GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier

B. Hong, S. Bae, and Y. Kim

NDSS 2018

Present by Tuan

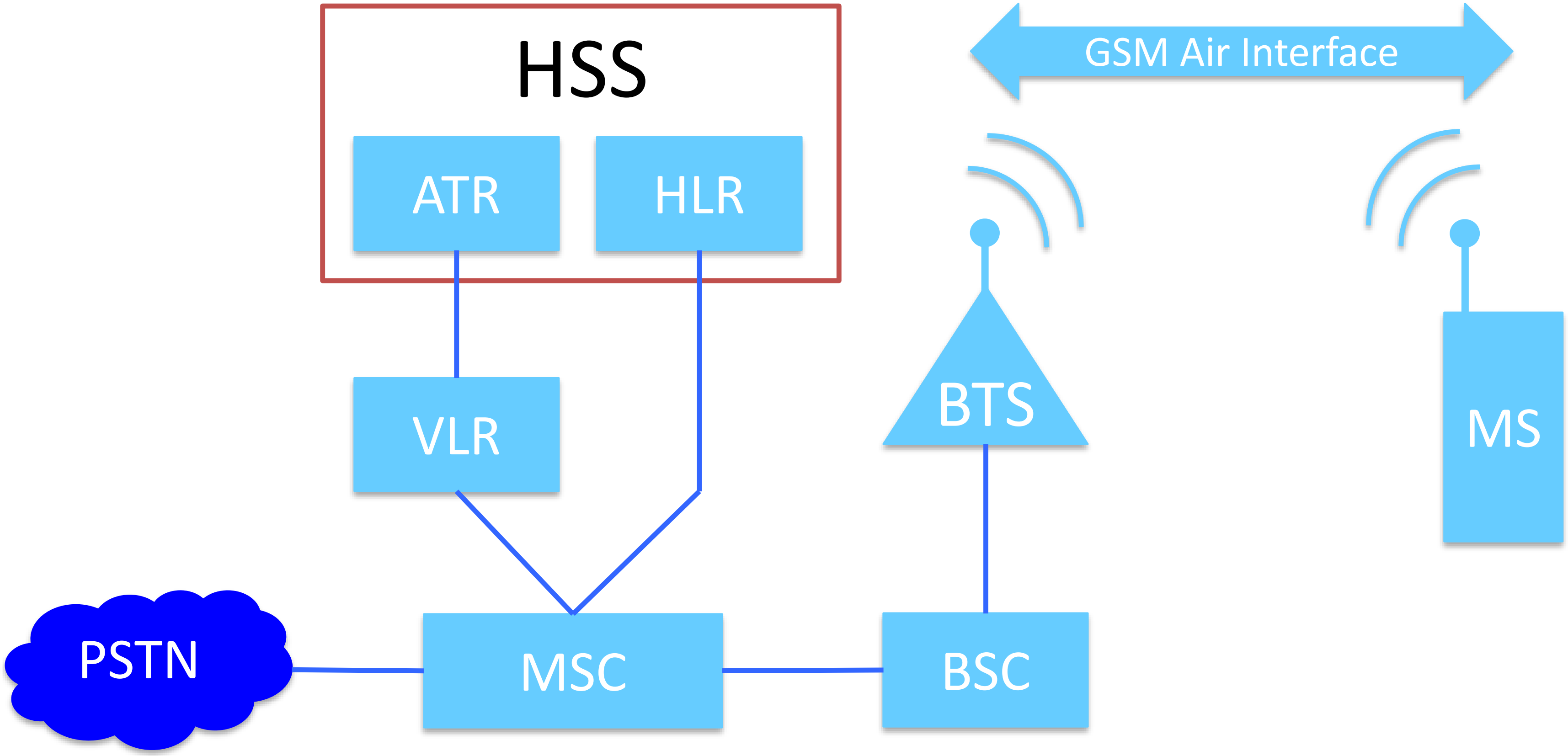
Introduction

- 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

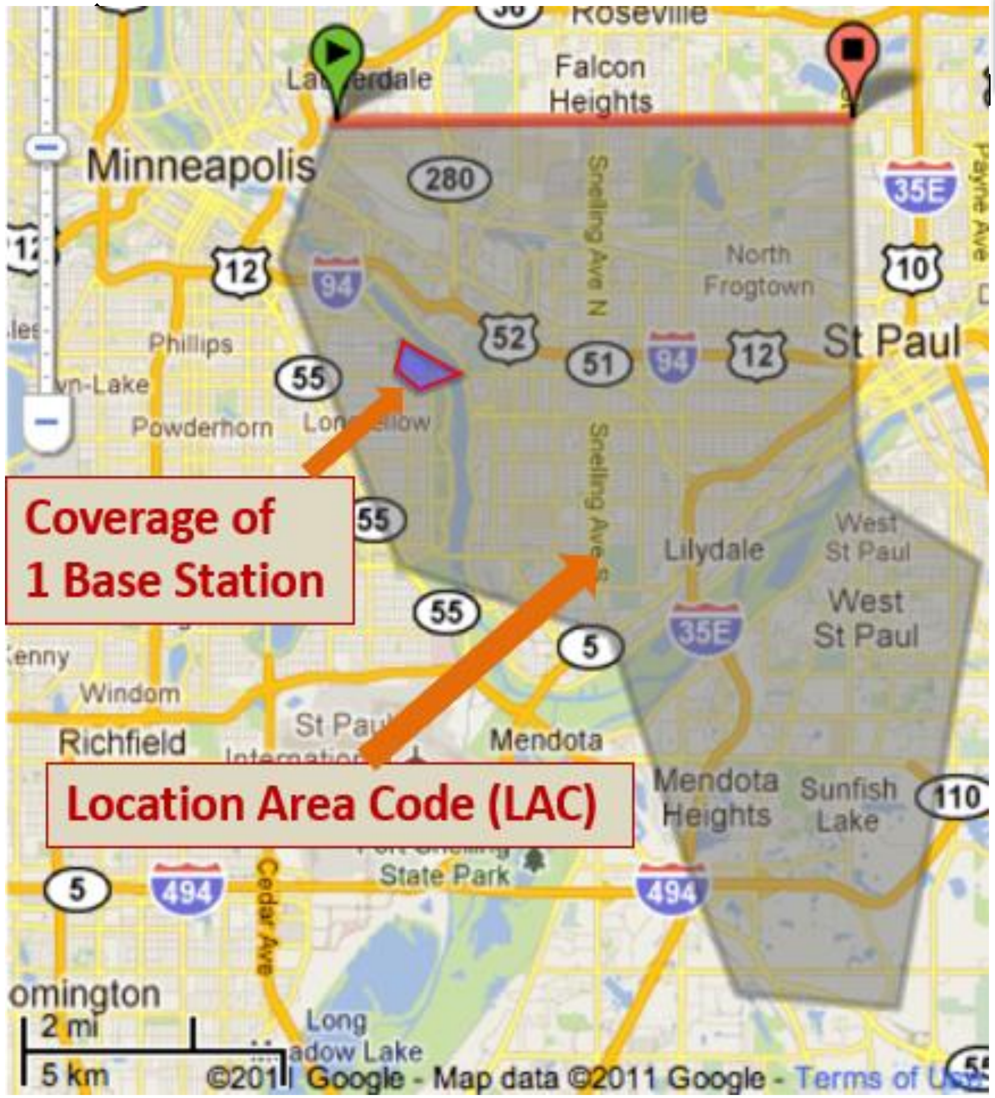
Previous Work - GSM

- Kune, Denis Foo, John Koelndorfer, Nicholas Hopper, and Yongdae Kim. "Location leak s on the GSM air interface." *ISOC NDSS* (2012).

GSM Network

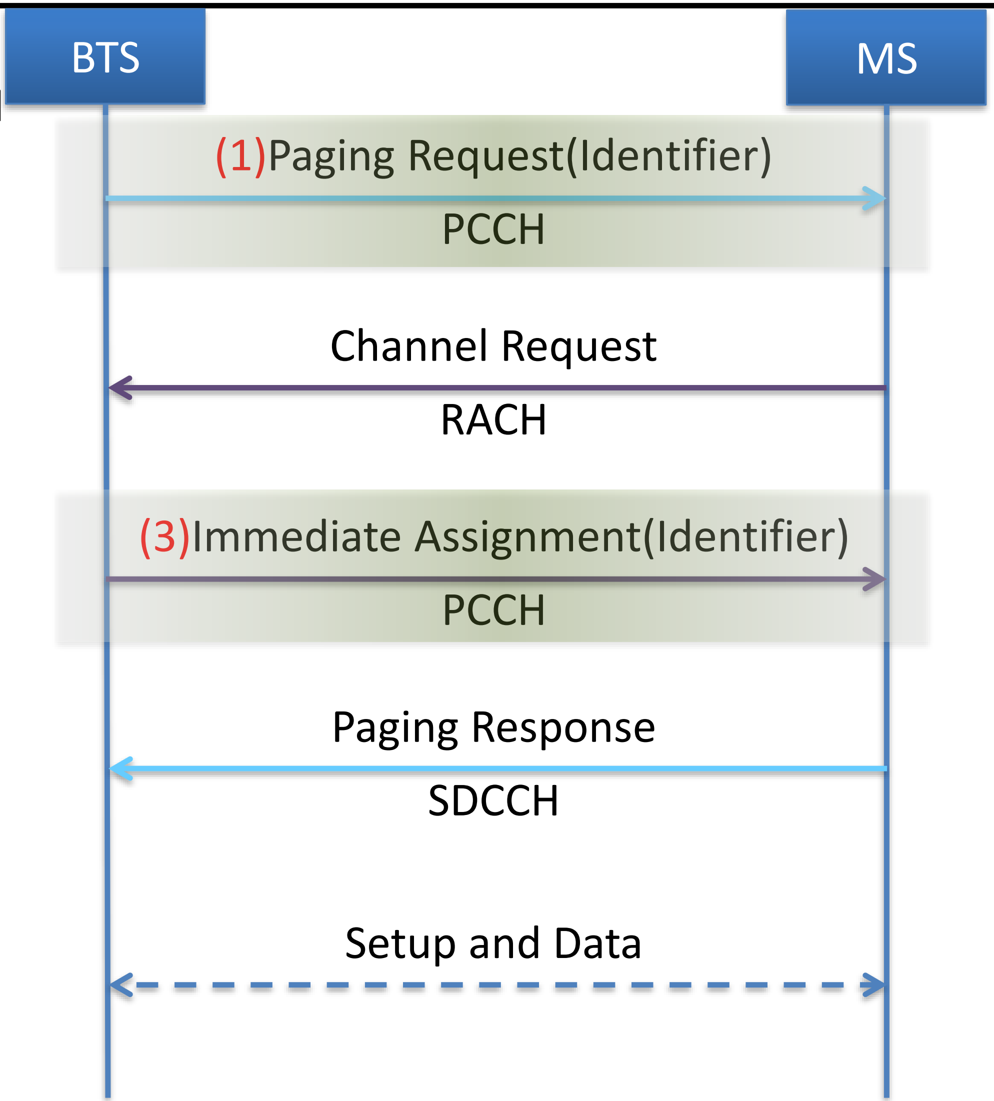


Location Leaks on GSM Network



Coverage of 1 Base Station

Location Area Code (LAC)



BTS

MS

(1)Paging Request(Identifier)

PCCH

Channel Request

RACH

(3)Immediate Assignment(Identifier)

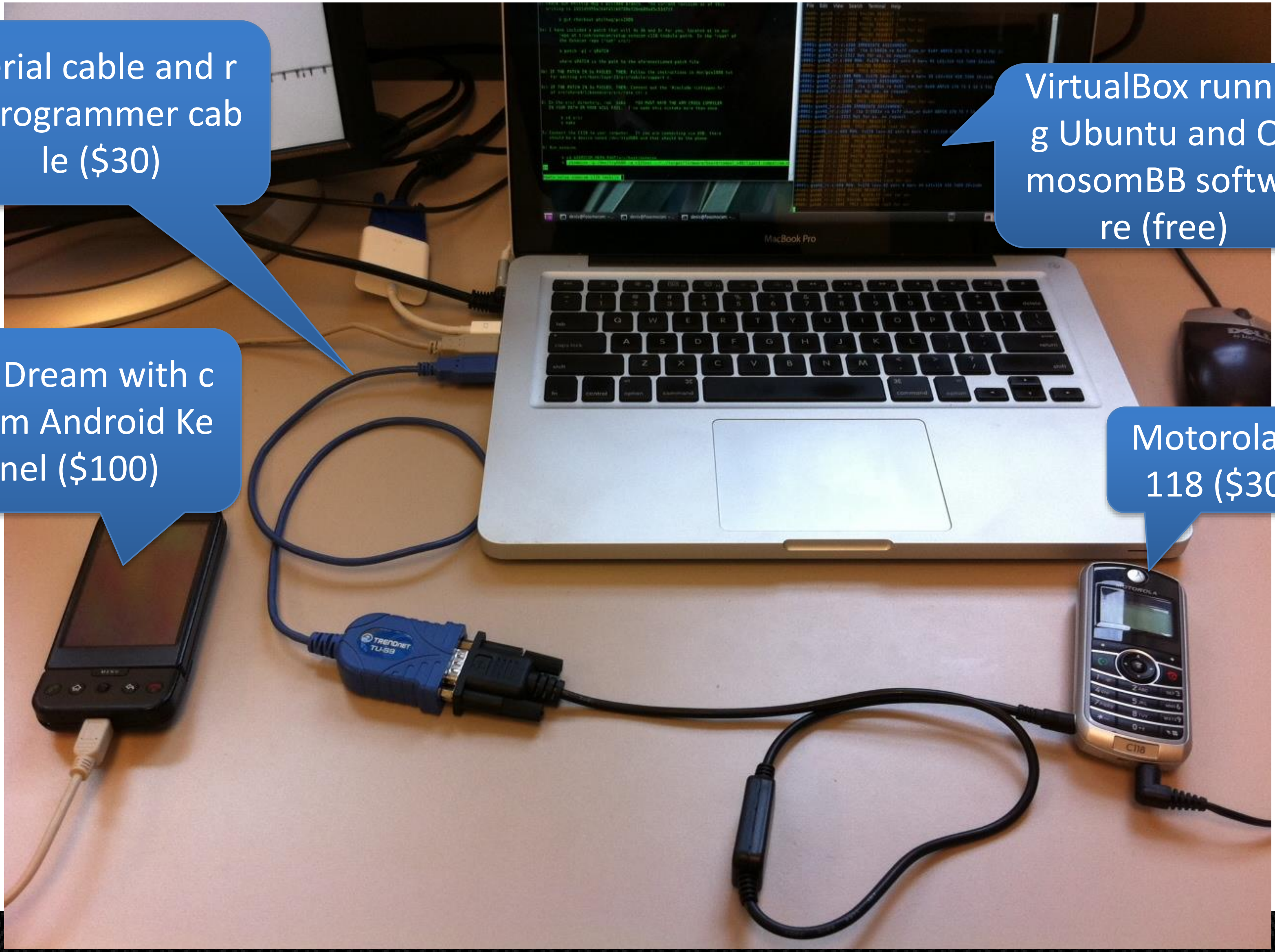
PCCH

Paging Response

SDCCH

Setup and Data

Platform



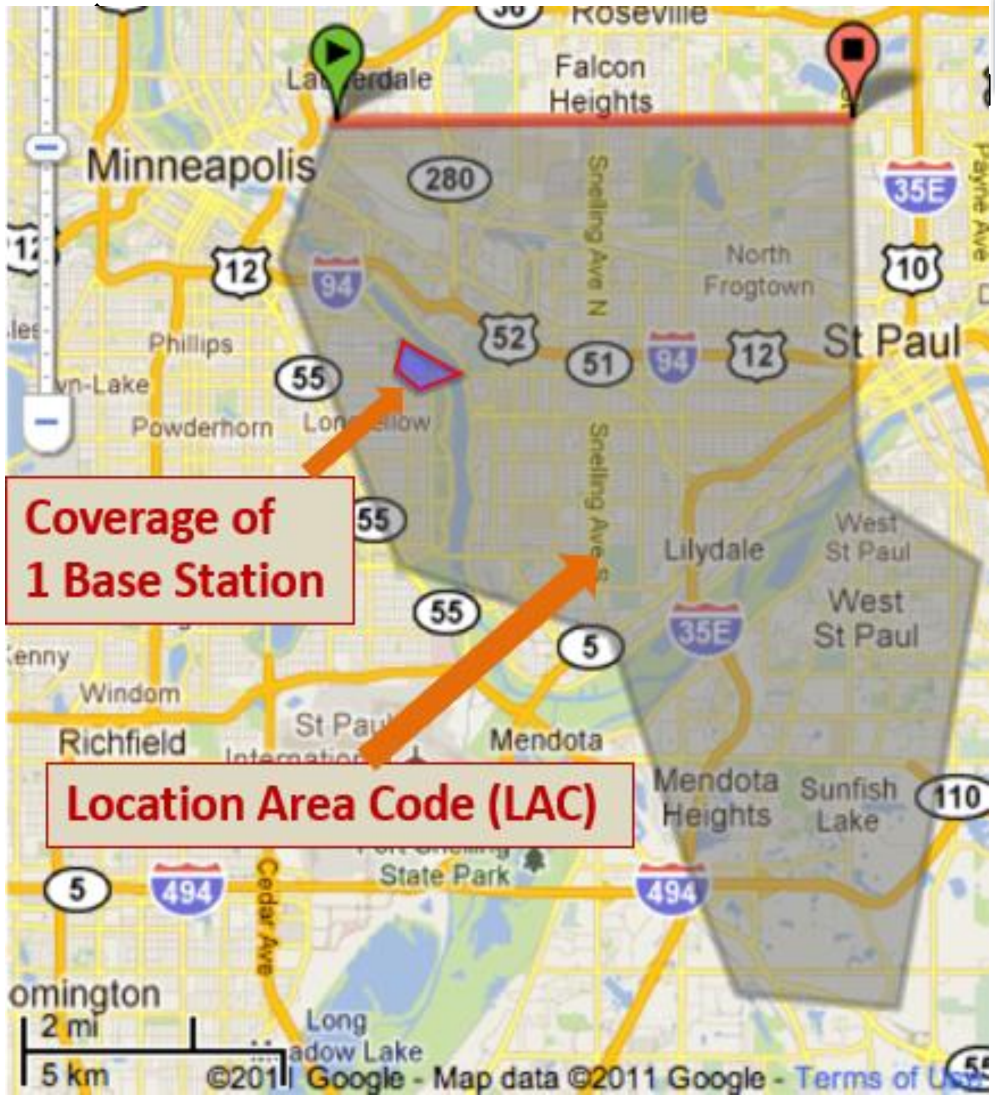
Serial cable and reprogrammer cable ($30)

VirtualBox running Ubuntu and OsmosomBB software (free)

HTC Dream with custom Android Kernel ($100)

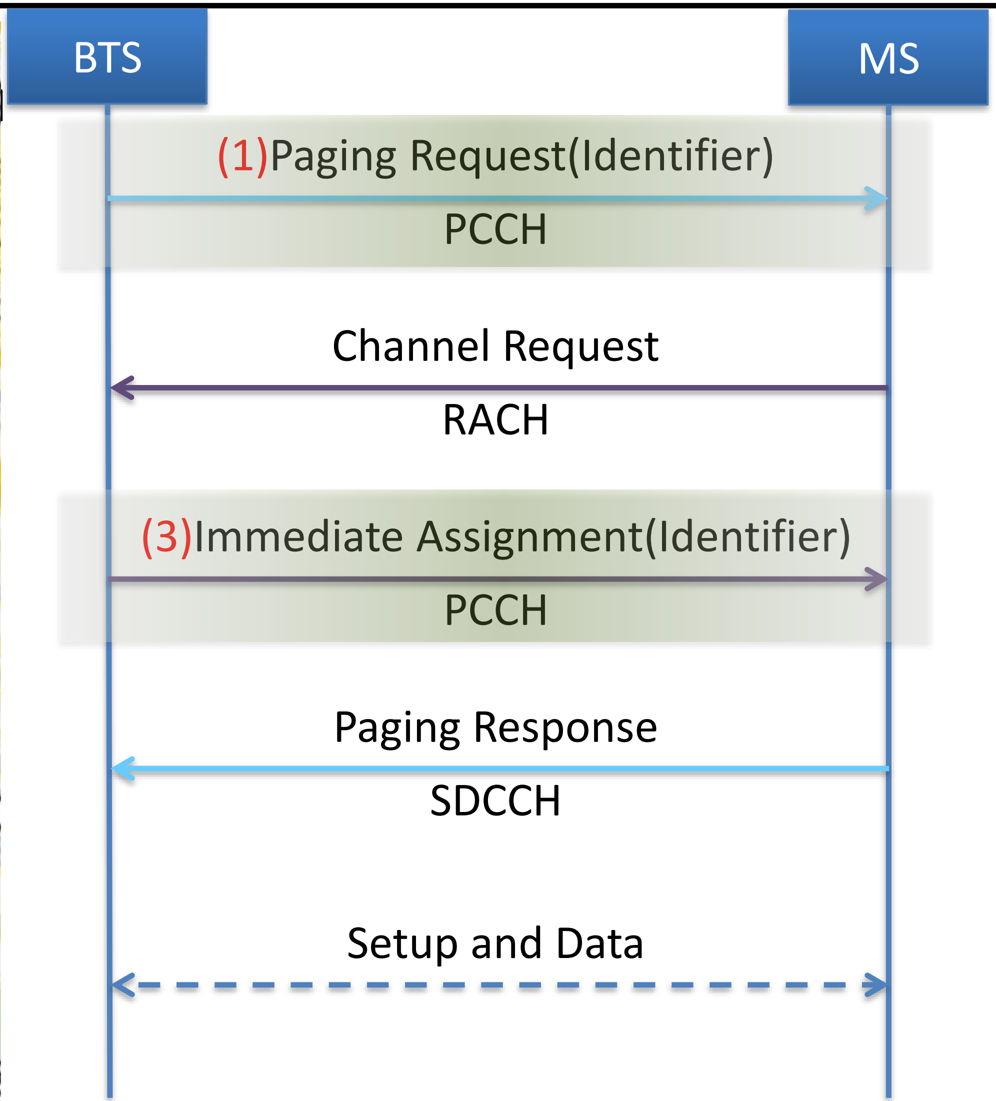
Motorola C118 ($30)

Location Leaks on GSM Network



Coverage of 1 Base Station

Location Area Code (LAC)



BTS

MS

(1)Paging Request(Identifier)

PCCH

Channel Request

RACH

(3)Immediate Assignment(Identifier)

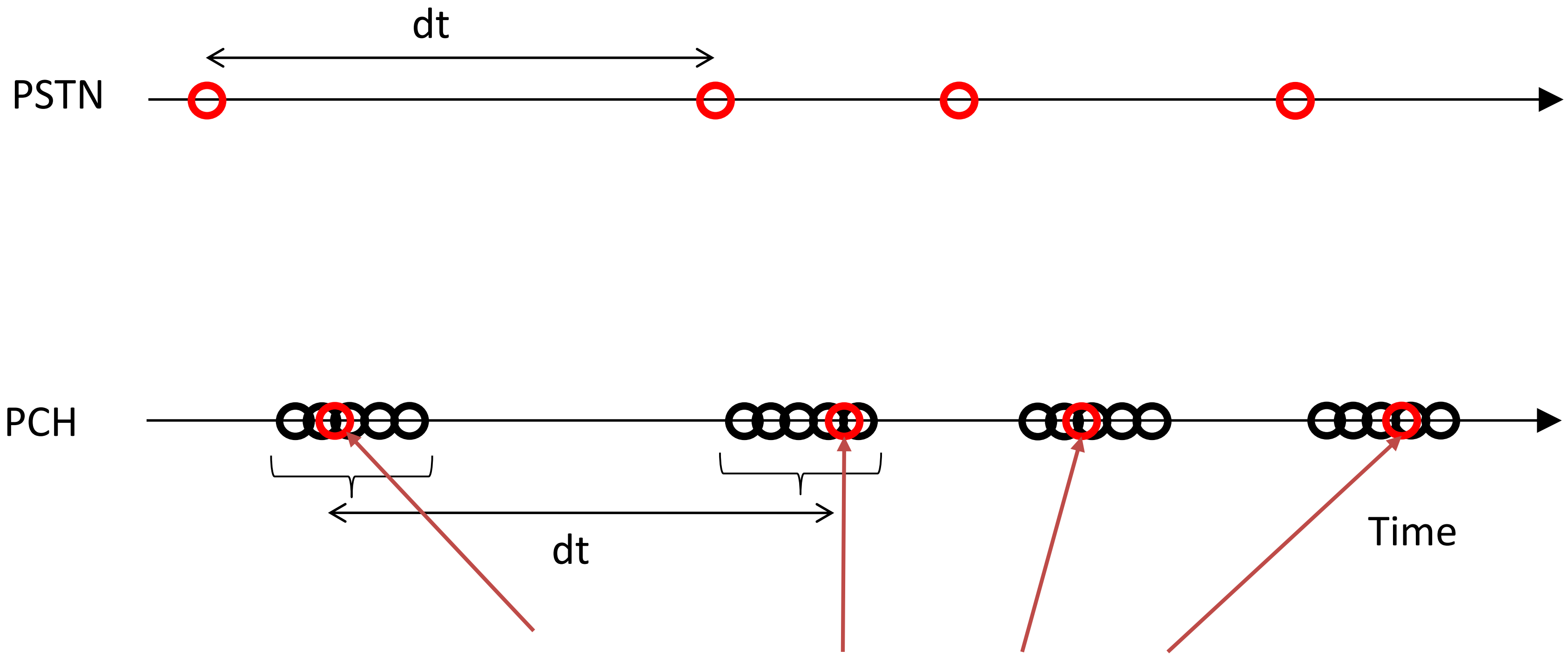
PCCH

Paging Response

SDCCH

Setup and Data

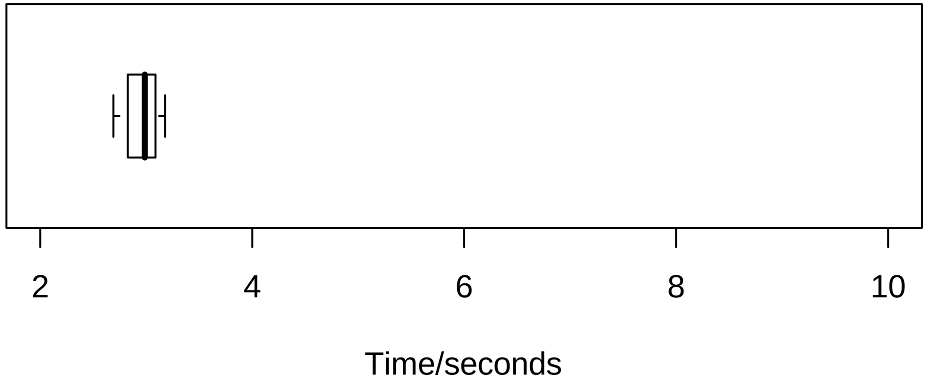
Phone number-TMSI mapping



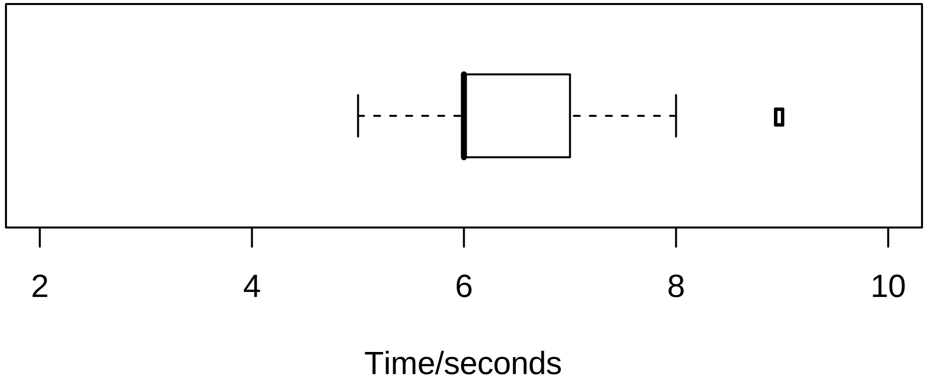
Vulnerability: Unchanged Identifier

Silent Paging

- Delay between the call initiation and the paging request: 3 sec



- Median delay between call initiation and ring: 6 sec



SysSec
System Security
Lab.

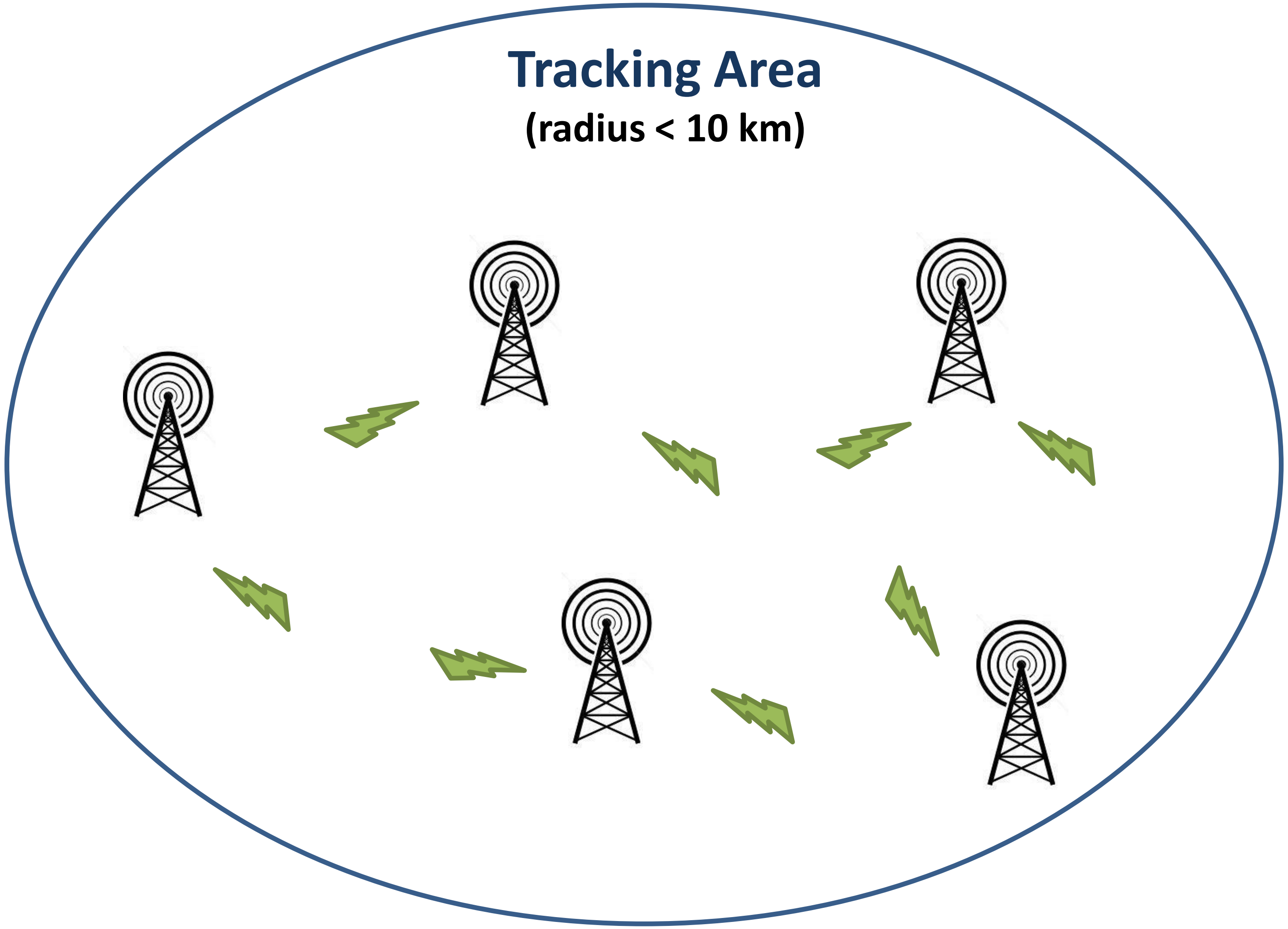
GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier

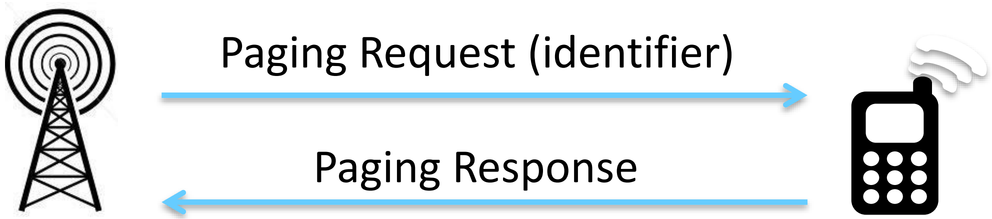
Byeongdo Hong, Sangwook Bae, Yongdae Kim

KAIST SysSec

Feb. 19, 2018

Paging Area in LTE Network





Paging:

A method to find specific subscriber

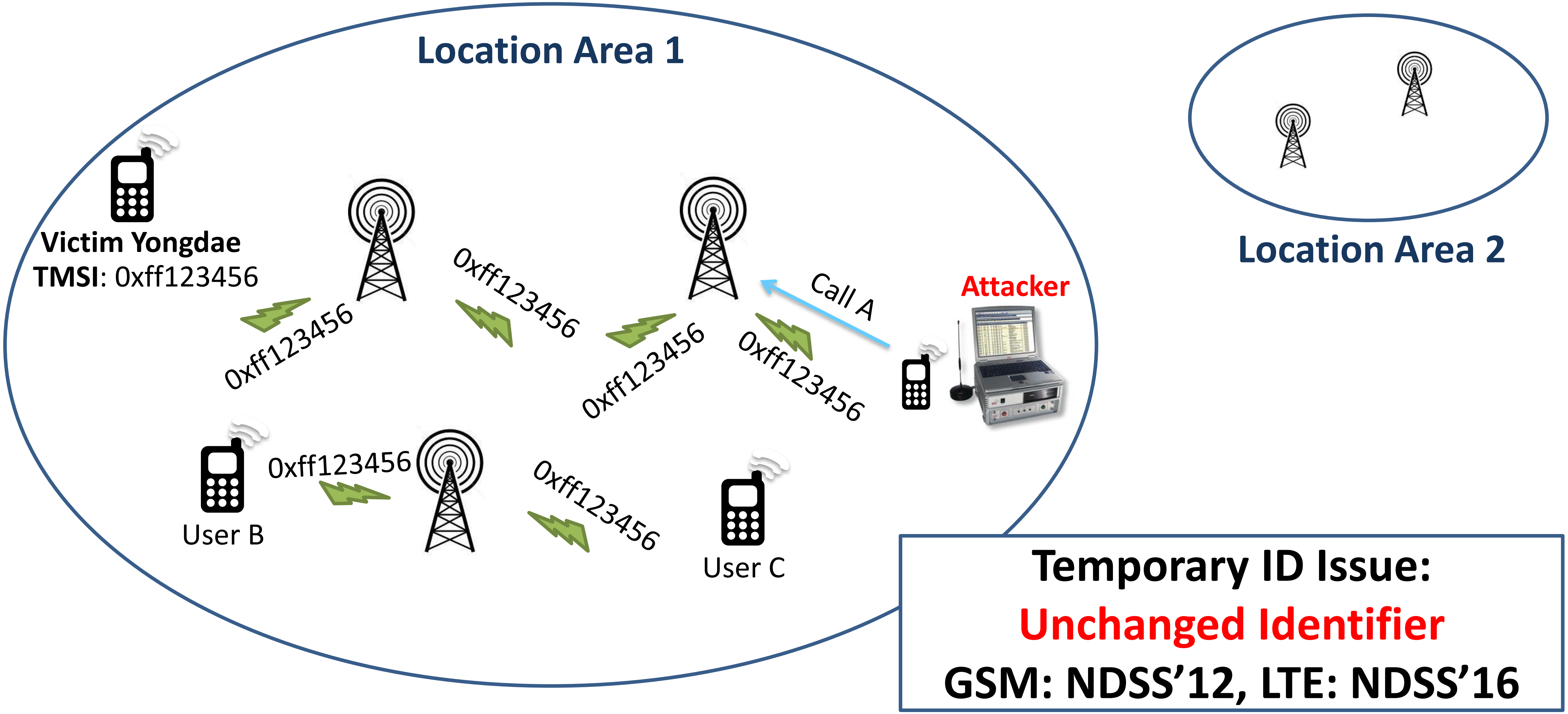
How?

By using subscriber’s ***identifier***

Identifiers in LTE Networks

- Permanent/Unique identifier
  - IMSI (International Mobile Subscriber Identity)
    - Provisioned in the SIM card
- Temporary identifier
  - Used to **hide** subscriber
    - **TMSI** (Temporary Mobile Subscriber Identity)
      - Used in 2G/3G
    - **GUTI** (Globally Unique Temporary Identity)
      - Used in LTE

Location Tracking in Cellular Network



Temporary ID Issue:

Unchanged Identifier

GSM: NDSS'12, LTE: NDSS'16

Defense of Location Tracking

- Temporary Identifier Reallocation
  - ***GUTI Reallocation*** in LTE
  - To prevent between subscriber and ID mapping

Q. Is ***GUTI Reallocation*** the solution to existing attacks?

A. It is Yes

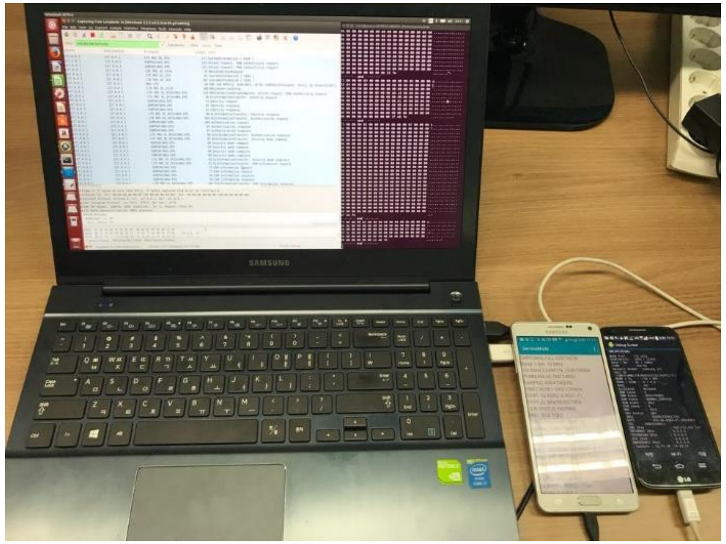
But **simply changing** is not a solution!

Experiment Setup

Needed messages: paging , identifier updating messages

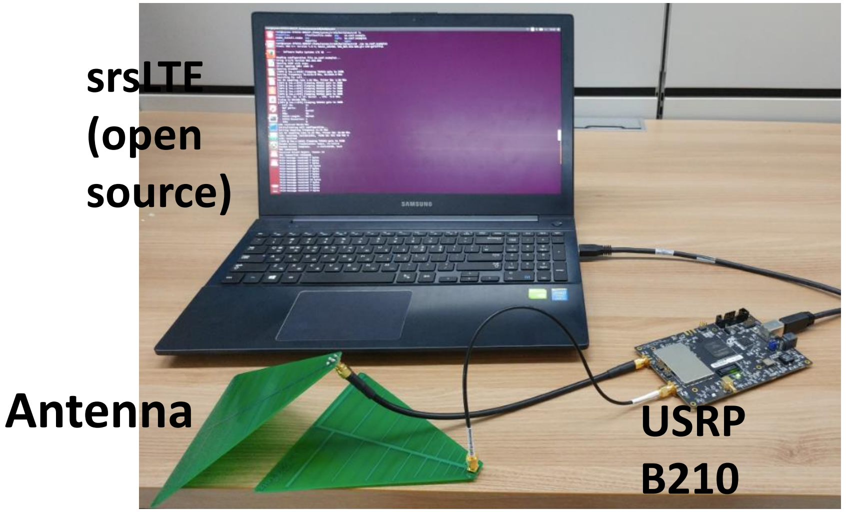
Device Analysis

Diagnostic Monitor



Signaling Collection and Analysis Tool (SCAT) [1]

Broadcast Channel Analysis



Broadcast Channel Receiver

[1] B. Hong, S. Park, H. Kim, D. Kim, H. Hong, H. Choi, J.P. Seifert, S. Lee, Y. Kim, *Peeking over the Cellular Walled Gardens - A Method for Closed Network Diagnosis -*, IEEE Transactions on Mobile Computing.

Worldwide Data Collection

Country	# of OP.	# of USIM	# of signalings	Country	# of OP.	# of USIM	# of signalings
U.S.A	3	22	763K	U.K.	1	1	41K
Austria	3	3	807K	Spain	2	2	51K
Belgium	3	3	372K	Netherlands	3	3	946K
Switzerland	3	3	559K	Japan	1	2	37K
Germany	4	19	841K	South Korea	3	14	1.7M
France	2	6	305K				

Data summary

Collection Period: **2014. 11. ~ 2017. 7.**

# of countries: **11** # of operators: **28** # of USIMs: **78** # of voice calls: **58K** # of signalings: **6.4M**

※ OP: operator, USIM: Universal Subscriber Identity Module, Signaling: control plane message

Same vs. Fingerprintable IDs

NDSS'12, '16: Same ID → Location Tracking!!

This work: ID Fingerprinting → Location Tracking!!

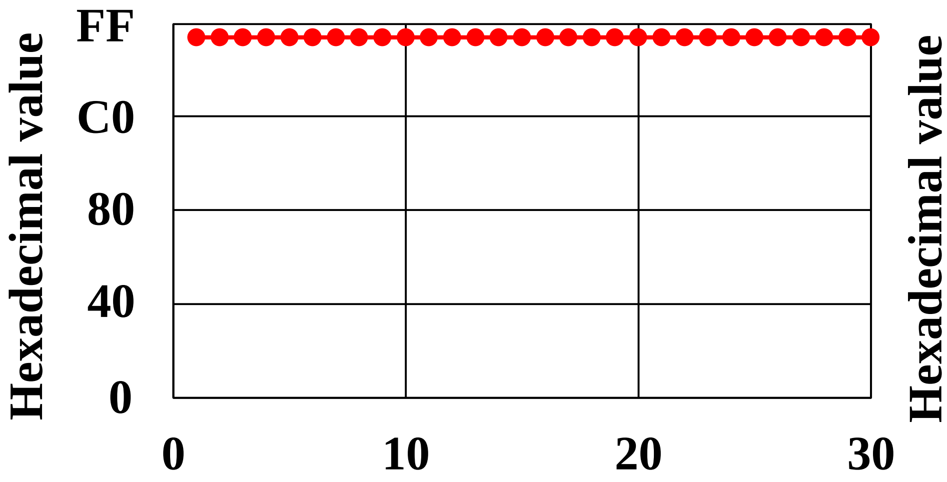
Fixed Bytes in *GUTI Reallocation*

- 19 operators have fixed bytes

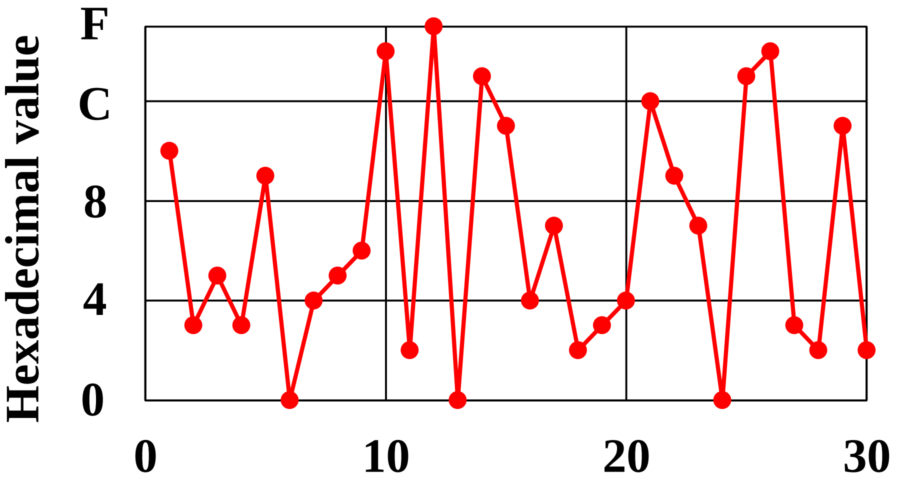
Allocation Pattern	Operators
Assigning the same GUTI	BE-III, DE-II, FR-II, JP-I
Three bytes fixed	CH-II, DE-III, NL-I, NL-II
Two bytes fixed	BE-II, CH-I, CH-III, ES-I, FR-I, NL-III
One bytes fixed	AT-I, AT-II, AT-III, BE-I, DE-I

AT: Austria, BE: Belgium, CH: Switzerland, DE: Germany, ES: Spain, FR: France, JP: Japan, NL: Netherlands

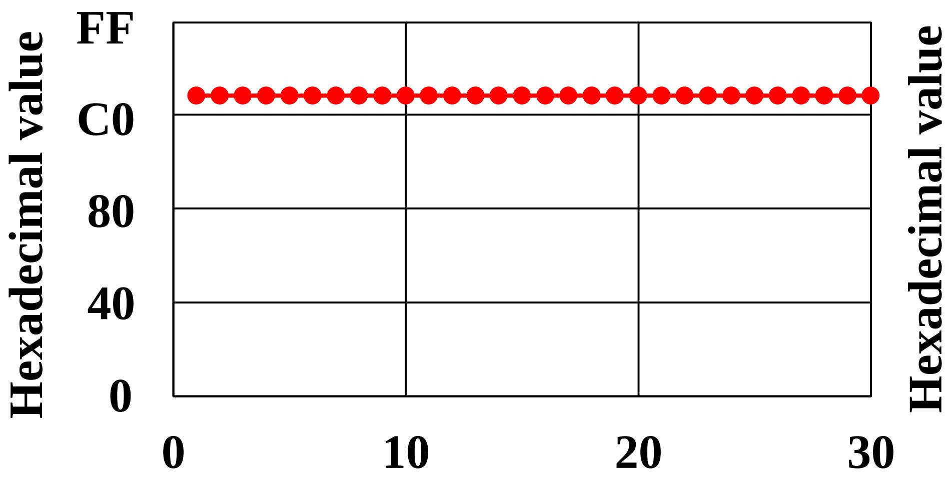
Case I: Netherlands (NL-I)



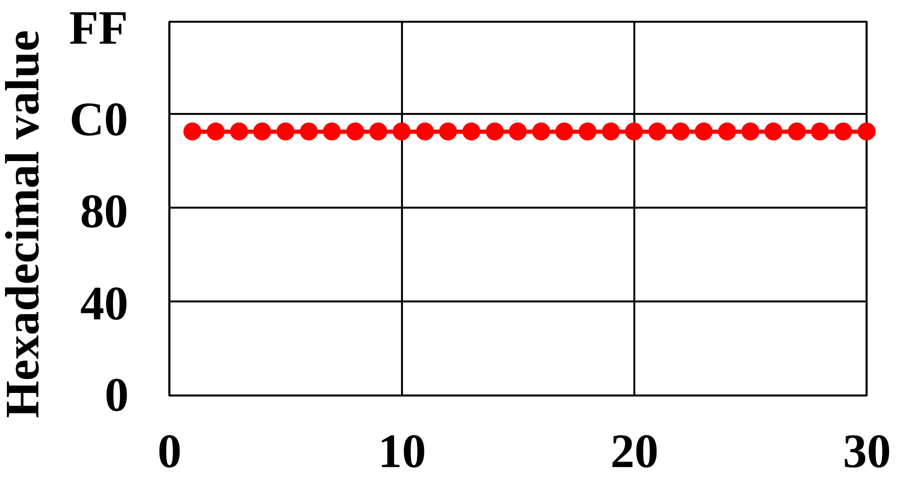
(a) 1st byte



(b) 2nd byte

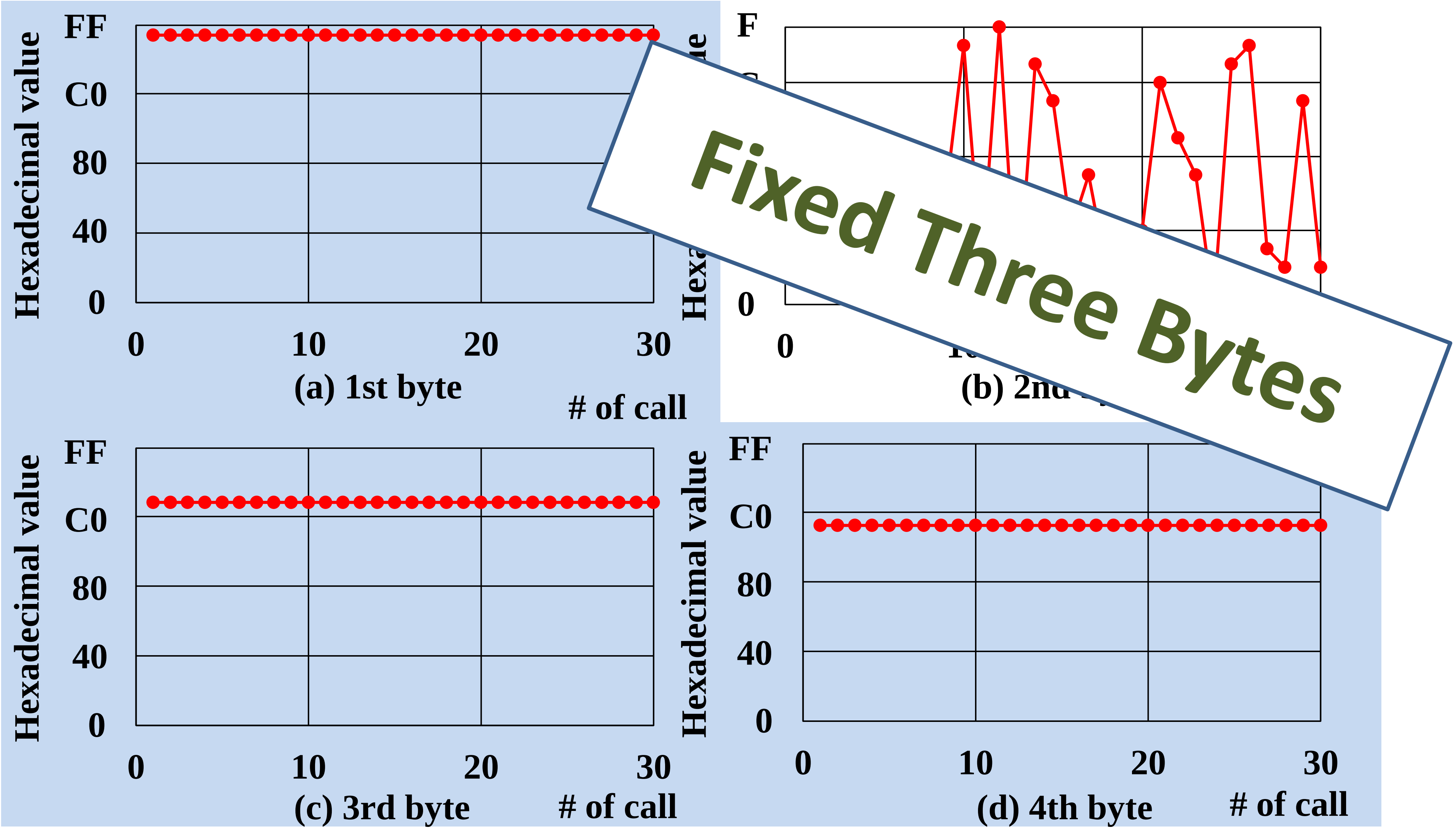


(c) 3rd byte



(d) 4th byte

Case I: Netherlands (NL-I)



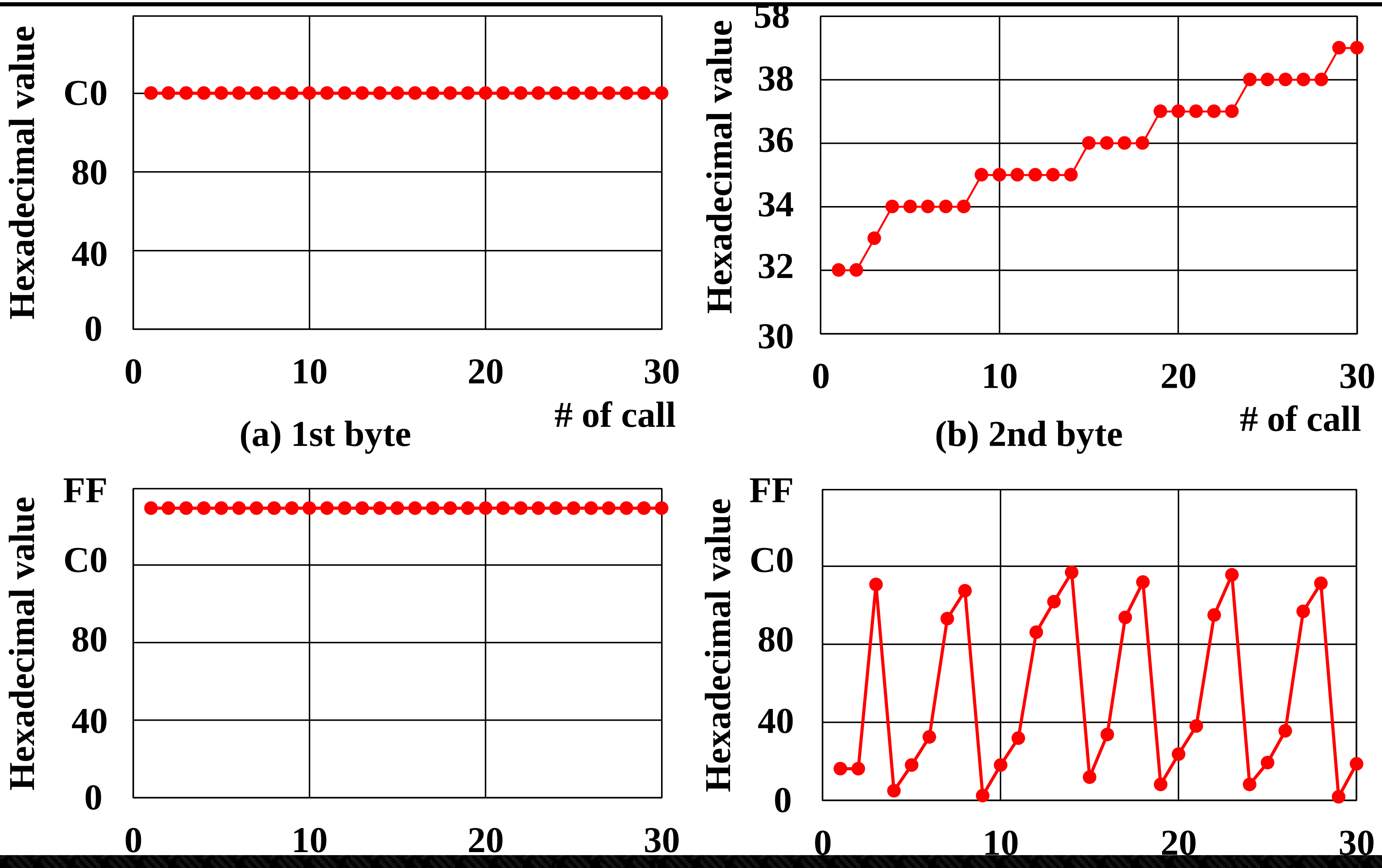
(a) 1st byte

(b) 2nd

(c) 3rd byte

(d) 4th byte

Case II: Belgium (BE-II)



(a) 1st byte

(b) 2nd byte

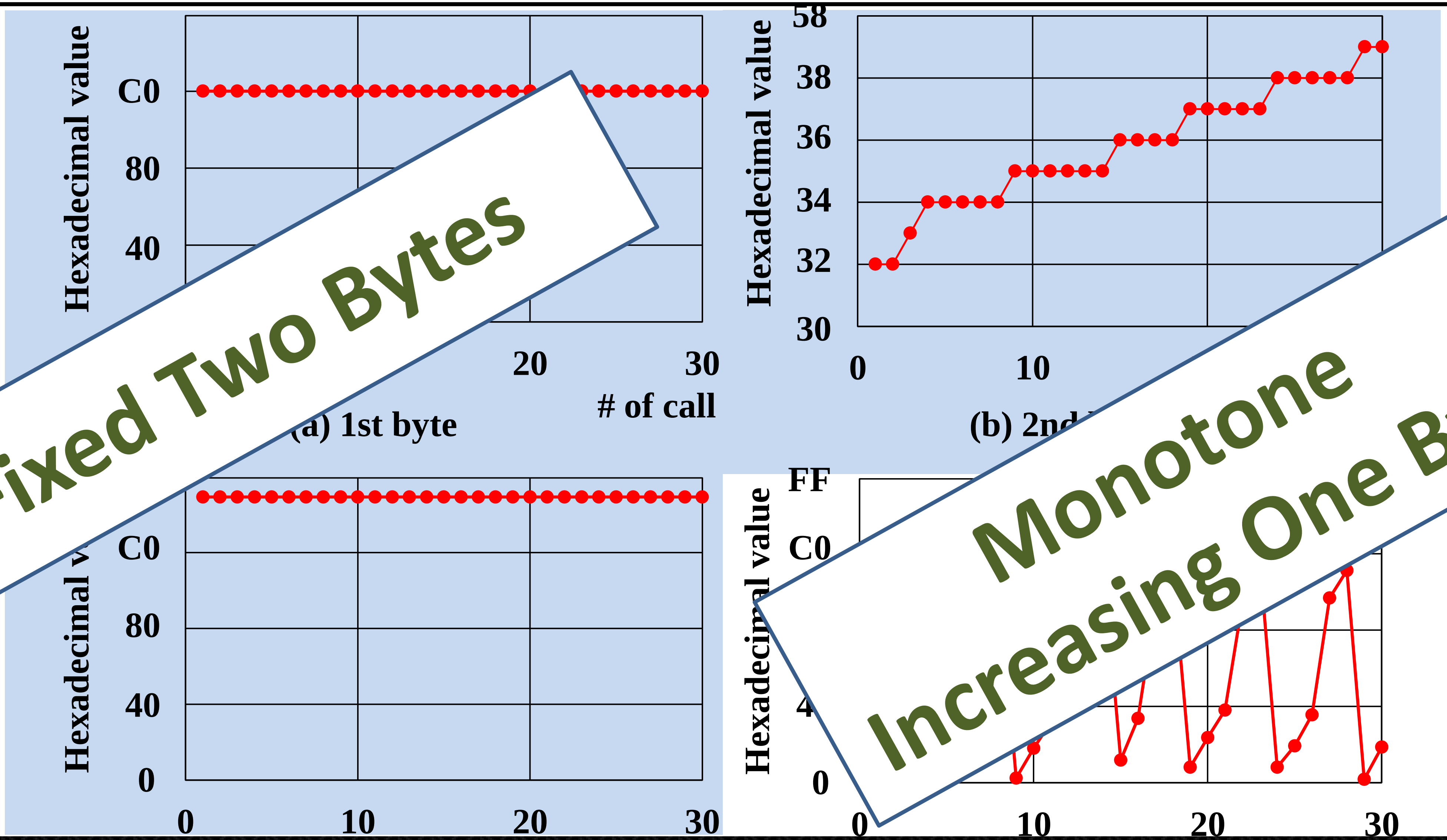
# of call

(c) 3rd byte

# of call

(d) 4th byte

Case II: Belgium (BE-II)



Fixed Two Bytes

Monotone Increasing One Byte

Fixed Bytes in *GUTI Reallocation*

- 19 operators have fixed bytes

Allocation Pattern	Operators
Assigning the same GUTI	BE-III, DE-II, FR-II, JP-I
Three bytes fixed	CH-II, DE-III, NL-I, NL-II
Two bytes fixed	BE-II, CH-I, CH-III, ES-I, FR-I, NL-III
One bytes fixed	AT-I, AT-II, AT-III, BE-I, DE-I

AT: Austria, BE: Belgium, CH: Switzerland, DE: Germany, ES: Spain, FR: France, JP: Japan, NL: Netherlands

Stress Testing

- No noticeable rule of *GUTI Reallocation* for some operators

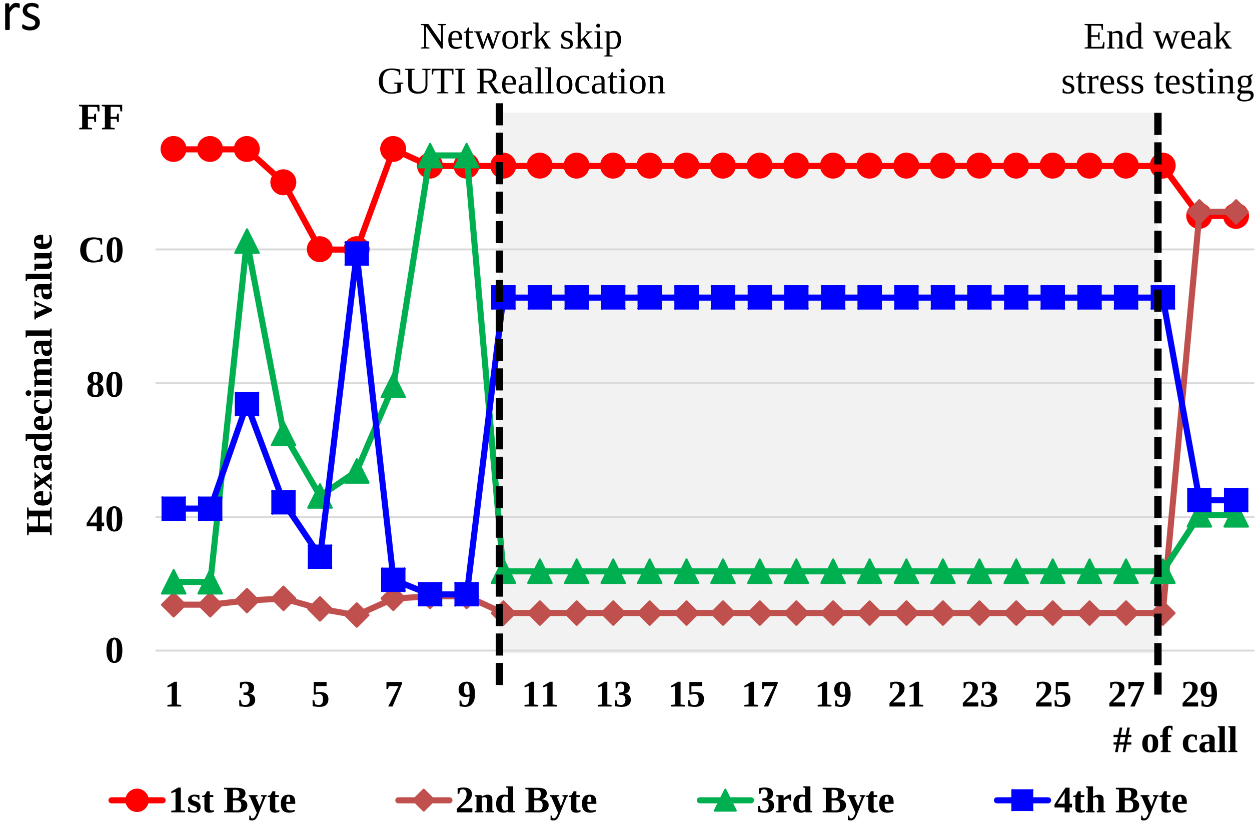
- Invoking voice call continuously with a short time
  - Two types of test
    - Weak stress testing
    - Hard stress testing
      - Calls at shorter intervals than weak stress test

Stress Testing Result

- Force the network to skip the *GUTI reallocation*
  - Perform experiments on US and Korean operators
    - Two US and two Korean operators

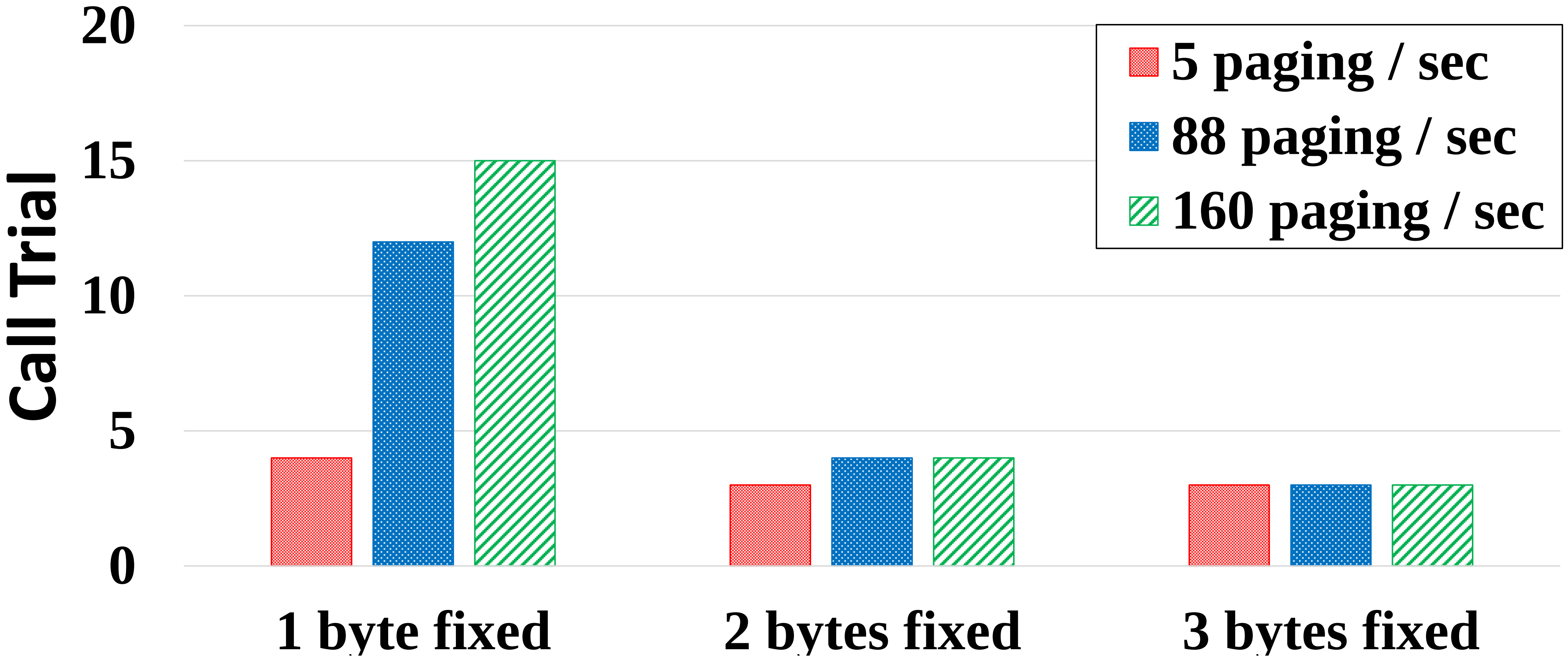
Operator	Weak Stress Testing	Hard Stress Testing
KR-I	O	O
KR-II	X	O
US-I	X	O
US-II	O	O

O: Reuse *GUTI*
X: No noticeable change



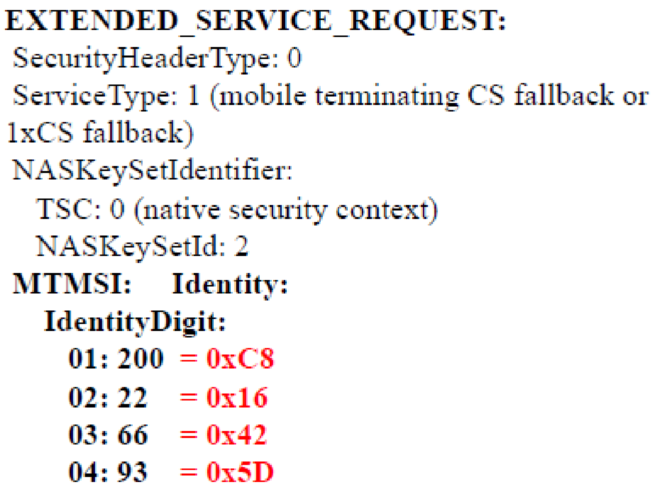
Success Rate of our Attack

- Required number of calls covering 99% success rate



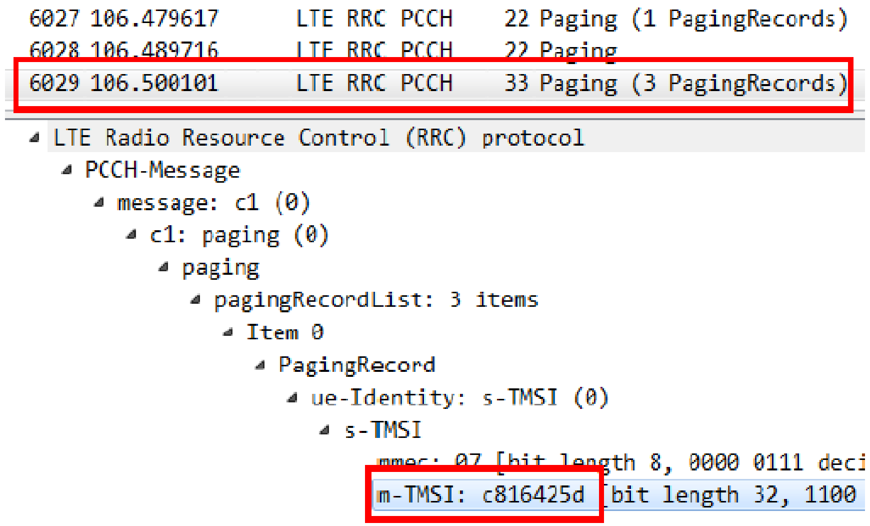
Location Tracking with GUTI

- Observation of broadcast channels after call invocation
  - Pattern matching (fixed bytes, assigning same GUTI)
  - Location tracking (Tracking Area, Cell)



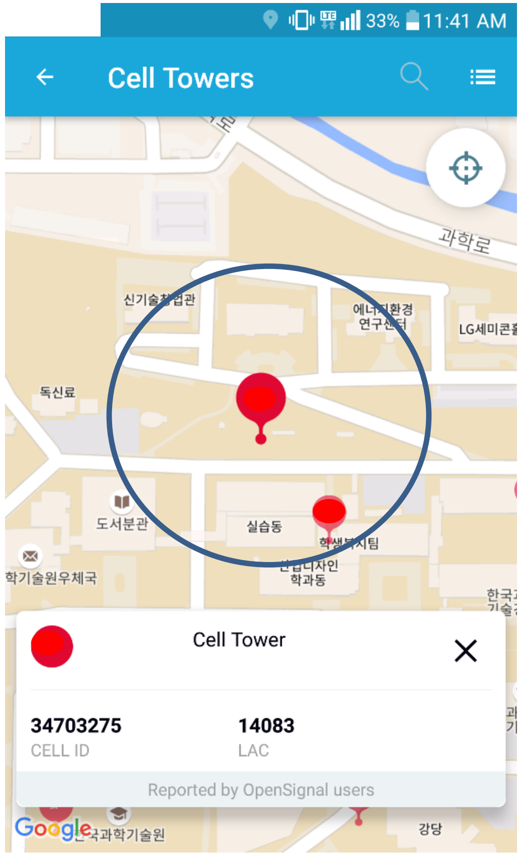
EXTENDED_SERVICE_REQUEST:
SecurityHeaderType: 0
ServiceType: 1 (mobile terminating CS fallback or 1xCS fallback)
NASKeySetIdentifier:
TSC: 0 (native security context)
NASKeySetId: 2
MTMSI: Identity:
IdentityDigit:
01: 200 = 0xC8
02: 22 = 0x16
03: 66 = 0x42
04: 93 = 0x5D

(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)



11:41 AM

Cell Towers

Cell Tower

34703275
CELL ID

14083
LAC

Reported by OpenSignal users

OpenSignal (at KAIST)

Defenses + Requirements

- **Frequent refreshing** of temporary identifier
  - Per service request
- **Unpredictable** identity allocation
  - Cryptographically secure pseudorandom number generation
    - Hash_DRBG can be used
- Collision avoidance
- Stress-testing resistance
- Low cost implementation

Conclusion

- Predictable reallocation logic
  - GUTI reallocation pattern
    - **Fixed** bytes (19 operators)
  - Same GUTI
    - By stress test (4 test cases)
    - Assigning **same** GUTI

- Location tracking is still possible in cellular network!
- Secure GUTI reallocation mechanism is required

Subsequent work

- ❖ Hussain, Syed Rafiul, et al. "Privacy attacks to the 4G and 5G cellular paging protocols using side channel information." Network and Distributed Systems Security (NDSS) Symposium2019.
- Calculate paging likelihood for every subframes after making phone calls to detect user is located at the same Tracking Area or not.

Questions

- 1. (Junho Ahn)
  This method track the TA and TA is very large. For example, in Korea, we can determ ine the location to large range more than 500km2. Are there any methods that ca n track the user more precisely?
- The range of TA depends on configuration of network carriers.
- In LTE, there is a message only be sent by the base station user is connecting to, we can use that message to track location more precise. More detail in paper on NDSS 16.

Questions

- 2. (Bumseok Oh)
  Why can’t standard (or 3GPP) specify one specific algorithm or method for “secure ” reallocation of identity? Once they fix the good algorithm, I think carriers don’t need to care about such security problems.

- The standard only defines which conditions must be satisfied, not about how to implement.
- There are many baseband chipset manufactures, each company has different algorithm, can not force them follow one’s.

Questions

- 3. (Yeongbin Hwang)
  Even in the case of SUCI in 5g, SUCI has to continuously update like GUTI, then is SUCI handled well?
- In 5G, the permanent identifier is SUPI (equal to IMSI in LTE), it is freshly encrypted to SUCI before every transmissions.
- Not implemented yet
- Chlosta, Merlin, et al. "5G SUCI-Catchers: Still catching them all?." WiSec 21. Demonstrated that we still can link between SUCIs even if it is freshly generated before transmissions.

The End
Thank you!