FALSE BASE STATIONS DETECTION WITH MACHINE LEARNING

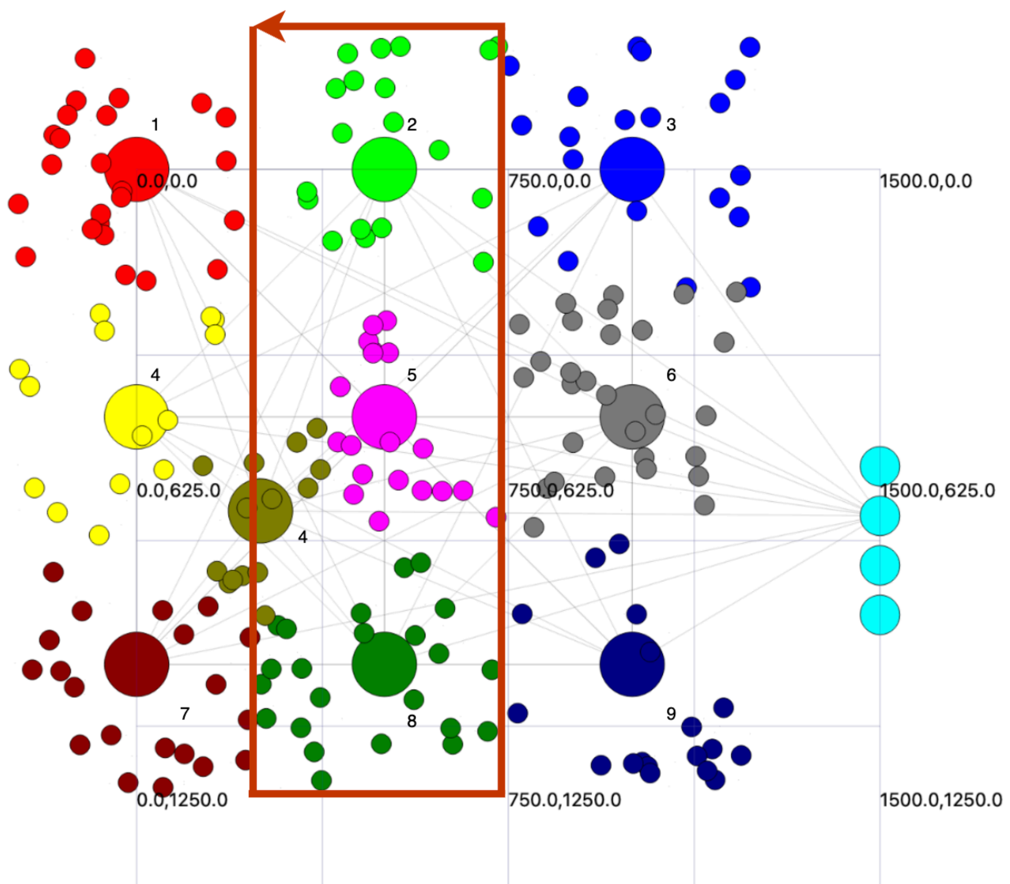
Sanish Gurung
Amy Sokhna Sidibé
Mohamed Taoufiq Damir
Tuomo Lehtilä
Valtteri Niemi
firstname.lastname@helsinki.fi,
Department of Computer Science,
University of Helsinki

PROBLEM

- False Base Stations (FBS) 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 [1].
- Novel research are exploring the application of Machine Learning in Access Networks to detect FBS attacks [2].

SCENARIOS

- **Case 1:** Attacker impersonates one legitimate Physical Cell Identifier (PCI).
- **Case 2:** The attacker is aware of the base station locations and their associated PCIs. The attacker switches between suitable PCIs to evade detection.
- In both cases, if the UE measures two signals belonging to the same PCI, it reports the stronger of the two.



ns-3 Network Topology

METHODS

- We run ns-3 simulator to simulate 9 legitimate eNBs for the training phase and 1 additional FBS for the testing phase.
- **Training data:** 9 serving cells with a total of 200 UEs (User Equipment) connected. UEs move according to a random walk pattern, with data collection over 1000 seconds.
- **Testing data:** 9 normal serving cells with a total of 200 UEs connected. One additional moving cell acts as a FBS. Data collection is performed over 9 rounds (1 for each legitimate PCI) for 225 seconds each round.
- Each data point corresponds to a **measurement report**.
- If there are two measurements for the same PCI, RSRP value with highest value is chosen.
- If the highest value does not actually belong to a legitimate base station, then this data point is flagged as showing an attack (Ground truth).
- These flags are used to calculate the recall percentage, but are never used in the ML algorithm.
- **ML Algorithms:**
  - Gaussian Mixture Model (GMM)
  - K-Nearest Neighbors (KNN)
  - Anomaly Detection Forest (ADF)[3]
- **Metrics:**
  - Recall
    $$\frac{TP}{TP+FN}$$
    The portion of attacks correctly identified as anomaly.
  - Precision
    $$\frac{TP}{TP+FP}$$
    The portion of detected anomalies that correspond to an attack.

Notes:

True Positive (TP)
False Positive (FP)
False Negative (FN)

RESULTS

- **Case 1:**

  Recall for each ML model

Serving Cell	GMM	KNN	ADF
1	70%	73%	38%
2	73%	72%	55%
3	29%	60%	35%
4	69%	52%	41%
5	66%	72%	57%
6	64%	63%	23%
7	67%	67%	30%
8	53%	66%	40%
9	81%	66%	62%

Precision for each ML model

Serving Cell	GMM	KNN	ADF
1	84%	69%	25%
2	84%	73%	50%
3	73%	52%	23%
4	63%	46%	23%
5	60%	60%	40%
6	53%	43%	24%
7	61%	59%	21%
8	63%	57%	32%
9	73%	52%	23%

- **Case 2: Work in Progress**

REFERENCES

[1] 3GPP. *Study on 5G security enhancements against False Base Stations (FBS)*. Technical Specification (TS). 33.809. 2023.

[2] Prajwol Kumar Nakarmi, Jakob Sternby, and Ikram Ullah. "Applying Machine Learning on RSRP-based Features for False Base Station Detection". In: *Proceedings of the 17th International Conference on Availability, Reliability and Security* (2022). URL: https://api.semanticscholar.org/CorpusID:251018706.

[3] Jakob Sternby, Erik Thormarker, and Michael Liljenstam. "Anomaly Detection Forest". In: *ECAI 2020 - 24th European Conference on Artificial Intelligence, 29 August-8 September 2020, Santiago de Compostela, Spain, August 29 - September 8, 2020 - Including 10th Conference on Prestigious Applications of Artificial Intelligence (PAIS 2020)*. Ed. by Giuseppe De Giacomo et al. Vol. 325. Frontiers in Artificial Intelligence and Applications. IOS Press, 2020, pp. 1507–1514. DOI: 10.3233/FAIA200258. URL: https://doi.org/10.3233/FAIA200258.