# Cellular Diversity and Location Tracking

Yongdae Kim
KAIST
SysSec Lab

Elimination of the 3G context can delete the LTE context (causing LTE to become unavailable)
G.-H. Tu et. al. “Control-Plane Protocol Interactions in Cellular Networks”, ACM Sigcomm’14

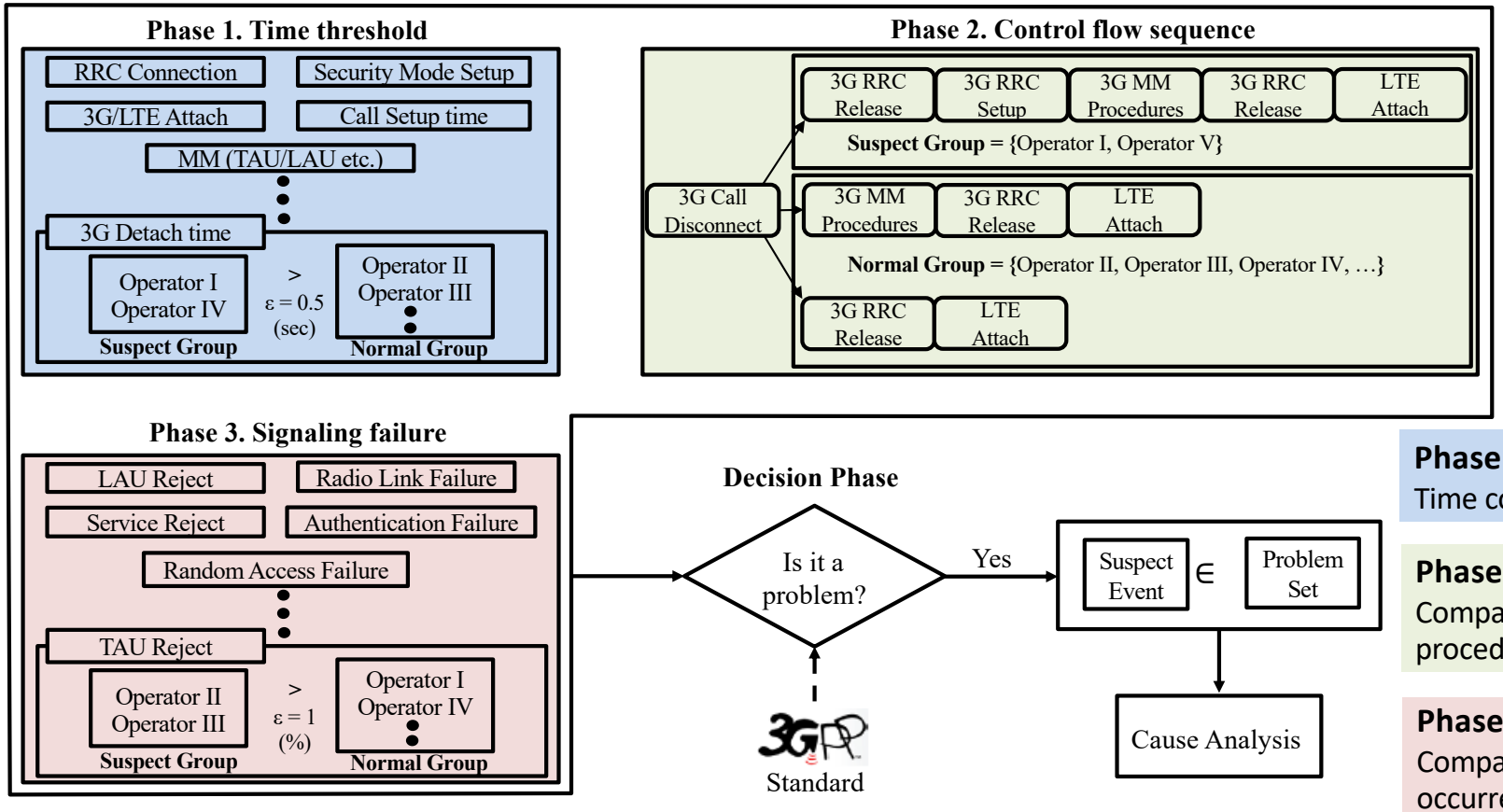
# Worldwide Data Collection

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

## Data summary

# of countries: **11**
# of operators: **28**
# of USIMs: **95**
# of voice calls: **52K**
# of signalings (control-plane message): **6.4M**

# Problem Diagnosis Overview



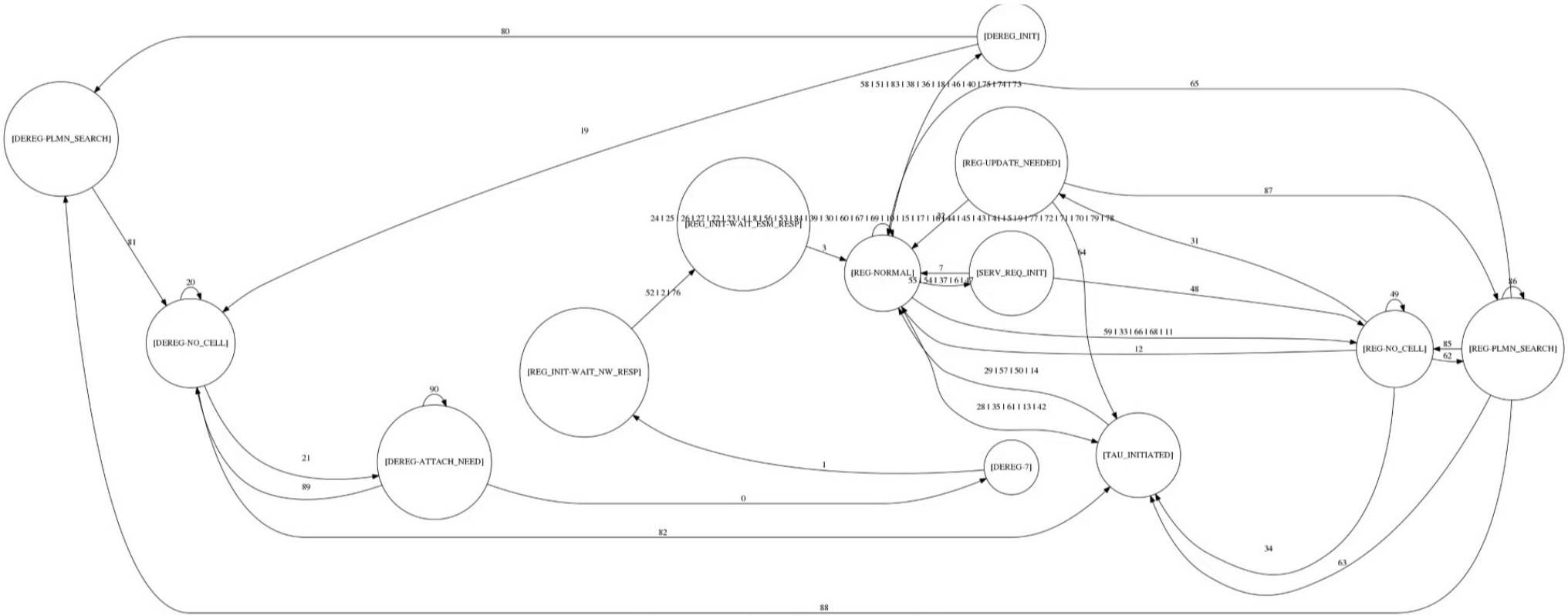

**Phase 1**
Time comparison by procedure

**Phase 2**
Comparison of signaling procedure sequence

**Phase 3**
Comparison of signaling failure occurrence probability

# Identified Problems

| Problem | Observation | Operator |
|---|---|---|
| LTE location update collision | **Out-of-service** about **11 sec**. | US-II |
| Mismatch procedures | Delay of 3G detach. Worst case: **10.5 sec.** | US-I, DE-I. DE-II, FR-I, FR-II |
| Allocation of incorrect frequency | **Out-of-service 30 sec**. and **stuck in 3G for 100 sec.** | DE-I |
| Redundant location update | Delay of LTE attach or call setup. Worst case: **6.5 sec.** | US-I, DE-I, DE-III, FR-II |
| Redundant authentication | Delay of CSFB procedures for 0.4 sec. | FR-I, FR-II, DE-I, DE-III, FR-II |
| Security context sharing error | Out-of-service 1.5 sec. | ES-I |
| Core node handover misconfiguration | Delay of LTE attach (0.4 sec.) | US-II |

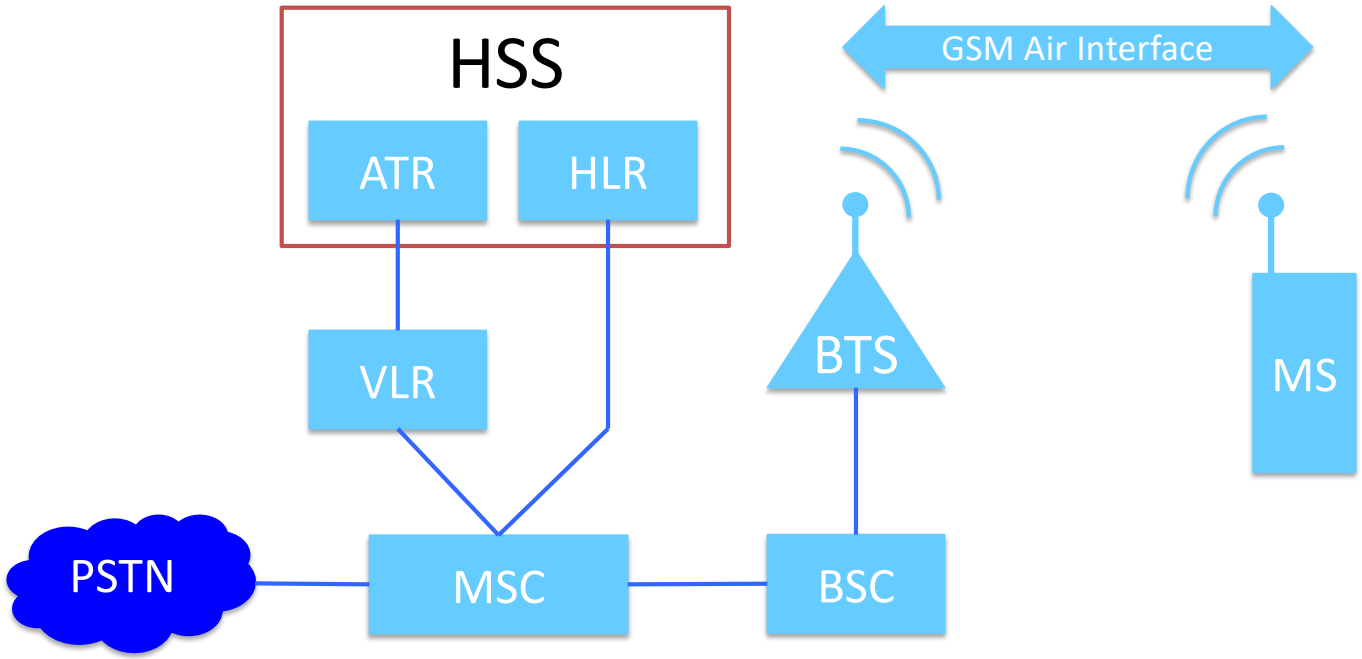

[DEREG_INIT]
[DEREG-PLMN_SEARCH]
[DEREG-NO_CELL]
[DEREG-ATTACH_NEED]
[DEREG-7]
[REG_INIT-WAIT_ESM_RESP]
[REG_INIT-WAIT_NW_RESP]
[REG-NORMAL]
[REG-UPDATE_NEEDED]
[SERV_REQ_INIT]
[TAU_INITIATED]
[REG-NO_CELL]
[REG-PLMN_SEARCH]
80
19
81
20
21
89
90
0
1
82
88
58 | 51 | 83 | 38 | 36 | 18 | 46 | 40 | 75 | 74 | 73
65
24 | 25 | 26 | 27 | 22 | 23 | 41 | 8 | 56 | 53 | 84 | 39 | 30 | 60 | 67 | 69 | 10 | 15 | 17 | 18 | 44 | 45 | 43 | 14 | 5 | 9 | 77 | 72 | 2 | 70 | 79 | 78
3
52 | 2 | 76
7
55 | 54 | 37 | 6 | 4
87
31
64
48
49
59 | 33 | 66 | 68 | 11
12
85
62
86
29 | 57 | 50 | 14
28 | 35 | 61 | 13 | 42
34
63

# Location Tracking

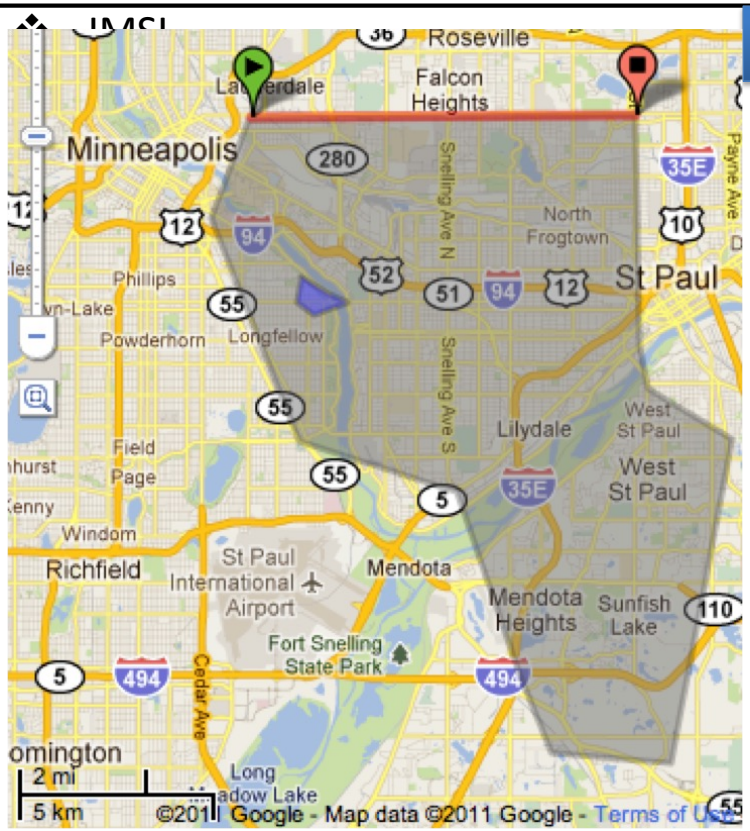
# Location Privacy Leaks on GSM

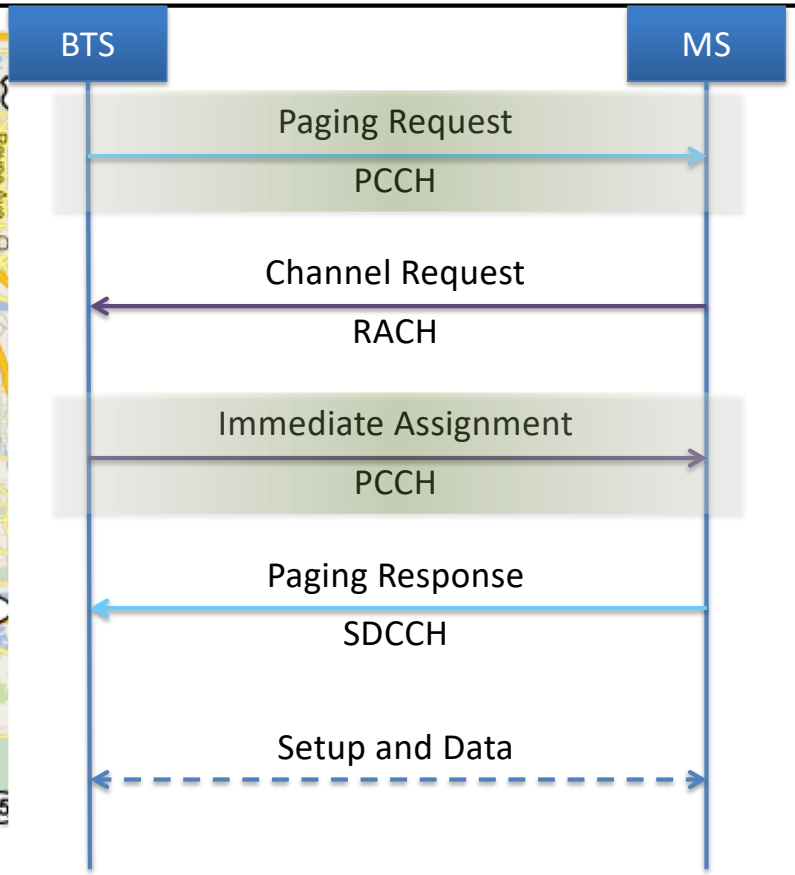
- We have the victim's mobile phone number
- Can we detect if the victim is in/out of an area of interest?
  - Granularity? 100 $km^2$? 1$km^2$? Next door?
- No collaboration from service provider
  - i.e. How much information leaks from the HLR over broadcast messages?
- Attacks by passively listening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

# Cellular Network

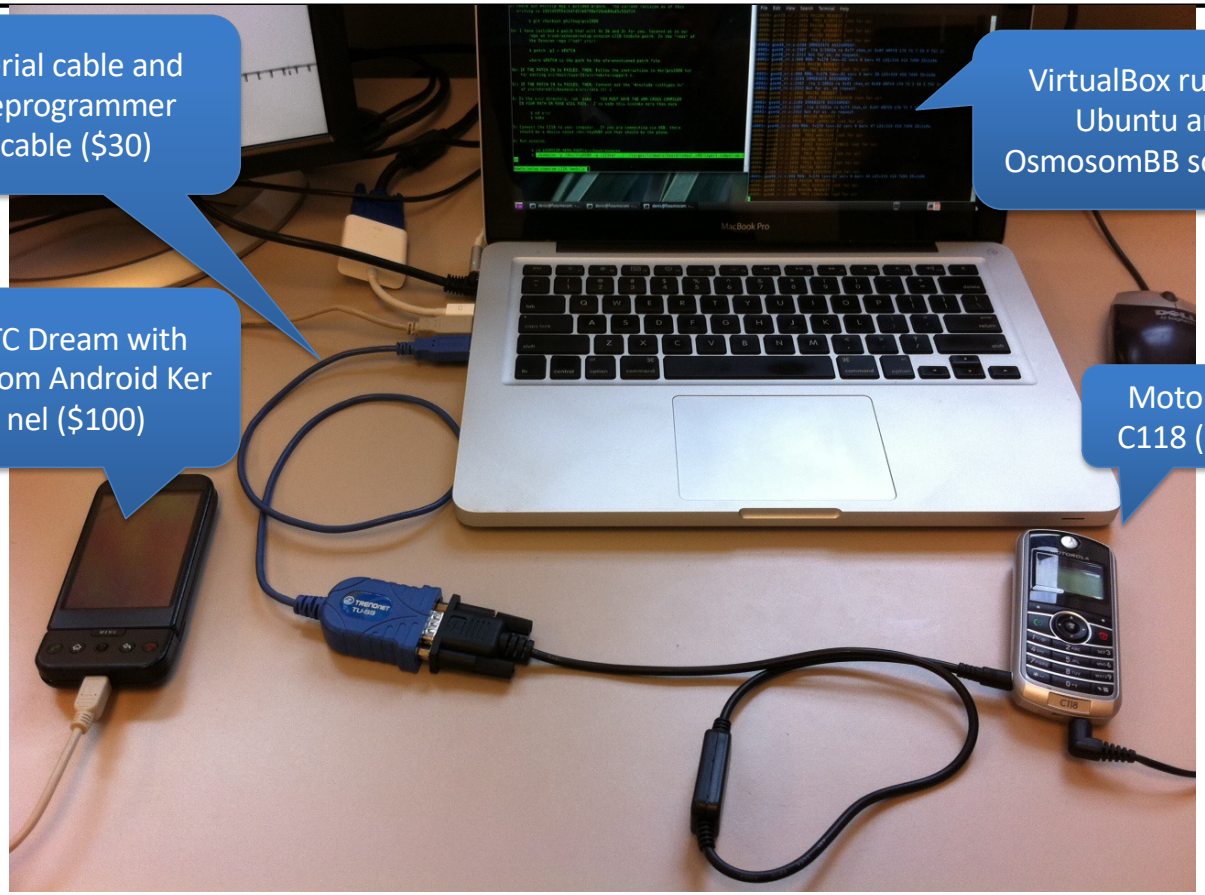


# Location Leaks on Cellular Network

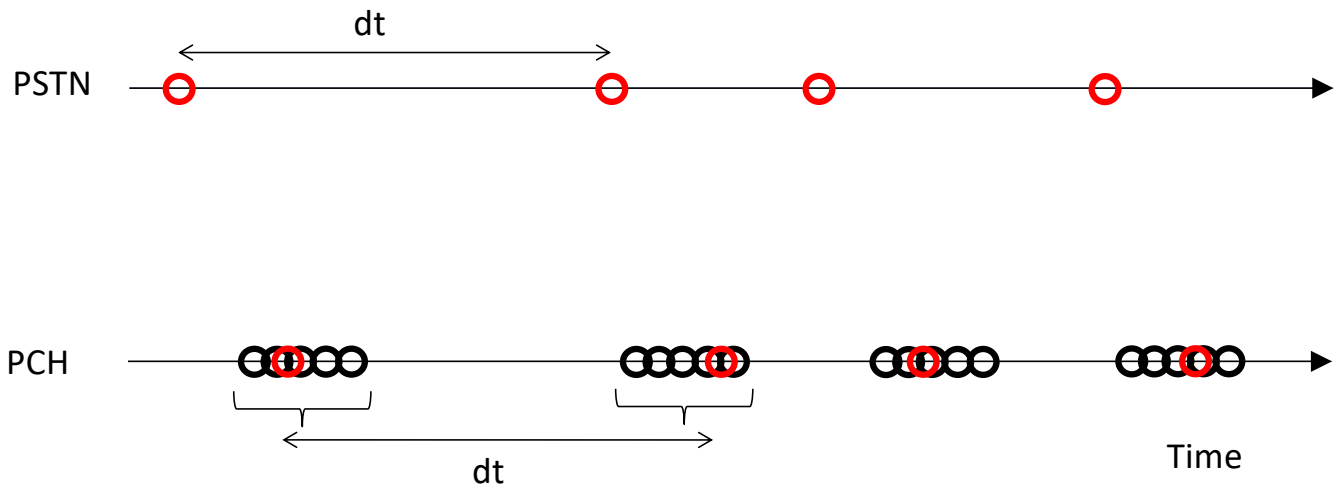


# Platform

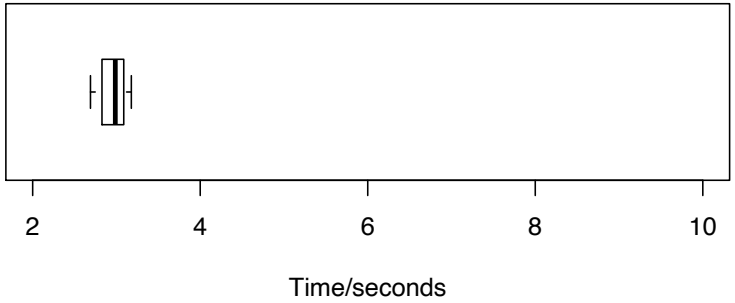

Serial cable and reprogrammer cable ($30)
VirtualBox running Ubuntu and OsmosomBB software
HTC Dream with custom Android Ker nel ($100)
Motorola C118 ($30)

# Phone number-TMSI mapping

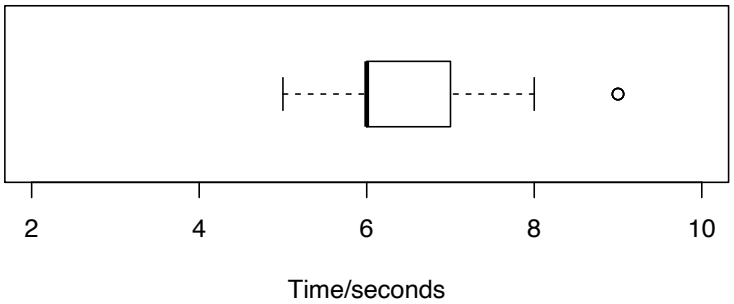


# Silent Paging

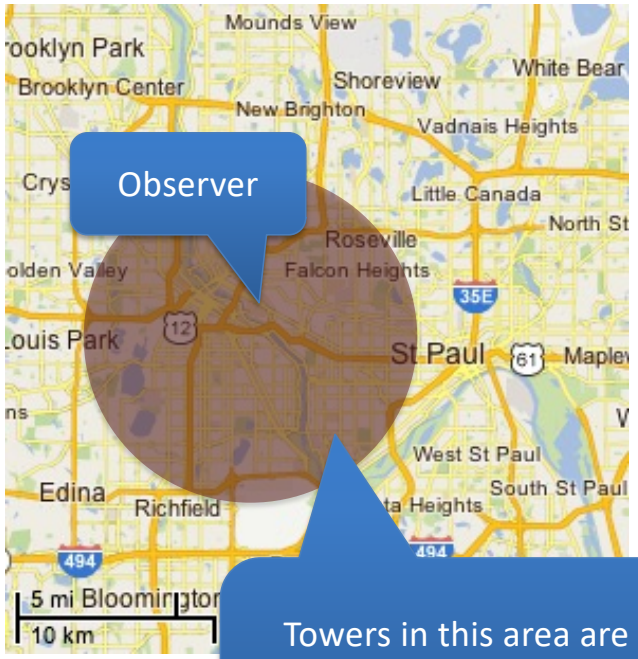
- Delay between the call initiation and the paging request: 3 sec



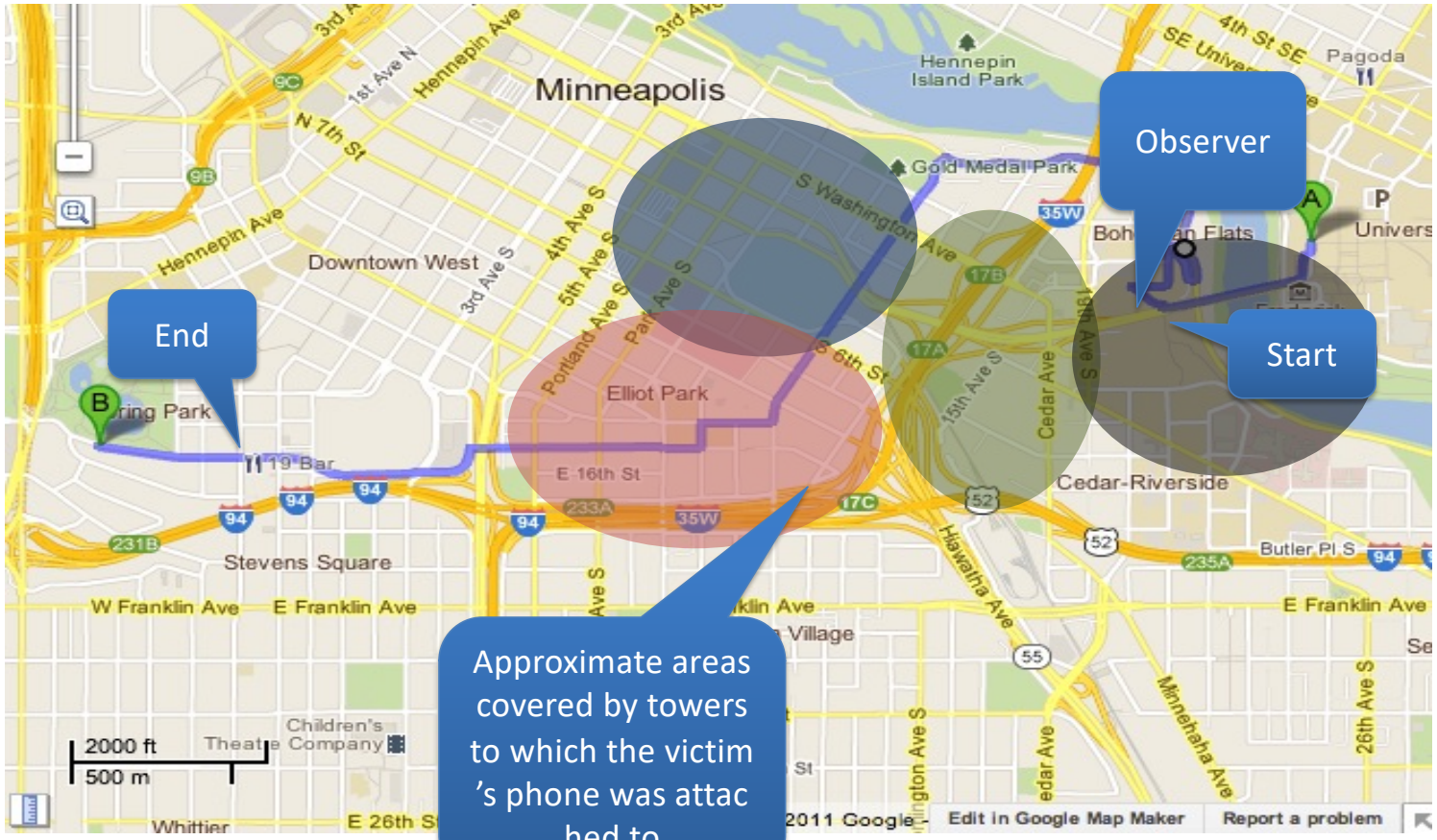

- Median delay between call initiation and ring: 6 sec



# Coverage area with 1 antenna

# Following a walking person



# 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

# 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 |

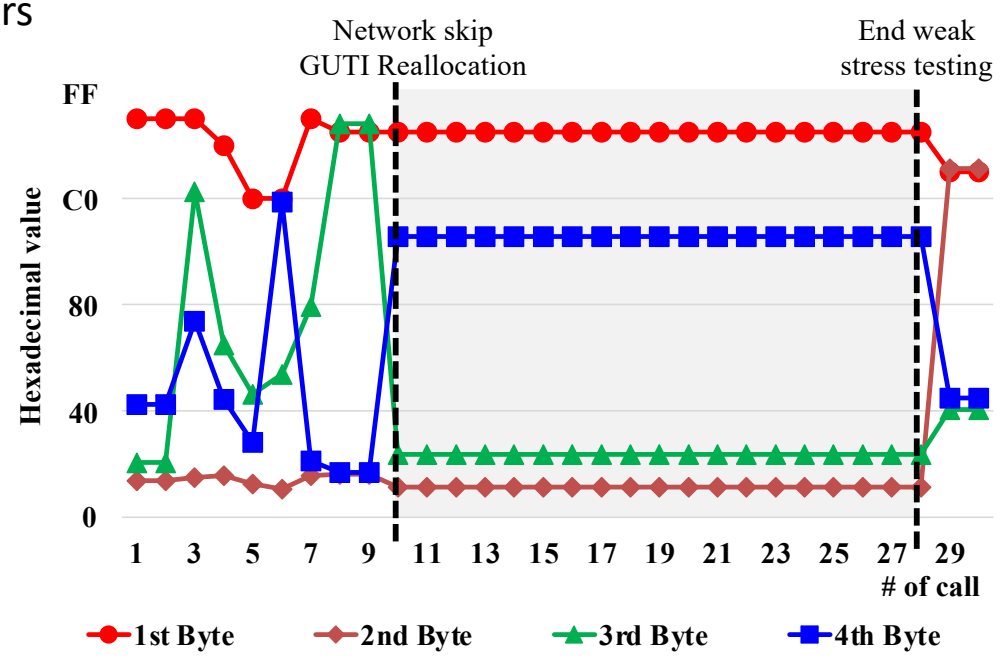
AT: Austria, BE: Belgium, CH: Switzerland, DE: Germany, ES: Spain, FR: France, JP: Japan, NL: Netherlands

# Stress Testing Result

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

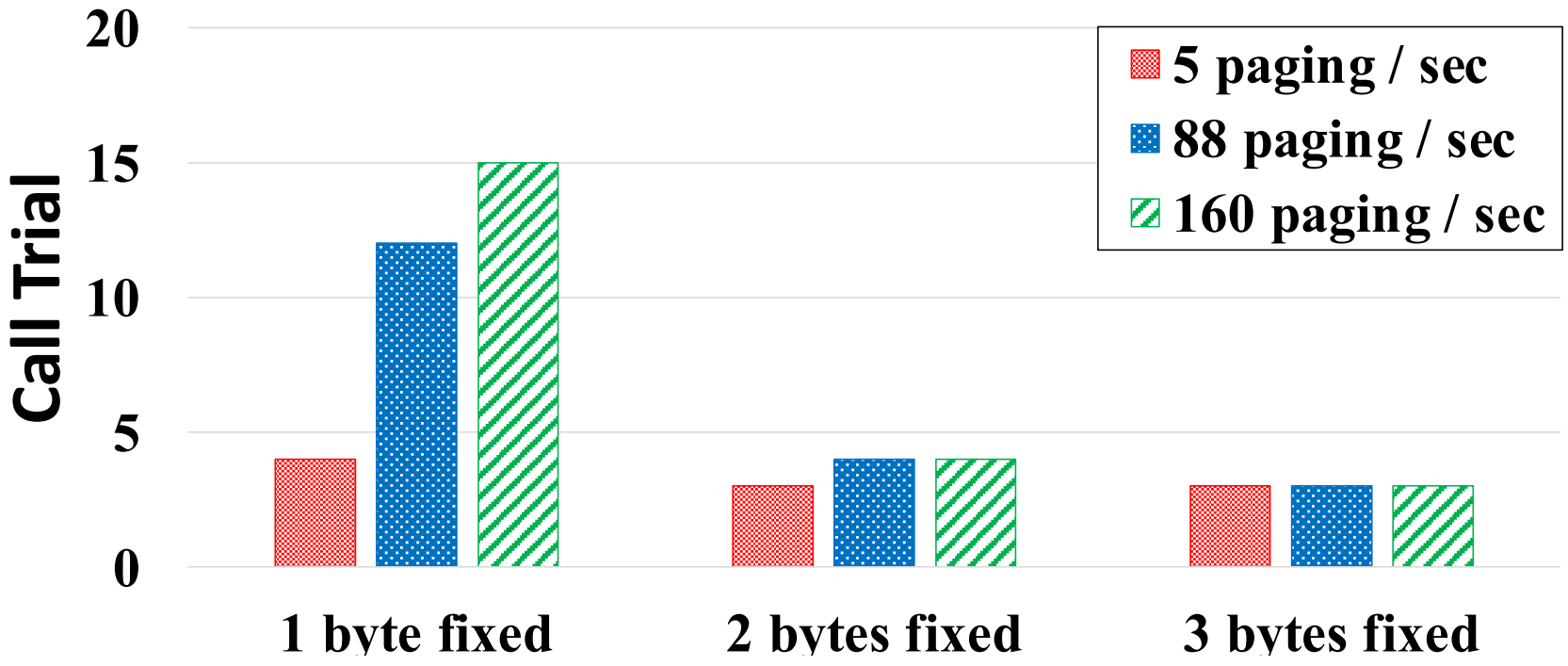
| Operator | Weak Stress Testing | Hard Stress Testing |
|---|---|---|
| KR-I | O | O |
| KR-II | X | O |
| US-I | X | O |
| US-II | O | O |

O: Reuse *GUTI*
X: No noticeable change



# Success Rate of our Attack

- Required number of calls covering 99% success rate



# Location Tracking with GUTI

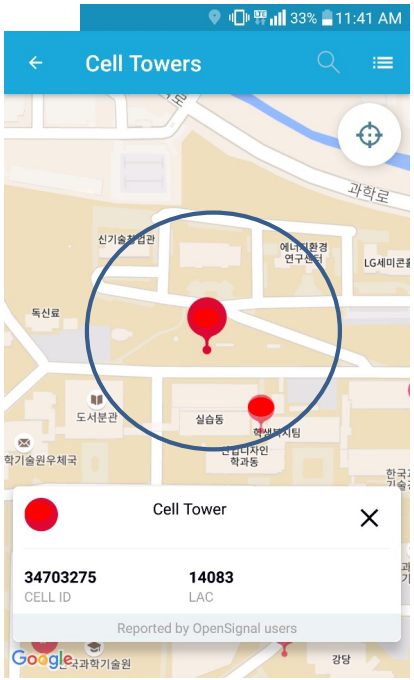
- Observation of broadcast channels after call invocation
  - Pattern matching (fixed bytes, assigning same GUTI)
  - Location tracking (Tracking Area, Cell)

**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)