MIXes in mobile communication systems: Location management with privacy

Hannes Federrath, Anja Jerichow, Andreas Pfitzmann

University of Dresden, Institute of Theoretical Computer Science
D-01062 Dresden, Germany

{federrath, jerichow, pfitza}@inf.tu-dresden.de

The problem

The Idea

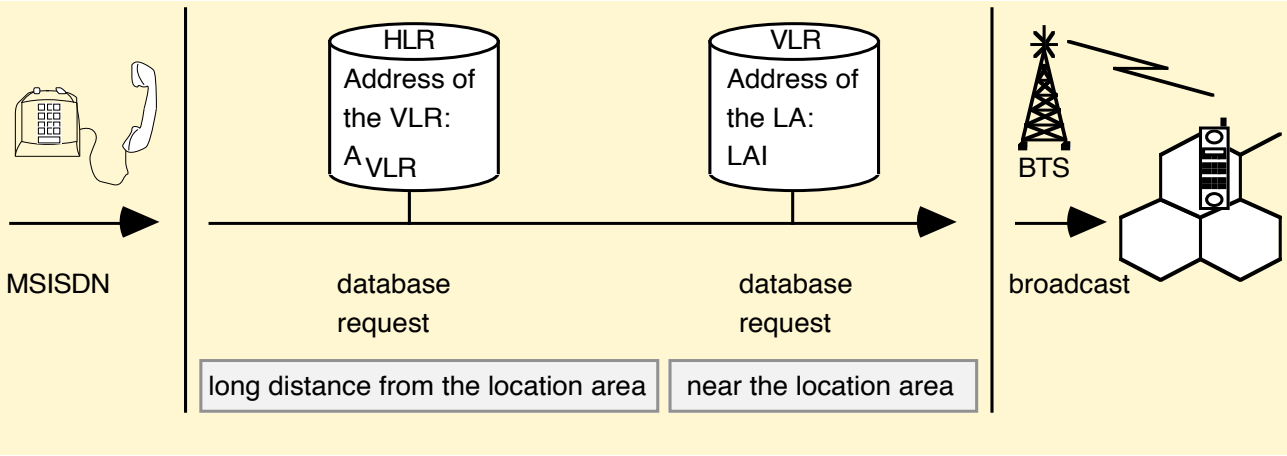
The MIX network

MIXes in mobile communications — the new procedures

Advantages and problems

The problem

Location management in GSM networks



- distributed storage at two stages
  - Home Location Register & Visitor Location Register
- network operator has a global view of the location information
- tracking of a mobile subscriber

The privacy aspect

- confidentiality of the location information

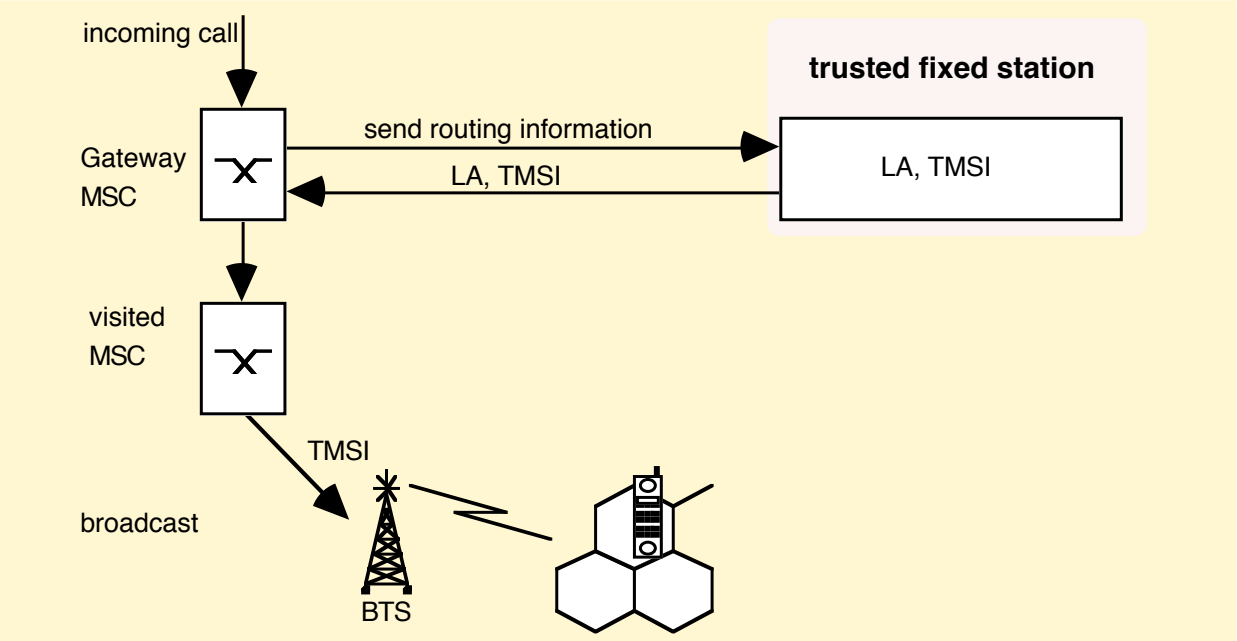
Related work

- trusted fixed station
  - stores the location information
  - stores a pseudonym,
    pseudonymous location management in GSM

Related works

Trusted fixed station

– stores the location information (centralized)



– stores a pseudonym,

decentralized pseudonymous location management in GSM

Trusted fixed station — trusted for whom?

– only trusted for the mobile subscriber

Centralization and decentralization

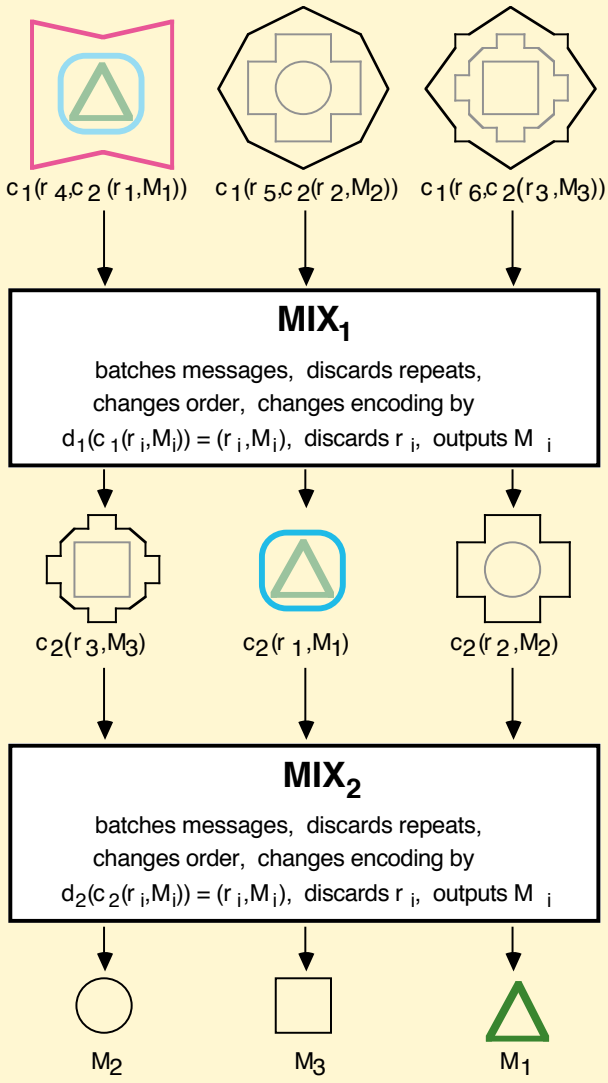
– decentralization increases the efficiency, not the security

The Idea

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

The MIX network

- unlinkability of sender and receipient (Chaum 1981)



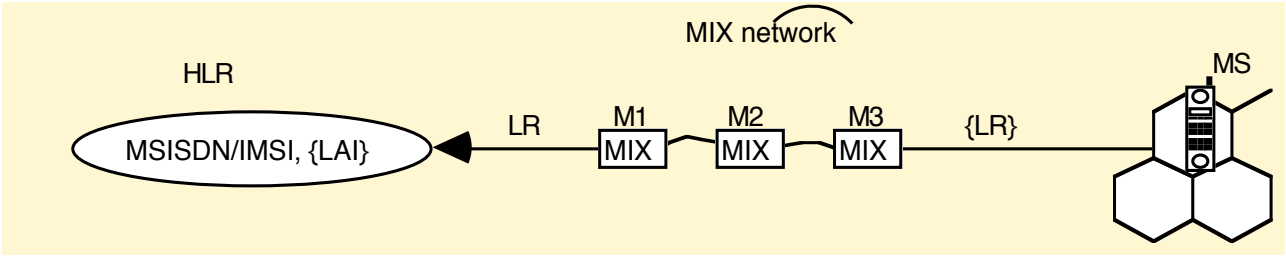
c_j is the public key of MIX $_j$ to cipher,
d_j is the private key of MIX $_j$ to decipher,
r_i are random bit strings, M_i are messages

Functions of a MIX

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

MIXes in mobile communications — the new procedures

Location registration — centralized



Location registration message

{LR} := A_{M3}, c_{M3}(A_{M2}, c_{M2}(A_{M1}, c_{M1}(A_{HLR}, LR))) with

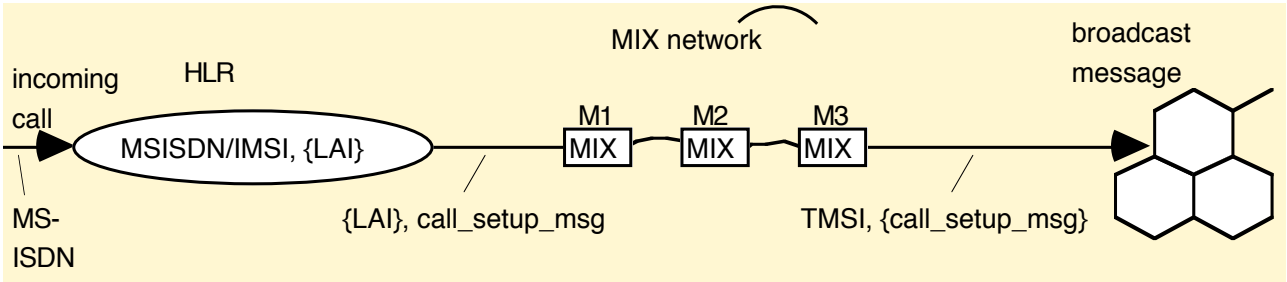
LR := IMSI, {LAI}, location_registration_msg

random numbers in {LR} not noted!

«Covered» location information

{LAI} := A_{M1}, c_{M1}(k_{M1}, A_{M2}, c_{M2}(k_{M2}, A_{M3}, c_{M3}(k_{M3}, TMSI)))

Call setup (mobile terminated) — centralized

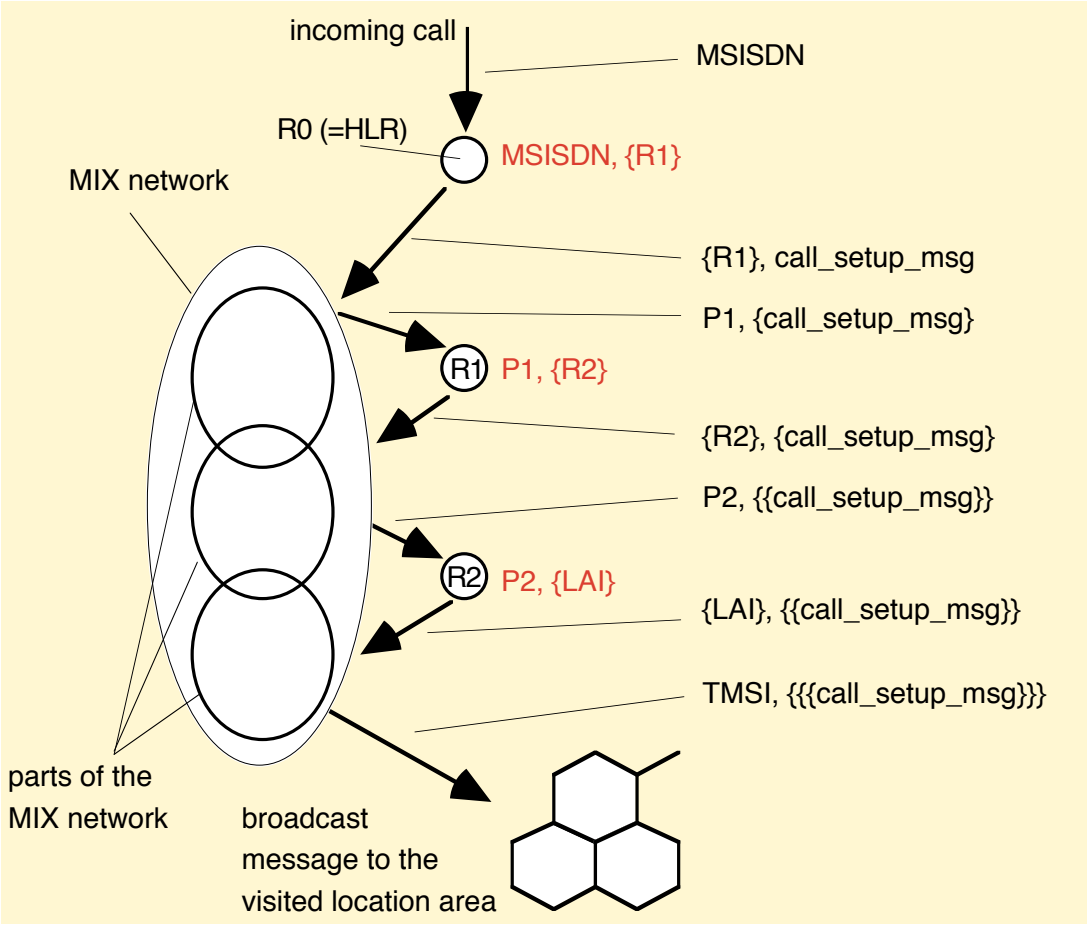


Call setup message

{call_setup_msg} := k_{M3}(k_{M2}(k_{M1}(call_setup_msg)))

MIXes in mobile communications — the new procedures (2)

Decentralized procedure (schematic)



- R0, R1 and R2 are registers
- {R1}, {R2} and {LAI} are untraceable return addresses
- P1 and P2 are pseudonyms (inside {R1} and {R2})

- chained list of untraceable return addresses
- use parts of the MIX networks close to Ri for efficiency

Advantages and problems

Advantages

- procedures can be decentralized
  - trusted fixed station is fixed
  - consequently difficult to decentralize
- no trustworthy environment is needed
- procedures with trusted fixed stations need a MIX network for untraceable location update
- location is not stored explicitly, however as a «path» through a MIX network

Security and efficiency

- security and privacy depends on the security (untraceability) of the MIX network
- no trust in parts of the mobile network is needed (for confidentiality)
- MIX network is
  - not used to hold the recipient (mobile subscriber) anonymously
  - used to hide the routing information to the mobile subscriber
- increased signalling load (compared to GSM)
  - higher bandwidth is needed:
    public key cryptography (modulus > 500 bit)
  - higher delay ?