Devilray: Reconfigurable, Evasive and Reference-Grade LTE Fake Base Station*

Taekkyung Oh[1], Duckwoo Kim[1], Beomseok Oh[1], Mincheol Kim[1], Kwangmin Kim[1], Sangmin Woo[1], Jaehoon Kim[1], CheolJun Park[2], and Yongdae Kim[1]

[1] KAIST, Daejeon, South Korea
{ohtk, 0731kdw, beomseoko, mcson, kwangmin.kim, wsm723, takeliberty, yongdaek}@kaist.ac.kr
[2] KyungHee University, Seoul, South Korea
cheoljunp@khu.ac.kr

1 Introduction

Fake Base Stations (FBS) pose significant threats to cellular security through IMSI-catching, location tracking, denial-of-service attacks, and 2G downgrades. Despite over a decade of research, FBS detection effectiveness remains difficult to assess due to restricted access to real-world FBS devices and the lack of uniform reference models. Existing self-built prototypes reflect narrow design choices, omit evasiveness as a design goal, and provide no consistent baseline for reproducible evaluation. This has led to fragmented research that often evaluates detection against weak adversaries making little effort to avoid exposure, yielding potentially optimistic assessments.

We present Devilray, a reconfigurable, evasive, and reference-grade LTE FBS model that addresses these critical gaps. Our key contributions are: (1) a unified four-phase operational model consolidating FBS behavior from diverse sources including commercial device analysis, (2) systematic classification of detection primitives and derivation of comprehensive evasion techniques (E1-E6), (3) a reconfigurable platform enabling flexible composition of adversarial strategies, and (4) extensive evaluation demonstrating consistent evasion against all tested detection systems while reproducing representative attack scenarios.

2 Four-Phase FBS Modeling

This work is the first to define and model a general, unified operational framework for FBS. By consolidating knowledge from academic literature, vendor manuals, technical reports, and analysis of a commercial LTE FBS device, we systematize FBS operations into four distinct phases:

Network Scanning: The FBS surveys the cellular environment to identify operating cells and collects broadcast information including MIB, SIB, and paging messages. Devilray extracts fine-grained network configurations and operational behaviors to maximize attack effectiveness.

Cell Launching: The FBS configures forged cell parameters and broadcasts signals to emulate legitimate base stations. Devilray provides multiple configuration options including full-mimic mode (replicating all legitimate parameters) and UE-recovery mode (strategic TAC modification), supporting both fixed and round-robin cell iteration across multiple frequency bands.

Connection Hijacking: The FBS actively redirects UE connections to itself. Devilray implements three mechanisms: (1) jamming (>20dB power, any UE state), (2) handover (>3dB, connected UEs via neighbor PCI reuse), and (3) cell reselection (>5dB, idle UEs via priority band exploitation).

*Proceedings of the 9th International Conference on Mobile Internet Security (MobiSec'25), Article No. P-71, December 16-18, 2025, Sapporo, Japan.

Application: The FBS exploits hijacked connections for actual attacks, including IMSI-catching, victim location tracking, 2G redirection with SMS injection, and denial-of-service attacks.

3 Design and Implementation

To design evasive FBS, we analyzed 22 existing FBS detection systems to identify their underlying detection primitives across different layers. Based on this systematization, Devilray integrates six evasion techniques targeting these primitives: E1 mimics legitimate cells by replicating broadcast parameters and paging patterns; E2 randomizes TA (Timing Advance) values (0-30 range) to counter concentrated low-TA signatures; E3 uses low-power hijacking (3-5dB) via cell reselection and handover to reduce signal and failure anomalies; E4 provides reject-based, adaptive (10-20% exposure), and targeted IMSI-catching to evade statistical detection; E5 eliminates NAS Reject patterns that could be used as a FBS signature, by using RRC Connection Release; E6 conceal physical-layer FBS signatures by utilizing GPSDO synchronization and RF tuning.

Additionaly, Devilray achieves reconfigurable architecture which enables flexible composition of these evasion techniques across all four operational phases, which is described in 1.

Devilray is implemented with 8K LoC extending srsRAN (LTE) and OpenBTS (2G), supporting USRP B210/X310 hardware. YAML-based profiles enable reproducible adversarial instantiation.

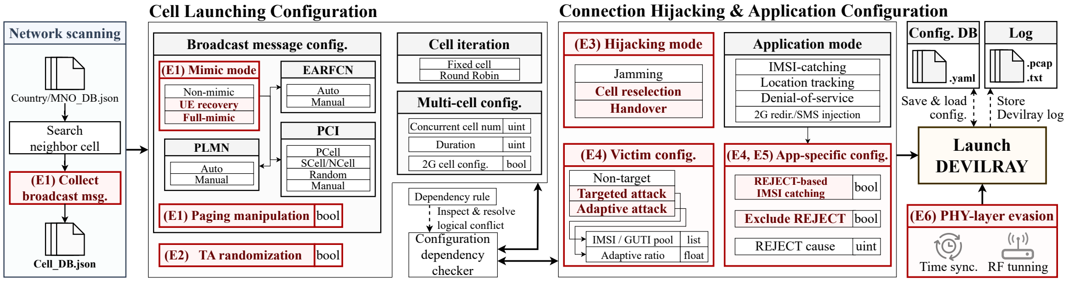

Figure 1: Reconfigurable architecture of Devilray with evasion techniques

4 Evaluation

We evaluate Devilray across six commercial UEs – Galaxy S10e, S20, S23, iPhone XS, 12 and 13 Pro – in shielded laboratories.

Functional Evaluation. First, we operate Devilray to attack victims, to confirm 3 connection hijacking methodologies and 4 applications impelemented in Devilray works well. For connection hijacking methodology, it is confirmed that jamming requires 20dB minimum, while cell reselection and handover succeed with 3-5dB advantages. Also, application-phase attacks successfully demonstrated IMSI-catching, location tracking, 2G redirection with SMS injection, and DoS attacks disabling network access for up to 30 minutes.

Evasiveness Evaluation. We evaluate Devilray against six publicly accessible detection systems (CellGuard, Crocodile Hunter, EAGLE Security, Rayhunter, PHOENIX, FBSDetector) and compared with one commercial FBS device. We derived eleven Devilray instances by combining different evasion techniques (hijacking mechanisms, catching modes, cell mimicry). Results show complete evasion when appropriately configured: low-power hijacking bypassed signal-based detectors (Crocodile Hunter, EAGLE Security); reject-based catching evaded protocol monitors (Rayhunter); unseen patterns defeated signature systems (PHOENIX); and FBSDetector's ML accuracy dropped to 0-50% versus reported >90%. The commercial C-FBS evaded only three systems, demonstrating Devilray's superior performnace of evasiveness and reconfigurability.