LTE Network Automation under Threat

Altaf Shaik

(Technische Universität Berlin & Kaitiaki Labs)

Ravishankar Borgaonkar

(SINTEF Digital & Kaitiaki Labs)

KAITIAKI

Blackhat USA 2018, Las Vegas

We Do…

- Mobile network and devices security

- Telecommunication protocol and device analysis

- Attacks and defenses

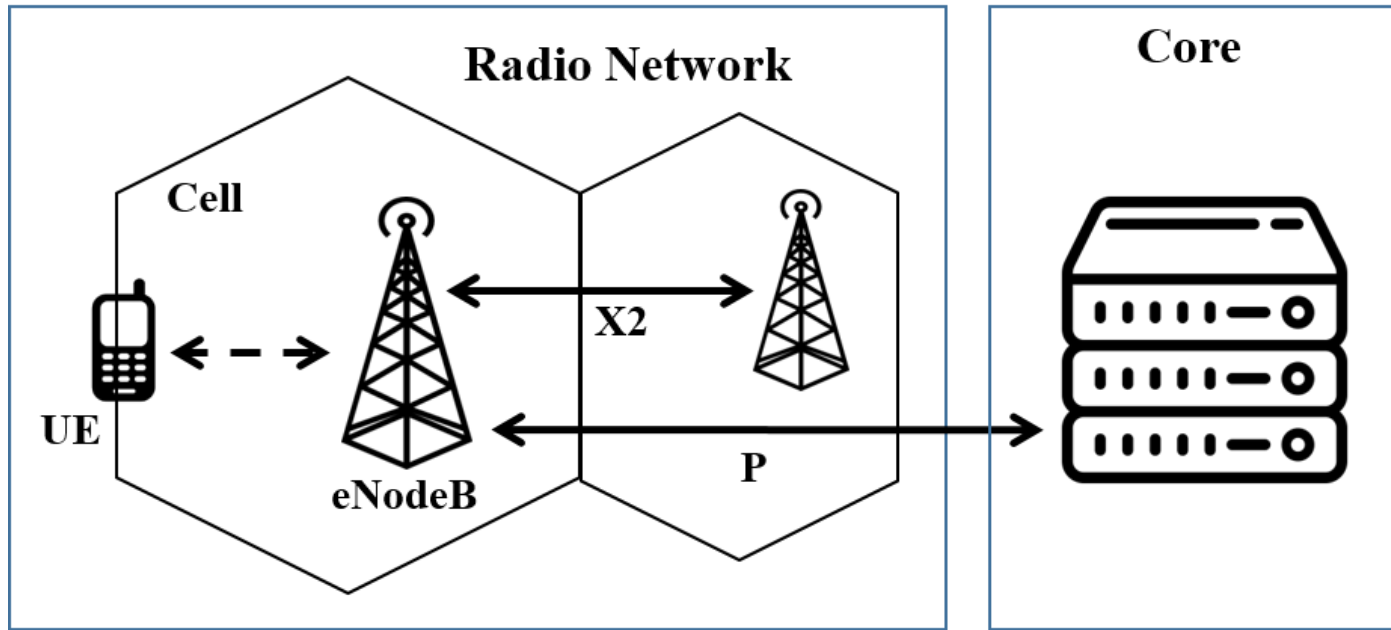- Secure network building

KAITIAKI

Overview

- 4G/LTE & SON operations

- Vulnerabilities and exploitation

- Setup and DoS attacks

- Impact and status
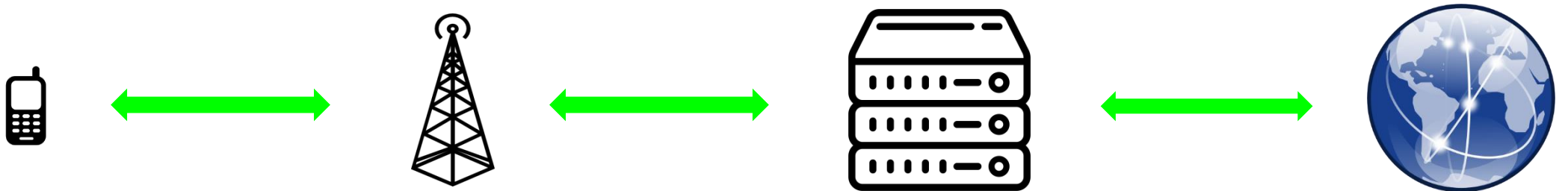
- Mitigations

- Takeaways

Mobile Network Architecture

- UE: User Equipment
- eNodeB: Evolved NodeB
- X2: New interface connecting eNodeBs
- P: Propreitary

Recap - Telco Attacks

- IMSI Catchers
- DoS (Radio channels & HLR)
- Interception (Passive)

- Man-in-the-middle
- SS7
  - Locate, Track, Manipulate

Our Focus – Network Automation

- Favorite Target we know   ->

- What about attacking base stations ->
  - Is it possible?
  - Remotely, without detection?

- Base stations can operate automatically (self operated)
  - **Self Organized Network (SON)**

Self Organized Network (SON)

- New X2 interface in LTE

- Plug & play network elements - Low CAPEX and OPEX

- Base stations - Automatic configure and control

- 3GPP standardized from LTE Rel. 8 (32.500)

- 5G SON : low-latency, end-to-end intelligent, complex networks

X2
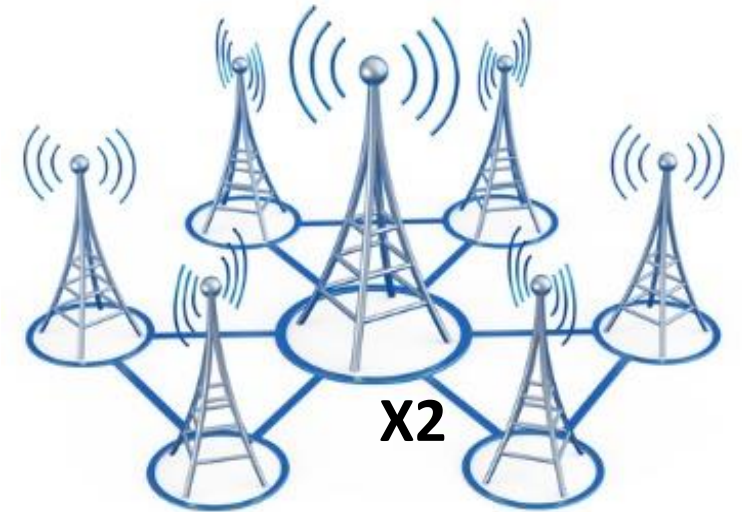
SON

- Software package installed on eNodeB or OAM

- Mix of standards and implementations

- Vendor implementations (UltraSON, Elastic-SON, NGSON, AirSON)

- 90% Operators support SON

    - No reported attacks till now..!

Background

SON Operation in Practice

Self-Configuration
Self-Optimization
Self-Healing

Control System
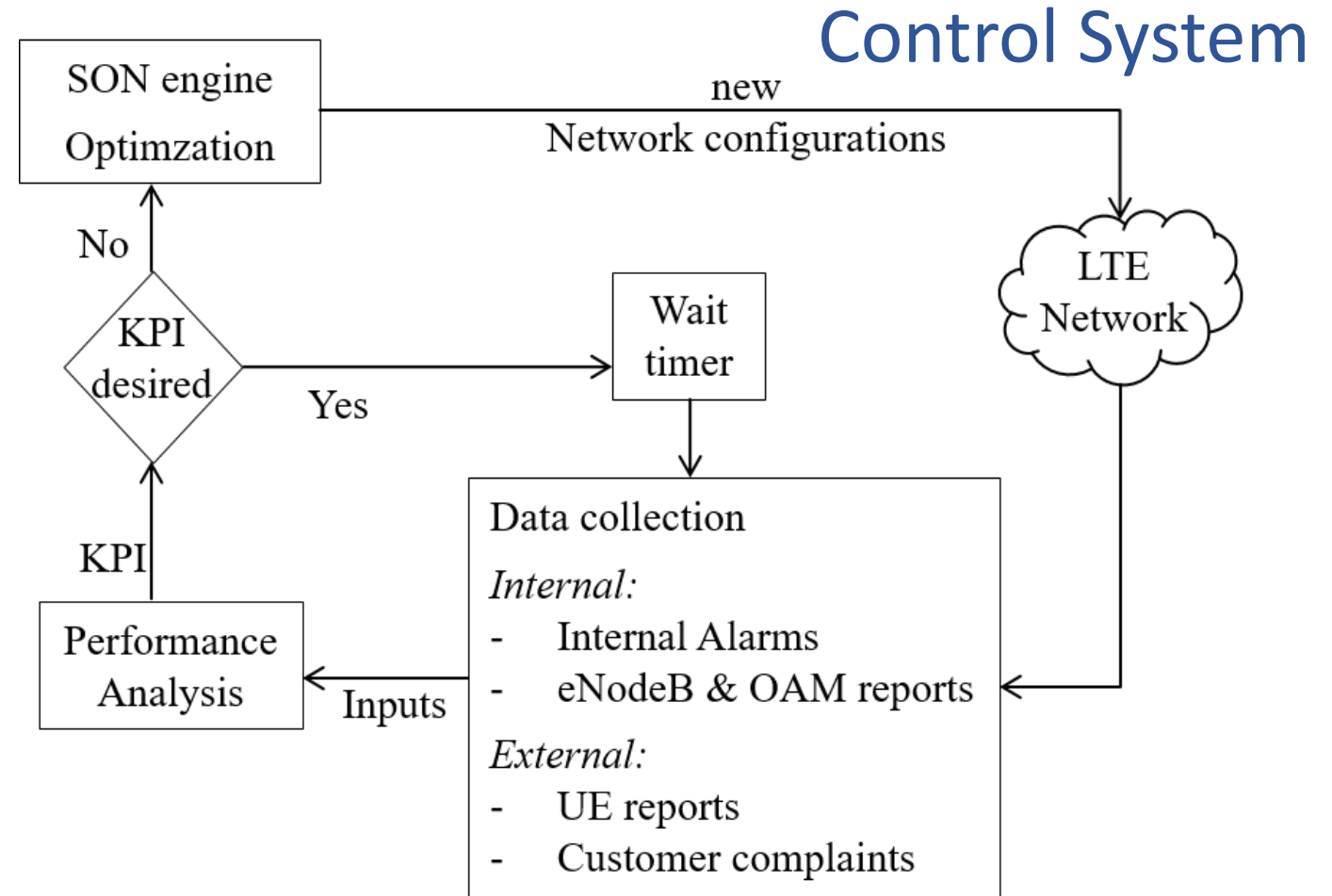
SON Technical Features

- ANR – Automatic Neighbor Relation
  - Discover & add new base stations into the network

- PCI Optimization
  - Solve adjacent cell ID conflicts

- MRO – Mobility Robustness Optimization
  - Control handover settings to adjust coverage

SON Operation Modes

- Off
  - Collect data, no parameter-change

- Manual apply
  - Parameter-change with operator confirmation

- Automatic apply
  - Automatic parameter change, autonomous operation

SON Design Issue

Design Flaw

information from phones & base stations

Trusted and Unverified

SON logic and intelligence

Key Question

LTE network

UE

Real eNodeB

Rogue eNodeB
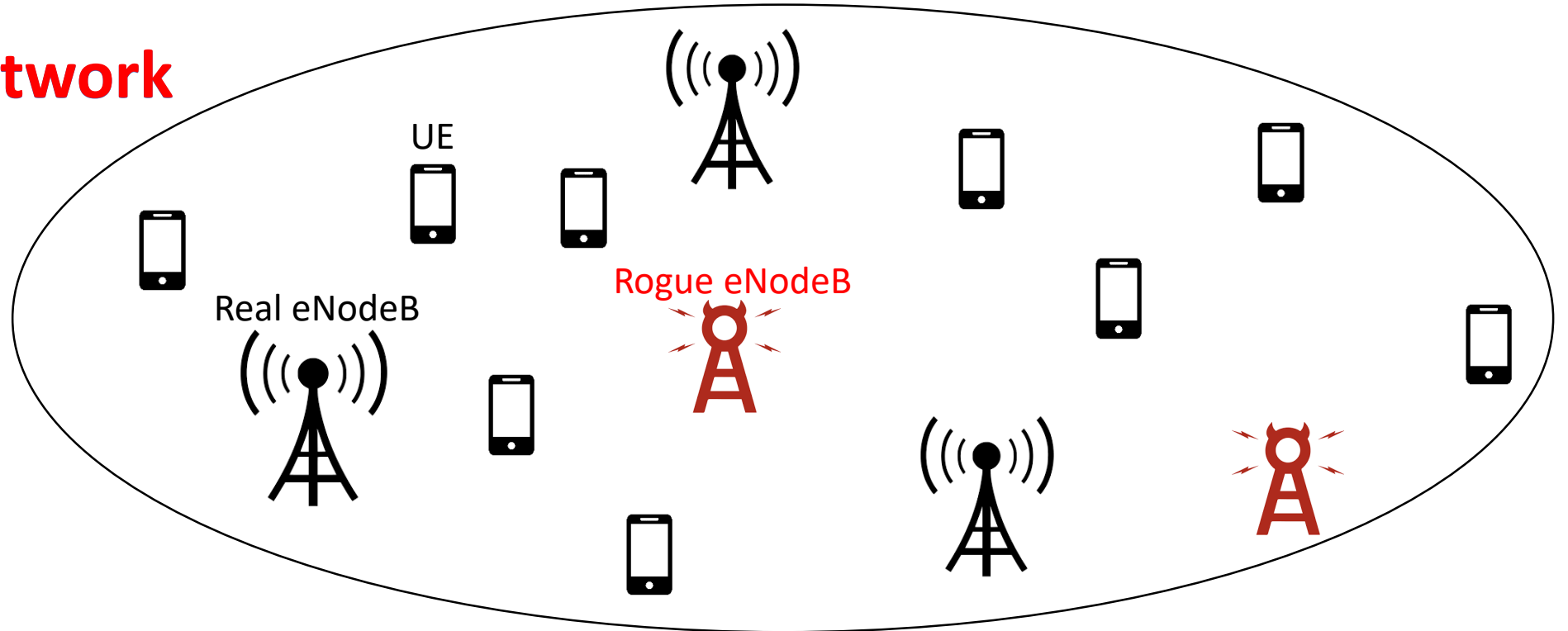
Automation in LTE – Vulnerable Points

- ## Cell configurations
  - PCI (Physical Cell ID)

- ## Neighbor relations
  - Discover eNodeBs, share configs - neighbor cells, load info

- ## Handover analysis
  - Performance statistics, success/drop rates

- ## Coverage enhancements
  - Radio Link Failure (RLF) report

Design Vulnerabilities

LTE PCI Optimization

- PCI: Physical Cell ID

- Adjacent cells: unique PCI, same frequency

- Network scanners, UE reports report PCI conflicts

- Same PCI: collision/confusion for UEs
  - Handover failures, connection issues
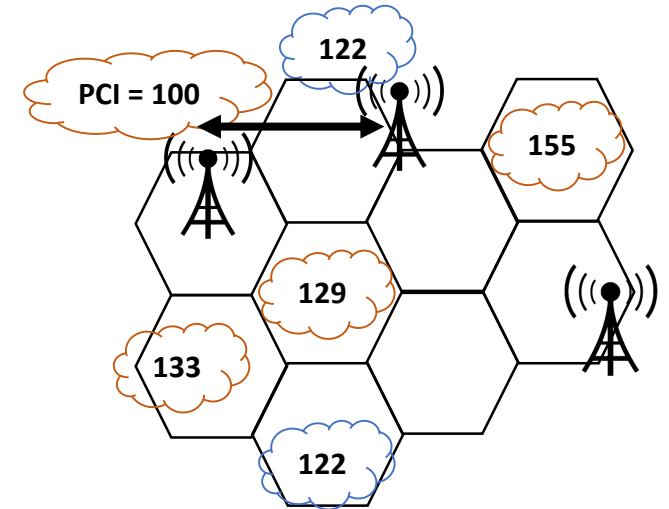
eNodeB forced to change their config

Automatic Neighbor Relation (ANR)

Cell A
Phy-CID=3
Global-CID =17

X2

Cell B
Phy-CID=5
Global-CID =19

1) report(Phy-CID=5, strong signal)

3) Report Global-CID=19

2b) Read BCCH()

2) Report Global-CID Request (Target Phy-CID=5)
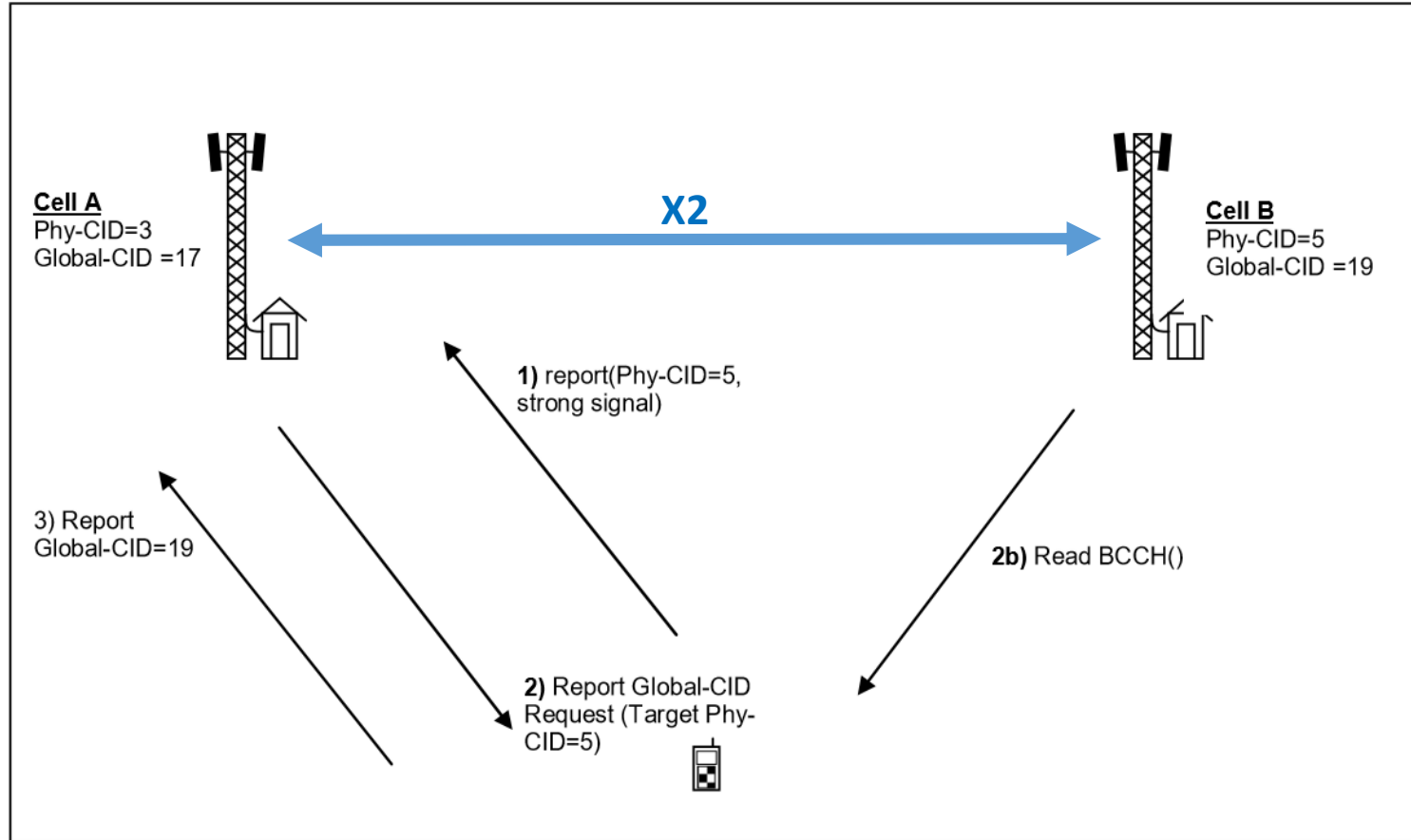
Source: 3GPP

- **Discover new eNodeBs**
- **Connect on X2 interface**

Automatic Neighbor Relation (ANR)

- Neighbor relation table

  - No Remove

  - NoHo : No Handover

  - NoX2

No attributes to authorize X2 setup

Neighbor Relation Table

Neighbour Relation		O&M controlled Neighbour Relation Attributes		
NR	TCI	No Remove	No HO	No X2
1	TCI#1			
2	TCI#1	✔		✔
3	TCI#1	✔		

Source: 3GPP

LTE Handover
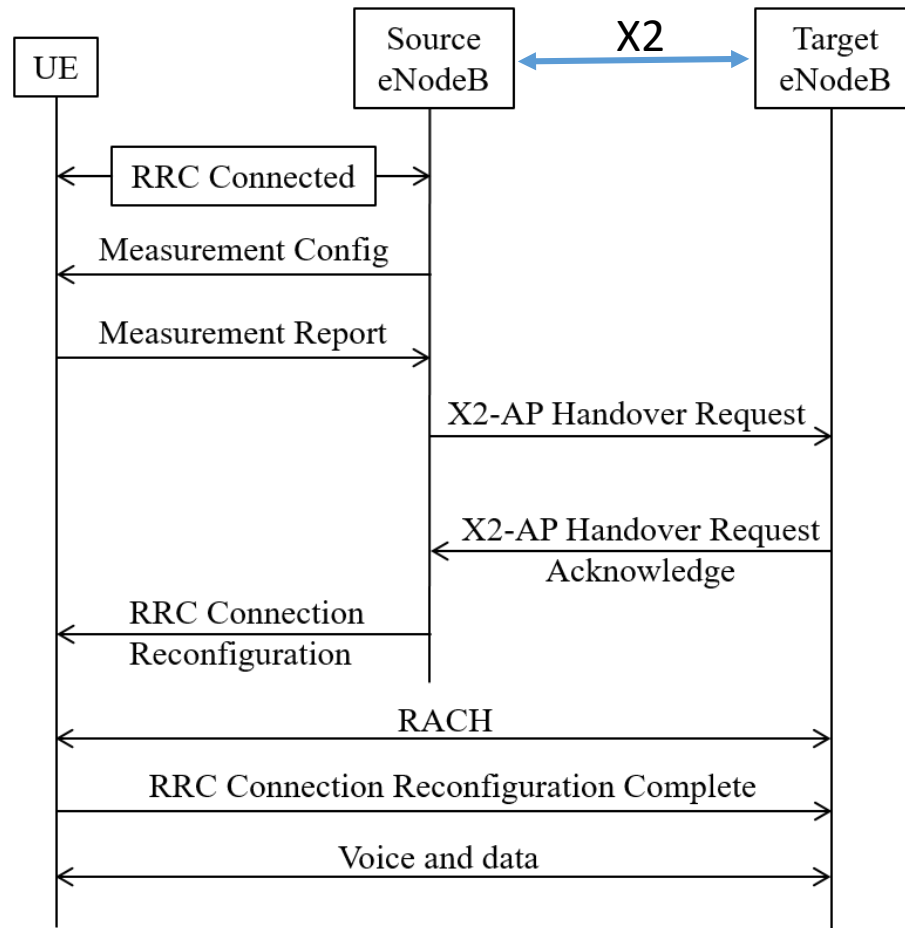
- X2 connected handovers

- GSM vs LTE handover

- No neighbor cell list for UE – detect all

- Based on PCI and EARFCN only

Reported Cells can be real or fake – No verification

LTE Handover

```
650.886795851 127.0.0.1              127.0.0.2              LTE RR…  111 MeasurementReport
651.350104071 127.0.0.1              127.0.0.2              LTE RR…   77 Paging (1 PagingRecords)
651.560286643 127.0.0.1              127.0.0.2              LTE RR…   81 MeasurementReport
652.001009274 127.0.0.1              127.0.0.2              LTE RR…   92 MeasurementReport
652.001608356 127.0.0.1              127.0.0.2              LTE RR…  127 RRCConnectionReconfiguration
652.001898243 127.0.0.1              127.0.0.2              LTE RR…   73 MasterInformationBlock (SFN=0)
652.002115375 127.0.0.1              127.0.0.2              LTE RR…   72 RRCConnectionReconfigurationComplete
652.002331473 127.0.0.1              127.0.0.2              LTE RR…   73 MasterInformationBlock (SFN=181)
652.002788061 127.0.0.1              127.0.0.2              LTE RR…   88 SystemInformationBlockType1
652.003037513 127.0.0.1              127.0.0.2              LTE RR…  119 SystemInformation [ SIB2 SIB3 ]
652.003263276 127.0.0.1              127.0.0.2              LTE RR…  102 SystemInformation [ SIB5 ]
```

```
            rrc-TransactionIdentifier: 2
        ▼ criticalExtensions: c1 (0)
            ▼ c1: rrcConnectionReconfiguration-r8 (0)
                ▼ rrcConnectionReconfiguration-r8
                    ▼ mobilityControlInfo
                        targetPhysCellId: 35
                    ▼ carrierFreq
                        dl-CarrierFreq: 3749
                        ul-CarrierFreq: 21749
                    ▼ carrierBandwidth
                        dl-Bandwidth: n25 (2)
                        ul-Bandwidth: n25 (2)
```

Handover Analysis

- Handover failure types
  - Early HO, Late HO, HO to wrong cell

- Identify faults
  - RLF reports (UE -> eNodeB)
  - HO reports (eNodeB <-> eNodeB)
  - Periodic KPI monitoring

- Solve faults, How?
  - Adjust coverage settings

HO blacklist (KPI < HO success threshold)

Handover success rate

$$\frac{\text{Handover preparation success rate}}{\text{Handover execution success rate}}$$

Handover problems – solutions
- Increase/decrease coverage
- Change cell index offset

Rogue Data Injection

- Measurement report

  - Can contain false information (3GPP 36.331) - for handovers and ANR

- Radio Link Failure (RLF) report

  - Can contain false information (3GPP 36.331) - for MRO

- Handover reports

  - Reports between eNodeBs about handover failures - for MRO

- **Information received from UE - content is not verified**

  - **Attackers can inject rogue data**

# Vulnerable Mobile Network Functions

- Cell detection and addition

- Cell ID interference detections

- LTE handover process

- Handover analysis

- Network coverage tuning

Exploitation

Rogue eNodeB

- 200 $ setup

- Broadcast channels sufficient

  - Spoof cell IDs of a legitimate eNodeB

- No interaction with UE

- Operating range depends on hardware

  - 50 meters without amplifiers

  - Open source software SRSLTE

  - For testing - SON base stations, faraday cage
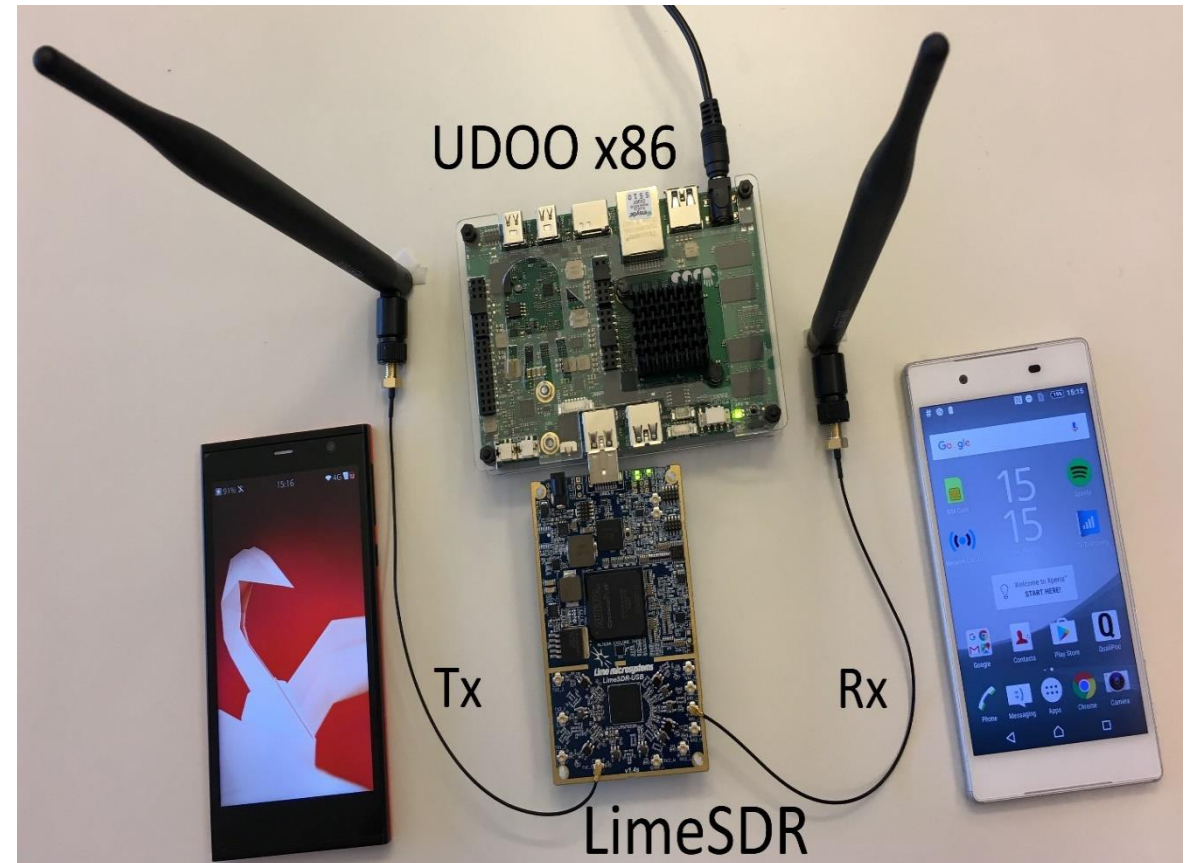
-> Exploiting X2 Signaling

- Adjacent eNodeBs are connected via X2 (ANR)

- Rogue eNodeB - legitimate PCI and ECGI (133, 272, 112)

- UEs report PCI 133 to eNodeB

- ANR begins to add 133 to NRT

- Problem
  - Zero control/authorize for X2 setup

- Effect
  - X2 signaling flood when more cells are impersonated
  - Handover failures

NR	PCI	No Remove	No HO	No X2
1	122	√		
2	109			√
3	133			
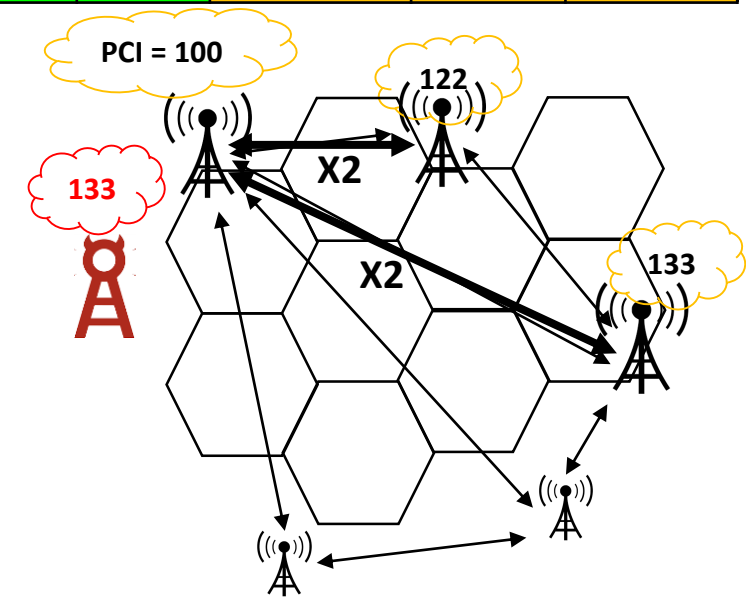
-> Remotely Kill & Restart LTE Base Station

- Adjacent cells/eNodeBs use unique PCI to avoid collision

- Rogue eNodeB Broadcast legitimate PCIs (100, 200, 300)

- Problem
  - Adjacent eNodeBs cannot use same PCI and starts optimization

- Effect
  - Restart eNodeB/cell and choose a new PCI
  - Restart time roughly 7-8 minutes
  - Release the connected UEs to other base stations (2G/3G)

PCI = 100
200
100
200
300
300
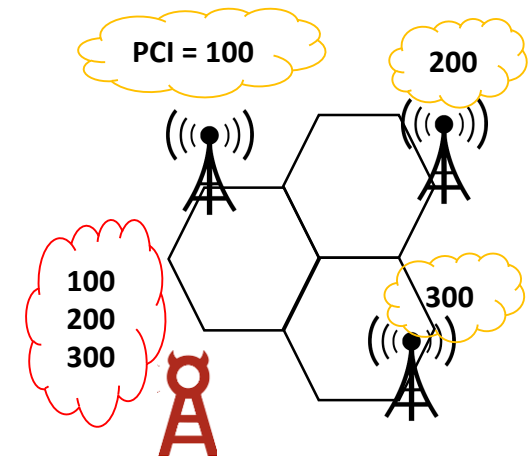
-> Handover Hijacking (Dropping Calls)

- UE in a voice call and sends periodic measurement reports

- Rogue eNodeB Broadcast legitimate neighboring PCI (100)

- Strong signal from PCI 100 causes handover

  - **PCI 100 already in neighbor list**

- Problem
  - Handover with false information

- Effect
  - UE connects to rogue eNodeB – Handover hijacked
  - RLF– report created against a real eNodeB
  - Ongoing calls are dropped

```
    ueInformationResponse-r9
        rlf-Report-r9
            measResultLastServCell-r9
                rsrpResult-r9: -78dBm <= RSRP < -77dBm (63)
                rsrqResult-r9: -3dB <= RSRQ (34)
            measResultNeighCells-r9
                measResultListEUTRA-r9: 1 item
                    Item 0
                        MeasResult2EUTRA-r9
                            carrierFreq-r9: 1300
                            measResultList-r9: 1 item
                                Item 0
                                    MeasResultEUTRA
                                        physCellId: 28
                                        measResult
                                            rsrpResult: -102dBm <= RSRP < -101dBm (39)
                                            rsrqResult: RSRQ < -19.5dB (0)
            failedPCellId-r10: pci-arfcn-r10 (1)
                pci-arfcn-r10
                    physCellId-r10: 101
                    carrierFreq-r10: 1300
            connectionFailureType-r10: rlf (0)
```

Impact of Handover Hijacking

- Rogue eNodeB calumniates (defames) a real eNodeB
  - RLF reports with false data
  - Handover failures
  - Coverage changes
  - KPI drops – **HO blacklisted or eNodeB/cell is shutdown**
  - 1 rogue eNodeB, 5 seconds – drop all cell (call + data) traffic..!

Impact – Grand Scale

Subscriber	Operator
Call and data drops	eNodeB maintenance and repairs
Poor network coverage	Poor network coverage
UE downgrades to 3G/2G	Revenue loss
	Customer complaints

- Detection by operators – no known methods to detect
- Persistent attacks – time needed for SON to heal
- Full Paper : https://dl.acm.org/citation.cfm?id=3212497

Security Status

Affected Products

- All LTE phones complying to 3GPP 36.331 >= Rel. 8
    - 4 basebands vendors (based on tested UEs)

- All network products complying with 32.500 >= Rel.8
    - 4 network vendors (based on available product documentation)

Vulnerability Status

- Disclosed with two operators (SON experts) and GSMA
  - Biggest European operators experts confirmed the issues

- Comments from GSMA and operators
  - Switch to less automation – reduce risk
  - PCI reallocation during maintenance period
  - Unplug a defective eNodeB (not really defective)
  - Difficulties to detect & add mitigations

- GSMA guidelines document (ongoing) – protection from rogue base stations

Mobile Security Research Hall of Fame

Welcome to the GSMA Mobile Security Research Hall of Fame.
The GSMA's Mobile Security Research Hall of Fame lists security vulnerability finders that have made contributions to increasing the security of the mobile industry by submitting disclosures to the GSMA or its members. It is the primary mechanism for the GSMA to recognise and acknowledge the positive impact the finder has had on the mobile industry by following the GSMA's CVD process.

The Hall of Fame also facilitates the nomination and recognition of other finders that may have made significant discoveries of vulnerabilities to individual GSMA member companies.

Entry to the Mobile Security Research Hall of Fame is purely optional and is at the discretion of the finder, the GSMA and/or the nominating GSMA member.

On behalf of the mobile industry, we would like to thank the following people for making a responsible disclosure to us and recognise their contribution to increasing the security of the mobile industry:

Date	CVD#	Name	Organisation & Link
13/06/2018	0007	Altaf Shaik	Technical University of Berlin and Kaitiaki Labs https://www.isti.tu-berlin.de/security_in_telecommunications
13/06/2018	0007	Ravishankar Borgaonkar	SINTEF Digital and Kaitiaki Labs https://www.sintef.no/en/cyber-security/#/

Solutions

- Signed broadcast messages
  - Prevent connection to rogue base stations (5G: NO, complicated design)

- Content verification
  - Verify measurement reports from UE
  - Compatibility issues, power issues, efficiency problems

- Adding actionable intelligence to SON

- Built-in baseband features to detect rogue base stations
  - Ongoing work with a vendor

Takeaways

- SON operate with unverified information from phones

- Current SON techniques cannot deal with Rogue base station attacks

- Lack of appropriate parameters for optimal automation decisions

- Automation lacks data verification and rely on few parameters

- **A 200 $ rogue device can modify network configurations and turn it OFF..!**

Thank you

✉ altaf329@sect.tu-berlin.de
rbbo@kth.se
director@kaitiaki.in