Network-based Detection of Mobile Fake Base Stations

HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Sanish Gurung, Tuomo Lehtilä,
Amy Sokhna Sidibé, Gizem Akman, Valtteri Niemi

[1] University of Helsinki [2] University of Turku
[1] sanish.gurung@helsinki.fi
[2] tualeh@utu.fi, [1] amy.sidibe@helsinki.fi, [1] gizem.akman@helsinki.fi, [1] valtteri.niemi@helsinki.fi

Problem Statement

Definitions:

- Fake base station (FBS), also known as IMSI-catcher, is specialized device that emulates legitimate base station (BS), but emits higher-powered signal to lure User Equipment (UE).
- This device can identify nearby UE either passively, by monitoring unencrypted signals, or actively, by presenting itself as a legitimate network to engage UE in signaling exchanges that reveal sensitive information (e.g., permanent identity IMSI).

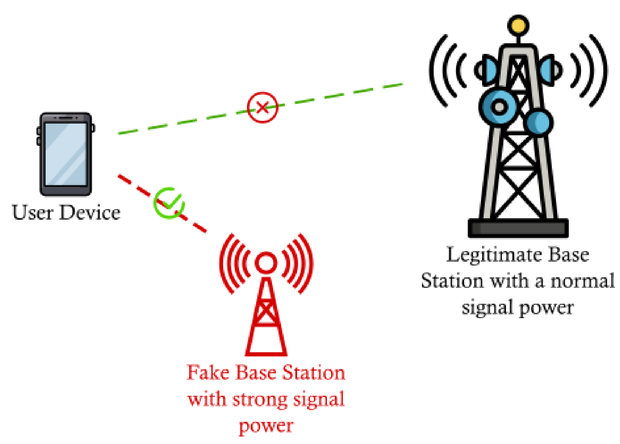

Figure 1 – Visualization of a fake base station in a network

FBS facilitates various forms of passive and active attacks:

- **Location Tracking.**
- **Eavesdropping.**
- **Man-in-the-Middle (MITM).**
- **Denial of Service (DoS).**

Data Collection & Processing

Training and ***Validation Datasets*** consist of measurement reports[a] (MRs) obtained during the **absence** of the FBS. We aggregated the MR data in 2s intervals and computed the mean of nonzero $RSRP_i$ values[b] for each time interval and each BS_i. This resulted in 250 intervals for training and validation.

Testing Dataset contains measurement reports collected in the **presence** of the FBS. The transmission power of the FBS is 6 dBm more than that of the legitimate BS.

- For FBS to masquerade as BS_i, we replaced $RSRP_i$ with max($RSRP_i$, $RSRP_{10}$).
- We aggregated the MR data in 2 s intervals and computed the mean of nonzero $RSRP_i$ for 100 intervals.

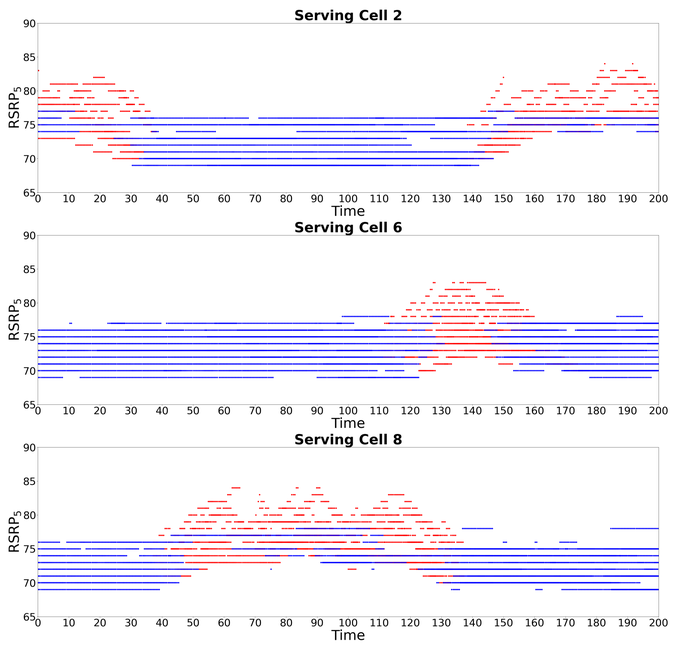

Figure 2 – FBS masquerading as BS_5 derived from MRs received by BS 2, 6, and 8

Notes

[a] **Measurement Report (MR)** is a message sent by an UE to its serving BS, containing signal measurements of neighboring cells to support mobility and handover decisions.

[b] **Reference Signal Received Power (RSRP)** is the average received power of single reference signal from a BS

Experimental Setup in Simulator (ns-3)

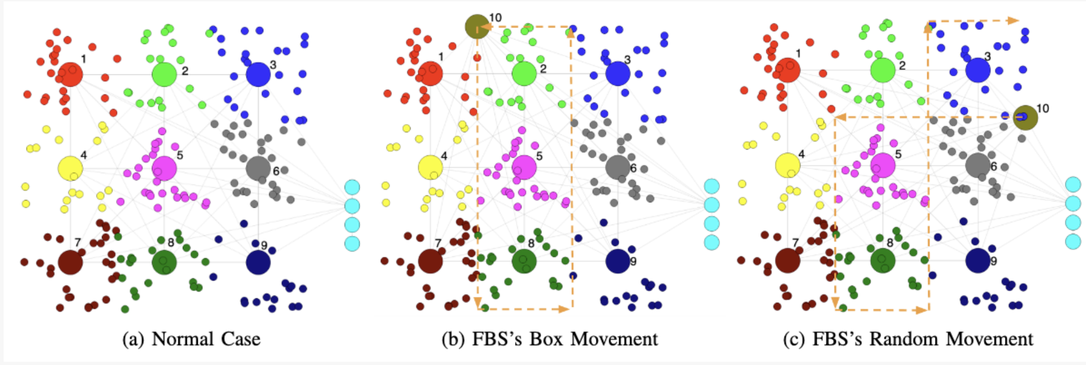

Figure 3 – Three Scenarios of Simulation Topology

- $1500m \times 1500m$ grid with 9 stationary legitimate base stations and one (or zero) FBS moving with a speed of 20 m/s; 200 UEs each moving with 2 m/s.
- Normal Case: Without FBS
- Box Movement: FBS (BS_{10}) moving along rectangular path
- Random Movement: FBS moving along random trajectory

Methodology

Z-score measures how far an RSRP value deviates from its expected mean, normalized by standard deviation. It helps identify unusual signal strength across different cells consistently.

$$z = \frac{x - \mu}{\sigma} \tag{1}$$

Anomaly Score (AS) is the sum of squared z-scores over 30 s (15 intervals). Squaring emphasizes large deviations, and summing smooths out noise, detecting sustained anomalies.

$$AS(j,k,t) = \sum_{i=k-14}^{k} \left(z(RSRP_j^i(SC_t))\right)^2 \tag{2}$$

Global Anomaly Score Threshold (GAST) is a threshold based on training data (max and mean anomaly scores). It sets a high bar to avoid false alarms but still detects real anomalies caused by FBS.

$$GAST = \frac{3}{2} \cdot \max_{j,k,t}(AS(j,k,t)) + \frac{1}{2}\mu_{j,k,t}(AS(j,k,t)) \tag{3}$$

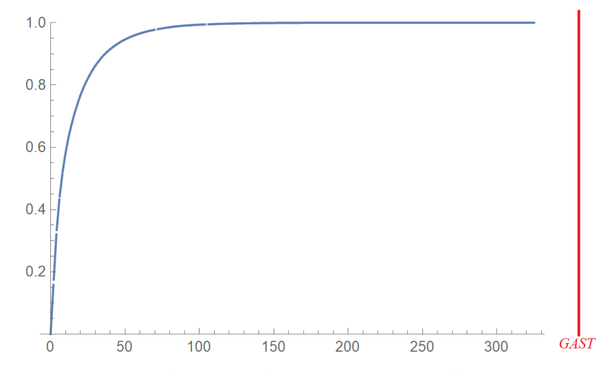

Figure 4 – Cumulative distribution of anomaly scores over all of the training sets. The x-axis presents the anomaly score. In this case $GAST = 356$.

Results

Table 1 – The number of times a **serving cell** BS_i (**SCi**) **does not raise alarm** when a fake base station (FBS) masquerades as BS_j (**Fj**), shown over 25 simulations using box movement (**left**) and 24 simulations using random movement (**right**).

	F1	F2	F3	F4	F5	F6	F7	F8	F9
SC1	25	10	0	11	0	0	0	0	0
SC2	0	25	0	0	0	0	0	0	0
SC3	0	3	25	0	0	0	0	0	0
SC4	2	0	0	25	9	0	2	0	0
SC5	0	0	0	0	25	0	0	0	0
SC6	0	0	6	0	12	25	0	0	8
SC7	0	0	0	3	0	0	25	19	0
SC8	0	0	0	0	0	0	0	25	0
SC9	0	0	0	0	0	3	0	0	25

	F1	F2	F3	F4	F5	F6	F7	F8	F9
SC1	24	24	1	24	1	1	1	1	5
SC2	0	24	0	0	1	0	0	0	0
SC3	0	0	24	0	0	0	0	0	0
SC4	1	0	0	24	8	0	2	0	0
SC5	0	0	0	0	24	0	0	0	0
SC6	0	0	3	0	11	24	0	0	0
SC7	0	0	0	4	0	0	24	20	0
SC8	0	0	0	0	0	0	0	23	0
SC9	0	0	0	0	0	3	0	2	24

NOTE: 0 means the serving BS_i always detected the FBS masquerading as BS_j.