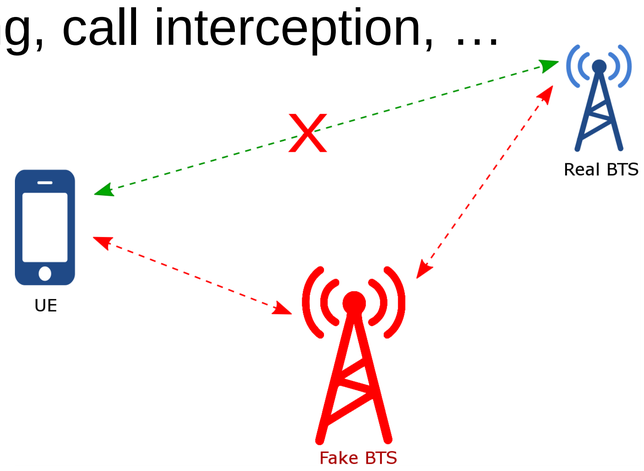
Cloud-Assisted Security Services
Secure Systems Group, Aalto University

Setareh Roshan, Yoan Miche, N. Asokan

Estimating and Predicting Path Loss for Fake Base Station Detection

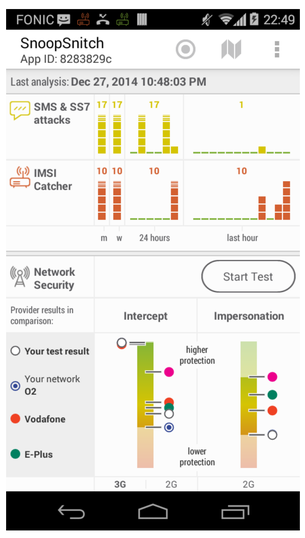
Problem Statement

- Many recent attacks reported using fake base stations
- Mutual authentication not enough [1]
- To spread malware [2]
- To spy on politicians [3]
- IMSI catching, call interception, …



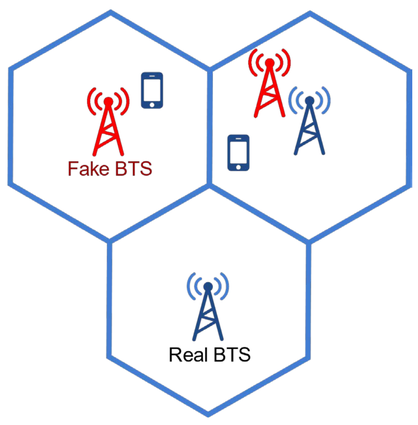
Current Detection Applications

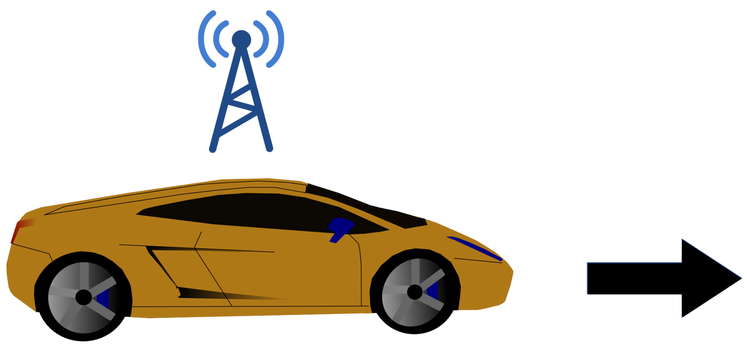
- Snoopsnitch, AIMSIC, Darshak
- Detect anomalies based on LAC/CID, encryption, …
- Reactive, not preventive
- Device already connected to fake BTS when detecting
- Too late to avoid some information leakage



Limitations

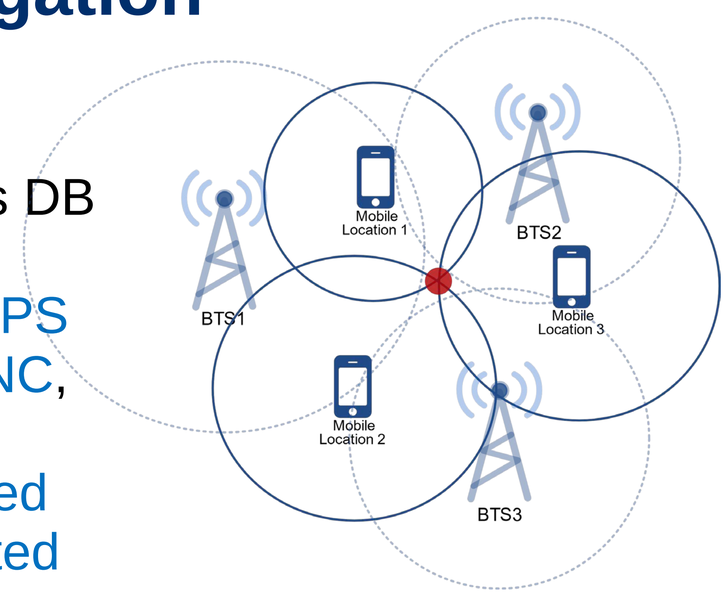
- Impersonation
  - Close and similar to real BTS
- No Real time detection for moving devices
  - Vehicles
  - IoT devices, robots





Proposed Mitigation

1. Estimate BTS Location.
2. Access operator's DB to get LAC/CID, emitting power, GPS location, MCC/MNC, 2G/3G/4G, etc.
3. Compare estimated location and emitted power with real ones in DB.
4. Is the device receiving the correct power from BTS, considering distance/terrain?

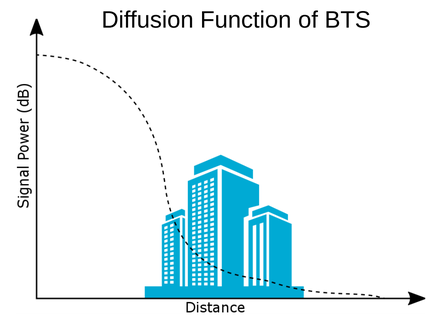


Path Loss Prediction

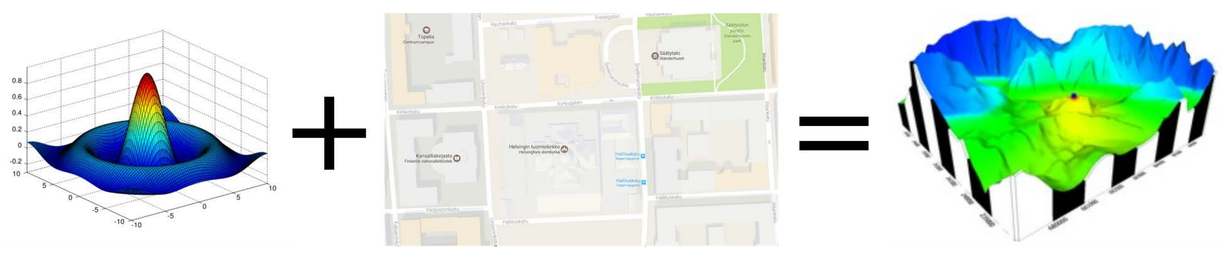
- Okumura-HATA, COST [4].
  - Formulate path loss based on environment type, antenna type, distance.
  - Not accurate
- Ray tracing [5]: Accurate but not efficient.

Using Machine Learning

- Approximate diffusion function of BTS



- Incorporate map of surroundings into model



References

[1] Shaik, Altaf, et al. "Practical attacks against privacy and availability in 4G/LTE mobile communication systems." *arXiv preprint arXiv:1510.07563* (2015).
[2] https://www.theregister.co.uk/2017/03/23/fake_base_stations_spreading_malware_in_china
[3] https://www.thelocal.no/20150624/pst-deny-fake-base-stations
[4] Hata, Masaharu. "Empirical formula for propagation loss in land mobile radio services." *IEEE transactions on Vehicular Technology* 29.3 (1980): 317-325.
[5] Liang, George, and Henry L. Bertoni. "A new approach to 3-D ray tracing for propagation prediction in cities." *IEEE Transactions on Antennas and Propagation* 46.6 (1998): 853-863.

Aalto University

NOKIA