0xB825]	LOG	2025/02/27 21:01:36	NR5G RRC Configuration Info	Length: 87
[0xB822]	LOG	2025/02/27 21:01:37	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 21:01:37	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/27 21:01:37	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/27 21:01:59	NR5G RRC Configuration Info	Length: 87
[0xB80C]	LOG	2025/02/27 21:01:59	NR5G NAS MM5G State	Length: 42
[0xB80D]	LOG	2025/02/27 21:02:29	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/27 21:02:29	NR5G NAS MM5G State	Length: 42
[0xB822]	LOG	2025/02/27 21:02:29	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 21:02:29	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/27 21:02:29	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/27 21:02:29	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/27 21:02:29	NR5G RRC Serving Cell Info	Length: 62
[0xB822]	LOG	2025/02/27 21:02:30	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 21:02:30	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB822]	LOG	2025/02/27 21:02:30	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 21:02:30	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1

Figure 59: UE Unable to Connect to 5G Home Network After RRC Release from FBS (UE QXDM Log)

This test case's results demonstrate that a UE is vulnerable to a DoS attack if a false base station attempts to attract the UE and then force it to reject registration by preventing access to 5GS services. Due to this behavior, the test team toggled the UE into Airplane Mode, after which it was able to register properly with the home radio base station. The test team captured logs for each of the interfaces demonstrating the test case behavior.

6.3 Outcomes for Both 5G AKA and Null Encryption Tests

Expected Results:
The UE does not connect with the false base station. If the UE connects with the FBS, the UE ignores the RRMU registration rejection message and waits for authentication to occur. If the UE accepts the RRMU registration rejection message and goes into a state that does not allow it to connect to any 5G network, then it is vulnerable to the DoS attack.

Success Criteria:
The UE does not connect with the FBS. If the UE connects with the FBS, the UE ignores the RRMU registration rejection message and waits for authentication to occur.

Test Results:
The test results demonstrate that the UE does not complete registration with the FBS. The FBS successfully prevents an authentication procedure and directly sends a registration reject message to the UE with cause code #7 – "5GS services not allowed." As a result, once the FBS is powered OFF, the UE enters a state where it is unable to reconnect with the home base station. Both the 5G AKA and 5G Null encryption SIMs demonstrated similar behavior. This test case demonstrates that a UE is vulnerable to the DoS attack, rendering it unable to reconnect to its home network if a higher-powered false base station forces it to reject the registration by preventing access to 5GS services.

Condition	Status
The UE does not connect with the FBS. If the UE connects with FBS, the UE ignores the RRMU reject message and waits for authentication to occur.	
Overall Test	Failure

Test Case 7 – Conducting DoS Attack Using "Cell Barred" Message

Test Case ID: TC-FBS-7

Test Case Name: Conducting DoS Attack Using "Cell Barred" Message

Description:
This test case is designed to observe false base station attempts to conduct a DoS attack against the UE by cloning the UE's home radio base station and using the cell-identifier's "Cell Barred" field to prevent the UE from connecting with its home network. The goal of this test is to confirm that the UE will store the value and not connect even when the false base station is no longer transmitting on a stronger signal than the home base station.[iii]

Objectives:

- Configure the FBS to use the same physical cell ID as the home network, send an SIB 1 message to the UE with the Cell Barred field "ON," and observe the UE behavior.
- Verify whether the UE is vulnerable to the Denial-of-Service attack at any stage.

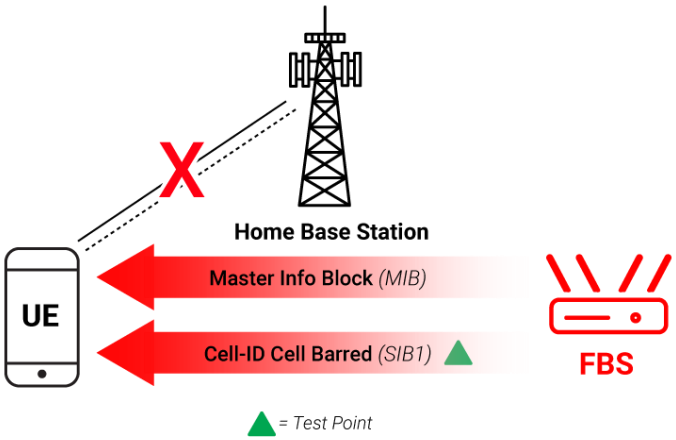


Figure 60: FBS Sends Cell Barred SIB 1 Message as a DoS Attack

7.1 5G AKA Test Results

For Test Case 7, the 5G test UE was initially turned OFF, the false base station's RAN configuration was modified to use the PCI with a value of 105, mirroring the home network PCI of 105, and the Cell Barred field was modified to ON prior to the test execution. The home network was powered ON initially, and the protocol capture was recorded using the Wireshark tool. Similarly, the FBS Core and gNB docker container services were initialized and ensured the services were up and operational. The protocol capture for the FBS was also recorded using the Wireshark tool. Note that both the home network and the FBS were configured to operate in the same frequency band.

The 5G UE was then turned ON, and the UE traces were collected using the QXDM tool. With both the home network and FBS transmitting at the same time, the UE performed a PLMN search as per Figure 61Figure 66. Upon the PLMN search, the UE found the FBS broadcasting with PCI 105 and read the FBS Master Information Block (MIB) information. However, as the FBS cell was "Barred" as indicated in Figure 62 below, the UE did not connect to the FBS and continued with the PLMN search procedure.

Key	Type	Time Stamp	Name
[0xB80D]	LOG	2025/02/27 23:49:04	NR5G NAS MM5G Service Request
[0xB80C]	LOG	2025/02/27 23:49:04	NR5G NAS MM5G State

```
98 01 00 00
68 BC D6 DE
00 00 02 13
00 00
```

```
2025/02/27 23:49:04 [0xB80C] NR5G NAS MM5G State
Version = 1
Version 1 {
   MM5G State = DEREGISTERED
   Mm5g Deregistered Substate = PLMN_SEARCH
```

Figure 61: UE Performing PLMN Search

Key	Type	Time Stamp	Name	Summary
[0xB80D]	LOG	2025/02/27 23:49:04	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/27 23:49:04	NR5G NAS MM5G State	Length: 42
[0xB822]	LOG	2025/02/27 23:49:05	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 23:49:05	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB80D]	LOG	2025/02/27 23:49:14	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/27 23:49:14	NR5G NAS MM5G State	Length: 42
[0xB825]	LOG	2025/02/27 23:49:14	NR5G RRC Configuration Info	Length: 87
[0xB825]	LOG	2025/02/27 23:49:14	NR5G RRC Configuration Info	Length: 87
[0xB822]	LOG	2025/02/27 23:49:15	NR5G RRC MIB Info	Length: 31

```
98 01 00 00
A5 5F DD DF
00 0E F0 01
01 02 60
```

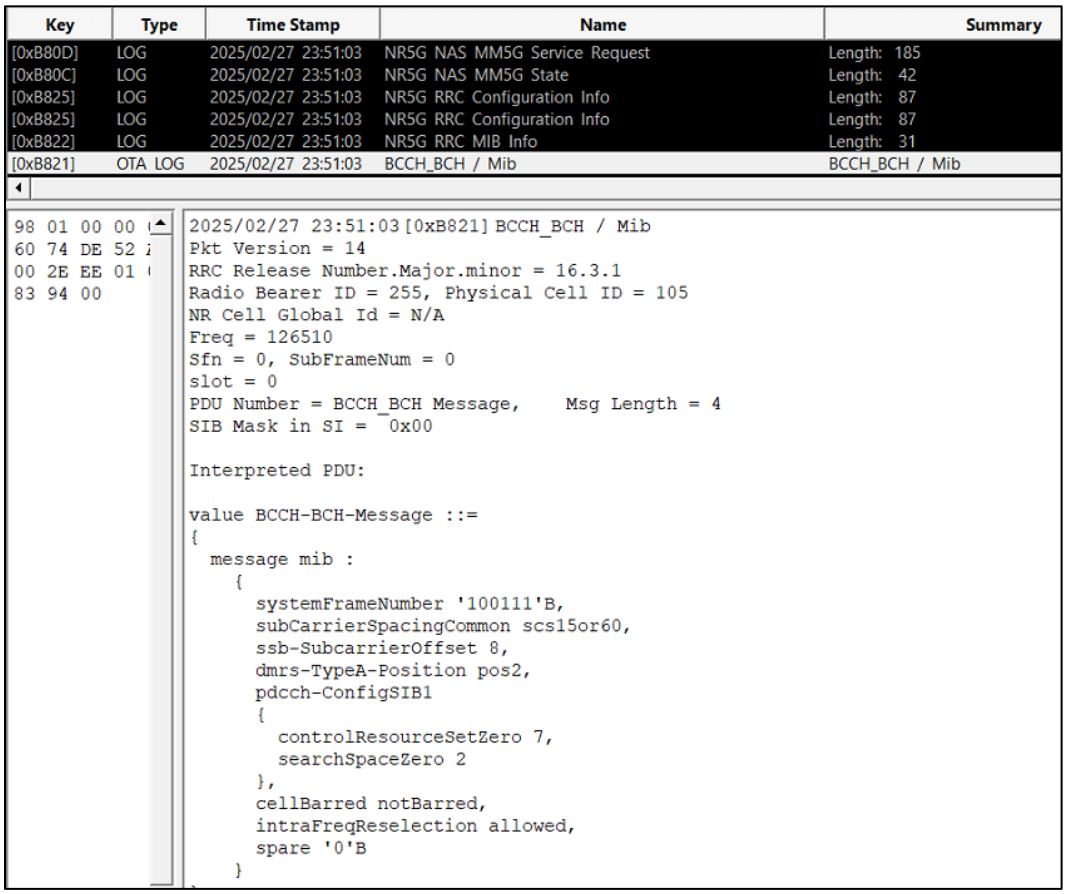
```
2025/02/27 23:49:05 [0xB821] BCCH_BCH / Mib
Pkt Version = 14
RRC Release Number.Major.minor = 16.3.1
Radio Bearer ID = 255, Physical Cell ID = 105
NR Cell Global Id = N/A
Freq = 126990
Sfn = 0, SubFrameNum = 0
slot = 0
PDU Number = BCCH_BCH Message,    Msg Length = 4
SIB Mask in SI =  0x00

Interpreted PDU:

value BCCH-BCH-Message ::=
{
  message mib :
    {
      systemFrameNumber '001001'B,
      subCarrierSpacingCommon scs15or60,
      ssb-SubcarrierOffset 0,
      dmrs-TypeA-Position pos2,
      pdcch-ConfigSIB1
      {
        controlResourceSetZero 2,
        searchSpaceZero 0
      },
      cellBarred barred,
      intraFreqReselection notAllowed,
      spare '0'B
    }
```

Figure 62: UE Reading MIB Information from FBS (UE QXDM Log)

The UE then continued to scan other cells, and after a few seconds, found the home RAN network broadcasting with the same PCI value of 105 and read its MIB information as shown in Figure 63. The UE was also able to read the SIB 1 information from the home base station as shown in Figure 64. At this stage, the UE continued to remain deregistered and did not connect to either the FBS or the home network.



Key	Type	Time Stamp	Name	Summary
[0xB80D]	LOG	2025/02/27 23:51:03	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/27 23:51:03	NR5G NAS MM5G State	Length: 42
[0xB825]	LOG	2025/02/27 23:51:03	NR5G RRC Configuration Info	Length: 87
[0xB825]	LOG	2025/02/27 23:51:03	NR5G RRC Configuration Info	Length: 87
[0xB822]	LOG	2025/02/27 23:51:03	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 23:51:03	BCCH_BCH / Mib	BCCH_BCH / Mib

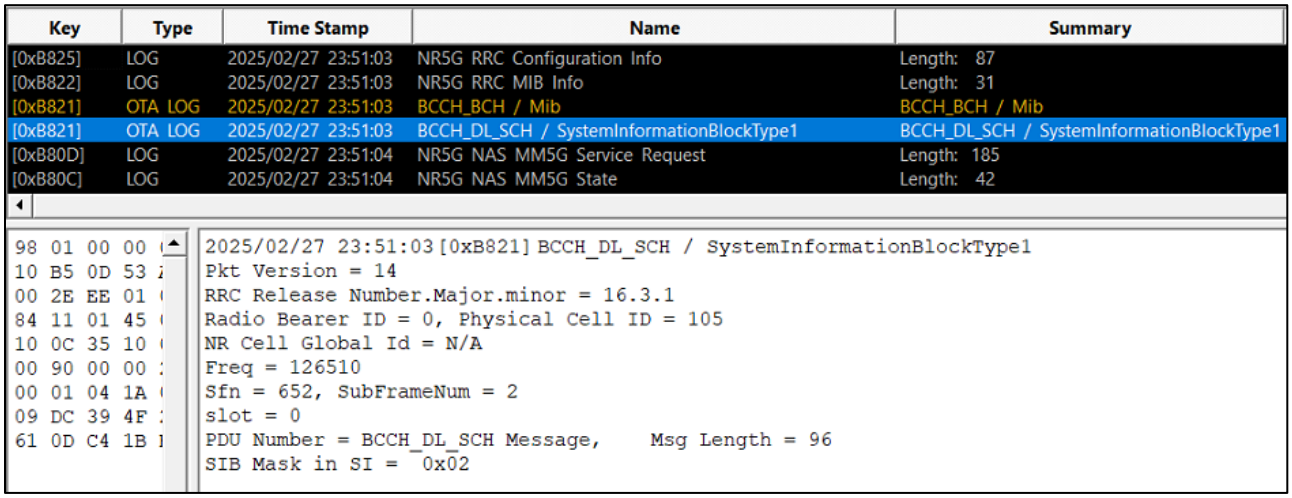
```
98 01 00 00
60 74 DE 52
00 2E EE 01
83 94 00
```

```
2025/02/27 23:51:03 [0xB821] BCCH_BCH / Mib
Pkt Version = 14
RRC Release Number.Major.minor = 16.3.1
Radio Bearer ID = 255, Physical Cell ID = 105
NR Cell Global Id = N/A
Freq = 126510
Sfn = 0, SubFrameNum = 0
slot = 0
PDU Number = BCCH_BCH Message,    Msg Length = 4
SIB Mask in SI =  0x00

Interpreted PDU:

value BCCH-BCH-Message ::=
{
  message mib :
    {
      systemFrameNumber '100111'B,
      subCarrierSpacingCommon scs15or60,
      ssb-SubcarrierOffset 8,
      dmrs-TypeA-Position pos2,
      pdcch-ConfigSIB1
      {
        controlResourceSetZero 7,
        searchSpaceZero 2
      },
      cellBarred notBarred,
      intraFreqReselection allowed,
      spare '0'B
    }
```

Figure 63: UE Reading MIB Information from Home Radio Base Station (UE QXDM Log)



Key	Type	Time Stamp	Name	Summary
[0xB825]	LOG	2025/02/27 23:51:03	NR5G RRC Configuration Info	Length: 87
[0xB822]	LOG	2025/02/27 23:51:03	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 23:51:03	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/27 23:51:03	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB80D]	LOG	2025/02/27 23:51:04	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/27 23:51:04	NR5G NAS MM5G State	Length: 42

```
98 01 00 00
10 B5 0D 53
00 2E EE 01
84 11 01 45
10 0C 35 10
00 90 00 00
00 01 04 1A
09 DC 39 4F
61 0D C4 1B
```

```
2025/02/27 23:51:03 [0xB821] BCCH_DL_SCH / SystemInformationBlockType1
Pkt Version = 14
RRC Release Number.Major.minor = 16.3.1
Radio Bearer ID = 0, Physical Cell ID = 105
NR Cell Global Id = N/A
Freq = 126510
Sfn = 652, SubFrameNum = 2
slot = 0
PDU Number = BCCH_DL_SCH Message,    Msg Length = 96
SIB Mask in SI =  0x02
```

Figure 64: UE Reading SIB1 Information from Home Radio Base Station (UE QXDM Log)

The protocol capture for the FBS was then disabled, and the FBS Core and RAN services were then turned OFF. As soon as the FBS was turned OFF, as the home network was "Not Barred," the UE initiated the registration procedure with the home radio base station. Figure 65 shows the RRC connection setup procedure, NAS security mode procedure, and subsequent PDU session establishment between the UE and the home network, demonstrating proper registration with the home Core network.

Key	Type	Time Stamp	Name	Summary
[0xB821]	OTA LOG	2025/02/27 23:52:33	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/27 23:52:33	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/27 23:52:33	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/27 23:52:33	NR5G NAS MM5G State	Length: 42
[0xB814]	OTA LOG	2025/02/27 23:52:33	NR5G NAS Plain Message Container	Length: 71
[0xB80B]	OTA LOG	2025/02/27 23:52:33	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/27 23:52:33	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 102
[0xB821]	OTA LOG	2025/02/27 23:52:33	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/27 23:52:33	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/27 23:52:33	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 23:52:33	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/27 23:52:34	DL_DCCH / securityModeCommand	DL_DCCH / securityModeCommand
[0xB825]	LOG	2025/02/27 23:52:34	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 23:52:34	UL_DCCH / SecurityMode Complete	UL_DCCH / SecurityMode Complete
[0xB821]	OTA LOG	2025/02/27 23:52:34	DL_DCCH / UeCapabilityEnquiry	DL_DCCH / UeCapabilityEnquiry
[0xB821]	OTA LOG	2025/02/27 23:52:34	UL_DCCH / UeCapabilityInformation	UL_DCCH / UeCapabilityInformation
[0xB821]	OTA LOG	2025/02/27 23:52:34	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB808]	OTA LOG	2025/02/27 23:52:34	NR5G NAS MM5G Security Protected OTA Incoming Msg	Length: 79
[0xB80A]	OTA LOG	2025/02/27 23:52:34	Registration accept	Registration accept
[0xB80B]	OTA LOG	2025/02/27 23:52:34	Registration complete	Registration complete
[0xB809]	OTA LOG	2025/02/27 23:52:34	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 33
[0xB821]	OTA LOG	2025/02/27 23:52:34	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB80C]	LOG	2025/02/27 23:52:34	NR5G NAS MM5G State	Length: 42
[0xB821]	OTA LOG	2025/02/27 23:52:34	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB808]	OTA LOG	2025/02/27 23:52:34	NR5G NAS MM5G Security Protected OTA Incoming Msg	Length: 52
[0xB80A]	OTA LOG	2025/02/27 23:52:34	Config update command	Config update command
[0xB801]	OTA LOG	2025/02/27 23:52:34	PDU session establishment req	PDU session establishment req
[0xB80B]	OTA LOG	2025/02/27 23:52:34	UL NAS transport	UL NAS transport
[0xB809]	OTA LOG	2025/02/27 23:52:34	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 119
[0xB821]	OTA LOG	2025/02/27 23:52:34	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/27 23:52:34	DL_DCCH / RRCReconfiguration	DL_DCCH / RRCReconfiguration
[0xB825]	LOG	2025/02/27 23:52:34	NR5G RRC Configuration Info	Length: 168
[0xB821]	OTA LOG	2025/02/27 23:52:34	UL_DCCH / RRCConfiguration Complete	UL_DCCH / RRCConfiguration Complete
[0xB808]	OTA LOG	2025/02/27 23:52:34	NR5G NAS MM5G Security Protected OTA Incoming Msg	Length: 118
[0xB80A]	OTA LOG	2025/02/27 23:52:34	DL NAS transport	DL NAS transport
[0xB800]	OTA LOG	2025/02/27 23:52:34	PDU session establishment accept	PDU session establishment accept

```
98 01 00 00 (
93 8B 58 6C i
40 10 02 13 @
00 02
```

```
2025/02/27 23:52:33 [0xB80C] NR5G NAS MM5G State
Version = 1
Version 1 {
   MM5G State = REGISTERED_INITIATED
   Mm5g Registered Initiated Substate = 1
```

Figure 65: UE Registering with the 5G Home Network (UE QXDM Log)

7.2 Null Encryption Test Results

For Test Case 7, the test results for the Null encryption SIM were similar to the results described in Section 7.1 above with the 5G AKA SIM. The 5G test UE was initially turned OFF, and the false base station's RAN configuration was modified to use the PCI with a value of "105," mirroring the home network PCI of "105," and the Cell Barred field was modified to ON prior to the test execution. The home network was powered ON initially and the protocol capture was recorded

using the Wireshark tool. Similarly, the FBS Core and gNB docker container services were initialized and ensured the services were up and operational. The protocol capture for FBS was also recorded using the Wireshark tool. Note that both the home network and the FBS were configured to operate in the same frequency band.

Key	Type	Time Stamp	Name
[0xB80D]	LOG	2025/02/27 21:31:49	NR5G NAS MM5G Service Request
[0xB80C]	LOG	2025/02/27 21:31:49	NR5G NAS MM5G State

```
98 01 00 00
7E B6 83 56
00 00 02 13
00 00
```

```
2025/02/27 21:31:49 [0xB80C] NR5G NAS MM5G State
Version = 1
Version 1 {
   MM5G State = DEREGISTERED
   Mm5g Deregistered Substate = PLMN_SEARCH
```

Figure 66: UE Performing PLMN Search

The 5G UE was then turned ON and the UE traces were collected using the QXDM tool. With both the home network and FBS transmitting at the same time, the UE began performing a PLMN search as per Figure 66. Upon the PLMN search, the UE found the FBS broadcasting with PCI 105 and reads the FBS Master Information Block (MIB) information. However, as the FBS cell was "Barred," as indicated in *Figure 67* below, the UE did not connect to the FBS and continued with the PLMN search procedure.

Key	Type	Time Stamp	Name	Summary
[0xB80D]	LOG	2025/02/27 21:31:49	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/27 21:31:49	NR5G NAS MM5G State	Length: 42
[0xB822]	LOG	2025/02/27 21:31:49	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 21:31:49	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB80D]	LOG	2025/02/27 21:31:59	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/27 21:31:59	NR5G NAS MM5G State	Length: 42
[0xB825]	LOG	2025/02/27 21:31:59	NR5G RRC Configuration Info	Length: 87
[0xB825]	LOG	2025/02/27 21:31:59	NR5G RRC Configuration Info	Length: 87

```
98 01 00 00
6A 15 7A 57
00 0E F0 01
01 02 B0
```

```
2025/02/27 21:31:49 [0xB821] BCCH_BCH / Mib
Pkt Version = 14
RRC Release Number.Major.minor = 16.3.1
Radio Bearer ID = 255, Physical Cell ID = 105
NR Cell Global Id = N/A
Freq = 126990
Sfn = 0, SubFrameNum = 0
slot = 0
PDU Number = BCCH_BCH Message,    Msg Length = 4
SIB Mask in SI =  0x00

Interpreted PDU:

value BCCH-BCH-Message ::=
{
  message mib :
    {
      systemFrameNumber '101000'B,
      subCarrierSpacingCommon scs15or60,
      ssb-SubcarrierOffset 0,
      dmrs-TypeA-Position pos2,
      pdcch-ConfigSIB1
      {
        controlResourceSetZero 2,
        searchSpaceZero 0
      },
      cellBarred barred,
      intraFreqReselection notAllowed,
      spare '0'B
    }
```

Figure 67: UE Reading MIB Information from FBS (UE QXDM Log)

The UE then continued to scan other cells, and after a few seconds, found the home network broadcasting with the same PCI value of 105 and read its MIB information, as shown in Figure 68. Unlike the 5G AKA SIM test result above, for the 5G Null encryption SIM in this test, the UE was unable to receive the SIB 1 message from the home RAN network. At this stage, the UE continued to remain deregistered and did not connect to either the FBS or the home network.

Key	Type	Time Stamp	Name	Summary
[0xB80C]	LOG	2025/02/27 21:31:59	NR5G NAS MM5G State	Length: 42
[0xB825]	LOG	2025/02/27 21:31:59	NR5G RRC Configuration Info	Length: 87
[0xB825]	LOG	2025/02/27 21:31:59	NR5G RRC Configuration Info	Length: 87
[0xB822]	LOG	2025/02/27 21:31:59	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 21:31:59	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB80D]	LOG	2025/02/27 21:32:00	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/27 21:32:00	NR5G NAS MM5G State	Length: 42
[0xB825]	LOG	2025/02/27 21:32:00	NR5G RRC Configuration Info	Length: 87
[0xB80D]	LOG	2025/02/27 21:32:10	NR5G NAS MM5G Service Request	Length: 185

```
98 01 00 00
88 A6 B3 76
00 2E EE 01
83 94 20
```

```
2025/02/27 21:31:59 [0xB821] BCCH_BCH / Mib
Pkt Version = 14
RRC Release Number.Major.minor = 16.3.1
Radio Bearer ID = 255, Physical Cell ID = 105
NR Cell Global Id = N/A
Freq = 126510
Sfn = 0, SubFrameNum = 0
slot = 0
PDU Number = BCCH_BCH Message,    Msg Length = 4
SIB Mask in SI =  0x00

Interpreted PDU:

value BCCH-BCH-Message ::=
{
  message mib :
    {
      systemFrameNumber '111110'B,
      subCarrierSpacingCommon scs15or60,
      ssb-SubcarrierOffset 8,
      dmrs-TypeA-Position pos2,
      pdcch-ConfigSIB1
      {
        controlResourceSetZero 7,
        searchSpaceZero 2
      },
      cellBarred notBarred,
      intraFreqReselection allowed,
      spare '0'B
    }
```

Figure 68: UE Reading MIB Information from the 5G Home Network (UE QXDM Log)

The protocol capture for the FBS was then disabled, and the FBS Core and RAN services were then turned OFF. As soon as the FBS was turned OFF, as the home RAN network was “Not Barred,” the UE initiated registration procedure with the home network. Figure 69 shows the RRC connection setup procedure, NAS security mode procedure, and subsequent PDU session establishment between the UE and the home network, demonstrating proper registration with the home radio base station.

Key	Type	Time Stamp	Name	Summary
[0xB823]	LOG	2025/02/27 21:34:21	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/27 21:34:21	NR5G NAS MM5G State	Length: 42
[0xB814]	OTA LOG	2025/02/27 21:34:21	NR5G NAS Plain Message Container	Length: 71
[0xB80B]	OTA LOG	2025/02/27 21:34:21	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/27 21:34:21	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 102
[0xB821]	OTA LOG	2025/02/27 21:34:21	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/27 21:34:21	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/27 21:34:21	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 21:34:21	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/27 21:34:21	DL_DCCH / securityModeCommand	DL_DCCH / securityModeCommand
[0xB825]	LOG	2025/02/27 21:34:21	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 21:34:21	UL_DCCH / SecurityMode Complete	UL_DCCH / SecurityMode Complete
[0xB821]	OTA LOG	2025/02/27 21:34:21	DL_DCCH / UeCapabilityEnquiry	DL_DCCH / UeCapabilityEnquiry
[0xB821]	OTA LOG	2025/02/27 21:34:21	UL_DCCH / UeCapabilityInformation	UL_DCCH / UeCapabilityInformation
[0xB821]	OTA LOG	2025/02/27 21:34:21	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB808]	OTA LOG	2025/02/27 21:34:21	NR5G NAS MM5G Security Protected OTA Incoming Msg	Length: 79
[0xB80A]	OTA LOG	2025/02/27 21:34:21	Registration accept	Registration accept
[0xB80B]	OTA LOG	2025/02/27 21:34:21	Registration complete	Registration complete
[0xB809]	OTA LOG	2025/02/27 21:34:21	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 33
[0xB821]	OTA LOG	2025/02/27 21:34:21	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB80C]	LOG	2025/02/27 21:34:21	NR5G NAS MM5G State	Length: 42
[0xB821]	OTA LOG	2025/02/27 21:34:21	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB808]	OTA LOG	2025/02/27 21:34:21	NR5G NAS MM5G Security Protected OTA Incoming Msg	Length: 52
[0xB80A]	OTA LOG	2025/02/27 21:34:21	Config update command	Config update command
[0xB801]	OTA LOG	2025/02/27 21:34:22	PDU session establishment req	PDU session establishment req
[0xB80B]	OTA LOG	2025/02/27 21:34:22	UL NAS transport	UL NAS transport
[0xB809]	OTA LOG	2025/02/27 21:34:22	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 119
[0xB821]	OTA LOG	2025/02/27 21:34:22	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/27 21:34:22	DL_DCCH / RRCReconfiguration	DL_DCCH / RRCReconfiguration
[0xB825]	LOG	2025/02/27 21:34:22	NR5G RRC Configuration Info	Length: 168
[0xB821]	OTA LOG	2025/02/27 21:34:22	UL_DCCH / RRCConfiguration Complete	UL_DCCH / RRCConfiguration ...
[0xB808]	OTA LOG	2025/02/27 21:34:22	NR5G NAS MM5G Security Protected OTA Incoming Msg	Length: 118
[0xB80A]	OTA LOG	2025/02/27 21:34:22	DL NAS transport	DL NAS transport
[0xB800]	OTA LOG	2025/02/27 21:34:22	PDU session establishment accept	PDU session establishment accept

```
98 01 00 00
D4 20 5E 33
40 10 02 13
00 02
```

```
2025/02/27 21:34:21 [0xB80C] NR5G NAS MM5G State
Version = 1
Version 1 {
   MM5G State = REGISTERED_INITIATED
   Mm5g Registered Initiated Substate = 1
```

Figure 69: UE Registering with the Home Radio Base Station (UE QXDM Log)

7.3 Outcomes for Both 5G AKA and Null Encryption Tests

Expected Results:
The UE ignores the false base station and maintains its connection with the home radio base station.

Success Criteria:
The UE ignores the false base station and maintains its connection with the home radio base station.

Test Results:
The test results demonstrate that if a false base station is cloned to use the same PCI as the home network, and the FBS sends an SIB 1 message with the Cell Barred field ON in the presence of a home network, then the UE does not connect to either the FBS or the home network. Once the FBS is powered OFF, the UE continues to perform a registration procedure with the home network and successfully completes registration as expected.

Condition	Status
The UE ignores the FBS and maintains its connection with its home radio base station.	
Overall Test	Success

Test Case 8 – Conducting DoS Attack Using "PLMN Not Allowed" Message

Test Case ID: TC-FBS-8

Test Case Name: Conducting DoS Attack Using "PLMN Not Allowed" Message

Description:
This test case is designed to observe false base station attempts to conduct a DoS attack against the UE by rejecting the UE's registration request with cause value #11 – "PLMN Not Allowed" that prevents the UE from reconnecting with the home radio base station.[iv] The primary goal of this test is to confirm that the UE will respond by ignoring the false base station's message and reconnecting to its own home radio base station.

Objectives:

- Configure the FBS to send a registration reject NAS message to the UE with NAS reject cause "PLMN Not Allowed."
- Observe the UE behavior and see if the UE ignores the FBS message and reconnects to the 5G home base station network.
- Verify if any at any stage the UE is vulnerable to the Denial-of-Service attack.

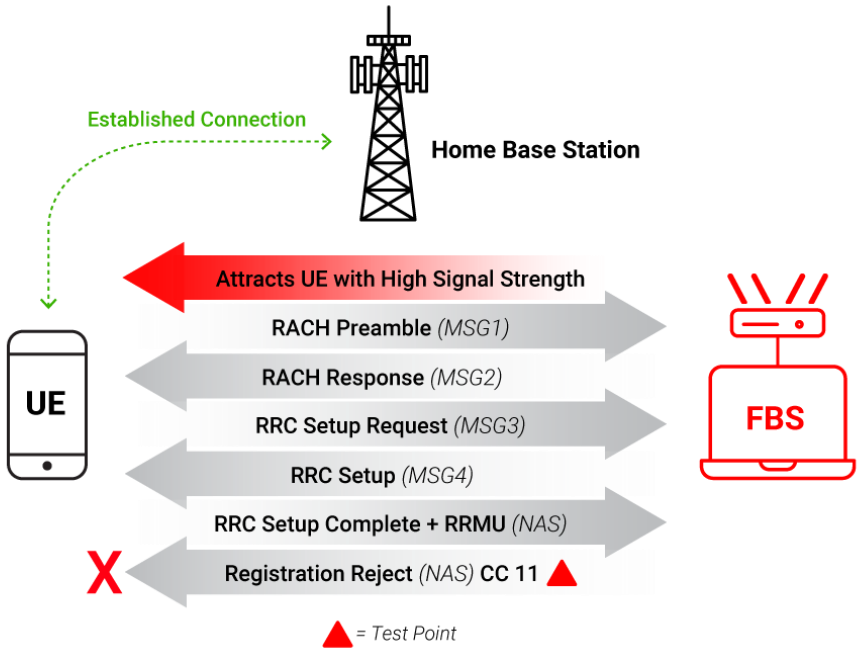
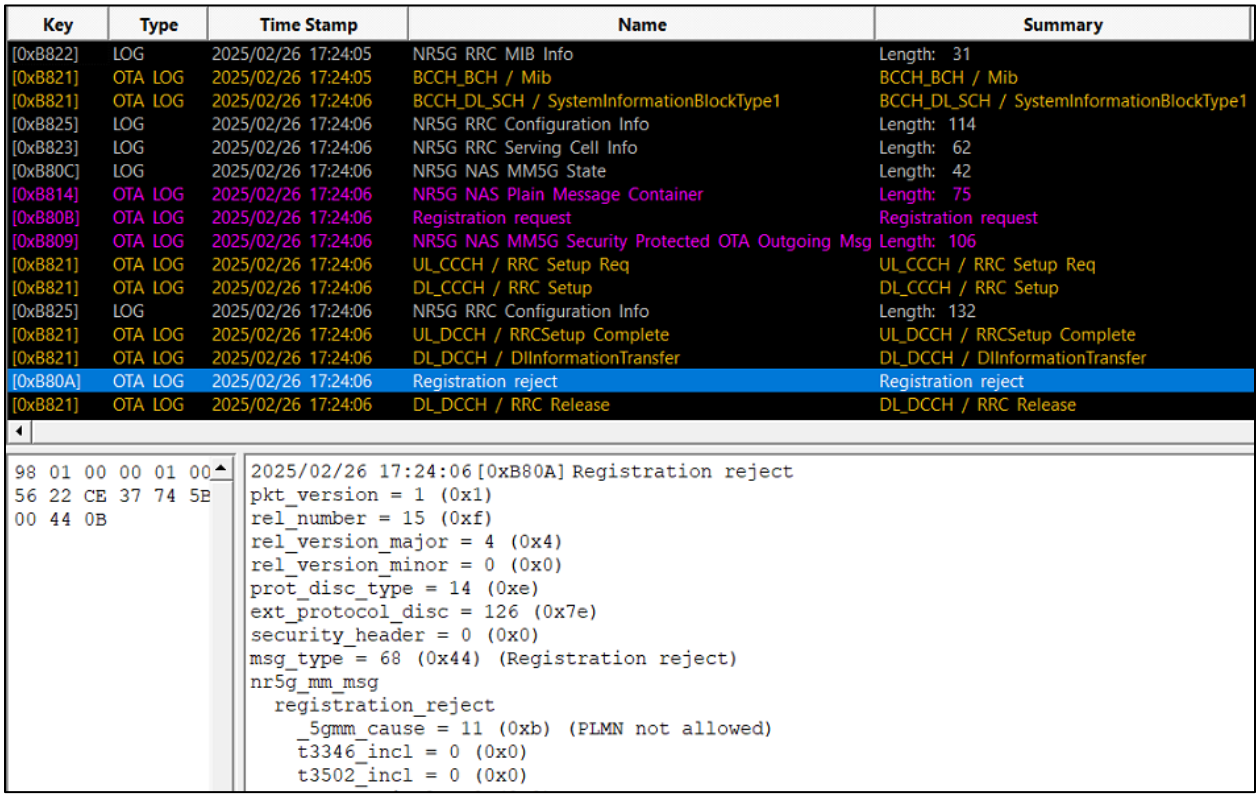


Figure 70: False Base Station Sends PLMN Not Allowed NAS Registration Reject to Deny UE of Any 5G Service

8.1 5G AKA Test Results

As described and performed in Test Case 2, the 5G test UE initially established a connection and properly authenticated with its home network. The test IMSI remained added to the FBS Core network subscriber profile with random subscription key "K" and Operator code "OPc" values. For Test Case 8, the FBS Core configuration was modified to include the NAS registration reject message with cause value #11 – "PLMN Not Allowed." The FBS Core and gNB docker container services were initialized and ensured the services were up and operational. The UE was then prompted by the higher-powered FBS to release its connection to home network. The UE, upon seeing a stronger signal being emitted from the FBS, attempted to connect to the FBS. The RRC connection to the FBS was successful, and the protocol capture was recorded using the Wireshark tool.

Once the RRC connection was established, the UE sent a mobility update registration request to register to the FBS Core network using the 5G-GUTI previously assigned by the home network. Upon receiving the mobility update registration request from the UE, the FBS Core network immediately sent a registration reject message to the UE with the cause code value #11 – "PLMN Not Allowed," as shown in Figure 71. This 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, in a PLMN where the UE, by subscription or due to operator determined barring, is not allowed to operate.



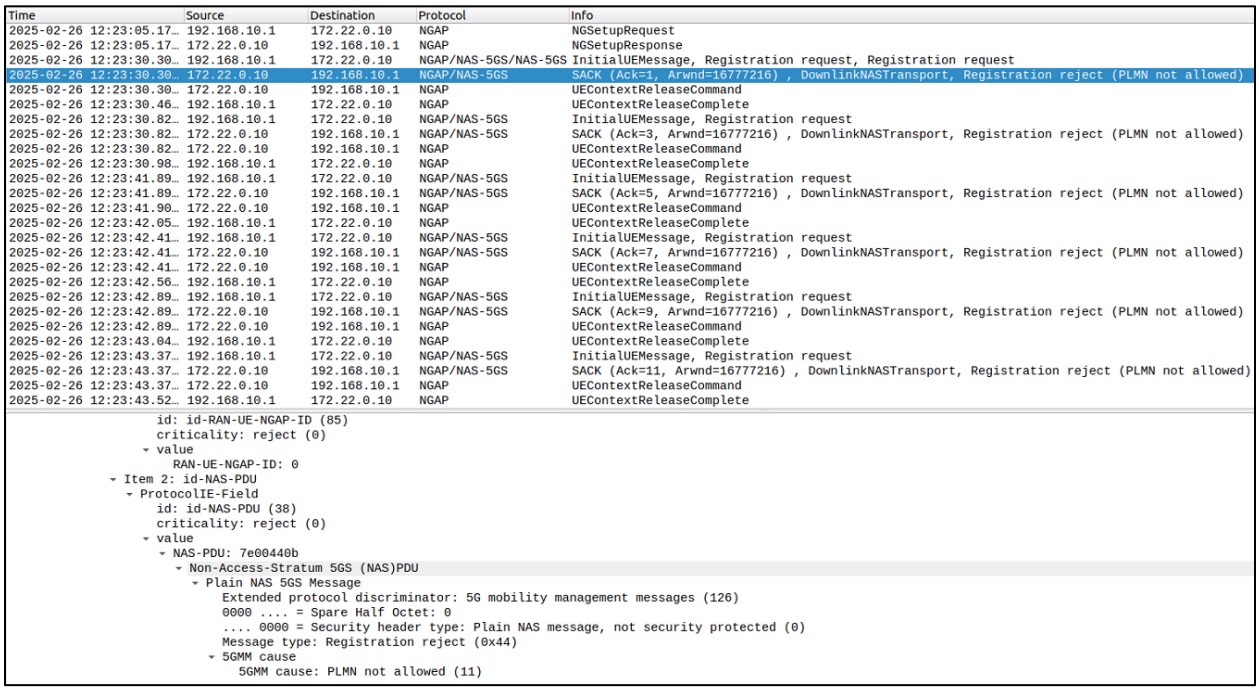
Key	Type	Time Stamp	Name	Summary
[0xB822]	LOG	2025/02/26 17:24:05	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 17:24:05	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/26 17:24:06	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/26 17:24:06	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/26 17:24:06	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/26 17:24:06	NR5G NAS MM5G State	Length: 42
[0xB814]	OTA LOG	2025/02/26 17:24:06	NR5G NAS Plain Message Container	Length: 75
[0xB80B]	OTA LOG	2025/02/26 17:24:06	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/26 17:24:06	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 106
[0xB821]	OTA LOG	2025/02/26 17:24:06	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/26 17:24:06	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/26 17:24:06	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/26 17:24:06	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/26 17:24:06	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/26 17:24:06	Registration reject	Registration reject
[0xB821]	OTA LOG	2025/02/26 17:24:06	DL_DCCH / RRC Release	DL_DCCH / RRC Release

```
98 01 00 00 01 00
56 22 CE 37 74 5B
00 44 0B
```

```
2025/02/26 17:24:06 [0xB80A] Registration reject
pkt_version = 1 (0x1)
rel_number = 15 (0xf)
rel_version_major = 4 (0x4)
rel_version_minor = 0 (0x0)
prot_disc_type = 14 (0xe)
ext_protocol_disc = 126 (0x7e)
security_header = 0 (0x0)
msg_type = 68 (0x44) (Registration reject)
nr5g_mm_msg
  registration_reject
    _5gmm_cause = 11 (0xb) (PLMN not allowed)
    t3346_incl = 0 (0x0)
    t3502_incl = 0 (0x0)
```

Figure 71: FBS NAS Registration Rejection (UE QXDM log)

The FBS then sent a UE context release message to the UE, and the registration process was terminated. The UE again sent a registration request (initial registration as discussed in Test Case 2) to the FBS, and the FBS rejected the registration with the same cause code value, sending the UE into a repetitive loop whereby it was unable to connect to the FBS or home network, as shown in Figure 72.



Time	Source	Destination	Protocol	Info
2025-02-26 12:23:05.17…	192.168.10.1	172.22.0.10	NGAP	NGSetupRequest
2025-02-26 12:23:05.17…	172.22.0.10	192.168.10.1	NGAP	NGSetupResponse
2025-02-26 12:23:30.30…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS/NAS-5GS	InitialUEMessage, Registration request, Registration request
2025-02-26 12:23:30.30…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-02-26 12:23:30.30…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-26 12:23:30.46…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-02-26 12:23:30.82…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-02-26 12:23:30.82…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=3, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-02-26 12:23:30.82…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-26 12:23:30.98…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-02-26 12:23:41.89…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-02-26 12:23:41.89…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=5, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-02-26 12:23:41.90…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-26 12:23:42.05…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-02-26 12:23:42.41…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-02-26 12:23:42.41…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=7, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-02-26 12:23:42.41…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-26 12:23:42.56…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-02-26 12:23:42.89…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-02-26 12:23:42.89…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=9, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-02-26 12:23:42.89…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-26 12:23:43.04…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-02-26 12:23:43.37…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-02-26 12:23:43.37…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=11, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-02-26 12:23:43.37…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-26 12:23:43.52…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete

```
            id: id-RAN-UE-NGAP-ID (85)
            criticality: reject (0)
          ▾ value
              RAN-UE-NGAP-ID: 0
        ▾ Item 2: id-NAS-PDU
          ▾ ProtocolIE-Field
            id: id-NAS-PDU (38)
            criticality: reject (0)
          ▾ value
            ▾ NAS-PDU: 7e00440b
              ▾ Non-Access-Stratum 5GS (NAS)PDU
                ▾ Plain NAS 5GS Message
                    Extended protocol discriminator: 5G mobility management messages (126)
                    0000 .... = Spare Half Octet: 0
                    .... 0000 = Security header type: Plain NAS message, not security protected (0)
                    Message type: Registration reject (0x44)
                  ▾ 5GMM cause
                      5GMM cause: PLMN not allowed (11)
```

Figure 72: Multiple NAS Registration Rejections (FBS Wireshark Trace)

The FBS Core and RAN services were then turned OFF. Upon disconnecting from the FBS network, the UE began performing a PLMN search and immediately received SIB 1 message from the home network and attempted to reconnect. The UE initiated the registration procedure with the home network, as per Figure 73. Figure 74 shows the RRC connection setup procedure, NAS authentication, and security mode procedure between the UE and the home network, demonstrating proper registration with the home Core network. The UE was then turned OFF, and the test team captured logs for each of the interfaces demonstrating the test case behavior.

Key	Type	Time Stamp	Name	Summary
[0xB821]	OTA LOG	2025/02/26 17:24:23	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/26 17:24:23	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/26 17:24:23	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/26 17:24:23	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/26 17:24:23	NR5G NAS MM5G State	Length: 42
[0xB80B]	OTA LOG	2025/02/26 17:24:23	Registration request	Registration request
[0xB821]	OTA LOG	2025/02/26 17:24:23	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/26 17:24:23	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/26 17:24:23	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/26 17:24:23	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB822]	LOG	2025/02/26 17:24:23	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 17:24:23	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB822]	LOG	2025/02/26 17:24:23	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 17:24:23	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB821]	OTA LOG	2025/02/26 17:24:23	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/26 17:24:23	Authentication req	Authentication req
[0xB80B]	OTA LOG	2025/02/26 17:24:23	Authentication resp	Authentication resp
[0xB821]	OTA LOG	2025/02/26 17:24:23	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/26 17:24:23	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB808]	OTA LOG	2025/02/26 17:24:23	NR5G NAS MM5G Security Protected OTA Incoming Msg	Length: 50
[0xB80A]	OTA LOG	2025/02/26 17:24:23	Security mode command	Security mode command
[0xB814]	OTA LOG	2025/02/26 17:24:23	NR5G NAS Plain Message Container	Length: 107
[0xB80B]	OTA LOG	2025/02/26 17:24:23	Security mode complete	Security mode complete
[0xB809]	OTA LOG	2025/02/26 17:24:23	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 132
[0xB821]	OTA LOG	2025/02/26 17:24:23	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/26 17:24:24	DL_DCCH / securityModeCommand	DL_DCCH / securityModeCommand
[0xB825]	LOG	2025/02/26 17:24:24	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/26 17:24:24	UL_DCCH / SecurityMode Complete	UL_DCCH / SecurityMode Complete
[0xB821]	OTA LOG	2025/02/26 17:24:24	DL_DCCH / UeCapabilityEnquiry	DL_DCCH / UeCapabilityEnquiry
[0xB821]	OTA LOG	2025/02/26 17:24:24	UL_DCCH / UeCapabilityInformation	UL_DCCH / UeCapabilityInformation
[0xB821]	OTA LOG	2025/02/26 17:24:24	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB808]	OTA LOG	2025/02/26 17:24:24	NR5G NAS MM5G Security Protected OTA Incoming Msg	Length: 79
[0xB80A]	OTA LOG	2025/02/26 17:24:24	Registration accept	Registration accept
[0xB80B]	OTA LOG	2025/02/26 17:24:24	Registration complete	Registration complete

```
98 01 00 00 01 00
DB 9C EF 6D 74 5E
00 2E EE 01 00 00
BE 51 57 5A 86
```

```
2025/02/26 17:24:23 [0xB821] UL_CCCH / RRC Setup Req
Pkt Version = 14
RRC Release Number.Major.minor = 16.3.1
Radio Bearer ID = 0, Physical Cell ID = 105
```

Figure 73: RRC Connection Setup with Home Network (UE QXDM log)

No.	Time	Source	Destination	Protocol	Info
309	2025-02-26 12:24:02…	10.220.67.18	10.205.67.205	NGAP/NAS-5GS	InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling]
311	2025-02-26 12:24:02…	10.205.67.205	10.220.67.18	NGAP/NAS-5GS	DownlinkNASTransport, Authentication request
313	2025-02-26 12:24:02…	10.220.67.18	10.205.67.205	NGAP/NAS-5GS	UplinkNASTransport, Authentication response
314	2025-02-26 12:24:02…	10.205.67.205	10.220.67.18	NGAP/NAS-5GS	SACK (Ack=9, Arwnd=32768) , DownlinkNASTransport, Security mode command
315	2025-02-26 12:24:02…	10.220.67.18	10.205.67.205	NGAP/NAS-5GS/NAS-5GS	SACK (Ack=6, Arwnd=16384) , UplinkNASTransport, Security mode complete, Registration request
320	2025-02-26 12:24:02…	10.205.67.205	10.220.67.18	NGAP	InitialContextSetupRequest
321	2025-02-26 12:24:02…	10.220.67.18	10.205.67.205	NGAP	SACK (Ack=7, Arwnd=16384) , UERadioCapabilityInfoIndication
322	2025-02-26 12:24:02…	10.220.67.18	10.205.67.205	NGAP	InitialContextSetupResponse
324	2025-02-26 12:24:02…	10.205.67.205	10.220.67.18	NGAP/NAS-5GS	DownlinkNASTransport, Registration accept
325	2025-02-26 12:24:02…	10.220.67.18	10.205.67.205	NGAP/NAS-5GS	SACK (Ack=8, Arwnd=16384) , UplinkNASTransport, Registration complete
326	2025-02-26 12:24:02…	10.205.67.205	10.220.67.18	NGAP/NAS-5GS	SACK (Ack=13, Arwnd=32768) , DownlinkNASTransport, Configuration update command
328	2025-02-26 12:24:03…	10.220.67.18	10.205.67.205	NGAP/NAS-5GS	UplinkNASTransport, UL NAS transport, PDU session establishment request
331	2025-02-26 12:24:03…	10.205.67.205	10.220.67.18	NGAP/NAS-5GS	PDUSessionResourceSetupRequest, DL NAS transport, PDU session establishment accept
333	2025-02-26 12:24:03…	10.220.67.18	10.205.67.205	NGAP	PDUSessionResourceSetupResponse

Figure 74: UE NAS Registration with Home Network (Home Network Wireshark Trace)

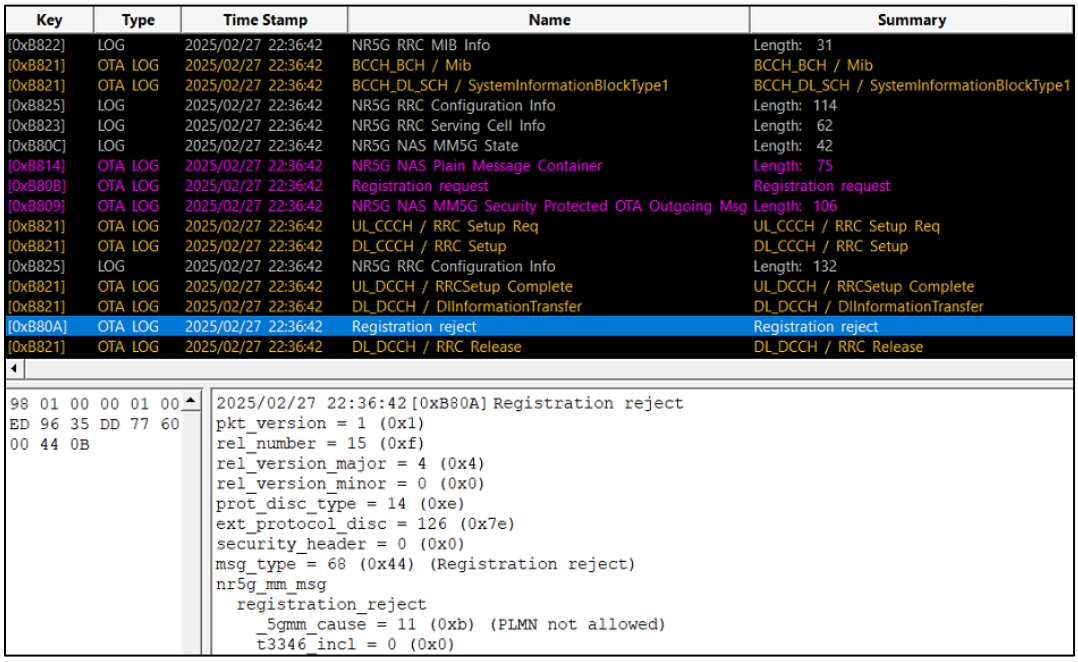
This test case's results demonstrated that a UE is vulnerable to a DoS attack if a false base station attempts to attract the UE, then forces it to reject the registration by not allowing the UE to operate in the same PLMN as its home network.

8.2 Null Encryption Test Results

For Test Case 8, the test results for the Null encryption SIM were similar to the results demonstrated in Section 8.1 above with the 5G AKA SIM. As described and performed in Test Case 2, the 5G test UE initially established connection and properly authenticated with the home

network. The test IMSI remained added to the FBS Core network subscriber profile with random subscription key "K" and Operator code "OPc" values. Similar to Section 8.1, the FBS Core configuration was modified to include the NAS registration reject message with cause value #11 – "PLMN Not Allowed." The FBS Core and gNB docker container services were initialized and ensured the services were up and operational. The UE was then prompted by the higher-powered FBS to release its connection with the home network. The UE upon seeing a stronger signal being emitted from the FBS, attempted to connect to FBS. The RRC connection to the FBS was successful, and the protocol capture was recorded using the Wireshark tool.

Once the RRC connection was established, the UE sent a mobility update registration request to register to the FBS Core network using the 5G-GUTI previously assigned by the 5G home network. Upon receiving the mobility update registration request from the UE, the FBS Core network immediately sent a registration reject message to the UE with the cause code value #11 – 'PLMN not allowed' as shown in Figure 75. This 5GMM cause is sent to the UE if it requests service, or if the network initiates a de-registration request, in a PLMN where the UE, by subscription or due to operator determined barring, is not allowed to operate.



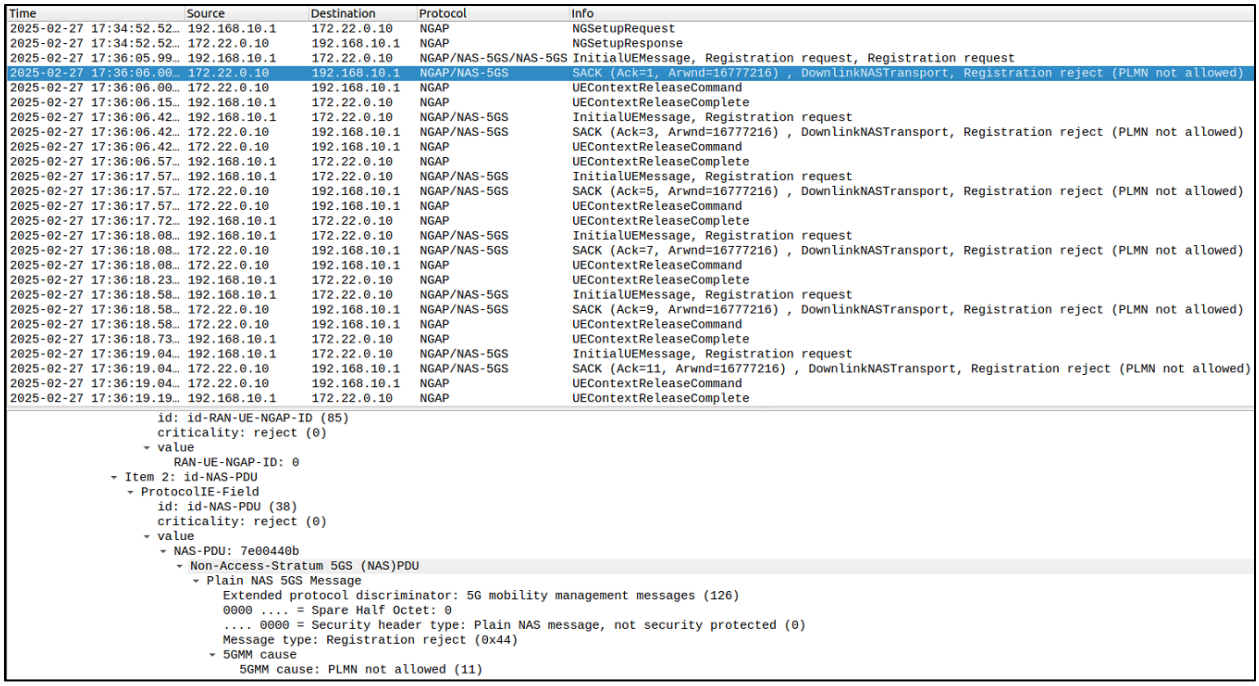
Key	Type	Time Stamp	Name	Summary
[0xB822]	LOG	2025/02/27 22:36:42	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 22:36:42	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/27 22:36:42	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/27 22:36:42	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/27 22:36:42	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/27 22:36:42	NR5G NAS MM5G State	Length: 42
[0xB814]	OTA LOG	2025/02/27 22:36:42	NR5G NAS Plain Message Container	Length: 75
[0xB80B]	OTA LOG	2025/02/27 22:36:42	Registration request	Registration request
[0xB809]	OTA LOG	2025/02/27 22:36:42	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 106
[0xB821]	OTA LOG	2025/02/27 22:36:42	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/27 22:36:42	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/27 22:36:42	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 22:36:42	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/27 22:36:42	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/27 22:36:42	Registration reject	Registration reject
[0xB821]	OTA LOG	2025/02/27 22:36:42	DL_DCCH / RRC Release	DL_DCCH / RRC Release

```
98 01 00 00 01 00
ED 96 35 DD 77 60
00 44 0B
```

```
2025/02/27 22:36:42 [0xB80A] Registration reject
pkt_version = 1 (0x1)
rel_number = 15 (0xf)
rel_version_major = 4 (0x4)
rel_version_minor = 0 (0x0)
prot_disc_type = 14 (0xe)
ext_protocol_disc = 126 (0x7e)
security_header = 0 (0x0)
msg_type = 68 (0x44) (Registration reject)
nr5g_mm_msg
  registration_reject
    _5gmm_cause = 11 (0xb) (PLMN not allowed)
    t3346_incl = 0 (0x0)
```

Figure 75: False Base Station NAS Registration Rejection (UE QXDM log)

The FBS then sent a UE context release message to the UE and the registration process was terminated. The UE again sent a registration request (initial registration, as discussed in Section 2.2) to the FBS and the FBS rejected the registration with the same cause code value sending the UE into a repetitive loop whereby it was unable to connect to either network, as shown in Figure 76.



Time	Source	Destination	Protocol	Info
2025-02-27 17:34:52.52…	192.168.10.1	172.22.0.10	NGAP	NGSetupRequest
2025-02-27 17:34:52.52…	172.22.0.10	192.168.10.1	NGAP	NGSetupResponse
2025-02-27 17:36:05.99…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS/NAS-5GS	InitialUEMessage, Registration request, Registration request
2025-02-27 17:36:06.00…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=1, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-02-27 17:36:06.00…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-27 17:36:06.15…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-02-27 17:36:06.42…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-02-27 17:36:06.42…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=3, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-02-27 17:36:06.42…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-27 17:36:06.57…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-02-27 17:36:17.57…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-02-27 17:36:17.57…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=5, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-02-27 17:36:17.57…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-27 17:36:17.72…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-02-27 17:36:18.08…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-02-27 17:36:18.08…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=7, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-02-27 17:36:18.08…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-27 17:36:18.23…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-02-27 17:36:18.58…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-02-27 17:36:18.58…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=9, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-02-27 17:36:18.58…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-27 17:36:18.73…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete
2025-02-27 17:36:19.04…	192.168.10.1	172.22.0.10	NGAP/NAS-5GS	InitialUEMessage, Registration request
2025-02-27 17:36:19.04…	172.22.0.10	192.168.10.1	NGAP/NAS-5GS	SACK (Ack=11, Arwnd=16777216) , DownlinkNASTransport, Registration reject (PLMN not allowed)
2025-02-27 17:36:19.04…	172.22.0.10	192.168.10.1	NGAP	UEContextReleaseCommand
2025-02-27 17:36:19.19…	192.168.10.1	172.22.0.10	NGAP	UEContextReleaseComplete

```
            id: id-RAN-UE-NGAP-ID (85)
            criticality: reject (0)
          ▾ value
              RAN-UE-NGAP-ID: 0
        ▾ Item 2: id-NAS-PDU
          ▾ ProtocolIE-Field
            id: id-NAS-PDU (38)
            criticality: reject (0)
          ▾ value
            ▾ NAS-PDU: 7e00440b
              ▾ Non-Access-Stratum 5GS (NAS)PDU
                ▾ Plain NAS 5GS Message
                    Extended protocol discriminator: 5G mobility management messages (126)
                    0000 .... = Spare Half Octet: 0
                    .... 0000 = Security header type: Plain NAS message, not security protected (0)
                    Message type: Registration reject (0x44)
                  ▾ 5GMM cause
                      5GMM cause: PLMN not allowed (11)
```

Figure 76: Multiple NAS Registration Rejections (FBS Wireshark Trace)

The FBS then sent a UE context release message to the UE and the registration process was terminated. The UE again sent a registration request (initial registration, as discussed in Section 2.2) to the FBS and the FBS rejected the registration with the same cause code value sending the UE into a repetitive loop whereby it was unable to connect to the FBS or home network as shown in Figure 76.

The FBS Core and RAN services were then turned OFF. Upon disconnecting from the FBS network, the UE began performing PLMN Search and immediately received SIB 1 message from the 5G home network and attempted to reconnect. The UE initiated registration procedure with the home Network as per Figure 77. Figure 78 shows the RRC connection set up procedure, NAS authentication and security mode procedure between the UE and the home network demonstrating proper registration with the home Core network. The UE was then turned OFF and the test team captured logs for each of the interfaces demonstrating the test case behavior.

Key	Type	Time Stamp	Name	Summary
[0xB821]	OTA LOG	2025/02/27 22:38:15	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/27 22:38:15	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/27 22:38:15	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/27 22:38:15	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/27 22:38:15	NR5G NAS MM5G State	Length: 42
[0xB80B]	OTA LOG	2025/02/27 22:38:15	Registration request	Registration request
[0xB821]	OTA LOG	2025/02/27 22:38:15	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/27 22:38:15	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/27 22:38:15	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 22:38:15	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/27 22:38:15	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/27 22:38:15	Authentication req	Authentication req
[0xB80B]	OTA LOG	2025/02/27 22:38:15	Authentication resp	Authentication resp
[0xB821]	OTA LOG	2025/02/27 22:38:15	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB821]	OTA LOG	2025/02/27 22:38:15	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB808]	OTA LOG	2025/02/27 22:38:15	NR5G NAS MM5G Security Protected OTA Incoming Msg	Length: 42
[0xB80A]	OTA LOG	2025/02/27 22:38:15	Security mode command	Security mode command
[0xB814]	OTA LOG	2025/02/27 22:38:15	NR5G NAS Plain Message Container	Length: 66
[0xB80B]	OTA LOG	2025/02/27 22:38:15	Security mode complete	Security mode complete
[0xB809]	OTA LOG	2025/02/27 22:38:15	NR5G NAS MM5G Security Protected OTA Outgoing Msg	Length: 91
[0xB821]	OTA LOG	2025/02/27 22:38:15	UL_DCCH / UlInformationTransfer	UL_DCCH / UlInformationTransfer
[0xB822]	LOG	2025/02/27 22:38:15	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 22:38:15	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB822]	LOG	2025/02/27 22:38:15	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/27 22:38:15	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB821]	OTA LOG	2025/02/27 22:38:15	DL_DCCH / securityModeCommand	DL_DCCH / securityModeCommand
[0xB825]	LOG	2025/02/27 22:38:15	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/27 22:38:15	UL_DCCH / SecurityMode Complete	UL_DCCH / SecurityMode Complete
[0xB821]	OTA LOG	2025/02/27 22:38:15	DL_DCCH / UeCapabilityEnquiry	DL_DCCH / UeCapabilityEnquiry
[0xB821]	OTA LOG	2025/02/27 22:38:15	UL_DCCH / UeCapabilityInformation	UL_DCCH / UeCapabilityInformation
[0xB821]	OTA LOG	2025/02/27 22:38:15	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB808]	OTA LOG	2025/02/27 22:38:15	NR5G NAS MM5G Security Protected OTA Incoming Msg	Length: 79
[0xB80A]	OTA LOG	2025/02/27 22:38:15	Registration accept	Registration accept
[0xB80B]	OTA LOG	2025/02/27 22:38:15	Registration complete	Registration complete

Figure 77: RRC Connection Setup with Home Network (UE QXDM log)

No.	Time	Source	Destination	Protocol	Info
1002	2025-02-27 17:37…	10.220.67.18	10.205.67.205	NGAP/NAS-5GS	InitialUEMessage, Registration request [RRCEstablishmentCause=mo-Signalling]
1004	2025-02-27 17:37…	10.205.67.205	10.220.67.18	NGAP/NAS-5GS	DownlinkNASTransport, Authentication request
1006	2025-02-27 17:37…	10.220.67.18	10.205.67.205	NGAP/NAS-5GS	UplinkNASTransport, Authentication response
1007	2025-02-27 17:37…	10.205.67.205	10.220.67.18	NGAP/NAS-5GS	SACK (Ack=11, Arwnd=32768) , DownlinkNASTransport, Security mode command
1008	2025-02-27 17:37…	10.220.67.18	10.205.67.205	NGAP/NAS-5GS/NAS-5GS	SACK (Ack=8, Arwnd=16384) , UplinkNASTransport, Security mode complete, Registration request
1011	2025-02-27 17:37…	10.205.67.205	10.220.67.18	NGAP	InitialContextSetupRequest
1012	2025-02-27 17:37…	10.220.67.18	10.205.67.205	NGAP	SACK (Ack=9, Arwnd=16384) , UERadioCapabilityInfoIndication
1013	2025-02-27 17:37…	10.220.67.18	10.205.67.205	NGAP	InitialContextSetupResponse
1015	2025-02-27 17:37…	10.205.67.205	10.220.67.18	NGAP/NAS-5GS	DownlinkNASTransport, Registration accept
1016	2025-02-27 17:37…	10.220.67.18	10.205.67.205	NGAP/NAS-5GS	SACK (Ack=10, Arwnd=16384) , UplinkNASTransport, Registration complete
1017	2025-02-27 17:37…	10.205.67.205	10.220.67.18	NGAP/NAS-5GS	SACK (Ack=15, Arwnd=32768) , DownlinkNASTransport, Configuration update command
1021	2025-02-27 17:37…	10.220.67.18	10.205.67.205	NGAP/NAS-5GS	UplinkNASTransport, UL NAS transport, PDU session establishment request
1025	2025-02-27 17:37…	10.205.67.205	10.220.67.18	NGAP/NAS-5GS	PDUSessionResourceSetupRequest, DL NAS transport, PDU session establishment accept
1027	2025-02-27 17:37…	10.220.67.18	10.205.67.205	NGAP	PDUSessionResourceSetupResponse

Figure 78: UE Registration with Home Network (Home Network Wireshark Trace)

This test case's results demonstrated that the UE is vulnerable to a DoS attack if a false base station attempts to attract the UE, then forces it to reject registration by not allowing the UE to operate in the same PLMN as its home network.

8.3 Outcomes for Both 5G AKA and Null Encryption Tests

Expected Results:

The UE does not connect with the false base station. If the UE connects with the false base station, the UE ignores the RRMU reject message and waits for authentication to occur. If the UE accepts the RRMU reject message and goes into a state that does not allow it to connect to any 5G network, then it is vulnerable to the DoS attack.

Success Criteria:
The UE does not connect with the false base station. If the UE connects with the false base station, the UE ignores the RRMU reject message and waits for authentication to occur.

Test Results:
The test results demonstrate that the UE does not complete registration with the false base station. The FBS successfully prevents an authentication procedure and sends a registration reject message to UE with cause code #11 – "PLMN Not Allowed." As a result, the UE goes into a repetitive loop whereby the FBS continues rejecting registration on the same PLMN as the home network and the UE is unable to connect to either the FBS or the home network. However, once the FBS is powered OFF, the UE is able to register with the home network successfully. The results demonstrate that a UE is vulnerable to the DoS attack if a higher-powered false base station forces it to reject the registration by not allowing the UE to operate in the same PLMN as the home network.

Condition	Status
The UE does not connect with the FBS. If the UE connects with the FBS, the UE ignores the RRMU reject message and waits for authentication to occur.	
Overall Test	Failure

Test Case 9 – Attempting Authentication with Spoofed Public Warning System Message

Test Case ID: TC-FBS-9

Test Case Name: Attempting Authentication with Spoofed Public Warning System Message

Description:
This test case is designed to observe the UE's behavior when the FBS sends a SIB 8 spoofed Public Warning System (PWS) message with the Commercial Mobile Alert System (CMAS). The primary goal of this test is to confirm that the UE will ignore the PWS messages and maintain its connection with its home radio base station.

Objectives:

- Verify whether the UE receives a SIB 8 spoofed PWS message from the FBS.
- Observe the UE behavior and verify that UE ignores the PWS messages and maintains its connection with the home network.
- Verify whether the UE is vulnerable to the Denial-of-Service attack at any stage.

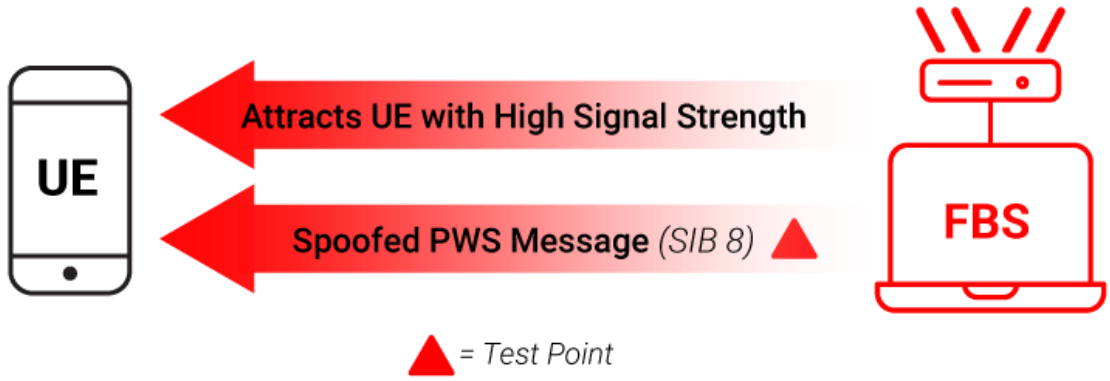


Figure 79: FBS Sends False PWS Message to the UE

9.1 5G AKA Test Results

As described and performed in Test Case 2, the 5G test UE initially established a connection and properly authenticated with its home network. The test IMSI remained added to the FBS Core network subscriber profile with random subscription key "K" and Operator code "OPc" values. For Test Case 9, the FBS RAN configuration was modified to transmit the SIB 8 PWS message containing "CMAS TEST" embedded within the SIB 1 broadcast message. The FBS Core and gNB docker container services were initialized and ensured the services were up and operational. The UE was then prompted by the higher-powered FBS to release its connection with the home

network. The UE, upon seeing a stronger signal being emitted from the FBS, attempted to connect to the FBS.

The MIB and SIB 1 messages broadcasted by the FBS were read by the UE, which also included the PWS message. The “sibType 8” message is shown in Figure 80 and Figure 81 as part of the SIB 1 message sent by the FBS in downlink direction to the UE. Although the 5G test UE did not display the CMAS message on the UE’s screen, the SI-Broadcasting status showed it as “broadcasting,” validating the SIB 8 sent by the FBS. Although the UE ignored the PWS message as expected, it proceeded to perform the RRC connection with the FBS.

The RRC connection to the FBS was successful, and as per the NAS procedure discussed in Section 2.1, the FBS requested the UE identity. The UE registration was rejected, as shown in Figure 82, with 5GMM cause code #9 – “UE identity cannot be derived by the network” due to the 5G SIM being encrypted. The network sent a context release message to the UE, and the protocol capture was recorded using the Wireshark tool.

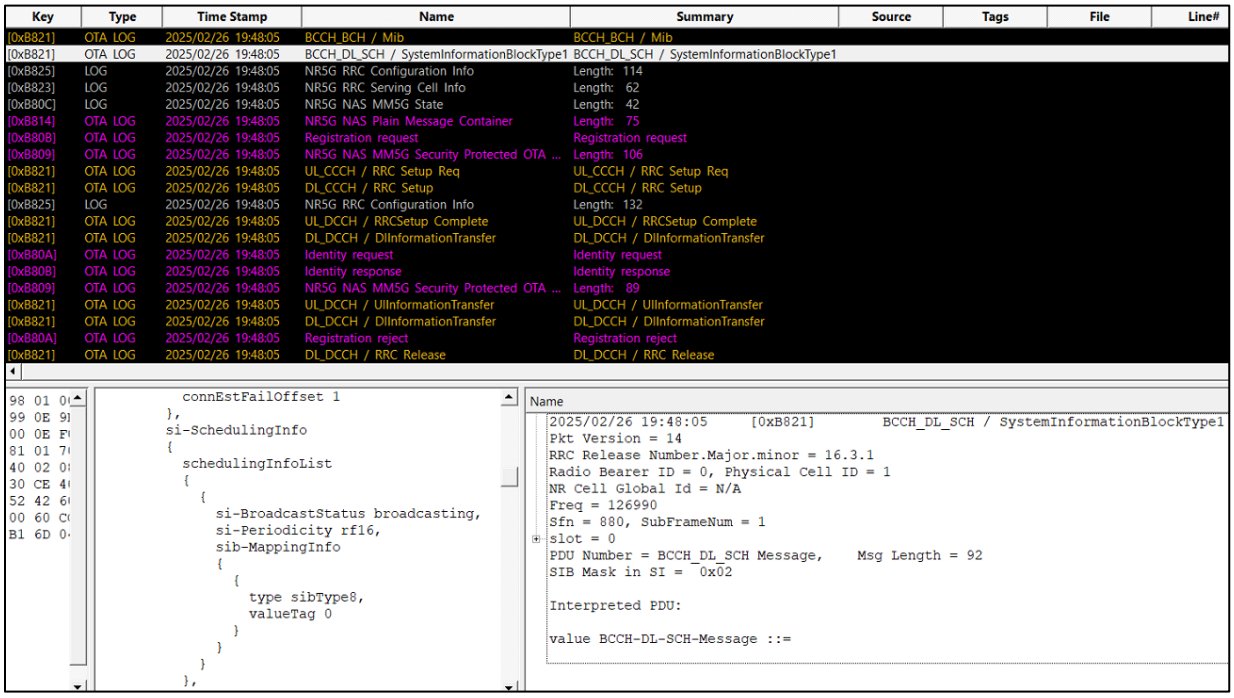


Figure 80: SIB 1 Message Containing the Spoofed PWS Message Broadcasting on the SIB 8 (UE QXDM Log)

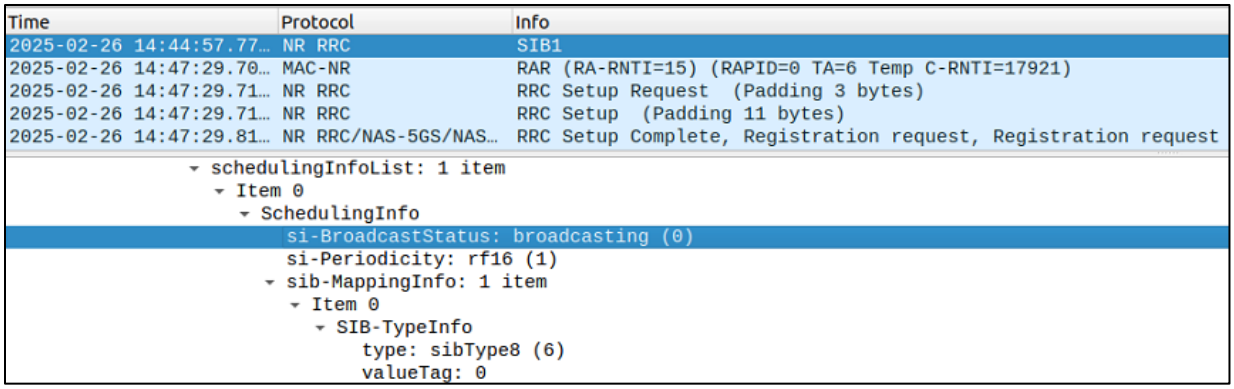


Figure 81: FBS RRC Logs (FBS Wireshark Trace)

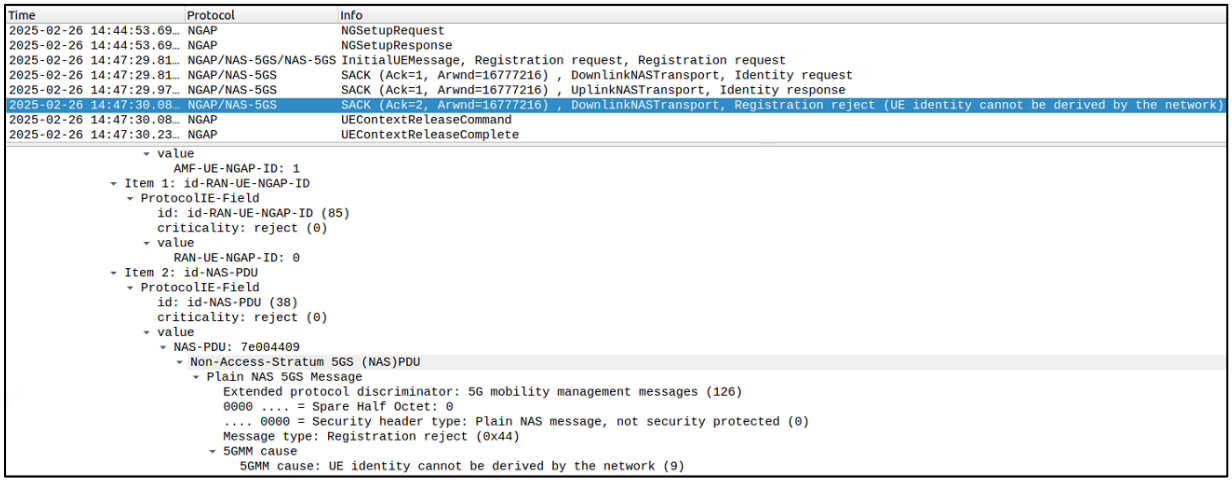


Figure 82: FBS NAS Registration Rejection (FBS Wireshark Trace)

The FBS Core and RAN services were then turned OFF. Upon disconnecting from the FBS network, the UE began performing a PLMN Search, immediately received a SIB 1 message from the home network, and attempted to reconnect. The UE initiated the registration procedure with the home network as per Figure 83, which shows the RRC connection setup procedure, NAS authentication and security mode procedure, and subsequent PDU session establishment between the UE and the 5G home network, demonstrating proper registration with the home Core network. The UE was then turned OFF, and the test team captured logs for each of the interfaces demonstrating the test case behavior.

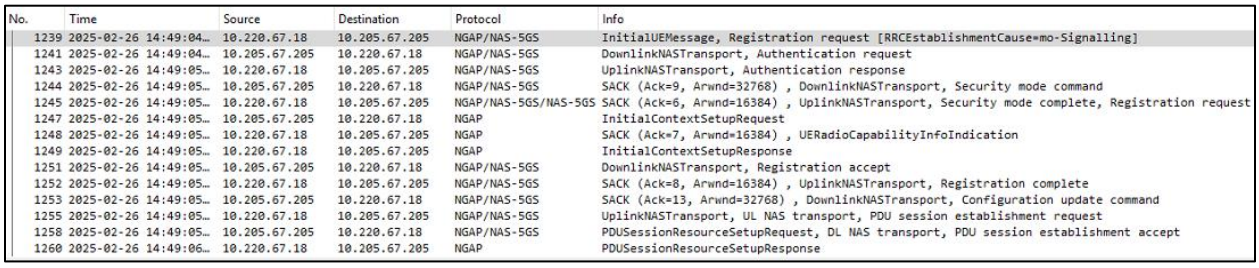


Figure 83: UE Registration with 5G Home Network (Home Network Wireshark Trace)

9.2 Null Encryption Test Results

As described and performed in Test Case 2, the 5G test UE initially established a connection and properly authenticated with the home network. The test IMSI remained added to the FBS Core network subscriber profile with random subscription key “K” and Operator code “OPc” values. For TC 9, the FBS RAN Configuration was modified to transmit the SIB 8 PWS message containing “CMAS TEST” embedded within the SIB 1 broadcast message. The FBS Core and gNB docker container services were initialized and ensured the services were up and operational. The UE was then prompted by the higher-powered FBS to release its connection with the home network.

The UE, upon seeing a stronger signal being emitted from the false base station, attempted to connect to it. The UE read the MIB and SIB1 messages broadcasted by the FBS, which also included the PWS message. The “sibType 8” message is shown in Figure 85 and Figure 85 as part of the SIB 1 message sent by the FBS in the downlink direction to the UE. Although the 5G test UE did not display the CMAS message on the UE’s screen, the SI-Broadcasting status showed it as “broadcasting,” validating the SIB 8 being sent by the FBS. Although the UE ignored the PWS message as expected, it proceeded to perform the RRC connection with the FBS.

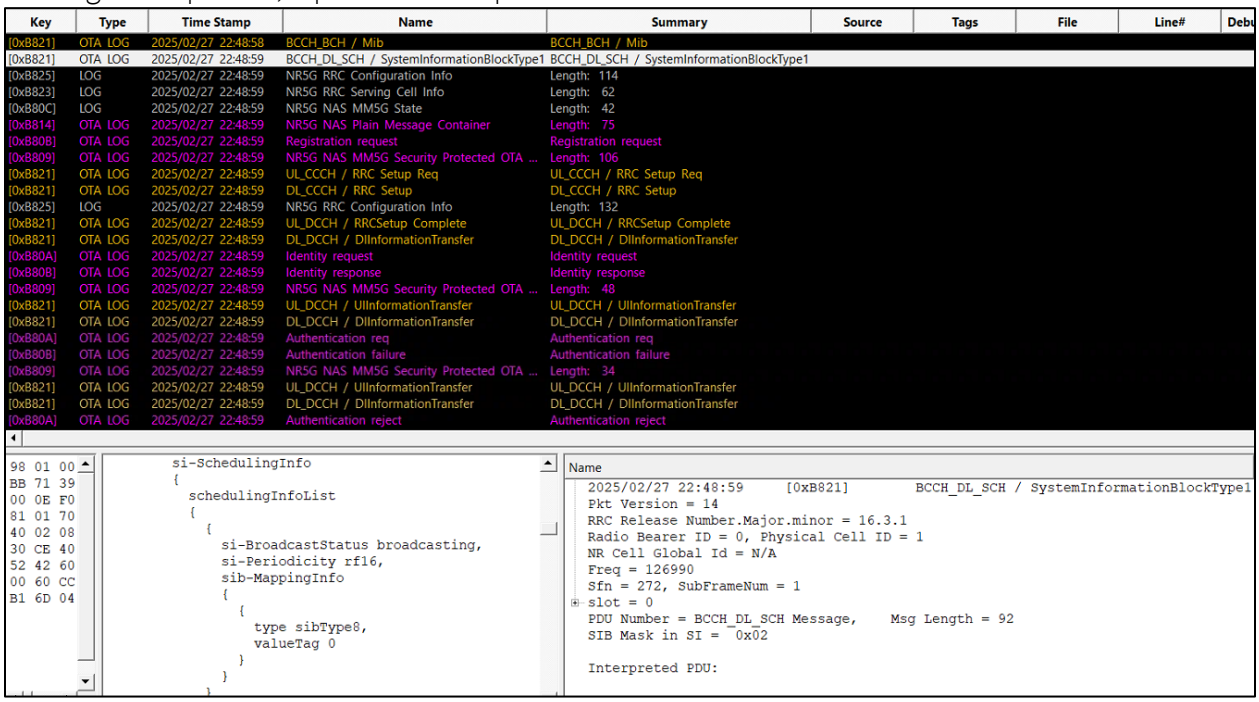


Figure 84: SIB 1 Message Containing the Spoofed PWS Message Broadcasting on SIB 8 (UE QXDM Log)

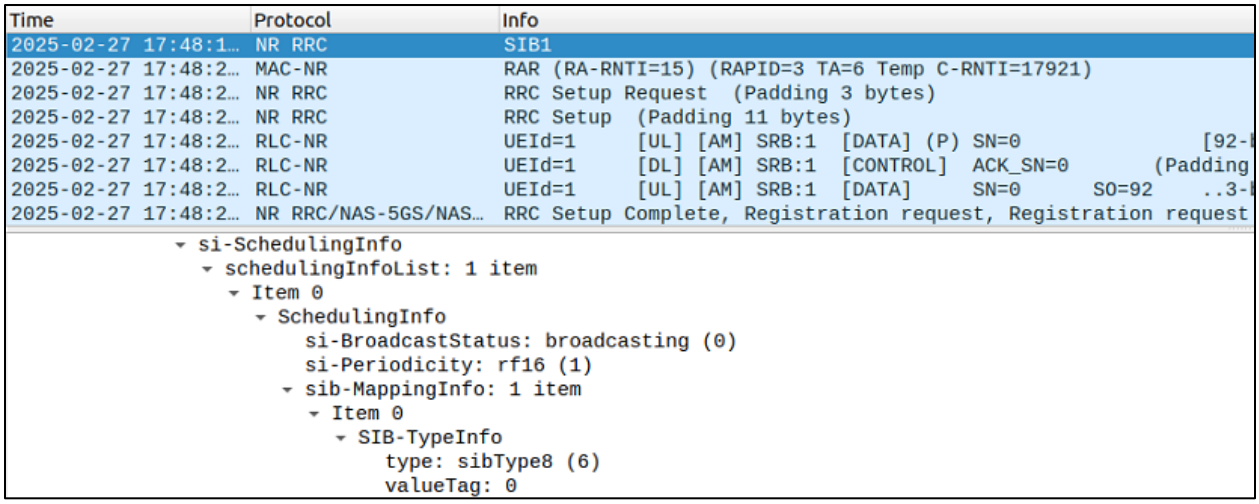


Figure 85: FBS RRC Logs (FBS Wireshark Trace)

The RRC connection to the FBS was successful, and as per the NAS procedure discussed in Section 4.2, the FBS initiated authentication procedures to authenticate the UE, but the UE rejected the authentication resulting in a 5G authentication failure as shown in Figure 86 with 5GMM cause code #20 – "MAC Failure" due to the 5G SIM not being encrypted. The network sent a context release message to the UE and the protocol capture was recorded using the Wireshark tool.

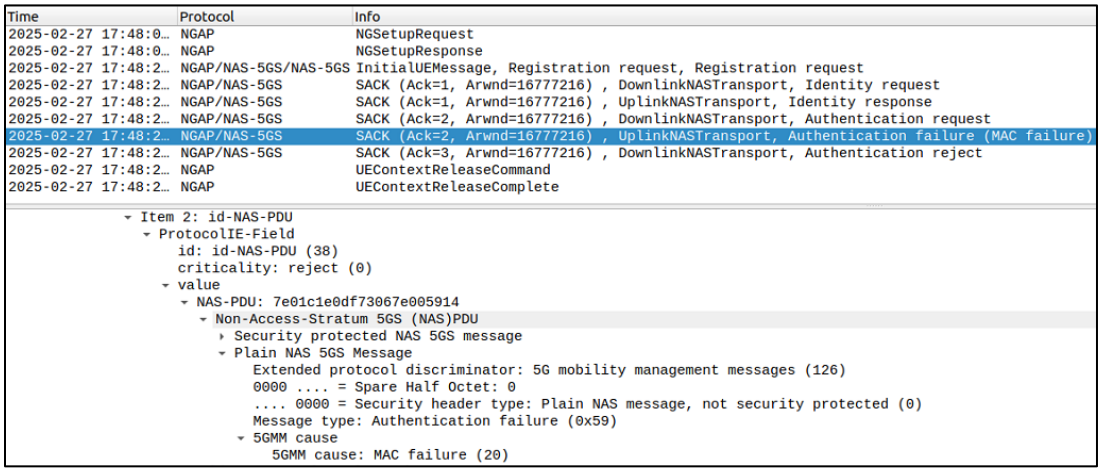


Figure 86: UE NAS Authentication Rejection (FBS Wireshark Trace)

The FBS Core and RAN services were then turned OFF. Upon disconnecting from the FBS network, the UE received a SIB 1 message from its home network and attempted to reconnect; however, the UE failed to connect to the home network. The UE entered an "Out of Service" state and remained deregistered from any network. Due to this behavior, the test team toggled the UE into Airplane Mode after which it registered properly with its home network. The test team captured logs for each of the interfaces demonstrating the test case behavior.

9.3 Outcomes for Both 5G AKA and Null Encryption Tests

Expected Results:
The UE ignores the spoofed PWS messages and maintains its connection with the home network.

Success Criteria:
The UE ignores the spoofed PWS messages and maintains its connection with the home network.

Test Results:
The test results verified that when the FBS sends a SIB 8 spoofed PWS message to the UE, the UE ignores the PWS CMAS message, as expected. For both test IMSIs, the UE proceeds to connect to the FBS but does not complete registration. With the 5G AKA SIM, once the FBS is powered OFF, the UE continues to perform a registration procedure with its home network and successfully completes registration. With the 5G Null encryption SIM, once the FBS is powered OFF, the UE is unable to reconnect with its home network unless the UE is toggled into Airplane Mode or power cycled. The test results demonstrated that a 5G UE with a Null encryption SIM is vulnerable to the DoS attack as it will not connect to its home network once the UE fails authentication ("MAC failure") with an FBS.

Condition	Status
The UE ignores the PWS messages and maintains its connection with the home radio base station.	
Overall Test	Failure

Test Case 10 – Attempting Authentication with Spoofed Public Warning System Message Followed by "PLMN Not Allowed" Message

Test Case ID: TC-FBS-10

Test Case Name: Attempting Authentication with Spoofed Public Warning System Message Followed by "PLMN Not Allowed" Message

Description:
This test case is designed to prompt the FBS to send the UE a SIB 8 spoofed Public Warning System message with a Commercial Mobile Alert System (CMAS) notification, then reject the UE's NAS registration with cause code #11 – "PLMN Not Allowed" (see Test Case 8). The goal of this test is to confirm that the UE will ignore the messages and maintain its connection with its home radio base station.

Objectives:

- Verify whether the UE receives the SIB 8 spoofed PWS message from the FBS.
- Configure the FBS to send the registration reject NAS message to the UE with the NAS reject cause "PLMN Not Allowed."
- Observe the UE behavior and verify that the UE ignores the PWS messages and maintains its connection with the home network.
- Verify if any at any stage the UE is vulnerable to the Denial-of-Service attack

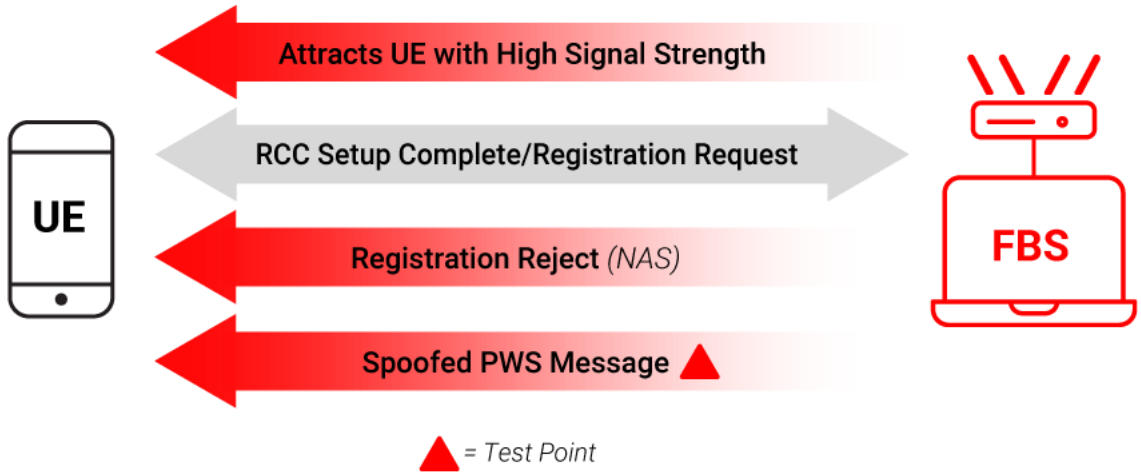


Figure 87: FBS Sends False PWS Message to the UE After a NAS Registration Reject

10.1 5G AKA Test Results

As described and performed in Test Case 2, the 5G test UE initially established a connection and properly authenticated with its home network. The test IMSI remained added to the FBS Core network subscriber profile with random subscription key "K" and Operator code "OPc" values. For Test Case 10, the FBS RAN configuration was modified to transmit a SIB 8 PWS message containing "CMAS TEST" embedded within the SIB 1 broadcast message. Similar to Test Case 8, the FBS Core configuration was also modified to include the NAS registration reject message with cause value #11 – "PLMN Not Allowed."

The FBS Core and gNB docker container services were initialized and ensured the services were up and operational. The UE was then prompted by the higher-powered FBS to release its connection with the home network. The UE, upon seeing a stronger signal being emitted from the FBS, attempted to connect to the FBS. The MIB and SIB1 messages broadcasted by the FBS were read by the UE, which also included the PWS message. The "sibType 8" message is shown in Figure 88 and Figure 89 as part of the SIB 1 message sent by the FBS in downlink direction to the UE. The 5G test UE did not display the CMAS message on the UE's screen, but the SI-Broadcasting status showed it as "broadcasting," validating the SIB 8 being sent by the FBS.

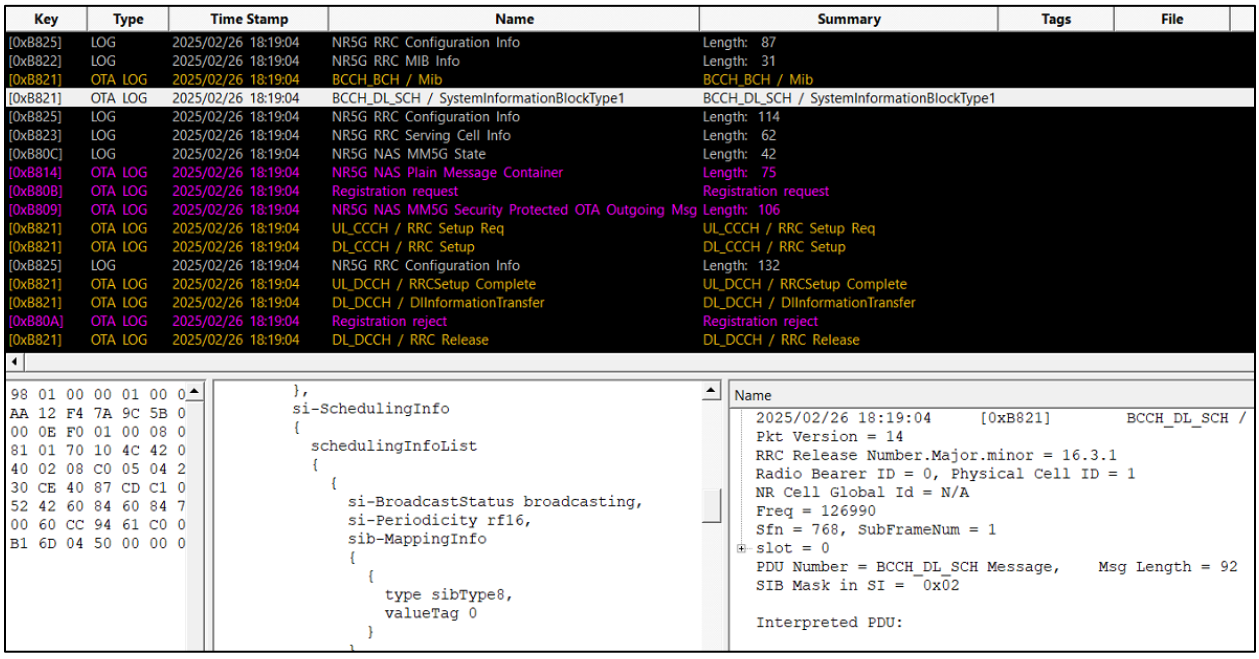


Figure 88: SIB 1 Message Containing the Spoofed PWS Message Broadcasting on SIB 8 (UE QXDM Log)

Time	Protocol	Info
2025-02-26 13:16:3…	NR RRC	SIB1
2025-02-26 13:18:2…	MAC-NR	RAR (RA-RNTI=15) (RAPID=3 TA=6 Temp C-RNTI=17921)
2025-02-26 13:18:2…	NR RRC	RRC Setup Request (Padding 3 bytes)
2025-02-26 13:18:2…	NR RRC	RRC Setup (Padding 11 bytes)
2025-02-26 13:18:2…	NR RRC/NAS-5GS/NAS…	RRC Setup Complete, Registration request, Registration request

```
▸ cellAccessRelatedInfo
▸ connEstFailureControl
▾ si-SchedulingInfo
  ▾ schedulingInfoList: 1 item
    ▾ Item 0
      ▾ SchedulingInfo
          si-BroadcastStatus: broadcasting (0)
          si-Periodicity: rf16 (1)
        ▾ sib-MappingInfo: 1 item
          ▾ Item 0
            ▾ SIB-TypeInfo
                type: sibType8 (6)
                valueTag: 0
```

Figure 89: FBS RRC Logs (FBS Wireshark Trace)

Although the UE ignored the PWS message as expected, it proceeded to perform an RRC connection with the false base station. The RRC connection to the FBS was successful, and similar to the results described in Section 7.1, upon receiving the mobility update registration request from the UE, the FBS Core network immediately sent a registration reject message to the UE with the cause code value #11 – "PLMN not allowed," as shown in Figure 90.

Key	Type	Time Stamp	Name	Summary
[0xB80A]	OTA LOG	2025/02/26 18:19:04	Registration reject	Registration reject
[0xB821]	OTA LOG	2025/02/26 18:19:04	DL_DCCH / RRC Release	DL_DCCH / RRC Release
[0xB80C]	LOG	2025/02/26 18:19:04	NR5G NAS MM5G State	Length: 42
[0xB825]	LOG	2025/02/26 18:19:04	NR5G RRC Configuration Info	Length: 87
[0xB80D]	LOG	2025/02/26 18:19:04	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/26 18:19:04	NR5G NAS MM5G State	Length: 42
[0xB822]	LOG	2025/02/26 18:19:04	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 18:19:04	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB825]	LOG	2025/02/26 18:19:04	NR5G RRC Configuration Info	Length: 87
[0xB822]	LOG	2025/02/26 18:19:04	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 18:19:04	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB801]	OTA LOG	2025/02/26 18:19:04	PDU session establishment req	PDU session establishment req
[0xB821]	OTA LOG	2025/02/26 18:19:04	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1
[0xB825]	LOG	2025/02/26 18:19:04	NR5G RRC Configuration Info	Length: 114
[0xB823]	LOG	2025/02/26 18:19:04	NR5G RRC Serving Cell Info	Length: 62
[0xB80C]	LOG	2025/02/26 18:19:04	NR5G NAS MM5G State	Length: 42
[0xB80B]	OTA LOG	2025/02/26 18:19:05	Registration request	Registration request
[0xB821]	OTA LOG	2025/02/26 18:19:05	UL_CCCH / RRC Setup Req	UL_CCCH / RRC Setup Req
[0xB821]	OTA LOG	2025/02/26 18:19:05	DL_CCCH / RRC Setup	DL_CCCH / RRC Setup
[0xB825]	LOG	2025/02/26 18:19:05	NR5G RRC Configuration Info	Length: 132
[0xB821]	OTA LOG	2025/02/26 18:19:05	UL_DCCH / RRCSetup Complete	UL_DCCH / RRCSetup Complete
[0xB821]	OTA LOG	2025/02/26 18:19:05	DL_DCCH / DlInformationTransfer	DL_DCCH / DlInformationTransfer
[0xB80A]	OTA LOG	2025/02/26 18:19:05	Registration reject	Registration reject
[0xB80C]	LOG	2025/02/26 18:19:05	NR5G NAS MM5G State	Length: 42
[0xB821]	OTA LOG	2025/02/26 18:19:05	DL_DCCH / RRC Release	DL_DCCH / RRC Release
[0xB825]	LOG	2025/02/26 18:19:05	NR5G RRC Configuration Info	Length: 87
[0xB80D]	LOG	2025/02/26 18:19:05	NR5G NAS MM5G Service Request	Length: 185
[0xB80C]	LOG	2025/02/26 18:19:05	NR5G NAS MM5G State	Length: 42
[0xB822]	LOG	2025/02/26 18:19:05	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 18:19:05	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB825]	LOG	2025/02/26 18:19:05	NR5G RRC Configuration Info	Length: 87
[0xB822]	LOG	2025/02/26 18:19:05	NR5G RRC MIB Info	Length: 31
[0xB821]	OTA LOG	2025/02/26 18:19:05	BCCH_BCH / Mib	BCCH_BCH / Mib
[0xB821]	OTA LOG	2025/02/26 18:19:05	BCCH_DL_SCH / SystemInformationBlockType1	BCCH_DL_SCH / SystemInformationBlockType1

```
98 01 00 00 01 00 0
F2 26 30 7D 9C 5B 0
00 44 0B
```

```
security_header = 0 (0x0)
msg_type = 68 (0x44) (Registration reject)
nr5g_mm_msg
  registration_reject
    _5gmm_cause = 11 (0xb) (PLMN not allowed)
    t3346 incl = 0 (0x0)
```

Figure 90: FBS NAS Registration Rejection (UE QXDM Log)

The false base station then sent a UE context release message to the UE, and the registration process was terminated. After the registration reject in the first attempt, the UE again read the MIB and SIB 1 messages broadcasted by the FBS, which included the PWS message and resent a registration request (initial registration as discussed in Section 2.2) to the FBS, but the FBS rejected the registration with the same cause code value, sending the UE into a repetitive loop whereby it was unable to connect to the FBS or home network, as shown in Figure 91.

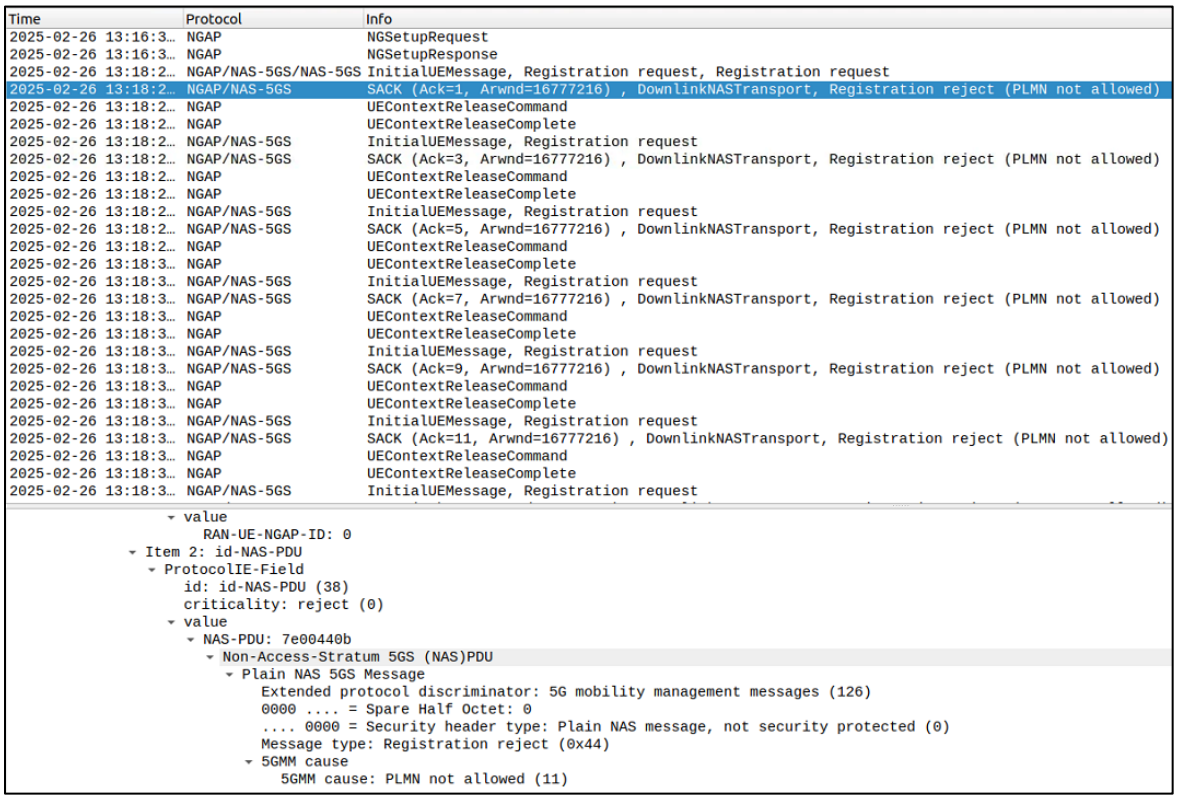


Figure 91: Multiple NAS Registration Rejections (FBS Wireshark Trace)

The network sent a context release message to the UE, and the protocol capture was recorded using the Wireshark tool. The FBS Core and RAN services were then turned OFF. Upon disconnecting from the FBS network, the UE began performing a PLMN search, immediately received an SIB 1 message from the 5G home network, and attempted to reconnect. The UE initiated the registration procedure with the home network, which contained the RRC connection set up procedure, NAS authentication and security mode procedure, and subsequent PDU session establishment, demonstrating proper registration with the home Core network. The UE was then turned OFF, and the test team captured logs for each of the interfaces demonstrating the test case behavior.

This test case's results demonstrated that a UE is vulnerable to the DoS attack if a false base station attempts to attract a UE and then forces it to reject the registration by not allowing the UE to operate in the same PLMN as the home network.

10.2 Null Encryption Test Results

As described and performed in Test Case 2, the 5G test UE initially established a connection and properly authenticated with the home network. The test IMSI remained added to the FBS Core network subscriber profile with random subscription key “K” and Operator code “OPc” values. For Test Cases 9 and 10, the FBS RAN configuration was modified to transmit the SIB 8 PWS message containing “CMAS TEST” embedded within the SIB 1 broadcast message. Similar to Test Case 8, the FBS Core configuration was also modified to include the NAS registration reject message with cause value #11 – “PLMN Not Allowed.” The FBS Core and gNB docker container services were initialized and ensured the services were up and operational. The UE was then prompted by the higher-powered FBS to release its connection to home network.

The UE, upon seeing a stronger signal being emitted from the false base station, attempted to connect to the FBS. The UE read the MIB and SIB1 messages broadcasted by the false base station, which also included the PWS message. The “sibType 8” message is shown in Figure 92 and Figure 93 as part of the SIB 1 message sent by the FBS in the downlink direction to the UE.

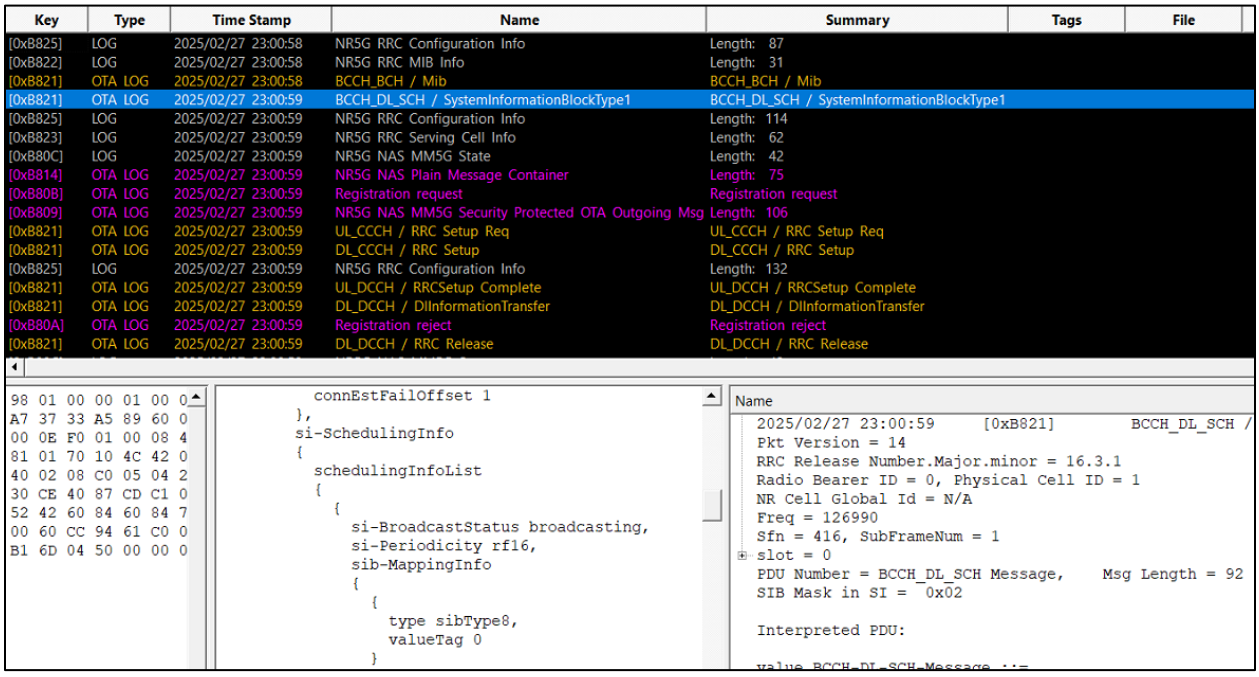


Figure 92: SIB 1 Message Containing the Spoofed PWS Message Broadcasting on SIB 8 (UE QXDM Log)

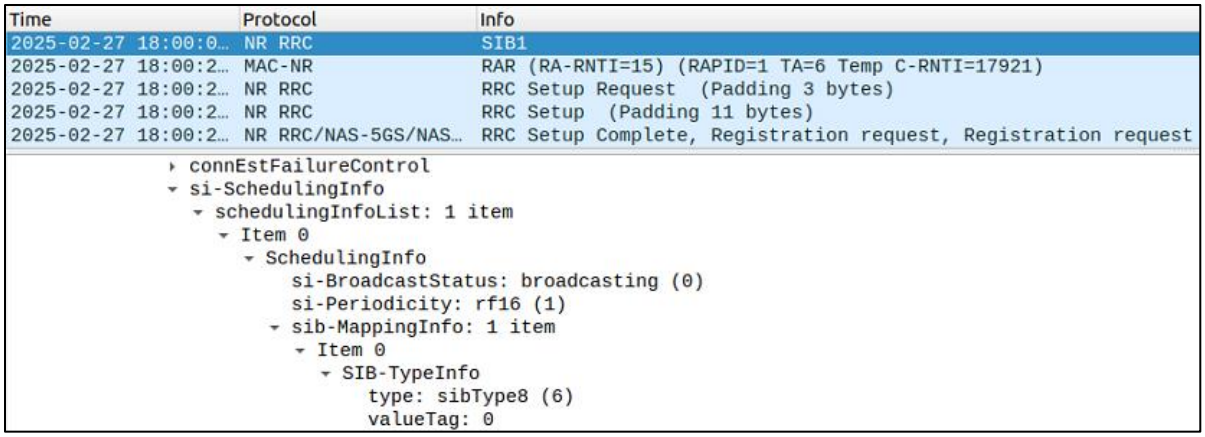


Figure 93: FBS RRC Logs (FBS Wireshark Trace)

The 5G test UE did not display the CMAS message on the UE's screen, but the SI-Broadcasting status showed it as "broadcasting," validating SIB 8 being sent by the FBS. Although the UE ignored the PWS message as expected, it proceeded to perform an RRC connection with the FBS. The RRC connection was successful, and similar to the results described in Section 7.1, upon receiving the mobility update registration request from the UE, the FBS Core network immediately sent a registration reject message to the UE with the cause code value #11 – "PLMN not allowed," as shown in Figure 94.

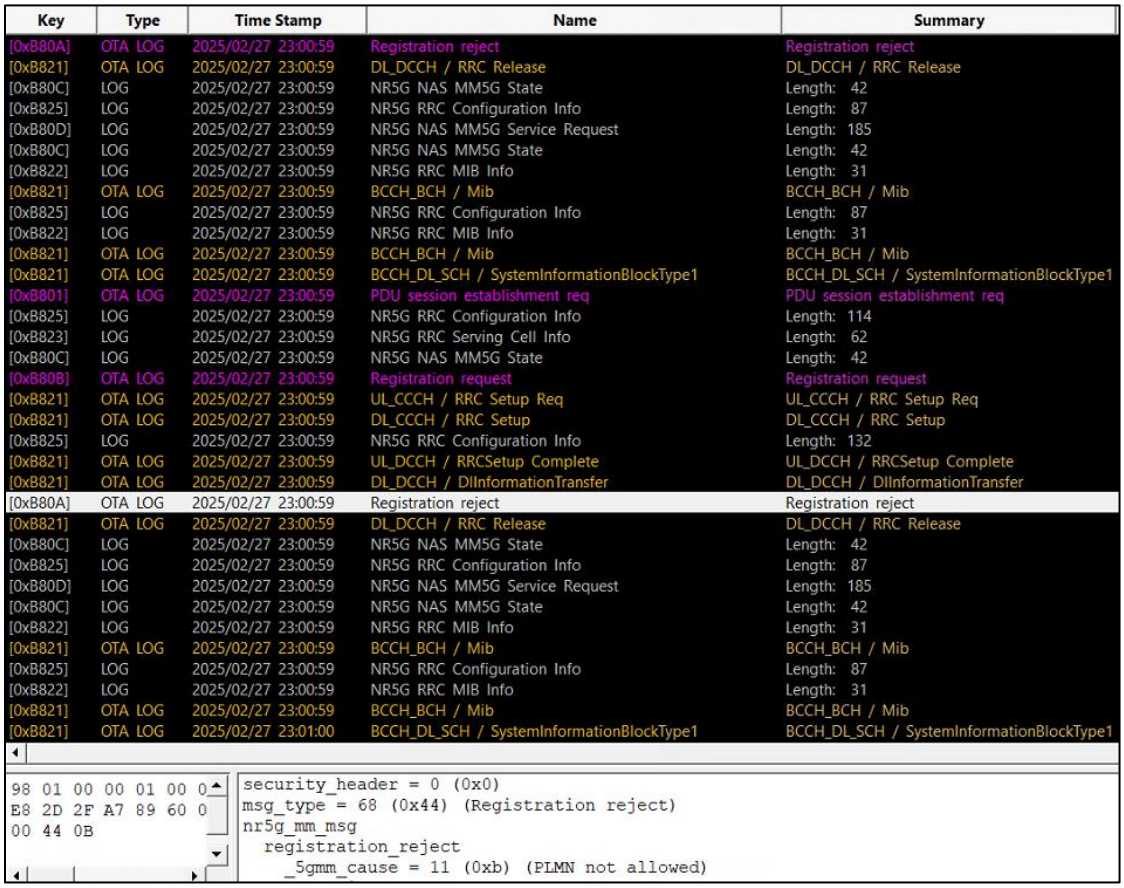


Figure 94: False Base Station NAS Registration Rejection (UE QXDM log)

After the registration reject in the first attempt, the UE again read the MIB and SIB 1 messages broadcasted by the FBS, which included the PWS message. The UE then re-sent a registration request (initial registration, as discussed in Section 2.2) to the FBS, but the FBS rejected the registration with the same cause code value, causing the UE to enter a repetitive loop whereby it was unable to connect to the FBS or home network, as shown in Figure 95.

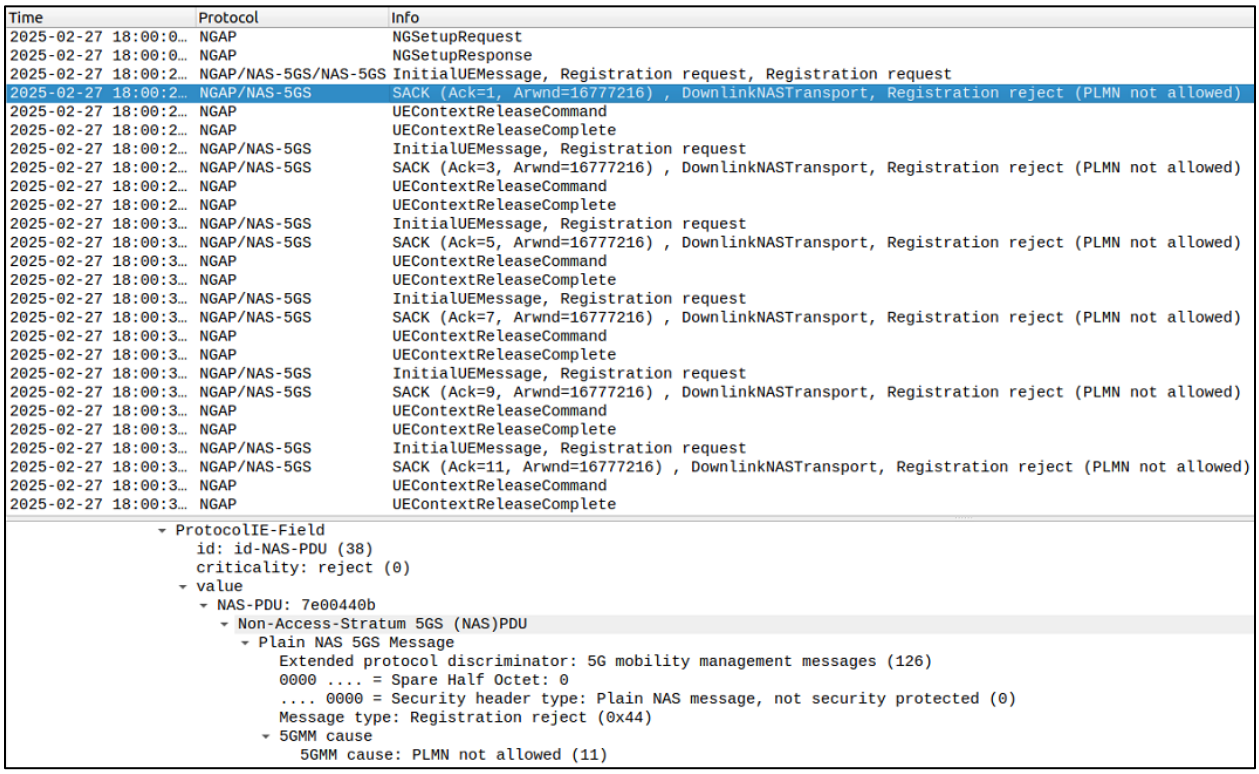


Figure 95: Multiple NAS Registration Rejections (FBS Wireshark Trace)

The network sent a context release message to the UE, and the protocol capture was recorded using the Wireshark tool. The FBS Core and RAN services were then turned OFF. Upon disconnecting from the FBS network, the UE began performing PLMN search, immediately received a SIB 1 message from the 5G home network, and attempted to reconnect. The UE initiated the registration procedure with the home network, which contains the RRC connection setup procedure, NAS authentication and security mode procedure, and subsequent PDU session establishment, demonstrating proper registration with the home Core network. The UE was then turned OFF, and the test team captured logs for each of the interfaces demonstrating the test case behavior.

This test case's results demonstrated that a UE is vulnerable to the DOS attack if a false base station attempts to attract a UE and then forces it to reject the registration by not allowing the UE to operate in the same PLMN as the home network.

10.3 Outcomes for Both 5G AKA and Null Encryption Tests

Expected Results:
The UE ignores the false base station's Public Warning System messages and maintains its connection with its home radio base station.

Success Criteria:
The UE ignores the false base station's Public Warning System messages and maintains its connection with its home radio base station.

Test Results:
The test results verified that when the FBS sends a SIB 8 spoofed PWS message to the UE, the UE ignores the PWS CMAS message and proceeds to connect to the FBS. At the mobility update registration request from the UE, the FBS then sends a registration reject message to the UE with cause code #11 and does not complete the registration. As a result, the UE goes into a repetitive loop whereby the FBS continues rejecting registration on the same PLMN as the home network and the UE is unable to connect to the FBS or its home network. However, once the FBS is powered OFF, the UE is able to register with its home network successfully. The test results demonstrate that a UE is vulnerable to a DoS attack if a higher-powered false base station forces it to reject NAS registration by not allowing the UE to operate in the same PLMN as its home network.

Condition	Status
The UE ignores the spoofed Public Warning System messages and maintains its connection with its home radio base station.	
Overall Test	Failure

Conclusion

For each of the test cases developed for the false base station use cases, the 5G Security Test Bed successfully executed each step as outlined in the detailed test plan, incorporating real-world conditions in a lab environment on a 5G SA network utilizing different SIM profiles: 5G AKA and null encryption. The test team implemented custom modifications to the FBS open-sourced software configurations enabling implementation of different scenarios for various test cases.

Test Results Summary

As discussed in the detailed test results, the majority of the test case scenarios were successfully validated as they met the success criteria and provided expected test results. Table 3 summarizes the test results and observations of the successful test cases, noting any differences in behavior and responses observed based on the SIM profile in use. Test Cases 1 through 5, along with Test Case 7, demonstrated that the false base station was able to establish an RRC connection with the 5G test UE but was not able to complete registration or authentication with a 5G UE associated with a valid home network, as expected. Despite the attempt by the false base station to connect to the UE, the UE disconnected from the FBS after a registration attempt.

Table 3: Test Results Summary – Successes

Test Cases	Test Description	Profile N Null Scheme SIM		Profile B 5G AKA SIM		Comments
		Test Results	Success/ Failure	Test Results	Success/ Failure	
TC 1	Establishing UE RRC Connection	FBS RRC connection established but registration is rejected with 5GMM Cause - 'PLMN not allowed'	Success	FBS RRC connection established but registration is rejected with 5GMM Cause - 'UE Identity cannot be derived by the network'	Success	
TC 2	Establishing UE RRC Connection After Forced Disconnect from Home Radio Base Station	FBS RRC connection established but registration is rejected with 5GMM Cause - 'PLMN not allowed'	Success	FBS RRC connection established but registration is rejected with 5GMM Cause - 'UE Identity cannot be derived by the network'	Success	Same as TC 1 but UE attached to home network prior. Test IMSIs not added to the FBS Core subscription profile
TC 3	Attempting Authentication After Omitting Authentication Handshake	FBS sends NAS registration accept but UE disconnects from FBS	Success	FBS sends NAS registration accept but UE disconnects from FBS	Success	

TC 4	Attempting Authentication Handshake Using Random Identifiers	UE rejects authentication with 5GMM Cause - "MAC Failure"	Success	UE rejects authentication with 5GMM Cause - "MAC Failure"	Success	* Test IMSIs added to the FBS Core network subscriber profile * FBS Core configuration modified to include test IMSI into the unified data management (UDM) of FBS to force authentication
TC 5	Attempting Authentication Handshake Using Replayed Credentials	UE rejects authentication with 5GMM Cause - "MAC Failure"	Success	UE rejects authentication with 5GMM Cause - "MAC Failure"	Success	* Test IMSIs added to the FBS Core network subscriber profile * FBS Core configuration modified to include test IMSI into the unified data management (UDM) of FBS to force authentication
TC 7	Conducting DoS Attack Using "Cell Barred" Message	UE does not connect to FBS or home network	Success	UE does not connect to FBS or home network	Success	

Table 4 shows the remaining four test cases that did not meet the success criteria and expected test results, exposing potential vulnerabilities on the 5G UE in the presence of the false base station. The TC 6 test results demonstrate the vulnerability of a 5G UE to a DoS attack as the 5G UE is unable to reconnect with the home network after the FBS initiates a forced registration reject with a specific 5GMM cause. Similarly, TCs 8 and 10 demonstrate that a 5G UE can receive a spoofed PWS message and then initiate multiple registrations in a loop with the FBS, resulting in the 5G UE being vulnerable to such a DoS attack.

Table 4: Test Results Summary – Vulnerabilities

Test Cases	Test Description	Profile N Null Scheme SIM		Profile B 5G AKA SIM		Comments
		Test Results	Success/ Failure	Test Results	Success/ Failure	
TC 6	Conducting DoS Attack Using "5GS Services Not Allowed" Message	FBS rejects registration with 5GMM Cause - '5GS Services Not Allowed' but does not reconnect to Home Network	Failure	FBS rejects registration with 5GMM Cause - '5GS Services Not Allowed' but does not reconnect to Home Network	Failure	UE is vulnerable to Denial-of-Service attack as the UE is unable to reconnect with the home RAN network
TC 8	Conducting DoS Attack Using "PLMN Not Allowed" Message	FBS rejects registration with 5GMM Cause - 'PLMN Not Allowed'.	Failure	FBS rejects registration with 5GMM Cause - 'PLMN Not Allowed'.	Failure	UE is vulnerable to Denial-of-Service attack as UE keeps on sending registration requests to FBS in a loop until FBS is powered off
TC 9	Attempting Authentication with Spoofed Public Warning System Message	UE ignores spoofed PWS CMAS alert message. UE rejects authentication with 5GMM Cause - "MAC Failure"	Failure	UE ignores spoofed PWS CMAS alert message. FBS registration is rejected with 5GMM Cause - 'UE Identity cannot be derived by the network	Success	* UE ignores False PWS message and attempts to register to FBS * 5G Null IMSI is unable to reconnect to home network

TC 10	Attempting Authentication with Spoofed Public Warning System Message Followed by "PLMN Not Allowed" Message	UE ignores spoofed PWS CMAS alert message. FBS rejects registration with 5GMM Cause - 'PLMN Not Allowed'.	Failure	UE ignores spoofed PWS CMAS alert message. FBS rejects registration with 5GMM Cause - 'PLMN Not Allowed'.	Failure	* UE ignores False PWS message and attempts to register to FBS * UE is vulnerable to Denial-of-Service attack as UE keeps on sending registration requests to FBS in a loop until FBS is powered off

In summary, most of the test cases when conducted across both SIM profiles (TCs 1, 2, 3, 4, 5, and 7), and one test case when conducted using the 5G AKA SIM (TC 9), successfully demonstrated that the false base station was unable to conduct a DoS attack. The results of these test cases demonstrate the resilience of 5G in overcoming false base station attacks in these scenarios. However, three test cases when executed across both SIM profiles (6, 8, and 10), and one test case when conducted using the Null profile (9), highlighted that the false base station could potentially conduct a DoS attack by preventing the UE from reconnecting with its home network.

It should be noted that for test cases 6, 7, 8, 9 and 10, the UE's SIM was added to the false base station's subscriber database. This, in turn, requires the attacker to have physical access to the SIM, which is highly improbable, as the subscriber's identity in 5G is always encrypted—except in the rare instances when the user is accessing emergency services.

Notwithstanding the successful false base station attacks, the device with the 5G AKA SIM was able to recover from all of the attacks after the FBS was turned off, or after the device was reset, and it never revealed any private identifiers. It is important to note that, although some tests are done with Null encryption, the Null scheme is never used on U.S. networks except during emergency services (e.g. when the user calls 911), as per recommendations from the Federal Communications Commission's (FCC) Communications Security, Reliability, and Interoperability Council (CSRIC).[v] U.S. wireless operators follow CSRIC recommendations, and as such, 5G devices are always protected with 5G AKA encryption protocols except in very rare cases.

Vulnerabilities Summary

Based on these test results, the vulnerabilities for each of the SIM profiles are summarized below:

5G AKA SIM Vulnerabilities:

- If the FBS Core configuration is modified to force an authentication procedure, and if the authentication is rejected by the UE with a "MAC failure" cause code, then the UE needs to be reset in order to reconnect with its home network once the false base station is powered off.
- If the FBS rejects the UE's registration with a "5GS Services Not Allowed" cause code, then the UE needs to be reset in order to reconnect with its home network once the false base station is powered off.

- If the FBS rejects the UE's registration with a "PLMN not allowed" cause code, then the UE continues to request registration to the FBS in a repetitive loop, not allowing the UE to reconnect with the home radio network until the false base station is powered off.

5G Null Profile SIM Vulnerabilities:

- If the authentication is rejected by the FBS with a "MAC failure" cause code, then the UE never reconnects back with its home network once the FBS is powered off.
- If the FBS rejects registration with a "5GS Services Not Allowed" cause code, then the UE never reconnects back with its home network once the FBS is powered off.
- If the FBS rejects the UE's registration with a "PLMN Not Allowed" cause code, or if the test IMSIs are not added to the FBS Core network subscriber profile, then the UE continues to request registration to the FBS in a repetitive loop, not allowing the UE to reconnect with RAN network until the FBS is powered off.

Common UE Behaviors Summary

The test team also observed some common UE behaviors depending upon certain test conditions that are highlighted below. These conditions were observed and validated for TC 2 through TC 10.

RRC Connection:

- The UE establishes a successful RRC connection for all test cases with the UE receiving MIB and SIB 1 messages from the FBS.

FBS Registration:

- The UE sends a registration request type as "mobility update registration" – the UE switches between two networks (its home network and the FBS) that have a different tracking area.
- For the UE using a 5G AKA SIM, the FBS rejects registration due to no matching identity/context stored in the FBS network.
- For the 5G Null encryption SIM –
    - If the test IMSI is added to the FBS Core network profile, the FBS proceeds with authentication, but the UE rejects the authentication due to the "MAC Failure" message.
    - If the test IMSI is not added to the FBS Core network profile, the FBS does not proceed with authentication and rejects the registration with "PLMN Not Allowed."

GUTI/SUCI Information:

- The UE sends a stored 5G-GUTI allocated by the home 5G Core to the new FBS 5G Core during the registration request.
- The FBS 5G Core does not recognize the GUTI and requests the UE to provide its SUCI.
- The FBS 5G Core sends an identity request to the UE, and the UE responds with a SUCI in the case of 5G AKA SIM, and with a SUPI in case of the 5G Null encryption SIM.

Next Steps

The potential vulnerabilities listed in Table 4 were observed with a single test device, but are expected to occur with other commercial UE devices. It is recommended that, as part of Phase II testing, test cases 6, 8, 9, and 10 be repeated with other vendor devices that are capable of connecting with the 5G Security Test Bed's private network. Resilience and recovery from FBS attacks can also be improved at the device level by shortening the wait timers defined in the 3GPP standards, which "[give] an opportunity to UEs to recover and avoid lock-outs," as 3GPP notes in its technical specifications.

As new participants and the diversity of test cases grow, the 5G Security Test Bed will continue contributing to the evolving future of 5G network security. The Test Bed continues to explore testing of network function security, roaming security, and aspects of 5G cloud security that arise with use of the Network Exposure Function (NEF), the Application Function (AF), and Multi-access Edge Computing (MEC). The Test Bed is also exploring opportunities to test configurations and enhance Open Radio Access Network (Open RAN) security.

About the 5G Security Test Bed

The 5G Security Test Bed reflects the industry's collaborative approach to 5G security—it was created by the Cybersecurity Working Group (CSWG), an industry initiative that convenes the world's leading telecom and tech companies to assess and address the present and future of cybersecurity. The Test Bed's members are wireless providers AT&T, T-Mobile, and UScellular; industry partners Ericsson, the MITRE Group, SecureG, Intel, and Syniverse; and academic partners the University of Maryland and Virgina Tech Advanced Research Corporation (VT-ARC).

The 5G Security Test Bed has a Technical Advisory Committee (TAC) made up of its members and the Test Bed Administrator. The TAC advises the Test Bed Administrator on the day-to-day technical and operational activities and decisions related to the Test Bed, including but not limited to: development of use cases to be tested, test plan development and review, raw test data analysis, test result and report generation, and development of recommendations to standards bodies based on results.

The 5G Security Test Bed further works with a broad array of government agencies, policymakers, international standards bodies, thought leaders, and partners in the telecommunications and information technology sectors. These groups include the 3rd Generation Partnership Project (3GPP), the International Telecommunication Union (ITU), the Department of Homeland Security (DHS), the National Institute of Standards and Technology (NIST), and the Federal Communications Commission (FCC), among others.

The 5G Security Test Bed Uses Real-World Equipment, Validating Real-World Applications

Real-World Testing

The 5G Security Test Bed advances wireless security by:

- Conducting real-world tests in a rigorous, transparent, and replicable manner that can assess and validate theoretical and policy concerns and overcome hypothetical laboratory testing limitations.
- Drawing on the expertise of government, wireless providers, and equipment manufactures to evaluate specific use cases and support new equipment development.
- Testing security functionality in different scenarios, enabling industry and government to identify, mitigate, and respond to evolving threats while protecting consumers, businesses, and government agencies.

Real-World Applications

The 5G Security Test Bed's tests and outcomes support several applications that can drive new technology and transform cities, government, and industries. Use cases include government and enterprise applications, general network security protections, and smart city applications such as:

- Primary Use Cases: Network Security
  - Protecting Information in Transit
  - Roaming Security
  - Subscriber Privacy
  - Zero Trust Network Security
  - False Base Station Detection and Protection
  - 5G Cloud Network Security
- Secondary Use Cases: Devices and Applications
  - High-Resolution Video Surveillance (e.g. Smart Cities, Large Venues)
  - LTE/5G Drones with High-Resolution Video Feedback (e.g. Smart Cities)
  - Dynamic Supply Chain Verification (Real-Time Monitoring and Logistics)
  - Automated, Reconfigurable Factories
  - Autonomous Vehicles
  - Immersive AR/VR

For more information, or to participate in the 5G Security Test Bed, please contact Harish Punjabi (hpunjabi@ctia.org; (202) 845-5701), or visit https://5gsecuritytestbed.com/.

Appendix: Acronyms

3GPP	Third Generation Partnership Project
5G AKA	5G Authentication and Key Agreement
5GMM	5G Mobility Management
5G STB	5G Security Test Bed
5GS	5G System
BBU	Baseband Unit
CMAS	Commercial Mobile Alert System
CSRIC	Communications Security, Reliability, and Interoperability Council
DoS	Denial-of-Service
FBS	False Base Station
FCC	Federal Communications Commission
gNB/gNodeB	Next Generation Node B
GUTI	Global Unique Temporary Identifier
IMSI	International Mobile Subscriber Identity
MAC	Message Authentication Code
MCC	Mobile Country Code
MIB	Master Information Block
MNC	Mobile Network Code
MSIN	Mobile Subscriber Identification Number
NAS	Non-Access Stratum
NUC	Next Unit of Computing
OPc	Operator Code
PCI	Physical Cell Identity
PLMN	Public Land Mobile Network
PWS	Public Warning System
QXDM	Qualcomm eXtensible Diagnostic Monitor
RAN	Radio Access Network
RBS	Radio Base Station
RRC	Radio Resource Control
RRMU	Registration Request of type “Mobility Update”
RSRP	Reference Signal Received Power
SA	Standalone
SDR	Software-Defined Radio
SIB	System Information Block
SIM	Subscriber Identity Module
STB	Security Test Bed
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TA	Tracking Area
TAC	Technical Advisory Committee
TP	Test Point

UDM	Unified Data Management
UE	User Equipment
USRP	Universal Software Radio Peripheral
VT-ARC	Virginia Tech Applied Research Corporation

References

[i] See CSRIC VII WG3, Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security (Mar. 2021), https://www.fcc.gov/file/20606/download.

[ii] See 3GPP TS 24.301 rel. 17.

[iii] See 3GPP TS 38.213 Physical layer procedures for control and 3GPP TS 38.331 Radio Resource Control (RRC) protocol specification.

[iv] See 3GPP TS 24.501.

[v] See CSRIC VII WG3, Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security (Mar. 2021), https://www.fcc.gov/file/20606/download.