PROTECTION IN MOBILE COMMUNICATION SYSTEMS

Trustworthy mobility management in telecommunication networks

Hannes Federrath

TU Dresden

INTRODUCTION

SECURITY DEFICITS

BASIC CONCEPTS

- Broadcast
- Trusted fixed station
- location hiding with MIXes

PERFORMANCE

SUMMARY

Security deficits of existing mobile networks

Example for security demands: Cooke, Brewster (1992)

1. protection of user data
2. protection of signalling information, incl. location
3. user authentication, equipment verification
4. fraud prevention (correct billing)

Security deficits of existing mobile networks

- only symmetric cryptography (algorithms not officially published)
- only weak protection of location, i.e. against outsider attacks
- no protection against insiders (location, message content)
- no end-to-end services (authentication, encryption)
- no anonymous communication (similar to public phones)

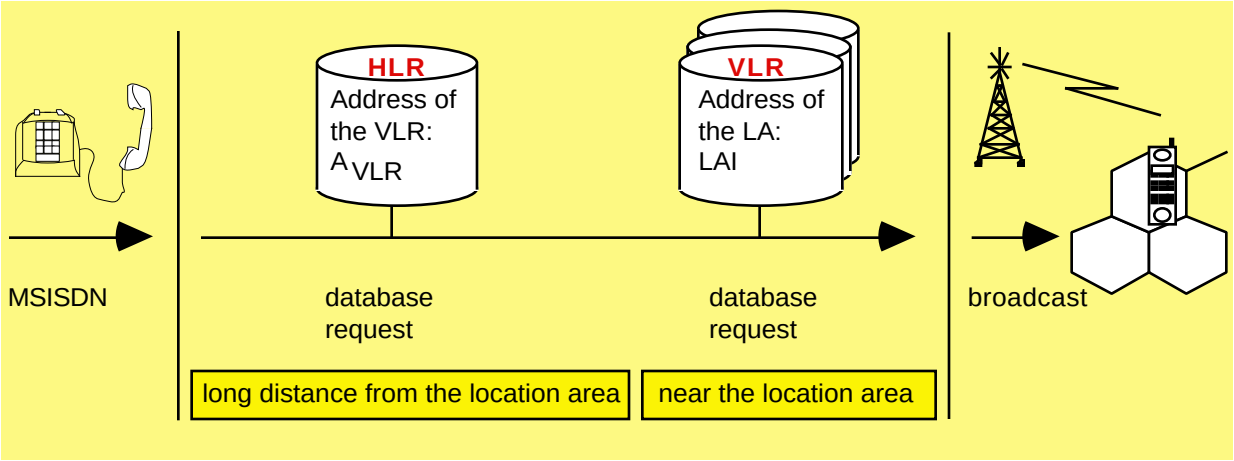
Summary

- protection against external attackers only
- Mouly, Pautet: (1992)
  „…the designers of GSM did not aim at a level of security much higer than that of the fixed trunk network.“

Trustworthy mobility management – The problem

Location management in GSM networks

– Global System for Mobile Communication



– distributed storage at two stages

- Home Location Register (HLR) & Visitor Location Register (VLR)

– network operator has a global view of the location information

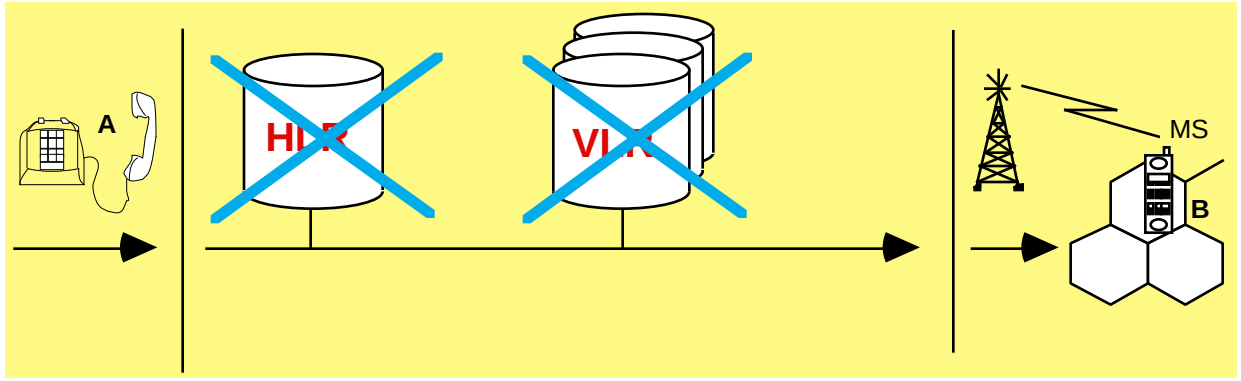
– tracking of mobile users and movement profiles possible

The privacy aspect

– confidentiality of the location information

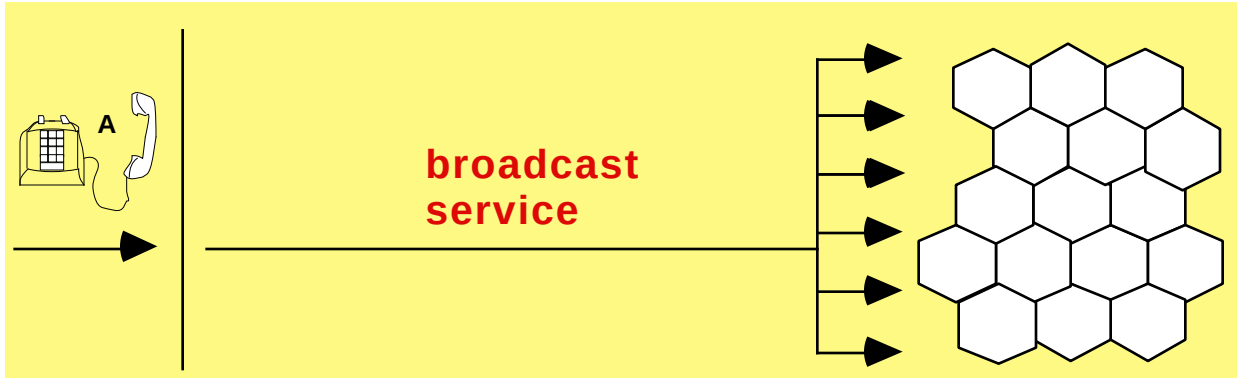
Basic concepts: Global broadcast

Global System for Mobile Communication (GSM)



«Global» broadcast

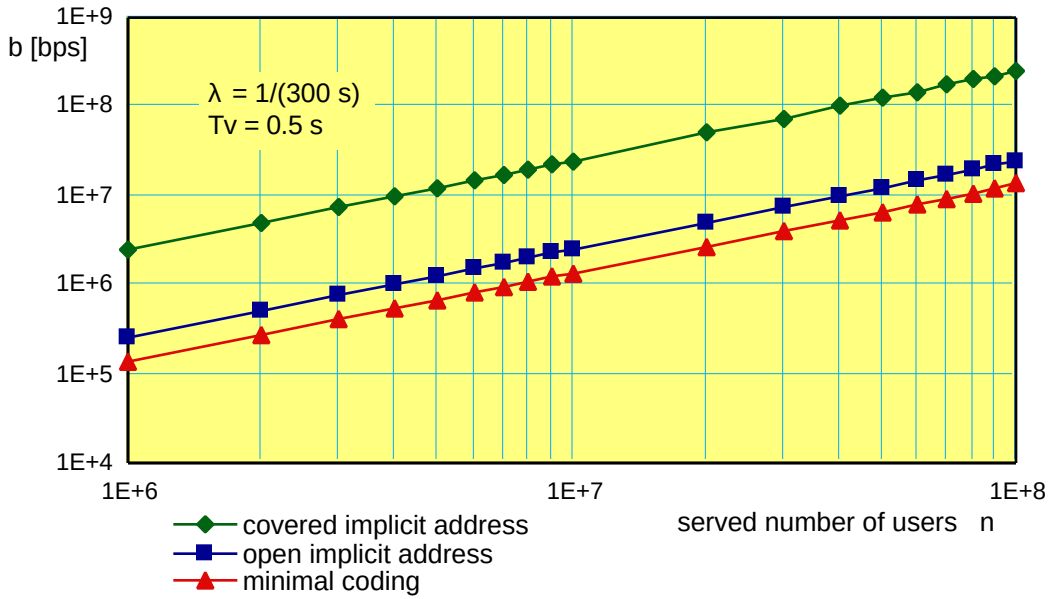
– no storage of locations: global paging



Broadcast – No storage of locations

Performance

– estimated number of users in the year 2000 in Europe: $80 \cdot 10^6$



– capacity needed for the broadcast channel: 10 Mbps

(efficient implementation of implicit addressing, open implicit addresses)

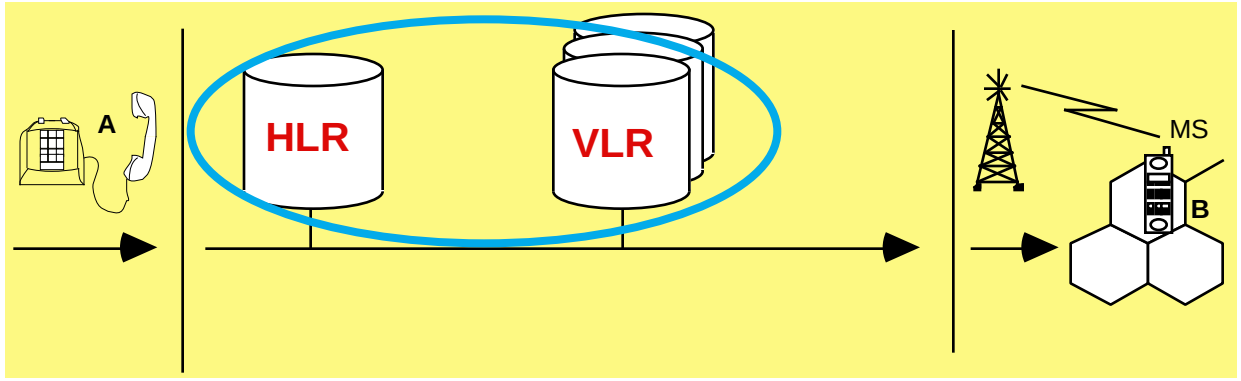
Realization

– low earth orbit satellites (global availability), overlay cells

– commercial paging services

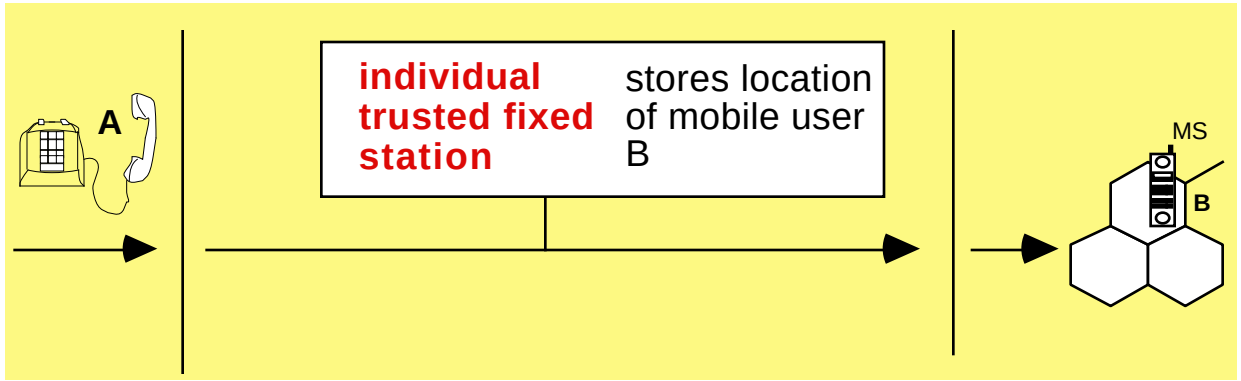
Basic concepts: Trusted fixed station

Global System for Mobile Communication (GSM)



Trusted fixed stations under control of each user

– replace databases by trusted devices in the fixed network



Security aspects

Methods with a trusted fixed station

Unauthorized requests by the network operator

- leads to localization
- defense: logging of requests by the trusted fixed station and logging of successfull mobile terminating calls, unusual frequency of differences indicate attacks
- normally: movement tracks with granularity of call frequencies

Observability of communication

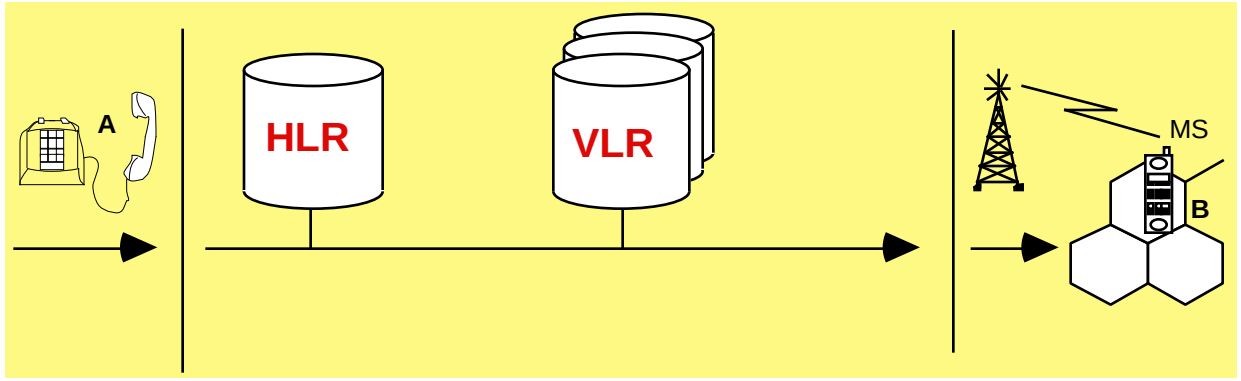
- between the mobile user and his trusted fixed station:
  location updating uncovers the location

Centralization and decentralization

- decentralization increases efficiency, not security

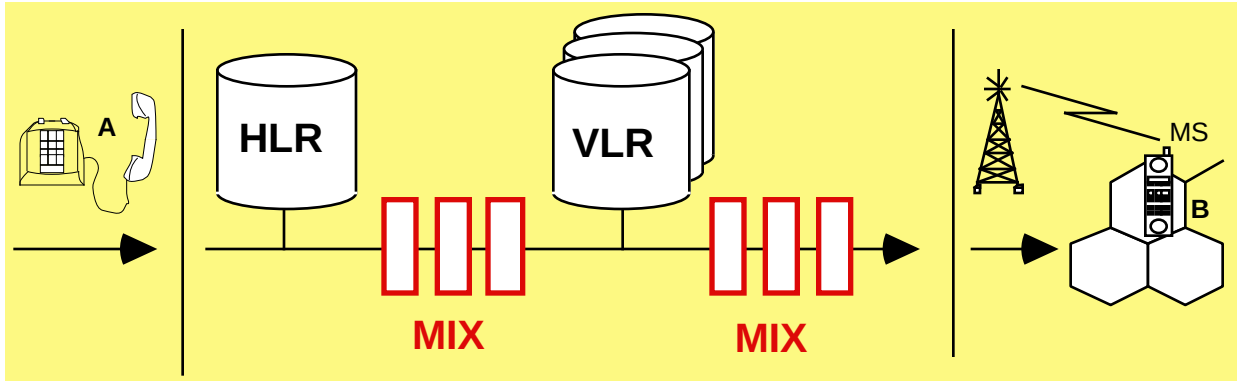
Basic concepts: Location hiding

Global System for Mobile Communication (GSM)



MIXes in mobile communication

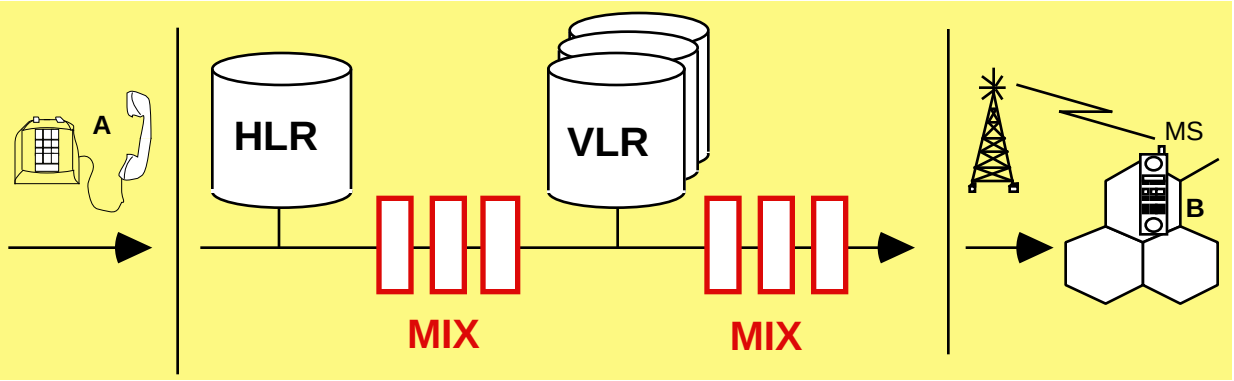
– covered storage of location information



Covered storage of location information

Location hiding

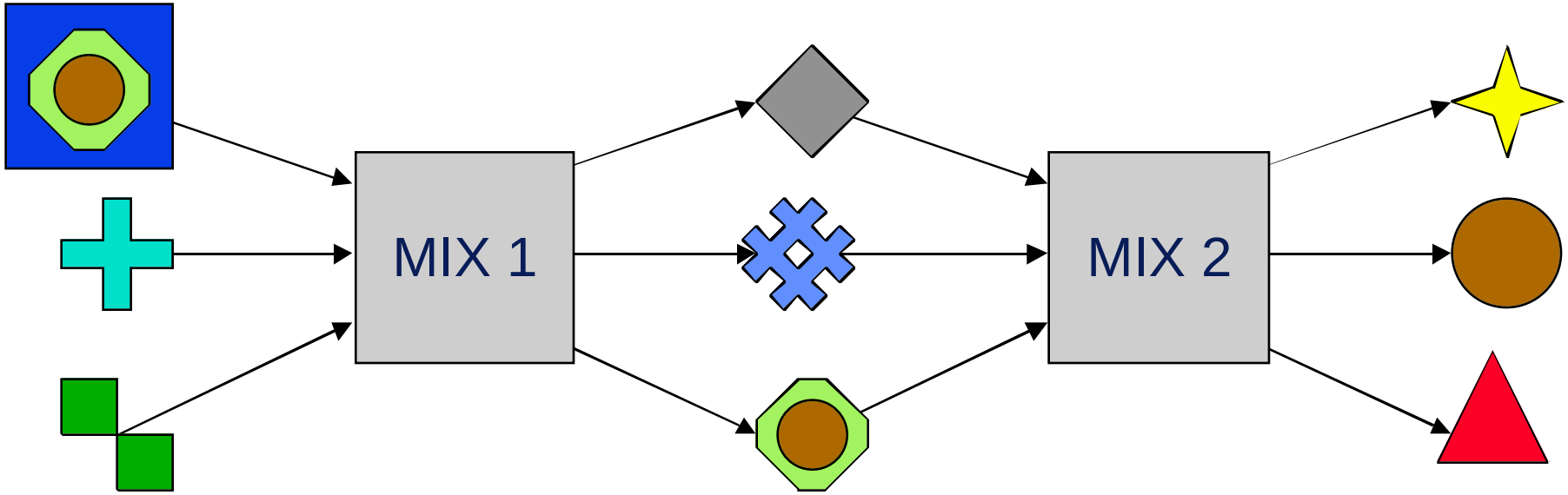
- location information is stored in a covered way
- MIX concept with untraceable return addresses is used
- mobile stations are involved into the MIX concept



location is not stored explicitly, but as a «path» through a MIX network

The MIX network

unlinkability of sender and recipient (Chaum 1981)



Functions of a MIX

1. store incoming messages
2. discard repeats
3. change encoding
4. change order
5. put messages out as a batch

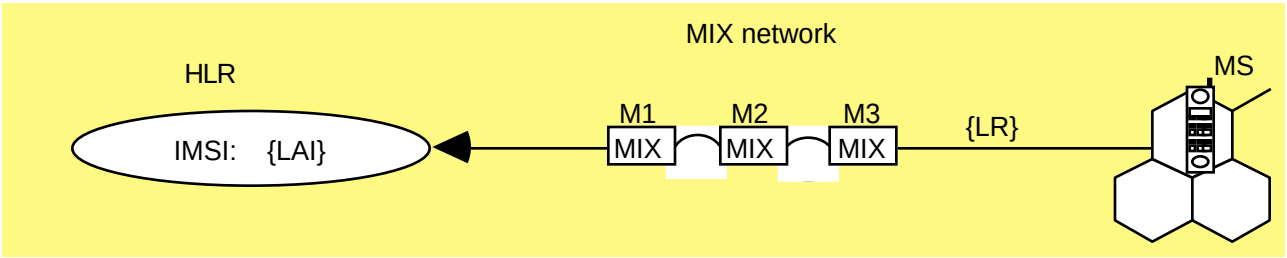
Attributes usable for linkability

- timing relations between input and output
- coding relations
- coding is based on asymmetric cryptography

MIXes in mobile communications

M_i	MIX i in a cascade
c_i	public encryption key
d_i	private decryption key (only known by M_i)

Location registration — centralized



1. MS computes «covered» location information

$$\{\mathrm{LAI}\} := c_1 (k_1, c_2 (k_2, c_3 (k_3, \mathit{ImpAdr})))$$

2. MS sends registration message (MS → MIXes → HLR)

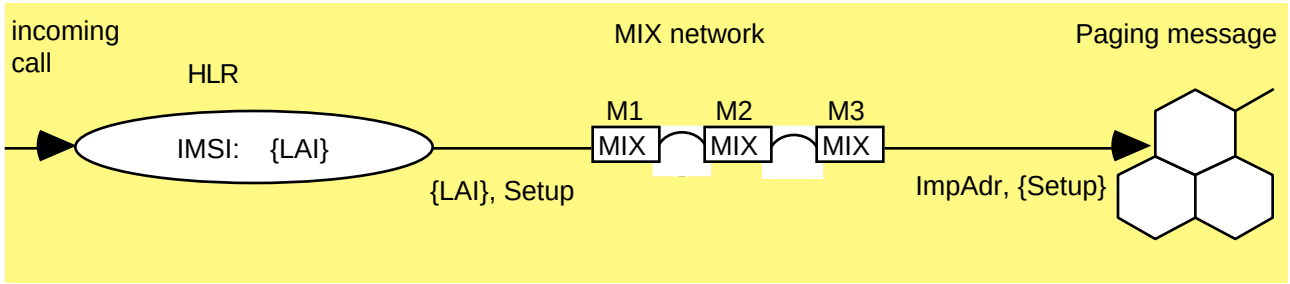
$$\{\mathrm{LR}\} := c_3 (c_2 (c_1 (\mathit{IMSI}, \{\mathrm{LAI}\})))$$

notation does not show random numbers in {LR}

MIXes in mobile communications

M_i	MIX i in a cascade
c_i	public encryption key
d_i	private decryption key (only known by M_i)

Call setup (mobile terminating) — centralized



1. access HLR database entry

$$\text{IMSI: } \{\text{LAI}\} = c_1 (k_1, c_2 (k_2, c_3 (k_3, \mathit{ImpAdr})))$$

2. send call setup message

$$\{\text{LAI}\}, \text{Setup}$$

3. MIXes: {LAI} is decrypted and Setup will be encrypted

$$\{\text{Setup}\} := k_3 (k_2 (k_1 (\text{Setup})))$$

4. Paging of the call

$$\mathit{ImpAdr}, \{\text{Setup}\}$$

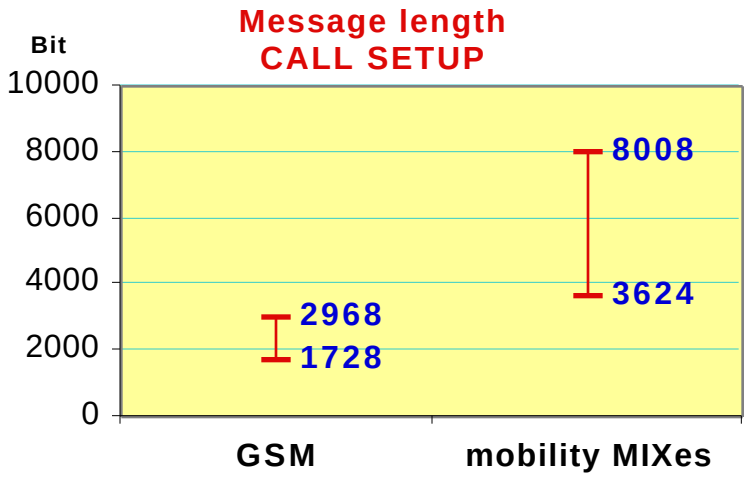
Performance

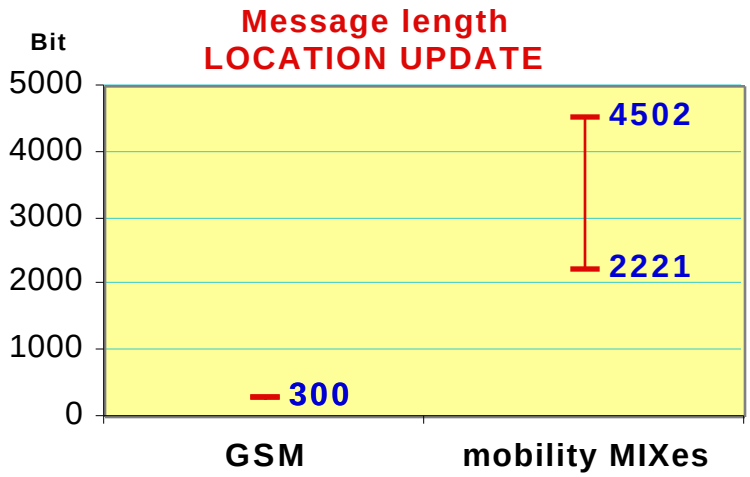
Message length on the air interface compared to GSM

Message length increases by a

- factor ≥1.2 for call setup and
- factor ≥ 6.8 for location updating

message length in bit	GSM	mobility MIXes
call setup	1728…2968	3624…8008
location updating	216…324	2221…4502





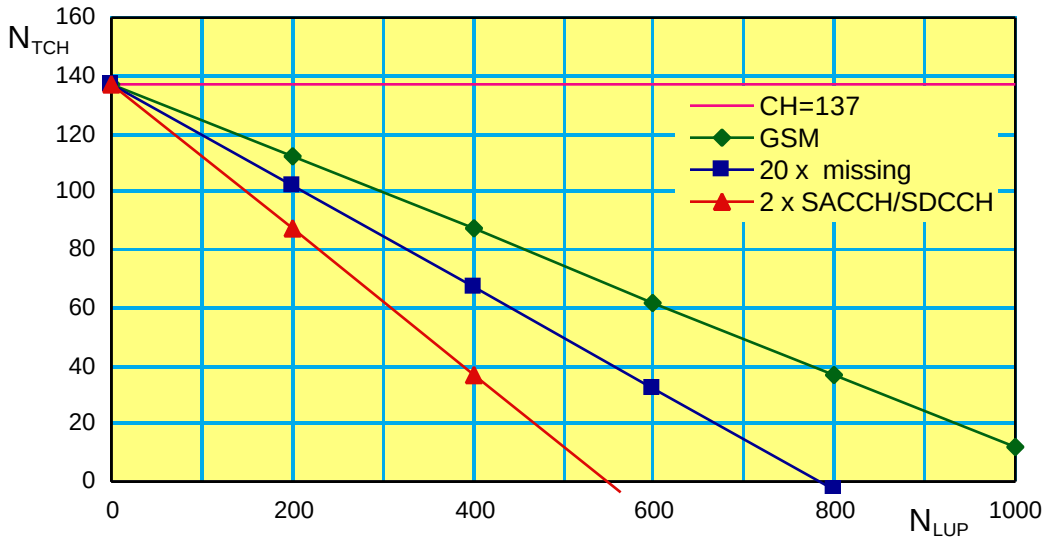
Efficiency

Measure of efficiency

– ratio of available traffic channels: $\frac{\text{GSM}}{\text{mobility MIXes}}$

– mobility behaviour of the users influences the efficiency

number of simultaneous available traffic channels



-

– decrease in serveable number of users is about 10 % with N_{LUP}=88 in 5 seconds (corresponds to 20.000 users per cell)

Summary of the basic concepts to protect locations

No storage of location information

- broadcast of mobile terminating calls
- immense bandwidth for paging needed
- no costs for location updating

Trusted fixed stations (TFS) under control of each user

- TFS stores the location information
- or stores a pseudonym
- pseudonymous location management

Covered storage of location information

- no trusted fixed station needed
- unobservable communication
- decentralization of security functions (MIXes)