HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI

Detecting False Base Stations in 4G/LTE using Machine Learning

An ns-3 simulation of false cells detection using RSRP-based features in measurement reports

Sanish Gurung, Amy Sokhna Sidibé, Mohamed Taoufiq Damir, Tuomo Lehtilä, Valtteri Niemi

(sanish.gurung, amy.sidibe, mohamed.damir, tuomo.lehtila, valtteri.niemi)@helsinki.fi

1. Problem Statement

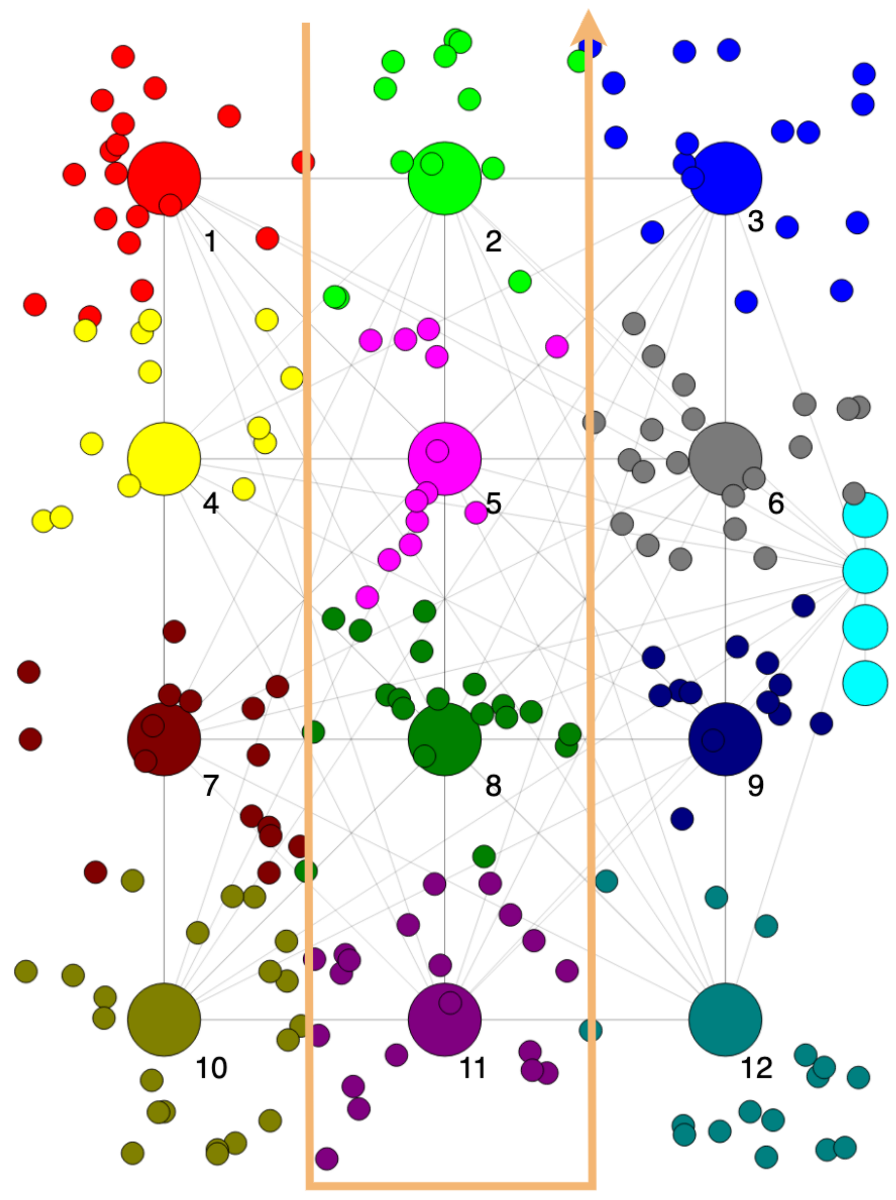
False Base Stations (FBS) also known as IMSI-Catchers are persistent threats in mobile networks starting from 2G to 5G Non-Standalone (NSA).

They can impersonate legitimate base stations deceiving users to connect to them.

FBSs present serious security risks including MiTM, Downgrade, DoS attacks; and privacy issues such as eavesdropping, location tracking, etc.

Many 4G/LTE networks remained vulnerable to this attack due to security issues in 3GPP specifications.

2. Hypothesis



- We assume the FBS impersonates a legitimate base station using its Physical Cell Identifier (PCI).

- The FBS broadcasts higher power signals to make User Equipments (UEs) select it as a best cell.

- UEs periodically send Measurement Reports (MRs) to their serving cell.

- MRs contain critical features such as RSRP/RSRQ to detect anomalies in the surrounding radio conditions.

- We apply machine learning to collected MRs for FBS detection using RSRP features.

3. Methods

- We use ns-3 to simulate 12 eNBs with three scenarios: training, testing and validation data [1].

- **Training data**: 12 serving cells with 200 UEs connected to each cell; UEs are moving at random walk. Data collection during 1000 seconds.

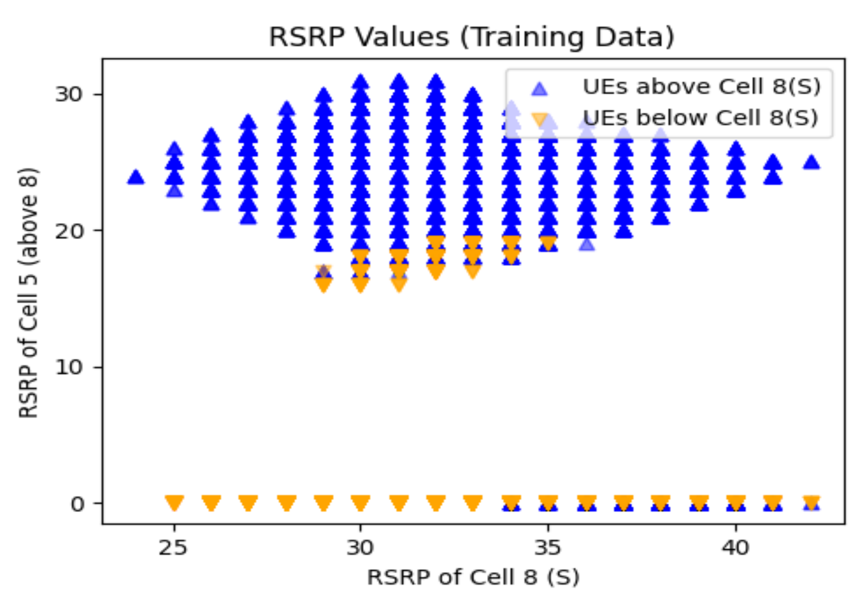
- **Testing data**: 11 normal serving cells with 100 UEs connected. 1 moving cell acting as a FBS following the orange trajectory in the topology. 12 rounds of data collection.

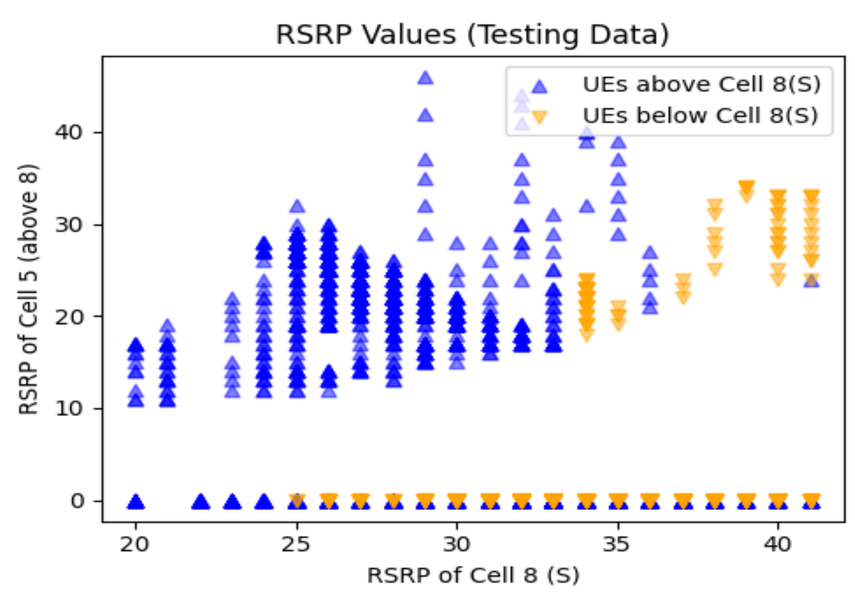
- **Validation data**: 12 serving cells with 100 UEs connected.

- ML model applied: **Autoencoder.**

Serving Cell ID	Neighbours in training	Anomalies (static)
1	2,3,4,5,7	4589 (1347)
2	1,3,4,5,6,	7116 (2867)
3	1,2,5,6,9	4034 (1110)
4	1,2,5,7,8,10	7551 (2162)
5	1,2,3,4,6,7,8,9	11302 (1074)
6	2,3,5,8,9,12	10885 (2285)
7	1,4,5,8,10,11	8301 (1650)
8	4,5,6,7,9,10,11,12	8953 (1518)
9	3,5,6,8,11,12	8133 (1076)
10	4,7,8,11,12	4286 (2432)
11	7,8,9,10,12	7996 (2121)
12	6,8,9,10,11	4618 (929)

4. Results





Serving Cell ID	Autoencoder
1	53% (65%)
2	51% (35%)
3	61% (78%)
4	75% (86%)
5	78% (83%)
6	81% (44%)
7	87% (89%)
8	86% (88%)
9	73% (62%)
10	45% (75%)
11	16% (12%)
12	22% (70%)

5. Future Work

- Extension of our solution to multiple Radio Access Technologies.

- Implementation of an Anomaly Detection Forest (ADF) for comparison.

- Include a real-time detection mechanism with the fine tuned models.

- Other features in measurement reports to be included in the data processing.

- Simulation with handover scenarios.

References

[1] Nakarmi, P. K., Sternby, J., & Ullah, I. (2022, August). Applying Machine Learning on RSRP-based Features for False Base Station Detection. In Proceedings of the 17th International Conference on Availability, Reliability and Security (pp. 1-7).