NKOSITHANDILEB SOLAR

How to solve abnormal communication with base station

Overview

What is a false base station?

2.2. Security Threat from a False Base Station A false base station refers to an unauthorized base station capable of launching attacks on User Equipment (UE) or the mobile communication network. These deceptive entities exploit the the common behavior observed in UEs, which is the tendency to connect to stronger wireless signals.

What happens if a base station is faulty?

The faulty base station establishes a radio connection with the user equipment and releases the connection afterward due to the worst channel conditions. Because our reference values come from the worst channel conditions, the optimal thresholds hence ensure fake base station detection with zero false positives under varying network conditions.

Does a fake base station make a connection?

In such attacks, the prerequisite is transmission of the signal at a higher strength than a legitimate base station ; hence, the base station with higher signal strength is always able to lure the user equipment to connect to it. Previous research also specifically studied the threat impacts after a fake base station makes a connection.

Can a fake base station exploit a randomized selection?

The fake base station cannot exploit the randomized selection to make the user equipment connect to it with 100% 100 % probability. An attacker can attempt to launch a threat beyond just availability and disrupting the connectivity, such as attempting to make the victim user equipment connect to a fake server.

How to solve abnormal communication with base station

2.2. Security Threat from a False Base Station A false base station refers to an unauthorized base station capable of launching attacks on User Equipment (UE) or the mobile communication network. These deceptive entities exploit the the common behavior observed in UEs, which is the tendency to connect to stronger wireless signals.

The faulty base station establishes a radio connection with the user equipment and releases the connection afterward due to the worst channel conditions. Because our reference values come from the worst channel conditions, the optimal thresholds hence ensure fake base station detection with zero false positives under varying network conditions.

In such attacks, the prerequisite is transmission of the signal at a higher strength than a legitimate base station ; hence, the base station with higher signal strength is always able to lure the user equipment to connect to it. Previous research also specifically studied the threat impacts after a fake base station makes a connection.

The fake base station cannot exploit the randomized selection to make the user equipment connect to it with 100% 100 % probability. An attacker can attempt to launch a threat beyond just availability and disrupting the connectivity, such as attempting to make the victim user equipment connect to a fake server.

These base stations exploit vulnerabilities in network protocols and often go undetected by traditional security measures. As such, the presence of rogue base stations ...

A fake base station is a well-known security issue in mobile networking. The fake base station exploits the vulnerability in the broadcasting message announcing the base ...

Why Do 5G Networks Still Experience Service Disruptions? While global communication base station deployments have surged by 38% since 2021, service interruptions still cost operators ...

To fully obtain power multiplexing gain and improve spectral efficiency, this paper investigates nonorthogonal multiple access (NOMA)-based WPT-charging UAV ...

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 ...

Air-to-ground (A2G) networks enable air-to-ground communications. An example of this is communication between an aircraft and a ground station. In an A2G network with ...

The advancement of cellular communication technology has profoundly transformed human life. People can now watch high-definition ...

The integrated sensing and communication base station can perform both communication and sensing tasks simultaneously. The key premise of accurate loc...

The advancement of cellular communication technology has profoundly transformed human life. People can now watch high-definition videos anytime, anywhere, and ...

Solving Signal Degradation at Base Stations Signal degradation at base stations can be addressed through various methods, including: Antenna Placement: Ensuring proper ...

Air-to-ground (A2G) networks enable air-to-ground communications. An example of this is communication between an ...

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 ...

Learn how to resolve multiple base station signal conflicts with BelFone's expert tips. Improve radio network performance and ensure clear, reliable communication.

Contact Us

For catalog requests, pricing, or partnerships, please contact:

NKOSITHANDILEB SOLAR

Phone: +27-11-934-5771

Email: info@nkosithandileb.co.za

Website: https://www.nkosithandileb.co.za

Scan QR code to visit our website: