

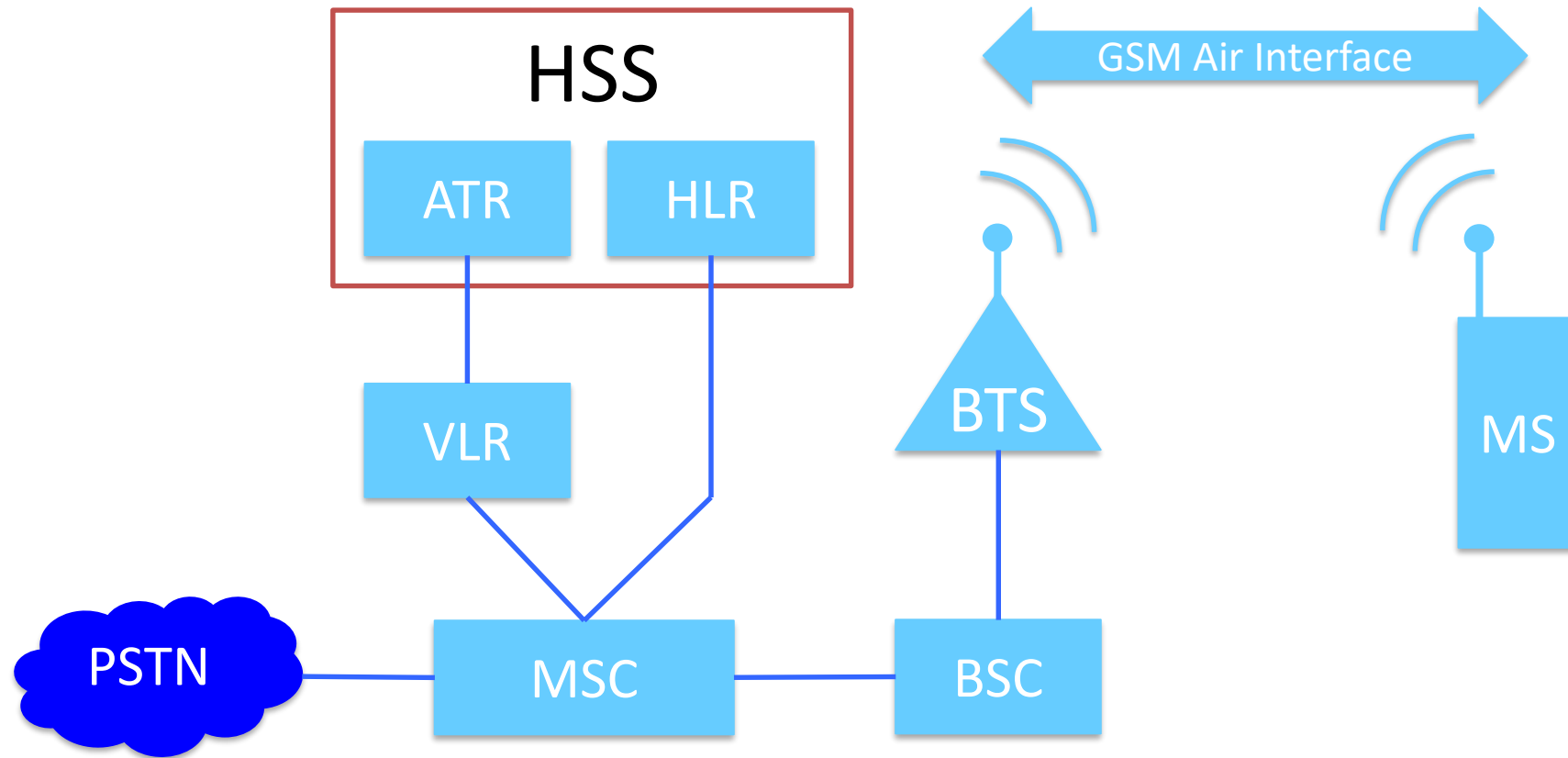
GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier

B. Hong, S. Bae, and Y. Kim
NDSS 2018

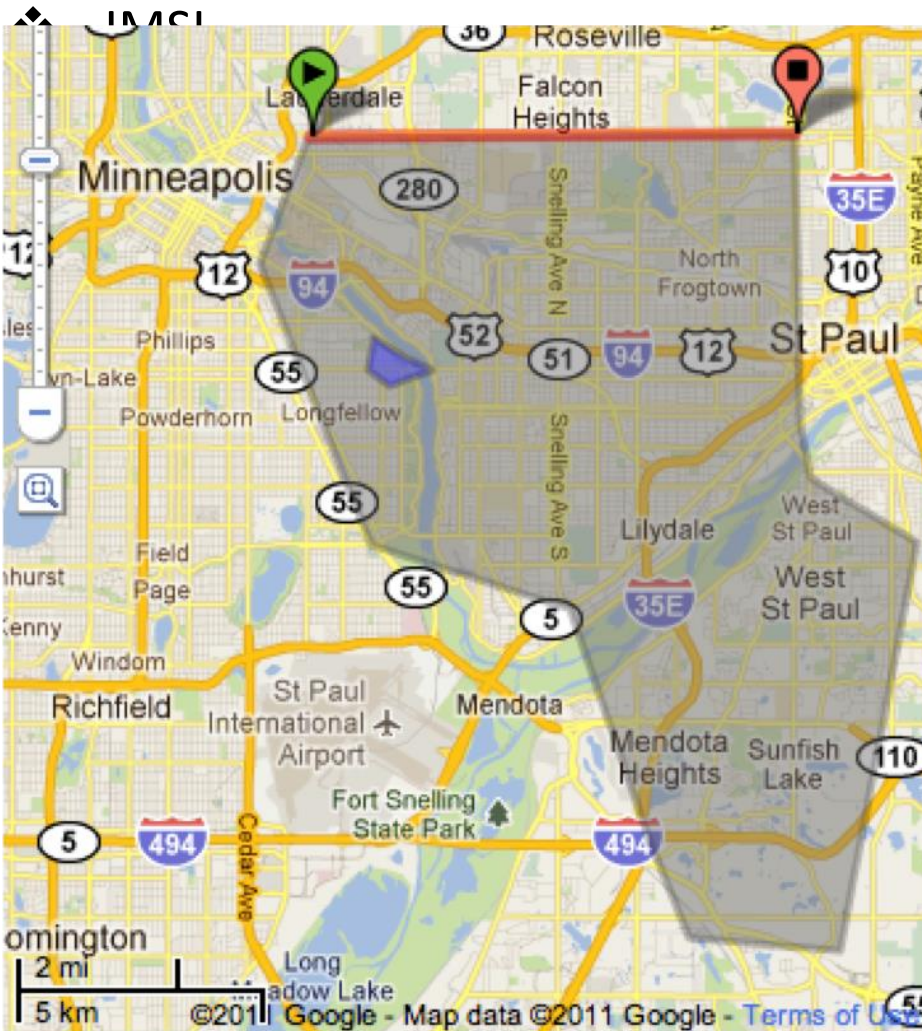
Location Privacy Leaks on GSM

- ❖ We have the victim's mobile phone number
- ❖ Can we detect if the victim is in/out of an area of interest?
 - Granularity? 100 km²? 1km²? 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

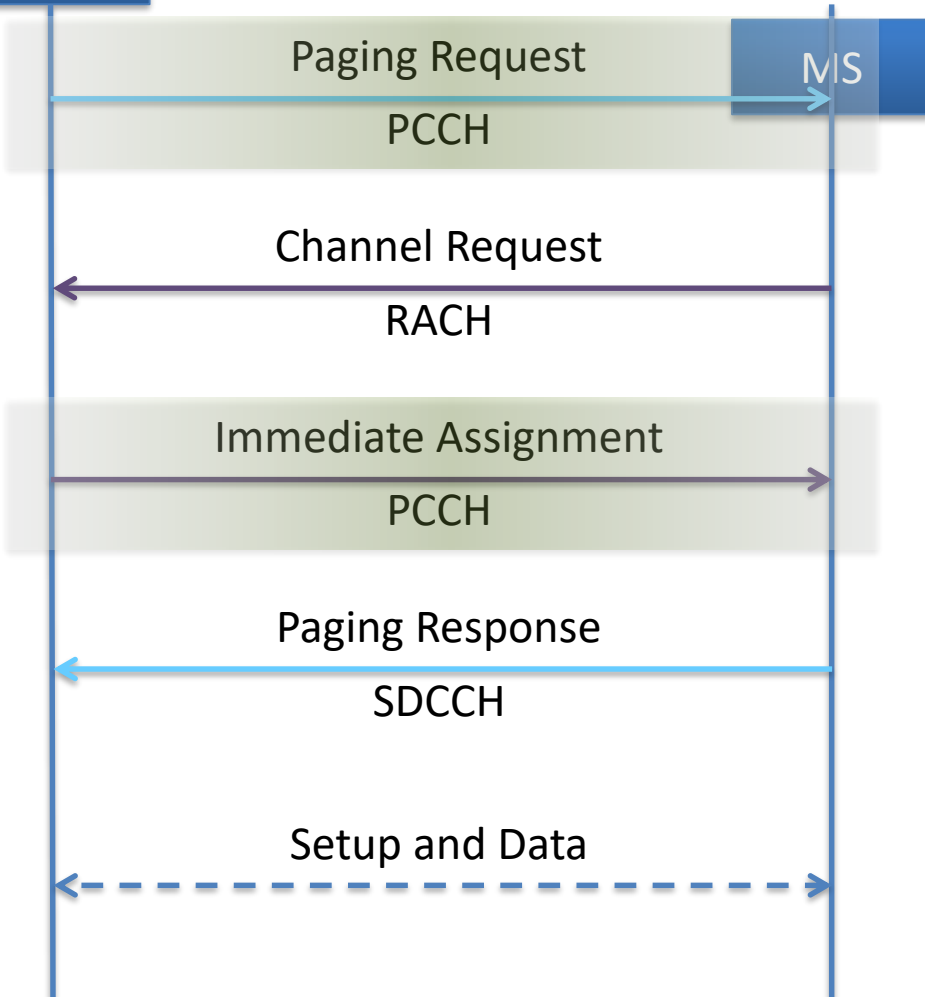
Cellular Network



Location Leaks on Cellular Network



BTS



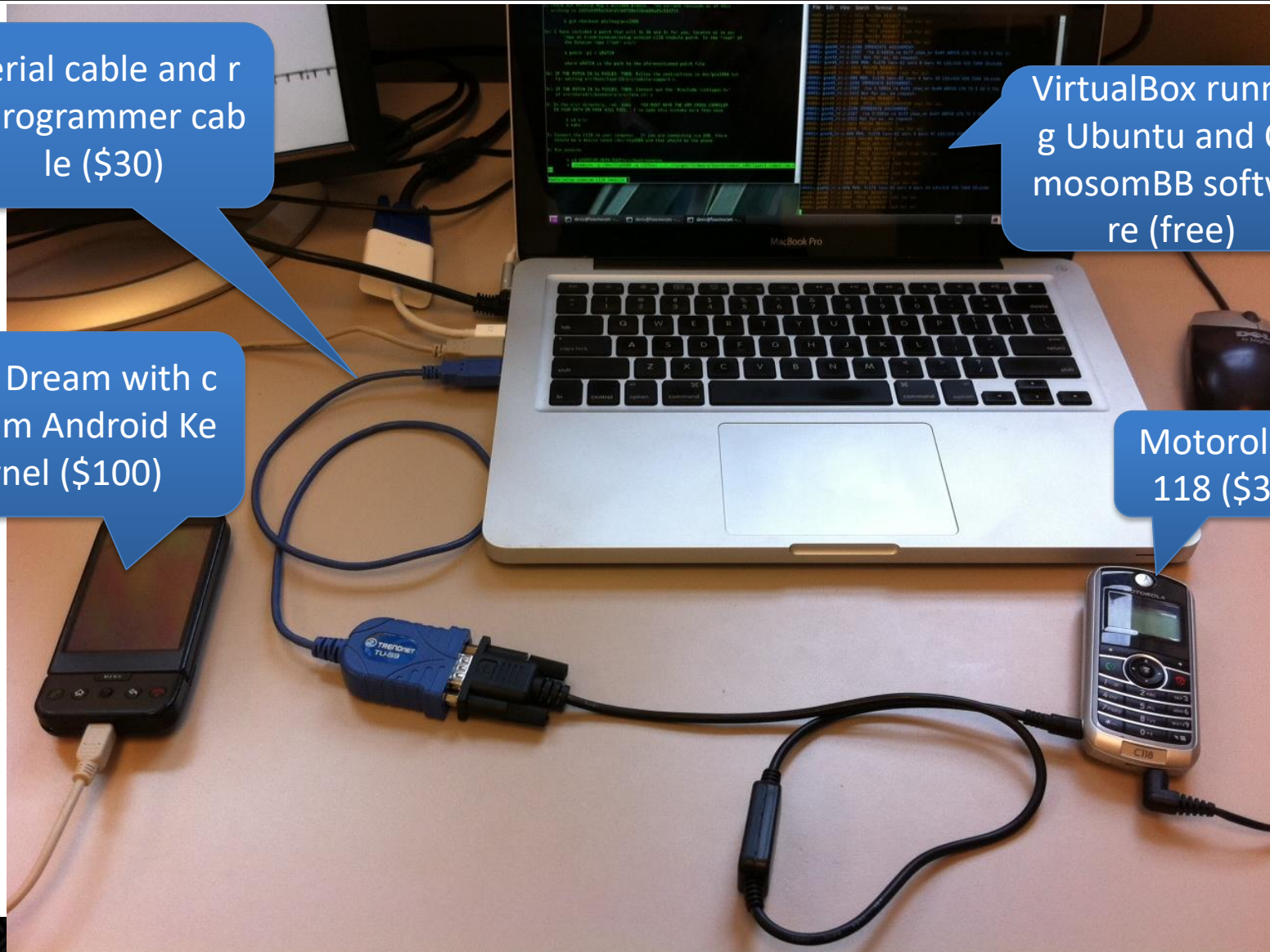
Platform

Serial cable and reprogrammer cable (\$30)

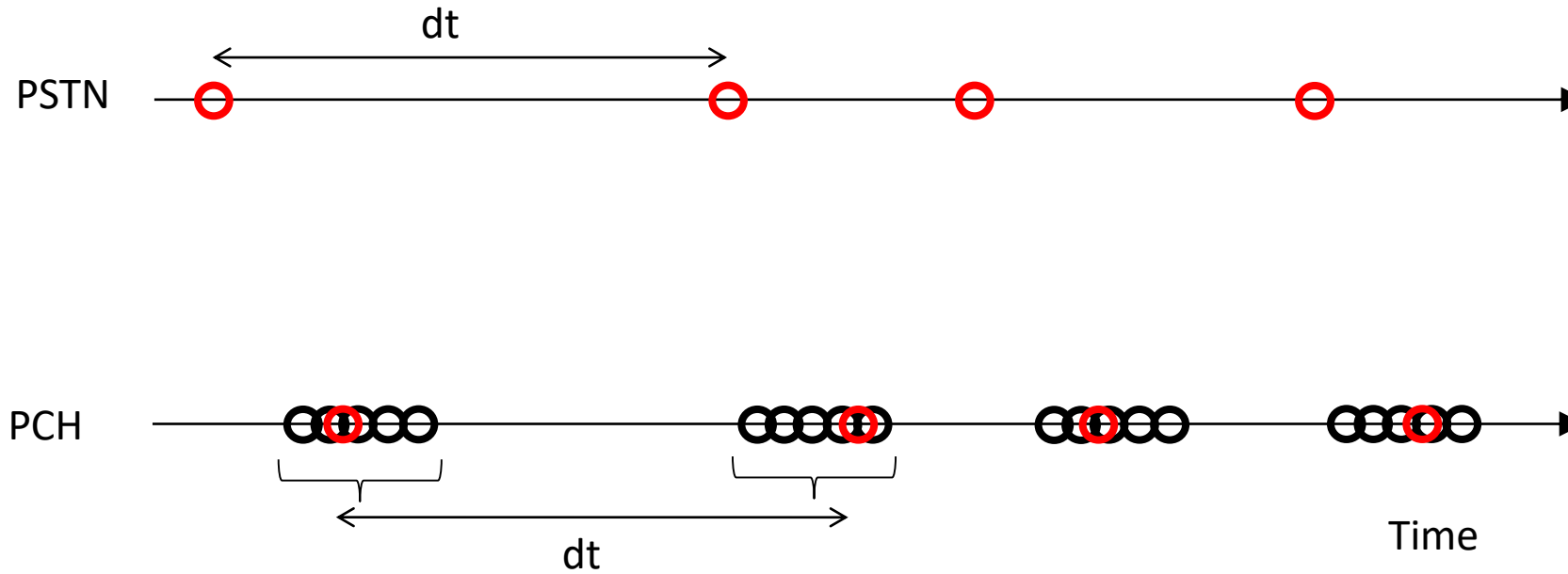
HTC Dream with custom Android Kernel (\$100)

VirtualBox running Ubuntu and OsmocomBB software (free)

Motorola C118 (\$30)

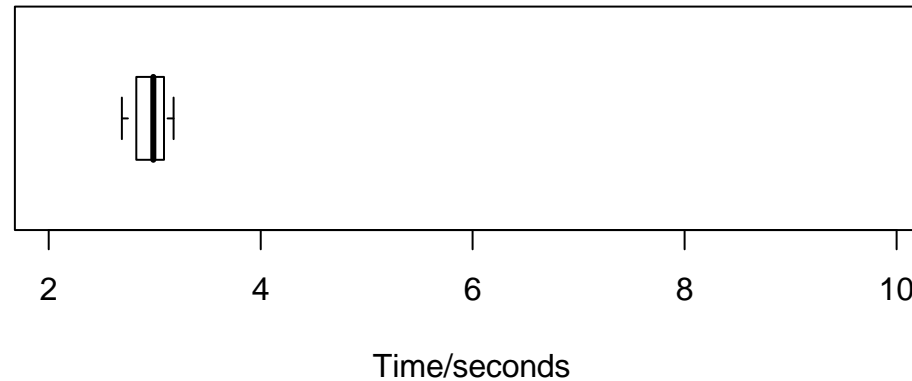


Phone number-TMSI mapping

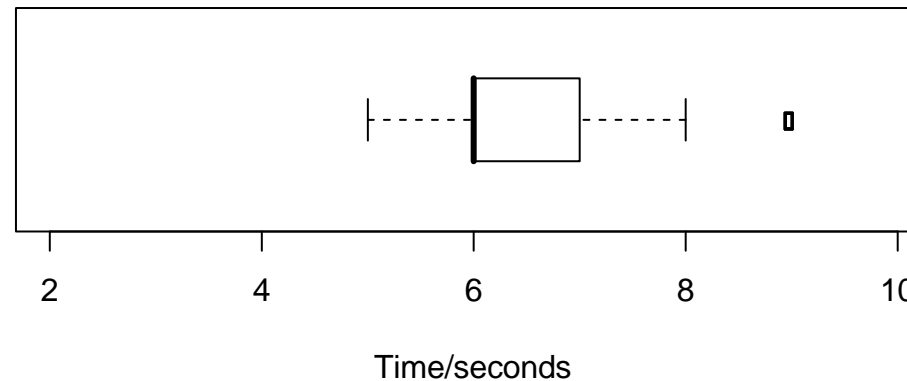


Silent Paging

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

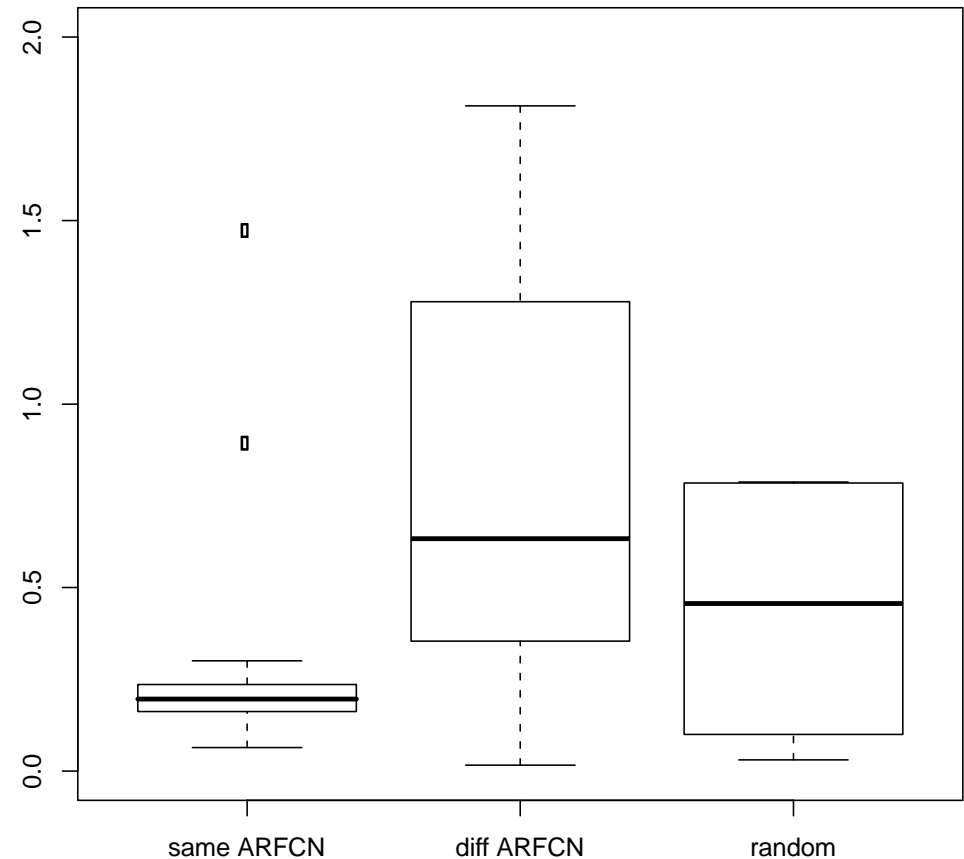


- Median delay between call initiation and ring: **6 sec**

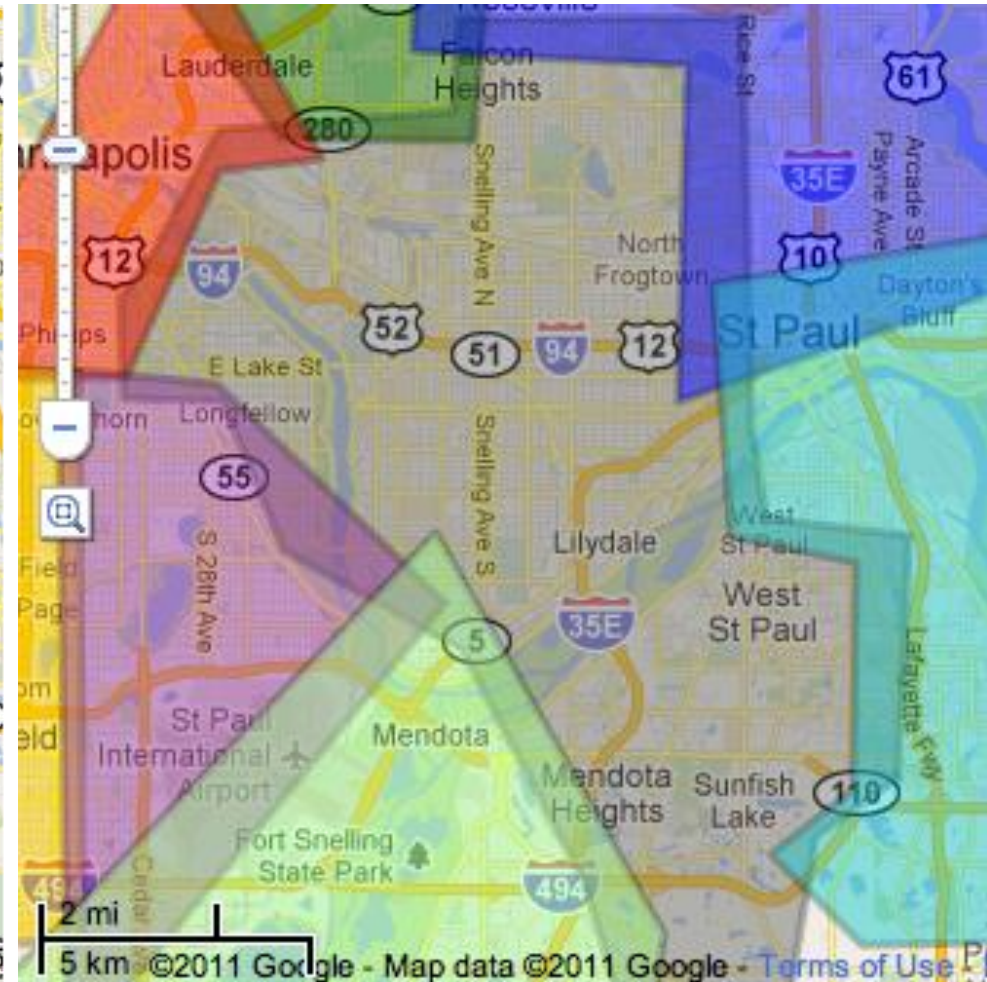
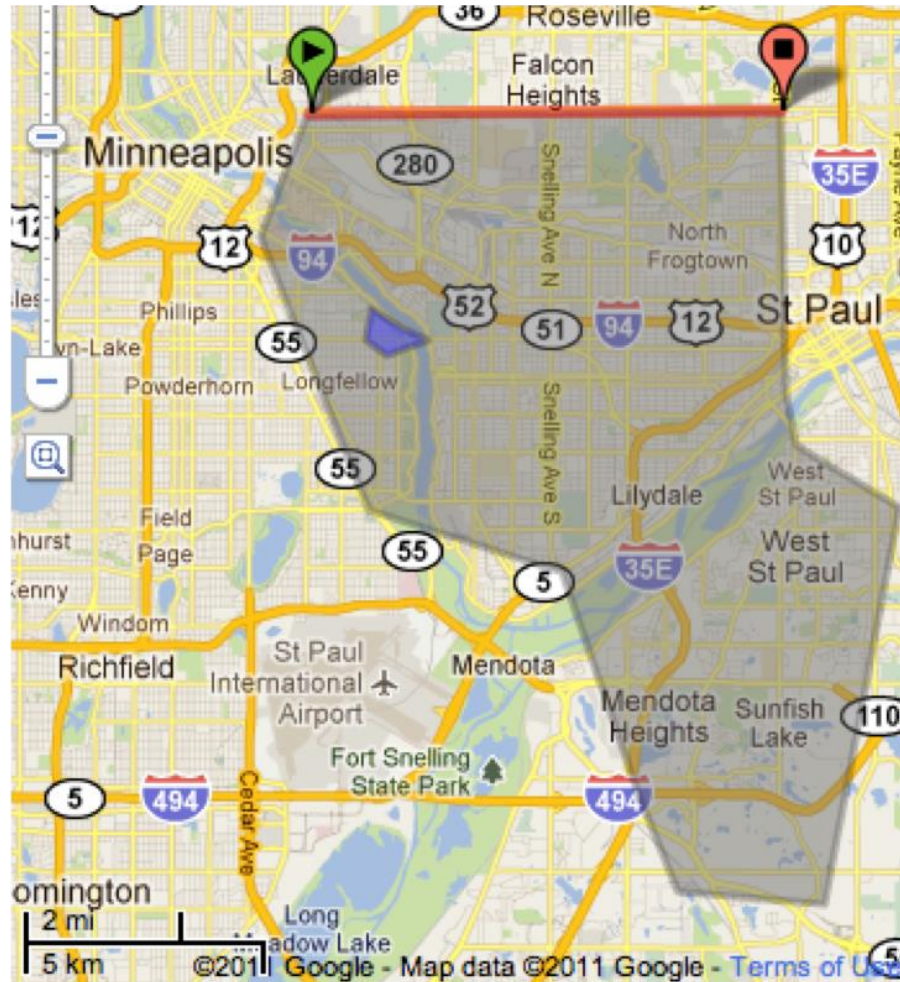


Immediate Assignment

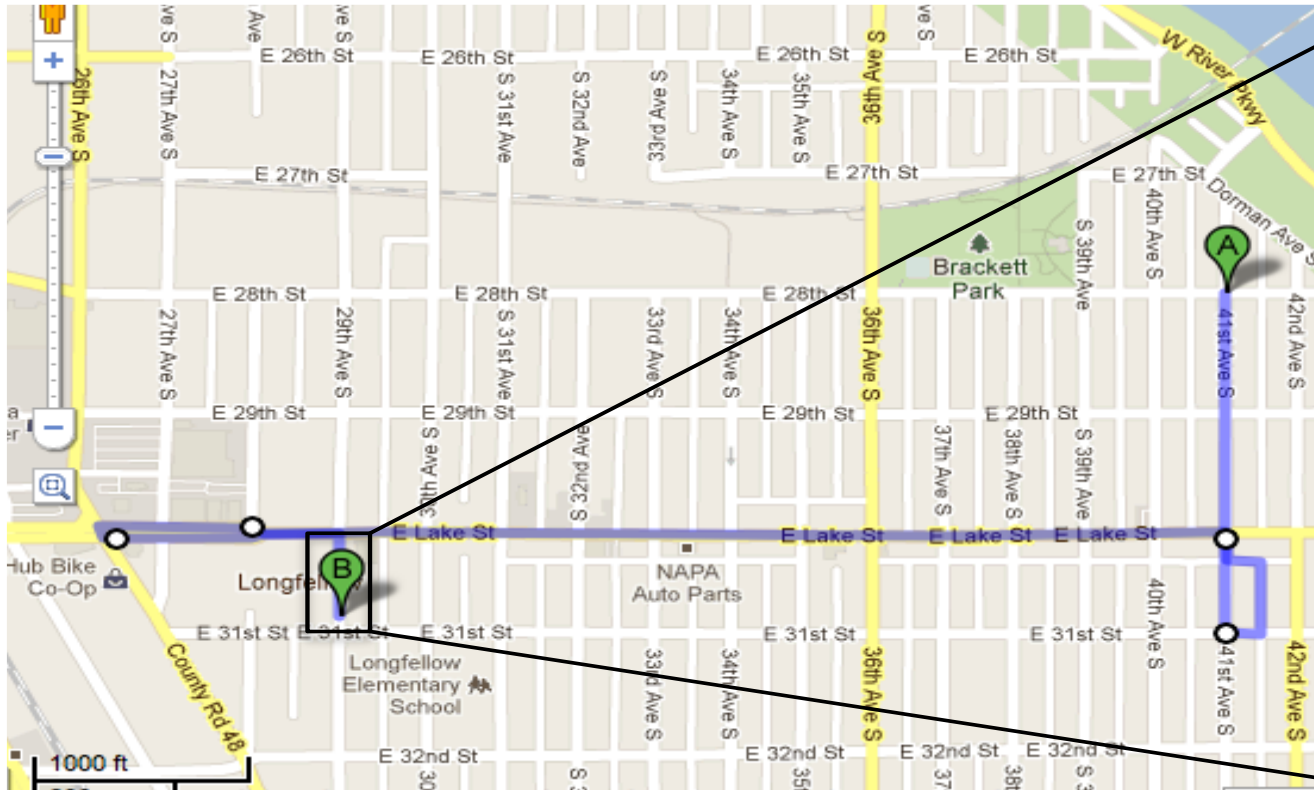
- ❖ Is IA message sent to all towers in the same LAC?
- ❖ How do we identify IA message?
 - No identifiable information
- ❖ Check the correlation between IA and Paging request



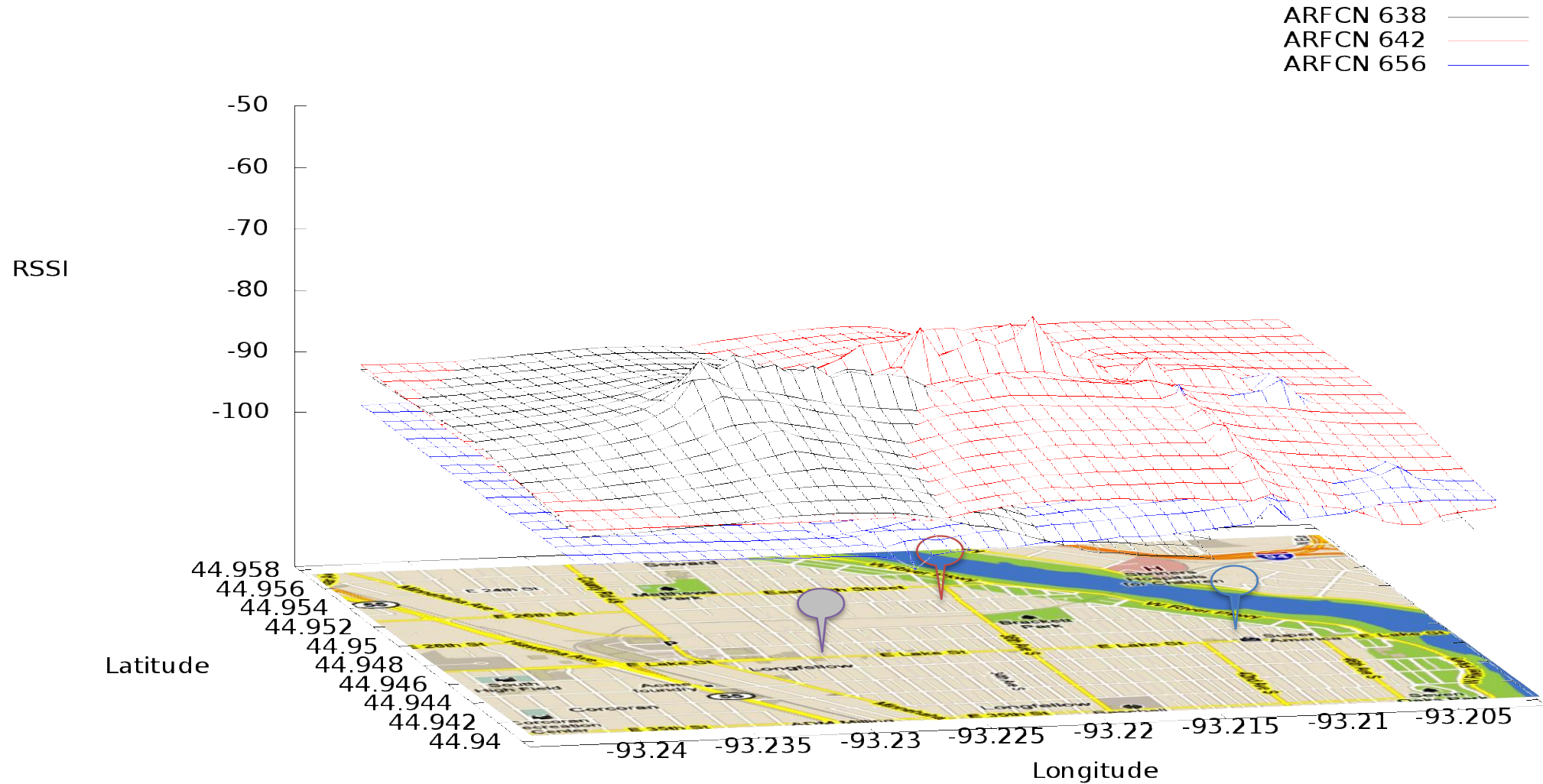
Location Area Code (LAC)



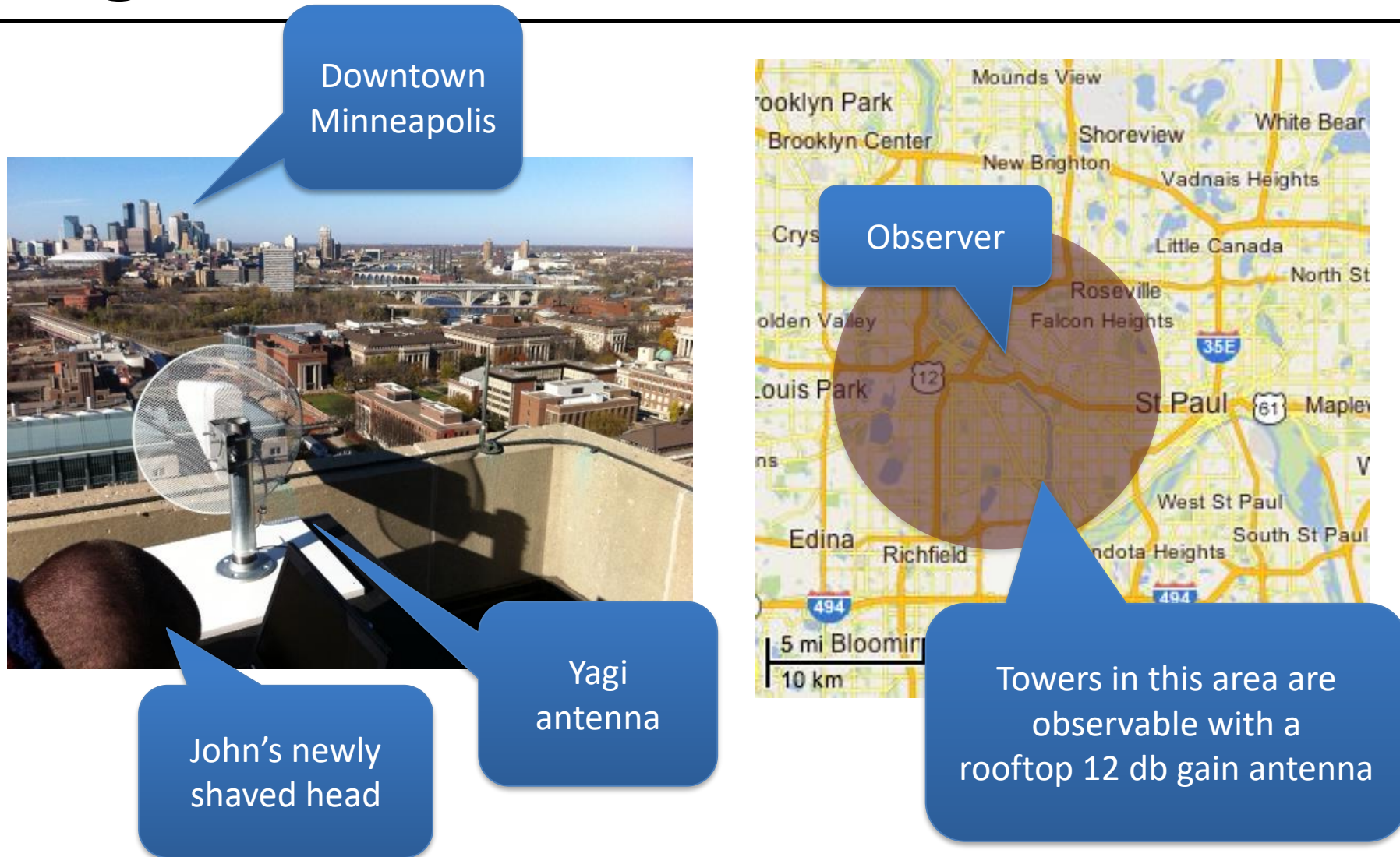
Hill Climbing to discover towers



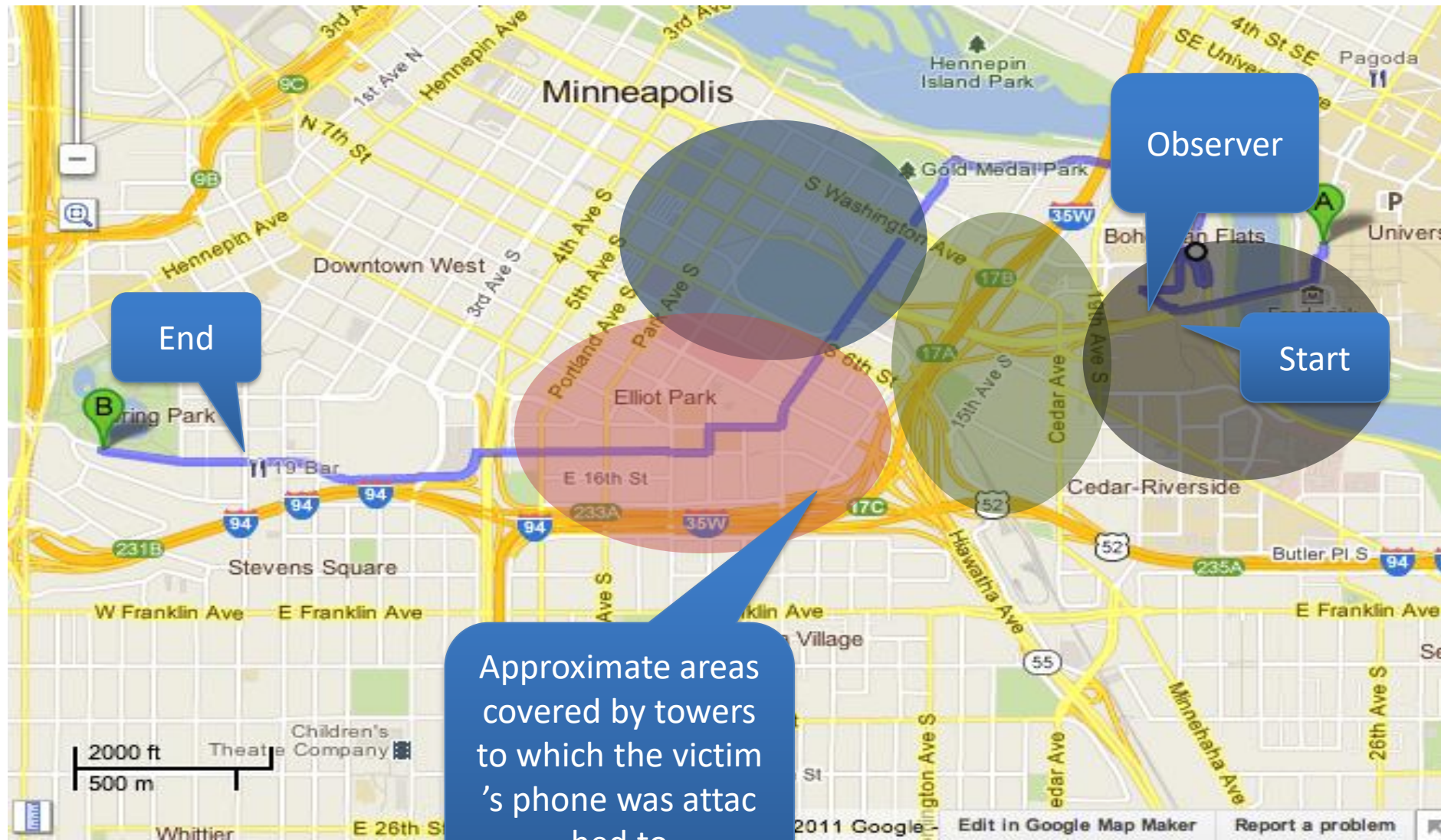
Mapping cell signal strength



Coverage area with 1 antenna



Following a walking person



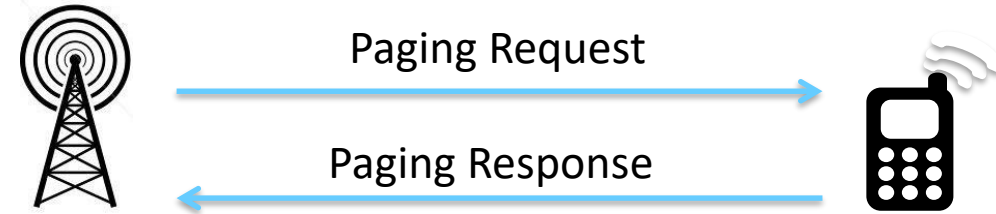
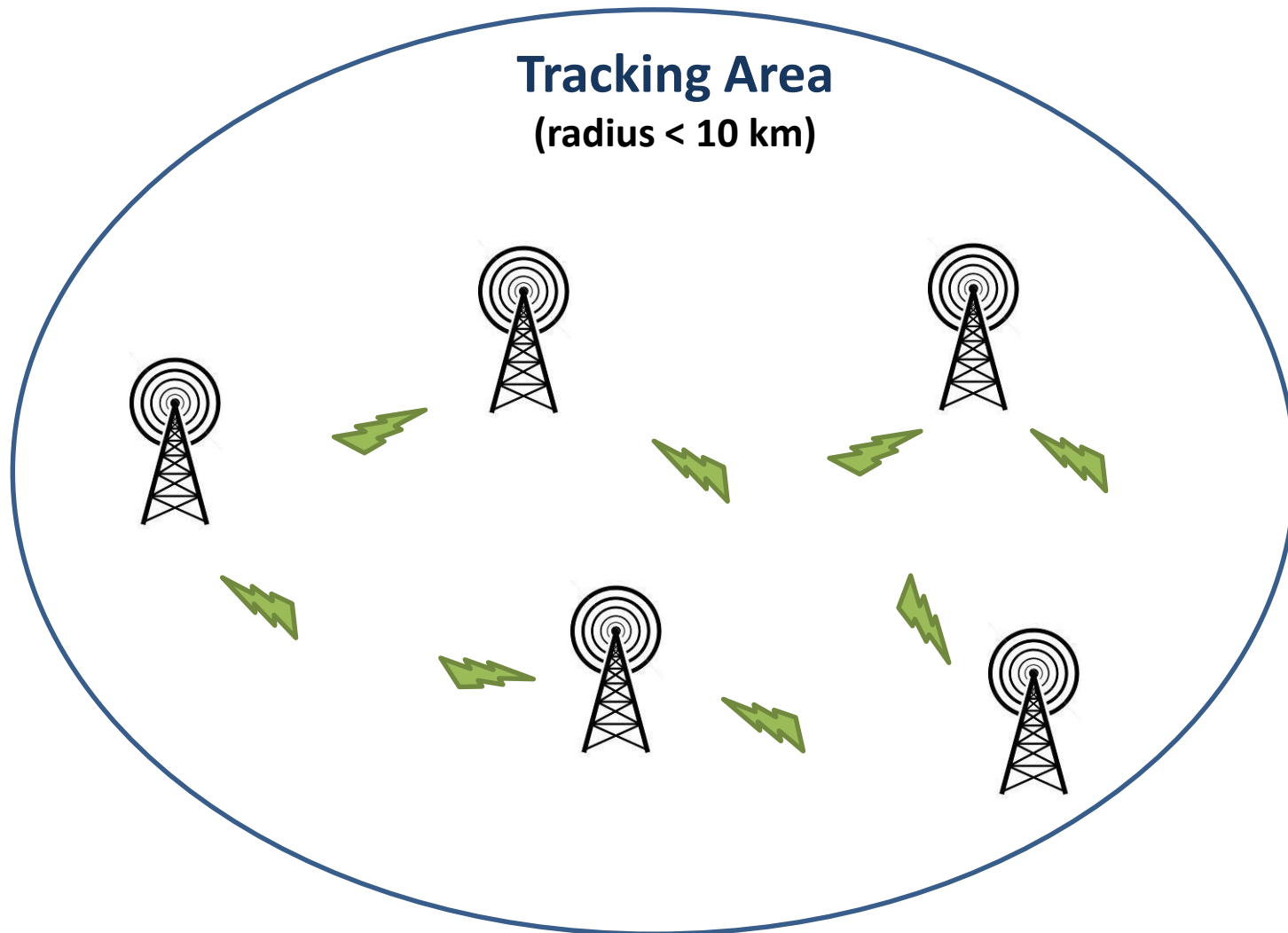
GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier

Byeongdo Hong, Sangwook Bae, Yongdae Kim

KAIST SysSec

Feb. 19, 2018

Paging Area in Cellular Network



Paging:

A method to find specific subscriber

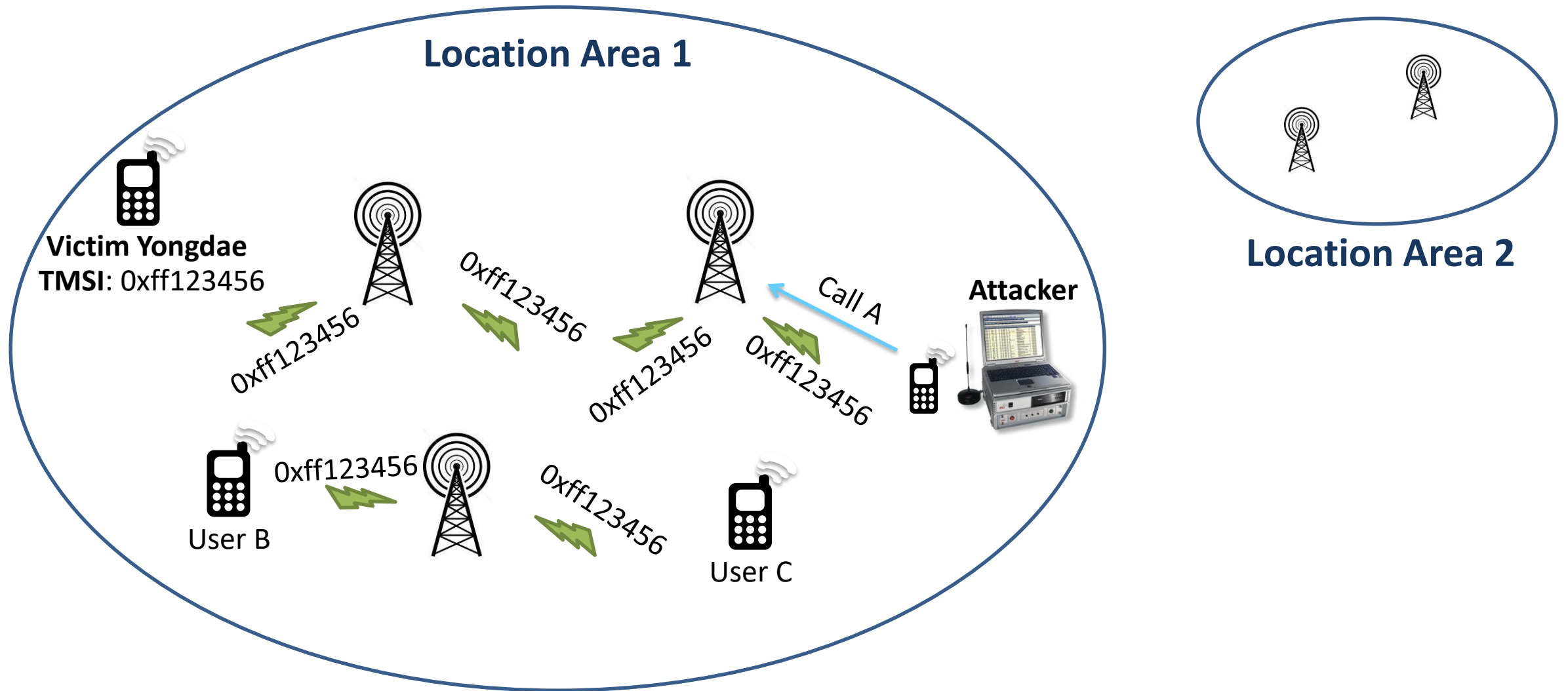
How?

By using subscriber's *identifier*

Identifiers in Cellular Networks

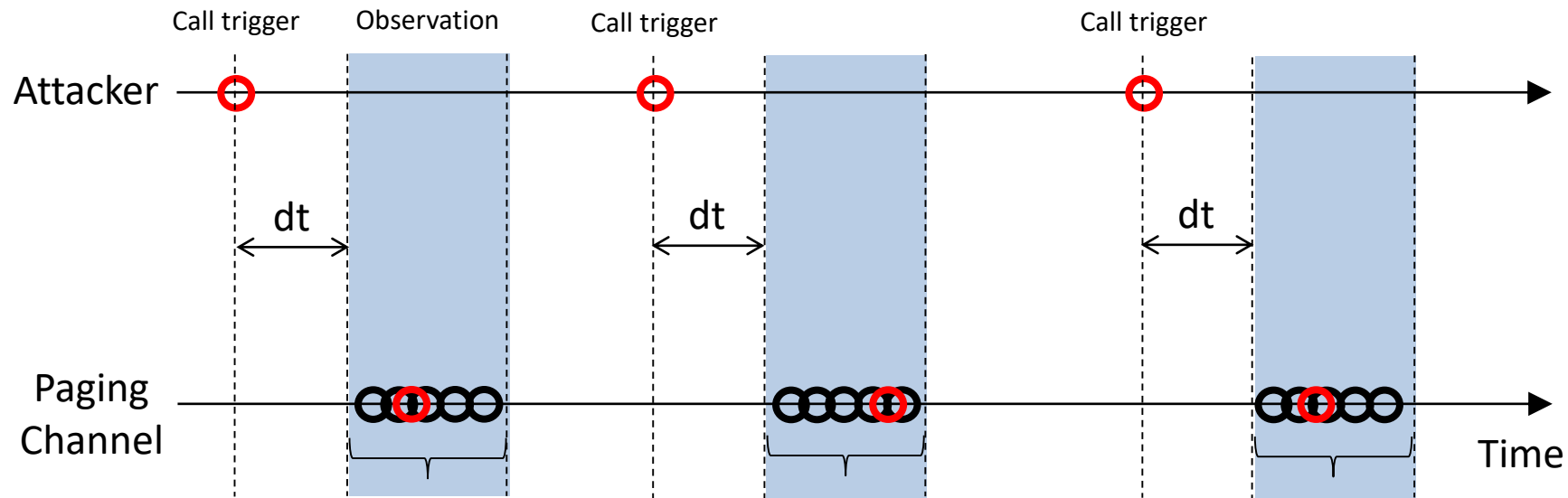
- ❖ Permanent/Unique identifier
 - IMSI (International Mobile Subscriber Identity)
 - Provisioned in the SIM card
- ❖ Temporary identifier
 - Used to **hide** subscriber
 - **TMSI** (Temporary Mobile Subscriber Identity)
 - Used in 2G/3G
 - **GUTI** (Globally Unique Temporary Identity)
 - Used in LTE

Location Tracking in Cellular Network



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

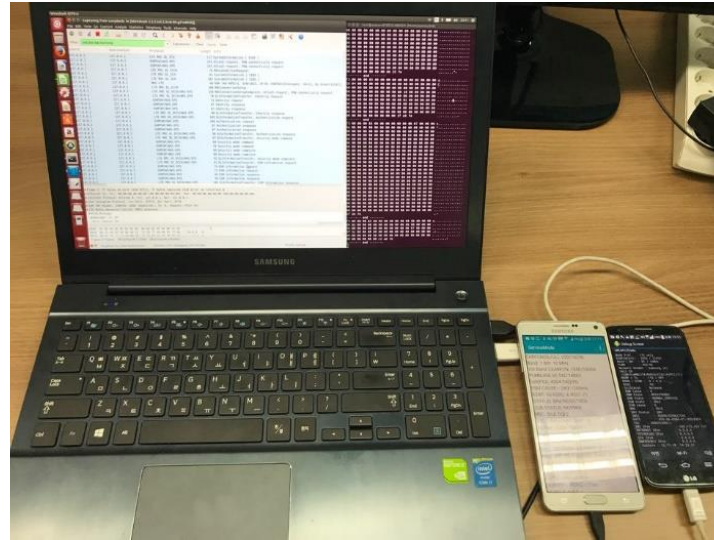
But **simply changing** is not a solution!

Experiment Setup

Device Analysis

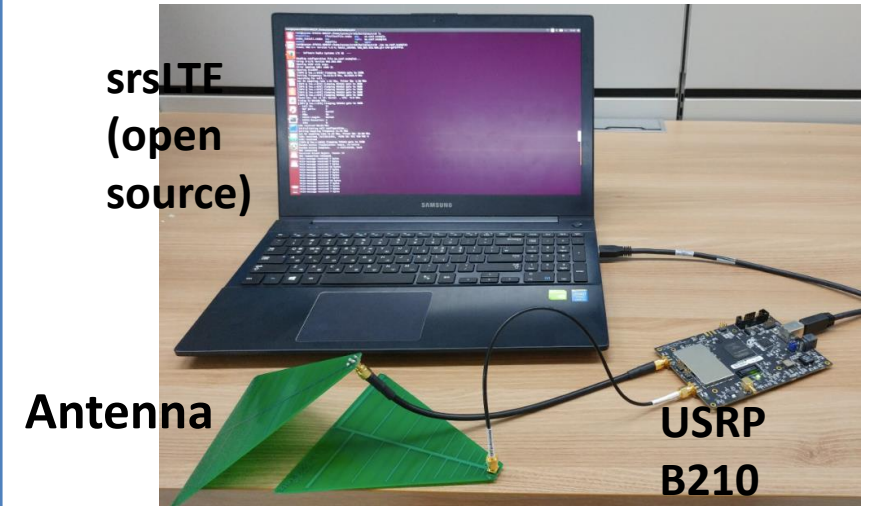


Diagnostic Monitor



Signaling Collection and Analysis Tool (SCAT) [1]

Broadcast Channel Analysis



srsLTE
(open
source)

Antenna

USRP
B210

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!!

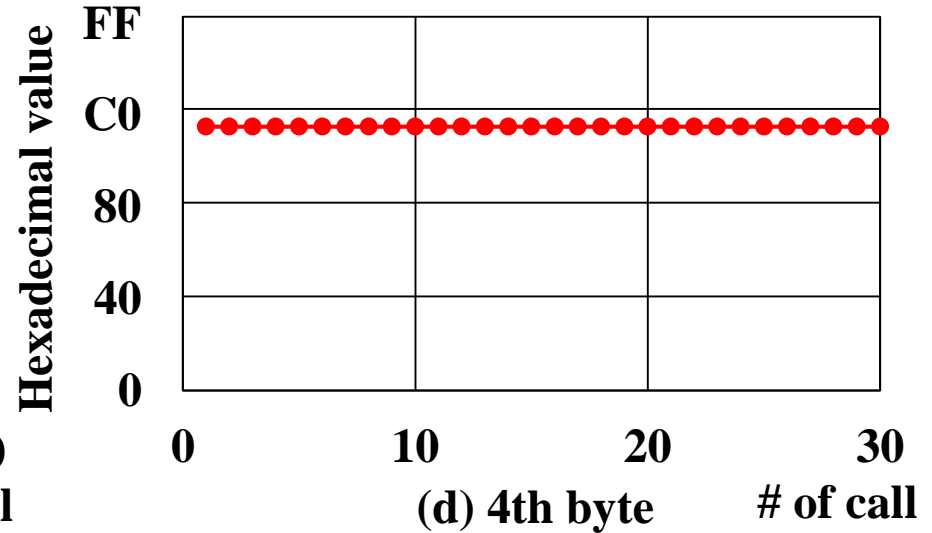
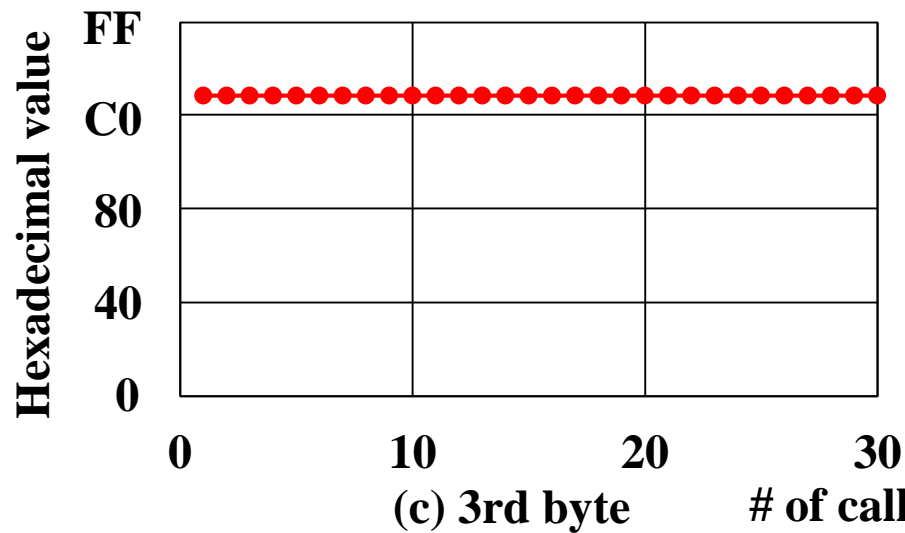
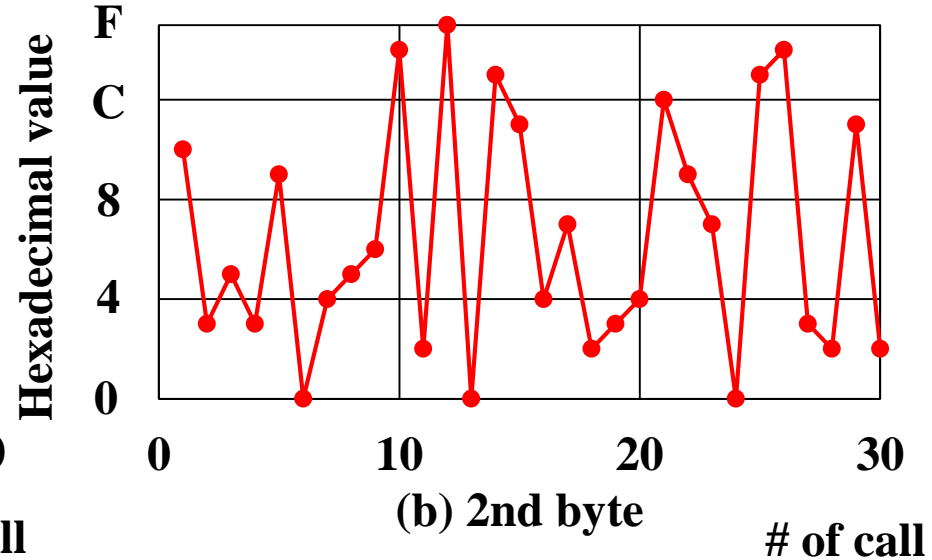
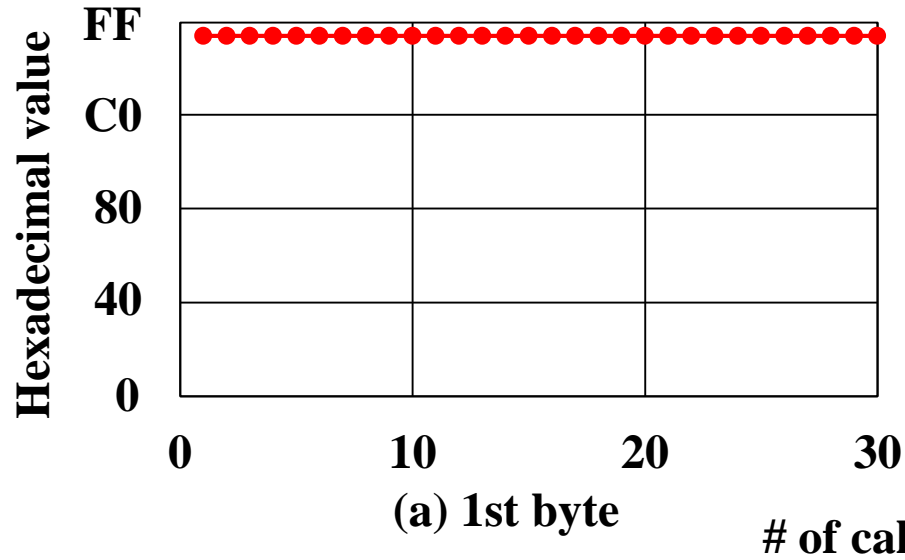
Fixed Bytes in *GUTI* Reallocation

- ❖ 19 operators have fixed bytes

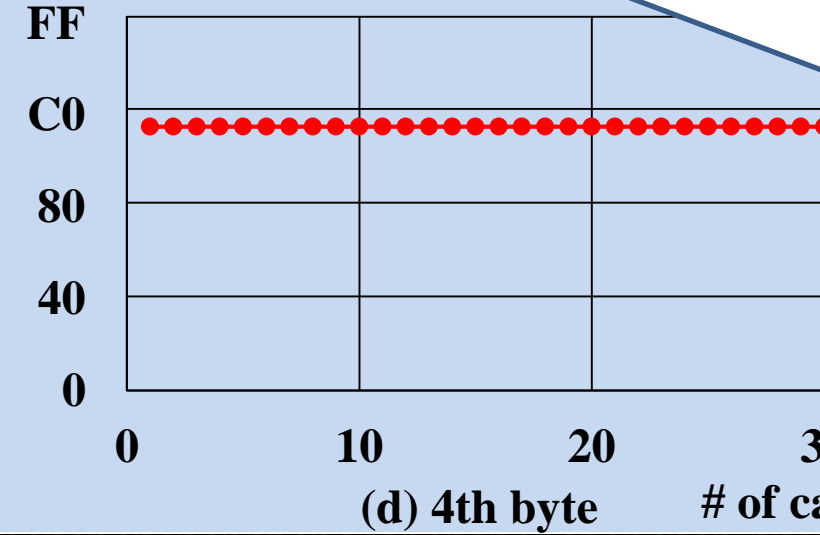
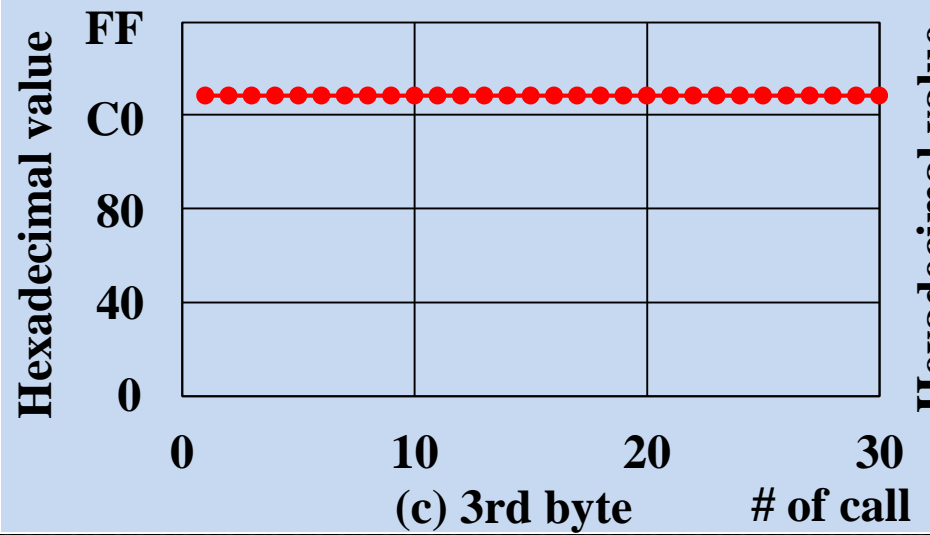
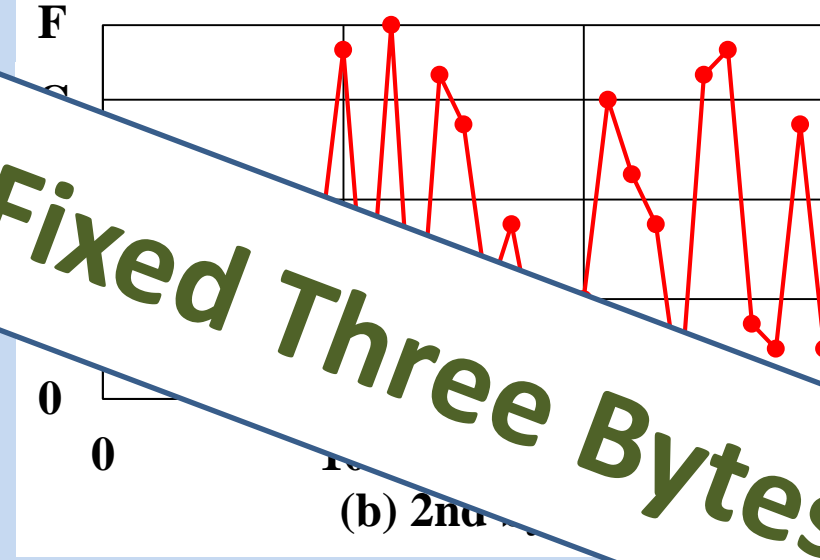
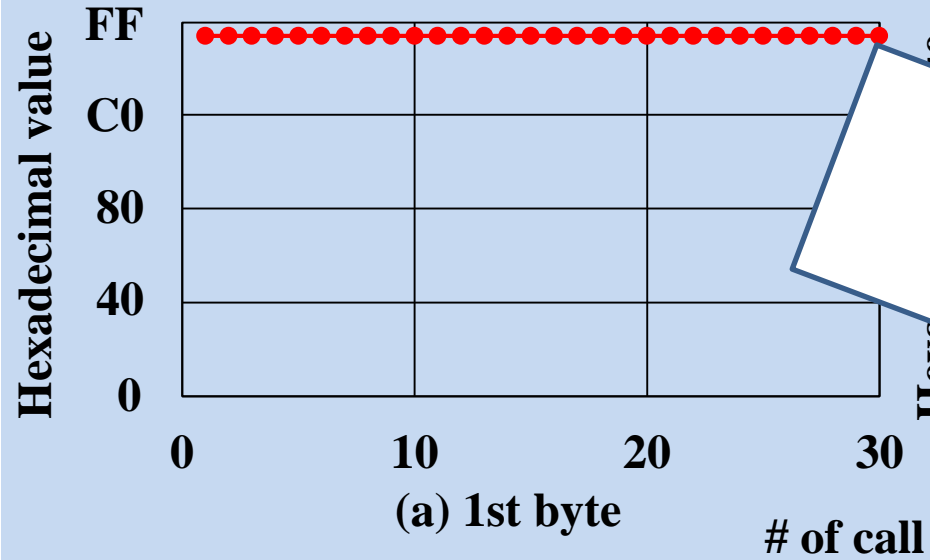
Allocation Pattern	Operators
Assigning the same GUTI	BE-III, DE-II, FR-II, JP-I
Three bytes fixed	CH-II, DE-III, NL-I, NL-II
Two bytes fixed	BE-II, CH-I, CH-III, ES-I, FR-I, NL-III
One bytes fixed	AT-I, AT-II, AT-III, BE-I, DE-I

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

Case I: Netherlands (NL-I)

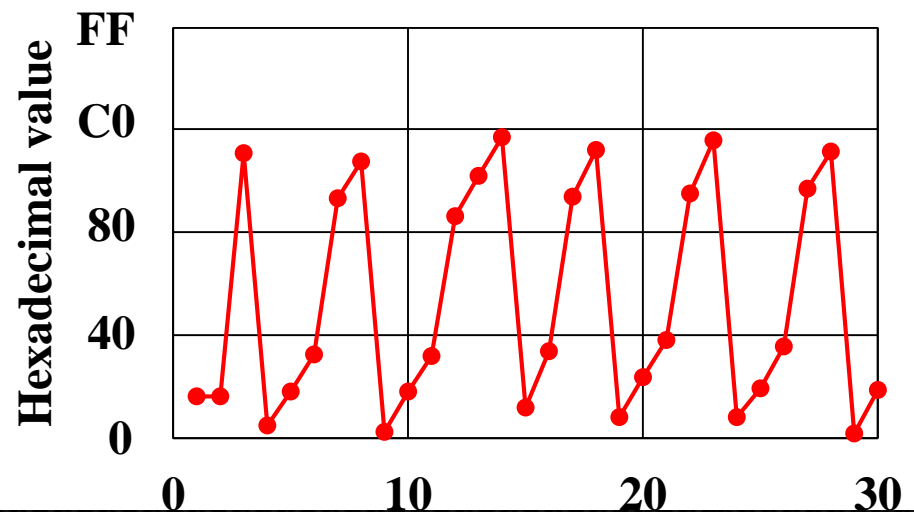
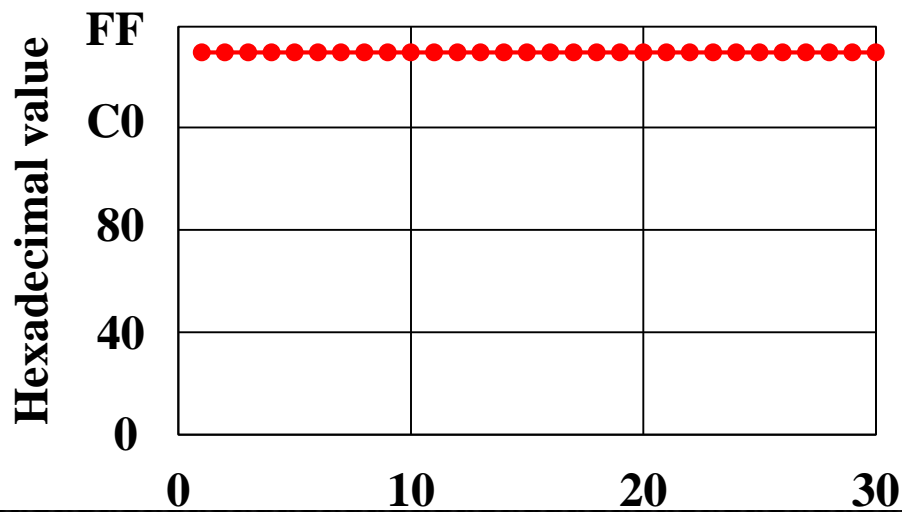
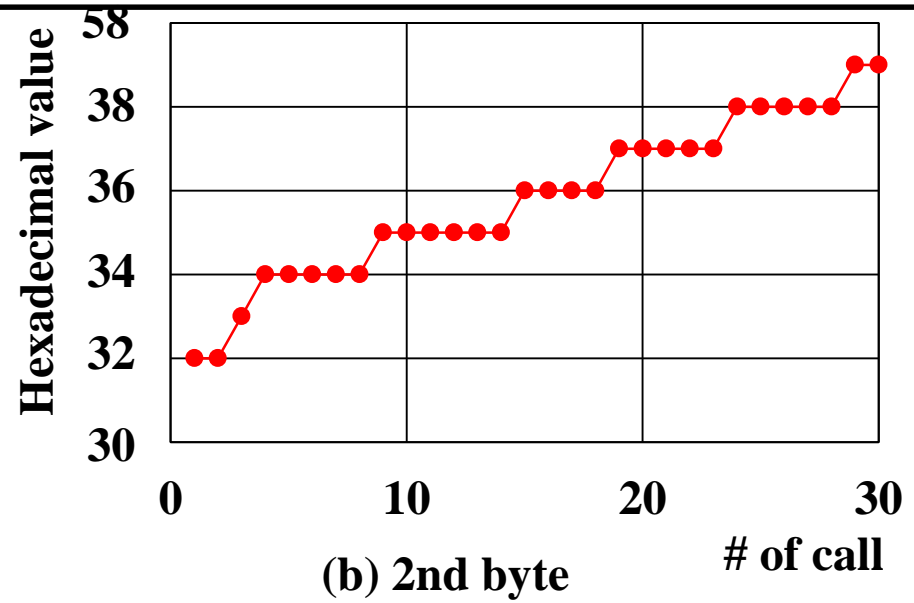
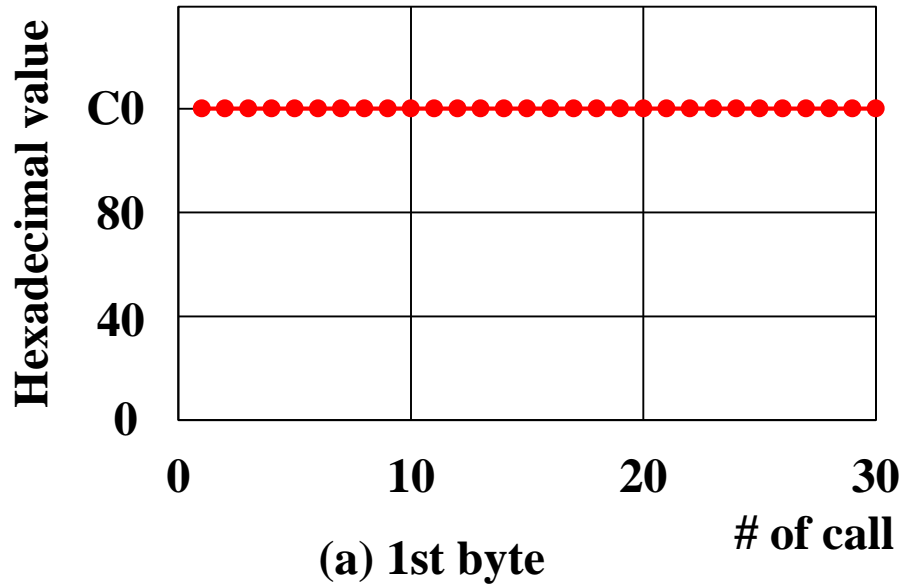


Case I: Netherlands (NL-I)

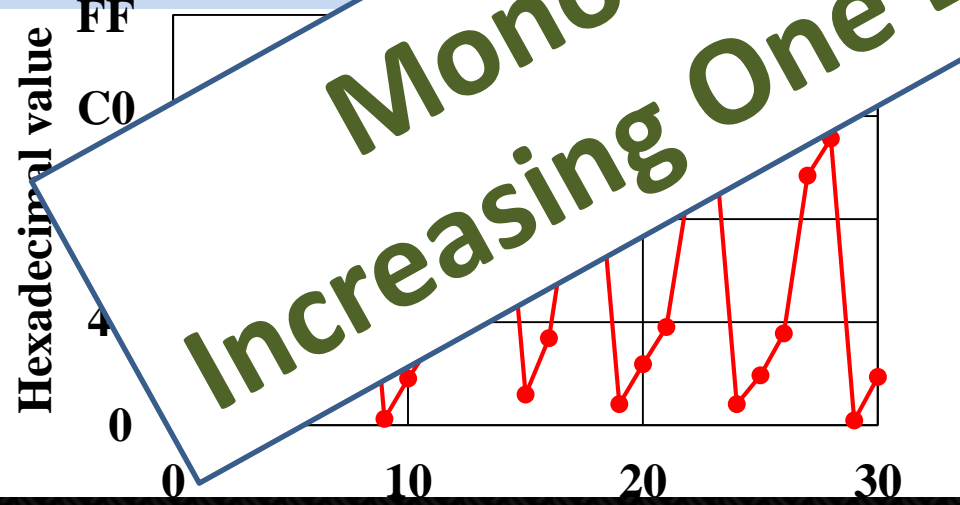
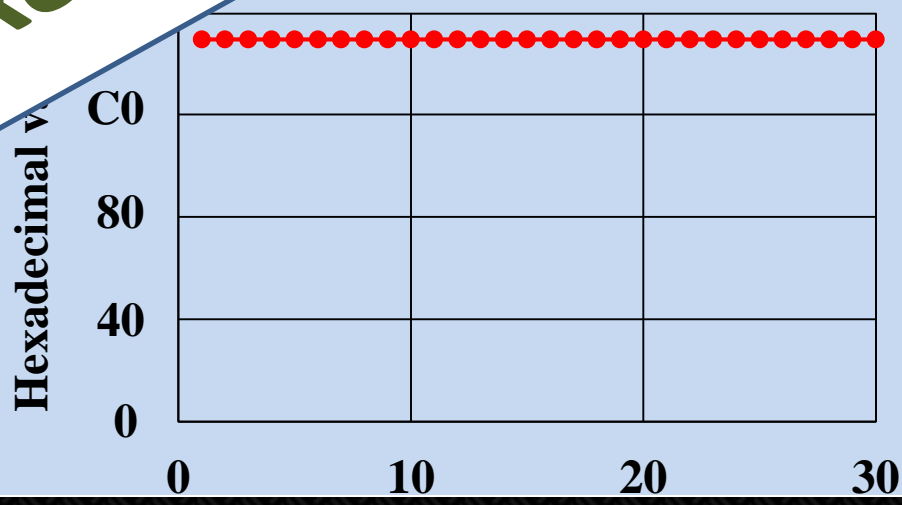
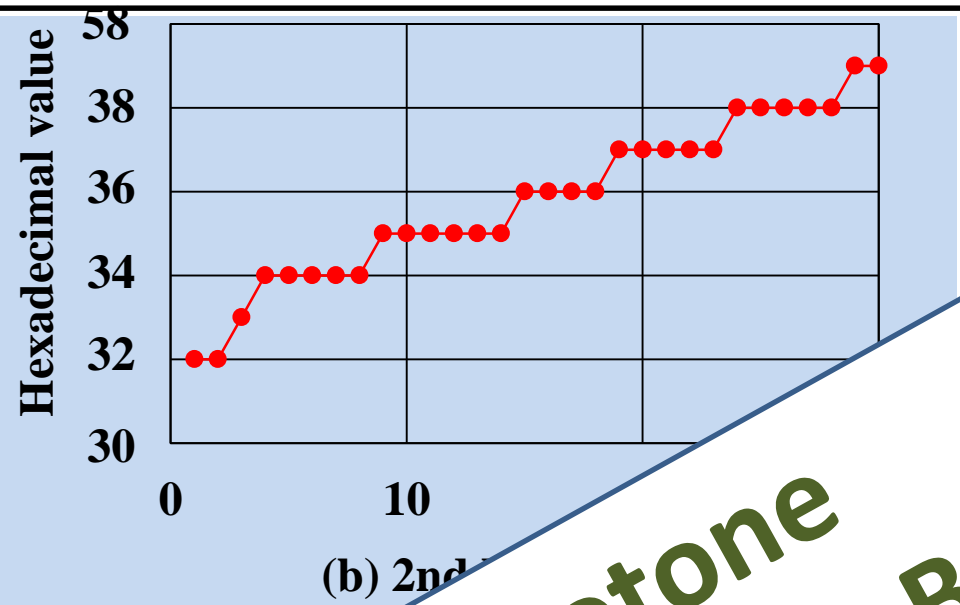
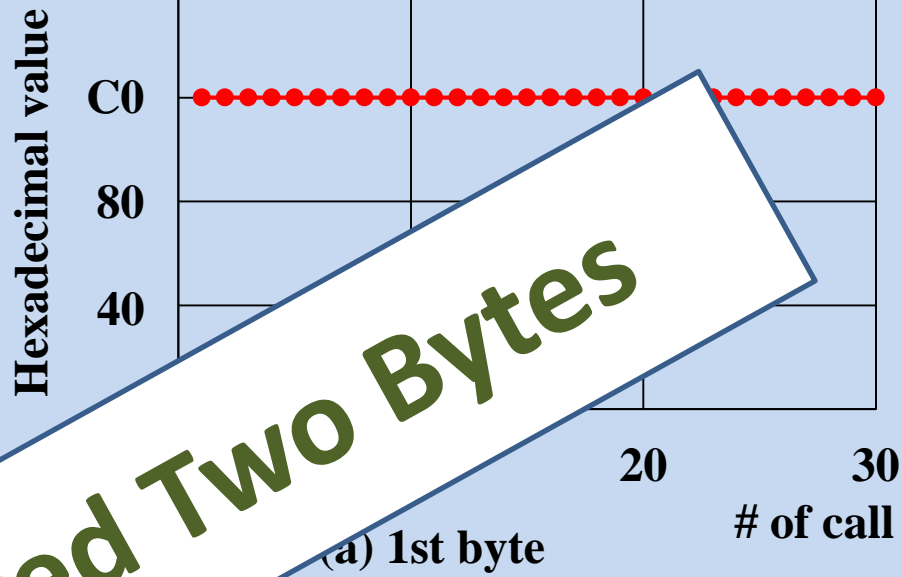


Fixed Three Bytes

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

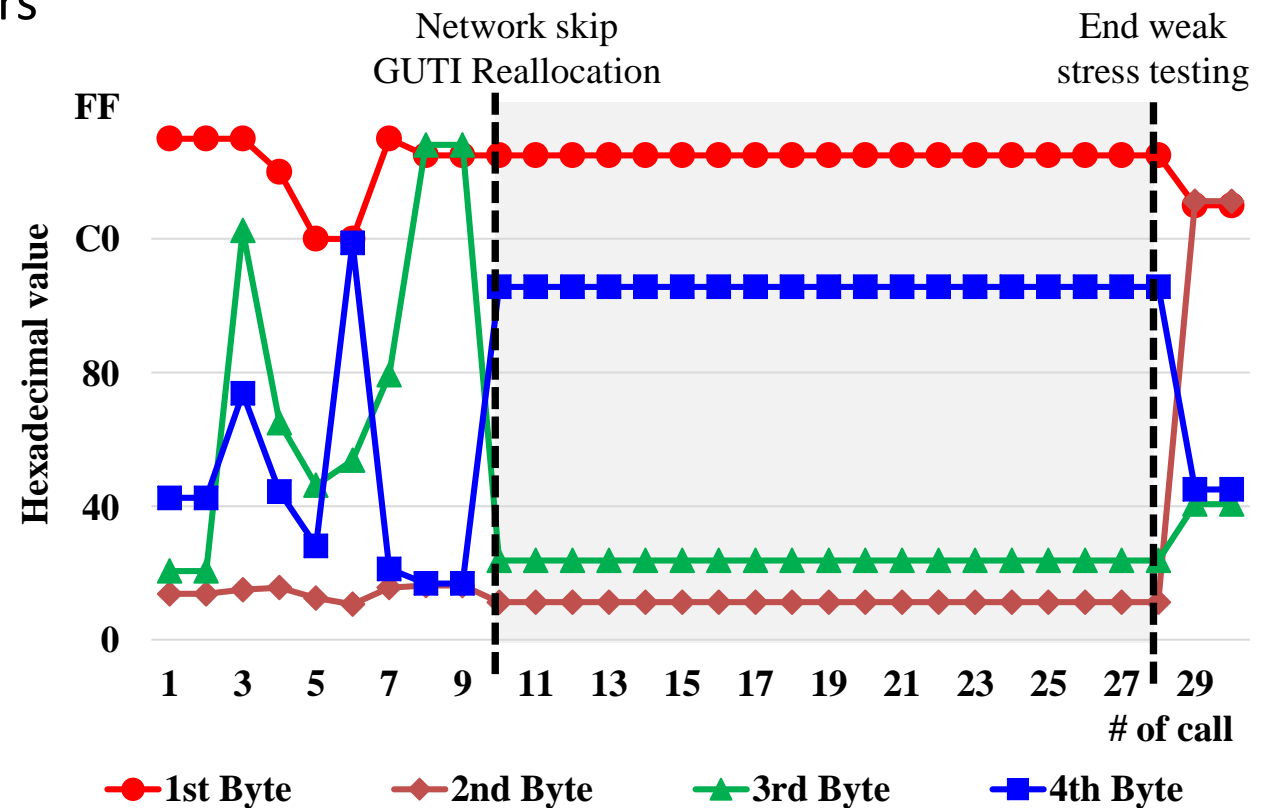
- ❖ No noticeable rule of *GUTI Reallocation* for some operators
- ❖ Invoking voice call continuously with a short time
 - Two types of test
 - Weak stress testing
 - Hard stress testing
 - Calls at shorter intervals than weak stress test

Stress Testing Result

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

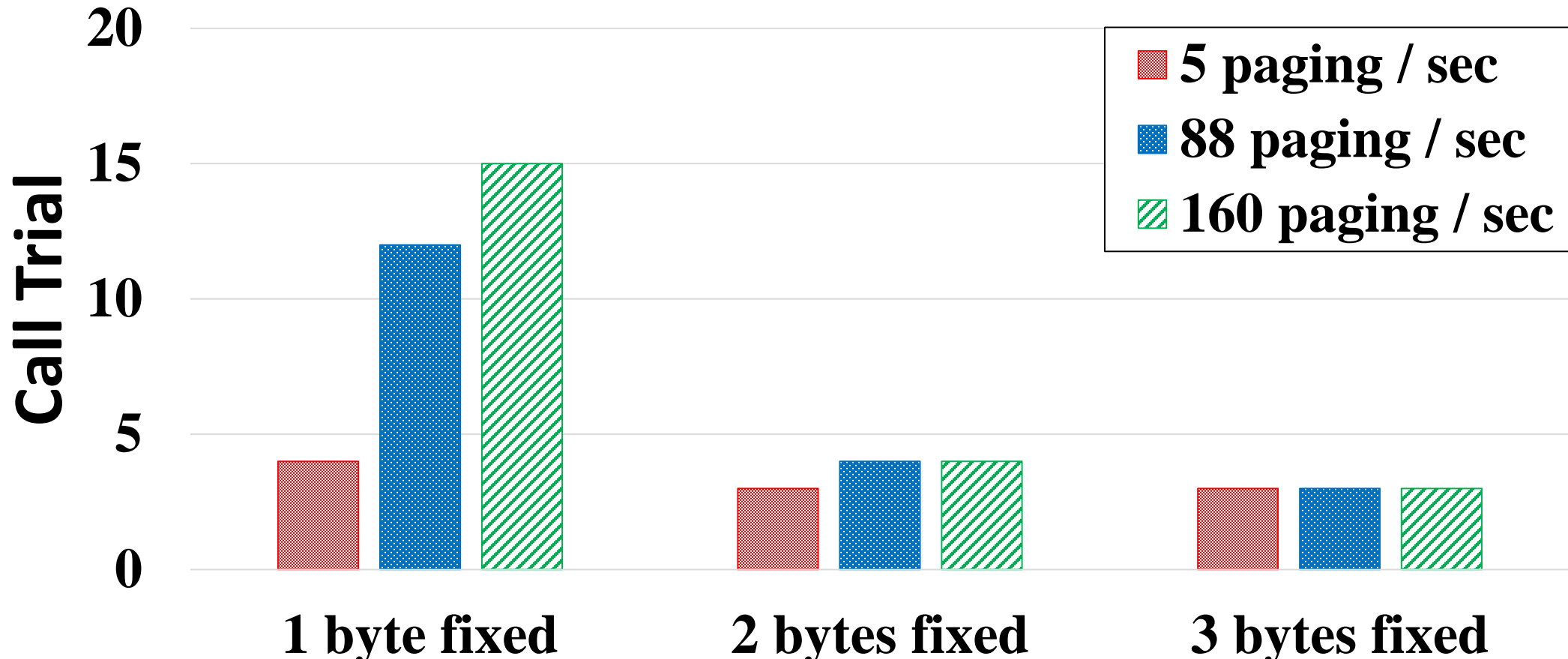
Operator	Weak Stress Testing	Hard Stress Testing
KR-I	O	O
KR-II	X	O
US-I	X	O
US-II	O	O

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)

```

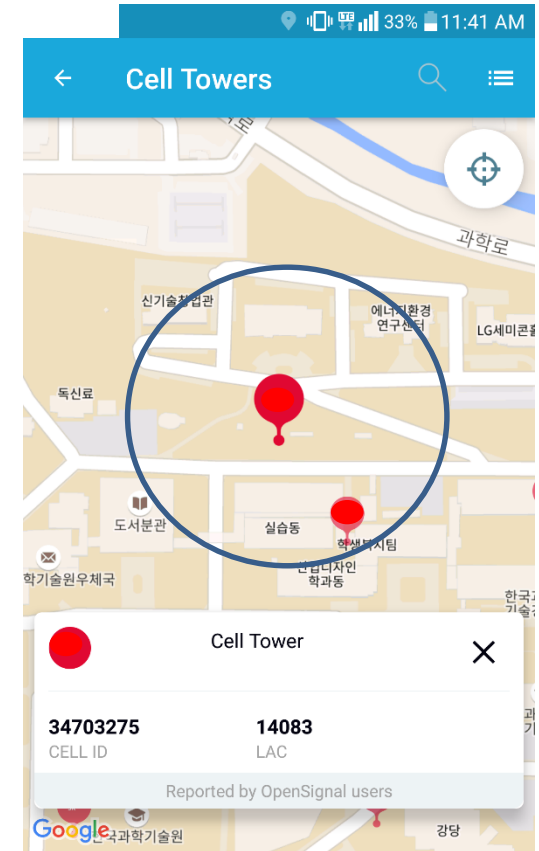
EXTENDED_SERVICE_REQUEST:
SecurityHeaderType: 0
ServiceType: 1 (mobile terminating CS fallback or 1xCS fallback)
NASKeySetIdentifier:
  TSC: 0 (native security context)
  NASKeySetId: 2
MTMSI: Identity:
  IdentityDigit:
    01: 200 = 0xC8
    02: 22 = 0x16
    03: 66 = 0x42
    04: 93 = 0x5D
    
```

```

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
    
```

(a) M-TMSI monitored by Device

(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