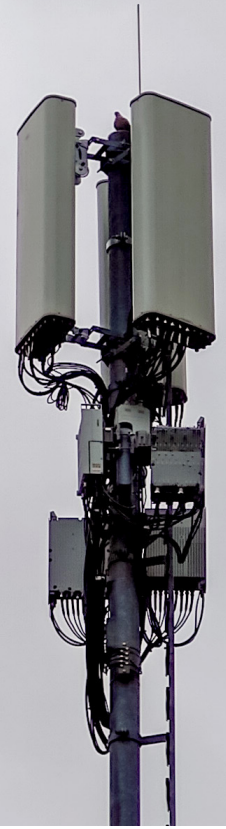
ETH zürich

System Security Group

LTrack: Stealthy Tracking of Mobile Phones in LTE

M. Kotuliak, S. Erni, P. Leu,
M. Röschlin, and S. Čapkun



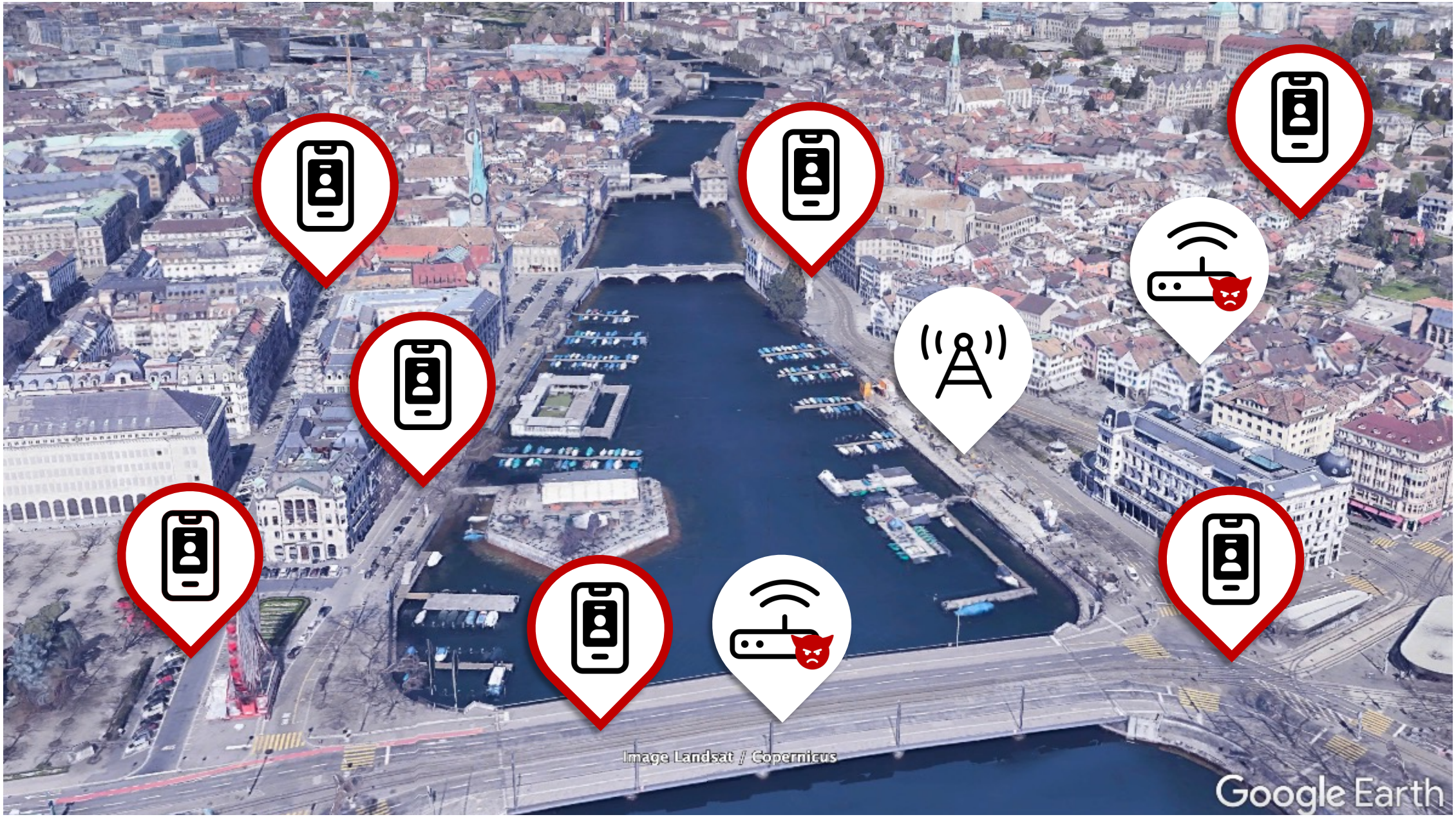


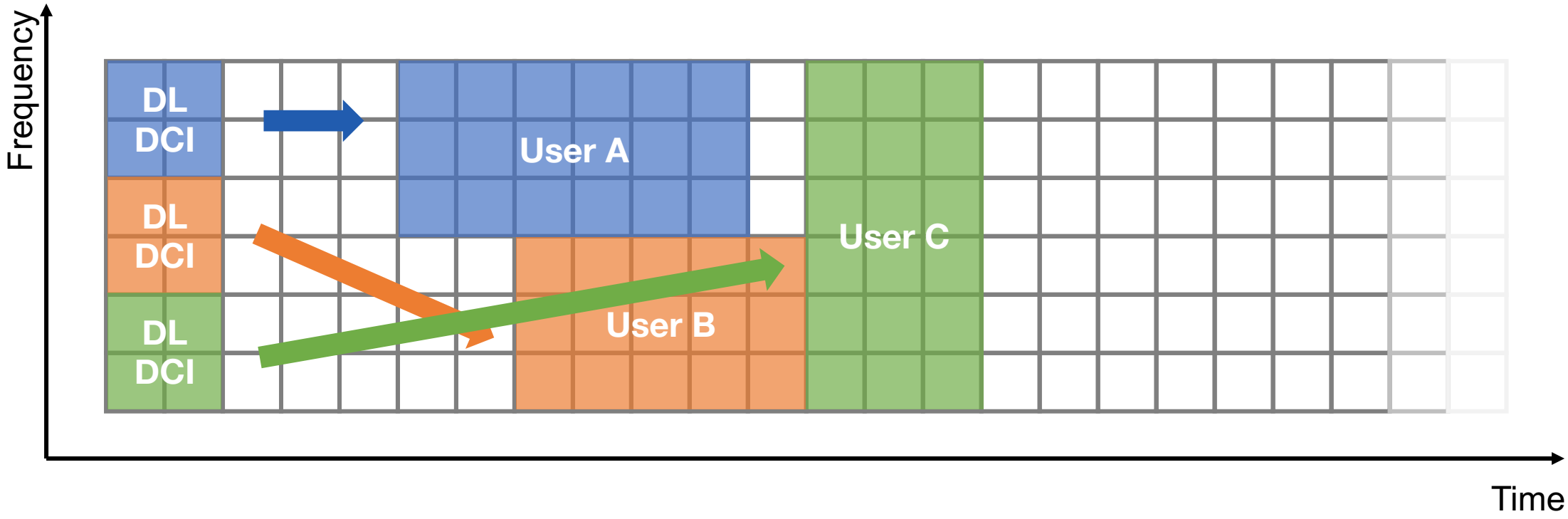
Image Landsat / Copernicus
Google Earth

LTrack
Passive Localization + Stealthy Identification
Image Landsat / Copernicus
Google Earth

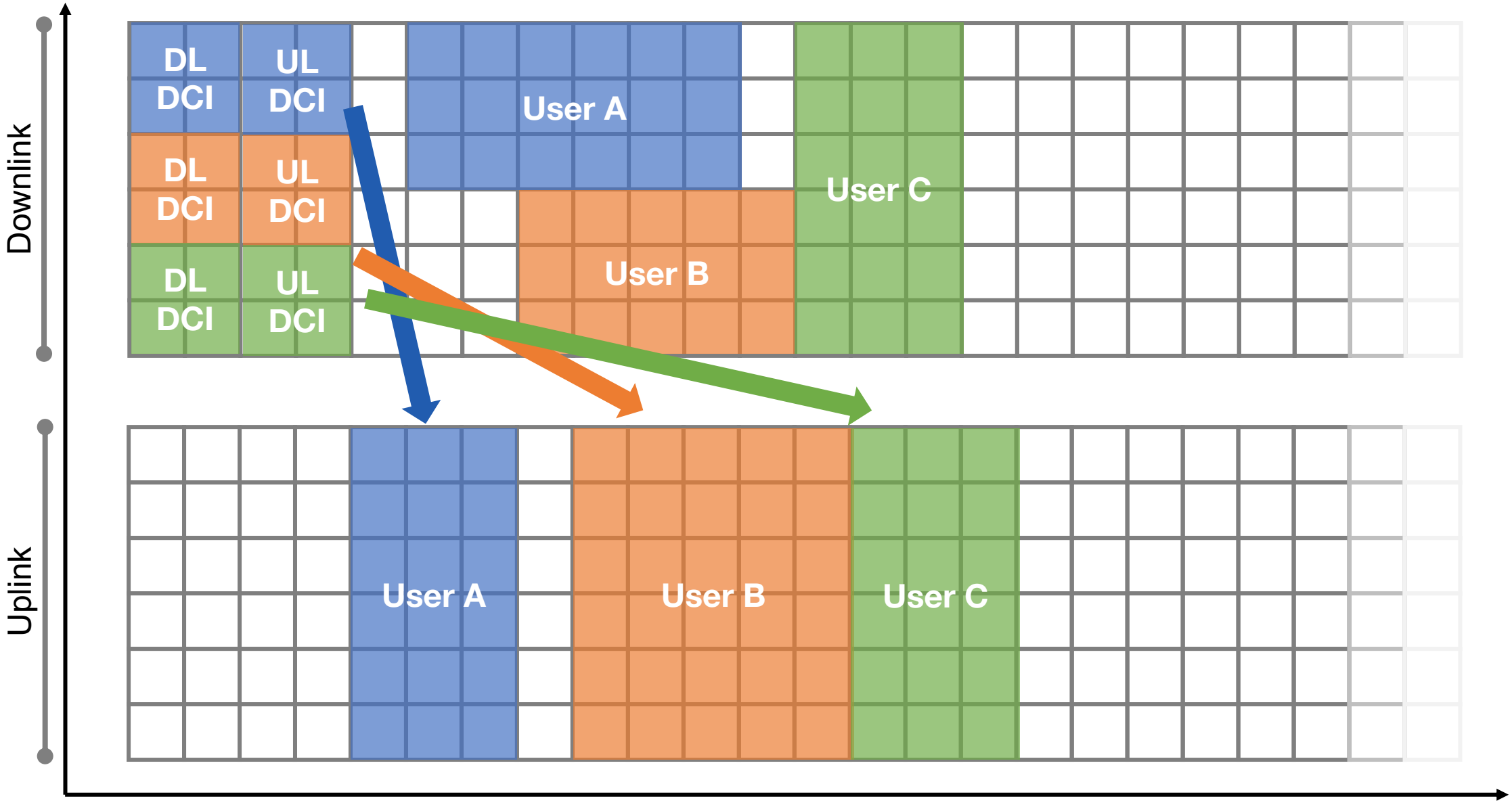
Background

Background ▪▪▪▪ Passive Localization ▪▪▪▪ Stealthy Identification

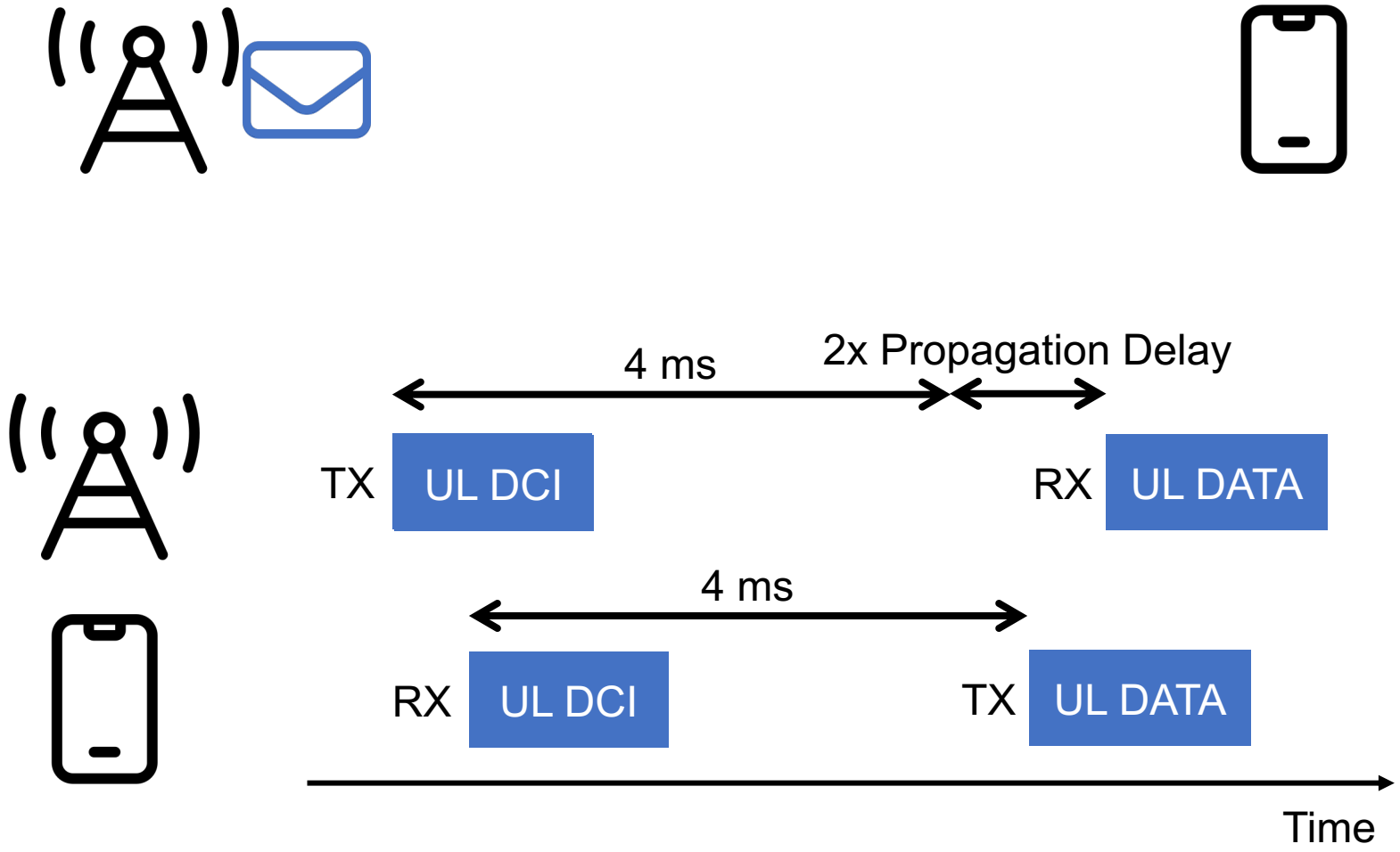
Physical Layer: Downlink



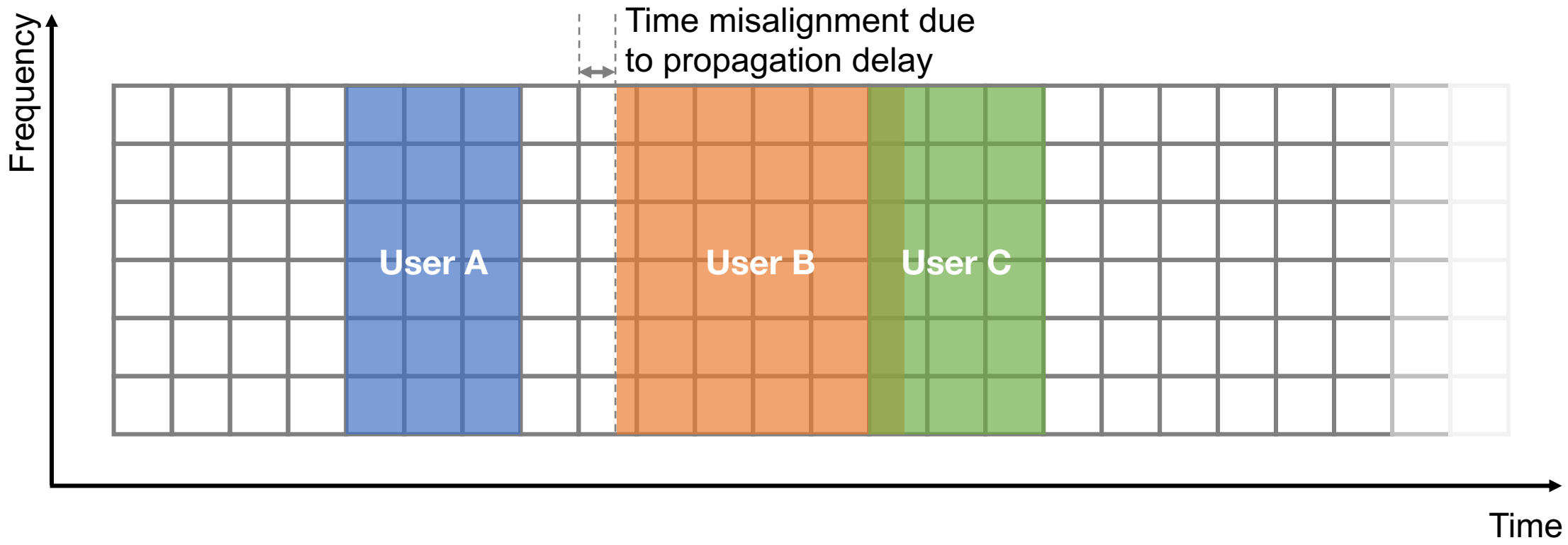
Physical Layer: Downlink & Uplink



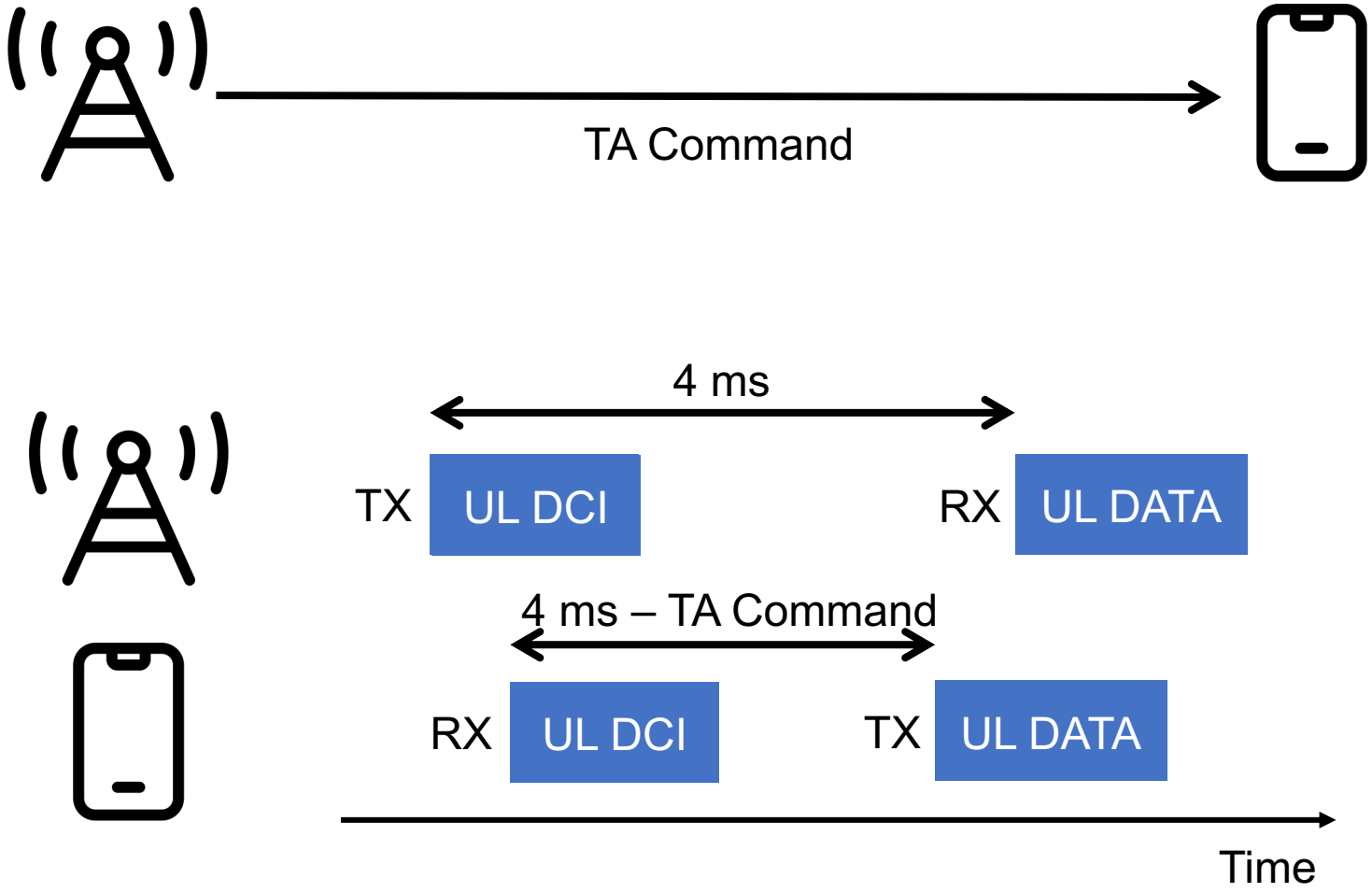
Unsynchronized Mobile Phones



Physical Layer: Uplink Time Alignment



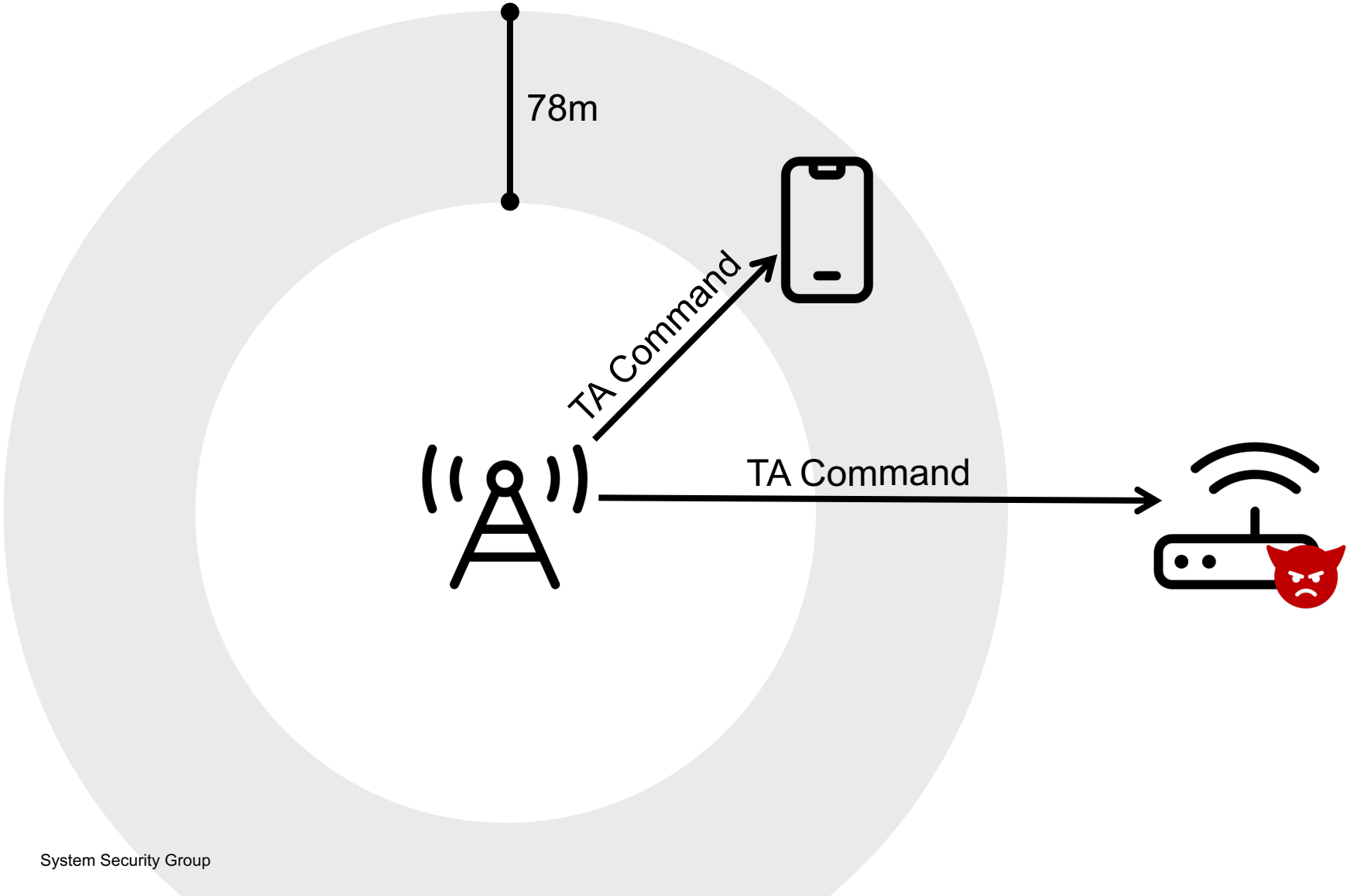
Unsynchronized Mobile Phones



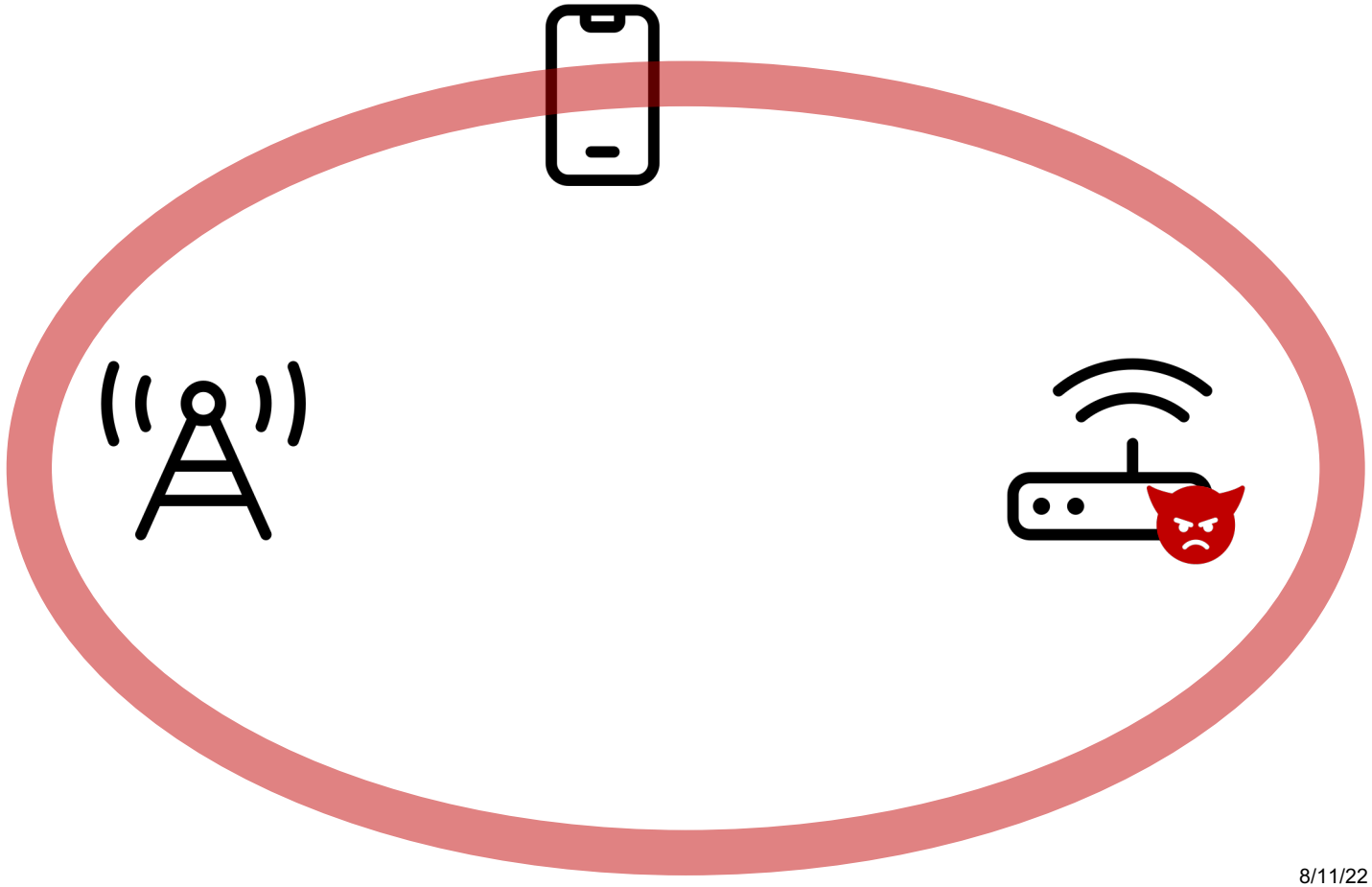
Passive Localization

Background ▪▪▪▪ Passive Localization ▪▪▪▪ Stealthy Identification

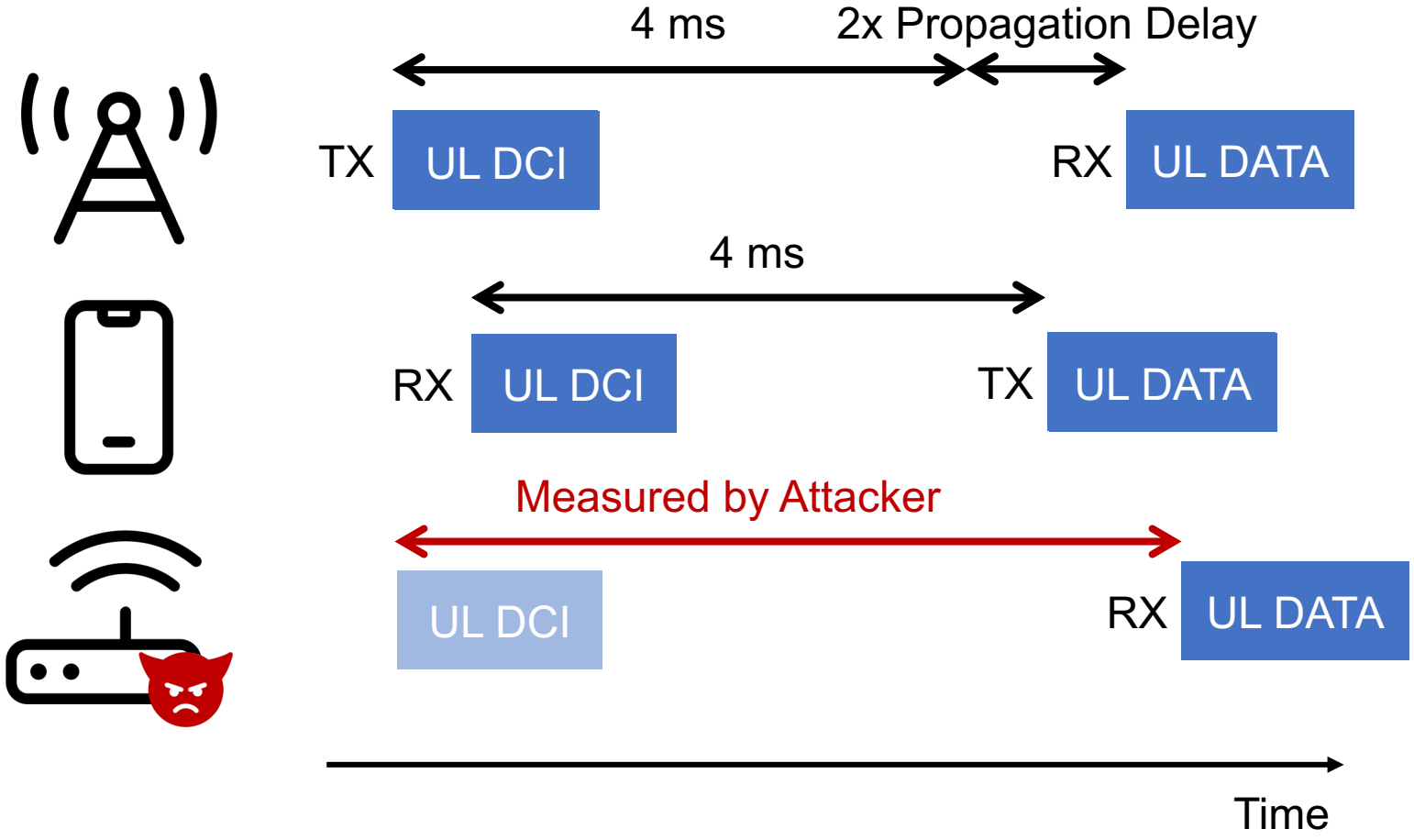
First Localization Constraint



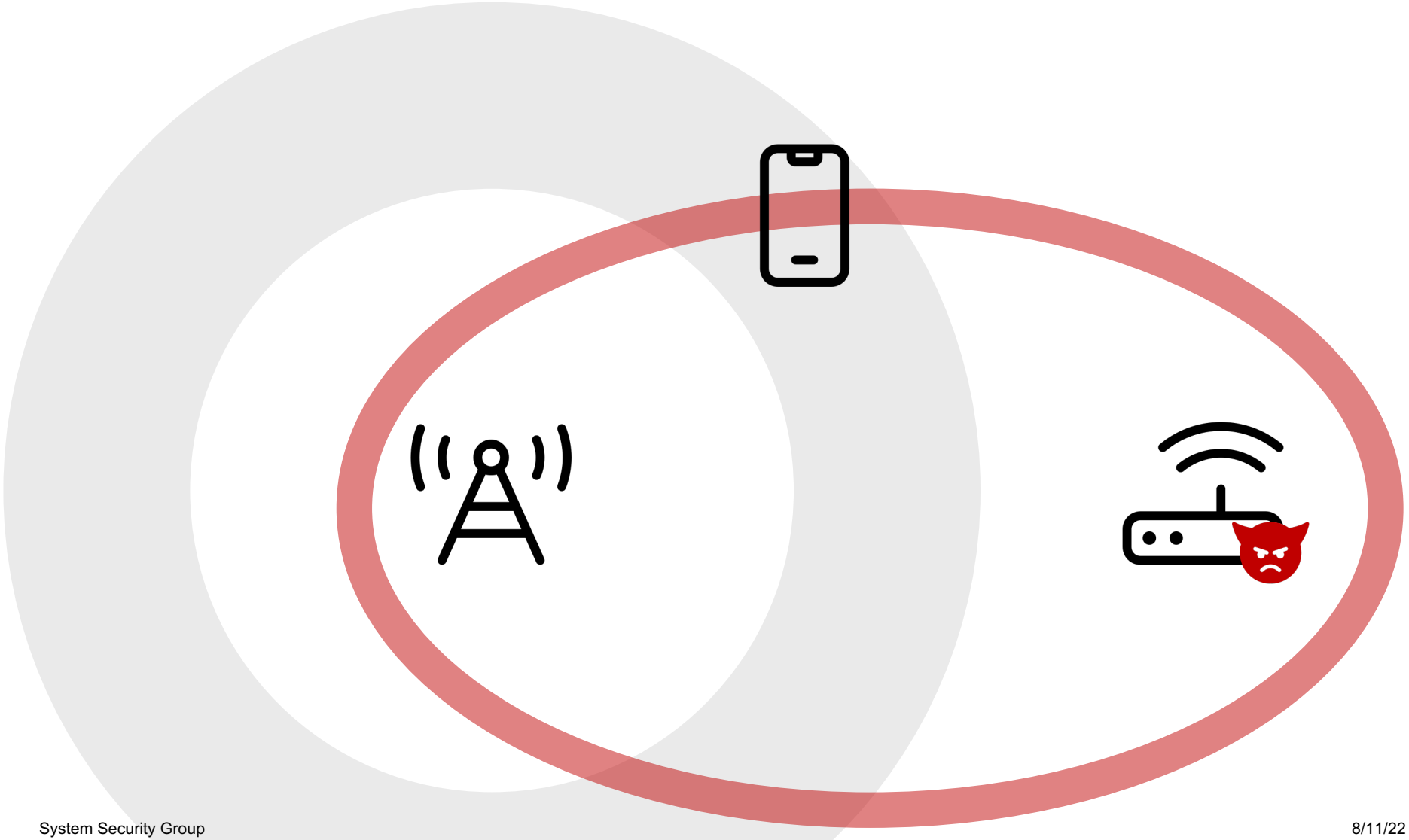
Second Localization Constraint



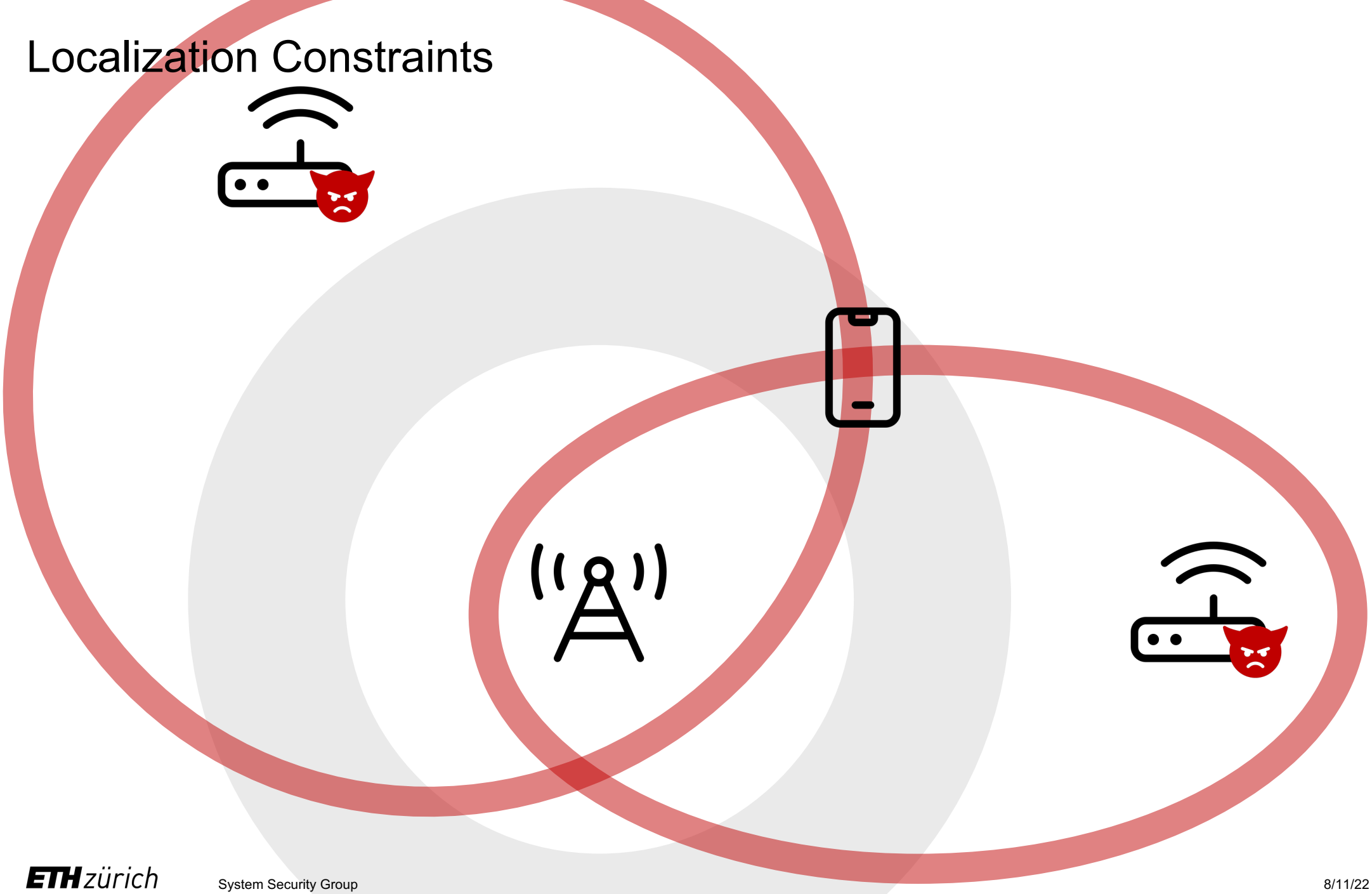
Second Localization Constraint



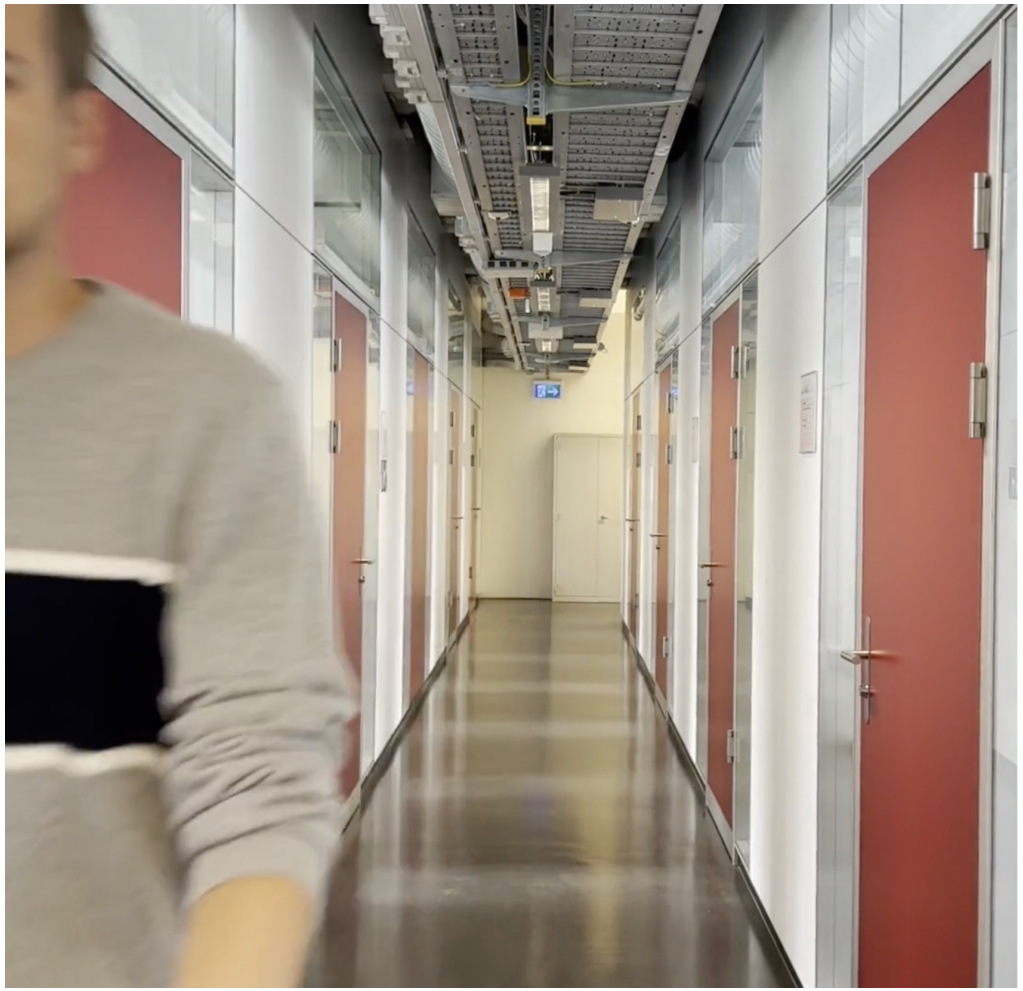
Localization Constraints

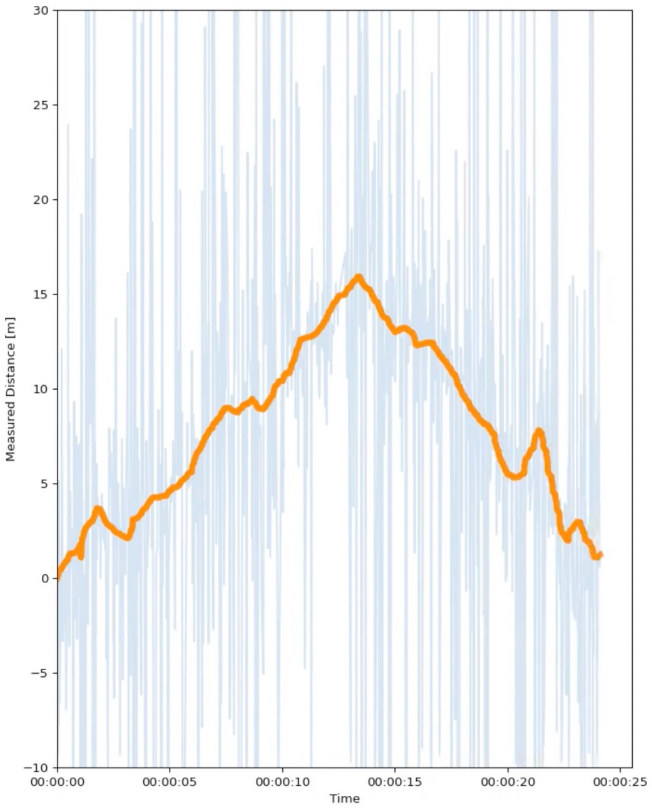


Localization Constraints

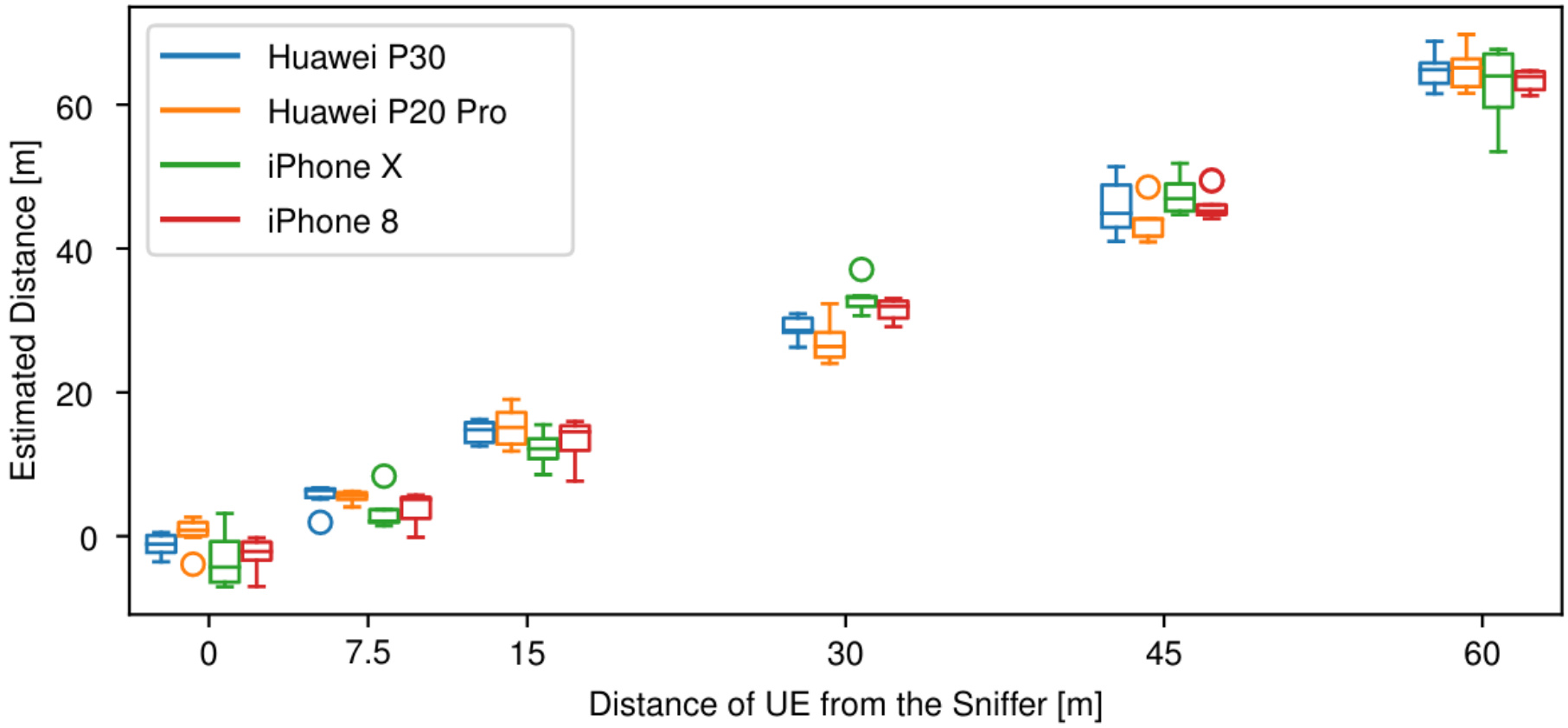


Distance Measurement in Action





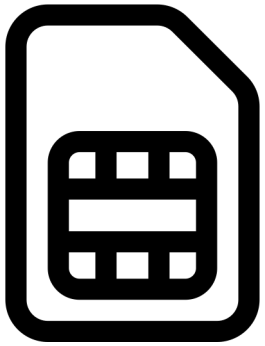
Distance Measurement Results



Stealthy Identification

Background ▪▪▪▪ Passive Localization ▪▪▪▪ Stealthy Identification

LTE Identities

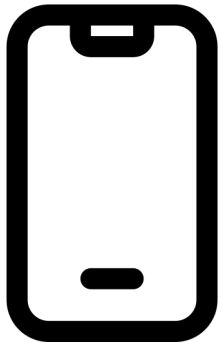


IMSI

Persistent Identifier

Hardcoded in the SIM card

Sent at the first connection attempt



TMSI

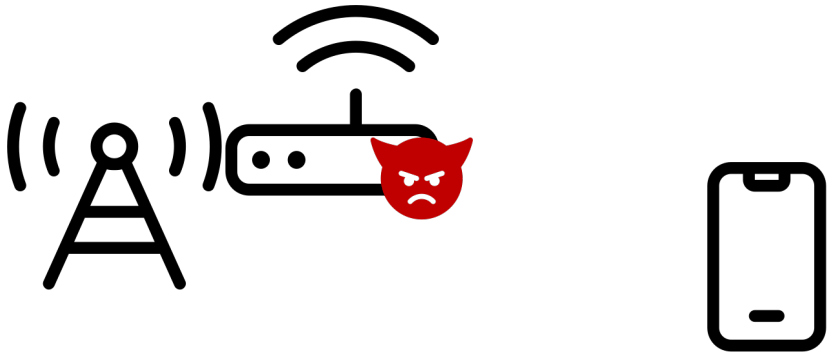
Temporary (Random) Identifier

Assigned by network, changes regularly

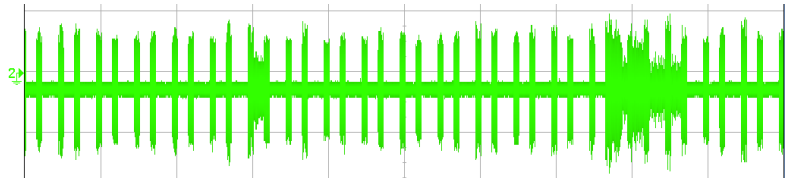
Sent at every connection attempt

Overshadowing vs Fake Base Stations

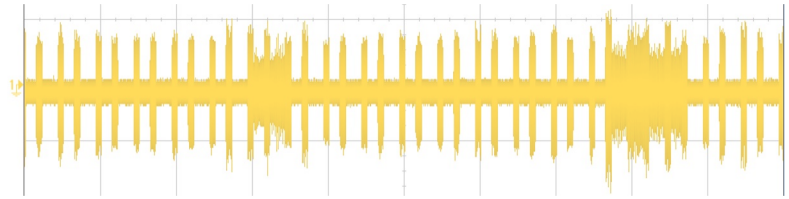
Fake Base Station



Overshadowing

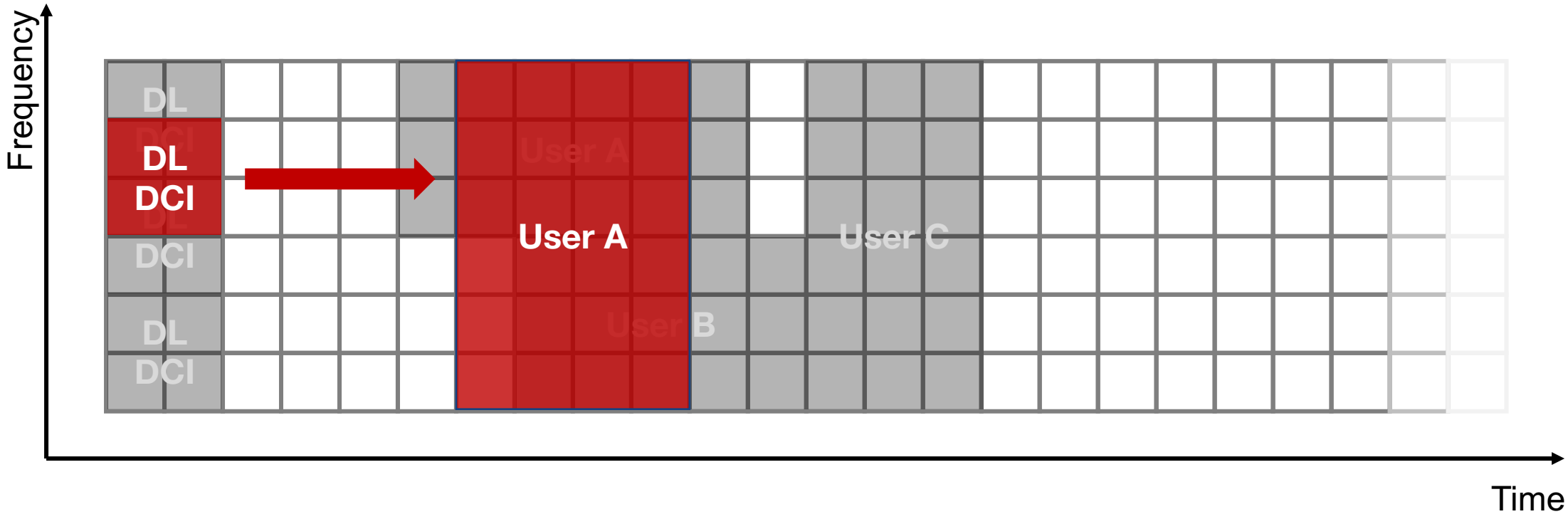


Original Signal

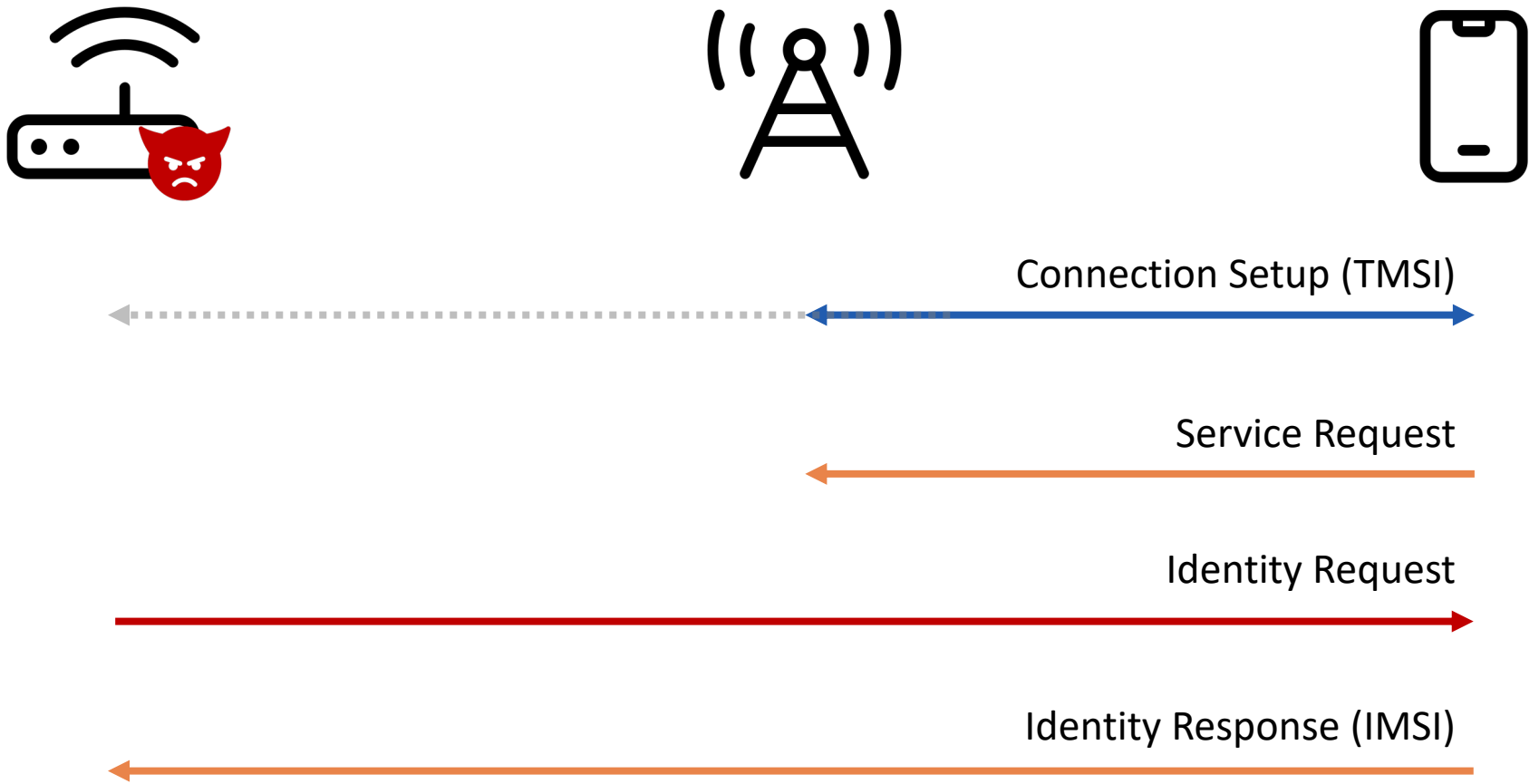


Attacker Signal (+ 1.8 dB)

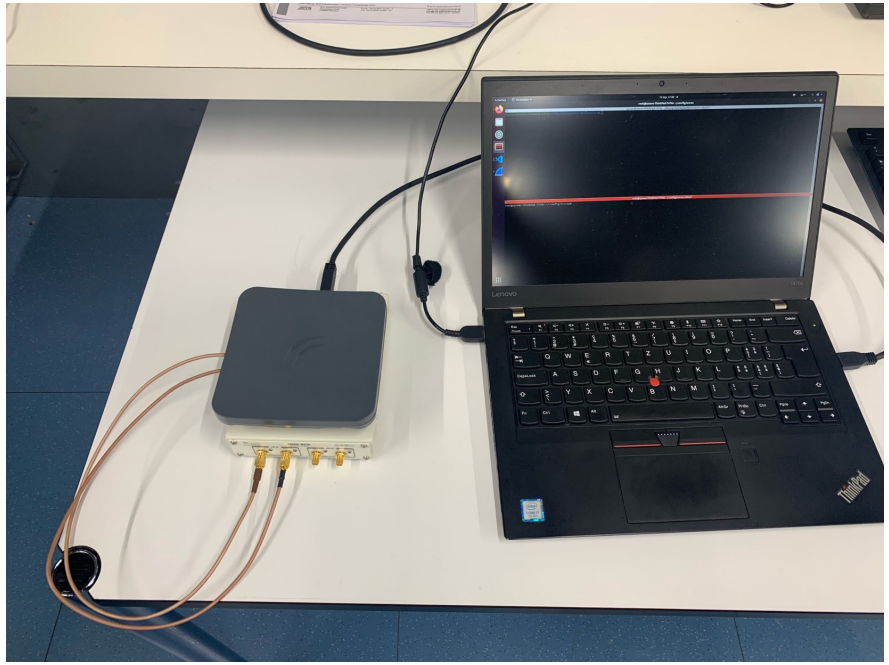
AdaptOver



IMSI Extractor



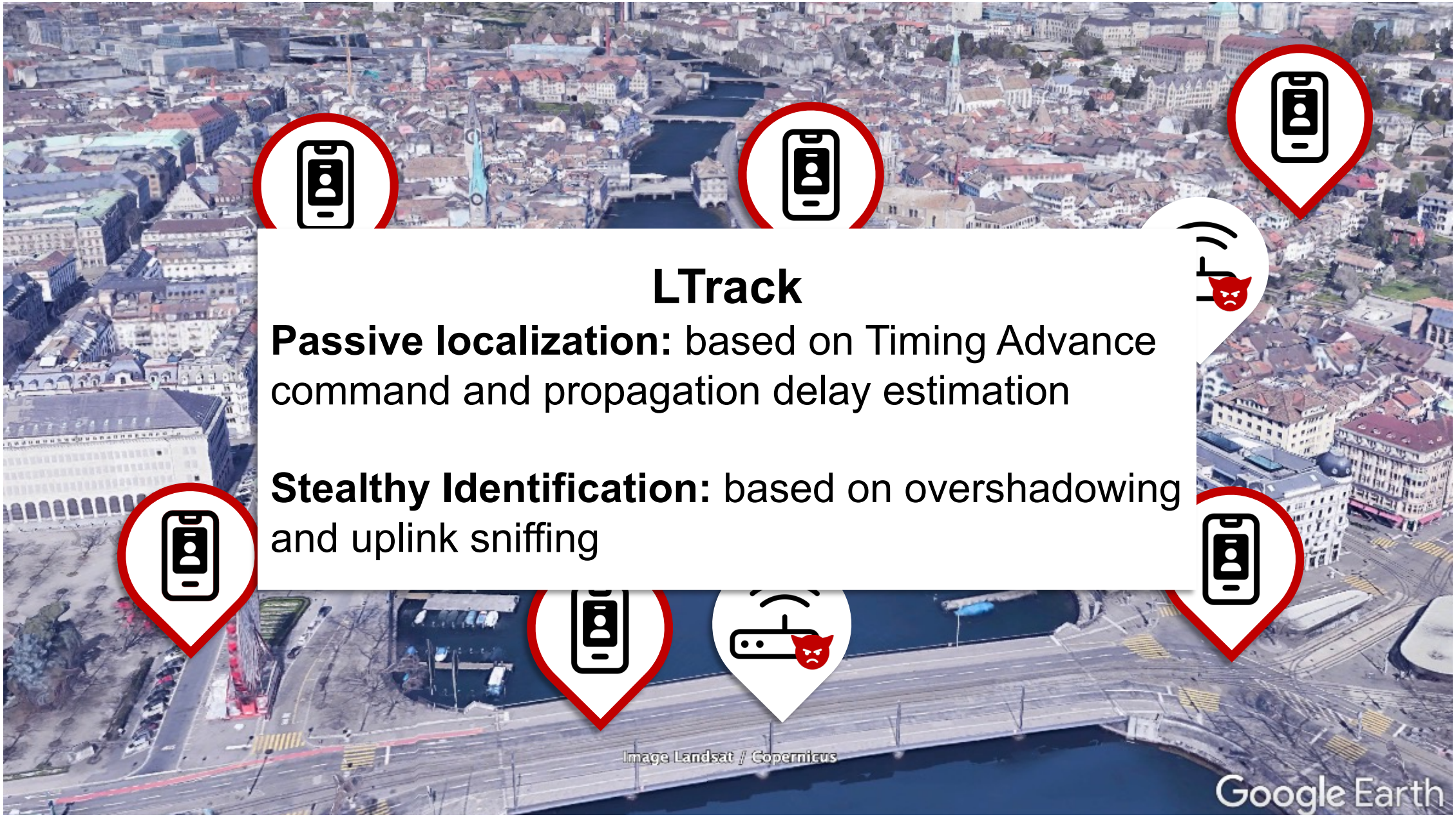
Evaluation



AdaptOver

LTEProbe

```
LTE RRC UL_DCCH/NAS-EPS          986 RRCConnectionSetupComplete, Service request
MAC-LTE                          986 UL-SCH: (SFN=812 , SF=8) UEId=0   (Long BSR) (Padding:remainder)
MAC-LTE                          986 UL-SCH: (SFN=813 , SF=8) UEId=0   (Long BSR) (Padding:remainder)
MAC-LTE                          986 UL-SCH: (SFN=814 , SF=8) UEId=0   (Long BSR) (Padding:remainder)
LTE RRC UL_DCCH/NAS-EPS          986  [UL] [AM] SRB:1  [CONTROL]  ACK_SN=1      ||   , ULInformationTransfer, Identity response
                                 .... .001 = Mobile Identity Type: IMSI (1)
                                 IMSI: 001010000004184
                               ▼ [Association IMSI: 001010000004184]
                                   Mobile Country Code (MCC): Unknown (1)
                                   Mobile Network Code (MNC): Unknown (010)
```


LTrack
Passive localization: based on Timing Advance command and propagation delay estimation
Stealthy Identification: based on overshadowing and uplink sniffing
Image Landsat / Copernicus
Google Earth

Thank You!
Questions?