SysSec
System Security Lab.

GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier

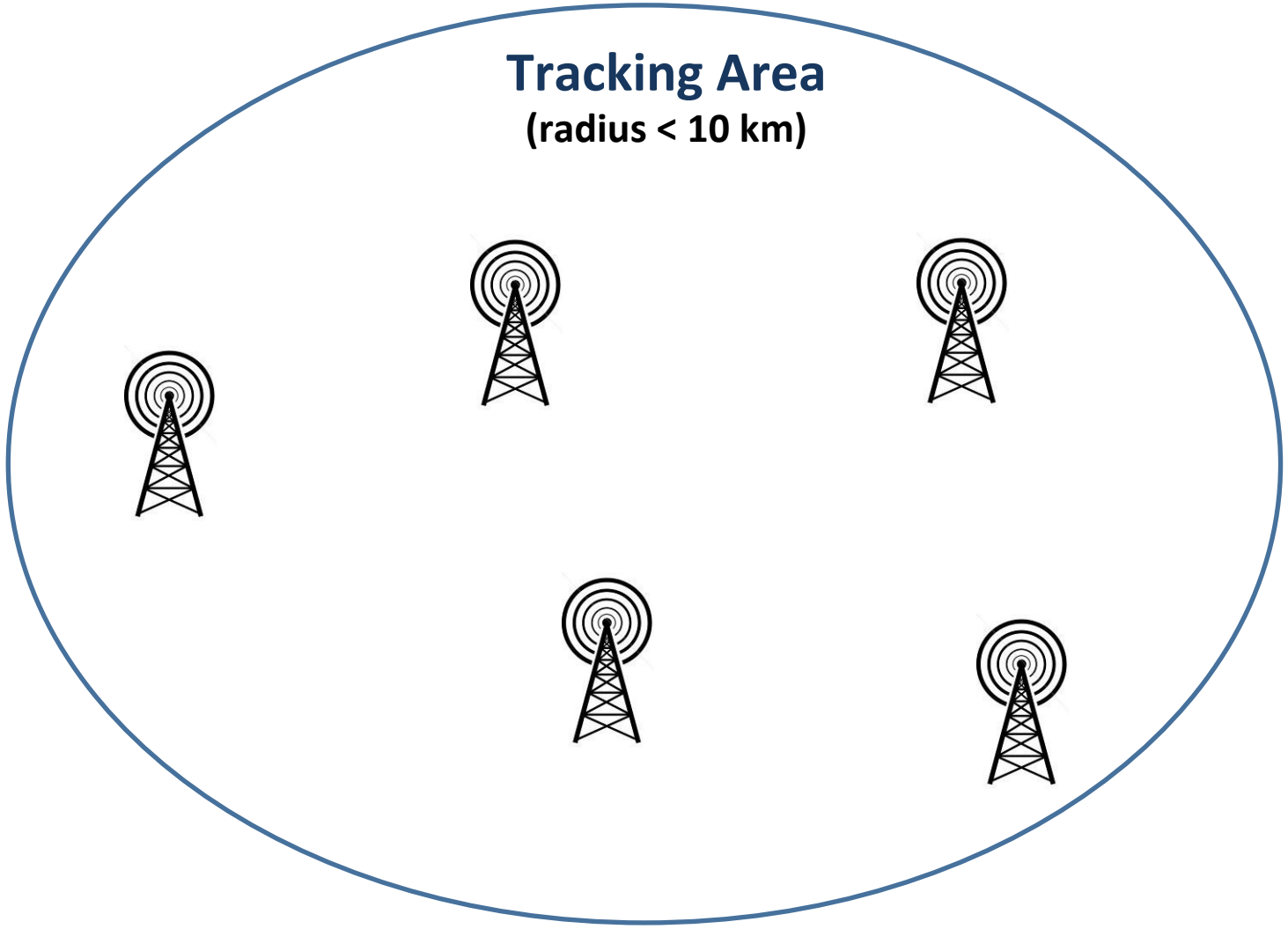
Byeongdo Hong, Sangwook Bae, Yongdae Kim

KAIST SysSec

Feb. 19, 2018

KAIST

Paging Area in Cellular Network



Yongdae

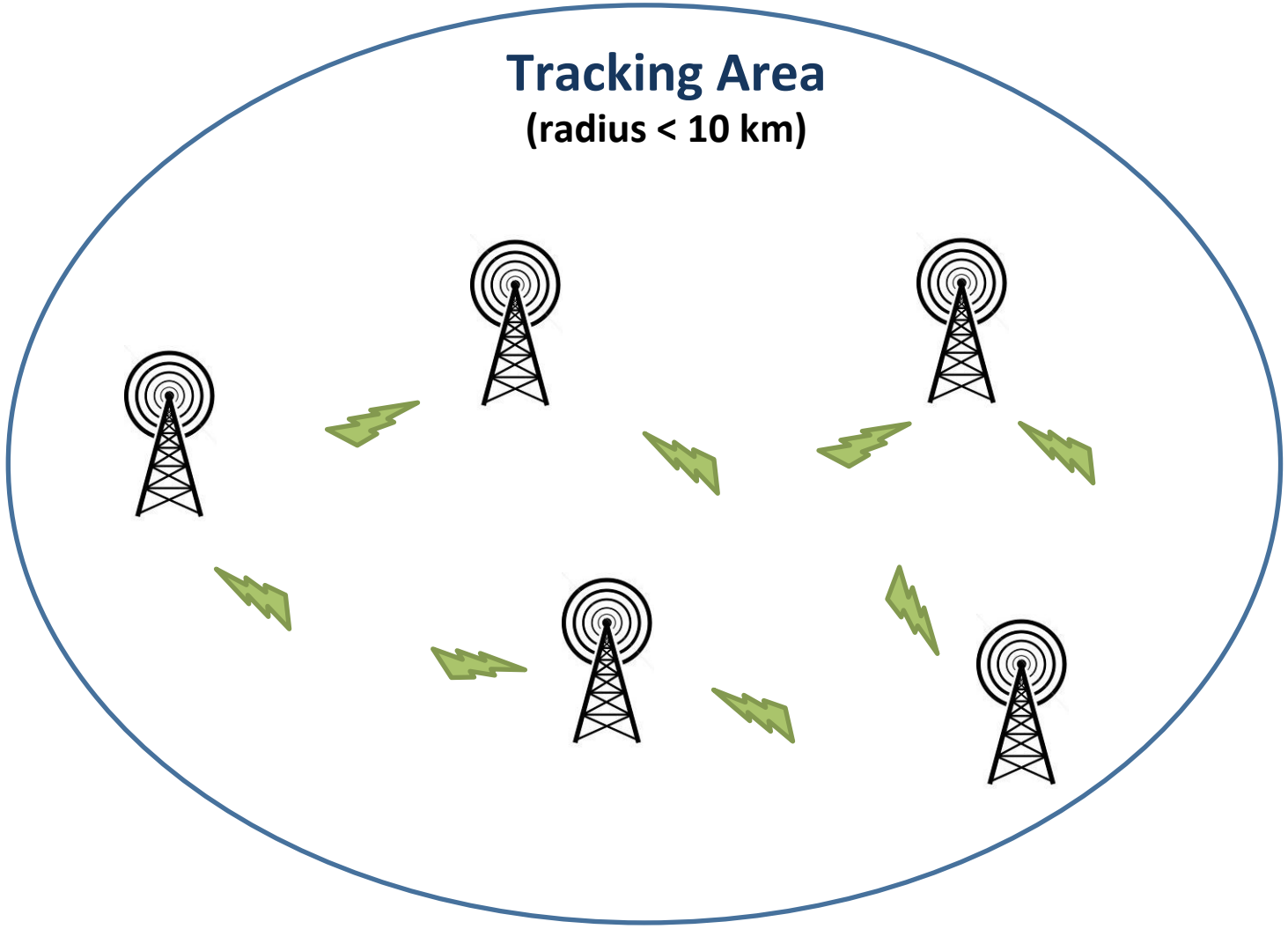
Paging:

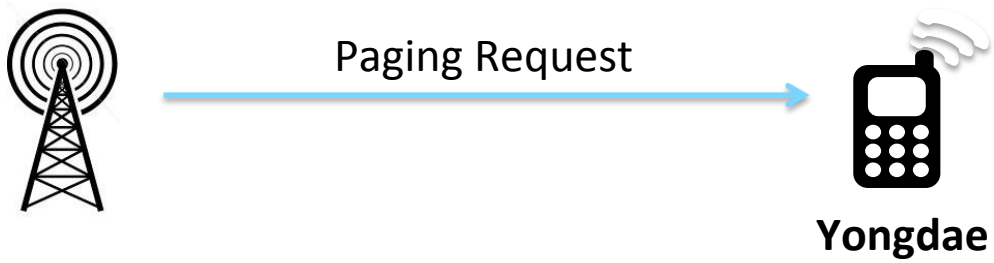
A method to find specific subscriber

How?

By using subscriber's ***identifier***

Paging Area in Cellular Network

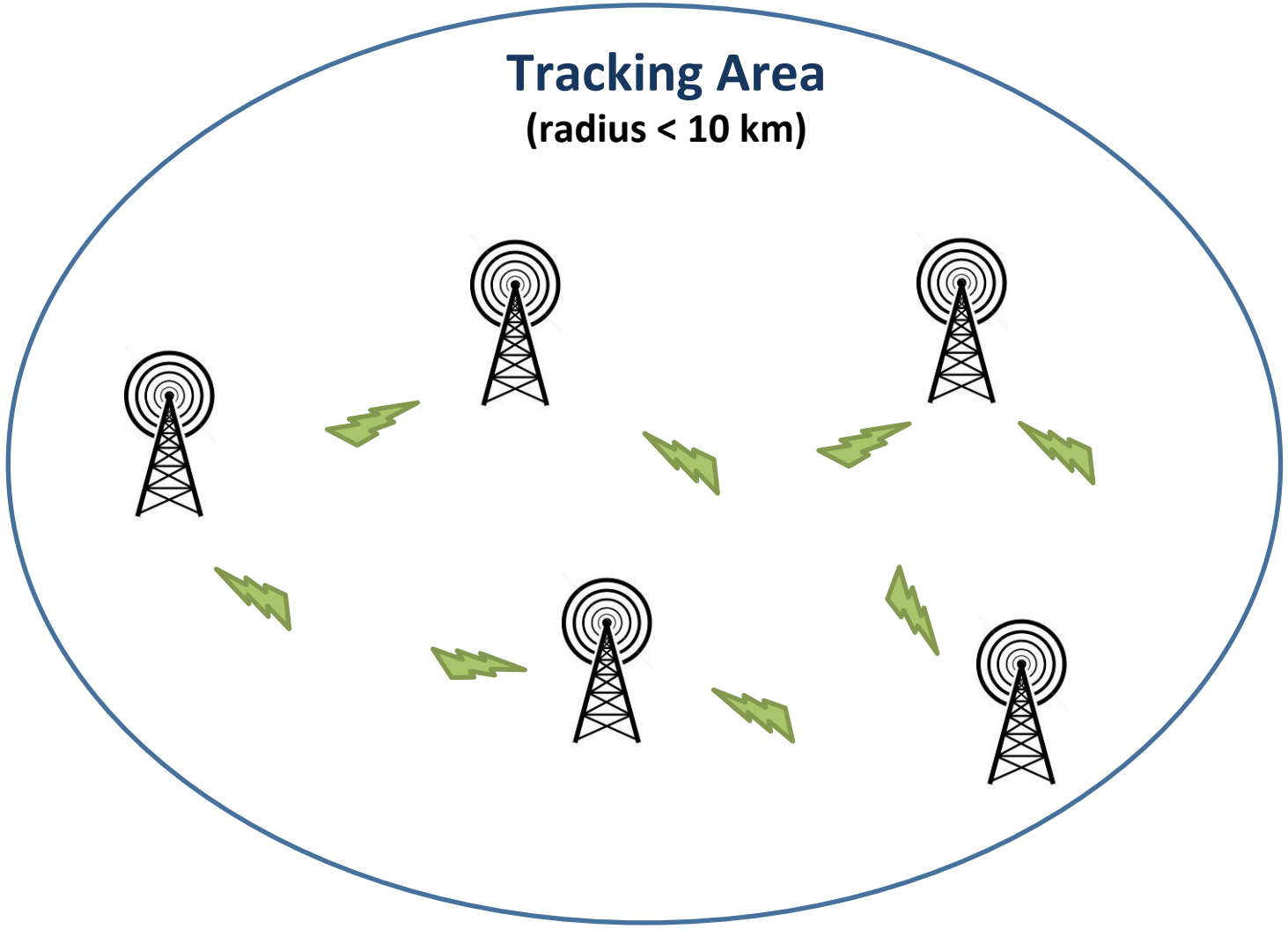


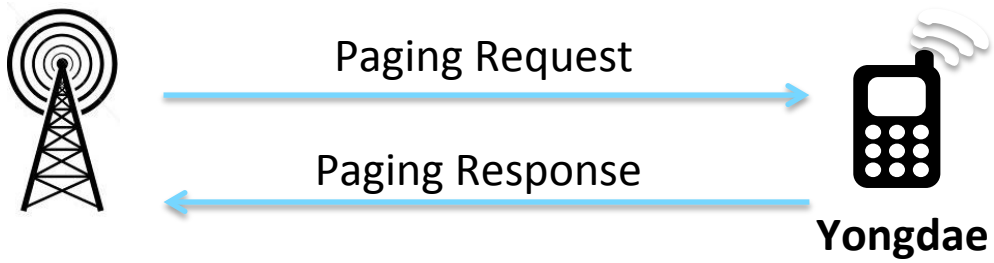


Paging:
A method to find specific subscriber

How?
By using subscriber's ***identifier***

Paging Area in Cellular Network





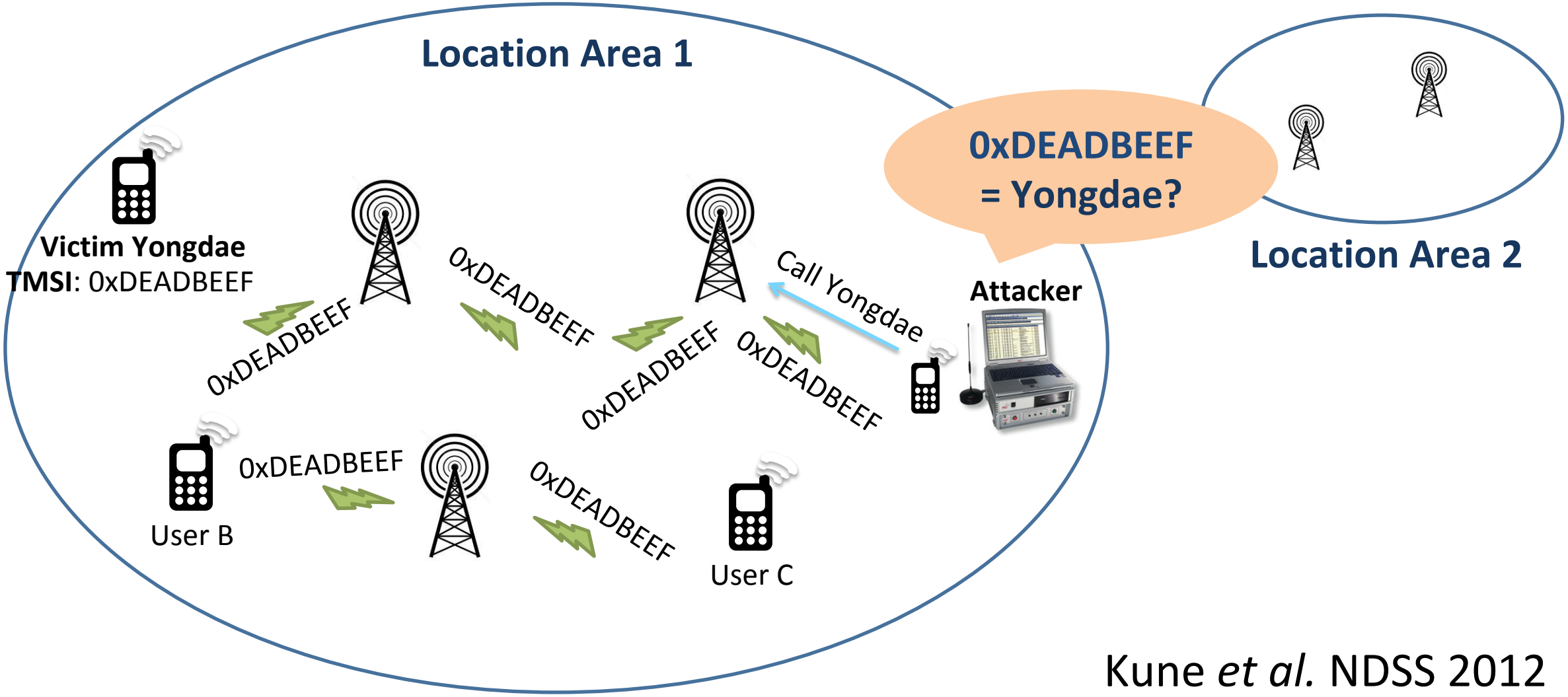
Paging:
A method to find specific subscriber

How?
By using subscriber's ***identifier***

Identifiers in Cellular Networks

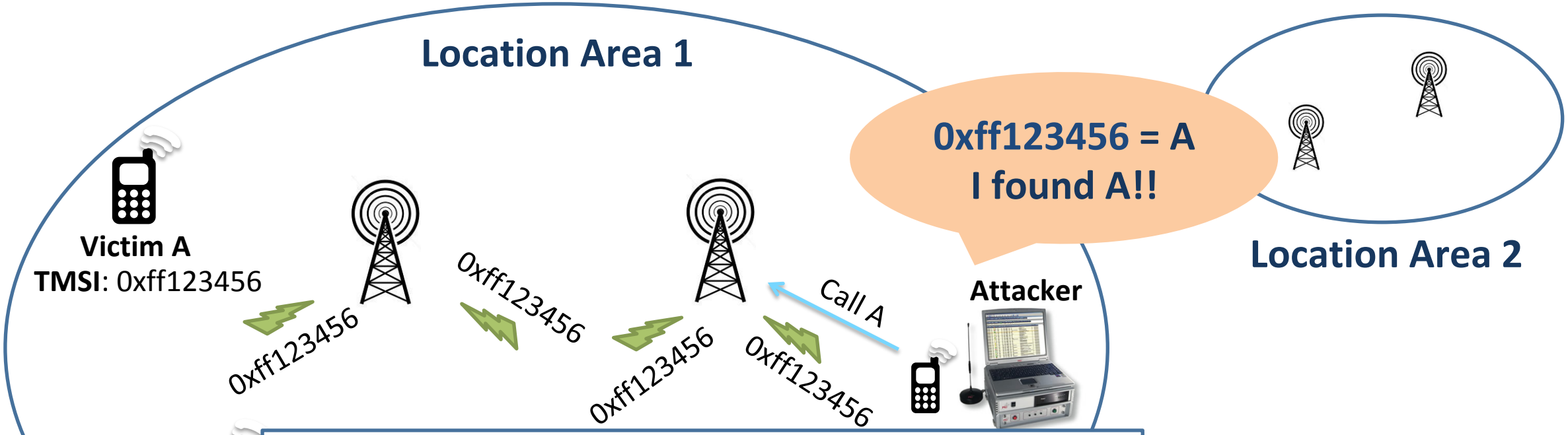
- Permanent/Unique identifier
  - IMSI (International Mobile Subscriber Identity)
    - Provisioned in the SIM card
- Temporary identifier
  - Used to **hide** subscriber
    - **TMSI** (Temporary Mobile Subscriber Identity)
      - Used in 2G/3G
    - **GUTI** (Globally Unique Temporary Identity)
 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

Location Tracking in Cellular Network



Kune *et al.* NDSS 2012

Location Tracking in Cellular Network



Temporary ID Issue:

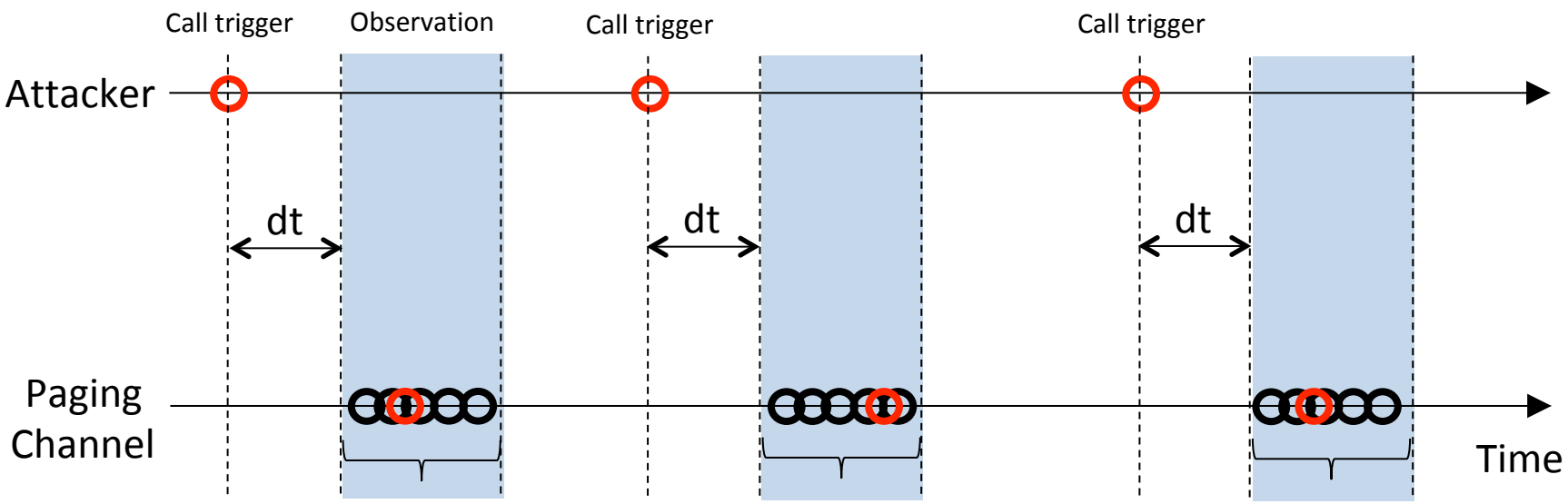
Unchanged Identifier

GSM: NDSS'12, LTE: NDSS'16

Repeat dialing

Phone number-Temporary ID mapping

- Traffic analysis to find the same TMSI (Kune *et al.* NDSS'12)
  - Find intersects of identifier's sets



- Using "Silent Call"
  - Terminating call before ringing
- Same vulnerability in LTE - unchanged GUTI (Shaik *et al.* 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?

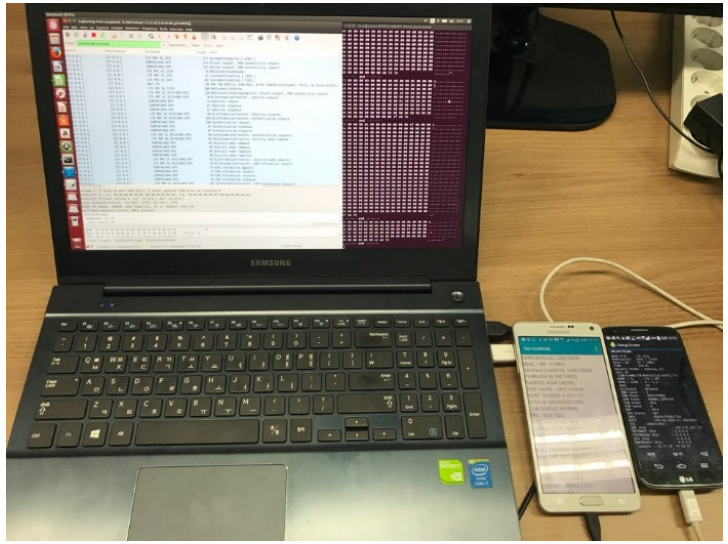
A. It is Yes

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

Experiment Setup

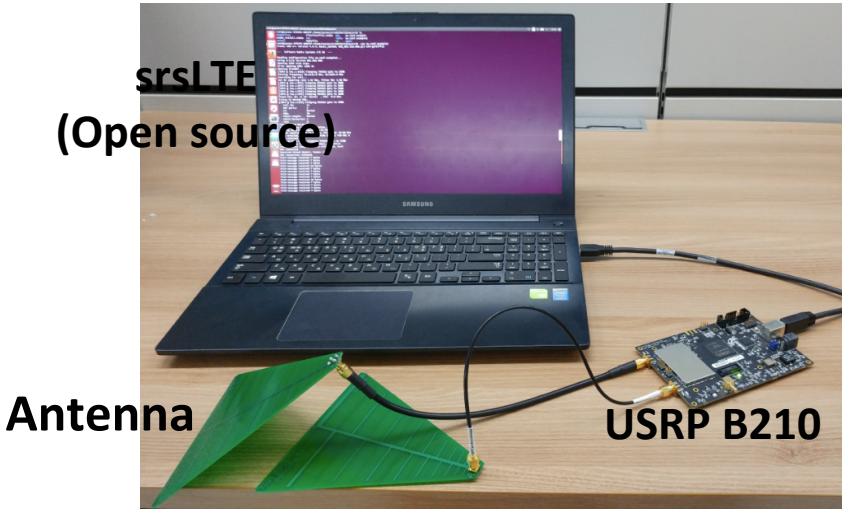
Device Analysis

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!!

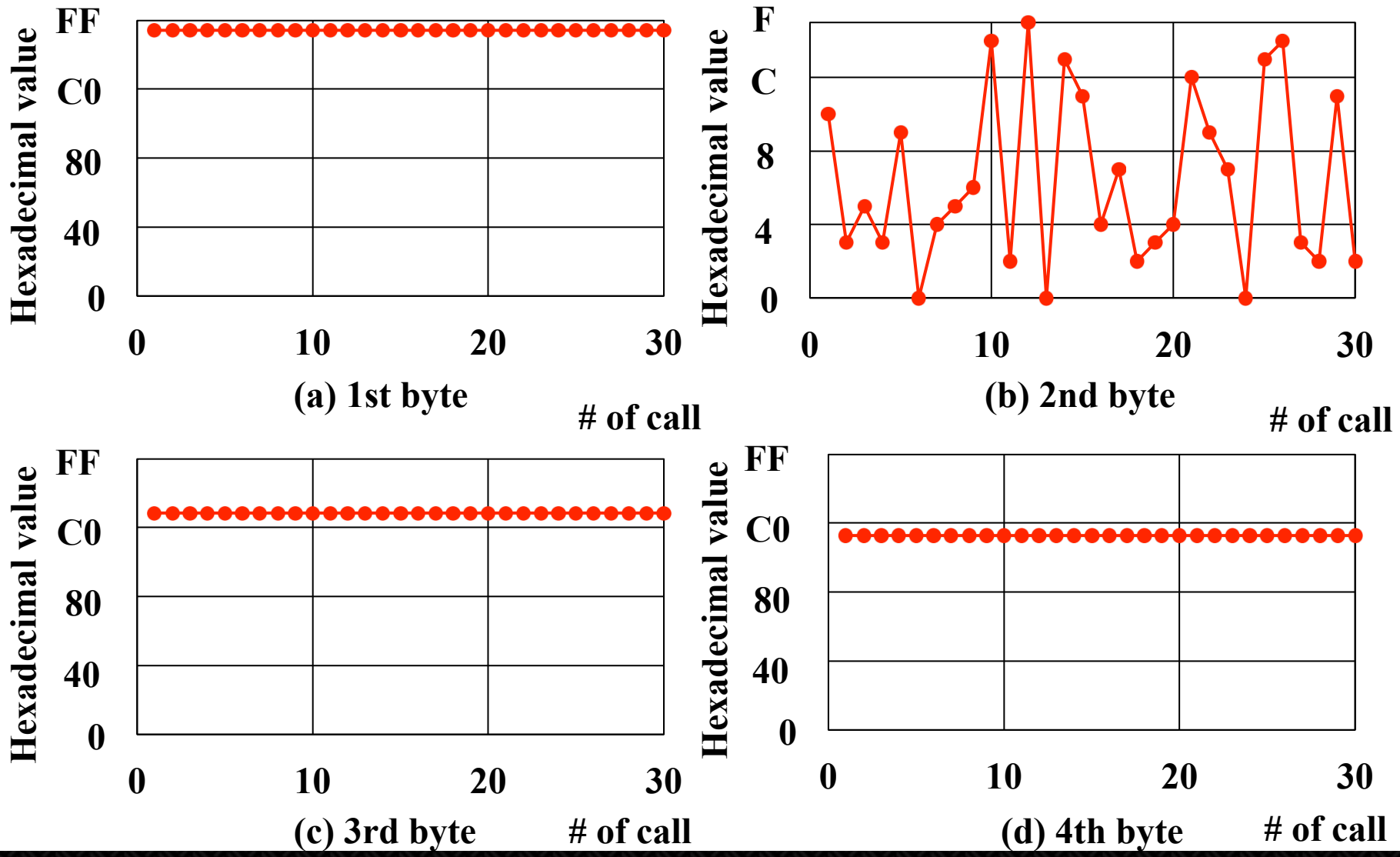
Fixed Bytes in *GUTI Reallocation*

- 19 operators have fixed bytes

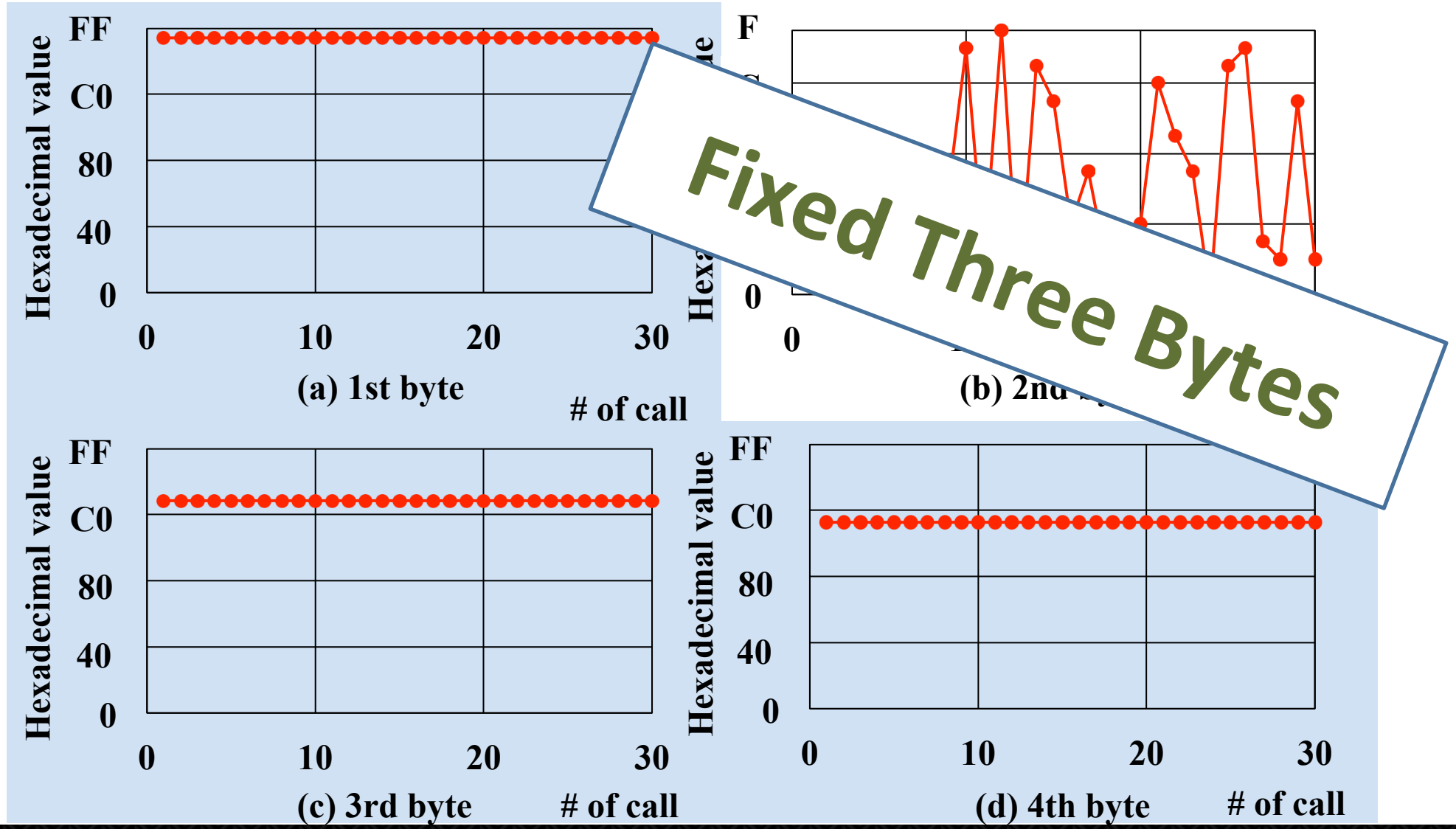
Allocation Pattern	Operators
Assigning the same GUTI	BE-III, DE-II, FR-II, JP-I
Three bytes fixed	CH-II, DE-III, NL-I, NL-II
Two bytes fixed	BE-II, CH-I, CH-III, ES-I, FR-I, NL-III
One bytes fixed	AT-I, AT-II, AT-III, BE-I, DE-I

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

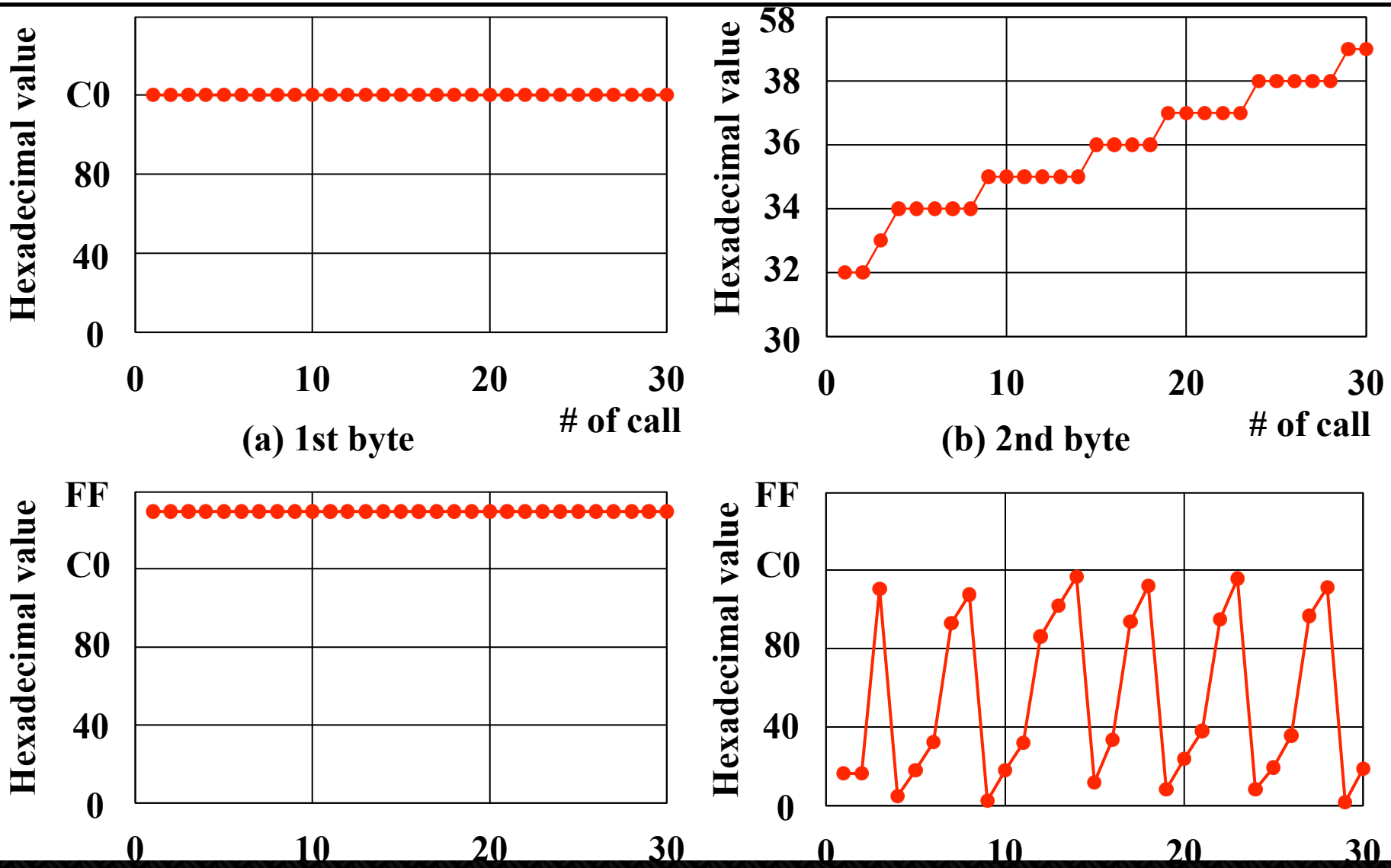
Case I: Netherlands (NL-I)



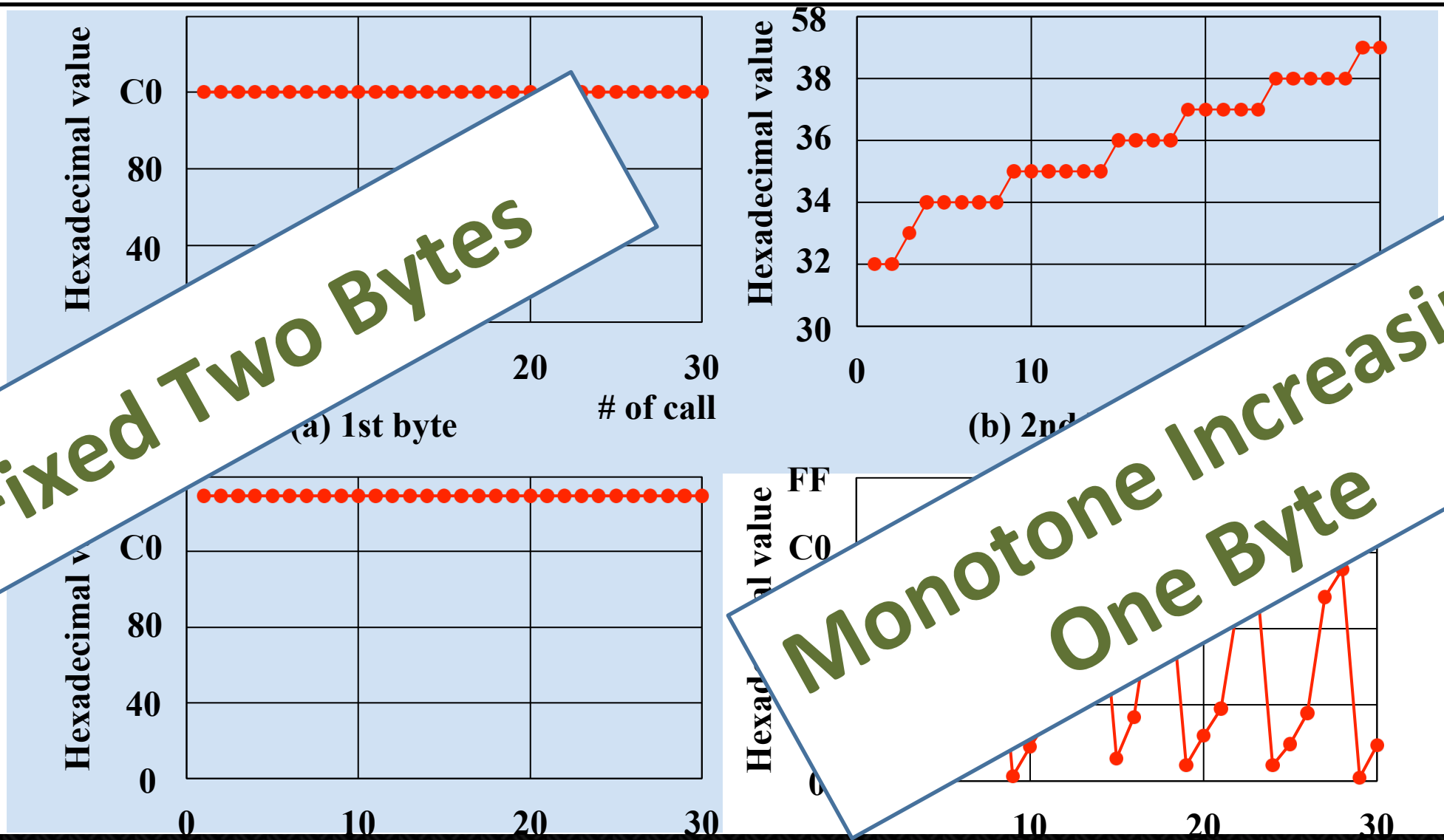
Case I: Netherlands (NL-I)



Case II: Belgium (BE-II)



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

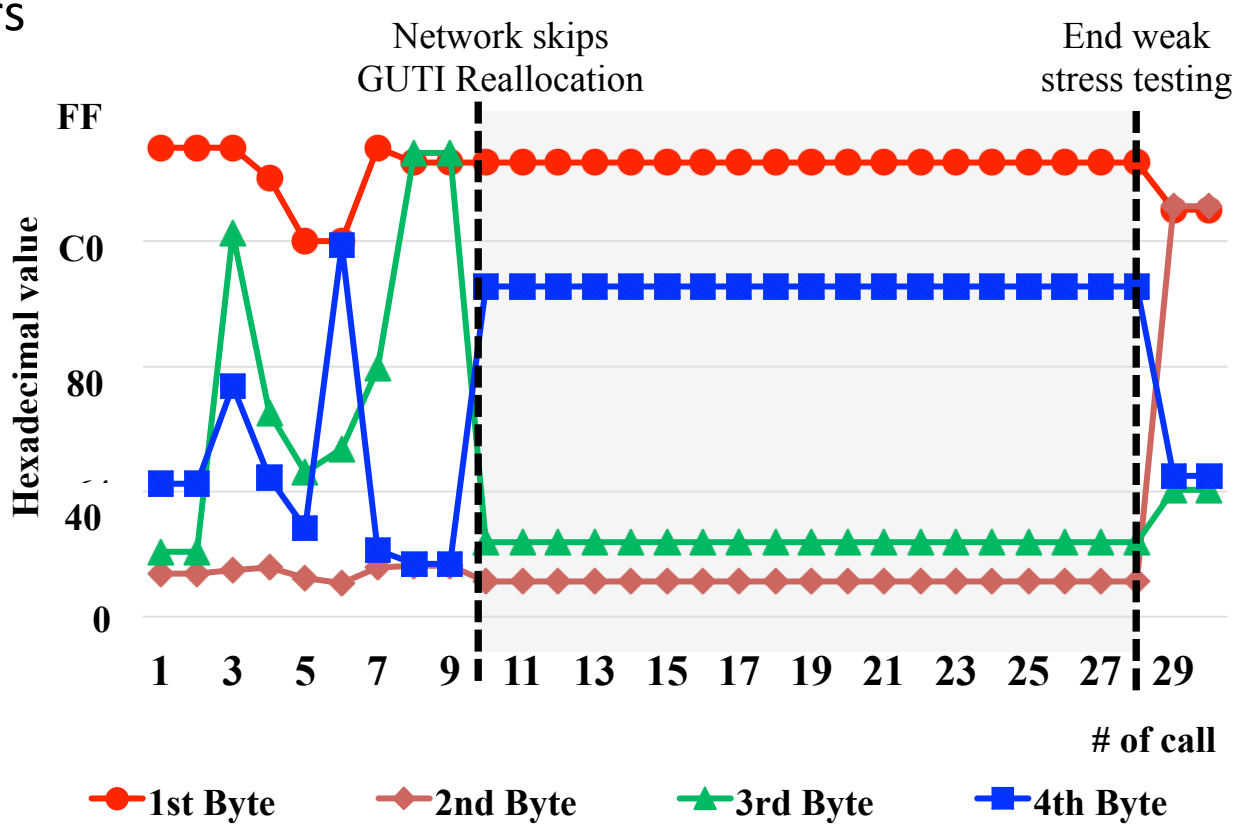
- Invoking voice call continuously with a short time
  - Two types of test
    - Weak stress testing
    - Hard stress testing
      - Calls at shorter intervals than weak stress test

Stress Testing Result

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

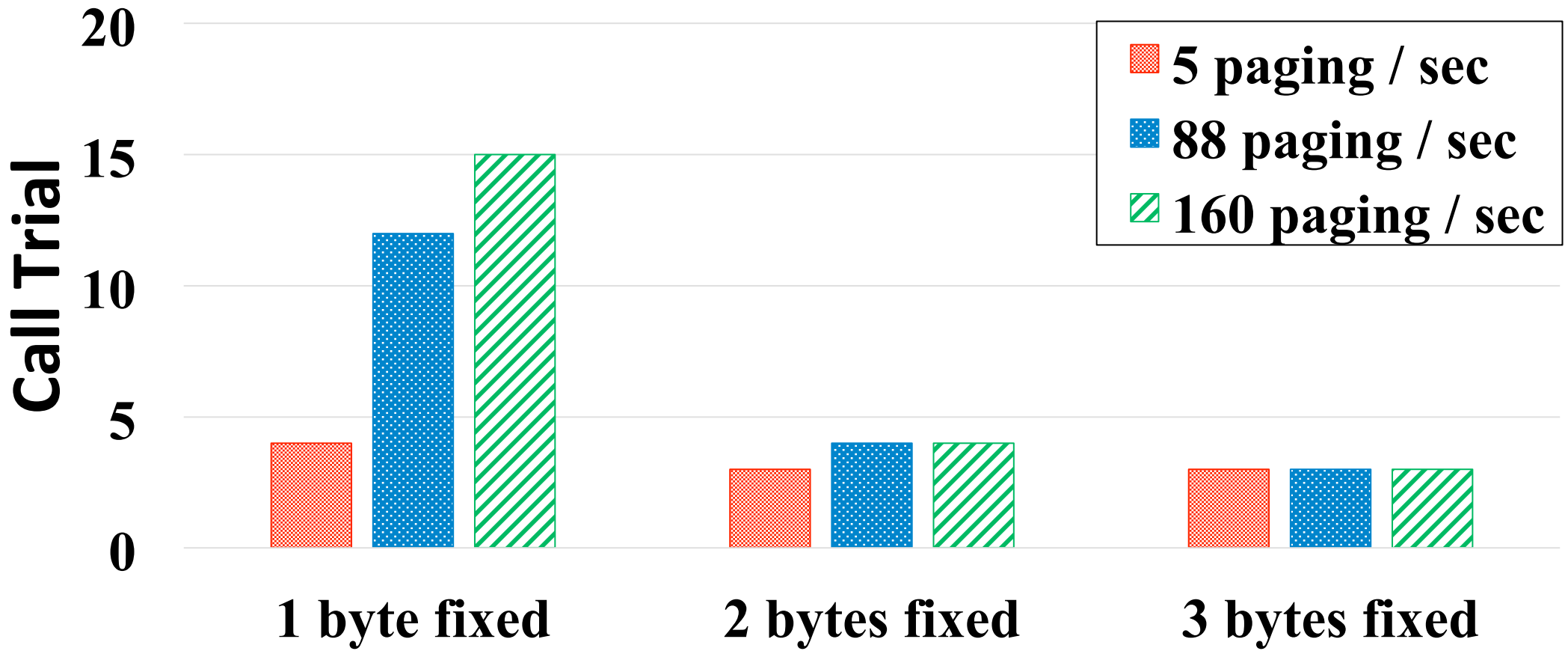
Operator	Weak Stress Testing	Hard Stress Testing
KR-I	O	O
KR-II	X	O
US-I	X	O
US-II	O	O

O: Reuse *GUTI*
X: No noticeable change



Success Rate of our Attack

❖ Required number of calls covering 99% success rate



Location Tracking with GUTI

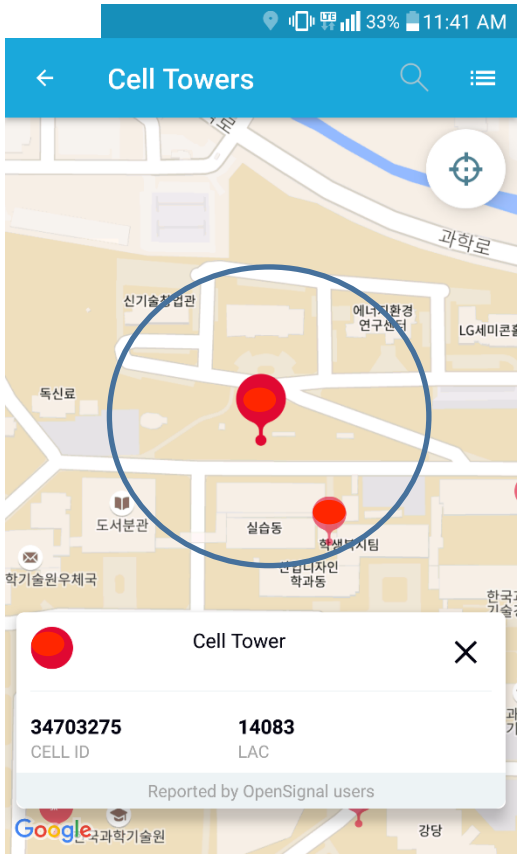
- Observation of broadcast channels after call invocation
  - Pattern matching (fixed bytes, assigning same GUTI)
  - Location tracking (Tracking Area, Cell)

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)



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

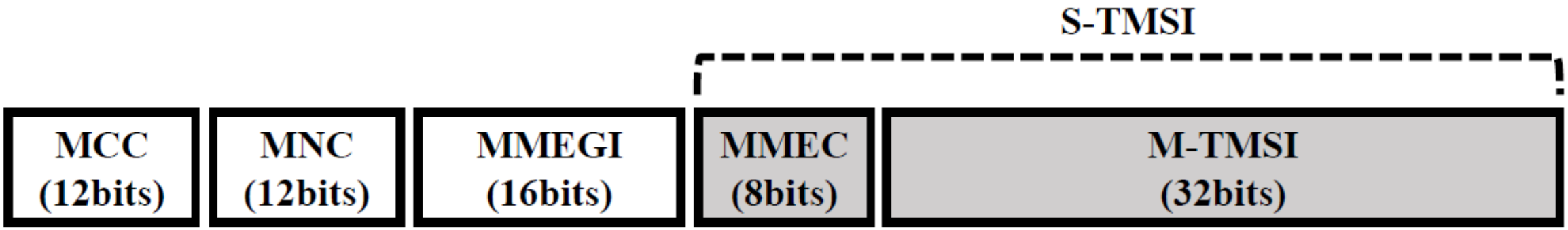
- Location tracking is still possible in cellular network!
- Secure GUTI reallocation mechanism is required

Thank you

Q & A

BACK UP SLIDES

GUTI Format



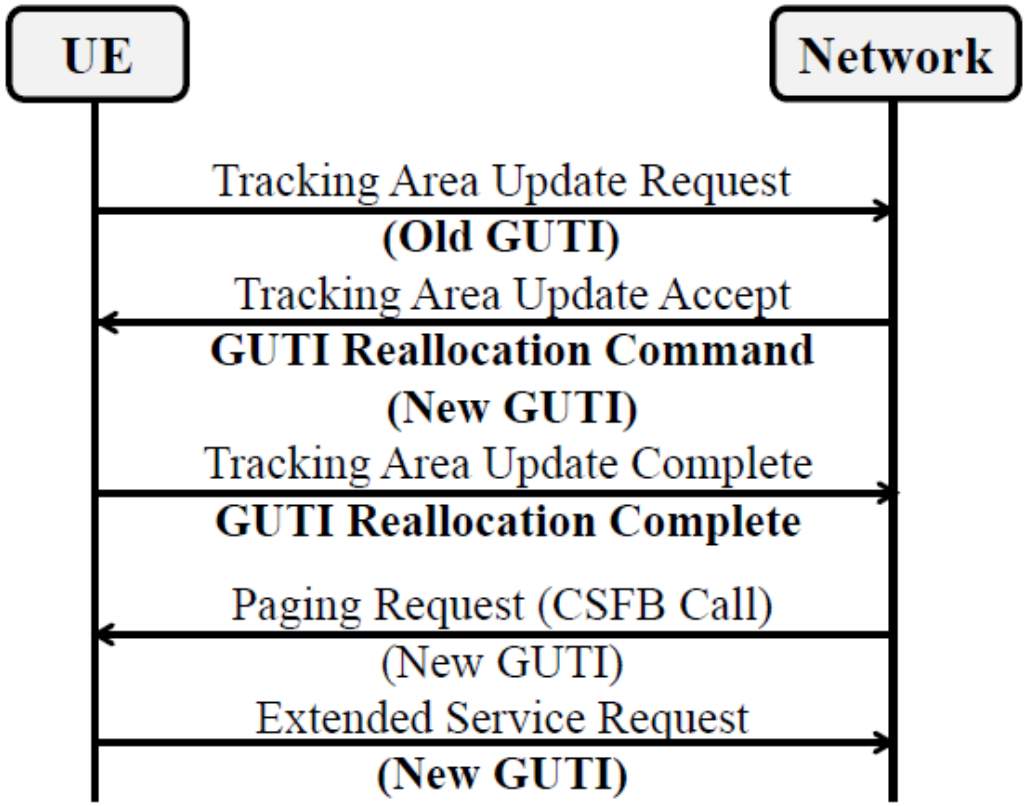
Dataset Release?

- Our dataset includes somewhat sensitive information.
  - Name of telcos ➔ Vulnerabilities can be linked to telcos.
  - Some IMSIs
- Not clear if releasing this dataset may cause any legal issues.

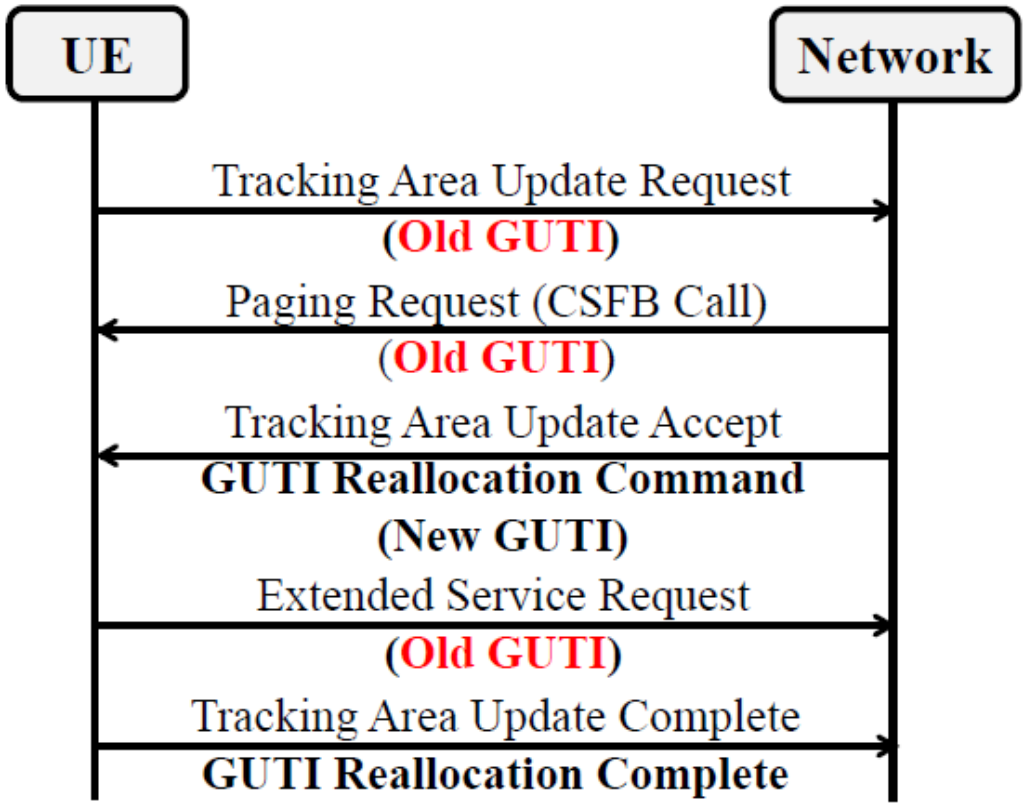
- B. Hong, et. al, “Peeking over the Cellular Walled Gardens - A Method for Closed Network Diagnosis -, IEEE Transactions on Mobile Computing.
  - Finding performance bugs by comparative analysis of call flows

- Should we build open-source dataset using crowdsourcing?
  - May help customers to push telcos to build secure and better cellular network!

Stress Testing Result: US-I



(a) Normal GUTI Reallocation with CSFB call

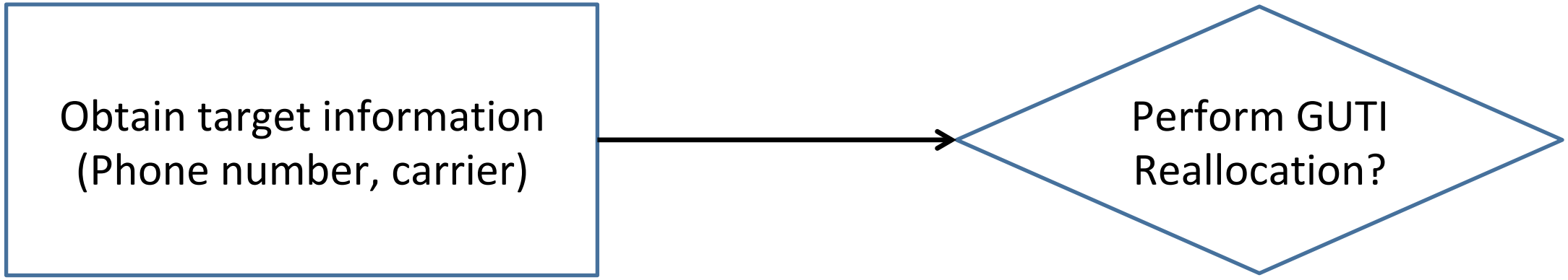


(b) GUTI Reallocation and CSFB call Collision

Probability with Fixed Bytes

$$
\begin{aligned}
Pr(\bigcap_{i=1}^{N-1} A_i \neq \emptyset) &= Pr(\bigvee_{a=0}^{2^{8k}-1} (a \in \bigcap_{i=1}^{N-1} A_i)) \\
&\leq \sum_{a=0}^{2^{8k}-1} Pr(a \in \bigcap_{i=1}^{N-1} A_i) \\
&= 2^{8k} Pr(a \in \bigcap_{i=1}^{N-1} A_i) \text{ for some } a \\
&= 2^{8k} \prod_{i=1}^{N-1} Pr(a \in A_i) \text{ for some a} \\
&= 2^{8k} \prod_{i=1}^{N-1} (1 - Pr(a \notin A_i)) \text{ for some a} \\
&= 2^{8k} \prod_{i=1}^{N-1} (1 - (\frac{2^{8k}-1}{2^{8k}})^t) \text{ for some a} \\
&= 2^{8k} (1 - (\frac{2^{8k}-1}{2^{8k}})^t)^{N-1}
\end{aligned}
$$

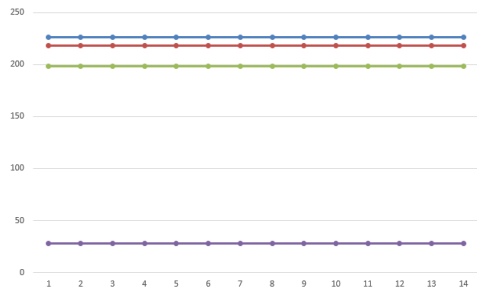
Attack Flow

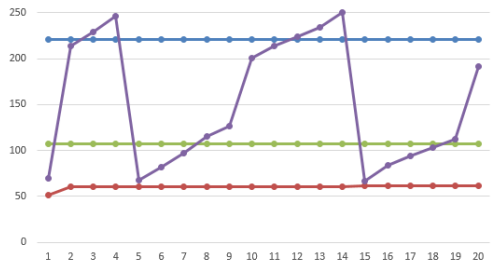

Obtain target information
(Phone number, carrier)
Perform GUTI
Reallocation?

Attack Flow

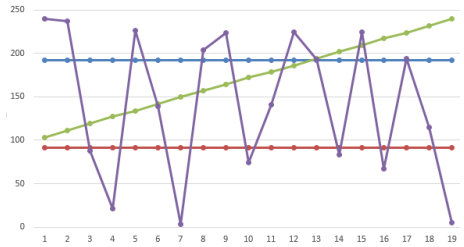
Perform GUTI Reallocation?

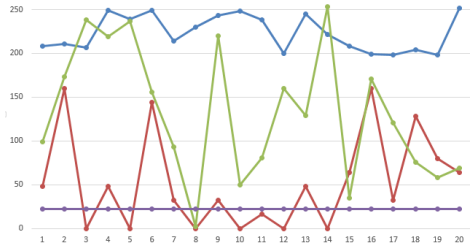
Yes





Analysis of rules for ID reallocation





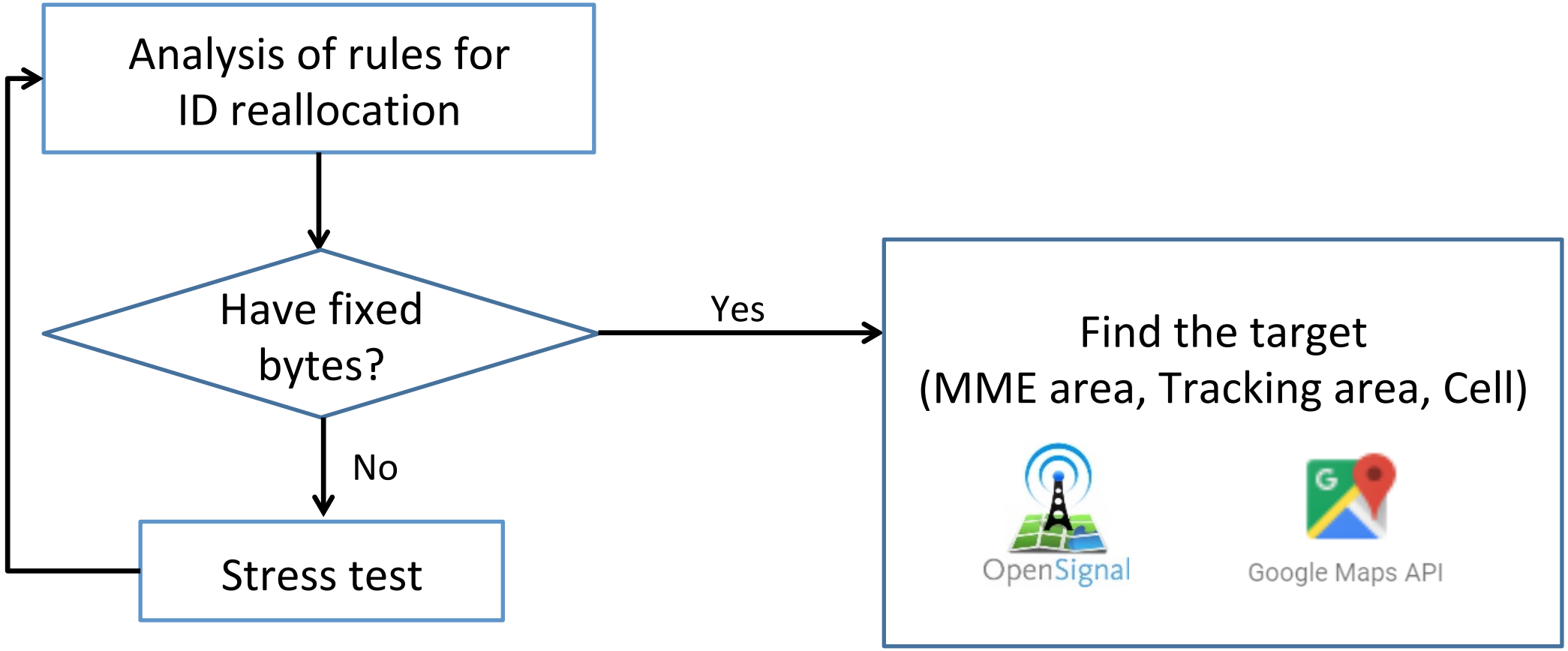
No

Find the target
(MME area, Tracking area, Cell)

OpenSignal

Google Maps API

Attack Flow



Paging Distribution in Korea (KR-I)