UNIVERSITY OF HELSINKI

Towards solutions for 5G security

Valtteri Niemi
University of Helsinki, Finland
Globecom workshop
San Diego 6 December 2015

What are the issues?

- NGMN 5G whitepaper, February 2015
- Ericsson security whitepaper, June 2015
- Schneider, Horn (Nokia), Trustcom WS, August 2015
- Ginzboorg (Huawei), Trustcom WS, August 2015

UNIVERSITY OF HELSINKI

	NGMN	E///	NOK	HW
Cloud security	✓	✓	✓	✓
E2E encryption	✓	✓	✓	✓
Identity privacy	✓	✓	✓	✓
Flexible security	✓	✓	✓	
Energy-efficiency		✓		✓
User plane integrity		✓	✓	
Authentication	✓		✓	
Security set-up	✓		✓	
DoS protection	✓		✓	

Cloud security

- Generic cloud security issues
  - Isolation
  - Platform security
  - etc.

Cloud security

- Generic cloud security issues
  - Isolation
  - Platform security
  - etc.
- 5G specific issues
  - Where to store cryptographic **keys** ?
  - How to manage **identities** ?

Cloud security

- Generic cloud security issues
  - Isolation
  - Platform security
  - etc.
- 5G specific issues
  - Where to store cryptographic keys ?
  - How to manage identities ?

→ (some sort of) security and identity **layer** is needed

End-to-end protection

- 2G, 3G, 4G traffic is protected **hop-by-hop**

End-to-end protection

- 2G, 3G, 4G traffic is protected **hop-by-hop**
- But **end-to-end** has many advantages:
  - Trust on cloud is minimized
  - Uniform protection
  - Better visibility for users
  - etc.

End-to-end protection

- 2G, 3G, 4G traffic is protected **hop-by-hop**
- But **end-to-end** has many advantages:
  - Trust on cloud is minimized
  - Uniform protection
  - Better visibility for users
  - etc.
- The main **disadvantage**:
  - There are **lots of** end points; also on **control plane**
  - Several other disadvantages, e.g. **traffic analysis**

End-to-end protection

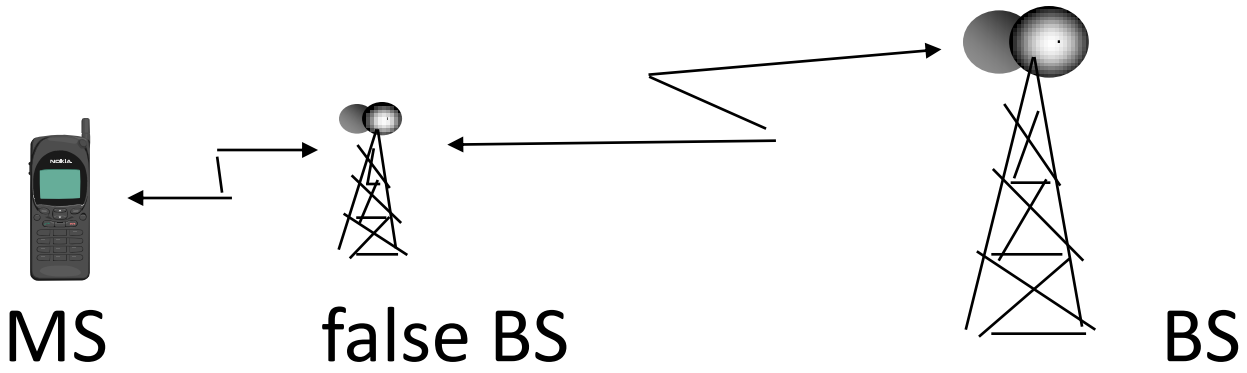
- **Separation** of user plane and control plane could drive towards end-to-end protection
- End-to-end is even more useful for **integrity** protection than for **encryption**

Identity and location privacy

- Key feature in mobile systems since GSM
- Protection against ***passive*** adversaries

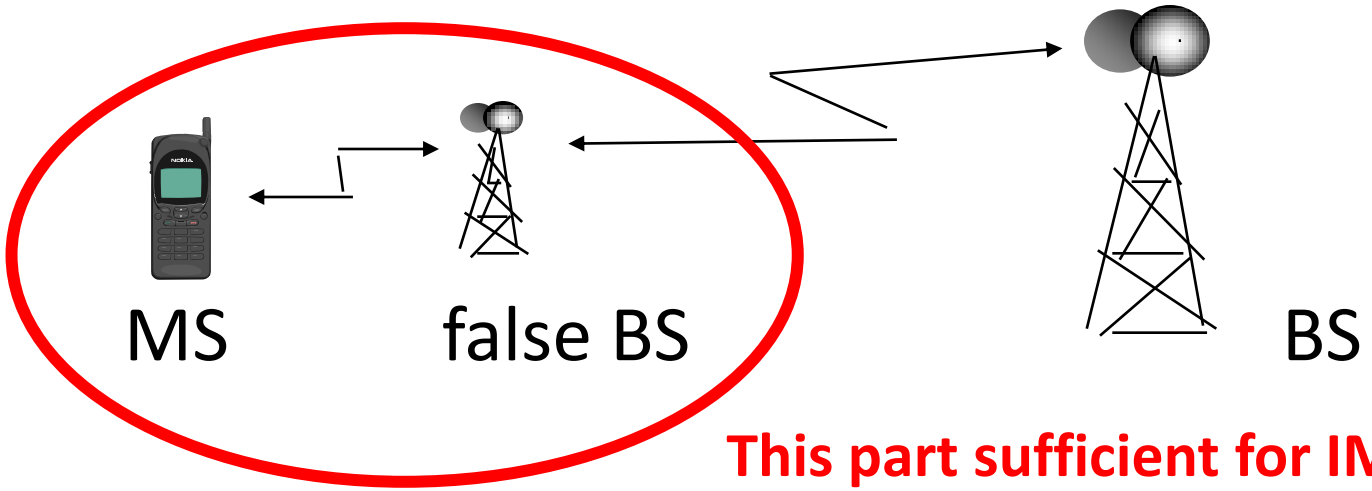
Active attack

- 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

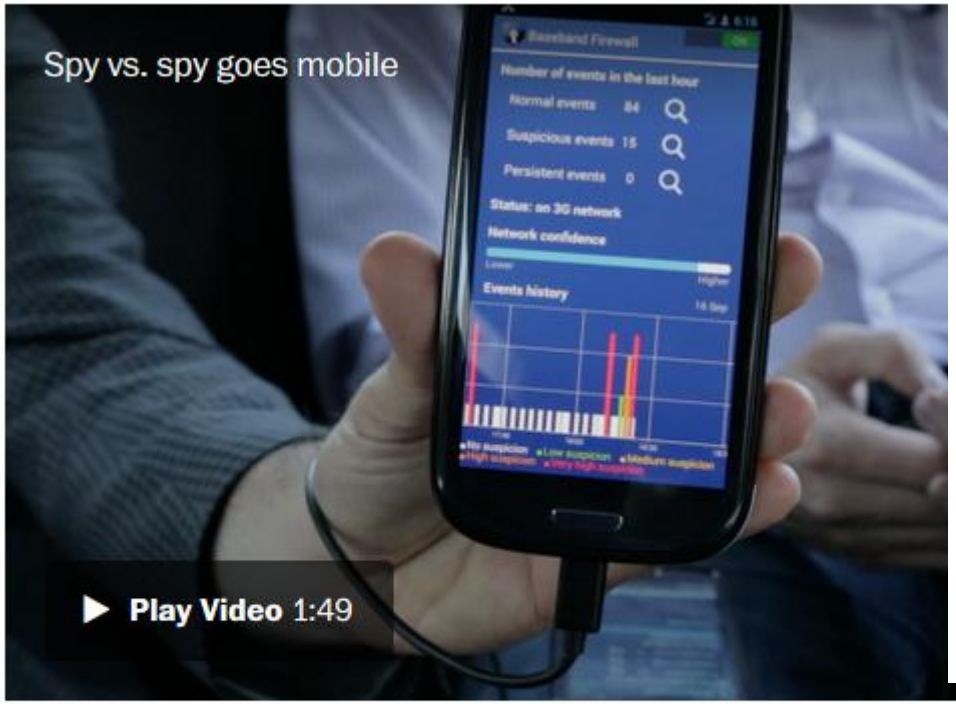
- A ***false*** element masquerades
  - as a base station towards terminal
  - as a terminal towards network
- Objectives of the attacker:
  - eavesdropping
  - stealing of connection
  - manipulating data



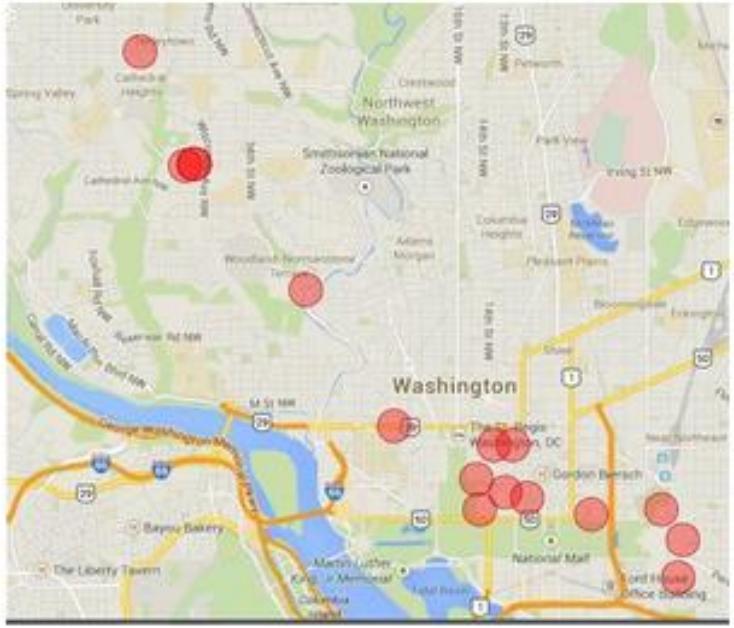
This part sufficient for IMSI catcher

IMSI catchers

The Washington Post



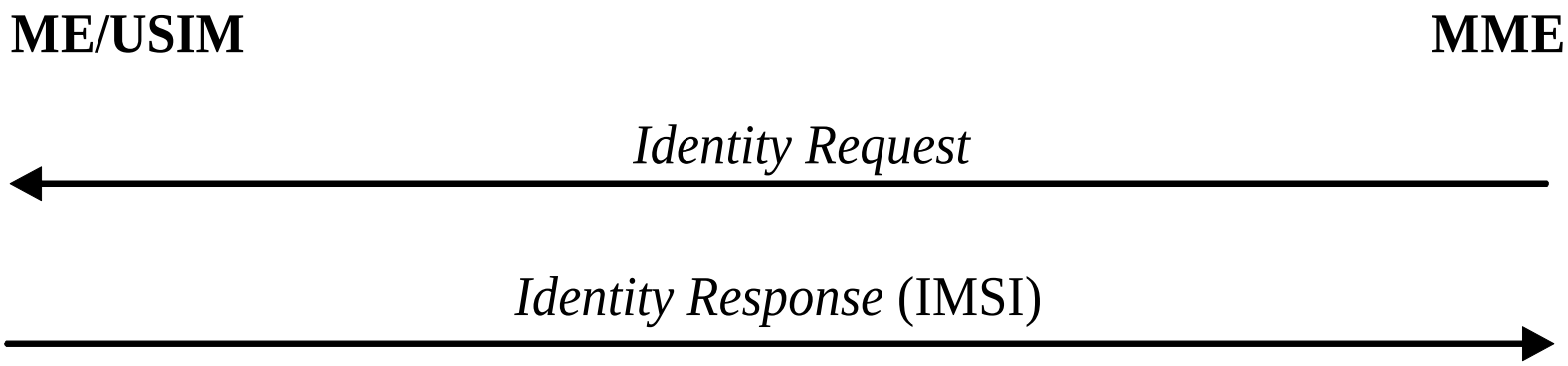
A German company called GSMK recently came out with the CryptoPhone, which for $3,500 can allegedly sense mobile surveillance technology. But there is some skepticism over the accuracy of its tracking. The Washington Post takes a ride to the Russian embassy to see the phone in action. (Alice Li/The Washington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



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)

Identity confidentiality in LTE

- Mechanism inherited from GSM and 3G
- User's permanent identity (IMSI) is sent to the network ***only if*** network cannot identify the UE otherwise



From 3GPP TS 33.401

Identity confidentiality in LTE (2/2)

- Network assigns a temporary identity for the UE
- It is sent to the UE in encrypted message
- In GSM/3G the temporary identity is
  - TMSI for CS domain
  - P-TMSI for PS domain
- In EPS the temporary identity is called GUTI (Globally Unique Temporary Identity)

Identity privacy in 5G

Joint work with P. Ginzboorg

(submitted)

Classification of adversaries

	Passive	Active
Outside of 5G RAN	collect IMSI (but cannot relate IMSI to TMSI)	False Base Station, could force 2G connection, then e.g. becomes Man-in-the-middle Identity probing: e.g., call target phone nr. and wait for answer.
5G RAN operator = attacker	maps TMSI to IMSI and collects (IMSI, time, location) records.	(i) This attacker has all the capabilities of the other attackers, and in addition (ii) he can observe and control the signaling messages in the 5G RAN. (This gives an advantage, for example, when doing identity probing.) (iii) The attacker may also try to analyze the user plane data, if that data is unprotected. For example, looks for application identities.

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	?
	MitM	No	Yes	Yes	Yes?
RAN=Attacker	Passive	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
- User identity is encrypted by network **public key** in the connection set-up
  - But some sort of PKI is needed

New attacks against LTE identity and location privacy

Joint work with A. Shaik, R. Borgaonkar, N. Asokan and J-P. Seifert

(Blackhat Europe, November 2015)

Experimental set-up

Passive attack

- Universal Software Radio Peripheral (USRP)
- *srsLTE* software
- Sniffing broadcast channels, incl. paging
- Observed LTE temporary identity GUTI

Results

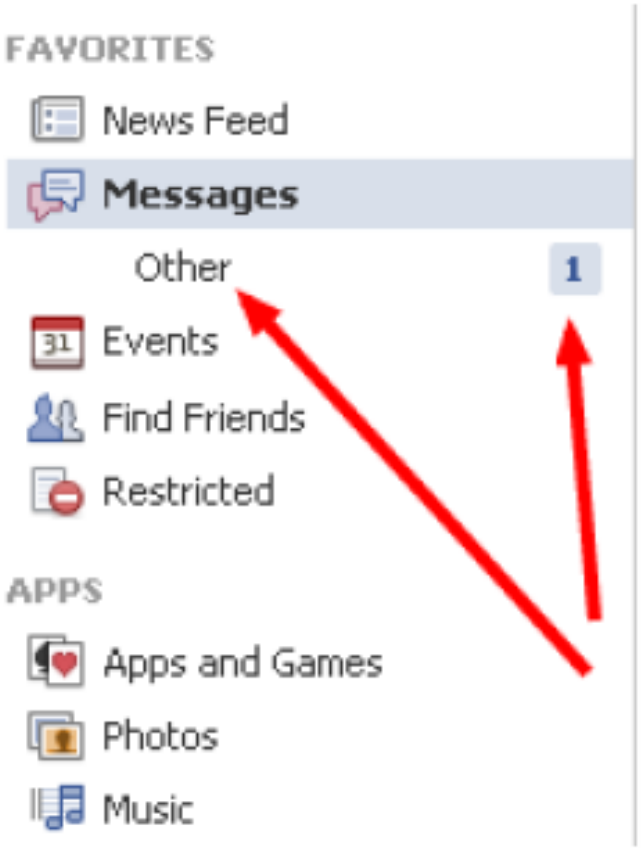
- Observed three major German operators in Berlin
- Sometimes no GUTI changes in up to 3 days
- Sometimes GUTI changed but only by one hexadigit

Semi-passive attack

- Passive monitoring + triggers LTE signaling by ***legitimate*** actions:
  - Call attempt towards the target
  - Sends messages via social media, e.g. Facebook, WhatsApp
- Tries to avoid alerting the target
- Analogous to ***”semi-honest”*** adversary model in crypto

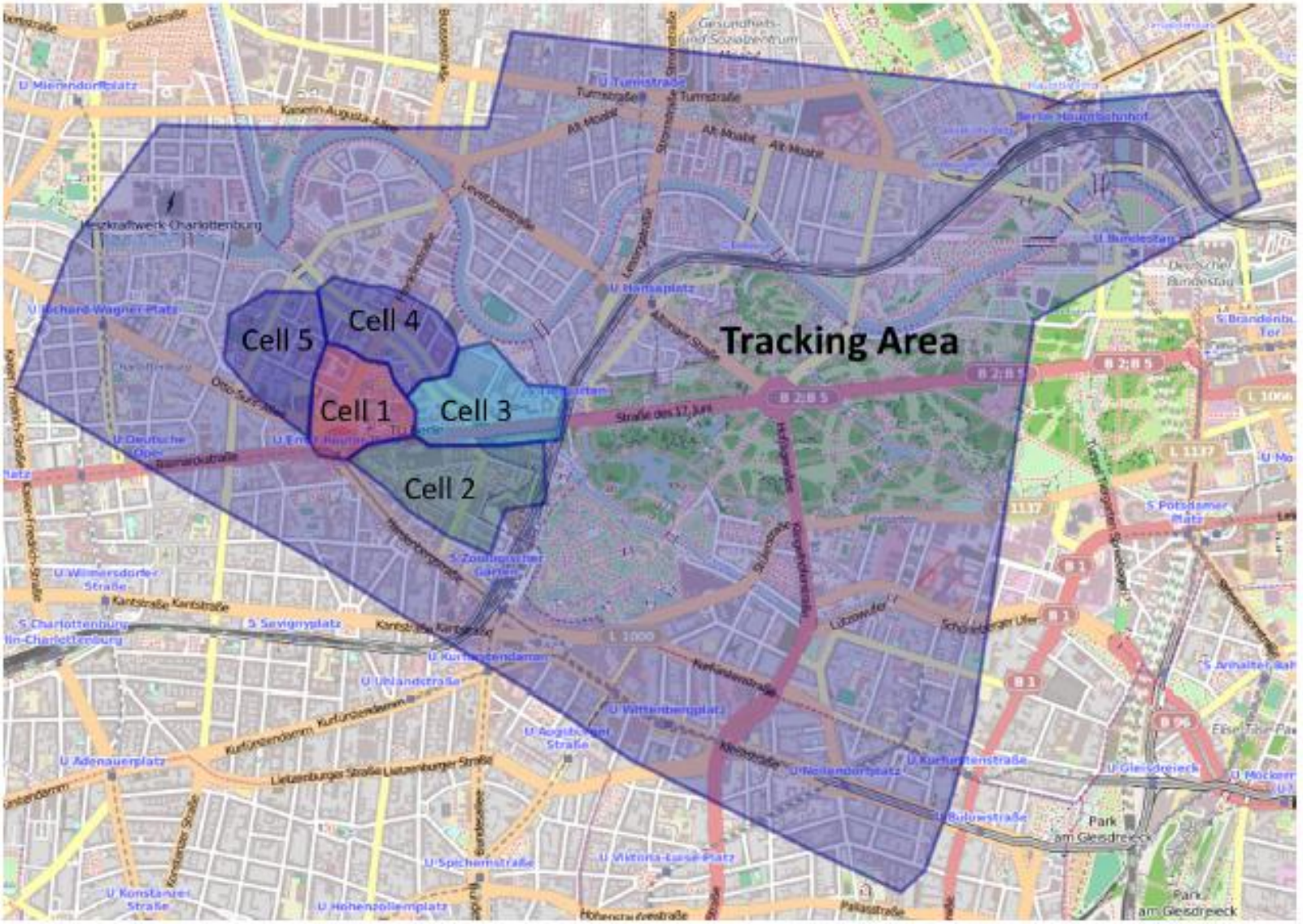
Facebook

- Incoming messages in ***"Other"*** folder often unnoticed



Smart paging

- First try paging ***only*** in the cell where the user was last seen
- If no answer, then try the whole ***tracking area***


Cell 5
Cell 4
Cell 1
Cell 3
Cell 2
Tracking Area

Semi-passive attack: results

- Facebook:
  - 10-20 messages from unknown Facebook user
  - Need to know Facebook ID of the target
  - Smart paging in use → localize in cell level (approx. 2 km^2 in Berlin city)
  - However, sniffer needs to be in the correct cell
- Similar results for VoLTE and WhatsApp

Active attack

- requires ***rogue*** eNodeB:
  - USRP B210 hardware
  - ***openLTE*** software, esp. ***LTE_Fdd_enodeb*** application

UE measurement reports

- Used for troubleshooting and SON purposes
- Some measurements may be sent before signaling security is activated
  - This exception against general principle of protecting all non-broadcast signaling explicitly allowed in specifications
- Measurements include info about neighbor cells etc
  - may even include **GPS** coordinates

Active attack accuracy

- Possible to get the exact location of the target
- However, we did not try this against targets in real networks

Summary of attacks

Adversary Type	Vulnerability	
	Type	Possible tradeoff
Passive	Under specification	(Perceived) security vs availability
Semi-passive	Application software architecture	Security vs functionality
Active	Specification & implementation flaw	(Perceived) security vs availability

General learnings

- Trade-off equilibrium between security and availability/usability/functionality/efficiency may change over time
- Include not only ***safety margins*** in security mechanims but also ***agility***
- Network programmalibility and Cloud computing enable this

Flexible security

- Different domains/verticals have **different needs**
- Network **slices** could help in satisfying these

Flexible security

- Different domains/verticals have **different needs**
- Network **slices** could help in satisfying these
- Example: **car** communications have **always-on** domain-specific security mechanisms

Flexible security

- Different domains/verticals have **different needs**
- Network **slices** could help in satisfying these
- Example: **car** communications have **always-on** domain-specific security mechanisms
- Car communications also require low **latency**

Flexible security

- Different domains/verticals have **different needs**
- Network **slices** could help in satisfying these
- Example: **car** communications have **always-on** domain-specific security mechanisms
- Car communications also require low **latency**

→ would be helpful if generic 5G security is **turned off**

Flexible security

- Same security layer could serve all domains but:

Flexible security

- Same security layer could serve all domains but:
- Domains could have their own domain-wide **policies**

Flexible security

- Same security layer could serve all domains but:
- Domains could have their own domain-wide **policies**
- **W A R N I N G !!!**

  Dangerous to turn off lower layer protection just because application layer claims to have protection

  - especially in **hop-by-hop** model
  - requires specific security for **configuration**

Energy-efficiency

- Driving force in whole 5G
- Difficult to save energy in security mechanisms, e.g. cryptographic algorithms
  - How to optimize bit manipulations?

Energy-efficiency

- Driving force in whole 5G
- Difficult to save energy in security mechanisms, e.g. cryptographic algorithms
  - How to optimize bit manipulations?
- **Lightweight** crypto
  - Seems to save on silicon, not energy (e.g. more rounds with same logical gates)

User plane integrity

- 3G, 4G signalling is protected by **message authentication code**
- User plane **not**
  - Would cause communication and computation **overhead**

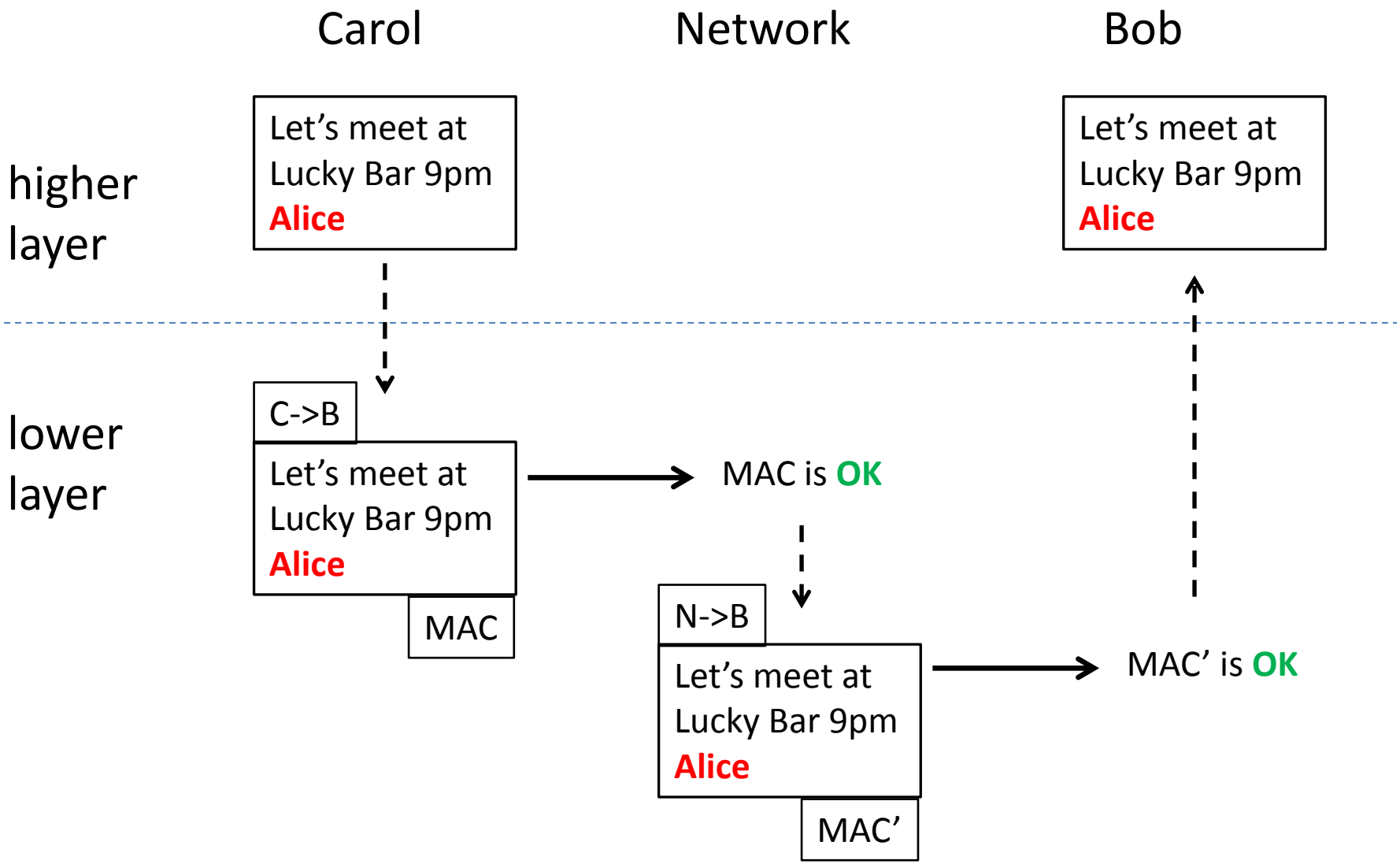
User plane integrity

- 3G, 4G signalling is protected by **message authentication code**
- User plane **not**
  - Would cause communication and computation **overhead**
- In principle, straight-forward to add this in 5G
  - If overhead is tolerable

User plane integrity

- Relates to **end-to-end vs hop-by-hop** discussion
  - Hop-by-hop authentication is tricky

Example


Carol
Network
Bob
higher layer
lower layer
Let's meet at Lucky Bar 9pm Alice
Let's meet at Lucky Bar 9pm Alice
C->B
Let's meet at Lucky Bar 9pm Alice
MAC
MAC is OK
N->B
Let's meet at Lucky Bar 9pm Alice
MAC'
MAC' is OK

Authentication

- In 3G, 4G symmetric key based mechanism for **authentication** and **key agreement** (AKA)
- Arkko et al. (2015) proposed embedding **Diffie-Hellman** to AKA
  - to achieve **perfect forward secrecy**
- Replacing AKA completely by public-key based mechanism would bring benefits:
  - **off-line** authentication, e.g. between devices
  - **non-repudiation**, e.g. for billing

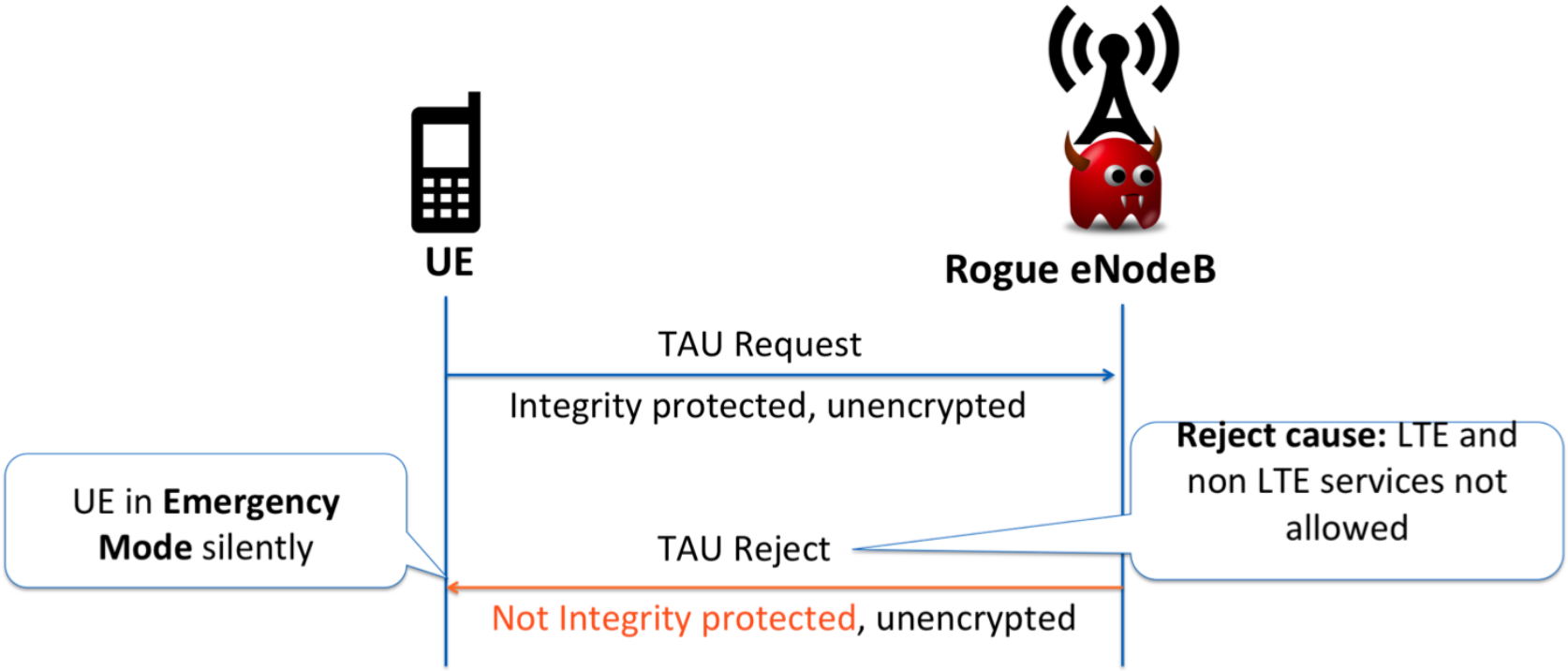
Security set-up

- Related to **flexible security**
- Has to be very fast for some domains, e.g. automobile, e-health
- Has to be done in **secure** manner
  - No room for e.g. **downgrading** attacks

DoS protection

- DoS attacks against **terminal devices** in LTE (Borgaonkar et al., Blackhat EU. November 2015):
  - Downgrade to 3G or GSM
  - Deny all services
  - Deny selected services (block incoming calls)
  - Persistent attacks
  - Recovery requires re-boot or re-insertion of SIM

Example attack in LTE



DoS protection in 5G

- Both network and terminals are potential targets
- Only **lightweight** computations before authentication, esp. on network side
- Re-consideration of availability vs security **trade-offs**

Thanks!
Q & A