GSM Research

Chair in Communication Systems

Department of Applied Sciences

University of Freiburg

2010

Albert-Ludwigs-Universität Freiburg

UNI FREIBURG

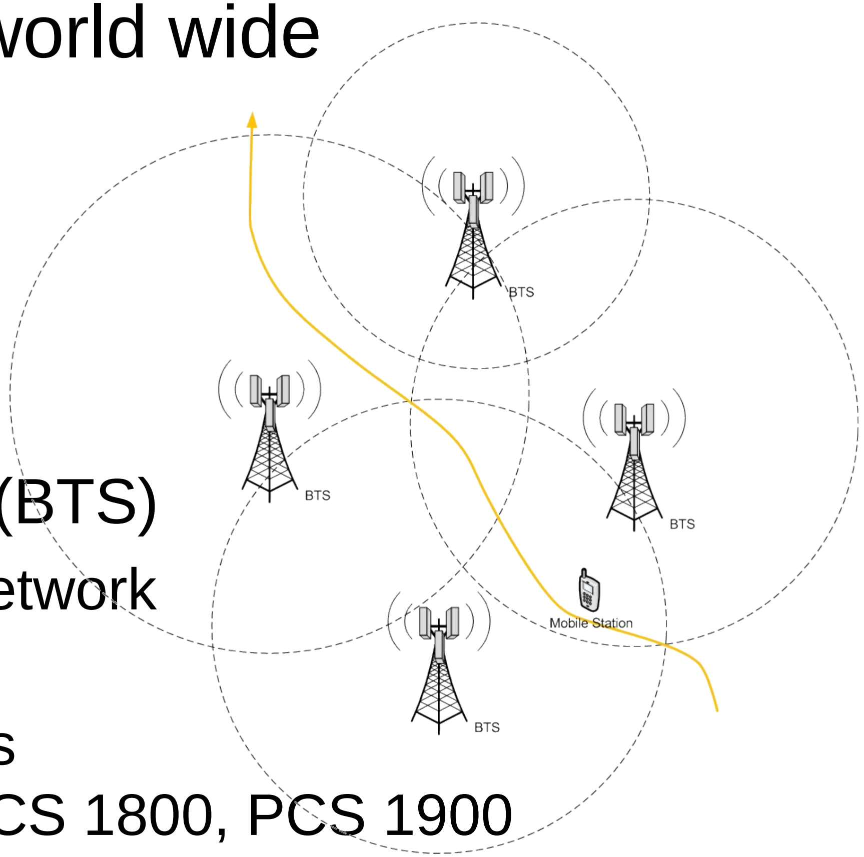
Dennis Wehrle, Konrad Meier, Dirk von Suchodoletz,
Klaus Rechert, Gerhard Schneider

Overview

1. GSM Infrastructure
2. Analysis of GSM
3. Our own GSM network
4. Security
    - 4.1 Localization
    - 4.2 IMSI-Catcher
    - 4.3 Encryption A5/1

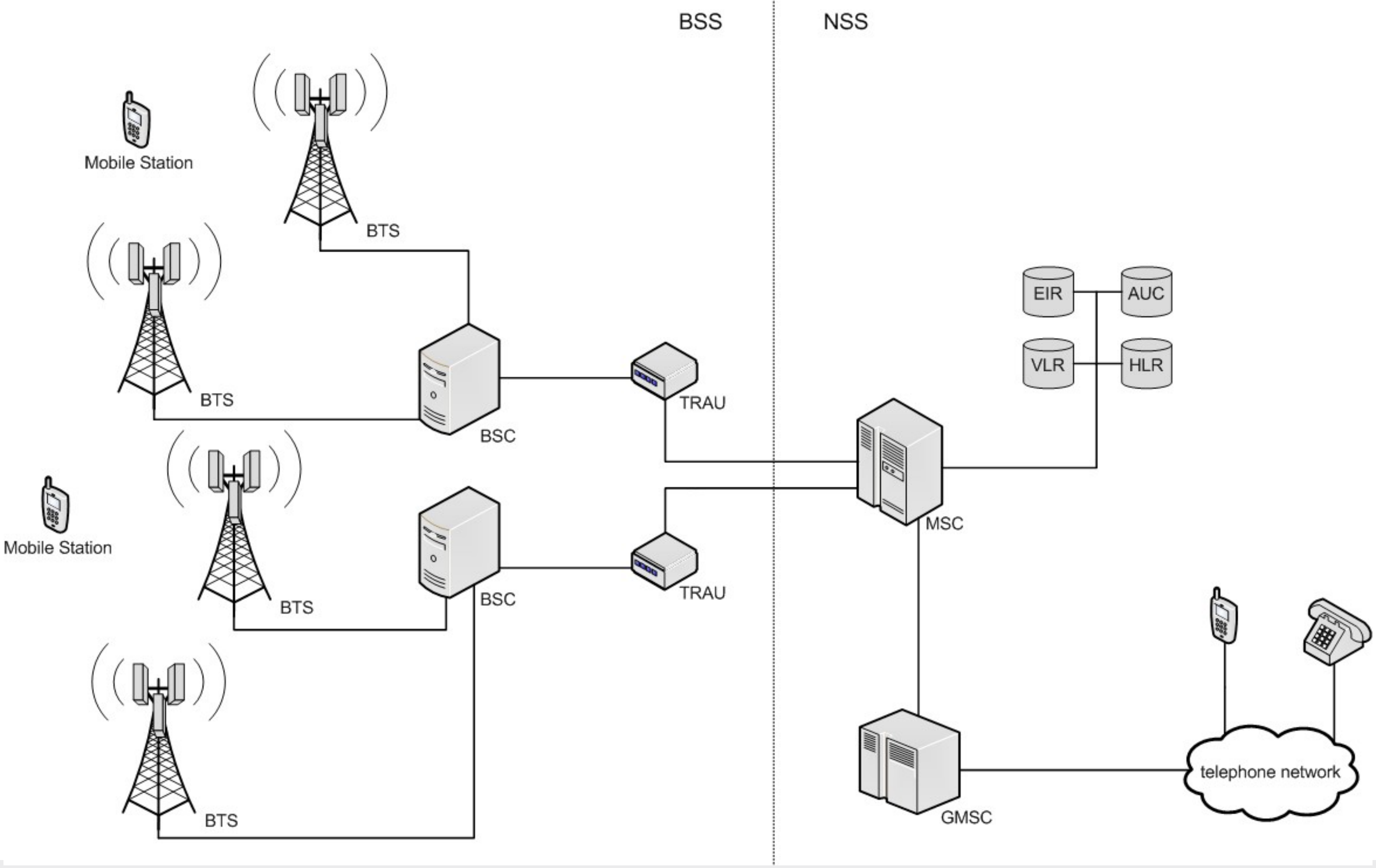
1. GSM Infrastructure

- GSM is a cellular network
- Largest mobile network world wide
- Subscriber view:
  - Mobile Station
    - Cell phone
    - SIM card
  - Base Station Transceiver (BTS)
    - Provides access to the network over the air interface
    - Different frequency bands GSM 850, EGSM 900, DCS 1800, PCS 1900



1. GSM Infrastructure

- Operator / Network view



Overview

1. GSM Infrastructure
2. Analysis of GSM
3. Our own GSM network
4. Security
    - 4.1 Localization
    - 4.2 IMSI-Catcher
    - 4.3 Encryption A5/1

2. GSM Analysis

- Analysis from the subscriber point of view
  - Nokia 3310
    - Netmonitor to show network parameters and cell phone state
    - Gammu[1] captures data received and transmitted by the phone.
  - USRP[2]
    - Flexible software radio
    - GSM signals can be captured.
    - Data processing is done with airprobe.[3]

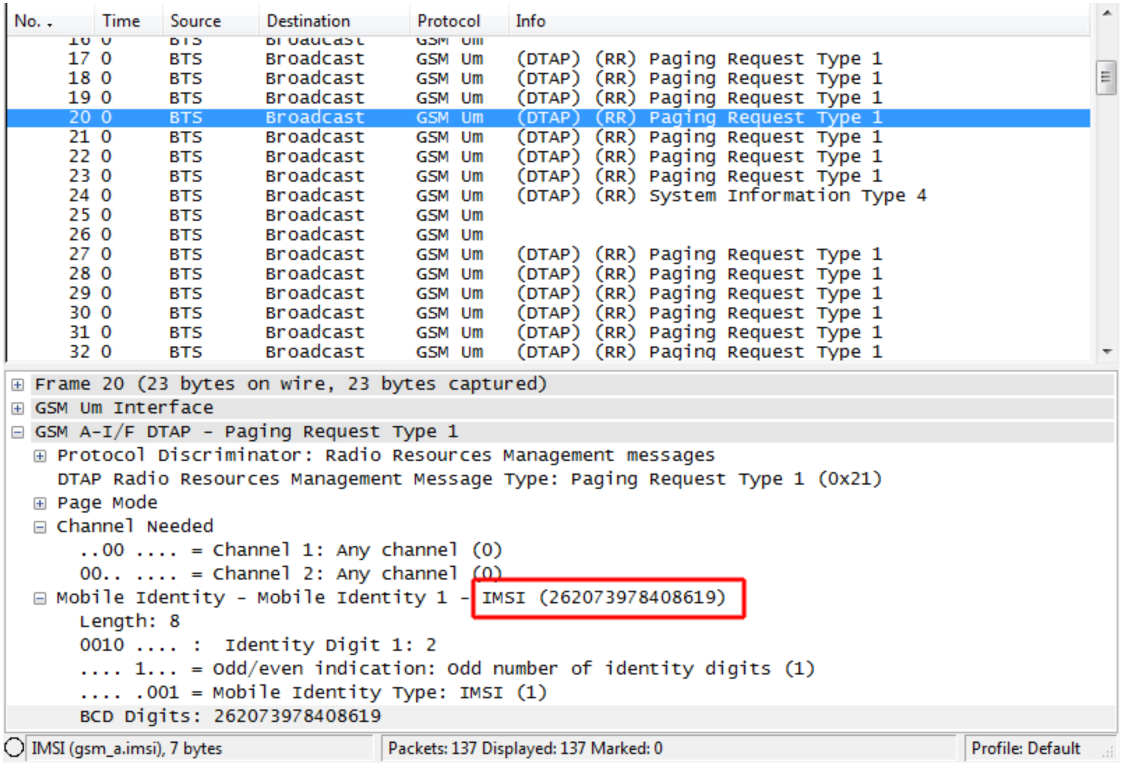
Nokia 3310

Universal Software Radio Peripheral (USRP)

[1] Gammu: http://wammu.eu/gammu/
[2] USRP from Ettus Research: http://www.ettus.com
[3] airprobe: https://svn.berlin.ccc.de/projects/airprobe/

2. GSM Analysis

- Gammu output displayed with Wireshark
- Nokia 3310 Netmonitor

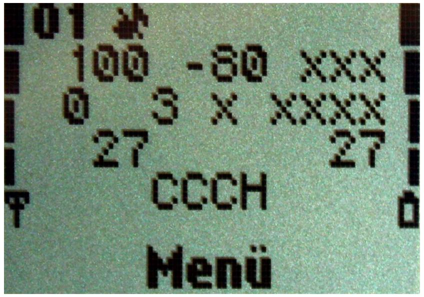


```
No. .   Time  Source  Destination  Protocol  Info
  16 0  BTS     Broadcast    GSM Um
  17 0  BTS     Broadcast    GSM Um    (DTAP) (RR) Paging Request Type 1
  18 0  BTS     Broadcast    GSM Um    (DTAP) (RR) Paging Request Type 1
  19 0  BTS     Broadcast    GSM Um    (DTAP) (RR) Paging Request Type 1
  20 0  BTS     Broadcast    GSM Um    (DTAP) (RR) Paging Request Type 1
  21 0  BTS     Broadcast    GSM Um    (DTAP) (RR) Paging Request Type 1
  22 0  BTS     Broadcast    GSM Um    (DTAP) (RR) Paging Request Type 1
  23 0  BTS     Broadcast    GSM Um    (DTAP) (RR) Paging Request Type 1
  24 0  BTS     Broadcast    GSM Um    (DTAP) (RR) System Information Type 4
  25 0  BTS     Broadcast    GSM Um
  26 0  BTS     Broadcast    GSM Um
  27 0  BTS     Broadcast    GSM Um    (DTAP) (RR) Paging Request Type 1
  28 0  BTS     Broadcast    GSM Um    (DTAP) (RR) Paging Request Type 1
  29 0  BTS     Broadcast    GSM Um    (DTAP) (RR) Paging Request Type 1
  30 0  BTS     Broadcast    GSM Um    (DTAP) (RR) Paging Request Type 1
  31 0  BTS     Broadcast    GSM Um    (DTAP) (RR) Paging Request Type 1
  32 0  BTS     Broadcast    GSM Um    (DTAP) (RR) Paging Request Type 1

⊞ Frame 20 (23 bytes on wire, 23 bytes captured)
⊞ GSM Um Interface
⊟ GSM A-I/F DTAP - Paging Request Type 1
    ⊞ Protocol Discriminator: Radio Resources Management messages
      DTAP Radio Resources Management Message Type: Paging Request Type 1 (0x21)
    ⊞ Page Mode
    ⊟ Channel Needed
        ..00 .... = Channel 1: Any channel (0)
        00.. .... = Channel 2: Any channel (0)
    ⊟ Mobile Identity - Mobile Identity 1 - IMSI (262073978408619)
        Length: 8
        0010 .... :  Identity Digit 1: 2
        .... 1... = Odd/even indication: Odd number of identity digits (1)
        .... .001 = Mobile Identity Type: IMSI (1)
        BCD Digits: 262073978408619

○ IMSI (gsm_a.imsi), 7 bytes | Packets: 137 Displayed: 137 Marked: 0 | Profile: Default
```

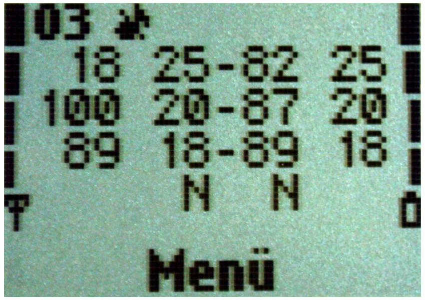
paging request with IMSI



```
01
 100  -80  XXX
  0   3  X  XXXX
  27          27
      CCCH

      Menü
```

cell parameters



```
03
  18  25-82  25
 100  20-87  20
  89  18-89  18
        N    N

      Menü
```

neighborhood list

2. GSM Analysis

- Analysis from the provider point of view
  - Access to a real-world GSM network is hard to get.
  - Therefore we have set up our own GSM network called RZ-GSM.
  - Research network for:
    - “Playing” with the GSM topic in a meaningful way
    - Statistics about user behavior within the network
    - Positioning of Mobile Station
    - GSM encryption A5/1
    - What information can/will be gathered by the provider?
    - How to protect the user in a GSM network?

Overview

1. GSM Infrastructure
2. Analysis of GSM
3. Our own GSM network
4. Security
   - 4.1 Localization
   - 4.2 IMSI-Catcher
   - 4.3 Encryption A5/1

3. Our own GSM network

- GSM network: RZ-GSM
  - Software:
    - OpenBSC[1]:
      Open-Source software implementation of a GSM Base Station Controller
    - LCR[2]
    - Asterisk[3]
      Voice communication server for routing the calls
  - Hardware
    - ip.access NanoBTS
    - Small GSM picocell

ip.access nanoBTS

[1] OpenBSC: http://openbsc.osmocom.org
[2] LCR: http://www.linux-call-router.de/
[3] Asterisk: http://www.asterisk.org/

3. Our own GSM network

- GSM network: RZ-GSM

Some facts:

3 BTS

1 BSC

MSC => Asterisk

Databases => SQL

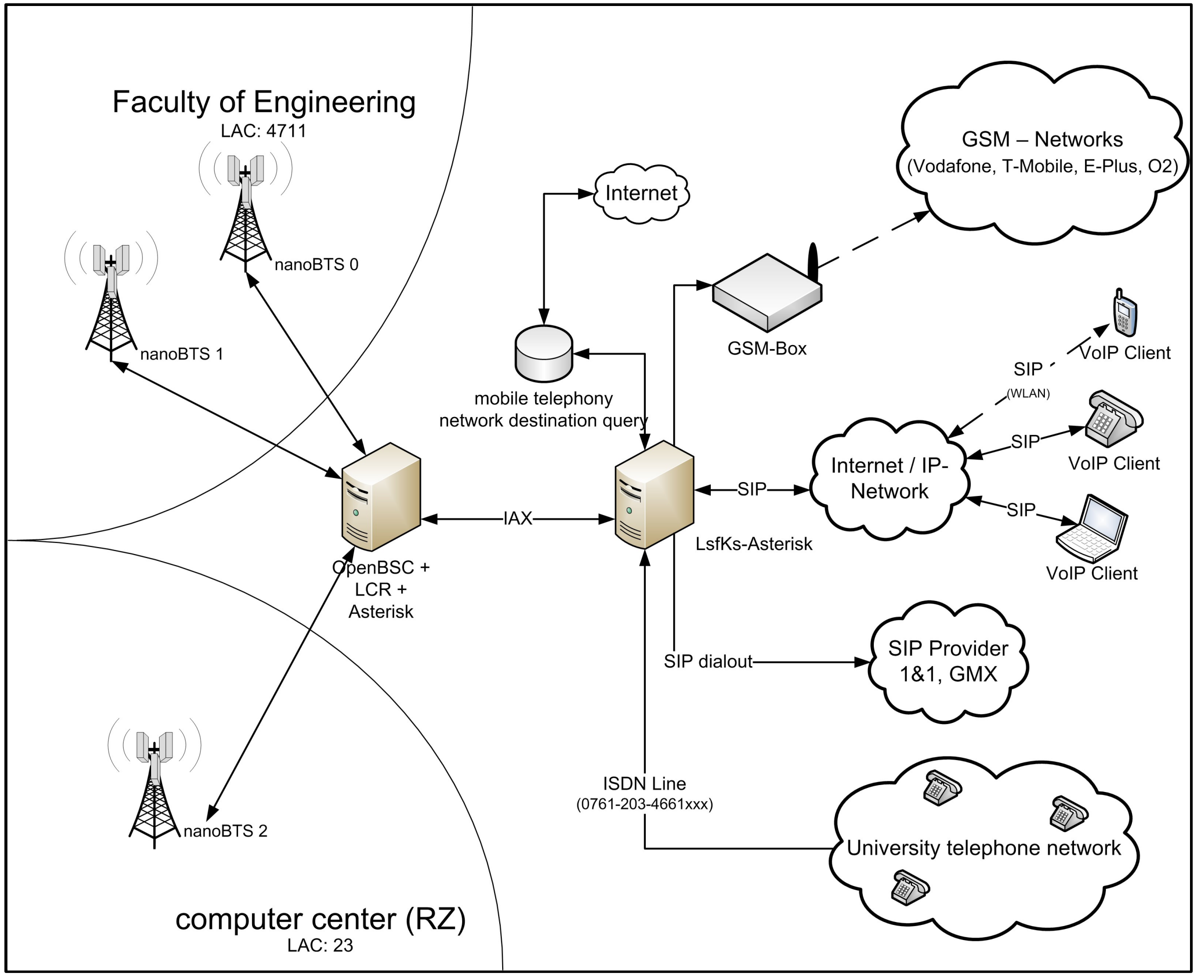
Connection to:

- SIP

- ISDN

- mobile networks

- fixed networks

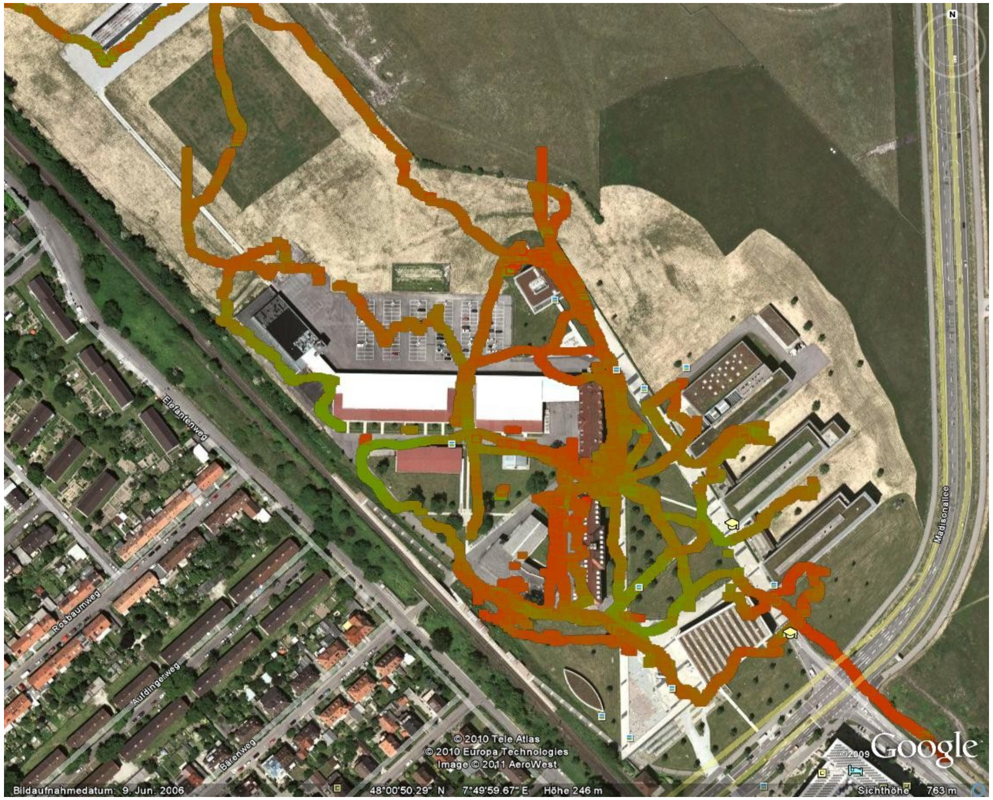


3. Our own GSM network

- Measuring the received signal strength

Can we use this data to calculate the position of a subscriber?

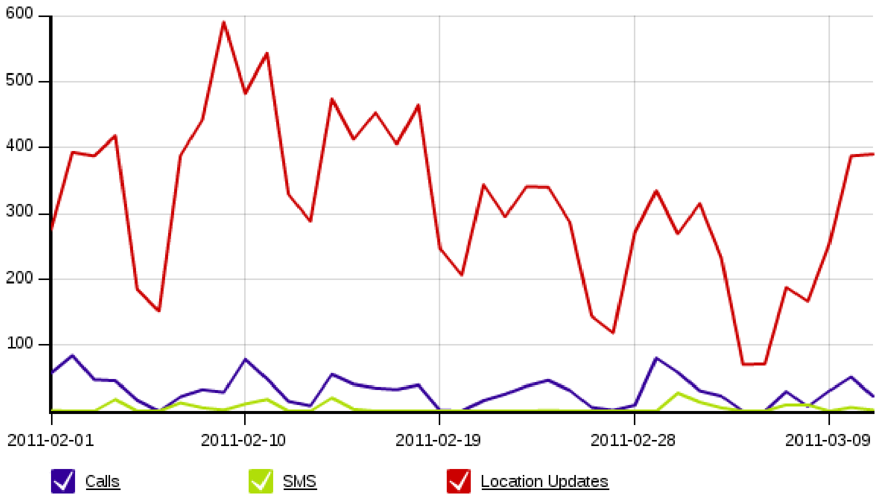
- How precise is it?
- Comparison of different approaches
- Ongoing research



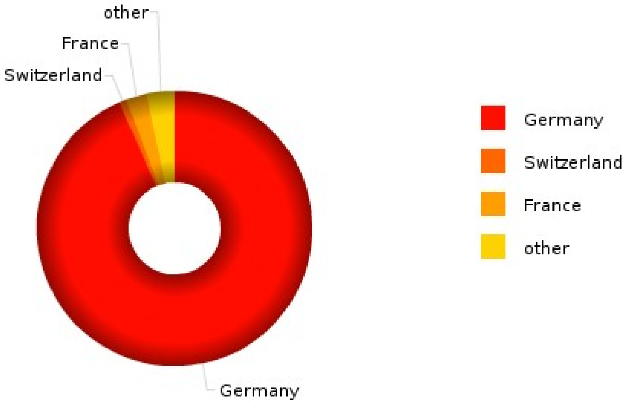
received signal strength at the faculty site

3. Our own GSM network

- Statistics about the network
  1.2.2011 to 9.3.2011



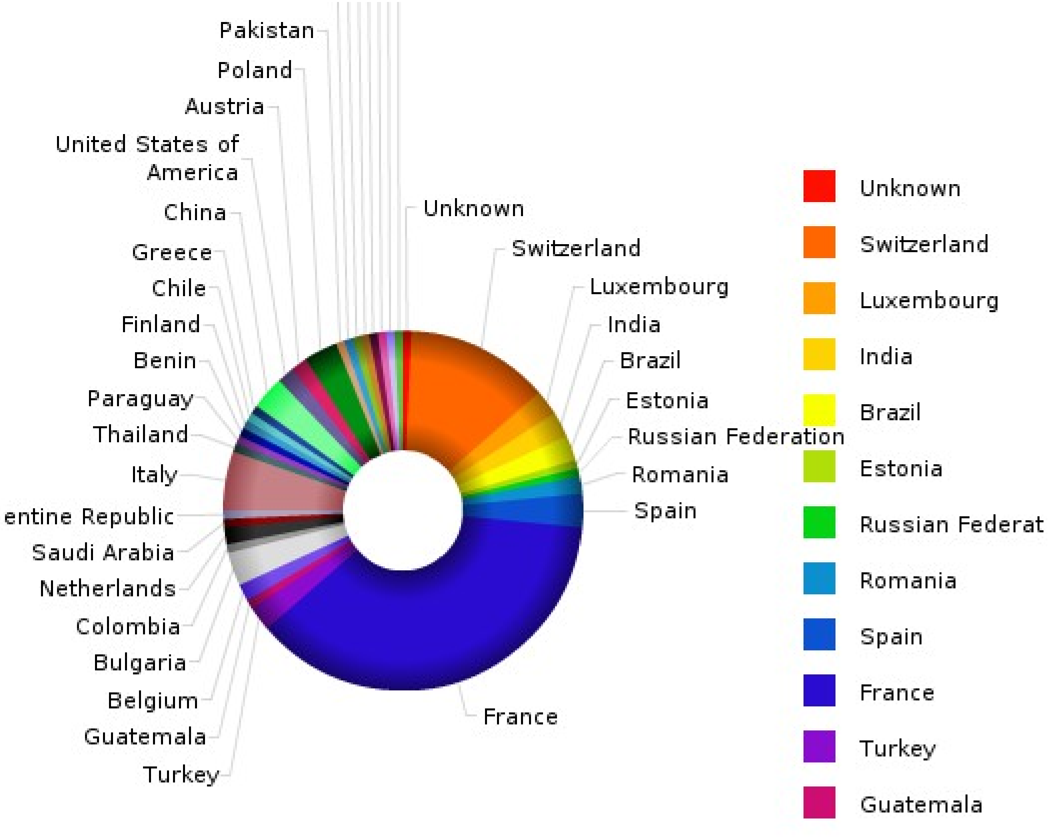
number of calls, SMS and location updates



origin of the subscribers

3. Our own GSM network

- Statistics about the network
  1.2.2011 to 9.3.2011



subscribers without Germany

Overview

1. GSM Infrastructure
2. Analysis of GSM
3. Our own GSM network
4. Security
   - 4.1 Localization
   - 4.2 IMSI-Catcher
   - 4.3 Encryption A5/1

4. Security on GSM

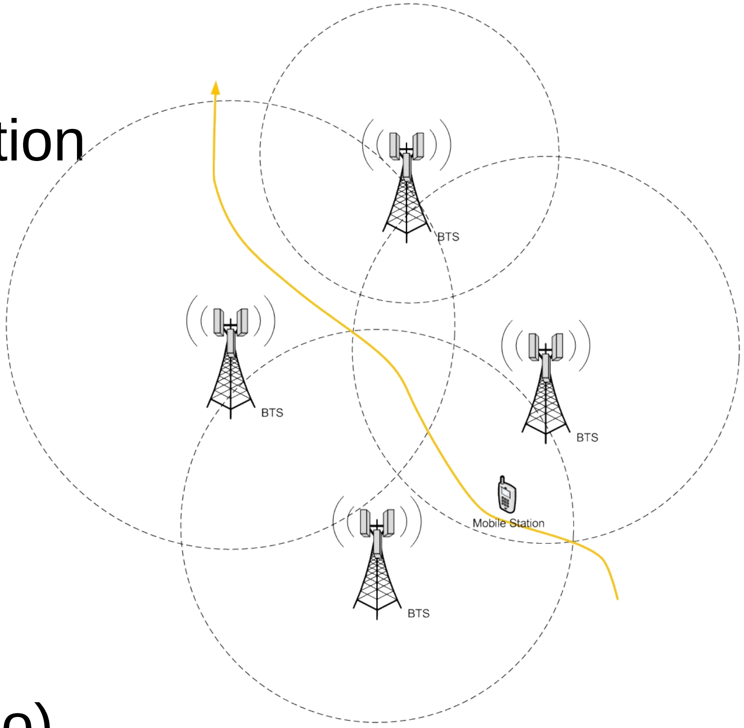
- Original intention:
  - Anonymization of subscribers (usage of temporary identifier TMSI)
  - Prevention of eavesdropping (encryption)
- Through the lack of computing power and suitable hardware for analysis, GSM was "secure" for a long time.
- But by now there exists several hardware components and software projects that can be used to analyze, crack and build up GSM networks.

4. Security on GSM

- Problems:
  - No physical access needed for attackers (e.g. cable-based communication)
  - Radio waves spread with less/no control.
  - Much information is not encrypted during transmission.

4.1 Localization in GSM

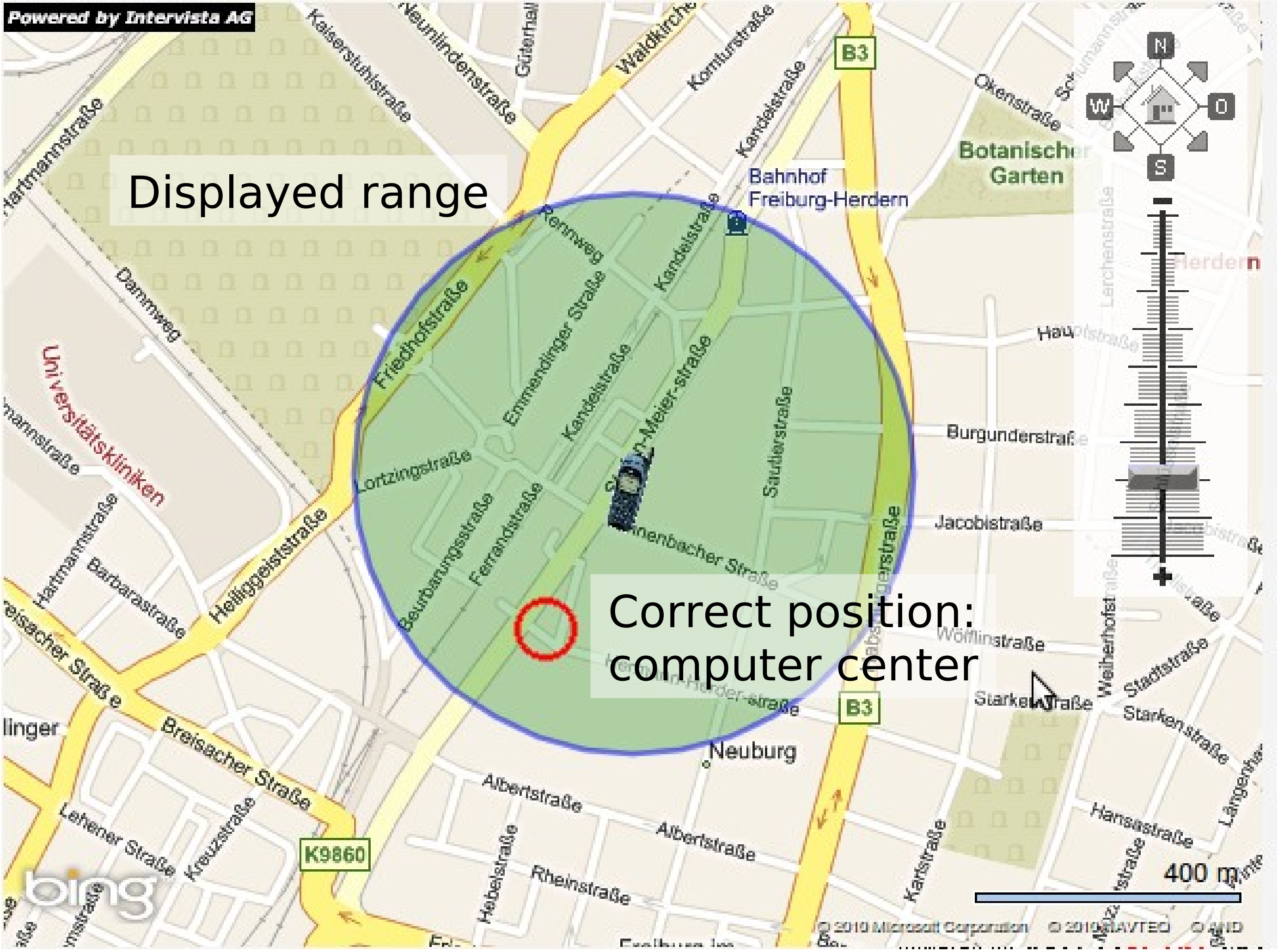
- Why is it necessary to know the position?
  - Subscribers are moving
    - The network has to know approximate position in order to deliver calls or SMS.
  - Security reasons
    - In case of emergency / prosecution
  - Charging / Services
    - Use the position for charging different fees (e.g. home zone)
  - Information-based
    - Where is the next restaurant?
  - Position-based
    - Business aspects (tracking cargo)



4.1 Localization in GSM

- Accuracy: Depends on the density of the network
  - City: up to a few (hundred) meters
  - Rural area: up to several kilometers
  - Improvement: Combination with GPS
- How does it work?
  - Depends on the service provider
    - HLR lookup of the last known position
    - Active lookup by sending silent SMS to get the current position
- Problem:
  - Misuse of the data
  - It is not clear what happens with the data:
    - e.g.: The Austria provider A1 sells anonymized data

4.1 Example: Localization in GSM



Displayed range

Correct position: computer center

Overview

1. GSM Infrastructure
2. Analysis of GSM
3. Our own GSM network
4. Security
   - 4.1 Localization
   - 4.2 IMSI-Catcher
   - 4.3 Encryption A5/1

4.2 IMSI-Catcher

- IMSI:
  - Worldwide unique identifier for the SIM
  - Stored on the SIM
- IMEI:
  - Worldwide unique identifier for the Mobile Station
- IMSI-Catcher:
  - May only be used by public authorities (in Germany)
  - Price is really high (> $100 000 Rohde & Schwarz)
  - But with USRP you can build a cheap one (~ $1500).
- Problems:
  - Identity of the user can be revealed
  - Record conversation
  - Produce a moving profile

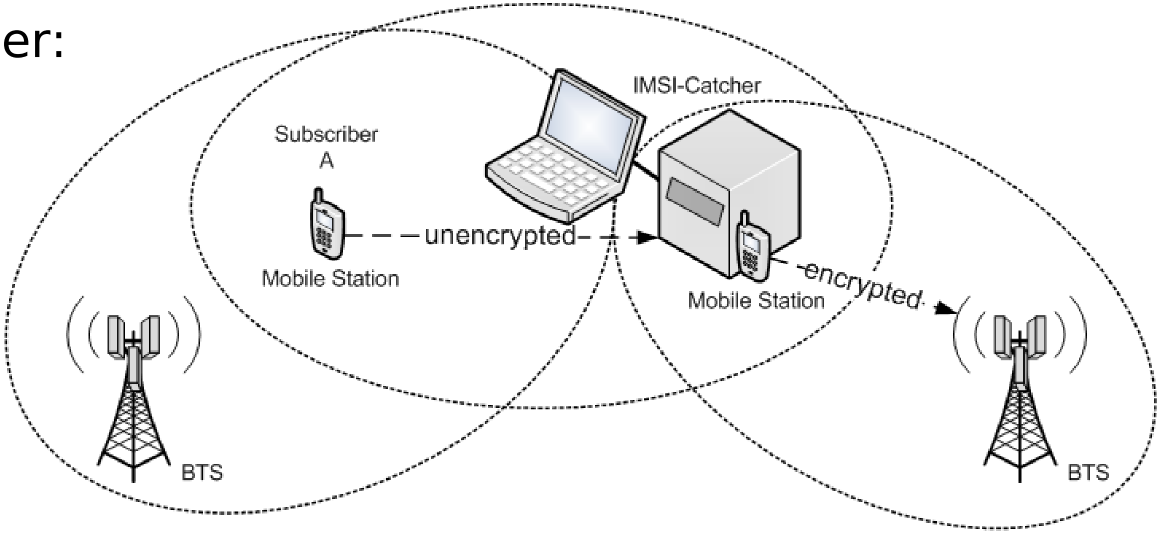
4.2 IMSI-Catcher

- How does it work?
  - Simulates a base station as part of a regular mobile radio network (in Germany: D1, D2, E-Plus, O2)
  - During the login procedure the Mobile Station transmits the IMSI / IMEI.

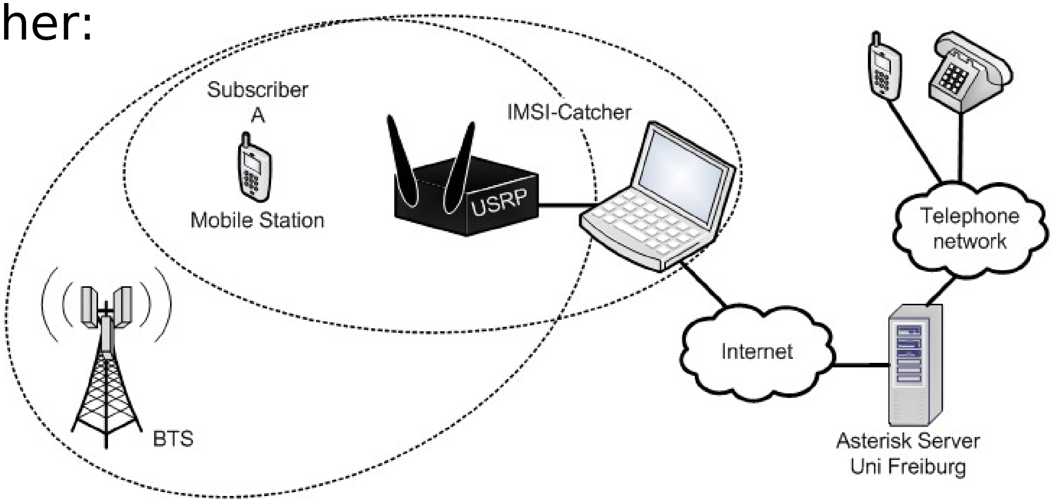
- This is successful because GSM doesn't provide mutual authentication. Only the Mobile Stations have to authenticate correctly.

4.2 IMSI-Catcher

'Standard' IMSI-Catcher:



Open Source IMSI-Catcher:



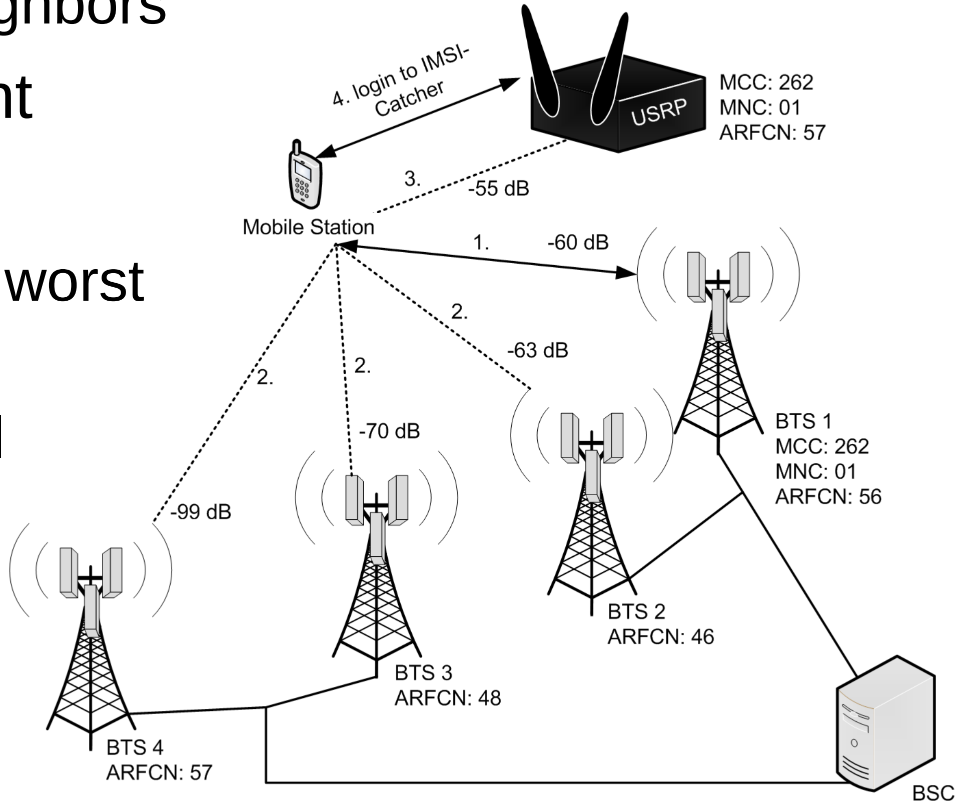
4.2 Login to IMSI-Catcher

- How to induce the Mobile Station to switch to the IMSI-Catcher?
- Mobile Station:
  - Stores the last used frequency on SIM.
  - Don't scan the whole frequency-band if it has a connection.
  - Try to stay in the formerly used network.
  - Use the neighborhood list to scan for proper BTS.
- Problem:
  - If the IMSI-Catcher isn't on the neighborhood list, it will not be recognized.
- Solutions:
  - Force the Mobile Station to switch to the IMSI-Catcher.
  - Use a GSM-Jammer to induce the Mobile Station to rescan the frequency-band

4.2 Login to IMSI-Catcher

Forcing the Mobile Station to switch to the IMSI-Catcher:

1. Mobile Station listens to BTS1
   - BTS1: Transmits list of neighbors
2. Neighborhood-Measurement
3. Turn IMSI-Catcher on
   - Fake BTS4, which has the worst receiving signal strength.
   - MS believes that the signal strength of BTS4 is now better than the signal strength of BTS1.
4. MS switch to IMSI-Catcher.

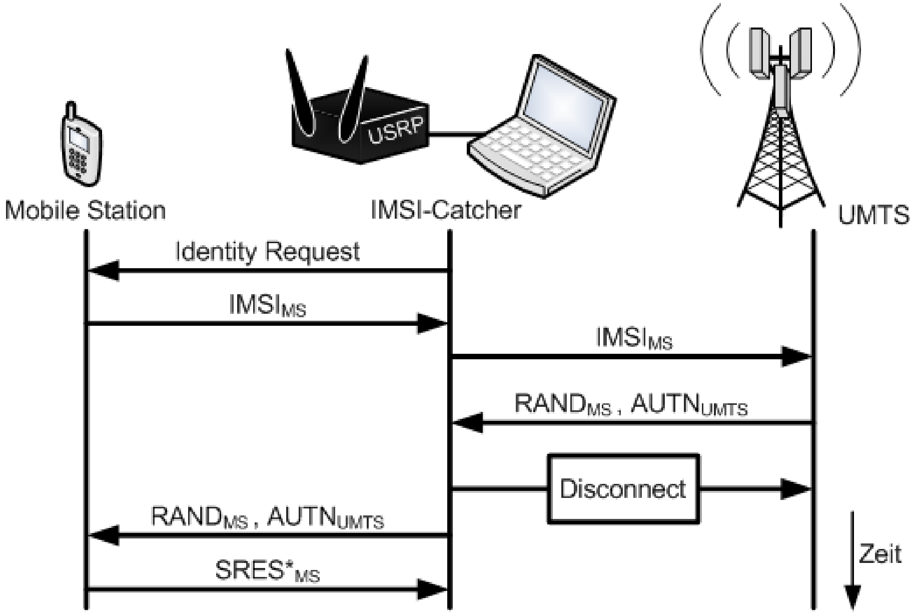


4.2 Protection against IMSI-Catchers

- „Catching“ IMSI:
  - No protection against catching the IMSI
  - Mobile phone can not differentiate between the “visible” radio cells
- Normally the user should be notified of the use of an unencrypted network.
  But:
  - Modern devices do not display if the connection is secure or not.
  - Notification about unencrypted connections can be disabled via a flag on the SIM card.
- Solution: Use cryptographic enabled mobile phones with an end-to-end encryption.

4.2 Protection against IMSI-Catchers

- Is it sufficient to use UMTS Mobile Stations for protection? No!:
  - A fall-back-to-GSM-function exists if there is no surrounding UMTS network available.
    => UMTS-Jammer
  - It is theoretically possible to build a UMTS-IMSI-Catcher



Overview

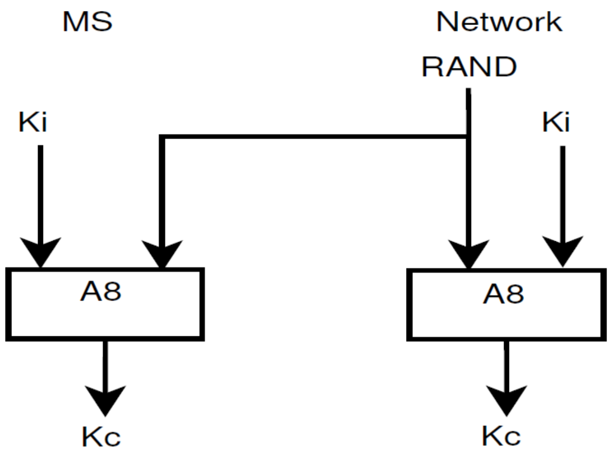
1. GSM Infrastructure
2. Analysis of GSM
3. Our own GSM network
4. Security
   - 4.1 Localization
   - 4.2 IMSI-Catcher
   - 4.3 Encryption A5/1

4.3 Encryption A5/1

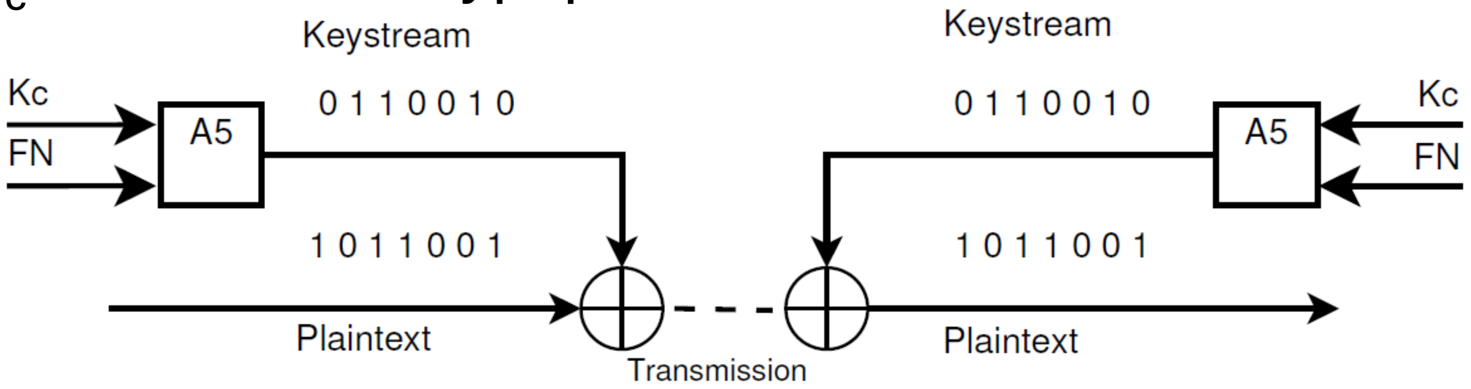
- Content of the communication is encrypted (speech data, SMS)
- Three GSM encryption standards:
  - A5/0: no encryption. Should not be used.
  - A5/1: “strongest” encryption. Currently used.
  - A5/2: weak encryption. No longer used.
- Encryption Algorithm A5/1 developed in 1987
  - Only 64 Bit Key
  - Security by Obscurity
  - General Design leaked in 1994, fully reverse engineered in 1999

4.3 Encryption A5/1

- Session key K_c is calculated from private key K_i and random number RAND



- K_c is used to encrypt plaintext:



4.3 Encryption A5/1

- Problem:
  - Algorithm is too old and not longer save.
  - Key space can be reduced
  - With today's computing power the encryption can be broken in seconds by using rainbow tables.
  - Interception of GSM signals is no longer a problem.
    - USRP
    - Motorola C123 with OsmocomBB[1]

Motorola C123

[1] OsmocomBB: http://bb.osmocom.org/

4.3 Encryption A5/1

- Rainbow Tables
  - Size 1.7 TB
  - Calculated with ATI graphic cards.
  - Available on the Internet via bittorrent.
- Attack is based on known plaintext
  - Some signaling messages are known both unencrypted and encrypted.
  - Session key K_c can be calculated in seconds.
  - Private key K_i can not be calculated with this attack. But this is not necessary to decode the encrypted data.

4.3 Encryption A5/1

- GSM encryption is no longer secure
- **BUT:** More and more devices are using GSM to transmit data.
  - Mobile TAN for online banking:
    TAN transmitted via SMS
  - Vending machines:
    Information about the fill level
  - Railway GSM:
    Information about the status of the train
  - Smart meter:
    Information about the electricity consumption
- Is this really a good idea?