# Mobile power fake base station



---

What is a fake base station?

A malicious or fake base station is a well-known security issue in mobile networking. For example,there are open-source tools and tutorials for setting up fake base stations,e.g.,Refs. [1,2]. The fake base station exploits the radio signal-based base station selection process and the vulnerability in the broadcasting SIB and RRC messages.

What happens if user equipment connects to a fake base station?

Once the benign user equipment connects to the fake base station at the RRC layer, the adversary can launch a protocol downgrade from 5G/4G to 2G (i.e., bidding down) attack ; user equipment device identification attack ; SMS phishing attack [10, 11]; or an attack that drains the user equipment battery [9, 12].

What are false base stations (FBS) and rogue base station (RBS)?

You might have heard of False Base Station (FBS), Rogue Base Station (RBS), International Mobile Subscriber Identifier (IMSI) Catcher or Stingray. All four of these terminologies refer to a tool consisting of hardware and software that allow for passive and active attacks against mobile subscribers over radio access networks (RANs).

What is a false base station attack?

Logical illustration of false base station attacks A false base station is a system built from both hardware and software, which enables the system to mimic legitimate cellular network base stations to carry out passive and active attacks on target mobile subscribers. Figure 3 illustrates the logical process followed by false base station attacks.

This study investigates the vulnerabilities of 5G networks exploited by FBSs, which hijack communications by mimicking legitimate base stations and compromising user equipment (UE).

We deploy FBSDetector as a real-world solution to protect end-users through a mobile app and validate it in real-world environments. Compared to the existing heuristic-based solutions ...

The aim of this study is to mitigate UE attachments against fake base stations through threshold-based detection and localization. The detection results showed low errors in various test ...

# Mobile power fake base station

False base stations execute attacks in the Radio Access Network (RAN) of cellular systems, adversely affecting the network or its users. To address this challenge, we propose a behavior rule specification ...

Fake base stations comprise a critical security issue in mobile networking. A fake base station exploits vulnerabilities in the broadcast message announcing a base station"s presence, ...

You might have heard of False Base Station (FBS), Rogue Base Station (RBS), International Mobile Subscriber Identifier (IMSI) Catcher or Stingray. All four of these terminologies ...

Consequently, mobile network operators and vendors struggle to identify, implement, and deploy a practical solution in the form of detection mechanisms. For the first time, we systematically study fake ...

Mobile networking in 4G and 5G remains vulnerable against fake base stations. A fake base station can inject and manipulate the radio resource control (RRC) communication protocol to ...

Introduce a native 5G network function that can detect false base stations using ML algorithms.

Web: https://mhlengwesecurityservices.co.za