SS7Tracker - Active GSM Cell-ID Tracking

*Where did you disappear?*

**Michal Ficek**, Katerina Dufkova, Jiri Danihelka, Ivan Gregor, Jan Kouba, Jakub Novak (R&D Centre / Charles University)

Jan Janecek (Czech TU), Lukas Kencl (R&D Centre / Czech TU)

Michal Fryda, Martin Tomek, Tomas Svoboda, Ladislav Soldan (Vodafone CZ)

Prague, Czech Republic
Outline

• Motivation – WHY??

• Solution – HOW?

• Results – WOW!

• Discussion

• Future – NOW!
Project motivation

• GSM network
  – cellular network
  – signal coverage
  – signal strength

• Roaming
  – 17% mobile revenues globally
  – United States only 3%
Project motivation

• GSM network
  – cellular network
  – signal coverage
  – signal strength

• Roaming
  – 17% mobile revenues globally
  – United States only 3%
  – most important region: Western Europe
Goal: Discover mobile network coverage weak points using inroamer active tracking

- Inroamers are foreign roaming clients subscribed to the studied network – can switch GSM network freely!
- Active tracking relies on sending extra queries to the network
- Typical scenario
Message flow

**SS7Tracker** (local)

**SUBSCRIBER** (local)

**MSC/VLR** (local)

**HLR** (abroad)

- **SRI_SM_REQ (MSISDN)**
- **SRI_SM_RSP (IMSI, VLR)**
- **SMS Class 0 (IMSI)**
- **PSI_REQ (IMSI)**
- **PSI_RSP (CGI, AOL)**

**HLR** .. Home Location Register
**VLR** .. Visitor Location Register
**MSC** .. Mobile Switching Centre
**MSISDN** .. Mobile Station International Subscriber Directory Number
**IMSI** .. International Mobile Subscriber Identity
**CGI** .. Cell Global Identity
Solution architecture

- **Server – SS7Box**
  - SS7Box located in RDC
  - Equipped with signalling card
  - Connected to live VF CZ network

- **Client – TrackerGUI**
  - Tracked data statistics in graphs
  - Tracking scenarios definition

- **Technology**
  - Signaling System No.7 (SS7)
  - Hidden-SMS-based solution
Results: Tracked and visualized data from real inroamers

– Experiment:
  – 105 inroamers
  – During 6 hours
– **Outcome: List of suspicious cells**
Results: Tracked and visualized data from real inroamers

- Experiment:
  - 105 inroamers
  - During 6 hours
- Outcome: List of suspicious cells
SS7Tracker Features

Location Server tracking a mobile unit to Cell ID precision in real time

• non-disruptive - requires no change to infrastructure (plug & play)
• can track a passive mobile station
• real-time
• configurable
• tried and tested in Vodafone CZ (in-roamer tracking)
Discussion: Capacity

- SMS-based solution may overwhelm network if many customers
  - signalling line utilization using discrete simulation
  - local site overload
Discussion: Battery lifetime

– may affect battery

SonyEricsson K750i

![Battery lifetime graph]

- Blue line: without tracking
- Red line: tracking interval 1 min
- Purple line: tracking interval 5 min
Discussion: Accuracy

- GSM based solution – Cell-Id accuracy
  + availability
  + works in every GSM network
  + no additional changes into network nor mobile stations (lowcost)
  + work with every mobile station HW (which supports SMS)
  - accuracy
    not really disadvantage!

- GPS
  + accuracy
  - need of special equipment
  - not reachable everywhere
Parallel Ongoing Activity: Location Data Mining

- Statistical evaluation and extended visualization of tracked data
  - cooperation with Faculty of Science, Charles University, Prague

- Focused on
  - Urban dynamics in real-time
  - Fluctuation of traffic density by seasons, weeks and hours
  - Space-time behavior studies

- Commercialization?
  - Customer behavior analysis
  - Targeted advertising

Urban dynamics of roamers in Prague
Future of SS7Tracker

- Network migration analysis
  - how often?
  - why?
  - especially in Europe

- Math & Modeling
  - handover between cells
  - handover effectivity

- Tracking parameters tuning
Future of SS7Tracker

- Network migration analysis
  - how often?
  - why?
  - especially in Europe

- Math & Modeling
  - handover between cells
  - handover effectivity

- Tracking parameters tuning

![Graph showing comparison of tracking intervals](https://via.placeholder.com/150)

2 minutes tracking interval

6 minutes tracking interval
Conclusion

• Demonstrated Cell-ID based location tracking usefulness

• Opens promising areas for further research
Thank you!

• Interested?
  • Ask questions
  • Read our article
  • Think about it


R&D Centre for Mobile Applications (RDC)

www.rdc.cz
Discussion: Privacy

• Country legal system
  – Czech Republic
  – EU directive

  legal for network optimization and scientific purposes

• Data in operators security perimeter
  – another view of information already managed

• Reports design
  – only aggregate data with no relation to individuals