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

5G networks are resilient to attacks from false base stations attempting to impersonate legitimate 5G network base stations, according to actual 5G network validations by the wireless industry's 5G Security Test Bed.

The 5G Security Test Bed is a collaborative effort between the wireless industry, academia, and government agencies to test 5G security features and validate how 5G security standards work in practical, real-world conditions. The Test Bed has completed a series of tests related to false base station (FBS) attacks, showing significant security improvements over 4G.

Validating 5G Device Protections Against Multiple False Base Station Attack Scenarios

The 5G Security Test Bed analyzed several false base station attack scenarios, assessing a 5G test device's response to these scenarios both with and without 5G encryption protocols. When provisioned with 5G encryption protocols, the test device ("user equipment," or UE) recovered from the false base station attacks or avoided them completely in all scenarios, and no identifying information was shared with the false base station.

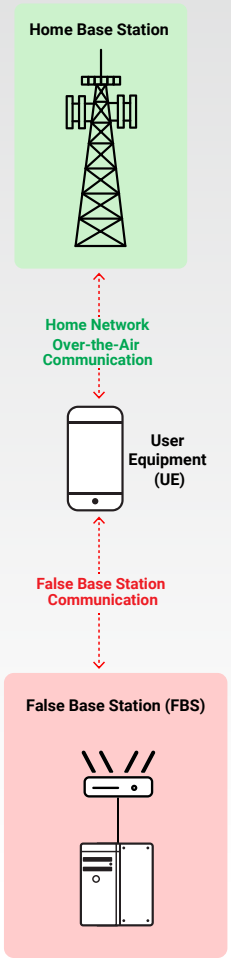
The test cases covered four high-level categories, assessing whether the UE could successfully mitigate against each type of false base station attack:

- **Radio Resource Control (RRC) Connection Scenarios,** which assessed whether the test device would successfully connect to the false base station's RRC—which routes user data and traffic—and if so, whether subsequent authentication procedures would protect the device from fully connecting to the FBS.
- **Authentication Handshake Scenarios,** which assessed whether the false base station could lure the test device to connect in three scenarios: when the false base station omitted the authentication handshake, used fabricated authentication credentials, or replayed old credentials.
- **Denial-of-Service (DoS) Attack Scenarios,** which assessed whether the false base station could bar the test device from connecting to its home network by sending "5GS Services Not Allowed," "Cell Barred," and "PLMN Not Allowed" messages.
- **False Public Warning System (PWS) Message Scenarios,** which assessed whether the test device would connect to the FBS after receiving spoofed Public Warning System messages, sometimes combined with "PLMN Not Allowed" messages.

WHAT IS A FALSE BASE STATION?

A false base station (FBS), also known as a rogue base station or IMSI catcher, is an unauthorized or malicious device that mimics a legitimate wireless network to intercept communications, track users, or disrupt network services.

A false base station exploits vulnerabilities in how mobile devices connect to networks, tricking them into connecting to the FBS instead of the legitimate "home" network. While 4G and older networks were susceptible to these attacks, 5G networks are fortified against them through 5G privacy and encryption protocols that are provisioned to the SIM cards on 5G devices.



5G SECURITY™ TEST BED

HOW DO 5G NETWORKS PROTECT AGAINST FALSE BASE STATION ATTACKS?

5G networks offer enhanced protection through end-to-end encryption—when user devices "talk" to networks, each must verify the other's identity through encrypted handshakes. When user devices provisioned with 5G-encrypted SIM cards encounter a false base station's attempt to connect, they reject the connection.

When a false base station is able to successfully prevent a 5G device from connecting to its home network, the FBS is still unable to decipher any identifying information from the device due to built-in encryption protections, a significant security improvement over legacy wireless networks.

5G Networks Are a Massive Improvement Over 4G, Protecting Private Data Against False Base Station Attacks

In all testing, the 5G device with encrypted identifiers recovered from the attacks or avoided them completely, and it did not reveal any private identifying information in any of the attack scenarios. The test results confirm 5G networks are significantly more resilient against false base station attacks compared to earlier systems, due to their encryption and authentication protocols:

- ✓ **Encrypted 5G Devices Reject Invalid Authentication and Connection Attempts from False Base Stations.**
- ✓ **Encrypted 5G Devices Do Not Share Data During False Base Station Attacks.**
- ✓ **5G Device Protections Work As Intended, Securing Data on Encrypted SIMs.**

5G device identifiers are always encrypted on 5G networks per international standards, except in rare scenarios when the device is in emergency mode, which is meant to connect with unknown networks by design. After false base station attacks, encrypted 5G devices will reconnect to their home networks automatically, reconnect after being reset (either by toggling airplane mode or power cycling the device), or automatically reset and reconnect after a timeout.

Resilience and recovery from false base station attacks can be further improved at the device level by shortening the wait timers in 3GPP standards, which "[give] an opportunity to [devices] to recover and avoid lock-outs," as 3GPP notes in its technical specifications. Additional testing in a future phase using different commercial devices is warranted to understand their behavior with respect these standards and the expected behavior for the DoS attack and false Public Warning System message test cases.