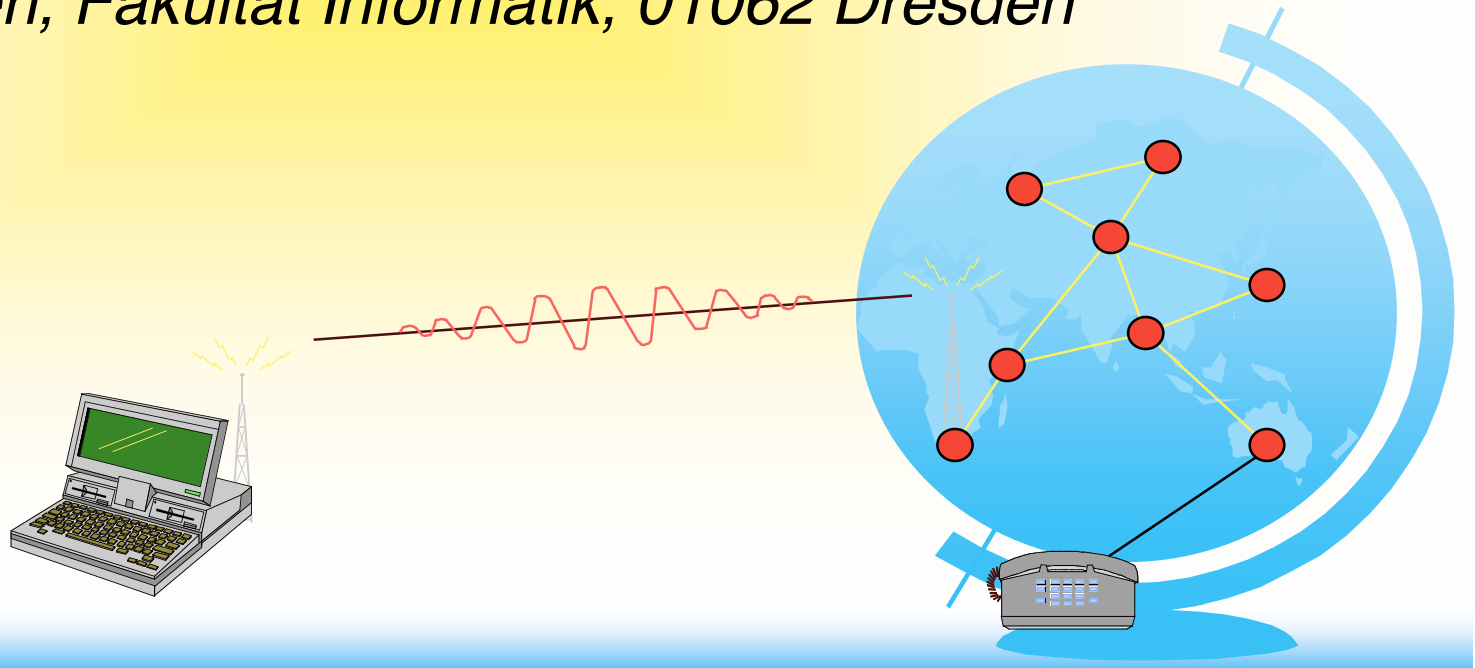
Unbeobachtbarkeit in Kommunikationsnetzen

Hannes Federrath, Anja Jerichow, Jan Müller, Andreas Pfitzmann

TU Dresden, Fakultät Informatik, 01062 Dresden

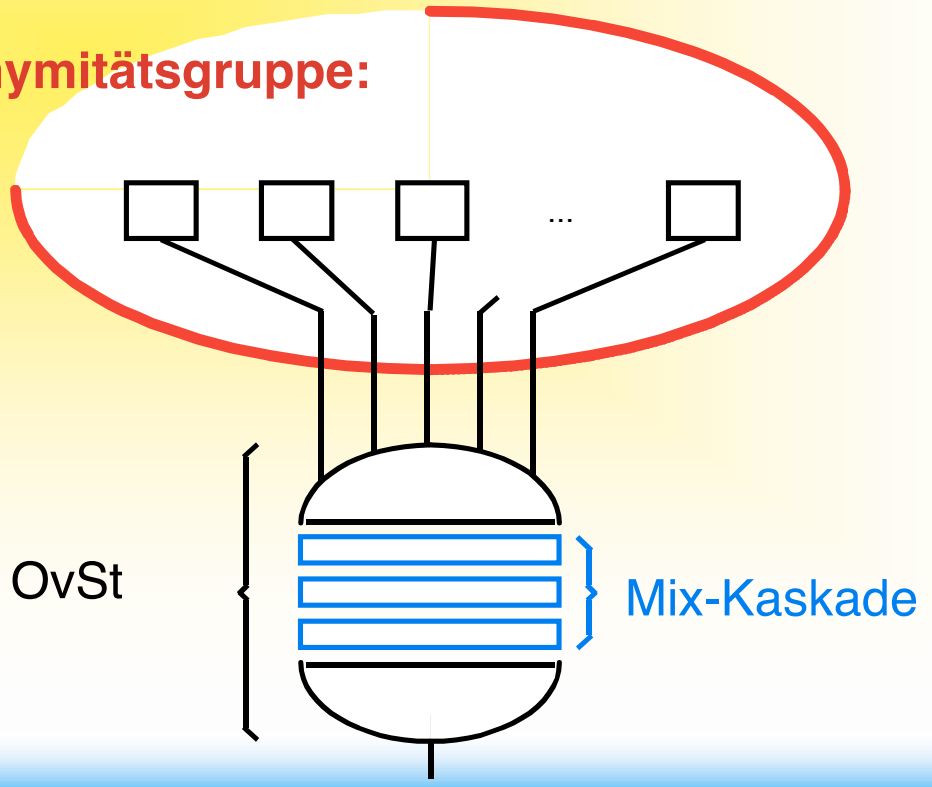


Anwendung des Mixverfahrens

- ISDN- (oder Telefon-) Mixe
  - Unbeobachtbarkeit der Kommunikationsbeziehung zwischen zwei Teilnehmern
    - gegenüber dem Netzbetreiber
    - gegenüber dem Kommunikationspartner
- Mobilkommunikationsmixe
  - Unbeobachtbarkeit der Kommunikationsbeziehung
  - Schutz der Vertraulichkeit des Aufenthaltsorts von mobilen Teilnehmern
    - auch gegenüber dem Netzbetreiber
    - gegenüber dem Kommunikationspartner

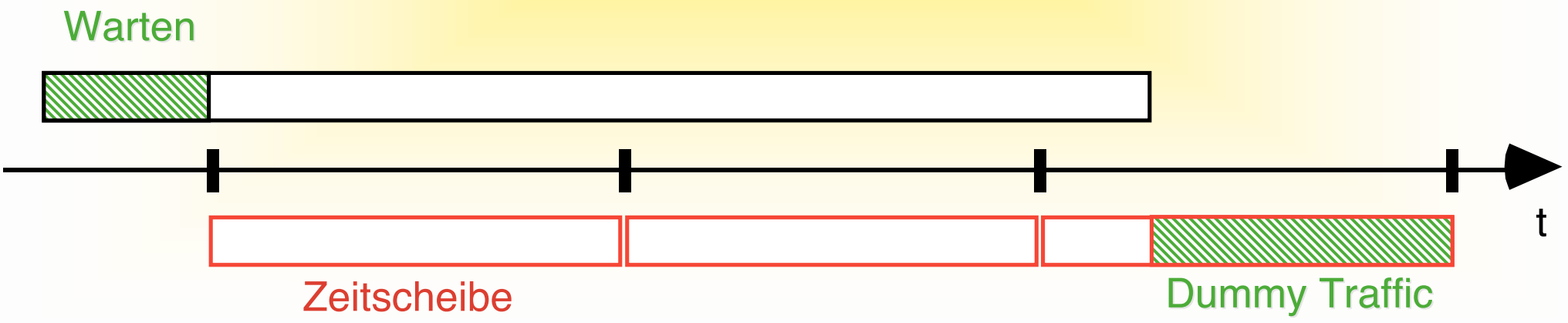
ISDN-Mixe

- Prinzip seit 1989 bekannt (Pfitzmann, Pfitzmann, Waidner)
- Gegenstand der Untersuchungen:
  - Implementierungsmöglichkeiten
  - Nachrichtenformate
  - Leistungsfähigkeit
  - Anwendbarkeit

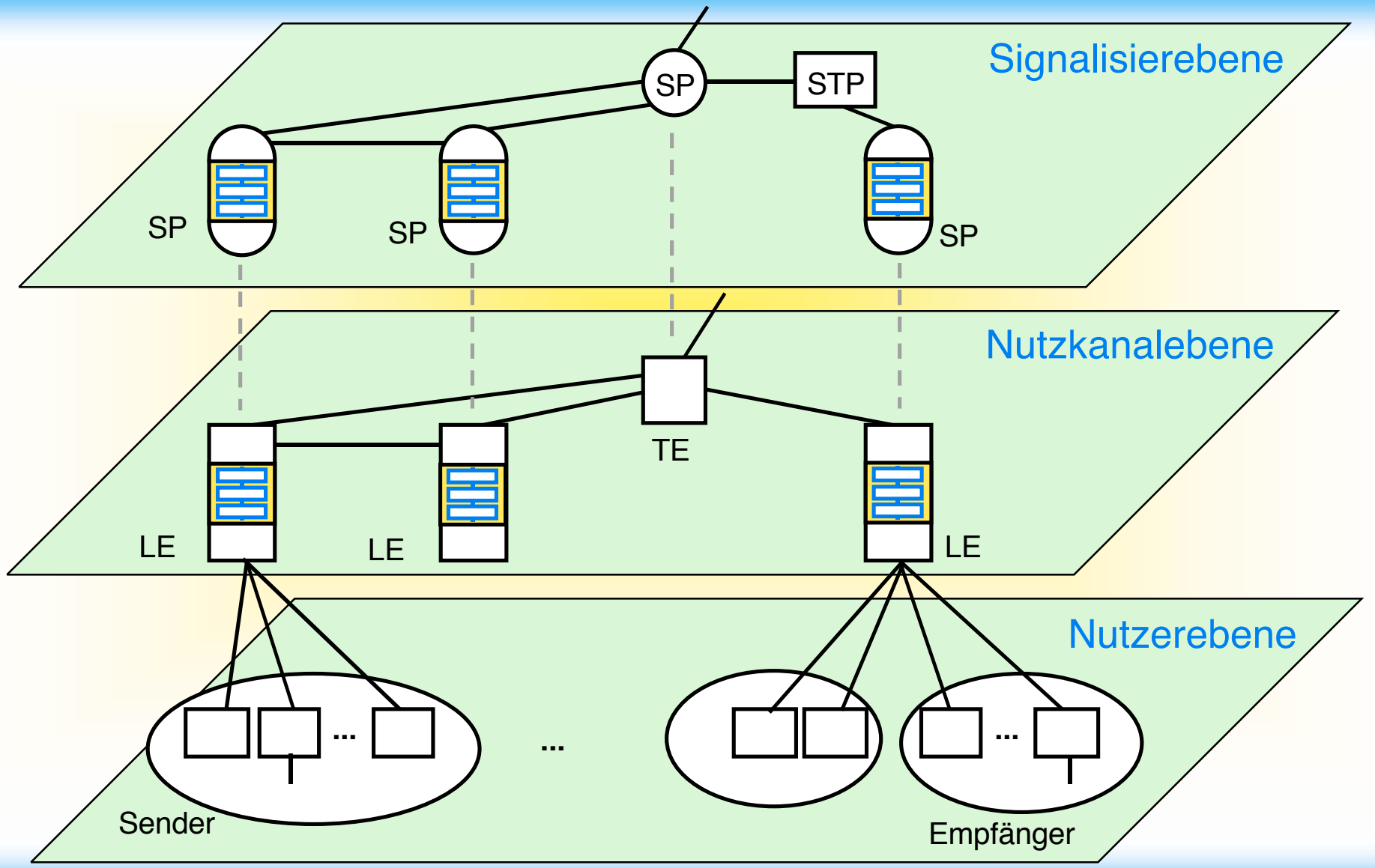


Prinzip der ISDN-Mixe

- Elemente:
  - **Mix-Kanäle** – zur Unverkettbarkeit des Nachrichtenlaufs
  - **Taktung (Zeitscheiben)** – Kommunikation wird in jeweils gleich lange unbeobachtbare Teilkommunikationen zerlegt
  - **Dummy Traffic** – zur Verhinderung der Beobachtbarkeit, ob jemand tatsächlich kommuniziert

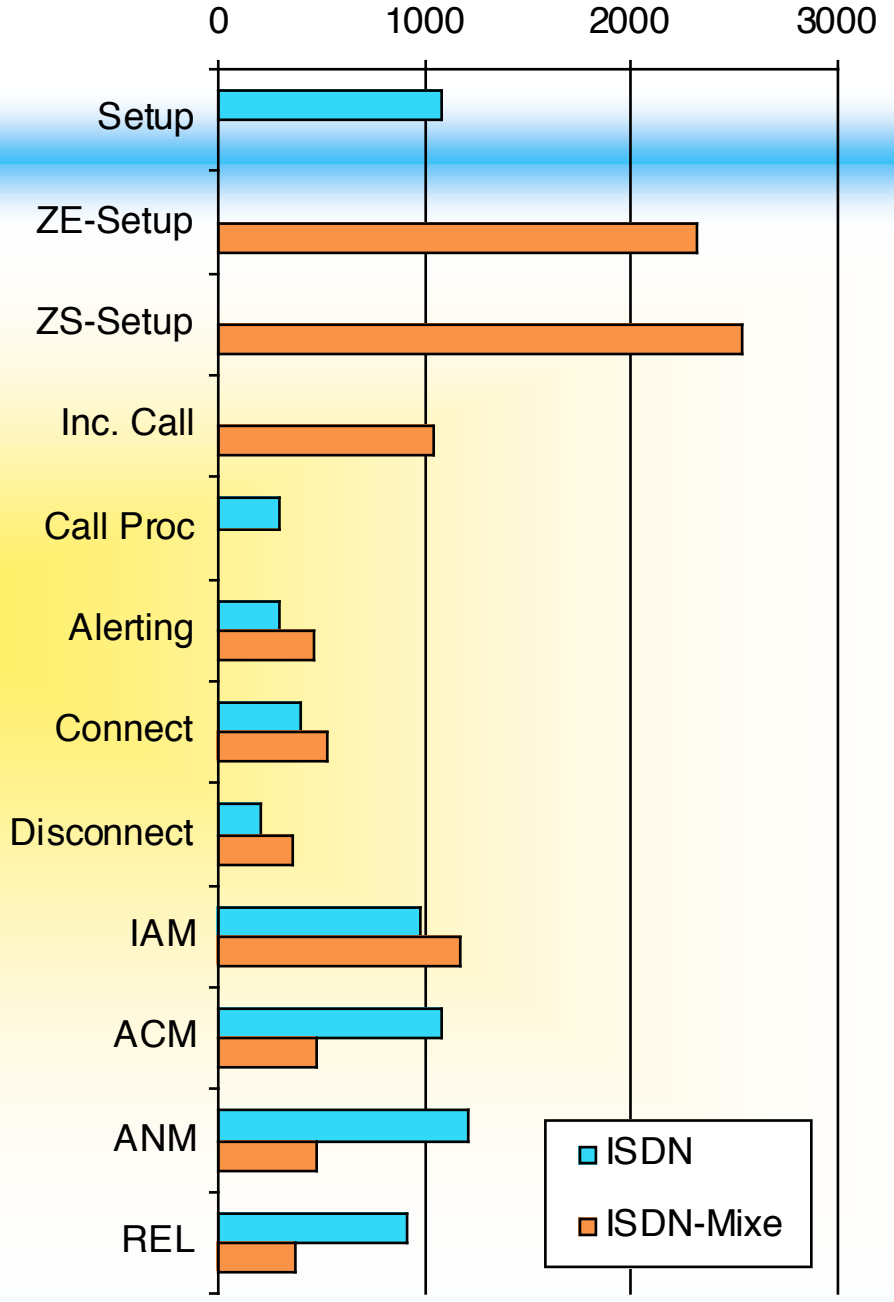


Integration in ISDN und CSS#7



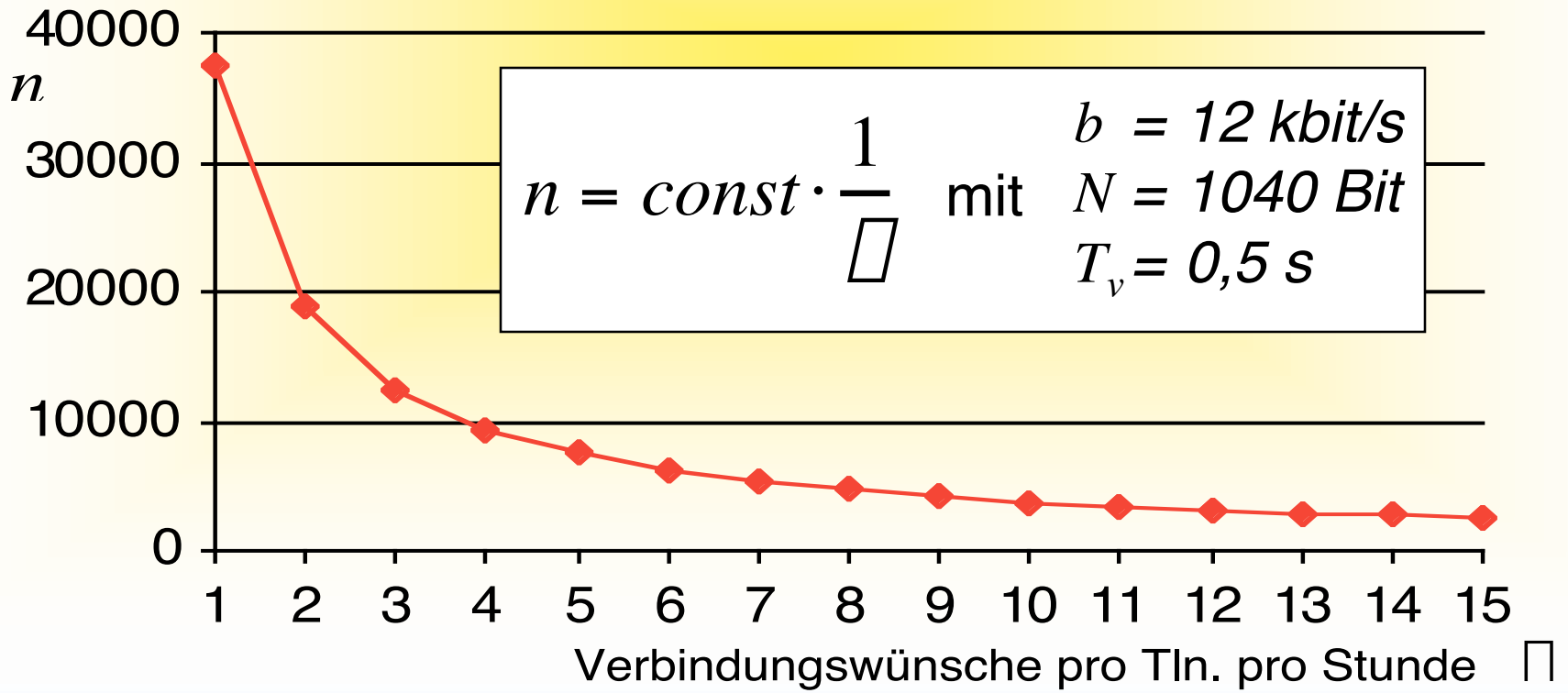
Nachrichtenlängen

	ISDN	ISDN-Mixe
Setup	1084	—
ZE-Setup	—	2322
ZS-Setup	—	2536
Incoming Call	—	1040
Call Proceeding	296	—
Alerting	296	458
Connect	404	530
Disconnect	204	366
IAM	976	1166
ACM	1076	470
ANM	1216	478
REL	912	374



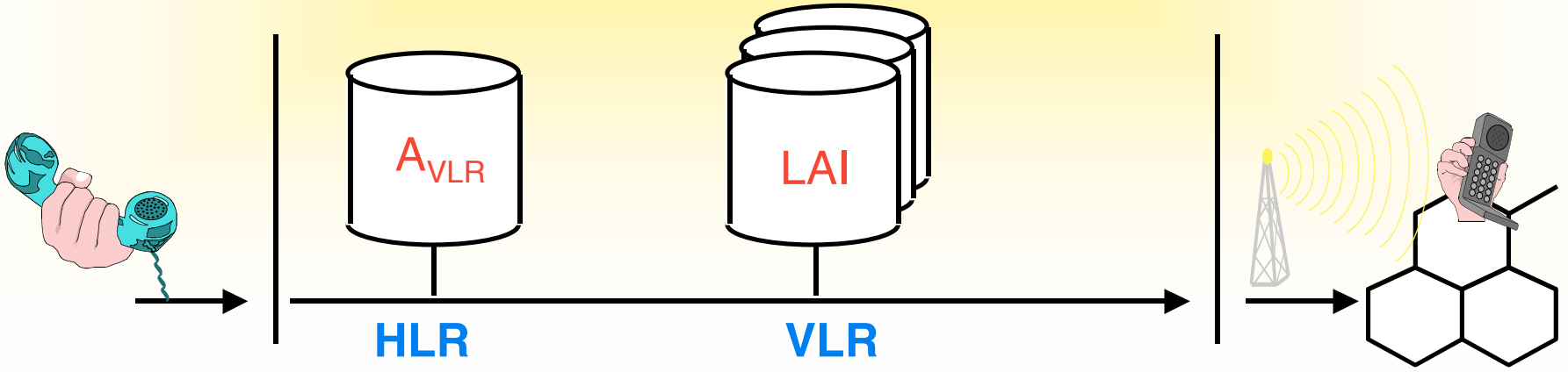
Leistungsfähigkeit

- minimal mögliche Taktung (Zeitscheibenlänge): *ca. 1,22 s*
- Verbindungsaufbauzeit: *ca. 2,5 s* , im Mittel: *ca. 1,25 s*
- bedienbare Teilnehmerzahl pro Kaskade:



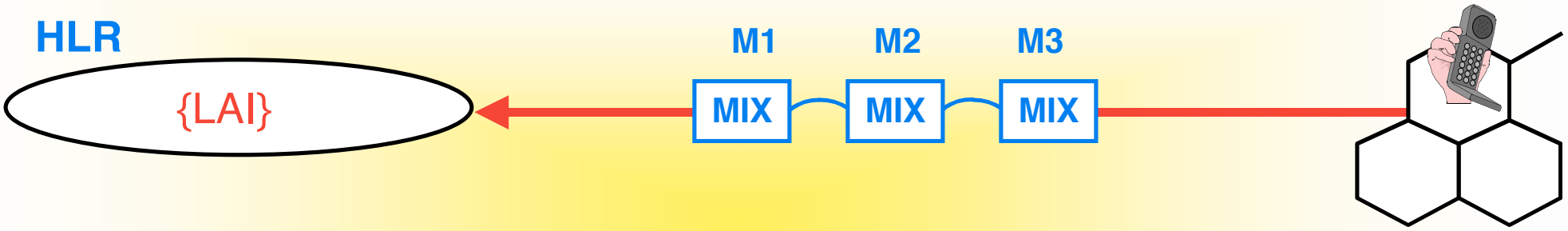
Mobilkommunikationsmixe

- Prinzip 1996 vorgestellt (Federrath, Jerichow, Pfitzmann)
  - Aufenthaltsort wird nicht mehr offen, sondern verdeckt gespeichert: Anonyme Rückadresse
- Gegenstand der Untersuchungen:
  - Konkretisierung
  - Leistungsfähigkeit



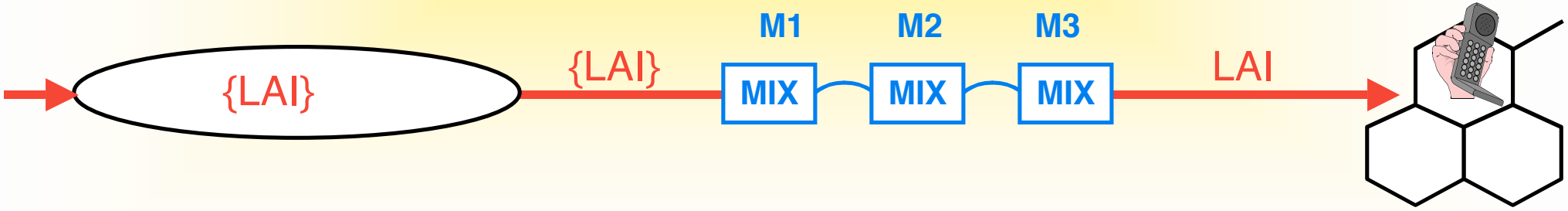
Verdeckte Speicherung

Location Update



Mix-Netz

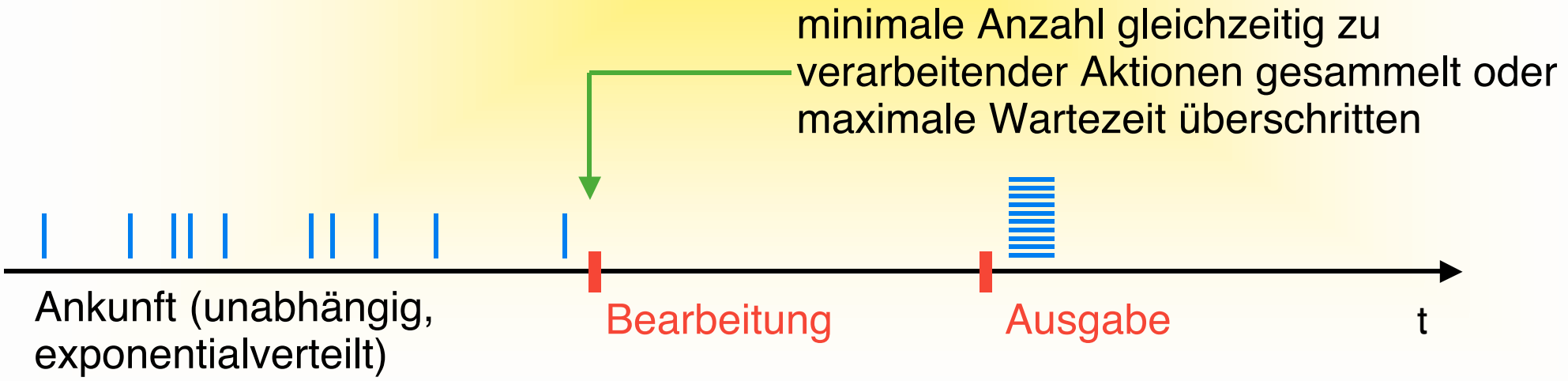
Call Setup



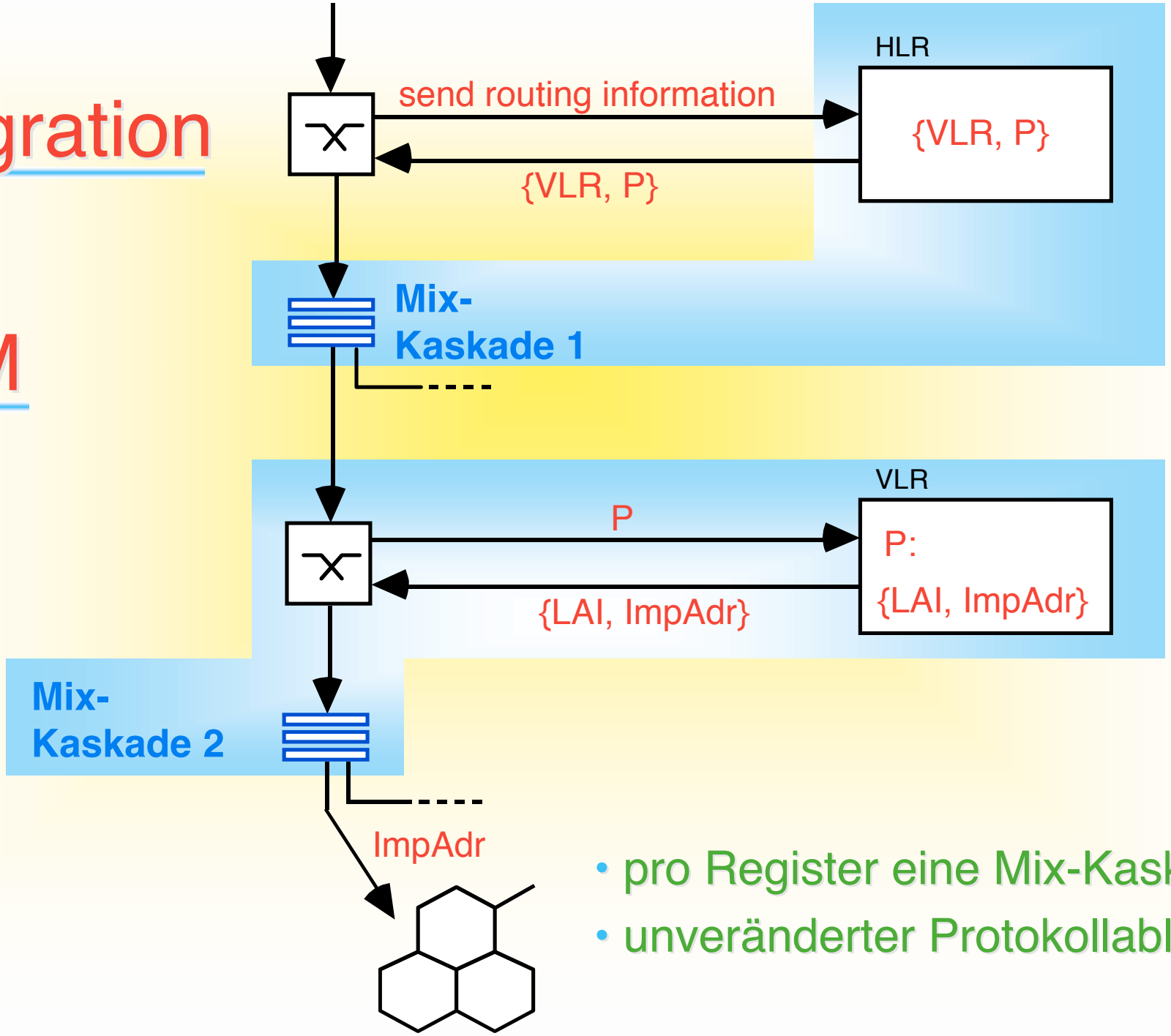
Verkettung wird abgearbeitet

Mobilkommunikationsmixe

- Elemente:
  - **Mix-Kanäle**
    - zur Unverkettbarkeit des Nachrichtenlaufs
  - **Taktung (Zeitscheiben)**
    - Zusammenfassung der Signalisiernachrichten mehrerer Teilnehmer



Integration in GSM



- pro Register eine Mix-Kaskade
- unveränderter Protokollablauf

Probleme

- Dummy Traffic nur eingeschränkt anwendbar
  - begrenzte Akkukapazität der Mobilstationen
- Verkehrsaufkommen im Netz muß hoch genug sein, damit Schutz erreicht wird
  - eine einzelne, isolierte Aktion ist im Netz beobachtbar
  - Teilnehmer wartet zu lange auf Erbringen der Funktion

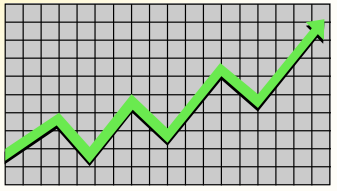
Leistungsfähigkeit

- Nachrichtenlängen:

	GSM	*MK-Mixe*
Location Update	*216...324*	*2221...4502*
Call Setup (MTC)	*1728...2968*	*3624...8080*

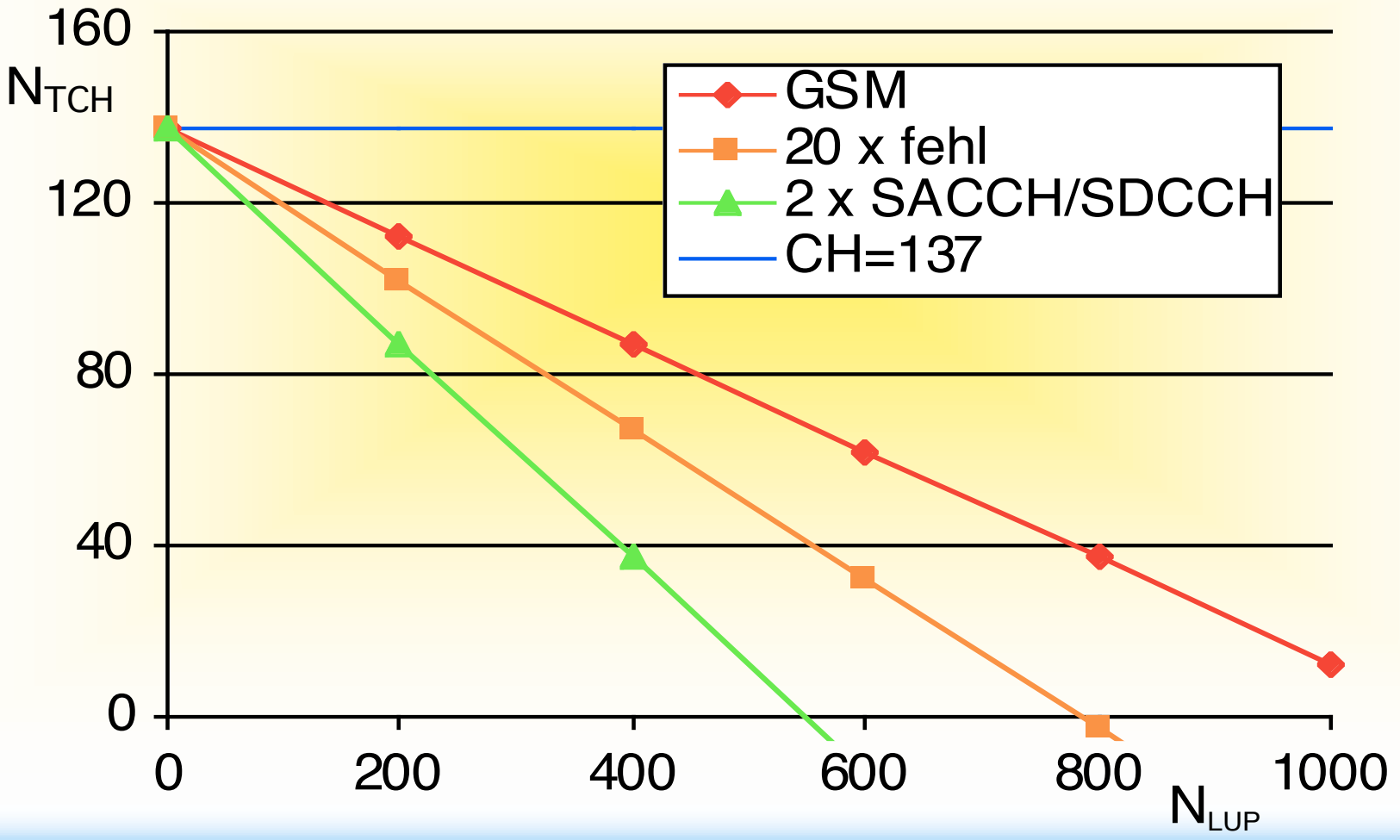
- minimal möglicher Call Setup Systemtakt: *ca. 5,7 s*
- minimal möglicher Location Update Systemtakt: *ca. 5 s*

- bedienbare Teilnehmerzahl pro Location Area:



Leistungsfähigkeit

- bedienbare Teilnehmerzahl pro Location Area:



Zusammenfassung

- Fragestellung war: Was ist in heutigen Netzen machbar?
- Effizienzverlust von ca. 10 % ist tragbar.
- Kanalstruktur muß geändert werden.
- Problem Abrechnung noch nicht betrachtet

Teilnehmerbezogener Schutz ist realisierbar!