Cellular Network Security
Part 2

Recap from last week

Basic concepts of mobile telephony

- Calls, paging, HLR, VLR, SS7, operators, SIM cards, crypto…

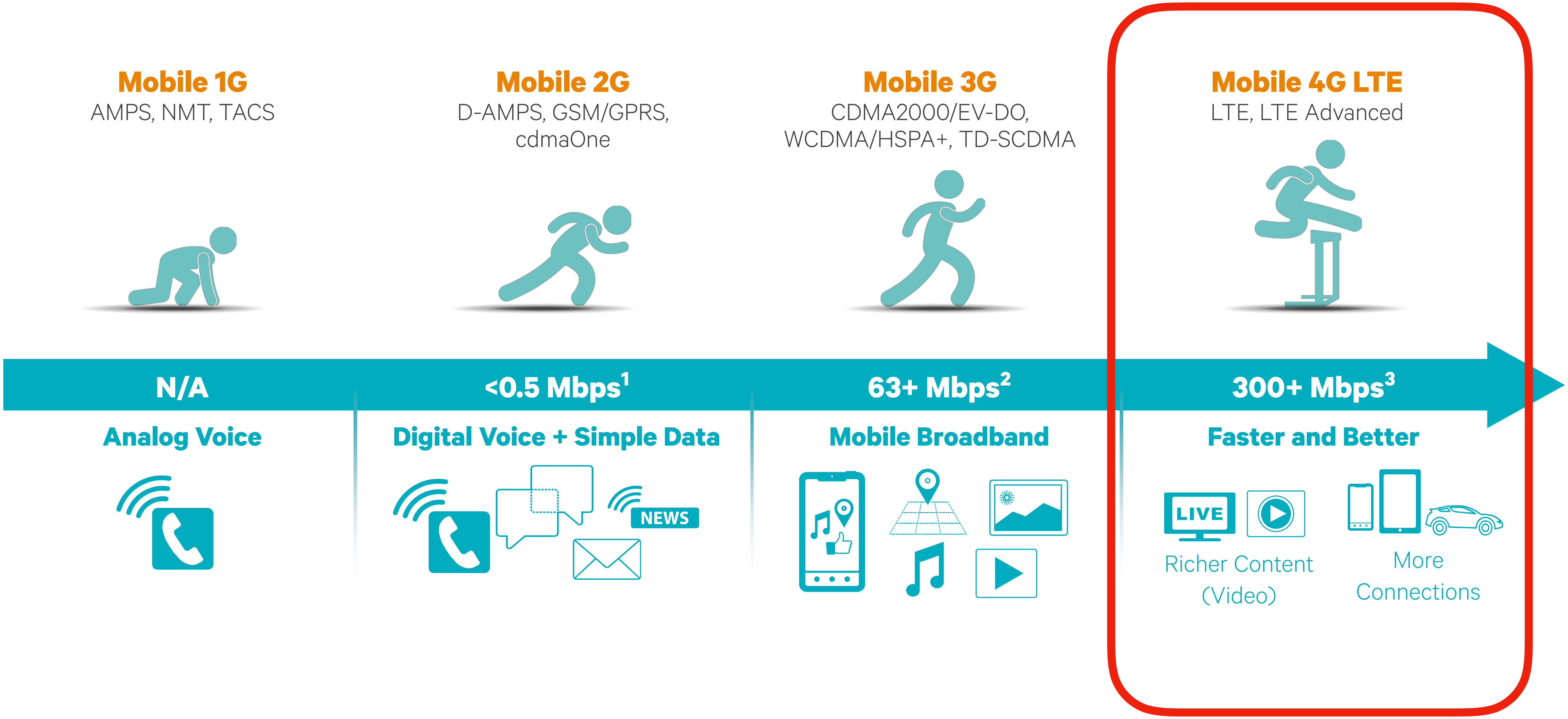
Common theme: security vs. performance vs. cost

- **1G —** no security
- **2G —** authentication and encryption, but weak crypto
- **SS7 —** attacks due open interfaces
- **3G —** stronger crypto and new AKA protocol

Remaining issues

- Limited identifier (IMSI/TMSI) leakage —> tracking
- Fake base station —> downgrading
- Physical layer —> integrity violation, denial of service…

4G



Mobile 1G	Mobile 2G	Mobile 3G	Mobile 4G LTE
AMPS, NMT, TACS	D-AMPS, GSM/GPRS, cdmaOne	CDMA2000/EV-DO, WCDMA/HSPA+, TD-SCDMA	LTE, LTE Advanced
N/A	<0.5 Mbps[1]	63+ Mbps[2]	300+ Mbps[3]
Analog Voice	Digital Voice + Simple Data	Mobile Broadband	Faster and Better
1980's	1990's	2000's	2010's

4G overview

Known also as **LTE** (Long-Term Evolution)

- Introduced around 2008

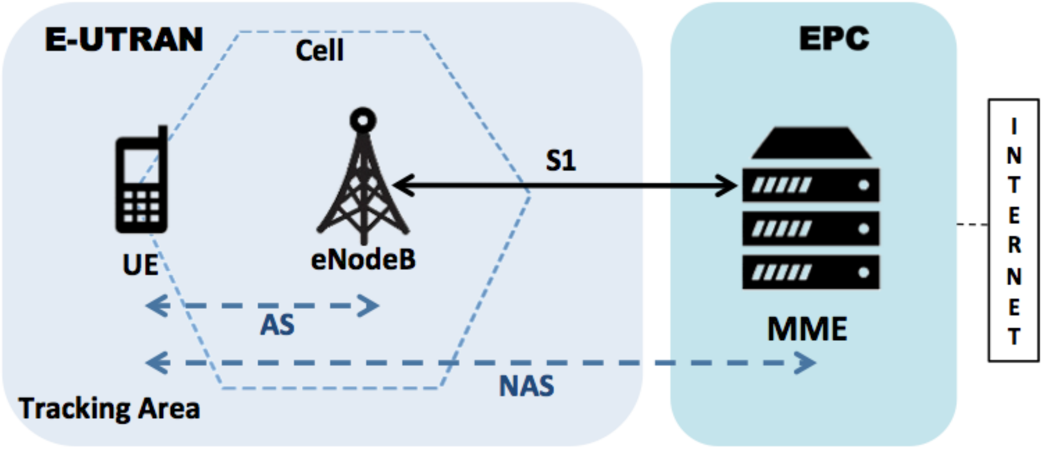
Updated architecture

- Fully packet-switched
- **Core network** called Evolved Packet Core (**EPC**)
- **Radio network** called Evolved-UTRAN (**E-UTRAN**)
- Interoperable with legacy systems

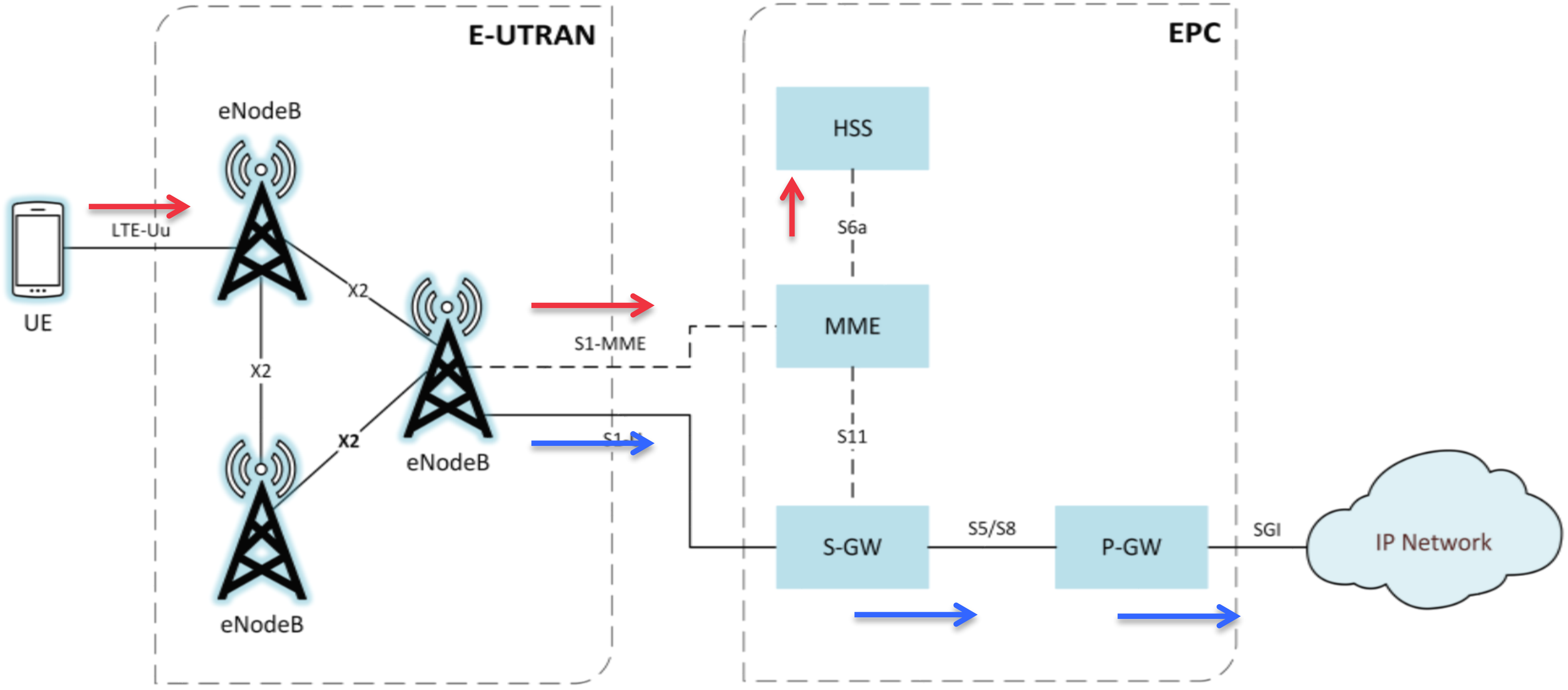
New physical layer

- Orthogonal frequency division multiplex (**OFDM**)
- Multiple antenna techniques like **MIMO**
- 300 Mbps downlink, 70 Mbps uplink, 5ms latency

LTE architecture and terminology



- **UE:** User Equipment (MS)
- **eNB**: enhanced NodeB (BS)
- **E-UTRAN:** Evolved Universal Terrestrial Radio Access Network
- **MME**: Mobility Management Entity (MSC)
- **HSS**: Home Subscriber Server (HLR)
- **S-GW:** Serving Gateway
- **P-GW:** Packet Gateway



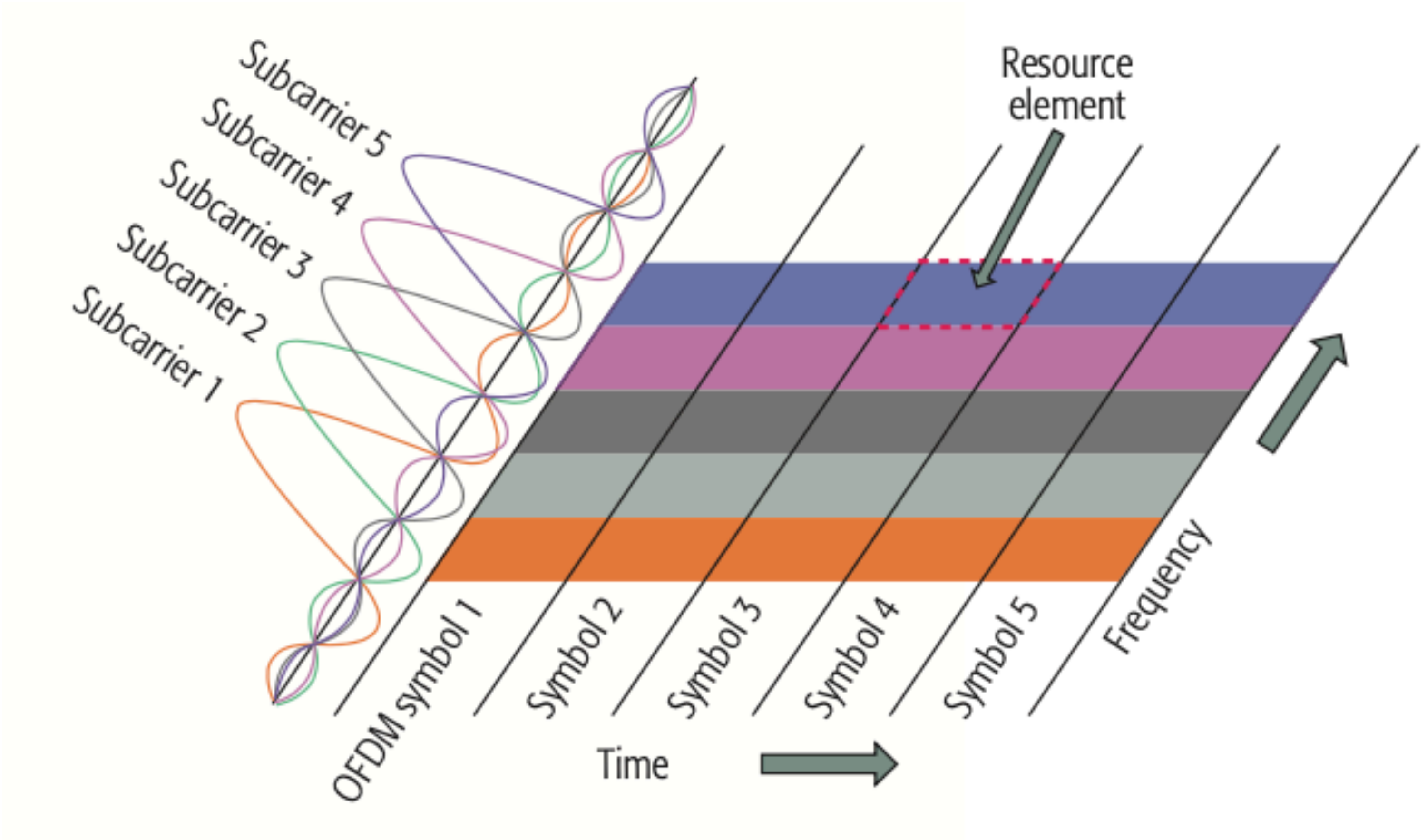
Some LTE physical layer details

OFDM downlink

- Multiple narrow sub-carriers spread over a wide channel bandwidth
- Sub-carriers mutually *orthogonal* in the frequency domain
- Mitigates inter-symbol interference, allows flexible utilization of spectrum

SC-FDMA uplink

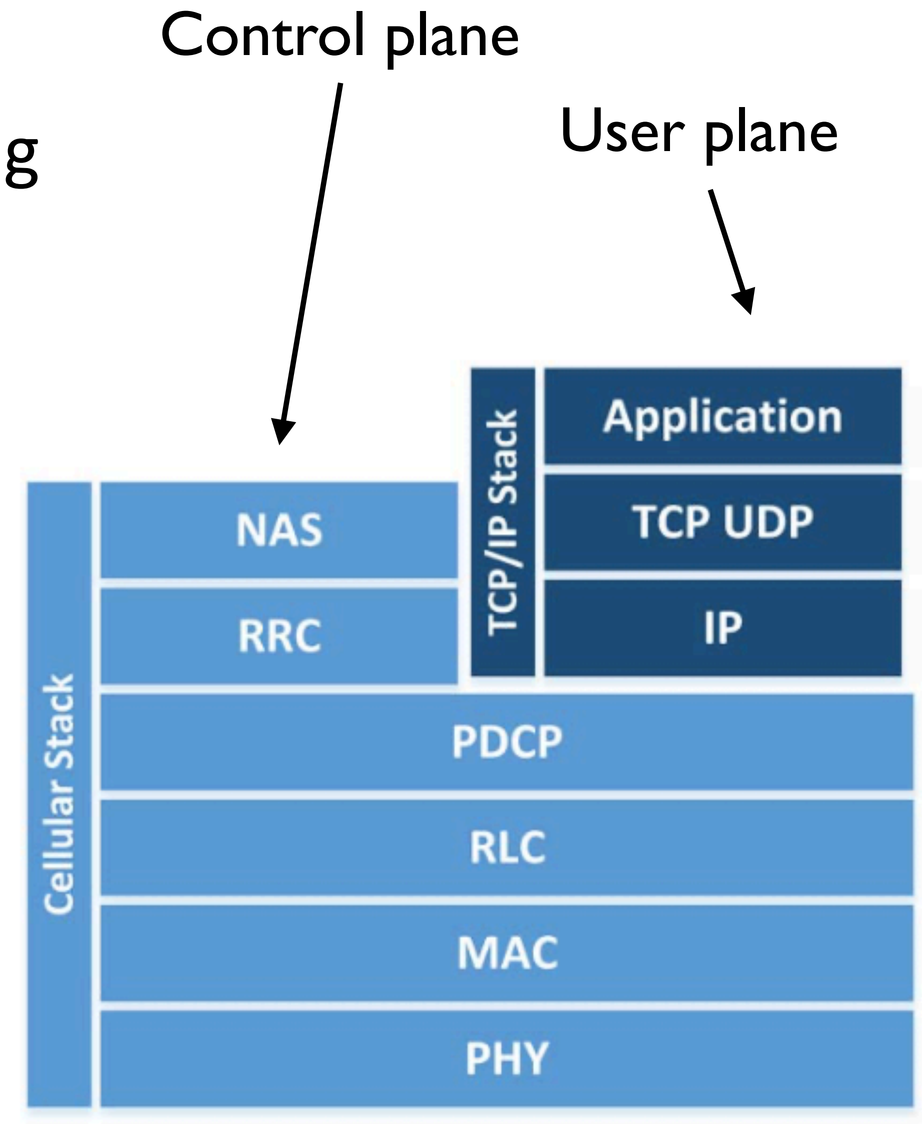
- Single-carrier FDMA



Source: Lichtman et al. LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation. IEEE Communications 2016.

LTE network protocols

- **MAC** layer
  - manages access to radio resources
- **RLC** (Radio Link Control)
  - error correction, segmentation, ordering
- **PDCP** (Packet Data Convergence Protocol)
  - compression, **encryption, integrity**
- **RRC** (Radio Resource Control)
  - system information broadcast, AKA
- **NAS** (Non-Access Stratum)
  - mobility management with the core network



Source: NIST. Guide to LTE Security. 2017.

LTE security overview

Similar Authentication and Key Agreement (AKA) as in 3G

- Mutual authentication, SQN used for replay protection

New crypto algorithms (3 variants)

- EEA = encryption, EIA = integrity
- EEA1 and EIA1 based on **Snow** (similar to KASUMI)
- EEA2 is **AES-CTR** and EIA2 is **AES-CMAC**
- EEA3 and EIA3 based on **ZUC**

Other security updates

- Extended Key Hierarchy
- Possibility for longer keys (256 bits)
- X2 handover (between eNodeBs)
- Backhaul (S1) protection

	Control plane	User plane
Encryption	operator option (often used)	operator option (often used)
Integrity	mandatory	operator option (often not used)

LTE Key Hierarchy

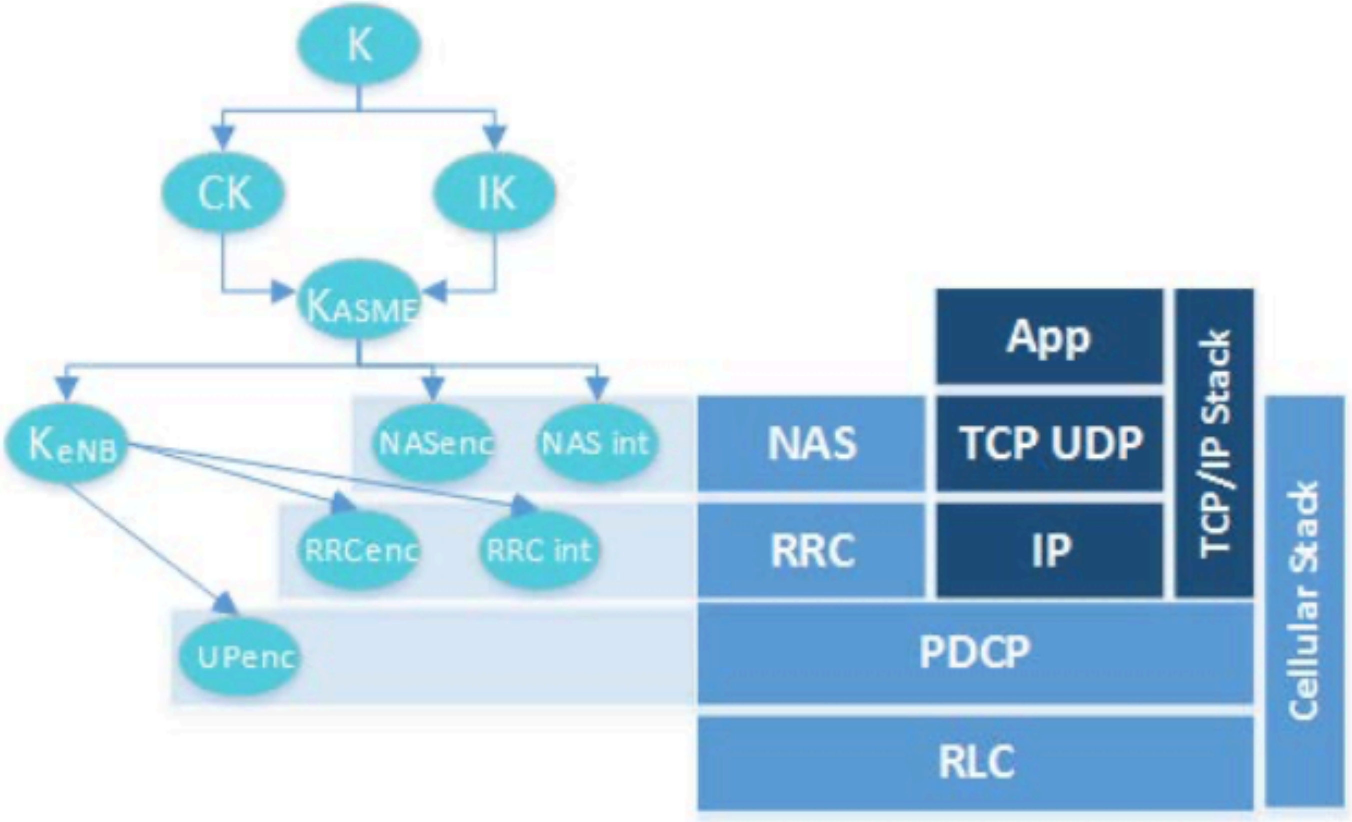
K = master key (128 bits, shared between HSS and USIM)

CK = confidentiality key (128 bits)

IK = integrity key (128 bits)

K_ASME = MME base key (256 bits)

and so on…



Source: NIST. Guide to LTE Security. 2017.

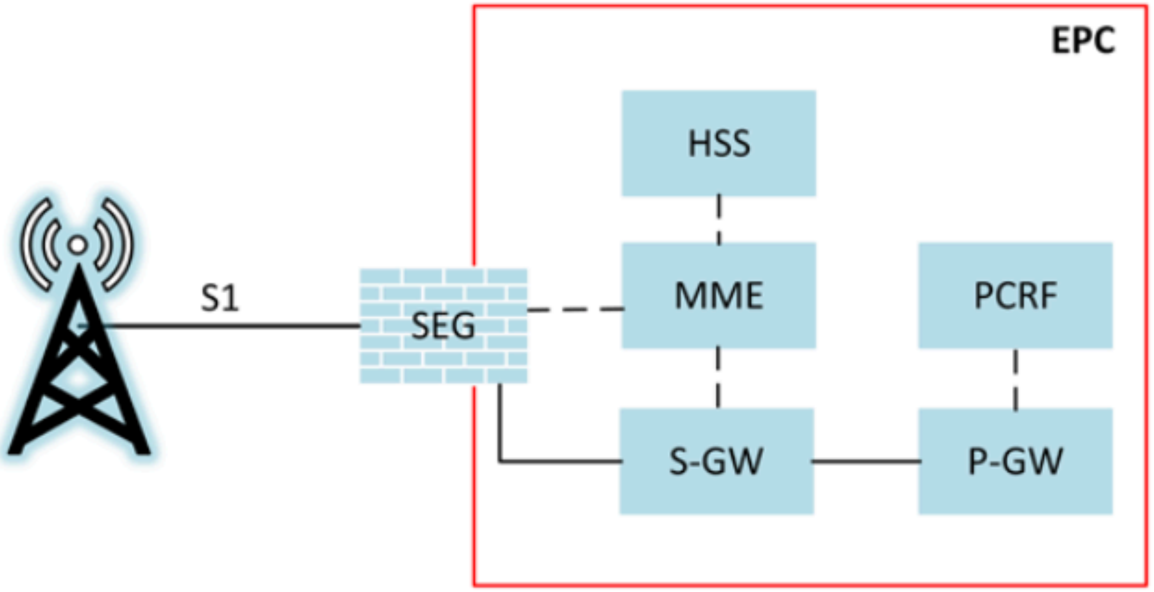
LTE backhaul and EPC protection

Backhaul (S1) protection

- Physical protection (difficult for long distances)
- Standard IP security (VPN, IPsec, PKI…)

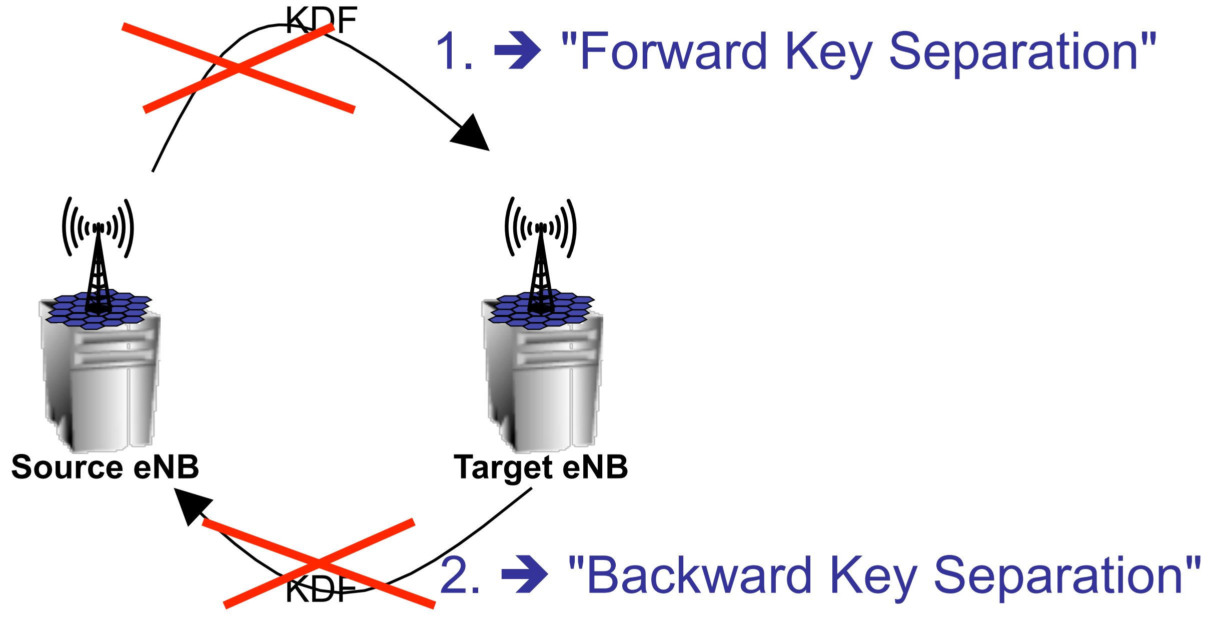
EPC protection

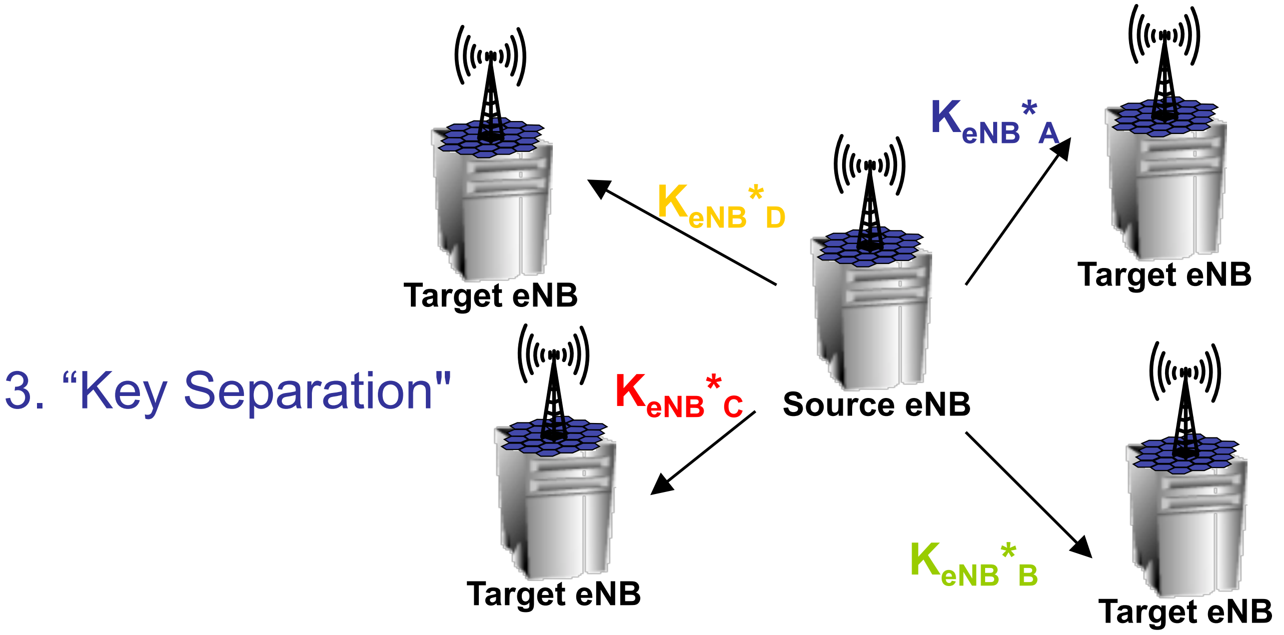
- Spec is vague: “Physical and logical division to security domains”
- Likely practice: standard IP security



LTE handovers and key updates

- LTE Security reduces the key scope and lifetime to minimize the threat of key compromise
  1. Forward key separation
     - New K_{eNB} key (called NH) from MME
  2. Backward key separation
     - Key chaining with one way hash function
  3. Key separation for different target eNBs/cells
     - Phycal cell id (PCI) and frequency bindings





LTE security research

Let’s look at three recent research examples:

- **Tracking:** Shaik et al. "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems" NDSS’16
- **Man in the middle:** Rupprecht et al. "Breaking LTE on Layer Two" S&P’19
- **Jamming:** Lichtman et al. "LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation" IEEE Communications, 2016

Other research

- **Signal injection:** Yang et al. “Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE” USENIX Security’19

Location tracking — Background

The service area of operator divided into **Tracking Areas** (TAs)

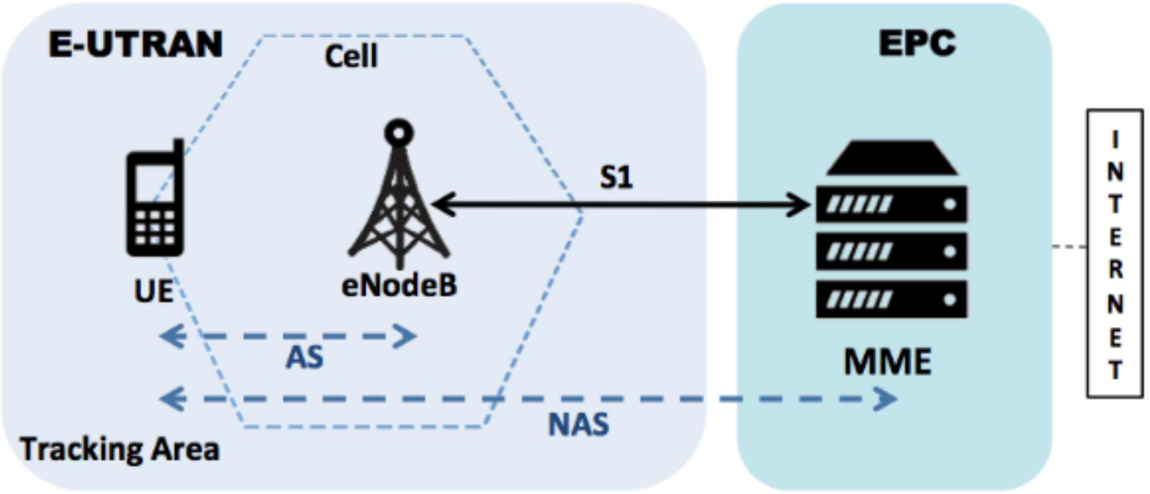
- contains a group of cells, each controlled by an eNodeB

eNodeB broadcasts operator-specific information

- Tracking Area code, Mobile Network code, cell ID

UE sends IMSI in first Attach request

- operator assigns **temporary identifier** (TMSI, GUTI)
- used for subsequent attach and paging



Location tracking — Adversary

Adversary capabilities:

- who can **receive and send over-the-air**
- possible with inexpensive equipment

Adversary goal:

- learn user's location

Attack-enabling observations:

- **GUTI reallocation depends on operator**
- Example: same GUTI for 3 days

Adversary with Universal Software Radio Peripheral (USRP)

Location tracking — Attack

Step 1: Setup fake BS

- Broadcast valid TA code, network code with higher power (or priority)

Step 2: Learn user presence in Tracking Area (TA)

- Repeated short Voice over LTE (VoLTE) calls or social media messages
- Adversary monitor any cell within Tracking Area
- Some intersection analysis… (details skipped)

Step 3: Learn precise location

- Fake BS sends unprotected “RRC Connection Reconfig” messages
- UE computes signal power for neighboring cells and responds with a “Measurement report”
- Measurement report contain UE’s GPS coordinates

Location tracking — Analysis

All signaling (control messages) should be integrity-protected…

- So how is this possible?

Attack root cause

- **LTE spec allows unprotected RRC measurement reports**
- This is an explicit exception to general policy
- Benign use: connection troubleshooting

Likely reason for such design decision

- Availability was seen more important than privacy in this particular case

How significant is such attack in practice?

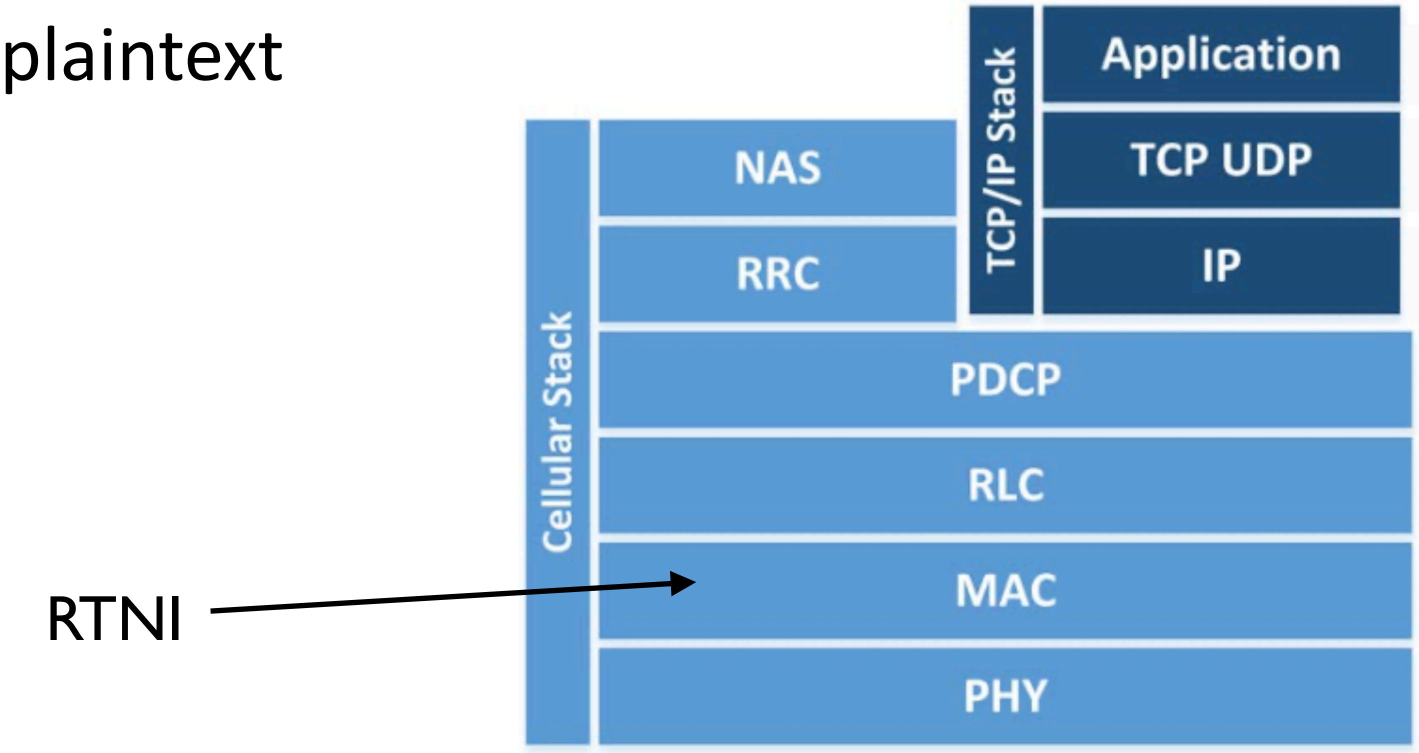
Man in the middle — Background

MAC layer: each UE must be uniquely distinguishable and needs a *Radio Network Temporary Identity (RNTI)*

eNodeB: utilizes *Downlink Control Information (DCI)* to notify when radio resources are available on downlink and uplink

Recall that LTE encryption using AES-CTR

- XOR keystream with plaintext

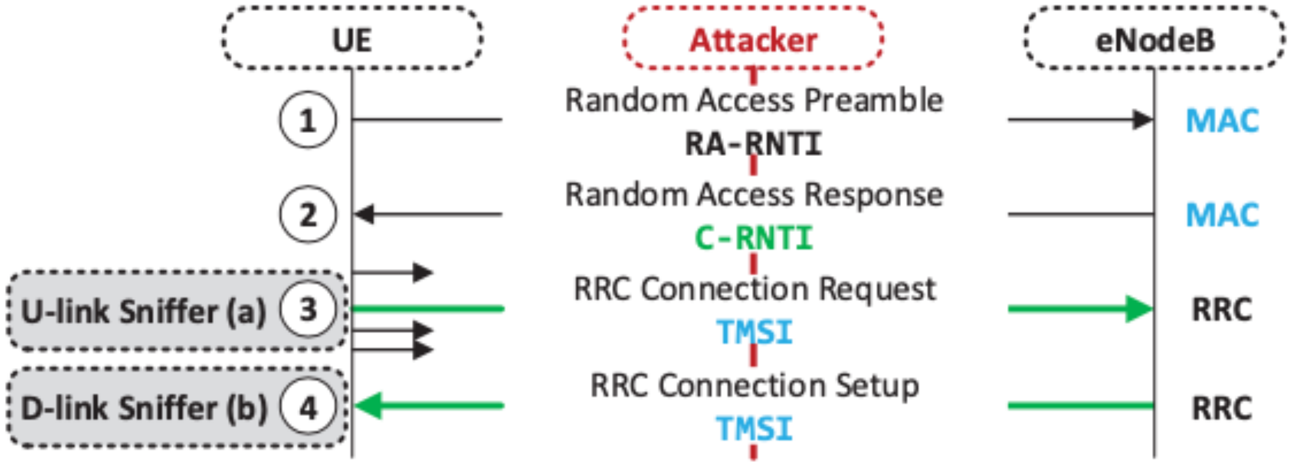


Man in the middle — Attack

Attacker model: low-budget software-defined radio

Step 1: Learn user from encrypted traffic

- exploit temporary identifier on MAC layer
- observe connection establishment
- learn both TMSI and RTNI (few details skipped)
- use paging to map TMSI to phone number



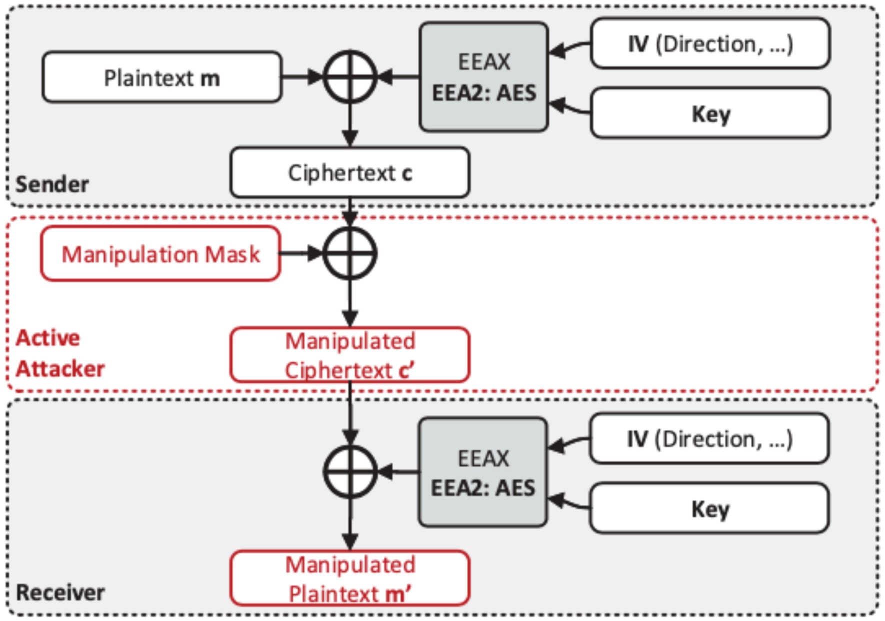
Enables traffic profiling!

Source: Rupprecht et al. Breaking LTE on Layer Two. S&P'19.

Man in the middle (3/4)

Step 2: Modify encrypted traffic —> redirection

- UE send encrypted packet to intended DNS server
- Adversary captures DNS request and applies "manipulation mask"
- Adversary forwards the manipulated packet
- Packet get decrypted and **delivered to false DNS server**



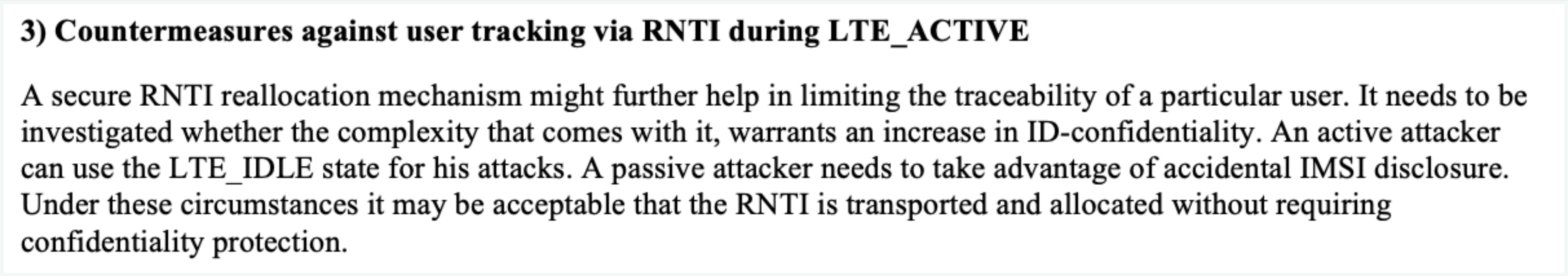
Source: Rupprecht et al. Breaking LTE on Layer Two. S&P'19.

Man in the middle — Analysis

Attack root causes

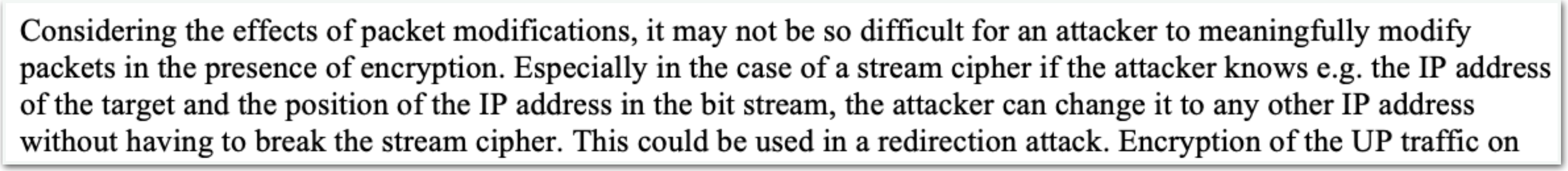
- Identifiers on lower stack levels (RTNI on MAC layer) while encryption done on higher levels (PDCP)
- Integrity protection optional

From LTE specification:



3) Countermeasures against user tracking via RNTI during LTE_ACTIVE

A secure RNTI reallocation mechanism might further help in limiting the traceability of a particular user. It needs to be investigated whether the complexity that comes with it, warrants an increase in ID-confidentiality. An active attacker can use the LTE_IDLE state for his attacks. A passive attacker needs to take advantage of accidental IMSI disclosure. Under these circumstances it may be acceptable that the RNTI is transported and allocated without requiring confidentiality protection.



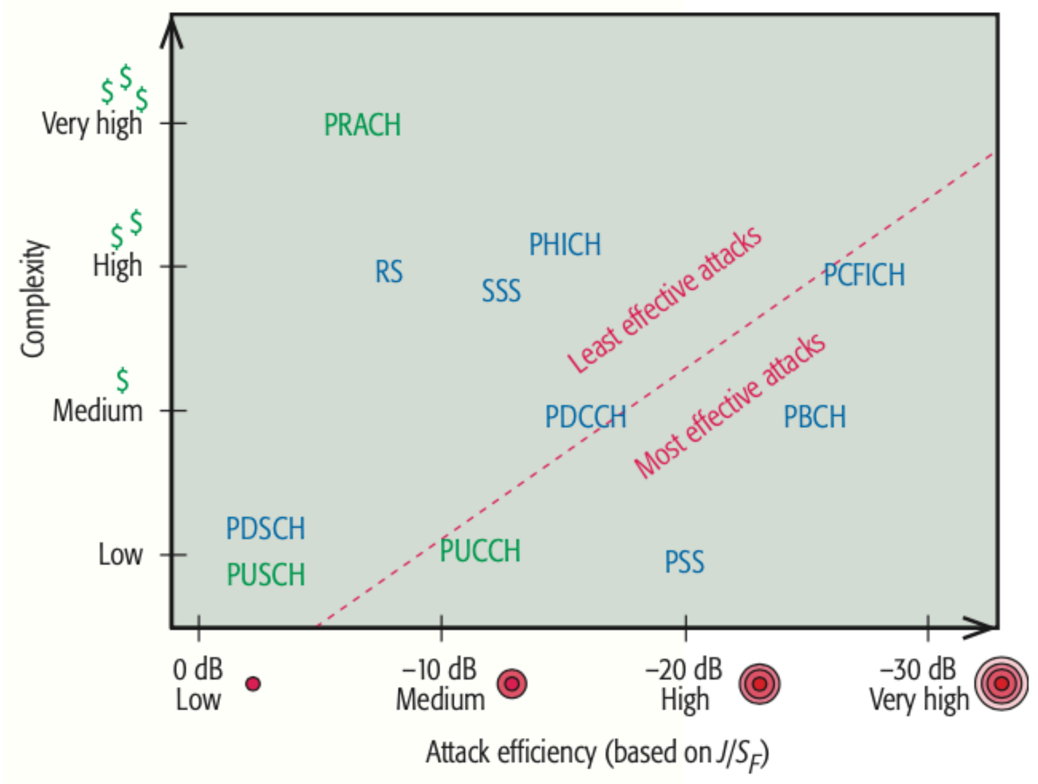
Considering the effects of packet modifications, it may not be so difficult for an attacker to meaningfully modify packets in the presence of encryption. Especially in the case of a stream cipher if the attacker knows e.g. the IP address of the target and the position of the IP address in the bit stream, the attacker can change it to any other IP address without having to break the stream cipher. This could be used in a redirection attack. Encryption of the UP traffic on

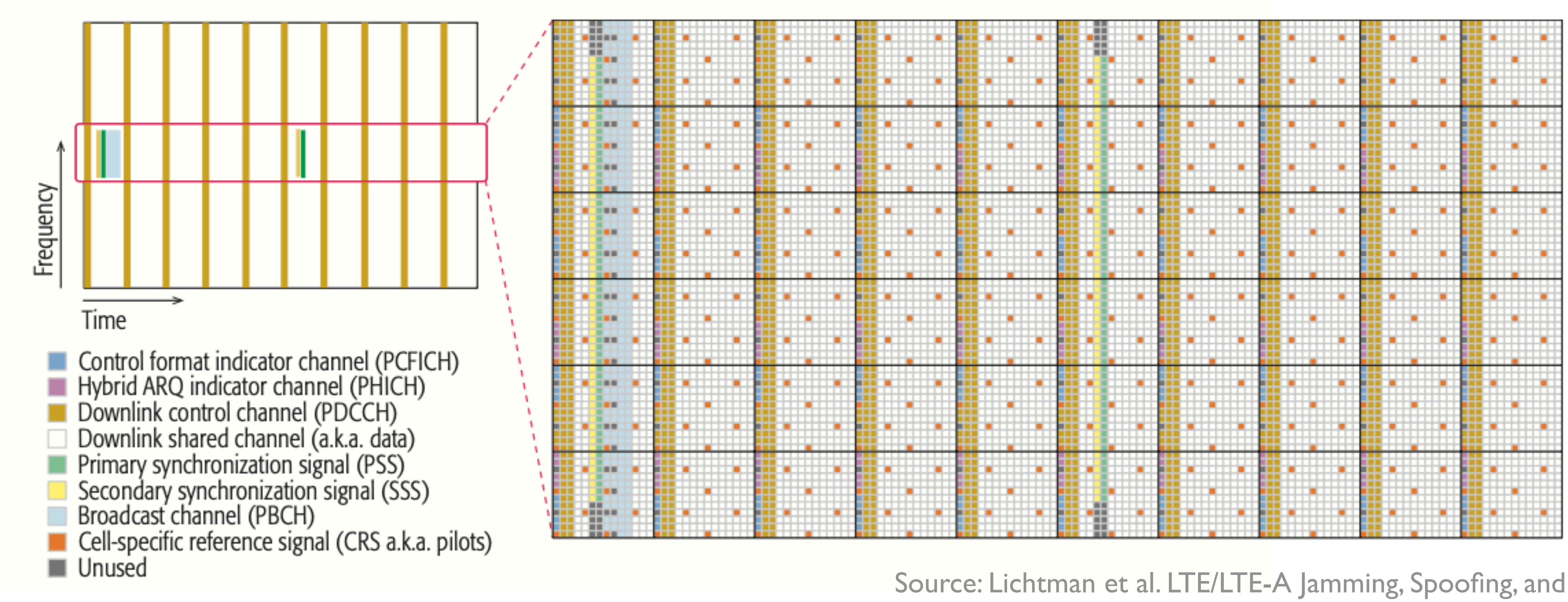
Threats were well-known some 10 years ago…

Jamming

Targeted jamming of different control channels and signals have different difficulty and effectiveness…

Brute force always possible…





Source: Lichtman et al. LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation. IEEE Communications 2016.

4G / LTE security summary

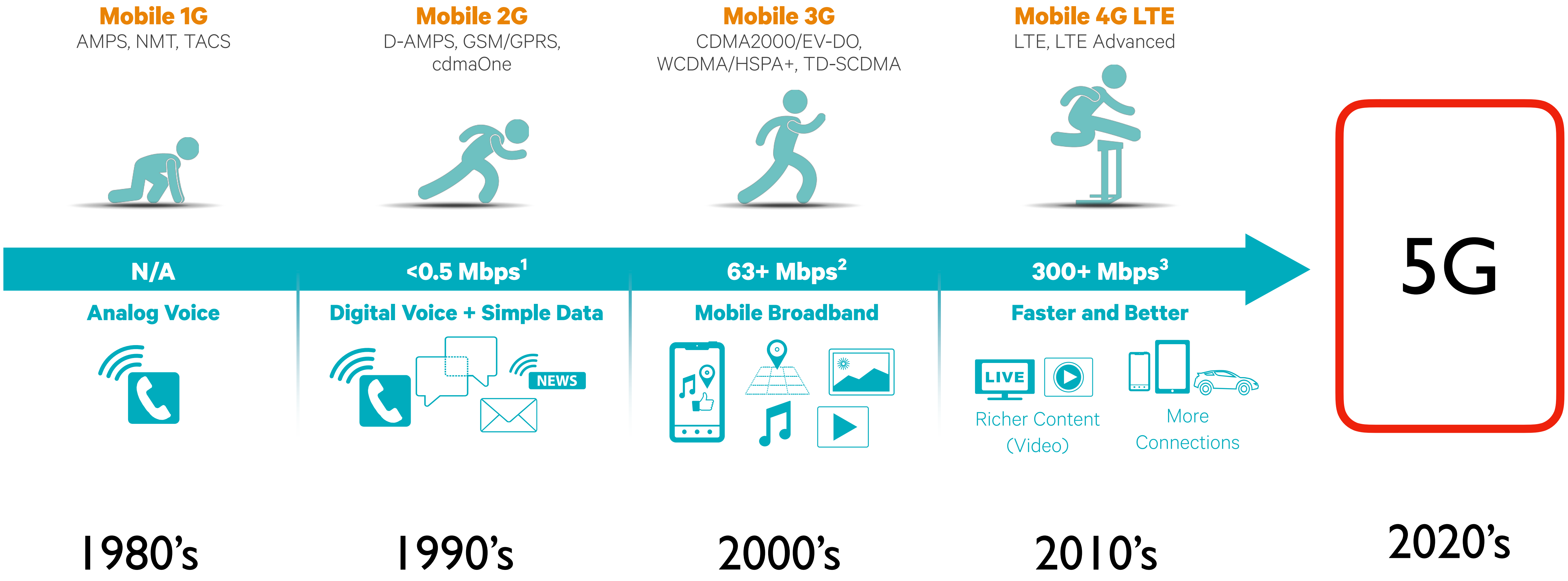
Security updates

- New crypto algorithms (Snow and AES)
- New core network (EPC)
- Minor security updates like extended key hierarchy, handover protection, backhaul protection…

Remaining issues

- Limited user tracking
- Minor integrity violation
- User traffic profiling

Fifth generation



Mobile 1G
AMPS, NMT, TACS

N/A

Analog Voice

1980's

Mobile 2G
D-AMPS, GSM/GPRS, cdmaOne

<0.5 Mbps[1]

Digital Voice + Simple Data

1990's

Mobile 3G
CDMA2000/EV-DO, WCDMA/HSPA+, TD-SCDMA

63+ Mbps[2]

Mobile Broadband

2000's

Mobile 4G LTE
LTE, LTE Advanced

300+ Mbps[3]

Faster and Better

Richer Content (Video)

More Connections

2010's

5G

2020's

5G overview

Deployments planned to start “soon“

Radio link: 5G New Radio (NR)

- Faster: e.g., 10 Gbps with 2ms latency
- Optimized OFDM
- Massive MIMO
- Two frequency ranges
  - FR1 (below 6Ghz) and FR2 (above 24 Ghz, mmWave)
- Various cell sizes
- Better support for different QoS requirements

Suggested usages

- IoT, AR/VR, entertainment, home broadband…

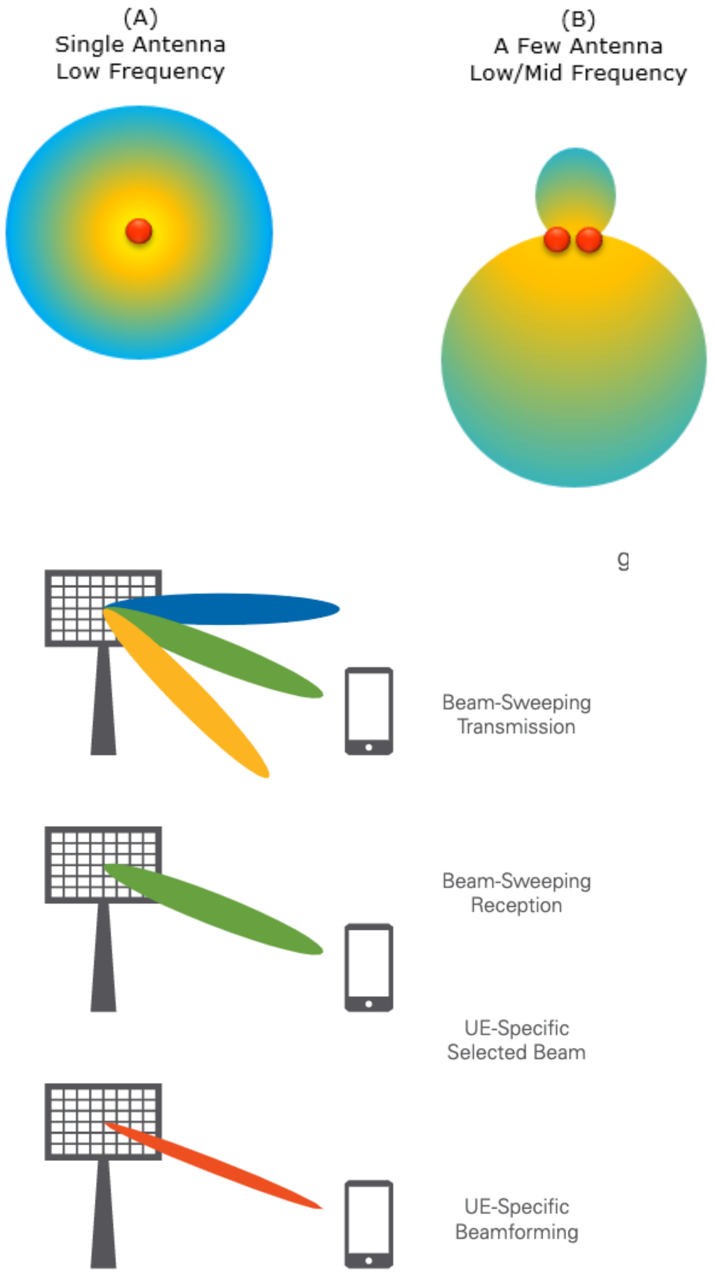
Some 5G physical layer features

Beam management using “massive MIMO”

Higher frequencies

- cannot penetrate solid objects
- shorter ranges
- less inference
- more devices per m2

Cell types: micro, macro, pico



Source: Native Instruments. 5G New Radio White Paper.

5G security overview

Crypto algorithms: mostly the same

AKA protocol: minor improvements

- better replay protection as SIM can generate nonces

User tracking: minor updates

- SIMs can encrypt IMSI/TMSI for home operator's public key
- More strict policies for updating temporary IDs like TMSI

Fake base station detection — heuristics like expected signal strengths…?

Examples of 5G security research

Basin et al. "A Formal Analysis of 5G Authentication" CCS’18

- Formal modeling and verification of 5G AKA
- Found minor inconsistencies in the spec

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

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

From 1G to 5G

	1G	2G	3G	4G	5G
crypto algorithms	none	weak	strong	strong	strong
AKA	none	one-way	mutual	mutual	mutual
core network	SS7	SS7	SS7	EPC	EPC
tracking	easy	limited	limited	limited	more limited?
fake BS	easy	easy	limited	limited	challenging?
jamming / DoS	possible	possible	possible	possible	possible

Discussion

Lecture end

Summary

- Cellular security evolution from 1G to 5G
- Radio link, core network, crypto, protocols, management…
- Common theme: security vs. functionality and cost
- Risks of global communication systems more broadly

Reading material:

- Rupprecht et al. "Breaking LTE on Layer Two" S&P'19