Hiding in Plain Signal:
Physical Signal Overshadowing Attack on LTE

Hojoon Yang, Sangwook Bae, Mincheol Son,
Hongil Kim, Song Min Kim, and Yongdae Kim

USENIX Security 2019

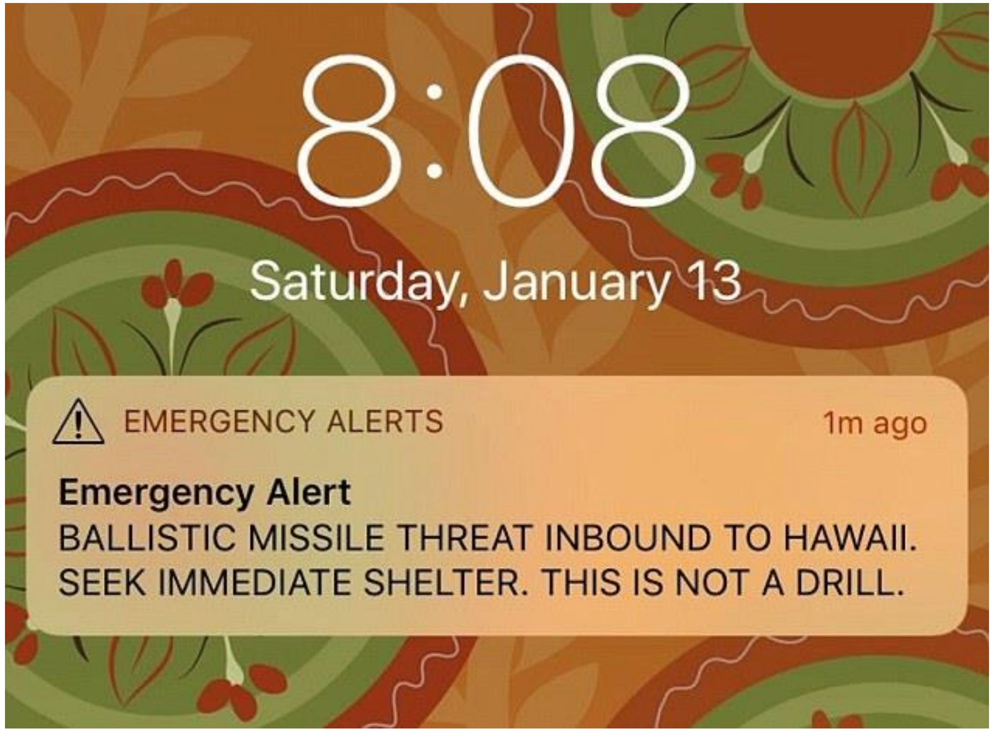
LTE is Everywhere

Voice

Data

Emergency SMS

…



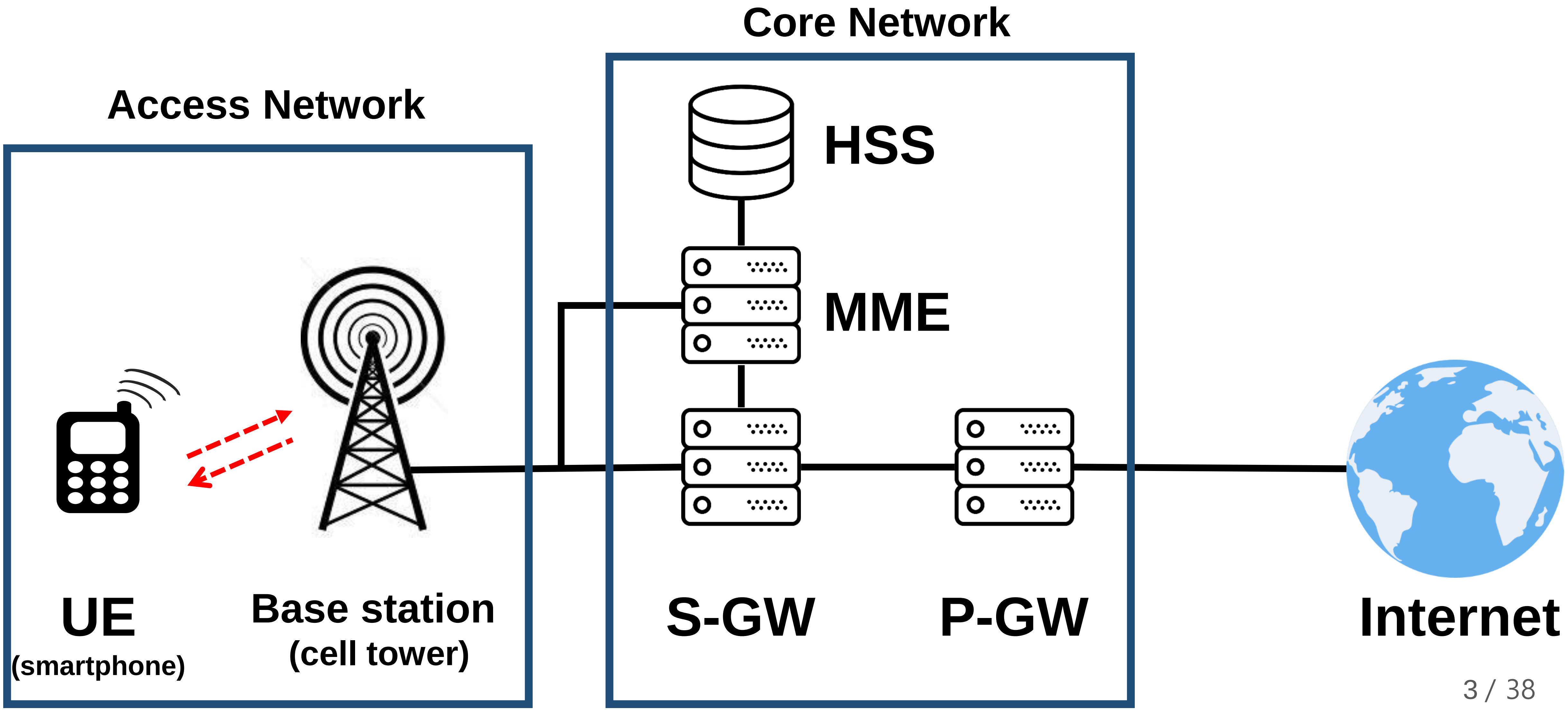
8:08

Saturday, January 13

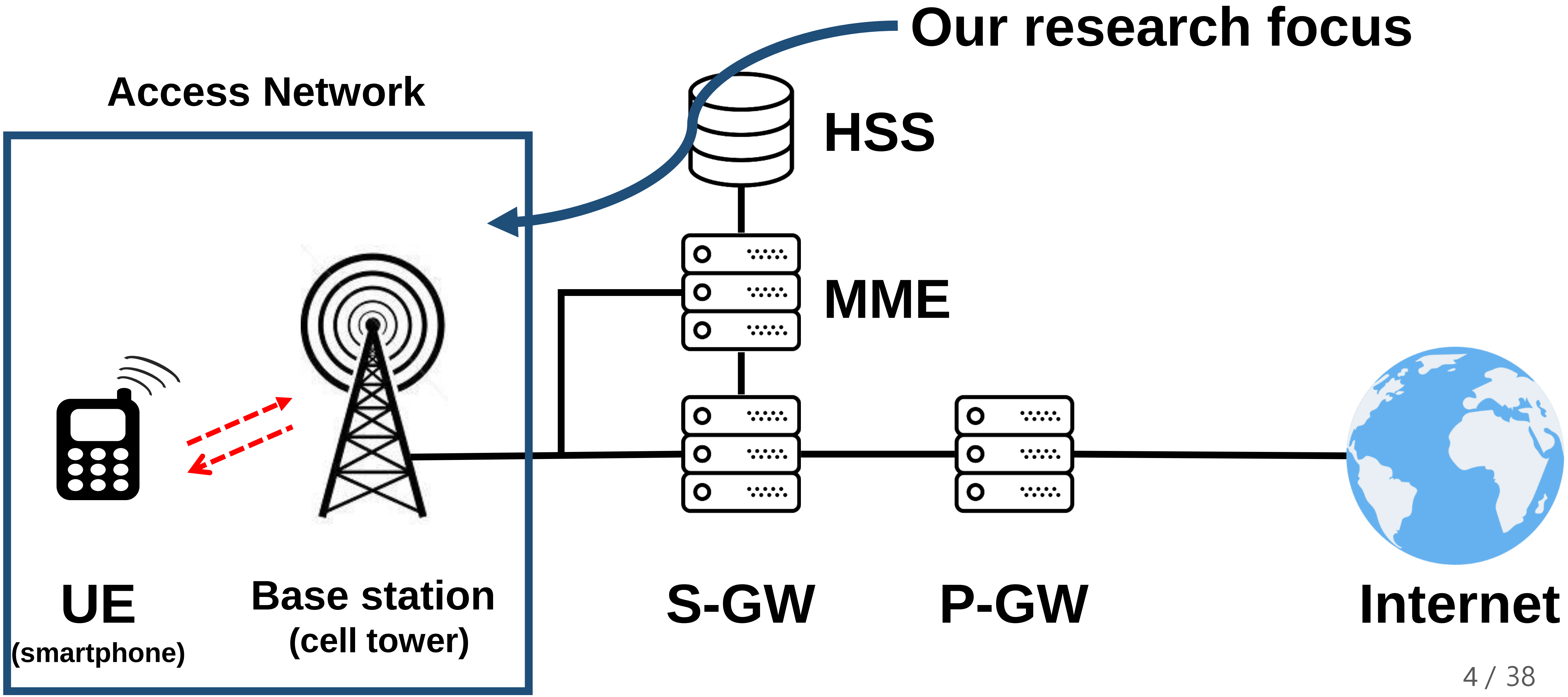
EMERGENCY ALERTS 1m ago

Emergency Alert
BALLISTIC MISSILE THREAT INBOUND TO HAWAII.
SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.

LTE Architecture Overview



LTE Architecture Overview



LTE security

- Most LTE control-plane messages are integrity protected
  - **Only after** UE authentication (after sharing security context)

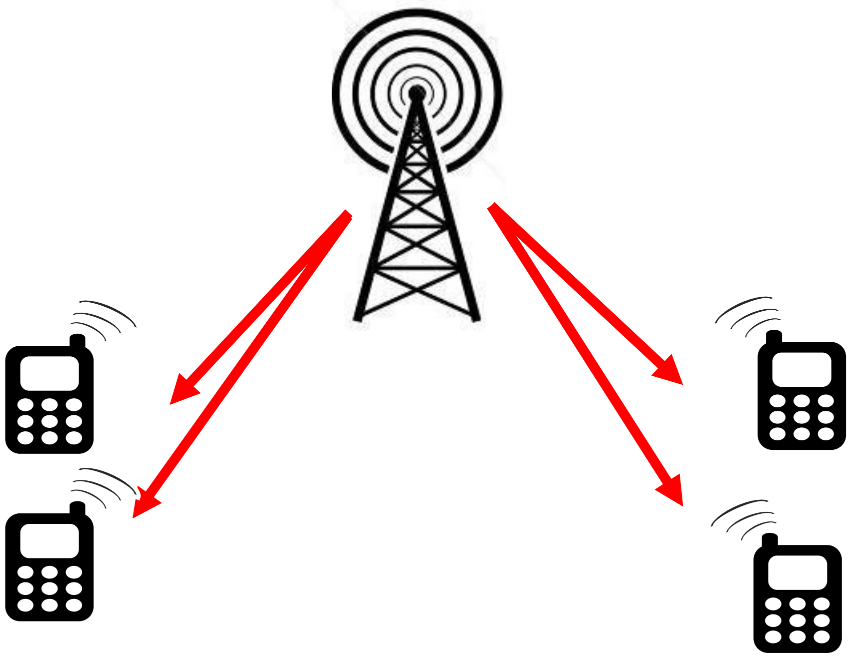
- Messages before authentication? **Not secure!**

- One of them is **broadcast messages**
  - Have never been integrity protected!
  - Thus, it is ***vulnerable***

Broadcast Messages

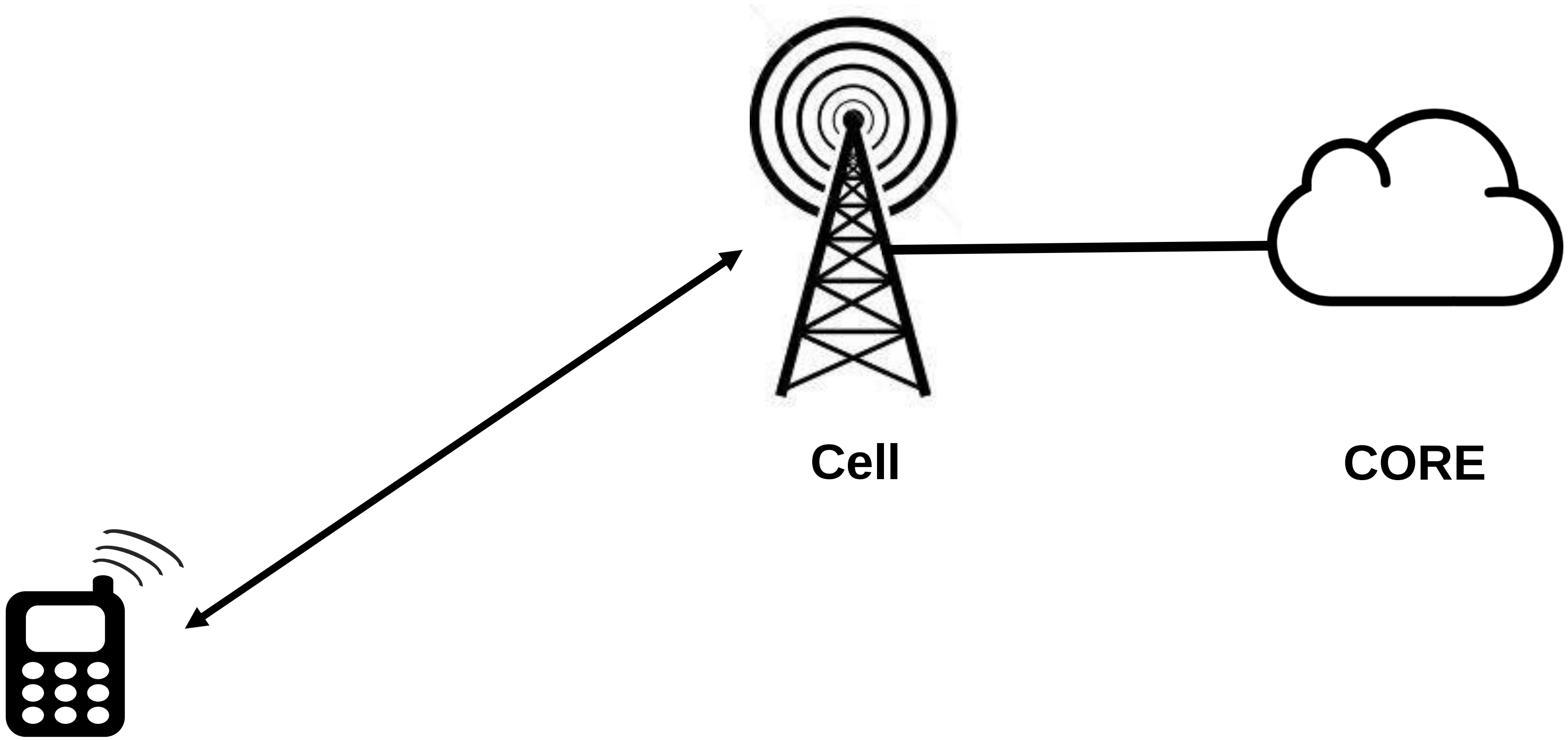
- Terminology
  - Messages targeting multiple UEs within a cell at the same time
  - Not a formal Terminology though ☺

- Messages
  - Paging
    - Establish connection with UE
  - System Information Block (SIB)
    - Tell cell information to UEs
  - …



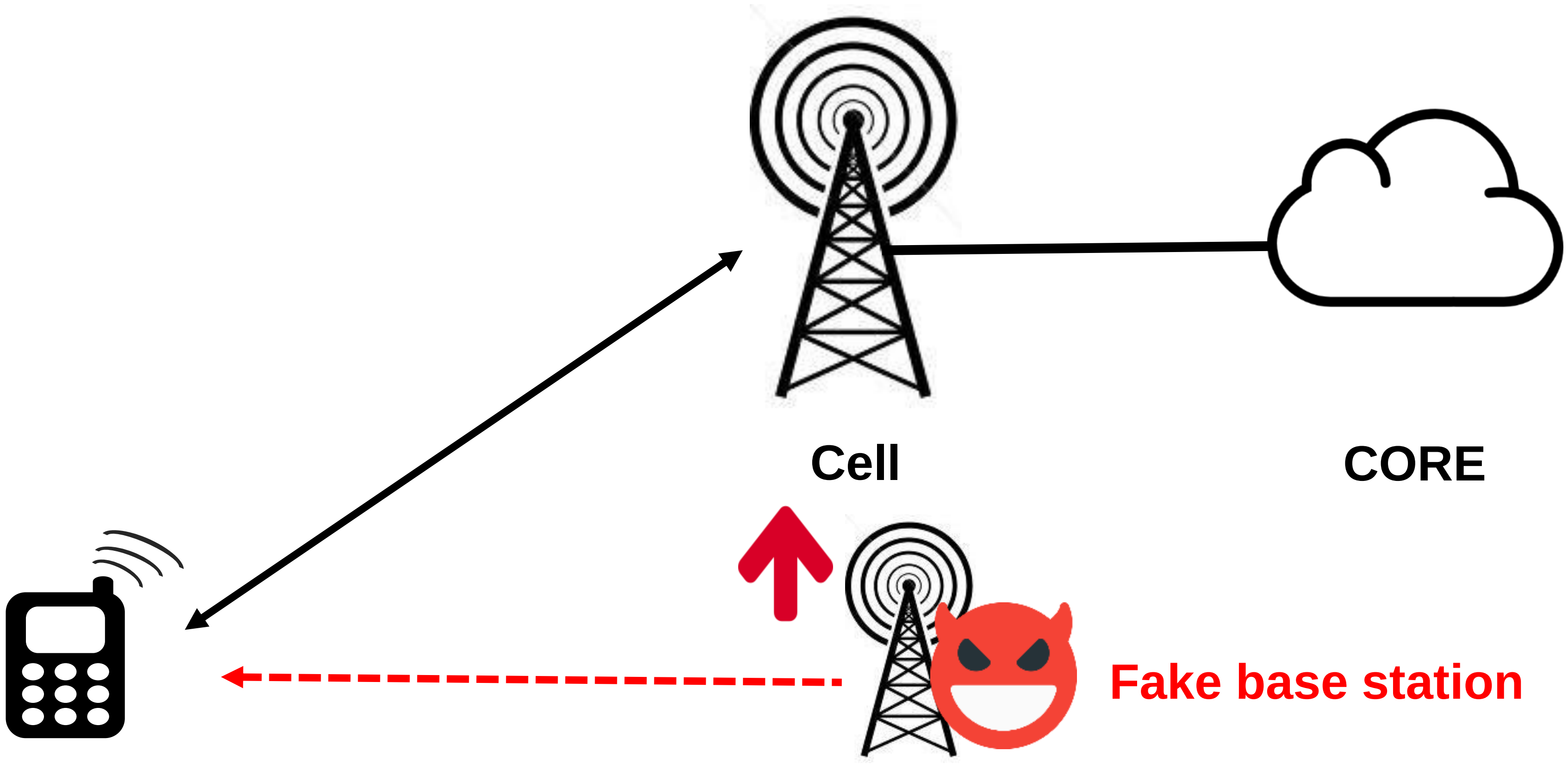
Playing with Broadcast Messages

- How can an attacker send a *malicious* broadcast messages to the UE?



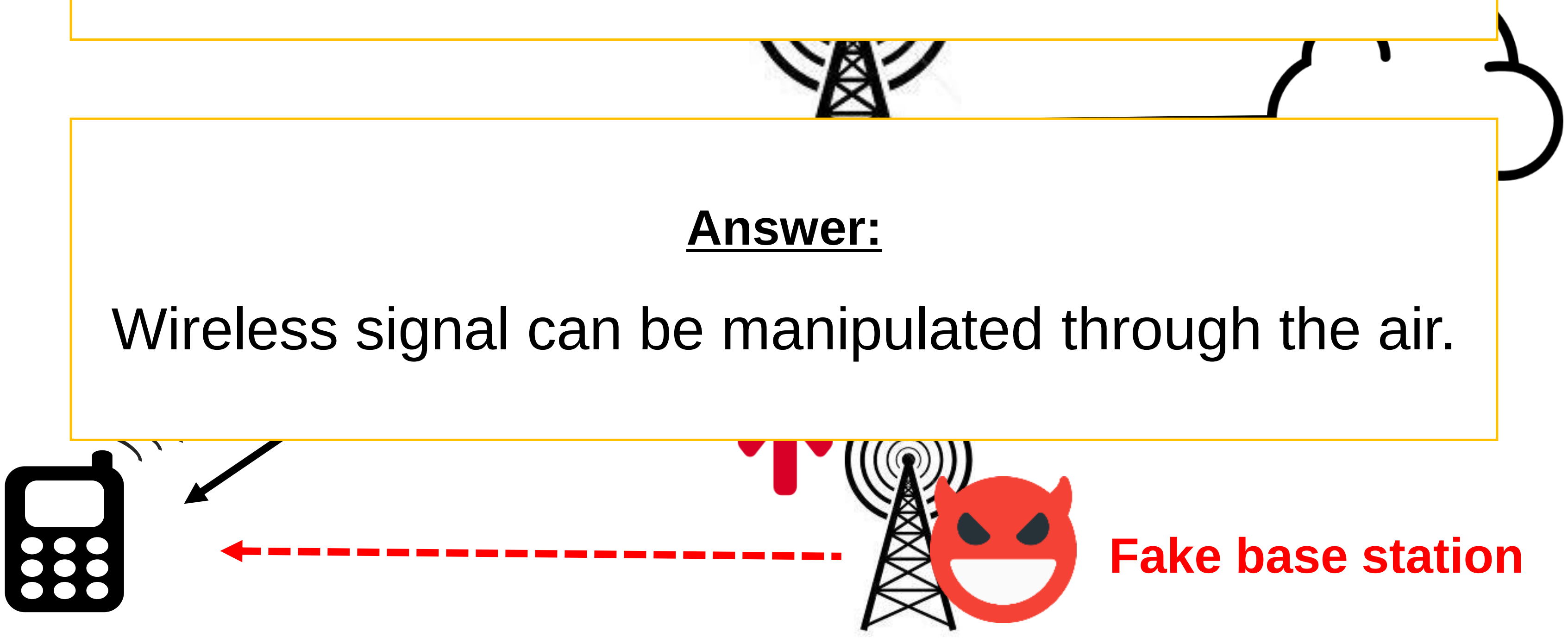
Playing with Broadcast Messages

- Previously, the only way is to use fake base station (FBS)



Playing with Broadcast Messages

- Previously, the only way is to use fake base station (FBS)



Question:

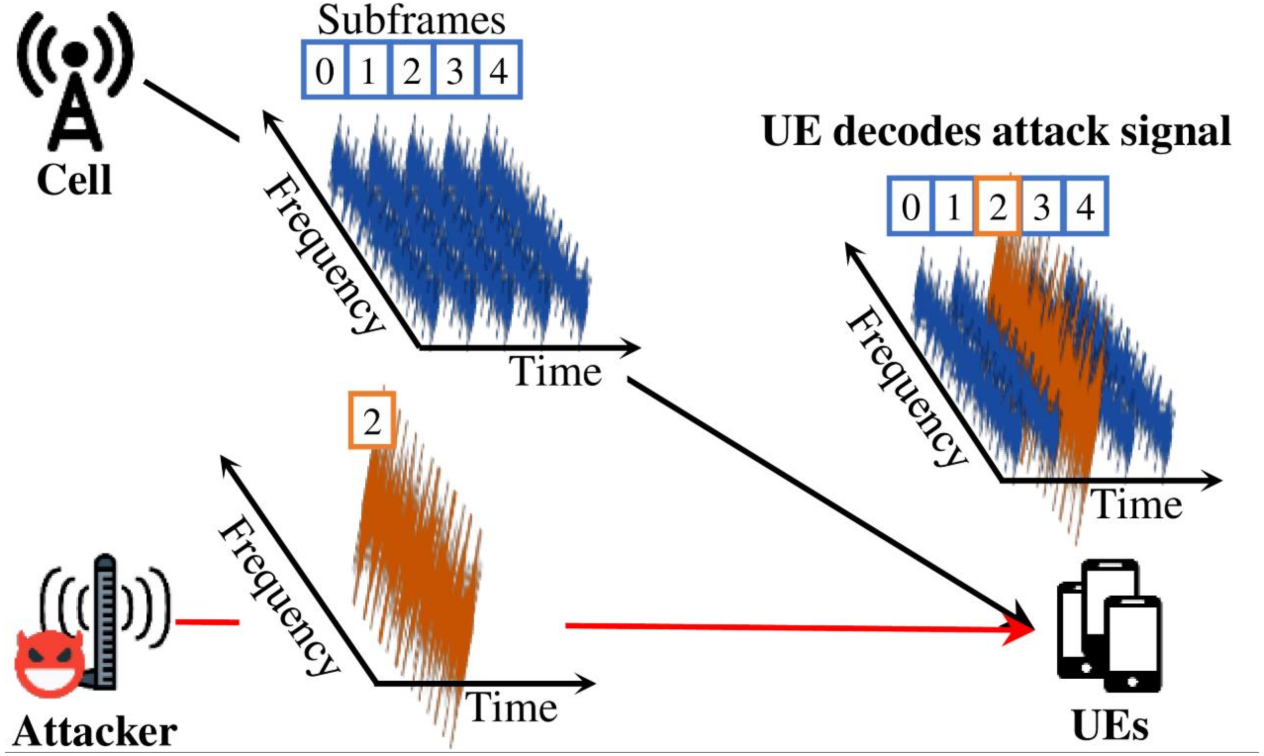
Is REALLY FBS the only way? What else?

Answer:

Wireless signal can be manipulated through the air.

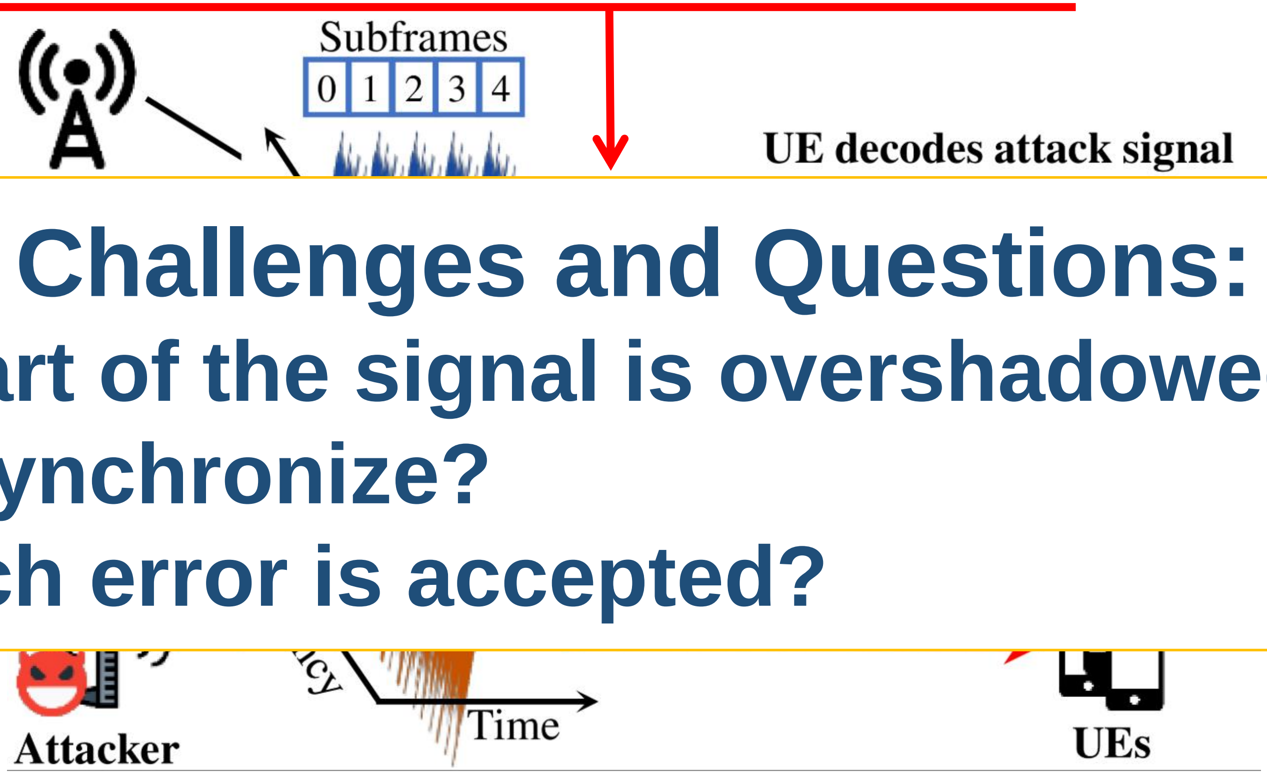
Signal Overshadowing (SigOver)

- Exploiting fundamental weakness of the wireless comm.
  - Wireless signal can be counterfeited by intentional signal
- Transmit **time and frequency synchronized** signal



Signal Overshadowing (SigOver)

- Exploiting fundamental weakness of the wireless comm.
  - Wireless signal can be counterfeited by intentional signal
- Transmit **time and frequency synchronized** signal

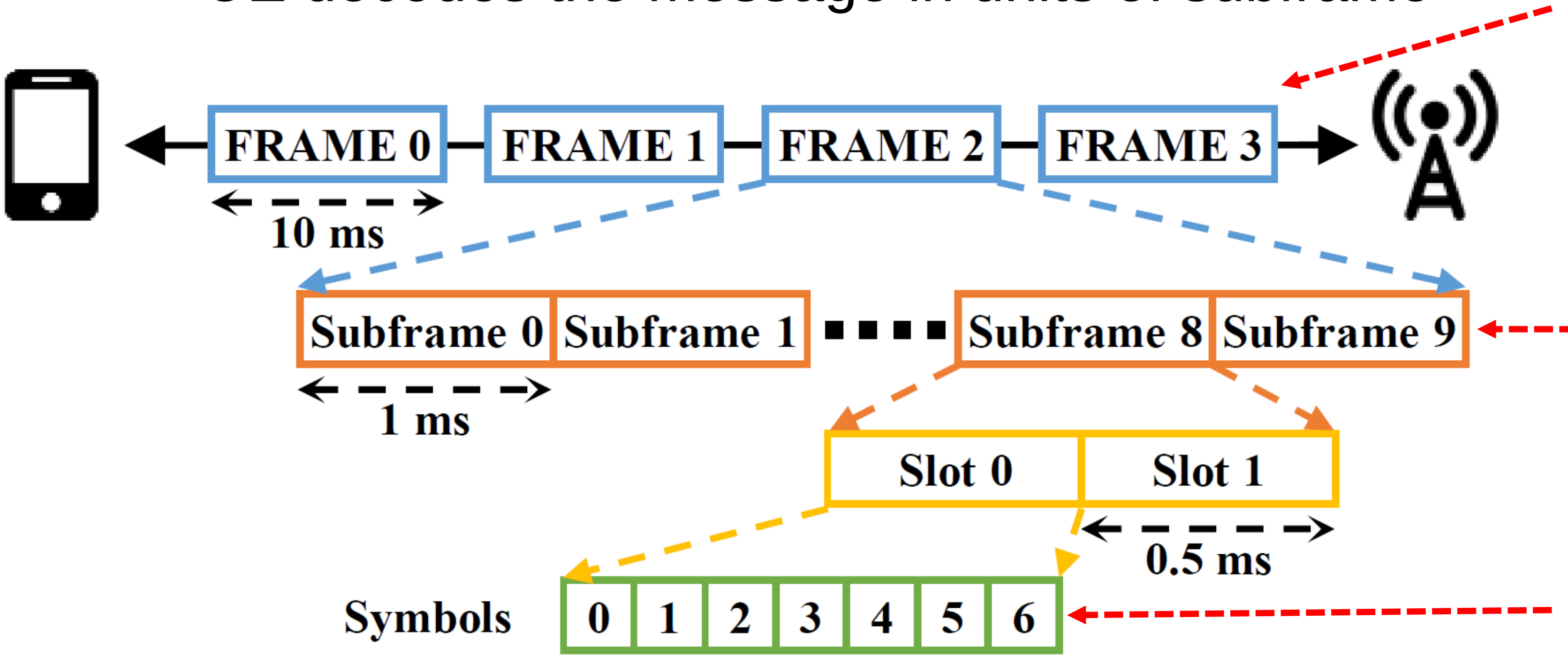


Challenges and Questions:

1. **Which part of the signal is overshadowed?**
2. **How to synchronize?**
3. **How much error is accepted?**

Attack Design

- Which part of the signal is overshadowed?
  - SigOver overshadows **a Subframe**
  - UE decodes the message in units of subframe



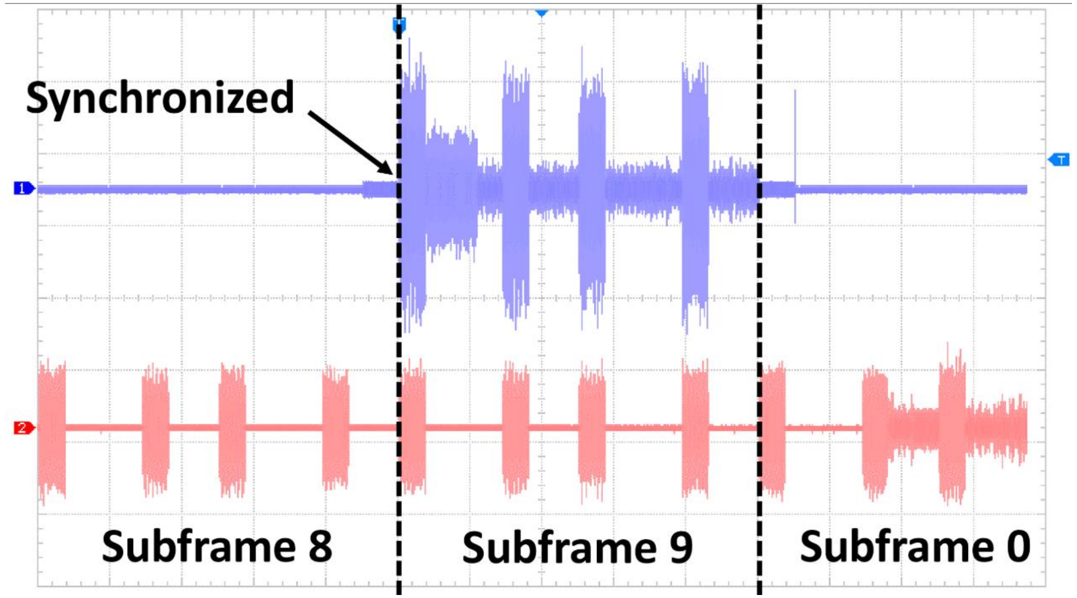
☹ Affects other msg.

☺ Our decision

☹ Low success rate

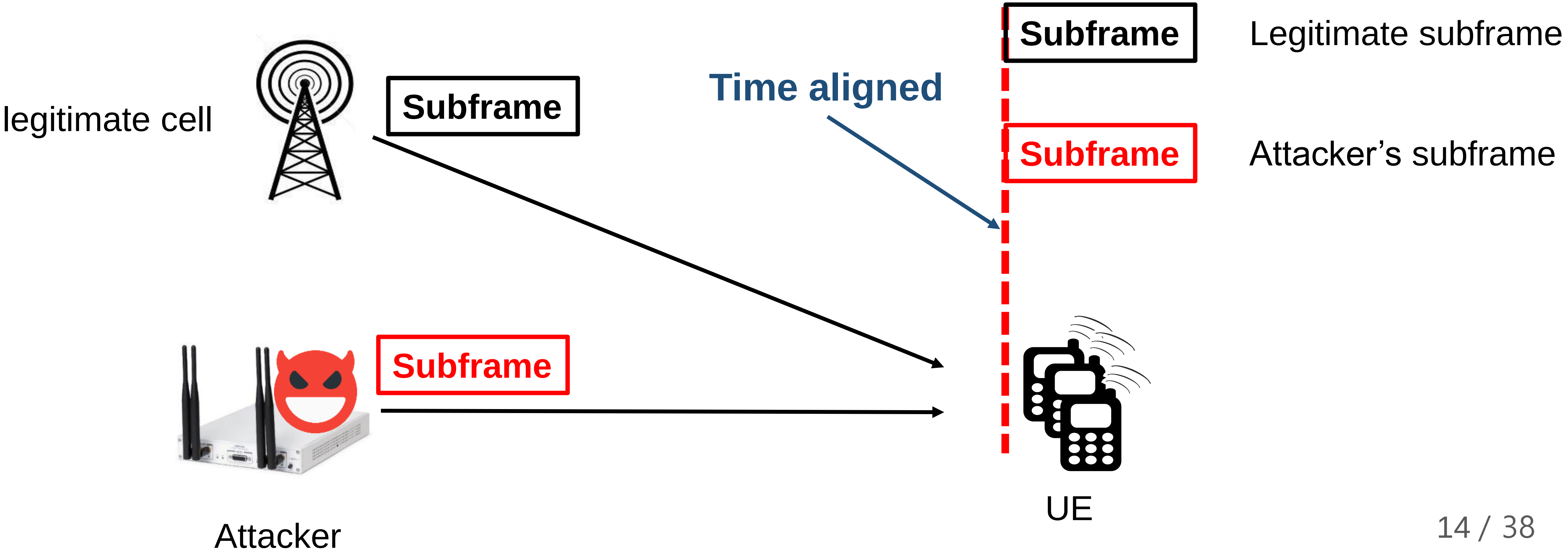
Attack Design

- Crafted subframe
    - Pilot symbols
        - Pilot of the attacker will help the victim to decode the message properly
    - Malicious messages
        - Consists of various channel (PDCCH, PDSCH)



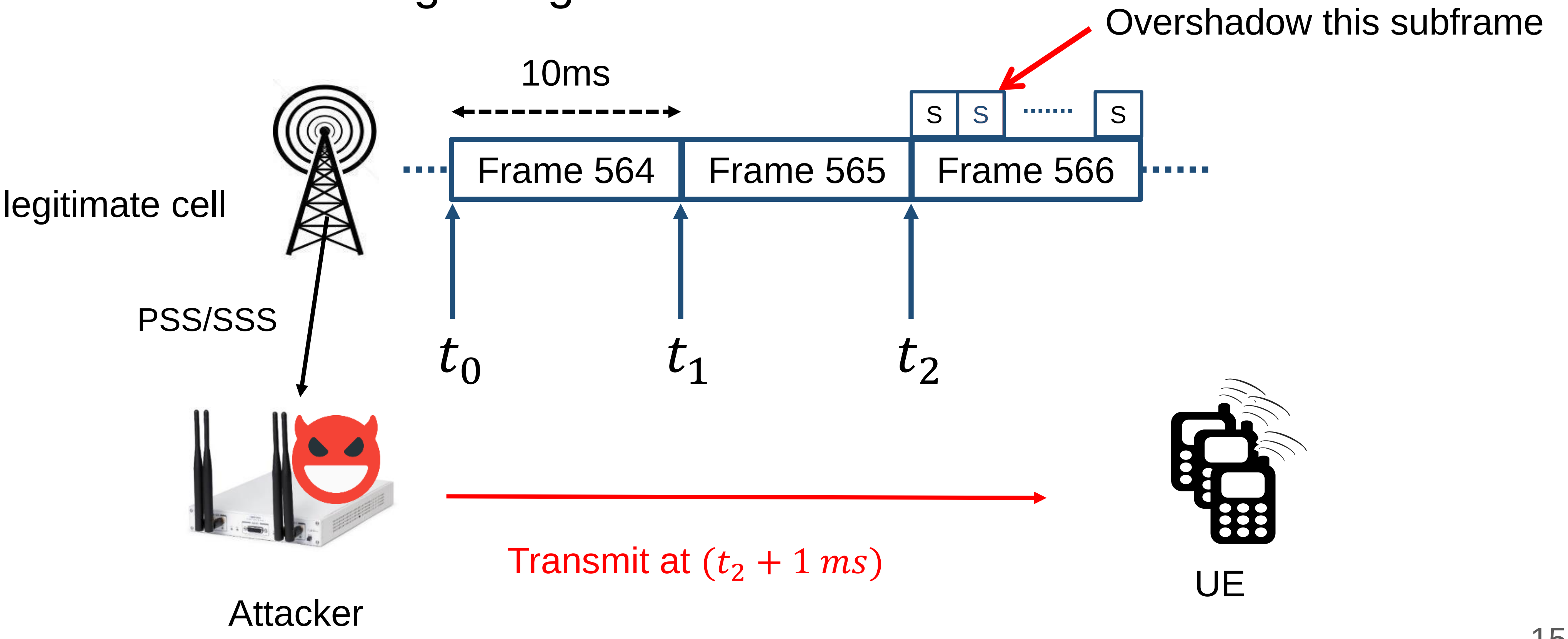
Time Synchronization

- Attacker’s subframe and legitimate subframe must arrive at the UE simultaneously
- For simplicity, let’s assume there is no propagation delay



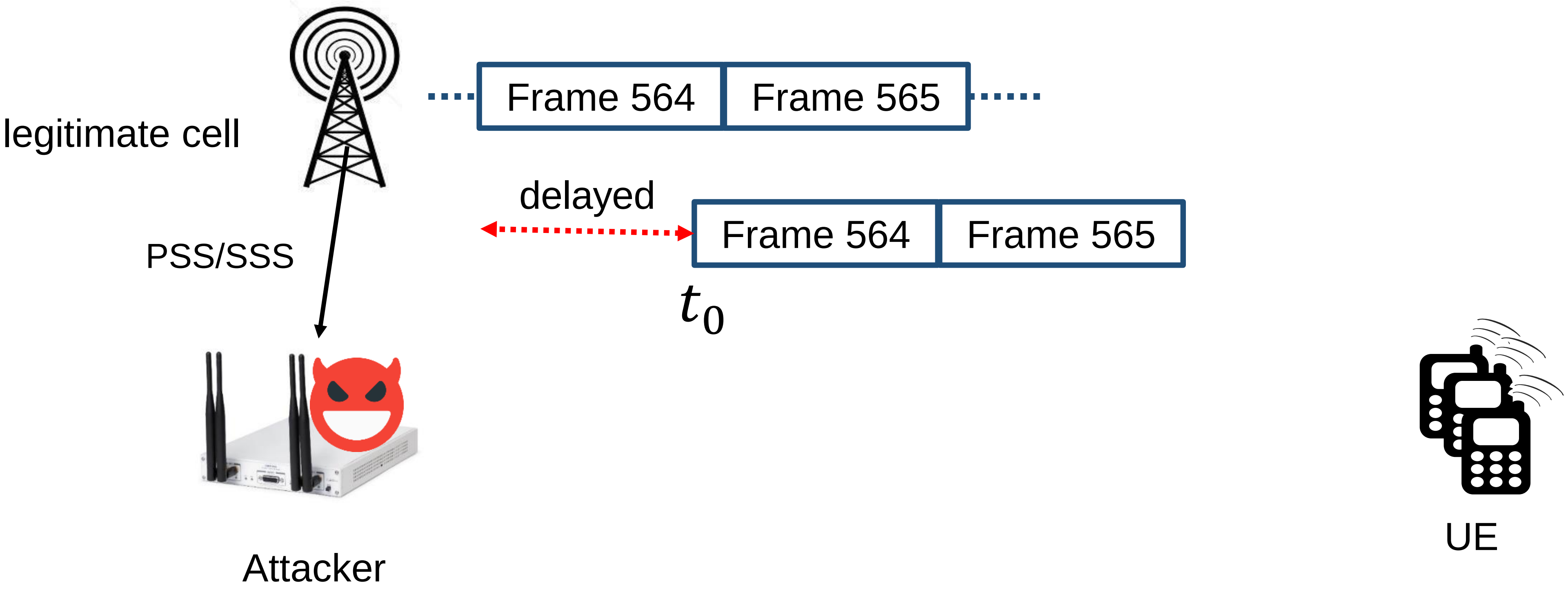
Time Synchronization

- Use synchronization signal (PSS/SSS) of the legitimate cell
  - Locate frame timing of legitimate cell



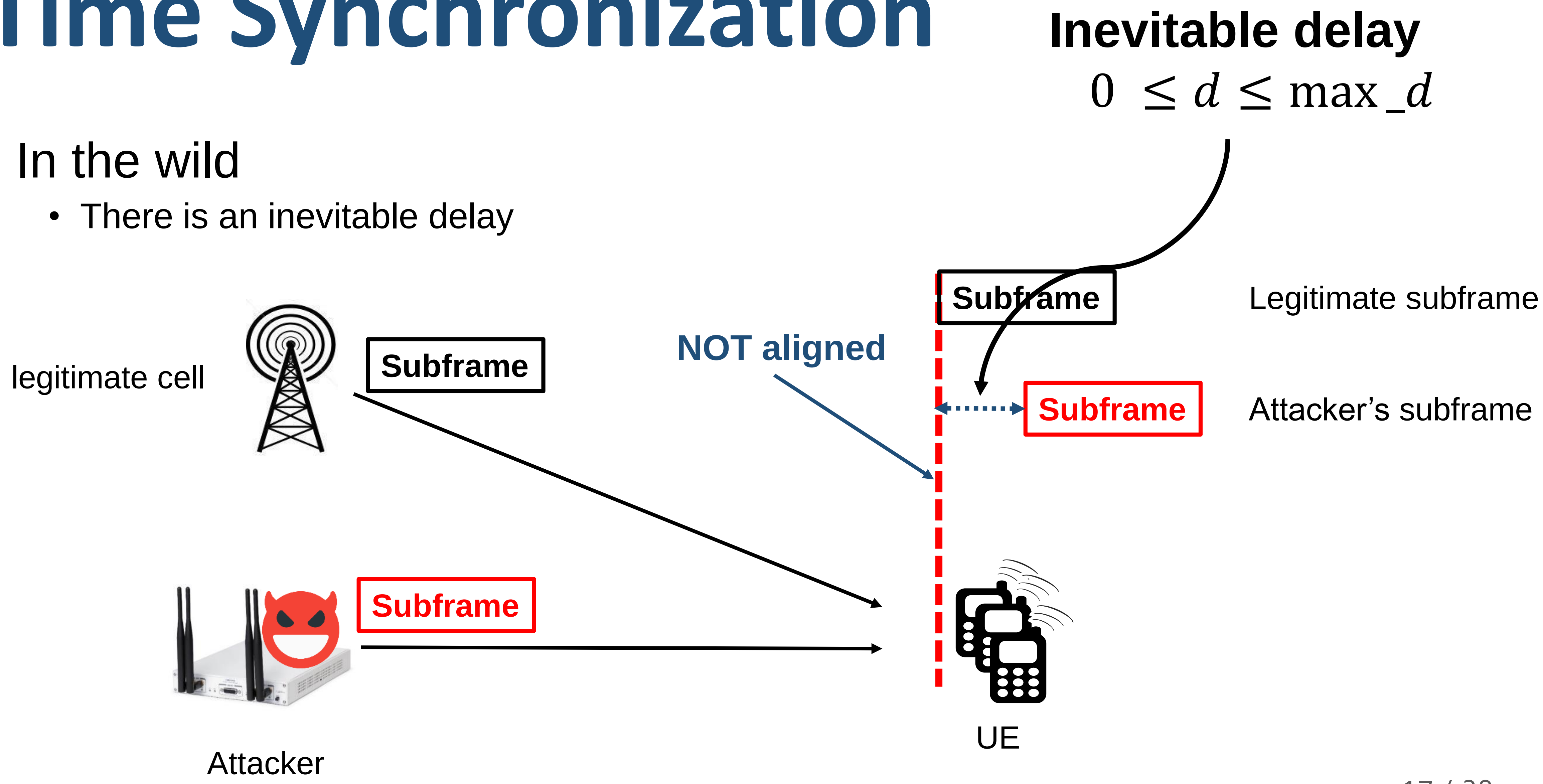
Time Synchronization

- Relax our assumption
  - There is a propagation delay depending on the location



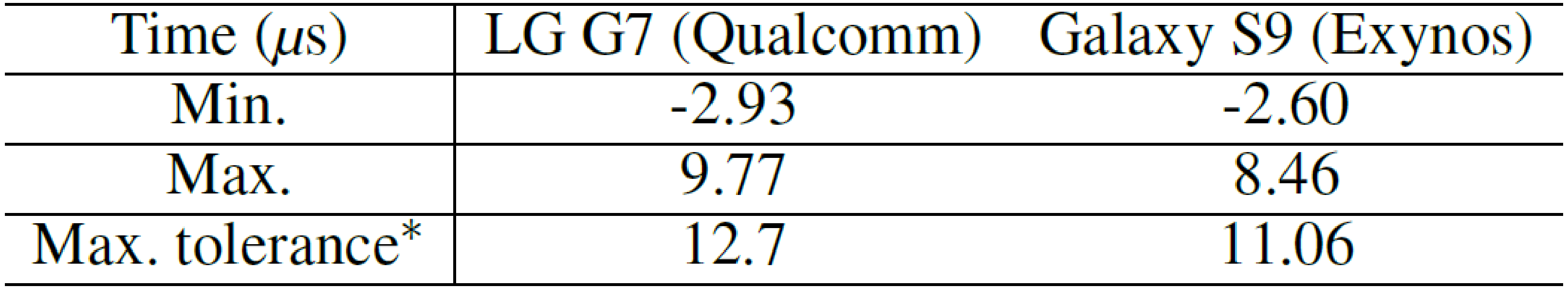
Time Synchronization

- In the wild
  - There is an inevitable delay



Time Synchronization

- Count on the LTE UE
  - LTE is designed to be **reliable** especially in outdoor environment
  - We let the UEs compensate those **errors**
- Measuring time tolerance of COTS smartphones
  - Qualcomm
  - Exynos



Time (μs)	LG G7 (Qualcomm)	Galaxy S9 (Exynos)
Min.	-2.93	-2.60
Max.	9.77	8.46
Max. tolerance*	12.7	11.06

In urban cell,
$r = 1.5\ km$
$d \leq 8.66\ \mu s$

Frequency Synchronization

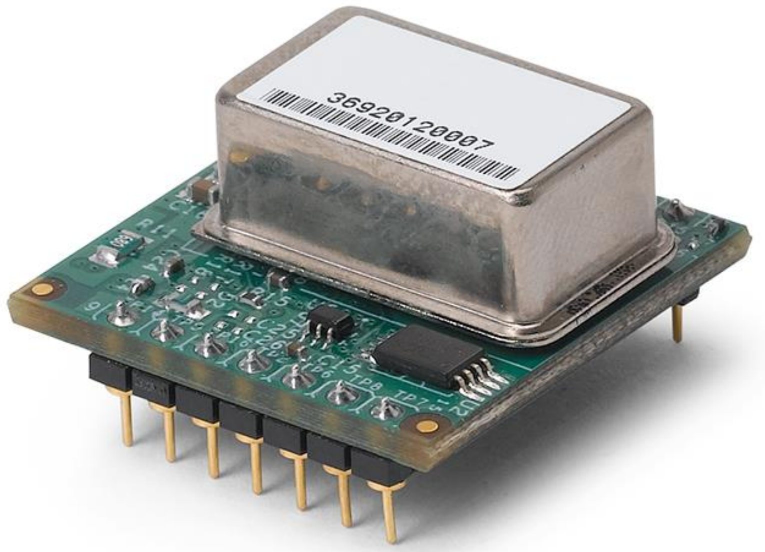
- Minimum frequency accuracy of legitimate cell
  - The standard defines minimum frequency accuracy of macro cell
  - 50 ppb ($\pm 90\ Hz\ @1.8GHz$)

- The attacker need at least 50 ppb frequency accuracy
- Residual frequency error be compensated by CFO correction

CFO: Center Frequency Offset
ppb: Parts Per Billion

Frequency Synchronization

- Need at least 50 ppb frequency accuracy
  - SigOver was run on a typical, inexpensive SDR with an inaccurate oscillator (2000 ppb for USRP B210)
  - We adopt GPSDO
    - 25 ppb w/o GPS antenna
    - 1 ppb w/ GPS antenna



- Residual frequency error
  - We used PSS/SSS based CFO correction

SDR: Software-Defined Radio

Summary of Main Questions

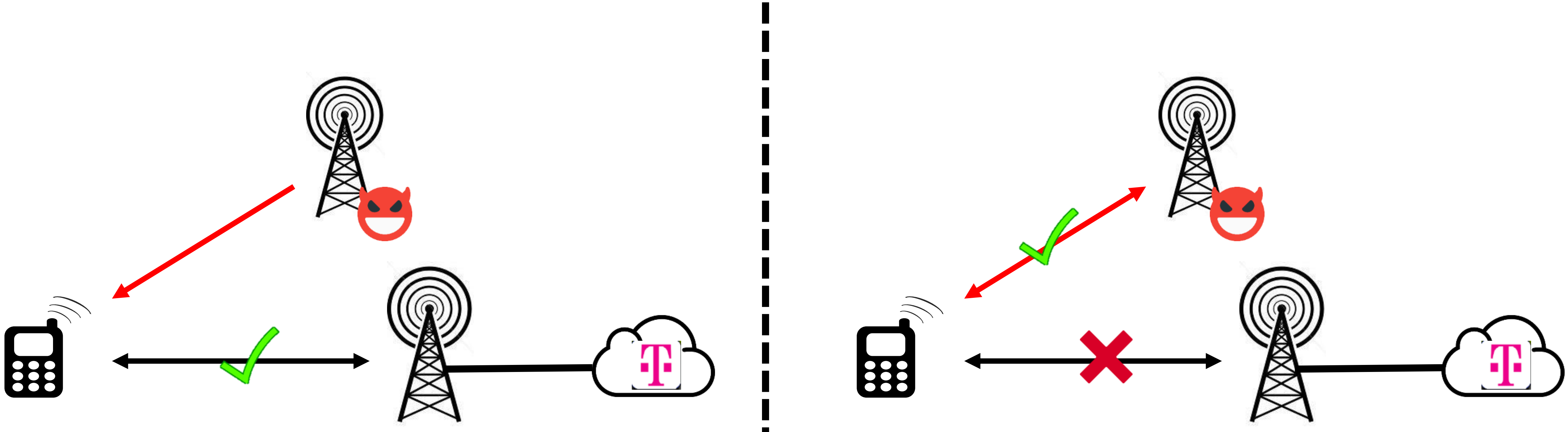
- Which part of the signal is overshadowed?
  - Subframe

- How to synchronize?
  - PSS/SSS for time sync
  - GPSDO and CFO correction for frequency sync

- How much error (time) is accepted?
  - Enough to cover the entire urban cell

FBS vs. SigOver

- Both FBS and SigOver can inject malicious broadcast messages to the UEs
- No need to connection establishment



SigOver

FBS

Advantages

- Power efficient
  - Requires **+3 dB** power (success rate: 98%)
  - cf. Fake base station needs **+40 dB** (success rate: 100%)

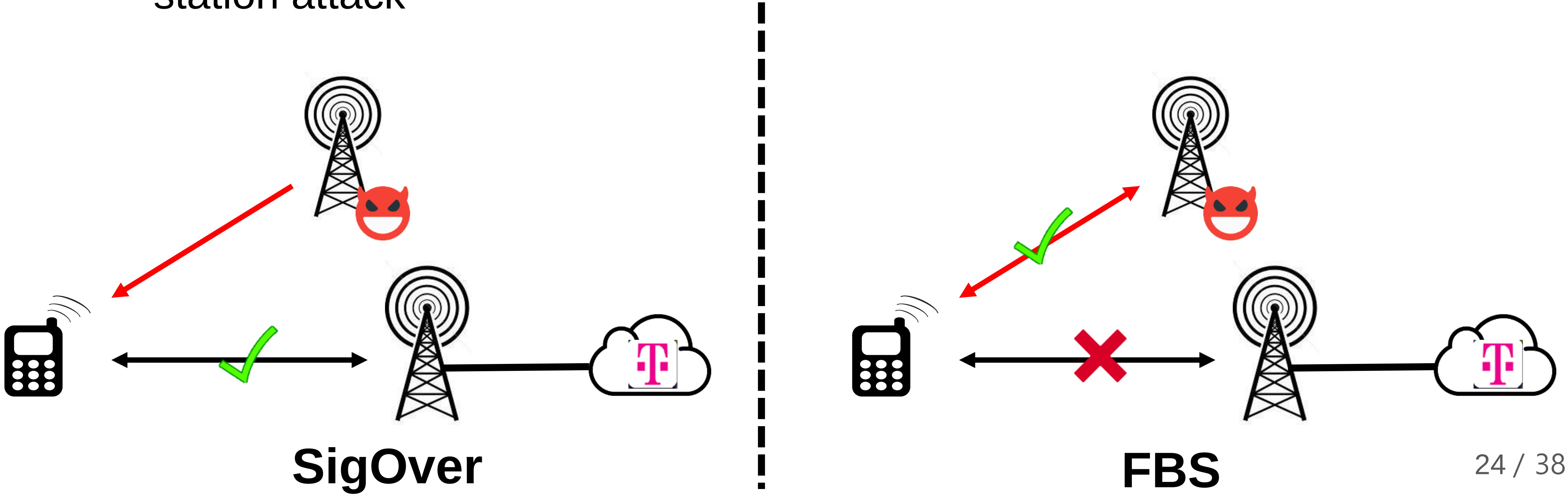
Relative Power (dB)	1	3	5	7	9
SigOver	38%	98%	100%	100%	98%

Relative Power (dB)	25	30	35	40	45
FBS*	0%	0%	80%	100%	100%

* Assume that the FBS sets the same freq. band, PCI, MIB and SIB1 to the legitimate cell

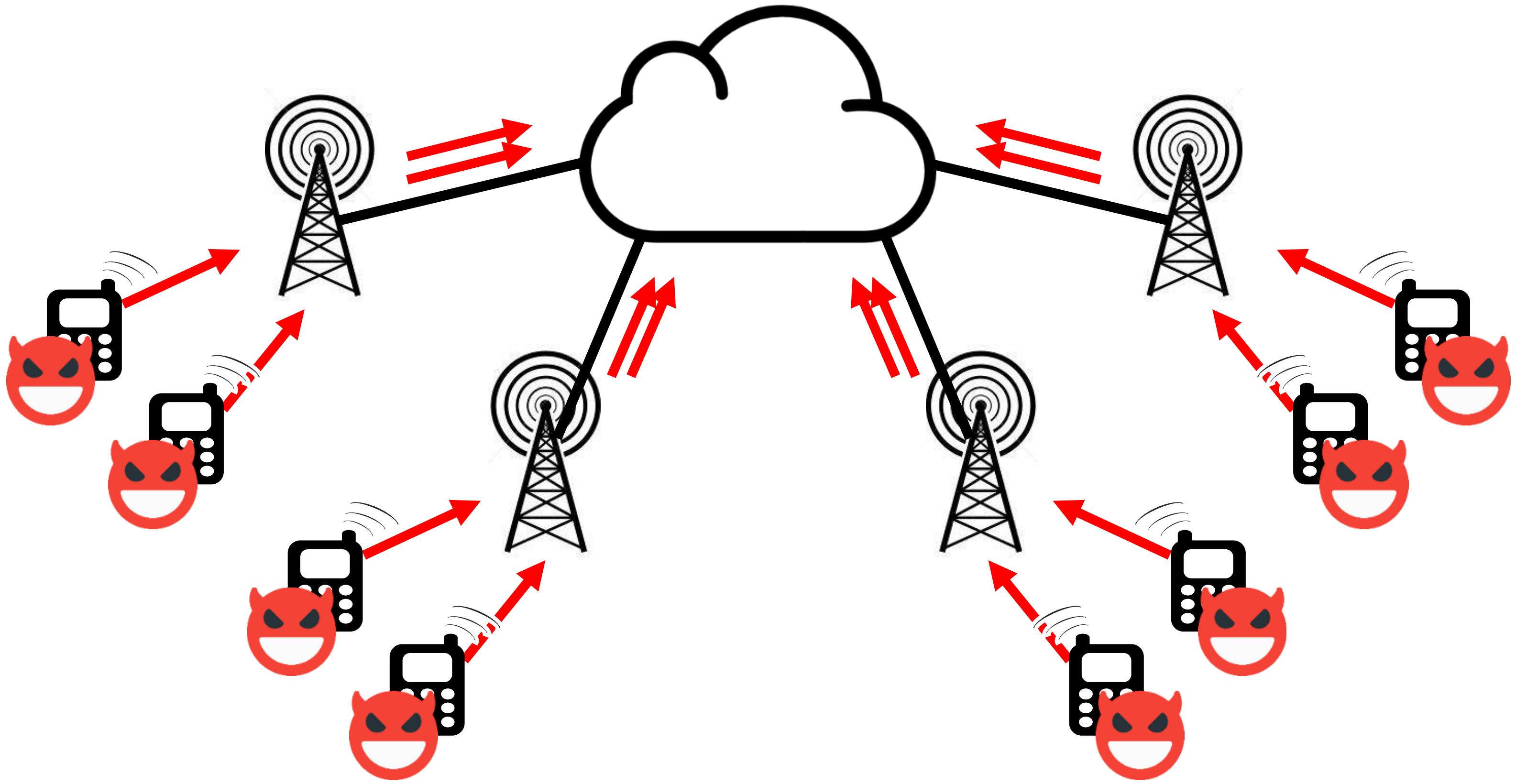
Advantages

- UEs are keep communicating with the legitimate cell
  - UEs can receive or transmit all messages from/to legitimate cell
  - cf. UEs cannot communicate with legitimate cell during the fake base station attack



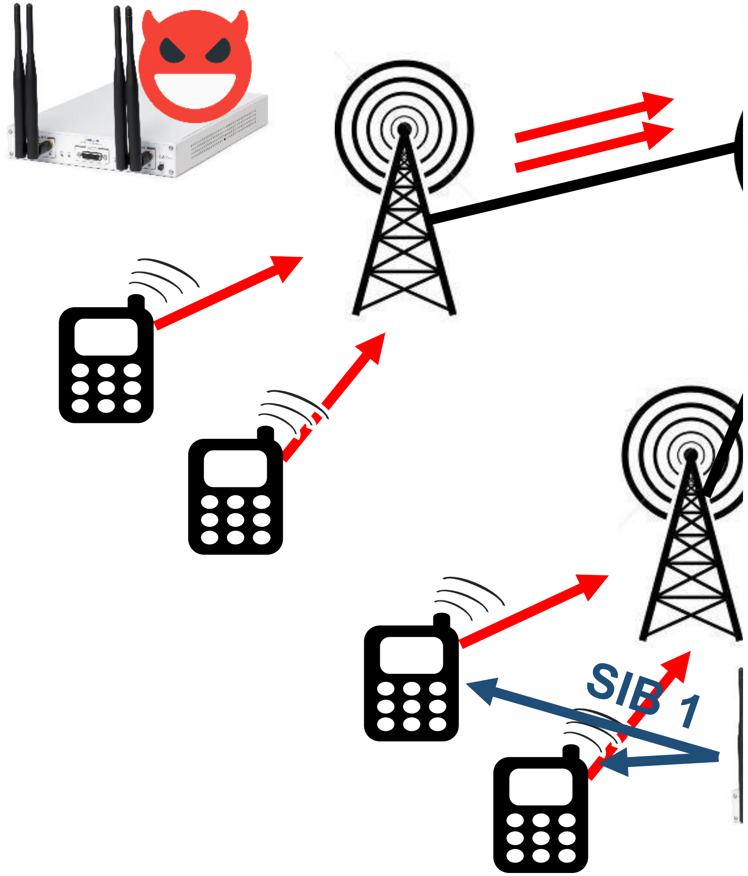
Signaling Storm

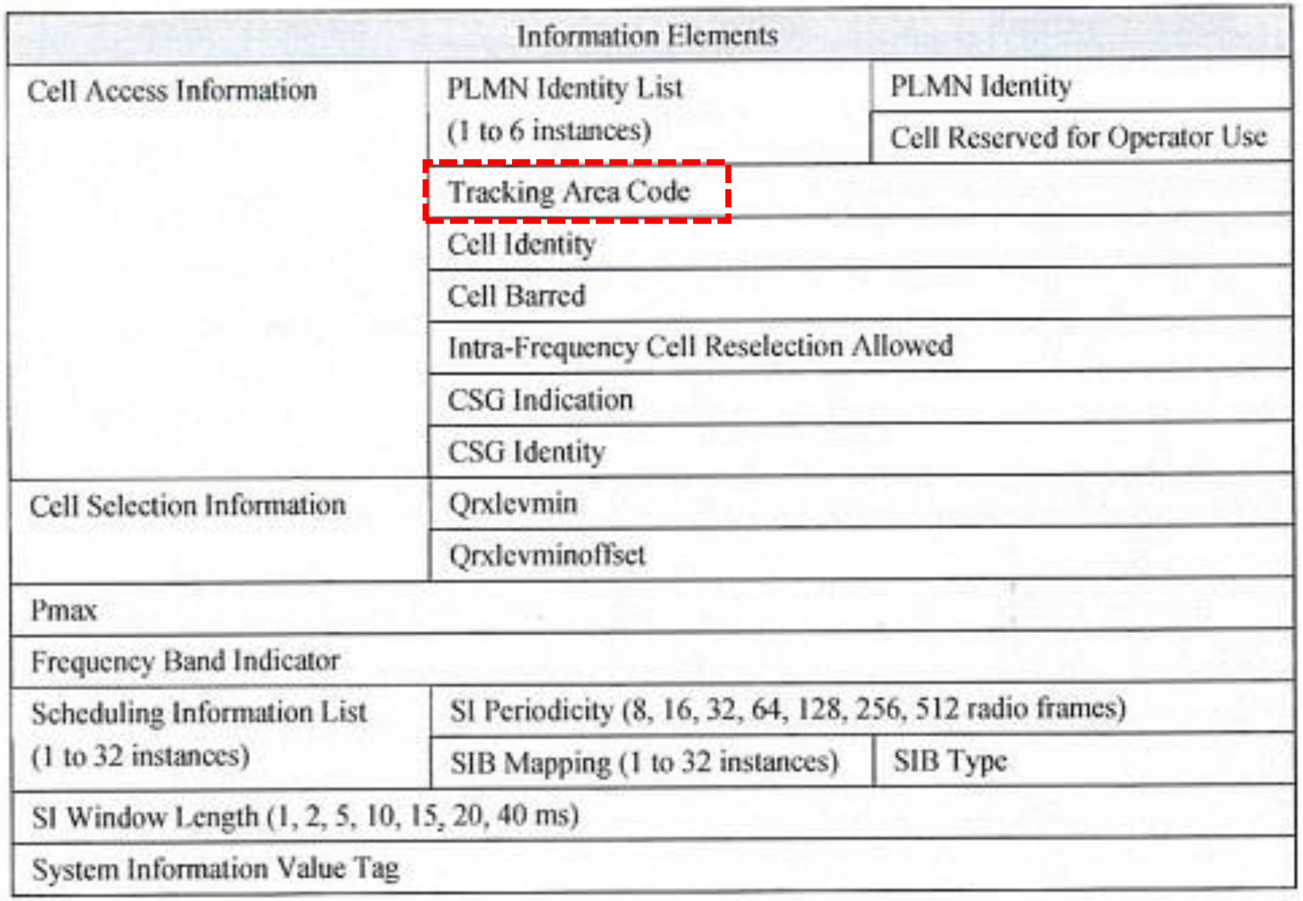
- Using a botnet in general



Signaling Storm

Using SigOver



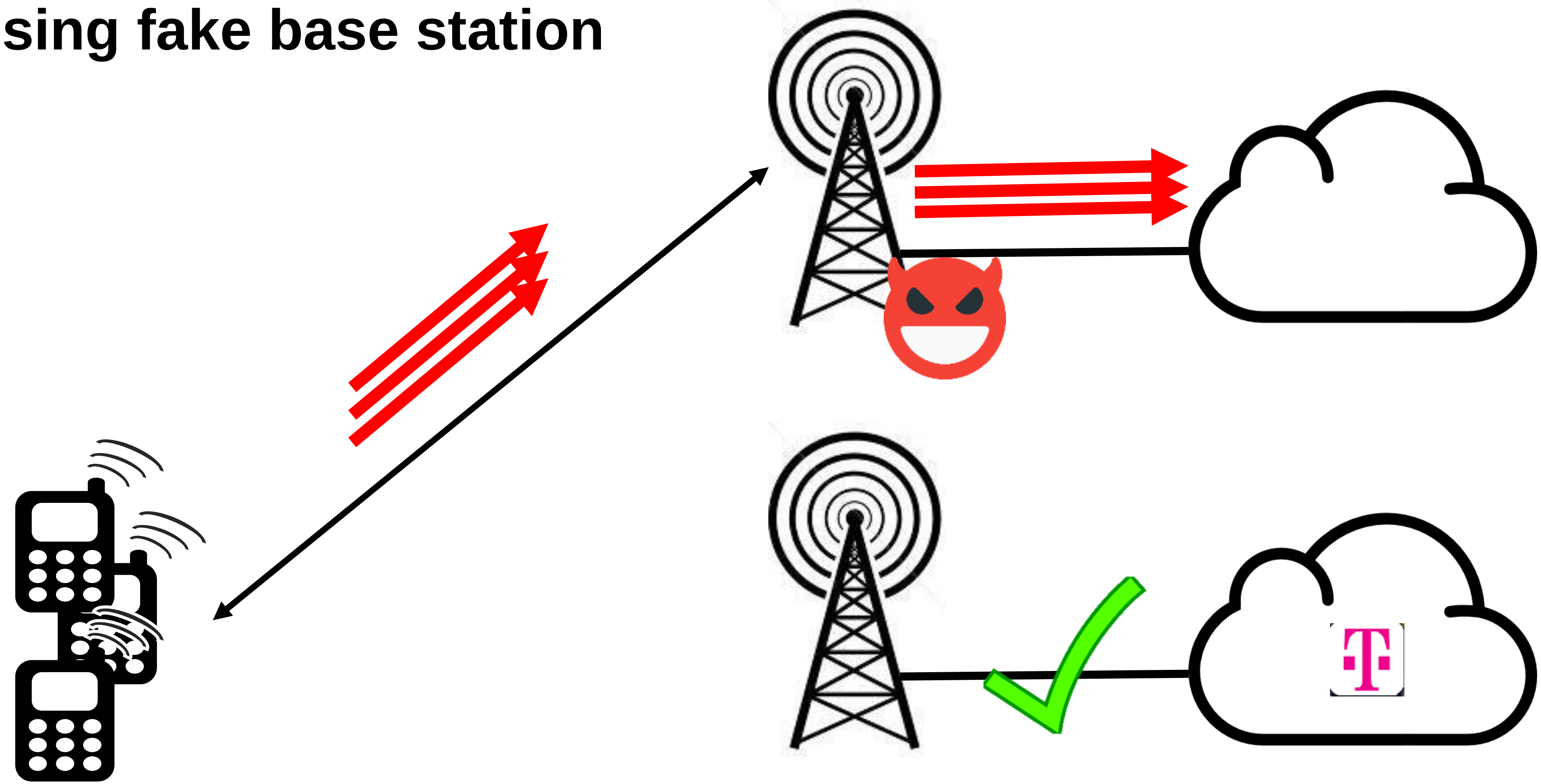


Information Elements		
Cell Access Information	PLMN Identity List (1 to 6 instances)	PLMN Identity
		Cell Reserved for Operator Use
	Tracking Area Code	
	Cell Identity	
	Cell Barred	
	Intra-Frequency Cell Reselection Allowed	
	CSG Indication	
	CSG Identity	
Cell Selection Information	Qrxlevmin	
	Qrxlevminoffset	
Pmax		
Frequency Band Indicator		
Scheduling Information List (1 to 32 instances)	SI Periodicity (8, 16, 32, 64, 128, 256, 512 radio frames)	
	SIB Mapping (1 to 32 instances)	SIB Type
SI Window Length (1, 2, 5, 10, 15, 20, 40 ms)		
System Information Value Tag		

LTE SIB-1

Signaling Storm

Using fake base station



Attack Efficiency

Normal

- 45 service request per UE per hour in peak busy hours [1]

SigOver

- 21,600 TAU per UE per hour

Note

Service request ≅ 15 messages
TAU ≅ 20 messages

Total number of Signaling Messages

- Normal : 675 per UE per hour
- SigOver : 432,000 per UE per hour (**640** times more than Normal)

TAU: Tracking Area Update

[1] LTE signaling: Prevent attach storms, Nokia, 2014

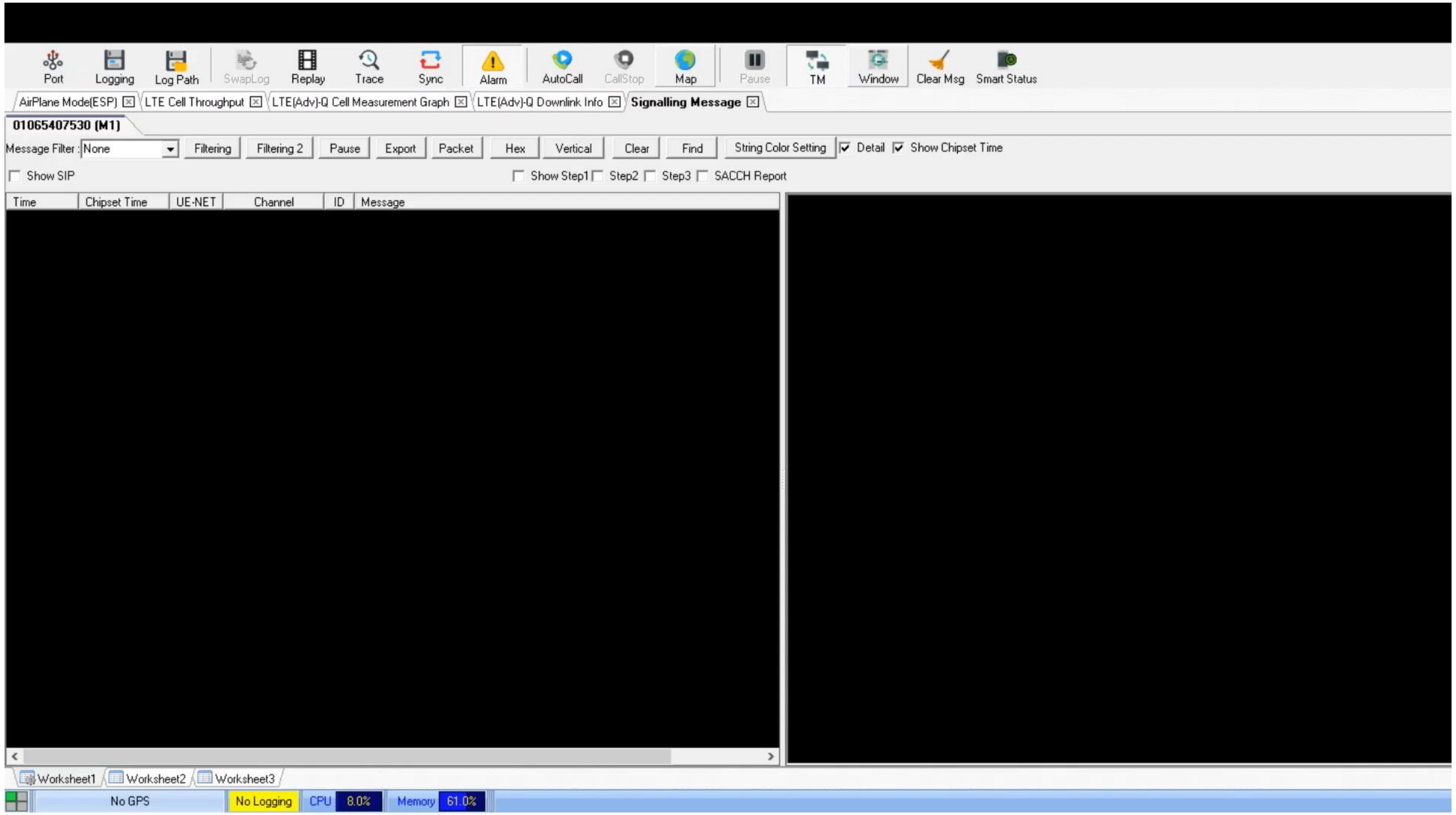
Test Environment

- Implementation
  - based on open-source LTE stack (srsLTE)
- Attacker
  - USRP X310 + GPSDO (OCXO)
  - USRP B210 + GPSDO (TCXO)

- Victim devices

  iPhone XS
  iPhone 7
  Galaxy S9
  Galaxy S6 Edge
  Galaxy S4
  LG G6
  LG G2
  …

Signaling Storm Demo



01065407530 (M1)

Message Filter : None

☑ Detail ☑ Show Chipset Time

□ Show SIP

□ Show Step1 □ Step2 □ Step3 □ SACCH Report

No GPS | No Logging | CPU 8.0% | Memory 61.0%

Fake Emergency Alert Message

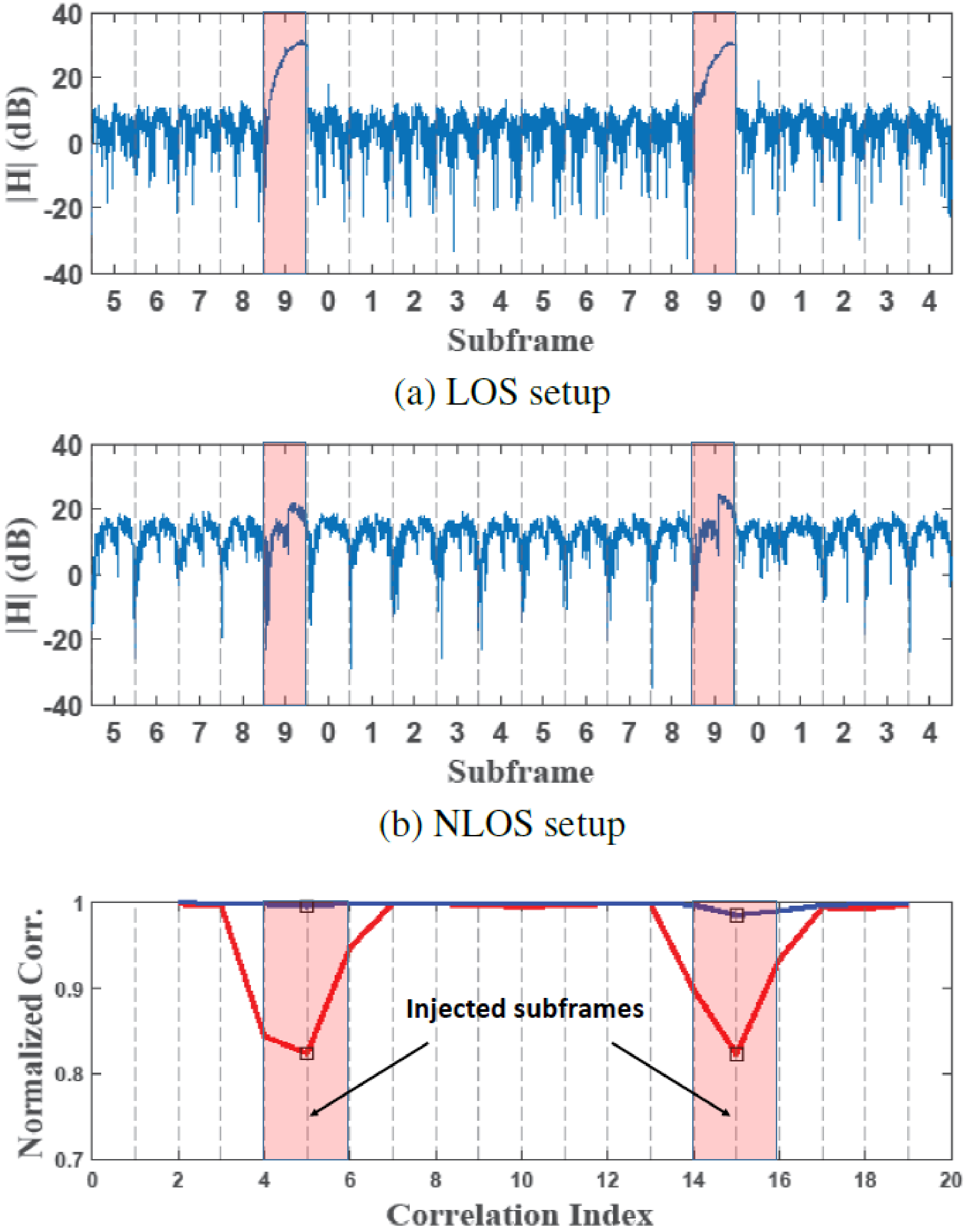
For more videos...

- Please check our YouTube channel
  - SYSSEC KAIST

https://www.youtube.com/channel/UCg1-TiATZj4qB0Xqknl18mA

Defense

- Physical layer detection
  - Using correlation



(a) LOS setup

(b) NLOS setup

Blue line: NLOS

Red line: LOS

Defense

- Integrity protection on broadcast messages
  - May add digital signature
- In 5G, operator’s public key will be provisioned on the USIM
  - In theory, integrity protection is feasible
  - But, 3GPP does not considering it for now

Conclusion

- SigOver attack
  - A new exploit on unpatched vulnerabilities in broadcast channel
  - Cheaper, stealthier than attacks using FBS
  - Found new attacks on broadcast messages; Expect to be used in the wild

- Responsible disclosure
  - GSMA: no practical implication ☺
  - Qualcomm: acknowledged

Good Questions

- Could we create physical security tools or hardware to protect against the SigOver attack?
- Are there any indications that 5G networks might also be vulnerable to similar attack vectors?
- Who do you think is more responsible for these vulnerabilities, LTE standards or baseband manufacturers? Can this type of attack be detected through fuzzing?
- Considering the high success rate of the SigOver attack with minimal power difference, what practical challenges might arise in implementing digital signatures for broadcast messages in existing LTE infrastructure?

Best Questions

- (Changgun Kang) Why is leaving broadcast signals unprotected unavoidable? Given those reasons for not protecting broadcast messages, what do you think would be the most promising approach to mitigate attacks proposed in this paper?
- (Jiwoo Suh) Does the timing synchronization requirement and timing delay threshold for the SigOver attack impose a limit on the attack range? If so, what techniques or advancements could be used to extend the attack range?
- (Boris) The paper mentions that the SigOver attack does not require active communication with UEs and does not relay messages. Could the SigOver attack be combined with techniques like IMSI catching to gather additional information about the victim UE or to launch more sophisticated attacks?

THANK YOU.
ANY QUESTIONS?

BACKUP

Adopting PKI for Broadcast Messages

- Deployment challenge @ *ISP*
  - Need to handle various events in the wild
    - Roaming, handover, MVNO, etc.
    - Transmitting *Warning Messages* to unsubscribed devices
  - Managing certificate
    - Establish Chain of trust, set up new eco system for managing the certificate
    - Maintain revocation list
- Technical challenge @ *base station & UE*
  - Verifying certificate & signature require additional **power consumption**

Will SigOver Work in 5G?

- We believe "Yes" for now
- Current Non-standalone design → Definitely "Yes"
  - 5G NSA uses the SAME Control plane messages in LTE
- Standalone design? → "Partially Yes" *(Unless PKI is adopted)*
  - 5G SA uses the SAME (and similar) frame structure
  - Subframe is sent every 1 msec
- Hardware issues
  - USRP supports up to 6 GHz
  - 5G SA supports up over 28 GHz

What Can We Do More with SigOver?

- We can launch various attacks on UE and Network!
- By SigOver on *broadcast message*,
  - **SIB:** Signaling storm, fake emergency alert, selective DoS
  - **Paging:** DoS attack, network downgrading attack, location tracking
- Can an attacker use SigOver to send *uplink/downlink* messages?
  - Sure! (If the message is not integrity-protected)
- Maybe used to attach UE to FBS (not verified)

- BTW, why do we focus on the broadcast messages?
  - Located at the fixed position by 3GPP, effective attack vector

Comparison over MitM & FBS

	Stealthiness	Power Efficiency	Attack sustainability
FBS	Low	Low	Low
MiTM	Limited	Low	Limited
SigOver	High	High	High

Previous study

- Previous Targets
    - LR-WPAN (802.15.4)
    - GPS

- None for 2G/3G/4G
    - Reviewer 1
        - “I did not find it intuitive in the beginning that overshadowing attacks are likely to succeed in real-world LTE setups due to tight dependencies on time and frequency synchronization”