ETH zürich

D INFK

Cellular Network Security

Dr. Kari Kostiainen, Prof. Srdjan Capkun

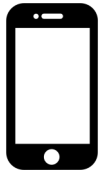
Security of Wireless Networks 2022

History Overview

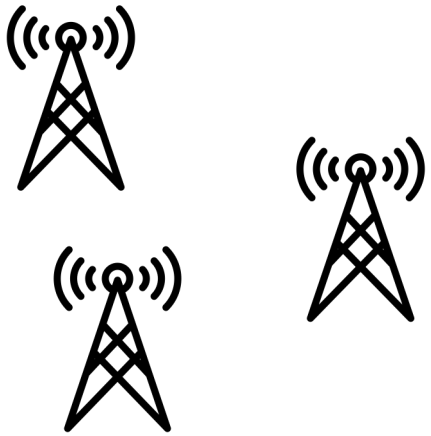
Generation	Protocol	Years in Use (Switzerland)		Theoretical Downlink Speed
1G	No standardization	1980 - 2003	Voice, Circuit switching, Analog	14.4Kbps
2G	GSM, GPRS, Edge	1991 - 2022	SMS, Packet Switching (GPRS, EDGE), Digital	300 Kbps
3G	UMTS, HSPA	1998 - today	Mobile Internet	42 Mbps
4G	LTE, LTE-A	2008 - today	MIMO, Video Streaming	100+ Mbps
5G	NR	2020 - today	Beamforming, VR, Cloud Gaming, Connected Cars	> 1Gbps

Components of a Mobile Network

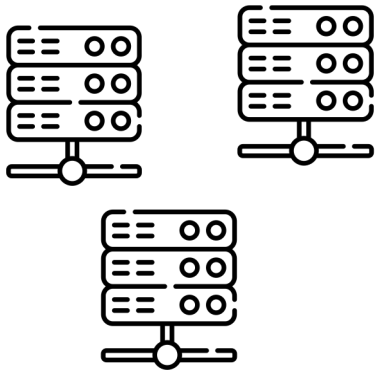
In all evolutions, there are 3 distinct high-level components, named differently and evolved independently



Mobile Phones
Mobile Station (MS)
User Equipment (UE)



Base Stations
Base Transceiver Station (BTS)
Node B
Evolved Node B (eNodeB)
Next Generation Node B (gNodeB)



Core Network
Evolved Packet core (EPC)
Signaling System #7 (SS7)

1G

1G – Example: „C-Netz“ (Germany)

First SIM cards, decoupled phone and subscriber

Capacity for up to 850‘000 subscribers

Handover-Capabilities

Transmission

- Analog FM audio
- Digital FSK control traffic

No Security

- Trivial interception of calls over the air
  - Obscured Voice by inverting in the frequency spectrum

From Rama, CC BY-SA 3.0 fr
https://commons.wikimedia.org/w/index.php?curid=54638770

Standardization

1G networks were country (”C-Netz”) or region specific (NMT / AMPS)

This means no interoperability between networks in different countries (no roaming)

- European Telecommunication Standards Institute (ETSI) was leading in standardizing a **G**lobal **S**ystem for **M**obile Communication (GSM)

  Technical Specifications (TS) available online

- To facilitate world-wide collaboration, 3GPP was founded (3rd Generation Partnership Project)

  Responsible today for standardization of GSM, UMTS, LTE and 5G

ETH zürich

D INFK

2G - GSM

Global System for Mobile Communication

2G – Global System for Mobile Communication (GSM)

Main Goal:

Develop interoperable system on a global scale.

Voice transmission is **digital** (64kbit/s PCM) and done over **circuit switched** connections.

A call may be routed via different base stations and core network components.

The new mobile switching center (**MSC**) is the component responsible for:

- Call establishment and call routing (+ SMS)
- Authentication of subscribers
- Keep an up-to-date location for each subscriber & initiate handover procedures

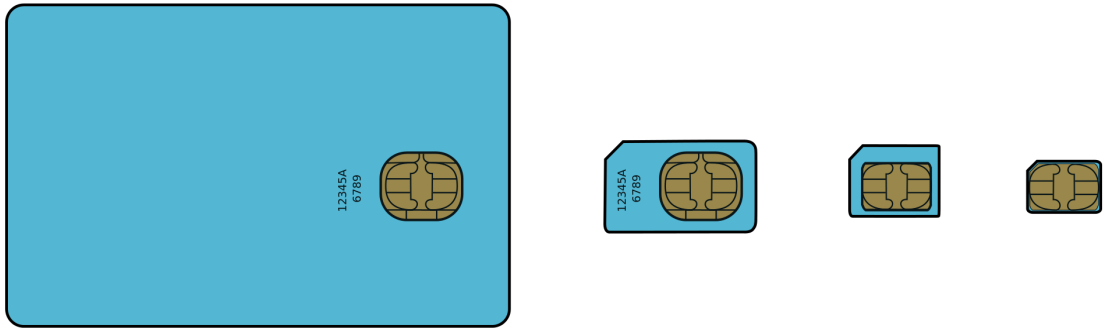
2G – Security

Main Goal

Prevent the misuse of a subscriber identity by a third party

Key Distribution

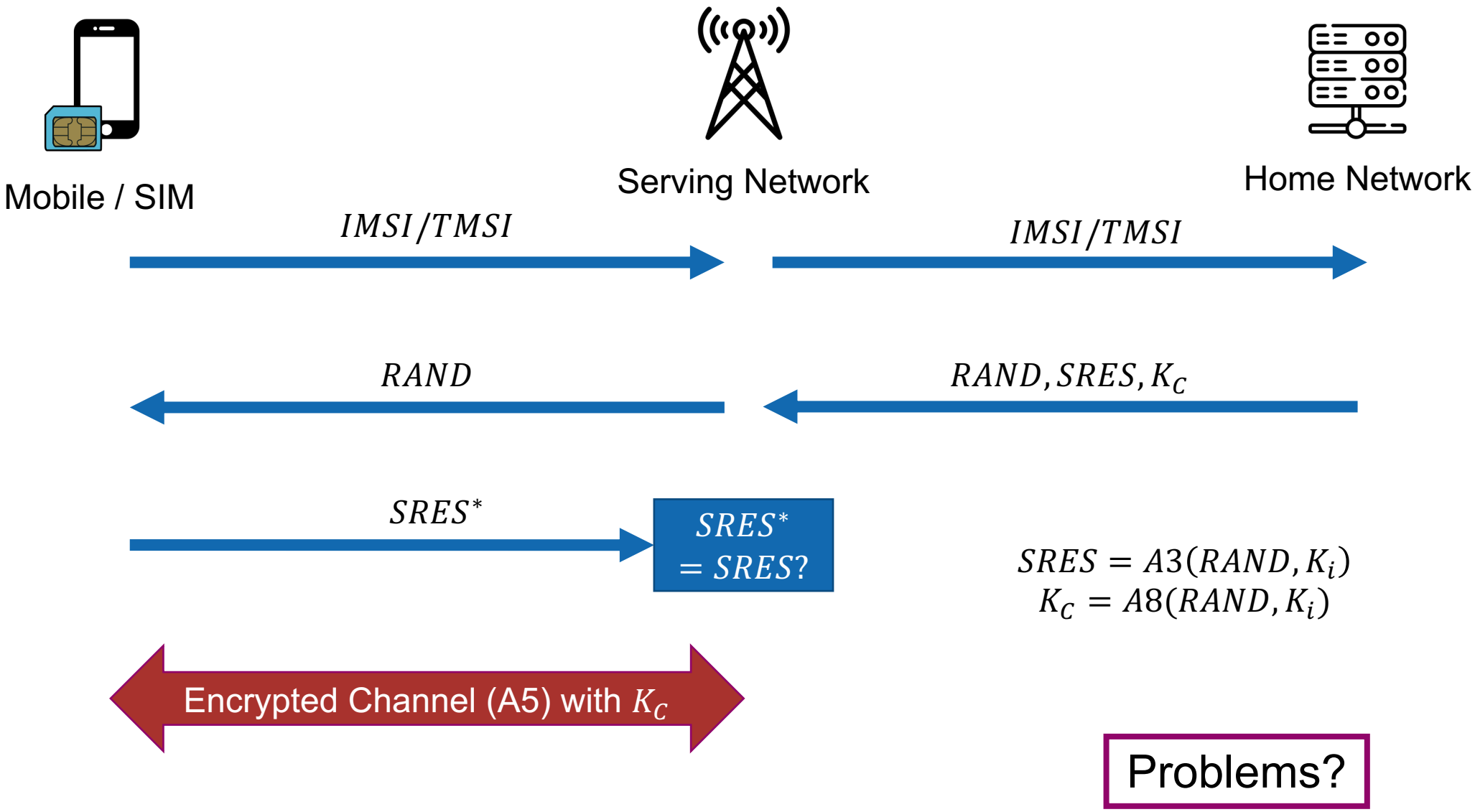
Every subscriber receives a physical **S**ubscriber **I**dentity **M**odule (SIM card), containing parameters of the subscriber and a **shared key** K_i . This key is physically protected and cannot be easily extracted.



User Identifiers in 2G, 3G, 4G

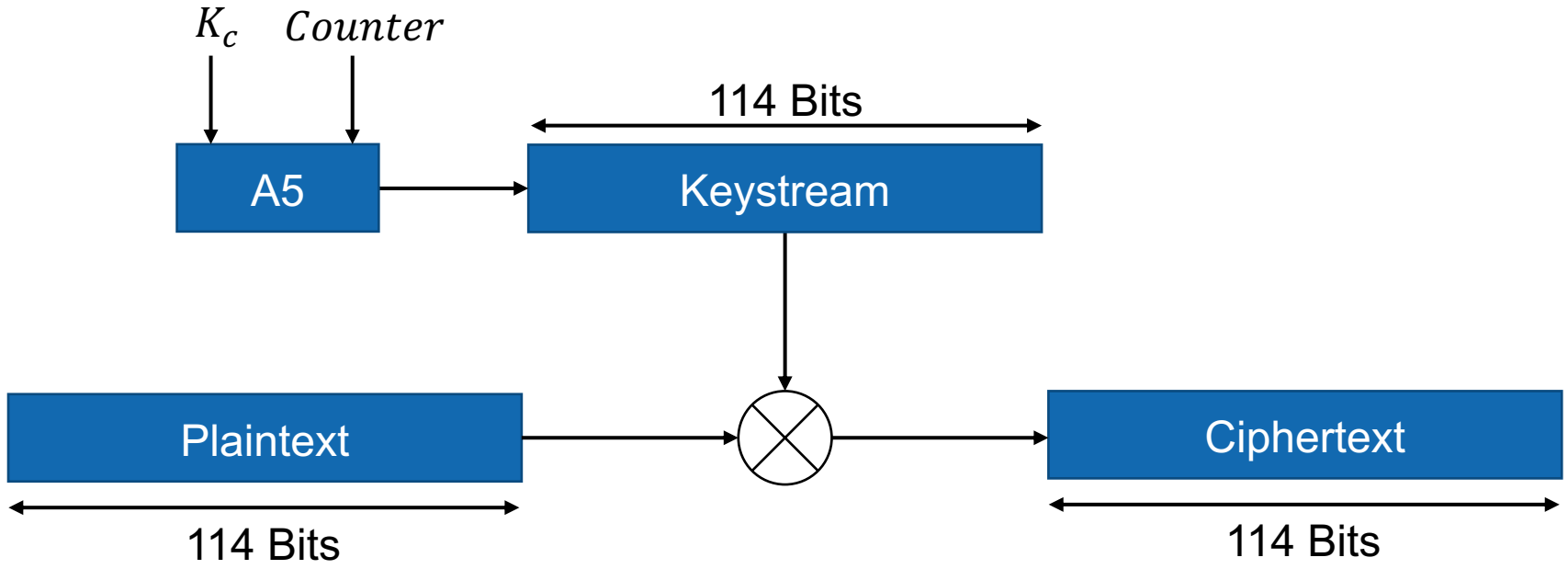
- Mobile provides its identity (**IMSI**) before authentication
  - Persistent ID which enables unique identification of users
  - Risk: Allows Long-Term Tracking
- Operator assigns **temporary** identity (**TMSI**)
  - Changes according to the TMSI update policy
  - If it is never updated, can serve as persistent ID as well
  - IMSI should never be sent again in cleartext, only after encryption is set up
- IMSI used again
  - Roaming (different network)
  - TMSI lost (phone crash, mobile network problem)
  - The network can **always** ask for the IMSI → When is this a problem?

2G – Authentication & Key Agreement (AKA) Procedure

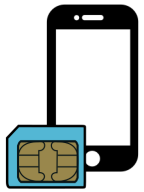


2G – Encryption with A5

A5 defines a ***class*** of encryption algorithms of which an operator may choose one



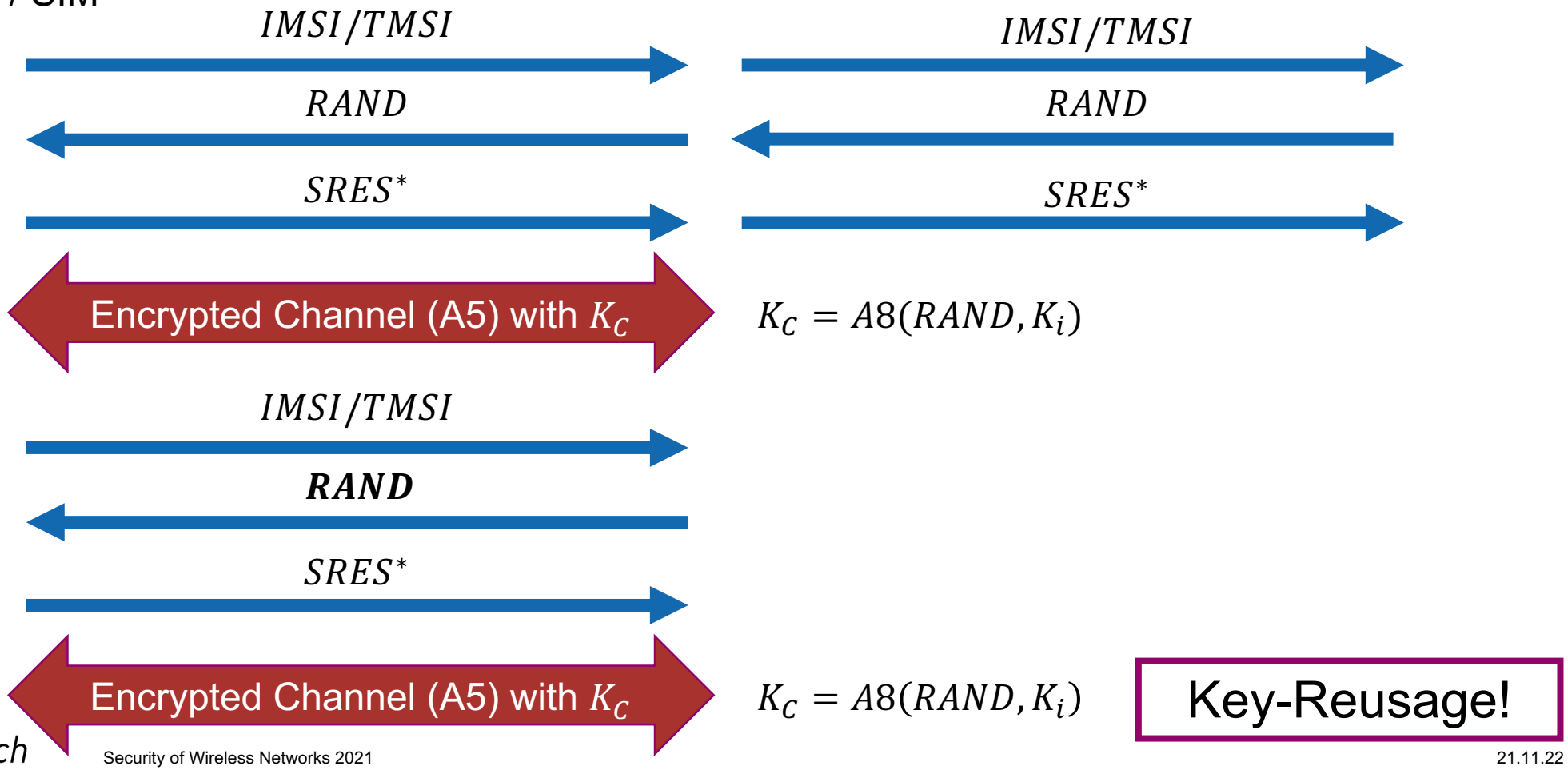
2G – Key-Reinstallation Attack



Mobile / SIM

Attacker

Serving Network



Key-Reusage!

2G – Attacks on Authentication and Key Exchange Procedure

2G has no mutual authentication (Network does not authenticate itself)

Fake Base Station Attacks

→ Possibility to eavesdrop on the communication by e.g., choosing null encryption

→ IMSI Catcher

2G is vulnerable to Key-Reinstallation via a Replay Attack on $RAND$

$$C_1 \otimes C_2 = (M_1 \oplus K) \oplus (M_2 \oplus K) = M_1 \oplus M_2$$

→ Why were these attacks not considered in the design phase?

2G – User Data Transport

1. In GSM, data is transported in 144bit frames with a rate of up to 14.4kbit/s
   - Digital Voice (PCM) for telephony

2. With GPRS & EDGE (both extensions to GSM), data rates of up to 170kbit/s and 270kbit/s are possible
   - Necessary addition, since GSM alone is *circuit-switched*

→ Both protocols have **no integrity protection** applied, although they are encrypted. Why?

2G – Security Algorithms

- Operators choose three algorithms:
  - A3 algorithm for authentication during AKA
    - Initially COMP128 keyed hash, but operators have free hand
    - COMP128 broken
  - A5 algorithm for encryption of data
    - Three options for operators: A5/1, A5/2, A5/3, **A5/4 (safe as of 2021, rest broken)**
    - Initially secret but leaked in mid 90's
  - A8 algorithm for key derivation during AKA
    - Initially COMP128 keyed hash as well
- A3, A5, A8 are just fancy names for authentication, encryption, and key derivation

2G – Summary of Flaws

1. Active Fake Base Station Attacks possible
2. Encryption is only on the Radio Access Network (Core is unencrypted)
3. Encryption itself is optional
4. On old networks: weak cryptographic primitives
5. Key Re-Installation via Replay Attacks is possible
6. No Data Integrity
7. Serving Networks (Roaming) could authenticate the user in any way they liked (or also not)

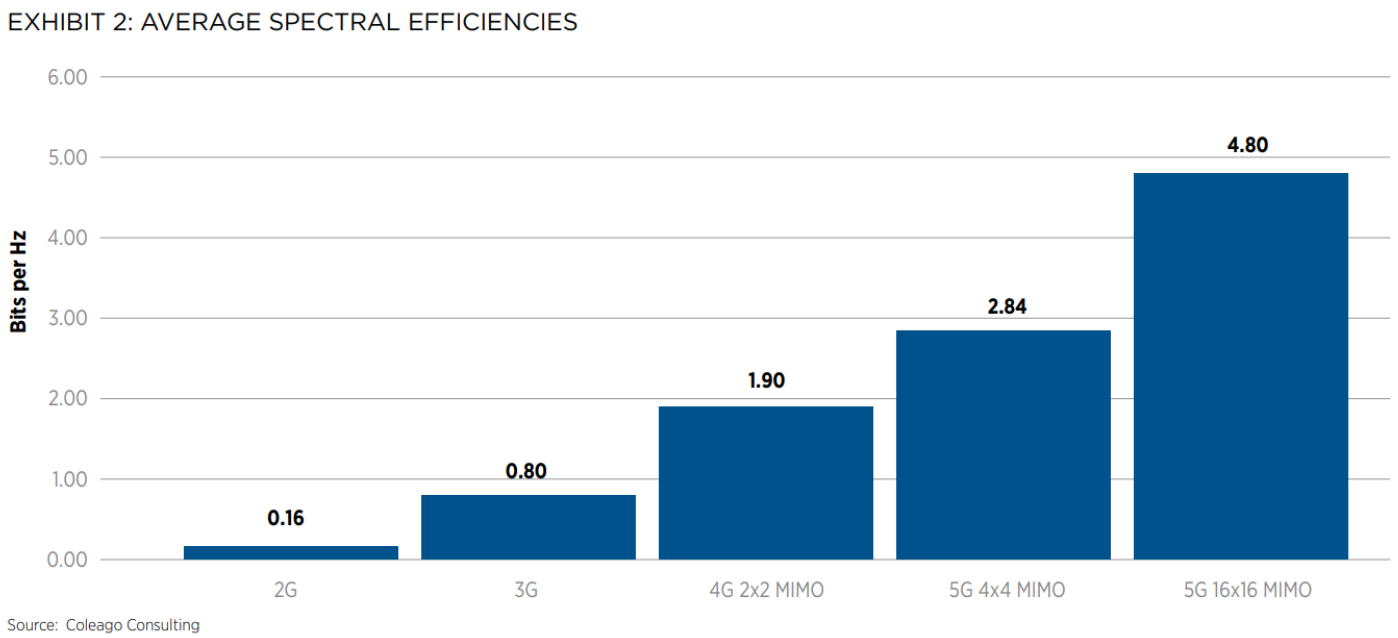
2G – Still Active Research

1. E.g., Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2 by Beierle et al.
    1. Problem in chosen initial state
        1. Reduction from 64-bits of security to 40-bits
    2. Random states do not have this problem
        1. Export laws? NSA?
2. Why should we continue doing research on these old systems?

Discussion – Situation Today

Older systems, such as elevators, IoT devices and home security systems connect even today via 2G.

Given that modern phones connect to modern systems (4G / 5G), why are operators shutting down their 2G networks?



ETH zürich

D INFK

3G - UMTS

Universal Mobile Telecommunications System

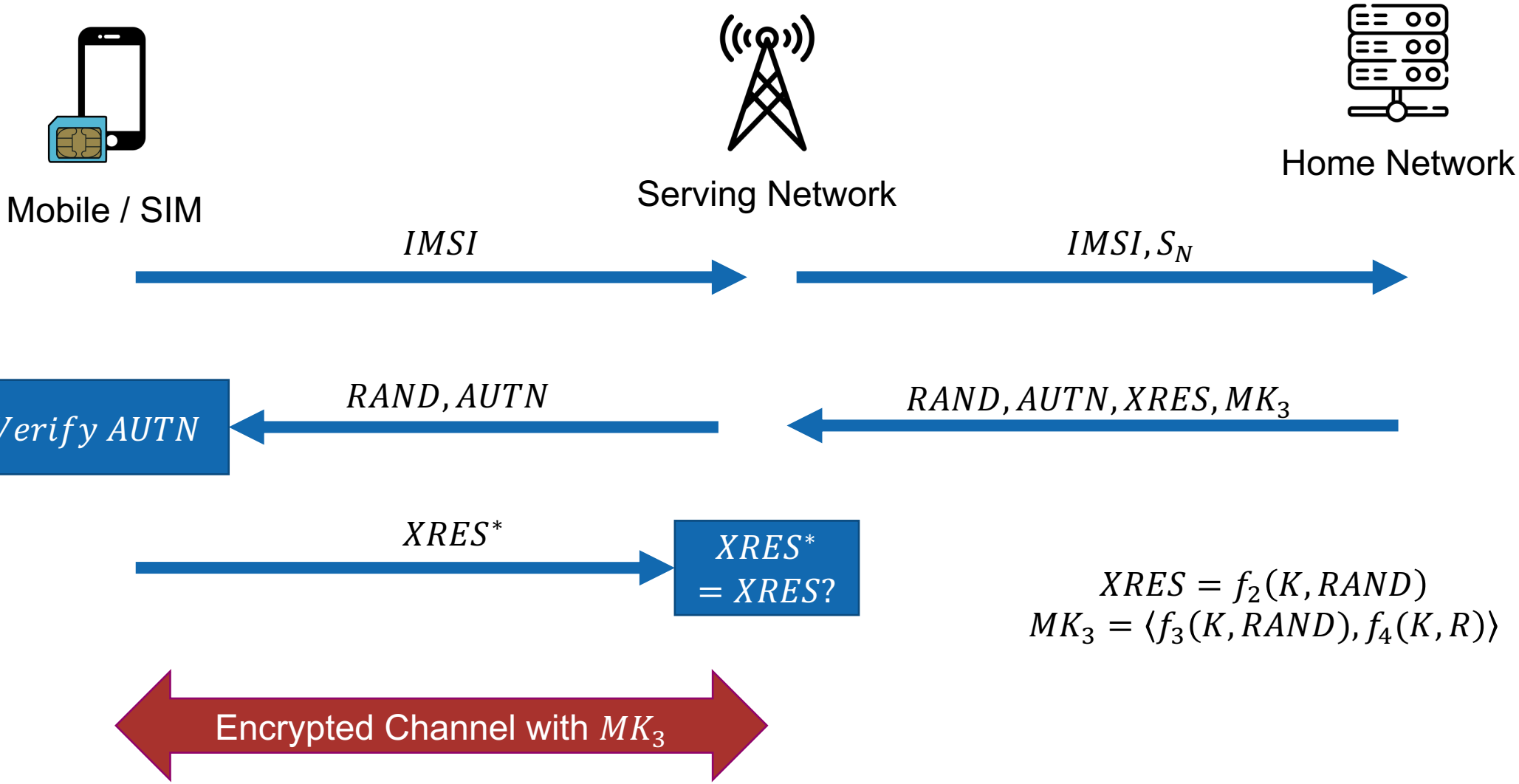
3G – Universal Mobile Telecommunications System (UMTS)

The third-generation wireless telecommunication system is the **U**niversal **M**obile **T**elecommunications **S**ystem.

Faster baseband chips enabled faster transmission rates due to more complex and efficient modulation schemes: **W-CDMA (**wideband code-division multiple access, with a separate code for each user).

Problem: All Users send on the same frequency

3G – Authentication & Key Agreement (AKA) Procedure



$$XRES = f_2(K, RAND)$$
$$MK_3 = \langle f_3(K, RAND), f_4(K, R) \rangle$$

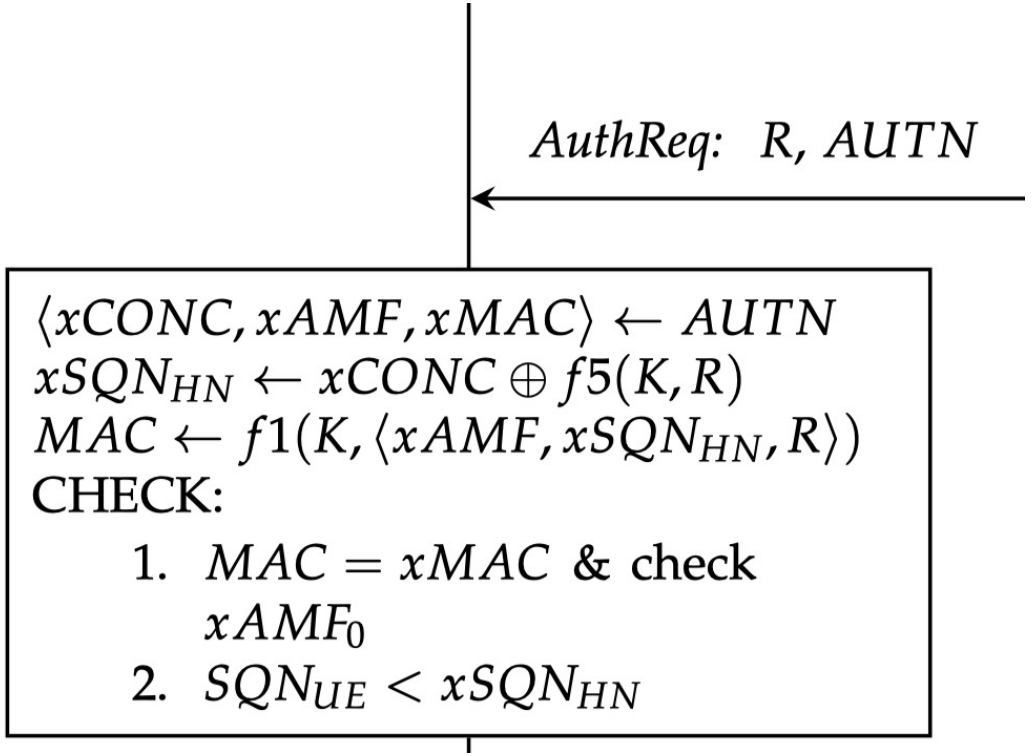
3G – Authentication Procedure

AUTN Verification

Verify that:

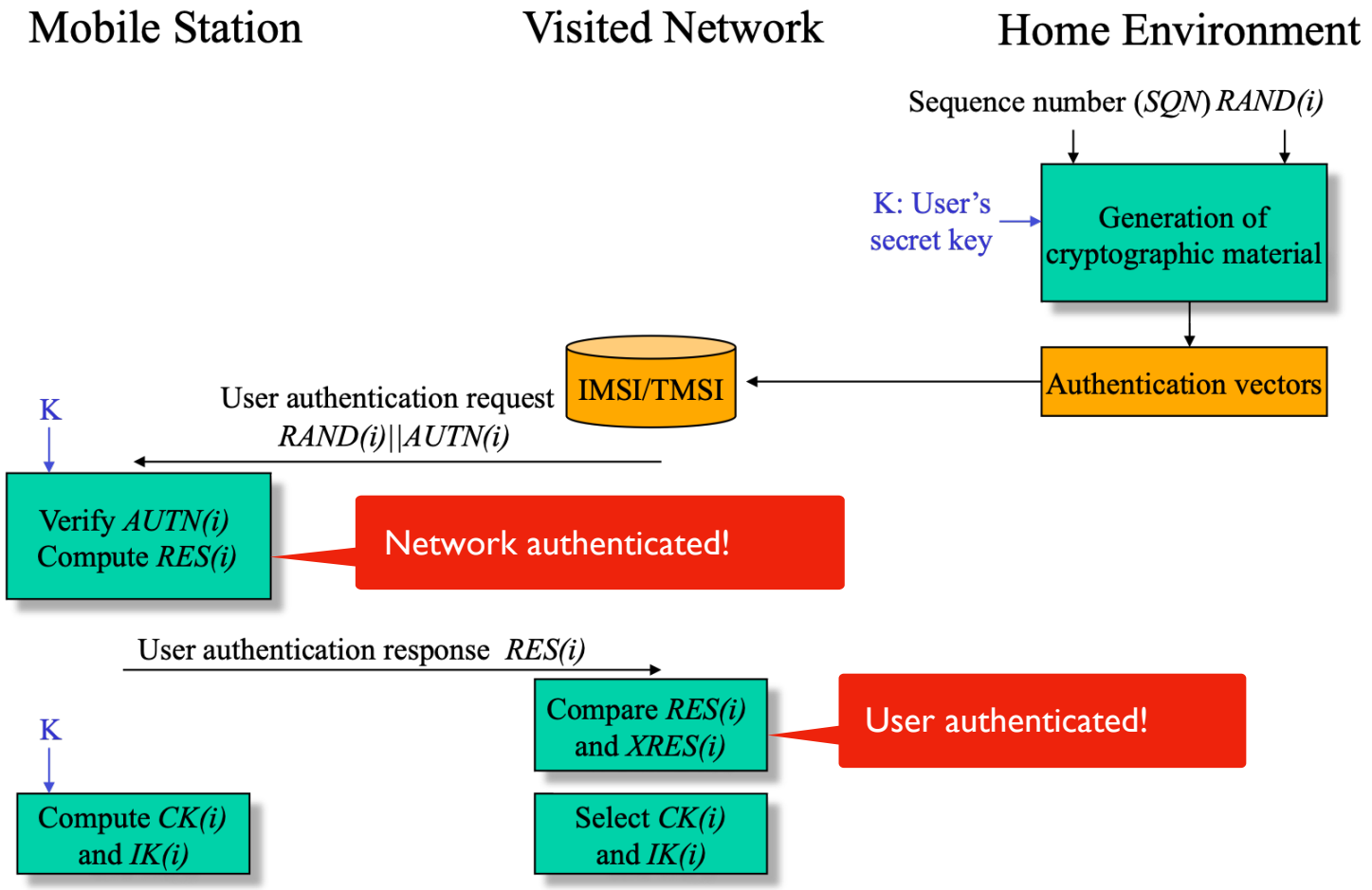
1. **MAC** is correctly authenticating the message
   → No network-impersonating attacks

2. **SQN** is correct ($SQN_{UE} < SQN_{HN}$)
   → No replay attacks

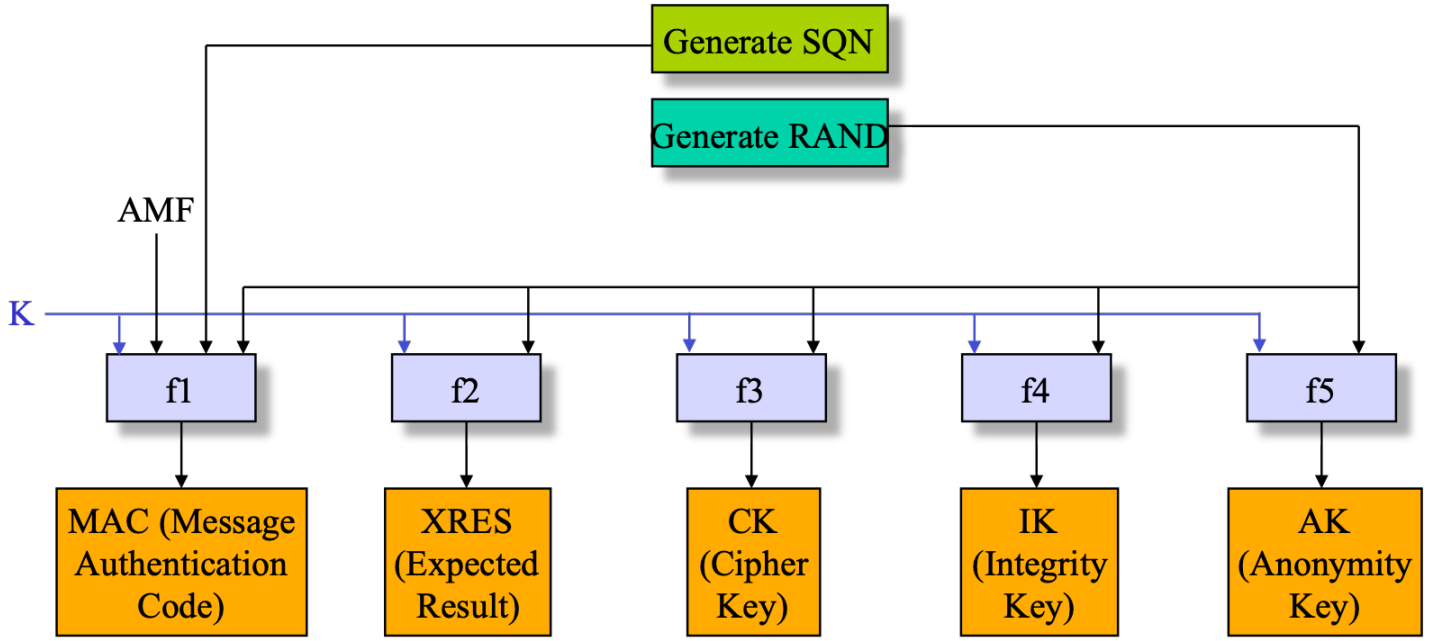


Rellstab, Angela. "Formalizing and Verifying Generations of AKA Protocols," 2019. https://doi.org/10.3929/ethz-b-000372339

UMTS Authentication (with a Visited Network)



Generation of Authentication Vectors (by the Home Environment)

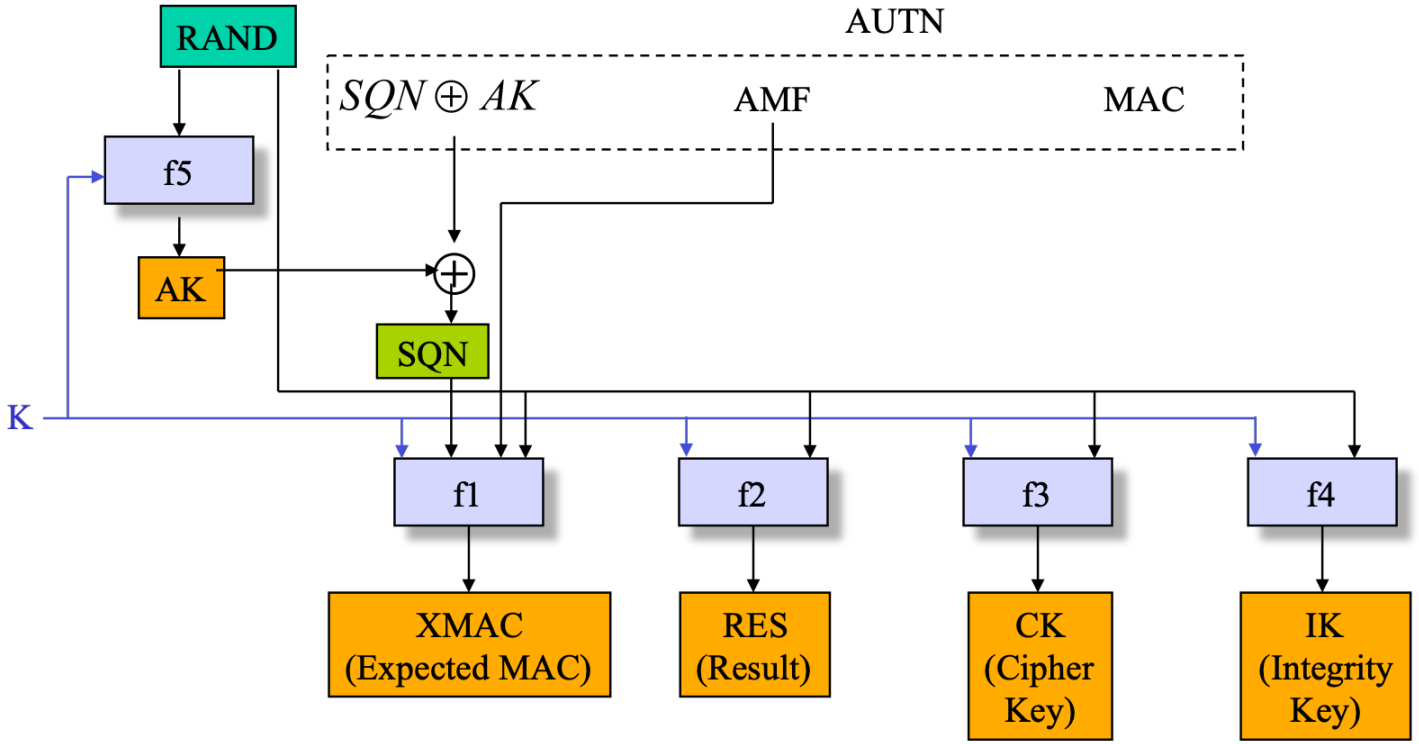


Authentication token: AUTN = (SQN⊕AK)|| AMF|| MAC

Authentication vector: AV = RAND|| XRES ||CK || IK || AUTN

AMF: Authentication and Key Management Field

User Authentication Functions in USIM



- Verify MAC = XMAC
- Verify that SQN is in the correct range

USIM: User Services Identity Module

3G – Cryptographic Primitives for the AKA Procedure

1. Functions need to be implemented in the USIM and the Home Network

   → Therefore, they do **not** need to be standardized, the functions can be freely implemented by the operator

2. **MILENAGE** was later chosen as a set of informative example algorithms, based on AES

3G – Cryptographic Primitives on the Radio Link

1. Decision to choose **public** algorithms (instead of ”secret” ones, like in 2G)

2. But which?
   - AES candidate was not yet chosen
   - Simply waiting was not an option

3. KASUMI as core building-block was specifically built for 3G, using an enhanced “MISTY”
   - Fast software & hardware implementation possible
   - Used in both encryption and integrity protection algorithms (UEA1, UIA1)

4. SNOW superseded KASUMI (UEA2, UIA2)

ETH zürich

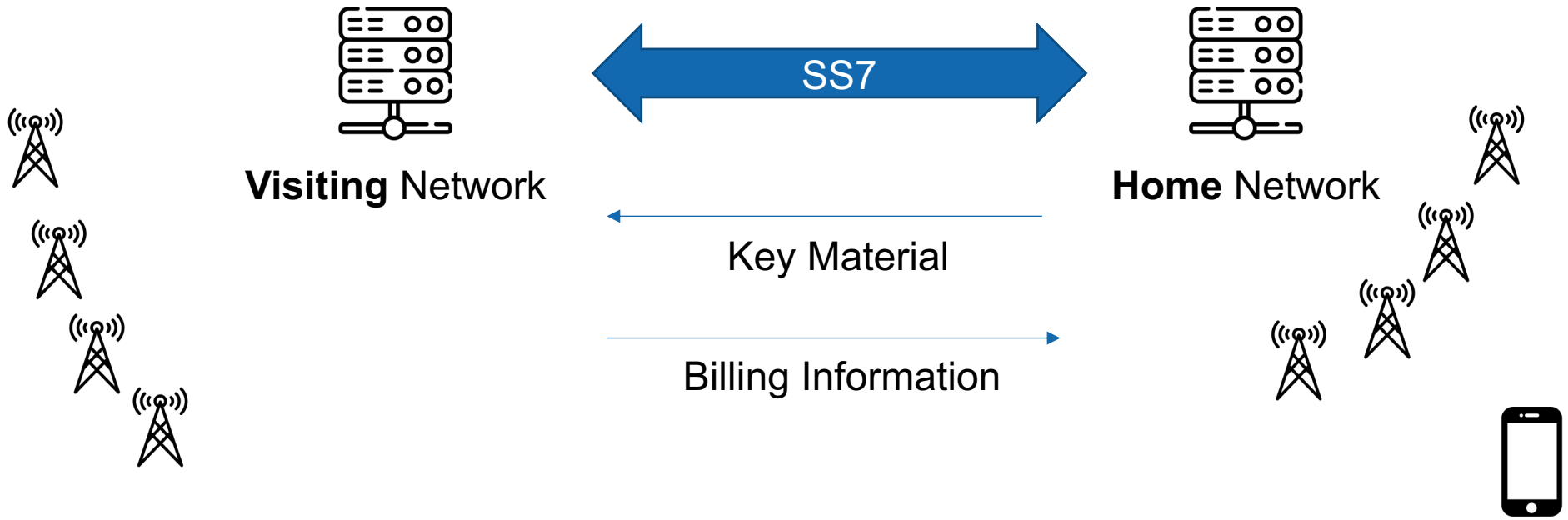
D INFK

Signaling System #7

Interconnecting 2G&3G Mobile Networks

2G&3G – Interconnecting Networks

Mobile Networks are **global** networks, supporting *roaming* of subscribers



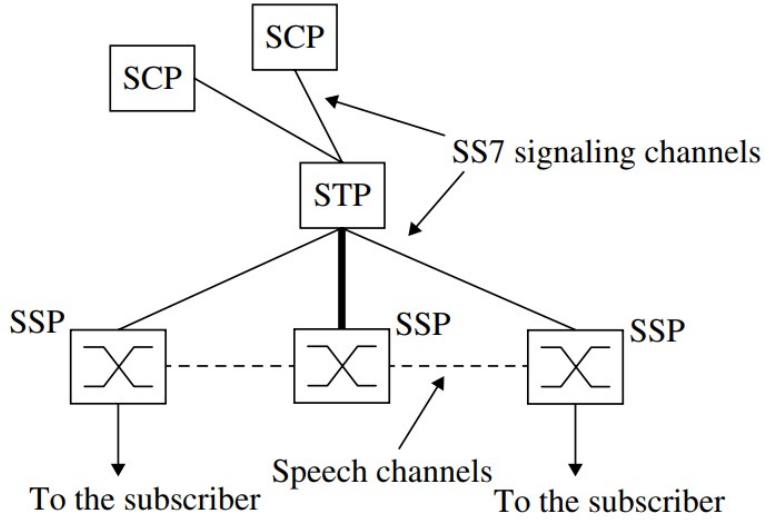
Signaling System #7 (SS7)

1. SS7 is based on **mutual trust**, all operators trust each other

2. In 2020, **6'255 active** signaling points (participants) were registered[1]

3. Messages can be exchanged between any participants, e.g., via roaming hubs

4. No special hardware required, only a subscription to SS7 (obtained e.g., from a roaming hub)



[1] https://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-Q.708B-2020-PDF-E.pdf

SS7 – Some Interesting Request Types

Read Data from HLR

- sendRoutingInfoForSM(ISMI / MSISDN) → Pointer to Current Visiting Network (VLR)

Read Data from VLR

- provideSubscriberInfo(IMSI) → SubscriberInfo
- provideSubscriberLocation(IMSI / MSISDN) → Estimate of Location
- sendIdentification(TMSI) → IMSI, Security Context

Write Data

- To VLR: insertSubscriberData(IMSI, Callback Address, …)
- To HLR: updateLocation(ISMI, VLR Number)

SS7 Attacks – Coarse Location Tracking

provideSubscriberInfo(IMSI) → SubscriberInfo

SubscriberInfo contains a **lot** of data:

- e.g., IMEI, Current Cell ID → What can you do with this kind of data?

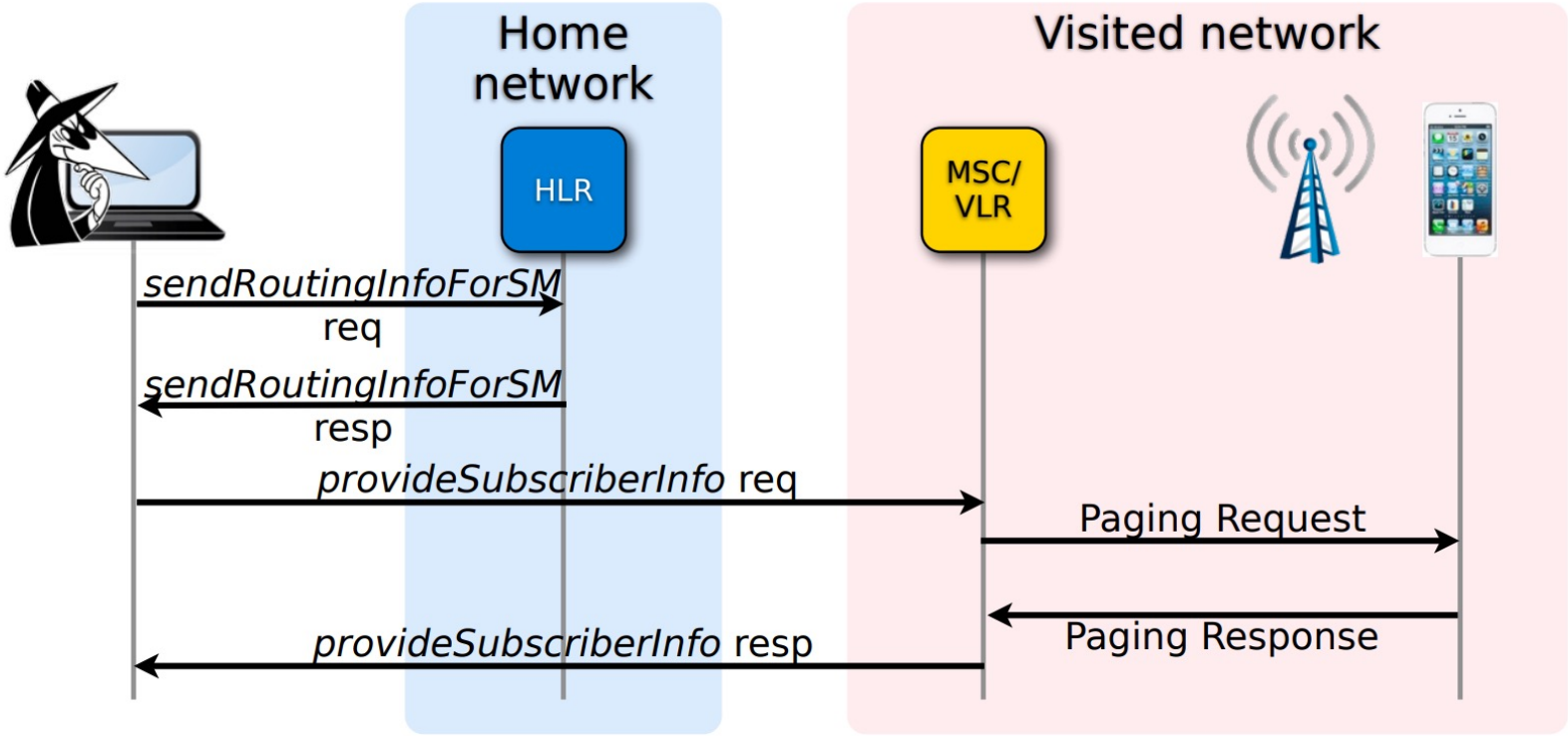


Figure: Engel, Tobias. "SS7: Locate. Track. Manipulate."
https://media.ccc.de/v/31c3_-_6249_-_en_-_saal_1_-_201412271715_-_ss7_locate_track_manipulate_-_tobias_engel

SS7 Attacks – Precise Location Tracking

provideSubscriberLocation(IMSI / MSISDN) → Estimate of Location

Even more precise attack:

- Ask the smart phone to provide its location, obtained via GPS or E-OTD

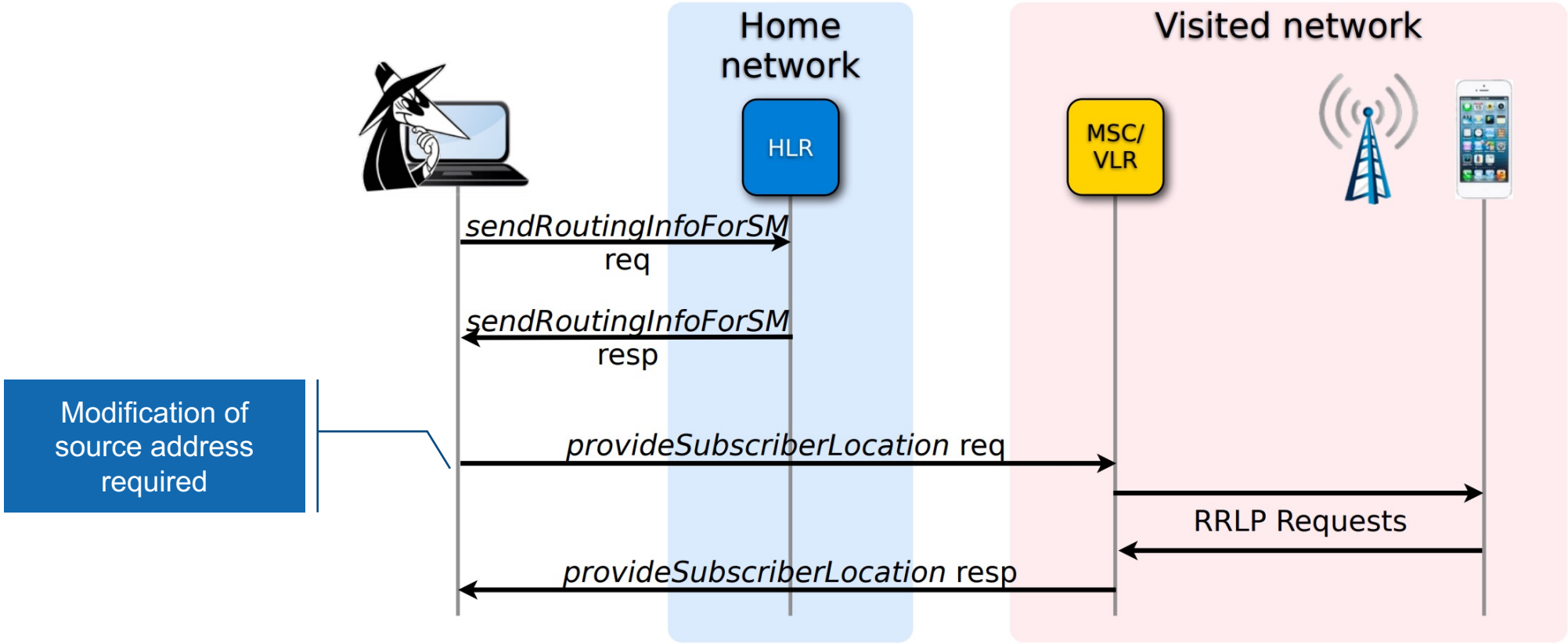


Figure: Engel, Tobias. "SS7: Locate. Track. Manipulate."
https://media.ccc.de/v/31c3_-_6249_-_en_-_saal_1_-_201412271715_-_ss7_locate_track_manipulate_-_tobias_engel

SS7 Attacks – Intercepting Calls

Write to VLR: insertSubscriberData(IMSI, Callback Address, …)

1. Register Callback at VLR
   - Example: “notify me whenever the subscriber wants to make a call”
     Use: *reroute a call to a different number.*

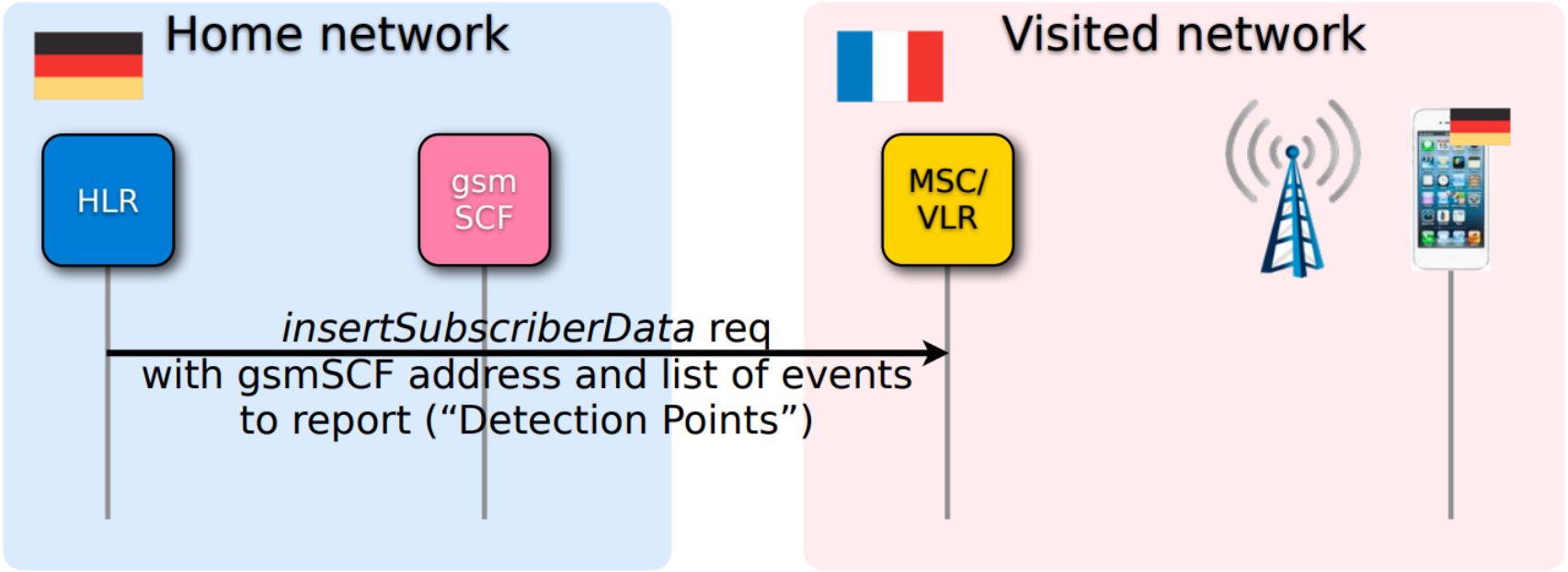


Figure: Engel, Tobias. “SS7: Locate. Track. Manipulate.”
https://media.ccc.de/v/31c3_-_6249_-_en_-_saal_1_-_201412271715_-_ss7_locate_track_manipulate_-_tobias_engel

SS7 Attacks – Intercepting Calls

Write to VLR: insertSubscriberData(IMSI, Callback Address, …)

2. Subscriber issues a call to a German Local number “031…”
   - Callback Function rewrites this to “+49 31 …”

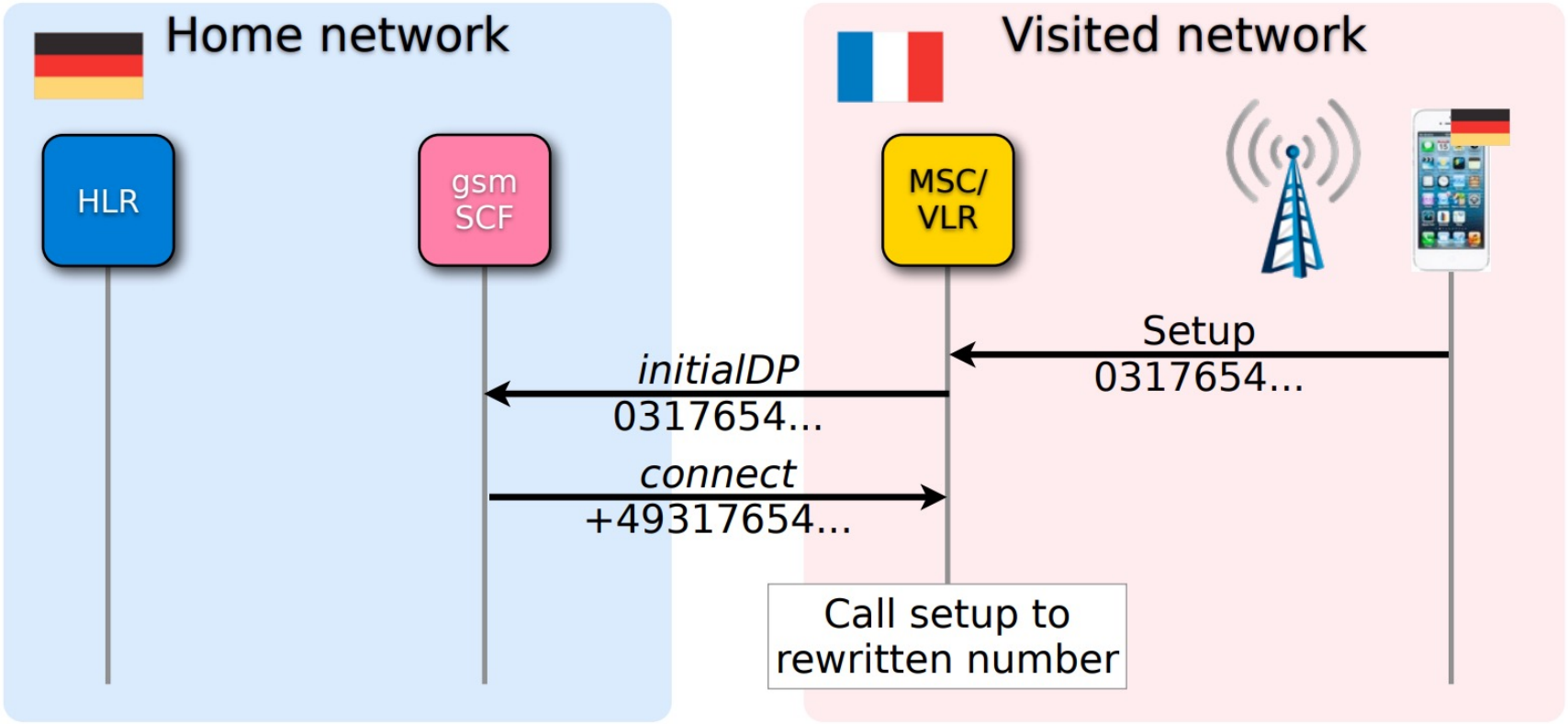


Figure: Engel, Tobias. “SS7: Locate. Track. Manipulate.”
https://media.ccc.de/v/31c3_-_6249_-_en_-_saal_1_-_201412271715_-_ss7_locate_track_manipulate_-_tobias_engel

SS7 Attacks – Intercepting Calls

Write to VLR: insertSubscriberData(IMSI, Callback Address, …)

1. An attacker can abuse this functionality to register his own callback handler, rewriting the phone number to one under his control.
2. The attacker can then forward the call to the original number and record the conversation.

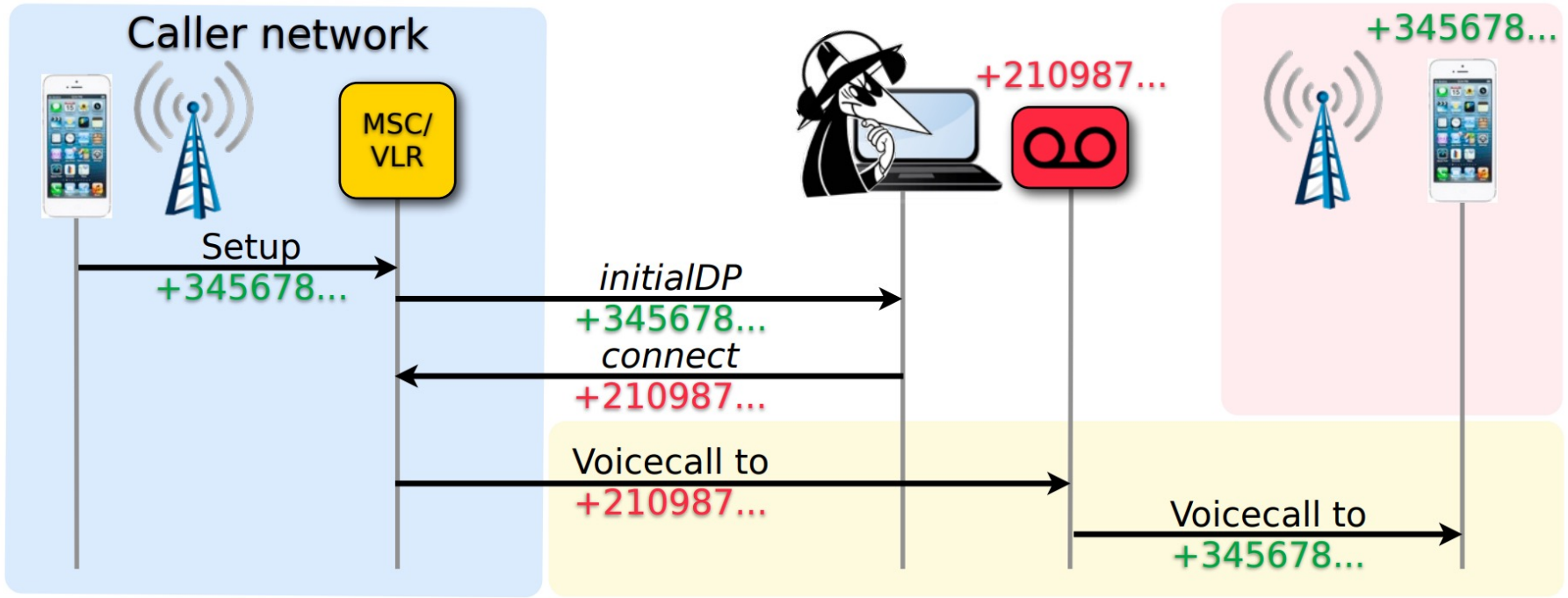


Figure: Engel, Tobias. “SS7: Locate. Track. Manipulate.”
https://media.ccc.de/v/31c3_-_6249_-_en_-_saal_1_-_201412271715_-_ss7_locate_track_manipulate_-_tobias_engel

SS7 Attacks – Intercepting SMS

Write to HLR: updateLocation(ISMI, VLR Number)

In similar fashion to the call interception, the attacker can update the current location of a subscriber by updating its location at the HLR.

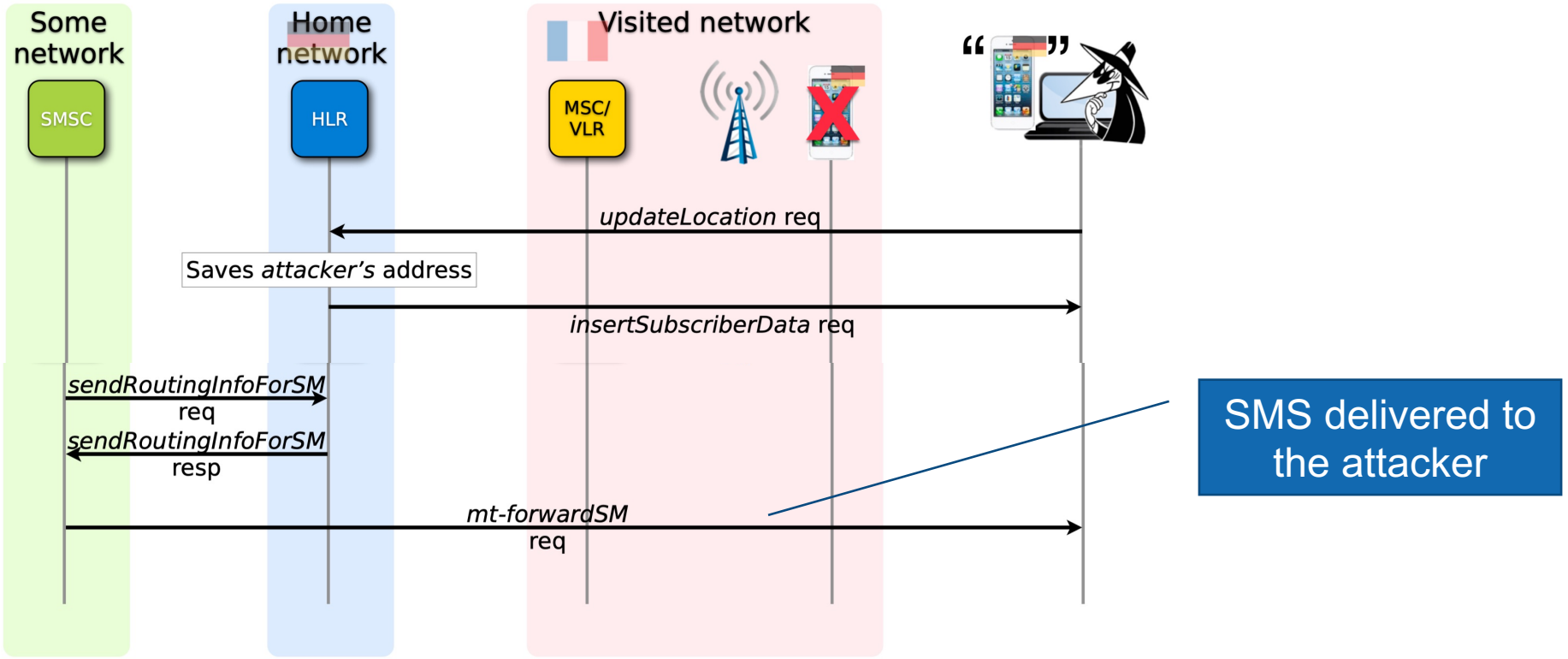


Figure: Engel, Tobias. "SS7: Locate. Track. Manipulate."
https://media.ccc.de/v/31c3_-_6249_-_en_-_saal_1_-_201412271715_-_ss7_locate_track_manipulate_-_tobias_engel

ETH zürich

D INFK

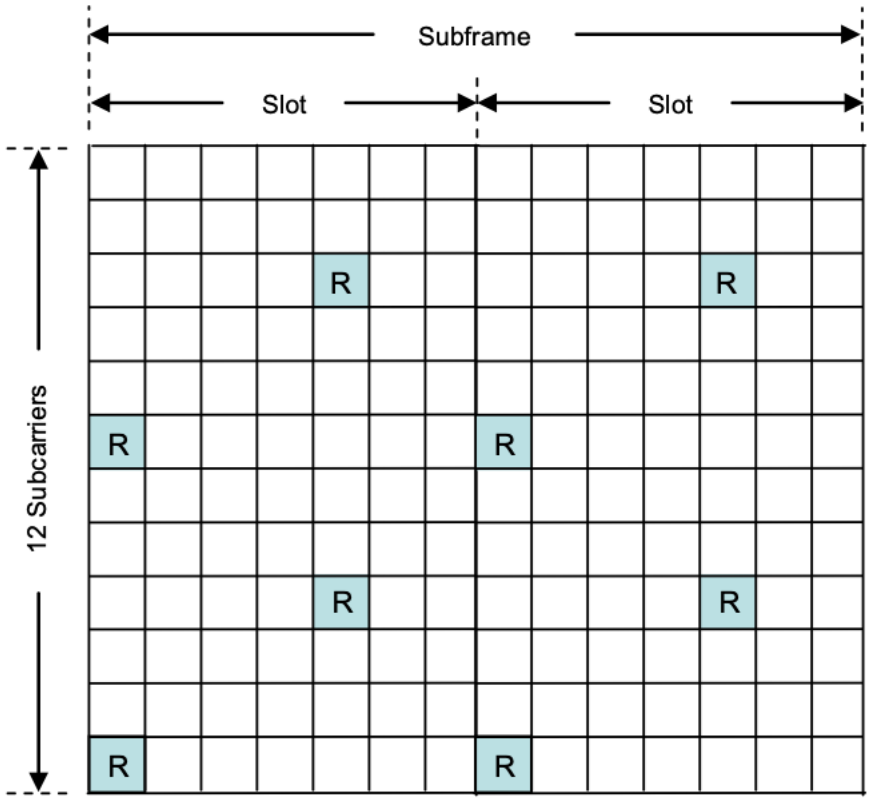
4G - LTE

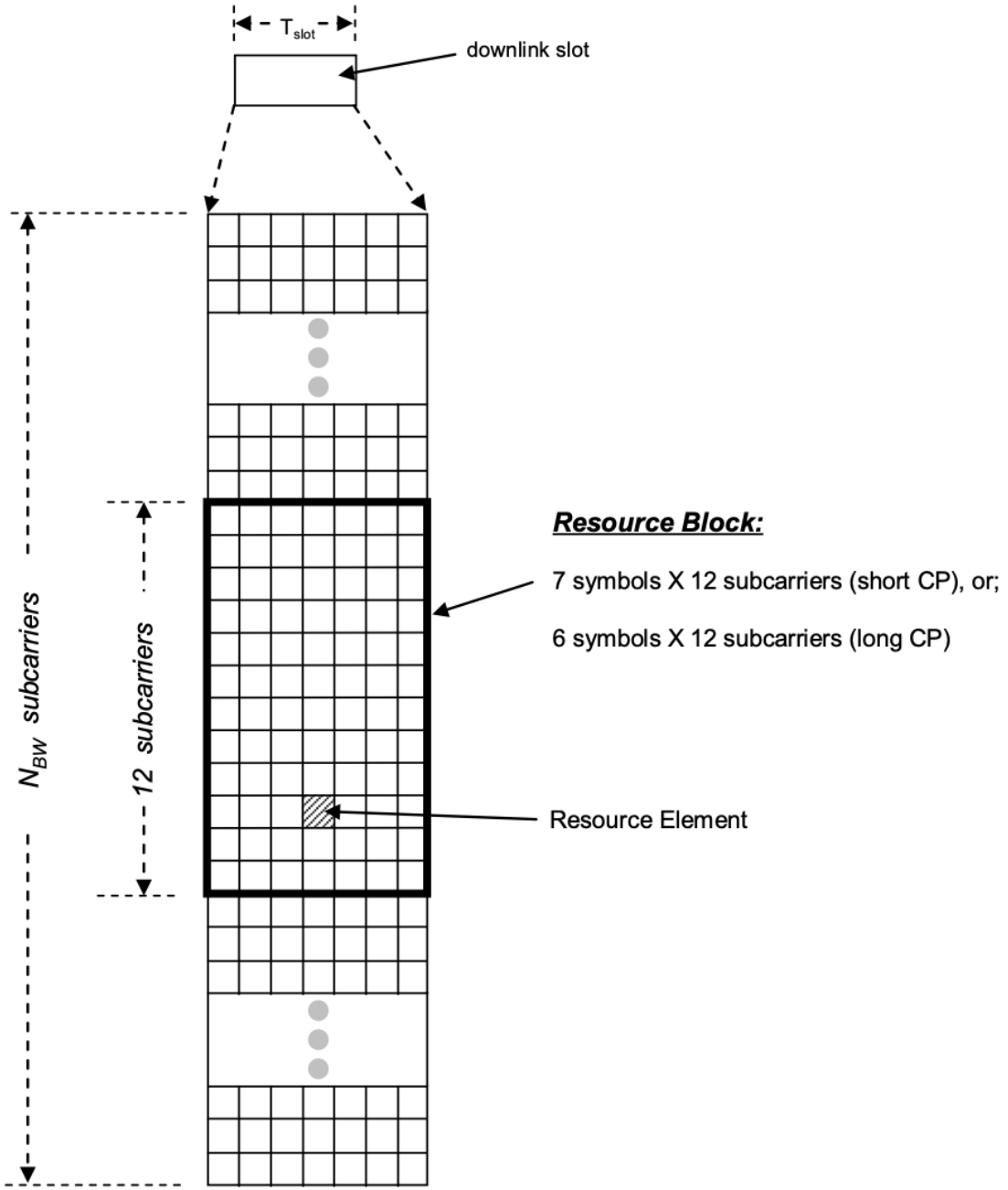
Long-Term Evolution

4G – Long-Term Evolution (LTE)

1. Introduced around 2008
2. Updated architecture
    1. Fully packet-switched
    2. Core network called Evolved Packet Core (EPC)
    3. Radio network called Evolved-UTRAN (E-UTRAN)
    4. Interoperable with legacy systems
3. New physical layer
    1. Orthogonal frequency division multiplex (**OFDM**)
    2. Multiple antenna techniques like **MIMO**
    3. 300 Mbps downlink, 70 Mbps uplink, 5ms latency

4G – Resource Grid

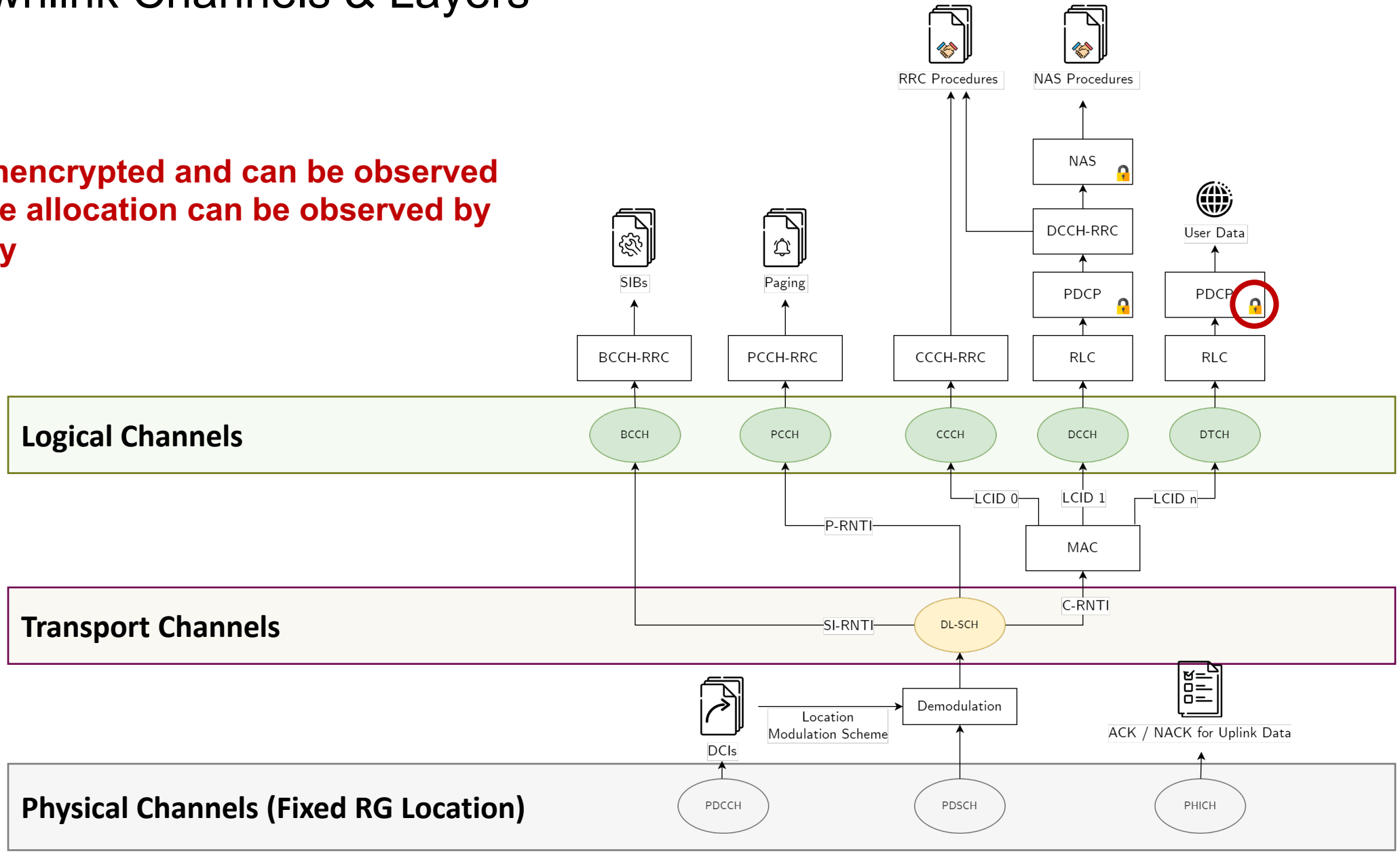




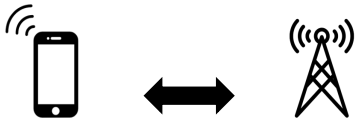
Reference signals are used for channel correction (in blue), the rest occupied by channels

4G – Downlink Channels & Layers

Phy layer unencrypted and can be observed i.e., resource allocation can be observed by an adversary

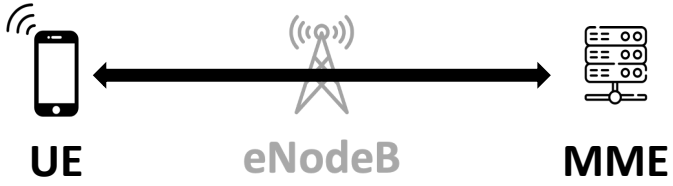


4G – From Power-Off to Internet Access



(1) RRC Setup Procedure

First, there is a connection established with the eNodeB via a RRC Setup Procedure.



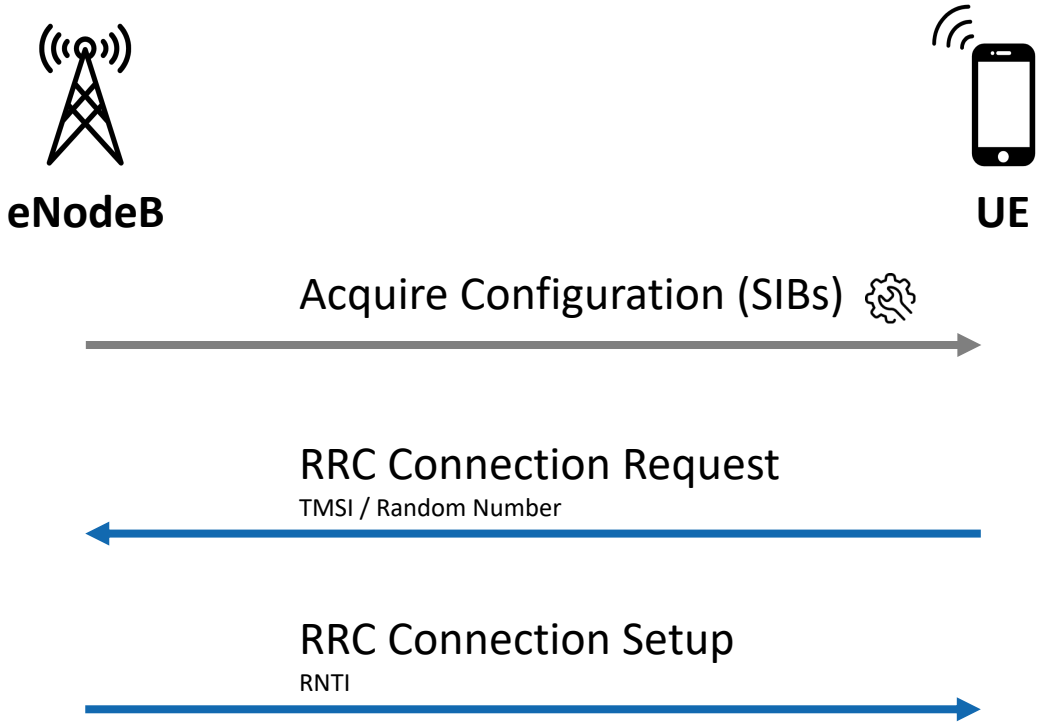
(2) NAS Attachment Procedure

Then, the UE registers in the Core Network at the Mobility Management Entity. To do so, it follows these sub-procedures:

1. Identification
2. Authentication & Key Agreement
3. Security

4G – From Power-Off to Internet Access

(1) RRC Setup Procedure

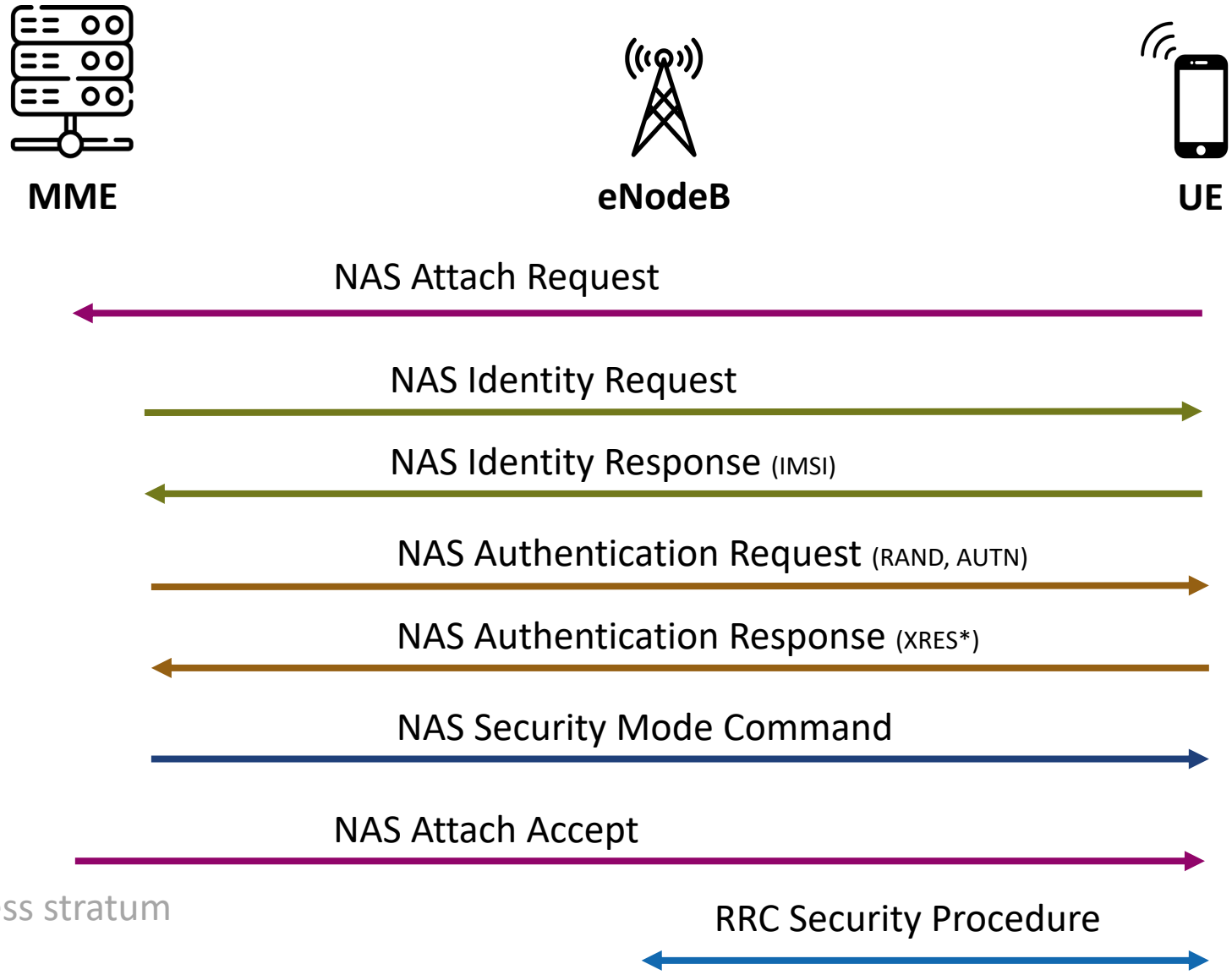


RRC: Radio Resource Control
SIB: System Information Block
eNodeB: Evolved Node B (cell tower)
UE: User Equipment (e.g. a smartphone)

RNTI: Radio Network Temporary Identifier
TMSI: Temporary Mobile Subscriber Identifier

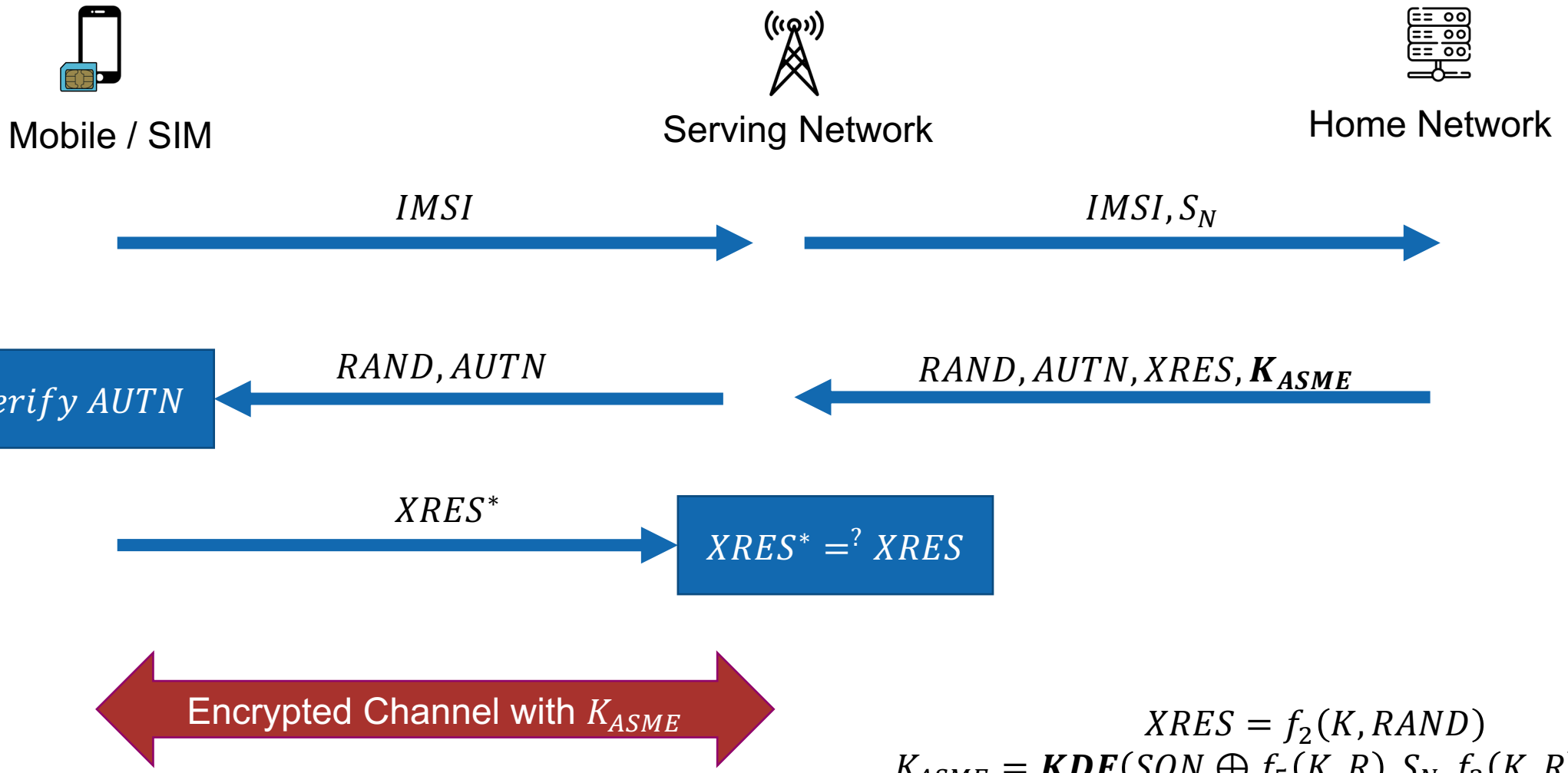
4G - From Power-Off to Internet Access

(2) NAS Attachment Procedure



NAS: Non-access stratum

4G – Authentication & Key Agreement (AKA) Procedure



$$XRES = f_2(K, RAND)$$
$$K_{ASME} = \boldsymbol{KDF}(SQN \oplus f_5(K,R), S_N, f_3(K,R), f_4(K,R))$$

4G – Encryption Algorithms

1. Strong Cryptographic Primitives for encryption and integrity protection
   - EEA = encryption, EIA = integrity

   - EEA1: SNOW
   - EEA2: AES-CTR EIA2: AES-CMAC
   - EEA3 & EIA3: ZUC

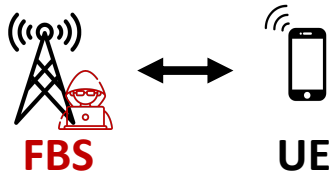
2. Encryption is optional for the user & control plane, but often used

3. Integrity protection is mandatory for the control plane, but not for user data

4G – Attack Methods

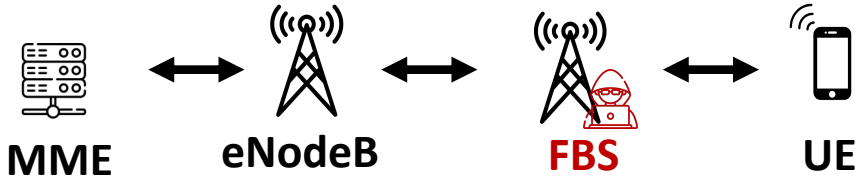
General Active Attack Methods for Mobile Networks

1. **Fake Base Station**
   - A. **Standalone**



Limited Attacks
e.g. Stingrays

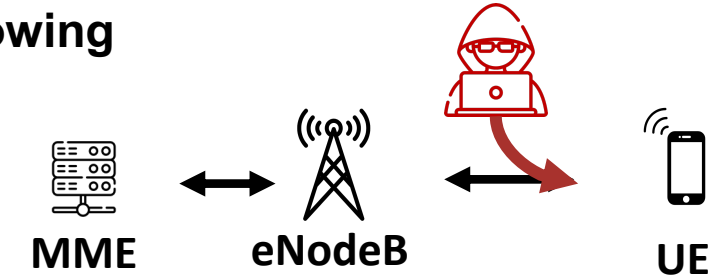
   - B. **Relaying**



All MiTM Attacks
possible

Highly Detectable
High Output Power
(+30dB)

2. **Overshadowing**



Complex Attacker,
Low Output Power (+3dB),
Hard to detect

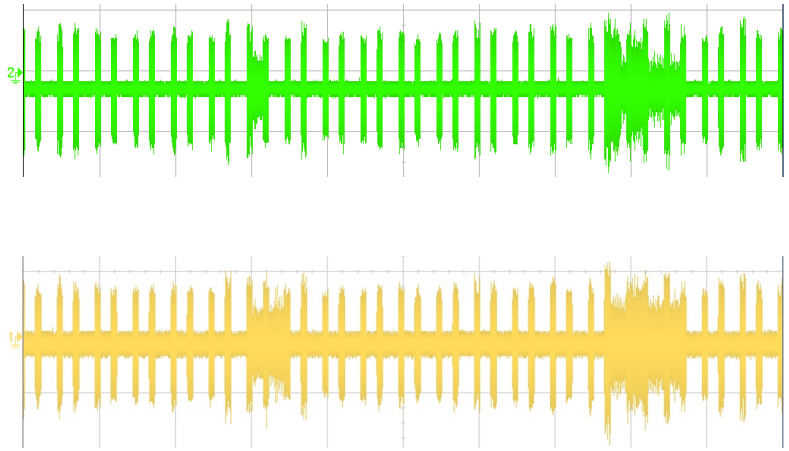
Overshadowing – Basics

Capture Effect

1. Collision of 2 Signals

   Aligned in Time ($< 10\mu s$) & Frequency ($< 1kHz$)

2. Stronger one can still be decoded



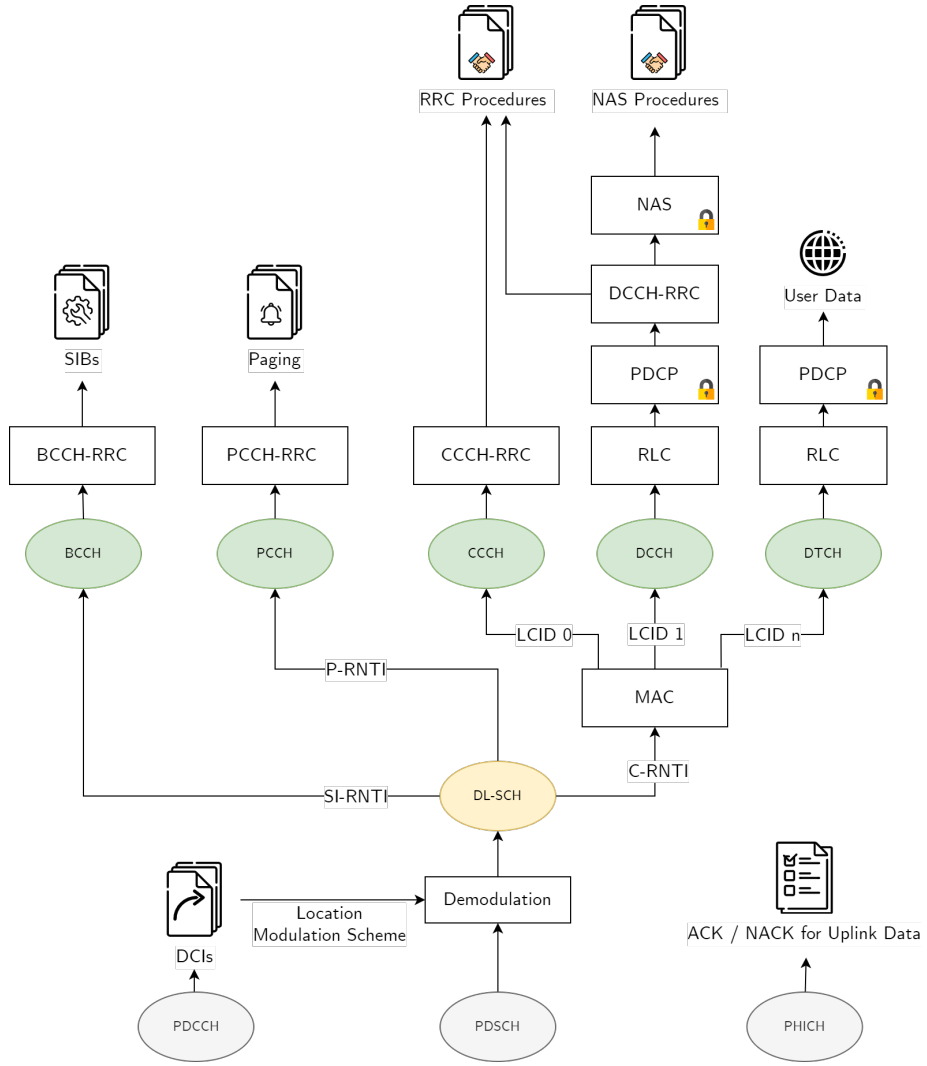
Original Signal

Attacker Signal (+ 1.8 dB)

Overshadowing LTE – Injecting Messages

Injecting Messages in an LTE signal requires:

1. Real-Time Low-Latency Downlink Decoder
2. Full-Stack Message Encoding
3. Overshadowing
4. Procedure Modification (RLC & MAC)



ETH zürich

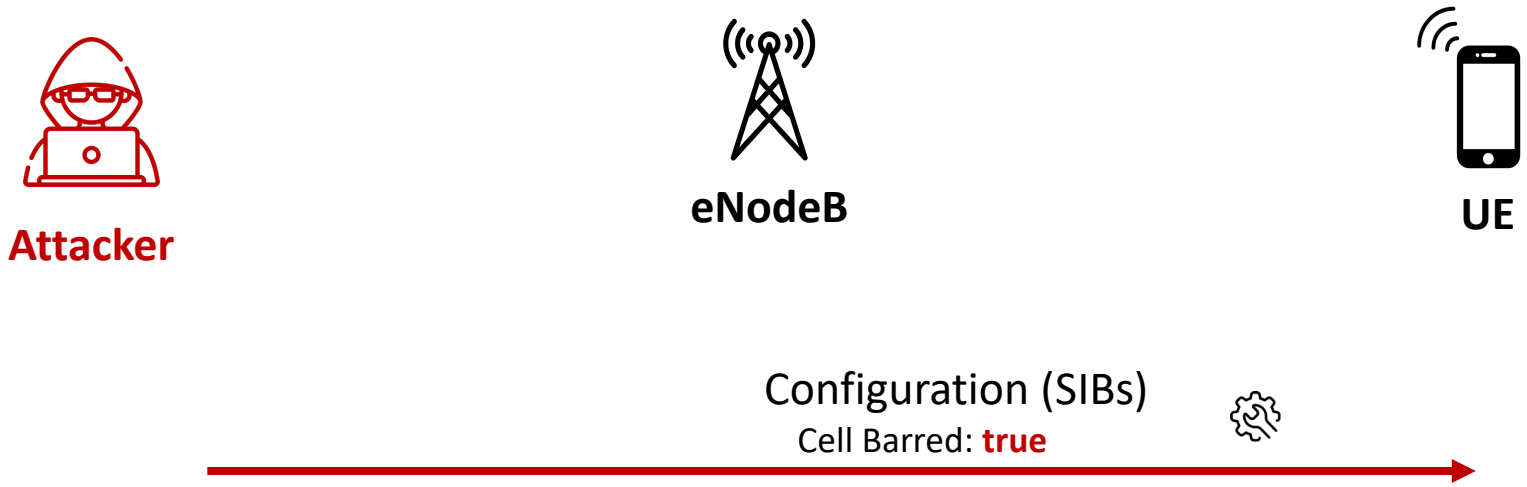
D INFK

4G – Protocol Attacks

Downlink Overshadowing

Yang et al.: Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE (2019)

SigOver – SIB Barring



Downlink Overshadowing

Yang et al.: Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE (2019)

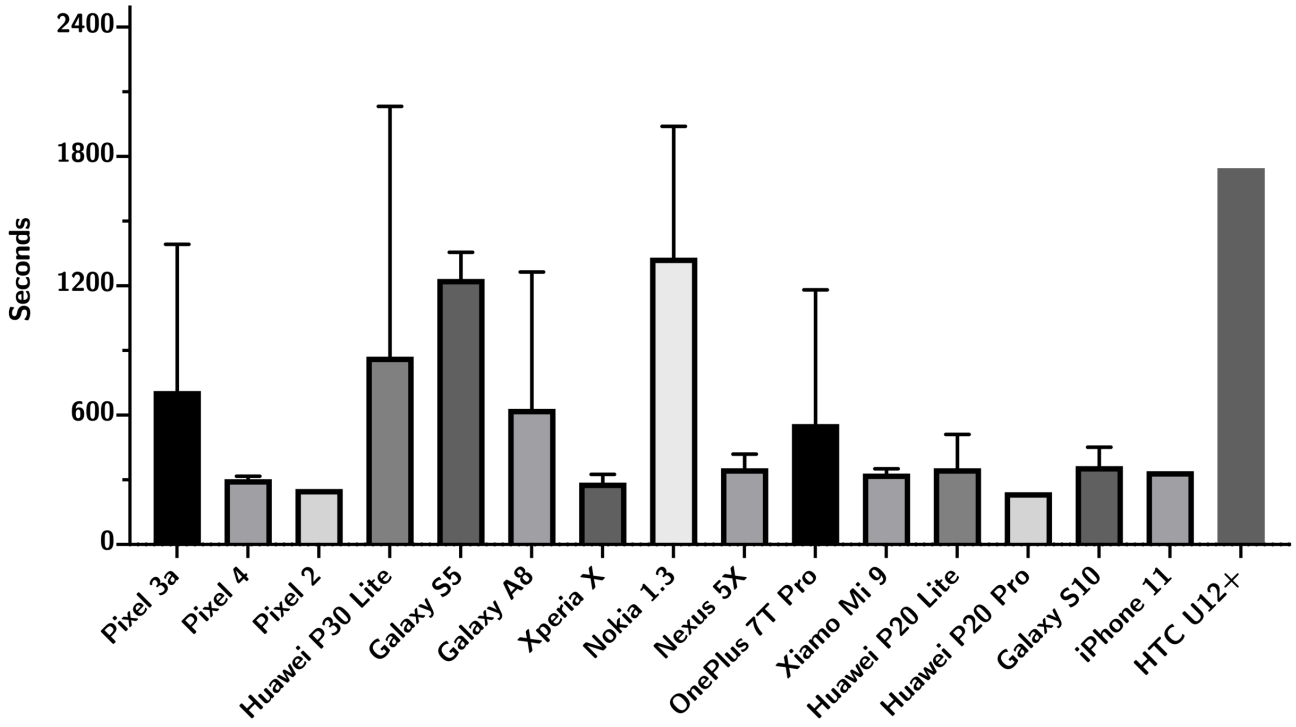
Results

- For single cell: $\leq 20\ min$
- Multi-Cell: $0\ min$

Limitations:

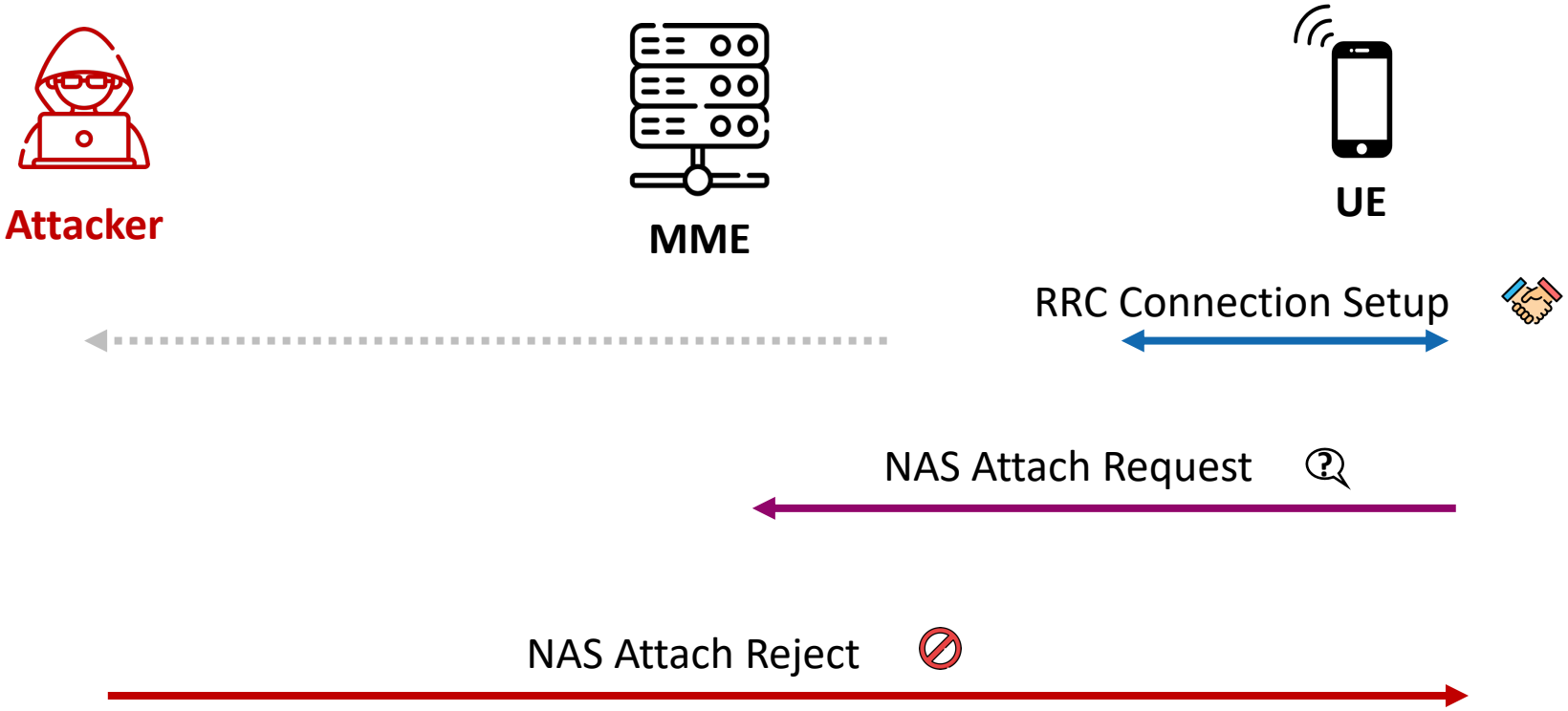
Real-World networks have multiple cells available (most of the time)

How long does it take until a UE **restores** connection?



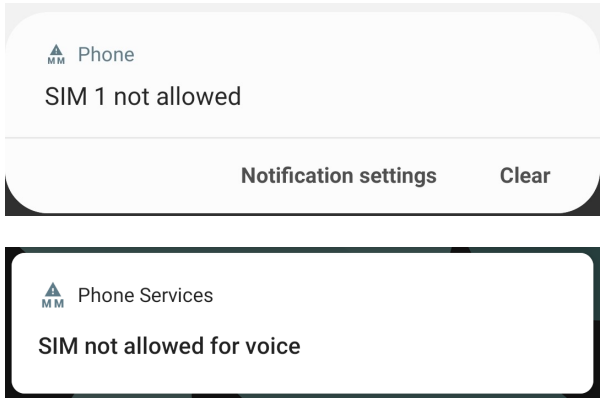
NAS Attach Reject Attack

Erni et al.: AdaptOver (2022)



NAS Attach Reject Attack – Evaluation Results

Erni et al.: AdaptOver (2022)

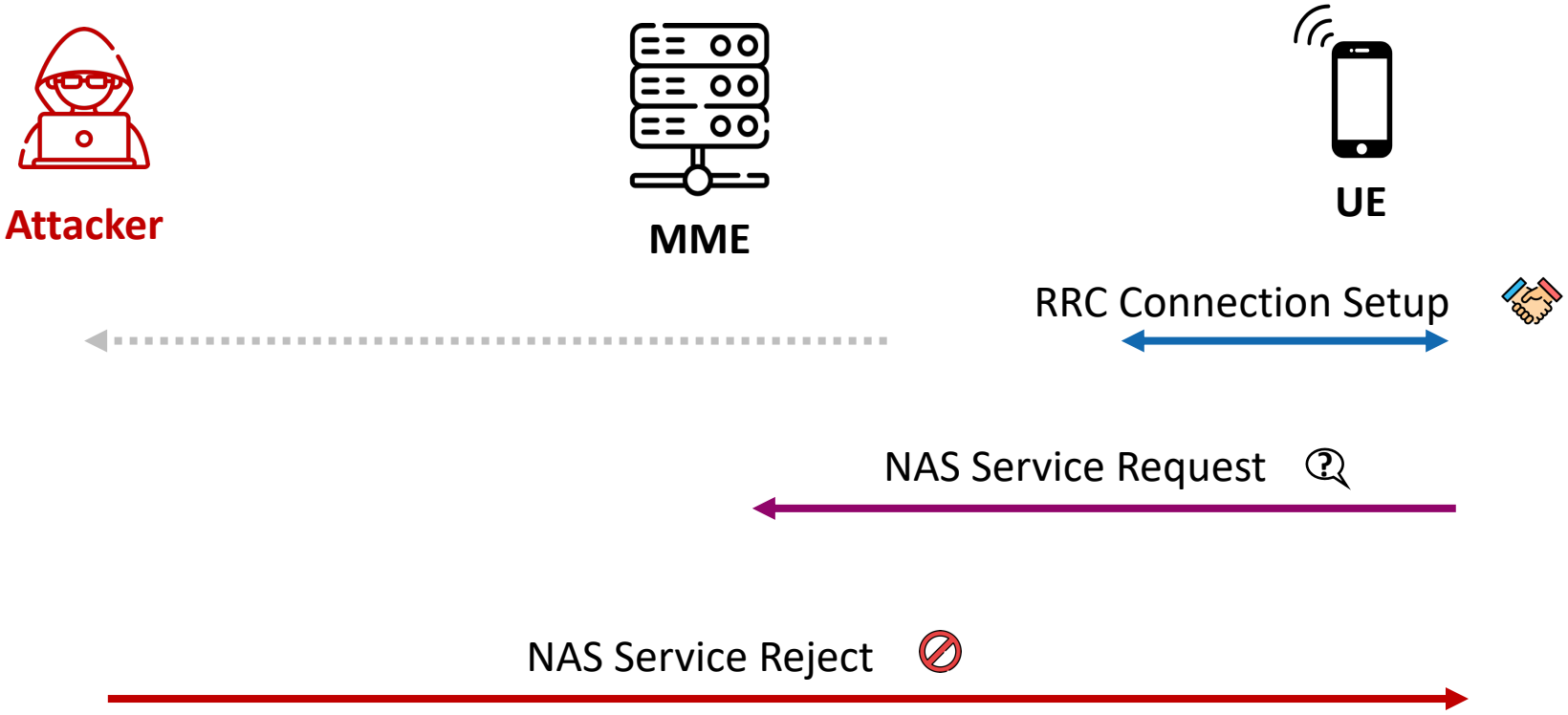


Phone	Reconnection Time	Actions Necessary	GUI Indicators
Pixel 2	> 12h	*Restart phone*	
Pixel 3a	> 20h	*Toggle Flightmode*	
Pixel 4	> 20h	Toggle Flightmode	
Huawei P20 Lite	> 12h	Toggle Flightmode	
Huawei P20 Pro	> 12h	Toggle Flightmode	
Huawei P30 Lite	> 20h	Toggle Flightmode	
Samsung Galaxy S5	> 20h	*Restart phone*	SIM not allowed
Samsung Galaxy A8	> 20h	Toggle Flightmode	SIM not allowed
Samsung Galaxy S10	> 12h	Toggle Flightmode	SIM not allowed
Sony Xperia X	> 20h	Restart phone	
Nokia 1.3	> 20h	Toggle Flightmode	
LG Nexus 5X	> 20h	Restart phone	
iPhone 7	> 12h	Toggle Flightmode	
iPhone 8	> 12h	Toggle Flightmode	
iPhone 11	> 12h	Toggle Flightmode	
iPhone 11 Pro	> 12h	Toggle Flightmode	
HTC U12+	> 20h	Toggle Flightmode	
OnePlus 7T Pro	> 20h	Toggle Flightmode	SIM not allowed
Xiaomi Mi 9	> 20h	Toggle Flightmode	
Xiaomi Mi Mix 3 5G	> 12h	Toggle Flightmode	

Table 7.5: Attack Results for Attach Reject

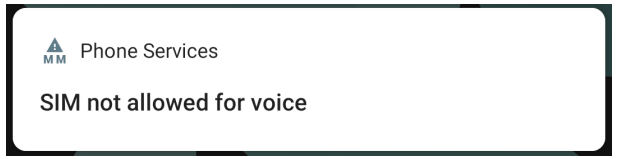
NAS Service Reject Attack

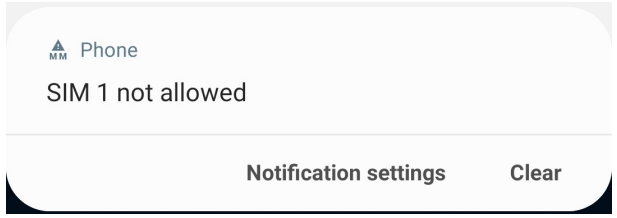
Erni et al.: AdaptOver (2022)

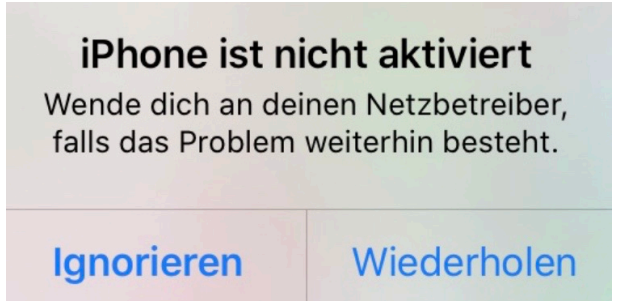


NAS Service Reject Attack – Evaluation Results

Erni et al.: AdaptOver (2022)



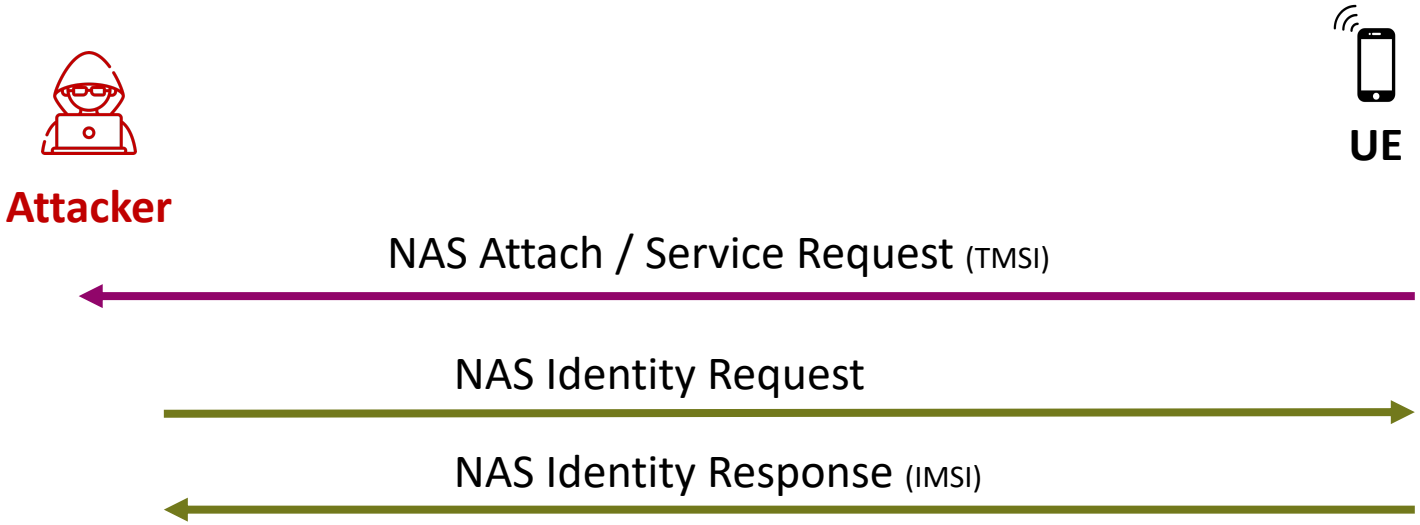




Phone	Reconnection Time	Actions Necessary	GUI Indicators
iPhone 6S	> 12h	Restart phone	iPhone not activated
iPhone 7	> 12h	Toggle Flightmode	
iPhone 8	> 12h	Toggle Flightmode	
iPhone 11	> 12h	Toggle Flightmode	
iPhone 11 Pro	> 12h	Toggle Flightmode	
Pixel 2	> 12h	Restart phone	
Pixel 3a	> 12h	Toggle Flightmode	
Pixel 4	> 12h	Toggle Flightmode	
Huawei P20 Lite	> 12h	Toggle Flightmode	
Huawei P20 Pro	> 12h	Toggle Flightmode	
Huawei P30 Lite	> 12h	Toggle Flightmode	
Samsung Galaxy S5	> 12h	Toggle Flightmode	SIM not allowed
Samsung Galaxy A8	> 12h	Toggle Flightmode	SIM not allowed
Samsung Galaxy S10	> 12h	Toggle Flightmode	SIM not allowed
LG Nexus 5X	> 12h	SIM reinsertion	SIM not allowed
HTC U12+	> 12h	Toggle Flightmode	
OnePlus 7T Pro	> 12h	Toggle Flightmode	
Xiaomi Mi 9	> 12h	Toggle Flightmode	
Xiaomi Mi MIX 3 5G	> 12h	Toggle Flightmode	

Table 7.6: Attack Results for Service Reject

General IMSI Catching



IMSI is bound to the SIM card and never changes!

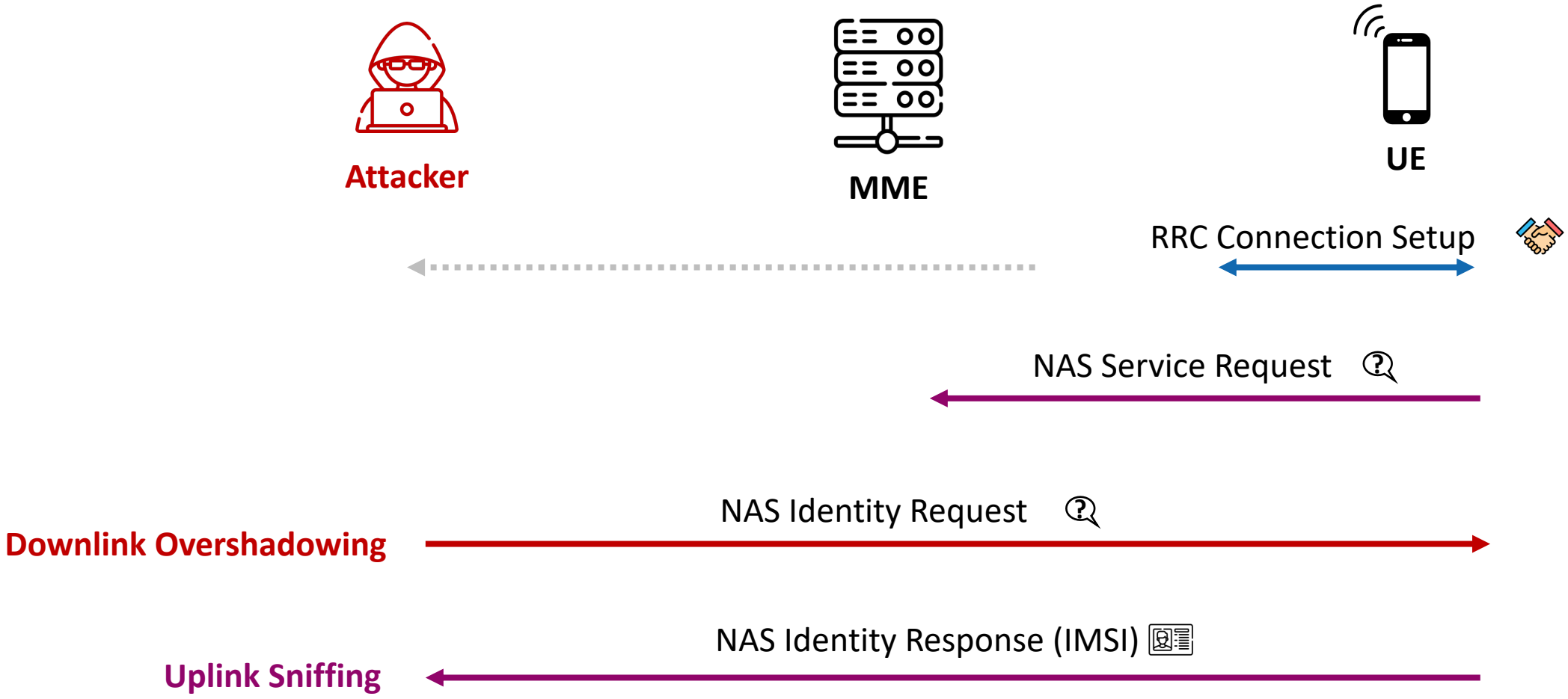
Allows Long-Term Tracking, by binding the TMSI to the IMSI.

NAS Identity Request can be sent at **any time (without authentication).**

Has been a problem since 2G, partial solution/remedy only presented in 5G.

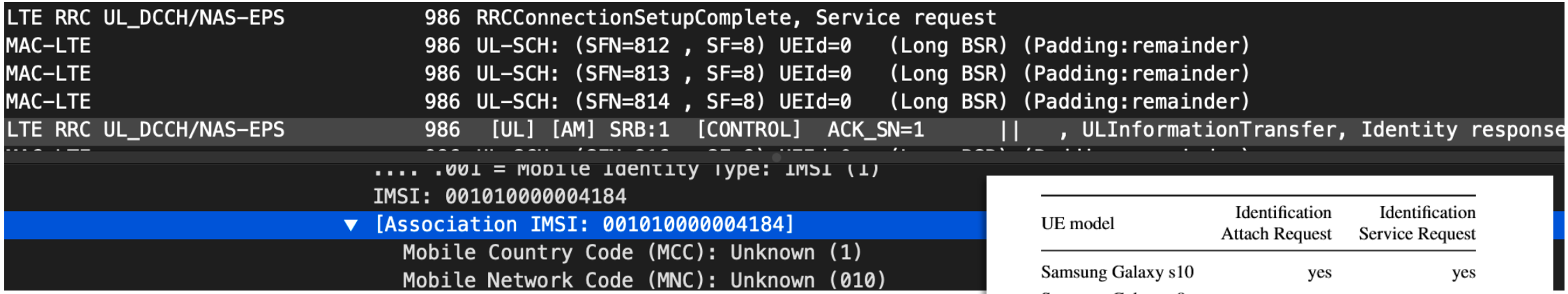
IMSI Extractor

Kotuliak et al.: LTrack (2022)



IMSI Extractor

Kotuliak et al.: LTrack (2022)

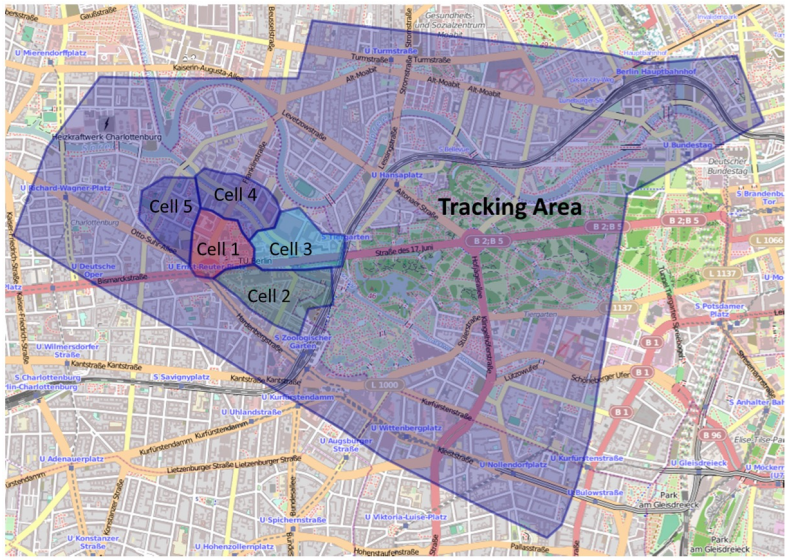


UE model	Identification Attach Request	Identification Service Request
Samsung Galaxy s10	yes	yes
Samsung Galaxy a8	yes	yes
Huawei P20 Pro	yes	yes
Huawei P30 Lite	yes	yes
Huawei P30	yes	yes
Xiaomi Mi9	yes	yes
Xiaomi MiX 3	yes	yes
Google Nexus 5X	yes	yes
Google Pixel 2	yes	yes
Google Pixel 3a	yes	yes
HTC U12+	yes	yes
OnePlus 7T	yes	yes
iPhone 6s	yes	yes
iPhone 7	yes	no
iPhone 8	yes	yes
iPhone X	yes	yes
iPhone 11	yes	yes
iPhone 11 Pro	yes	yes

- It works for all tested smartphone models
- It works during both Service- and Attach-Procedure

Localization
Active Variant (Shaik et al. 2017)

- Active Localization using Fake Base station
  - FBS queries UE for Measurement Report (Signal Strength of neighbor cells)
    - Locate UE using the power measurements
  - FBS queries UE for Measurement Report (GPS Location of UE)
- Semi-Passive Localization using Paging Messages
  - Paging Message used when UE not connected to notify it to connect again
  - Paging Message sent when
    e.g., WhatsApp message, FB friend request
  - Observe Paging Messages in various cells
  - Paging Message first sent in the
    last cell used by the UE (if Smart Paging used)
  - Paging Message first sent in the
    Tracking Area used by the UE (if Smart Paging not used)

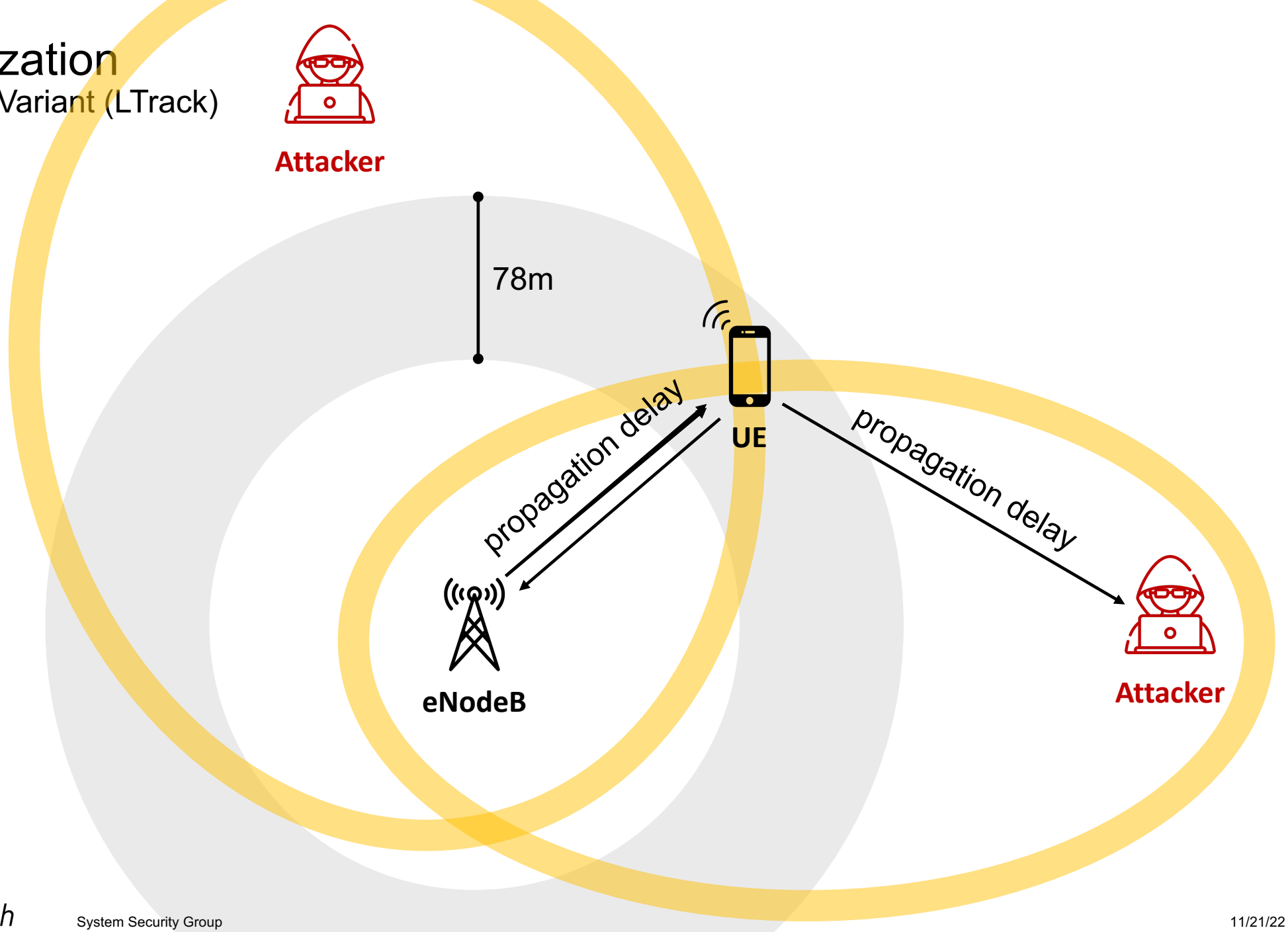


Shaik, Altaf, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. “Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems.” *ArXiv:1510.07563 [Cs]*, August 7, 2017. http://arxiv.org/abs/1510.07563.

Localization
Passive Variant (LTrack, 2022)

1. Fully Passive Localization
2. Downlink
    1. Base Station notifies UE about the propagation delay between them
        1. Specifies a ring around a base station
        2. Unencrypted on MAC layer
    2. LTE-A: UE connects to multiple base stations
3. Uplink
    1. Reference Signals used for channel correction – Propagation delay is channel condition
    2. Observe propagation delay from multiple points – TDOA
4. More accurate than 2G and 3G since 4G requires tighter synchronization

Localization
Passive Variant (LTrack)

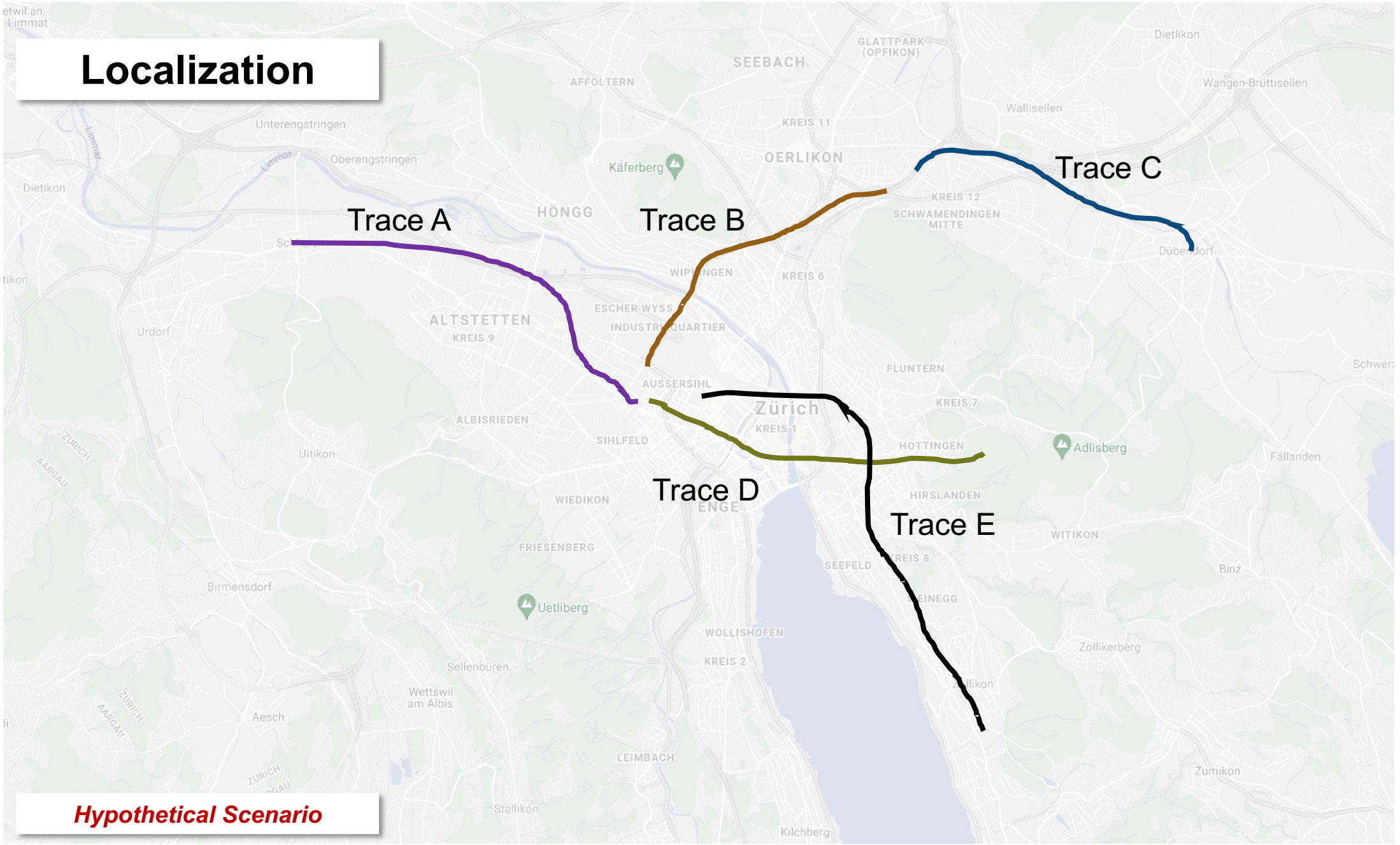


LTrack – Tracking of Mobile Phones in LTE

1. Use Localization Attack to know **where** mobile phones are
   - Fully Passive Attack
   - Link Traces via TMSI

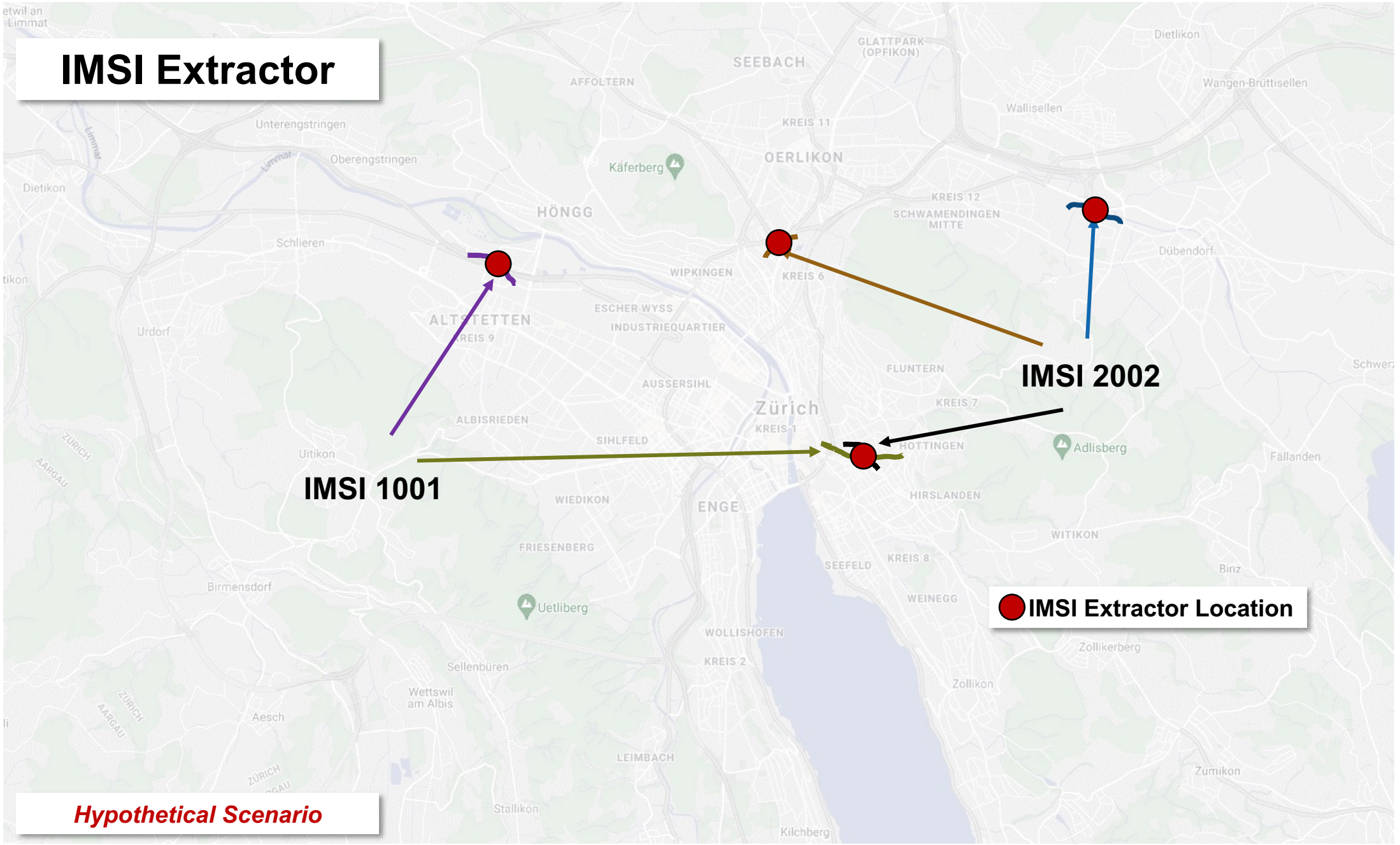
2. Use IMSI Extractor to know **who** mobile phones belong to
   - Active Overshadowing Attack
   - Reveal TMSI → IMSI Binding

Localization

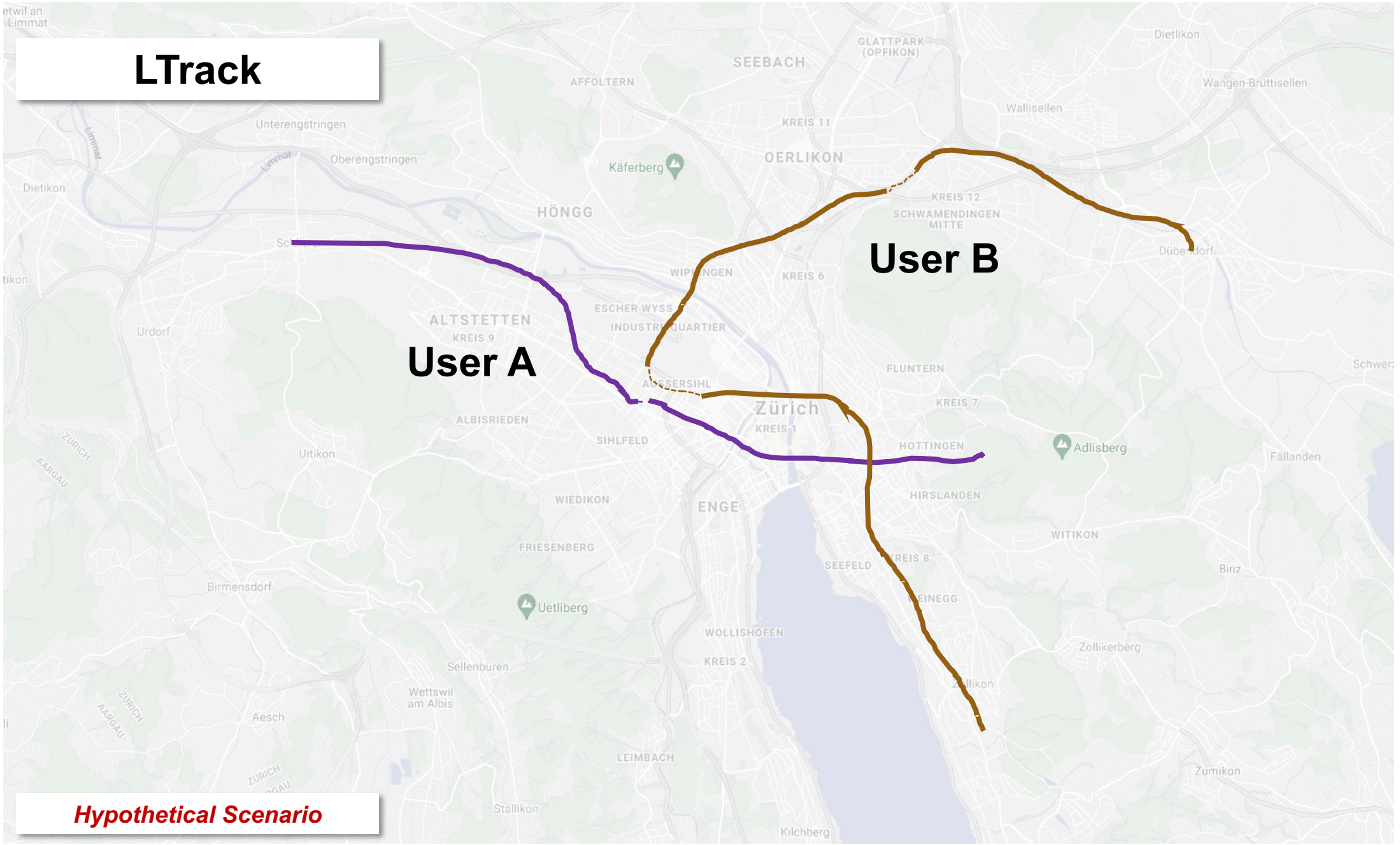


Hypothetical Scenario

IMSI Extractor

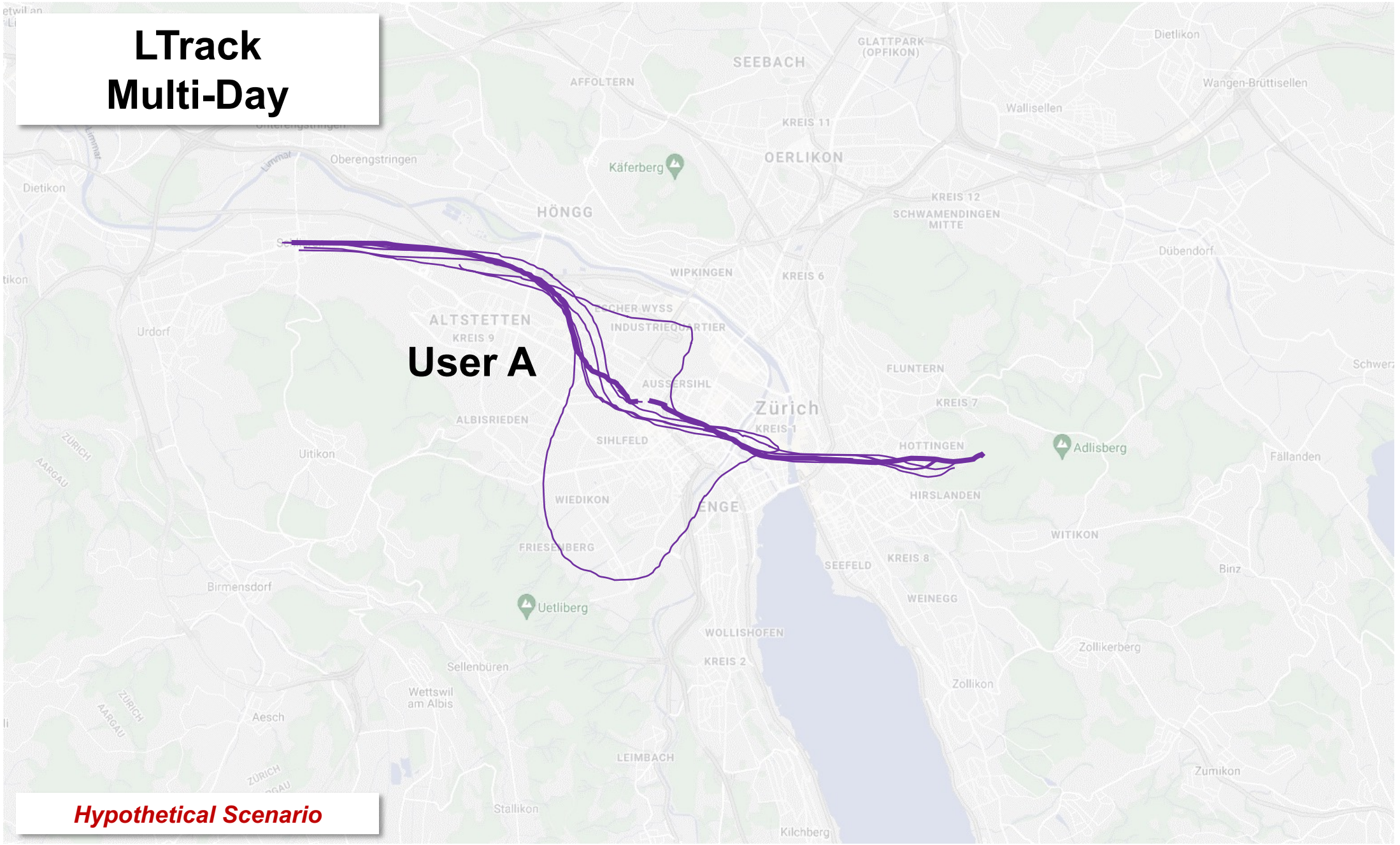


LTrack



Hypothetical Scenario

LTrack Multi-Day



Hypothetical Scenario

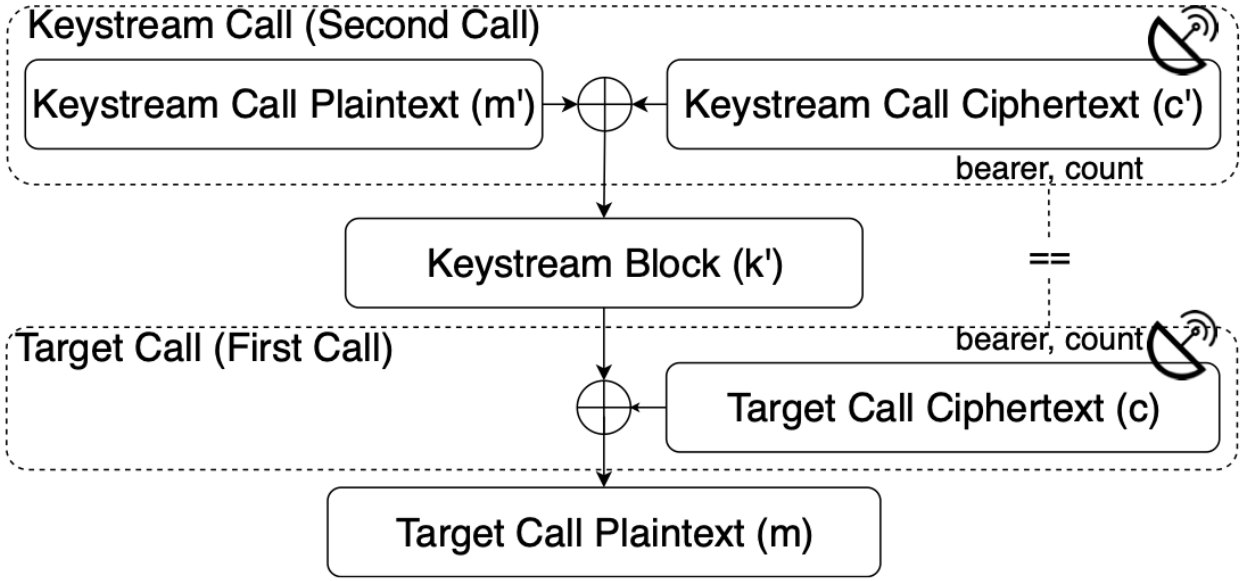
4G – Protocol Attacks

Rupprecht et al.: Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE (2020)

Problem: VoLTE calls during the same connection of the UE to the base station use the same input parameters to the encryption algorithm

1. Two VoLTE calls are encrypted with the same Key Stream
2. Attacker records first call
3. Attacker calls the victim, and records both unencrypted and ciphered call
4. Attacker obtains keystream and applies it to the first call to decrypt it

The attack should be fixed now



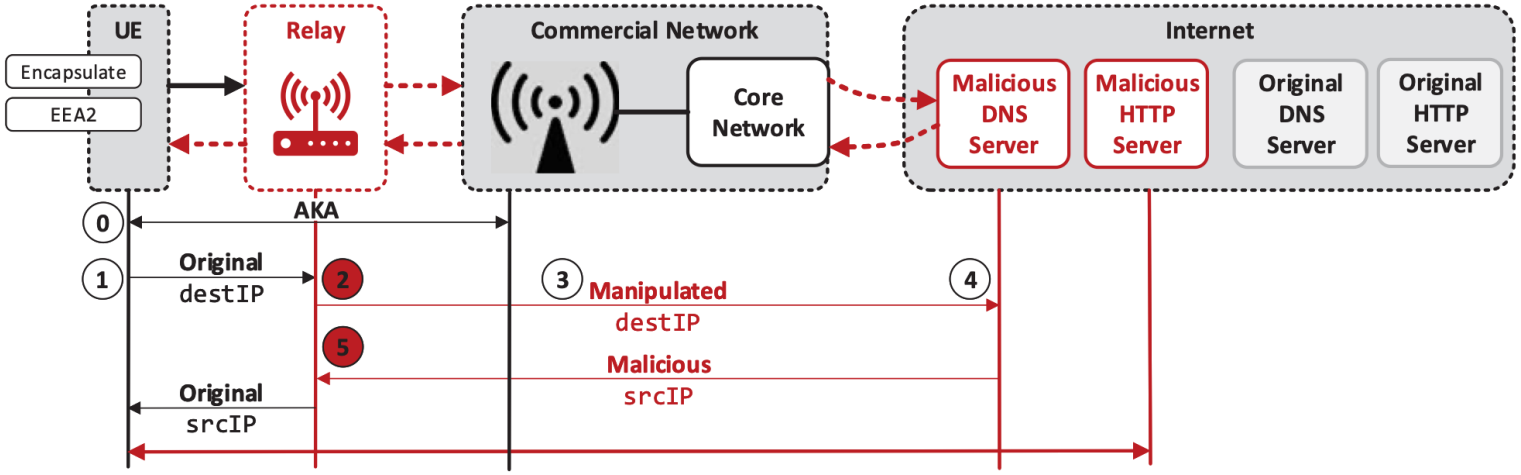
4G – Protocol Attacks

Rupprecht et al.: Breaking LTE on Layer Two (2019)

Problem: User Data Plane is only encrypted using a stream cipher and not integrity protected.

→ Thus, an attacker can flip targeted bits

Attack: Apply mask to IP addresses in DNS packets, redirect traffic flow to the attacker



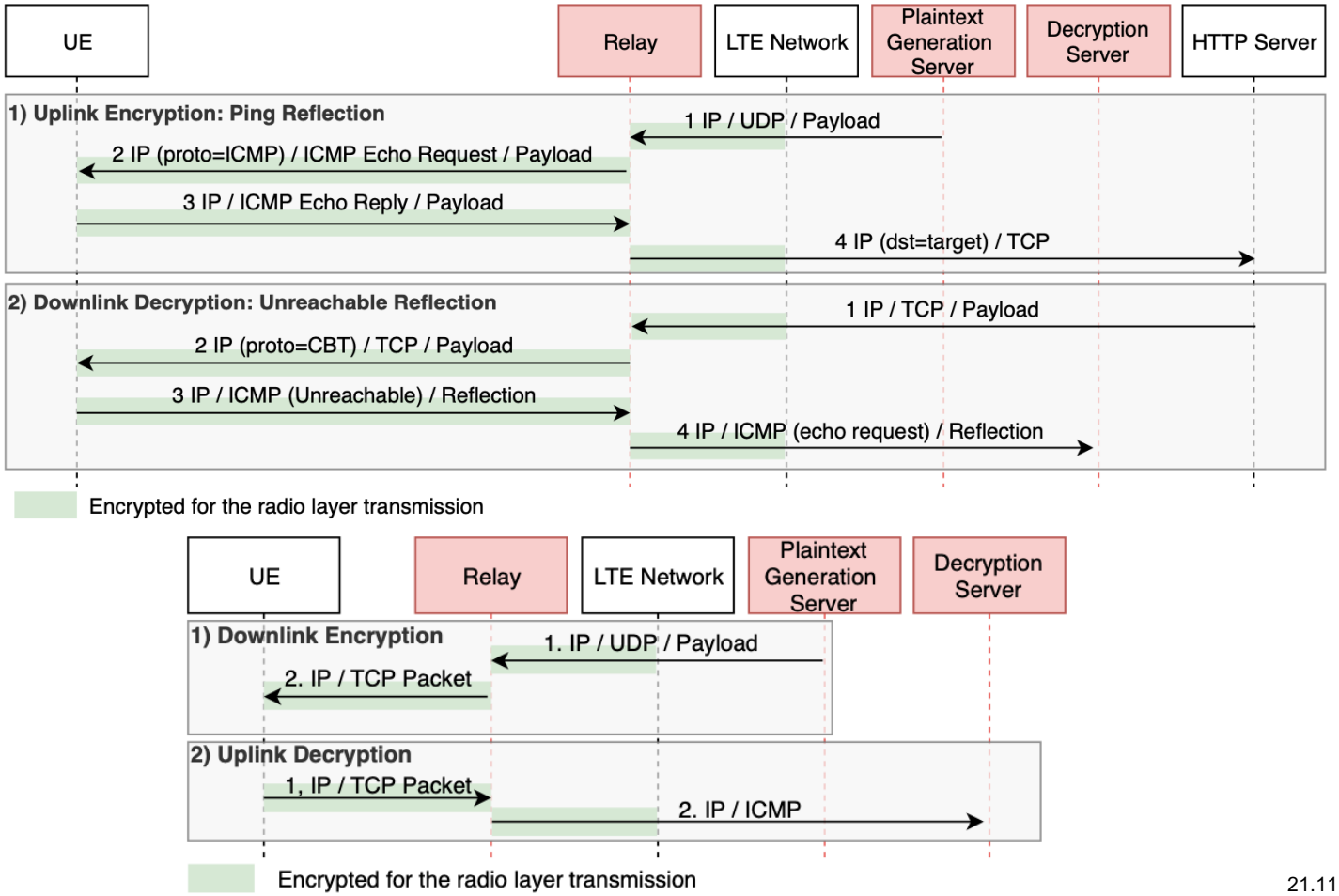
4G – Protocol Attacks

Rupprecht et al.: IMP4GT: IMPersonation Attacks in 4G NeTworks (2020)

Attack: *full impersonation* on the user plane in both uplink and downlink direction

1. Uplink IMP4GT

2. Downlink IMP4GT



ETH zürich

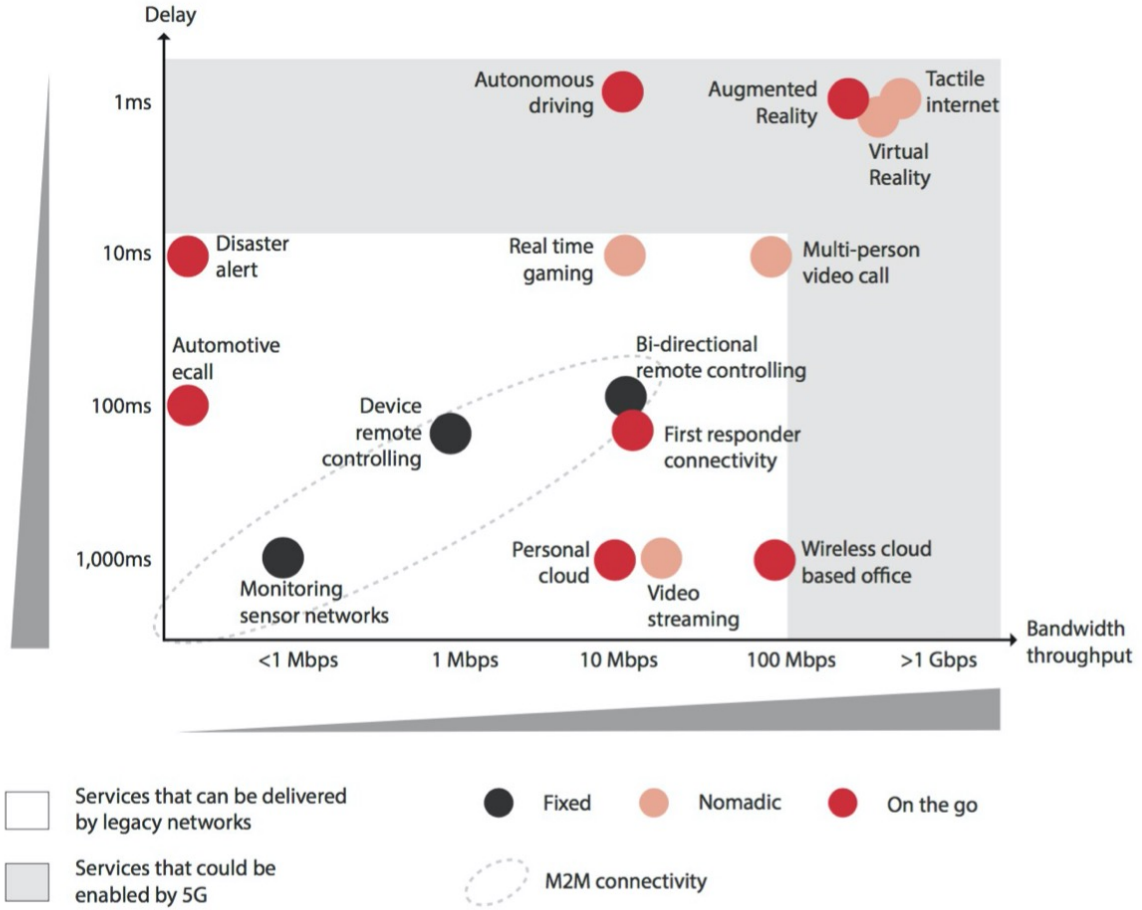
D INFK

5G - NR

New Radio

5G – New Radio

- Need for data rates and latency for emerging use-cases
- 3GPP published the first version in 2018
- First Deployment in Switzerland in 2019
- Physical layer similar to LTE
  - OFDMA
  - Slot duration and subcarrier spacing is modular
- Non-stadalone mode which relies on 4G core network to speed up 5G deployment
- Standalone mode afterwards with its own core



5G – Subscription Identifier Privacy

- In order to thwart IMSI Catcher attacks, 5G implements **concealment** of the permanent identifiers
- **Su**bscription **P**ermanent **I**dentifier (SUPI) vs **Su**bscription **C**oncealed Identifier (SUCI)
- SUPI can be: IMSI, random identifier
- Each SUCI is generated using a random ephemeral ECC public/private key-pair

Simplified:

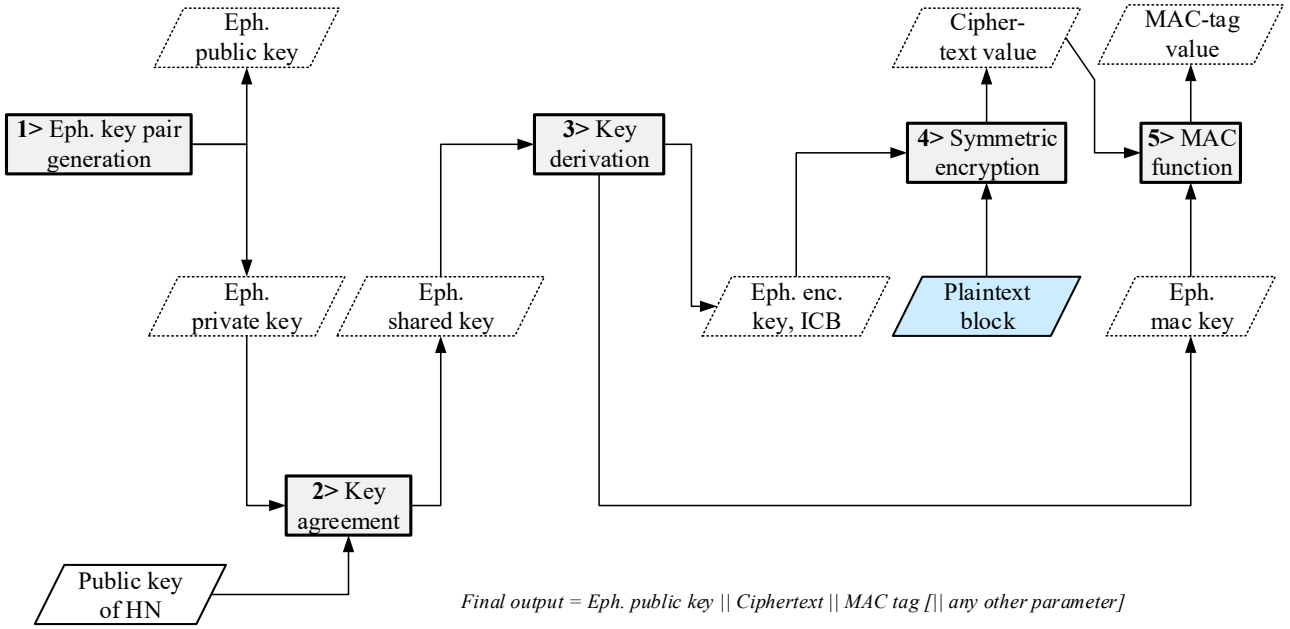
$$Public\ Key\ HN = g^x$$

$$SUCI = g^y, \{|SUPI|\}_{g^{xy}}$$

SUCI is generated:

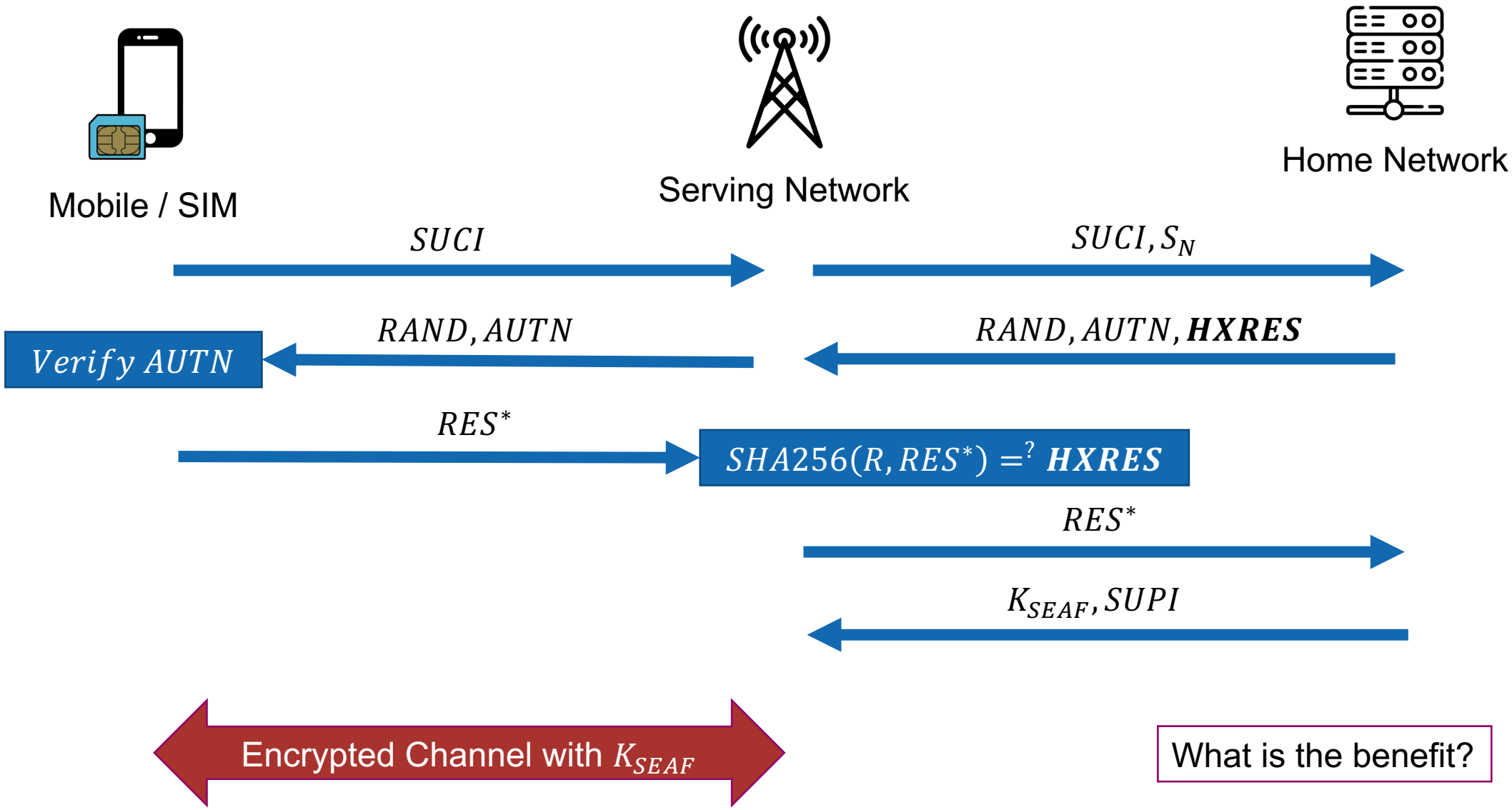
a) On the SIM card (requires special SIM)

b) On the UE



3GPP TS 33.501 V15.4.0 (2019-03)

5G – Authentication & Key Agreement (5G – AKA) Procedure



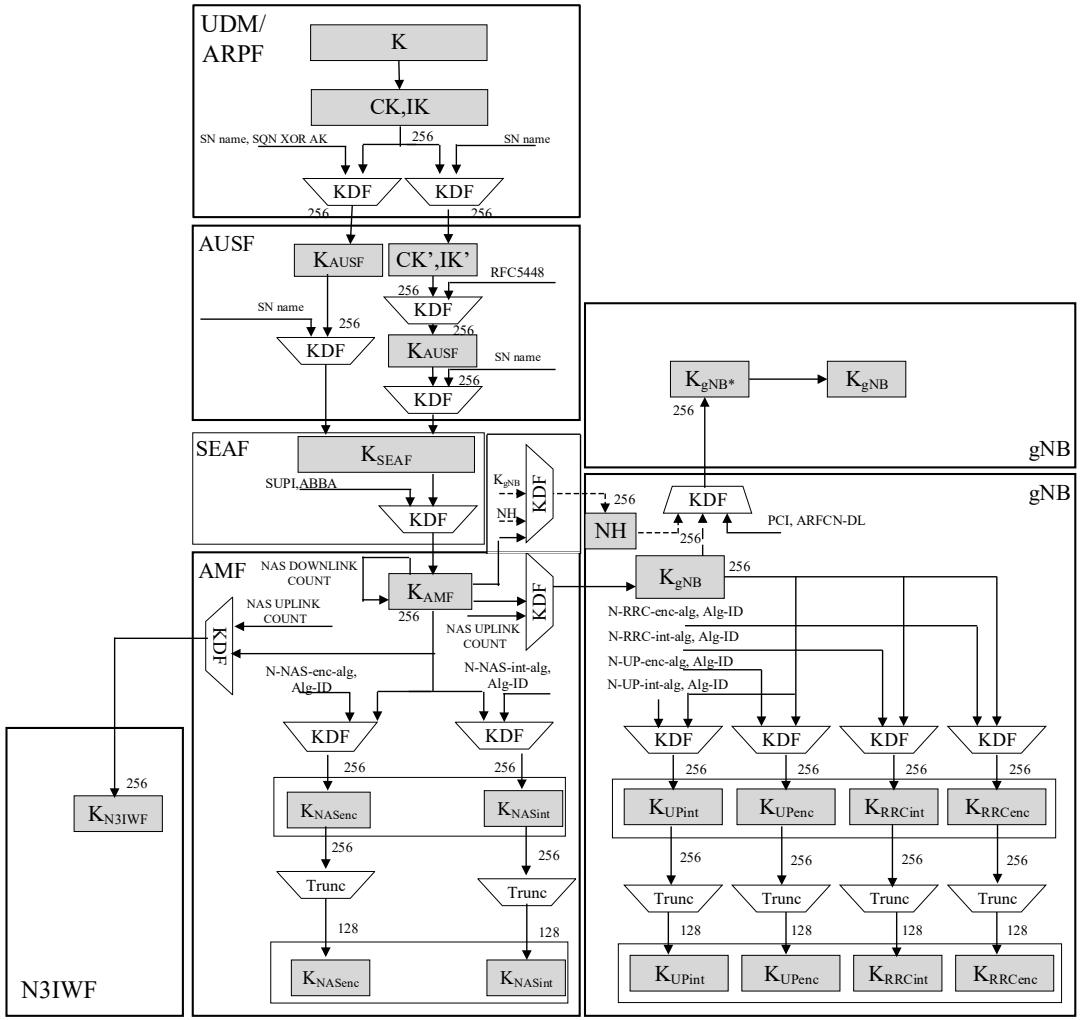
5G – Key Derivation

Derived Shared Session Key depends on:

1. SN Name
2. SQN
3. SUPI

Individual Keys for different network components

- High-Trust components (e.g., AMF) derive keys for Low-Trust components (e.g., gNodeB)



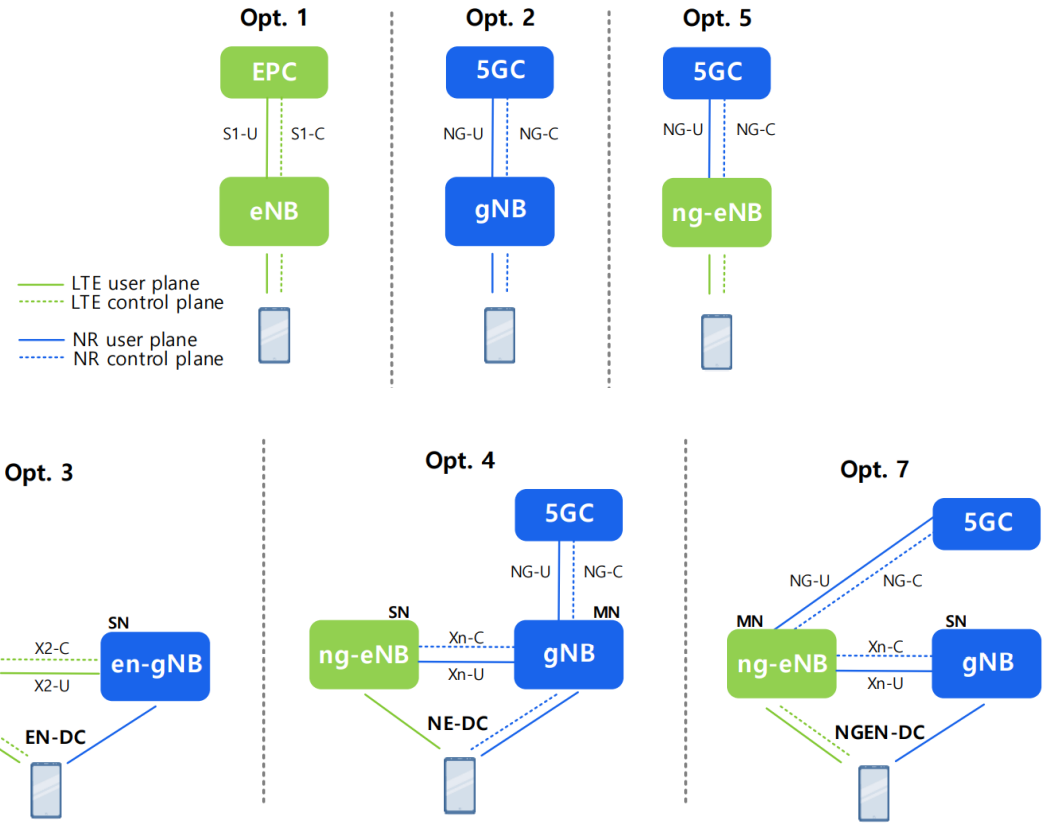
3GPP TS 33.501 V15.4.0 (2019-03)

5G – Current Deployment (NSA vs SA)

Most operators today (2021) are not ready to deploy their 5G core network and operate in NSA mode.

Standalone (SA)

Non-Standalone (NSA)

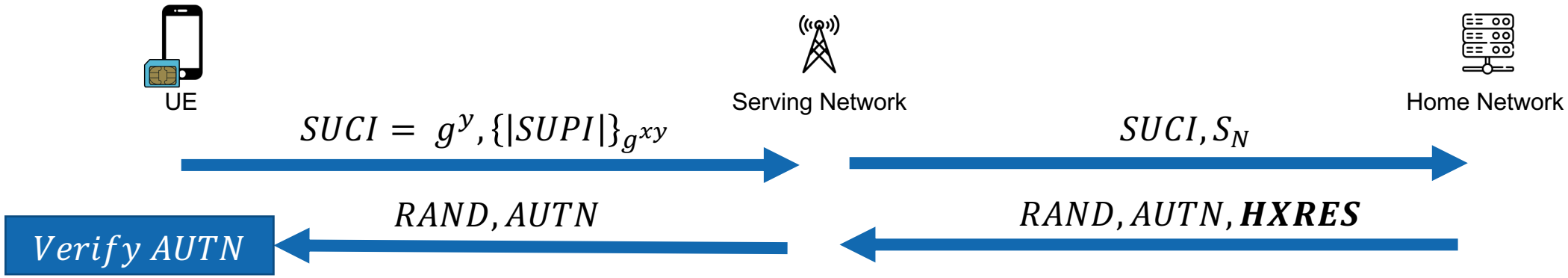


https://images.samsung.com/is/content/samsung/p5/global/business/networks/insights/white-papers/0107_5g-standalone-architecture/5G_SA_Architecture_Technical_White_Paper_Public.pdf

5G – Formal Verification

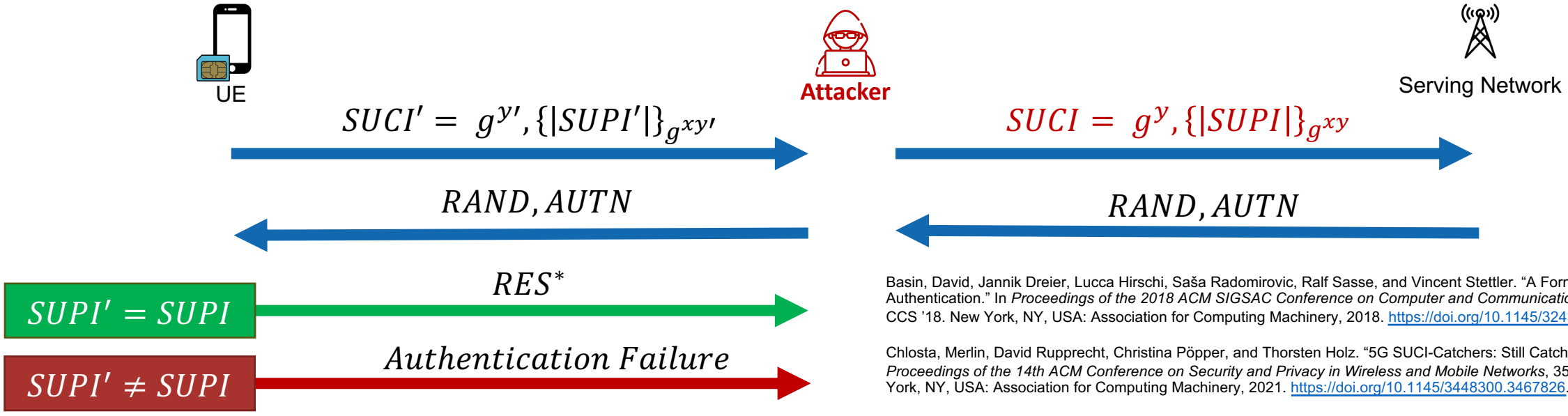
- Basin et al. "A Formal Analysis of 5G Authentication" CCS'18
  - Formal modeling and verification of 5G AKA
  - Found minor inconsistencies in the spec
  - IMSI Catcher alternative – **SUCI Catcher**
- Hussain et al. "5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol" CCS'19
  - Cross-layer modeling and analysis
  - Findings: minor vulnerabilities in RRC and NAS layer to learn the victims TMSI
  - Localization based on paging is still possible
- Hussain et al. "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information" NDSS'19
  - Multiple paging messages may enable tracking even if TMSI is changed frequently

5G – SUCI Catcher



Problem: RAND, AUTN is not bound to g^y (no freshness captured from the UE)

This means that the $SUCI'$ can be 1) replaced with a previously captured $SUCI$ and 2) tested for equality

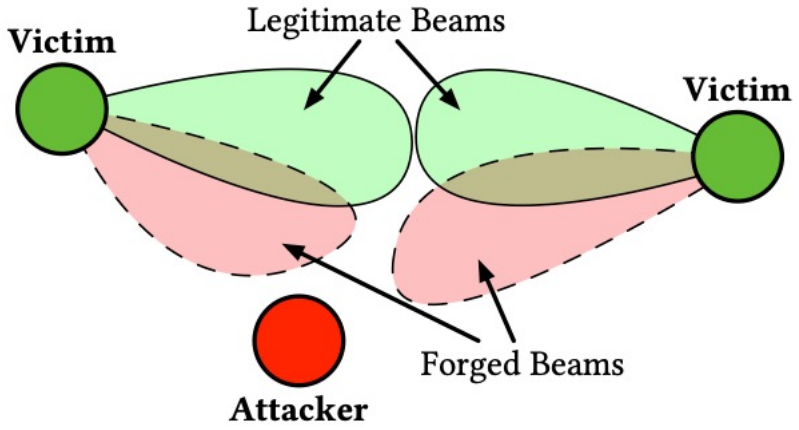


Basin, David, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. "A Formal Analysis of 5G Authentication." In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 1383–96. CCS '18. New York, NY, USA: Association for Computing Machinery, 2018. https://doi.org/10.1145/3243734.3243846.

Chlosta, Merlin, David Rupprecht, Christina Pöpper, and Thorsten Holz. "5G SUCI-Catchers: Still Catching Them All?" In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 359–64. WiSec '21. New York, NY, USA: Association for Computing Machinery, 2021. https://doi.org/10.1145/3448300.3467826.

5G – Denial of Service

1. Blanket Jamming
    1. 5G DL/UL is broadband: Jamming requires a lot of energy (high J/S)
2. SIB Overshadowing
    1. Done in simulations
    2. Ludant & Noubir: SigUnder: a stealthy 5G low power attack and defenses
3. Beam steering
    1. 5G uses beamforming
    2. Steer the beam in the wrong direction



5G – Localization

- 5G physical layer structure is similar to 4G
  - Using reference signals for propagation delay estimation still possible

- Localization based on paging messages still possible, too
  - If TMSI is known
  - TMSI should be refreshed often

References

[1] Sauter, Martin. “GSM.” In *Grundkurs Mobile Kommunikationssysteme: LTE-Advanced Pro, UMTS, HSPA, GSM, GPRS, Wireless LAN und Bluetooth*, edited by Martin Sauter, 1–73. Wiesbaden: Springer Fachmedien, 2018. https://doi.org/10.1007/978-3-658-21647-4_1.

[2] Zhang, Bin. “Cryptanalysis of GSM Encryption in 2G/3G Networks Without Rainbow Tables.” *Advances in Cryptology – ASIACRYPT 2019*, Advances in Cryptology – ASIACRYPT 2019, 11923 (2019): 428–56. https://doi.org/10.1007/978-3-030-34618-8_15.

[3] From GSM to LTE-Advanced Pro and 5G: An Introduction to Mobile Networks and Mobile Broadband, Third Edition. John Wiley & Sons, Ltd, 2017. https://onlinelibrary.wiley.com/doi/abs/10.1002/9781119346913.

[4] Yang, Hojoon, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim. “Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE.” In *Proceedings of the 28th USENIX Conference on Security Symposium*, 55–72. SEC’19. USA: USENIX Association, 2019.

[5] Rupprecht, David, Katharina Kohls, Thorsten Holz, and Christina Pöpper. “IMP4GT: IMPersonation Attacks in 4G NeTworks.” In *ISOC Network and Distributed System Security Symposium (NDSS)*. ISOC, 2020.

[6] Rupprecht, David, Katharina Kohls, Thorsten Holz, and Christina Popper. “Breaking LTE on Layer Two.” In *2019 IEEE Symposium on Security and Privacy (SP)*, 1121–36. San Francisco, CA, USA: IEEE, 2019. https://doi.org/10.1109/SP.2019.00006.

[7] Rupprecht, David, Katharina Kohls, Christina Pöpper, and Thorsten Holz. “Eavesdropping Encrypted LTE Calls With REVOLTE,” n.d., 17.

[8] Rellstab, Angela. “Formalizing and Verifying Generations of AKA Protocols,” 2019. https://doi.org/10.3929/ethz-b-000372339.

[9] Hussain, Syed Rafiul, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. “Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information.” In *Proceedings 2019 Network and Distributed System Security Symposium*. San Diego, CA: Internet Society, 2019. https://doi.org/10.14722/ndss.2019.23442.

[10] Kotuliak, Martin, Simon Erni, Patrick Leu, Marc Roeschlin, and Srdjan Capkun. "LTrack: Stealthy Tracking of Mobile Phones in LTE." *arXiv preprint arXiv:2106.05007* (2021). https://arxiv.org/pdf/2106.05007.pdf

[11] Erni, Simon, Patrick Leu, Martin Kotuliak, Marc Röschlin, and Srdjan Čapkun. "AdaptOver: Adaptive Overshadowing of LTE signals." *arXiv preprint arXiv:2106.05039* (2021). https://arxiv.org/pdf/2106.05039.pdf