UNIVERSITY OF HELSINKI

Fake base stations in 5G networks

Valtteri Niemi

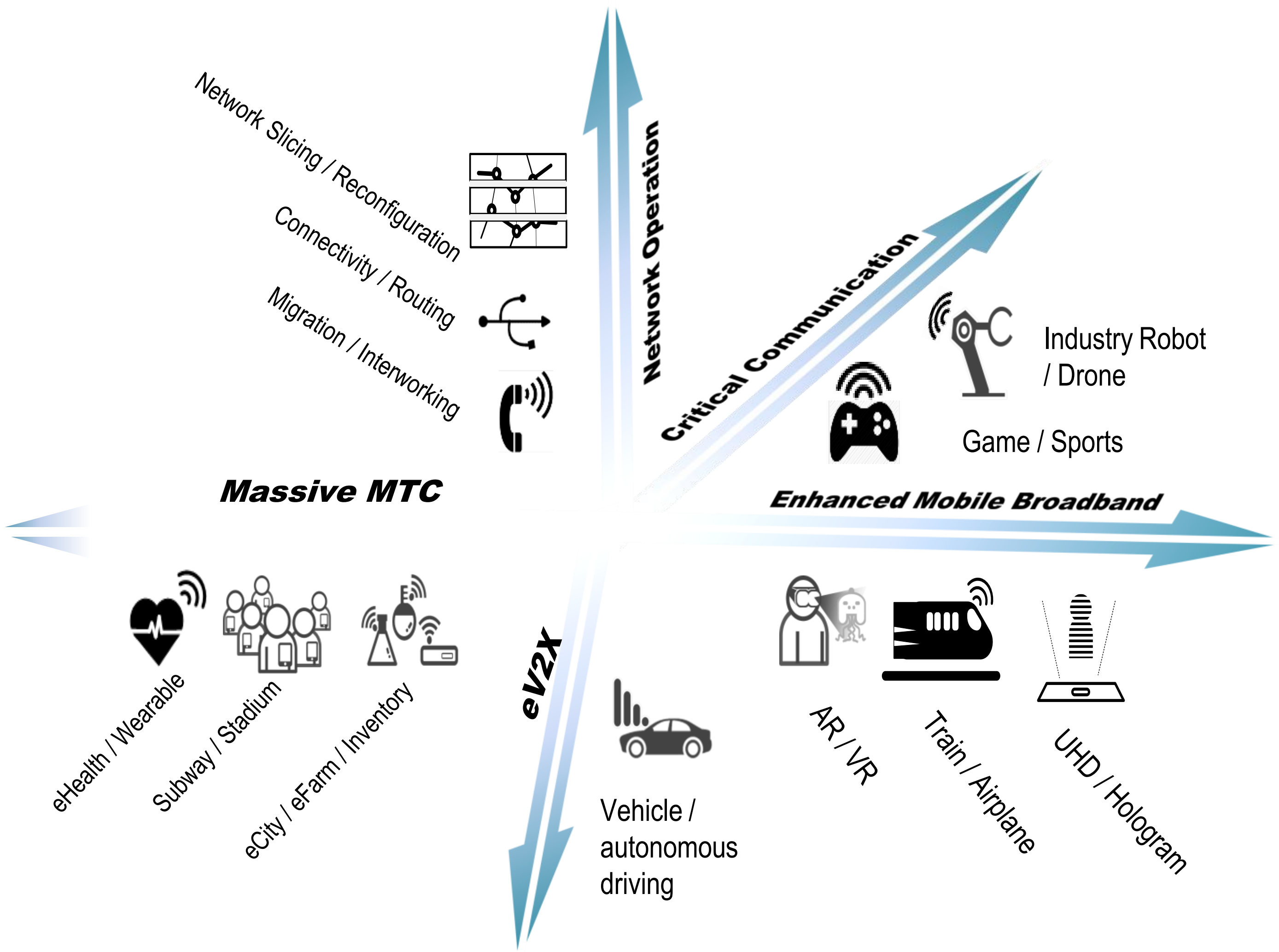
NATO SET-247, Helsinki

8 May 2017

Outline

- What is 5G?
- What is a fake base station?
- Fake base station attacks in LTE (4G)
- Countermeasures planned for 5G
- Conclusions

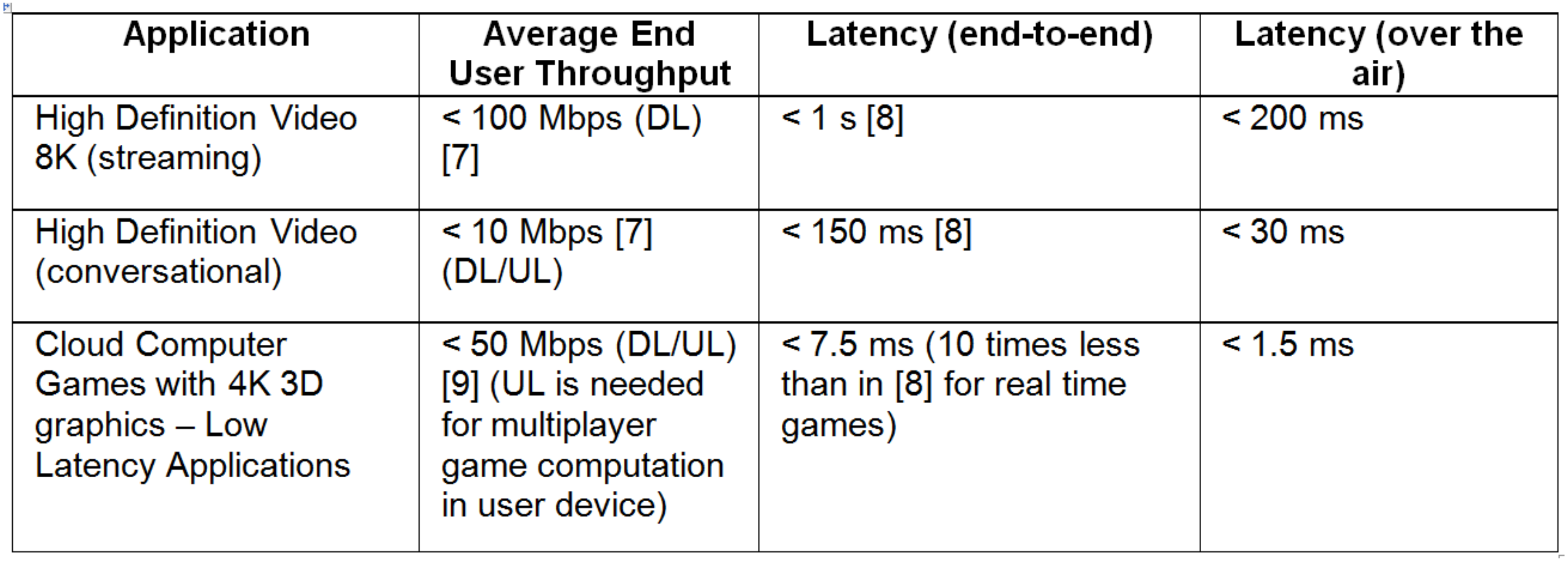
5G service dimensions (3GPP)



5G service requirements (3GPP)

- User experienced data rate up to Gbps.
- User peak data rate at tens of Gbps;
- The whole traffic volume at Tbps/ km^2.
- Very low latency for user experienced data exchange (~1 ms).

Selected services



Application	Average End User Throughput	Latency (end-to-end)	Latency (over the air)
High Definition Video 8K (streaming)	< 100 Mbps (DL) [7]	< 1 s [8]	< 200 ms
High Definition Video (conversational)	< 10 Mbps [7] (DL/UL)	< 150 ms [8]	< 30 ms
Cloud Computer Games with 4K 3D graphics – Low Latency Applications	< 50 Mbps (DL/UL) [9] (UL is needed for multiplayer game computation in user device)	< 7.5 ms (10 times less than in [8] for real time games)	< 1.5 ms

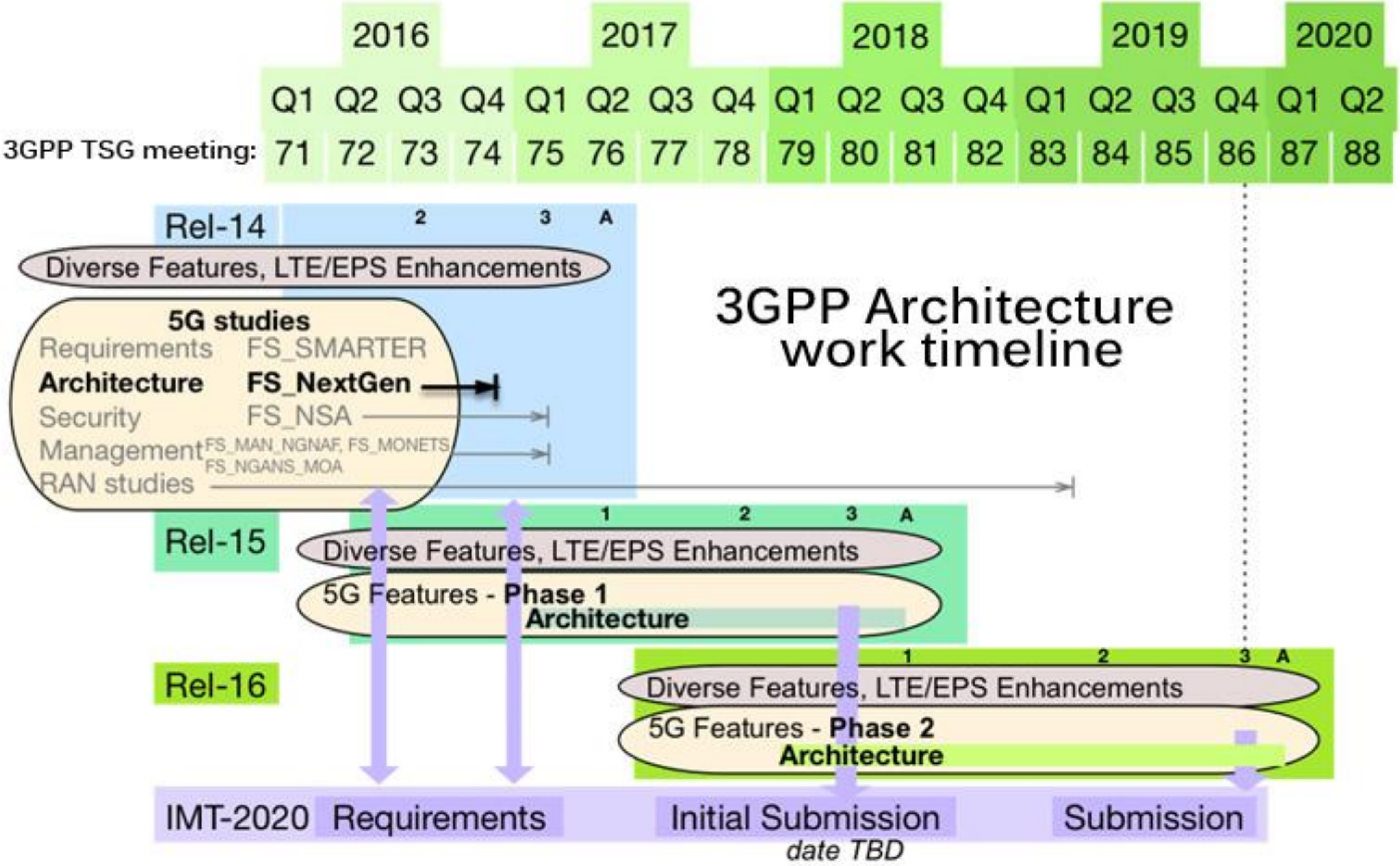
5G key technologies

- Cloud computing
- Software-defined networking (SDN)
- Network function virtualization (NFV)
- (massive) Internet of Things
- Machine-to-machine communications
- Critical communications
- Network slicing

5G key technologies

- Cloud computing
- Software-defined networking (SDN)
- Network function virtualization (NFV)
- (massive) Internet of Things
- Machine-to-machine communications
- Critical communications
- Network slicing
- ***All have implications on security !***

Schedule



	2016				2017				2018				2019				2020	
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2
3GPP TSG meeting:	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88

Rel-14 2 3 A

Diverse Features, LTE/EPS Enhancements

5G studies

Requirements FS_SMARTER

Architecture FS_NextGen

Security FS_NSA

Management FS_MAN_NGNAF, FS_MONETS FS_NGANS_MOA

RAN studies

3GPP Architecture work timeline

Rel-15 1 2 3 A

Diverse Features, LTE/EPS Enhancements

5G Features - **Phase 1**

Architecture

Rel-16 1 2 3 A

Diverse Features, LTE/EPS Enhancements

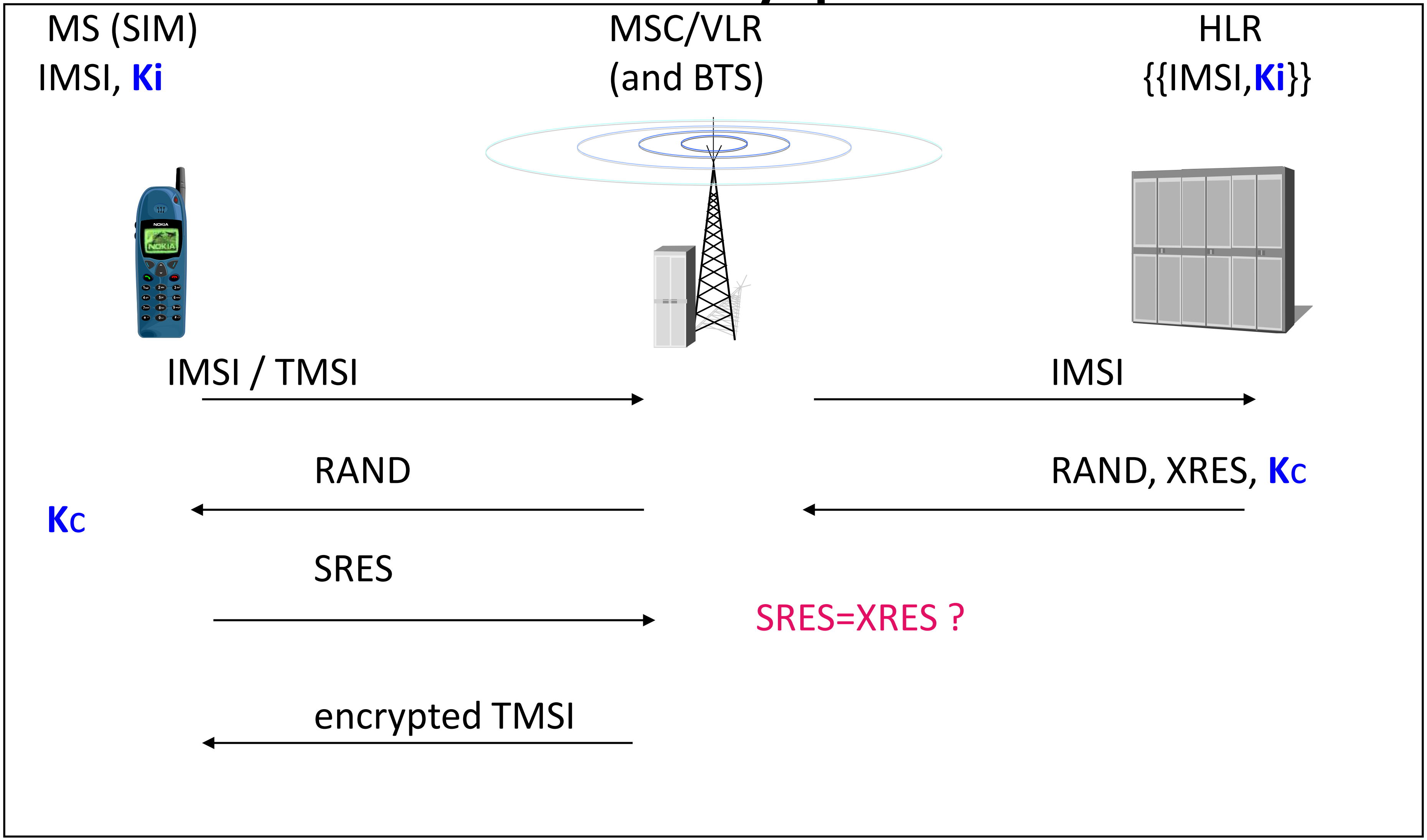
5G Features - **Phase 2**

Architecture

IMT-2020 Requirements Initial Submission Submission

date TBD

GSM security protocol



MS (SIM)

IMSI, Ki

MSC/VLR

(and BTS)

HLR

{{IMSI,Ki}}

IMSI / TMSI

IMSI

RAND

RAND, XRES, Kc

Kc

SRES

SRES=XRES ?

encrypted TMSI

Mutual authentication in 3G

- There are three entities involved:
  - Home network HN (AuC)
  - Serving network SN (VLR/SGSN)
  - Mobile station MS (USIM)
- Executed whenever SN decides

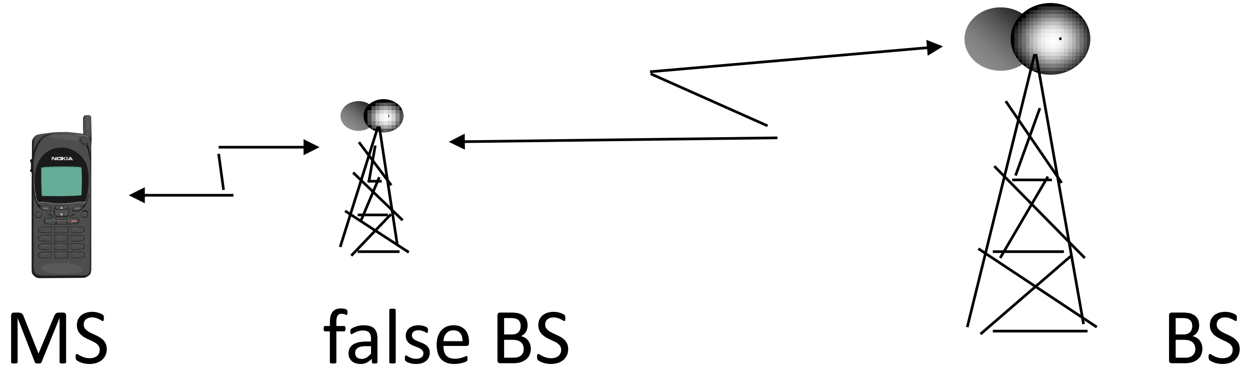
- The idea: SN checks MS's identity (as in GSM) and MS checks that SN has *authorization* from HN
- A *master key K* is shared between MS and HN
- GSM-like *challenge-response* in *user-to-network* authentication
- Network proves its authorization by giving a token AUTN which is protected by K and contains a sequence number SQN

Identity and location privacy

- Key feature in mobile systems since GSM
- Protection against ***passive*** adversaries:
  - ***Temporary*** identity is allocated over ***encrypted*** channel

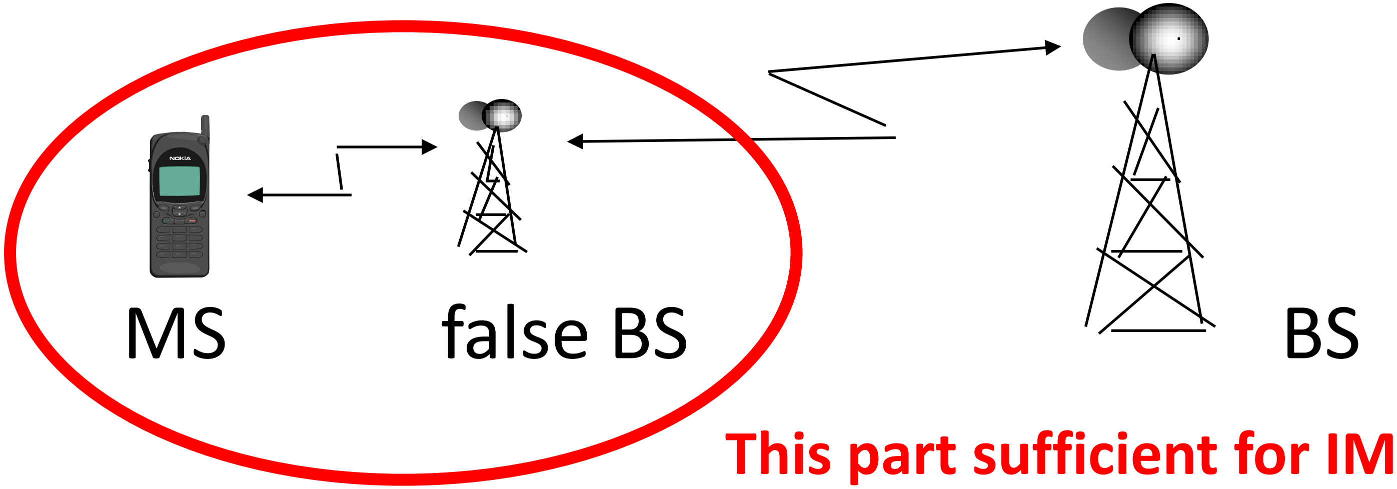
Active attack

- A ***false*** element masquerades
  - as a base station towards terminal
  - as a terminal towards network
- Objectives of the attacker:
  - eavesdropping
  - stealing of connection
  - manipulating data



Active attack

- A ***false*** element masquerades
  - as a base station towards terminal
  - as a terminal towards network
- Objectives of the attacker:
  - eavesdropping
  - stealing of connection
  - manipulating data



MS

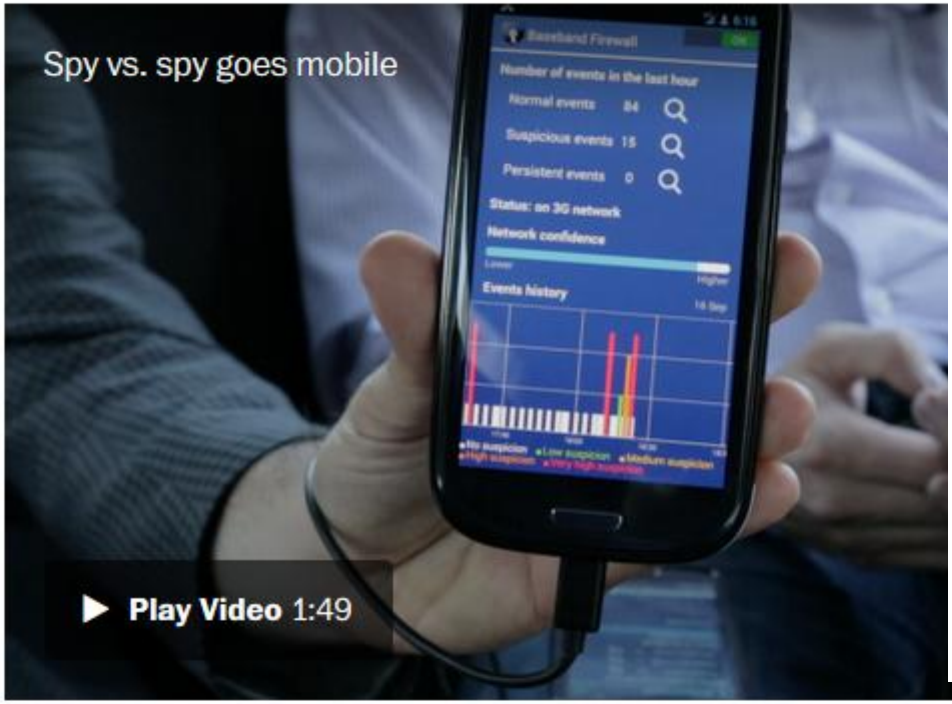
false BS

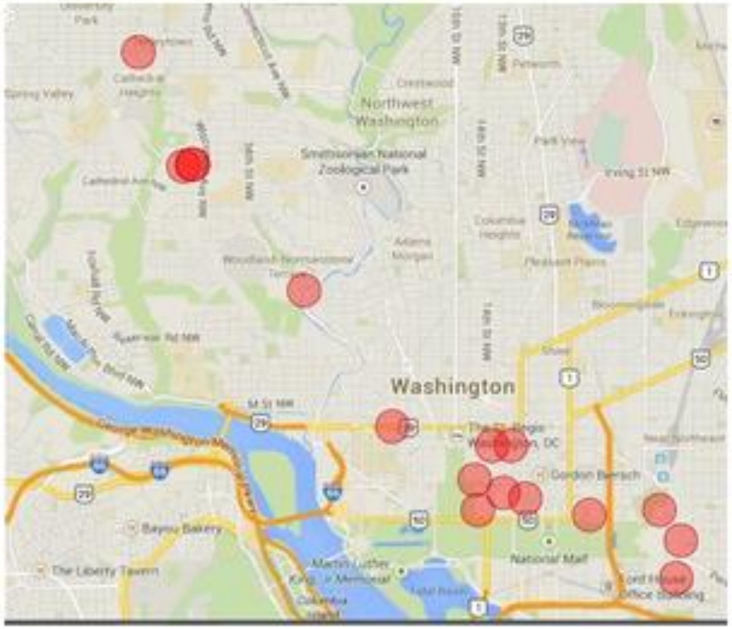
BS

This part sufficient for IMSI catcher

IMSI catchers

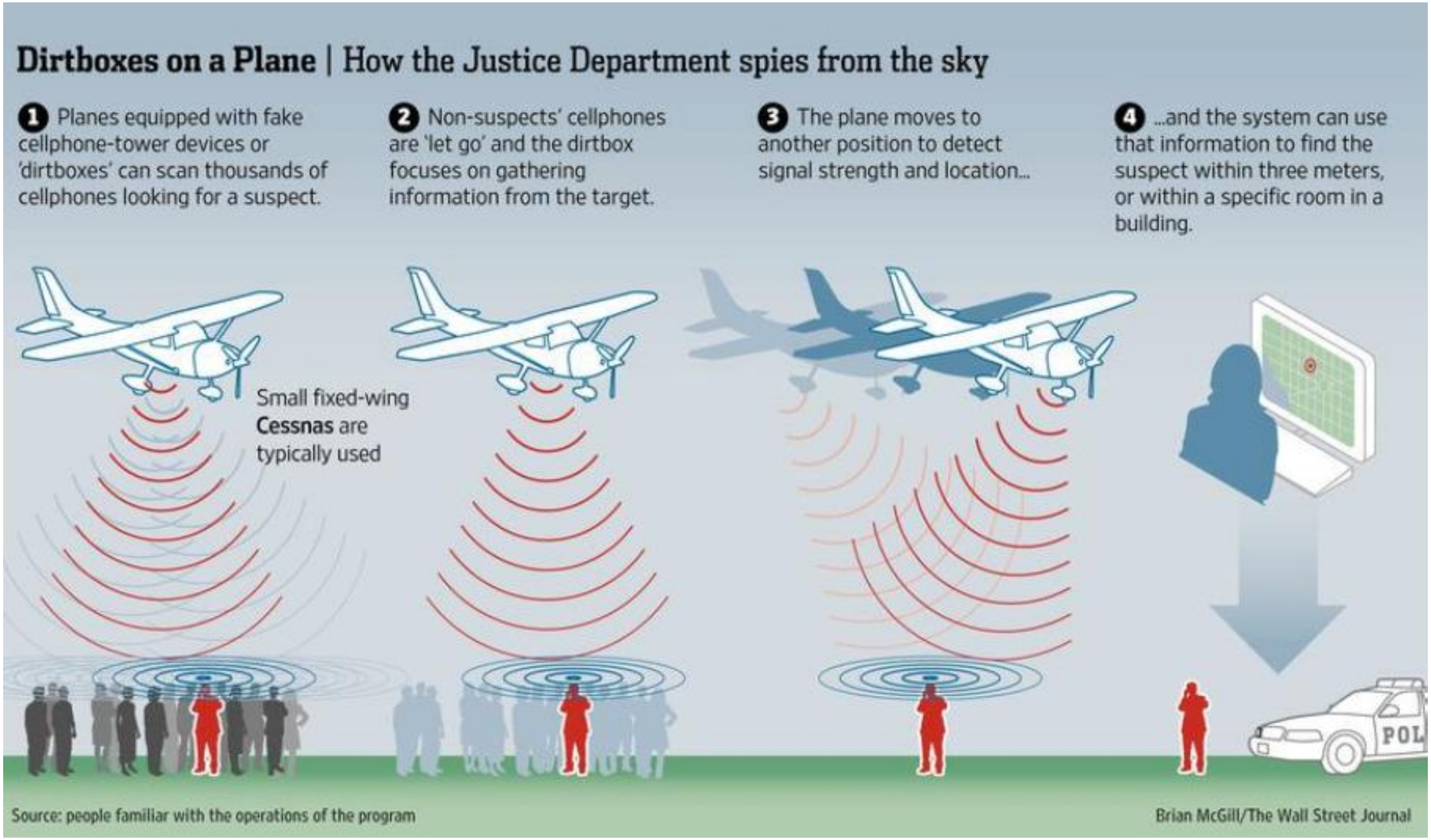
The Washington Post





Locations in Washington where the Crytophone detected "suspicious activity" that may indicate the presence of a surveillance device known as an "IMSI catcher." (ESD, IntegriCell)

A German company called GSMK recently came out with the CryptoPhone, which for $3,500 can allegedly sense mobile surveillance technology. But there is some skepticism over the accuracy of its tracking. The Washington Post takes a ride to the Russian embassy to see the phone in action. (Alice Li/The Washington Post)



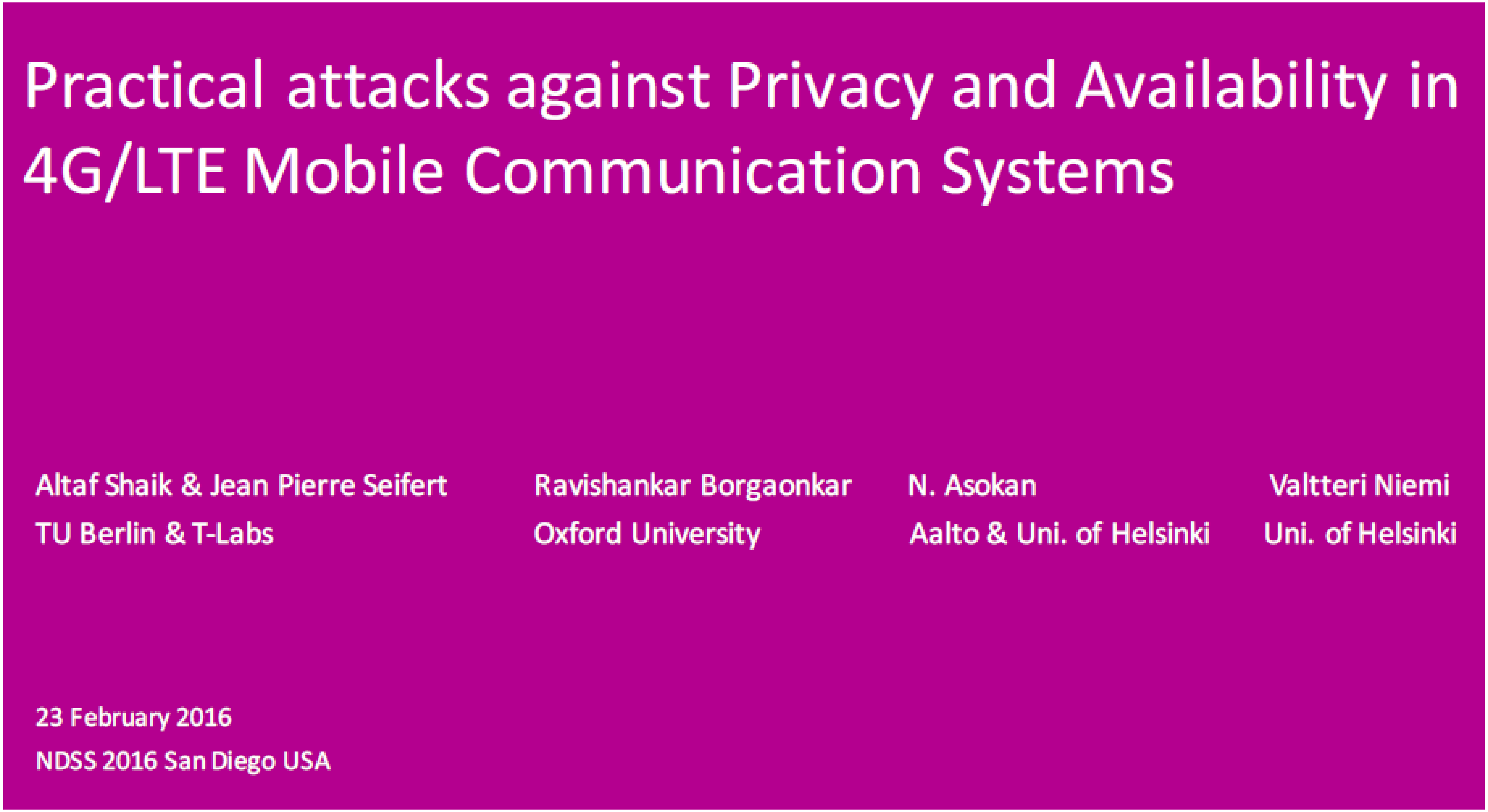
Dirtboxes on a Plane | How the Justice Department spies from the sky

1. Planes equipped with fake cellphone-tower devices or 'dirtboxes' can scan thousands of cellphones looking for a suspect.
2. Non-suspects' cellphones are 'let go' and the dirtbox focuses on gathering information from the target.
3. The plane moves to another position to detect signal strength and location...
4. ...and the system can use that information to find the suspect within three meters, or within a specific room in a building.

Source: people familiar with the operations of the program

Brian McGill/The Wall Street Journal

Our experiments with fake base stations have been reported in:



Practical attacks against Privacy and Availability in 4G/LTE Mobile Communication Systems

Altaf Shaik & Jean Pierre Seifert
TU Berlin & T-Labs

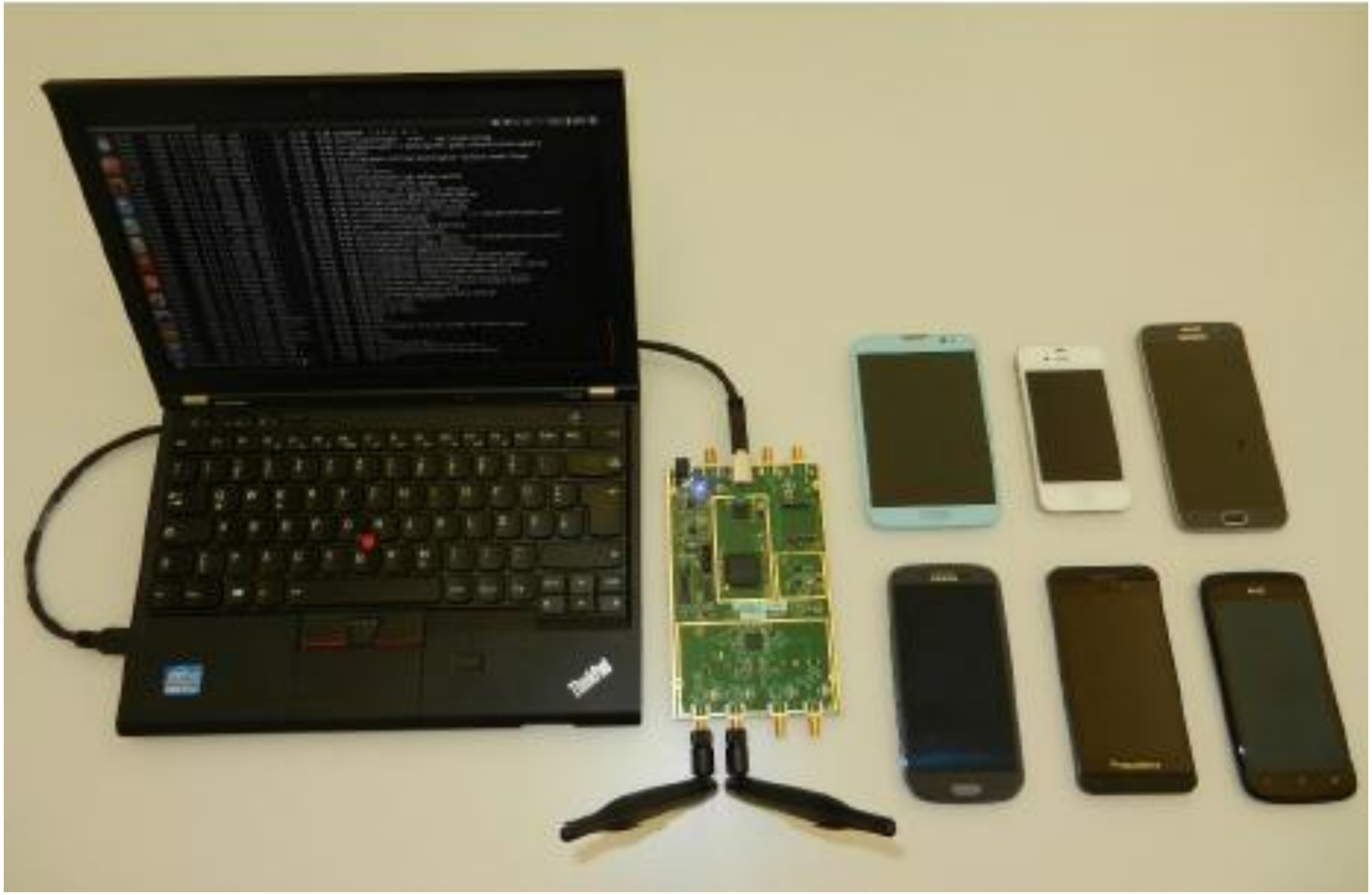
Ravishankar Borgaonkar
Oxford University

N. Asokan
Aalto & Uni. of Helsinki

Valtteri Niemi
Uni. of Helsinki

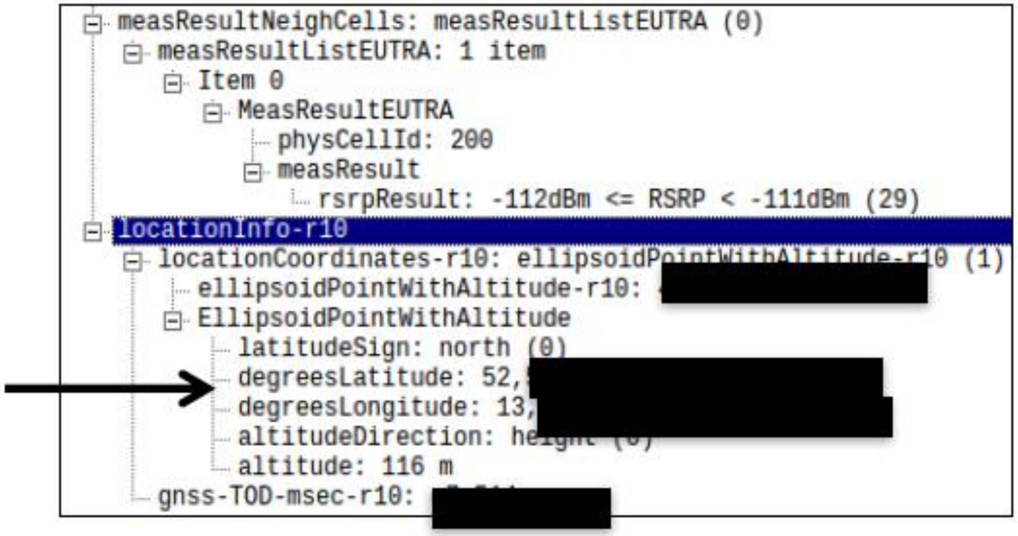
23 February 2016
NDSS 2016 San Diego USA

Experimental set-up (~1 k$)

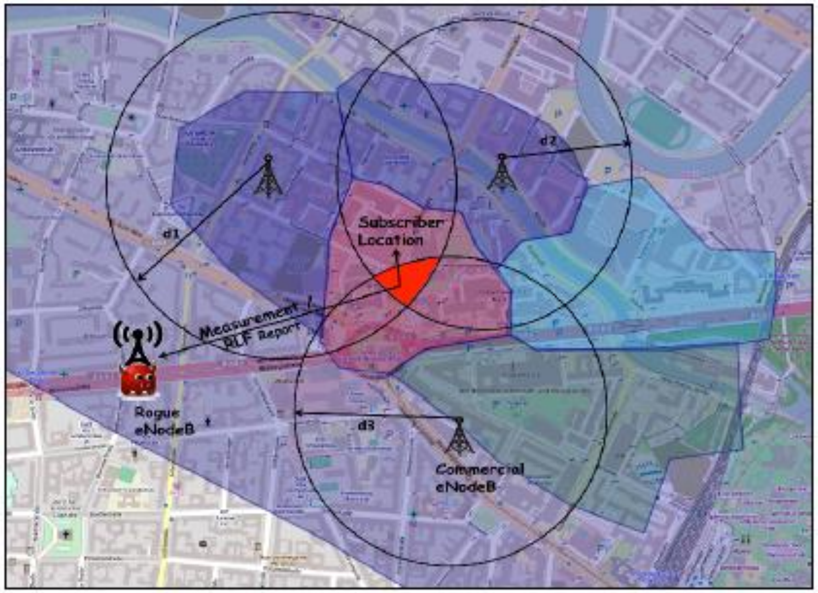


Precise location using trilateration or GPS !

- Measurement/RLF report
  - ✓ Two rogue eNodeBs for RLF
  - ✓ eNodeB1 triggers RL failure: disconnects mobile
  - ✓ eNodeB2 then requests RLF report from mobile



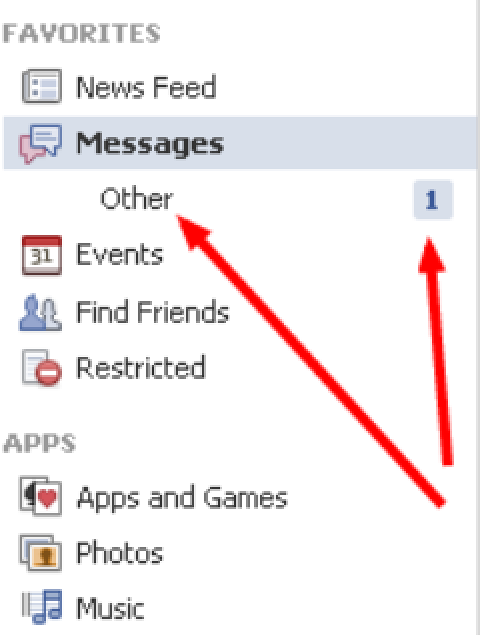
```
⊟ measResultNeighCells: measResultListEUTRA (0)
   ⊟ measResultListEUTRA: 1 item
      ⊟ Item 0
         ⊟ MeasResultEUTRA
              physCellId: 200
            ⊟ measResult
                 rsrpResult: -112dBm <= RSRP < -111dBm (29)
⊟ locationInfo-r10
   ⊟ locationCoordinates-r10: ellipsoidP[redacted]-r10 (1)
        ellipsoidPointWithAltitude-r10: [redacted]
      ⊟ EllipsoidPointWithAltitude
           latitudeSign: north (0)
           degreesLatitude: 52,[redacted]
           degreesLongitude: 13,[redacted]
           altitudeDirection: he[redacted]
           altitude: 116 m
     gnss-TOD-msec-r10: [redacted]
```



Semi-Passive : determine tracking area & cell ID

- VoLTE calls: Mapping GUTIs to phone number
  - ✓ 10 silent calls to victim's number
  - ✓ High priority → paging to entire tracking area(TA)
  - ✓ Passive sniffer in a TA

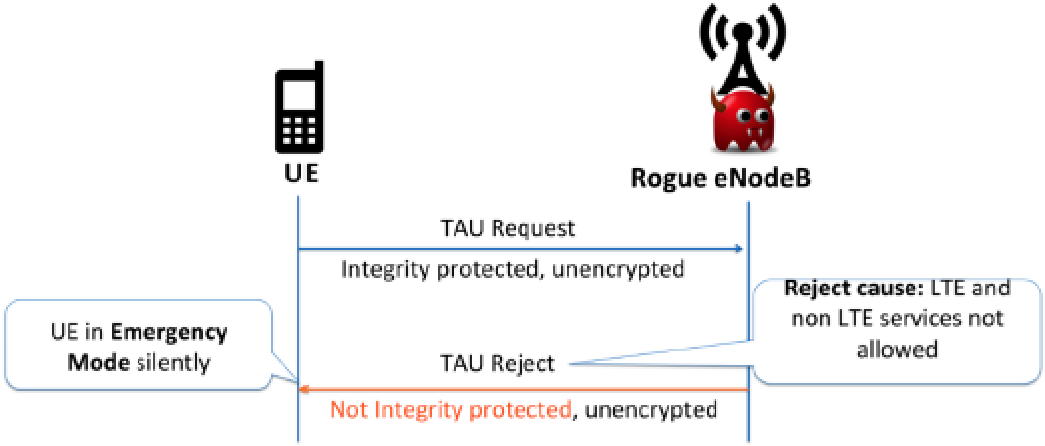
- Social identities: Mapping GUTIs to Social Network IDs
  - ✓ E.g., 10 Facebook messages, whatsapp/viber
  - ✓ Low priority → Smart paging to a last seen cell
  - ✓ Passive sniffer in a cell



DoS Attacks

Exploiting specification vulnerability in EMM protocol!

- Downgrade to non-LTE network services (2G/3G)
- Deny all services (2G/3G/LTE)
- Deny selected services (block incoming calls)
- Persistent DoS
- Requires reboot/SIM re-insertion


UE
Rogue eNodeB
TAU Request
Integrity protected, unencrypted
Reject cause: LTE and non LTE services not allowed
UE in **Emergency Mode** silently
TAU Reject
Not Integrity protected, unencrypted

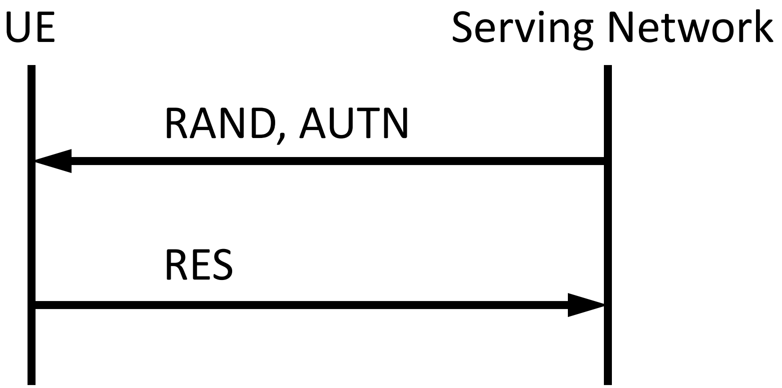
Identity protection in 2G/3G/4G/5G

Attacker type		2G	3G	4G	5G
Attacker is outside RAN	Passive	Yes	Yes	Yes	Yes?
	IMSI catcher	No	No	No	**Yes?**
	MitM	No	Yes	Yes	Yes?
RAN=Attacker	Passive	No	No	No	**No?**
	Active	No	No	No	No?

Methods to prevent IMSI catchers

- Second layer of ***pseudonyms***
  - Shared with home network operator
  - But requires keeping synchronized state with every user
  - Could look like IMSI → would work also in ***legacy*** networks (backwards compatibility)
- User identity is encrypted by network ***public key*** in the connection set-up
  - But some sort of PKI is needed
  - Not backwards compatible

Pseudonym-based approach can be backward compatible: van den Broek, Verdult and de Ruiter, CCS 2015; Khan and Mitchell, SSR 2015.



|RAND|=|AUTN|=128b

1. The pseudonym looks like IMSI. There is a non-changing part (pointing to the correct home network) and the changing part P that is in the form of MSIN, 9-10 decimal digits (< 40b).
2. RAND carries Enc(P'), the encryption of next pseudo P'
3. Decryption of P' is done by the USIM.

ME-based variant (Ginzboorg, Niemi ’16)

- The above designs require ***new USIM***. But 5G ME that has a legacy 4G USIM is also a likely scenario in 5G.
- The combination of 5G USIM + legacy ME is not very important in 5G; to get benefits from 5G, a new ME is likely to be required.
- → design that ***does not require changes to USIM***, but ***requires changes to ME*** could be used in 5G.
  - Pseudonyms encrypted with a key available in ME
  - AMF indicates RAND contains encrypted pseudonym

Summary of different options for enhancing user identity privacy in 5G

	Public- or group- key based approach	Generic pseudonym-based approach	USIM-based pseudonyms	ME-based pseudonyms
Changes needed in:				
USIM	**NO**	**NO**	**YES**	**NO**
ME	**YES**	**YES**	**NO**	**YES**
Serving Network	**YES**	**YES**	**NO**	**NO**
Home Network	**YES**	**YES**	**YES**	**YES**
Protection given in:				
legacy 3G/4G networks	**NO**	**NO**	**YES**	**YES**
5G networks	**YES**	**YES**	**YES**	**YES**

Conclusions

- Fake base stations can be used in GSM/3G/LTE
  - Identity and location tracking
  - Targeted denial of service
- Semi-passive attacks are also possible
- 5G is planned to defend better against fake base station attacks
- But:
  - Semi-passive attacks (may) still work
  - Downgrade to 4G (may) still enable the attacks

Thanks!