Machine Learning for 5G Self Organized Network

Altaf Shaik
Security in Telecommunications
PhD student at Technische Universität Berlin (TUB)
Telekom Innovation Labs

What is a Self Organized Network

- Automatic network planning, configuring, and controlling
- Low CAPEX and OPEX – pressure to reduce them
- Optimal QoS, coverage and capacity : dynamic, run-time
- SON functions into 3GPP standards in LTE Rel. 8 and >>>> 9, 10 , 11 – offers interoperability among vendors (2008).. 10 years already
- 5G SON : low-latency, end-to-end intelligent, complex network deployments
- ‘N’ Vendors = ‘N’ solutions

SON functions set

- ANR – Automatic Neighbor Relation
  - Adding newly deployed and discovered base stations into the network
- PCI optimization – solving PCI conflicts
  - Cells with same cell ID generate interference. Base stations restart
- MRO optimization – Mobility Robustness Optimization
  - Handover settings are controlled to alter coverage
- Energy Savings
  - Sleep mode features to base station when zero load

Did SON succeed.?

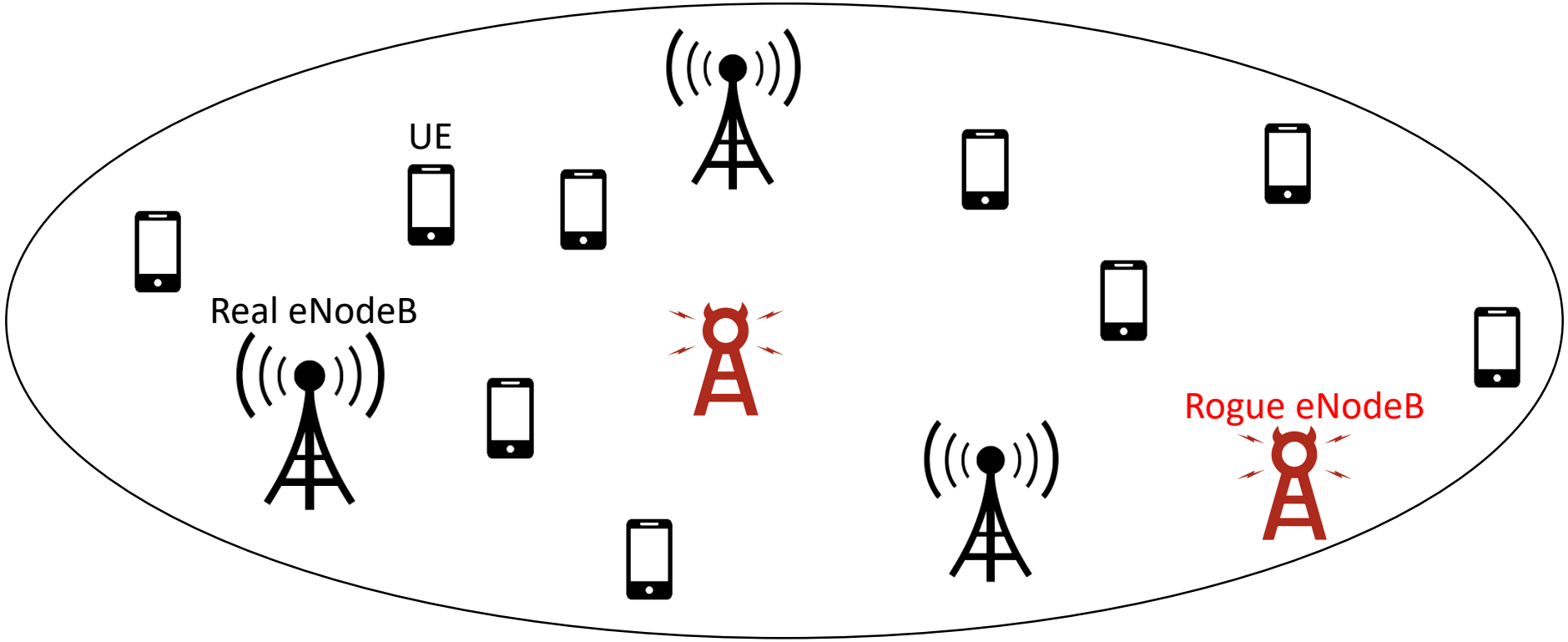
- Partly..! 30%
- SON is an optional element
- Operators are using ANR function – (automatically detecting new cells and adding them into the network)
- Other functions like PCI optimization, MRO are not activated or used
  - Operators are not ready to transform a manual network into a SON

Reasons for partial success of SON

- SON algorithms are not bullet-proof
- Design weaknesses
  - It is a control system that monitors system health with instantaneous KPI's
  - A network action (optimization) is based on simple analysis of parameters
  - Decision making approach is not efficient
  - SON takes direct control over network configurations
  - Trusting LTE air-interface protocol information
  - Lack of reliable and robust algorithms – security problems (research at TUB)

SON data from vulnerable locations

SON data ⇔ information from phones & base stations



Operating a 

- Impersonates real eNodeBs (same broadcast settings)
- Creates fake measurement information
- Causes Handover Failures
- Generates rogue data in the network and DoS to subscribers and operators

The content inside these reports is not verified..!

UE and Network cannot distinguish between real and rogue data

Intelligent 5G SON ← accurate data

*** Research Gap ***

Research status

- Reported to GSMA (in progress)
- Tested with two other operators (SON experts) acknowledged

Solution - ML

- Changing LTE standards
  - Not to connect to rogue base stations
  - Public key based authentication
  - Complex
  - Compatibility issues, power issues, efficiency problems
- Adding intelligence to SON
  - Machine learning
  - Easy to implement

ML for SON

- Data verification inside the network
  - learn by co-relating existing network data with newly acquired data
  - SON learns the locations where handovers successfully occurred by acquiring signal strength with angle of arrival
  - Control handovers based on successful data

- Detect faulty data
  - identify patterns across collected data for certain period of time
  - Training the SON engine with huge sets of network data
  - Detect if the fault is real or fake
  - **Lack of real data (most important for research)

5G SELFNET

- H2020 project
- Support for SDN/NFV enabled 5G networks
- Advanced network management framework for fully automatic and intelligent 5G network
- Decreased OPEX, improved QoS, security
- Self-healing, self-protection, self-optimization
- Self-protection : protection from signaling DoS attacks
- Still vulnerable to rogue base station attacks, accepts rogue data