Hiding in Plain Signal:
Physical Signal Overshadowing Attack on LTE

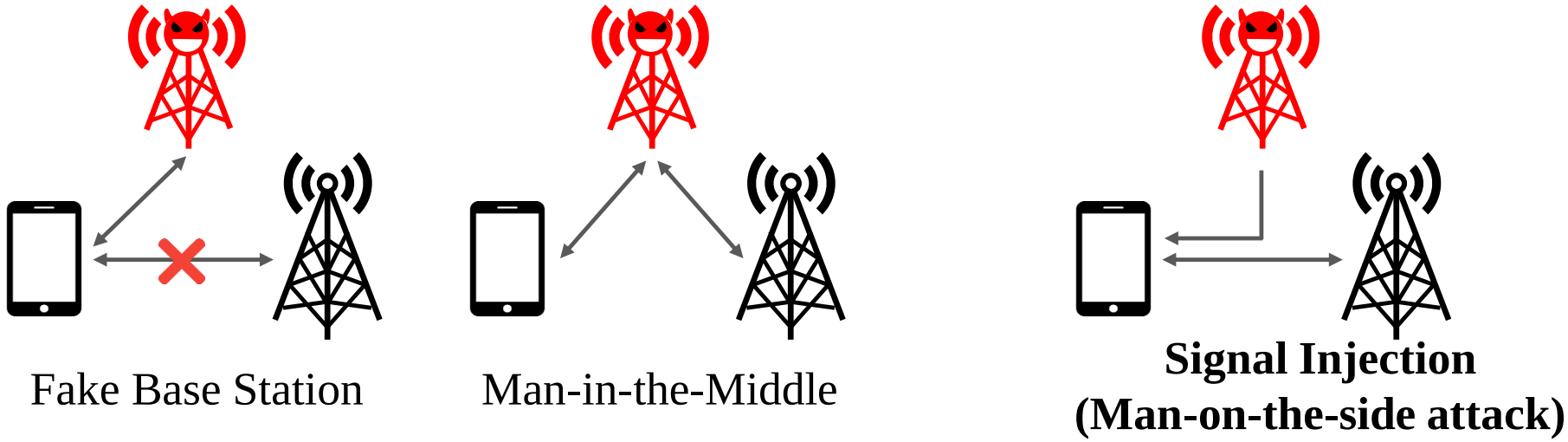
Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim,
Song Min Kim, and **Yongdae Kim**

USENIX Security 2019

21/11/04
CheolJun Park

People loves this work. Why?

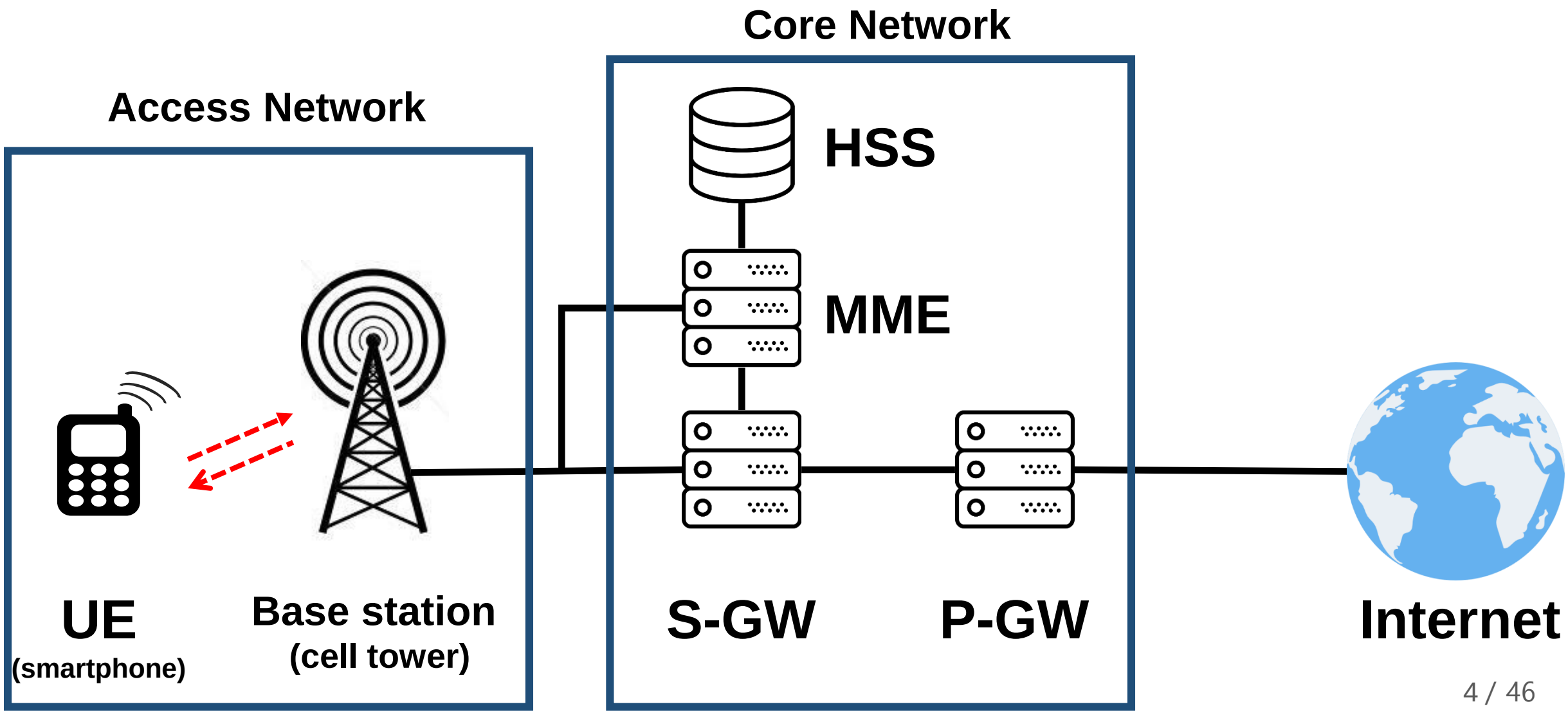
- New active attacker model in LTE
  - ➢ Have shown the feasibility of signal injection attack



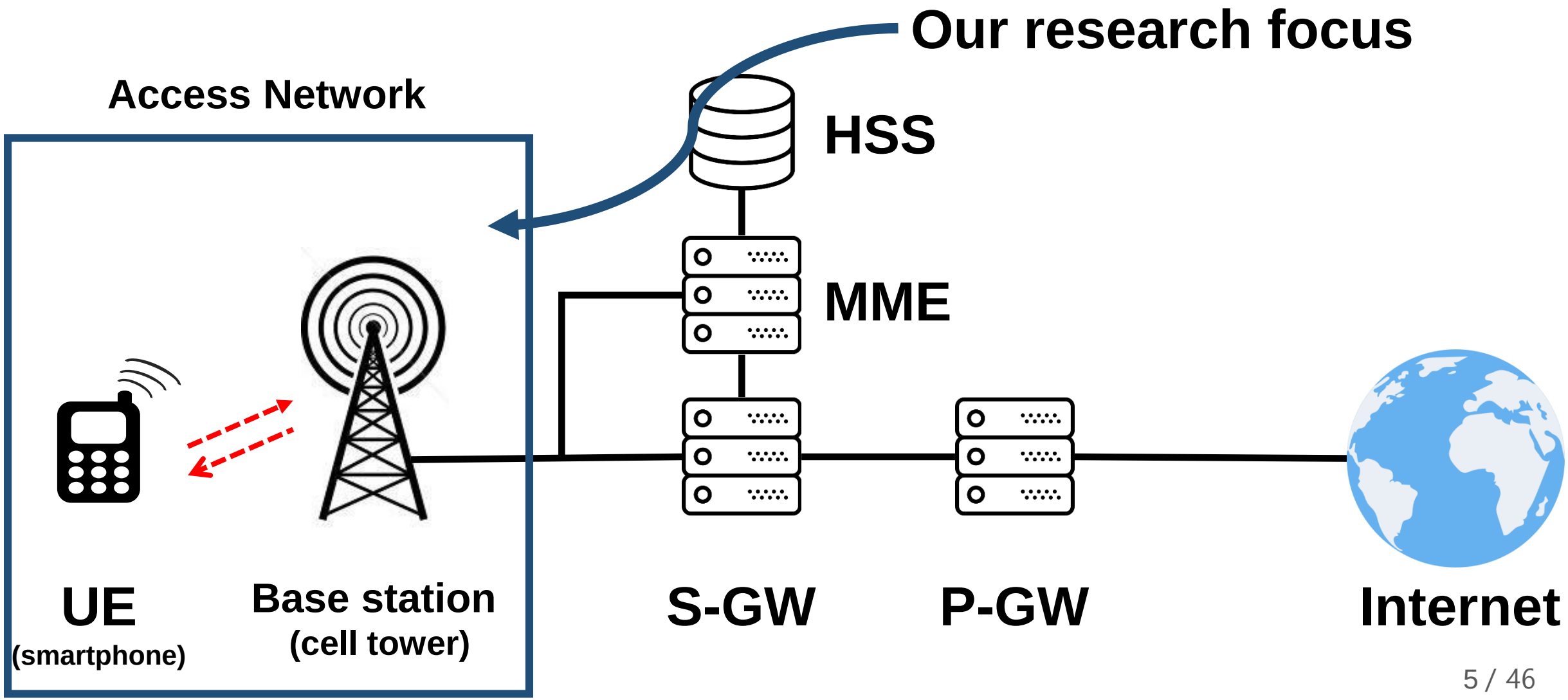
Overshadowing physical signal?

- Sounds easy
  - Strong physical signal
  - No security in the physical level
- Previous Targets
  - LR-WPAN (Low-Rate Wireless Personal Area Network) (802.15.4)
  - GPS
- None for cellular network
- However, there are technical challenges!
  - Reviewer: “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**”

LTE Architecture Overview



LTE Architecture Overview



LTE security

- Most LTE messages are integrity protected
  - **Only after** sharing security context

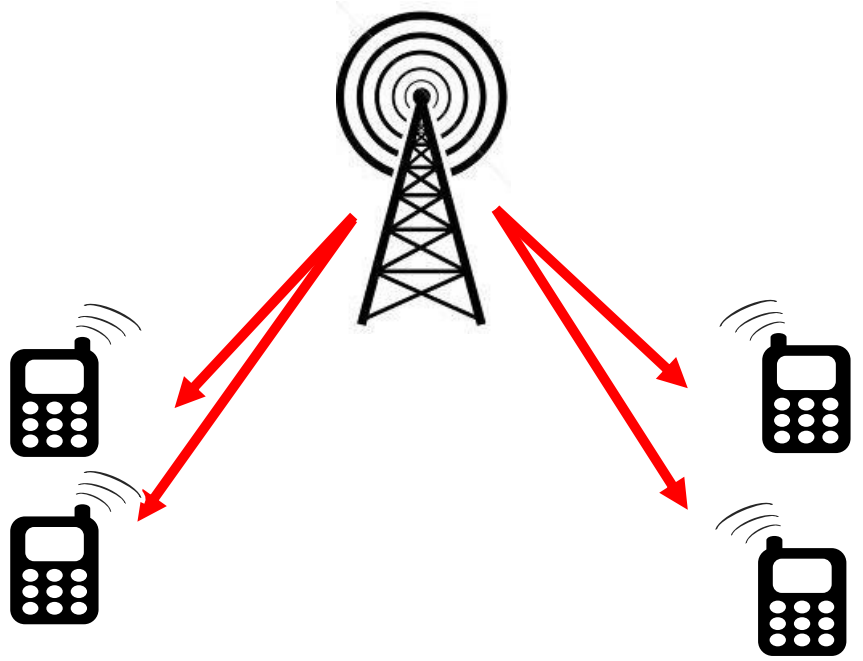
- Messages before sharing security context? **Not secure!**

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

Broadcast Messages

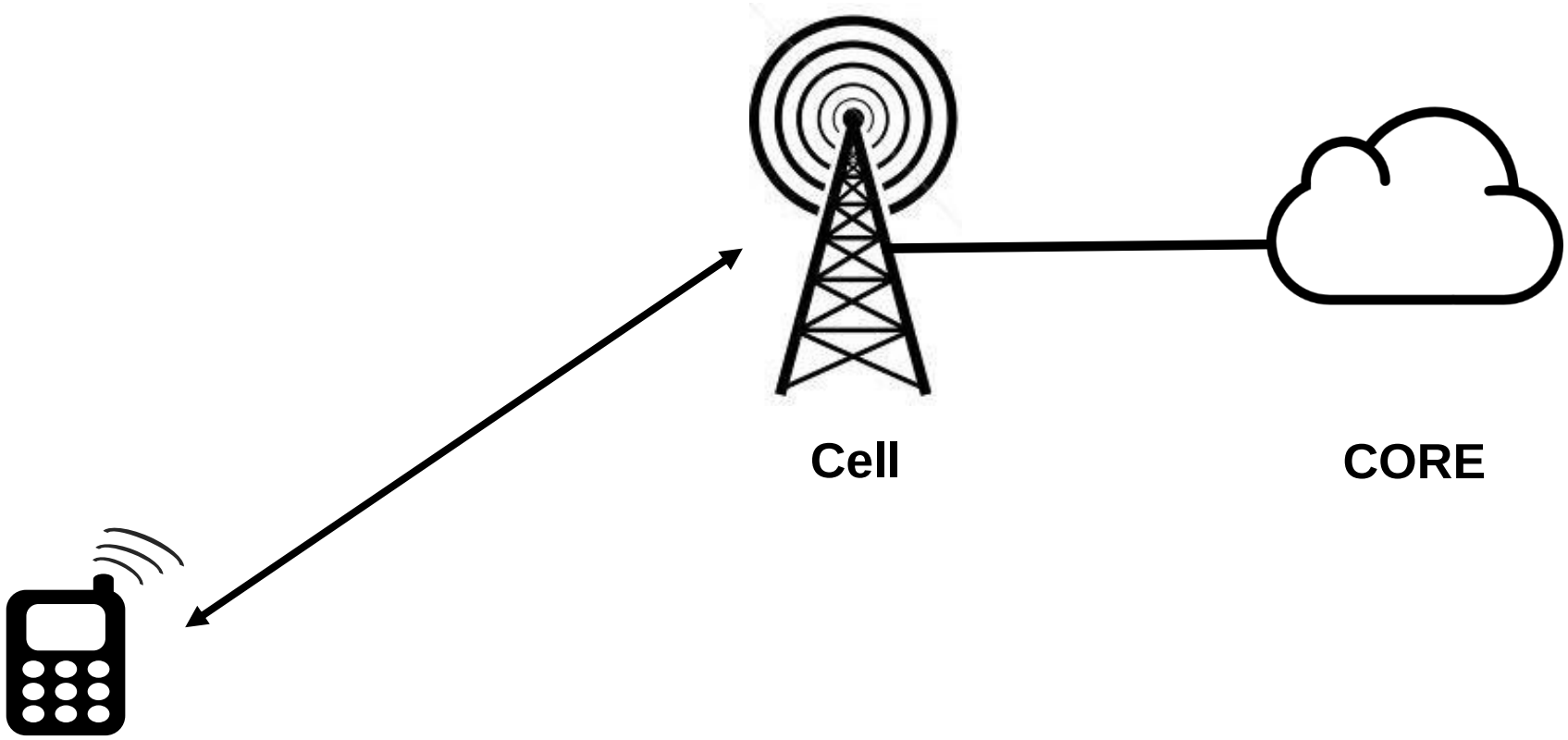
- Terminology
  - Messages targeting multiple UEs within a cell at the same time
  - Not a formal Terminology though ☺

- Messages
  - Paging
  - System Information Block (SIB)
  - …



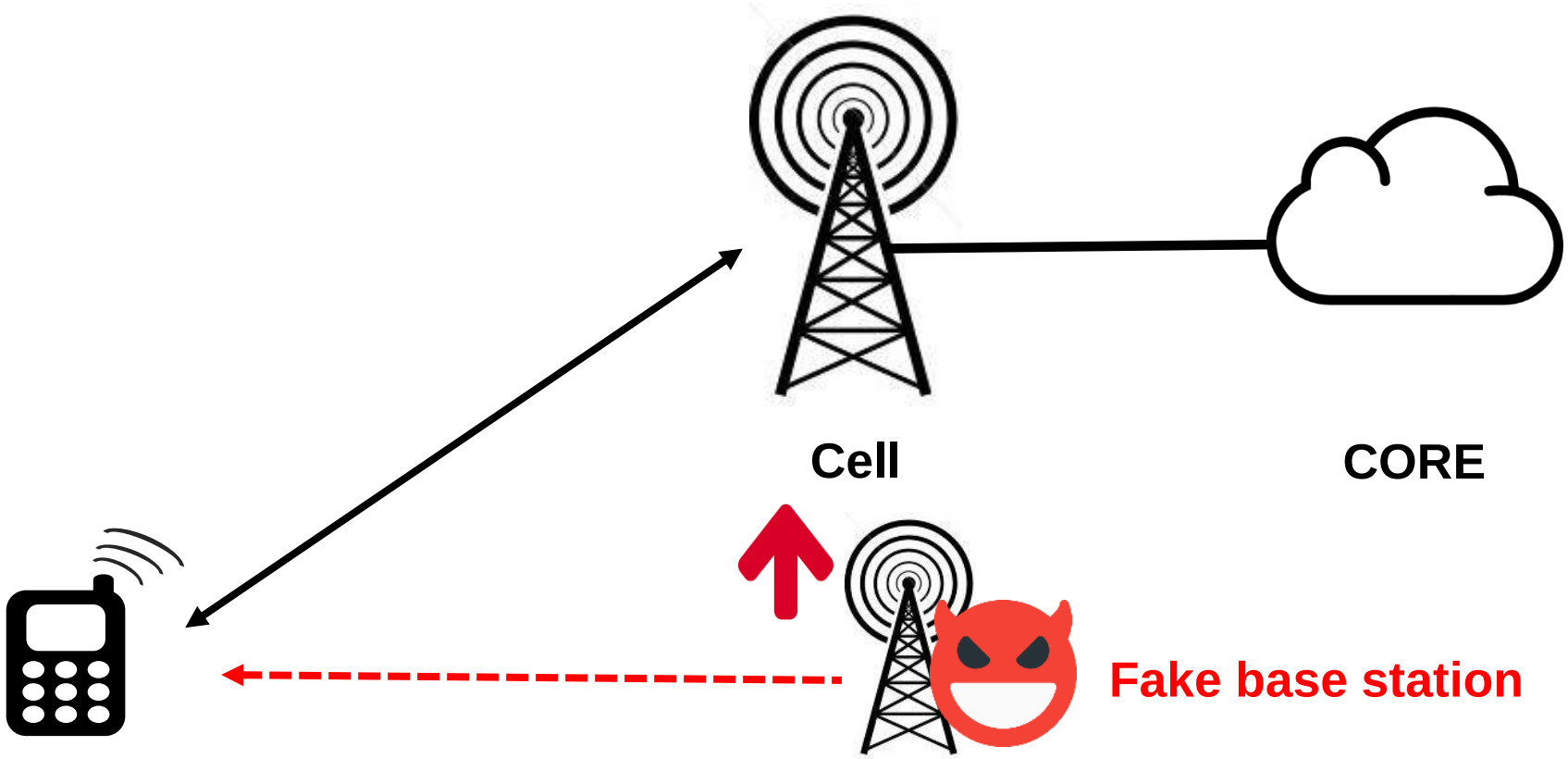
Playing with Broadcast Messages

- 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

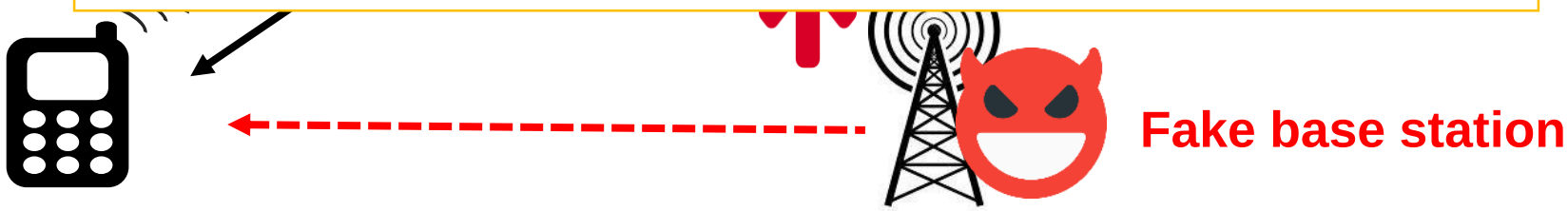
- Previously, the only way is to use fake base station (FBS)

Question:

Is REALLY FBS the only way? What else?

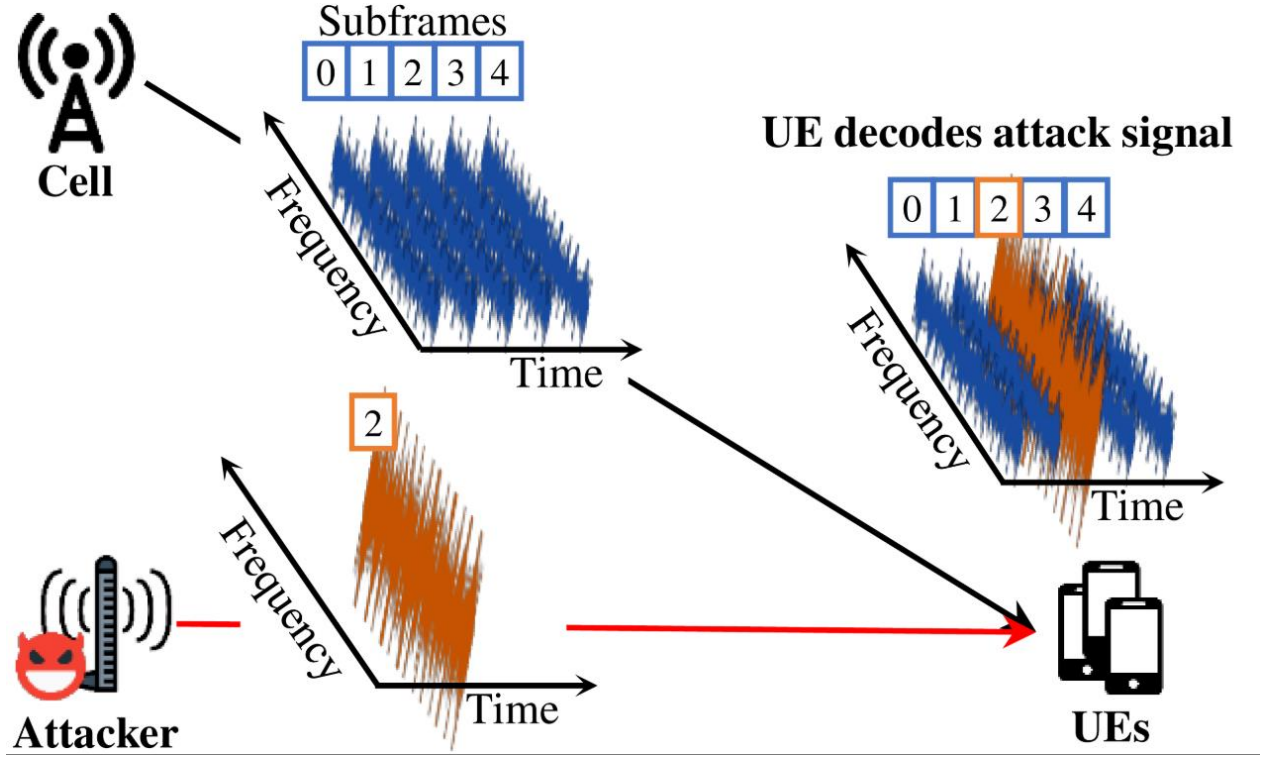
Answer:

Wireless signal can be manipulated through the air.



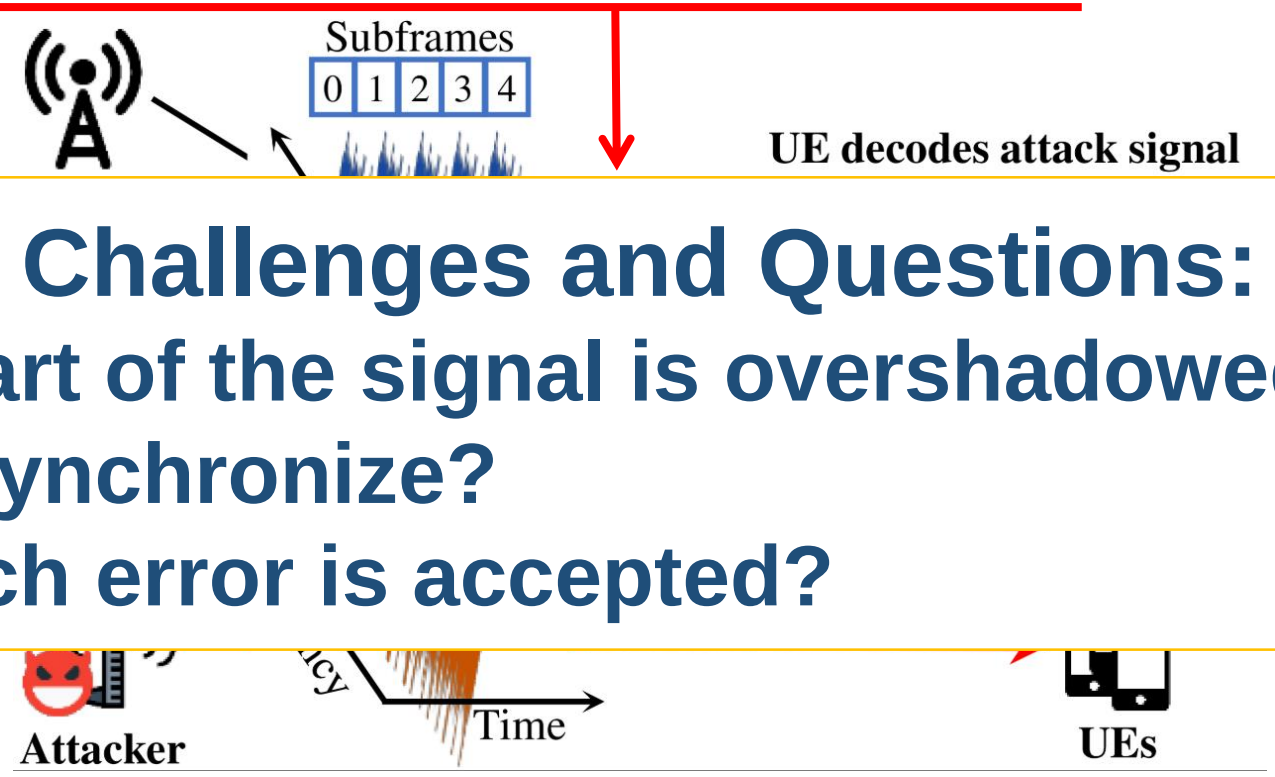
Signal Overshadowing (SigOver)

- 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

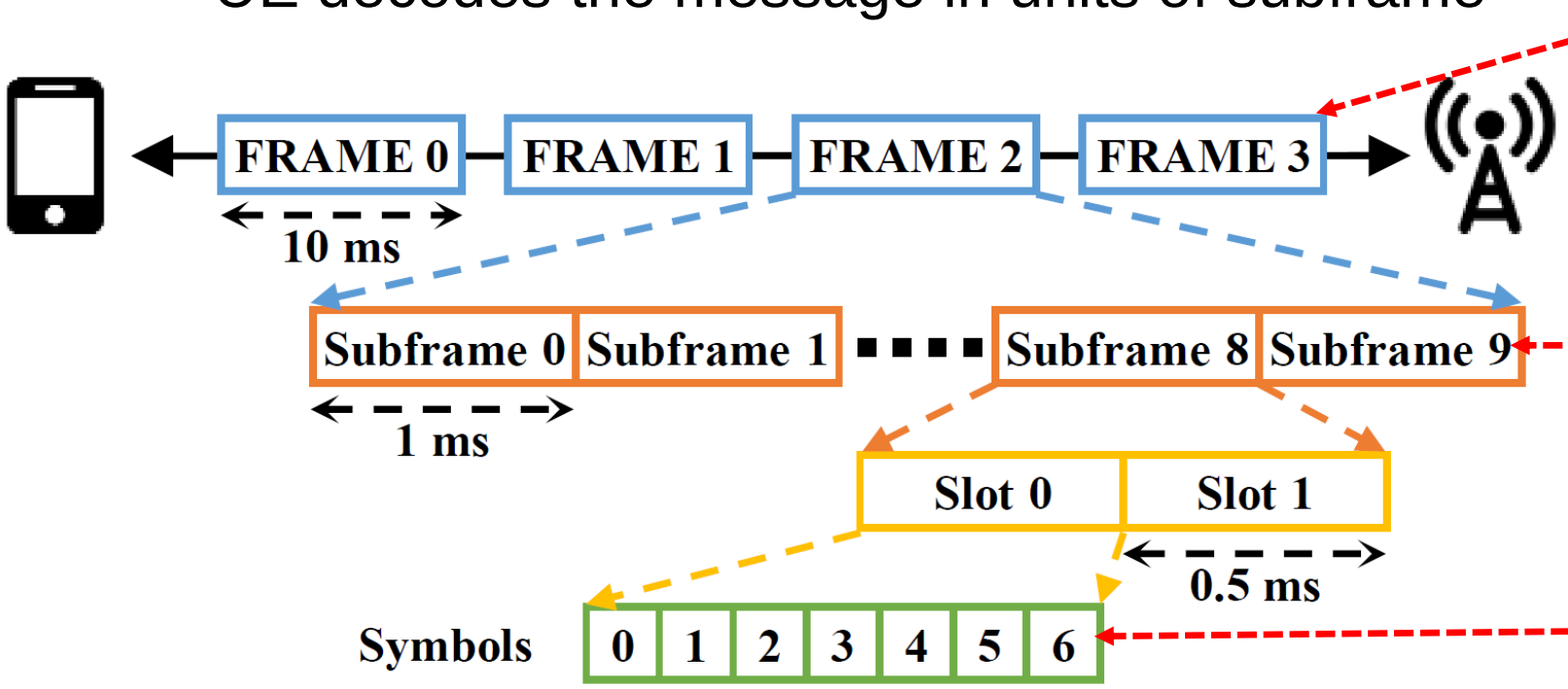


Challenges and Questions:

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



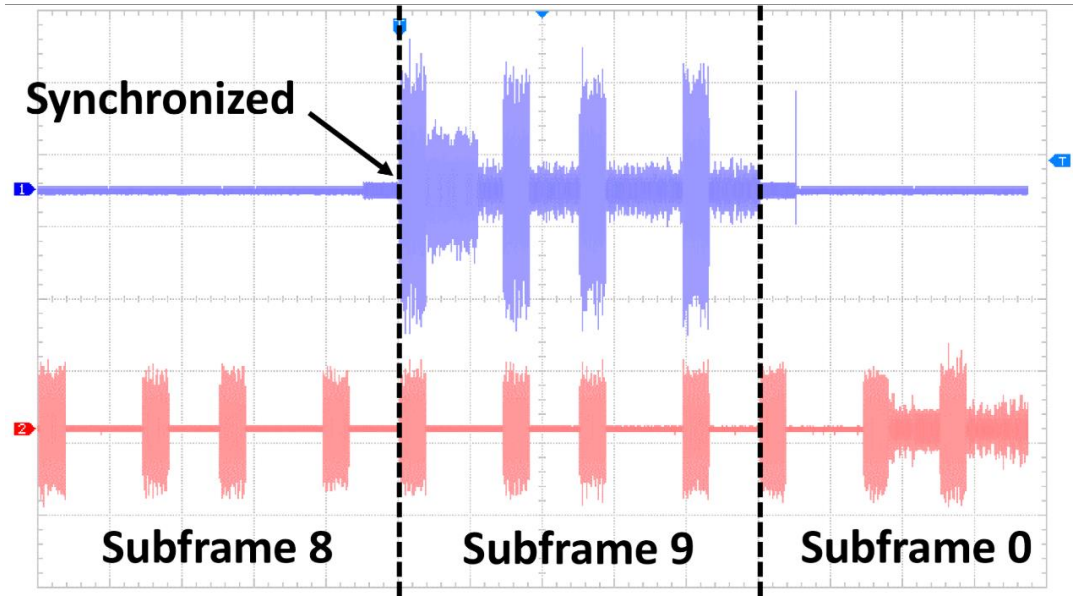
☹ **Affects other msg.**

☺ **Our decision**

☹ **Low success rate**

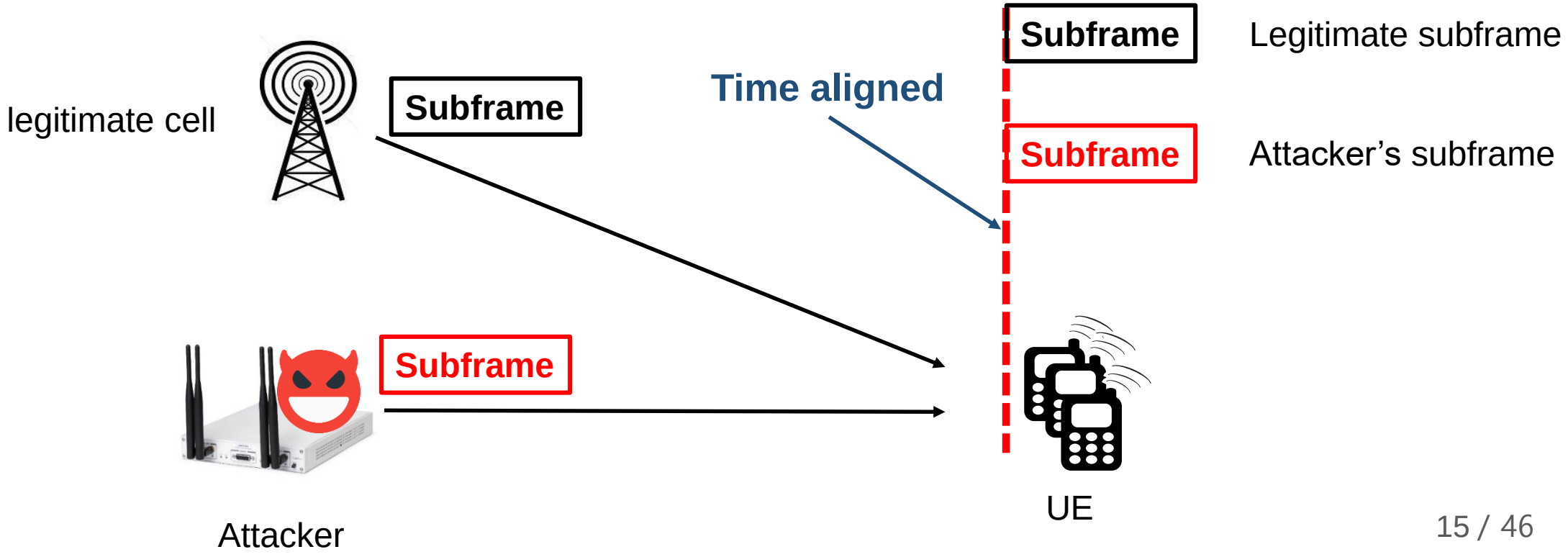
Attack Design

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



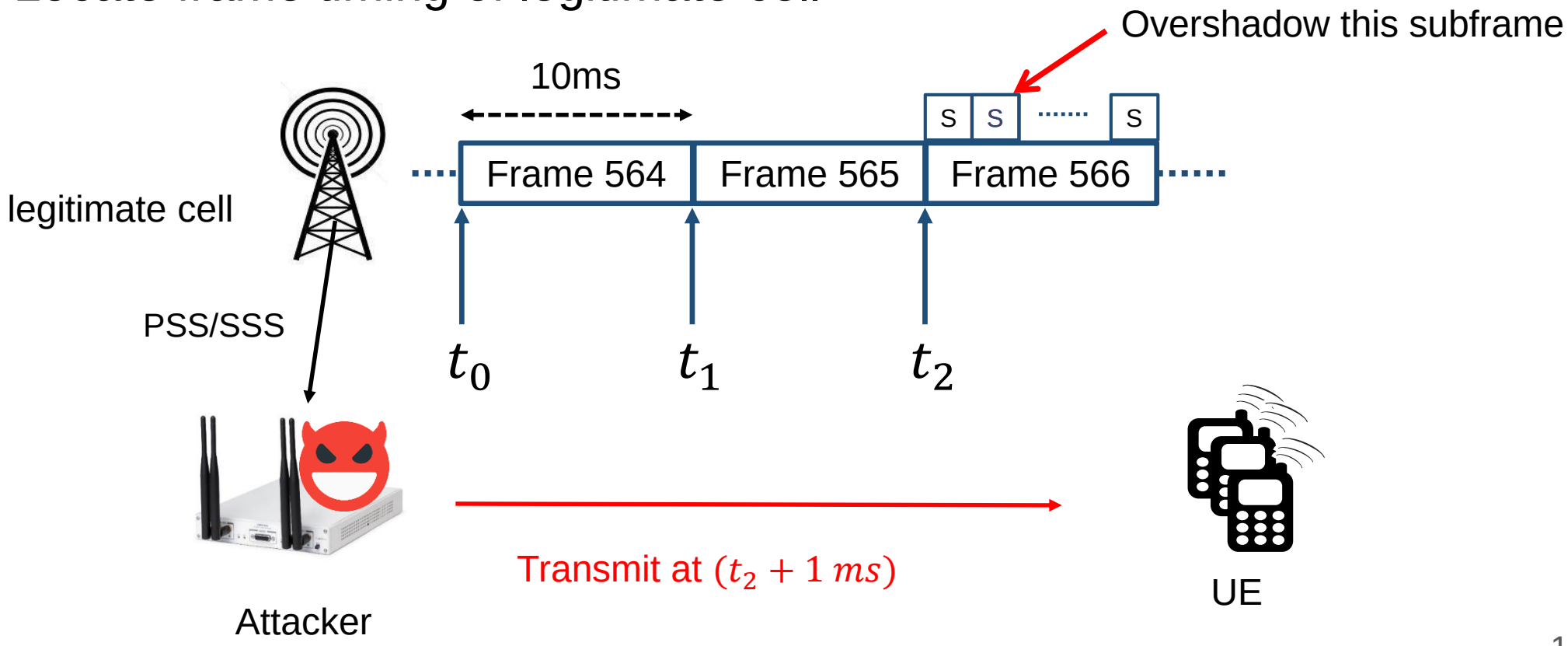
Time Synchronization

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



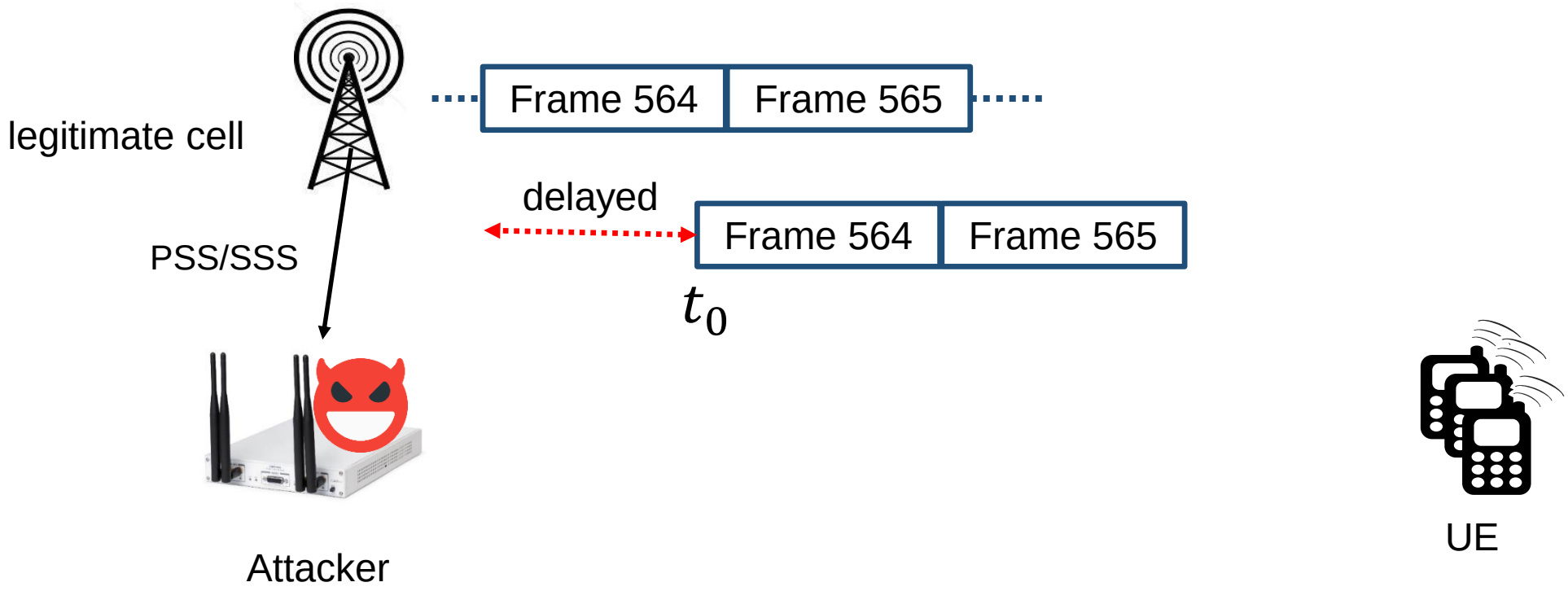
Time Synchronization

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



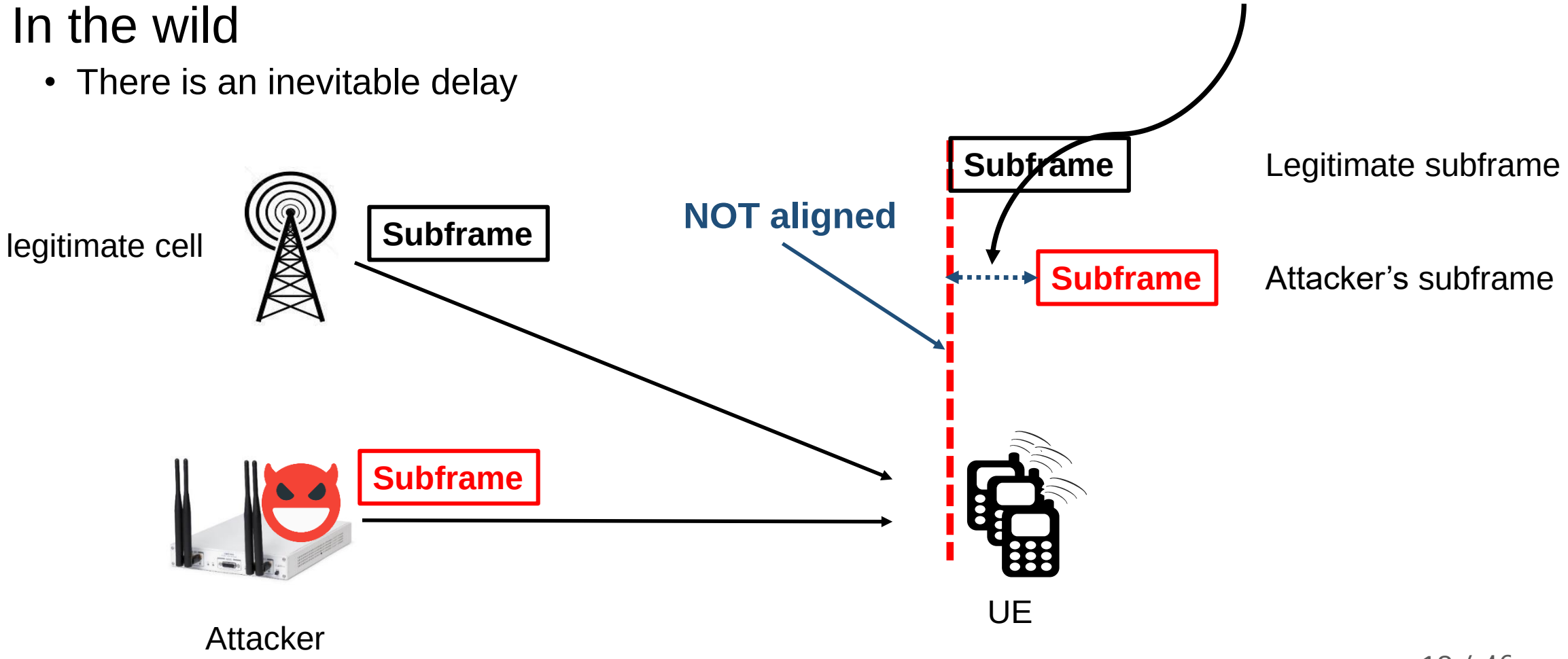
Time Synchronization

- 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

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

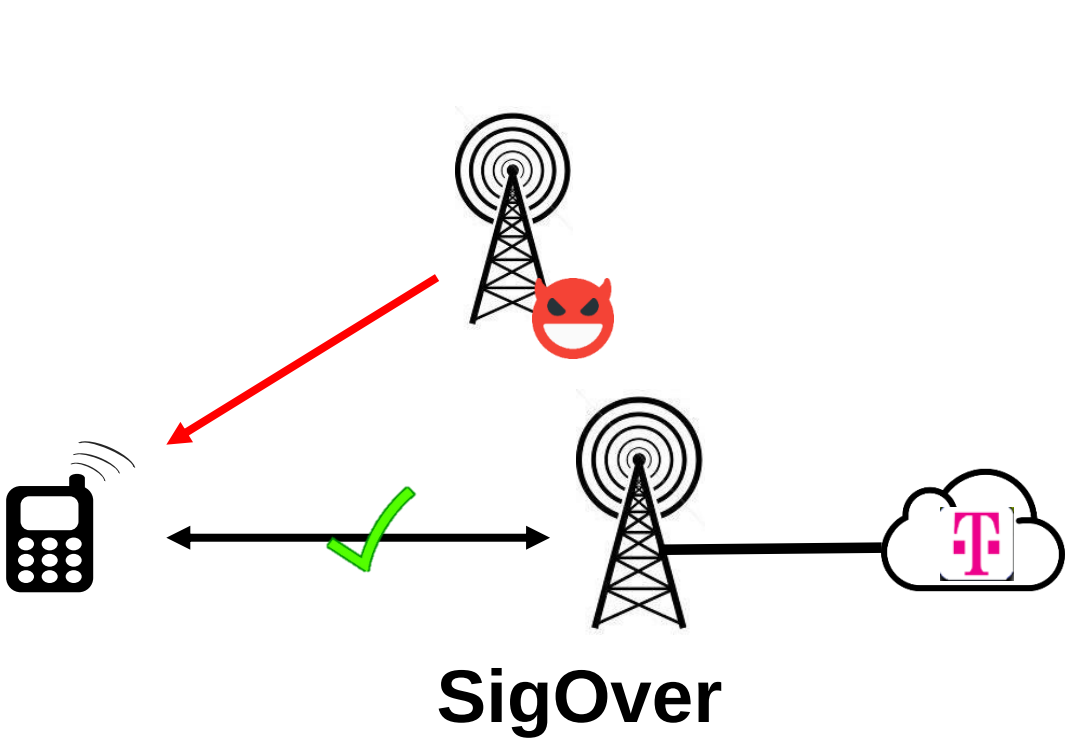
  LG G6

  LG G2

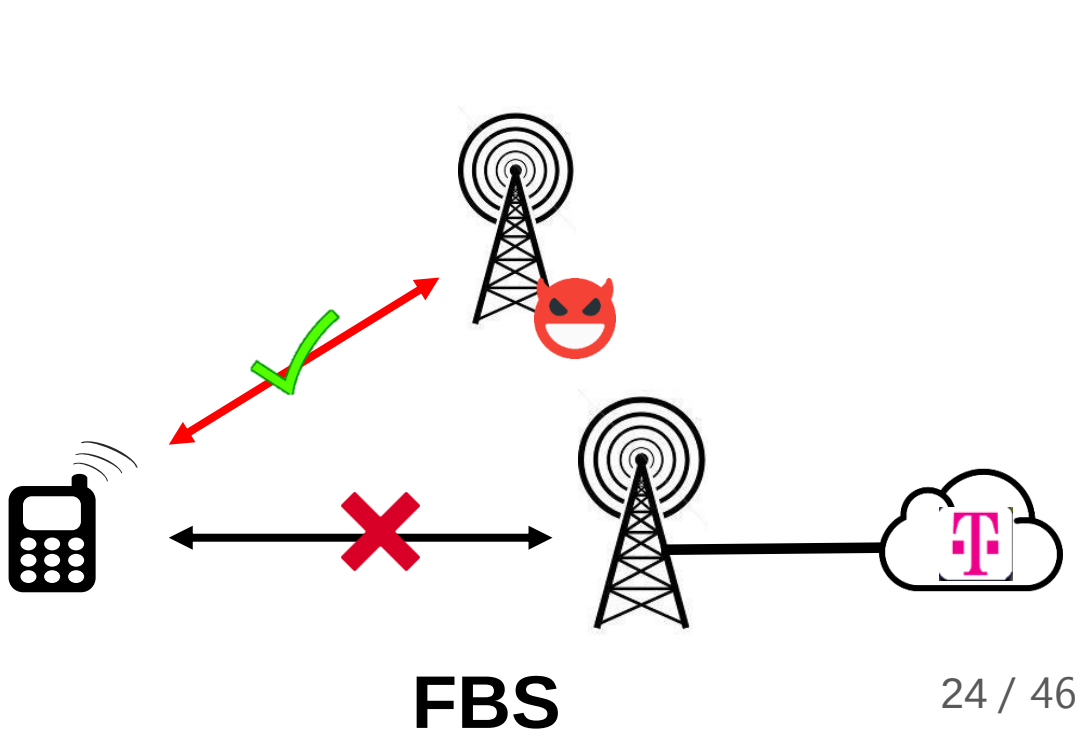
  …

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%)

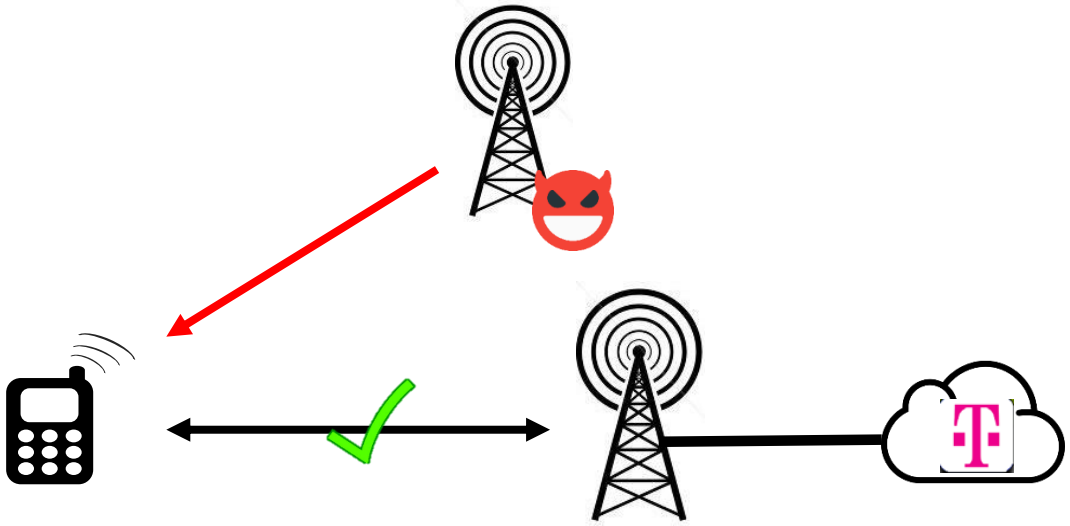
Relative Power (dB)	1	3	5	7	9
SigOver	38%	98%	100%	100%	98%

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

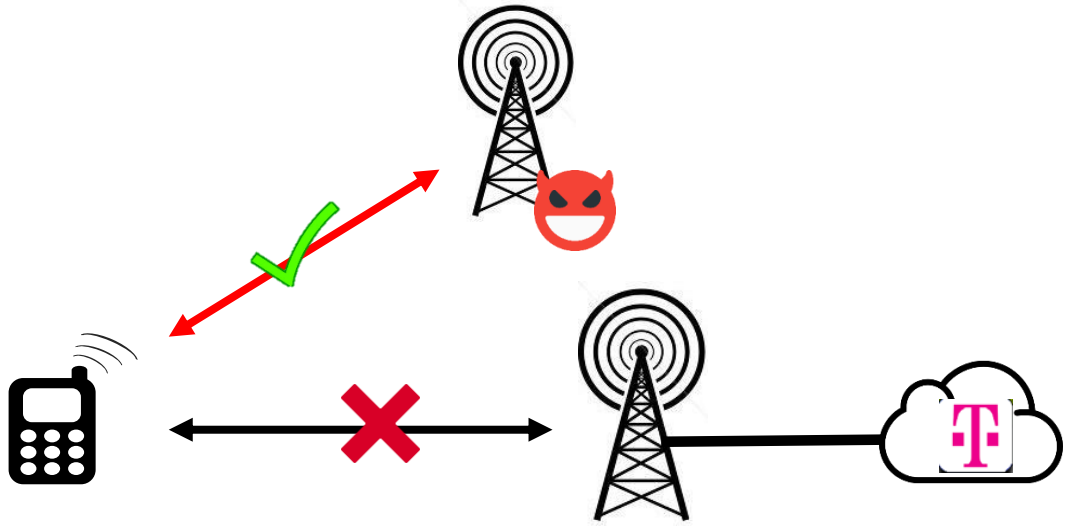
* Assume that the FBS sets the same freq. band, PCI, MIB and SIB1 to the legitimate cell

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



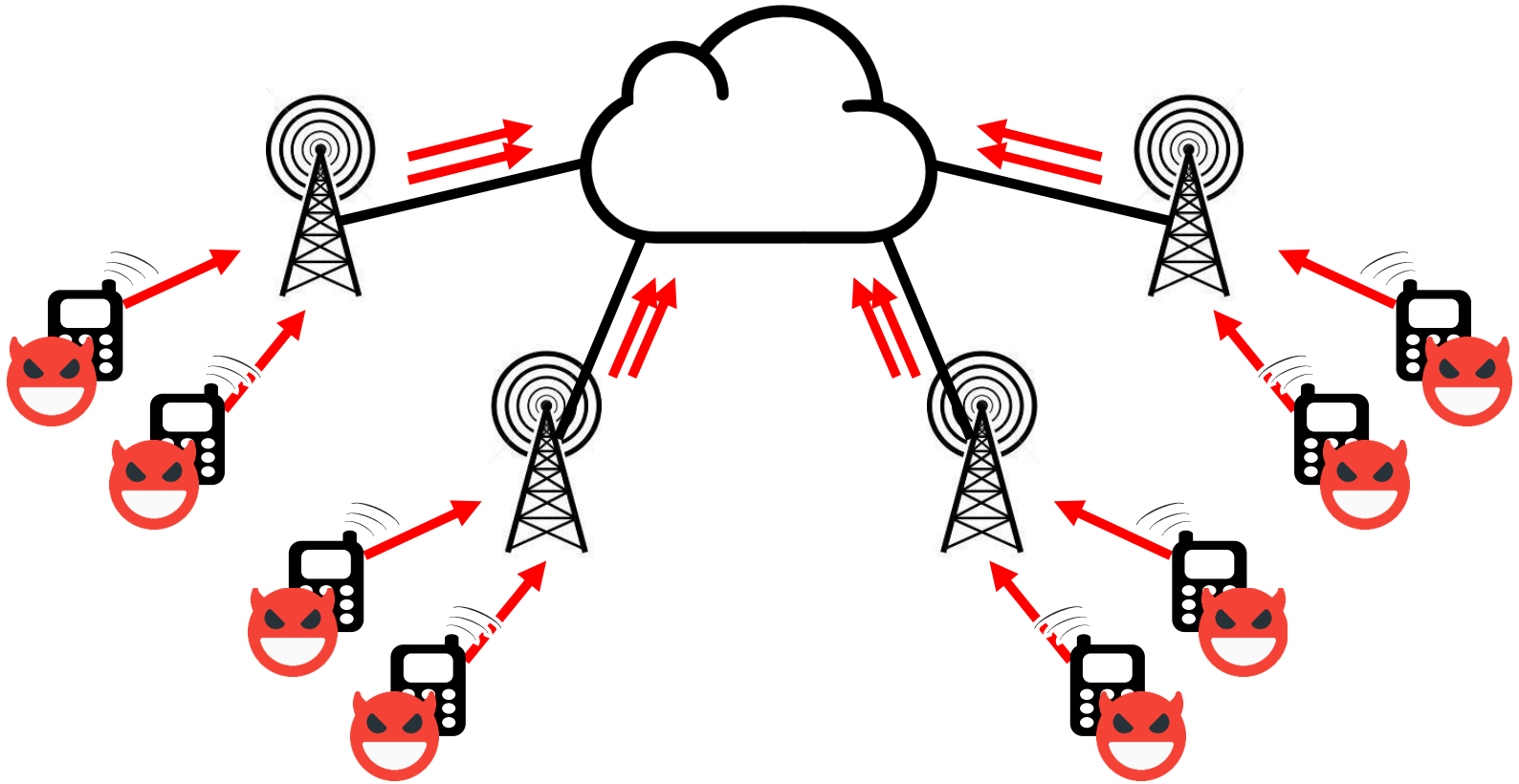
SigOver



FBS

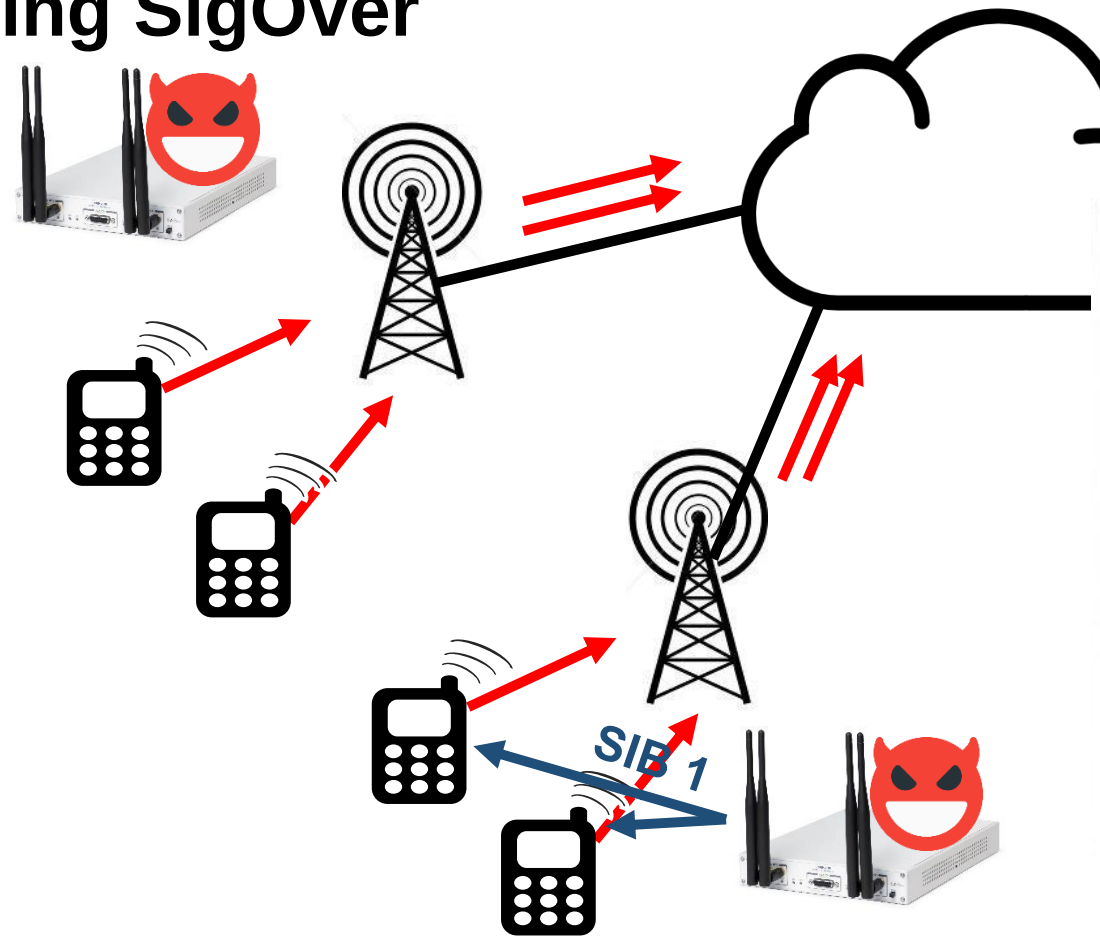
Signaling Storm

- Using a botnet in general



Signaling Storm

Using SigOver

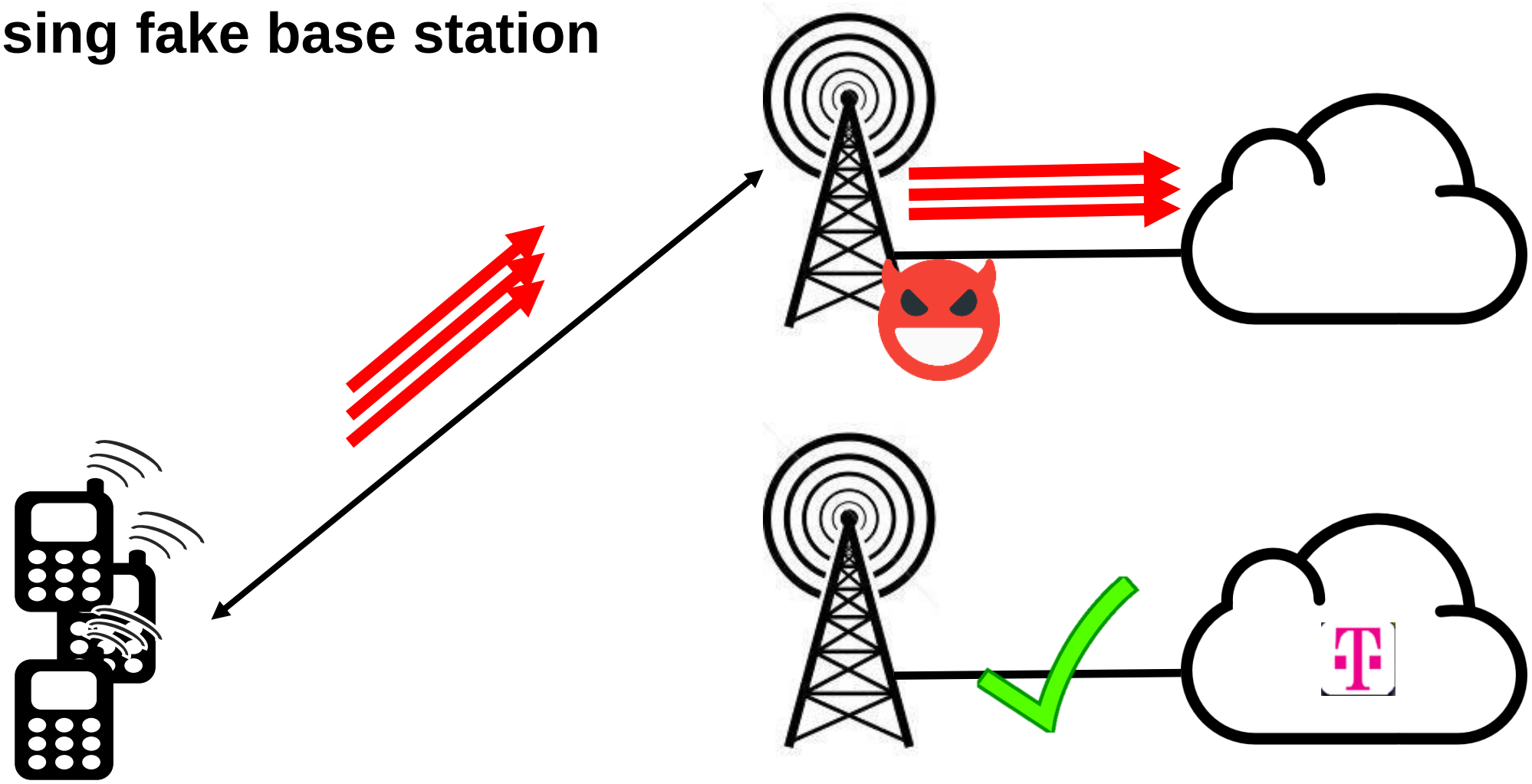


Information Elements		
Cell Access Information	PLMN Identity List (1 to 6 instances)	PLMN Identity
		Cell Reserved for Operator Use
	Tracking Area Code	
	Cell Identity	
	Cell Barred	
	Intra-Frequency Cell Reselection Allowed	
	CSG Indication	
	CSG Identity	
Cell Selection Information	Qrxlevmin	
	Qrxlevminoffset	
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

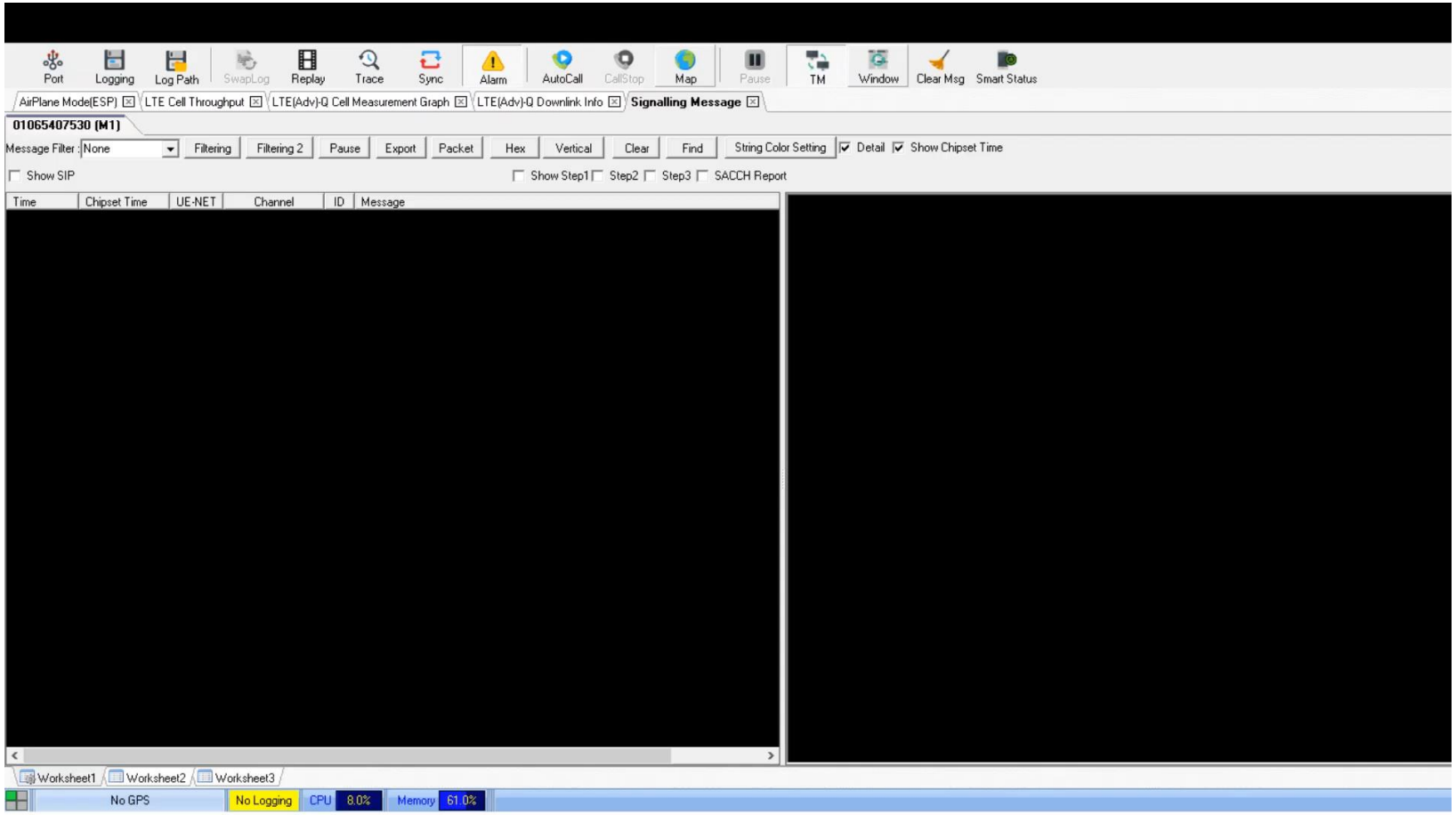
Total number of Signaling Messages

- 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

Signaling Storm Demo



Fake Emergency Alert Message

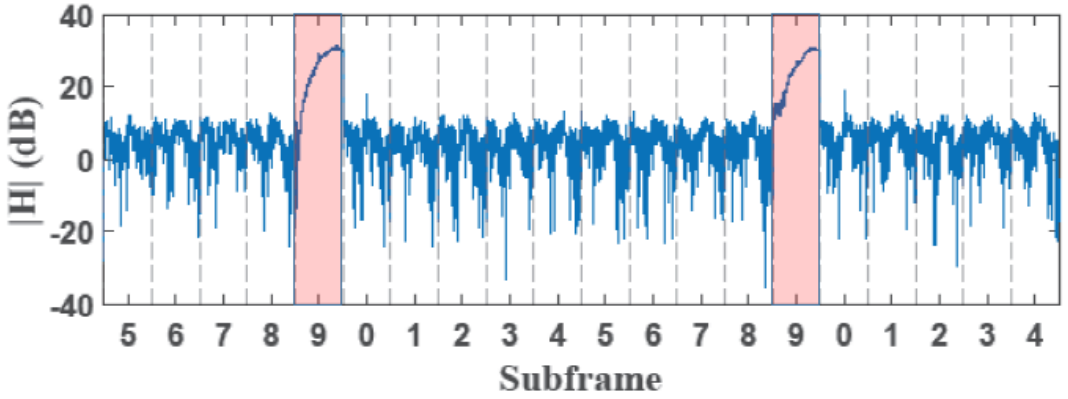
For more videos…

- Please check our YouTube channel
  - SYSSEC KAIST

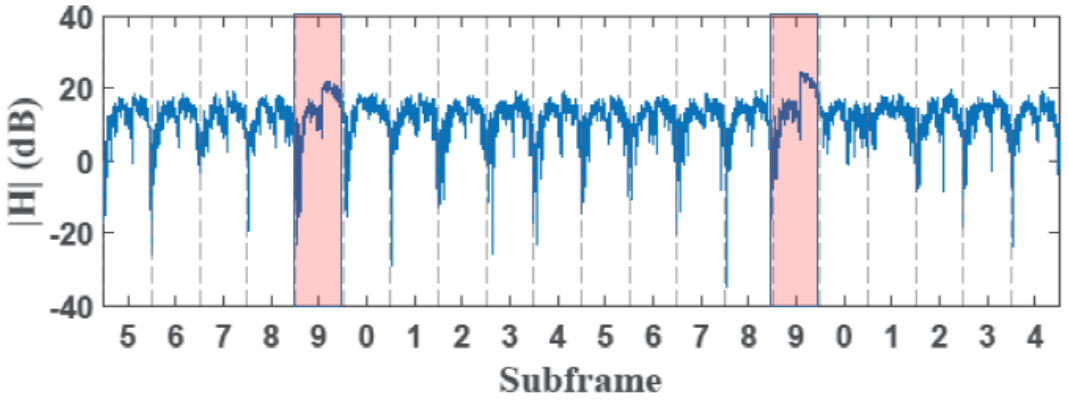
https://www.youtube.com/channel/UCg1-TiATZj4qB0Xqknl18mA

Defense

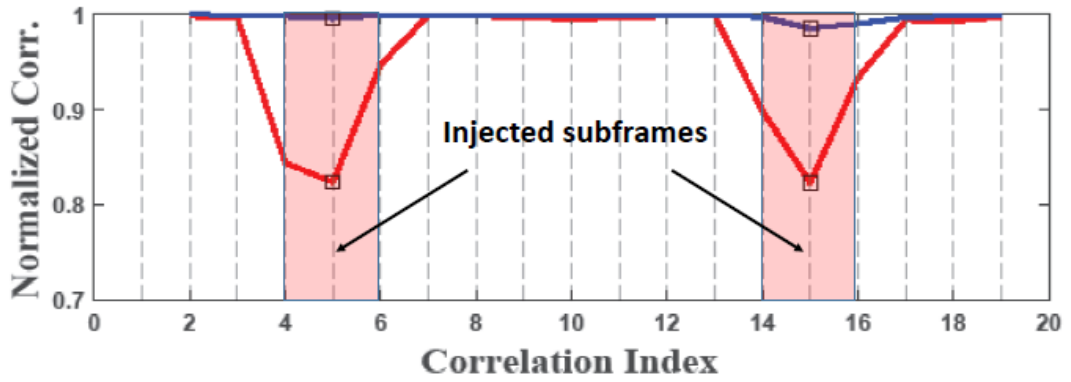
- Detect it physically
  - Correlation



(a) LOS setup



(b) NLOS setup



Blue line: NLOS

Red line: LOS

Defense

- Integrity protection on broadcast messages

- 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
- 3GPP to use digital signature despite key management issue

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
- 3GPP to use digital signature despite key management issue
- Responsible disclosure
  - GSMA: no practical implication ☺
  - Qualcomm: acknowledged

Question List

- **SigOver in 5G**
  - Is this attack also possible in 5G?
  - For now, is the 5G NR against the SigOver attack evaluated?
- **Future work**
  - What is the information contained in single subframe, and also critical so that it can be selected as target? I wonder if I can know some examples.
  - Could you explain more about SigOver attack used to attach UE to FBS?
- **Action of 3GPP**
  - This paper and the previous paper “Breaking LTE on layer two” show that integrity protection is needed. However, because of the various reasons like overhead, it is still not mandatory so I think the attack is still possible. Then this means security is less important than the reasons?
  - Is there any change in the design of broadcast messages after the publication of this paper?
  - Is digital signing (using PKI) or another defense mechanism suggested in this paper (ex - Leveraging Channel Diversity) now implemented in 3GPP standard for LTE or 5G?

SigOver in 5G

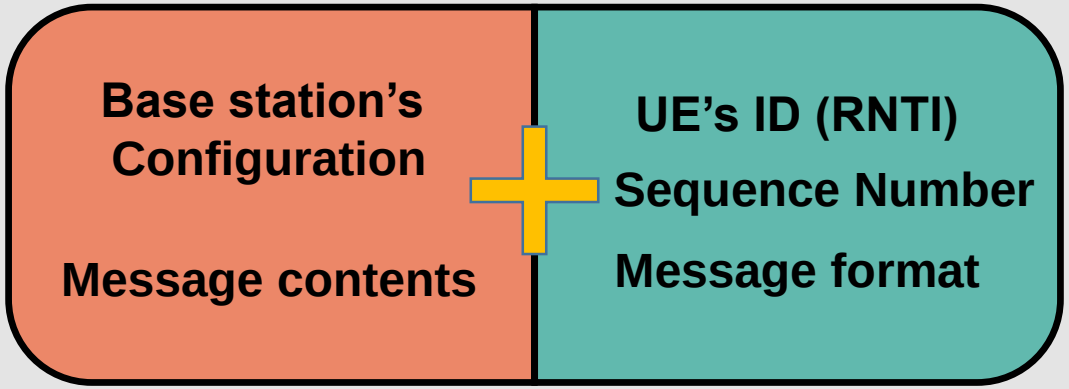
- Will SigOver Work in 5G?
  - “Yes” for now
  - Current Non-standalone design → Definitely “Yes”
    - 5G NSA uses the SAME Control plane messages in LTE
  - Standalone design? → “Partially Yes” (*Unless PKI is adopted)*
    - 5G SA uses the SAME (and similar) frame structure
    - Subframe is sent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

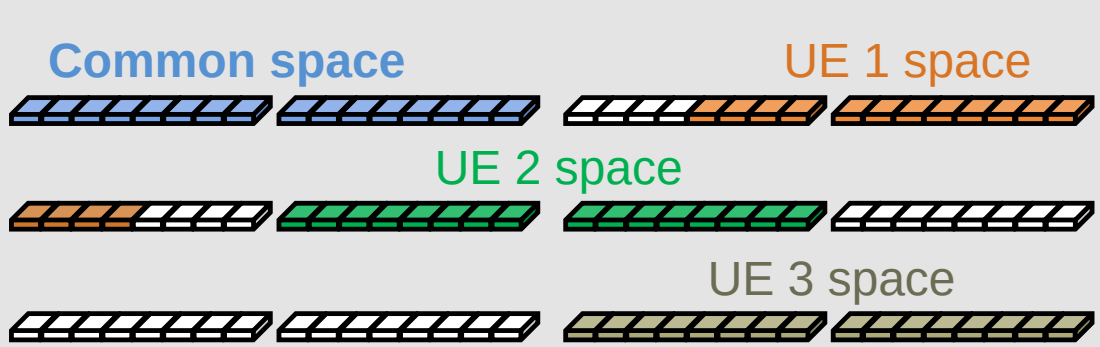
After then?

- SigOver + alpha : Signal overshadowing attack on LTE and its applications (The 36th Chaos Communication Congress, 2019)
- AdaptOver: Adaptive Overshadowing of LTE signals (submitted to USENIX Security ’22, arXiv)
- Data-Plane Signaling in Cellular IoT: Attacks and Defense (MobiCom 2021)

After then?

- SigOver + alpha : Signal overshadowing attack on LTE and its applications (The 36th Chaos Communication Congress)
  - ➢ Inject **unicast message** with SigOver to force victim to attach to FBS

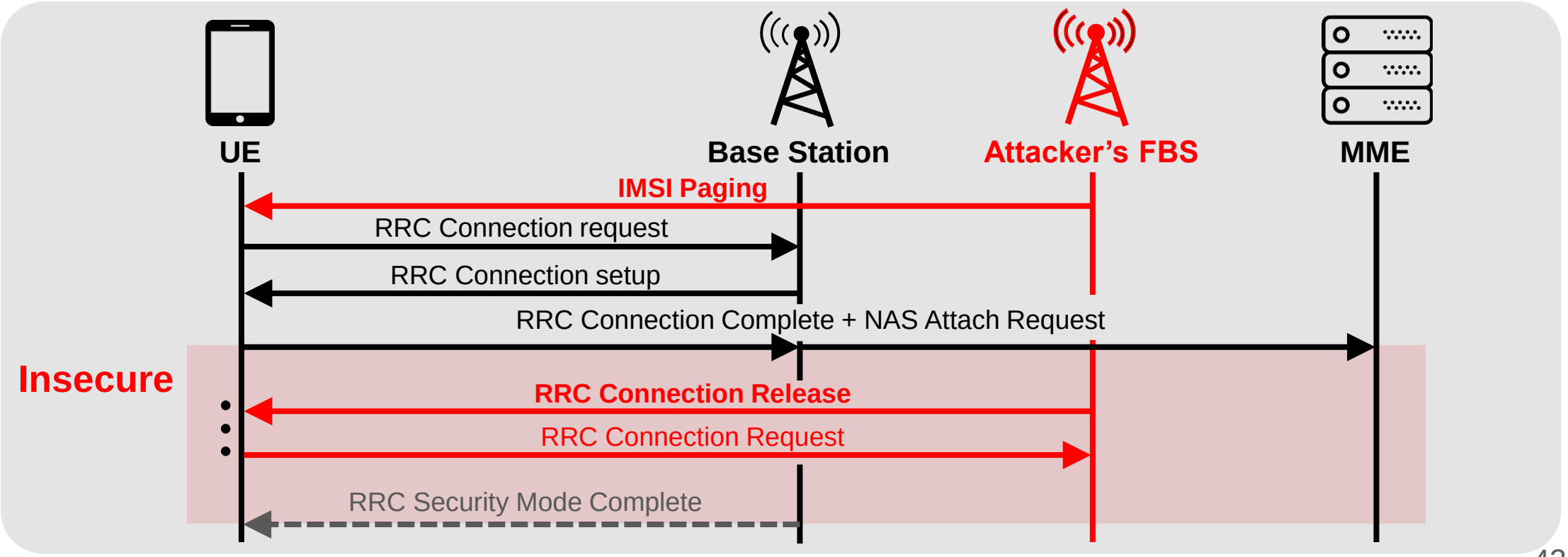




RNTI : Radio Network Temporary Identifier

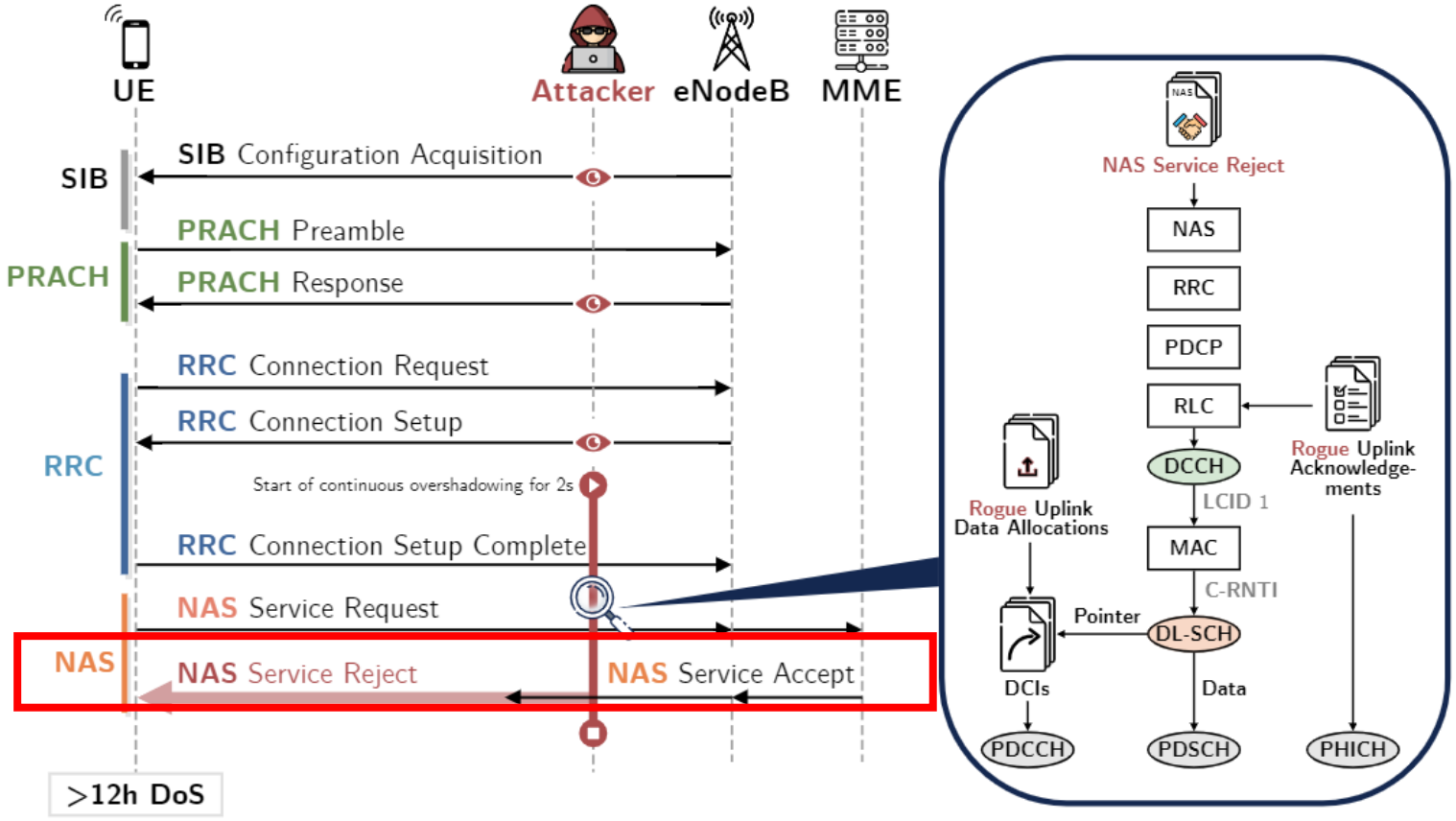
SigOver + Alpha

- Brief overview of the attack
  - ➢ Inject plain RRC message before security activation



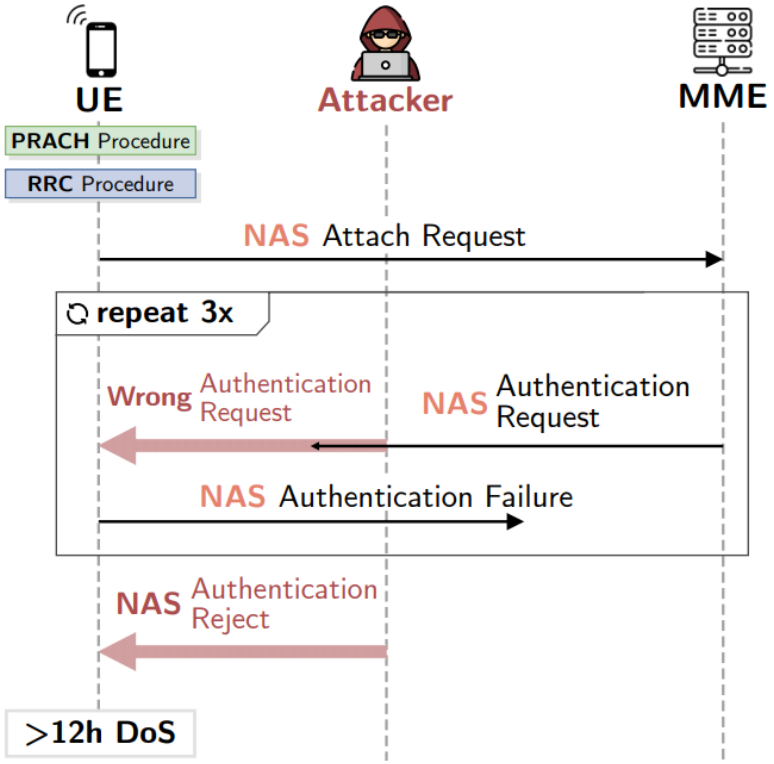
After then?

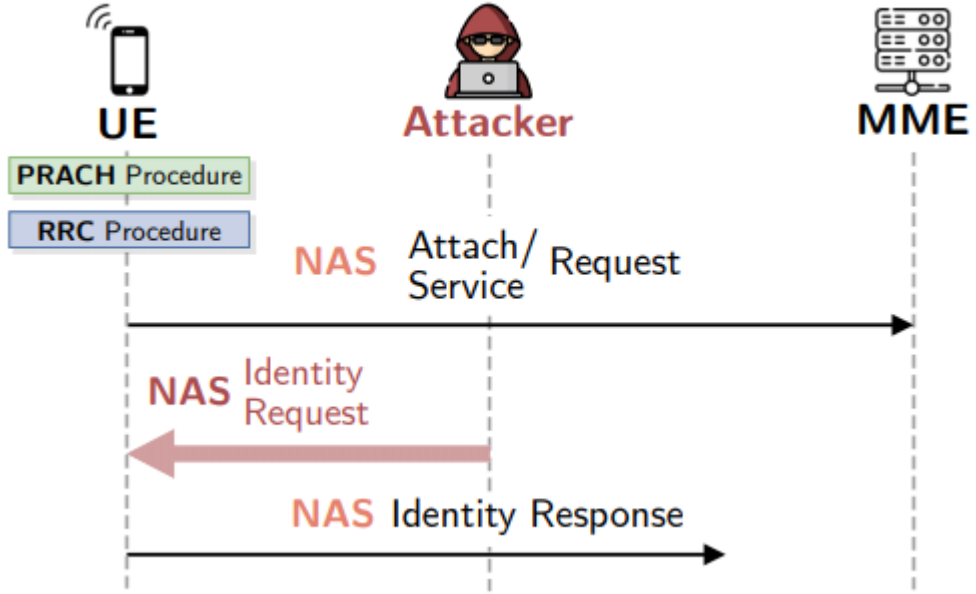
- AdaptOver: Adaptive Overshadowing of LTE signals (submitted to USENIX Security ’22, arXiv)
  - Inject **unicast NAS message** with SigOver to 12h DoS and IMSI catching



AdaptOver

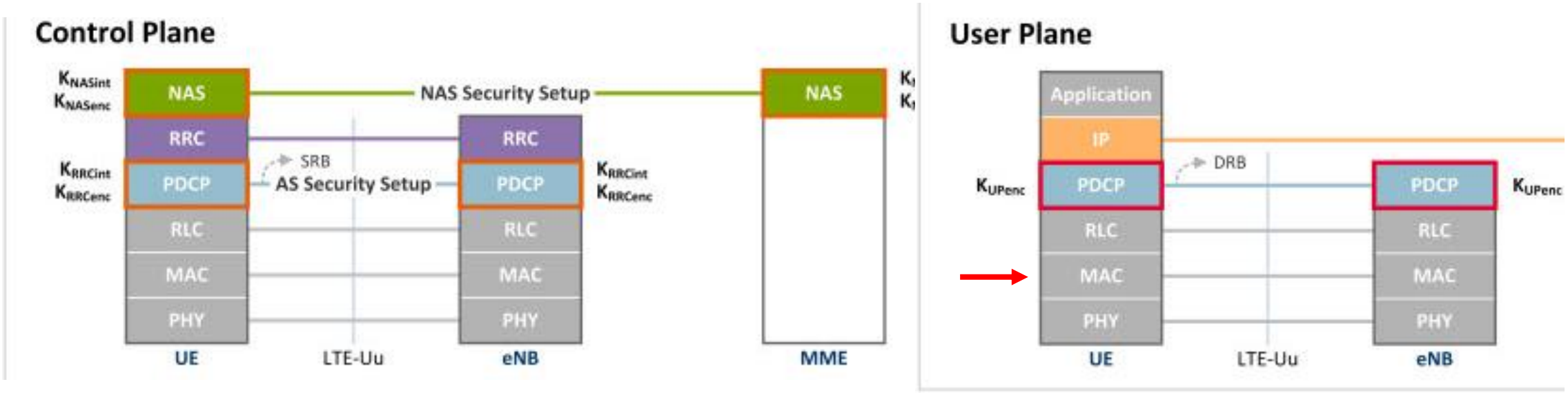
- Authentication Reject Attack
- IMSI Catching Attack





After then?

- Data-Plane Signaling in Cellular IoT: Attacks and Defense (MobiCom 2021)
  - Inject unicast MAC CE message with SigOver for various attacks



Action of 3GPP

- Adopting PKI for Broadcast Messages have several challenges

- 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**

THANK YOU.
ANY QUESTIONS?

BACKUP

Will SigOver Work in 5G?

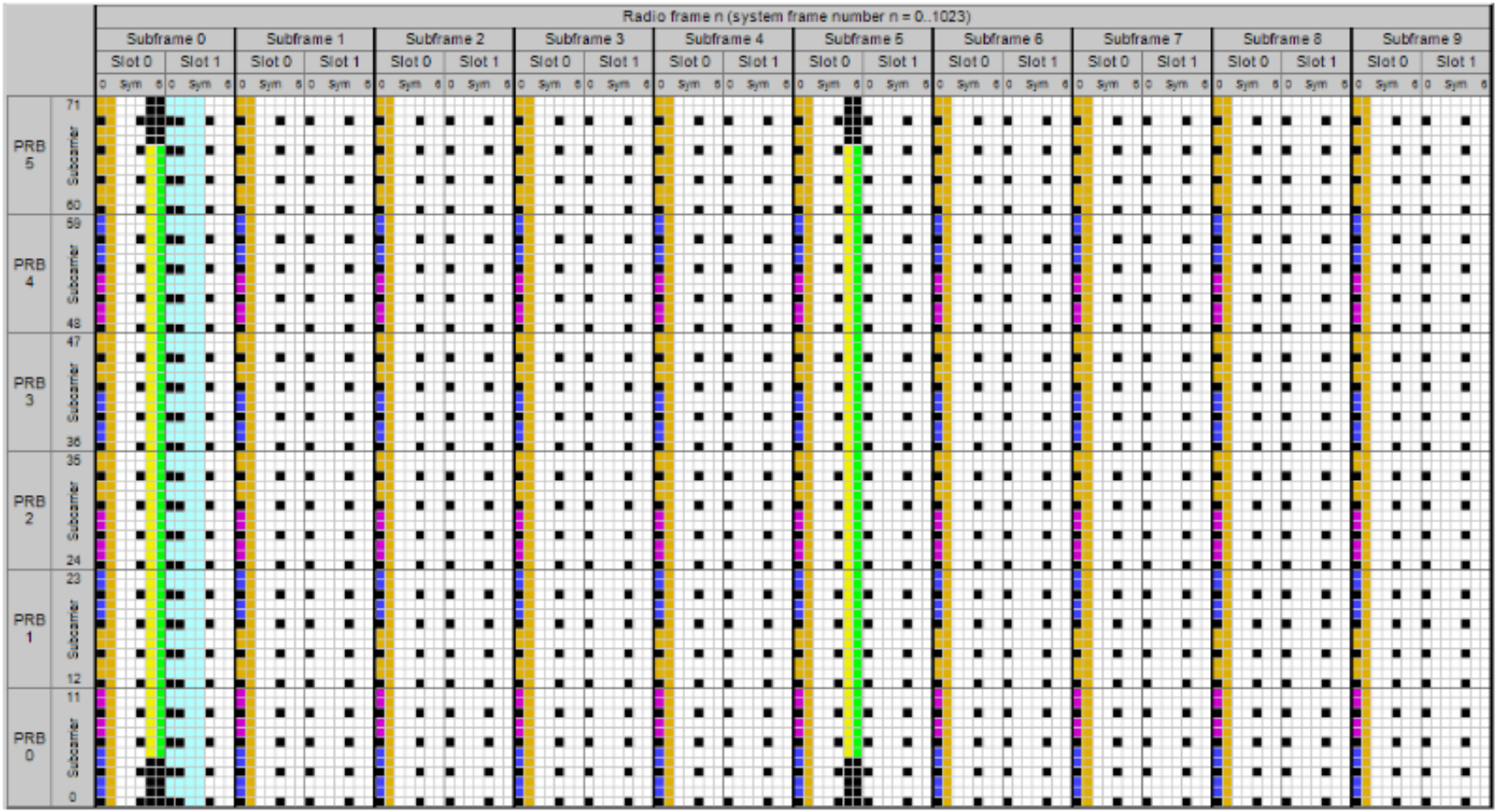
- We believe “Yes” for now
- Current Non-standalone design → Definitely “Yes”
  - 5G NSA uses the SAME Control plane messages in LTE
- Standalone design? → “Partially Yes” (*Unless PKI is adopted)*
  - 5G SA uses the SAME (and similar) frame structure
  - Subframe is sent every 1 msec
- Hardware issues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

LTE Resource Grid



Comparison over MitM & FBS

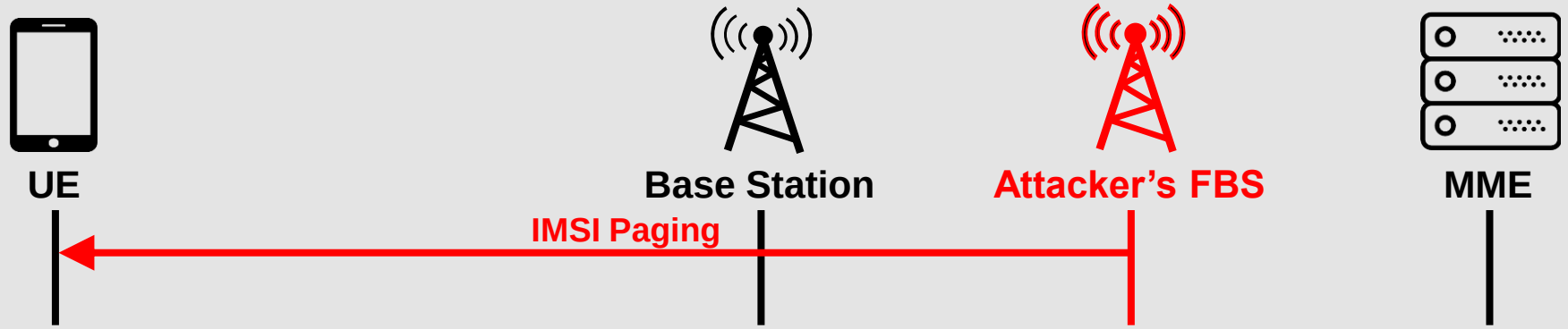
	Stealthiness	Power Efficiency	Attack sustainability
FBS	Low	Low	Low
MiTM	Limited	Low	Limited
SigOver	High	High	High

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”

SigOver + Alpha

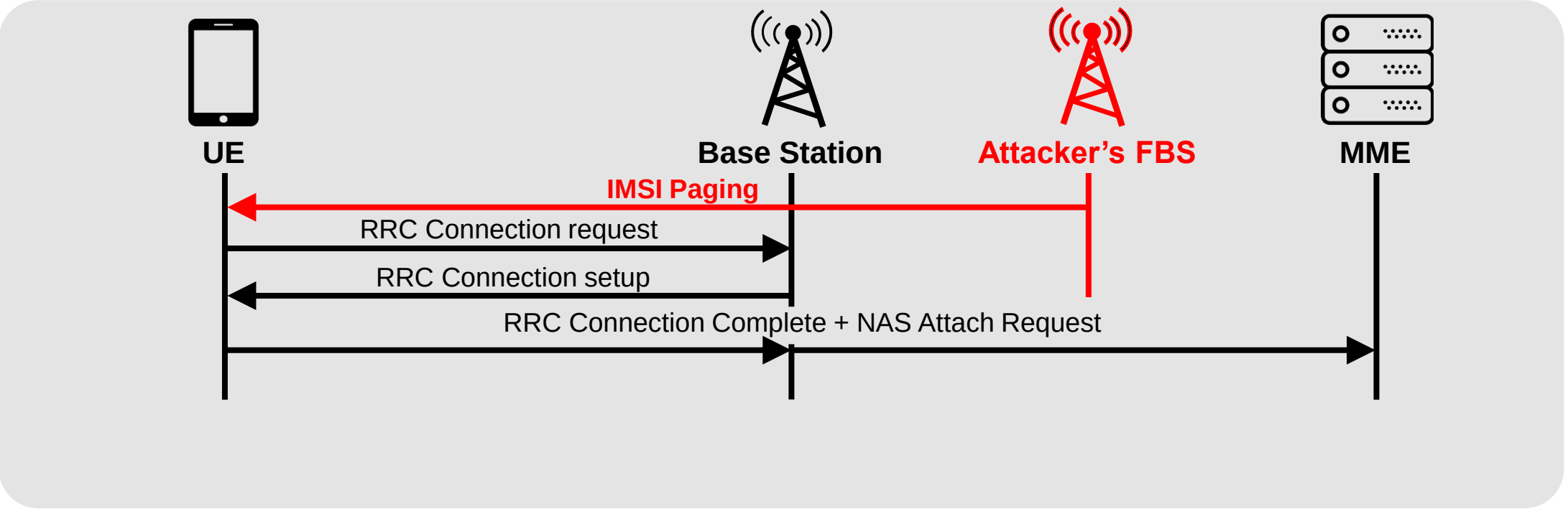
- 1 : Victim is connected to the legitimate network and has security context
  - **SigOver IMSI paging** to delete the security context



3GPP 24.301 : **UE immediately terminates all service sessions, deletes parameters** including GUTI, KSI_{ASME} and **initiates the registration procedure** using the IMSI as the identifier on **paging message.**

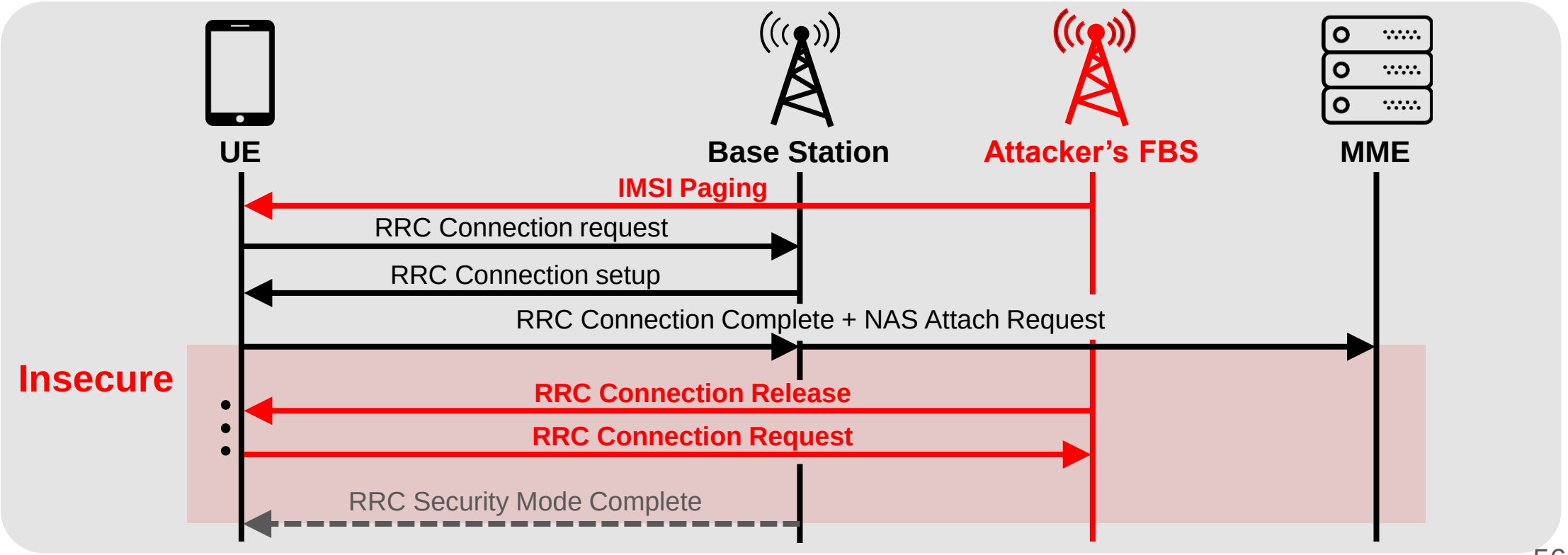
SigOver + Alpha

- 2 : Victim performs the connection and registration process again



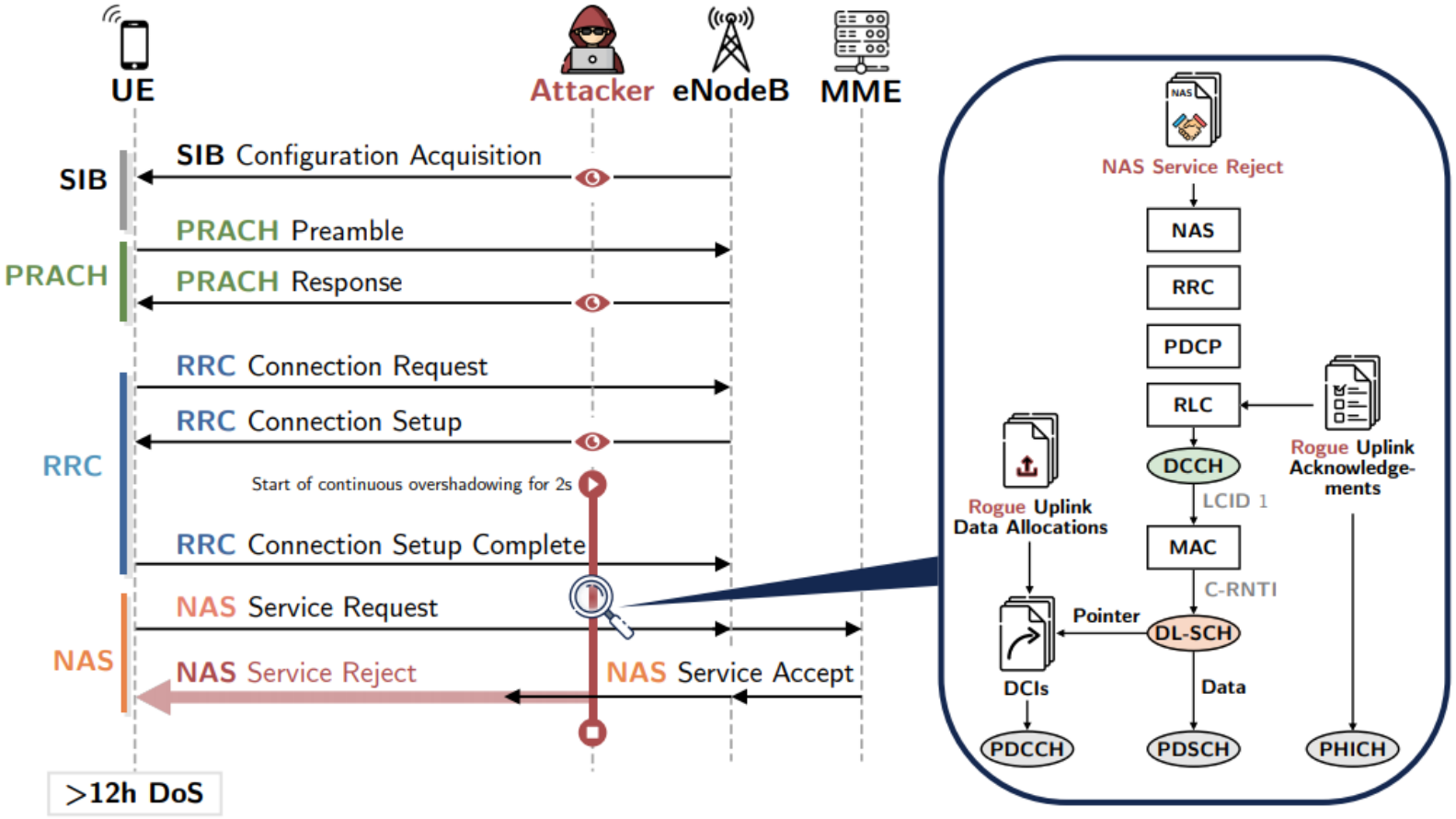
SigOver + Alpha

- 3 : Before the victim and the network completes the security process, attacker injects a message



AdaptOver w/ Service Reject

- Attacker assumption
  - No key
  - DL Sniffer
  - Power >3dB
- Service Request
  - UE with light usage: every 6 mins
  - ***EMM cause 8:*** EPS services and non-EPS services not allowed

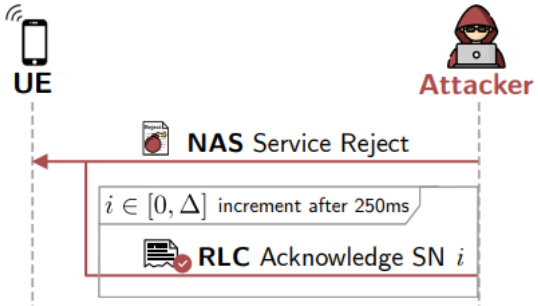


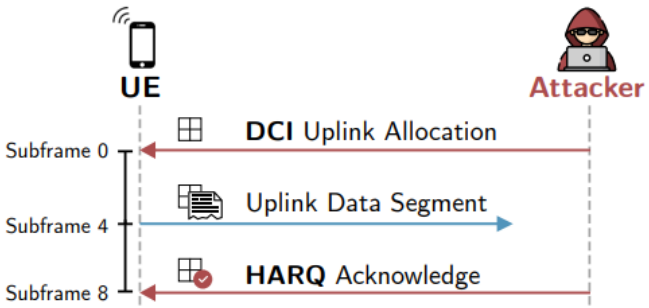
AdaptOver w/ Service Reject in detail

- Service Reject with cause 8
  - UE considering the SIM card as invalid
  - Unless the user retries, the UE will back off by more than 12 h
- Attack timing
  - Upon receiving the **RRC Connection Setup**, it **continuously** inject Service Reject message on every subframe for **2 sec**
  - Experiment showed that 50ms also sufficed
- Challenge
  1. Too early injection : can overshadow uplink allocation for Service Request
  2. Injection must happen before the next DL message (at most before 8ms)
- Approach
  - Also inject uplink allocation and ACK
  - Achieve a latency of less than 6ms between receiving DL message and starting AdaptOver

Implementation

- DL decoder
  - Listen PRACH Response message to acquire RNTI
  - Decode PDSCH messages (parameter, attack timing)
- Uplink allocation
  - Send uplink allocation at the subframe 0 of every frame
  - Send HARQ ACK at the subframe 8
- Sequence number of ACK
  - RLC : While messages are segmented, ACK must be sent for the highest seq number
  - MAC





EMM cause #8?

- Well, it was covered
  - LTE and IMSI catcher myths (2015, Altaf, BlackHat Europe)
  - Practical attacks against privacy and ~ (2016, Altaf, NDSS)
  - LTE security, protocol exploits and location~ (2016, Roger Piqueras Jover)

Cause #8 – EPS services and non-EPS services not allowed

This EMM cause is sent to the UE when it is not allowed to operate either EPS or non-EPS services.

5.6.1.5 Service request procedure not accepted by the network

The UE shall take the following actions depending on the received EMM cause value in the SERVICE REJECT message.

#3 (Illegal UE);

#6 (Illegal ME); or

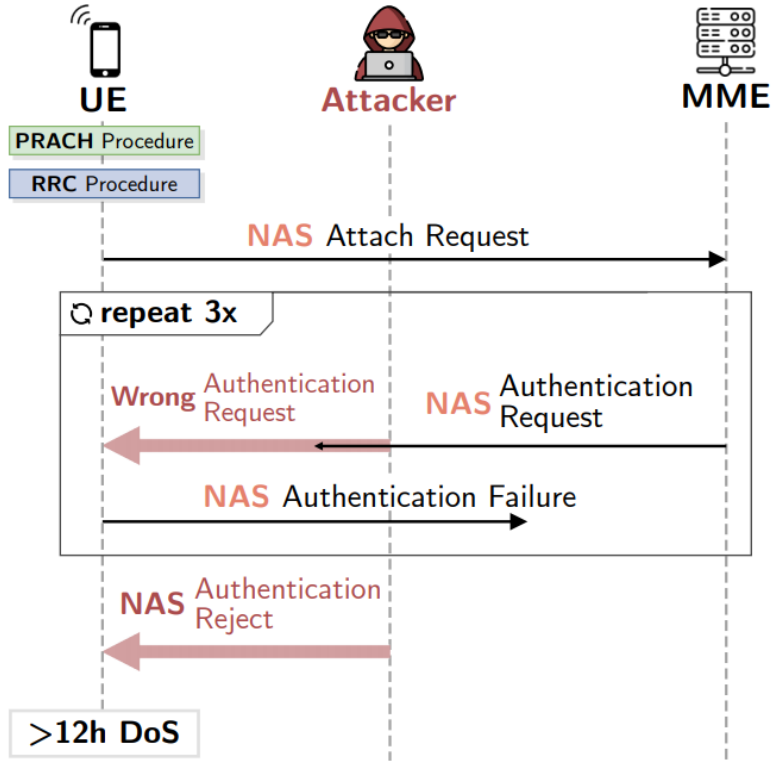
#8 (EPS services and non-EPS services not allowed);

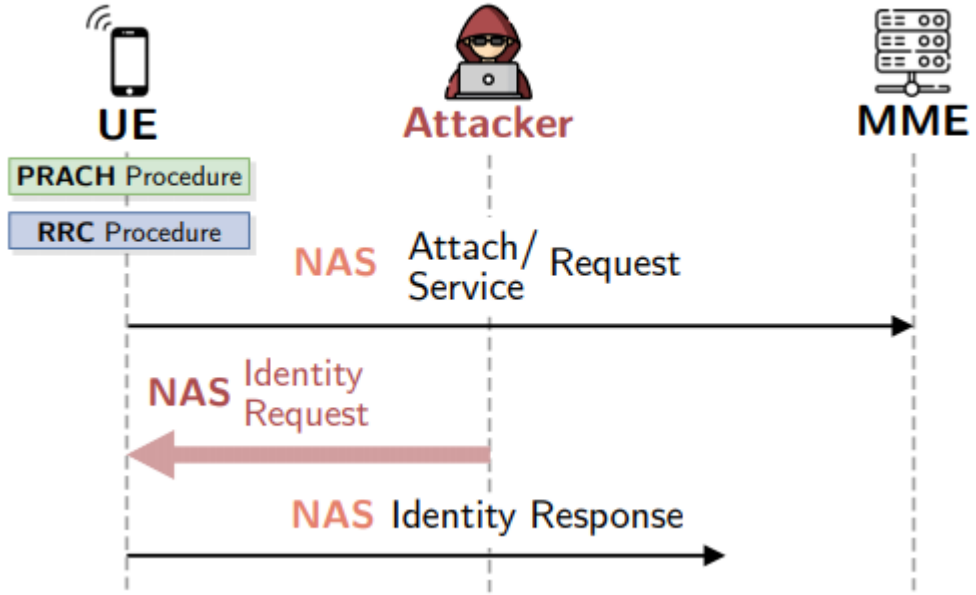
The UE shall set the EPS update status to EU3 ROAMING NOT ALLOWED (and shall store it according to subclause 5.1.3.3) and shall delete any GUTI, last visited registered TAI, TAI list and eKSI. The UE shall consider the USIM as invalid for EPS services until switching off or the UICC containing the USIM is removed or the timer T3245 expires as described in subclause 5.3.7a. The UE shall enter the state EMM-DEREGISTERED. If the message has been successfully integrity checked by the NAS and the UE maintains a counter for "SIM/USIM considered invalid for GPRS services", then the UE shall set this counter to UE implementation-specific maximum value.

If A/Gb mode or Iu mode is supported by the UE, the UE shall handle the GMM parameters GMM state, GPRS update status, P-TMSI, P-TMSI signature, RAI and GPRS ciphering key sequence number and the MM parameters update status, TMSI, LAI and ciphering key sequence number as specified in 3GPP TS 24.008 [13] for the case when the service request procedure is rejected with the GMM cause with the same value. The USIM shall be considered as invalid also for non-EPS services until switching off or the UICC containing the USIM is removed or the timer T3245 expires as described in subclause 5.3.7a. If the message has been successfully integrity checked by the NAS and the UE maintains a counter for "SIM/USIM considered invalid for non-GPRS services", then the UE shall set this counter to UE implementation-specific maximum value.

Other Attacks Based on AdaptOver

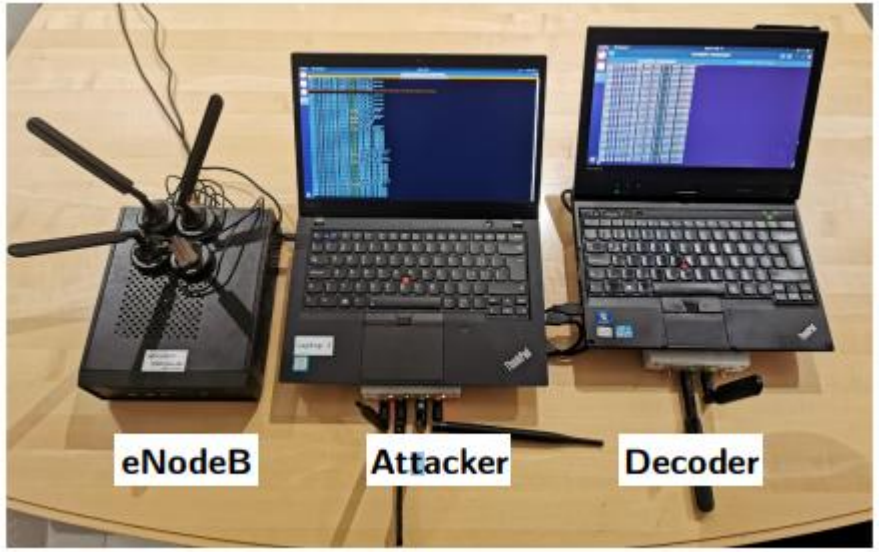
- Authentication Reject Attack
- IM





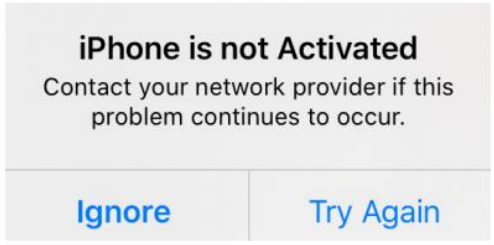
Hardware Setup

- Laptop
- B210
- srsLTE
- Amarisoft Callbox

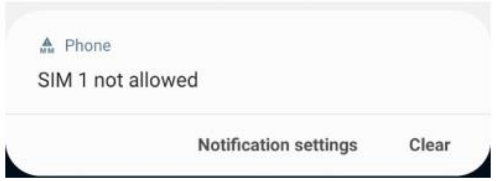


Result

- DoS Attack



(a) iPhone 6S



(b) Samsung Galaxy A8

	Service Reject			Attach Reject			Authentication Reject		
Phone	Duration[1]	Action[2]	GUI[3]	Duration[1]	Action[2]	GUI[3]	Duration[1]	Action[2]	GUI[3]
Pixel 2	>12h	R	☐	> 12h	R	☐	> 12h	R	☐
Pixel 3a	>12h	T	☐	> 12h	T	☐	> 12h	T	☐
Huawei P20 Pro	>12h	T	☐	> 12h	T	☐	> 12h	T	☐
Huawei P30	>12h	T	■	> 12h	T	■	>12h	T	■
Huawei P30 Lite	>12h	T	☐	> 12h	T	☐	> 12h	T	☐
Samsung Galaxy A8	>12h	T	■	> 12h	T	■	> 12h	T	☐
Samsung Galaxy S10	>12h	T	■	> 12h	T	■	> 12h	T	☐
LG Nexus 5X	>12h	S	■	> 12h	R	☐	> 12h	R	☐
iPhone 6S	>12h	R	■	> 12h	R	■	> 12h	R	■
iPhone 7	>12h	T	☐	> 12h	T	☐	> 12h	T	☐
iPhone 8	>12h	T	☐	> 12h	T	☐	> 12h	T	☐
iPhone 11	>12h	T	☐	> 12h	T	☐	> 12h	T	☐
iPhone 11 Pro	>12h	T	☐	> 12h	T	☐	> 12h	T	☐
iPhone X	9.78h	T	☐	> 12h	T	☐	> 12h	T	☐
HTC U12+	>12h	T	☐	> 12h	T	☐	> 12h	T	☐
OnePlus 7T Pro	>12h	T	☐	> 12h	T	■	> 12h	T	☐
Xiaomi Mi 9	>12h	T	☐	> 12h	T	☐	> 12h	T	☐
Xiaomi Mi Mix 3 5G	>12h	T	☐	> 12h	T	☐	> 12h	T	☐

[1] Duration until the UE re-established a connection by itself
[2] Action that will re-connect the phone immediately, **T**: Toggle flight mode, **R**: Restart phone, **S**: Reinsert SIM Card
[3] Whether an indicator on the GUI is present

Table 1: Attack Results for DoS Attack carried out by AdaptOver

Power & Distance Requirement

- Power advantage
  - 1.8dB is sufficient
- Distance
  - Assuming 40dBm eNB and 20dBm attacker

$$d_{Attacker} \leq d_{\leftrightarrow} \cdot 10^{\left(\frac{P_{Attacker} - P_{eNodeB} - 3\text{dB}}{20}\right)}$$

$\mu_{J/S}$	$\sigma_{J/S}$	Success Rate
-2.049 dB	0.627	0%
-1.1202 dB	0.675	1.325%
-0.117 dB	0.665	30.625%
0.639 dB	0.619	96.825%
1.870 dB	0.641	100%
2.559 dB	0.733	100%

Table 2: Summary of Overshadowing Success Rate and Resulting J/S

$d_{\leftrightarrow}$	**Downlink** max $d_{Attacker}$
100m	7.1m
500m	35.4m
1km	70.8m

Table 3: Estimated Attack Range for an attacker transmit power of 20dB. The basestation emits its downlink signal with a power of 40dB. $d_{\leftrightarrow}$ denotes distance between UE and basetation. max $d_{Attacker}$ is the distance between attacker and victim UE.