Enabling Physical Localization of Uncooperative Cellular Devices

Taekkyung Oh, Sangwook Bae, Junho Ahn, Yonghwa Lee, Tuan Dinh Hoang,
Min Suk Kang, Nils Ole Tippenhauer, and Yongdae Kim

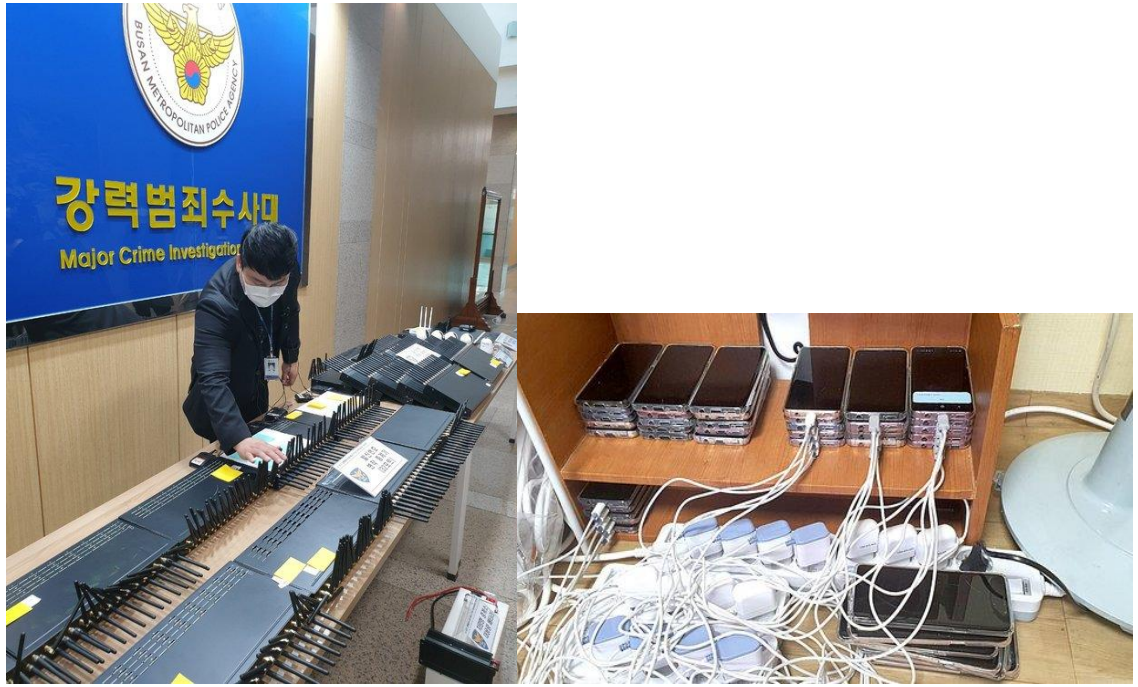
This research was supported and funded by the Korean National Policy Agency
[Tracking and identifying devices and call traffic in voice phishing ecosystem / PR10-03-020-22]

[Homepage] https://sites.google.com/view/uma-site

Localization of uncooperative cellular devices

- In cellular networks, it may need to trace **uncooperative** devices
  - Tracking criminals by law enforcement
    - Vishing (voice phishing, voice scam) investigation: tracking devices used in vishing fraud
  - Search and rescue
    - Kidnapped, missing, etc.

Search and rescue

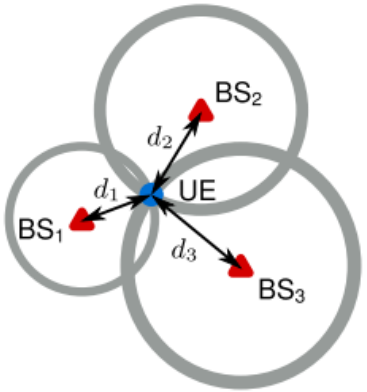


Confiscated vishing devices by Korean Police

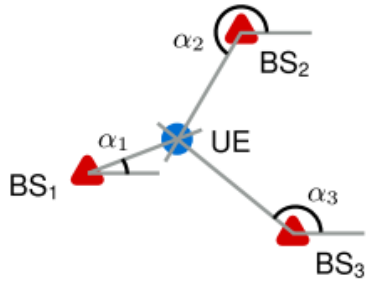
Uncooperative devices: those who don't (can't) collaborate on localization efforts or report their own location

Physical localization of uncooperative devices

- **Physical localization**
  - Tracking the target device "down to the front door" by monitoring its signals
    - Finding location (coordinates, distance, direction) of a target device using wireless signals
    - Fine-grained localization
      - ToA: Time-of-Arrival (Multilateration)
      - AoA: Angle-of-Arrival (Multiangluation)
- **Uncooperative UE (User Equipment)**
  - Devices that neither report their location nor control their traffic (signals) in the physical localization process
  - Criminals, missing person, kidnappee…



(a) Trilateration *



(b) Triangulation *

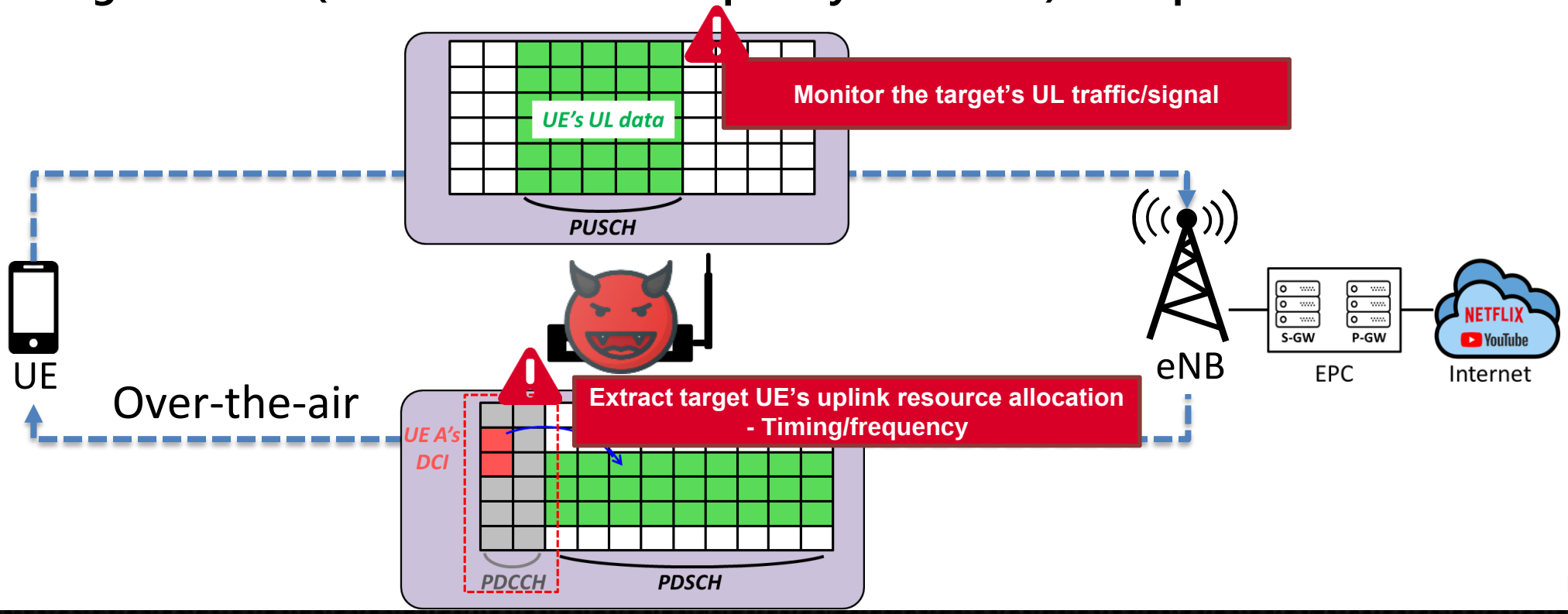
* J. A. del Peral-Rosado et al., "Survey of Cellular Mobile Radio Localization Methods: From 1G to 5G," *IEEE COMST*, 2018

Challenges in LTE networks

- Distinguishing the target's signals from others'
- Trackable only when the target UE generates uplink traffic
- Detecting the target's low-power signals (shadow area & cellular repeater)

1) Differentiating the target's signal

- With LTESniffer*
  - Eavesdropping downlink channel to acquire uplink resource allocation
  - Monitoring uplink signals on target's resources
  - **Target's RNTI (Radio Network Temporary Identifier) is required!**



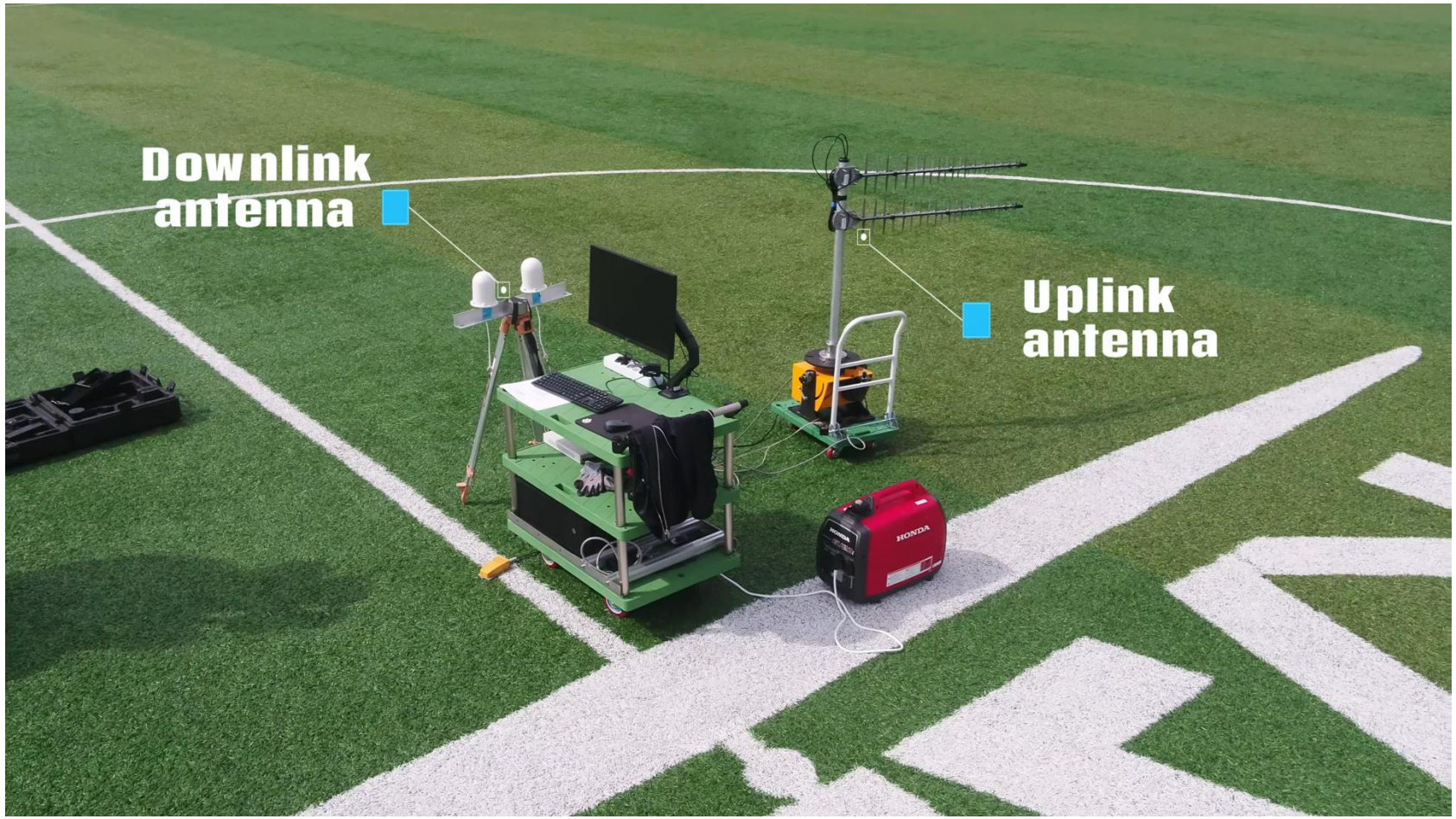
SCAN ME
LTESniffer code

* Hoang et al., "LTESniffer: An Open-source LTE Downlink/Uplink Eavesdropper," *ACM WiSec*, 2023

Identifying the target's RNTI

- Generating traffic pattern with the target's online identity (phone number)
  - Making multiple (silent) SMSes or calls with a specific time gap
- Monitoring downlink traffic of SMSes or calls
- Finding out the connection showing the intended traffic pattern
- Determining the RNTI of that connection as belonging to the target UE

Physical localization with RNTI



2) Depending on the target's traffic and RNTI

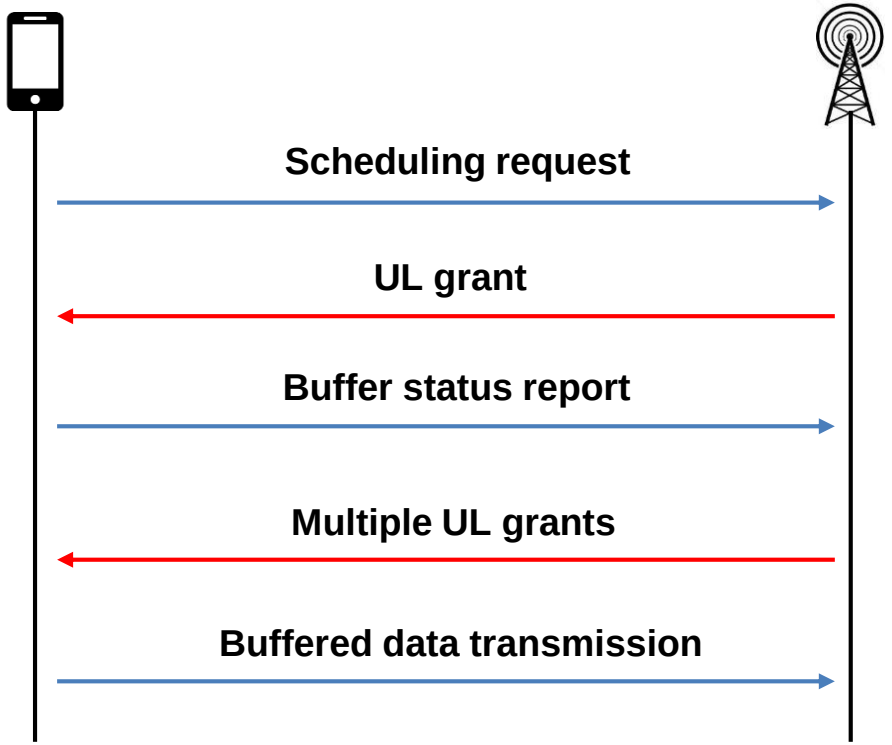
- Trackable only when the target UE generates uplink traffic
- Localization is impossible when the target UE is silent
  - Not transmitting any uplink data during the localization process

- RNTI changes (expires) frequently (about every 15 to 30 seconds*)
  - Trackers should identify the target's RNTI every 15 seconds in the worst case

* Bae et al., "Watching the Watchers: Practical Video Identification Attack in LTE Networks," USENIX *Security*, 2022

Exploiting uplink scheduling

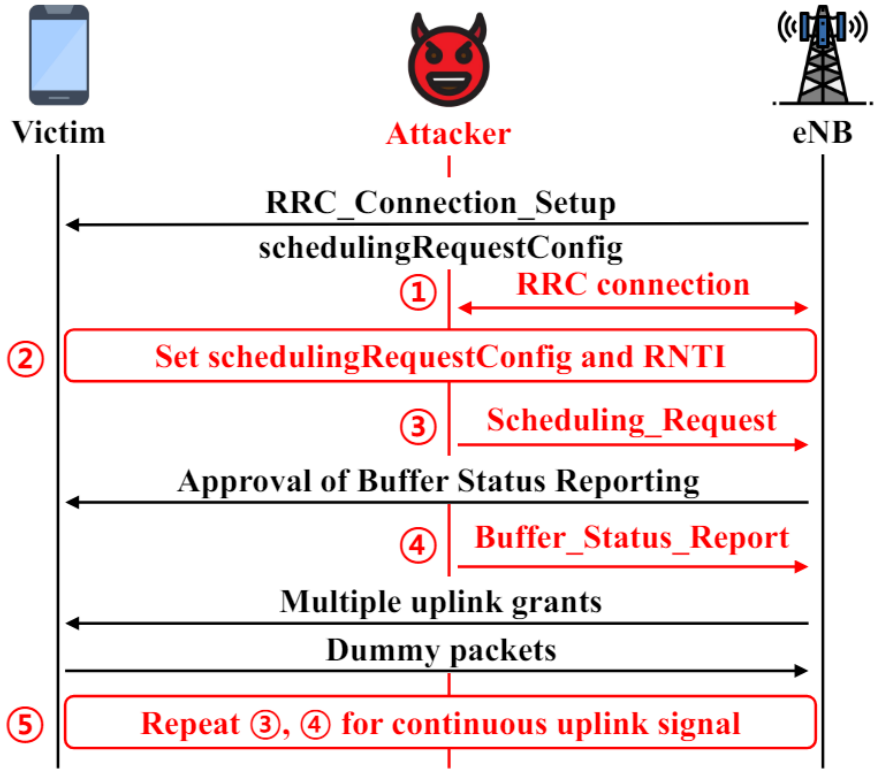
- UE requests uplink scheduling when they have data to transmit
  - Scheduling Request (SR) and Buffer Status Report (BSR)



Uplink scheduling procedure

Scheduling manipulation attack

- **Vulnerability**: Lack of security protection
- Maintaining the target's radio connection and RNTI
- Forcing the target UE to continuously generate uplink traffic

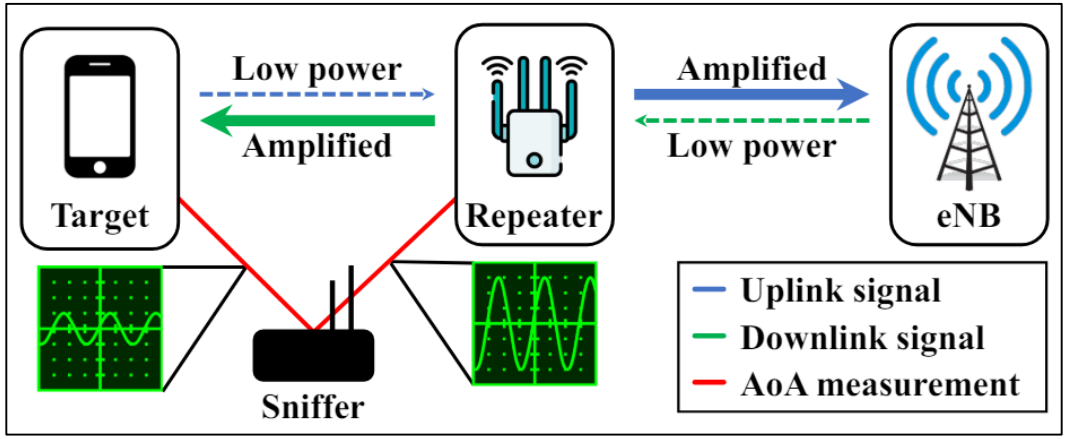


3) Shadow area and cellular repeater

- Uplink transmission power gets very low when the UE is close to the base station (eNB)

Distance (m)	10	20	30	40	50	60	70	80	90	100	110
Tx PWR (dBm)	-7.04	-10.64	0.49	4.74	5.05	4.33	7.65	7.45	7.2	7.39	7.56
RSRP (dBm)	-62.37	-62.63	-73.43	-76.66	-78.91	-81.69	-85.36	-85.51	-86.45	-84.23	-87.6

- Repeaters designed to amplify and replay DL/UL signals to reduce signal path loss between the eNB and UE
  - Repeaters make trackers mistakenly determine the repeater's location as the target's



Exploiting Transmit Power Control

- Uplink transmission power is adjusted to compensate path loss
  - Coordination with UE and eNB
  - Reference Signals Received Power (RSRP)
  - TPC command

- Transmit Power Control (TPC) command
  - Delivered by eNB over DCI 0

- UE can increase its uplink transmission power up to 23 dBm

TABLE 2. Δ_{PUSCH} ACCORDING TO TPC COMMAND IN DCI 0.

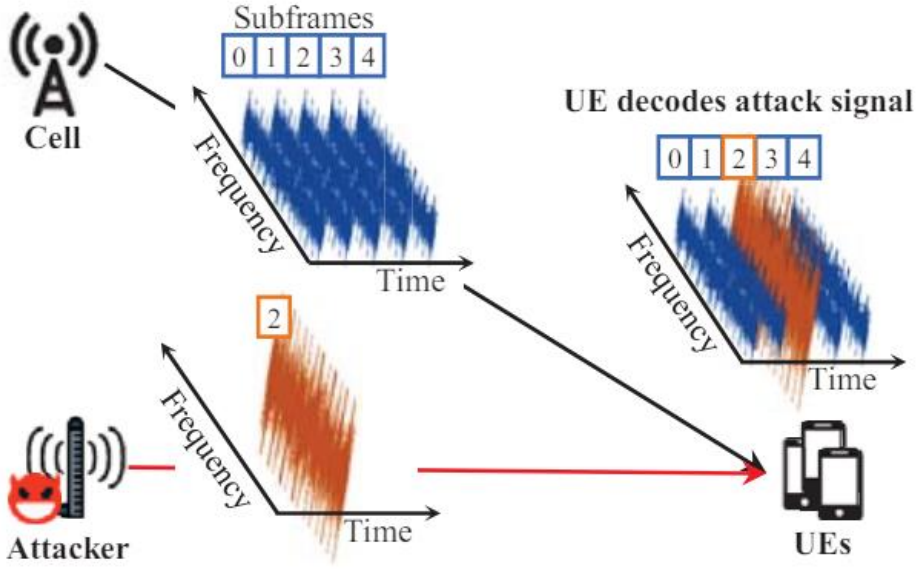
TPC command in DCI 0	0	1	2	3
Accumulated Δ_{PUSCH} (dB)	-1	0	+1	+3

Power boosting attack

- **Vulnerability**: Lack of security protection in DCI 0 message
  - Encryption **X**
  - Integrity check **X**

- Signal overshadowing DCI 0 using SigOver*
  - Targeting the victim's RNTI
  - TPC command 3

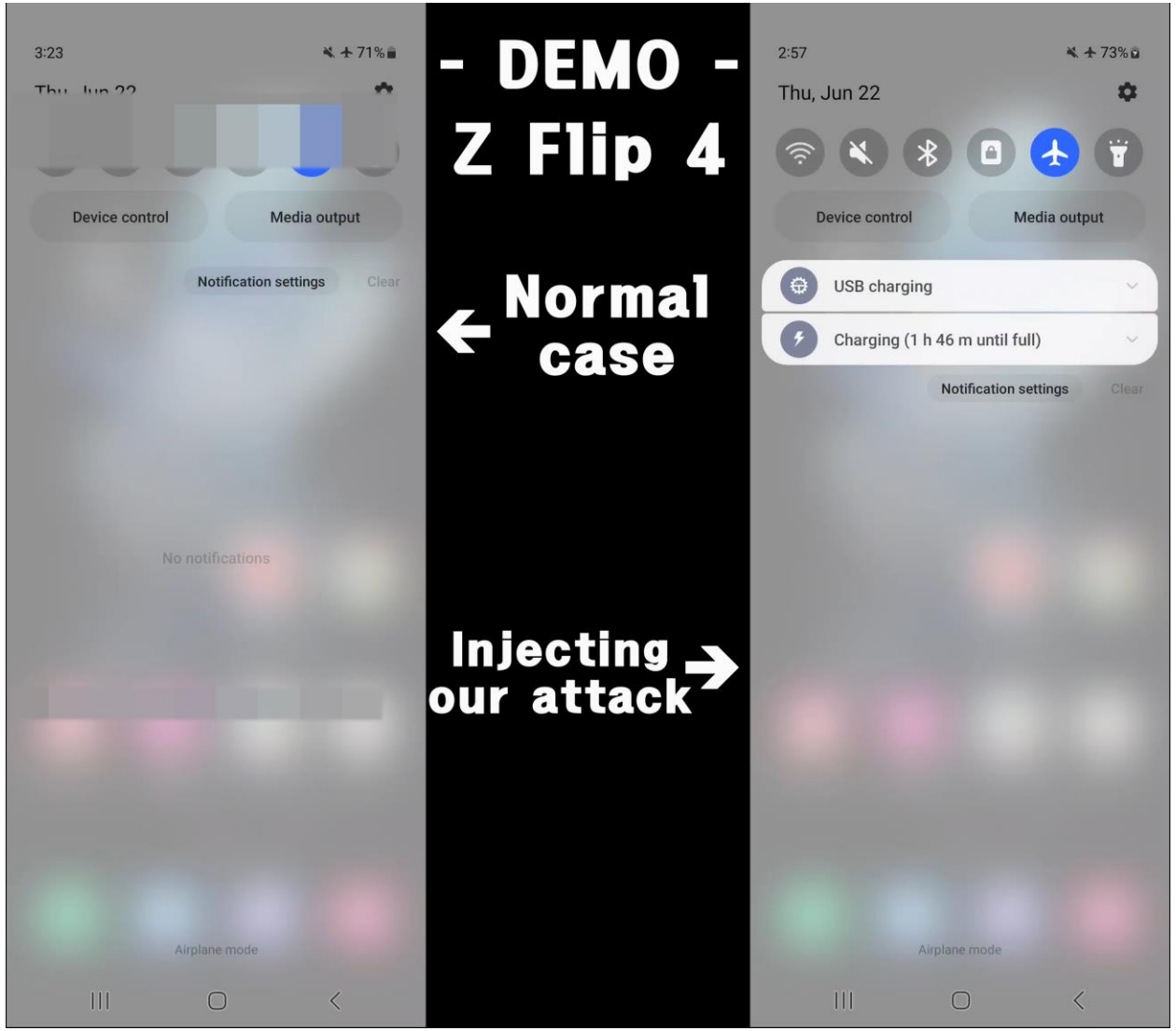
- UE increases its transmission power up to max.
  - 20-23 dBm in 3GPP specification



Physical signal overshadowing attack*

* Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE

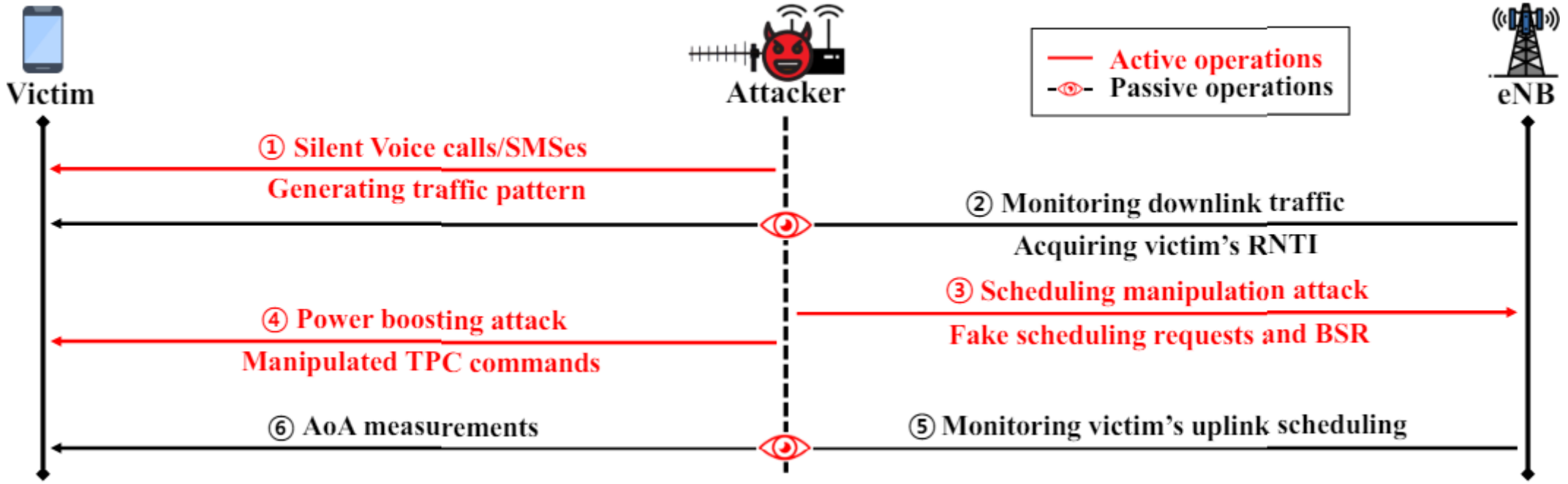
Demo



SYSSEC KAIST

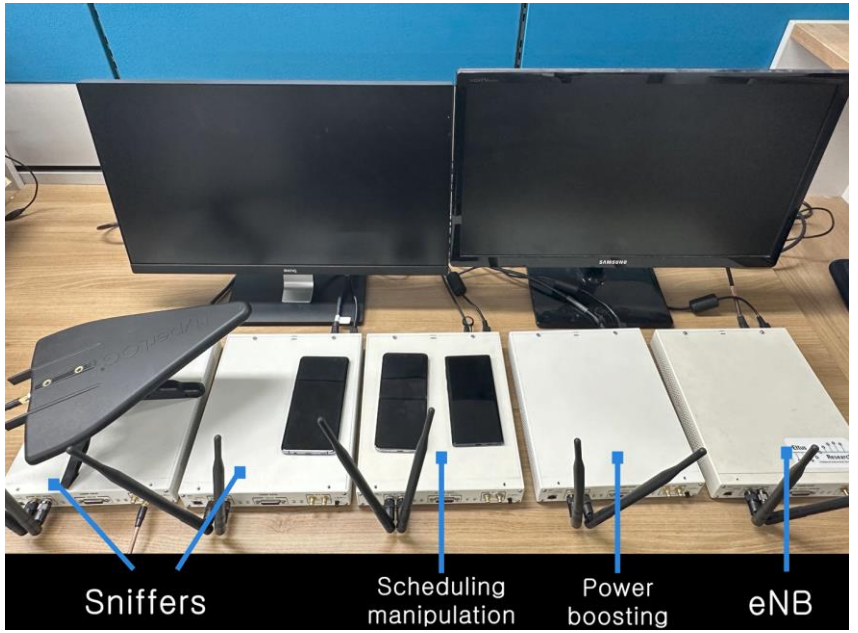
UMA: Uncooperative Multiangulation Attack

- **End-to-End** physical localization of **uncooperative** cellular devices
  - From the target's online identity, down to the front door
  - Without direct control of the network infrastructure and the target devices



End-to-end evaluation

- Three testbed environments with ethical considerations
  - Operational (commercial) network only for passive experiments
  - Lab testbed using srsRAN and USRP X310
  - Commercial testbed with industry-grade LTE solution from Nokia
- Nine COTS cellular devices including five baseband vendors
  - Galaxy Note FE
  - Galaxy Note 10
  - Galaxy S10
  - Galaxy S20
  - LG G8
  - Huawei P30 Pro
  - Galaxy Z Flip 4
  - iPhone XS
  - Redmi Note 9T



Lab testbed environment

End-to-end demo

Conclusion

- **Goal**: Enabling physical localization without coordination of devices
  - From phone number to physical location (reliable & fine-grained)
  - Addressing three realistic challenges with two novel approaches
- Responsible disclosure (GSMA)*
  - *"The risk assessment made by 3GPP has been that attacks on layers below PDCP do not warrant cryptographic protection."*
  - *"For 4G security below PDCP was considered in clause 7.1 of TR 33.821 and it was concluded no cryptographic protected needed."*
- UMA is applicable to other localization techniques
  - Channel State Information (CSI) based, LTrack, LTEye…
- UMA is planned to be utilized for vishing investigation in Korea

Vehicle-mounted localization system

* CVD-2023-70 and CVD-2023-77

Taekkyung Oh

ohtk@kaist.ac.kr

https://ohta

Q&A

Tha

Homepage

[Homepage] https://sites.google.com/view/uma-site