

False Base Station

Applying 5G Cybersecurity and Privacy Capabilities

NIST Cybersecurity White Paper

NIST CSWP 36G ipd

Michael Bartock

Jeffrey Cichonski

*Information Technology
Laboratory*

Parisa Grayeli

Sanjeev Sharma

The MITRE Corporation

September 2026

Initial Public Draft

Abstract

This white paper is part of a series called Applying 5G Cybersecurity and Privacy Capabilities, which covers 5G cybersecurity- and privacy-supporting capabilities that were implemented as part of the [5G Cybersecurity testbed](#) at the National Cybersecurity Center of Excellence (NCCoE). This white paper provides details regarding security risks posed by False Base Stations (FBS) in 5G networks. It details how the availability of inexpensive, off-the-shelf hardware and software tools allows attackers to simulate legitimate cells and exploit pre-authentication vulnerabilities. Incremental standards improvements over several generations have addressed many of the risks posed by FBS, limiting privacy breaches and location tracking for users and making FBS less effective against 5G devices. This white paper evaluates multiple FBS scenarios using the NCCoE 5G Cybersecurity testbed to assess how the tested 5G devices respond to FBS attacks, including when they are still vulnerable to Denial-of-Service (DoS) attacks. It identifies areas for improvement in standards and available device-configurable protections.

Audience

Technology, cybersecurity, and privacy professionals who are involved in using, managing, or providing 5G-enabled services and products. This includes commercial mobile network operators, potential private 5G network operators, and end-user organizations. Readers should already be familiar with the basics of mobile network architecture and components.

Keywords

3GPP, 5G, cybersecurity, privacy, False Base Station, Fake Base Station, Rogue Base Station, Software Defined Radio.

Note to Reviewers

NIST is particularly interested in your feedback on the following questions:

1. How do you envision using this paper? What changes would you like to see to improve that use?
2. What additional information would you like this paper to provide?
3. What other 5G cybersecurity and privacy capabilities are you most interested in learning more about?

Acknowledgments

We are grateful to the following individuals for their generous contributions.

AMI: Muthukkumaran Ramalingam, Stefano Righi

AT&T: Jitendra Patel, Bogdan Ungureanu

CableLabs: Tao Wan

Cisco: Kori Rongey

Dell Technologies: Dan Carroll

Intel Corporation: Steve Orrin

Keysight Technologies: Corey Piggott

The MITRE Corporation: John Kent, Theresa Suloway*, Thomas Walters

NIST: Cherilyn Pascoe, Kevin Stine

Nokia Federal Solutions: Jorge Escobar, Michael Hammons

Palo Alto Networks: Aarin Buskirk, Julie Klein

T-Mobile: Todd Gibson

* Former employee; all work for this publication was done while at that organization

Overview

The term ‘False (aka Rogue or Fake) Base Station’ or FBS [\[1\]\[2\]](#) is used to imply a system which impersonates a real carrier radio access network (RAN). It transmits and receives radio signals that mimic a legitimate 5G cell. An FBS tricks unsuspecting device aka User Equipment (UE), to connect to it. This potentially creates cybersecurity risks, including service degradation, privacy breaches, and location tracking for the user. With each successive generation of cellular standards, incremental mitigations have been developed to address the cybersecurity vulnerabilities posed by FBS. However, more research is needed to determine whether some vulnerabilities still exist and to evolve standards with additional mitigations.

What’s the problem?

A 5G network provides connectivity to many subscribers. The process of setting up wireless connections begins with your operator's RAN constantly broadcasting a lot of useful system-related information in cleartext. This system information includes a unique cellular network identity called Public Land Mobile Network (PLMN) ID, which helps your device (the UE) find and establish a communication channel with the correct tower. Your device then uses this broadcasted system information to “register” with the core network (CN), and shortly after, it has connectivity.

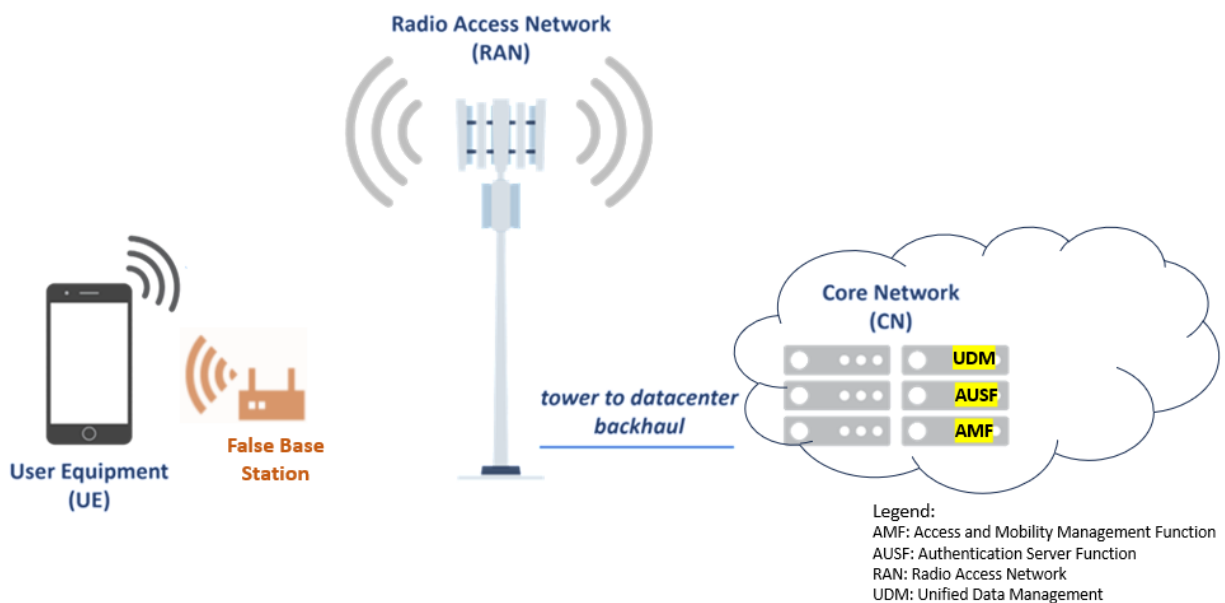


Figure 1. 5G architecture with an intruder FBS near the UE

A lot of complex signaling and configuration happens in the few milliseconds from a device being turned on and gaining cellular connectivity. A key step in this process is when the UE establishes a security context during its initial registration with the CN via the RAN (see Figure 1). During this setup, ciphering and integrity keys are mutually agreed upon to protect future communication. Until this process is completed, control messages between the UE, RAN, and the CN are sent in cleartext. Consequently, this brief pre-authentication phase creates a critical window of exposure. By intercepting and manipulating

unauthenticated cleartext messages, an attacker can harvest subscriber identities, force fallbacks to weaker legacy protocols, or execute Denial-of-Service (DoS) attacks — effectively compromising the connection before mutual security is ever established.

In the early generations of cellular systems (2G and 3G), building an FBS required substantial capital and proprietary hardware, limiting these attacks to well-resourced adversaries. During the 2G era, the total lack of mutual authentication allowed attackers to effortlessly capture plaintext calls and texts, harvest permanent identifiers, and crack weak encryption. By the 3G era, while mutual authentication was introduced, attackers could still force downgrades to 2G, exploit unauthenticated error codes to trigger network fallbacks, and harvest identities during initial access.

The landscape shifted in 2010 when researchers demonstrated cellphone traffic interception using low-cost, commodity Software Defined Radios (SDRs) — democratizing false base station attacks and kicking off a decade of widespread security research. Given these advancements and the accessibility of SDR technology, an FBS can be readily deployed using inexpensive commercial off-the-shelf (COTS) hardware and software. Various open-source software tools now enable reception and generation of cellular radio signals using general-purpose SDR [\[3\]](#) hardware. Leveraging this setup, attackers can scan radio channels, decode the cleartext system information broadcast by a legitimate cell, and rebroadcast modified or copied information to impersonate a legitimate mobile network.

With 4G LTE, despite strong core encryption and mandatory mutual authentication (i.e., Evolved Packet System-Authentication and Key Agreement, EPS-AKA), the registration phase still transmitted permanent subscriber identities (i.e., International Mobile Subscriber Identities, IMSIs) in unencrypted cleartext. This allowed attackers to deploy 4G IMSI catchers (such as Hailstorm) to track user locations, hijack radio resource control (RRC), and inject unauthenticated rejection codes to disconnect devices from legitimate networks.

5G took another step toward greater security, further reducing the attack surface with new standards-based features that protect subscribers' permanent identifiers [\[4\]\[5\]\[6\]](#). However, DoS attacks remain a challenge.

How have cellular standards addressed the problem?

Cellular standards have evolved across multiple generations. 5G standards were informed by cybersecurity threats and lessons learned from earlier generations. The standardized security architecture sought to mitigate most of the vulnerabilities exploited in 2G, 3G, and 4G including threats posed by false base stations. For example:

- Mutual Authentication and Key Agreement (AKA) was added in 3G. The procedure succeeds only if the pre-shared secret keys match on the device and the core network ends. Unlike 2G, where a device blindly trusts the network, a malicious 3G network cannot authenticate itself with the device and gain full control of the connection.
- 4G enhanced the security algorithms and separated the RAN and Non-Access Stratum (NAS) message protections by using a derived key hierarchy. Unlike 3G, where ciphering and integrity were applied at the RAN level, for both the plaintext NAS payloads encapsulated inside RAN packets and the RAN-specific signaling, 4G used the root key to derive separate ciphering and integrity keys for NAS and RAN. Because RAN and NAS messages were protected with separate keys, a malicious FBS could no longer steal and reuse the static RAN keys and decipher or tamper with NAS messages.

False Base Station

- 5G added a capability to conceal the subscriber's permanent identifier [\[4\]](#). If a 5G device uses a non-null protection scheme for the Subscription Concealed Identifier (SUCI) during the initial handshake, a malicious network cannot harvest the permanent identifier and target a specific subscriber for attacks.
- 5G tightened the rules to disable frequent reuse of temporary subscriber identities between the device and the core network [\[5\]](#). This weakened the FBS's capabilities to track specific users.
- 5G removed the option of permanent subscriber identity-based paging [\[6\]](#), further weakening the FBS capabilities to track and target specific users.
- 5G also applied a comprehensive approach to protect the initial NAS message by packaging most of the information inside a ciphered and integrity-protected container [\[7\]](#). This further reduced the leakage of sensitive information to a malicious FBS.

These incremental enhancements mean that 5G systems are the most secure cellular network generation, including against FBS attacks.

What else should I know about FBS?

Legacy generations of cellular networks are still deployed and operating globally. So long as commercial carriers continue to operate older 2G and 3G technologies (i.e., providing coverage where 5G hasn't been deployed yet), devices will be able to connect to them. If an attacker tricks a device into falling back to previous-generation technology (a “bid-down attack”), the attacker would be able to exploit many of the older-generation vulnerabilities.

As a byproduct of global network evolution, most commercial carriers are currently decommissioning 2G/3G networks to repurpose the radio spectrum for 4G/5G [8]. This transition, combined with device-level restrictions preventing 2G/3G access, significantly reduces the effectiveness of legacy FBS attacks.

Attackers have adapted their FBS techniques to target vulnerabilities in newer generations. Several research papers have examined the use of FBS in 4G and 5G networks [9][10]. Risks posed by FBS persist in 5G networks, although the number of threats is minimized compared to previous cellular generations. Many of the remaining risks stem from unprotected signaling and configuration information transmitted between devices and networks. 5G standards addressed these issues in 3GPP TR 33.809. “Study on 5G security enhancements against False Base Stations”[11]. The following table lists some of the issues identified as a part of that work.

Table 1. Threats identified in 3GPP TR 33.809

Threat	How the Hacker Does It	What the Phone Does	Real-World Impact
Pre-Connection Fake Signaling	Floods the phone with malicious setup messages before official security kicks in.	Gets stuck in a continuous failure loop trying to connect.	Prevents the phone from reaching service (DoS).
Cell Blocking	Sends fake "tower is busy/blocked" restriction flags.	Refuses to connect to the cellular network.	Complete DoS (you lose cellular connection).
Schedule Tampering	Sends broken timetable data for how the network broadcasts information.	Cannot properly decode incoming network broadcasts.	The phone fails to register or log onto the network.
Forced Downgrade	Sends false preference rules telling the phone 5G isn't available.	Drops connection down to older 4G or 2G networks.	Forces the phone onto legacy networks with weaker security.
Fake Network Map Data	Feeds the phone fake details about surrounding cell towers.	Gets trapped connecting to rogue tower layouts.	Blocks access to legitimate service (DoS).

Researchers have designed and tested innovative scenarios in lab environments to uncover and mitigate security vulnerabilities [\[12\]](#). Countermeasures for discouraging FBS-based attacks — such as detecting FBS presence [\[13\]](#) and FBS location [\[14\]](#) — have also been highlighted. The 5G architecture includes a Network Data Analytics Function (NWDAF) to collect network metrics. This network function can be utilized to deploy machine learning-based capabilities for detecting and mitigating FBS threats [\[15\]](#). For example, NWDAF can collect metrics regarding failed paging or missed periodic updates from the devices to detect anomalies. Artificial Intelligence/Machine Learning (AI/ML) can also be leveraged for these countermeasures. This is an active area of research that should be monitored by 5G stakeholders.

For private 5G networks deployed by enterprises and governments, resiliency and security should be given the same weight as that of any other enterprise or critical infrastructure. Consequently, these networks can deploy FBS detection and mitigation techniques until standards provide foolproof, built-in protection against FBS attacks. Such networks may also employ out-of-band or dual connectivity (e.g., satellite, Wi-Fi) for increased resilience.

The NCCoE 5G security testbed demonstrates example scenarios based on the current implementation of 5G standards to determine if FBS attacks against 5G devices would succeed. The list of scenarios in the ‘Technical details of False Base Station attacks’ section is not exhaustive and should be considered complementary to other work in this area.

How can you protect against FBS?

Researchers and organizations can utilize an FBS as an experimental tool for simulating unexpected or unspecified scenarios. This approach requires a careful study of the standards from the perspective of a network analyst. Through this type of analysis, both standards and vendor implementations can be improved incrementally. The NCCoE testbed research demonstrates that 5G devices remain vulnerable to DoS attacks. By incorporating these findings into 3GPP studies for 6G security, we can help improve the next generation of cellular systems.

Organizations can disable legacy connectivity options (such as 2G and 3G) via Mobile Device Management (MDM) profiles or device settings, where available [\[16\]](#), as older networks lack robust authentication and are easily spoofed by False Base Station (FBS) setups.

5G network operators can limit cleartext exposure of subscriber identity over the air interface by implementing specific optional capabilities outlined across the NIST CSWP 36 [\[5\]\[6\]\[7\]](#).

3GPP contributors should prioritize technical research and standards contributions to mitigate remaining False Base Station (FBS) DoS risks in 5G networks.

Private 5G networks should evaluate, and where applicable, deploy FBS detection and mitigation techniques.

Summary

It is now possible to implement an FBS with a relatively small investment using SDR software and hardware tools. Using an FBS, malicious actors may attack the users and networks through unexpected “corner cases” that are either undefined in standards or not implemented by network vendors. It is critical to understand such vulnerabilities and safeguard against them through the continuous improvement of both standards and implementations. Network functions like NWDAF can be utilized to deploy machine learning-based capabilities for detecting and mitigating FBS threats.

False Base Station

The NCCoE 5G security testbed results (detailed in the next section) show that all six “corner cases” tested with an FBS resulted in a successful DoS attack. The primary takeaway is that 3GPP standards should be enhanced to mitigate these vulnerabilities.

Technical details of False Base Station attacks

The rest of this white paper is intended for readers seeking more in-depth knowledge of FBS attacks.

For background information on the NCCoE 5G Cybersecurity project, including the architecture and components of the 5G standalone network built within the demonstration testbed environment, see NIST SP 1800-33 Volume B, 5G Cybersecurity, Approach, Architecture, and Security Characteristics [\[17\]](#).

Using research FBS to verify 5G behavior

There are several possible FBS deployment options. This white paper provides one example of an FBS setup in our lab. However, no endorsements or limitations of the hardware and software used are implied.

Our lab setup is deployed according to the documentation provided by srsRAN [\[18\]](#). It uses the following components (see Figure 2):

1. Ettus Research USRP B210 SDR
2. srsRAN open-source software for RAN functionality (3GPP Release 17)
3. Open5GS open-source software for core network functionality (3GPP Release 17)
4. Dell laptop running the Ubuntu operating system
5. Samsung Galaxy S22/S23 smartphones as UEs (3GPP Release 16)

For brevity, only two interfaces between RAN and CN are shown in Figure 2. N2 is the interface between the 5G RAN node (aka gNB) and AMF. N3 is the interface between the gNB and the User Plane Function (UPF).

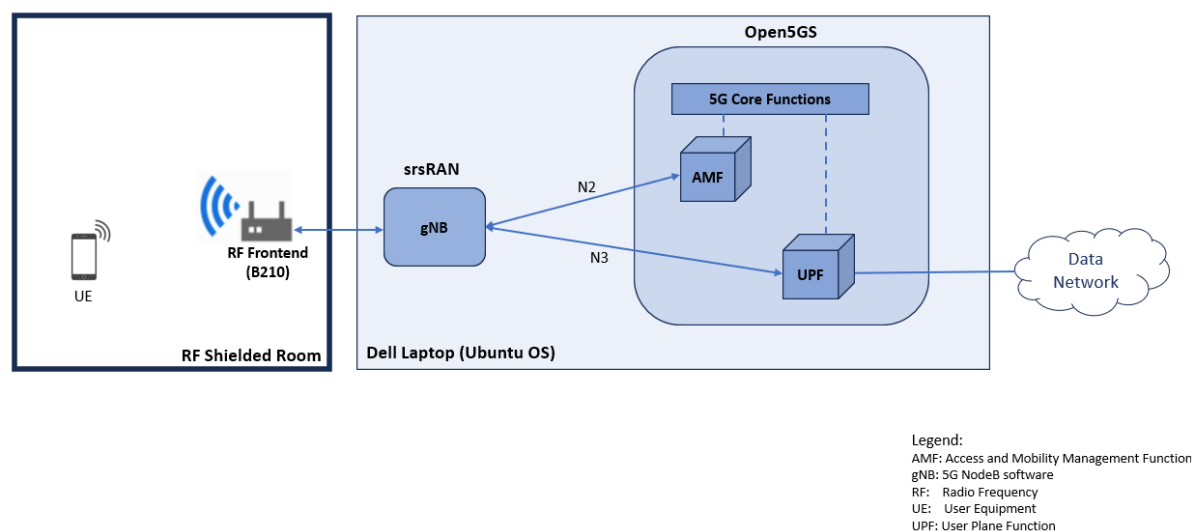


Figure 2. False Base Station setup

Evaluating 5G systems against FBS attacks

We simulated six FBS scenarios (“corner cases”) in our lab. In all scenarios, the UE is a subscriber of a Public Land Mobile Network (PLMN), also referred to as the “home network.” The goal of these scenarios is to identify potential security gaps in 5G standards [\[19\]](#) and implementations. These scenarios and their corresponding results are described below. Note that in the first five scenarios, the FBS impersonates both the RAN and the AMF, while in the sixth scenario, it impersonates the RAN only. In other words, the FBS handles both Access Stratum (AS) and Non-Access Stratum (NAS) messages in the first five scenarios but handles only AS messages in the sixth. In these scenarios, the FBS transmits a Tracking Area ID different from that of the home network. Although not strictly required to demonstrate the attacks, this causes the UE to trigger immediate mobility-based signaling with the FBS after idle mode cell reselection. Additionally, the UE uses the default timer and counter values defined in the standards, although some of these may be configurable by the network.

False Base Station

Scenario 1:

Description

- UE turns on, registers with the home network, and goes back to idle mode.
- FBS turns on in this area. FBS has stronger signals than a legitimate cell and is broadcasting PLMN ID equivalent to the home network of the UE.
- UE reselects to the FBS cell and tries to do mobility registration with a connection request.
- FBS keeps ignoring the connection request.
- UE reattempts the connection request 5 times after a short timeout and finally gives up.
- What will UE do next?
- Try to select a different (weaker) cell of the same PLMN?
- Try to select a cell in a different PLMN?

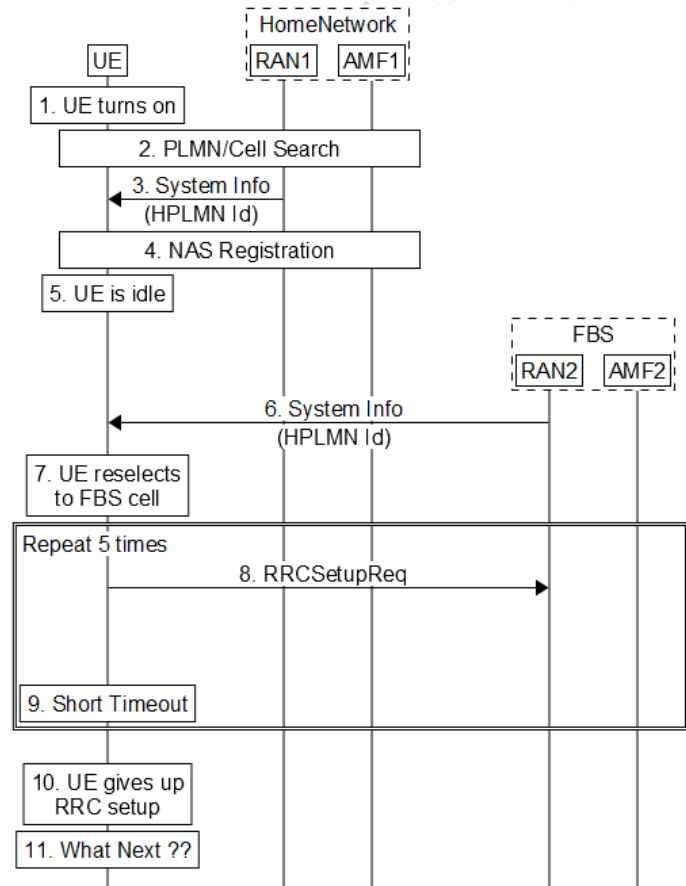


Figure 3. Scenario 1 flowchart

Observed behavior

- UE does not repeat the registration attempt on the same cell for about 12 minutes (long timeout).
- After a 12-minute timeout, UE repeats the cycle with FBS again.
- If FBS is turned off anytime during those 12 minutes, UE selects the legitimate cell after the long timeout and completes registration with the home network.

Results

- UE falls victim to the FBS DoS attack.
- UE can recover only when FBS is turned off, and a 12-minute timeout expires.

False Base Station

Scenario 2:

Description

- UE turns on, registers with the home network, and goes back to idle mode.
- FBS turns on in this area. FBS has stronger signals than a legitimate cell and is broadcasting PLMN ID equivalent to the home network of the UE.
- UE reselects to the FBS cell and tries to do mobility registration with a connection request.
- FBS replies with a connection reject.
- What will UE do next?
- Try to select a different (weaker) cell of the same PLMN?
- Try to select a cell in a different PLMN?

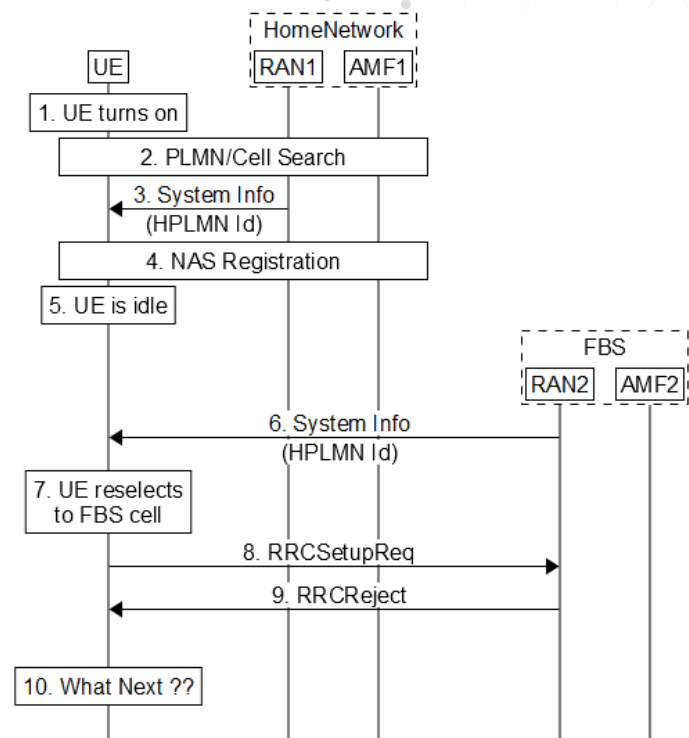


Figure 4. Scenario 2 flowchart

Observed behavior

- UE keeps trying the strongest cell of FBS repeatedly.
- Does not try to connect with a legitimate cell until FBS is turned off.

Results

- UE has fallen victim to a DoS attack!

False Base Station

Scenario 3:

Description

- UE turns on, registers with the home network, and goes back to idle mode.
- FBS turns on in this area. FBS has stronger signals than a legitimate cell and is broadcasting PLMN ID equivalent to the home network of the UE.
- UE reselects to the FBS cell and tries to do mobility registration with a connection request.
- FBS replies with the connection response.
- UE sends out the NAS registration message.
- FBS keeps ignoring the NAS registration message.
- UE reattempts NAS registration 5 times after a short timeout and finally gives up.
- What will UE do next?
- Try to select a different (weaker) cell of the same PLMN?
- Try to select a cell in a different PLMN?

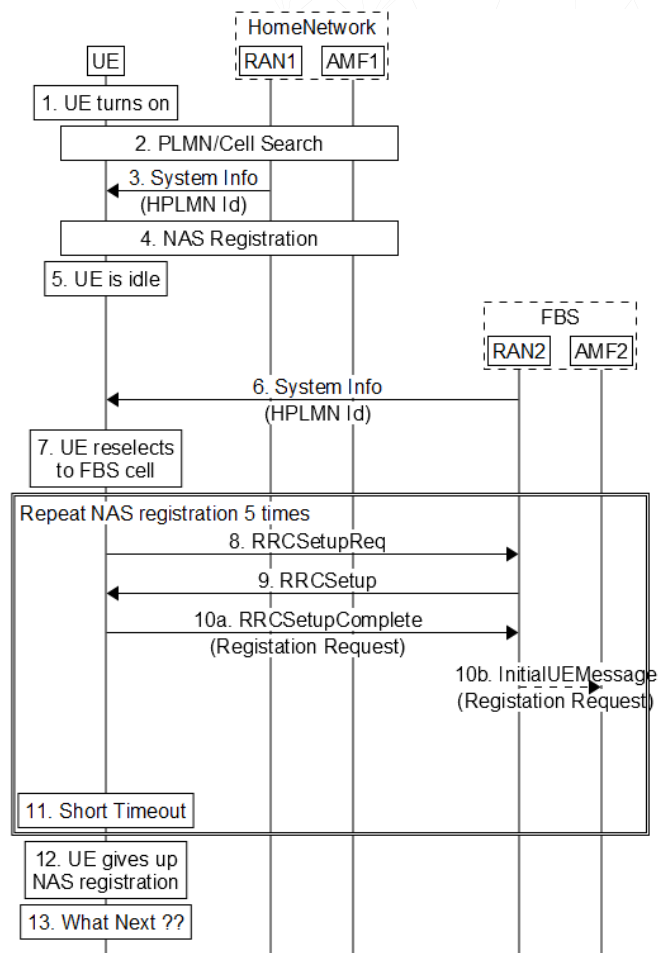


Figure 5. Scenario 3 flowchart

Observed behavior

- UE does not repeat registration attempts on the same cell for about 12 minutes (long timeout).
- After a 12-minute timeout, UE repeats the cycle with FBS again.
- If FBS is turned off anytime during those 12 minutes, UE selects the legitimate cell after the long timeout and completes registration with the home network.

Results

- UE falls victim to the FBS DoS attack.
- UE can recover only when FBS is turned off, and a 12-minute timeout expires.

False Base Station

Scenario 4:

Description

- UE turns on, registers with the home network, and goes back to idle mode.
- FBS turns on in this area. FBS has stronger signals than a legitimate cell and is broadcasting PLMN ID equivalent to the home network of the UE.
- UE reselects to the FBS cell and tries to do mobility registration with a connection request.
- FBS replies with the connection response.
- UE sends out the NAS registration message.
- FBS replies with a fake NAS registration accept response, bypassing mutual authentication steps.
- What will UE do next?
- Start receiving service without integrity/ciphering?
- Try to select a different (weaker) cell of the same PLMN?
- Try to select a cell in a different PLMN?

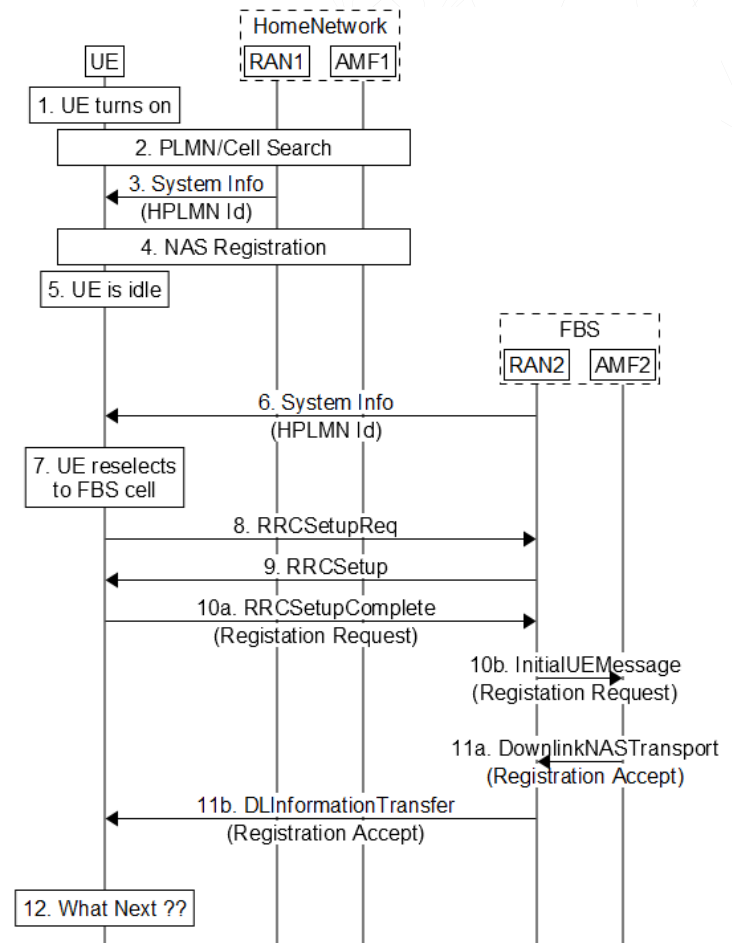


Figure 6. Scenario 4 flowchart

Observed behavior

- UE ignores Registration Accept and sends Registration Request again.
- Registration is attempted 5 times.
- UE does not repeat the registration attempt on the same cell for about 12 minutes (long timeout).
- After a 12-minute timeout, UE repeats the cycle with FBS again.
- If FBS is turned off anytime during those 12 minutes, UE selects the legitimate cell after the long timeout and completes registration with the home network.

Results

- Because UE ignores fake Registration Accept, it is protected against the FBS bypassing mutual authentication.
- However, UE falls victim to the FBS DoS attack.
- UE can recover only when FBS is turned off, and a 12-minute timeout expires.

False Base Station

Scenario 5:

Description

- UE turns on, registers with the home network, and goes back to idle mode.
- FBS turns on in this area. FBS has stronger signals than a legitimate cell and is broadcasting PLMN ID equivalent to the home network of the UE.
- UE reselects to the FBS cell and tries to do mobility registration with a connection request.
- FBS replies with the connection response.
- UE sends out the NAS registration message.
- FBS replies with a fake NAS registration reject response.
- What will UE do next?
- Try to select a different (weaker) cell of the same PLMN?
- Try to select a cell in a different PLMN?

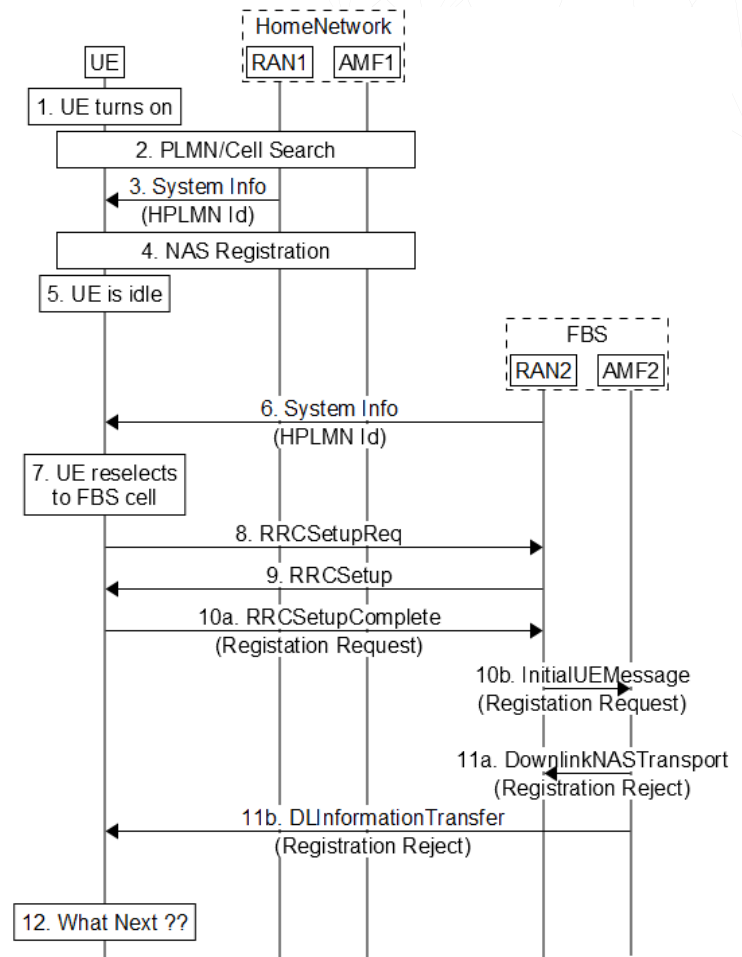


Figure 7. Scenario 5 flowchart

Observed behavior

- UE keeps trying the strongest cell of FBS repeatedly.
- Does not try to connect with a legitimate cell until FBS is turned off.

Results

- UE has fallen victim to a DoS attack!
- Depending on the cause given in Registration Reject, UE retries:
- Immediately for "PLMN not allowed."
- After 12 minutes, a timeout for "semantically incorrect message."

False Base Station

Scenario 6:

Description

- UE turns on, registers with the home network, and goes back to idle mode.
- FBS turns on in this area. FBS has stronger signals than a legitimate cell and is broadcasting PLMN ID equivalent to the home network of the UE.
- UE reselects to the FBS cell and tries to do mobility registration with a connection request.
- Unlike previous scenarios where FBS did not need any interaction with a real CN, this scenario assumes that FBS also has a roaming agreement with the UE's home network. This may happen, for example, if a foreign roaming partner goes rogue or is hacked.
- UE turns on in an area where FBS is visible and has the strongest signal. It is broadcasting the PLMN ID equivalent to the home network of the UE.
- UE selects the FBS cell and tries to get service with a connection request.
- FBS sets up the connection.
- UE sends NAS registration request, which includes UE security capabilities.
- FBS tampers with the message, indicating UE does not support any integrity or ciphering.
- What will the AMF do next?
- Will the AMF not send the Security Mode Command?
- Keep integrity and ciphering turned off for subsequent NAS messages?

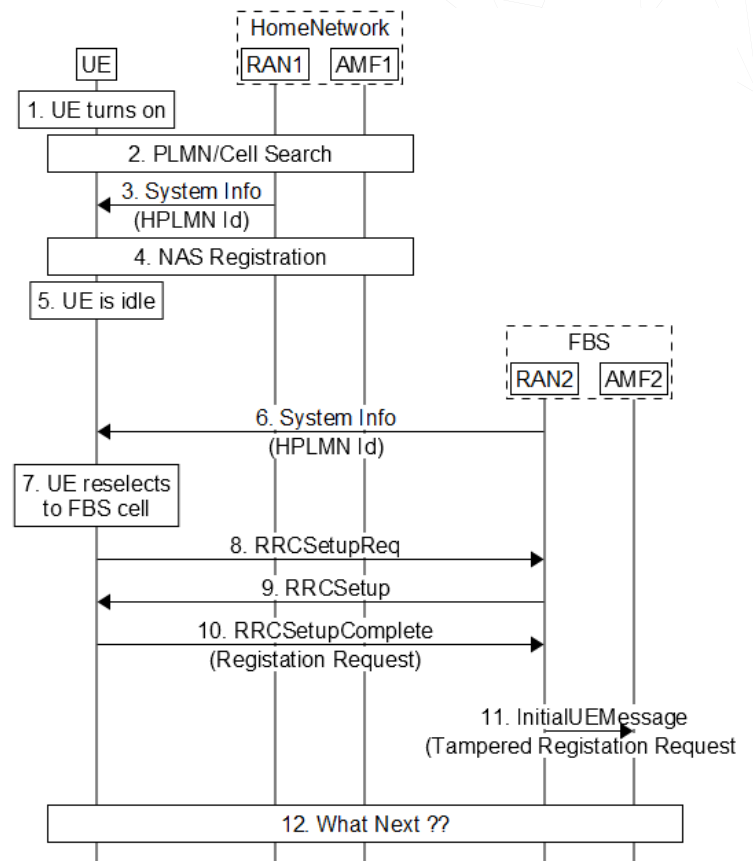


Figure 8. Scenario 6 flowchart

Observed behavior

- AMF rejects the tampered message because null integrity is not allowed in 5G.
- However, UE keeps trying the strongest cell of FBS repeatedly.
- Does not try to connect with a legitimate cell until FBS is turned off.

Results

- UE is protected against the tampering of certain IEs in the Initial NAS message.
- However, UE has still fallen victim to a DoS attack!

Summary of results

Tests conducted in the NCCoE testbed lab demonstrate that all six scenarios result in successful DoS attacks. The severity of these attacks is divided into two categories:

1. **Continuous Registration Loop:** The UE enters a loop of continuous registration attempts with the FBS. These attempts occur with short timeouts (driven by the RRC wait timer or the short NAS registration retry timer). As the UE continuously expends power on signaling and radio access, the device battery is rapidly depleted. The following scenarios fall into this category:
 - FBS sends RRC Reject.
 - FBS sends a fake NAS Registration Reject (e.g., “PLMN not allowed”).
2. **Intermittent Registration Cycle:** The UE attempts five failed registrations (governed by the NAS maximum-registration-attempts counter). These attempts occur with short timeouts, followed by a long timeout period (driven by the NAS backoff timer) before the UE repeats the full registration cycle with the FBS. Because the UE suspends signaling and radio access during the backoff duration, battery drain is less severe. The following scenarios fall into this category:
 - FBS fails to respond to the RRC Setup Request.
 - FBS fails to respond to the NAS Registration Request after RRC Setup.
 - FBS sends a fake NAS Registration Accept, bypassing mutual authentication.
 - FBS sends a NAS Registration Reject with causes such as “UE security capabilities mismatch” or “semantically incorrect message.”

These results indicate that 5G standards should be reviewed to investigate and mitigate vulnerabilities associated with these FBS attacks.

Appendix

UE log for Scenario 1

EventId	Time	RRC subch...	RRC direction	RRC message name	LAYER 3 SIGNALING MESSAGE
RRCSM	12:43:24.313	BCCH-BCH	Downlink	MIB	Time: 12:43:24.404
RRCSM	12:43:24.393	BCCH-SCH	Downlink	SIB1	
L3SM	12:43:24.404	Uplink	Uplink	REGISTRATION_REQUEST	REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)
RRCSM	12:43:24.404	CCCH	Uplink	RRCSetupRequest	M Extended protocol discriminator (hex data: 7e) EPD value: 126 (5GS mobility management)
RRCSM	12:43:24.464	CCCH	Downlink	RRCSetup	M Security header type (hex data: 0) Security header type: 0 (Plain 5GS NAS message, not security protected)
RRCSM	12:43:24.469	BCCH-SCH	Downlink	SystemInformation - SIB3,SIB5,SIB4,SIB2	M Spare Half Octet (hex data: 0)
RRCSM	12:43:24.477	DCCH	Uplink	RRCSetupComplete	M Message Type (hex data: 41) Message number: 65
RRCSM	12:43:24.599	DCCH	Downlink	DLInformationTransfer	M 5GS registration type (hex data: 9) 5GS registration type value: initial registration FOR: Follow-on request pending
L3SM	12:43:24.600	Downlink	Downlink	AUTHENTICATION_REQUEST	M ngKSI (hex data: 0) TSC: native security context NAS key set identifier: 0
L3SM	12:43:24.634	Uplink	Uplink	AUTHENTICATION_RESPONSE	M 5GS mobile identity (hex data: 000bf200 f1100a40 01c00000 04) Type of identity: 5G-GUTI MCC: 1 MNC: 1 AMF Region ID: 10 AMF Set ID: 256 AMF Pointer: 1 5G-TMSI: 0xc0000004
RRCSM	12:43:24.635	DCCH	Uplink	ULInformationTransfer	O UE security capability (hex data: 2e04f070 f070) 5G-EA0: supported 128-5G-EA1: supported 128-5G-EA2: supported 128-5G-EA3: supported 5G-EA4: not supported 5G-EA5: not supported
RRCSM	12:43:24.651	DCCH	Downlink	DLInformationTransfer	
L3SM	12:43:24.651	Downlink	Downlink	SECURITY_MODE_COMMAND	
L3SM	12:43:24.652	Uplink	Uplink	SECURITY_MODE_COMPLETE	
RRCSM	12:43:24.652	DCCH	Uplink	ULInformationTransfer	
RRCSM	12:43:24.790	DCCH	Downlink	DLInformationTransfer	
L3SM	12:43:24.790	Downlink	Downlink	REGISTRATION_ACCEPT	
RRCSM	12:43:24.791	DCCH	Downlink	DLInformationTransfer	
L3SM	12:43:24.792	Downlink	Downlink	CONFIGURATION_UPDATE_COMMAND	
RRCSM	12:43:24.833	BCCH-BCH	Downlink	MIB	
L3SM	12:43:24.901	Uplink	Uplink	PDU_SESSION_ESTABLISHMENT_REQU...	
RRCSM	12:43:55.003	BCCH-BCH	Downlink	MIB	
RRCSM	12:43:55.036	BCCH-SCH	Downlink	SIB1	
RRCSM	12:43:55.037	BCCH-BCH	Downlink	MIB	
RRCSM	12:43:55.113	BCCH-SCH	Downlink	SIB1	
RRCSM	12:44:02.208	BCCH-BCH	Downlink	MIB	
RRCSM	12:44:02.396	BCCH-SCH	Downlink	SIB1	

Figure 9. Scenario 1 UE log showing steps 1 to 7

EventId	Time	RRC subch...	RRC direction	RRC message name	LAYER 3 SIGNALING MESSAGE
L3SM	12:44:02.405	Uplink	Uplink	REGISTRATION_REQUEST	Time: 12:44:02.405
RRCSM	12:44:02.405	CCCH	Uplink	RRCSetupRequest	REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)
RRCSM	12:44:03.207	BCCH-BCH	Downlink	MIB	M Extended protocol discriminator (hex data: 7e) EPD value: 126 (5GS mobility management)
RRCSM	12:44:03.207	BCCH-BCH	Downlink	MIB	M Security header type (hex data: 0) Security header type: 0 (Plain 5GS NAS message, not security protected)
RRCSM	12:44:03.356	BCCH-SCH	Downlink	SIB1	M Spare Half Octet (hex data: 0)
L3SM	12:44:13.447	Uplink	Uplink	REGISTRATION_REQUEST	M Message Type (hex data: 41) Message number: 65
RRCSM	12:44:13.447	CCCH	Uplink	RRCSetupRequest	M 5GS registration type (hex data: 2) 5GS registration type value: mobility registration updating FOR: No follow-on request pending
L3SM	12:44:24.488	Uplink	Uplink	REGISTRATION_REQUEST	M ngKSI (hex data: 1) TSC: native security context NAS key set identifier: 1
RRCSM	12:44:24.488	CCCH	Uplink	RRCSetupRequest	M 5GS mobile identity (hex data: 000bf200 f1100a40 01c00000 04) Type of identity: 5G-GUTI MCC: 1 MNC: 1 AMF Region ID: 10 AMF Set ID: 256 AMF Pointer: 1 5G-TMSI: 0xc0000004
L3SM	12:44:35.530	Uplink	Uplink	REGISTRATION_REQUEST	O UE security capability (hex data: 2e04f070 f070)
RRCSM	12:44:35.530	CCCH	Uplink	RRCSetupRequest	
L3SM	12:44:46.571	Uplink	Uplink	REGISTRATION_REQUEST	
RRCSM	12:44:46.571	CCCH	Uplink	RRCSetupRequest	
RRCSM	12:45:17.967	BCCH-BCH	Downlink	MIB	
RRCSM	12:45:18.075	BCCH-SCH	Downlink	SIB1	
RRCSM	12:45:18.076	BCCH-BCH	Downlink	MIB	
RRCSM	12:45:18.153	BCCH-SCH	Downlink	SIB1	
RRCSM	12:46:01.084	BCCH-BCH	Downlink	MIB	
RRCSM	12:46:01.116	BCCH-SCH	Downlink	SIB1	
RRCSM	12:47:32.620	BCCH-BCH	Downlink	MIB	
RRCSM	12:47:32.795	BCCH-SCH	Downlink	SIB1	
RRCSM	12:47:33.126	BCCH-BCH	Downlink	MIB	

Figure 10. Scenario 1 UE log showing steps 8 to 11

False Base Station

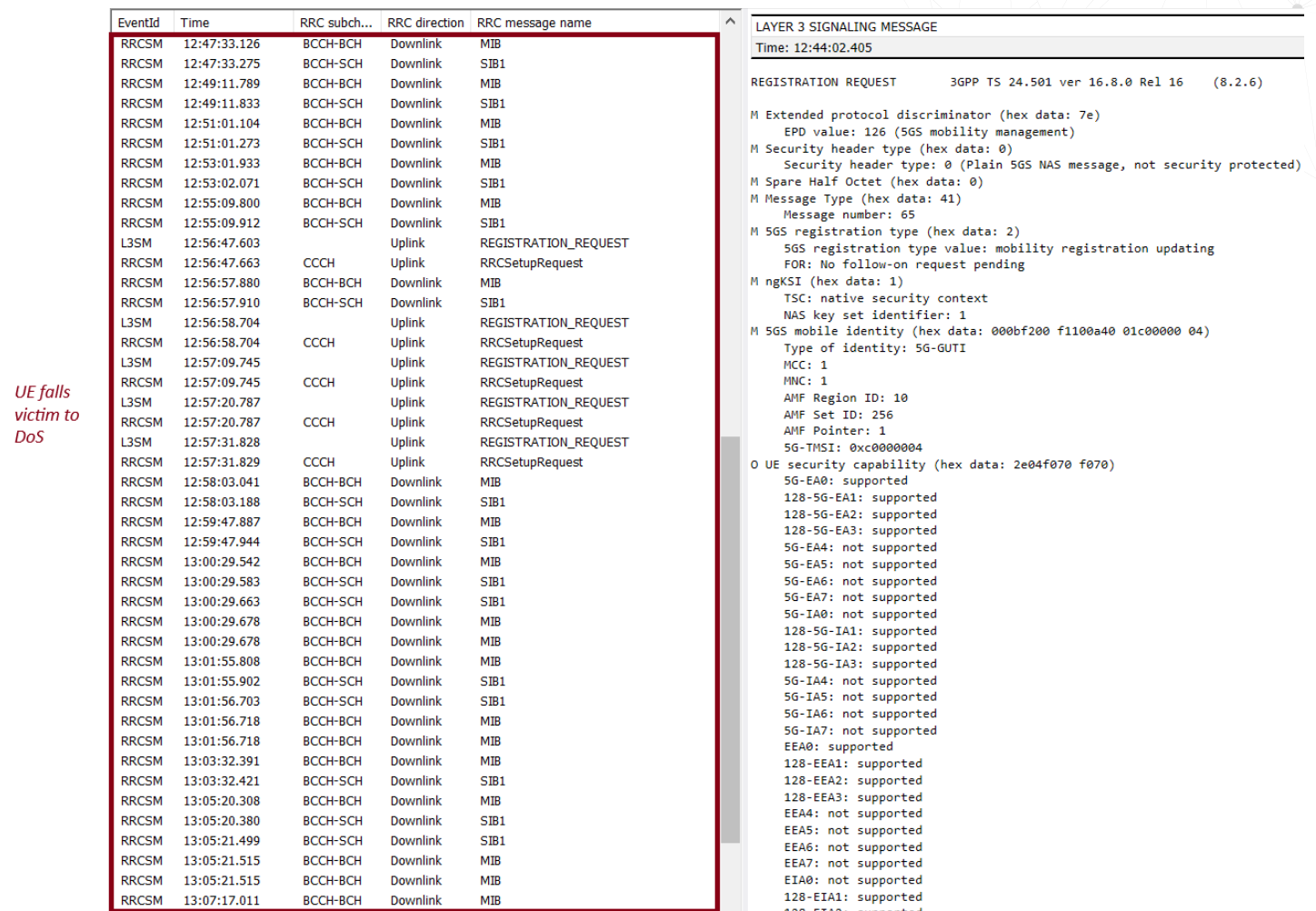


Figure 11. Scenario 1 UE log showing DoS conditions

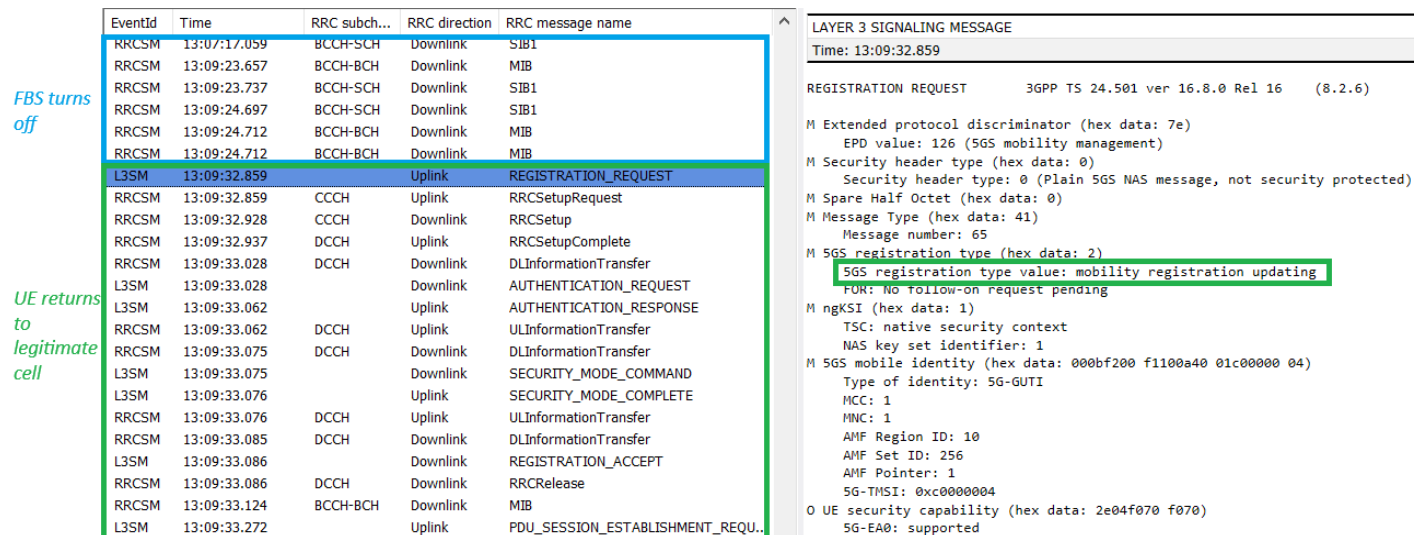


Figure 12. Scenario 1 UE log showing return to legitimate cell after FBS turns off

UE log for Scenario 2

EventId	Time	RRC subch...	RRC direction	RRC message name	
RRCSM	15:23:52.173	BCCH-BCH	Downlink	MIB	Steps 1 - 3
RRCSM	15:23:52.247	BCCH-SCH	Downlink	SIB1	
L3SM	15:23:52.256		Uplink	REGISTRATION_REQUEST	
RRCSM	15:23:52.256	CCCH	Uplink	RRCSetupRequest	Steps 4 - 5
RRCSM	15:23:52.318	CCCH	Downlink	RRCSetup	
RRCSM	15:23:52.323	BCCH-SCH	Downlink	SystemInformation - SIB3,SIB5,SIB4,SIB2	
RRCSM	15:23:52.331	DCCH	Uplink	RRCSetupComplete	
RRCSM	15:23:52.476	DCCH	Downlink	DLInformationTransfer	
L3SM	15:23:52.476		Downlink	AUTHENTICATION_REQUEST	
L3SM	15:23:52.516		Uplink	AUTHENTICATION_RESPONSE	
RRCSM	15:23:52.516	DCCH	Uplink	ULInformationTransfer	
RRCSM	15:23:52.535	DCCH	Downlink	DLInformationTransfer	
L3SM	15:23:52.536		Downlink	SECURITY_MODE_COMMAND	
L3SM	15:23:52.536		Uplink	SECURITY_MODE_COMPLETE	Steps 6 - 7
RRCSM	15:23:52.536	DCCH	Uplink	ULInformationTransfer	
RRCSM	15:23:52.583	DCCH	Downlink	DLInformationTransfer	
L3SM	15:23:52.583		Downlink	REGISTRATION_ACCEPT	
RRCSM	15:23:52.583	DCCH	Downlink	DLInformationTransfer	
L3SM	15:23:52.585		Downlink	CONFIGURATION_UPDATE_COMMAND	
RRCSM	15:23:52.626	BCCH-BCH	Downlink	MIB	
L3SM	15:23:52.697		Uplink	PDU_SESSION_ESTABLISHMENT_REQU...	
RRCSM	15:24:27.740	BCCH-BCH	Downlink	MIB	
RRCSM	15:24:27.879	BCCH-SCH	Downlink	SIB1	
RRCSM	15:24:27.880	BCCH-BCH	Downlink	MIB	Steps 8 - 10
RRCSM	15:24:27.927	BCCH-SCH	Downlink	SIB1	
RRCSM	15:24:35.042	BCCH-BCH	Downlink	MIB	
RRCSM	15:24:35.079	BCCH-SCH	Downlink	SIB1	
L3SM	15:24:35.088		Uplink	REGISTRATION_REQUEST	
RRCSM	15:24:35.088	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:24:35.253	CCCH	Downlink	RRCReject	
L3SM	15:24:51.255		Uplink	REGISTRATION_REQUEST	
RRCSM	15:24:51.255	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:24:51.444	CCCH	Downlink	RRCReject	
L3SM	15:25:07.445		Uplink	REGISTRATION_REQUEST	Steps 8 - 10
RRCSM	15:25:07.445	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:25:07.634	CCCH	Downlink	RRCReject	
L3SM	15:25:23.645		Uplink	REGISTRATION_REQUEST	
RRCSM	15:25:23.646	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:25:23.834	CCCH	Downlink	RRCReject	
L3SM	15:25:39.845		Uplink	REGISTRATION_REQUEST	
RRCSM	15:25:39.846	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:25:40.034	CCCH	Downlink	RRCReject	
L3SM	15:25:56.045		Uplink	REGISTRATION_REQUEST	
RRCSM	15:25:56.046	CCCH	Uplink	RRCSetupRequest	Steps 8 - 10
RRCSM	15:25:56.214	CCCH	Downlink	RRCReject	
L3SM	15:26:12.215		Uplink	REGISTRATION_REQUEST	
RRCSM	15:26:12.215	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:26:12.404	CCCH	Downlink	RRCReject	
L3SM	15:26:28.405		Uplink	REGISTRATION_REQUEST	
RRCSM	15:26:28.406	CCCH	Uplink	RRCSetupRequest	

LAYER 3 SIGNALING MESSAGE
Time: 15:23:52.256

REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)

M Extended protocol discriminator (hex data: 7e)
EPD value: 126 (5GS mobility management)

M Security header type (hex data: 0)
Security header type: 0 (Plain 5GS NAS message, not security protected)

M Spare Half Octet (hex data: 0)

M Message Type (hex data: 41)
Message number: 65

M 5GS registration type (hex data: 9)
5GS registration type value: initial registration

FOR: Follow-on request pending

M ngKSI (hex data: 0)
TSC: native security context
NAS key set identifier: 0

M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 0e)
Type of identity: 5G-GUTI
MCC: 1
MNC: 1
AMF Region ID: 10
AMF Set ID: 256
AMF Pointer: 1
5G-TMSI: 0xc100000e

O UE security capability (hex data: 2e04f070 f070)
5G-EA0: supported
128-5G-EA1: supported
128-5G-EA2: supported
128-5G-EA3: supported
5G-EA4: not supported
5G-EA5: not supported
5G-EA6: not supported
5G-EA7: not supported
5G-IA0: not supported
128-5G-IA1: supported
128-5G-IA2: supported
128-5G-IA3: supported
5G-IA4: not supported
5G-IA5: not supported
5G-IA6: not supported
5G-IA7: not supported
EEA0: supported
128-EEA1: supported
128-EEA2: supported
128-EEA3: supported
EEA4: not supported
EEA5: not supported
EEA6: not supported
EEA7: not supported
EIA0: not supported
128-EIA1: supported
128-EIA2: supported
128-EIA3: supported
EIA4: not supported
EIA5: not supported
EIA6: not supported
EIA7: not supported

O NAS message container (hex data: 71004016 f3dfe341 bf59a670 4a41019e a285z

Figure 13. Scenario 2 UE log showing steps 1 to 10

False Base Station

EventId	Time	RRC subch...	RRC direction	RRC message name	LAYER 3 SIGNALING MESSAGE
RRCSM	15:26:28.406	CCCH	Uplink	RRCSetupRequest	Time: 15:26:44.585
RRCSM	15:26:28.574	CCCH	Downlink	RRCReject	
L3SM	15:26:44.585		Uplink	REGISTRATION_REQUEST	REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)
RRCSM	15:26:44.586	CCCH	Uplink	RRCSetupRequest	M Extended protocol discriminator (hex data: 7e) EPD value: 126 (5GS mobility management)
RRCSM	15:26:44.755	CCCH	Downlink	RRCReject	M Security header type (hex data: 0) Security header type: 0 (Plain 5GS NAS message, not security protected)
L3SM	15:27:00.756		Uplink	REGISTRATION_REQUEST	M Spare Half Octet (hex data: 0)
RRCSM	15:27:00.757	CCCH	Uplink	RRCSetupRequest	M Message Type (hex data: 41) Message number: 65
RRCSM	15:27:00.924	CCCH	Downlink	RRCReject	M 5GS registration type (hex data: 2) 5GS registration type value: mobility registration updating FOR: No follow-on request pending
L3SM	15:27:16.925		Uplink	REGISTRATION_REQUEST	M ngKSI (hex data: 1) TSC: native security context NAS key set identifier: 1
RRCSM	15:27:16.926	CCCH	Uplink	RRCSetupRequest	M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 0e) Type of identity: 5G-GUTI MCC: 1 MNC: 1
RRCSM	15:27:17.114	CCCH	Downlink	RRCReject	AMF Region ID: 10 AMF Set ID: 256 AMF Pointer: 1 5G-TMSI: 0xc100000e
L3SM	15:27:33.125		Uplink	REGISTRATION_REQUEST	O UE security capability (hex data: 2e04f070 f070) 5G-EA0: supported 128-5G-EA1: supported 128-5G-EA2: supported 128-5G-EA3: supported 5G-EA4: not supported 5G-EA5: not supported 5G-EA6: not supported 5G-EA7: not supported 5G-IA0: not supported 128-5G-IA1: supported 128-5G-IA2: supported 128-5G-IA3: supported 5G-IA4: not supported 5G-IA5: not supported 5G-IA6: not supported 5G-IA7: not supported EEA0: supported 128-EEA1: supported 128-EEA2: supported 128-EEA3: supported EEA4: not supported EEA5: not supported EEA6: not supported EEA7: not supported EIA0: not supported 128-EIA1: supported 128-EIA2: supported 128-EIA3: supported EIA4: not supported EIA5: not supported EIA6: not supported EIA7: not supported
RRCSM	15:27:33.126	CCCH	Uplink	RRCSetupRequest	O NAS message container (hex data: 710044d3 71f14a55 cc8c8501 7c6078bf f7a11)
RRCSM	15:27:33.314	CCCH	Downlink	RRCReject	
L3SM	15:27:49.315		Uplink	REGISTRATION_REQUEST	
RRCSM	15:27:49.316	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:27:49.504	CCCH	Downlink	RRCReject	
L3SM	15:28:05.505		Uplink	REGISTRATION_REQUEST	
RRCSM	15:28:05.506	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:28:41.138	BCCH-BCH	Downlink	MIB	
RRCSM	15:28:41.207	BCCH-SCH	Downlink	SIB1	
RRCSM	15:28:48.302	BCCH-BCH	Downlink	MIB	
RRCSM	15:28:48.407	BCCH-SCH	Downlink	SIB1	
L3SM	15:28:48.417		Uplink	REGISTRATION_REQUEST	
RRCSM	15:28:48.417	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:28:48.500	CCCH	Downlink	RRCSetup	
RRCSM	15:28:48.510	DCCH	Uplink	RRCSetupComplete	
RRCSM	15:28:48.592	DCCH	Downlink	DLInformationTransfer	
L3SM	15:28:48.593		Downlink	AUTHENTICATION_REQUEST	
L3SM	15:28:48.626		Uplink	AUTHENTICATION_RESPONSE	
RRCSM	15:28:48.627	DCCH	Uplink	ULInformationTransfer	
RRCSM	15:28:48.645	DCCH	Downlink	DLInformationTransfer	
L3SM	15:28:48.645		Downlink	SECURITY_MODE_COMMAND	
L3SM	15:28:48.646		Uplink	SECURITY_MODE_COMPLETE	
RRCSM	15:28:48.646	DCCH	Uplink	ULInformationTransfer	
RRCSM	15:28:48.665	DCCH	Downlink	DLInformationTransfer	
L3SM	15:28:48.666		Downlink	REGISTRATION_ACCEPT	
RRCSM	15:28:48.666	DCCH	Downlink	RRCRelease	
RRCSM	15:28:48.706	BCCH-BCH	Downlink	MIB	
L3SM	15:28:48.843		Uplink	PDU_SESSION_ESTABLISHMENT_REQU...	
L3SM	15:28:48.843		Uplink	SERVICE_REQUEST	
RRCSM	15:28:48.844	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:28:48.937	CCCH	Downlink	RRCSetup	
RRCSM	15:28:48.946	DCCH	Uplink	RRCSetupComplete	
RRCSM	15:28:48.966	DCCH	Downlink	DLInformationTransfer	
L3SM	15:28:48.967		Downlink	SERVICE_ACCEPT	
L3SM	15:28:48.967		Uplink	UL_NAS_TRANSPORT	
RRCSM	15:28:48.967	DCCH	Uplink	ULInformationTransfer	
RRCSM	15:28:49.371	DCCH	Downlink	SecurityModeCommand	
RRCSM	15:28:49.373	DCCH	Uplink	SecurityModeComplete	

Figure 14. Scenario 2 UE log showing return to legitimate cell after FBS turns off

UE log for Scenario 3

EventId	Time	RRC subch...	RRC direction	RRC message name	
RRCSM	15:30:41.982	BCCH-BCH	Downlink	MI	Steps 1 - 3
RRCSM	15:30:42.005	BCCH-SCH	Downlink	SIB1	
L3SM	15:30:42.014		Uplink	REGISTRATION_REQUEST	Steps 4 - 5
RRCSM	15:30:42.014	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:30:42.081	BCCH-SCH	Downlink	SystemInformation - SIB3,SIB5,SIB4,SIB2	
RRCSM	15:30:42.098	CCCH	Downlink	RRCSetup	
RRCSM	15:30:42.108	DCCH	Uplink	RRCSetupComplete	
RRCSM	15:30:42.262	DCCH	Downlink	DLInformationTransfer	
L3SM	15:30:42.262		Downlink	AUTHENTICATION_REQUEST	
L3SM	15:30:42.310		Uplink	AUTHENTICATION_RESPONSE	
RRCSM	15:30:42.311	DCCH	Uplink	ULInformationTransfer	
RRCSM	15:30:42.328	DCCH	Downlink	DLInformationTransfer	
L3SM	15:30:42.328		Downlink	SECURITY_MODE_COMMAND	
L3SM	15:30:42.329		Uplink	SECURITY_MODE_COMPLETE	
RRCSM	15:30:42.329	DCCH	Uplink	ULInformationTransfer	
RRCSM	15:30:42.448	DCCH	Downlink	DLInformationTransfer	
L3SM	15:30:42.448		Downlink	REGISTRATION_ACCEPT	
RRCSM	15:30:42.449	DCCH	Downlink	DLInformationTransfer	
L3SM	15:30:42.450		Downlink	CONFIGURATION_UPDATE_COMMAND	
RRCSM	15:30:42.490	BCCH-BCH	Downlink	MI	

LAYER 3 SIGNALING MESSAGE

Time: 15:30:42.014

REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)

M Extended protocol discriminator (hex data: 7e)
EPD value: 126 (5GS mobility management)

M Security header type (hex data: 0)
Security header type: 0 (Plain 5GS NAS message, not security protected)

M Spare Half Octet (hex data: 0)

M Message Type (hex data: 41)
Message number: 65

M 5GS registration type (hex data: 9)
5GS registration type value: initial registration
FOR: Follow-on request pending

M ngKSI (hex data: 4)
TSC: native security context
NAS key set identifier: 4

M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 10)
Type of identity: 5G-GUTI
MCC: 1
MNC: 1
AMF Region ID: 10
AMF Set ID: 256
AMF Pointer: 1

Figure 15. Scenario 3 UE log showing steps 1 to 5

EventId	Time	RRC subch...	RRC direction	RRC message name	
RRCSM	15:31:13.647	BCCH-BCH	Downlink	MI	Steps 6 - 7
RRCSM	15:31:13.755	BCCH-SCH	Downlink	SIB1	
RRCSM	15:31:13.755	BCCH-BCH	Downlink	MI	
RRCSM	15:31:13.845	BCCH-SCH	Downlink	SIB1	
RRCSM	15:31:20.943	BCCH-BCH	Downlink	MI	
RRCSM	15:31:21.115	BCCH-SCH	Downlink	SIB1	Steps 8 - 11
L3SM	15:31:21.123		Uplink	REGISTRATION_REQUEST	
RRCSM	15:31:21.124	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:31:21.309	CCCH	Downlink	RRCSetup	
RRCSM	15:31:21.318	DCCH	Uplink	RRCSetupComplete	
RRCSM	15:31:22.414	BCCH-BCH	Downlink	MI	
RRCSM	15:31:22.414	BCCH-BCH	Downlink	MI	
RRCSM	15:31:22.554	BCCH-SCH	Downlink	SIB1	
RRCSM	15:31:36.159	BCCH-BCH	Downlink	MI	
L3SM	15:31:46.124		Uplink	REGISTRATION_REQUEST	
RRCSM	15:31:46.124	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:31:46.309	CCCH	Downlink	RRCSetup	
RRCSM	15:31:46.317	DCCH	Uplink	RRCSetupComplete	
RRCSM	15:32:01.160	BCCH-BCH	Downlink	MI	
L3SM	15:32:11.125		Uplink	REGISTRATION_REQUEST	
RRCSM	15:32:11.126	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:32:11.318	CCCH	Downlink	RRCSetup	
RRCSM	15:32:11.327	DCCH	Uplink	RRCSetupComplete	
RRCSM	15:32:26.161	BCCH-BCH	Downlink	MI	
L3SM	15:32:36.127		Uplink	REGISTRATION_REQUEST	
RRCSM	15:32:36.127	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:32:36.318	CCCH	Downlink	RRCSetup	
RRCSM	15:32:36.327	DCCH	Uplink	RRCSetupComplete	
RRCSM	15:32:51.163	BCCH-BCH	Downlink	MI	

LAYER 3 SIGNALING MESSAGE

Time: 15:31:21.123

REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)

M Extended protocol discriminator (hex data: 7e)
EPD value: 126 (5GS mobility management)

M Security header type (hex data: 0)
Security header type: 0 (Plain 5GS NAS message, not security protected)

M Spare Half Octet (hex data: 0)

M Message Type (hex data: 41)
Message number: 65

M 5GS registration type (hex data: 2)
5GS registration type value: mobility registration updating
FOR: No follow-on request pending

M ngKSI (hex data: 5)
TSC: native security context
NAS key set identifier: 5

M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 10)
Type of identity: 5G-GUTI
MCC: 1
MNC: 1
AMF Region ID: 10
AMF Set ID: 256
AMF Pointer: 1
5G-TMSI: 0xc1000010

O UE security capability (hex data: 2e04f070 f070)
5G-EA0: supported
128-5G-EA1: supported
128-5G-EA2: supported
128-5G-EA3: supported
5G-EA4: not supported
5G-EA5: not supported
5G-EA6: not supported
5G-EA7: not supported
5G-TA0: not supported

Figure 16. Scenario 3 UE log showing steps 6 to 11

False Base Station

Steps 8 - 11

Step 12

Step 13

EventId	Time	RRC subch...	RRC direction	RRC message name
L3SM	15:33:01.199		Uplink	REGISTRATION_REQUEST
RRCSM	15:33:01.199	CCCH	Uplink	RRCSetupRequest
RRCSM	15:33:01.323	CCCH	Downlink	RRCSetup
RRCSM	15:33:01.330	DCCH	Uplink	RRCSetupComplete
RRCSM	15:33:16.165	BCCH-BCH	Downlink	MIB
RRCSM	15:33:45.930	BCCH-BCH	Downlink	MIB
RRCSM	15:33:46.074	BCCH-SCH	Downlink	SIB1
RRCSM	15:33:46.074	BCCH-BCH	Downlink	MIB
RRCSM	15:33:46.164	BCCH-SCH	Downlink	SIB1
RRCSM	15:34:29.103	BCCH-BCH	Downlink	MIB
RRCSM	15:34:29.274	BCCH-SCH	Downlink	SIB1
RRCSM	15:36:00.476	BCCH-BCH	Downlink	MIB
RRCSM	15:36:00.631	BCCH-SCH	Downlink	SIB1
RRCSM	15:37:41.726	BCCH-BCH	Downlink	MIB
RRCSM	15:37:41.911	BCCH-SCH	Downlink	SIB1
RRCSM	15:39:27.825	BCCH-BCH	Downlink	MasterInformationBlock
RRCSM	15:39:35.045	BCCH-BCH	Downlink	MIB
RRCSM	15:39:35.191	BCCH-SCH	Downlink	SIB1
RRCSM	15:41:34.354	BCCH-BCH	Downlink	MIB
RRCSM	15:41:34.389	BCCH-SCH	Downlink	SIB1
RRCSM	15:43:44.384	BCCH-BCH	Downlink	MIB
RRCSM	15:43:44.468	BCCH-SCH	Downlink	SIB1
RRCSM	15:43:44.799	BCCH-BCH	Downlink	MIB
RRCSM	15:43:44.799	BCCH-BCH	Downlink	MIB
RRCSM	15:43:44.948	BCCH-SCH	Downlink	SIB1
L3SM	15:45:16.122		Uplink	REGISTRATION_REQUEST
RRCSM	15:45:16.183	CCCH	Uplink	RRCSetupRequest
RRCSM	15:45:16.373	CCCH	Downlink	RRCSetup
RRCSM	15:45:16.382	DCCH	Uplink	RRCSetupComplete
RRCSM	15:45:31.157	BCCH-BCH	Downlink	MIB
RRCSM	15:45:32.317	BCCH-BCH	Downlink	MIB
RRCSM	15:45:32.317	BCCH-BCH	Downlink	MIB
RRCSM	15:45:32.467	BCCH-SCH	Downlink	SIB1
L3SM	15:45:41.121		Uplink	REGISTRATION_REQUEST
RRCSM	15:45:41.178	CCCH	Uplink	RRCSetupRequest
RRCSM	15:45:41.361	CCCH	Downlink	RRCSetup
RRCSM	15:45:41.370	DCCH	Uplink	RRCSetupComplete
RRCSM	15:45:56.158	BCCH-BCH	Downlink	MIB
RRCSM	15:46:02.839	BCCH-BCH	Downlink	MIB
RRCSM	15:46:02.867	BCCH-SCH	Downlink	SIB1
RRCSM	15:46:03.037	BCCH-BCH	Downlink	MIB
RRCSM	15:46:03.037	BCCH-BCH	Downlink	MIB
RRCSM	15:46:03.187	BCCH-SCH	Downlink	SIB1
L3SM	15:46:06.123		Uplink	REGISTRATION_REQUEST
RRCSM	15:46:06.123	CCCH	Uplink	RRCSetupRequest
RRCSM	15:46:06.311	CCCH	Downlink	RRCSetup
RRCSM	15:46:06.320	DCCH	Uplink	RRCSetupComplete
RRCSM	15:46:21.160	BCCH-BCH	Downlink	MIB
L3SM	15:46:31.124		Uplink	REGISTRATION_REQUEST
RRCSM	15:46:31.125	CCCH	Uplink	RRCSetupRequest

LAYER 3 SIGNALING MESSAGE

Time: 15:33:01.199

REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)

M Extended protocol discriminator (hex data: 7e)
EPD value: 126 (5GS mobility management)

M Security header type (hex data: 0)
Security header type: 0 (Plain 5GS NAS message, not security protected)

M Spare Half Octet (hex data: 0)

M Message Type (hex data: 41)
Message number: 65

M 5GS registration type (hex data: 2)
5GS registration type value: mobility registration updating
FOR: No follow-on request pending

M ngKSI (hex data: 5)
TSC: native security context
NAS key set identifier: 5

M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 10)
Type of identity: 5G-GUTI
MCC: 1
MNC: 1
AMF Region ID: 10
AMF Set ID: 256
AMF Pointer: 1
5G-TMSI: 0xc1000010

O UE security capability (hex data: 2e04f070 f070)
5G-EA0: supported
128-5G-EA1: supported
128-5G-EA2: supported
128-5G-EA3: supported
5G-EA4: not supported
5G-EA5: not supported
5G-EA6: not supported
5G-EA7: not supported
5G-IA0: not supported
128-5G-IA1: supported
128-5G-IA2: supported
128-5G-IA3: supported
5G-IA4: not supported
5G-IA5: not supported
5G-IA6: not supported
5G-IA7: not supported
EEA0: supported
128-EEA1: supported
128-EEA2: supported
128-EEA3: supported
EEA4: not supported
EEA5: not supported
EEA6: not supported
EEA7: not supported
EIA0: not supported
128-EIA1: supported
128-EIA2: supported
128-EIA3: supported
EIA4: not supported
EIA5: not supported
EIA6: not supported
EIA7: not supported

O NAS message container (hex data: 710044a8 42608627 063320b0 a9e8e6d6 164a4

Figure 17. Scenario 3 UE log showing steps 8 to 13

False Base Station

Step 13

FBS turns off

Return to legitimate cell

EventId	Time	RRC subch...	RRC direction	RRC message name	LAYER 3 SIGNALING MESSAGE
RRCSM	15:46:31.311	CCCH	Downlink	RRCSetup	Time: 15:59:11.119
RRCSM	15:46:31.320	DCCH	Uplink	RRCSetupComplete	
RRCSM	15:46:46.160	BCCH-BCH	Downlink	MIB	REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)
L3SM	15:46:56.126		Uplink	REGISTRATION_REQUEST	
RRCSM	15:46:56.126	CCCH	Uplink	RRCSetupRequest	M Extended protocol discriminator (hex data: 7e) EPD value: 126 (5GS mobility management)
RRCSM	15:46:56.312	CCCH	Downlink	RRCSetup	M Security header type (hex data: 0) Security header type: 0 (Plain 5GS NAS message, not security protected)
RRCSM	15:46:56.320	DCCH	Uplink	RRCSetupComplete	M Spare Half Octet (hex data: 0) M Message Type (hex data: 41) Message number: 65
RRCSM	15:47:11.161	BCCH-BCH	Downlink	MIB	M 5GS registration type (hex data: 2) 5GS registration type value: mobility registration updating FOR: No follow-on request pending
RRCSM	15:47:43.216	BCCH-BCH	Downlink	MIB	
RRCSM	15:47:43.347	BCCH-SCH	Downlink	SIB1	M ngKSI (hex data: 5) TSC: native security context NAS key set identifier: 5
RRCSM	15:48:44.035	BCCH-BCH	Downlink	MIB	M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 10) Type of identity: 5G-GUTI MCC: 1 MNC: 1 AMF Region ID: 10 AMF Set ID: 256 AMF Pointer: 1 5G-TMSI: 0xc1000010
RRCSM	15:48:44.075	BCCH-SCH	Downlink	SIB1	O UE security capability (hex data: 2e04f070 f070) 5G-EA0: supported 128-5G-EA1: supported 128-5G-EA2: supported 128-5G-EA3: supported 5G-EA4: not supported 5G-EA5: not supported 5G-EA6: not supported 5G-EA7: not supported 5G-IA0: not supported 128-5G-IA1: supported 128-5G-IA2: supported 128-5G-IA3: supported 5G-IA4: not supported 5G-IA5: not supported 5G-IA6: not supported 5G-IA7: not supported EEA0: supported 128-EEA1: supported 128-EEA2: supported 128-EEA3: supported EEA4: not supported EEA5: not supported EEA6: not supported EEA7: not supported EIA0: not supported 128-EIA1: supported 128-EIA2: supported 128-EIA3: supported EIA4: not supported EIA5: not supported EIA6: not supported EIA7: not supported
RRCSM	15:49:23.864	BCCH-BCH	Downlink	MIB	O NAS message container (hex data: 7100445a c1ff41bb 49cb779c 452e3709 b9377)
RRCSM	15:49:23.914	BCCH-SCH	Downlink	SIB1	
RRCSM	15:50:52.345	BCCH-BCH	Downlink	MIB	
RRCSM	15:50:52.394	BCCH-SCH	Downlink	SIB1	
RRCSM	15:50:53.514	BCCH-SCH	Downlink	SIB1	
RRCSM	15:50:53.529	BCCH-BCH	Downlink	MIB	
RRCSM	15:50:53.529	BCCH-BCH	Downlink	MIB	
RRCSM	15:52:30.636	BCCH-BCH	Downlink	MIB	
RRCSM	15:52:30.672	BCCH-SCH	Downlink	SIB1	
RRCSM	15:52:30.792	BCCH-SCH	Downlink	SIB1	
RRCSM	15:52:30.807	BCCH-BCH	Downlink	MIB	
RRCSM	15:52:30.807	BCCH-BCH	Downlink	MIB	
RRCSM	15:54:18.227	BCCH-BCH	Downlink	MIB	
RRCSM	15:54:18.312	BCCH-SCH	Downlink	SIB1	
RRCSM	15:56:17.792	BCCH-BCH	Downlink	MIB	
RRCSM	15:56:17.832	BCCH-SCH	Downlink	SIB1	
RRCSM	15:56:18.632	BCCH-SCH	Downlink	SIB1	
RRCSM	15:56:18.647	BCCH-BCH	Downlink	MIB	
RRCSM	15:56:18.647	BCCH-BCH	Downlink	MIB	
RRCSM	15:58:26.103	BCCH-BCH	Downlink	MIB	
RRCSM	15:58:26.149	BCCH-SCH	Downlink	SIB1	
RRCSM	15:58:26.629	BCCH-SCH	Downlink	SIB1	
RRCSM	15:58:26.644	BCCH-BCH	Downlink	MIB	
RRCSM	15:58:26.644	BCCH-BCH	Downlink	MIB	
L3SM	15:59:11.119		Uplink	REGISTRATION_REQUEST	
RRCSM	15:59:11.119	CCCH	Uplink	RRCSetupRequest	
RRCSM	15:59:11.202	CCCH	Downlink	RRCSetup	
RRCSM	15:59:11.211	DCCH	Uplink	RRCSetupComplete	
RRCSM	15:59:11.392	DCCH	Downlink	DLInformationTransfer	
L3SM	15:59:11.393		Downlink	AUTHENTICATION_REQUEST	
L3SM	15:59:11.427		Uplink	AUTHENTICATION_RESPONSE	
RRCSM	15:59:11.427	DCCH	Uplink	ULInformationTransfer	
RRCSM	15:59:11.442	DCCH	Downlink	DLInformationTransfer	
L3SM	15:59:11.442		Downlink	SECURITY_MODE_COMMAND	
L3SM	15:59:11.443		Uplink	SECURITY_MODE_COMPLETE	
RRCSM	15:59:11.443	DCCH	Uplink	ULInformationTransfer	
RRCSM	15:59:11.453	DCCH	Downlink	DLInformationTransfer	
L3SM	15:59:11.454		Downlink	REGISTRATION_ACCEPT	

Figure 18. Scenario 3 UE log showing return to legitimate cell after FBS turns off

UE log for Scenario 4

EventId	Time	RRC subch...	RRC direction	RRC message name	LAYER 3 SIGNALING MESSAGE
RRCSM	16:34:35.073	BCCH-BCH	Downlink	MIB	Time: 16:34:35.137
RRCSM	16:34:35.129	BCCH-SCH	Downlink	SIB1	
L3SM	16:34:35.137		Uplink	REGISTRATION_REQUEST	REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)
RRCSM	16:34:35.137	CCCH	Uplink	RRCSetupRequest	M Extended protocol discriminator (hex data: 7e) EPD value: 126 (5GS mobility management)
RRCSM	16:34:35.199	CCCH	Downlink	RRCSetup	M Security header type (hex data: 0) Security header type: 0 (Plain 5GS NAS message, not security protected)
RRCSM	16:34:35.209	DCCH	Uplink	RRCSetupComplete	M Spare Half Octet (hex data: 0) M Message Type (hex data: 41) Message number: 65
RRCSM	16:34:35.244	BCCH-SCH	Downlink	SystemInformation - SIB3,SIB5,SIB4,SIB2	M 5GS registration type (hex data: 9) 5GS registration type value: initial registration FOR: Follow-on request pending
RRCSM	16:34:35.358	DCCH	Downlink	DLInformationTransfer	M ngKSI (hex data: 6) TSC: native security context NAS key set identifier: 6
L3SM	16:34:35.359		Downlink	AUTHENTICATION_REQUEST	M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 10) Type of identity: 5G-GUTI MCC: 1 MNC: 1 AMF Region ID: 10 AMF Set ID: 256 AMF Pointer: 1 5G-TMSI: 0xc1000010
L3SM	16:34:35.392		Uplink	AUTHENTICATION_RESPONSE	O UE security capability (hex data: 2e04f070 f070) 5G-EA0: supported 128-5G-EA1: supported 128-5G-EA2: supported 128-5G-EA3: supported 5G-EA4: not supported 5G-EA5: not supported
RRCSM	16:34:35.393	DCCH	Uplink	ULInformationTransfer	
RRCSM	16:34:35.411	DCCH	Downlink	DLInformationTransfer	
L3SM	16:34:35.412		Downlink	SECURITY_MODE_COMMAND	
L3SM	16:34:35.412		Uplink	SECURITY_MODE_COMPLETE	
RRCSM	16:34:35.412	DCCH	Uplink	ULInformationTransfer	
RRCSM	16:34:35.628	DCCH	Downlink	DLInformationTransfer	
L3SM	16:34:35.629		Downlink	REGISTRATION_ACCEPT	
RRCSM	16:34:35.629	DCCH	Downlink	DLInformationTransfer	
L3SM	16:34:35.630		Downlink	CONFIGURATION_UPDATE_COMMAND	
RRCSM	16:34:35.672	BCCH-BCH	Downlink	MIB	
L3SM	16:34:35.770		Uplink	PDU_SESSION_ESTABLISHMENT_REQU...	
RRCSM	16:35:11.591	BCCH-BCH	Downlink	MIB	
RRCSM	16:35:11.696	BCCH-SCH	Downlink	SIB1	
RRCSM	16:35:11.697	BCCH-BCH	Downlink	MIB	
RRCSM	16:35:11.768	BCCH-SCH	Downlink	SIB1	
RRCSM	16:35:18.873	BCCH-BCH	Downlink	MIB	
RRCSM	16:35:19.056	BCCH-SCH	Downlink	SIB1	

Figure 19. Scenario 4 UE log showing steps 1 to 7

EventId	Time	RRC subch...	RRC direction	RRC message name	LAYER 3 SIGNALING MESSAGE
L3SM	16:35:19.065		Uplink	REGISTRATION_REQUEST	Time: 16:35:19.065
RRCSM	16:35:19.065	CCCH	Uplink	RRCSetupRequest	REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)
RRCSM	16:35:19.251	CCCH	Downlink	RRCSetup	M Extended protocol discriminator (hex data: 7e) EPD value: 126 (5GS mobility management)
RRCSM	16:35:19.259	DCCH	Uplink	RRCSetupComplete	M Security header type (hex data: 0) Security header type: 0 (Plain 5GS NAS message, not security protected)
RRCSM	16:35:19.356	DCCH	Downlink	DLInformationTransfer	M Spare Half Octet (hex data: 0) M Message Type (hex data: 41) Message number: 65
L3SM	16:35:19.356		Downlink	REGISTRATION_ACCEPT	M 5GS registration type (hex data: 2) 5GS registration type value: mobility registration updating FOR: No follow-on request pending
RRCSM	16:35:22.356	DCCH	Downlink	RRCRelease	M ngKSI (hex data: 0) TSC: native security context NAS key set identifier: 0
RRCSM	16:35:22.408	BCCH-BCH	Downlink	MIB	M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 10) Type of identity: 5G-GUTI MCC: 1 MNC: 1 AMF Region ID: 10 AMF Set ID: 256 AMF Pointer: 1 5G-TMSI: 0xc1000010
L3SM	16:35:32.408		Uplink	REGISTRATION_REQUEST	O UE security capability (hex data: 2e04f070 f070) 5G-EA0: supported 128-5G-EA1: supported
RRCSM	16:35:32.408	CCCH	Uplink	RRCSetupRequest	
RRCSM	16:35:32.591	CCCH	Downlink	RRCSetup	
RRCSM	16:35:32.599	DCCH	Uplink	RRCSetupComplete	
RRCSM	16:35:32.706	DCCH	Downlink	DLInformationTransfer	
L3SM	16:35:32.706		Downlink	REGISTRATION_ACCEPT	
RRCSM	16:35:35.706	DCCH	Downlink	RRCRelease	
RRCSM	16:35:35.768	BCCH-BCH	Downlink	MIB	
RRCSM	16:35:36.827	BCCH-BCH	Downlink	MIB	
RRCSM	16:35:36.827	BCCH-BCH	Downlink	MIB	
RRCSM	16:35:36.976	BCCH-SCH	Downlink	SIB1	
L3SM	16:35:45.768		Uplink	REGISTRATION_REQUEST	
RRCSM	16:35:45.768	CCCH	Uplink	RRCSetupRequest	
RRCSM	16:35:45.961	CCCH	Downlink	RRCSetup	
RRCSM	16:35:45.969	DCCH	Uplink	RRCSetupComplete	

Figure 20. Scenario 4 UE log showing steps 8 to 12

False Base Station

UE repeats
registration
attempt
5 times

12 min
long
timeout

UE
repeats
registration
on FBS

EventId	Time	RRC subch...	RRC direction	RRC message name
RRCSM	16:35:46.036	DCCH	Downlink	DLInformationTransfer
L3SM	16:35:46.036		Downlink	REGISTRATION_ACCEPT
RRCSM	16:35:49.036	DCCH	Downlink	RRCRelease
RRCSM	16:35:49.088	BCCH-BCH	Downlink	MIB
L3SM	16:35:59.088		Uplink	REGISTRATION_REQUEST
RRCSM	16:35:59.088	CCCH	Uplink	RRCSetupRequest
RRCSM	16:35:59.251	CCCH	Downlink	RRCSetup
RRCSM	16:35:59.259	DCCH	Uplink	RRCSetupComplete
RRCSM	16:35:59.321	DCCH	Downlink	DLInformationTransfer
L3SM	16:35:59.321		Downlink	REGISTRATION_ACCEPT
RRCSM	16:36:02.321	DCCH	Downlink	RRCRelease
RRCSM	16:36:02.373	BCCH-BCH	Downlink	MIB
RRCSM	16:36:02.427	BCCH-BCH	Downlink	MIB
RRCSM	16:36:02.427	BCCH-BCH	Downlink	MIB
RRCSM	16:36:02.576	BCCH-SCH	Downlink	SIB1
L3SM	16:36:12.373		Uplink	REGISTRATION_REQUEST
RRCSM	16:36:12.373	CCCH	Uplink	RRCSetupRequest
RRCSM	16:36:12.541	CCCH	Downlink	RRCSetup
RRCSM	16:36:12.549	DCCH	Uplink	RRCSetupComplete
RRCSM	16:36:12.621	DCCH	Downlink	DLInformationTransfer
L3SM	16:36:12.621		Downlink	REGISTRATION_ACCEPT
RRCSM	16:36:15.621	DCCH	Downlink	RRCRelease
RRCSM	16:36:15.673	BCCH-BCH	Downlink	MIB
RRCSM	16:36:47.769	BCCH-BCH	Downlink	MIB
RRCSM	16:36:47.855	BCCH-SCH	Downlink	SIB1
RRCSM	16:36:47.856	BCCH-BCH	Downlink	MIB
RRCSM	16:36:47.927	BCCH-SCH	Downlink	SIB1
RRCSM	16:37:31.605	BCCH-BCH	Downlink	MIB
RRCSM	16:37:31.696	BCCH-SCH	Downlink	SIB1
RRCSM	16:39:03.051	BCCH-BCH	Downlink	MIB
RRCSM	16:39:03.214	BCCH-SCH	Downlink	SIB1
RRCSM	16:40:43.184	BCCH-BCH	Downlink	MIB
RRCSM	16:40:43.214	BCCH-SCH	Downlink	SIB1
RRCSM	16:40:44.025	BCCH-BCH	Downlink	MIB
RRCSM	16:40:44.025	BCCH-BCH	Downlink	MIB
RRCSM	16:40:44.174	BCCH-SCH	Downlink	SIB1
RRCSM	16:42:33.227	BCCH-BCH	Downlink	MIB
RRCSM	16:42:33.293	BCCH-SCH	Downlink	SIB1
RRCSM	16:44:31.980	BCCH-BCH	Downlink	MIB
RRCSM	16:44:32.012	BCCH-SCH	Downlink	SIB1
RRCSM	16:46:40.628	BCCH-BCH	Downlink	MIB
RRCSM	16:46:40.811	BCCH-SCH	Downlink	SIB1
L3SM	16:48:15.664		Uplink	REGISTRATION_REQUEST
RRCSM	16:48:15.720	CCCH	Uplink	RRCSetupRequest
RRCSM	16:48:15.884	CCCH	Downlink	RRCSetup
RRCSM	16:48:15.893	DCCH	Uplink	RRCSetupComplete
RRCSM	16:48:15.955	DCCH	Downlink	DLInformationTransfer
L3SM	16:48:15.955		Downlink	REGISTRATION_ACCEPT
RRCSM	16:48:18.955	DCCH	Downlink	RRCRelease
RRCSM	16:48:19.006	BCCH-BCH	Downlink	MIB

LAYER 3 SIGNALING MESSAGE
Time: 16:48:15.664

REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)

M Extended protocol discriminator (hex data: 7e)
EPD value: 126 (5GS mobility management)

M Security header type (hex data: 0)
Security header type: 0 (Plain 5GS NAS message, not security protected)

M Spare Half Octet (hex data: 0)

M Message Type (hex data: 41)
Message number: 65

M 5GS registration type (hex data: 2)
5GS registration type value: mobility registration updating
FOR: No follow-on request pending

M ngKSI (hex data: 0)
TSC: native security context
NAS key set identifier: 0

M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 10)
Type of identity: 5G-GUTI
MCC: 1
MNC: 1
AMF Region ID: 10
AMF Set ID: 256
AMF Pointer: 1
5G-TMSI: 0xc1000010

O UE security capability (hex data: 2e04f070 f070)
5G-EA0: supported
128-5G-EA1: supported
128-5G-EA2: supported
128-5G-EA3: supported
5G-EA4: not supported
5G-EA5: not supported
5G-EA6: not supported
5G-EA7: not supported
5G-IA0: not supported
128-5G-IA1: supported
128-5G-IA2: supported
128-5G-IA3: supported
5G-IA4: not supported
5G-IA5: not supported
5G-IA6: not supported
5G-IA7: not supported
EEA0: supported
128-EEA1: supported
128-EEA2: supported
128-EEA3: supported
EEA4: not supported
EEA5: not supported
EEA6: not supported
EEA7: not supported
EIA0: not supported
128-EIA1: supported
128-EIA2: supported
128-EIA3: supported
EIA4: not supported
EIA5: not supported
EIA6: not supported
EIA7: not supported

O NAS message container (hex data: 710044e8 5c4746de 25d987ff b5ca4418 099d)

Figure 21. Scenario 4 UE log showing it repeating registration on FBS after short and long timeouts

False Base Station

EventId	Time	RRC subch...	RRC direction	RRC message name	LAYER 3 SIGNALING MESSAGE
RRCSM	16:48:19.701	BCCH-BCH	Downlink	MIB	Time: 16:48:15.664
RRCSM	16:48:19.701	BCCH-BCH	Downlink	MIB	
RRCSM	16:48:19.850	BCCH-SCH	Downlink	SIB1	REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)
L3SM	16:48:29.007		Uplink	REGISTRATION_REQUEST	M Extended protocol discriminator (hex data: 7e) EPD value: 126 (5GS mobility management)
RRCSM	16:48:29.069	CCCH	Uplink	RRCSetupRequest	M Security header type (hex data: 0) Security header type: 0 (Plain 5GS NAS message, not security protected)
RRCSM	16:48:29.254	CCCH	Downlink	RRCSetup	M Spare Half Octet (hex data: 0)
RRCSM	16:48:29.263	DCCH	Uplink	RRCSetupComplete	M Message Type (hex data: 41) Message number: 65
RRCSM	16:48:29.369	DCCH	Downlink	DLInformationTransfer	M 5GS registration type (hex data: 2) 5GS registration type value: mobility registration updating FOR: No follow-on request pending
L3SM	16:48:29.370		Downlink	REGISTRATION_ACCEPT	M ngKSI (hex data: 0) TSC: native security context NAS key set identifier: 0
RRCSM	16:48:32.370	DCCH	Downlink	RRCRelease	M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 10) Type of identity: 5G-GUTI MCC: 1 MNC: 1 AMF Region ID: 10 AMF Set ID: 256 AMF Pointer: 1 5G-TMSI: 0xc1000010
RRCSM	16:48:32.431	BCCH-BCH	Downlink	MIB	O UE security capability (hex data: 2e04f070 f070)
RRCSM	16:48:35.071	BCCH-BCH	Downlink	MIB	5G-EA0: supported 128-5G-EA1: supported 128-5G-EA2: supported 128-5G-EA3: supported 5G-EA4: not supported 5G-EA5: not supported 5G-EA6: not supported 5G-EA7: not supported 5G-IA0: not supported 128-5G-IA1: supported 128-5G-IA2: supported 128-5G-IA3: supported 5G-IA4: not supported 5G-IA5: not supported 5G-IA6: not supported 5G-IA7: not supported EEA0: supported 128-EEA1: supported 128-EEA2: supported 128-EEA3: supported EEA4: not supported EEA5: not supported EEA6: not supported EEA7: not supported EIA0: not supported 128-EIA1: supported 128-EIA2: supported 128-EIA3: supported EIA4: not supported EIA5: not supported EIA6: not supported EIA7: not supported
RRCSM	16:48:35.210	BCCH-SCH	Downlink	SIB1	O NAS message container (hex data: 710044e8 5c4746de 25d987ff b5ca4418 099d0
L3SM	16:48:42.432		Uplink	REGISTRATION_REQUEST	
RRCSM	16:48:42.432	CCCH	Uplink	RRCSetupRequest	
RRCSM	16:48:42.625	CCCH	Downlink	RRCSetup	
RRCSM	16:48:42.633	DCCH	Uplink	RRCSetupComplete	
RRCSM	16:48:42.700	DCCH	Downlink	DLInformationTransfer	
L3SM	16:48:42.700		Downlink	REGISTRATION_ACCEPT	
RRCSM	16:48:45.700	DCCH	Downlink	RRCRelease	
RRCSM	16:48:45.752	BCCH-BCH	Downlink	MIB	
L3SM	16:48:55.752		Uplink	REGISTRATION_REQUEST	
RRCSM	16:48:55.752	CCCH	Uplink	RRCSetupRequest	
RRCSM	16:48:55.935	CCCH	Downlink	RRCSetup	
RRCSM	16:48:55.943	DCCH	Uplink	RRCSetupComplete	
RRCSM	16:48:56.039	DCCH	Downlink	DLInformationTransfer	
L3SM	16:48:56.040		Downlink	REGISTRATION_ACCEPT	
RRCSM	16:48:59.039	DCCH	Downlink	RRCRelease	
RRCSM	16:48:59.092	BCCH-BCH	Downlink	MIB	
L3SM	16:49:09.092		Uplink	REGISTRATION_REQUEST	
RRCSM	16:49:09.092	CCCH	Uplink	RRCSetupRequest	
RRCSM	16:49:09.265	CCCH	Downlink	RRCSetup	
RRCSM	16:49:09.273	DCCH	Uplink	RRCSetupComplete	
RRCSM	16:49:09.345	DCCH	Downlink	DLInformationTransfer	
L3SM	16:49:09.345		Downlink	REGISTRATION_ACCEPT	
RRCSM	16:49:12.345	DCCH	Downlink	RRCRelease	
RRCSM	16:49:12.397	BCCH-BCH	Downlink	MIB	
RRCSM	16:49:44.819	BCCH-BCH	Downlink	MIB	
RRCSM	16:49:44.969	BCCH-SCH	Downlink	SIB1	
RRCSM	16:50:50.523	BCCH-BCH	Downlink	MIB	
RRCSM	16:50:50.601	BCCH-SCH	Downlink	SIB1	
RRCSM	16:51:31.346	BCCH-BCH	Downlink	MIB	
RRCSM	16:51:31.400	BCCH-SCH	Downlink	SIB1	
RRCSM	16:53:00.332	BCCH-BCH	Downlink	MIB	
RRCSM	16:53:00.362	BCCH-SCH	Downlink	SIB1	
RRCSM	16:53:00.842	BCCH-SCH	Downlink	SIB1	
RRCSM	16:53:00.857	BCCH-BCH	Downlink	MIB	
RRCSM	16:53:00.857	BCCH-BCH	Downlink	MIB	
RRCSM	16:54:38.818	BCCH-BCH	Downlink	MIB	
RRCSM	16:54:38.917	BCCH-SCH	Downlink	SIB1	

Figure 22. Scenario 4 UE log showing DoS conditions

False Base Station

FBS turns off

UE returns to legitimate cell

EventId	Time	RRC subch...	RRC direction	RRC message name	
RRCSM	16:56:26.702	BCCH-BCH	Downlink	MIB	
RRCSM	16:56:26.758	BCCH-SCH	Downlink	SIB1	
RRCSM	16:58:24.385	BCCH-BCH	Downlink	MIB	
RRCSM	16:58:24.435	BCCH-SCH	Downlink	SIB1	
RRCSM	17:00:33.655	BCCH-BCH	Downlink	MIB	
RRCSM	17:00:33.715	BCCH-SCH	Downlink	SIB1	
RRCSM	17:00:33.955	BCCH-SCH	Downlink	SIB1	
RRCSM	17:00:33.970	BCCH-BCH	Downlink	MIB	
RRCSM	17:00:33.970	BCCH-BCH	Downlink	MIB	
L3SM	17:01:12.389		Uplink	REGISTRATION_REQUEST	
RRCSM	17:01:12.390	CCCH	Uplink	RRCSetupRequest	
RRCSM	17:01:12.466	CCCH	Downlink	RRCSetup	
RRCSM	17:01:12.475	DCCH	Uplink	RRCSetupComplete	
RRCSM	17:01:12.614	DCCH	Downlink	DLInformationTransfer	
L3SM	17:01:12.615		Downlink	AUTHENTICATION_REQUEST	
L3SM	17:01:12.650		Uplink	AUTHENTICATION_RESPONSE	
RRCSM	17:01:12.651	DCCH	Uplink	ULInformationTransfer	
RRCSM	17:01:12.667	DCCH	Downlink	DLInformationTransfer	
L3SM	17:01:12.667		Downlink	SECURITY_MODE_COMMAND	
L3SM	17:01:12.668		Uplink	SECURITY_MODE_COMPLETE	
RRCSM	17:01:12.668	DCCH	Uplink	ULInformationTransfer	
RRCSM	17:01:12.687	DCCH	Downlink	DLInformationTransfer	
L3SM	17:01:12.688		Downlink	REGISTRATION_ACCEPT	
RRCSM	17:01:12.688	DCCH	Downlink	RRCRelease	
RRCSM	17:01:12.725	BCCH-BCH	Downlink	MIB	
L3SM	17:01:12.863		Uplink	PDU_SESSION_ESTABLISHMENT_REQU...	

LAYER 3 SIGNALING MESSAGE

Time: 17:01:12.389

REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)

M Extended protocol discriminator (hex data: 7e)
EPD value: 126 (5GS mobility management)

M Security header type (hex data: 0)
Security header type: 0 (Plain 5GS NAS message, not security protected)

M Spare Half Octet (hex data: 0)

M Message Type (hex data: 41)
Message number: 65

M 5GS registration type (hex data: 2)
5GS registration type value: mobility registration updating
FOR: No follow-on request pending

M ngKSI (hex data: 0)
TSC: native security context
NAS key set identifier: 0

M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 10)
Type of identity: 5G-GUTI
MCC: 1
MNC: 1
AMF Region ID: 10
AMF Set ID: 256
AMF Pointer: 1
5G-TMSI: 0xc1000010

O UE security capability (hex data: 2e04f070 f070)
5G-EA0: supported
128-5G-EA1: supported
128-5G-EA2: supported
128-5G-EA3: supported
5G-EA4: not supported

Figure 23. Scenario 4 UE log showing return to legitimate cell after FBS turns off

UE log for Scenario 5

Steps 1 - 3

EventId	Time	RRC subch...	RRC direction	RRC message name
RRCSM	17:02:56.921	BCCH-BCH	Downlink	MIB
RRCSM	17:02:56.921	BCCH-SCH	Downlink	SIB1
L3SM	17:02:56.921		Uplink	REGISTRATION_REQUEST
RRCSM	17:02:56.921	CCCH	Uplink	RRCSetupRequest
RRCSM	17:02:56.983	CCCH	Downlink	RRCSetup
RRCSM	17:02:56.990	BCCH-SCH	Downlink	SystemInformation - SIB3,SIB5,SIB4,SIB2
RRCSM	17:02:56.996	DCCH	Uplink	RRCSetupComplete
RRCSM	17:02:57.202	DCCH	Downlink	DLInformationTransfer
L3SM	17:02:57.203		Downlink	AUTHENTICATION_REQUEST
L3SM	17:02:57.236		Uplink	AUTHENTICATION_RESPONSE
RRCSM	17:02:57.237	DCCH	Uplink	ULInformationTransfer
RRCSM	17:02:57.254	DCCH	Downlink	DLInformationTransfer
L3SM	17:02:57.254		Downlink	SECURITY_MODE_COMMAND
L3SM	17:02:57.255		Uplink	SECURITY_MODE_COMPLETE
RRCSM	17:02:57.255	DCCH	Uplink	ULInformationTransfer
RRCSM	17:02:57.312	BCCH-SCH	Downlink	SIB1
RRCSM	17:02:57.327	BCCH-BCH	Downlink	MIB
RRCSM	17:02:57.327	BCCH-BCH	Downlink	MIB
RRCSM	17:02:57.465	DCCH	Downlink	DLInformationTransfer
L3SM	17:02:57.466		Downlink	REGISTRATION_ACCEPT
RRCSM	17:02:57.466	DCCH	Downlink	DLInformationTransfer
L3SM	17:02:57.467		Downlink	CONFIGURATION_UPDATE_COMMAND
RRCSM	17:02:57.508	BCCH-BCH	Downlink	MIB
L3SM	17:02:57.602		Uplink	PDU_SESSION_ESTABLISHMENT_REQU...
RRCSM	17:03:28.097	BCCH-BCH	Downlink	MIB

Steps 4 - 5

RRCSM	17:03:28.179	BCCH-SCH	Downlink	SIB1
RRCSM	17:03:28.180	BCCH-BCH	Downlink	MIB
RRCSM	17:03:28.232	BCCH-SCH	Downlink	SIB1
RRCSM	17:03:35.332	BCCH-BCH	Downlink	MIB
RRCSM	17:03:35.379	BCCH-SCH	Downlink	SIB1

Steps 6 - 7

LAYER 3 SIGNALING MESSAGE

Time: 17:02:56.921

REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)

M Extended protocol discriminator (hex data: 7e)
EPD value: 126 (5GS mobility management)

M Security header type (hex data: 0)
Security header type: 0 (Plain 5GS NAS message, not security protected)

M Spare Half Octet (hex data: 0)

M Message Type (hex data: 41)
Message number: 65

M 5GS registration type (hex data: 9)
5GS registration type value: initial registration
FOR: Follow-on request pending

M ngKSI (hex data: 1)
TSC: native security context
NAS key set identifier: 1

M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 10)
Type of identity: 5G-GUTI
MCC: 1
MNC: 1
AMF Region ID: 10
AMF Set ID: 256
AMF Pointer: 1
5G-TMSI: 0xc1000010

O UE security capability (hex data: 2e04f070 f070)
5G-EA0: supported
128-5G-EA1: supported
128-5G-EA2: supported
128-5G-EA3: supported
5G-EA4: not supported
5G-EA5: not supported
5G-EA6: not supported
5G-EA7: not supported
5G-EA8: not supported
128-5G-EA9: supported

Figure 24. Scenario 5 UE log showing steps 1 to 7

Steps 7-11

EventId	Time	RRC subch...	RRC direction	RRC message name
L3SM	17:03:35.388		Uplink	REGISTRATION_REQUEST
RRCSM	17:03:35.388	CCCH	Uplink	RRCSetupRequest
RRCSM	17:03:35.574	CCCH	Downlink	RRCSetup
RRCSM	17:03:35.582	DCCH	Uplink	RRCSetupComplete
RRCSM	17:03:35.689	DCCH	Downlink	DLInformationTransfer
L3SM	17:03:35.689		Downlink	REGISTRATION_REJECT
RRCSM	17:03:38.689	DCCH	Downlink	RRCRelease
RRCSM	17:03:38.752	BCCH-BCH	Downlink	MIB
RRCSM	17:03:38.847	BCCH-BCH	Downlink	MIB
RRCSM	17:03:38.899	BCCH-SCH	Downlink	SIB1
L3SM	17:03:38.910		Uplink	REGISTRATION_REQUEST
RRCSM	17:03:38.910	CCCH	Uplink	RRCSetupRequest
RRCSM	17:03:39.074	CCCH	Downlink	RRCSetup
RRCSM	17:03:39.082	DCCH	Uplink	RRCSetupComplete
RRCSM	17:03:39.194	DCCH	Downlink	DLInformationTransfer
L3SM	17:03:39.194		Downlink	REGISTRATION_REJECT
RRCSM	17:03:42.189	DCCH	Downlink	RRCRelease
RRCSM	17:03:42.252	BCCH-BCH	Downlink	MIB
RRCSM	17:03:42.346	BCCH-BCH	Downlink	MIB
RRCSM	17:03:42.419	BCCH-SCH	Downlink	SIB1

Step 12

LAYER 3 SIGNALING MESSAGE

Time: 17:03:35.388

REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)

M Extended protocol discriminator (hex data: 7e)
EPD value: 126 (5GS mobility management)

M Security header type (hex data: 0)
Security header type: 0 (Plain 5GS NAS message, not security protected)

M Spare Half Octet (hex data: 0)

M Message Type (hex data: 41)
Message number: 65

M 5GS registration type (hex data: 2)
5GS registration type value: mobility registration updating
FOR: No follow-on request pending

M ngKSI (hex data: 2)
TSC: native security context
NAS key set identifier: 2

M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 10)
Type of identity: 5G-GUTI
MCC: 1
MNC: 1
AMF Region ID: 10
AMF Set ID: 256
AMF Pointer: 1

Figure 25. Scenario 5 UE log showing steps 7 to 12

False Base Station

UE falls
victim to
DoS

EventId	Time	RRC subch...	RRC direction	RRC message name	LAYER 3 SIGNALING MESSAGE
L3SM	17:03:42.429		Uplink	REGISTRATION_REQUEST	Time: 17:03:35.388
RRCSM	17:03:42.429	CCCH	Uplink	RRCSetupRequest	
RRCSM	17:03:42.594	CCCH	Downlink	RRCSetup	REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)
RRCSM	17:03:42.602	DCCH	Uplink	RRCSetupComplete	
RRCSM	17:03:42.711	DCCH	Downlink	DLInformationTransfer	M Extended protocol discriminator (hex data: 7e) EPD value: 126 (5GS mobility management)
L3SM	17:03:42.711		Downlink	REGISTRATION_REJECT	M Security header type (hex data: 0) Security header type: 0 (Plain 5GS NAS message, not security protected)
RRCSM	17:03:45.708	DCCH	Downlink	RRCRelease	M Spare Half Octet (hex data: 0)
RRCSM	17:03:45.772	BCCH-BCH	Downlink	MIB	M Message Type (hex data: 41) Message number: 65
RRCSM	17:03:45.868	BCCH-BCH	Downlink	MIB	M 5GS registration type (hex data: 2) 5GS registration type value: mobility registration updating FOR: No follow-on request pending
RRCSM	17:03:45.939	BCCH-SCH	Downlink	SIB1	M ngKSI (hex data: 2) TSC: native security context NAS key set identifier: 2
L3SM	17:03:45.949		Uplink	REGISTRATION_REQUEST	M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 10) Type of identity: 5G-GUTI
RRCSM	17:03:45.950	CCCH	Uplink	RRCSetupRequest	MCC: 1 MNC: 1
RRCSM	17:03:46.134	CCCH	Downlink	RRCSetup	AMF Region ID: 10 AMF Set ID: 256 AMF Pointer: 1
RRCSM	17:03:46.142	DCCH	Uplink	RRCSetupComplete	5G-TMSI: 0xc1000010
RRCSM	17:03:46.206	DCCH	Downlink	DLInformationTransfer	O UE security capability (hex data: 2e04f070 f070) 5G-EA0: supported 128-5G-EA1: supported 128-5G-EA2: supported 128-5G-EA3: supported 5G-EA4: not supported 5G-EA5: not supported 5G-EA6: not supported 5G-EA7: not supported 5G-EA8: not supported 128-5G-EA9: supported 128-5G-EA10: supported 128-5G-EA11: supported 5G-EA12: not supported 5G-EA13: not supported 5G-EA14: not supported 5G-EA15: not supported 5G-EA16: not supported 5G-EA17: not supported EEA0: supported 128-EEA1: supported 128-EEA2: supported 128-EEA3: supported EEA4: not supported EEA5: not supported EEA6: not supported EEA7: not supported EIA0: not supported 128-EIA1: supported 128-EIA2: supported 128-EIA3: supported EIA4: not supported EIA5: not supported EIA6: not supported EIA7: not supported
L3SM	17:03:46.206		Downlink	REGISTRATION_REJECT	
RRCSM	17:03:49.204	DCCH	Downlink	RRCRelease	
RRCSM	17:03:49.256	BCCH-BCH	Downlink	MIB	
RRCSM	17:03:49.351	BCCH-BCH	Downlink	MIB	
RRCSM	17:03:49.459	BCCH-SCH	Downlink	SIB1	
L3SM	17:03:49.469		Uplink	REGISTRATION_REQUEST	
RRCSM	17:03:49.470	CCCH	Uplink	RRCSetupRequest	
RRCSM	17:03:49.634	CCCH	Downlink	RRCSetup	
RRCSM	17:03:49.642	DCCH	Uplink	RRCSetupComplete	
RRCSM	17:03:49.736	DCCH	Downlink	DLInformationTransfer	
L3SM	17:03:49.736		Downlink	REGISTRATION_REJECT	
RRCSM	17:03:50.758	BCCH-BCH	Downlink	MIB	
RRCSM	17:03:50.758	BCCH-BCH	Downlink	MIB	
RRCSM	17:03:50.899	BCCH-SCH	Downlink	SIB1	
RRCSM	17:03:52.733	DCCH	Downlink	RRCRelease	
RRCSM	17:03:52.796	BCCH-BCH	Downlink	MIB	
RRCSM	17:03:52.890	BCCH-BCH	Downlink	MIB	
RRCSM	17:03:52.979	BCCH-SCH	Downlink	SIB1	
L3SM	17:03:52.989		Uplink	REGISTRATION_REQUEST	
RRCSM	17:03:52.990	CCCH	Uplink	RRCSetupRequest	
RRCSM	17:03:53.174	CCCH	Downlink	RRCSetup	
RRCSM	17:03:53.182	DCCH	Uplink	RRCSetupComplete	
RRCSM	17:03:53.246	DCCH	Downlink	DLInformationTransfer	
L3SM	17:03:53.246		Downlink	REGISTRATION_REJECT	
RRCSM	17:03:56.243	DCCH	Downlink	RRCRelease	
RRCSM	17:03:56.296	BCCH-BCH	Downlink	MIB	
RRCSM	17:03:56.390	BCCH-BCH	Downlink	MIB	
RRCSM	17:03:56.499	BCCH-SCH	Downlink	SIB1	
L3SM	17:03:56.509		Uplink	REGISTRATION_REQUEST	
RRCSM	17:03:56.510	CCCH	Uplink	RRCSetupRequest	
RRCSM	17:03:56.674	CCCH	Downlink	RRCSetup	
RRCSM	17:03:56.682	DCCH	Uplink	RRCSetupComplete	
RRCSM	17:03:56.751	DCCH	Downlink	DLInformationTransfer	
L3SM	17:03:56.751		Downlink	REGISTRATION_REJECT	
RRCSM	17:03:59.748	DCCH	Downlink	RRCRelease	O NAS message container (hex data: 7100445a 9953bfff 91d8db51 e97c3bdc 7aeb2)

Figure 26. Scenario 5 UE log showing DoS conditions

UE log for Scenario 6

Steps 1 - 3	EventId	Time	RRC subch...	RRC direction	RRC message name	LAYER 3 SIGNALING MESSAGE Time: 17:08:58.038 REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6) M Extended protocol discriminator (hex data: 7e) EPD value: 126 (5GS mobility management) M Security header type (hex data: 0) Security header type: 0 (Plain 5GS NAS message, not security protected) M Spare Half Octet (hex data: 0) M Message Type (hex data: 41) Message number: 65 M 5GS registration type (hex data: 9) 5GS registration type value: initial registration FOR: Follow-on request pending M ngKSI (hex data: 2) TSC: native security context NAS key set identifier: 2 M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 11) Type of identity: 5G-GUTI MCC: 1 MNC: 1 AMF Region ID: 10 AMF Set ID: 256 AMF Pointer: 1 5G-TMSI: 0xc1000011 O UE security capability (hex data: 2e04f070 f070) 5G-EA0: supported 128-5G-EA1: supported 128-5G-EA2: supported 128-5G-EA3: supported 5G-EA4: not supported 5G-EA5: not supported 5G-EA6: not supported 5G-EA7: not supported 5G-IA0: not supported 128-5G-IA1: supported
	RRCSM	17:08:57.993	BCCH-BCH	Downlink	MIB	
	RRCSM	17:08:58.029	BCCH-SCH	Downlink	SIB1	
Steps 4 - 5	L3SM	17:08:58.038		Uplink	REGISTRATION_REQUEST	
	RRCSM	17:08:58.038	CCCH	Uplink	RRCSetupRequest	
	RRCSM	17:08:58.099	CCCH	Downlink	RRCSetup	
	RRCSM	17:08:58.105	BCCH-SCH	Downlink	SystemInformation - SIB3,SIB5,SIB4,SIB2	
	RRCSM	17:08:58.113	DCCH	Uplink	RRCSetupComplete	
	RRCSM	17:08:58.215	DCCH	Downlink	DLInformationTransfer	
	L3SM	17:08:58.216		Downlink	AUTHENTICATION_REQUEST	
	L3SM	17:08:58.256		Uplink	AUTHENTICATION_RESPONSE	
	RRCSM	17:08:58.256	DCCH	Uplink	ULInformationTransfer	
	RRCSM	17:08:58.269	BCCH-SCH	Downlink	SIB1	
	RRCSM	17:08:58.275	DCCH	Downlink	DLInformationTransfer	
	L3SM	17:08:58.275		Downlink	SECURITY_MODE_COMMAND	
	L3SM	17:08:58.275		Uplink	SECURITY_MODE_COMPLETE	
	RRCSM	17:08:58.275	DCCH	Uplink	ULInformationTransfer	
	RRCSM	17:08:58.283	BCCH-BCH	Downlink	MIB	
Steps 6 - 7	RRCSM	17:08:58.283	BCCH-BCH	Downlink	MIB	
	RRCSM	17:08:58.434	DCCH	Downlink	DLInformationTransfer	
	L3SM	17:08:58.435		Downlink	REGISTRATION_ACCEPT	
	RRCSM	17:08:58.435	DCCH	Downlink	DLInformationTransfer	
	L3SM	17:08:58.436		Downlink	CONFIGURATION_UPDATE_COMMAND	
	RRCSM	17:08:58.494	BCCH-BCH	Downlink	MIB	
	L3SM	17:08:58.547		Uplink	PDU_SESSION_ESTABLISHMENT_REQ...	
	RRCSM	17:09:28.909	BCCH-BCH	Downlink	MIB	
	RRCSM	17:09:28.964	BCCH-SCH	Downlink	SIB1	
	RRCSM	17:09:28.965	BCCH-BCH	Downlink	MIB	
	RRCSM	17:09:29.028	BCCH-SCH	Downlink	SIB1	
	RRCSM	17:09:36.138	BCCH-BCH	Downlink	MIB	
	RRCSM	17:09:36.325	BCCH-SCH	Downlink	SIB1	

Figure 27. Scenario 6 UE log showing steps 1 to 7

Steps 8-11	EventId	Time	RRC subch...	RRC direction	RRC message name	LAYER 3 SIGNALING MESSAGE Time: 17:09:36.333 REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6) M Extended protocol discriminator (hex data: 7e) EPD value: 126 (5GS mobility management) M Security header type (hex data: 0) Security header type: 0 (Plain 5GS NAS message, not security protected) M Spare Half Octet (hex data: 0) M Message Type (hex data: 41) Message number: 65 M 5GS registration type (hex data: 2) 5GS registration type value: mobility registration updating FOR: No follow-on request pending M ngKSI (hex data: 3) TSC: native security context NAS key set identifier: 3 M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 11) Type of identity: 5G-GUTI MCC: 1 MNC: 1 AMF Region ID: 10 AMF Set ID: 256 AMF Pointer: 1
	L3SM	17:09:36.333		Uplink	REGISTRATION_REQUEST	
	RRCSM	17:09:36.333	CCCH	Uplink	RRCSetupRequest	
Step 12	RRCSM	17:09:36.519	CCCH	Downlink	RRCSetup	
	RRCSM	17:09:36.527	DCCH	Uplink	RRCSetupComplete	
	RRCSM	17:09:36.604	DCCH	Downlink	DLInformationTransfer	
	L3SM	17:09:36.605		Downlink	REGISTRATION_REJECT	
	RRCSM	17:09:36.605	DCCH	Downlink	RRCRelease	
	RRCSM	17:09:36.655	BCCH-BCH	Downlink	MIB	
	RRCSM	17:09:36.975	BCCH-BCH	Downlink	MIB	
	RRCSM	17:09:36.975	BCCH-BCH	Downlink	MIB	
	RRCSM	17:09:37.125	BCCH-SCH	Downlink	SIB1	
	L3SM	17:09:46.606		Uplink	REGISTRATION_REQUEST	
	RRCSM	17:09:46.606	CCCH	Uplink	RRCSetupRequest	
	RRCSM	17:09:46.779	CCCH	Downlink	RRCSetup	
	RRCSM	17:09:46.787	DCCH	Uplink	RRCSetupComplete	
	RRCSM	17:09:46.865	DCCH	Downlink	DLInformationTransfer	
	L3SM	17:09:46.865		Downlink	REGISTRATION_REJECT	
	RRCSM	17:09:46.865	DCCH	Downlink	RRCRelease	
	RRCSM	17:09:46.916	BCCH-BCH	Downlink	MIB	
	RRCSM	17:09:47.215	BCCH-BCH	Downlink	MIB	

Figure 28. Scenario 6 UE log showing steps 8 to 12

False Base Station

UE repeats
registration
attempt
5 times

UE falls
victim to
DoS

EventId	Time	RRC subch...	RRC direction	RRC message name
RRCSM	17:09:47.215	BCCH-BCH	Downlink	MIB
RRCSM	17:09:47.365	BCCH-SCH	Downlink	SIB1
L3SM	17:09:56.866		Uplink	REGISTRATION_REQUEST
RRCSM	17:09:56.867	CCCH	Uplink	RRCSetupRequest
RRCSM	17:09:57.059	CCCH	Downlink	RRCSetup
RRCSM	17:09:57.067	DCCH	Uplink	RRCSetupComplete
RRCSM	17:09:57.145	DCCH	Downlink	DLInformationTransfer
L3SM	17:09:57.145		Downlink	REGISTRATION_REJECT
RRCSM	17:09:57.145	DCCH	Downlink	RRCRelease
RRCSM	17:09:57.195	BCCH-BCH	Downlink	MIB
RRCSM	17:09:57.455	BCCH-BCH	Downlink	MIB
RRCSM	17:09:57.455	BCCH-BCH	Downlink	MIB
RRCSM	17:09:57.605	BCCH-SCH	Downlink	SIB1
L3SM	17:10:07.146		Uplink	REGISTRATION_REQUEST
RRCSM	17:10:07.147	CCCH	Uplink	RRCSetupRequest
RRCSM	17:10:07.339	CCCH	Downlink	RRCSetup
RRCSM	17:10:07.348	DCCH	Uplink	RRCSetupComplete
RRCSM	17:10:07.440	DCCH	Downlink	DLInformationTransfer
L3SM	17:10:07.440		Downlink	REGISTRATION_REJECT
RRCSM	17:10:07.440	DCCH	Downlink	RRCRelease
RRCSM	17:10:07.500	BCCH-BCH	Downlink	MIB
RRCSM	17:10:07.695	BCCH-BCH	Downlink	MIB
RRCSM	17:10:07.695	BCCH-BCH	Downlink	MIB
RRCSM	17:10:07.845	BCCH-SCH	Downlink	SIB1
L3SM	17:10:17.441		Uplink	REGISTRATION_REQUEST
RRCSM	17:10:17.442	CCCH	Uplink	RRCSetupRequest
RRCSM	17:10:17.629	CCCH	Downlink	RRCSetup
RRCSM	17:10:17.637	DCCH	Uplink	RRCSetupComplete
RRCSM	17:10:17.740	DCCH	Downlink	DLInformationTransfer
L3SM	17:10:17.740		Downlink	REGISTRATION_REJECT
RRCSM	17:10:17.740	DCCH	Downlink	RRCRelease
RRCSM	17:10:49.126	BCCH-BCH	Downlink	MIB
RRCSM	17:10:49.285	BCCH-SCH	Downlink	SIB1
RRCSM	17:10:49.285	BCCH-BCH	Downlink	MIB
RRCSM	17:10:49.348	BCCH-SCH	Downlink	SIB1
RRCSM	17:11:31.905	BCCH-BCH	Downlink	MIB
RRCSM	17:11:32.005	BCCH-SCH	Downlink	SIB1
RRCSM	17:12:23.423	BCCH-BCH	Downlink	MIB
RRCSM	17:12:23.468	BCCH-SCH	Downlink	SIB1
RRCSM	17:13:06.240	BCCH-BCH	Downlink	MIB
RRCSM	17:13:06.268	BCCH-SCH	Downlink	SIB1
RRCSM	17:13:06.589	BCCH-SCH	Downlink	SIB1
RRCSM	17:13:06.604	BCCH-BCH	Downlink	MIB
RRCSM	17:13:06.604	BCCH-BCH	Downlink	MIB
RRCSM	17:14:36.051	BCCH-BCH	Downlink	MIB
RRCSM	17:14:36.106	BCCH-SCH	Downlink	SIB1
RRCSM	17:14:36.186	BCCH-SCH	Downlink	SIB1
RRCSM	17:14:36.201	BCCH-BCH	Downlink	MIB
RRCSM	17:14:36.201	BCCH-BCH	Downlink	MIB
RRCSM	17:16:14.474	BCCH-BCH	Downlink	MIB

LAYER 3 SIGNALING MESSAGE

Time: 17:09:57.145

REGISTRATION REJECT 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.9)

M Extended protocol discriminator (hex data: 7e)
EPD value: 126 (5GS mobility management)

M Security header type (hex data: 0)
Security header type: 0 (Plain 5GS NAS message, not security protected)

M Spare Half Octet (hex data: 0)

M Message Type (hex data: 44)
Message number: 68

M 5GMM cause (hex data: 17)
Cause value: 23 (UE security capabilities mismatch)

Layer 3 data:
7e 00 44 17

Figure 29. Scenario 6 UE log showing DoS conditions

False Base Station

FBS turns off

UE returns to legitimate cell

EventId	Time	RRC subch...	RRC direction	RRC message name	
RRCSM	17:16:14.505	BCCH-SCH	Downlink	SIB1	
RRCSM	17:18:04.059	BCCH-BCH	Downlink	MIB	
RRCSM	17:18:04.103	BCCH-SCH	Downlink	SIB1	
RRCSM	17:20:01.272	BCCH-BCH	Downlink	MIB	
RRCSM	17:20:01.303	BCCH-SCH	Downlink	SIB1	
RRCSM	17:22:10.174	BCCH-BCH	Downlink	MIB	
RRCSM	17:22:10.263	BCCH-SCH	Downlink	SIB1	
L3SM	17:22:17.735		Uplink	REGISTRATION_REQUEST	
RRCSM	17:22:17.735	CCCH	Uplink	RRCSetupRequest	
RRCSM	17:22:17.814	CCCH	Downlink	RRCSetup	
RRCSM	17:22:17.823	DCCH	Uplink	RRCSetupComplete	
RRCSM	17:22:18.024	DCCH	Downlink	DLInformationTransfer	
L3SM	17:22:18.025		Downlink	AUTHENTICATION_REQUEST	
L3SM	17:22:18.060		Uplink	AUTHENTICATION_RESPONSE	
RRCSM	17:22:18.061	DCCH	Uplink	ULInformationTransfer	
RRCSM	17:22:18.081	DCCH	Downlink	DLInformationTransfer	
L3SM	17:22:18.082		Downlink	SECURITY_MODE_COMMAND	
L3SM	17:22:18.082		Uplink	SECURITY_MODE_COMPLETE	
RRCSM	17:22:18.082	DCCH	Uplink	ULInformationTransfer	
RRCSM	17:22:18.097	DCCH	Downlink	DLInformationTransfer	
L3SM	17:22:18.098		Downlink	REGISTRATION_ACCEPT	
RRCSM	17:22:18.098	DCCH	Downlink	RRCRelease	
RRCSM	17:22:18.135	BCCH-BCH	Downlink	MIB	
L3SM	17:22:18.292		Uplink	PDU_SESSION_ESTABLISHMENT_REQU...	

LAYER 3 SIGNALING MESSAGE

Time: 17:22:17.735

REGISTRATION REQUEST 3GPP TS 24.501 ver 16.8.0 Rel 16 (8.2.6)

M Extended protocol discriminator (hex data: 7e)
EPD value: 126 (5GS mobility management)

M Security header type (hex data: 0)
Security header type: 0 (Plain 5GS NAS message, not security protected)

M Spare Half Octet (hex data: 0)

M Message Type (hex data: 41)
Message number: 65

M 5GS registration type (hex data: 2)
5GS registration type value: mobility registration updating
FUR: No follow-on request pending

M ngKSI (hex data: 3)
TSC: native security context
NAS key set identifier: 3

M 5GS mobile identity (hex data: 000bf200 f1100a40 01c10000 11)
Type of identity: 5G-GUTI
MCC: 1
MNC: 1
AMF Region ID: 10
AMF Set ID: 256
AMF Pointer: 1
5G-TMSI: 0xc1000011

O UE security capability (hex data: 2e04f070 f070)
5G-EA0: supported
128-5G-EA1: supported
128-5G-EA2: supported

Figure 30. Scenario 6 UE log showing return to legitimate cell after FBS turns off

References

- [1] Tao Wan (2019). False Base Station or IMSI Catcher: What You Need to Know. Available at <https://www.cablelabs.com/blog/false-base-station-or-imsi-catcher-what-you-need-to-know>
- [2] Cichonski JA, Franklin JM, Bartock MJ (2016) Guide to LTE Security. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-187 <https://doi.org/10.6028/NIST.SP.800-187>
- [3] Wireless Innovation Forum (2025) What is Software Defined Radio. Available at <https://winnforum.org/wp-content/uploads/WinnForum/documents/SoftwareDefinedRadio.pdf>
- [4] Bartock M, Cichonski J, Souppaya M, Kent K, Grayeli P, Sharma S, Teague C (2026). Protecting Subscriber Identifiers with Subscription Concealed Identifier (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) 36A. <https://doi.org/10.6028/NIST.CSWP.36A>
- [5] Bartock M, Cichonski J, Souppaya M, Kent K, Grayeli P, Sharma S (2026). Reallocation of Temporary Identities (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) 36C. <https://doi.org/10.6028/NIST.CSWP.36C>
- [6] Bartock M, Cichonski J, Souppaya M, Kent K, Grayeli P, Sharma S, Teague C (2026). No SUPI-Based Paging (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) 36D. <https://doi.org/10.6028/NIST.CSWP.36D>
- [7] Bartock M, Cichonski J, Grayeli P, Sharma S (2026). Initial NAS Message Security (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) 36F. <https://doi.org/10.6028/NIST.CSWP.36F.ipd>
- [8] Linkmobility (2026). *The global 2G and 3G shutdown is accelerating*. Available at <https://www.linkmobility.com/news/the-global-2g-and-3g-shutdown-is-accelerating>
- [9] Singla A, Behnia R, Hussain SR, Yavuz AA, Bertino E (2021). Look Before You Leap: Secure Connection Bootstrapping for 5G Networks to Defend Against Fake Base-Stations. *ASIA CCS '21: Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security* (ACM, Hong Kong). <https://doi.org/10.1145/3433210.3453082>
- [10] Eleftherakis S, Giustiniano D, Kourtellis N (2024). SoK: Evaluating 5G Protocols Against Legacy and Emerging Privacy and Security Attacks (Imdea Networks Institute, Telefonica Research). <https://doi.org/10.48550/arXiv.2409.06360>
- [11] 3rd Generation Partnership Project. Report # 33.809: Study on 5G security enhancements against False Base Stations (FBS). Available at <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3539>
- [12] Purification S, Kim J, Kim J, Chang, SY (2024). Fake Base Station Detection and Link Routing Defense (Electronics 2024). <https://doi.org/10.3390/electronics13173474>

- [13] Mubasshir KS, Karim I, Bertino E (2025). Gotta Detect 'Em All: Fake Base Station and Multi-Step Attack Detection in Cellular Networks (Purdue University).
<https://doi.org/10.48550/arXiv.2401.04958>
- [14] Karaçay L, Bilgin Z, Gunduz AB, Çomak P, Tomur E, Ustundag ES, Gulen U, Karakoc F (2021). A Network-Based Positioning Method to Locate False Base Stations (Ericsson).
<https://doi.org/10.1109/ACCESS.2021.3103673>
- [15] Ardestani FS, Saha N, Limam N, Boutaba R (2025). Towards NWDAF-enabled Analytics and Closed-Loop Automation in 5G Networks (University of Waterloo, Waterloo, Ontario, Canada). <https://doi.org/10.48550/arXiv.2505.06789>
- [16] The Hacker News (2024) *Google Adds New Pixel Security Features to Block 2G Exploits and Baseband Attacks*. Available at <https://thehackernews.com/2024/10/android-14-adds-new-security-features.html>
- [17] Bartock M, Cichonski J, Souppaya M, Dey S, Grayeli P, Mulugeta B, Sharma S, Teague C, Scarfone K, Righi S, Ramalingam M, Rhea P, Santharam M, Mosley R, Ungureanu B, Patel J, Wan T, Romness P, Hyatt M, Lebel L, Carroll D, Orrin S, Brown L, Zhou Y, Piggott C, Jones M, Yeh M, Atkinson G, Eustace D, Wenger B, Morgan S, Balmakhtar M, Schumacher G (2022) 5G Cybersecurity. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 1800-33B. Available at <https://www.nccoe.nist.gov/sites/default/files/2022-04/nist-5G-sp1800-33b-preliminary-draft.pdf>
- [18] srsRAN (2025) srsRAN gNB with COTS UEs. Available at <https://docs.srsran.com/projects/project/en/latest/tutorials/source/cotsUE/source/index.html>
- [19] 3rd Generation Partnership Project. Specification # 24.501: Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3. Available at <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3370>



Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

NIST Technical Series Policies

Copyright, Use, and Licensing Statements

NIST Technical Series Publication Identifier Syntax

Author ORCID IDs

Michael Bartock: 0000-0003-0875-4555

Jeffrey Cichonski: 0009-0006-1137-2549

How to Cite this NIST Technical Series Publication:

Bartock M. et al. (2026) False Base Station: Applying 5G Cybersecurity and Privacy Capabilities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 36G ipd. <https://doi.org/10.6028/NIST.CSWP.36G.ipd>

Public Comment Period

September 30, 2026 – October 31, 2026

Submit Comments

5g-security@nist.gov

Or submit the web form at <https://www.nccoe.nist.gov/5g-cybersecurity>

National Institute of Standards and Technology

Attn: Applied Cybersecurity Division, Information Technology Laboratory 100 Bureau Drive (Mail Stop 2000)

Gaithersburg, MD 20899-2000

Additional Information

Additional information about this publication is available at <https://www.nccoe.nist.gov/5g-cybersecurity>, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).