Unpatched Design Vulnerabilities in Cellular Standards

Yongdae Kim

SysSec@KAIST

joint work with many of my students and collaborators

Cellular Security Publications (Selected)

- Location leaks on the GSM Air Interface, NDSS'12
- Gaining Control of Cellular Traffic Accounting by Spurious TCP Retransmission, NDSS' 14
- Breaking and Fixing VoLTE: Exploiting Hidden Data Channels and Mis-implementations, CCS'15
- When Cellular Networks Met IPv6: Security Problems of Middleboxes in IPv6 Cellular Networks, EuroS&P'17
- GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier, NDSS'18
- Peeking over the Cellular Walled Gardens: A Method for Closed Network Diagnosis, IEEE TMC’18
- Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane, S&P’19
- Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE, Usenix Sec’19
- Hidden Figures: Comparative Latency Analysis of Cellular Networks with Fine-grained State Machine Models, Hotmobile’19
- BASESPEC: Comparative Analysis of Baseband Software and Cellular Specifications for L3 Protocols, NDSS’21
- DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices, Usenix Sec’22
- Watching the Watchers: Practical Video Identification Attack in LTE Networks, Usenix Sec’22

Cellular Security: Why Difficult? Meta

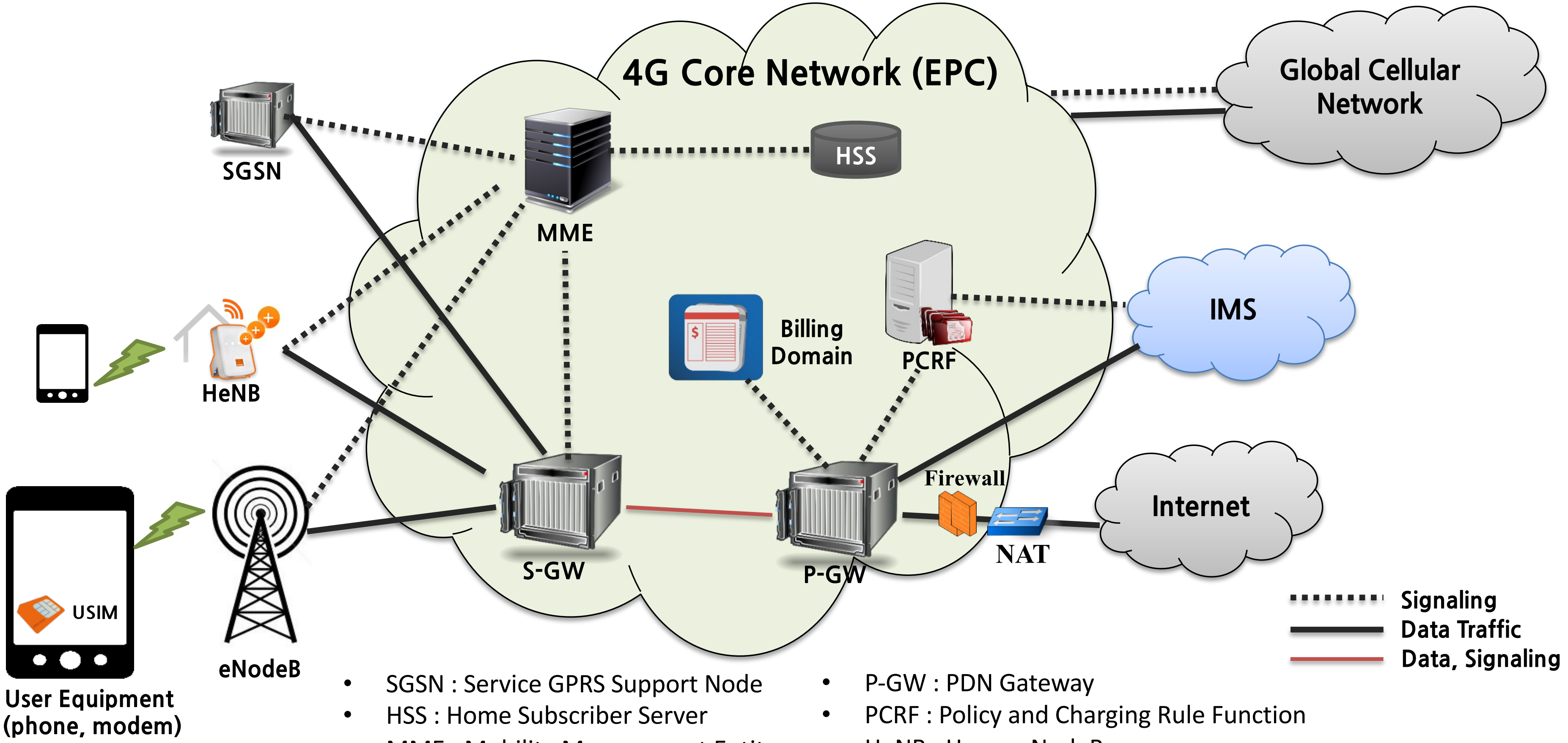
- New Generation (Technology) every 10 years
  - New Standards, Implementation, and Deployment ➔ New vulnerabilities
- Generation overlap: e.g. 3G, LTE and CSFB vulnerabilities in CSFB
- Backward compatibility: e.g. supporting 2G
- Government > Carrier > Device vendors > Customers ☺
- Walled Garden
  - Carriers and vendors don’t talk to each other.
  - Carriers: (Mostly) No response to responsible disclosure
- New HW/SW tools are needed for each generation.
  - Slow/imperfect open-source development (Thank you, SRS)
  - Still waiting for 5G SA radio (USRP was useful for LTE)

"Cellular Security: Why is it difficult?", A Keynote at AsiaCCS’22, https://youtu.be/I9bUWn_xu-E

Cellular Security: Why difficult? Standard

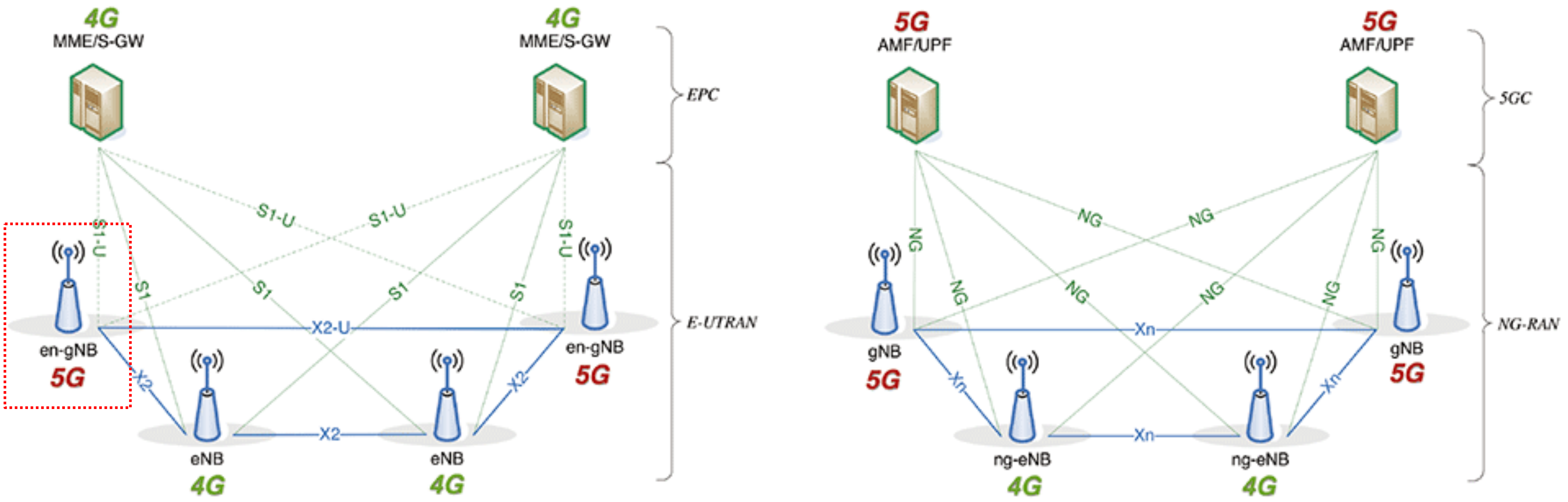
- Complicated and huge standards ➔ Hard to find bugs, need a large group
  - Multiple protocols co-work, but written in separate docs
- Quite a few unpatched design vulnerabilities
- Standards are written ambiguously
  - Misunderstanding by vendors and carriers
  - Spec ➔ State machine for formal analysis
- Leave many implementation details for vendors
- Cellular networks/devices could be different from each carrier and vendor
  - Therefore, vulnerabilities are different
- Conformance testing standard, but (almost) no security testing standard

4G LTE Cellular Network Overview



- SGSN : Service GPRS Support Node
- HSS : Home Subscriber Server
- MME : Mobility Management Entity
- S-GW : Serving Gateway
- P-GW : PDN Gateway
- PCRF : Policy and Charging Rule Function
- HeNB : Home eNodeB
- EPC : Evolved Packet Core

5G NSA vs. 5G SA



gNB (Next generation NodeB), eNB (Evolved Node B), MME (Mobility Management Entity), SPGW (Serving/Packet data network Gateway), HSS (Home Subscriber Server), IMS (IP Multimedia Subsystem)

Unpatched Cellular Vulnerabilities up to 5G

- From 2G to 5G, many security vulnerabilities are found and patched.
- Vulnerabilities
  - Design vulnerabilities: insecure design that requires specification update
  - Implementation vulnerabilities: typical software bugs + misimplementation due to misunderstanding specification

- We will talk about UNPATCHED CELLULAR DESIGN VULNERABILITIES.

The Roaming

Roaming service = Carriers trust carriers!

- SS7
  - Protocol suite used by most cellular operators throughout the world to talk to each other
  - When it was designed, there were only few operators
  - Closed and trusted, no authentication built in
- Getting an access to SS7 is easier than ever
  - Bought from operators or roaming hubs for a few hundred euros a month
  - Some operators are reselling roaming agreements
  - Unsecured equipment on the Internet
- Diameter for 4G LTE

SS7 Testing under GLR

MAP message	*Threat Category*	*Target*	*Prerequisites*
updateLocation	***DoS, Interception***	***All the subscriber***	***IMSI***
cancelLocation	*DoS*	*Roaming subscriber*	*IMSI*
purgeMS	*DoS*	*Roaming subscriber*	*IMSI*
insertSubscriberData *deleteSubscriberData*	*DoS*	*Roaming subscriber*	*IMSI and MSISDN*
restoreData	*Leak, DoS*	*Roaming subscriber*	*IMSI*
sendIMSI	*Leak*	*Roaming subscriber*	*MSISDN*
provideSubscriberInfo	*Tracking*	*Roaming subscriber*	*IMSI*

Unprotected Broadcast Channel

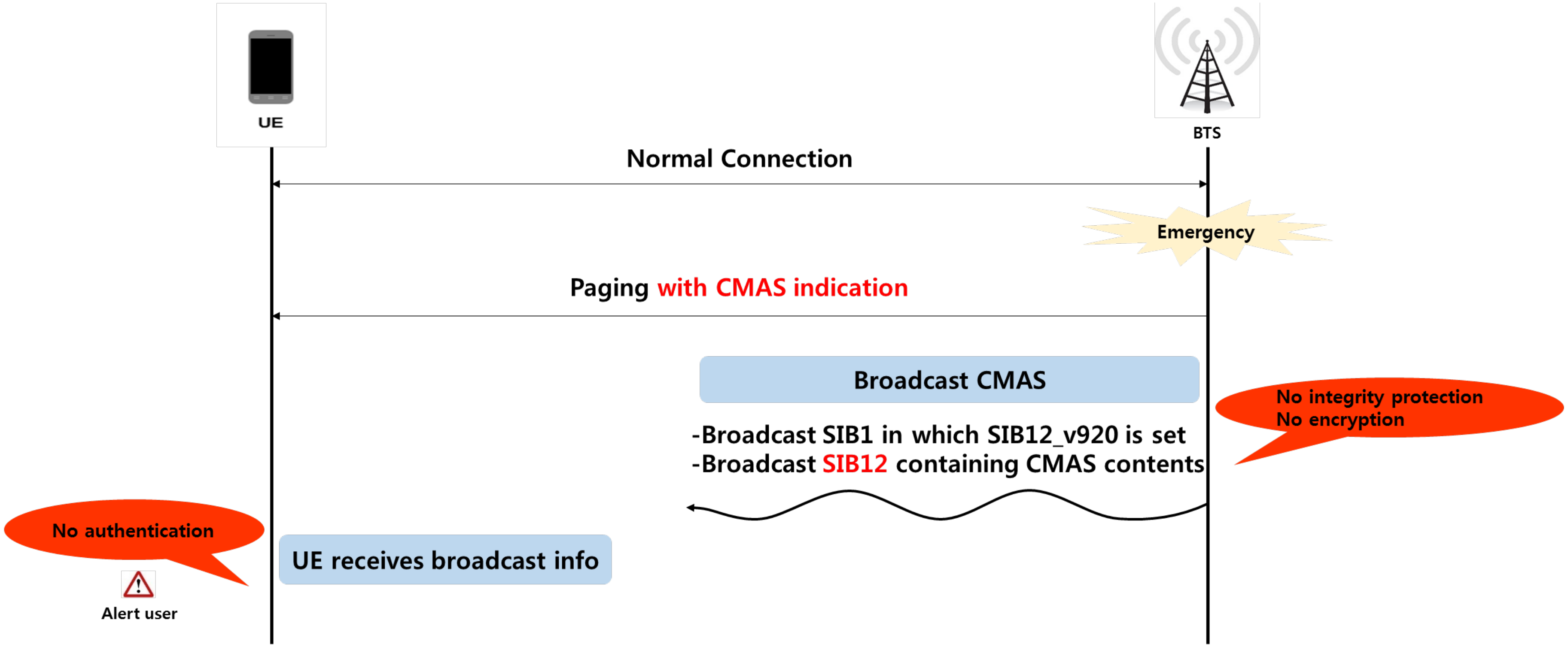
Unprotected Broadcast Channel

- eNB broadcasts System Information (SI) periodically
  - Master Information Block (MIB)
    - SIB scheduling information, most frequently used
  - System Information Block (SIB)
    - Various system info (e.g. information needed for UE’s cell selection)
    - Might include emergency alert
  - Paging Message
    - Tell Idle/Inactive UE about existing downlink data

- No authentication whatsoever

1. The confidentiality protection is recommended to be used.

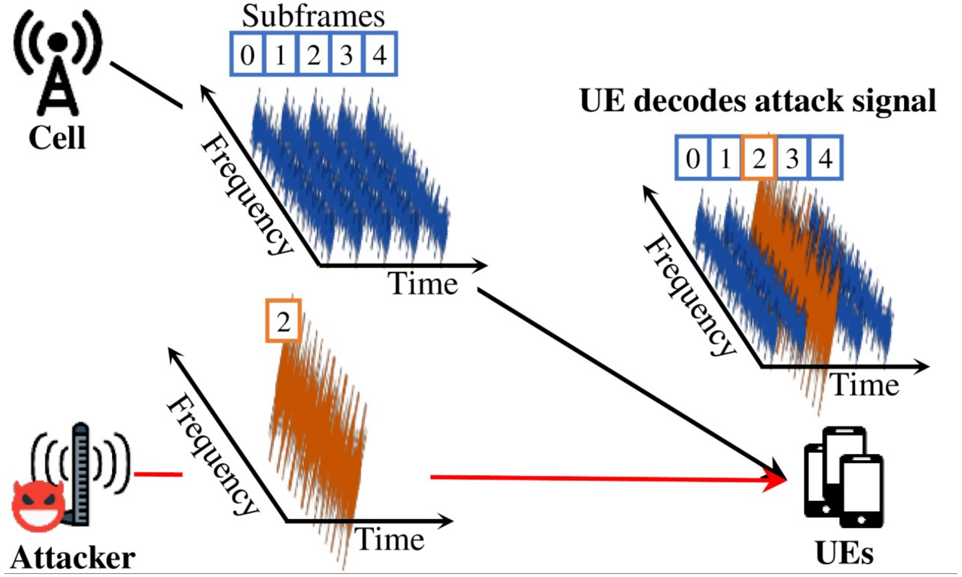
Vulnerabilities of CMAS broadcast messages

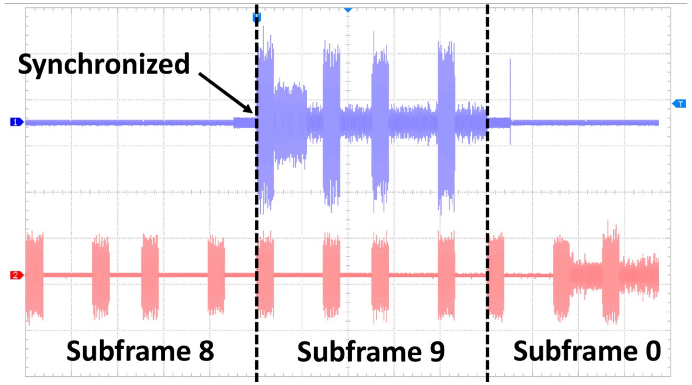

UE
BTS
Normal Connection
Emergency
Paging with CMAS indication
Broadcast CMAS
No integrity protection
No encryption
-Broadcast SIB1 in which SIB12_v920 is set
-Broadcast SIB12 containing CMAS contents
No authentication
UE receives broadcast info
Alert user

Fake CMAS broadcast attack

Signal Overshadowing: SigOver Attack

- ❖ Signal injection attack exploits broadcast messages in LTE
  - – Broadcast messages in LTE have never been integrity protected!
- ❖ Transmit time- and frequency-synchronized signal





Attack Efficiency (Power)

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

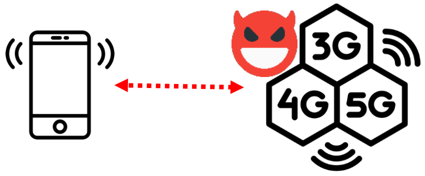
Relative Power (dB)	25	30	35	40	45
FBS attack	0%	0%	80%	100%	100%

FBS consumes x5000 more power
to achieve a comparable attack success rate

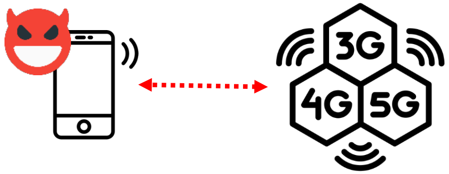
Demonstration of Signal Injection attack

DATA RESTRICTIONS

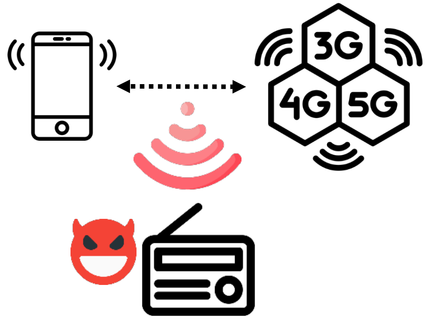
Threat Model



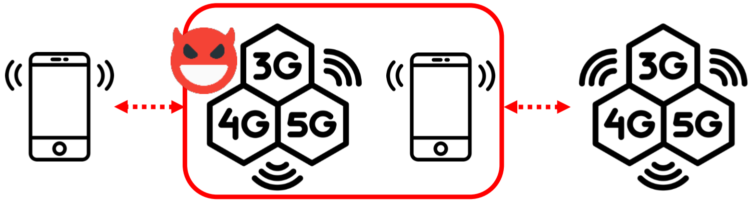
Fake base station



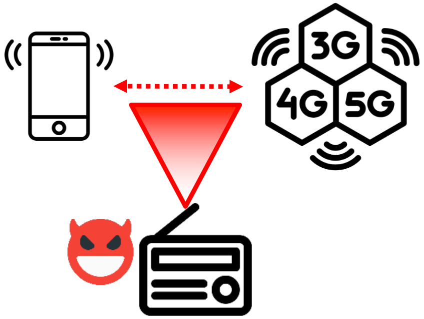
Fake UE



Sniffer



Man-in-the-Middle (MitM)



SigOver (Overshadowing)

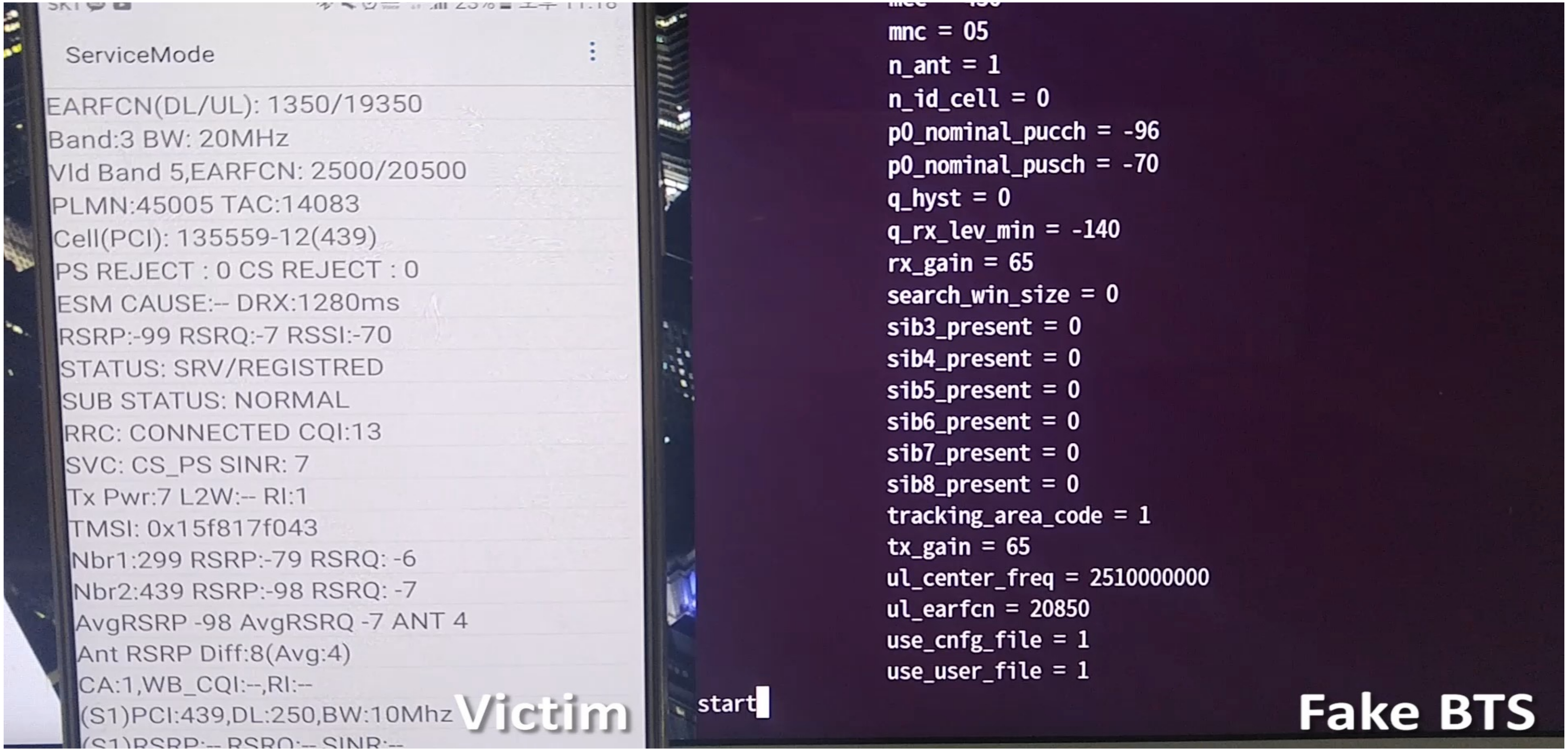
Unprotected Unicast Messages

Unprotected Unicast Messages

- Types
  - Pre-authentication messages: Attach/Identity/Authentication/TAU Request
  - Reject messages: Attach/TAU reject, Authentication failure

Test messages	Direction	Property 1-1	Property 1-2 (P)	Property 2-1 (I)	Property 2-2 (R)	Property 3	Affected component
NAS							
Attach request (IMSI/GUTI)	UL	B	DoS	DoS	DoS	-	Core network (MME)
Detach request (UE originating detach)	UL	-	DoS [1]	DoS	DoS	-	Core network (MME)
Service request	UL	-	-	B	Spoofing	-	Core network (MME)
Tracking area update request	UL	-	DoS	DoS	FLU and DoS	-	Core network (MME)
Uplink NAS transport	UL	-	SMS phishing and DoS	SMS phishing and DoS	SMS replay	-	Core network (MME)
PDN connectivity request	UL	B	B	DoS	DoS	-	Core network (MME)
PDN disconnect request	UL	-	B	DoS	selective DoS	-	Core network (MME)
Attach reject	DL	DoS [2]	DoS [3]	-	-	-	Baseband
Authentication reject	DL	DoS [4]	-	-	-	-	Baseband
Detach request (UE terminated detach)	DL	-	DoS [4]	-	-	-	Baseband
EMM information	DL	-	Spoofing [5]	-	-	-	Baseband
GUTI reallocation command	DL	-	B	B	ID Spoofing	-	Baseband
Identity request	DL	Info. leak [6]	B	B	Info. leak	-	Baseband
Security mode command	DL	-	B	B	Location tracking [4]	-	Baseband
Service reject	DL	-	DoS [3]	-	-	-	Baseband
Tracking area update reject	DL	-	DoS [3]	-	-	-	Baseband
RRC							
RRCConnectionRequest	UL	DoS and con. spoofing	-	-	-	-	Core network (eNB)
RRCConnectionSetupComplete	UL	Con. spoofing	-	-	-	-	Core network (eNB)
MasterInformationBlock	DL	Spoofing	-	-	-	-	Baseband
Paging	DL	DoS [4] and Spoofing	-	-	-	-	Baseband
RRCConnectionReconfiguration	DL	-	MitM	DoS	B	-	Baseband
RRCConnectionReestablishment	DL	-	Con. spoofing	-	-	-	Baseband
RRCConnectionReestablishmentReject	DL		DoS			-	Baseband
RRCConnectionReject	DL	DoS	-	-	-	-	Baseband
RRCConnectionRelease	DL	DoS [2]	-	-	-	-	Baseband
RRCConnectionSetup	DL	Con. spoofing	-	-	-	-	Baseband
SecurityModeCommand	DL	-	B	B	B	MitM	Baseband
SystemInformationBlockType1	DL	Spoofing [4]	-	-	-	-	Baseband
SystemInformationBlockType 10/11	DL	Spoofing [4]	-	-	-	-	Baseband
SystemInformationBlockType12	DL	Spoofing [4]	-	-	-	-	Baseband
UECapabilityEnquiry	DL	Info. leak	-	Info. leak	Info. leak	-	Baseband

DoS using FBS



ServiceMode

```
EARFCN(DL/UL): 1350/19350
Band:3 BW: 20MHz
Vld Band 5,EARFCN: 2500/20500
PLMN:45005 TAC:14083
Cell(PCI): 135559-12(439)
PS REJECT : 0 CS REJECT : 0
ESM CAUSE:-- DRX:1280ms
RSRP:-99 RSRQ:-7 RSSI:-70
STATUS: SRV/REGISTRED
SUB STATUS: NORMAL
RRC: CONNECTED CQI:13
SVC: CS_PS SINR: 7
Tx Pwr:7 L2W:-- RI:1
TMSI: 0x15f817f043
Nbr1:299 RSRP:-79 RSRQ: -6
Nbr2:439 RSRP:-98 RSRQ: -7
AvgRSRP -98 AvgRSRQ -7 ANT 4
Ant RSRP Diff:8(Avg:4)
CA:1,WB_CQI:--,RI:--
(S1)PCI:439,DL:250,BW:10Mhz
(S1)RSRP:-- RSRQ:-- SINR:--
```

```
mcc = 450
mnc = 05
n_ant = 1
n_id_cell = 0
p0_nominal_pucch = -96
p0_nominal_pusch = -70
q_hyst = 0
q_rx_lev_min = -140
rx_gain = 65
search_win_size = 0
sib3_present = 0
sib4_present = 0
sib5_present = 0
sib6_present = 0
sib7_present = 0
sib8_present = 0
tracking_area_code = 1
tx_gain = 65
ul_center_freq = 2510000000
ul_earfcn = 20850
use_cnfg_file = 1
use_user_file = 1
start
```

Unprotected Control Channel

Unprotected Control Channel

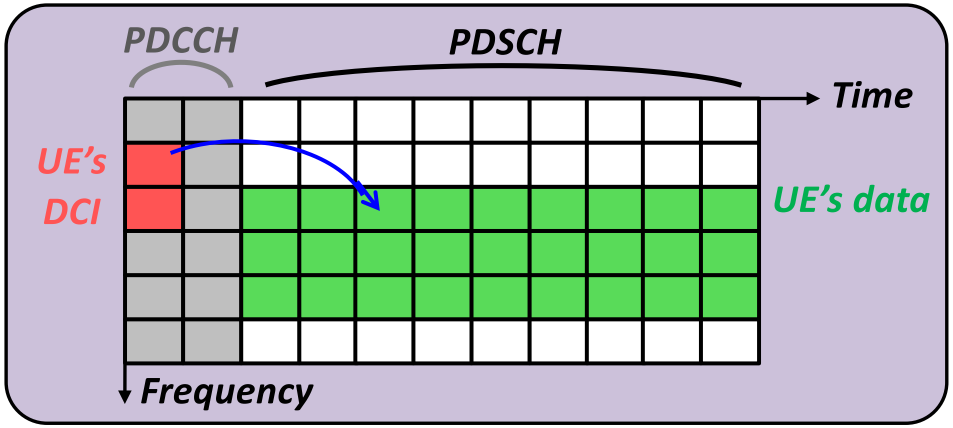
- Downlink Control Information (DCI)
  - Requested resource by the UE
  - Scheduling information of a UE

- MAC Control Element
  - Carrier Aggregation (CA) Information
  - # of Secondary Cell

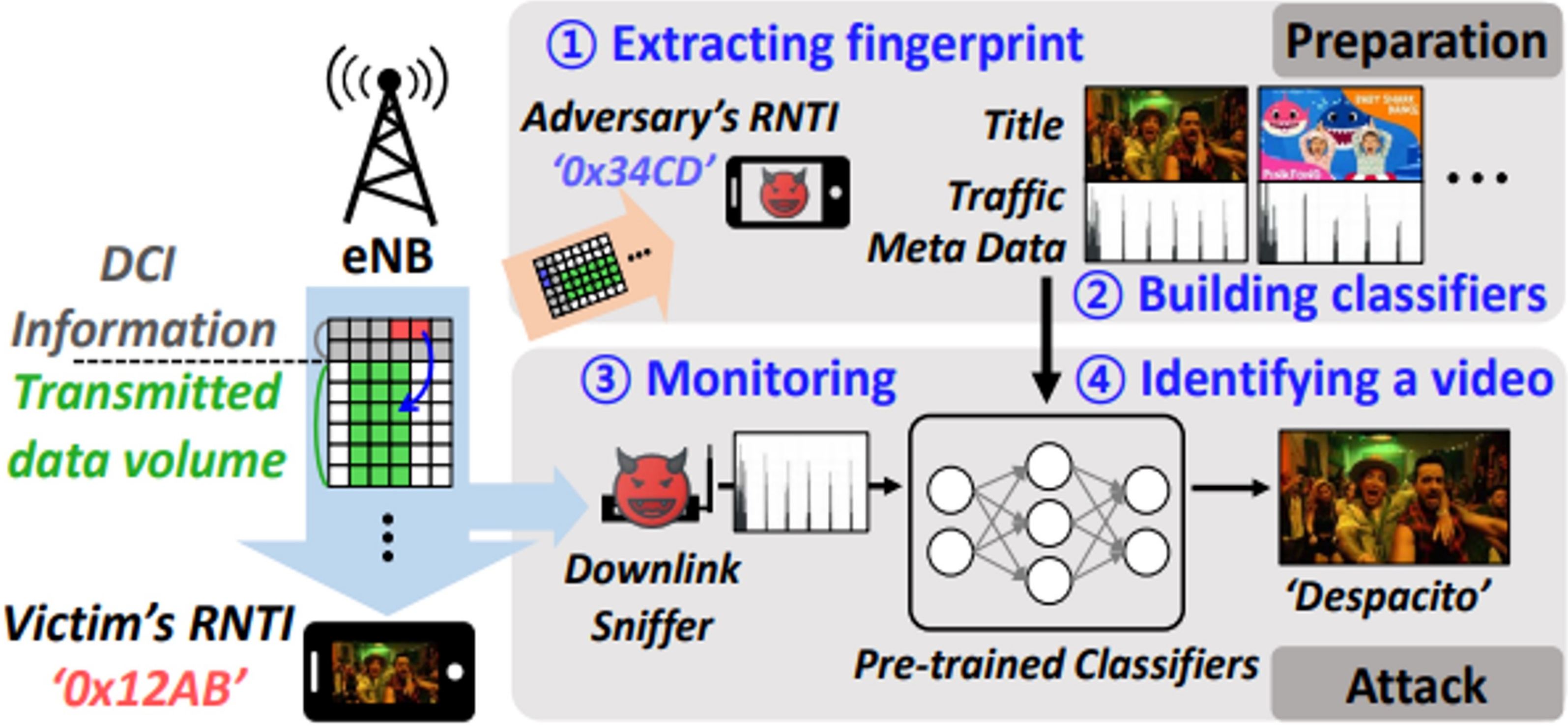
Downlink Data Transmission Information is Leaked

- eNB (base station) controls DL data transmission by broadcasting DCI
- Downlink Control Indicator (DCI)
  - Descriptions about DL data transmitted to the UE
    - Data volume, modulation scheme, allocated resource blocks (RB)
  - Distinguished by RNTI

This information is broadcast in plain text



Video Identification



Watching the Watchers: Practical Video Identification Attack in LTE Networks, Bae, Son, Kim, Park, Lee, Son, Kim, Usenix Sec'22

LTrack

- ❖ LTrack: Stealthy Tracking of Mobile Phones in LTE, Martin Kotuliak, Simon Erni, Patrick Leu, Marc Röschlin, and Srdjan Čapkun, Usenix Security'22
  - Passive localization: based on Timing Advance command and propagation delay estimation
  - Stealthy Identification: based on overshadowing and uplink sniffing
  - https://www.usenix.org/conference/usenixsecurity22/presentation/kotuliak

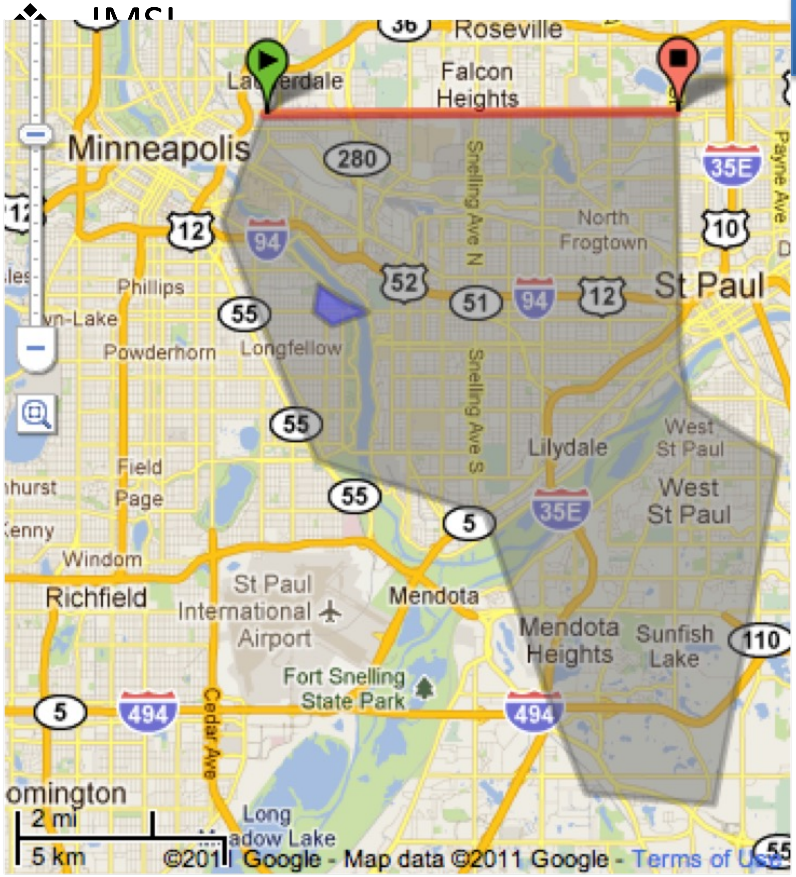
Linkable Identities

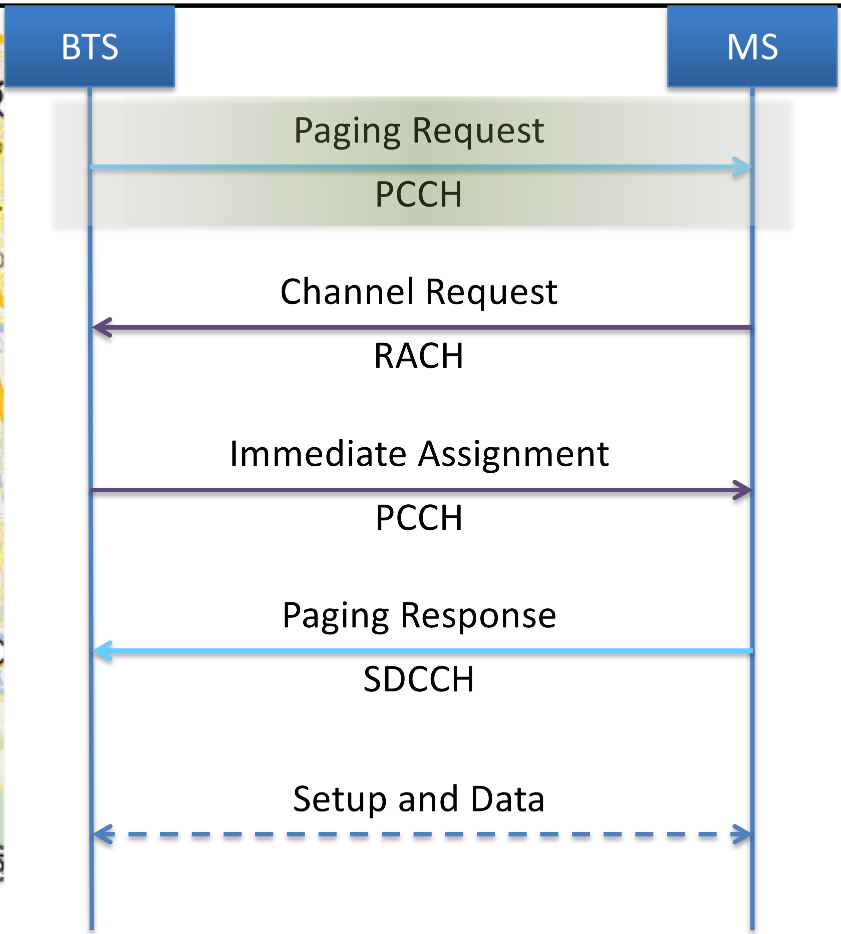
Location Privacy Leaks on GSM

- We have the victim’s mobile phone number
- Can we detect if the victim is in/out of an area of interest?
  - Granularity? 100 km^2? 1km^2? Next door?
- No collaboration from service provider
  - i.e. How much information leaks from the HLR over broadcast messages?
- Attacks by passively listening
  - Paging channel
  - Random access channel

Location Privacy Leaks on GSM

- IMSI




BTS

MS

Paging Request

PCCH

Channel Request

RACH

Immediate Assignment

PCCH

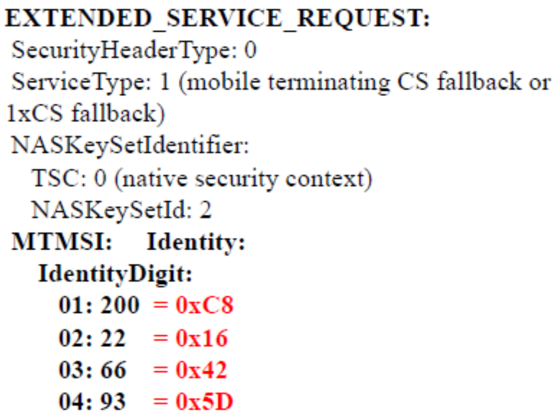
Paging Response

SDCCH

Setup and Data

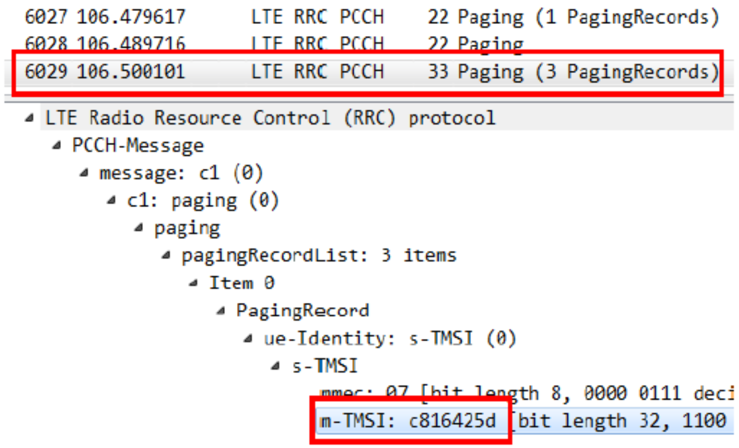
Location Tracking with GUTI

- Continue calling the target
  - Using “silent call” method: hang up before the phone rings
- Observation of broadcast channels after call invocation
  - Pattern matching (fixed bytes, assigning same GUTI)
  - Location tracking (Tracking Area, Cell)



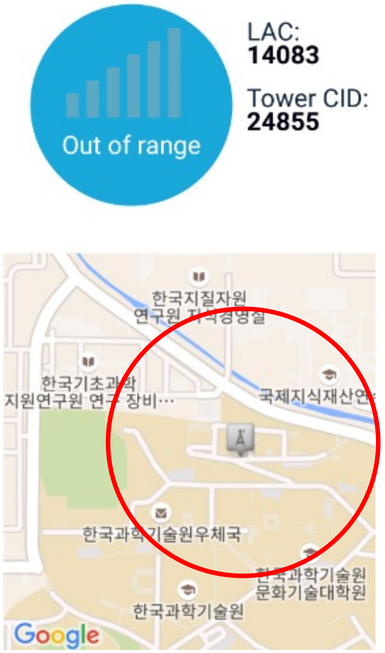
```
EXTENDED_SERVICE_REQUEST:
 SecurityHeaderType: 0
 ServiceType: 1 (mobile terminating CS fallback or
1xCS fallback)
 NASKeySetIdentifier:
   TSC: 0 (native security context)
   NASKeySetId: 2
 MTMSI:    Identity:
   IdentityDigit:
     01: 200  = 0xC8
     02: 22   = 0x16
     03: 66   = 0x42
     04: 93   = 0x5D
```

(a) M-TMSI monitored by Device



```
6027 106.479617      LTE RRC PCCH     22 Paging (1 PagingRecords)
6028 106.489716      LTE RRC PCCH     22 Paging
6029 106.500101      LTE RRC PCCH     33 Paging (3 PagingRecords)
◢ LTE Radio Resource Control (RRC) protocol
  ◢ PCCH-Message
    ◢ message: c1 (0)
      ◢ c1: paging (0)
        ◢ paging
          ◢ pagingRecordList: 3 items
            ◢ Item 0
              ◢ PagingRecord
                ◢ ue-Identity: s-TMSI (0)
                  ◢ s-TMSI
                      mmec: 07 [bit length 8, 0000 0111 deci
                      m-TMSI: c816425d [bit length 32, 1100
```

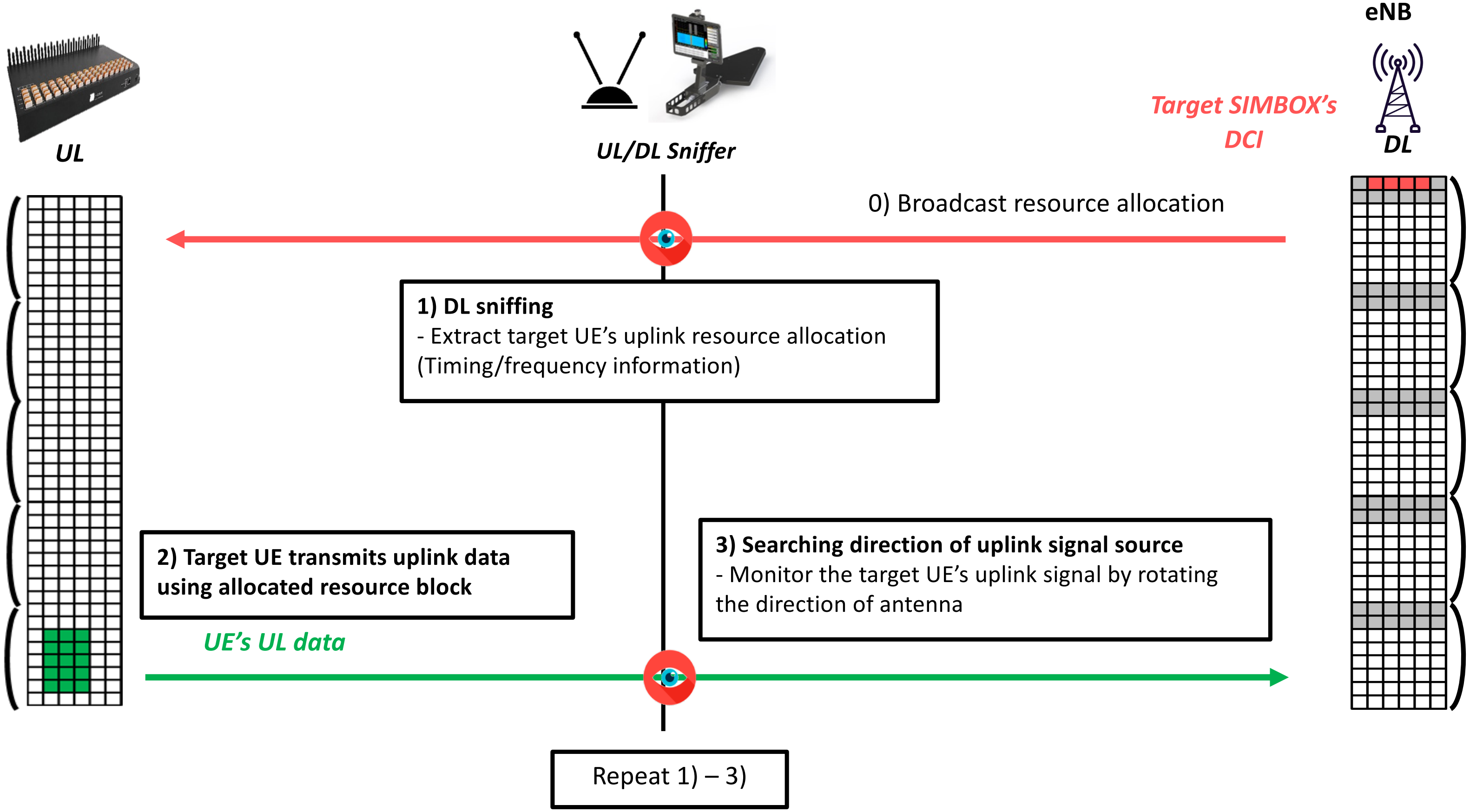
(b) Paging Message in Broadcast Channel (USRP)



OpenSignal

GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier, Hong, Bae, Kim, NDSS’18

Localization



0) Broadcast resource allocation

1) DL sniffing
- Extract target UE's uplink resource allocation (Timing/frequency information)

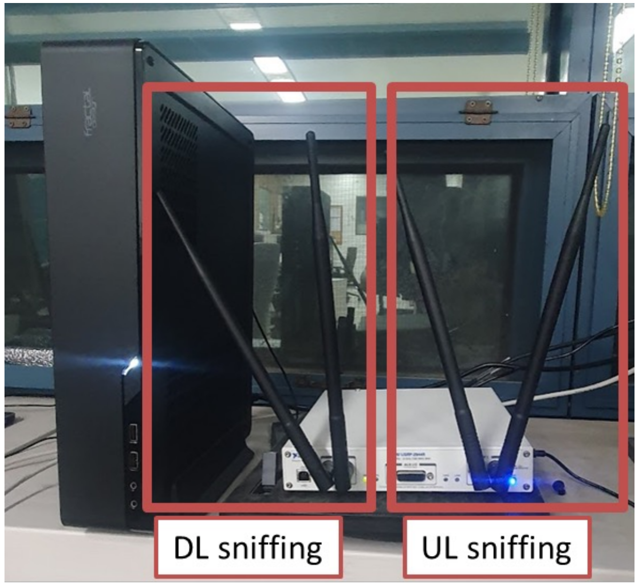
2) Target UE transmits uplink data using allocated resource block

3) Searching direction of uplink signal source
- Monitor the target UE's uplink signal by rotating the direction of antenna

Repeat 1) – 3)

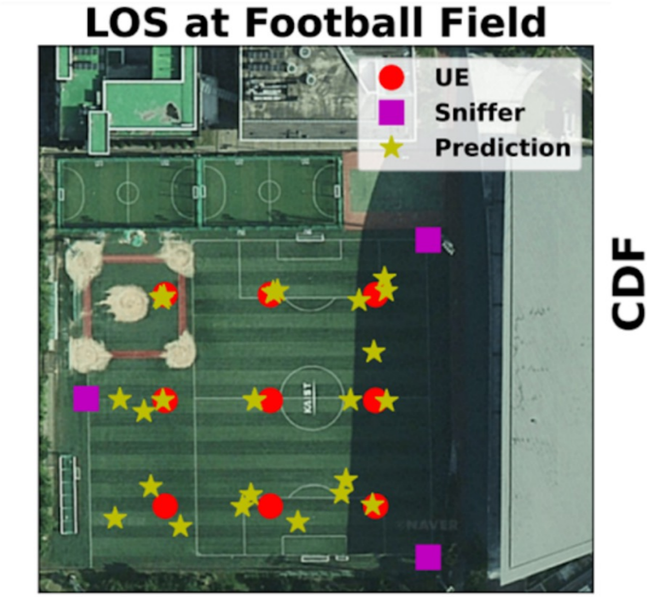
Implementation

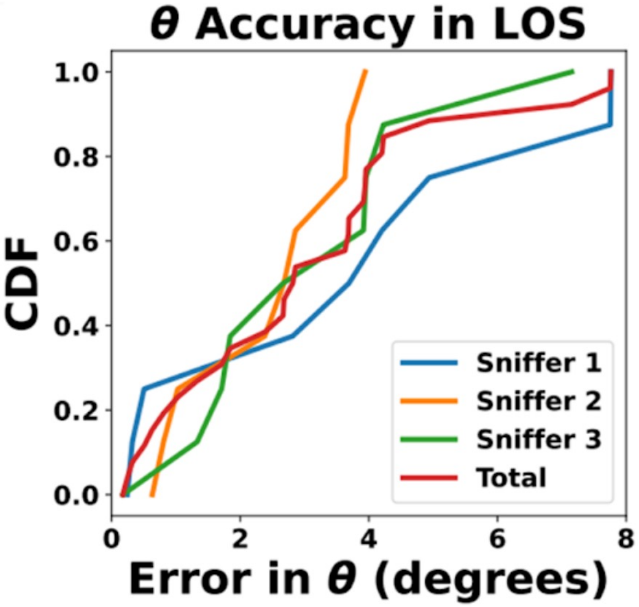
- UL Sniffer
  - Operate with Single USRP X310
    - Capture uplink/downlink signal simultaneously
      - Octoclock is not needed
    - Sync with DL signal from eNB
  - Operate in real time
    - Modify/Add ~1K LoC of C++ FALCON (open-source DL sniffer)
      - Match with monitored UL
      - Compute signal strength
    - Optimize to UL resource allocation extraction

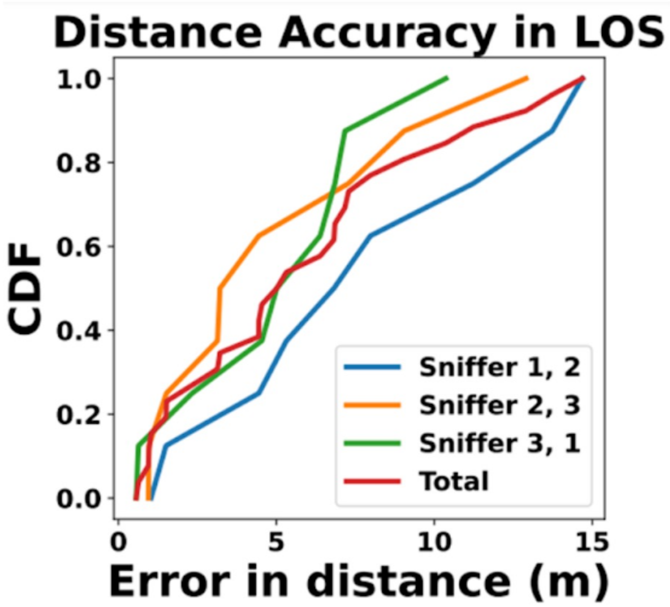


- RF frontend
  - Directional antenna (Various gain/beam width)

LoS Experiment


LOS at Football Field


θ Accuracy in LOS

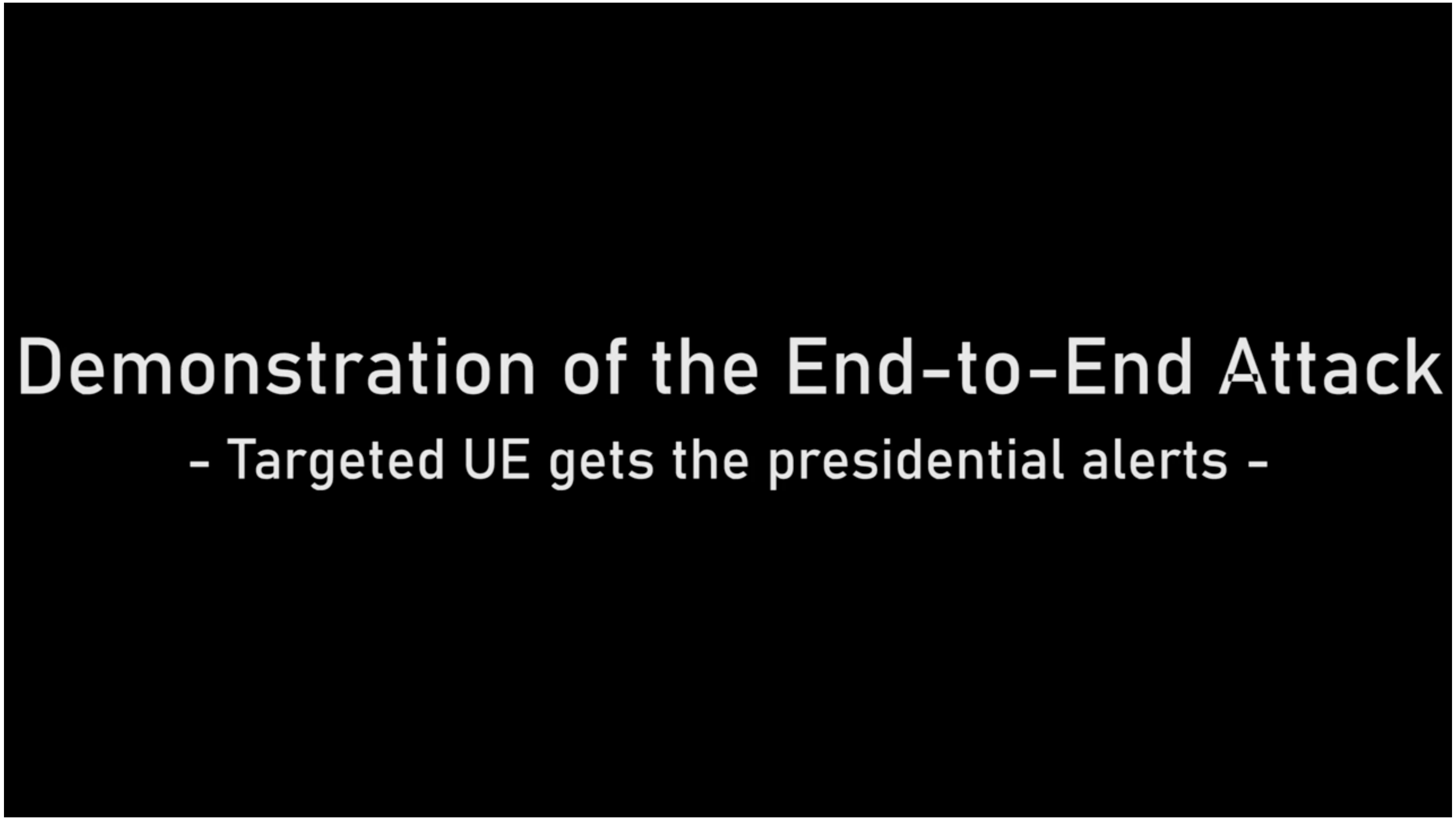

Distance Accuracy in LOS

Etc.

Etc.

- Still symmetric key-based key management
- Lawful interception
  - Voice call/SMS, location tracking
- eSIM vs. Physical SIM
  - SIMswap vs. SIMClone
- IMEI Spoofing

Unencrypted DCI + Unprotected Unicast



Demonstration of the End-to-End Attack

- Targeted UE gets the presidential alerts -

Conclusion

Lots of unprotected and insecure design issues unpatched for a long time

maybe because

1. Backward compatibility: e.g. supporting 2G
2. Government > Carrier > Device vendors > Customers

Hopefully, they are patched in 6G.

Questions?

- ❖ Yongdae Kim
  - email: yongdaek@kaist.ac.kr
  - Home: http://syssec.kaist.ac.kr/~yongdaek
  - Facebook: https://www.facebook.com/y0ngdaek
  - Twitter: https://twitter.com/yongdaek
  - Google “Yongdae Kim”

Ministry of Science and ICT IITP Institute of Information & Communications Technology Planning & Evaluation 경찰청 KOREAN NATIONAL POLICE AGENCY SAMSUNG