Anonyme Signalisierung in Kommunikationsnetzen

DIPLOMARBEIT

an der
TECHNISCHEN UNIVERSITÄT DRESDEN
Fakultät Informatik
Institut für Theoretische Informatik

von
Jan Müller
geboren am 4. Juni 1972 in Görlitz

eingereicht am: 28. Februar 1997

Verantwortlicher Hochschullehrer: Prof. Dr. Andreas Pfitzmann

Betreuer: Dipl.-Inform. Hannes Federrath
Dipl.-Inform. Anja Jerichow

Inhaltsverzeichnis

1. MOTIVATION 5

2. EINFÜHRUNG 7

2.1 Grundlagen des Datenschutzes 7
2.1.1 Angreifermodell und Annahmen 7
2.1.2 Abgeleitete Datenschutzanforderungen 8

2.2 Grundlagen der Signalisierung 9
2.2.1 Signalisierung in Kommunikationsnetzen 9
2.2.2 Das Common Channel Signalling System CCITT No. 7 (CCS7) 10
2.2.3 Das Digital Subscriber Signalling System No. 1 (DSS1) 13

2.3 Grundlagen der betrachteten Kommunikationsnetze 14
2.3.1 Das Integrated Services Digital Network (ISDN) 14
2.3.2 Das Global System for Mobile Communication (GSM) 15

2.4 Verfahren zur Schaffung von Anonymität und Unbeobachtbarkeit 16
2.4.1 Lösungskonzepte für Datenschutz garantierende Netze 16
2.4.2 Grundprinzip des MIX-Netzes 17
2.4.3 Prinzip der MIX-Kanäle 20
2.4.4 Konzept des getakteten Kommunikationssystems 23

3. REALISIERUNG VON ANONYMER SIGNALISIERUNG 25

3.1 Anonyme Signalisierung am Beispiel des ISDN-Festnetzes 25
3.1.1 Modifikation der Netzstruktur 25
3.1.2 Modifikation des Signalisierungsprotokolles zum Verbindungsaufbau 26
3.1.3 Umsetzung der anonymen Signalisierung in DSS1 und CCS7 30
3.1.3.1 Signalisierungsnachrichten im DSS1-Protokoll 30
3.1.3.2 Änderungen der Datenstrukturen im DSS1-Protokoll 33
3.1.3.3 Signalisierungsnachrichten im MIX-Protokoll 36
3.1.3.4 Signalisierungsnachrichten im CCS7-Protokoll 37
3.1.3.5 Änderungen der Datenstrukturen im CCS7-Protokoll 38

3.2 Anonyme Signalisierung am Beispiel des GSM-Mobilfunknetzes 44
3.2.1 Modifikation der Netzstruktur 44
3.2.2 Modifikation des Authentikationsprotokolls 46
3.2.3 Modifikation der Signalisierungsprotokolle zum Location Management 47
3.2.4 Modifikation des Signalisierungsprotokolles zum Verbindungsaufbau 49
3.2.5 Umsetzung der anonymen Signalisierung in RIL3 und CCS7 52
3.2.5.1 Signalisierungsnachrichten im RIL3-Protokoll 52
3.2.5.2 Änderungen der Datenstrukturen im RIL3-Protokoll 56
3.2.5.3 Signalisierungsnachrichten im MIX-Protokoll 60
3.2.5.4 Signalisierungsnachrichten im CCS7-Protokoll 62
3.2.5.5 Änderungen der Datenstrukturen im CCS7-Protokoll 65

3.3 Interworking bei unbeobachtbarer Signalisierung 67

4. EFFIZIENZBETRACHTUNGEN 69

4.1 Voraussetzungen zur Leistungsbewertung 69

4.1.1 Berechnung der Länge einer MIX-Eingabenachricht 69
4.1.2 Länge der Parameter in den verwendeten Kommunikationsnetzen 70

4.2 Leistungsbewertung für das ISDN-Festnetz 70
4.2.1 Länge der ISDN-Signalisierungsnachrichten im Vergleich 70
4.2.2 Minimale Dauer des Systemtaktes 72
4.2.3 Maximale Anzahl der von einer MIX-Kaskade bedienbaren Netzabschlüsse 73
4.2.4 Berechnungsaufwand der Netzabschlüsse und MIXe 74
4.2.5 Verbindungsaufbauzeit 75

4.3 Leistungsbewertung für das GSM-Mobilfunknetz 76
4.3.1 Länge der GSM-Signalisierungsnachrichten im Vergleich 76
4.3.2 Minimale Dauer des Systemtaktes 77
4.3.3 Minimale Dauer des Location-Update-Taktes 79
4.3.4 Maximale Anzahl der von einer Funkzelle bedienbaren Mobilstationen 81
4.3.5 Berechnungsaufwand der Mobilstationen und MIXe 82
4.3.6 Verbindungsaufbauzeit 83

5. ZUSAMMENFASSUNG UND AUSBLICK 84

6. ABKÜRZUNGSVERZEICHNIS 86

7. ABBILDUNGSVERZEICHNIS 89

8. LITERATURVERZEICHNIS 91

1. Motivation

Die 90-iger Jahre zeichnen sich durch ein enormes Wachstum des Telekommunikationsmarktes aus. Schon heute gibt es eine große Anzahl von Kommunikationsmöglichkeiten und -diensten und dieses Geschäftsfeld wird durch die Marktliberalisierung 1998 einen weiteren Boom erleben. Die Kehrseite der Medaille bildet die Vielzahl der anfallenden Informationen über die Nutzer bei der Nutzung von Kommunikationsnetzen. Diese Informationen beinhalten meist sensible personenbezogene Daten, bei deren Mißbrauch dem Nutzer teils erheblicher Schaden zugefügt werden kann.

An dieser Stelle muß die Datensicherheit und der technische Datenschutz wirksam eingreifen, um die Nutzer von Kommunikationsnetzen vor Schaden zu bewahren. In dieser Arbeit sollen die Datenschutzprobleme im Vordergrund stehen, wobei durch die vorgestellten Verfahren (z.B. verbesserte Authentikation im Global System for Mobile Communication (GSM)) auch Sicherheitsprobleme entschärft werden. Schützenswerte Teilnehmerdaten kann man in Nutz-[1] und Vermittlungsdaten[2] aufteilen. Die daraus zu gewinnenden personenbezogenen Daten sind Inhalts-, Interessens- und Verkehrsdaten[3]. Der Schutz der Inhaltsdaten kann durch Ende-zu-Ende-Verschlüsselung erreicht werden. Schwieriger gestaltet sich der Schutz der Interessens- und Verkehrsdaten. Diesem meist weniger beachteten Thema widmet sich diese Arbeit.

Es wird ein Verfahren zum Schutz der Vermittlungsdaten vorgestellt, das es den Nutzern von zukünftigen Kommunikationsnetzen ermöglicht, diese Netze unbeobachtbar und anonym zu nutzen.

Dieses Verfahren wird hergeleitet (*Kapitel 2.4*), detailliert beschrieben (*Kapitel 3*) und dessen Realisierungsmöglichkeiten am Beispiel eines Festnetzes (ISDN: Integrated Services Digital Network) (*Kapitel 3.1*) und eines Mobilfunknetzes (GSM) (*Kapitel 3.2*) aufgezeigt.

Die in den Kommunikationsnetzen eingesetzten Signalisierungssysteme Common Channel Signalling System No. 7 (CCS7) (*Kapitel 2.2.2*) und Digital Subscriber Signalling System No. 1 (DSS1) (*Kapitel 2.2.3*) und deren Modifikationen zur Realisierung des Schutzes der Vermittlungsdaten werden detailliert beschrieben (*Kapitel 3*).

Außerdem wird die Leistungsfähigkeit des Verfahrens bezüglich Performance (*Kapitel 4*) und Datenschutz bewertet.

Es soll in dieser Arbeit gezeigt werden, daß sich Unbeobachtbarkeit und Anonymität von Teilnehmern bei der Signalisierung von Verbindungswünschen und Location Updates bereits mit der zur Verfügung stehenden Bandbreite bestehender Kommunikationsnetze realisieren läßt.

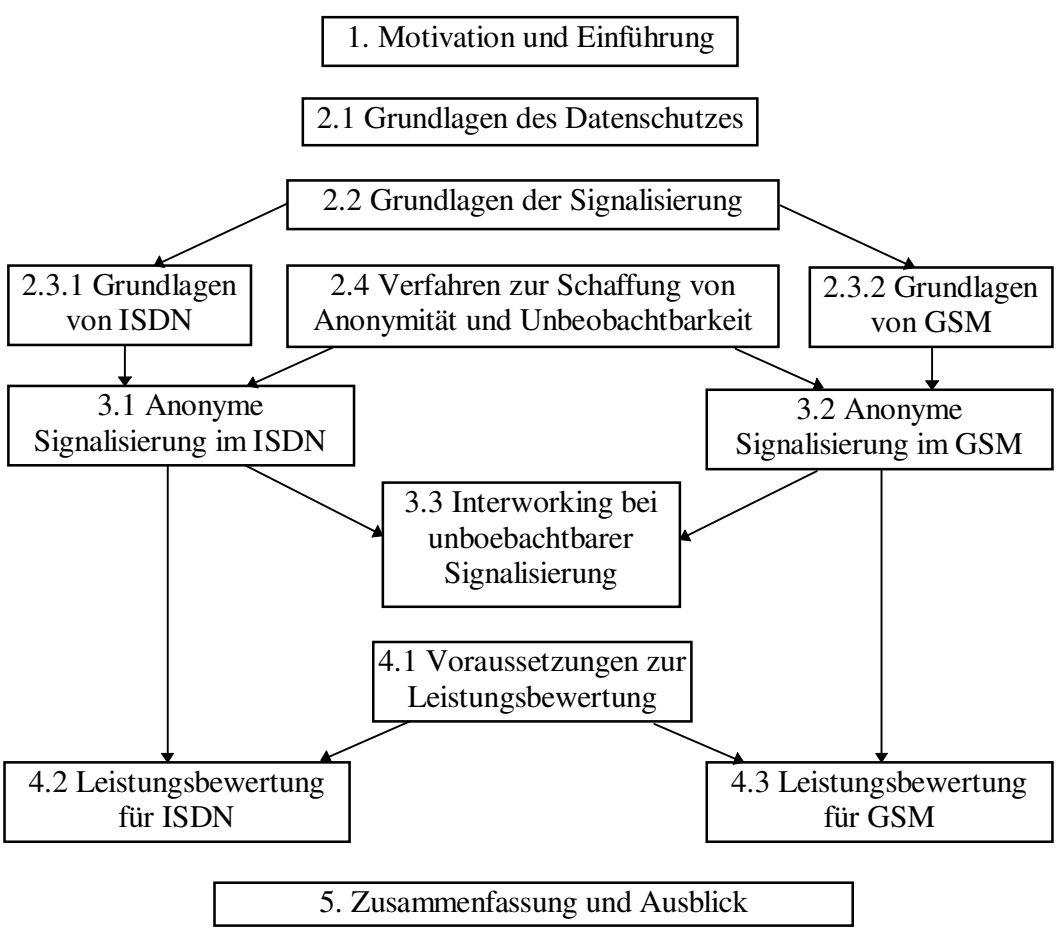
Im folgenden werden einige Hinweise gegeben, die dem Leser zum besseren Verständnis der Zusammenhänge zwischen den einzelnen Kapiteln und damit zum besseren Verständnis der in dieser Arbeit vermittelten Informationen dienen sollen.

Im *Kapitel 1* werden die in dieser Arbeit behandelten Gebiete kurz benannt und eingeordnet. In *Kapitel 2* werden alle zum Verständnis dieser Arbeit benötigten Grundlagen

[1] Nutzdaten sind z.B. Bild, Ton und Text.
[2] Vermittlungsdaten sind z.B. Adressen der Kommunikationspartner, Datenumfang, Dienstart, Beginn und Dauer.
[3] Definitionen siehe [Pfit_89].

erklärt bzw. auf Sekundärliteratur verwiesen. Die Grundlagen der ISDN-MIXe aus [PfPW_89] werden mit geringen Modifikationen und Optimierungen in *Kapitel 2.4* eingeführt. In *Kapitel 3* und *4* gliedert sich die Arbeit jeweils in die betrachteten Kommunikationsnetze ISDN und GSM. Dabei werden im *Kapitel 3* zuerst die Modifikationen an den Netzstrukturen und an den Signalisierungsprotokollen des Basisablaufes beschrieben. Anschließend werden in *Kapitel 3.1.3* bzw. *3.2.5* die Modifikationen der Signalisierungsnachrichten der eingesetzten Protokolle beschrieben. Dabei werden die verschiedenen Signalisierungsprotokolle nacheinander entsprechend ihrer Nutzung in den Kommunikationsnetzen betrachtet. Es werden jeweils die Modifikationen der Signalisierungsnachrichten (inhaltlich mit kurzer Längenangabe), die Codierungen der Nachrichtentypen und Informationselemente und anschließend die Codierungen der Signalisierungsnachrichten angegeben. *Kapitel 3.3* beschäftigt sich kurz mit dem Interworking verschiedener modifizierter Netze. In *Kapitel 4.1* werden die Grundlagen zur Berechnung der Länge von MIX-Eingabenachrichten und die Länge der Ausgangsgrößen der Kommunikationsnetze eingeführt. Danach wird jeweils für ISDN (*Kapitel 4.2*) und GSM (*Kapitel 4.3*) die Berechnung der Nachrichtenlänge an einem Beispiel vorgeführt. Anschließend werden jeweils alle Signalisierungsnachrichten mit ihrer bisherigen und neuen Länge (mit 5 bzw. 10 MIXen) tabellarisch aufgelistet, gefolgt von der Berechnung der Performance des modifizierten Systems. *Kapitel 5* faßt die Ergebnisse zusammen und gibt einen Ausblick für dieses Forschungsgebiet.

In dem folgenden Diagramm sind die Zusammenhänge der einzelnen Kapitel dargestellt. Pfeile geben an, daß die Kenntnis des jeweils (am Pfeil) vorangegangenen Kapitels zum Verständnis des (am Pfeil) folgenden Kapitels vorausgesetzt wird.



2. Einführung

2.1 Grundlagen des Datenschutzes

2.1.1 Angreifermodell und Annahmen

Schutz vor einem allmächtigen Angreifer ist natürlich nicht möglich. Deshalb sind alle folgenden Maßnahmen nur Annäherungen an den perfekten Schutz der Teilnehmer vor jedem möglichen Angreifer (nach [Pfit_89]).

Als potentielle Angreifer müssen Außenstehende, Teilnehmer, Betreiber, Hersteller, Entwickler und Wartungstechniker betrachtet werden, die natürlich auch kombiniert auftreten können.

In dieser Arbeit wird der **Schutz der Vermittlungsdaten** untersucht, also nicht die Vertraulichkeit von Inhaltsdaten. Diese können durch Ende-zu-Ende-Verschlüsselung geschützt werden. Ebenfalls nicht betrachtet werden die Schutzziele Integrität, Verfügbarkeit.

Die folgenden Definitionen sind in Anlehnung an den jeweils perfekten Fall aus [Pfit_89] entstanden.

Ein Ereignis E heißt **unbeobachtbar** bezüglich eines Angreifers A, wenn die Wahrscheinlichkeit des Auftretens von E vor und nach jeder für A möglichen Beobachtung gleich ist, d.h. daß die Beobachtung A keinerlei zusätzliche Informationen über E liefern kann. Ein Teilnehmer T eines Kommunikationsnetzes heißt demzufolge unbeobachtbar bezüglich eines Angreifers A, wenn alle Ereignisse E, die T auslöst (z.B. Senden einer Nachricht) bzw. an denen er beteiligt ist (z.B. Empfangen einer Nachricht), bezüglich A unbeobachtbar sind.

Ein Teilnehmer T eines Kommunikationssystems heißt in einer Rolle R (z.B. Sender oder Empfänger einer Nachricht) **anonym** bezüglich eines Ereignisses E und eines Angreifers A, wenn für jeden nicht mit A kooperierenden Teilnehmer die Wahrscheinlichkeit, daß er bei E die Rolle R wahrnimmt, vor und nach jeder Beobachtung gleich ist, d.h. daß die Beobachtung A keinerlei zusätzliche Informationen darüber liefert, wer bei E die Rolle R wahrnimmt.

Zwei Ereignisse E und F heißen bezüglich eines Merkmals M (z.B. zwei Nachrichten bezüglich ihres Senders) und bezüglich eines Angreifers A **unverkettbar**, wenn die Wahrscheinlichkeit, daß sie in M übereinstimmen, vor und nach jeder für A möglichen Beobachtung gleich ist, d.h. daß die Beobachtung A keinerlei zusätzliche Information darüber liefert, ob E und F in M übereinstimmen.

Darüber hinaus muß man einige Bedingungen für die **maximal erreichbare Unbeobachtbarkeit** festhalten. So ist ein gutartiger Teilnehmer nur in der Gruppe der nicht vom Angreifer kontrollierten Teilnehmer seiner Anonymitätsgruppe unbeobachtbar. Außerdem ist die vorgeschlagene Lösung maximal komplexitätstheoretisch sicher, da auch das MIX-Netz nur komplexitätstheoretische Sicherheit (bis auf den ersten MIX im ISDN der symmetrisch arbeitet, falls dieser ein perfektes symmetrisches Kryptosystem verwendet) bietet. Die komplexitätstheoretische Sicherheit gilt zur Zeit aber als völlig ausreichend, da ein realer Angreifer in seiner Speicher- und Rechenkapazität beschränkt ist. Es werden in der Literatur (z.B. [PfPW_89]) außerdem aktive Angriffe beschrieben,

die z.B. die Verfügbarkeit stören und dadurch versuchen, Teilnehmer zu deanonymisieren. Darauf soll in diesem Rahmen nicht näher eingegangen werden.

Außerdem werden die Teilnehmerendgeräte, also die Mobilstation und das Teilnehmerendgerät im Festnetz als **vertrauenswürdige Bereiche** festgelegt. Zusätzlich haben die Teilnehmer bereits die notwendigen Schlüssel nach einem sicheren Verfahren ausgetauscht.

Damit schränkt sich auch das **Angreifermodell** entsprechend ein:

1. Ein Angreifer (Outsider) versucht durch Abhören der Leitungen bzw. Funkstrecken Vermittlungsdaten zu ermitteln.
2. Ein Angreifer (Outsider) versucht durch aktive Eingriffe in das Festnetz gespeicherte oder übertragene Vermittlungsdaten zu ermitteln.
3. Der Netzbetreiber nutzt die Kontrolle der Netzeinrichtungen zur Ermittlung von Vermittlungsdaten.
4. Die Hersteller oder Entwickler der Netzkomponenten bauen in die Geräte Trojanische Pferde ein, um übermittelte Vermittlungsdaten abhören und auswerten, bzw. gespeicherte Verbindungsdaten einsehen zu können.
5. Der Wartungsdienst versucht, während der regulären Systemwartung, Netzkomponenten des Netzbetreibers zu kompromittieren.

In den bestehenden Netzen (speziell ISDN, GSM) haben alle in 1.-5. beschriebenen Angreifer mit unterschiedlich geringem Aufwand Erfolg. Ein Outsider als Angreifer muß in der Lage sein, die Kommunikations- bzw. die Signalisierungsverbindungen abzuhören. Dies ist mit minimalem technischen Aufwand möglich, da die komplette Signalisierung, ebenso wie die spätere Kommunikation auf dem Nutzkanal, unverschlüsselt übertragen wird. Lediglich in GSM werden die Nutzdaten auf dem Funkweg verbindungsverschlüsselt übertragen. Dadurch kann der Angreifer die aktuell ablaufende Kommunikation aufzeichnen und erhält Angaben über die Rufnummern der Kommunikationspartner, Beginn und Dauer von Gesprächen und genutzte Dienste. Interessieren einen Outsider die Vermittlungsdaten bereits beendeter Gespräche, so muß er aktiv in Datenbanken des Festnetzes einbrechen. Dort werden die Daten zu Abrechnungszwecken nahezu vollständig (bis auf die 3 letzten Ziffern der Rufnummer des Empfängers) und unverschlüsselt gespeichert. Einem Netzbetreiber als Angreifer stehen momentan alle Vermittlungsdaten jederzeit zur Verfügung, da er die globale Sicht auf alle Daten des Netzes hat. Das Erstellen von Kommunikations- oder Bewegungsprofilen stellt für den Netzbetreiber keinen nennenswerten Aufwand dar. Auch Herstellern und Wartungsdienst wäre es momentan möglich, Netzeinrichtungen, die sensitive Informationen erhalten, zu kompromittieren.

Zusammenfassend kann man feststellen, daß zur Zeit Vermittlungsdaten, die sensible Informationen über das **Kommunikationsprofil** und in Mobilfunknetzen auch über das **Bewegungsprofil** eines Teilnehmers beinhalten, **jedem Angreifer** ohne großen Aufwand zur Verfügung stehen.

2.1.2 Abgeleitete Datenschutzanforderungen

Aus dem Angreifermodell kann man folgende **Sicherheitsanforderungen** ableiten:

1. Die Vermittlungsdaten müssen während der Übertragung verschlüsselt sein, bzw. dürfen keine Teilnehmerverkettung ermöglichen.

2. Die Speicherung von Abrechnungsdaten muß gesichert erfolgen und darf keine Aussage zum Kommunikationsverhalten ermöglichen.[4]
3. Netzkomponenten müssen auf das Vorhandensein von Trojanischen Pferden untersucht werden, bevor sie in Betrieb genommen werden. Diese Kontrolle sollte entwicklungs- und produktionsbegleitend sein.
4. Die Befugnisse des Wartungsdienstes müssen genau festgelegt und kontrolliert werden, um den Einbau von Trojanischen Pferden während der Wartung auszuschließen.

Diese Anforderungen müssen die vorgeschlagenen Verfahren erfüllen, wobei die Punkte 3. und 4. durch organisatorische Maßnahmen außerhalb des Kommunikationsnetzes gelöst werden müssen.

2.2 Grundlagen der Signalisierung

2.2.1 Signalisierung in Kommunikationsnetzen

Signalisierung[5] ist nach [BGGH_95] die Übermittlung von Information zu Steuerungszwecken. Im Bereich der Telekommunikation werden diese Nachrichten meist in codierter Form übermittelt. Zweck der Signalisierung ist die Verständigung von Teilnehmern des Netzes mit dem Netz bzw. mit Einrichtungen des Netzes und umgekehrt. Signalisierungsnachrichten können in mechanischer, optischer und elektrischer Form übermittelt werden. Sender und Empfänger von Signalisierungsnachrichten können Personen und/ oder Maschinen (Prozesse) sein.

Signalisierung ermöglicht die Steuerung einzelner Nachrichten, einzelner Kanäle und die Steuerung kompletter Netze. In modernen Netzen wird Signalisierung nicht nur zum Auf- und Abbau von Verbindungen, sondern auch zur Steuerung des Informationsflusses von bestehenden Verbindungen eingesetzt. Mittels Signalisierung werden sowohl der Verbindungsauf- und -abbau, die Nutzung von Dienstmerkmalen, Kompatibilitätsprüfungen, Meß- und Prüfroutinen, Lastverteilung in Netzen als auch der Datenaustausch zwischen Informationsdatenbanken gesteuert.

Signalisierung muß im Hintergrund ablaufen, d.h. ein Teilnehmer soll nur die Ergebnisse wahrnehmen, nicht aber die Signalisierung selbst. Deshalb müssen die Verzögerungszeiten für Verbindungsauf- und -abbau und Zeiten für die Steuerung von Dienstmerkmalen möglichst klein sein. Die Entwicklung der Signalisierung ging von der Nutzkanal-gebundenen Zeichengabe zur Zentralkanalzeichengabe. Dieser Schritt war notwendig, um den wachsenden Anforderungen an die Signalisierung gerecht werden zu können. Die neuen Verfahren verwenden zentrale, eigens für diesen Zweck reservierte, Signalisierkanäle, statt die Steuerinformationen auf dem für die Verbindung genutzten Kanal zu übertragen, wie es Nutzkanal-gebundene Verfahren machen. Die Vorzüge der neuen Verfahren im Vergleich zu den früheren Systemen sind Universalität, Leistungsfähigkeit und Zuverlässigkeit. Ein solches neues Verfahren ist CCS7, dessen wichtigste Merkmale (aus [Bial_94]) im folgenden zusammengestellt sind:

- erstmals Elemente der OSI-Strukturierung in der Signalisierung,
- optimale Ausnutzung der 64 kBit/s (kbps) Leitungen der PCM-Übertragung,
- kurze Verbindungsaufbauzeiten,
- hohe Signalisierungskapazität,

[4] Die Abrechnung wurde in diese Arbeit nicht einbezogen. Portierbare Lösungen bietet [PfPW_89] an.
[5] Synonyme sind: Zeichengabe oder Kennzeichengabe.

- anpaßbar an verschiedenste Transportmedien (Funkstrecken usw.),
- heterogene, modulare Struktur mit verschiedenen Protokollen, dadurch auf zukünftige und vielfältige Dienste erweiterbar (variable Message-Länge),
- unterschiedliche Fehlerkorrekturverfahren möglich,
- Erhaltung der Reihenfolge der Meldungen,
- Fehlertoleranz,
- Redundanzkonzept (Nachrichten, Leitungen, Baugruppen, Netzkomponenten),
- geringe Hardwarekosten durch direkte Vermittlungsstellen-Verbindung,
- Signalisierung unabhängig von der physikalischen Verbindungsleitung,
- verbindungslose/ verbindungsorientierte Services,
- flexible und effektive Routing-Funktionen (z.B. mit Global Title über nationale Netzgrenzen hinaus),
- ausbaufähige Datenflußüberwachung,
- gute Stabilität auch bei hoher Verkehrslast,
- wirksame Netzmanagementfunktionen für hohe Zuverlässigkeit,
- Rekonfigurierbarkeit,
- eingebaute Selbstüberwachungsprozeduren und -tests auf unterschiedlichsten Protokollebenen.

Das CCS7 arbeitet mit Paketvermittlung, was die Flexibiltät des Systems steigert, die Operationsdauer verkürzt und zu vereinfachten Interworking Functions (IWF) führt. Das CCS7 muß in Bezug auf offene Intelligent Network-Architektur (IN) und die Spezifika zellularer Netze noch weiteren, höheren Anforderungen genügen:

- Unterstützung unterschiedlicher, auch verteilter Netzarchitekturen,
- sehr hoher Anteil an Echtzeit-Prozeßkapazität,
- steigende Bedeutung von Datenbankoperationen für verschiedene Dienste,
- Signalisierungsverkehr aufwendiger Dienstarten muß zur Hauptverkehrszeit die typische Public Switched Telephone Network-Signalisierung (PSTN) um mehrere Größenordnungen übersteigen können.

Im folgenden Abschnitt wird der funktionale Aufbau und die Arbeitsweise von CCS7 genauer beschrieben.

2.2.2 Das Common Channel Signalling System CCITT No. 7 (CCS7)

Der schematische Aufbau des CCS7-Netzes und dessen Einbettung in ISDN ist in *Abb. 2.3.1.1* dargestellt. Das CCS7 ist ein Overlay-Netz. Es besteht aus Signalisierungspunkten (SP) und Signalisiertransferpunkten (STP), die redundant über Zeichengabestrecken (SL: Signalling Link) miteinander verbunden sind. Haben zwei SPs die Möglichkeit, Signalisierungsnachrichten miteinander auszutauschen, so besteht zwischen ihnen eine sogenannte Signalisierbeziehung. Je nachdem, ob diese beiden SPs direkt oder indirekt über STPs miteinander verbunden sind, spricht man von assoziierter[6] oder quasi-assoziierter[7] Betriebsweise. Dadurch ist die Struktur nur noch bedingt an die des Nutzkanalnetzes gebunden und kann dadurch weitgehend vom jeweiligen Netzbetreiber bestimmt werden.

Bei Signalisierungspunkten ist zu unterscheiden, ob Sie die Quelle oder das Ziel einer Signalisierungsnachricht sind. Man spricht dann entweder von einem Originating

[6] Im Associated Mode erfolgt die Signalisierung auf einer Leitung parallel zum Nutzkanalbündel.
[7] Zum Teil unterschiedliche Wegführung für Signalisierung und Nutzkanäle.

Signalling Point (OSP) oder von einem Destination Signalling Point (DSP). Jeder Vermittlungsstelle im ISDN, aber auch anderen Netzeinrichtungen, wie dem Base Station Controler (BSC) im GSM, ist ein SP zugeordnet. Ein Signalisierungsnetz wird, weil es sich in der Regel um große Systeme handelt, in zwei unabhängige Bereiche eingeteilt, in eine internationale Ebene mit nur einem Netz und in eine nationale Ebene mit mehreren nationalen Netzen. Dementsprechend wird die SP-Numerierung für jedes Netzwerk eigenständig vergeben, dies soll in dieser Arbeit allerdings nicht näher betrachtet werden.

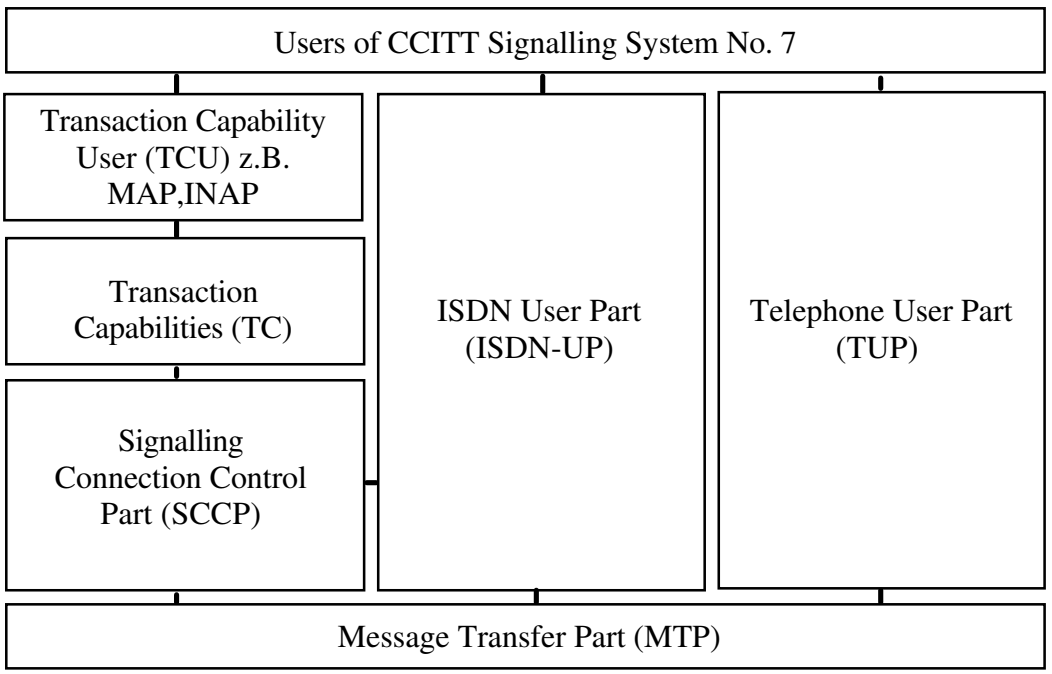


Abb. 2.2.2.1: Funktionale Struktur des CCS7

In *Abb. 2.2.2.1* ist, entsprechend [ITU_Q.700, *Abb.2*], die vereinfachte funktionale Struktur des CCS7 dargestellt. Die grundlegende Idee ist die Trennung des Message Transfer Part (MTP) als reines Transportsystem von den verschiedenen Anwendern dieses Transportsystems. Die Anwenderteile umfassen jeweils einen bestimmten Anwendertyp (z.B. ISDN) und die Funktionen, Protokolle und Codierungen für die Signalisierung über das CCS7. Die Anwenderkomponenten steuern z.B. den Auf- und Abbau von Nutzkanalverbindungen, die Abwicklung von Dienstmerkmalen sowie Verwaltungs- und Wartungsfunktionen für die Nutzkanäle. Deshalb sind die in *Kapitel 3* beschriebenen **Modifikationen zur Erreichung von unbeobachtbarer Signalisierung ausschließlich** in den Anwenderteilen **ISDN-User Part** (ISDN-UP) für ISDN und **Mobile Application Part** (MAP) für GSM durchzuführen.

Die Funktionen des Nachrichtentransferteils (MTP: **Message Transfer Part**) und der Anwenderteile des CCS7 sind in 4 Ebenen unterteilt. Dabei entfallen auf den MTP die Ebenen 1 bis 3, die Anwenderteile sind auf der Ebene 4 angeordnet. Die Funktionsblöcke des CCS7 sollen in dieser Arbeit nicht im Einzelnen beschrieben werden, da nur der ISDN-UP und der MAP als Transaction Capability Application Part (TCAP)-Anwender benötigt werden.

Die **Transaction Capabilities** (TC bzw. TCAP) unterstützen den Austausch von Nachrichten zwischen Anwendern in verschiedenen CCS7-Netzknoten über zentrale Zeichen-

gabestrecken, ohne daß dazu Nutzkanalverbindungen aufgebaut werden müssen. Anwendungsgebiete des TCAP sind z.B.:

- das Location Update (LUP) im GSM-Netz (Meldung eines neuen Aufenthaltsortes),
- der Austausch nicht nutzkanalbezogener Zeichengabeinformationen bei geschlossenen Benutzergruppen,
- die Bedienung und Instandhaltung für die Abfrage von Betriebszuständen oder auch für das Aufrufen von Aktionen in entfernten Netzknoten.

Der TCAP ist ein Anwender des SCCP und nutzt den Nachrichtentransport ohne virtuelle Signalisierverbindung. Anwender des TCAP sind z.B. der Mobile Application Part (MAP) und der Intelligent Network Application Part (INAP). Das INAP-Protokoll soll unter anderem UPT-Dienste[8] unterstützen.

Der **MAP** ist der Anwenderteil für den Mobilfunk und ist in [GSM_09.02] spezifiziert. Dabei handelt es sich um Applikationsprozesse der Teilsystemkomponenten (Mobile Switching Center (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR), Authentication Center (AuC) im CCS7-Netz des europäischen GSM-Netzes. In der MAP-Entwicklung werden zwei Phasen unterschieden. Zu der Phase 1 gehört z.B. der Short Message Service (SMS). Zu den MAP-Features gehören unter anderem Access Management, Location Management, Handover, Security Management und Operation and Maintenance.

Routing Label
Circuit Identification Code (CIC)
Message Type Code (Nachrichtentyp)
Mandatory Fixed Part (Pflichtteil fester Länge)
Mandatory Variable Part (Pflichtteil variabler Länge)
Optional Part (Optionaler Teil)

Abb. 2.2.2.2: Generelles Nachrichtenformat des ISDN-UP

Der **ISDN-UP** dient zur Steuerung von durchschaltevermittelten 64 kbps-ISDN-Verbindungen unter Nutzung des SCCP mit End-to-End Signalisierverbindungen. Dies schließt neben dem reinen Auf- und Abbau von Verbindungen auch weitere ISDN-Dienstmerkmale, wie Anrufweiterleitung oder Identifizierung des rufenden Teilnehmers ein. Im folgenden soll jedoch nur der Basisablauf eines Verbindungsaufbaus betrachtet werden.

Die Funktion der anderen CCS7-Teile ist der Literatur zu entnehmen, z.B. [MoSk_90]. Der allgemeine Aufbau der CCS7-Signalisierungsnachrichten ist beispielsweise in [BGGH_95] in *Abb. 6.16* dargestellt. *Abb. 2.2.2.2* zeigt den Aufbau und die Anordnung der Parameter von Signalisierungsnachrichten des ISDN-UP (nach [ITU_Q.763], *Abb. 1*). Der Nachrichtenkopf ist stets 52 Bit lang, wird aber mit vollen 7 Bit codiert.

[8] UPT: Universal Personal Telecommunications, also Mobilitätsaspekte in IN-Systemen.

Die in *Kapitel 3* vorgeschlagenen Modifikationen sind ausschließlich im ISDN-UP und im MAP vorzunehmen. Die Funktionalität aller anderen CCS7-Teile bleibt unverändert, ebenso das Management der Signalisierungsstrecken und das Routing der Nachrichten, da der unveränderte MTP genutzt wird.

2.2.3 Das Digital Subscriber Signalling System No. 1 (DSS1)

Die D-Kanal-Signalisierung wurde mit dem ISDN erstmals eingeführt. Es handelt sich bei dem D-Kanal-Protokoll ebenfalls um ein Zentralzeichengabesystem. Mit Hilfe des D-Kanal-Protokolls können Verbindungen zwischen Teilnehmereinrichtungen und lokalen Ortsvermittlungsstellen (LE: Local Exchange) im ISDN auf- und abgebaut werden, Dienstmerkmale aktiviert und deaktiviert werden und Informationen z.B. zur Benutzerführung übertragen werden. Im ISDN hat der D-Kanal eine Bandbreite von 16 kbps und steuert pro Netzabschluß zwei 64 kbps Nutzkanäle zur Sprach- und/oder Datenübertragung. Man kann jedoch auch ISDN-Nebenstellenanlagen mit einem Primärmultiplexanschluß im ISDN integrieren. Darauf soll hier jedoch nicht ausführlicher eingegangen werden. Die CCITT[9] -Empfehlungen umfassen die Schichten 1-3 entsprechend dem ISO-OSI[10] -Referenzmodell für offene Kommunikation. Für diese Arbeit ist dabei nur die Schicht 3 des DSS1 interessant, die dem ISDN-Nutzer einen standardisierten Netzzugang bereitstellt. Die Schicht 3-Prozeduren zur Steuerung des Auf- und Abbaus von Kommunikationsverbindungen werden als Basisabläufe bezeichnet, worauf sich diese Arbeit konzentriert.

Protokoll-Diskriminator (PD)
Verbindungskennung Call Reference (CR)
Nachrichtentyp Message Type (MT)
Informationselement(e) (I.E.)

Abb. 2.2.3.1: Aufbau einer DSS1-Nachricht der Schicht 3

Abb. 2.2.3.1 zeigt den generellen Aufbau einer DSS1-Signalisierungsnachricht in der Schicht 3. Die Bedeutung von PD und CR wird in [BGGH_95] beschrieben, der Nachrichtenkopf einer DSS1-Nachricht hat eine Länge von 32 Bit. Der Nachrichtenfluß eines Verbindungsaufbaus (Basisablauf) wird in *Abb. 2.3.1.2* dargestellt, wobei dort die DSS1- und die CCS7-Nachrichten angegeben werden. Die Codierung der Nachrichtentypen ist in [BGGH_95] in *Abb. 5.19* und die Codierung der enthaltenen I.E.´s in [BGGH_95] in *Abb. 5.20* dargestellt.

Damit sind die wichtigsten in dieser Arbeit benötigten Grundlagen der Signalisierung und der zum Einsatz kommenden Signalisierungssysteme erläutert. Für eine detailliertere Einarbeitung in DSS1 und CCS7 sei auf die Literatur, z.B. [BGGH_95, KoSk_90] verwiesen. Spezielle in GSM verwendete Grundlagen des CCS7-Mobile Application Parts (MAP) und des **Radio Interface Layer 3-Protokolls** (RIL3) für die **Funkschnittstelle** werden im *Kapitel 3.2* kurz eingeführt.

[9] Comité Consultatif International Télégraphique et Téléphonique.
[10] ISO (International Standardisation Organisation)- OSI (Open Systems Interconnection).

2.3 Grundlagen der betrachteten Kommunikationsnetze

2.3.1 Das Integrated Services Digital Network (ISDN)

Das ISDN stellt dem Nutzer an seinem Netzabschluß (NT: Network Termination) zwei unabhängige Nutzkanäle (B-Kanäle) mit einer Bandbreite von 64 kbps zur Verfügung, die über den Signalisierungskanal (D-Kanal) von 16 kbps gesteuert werden. Jeweils eine größere Gruppe von Nutzern ist sternförmig an Ortsvermittlungsstellen angeschlossen. Diese Sternnetze sind ihrerseits über eventuell mehrstufige Fernnetze (Transitvermittlungsstellen (TE: Transit Exchange)) miteinander verbunden und die Signalisierungsnachrichten und Nutzkanäle werden vermittelt. Dieser **prinzipielle Netzaufbau** ist in *Abb. 2.3.1.1* dargestellt, wobei zwischen der Signalisierungsebene (CCS7), der Nutzkanalebene (ISDN) und der Nutzerebene unterschieden wird. Man erkennt die Zuordnung der Signalisierungspunkte zu den Vermittlungsstellen und die Lage der Nutzkanäle (**fett**) im Vergleich zu den Signalisierungskanälen (dünn).

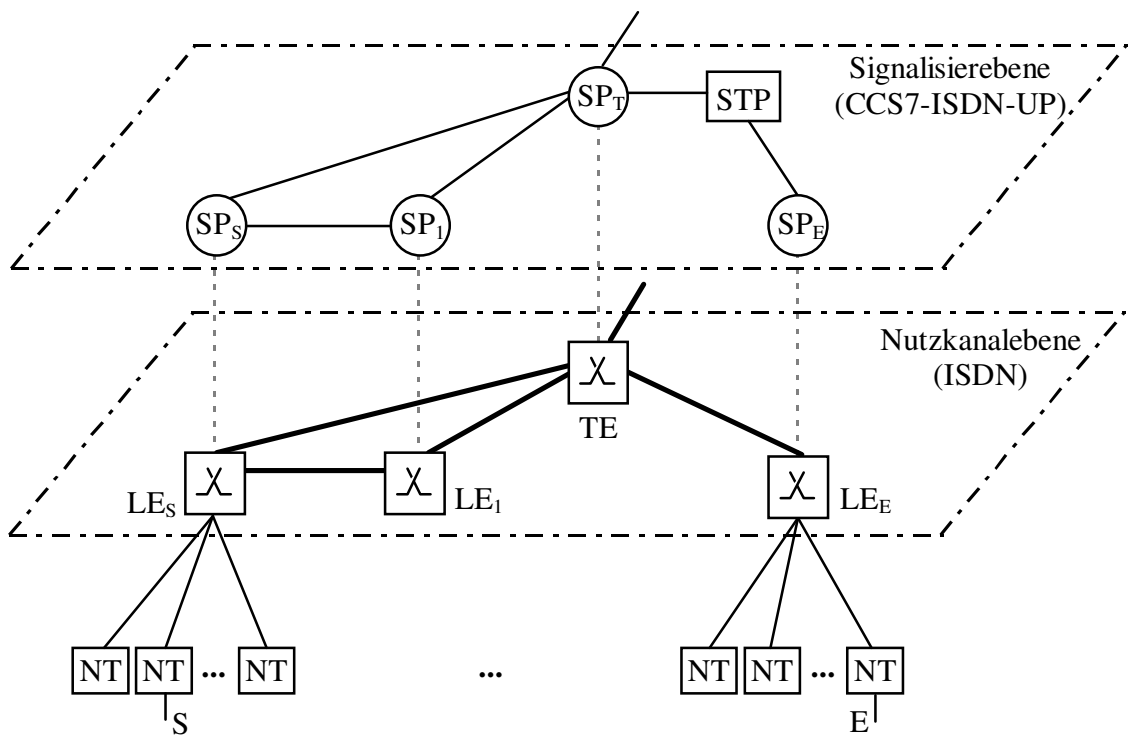


Abb. 2.3.1.1: ISDN-Netzstruktur

Abb. 2.3.1.2 zeigt den **Basisablauf eines Verbindungsaufbaus** im ISDN. Außerdem wird die Zusammenarbeit der Signalisierungsprotokolle DSS1 und CCS7 dargestellt. In ISDN kommt der CCS7-Anwenderteil ISDN-User Part (ISDN-UP) zum Einsatz. Dieser bildet gemeinsam mit der grundlegenden Netzstruktur und dem Verbindungsaufbauprotokoll den Ausgangspunkt der in *Kapitel 3.1* beschriebenen Modifikationen zur Schaffung von Unbeobachtbarkeit bei der Signalisierung eines Verbindungsaufbaus. Die Zusatzdienste des ISDN, wie z.B. Anrufweiterleitung, Halten oder Anklopfen wurden in diese Modifikationen nicht einbezogen und sollen aus diesem Grund hier nicht beschrieben werden. Momentan bietet das ISDN keine integrierten Sicherheitsfunktionen, weder eine Ende-zu-Ende-Verschlüsselung der Nutzdaten noch einen Schutz der Vermittlungsdaten, wie er in dieser Arbeit beschrieben werden soll. Lösungen zur Ende-zu-Ende-Verschlüsselung werden z.B. in [Axla_95, Stol_95, Tele_95] beschrieben.

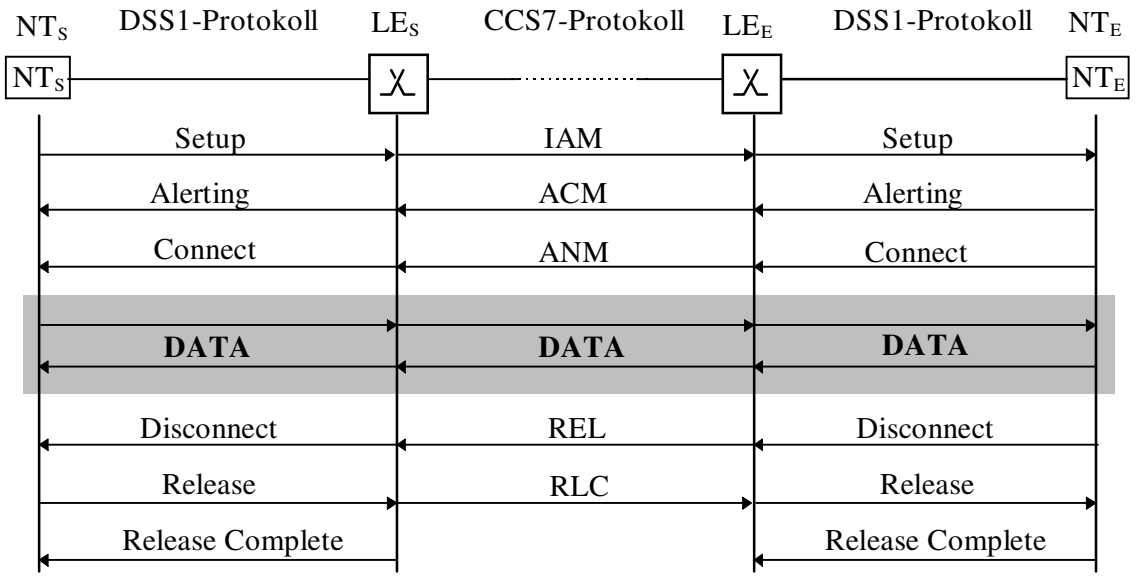


Abb. 2.3.1.2: Signalisierungsprotokoll des Verbindungsaufbaus

2.3.2 Das Global System for Mobile Communication (GSM)

Abb. 2.3.2.1 zeigt die **GSM-Netzstruktur** als hierarchisch gegliedertes System verschiedener Netzelemente. Die unterste Ebene ist, wie im ISDN, die Nutzerebene mit den Mobilstationen (MS). Hinzu kommt die Mobilität der Teilnehmer. Die Mobilteilnehmer halten sich stets in einer bestimmten Funkzelle eines Location Areas (LA) auf. Jede Funkzelle wird von einer Base Transceiver Station (BTS) versorgt, wobei jeweils eine bestimmte BTS-Anzahl von einem Base Station Controler, der in der Abbildung zur Vereinfachung nicht dargestellt wurde, gesteuert wird. Diese Netzeinrichtungen bilden zusammen ein Base Station Subsystem (BSS). Verschiedene BSS werden in der nächsten Verwaltungsstufe zu einem Mobile Switching Center (MSC) und dessen Visitor Location Register (VLR) zugeordnet. Die höchste Stufe der Verwaltungshierarchie bildet das Home Location Register (HLR). In der Netzstruktur werden die Datenbanken der Intelligenten Netzwerk-Ebene (IN) bzw. dem Intelligent Network Application Part (INAP) zugeordnet, der oberhalb der Signalisierungsebene dargestellt wird. Neben den MSCs existieren Gateway-MSCs (GMSC), die Interworking Functions (IWF) beim Übergang zu anderen Kommunikationsnetzen realisieren. Im Authentication Center (AuC) werden die Teilnehmerauthentikationsdaten und im Equipment Identity Register (EIR) die Geräteidentitäten gespeichert.

Beim Verbindungsaufbau wird auf der Funkschnittstelle das Radio Interface Layer 3 (RIL3)-Protokoll eingesetzt und im Festnetzbereich CCS7-MAP und CCS7-ISDN-UP. Andere verwendete Protokolle bzw. spezielle Schnittstellen zwischen Netzeinrichtungen werden in dieser Arbeit nicht beschrieben, da deren Kenntnis zum Verständnis der Modifikationen zum Schutz der Vermittlungsdaten nicht zwingend notwendig ist.

Die Protokolle der Basisabläufe des Location Updates (LUP) und des Verbindungsauf- bzw. -abbaus sollen hier ebenfalls nicht dargestellt werden. Sie können [GSM_03.20] entnommen werden. In der modifizierten Variante werden diese Protokolle im *Kapitel 3.2* beschrieben.

GSM bietet verschiedene Kommunikationskanäle mit unterschiedlicher Datenrate. Die leistungsstärksten sind der nichttransparente Sprachkanal mit 13 kbps und der bittranspa-

rente Datenkanal mit 9,6 kbps. Darüber hinaus existieren Half Rate-Kanäle bzw. Datenkanäle mit niedrigerer Datenrate.

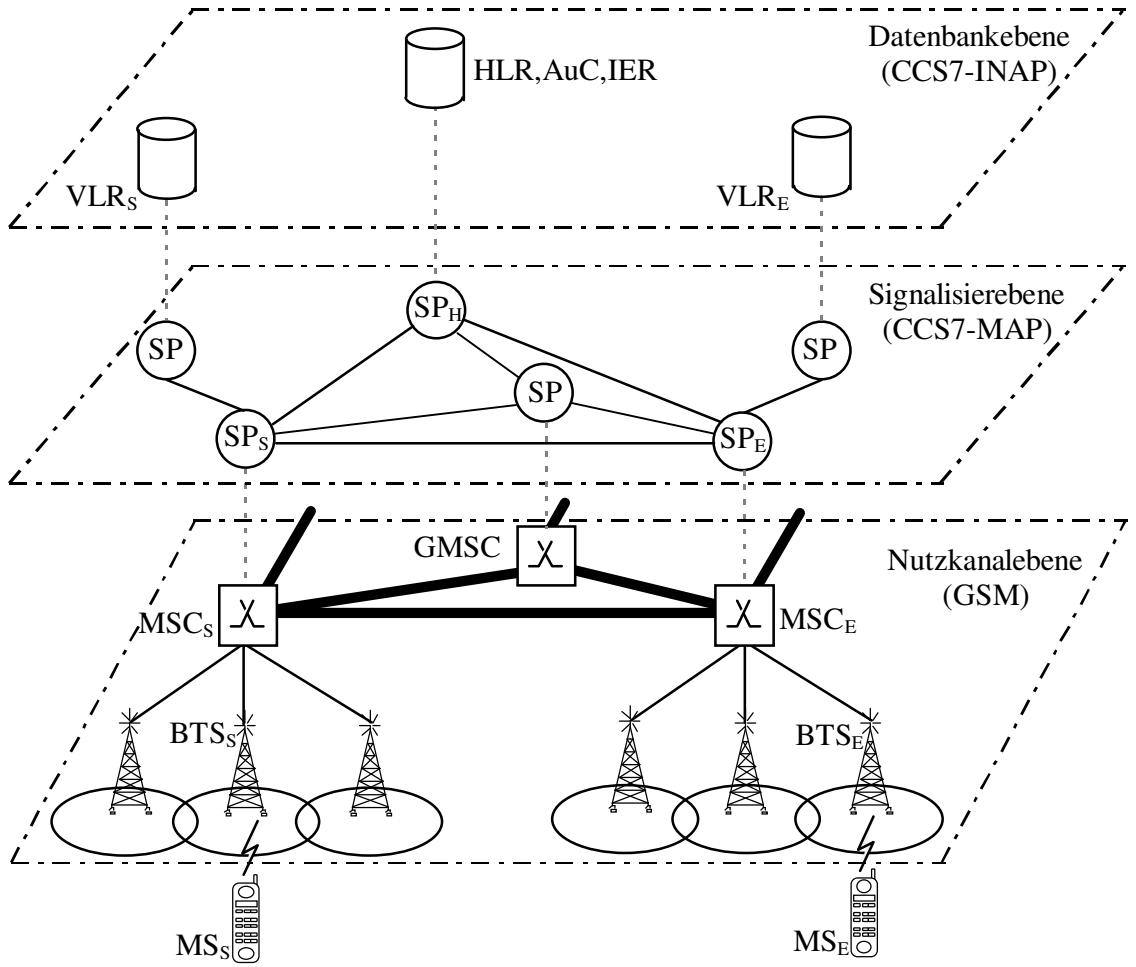


Abb. 2.3.2.1: GSM-Netzstruktur

2.4 Verfahren zur Schaffung von Anonymität und Unbeobachtbarkeit

2.4.1 Lösungskonzepte für Datenschutz garantierende Netze

In [PfPW_89] werden zur Realisierung Datenschutz garantierender Digitalnetze drei Lösungskonzeppte angegeben:

1. das **DC-Netz** [Chau_88] mit den Verbesserungen in [Waid_89, WaPf_89, WaPf1_89],
2. das Konzept der **physikalischen Unbeobachtbarkeit** [Pfit1_83, Pfit_89] und
3. das **MIX-Netz** [Chau_81], mit den Verbesserungen aus [PfPW_89] zur Vermeidung der Angriffsmöglichkeit aus [PfPf_89].

Weiterhin wird in [PfPW_89] festgestellt, daß die ersten beiden Konzepte es erfordern, daß jeder Netzabschluß im physikalischen Sinne mindestens halb soviel sendet, wie alle Netzabschlüsse zusammen im logischen Sinne senden. Auf den existierenden schmalbandigen Signalisierungskanälen sind diese Konzepte daher nicht realisierbar, so daß unter der gesetzten Zielstellung, vorhandene Netze zu modifizieren und nicht neue Netze zu entwerfen, entsprechend [PfPW_89] nur das MIX-Netz in Frage kommt. Deshalb basiert

das im folgenden vorgestellte Verfahren auf dem MIX-Netz. Die detaillierte Beschreibung der Idee erfolgt in den *Abschnitten 2.4.2-2.4.4*, wobei die in [PfPW_89] beschriebenen Telefon-MIXe den Ausgangspunkt darstellen.

2.4.2 Grundprinzip des MIX-Netzes

In diesem Abschnitt soll kurz das Grundprinzip des MIX-Netzes eingeführt werden. Das MIX-Netz wurde in 1981 von David Chaum in [Chau_81] erstmals veröffentlicht. Es gibt prinzipiell zwei grundlegende Möglichkeiten, ein MIX-Netz zu betreiben.

Einmal kann man dem Teilnehmer die Wahl der MIXe und deren Reihenfolge überlassen. Dadurch ist der Teilnehmer in seinem Vertrauen in die MIX-Betreiber flexibler, es müssen aber Listen verfügbarer MIXe geführt werden, Schlüssel verteilt werden und die gewünschten MIXe adressiert werden. Dadurch werden die MIX-Nachrichten verlängert und es sind abhängig von der Lage der vom Teilnehmer gewählten MIXe nicht die effizientesten Wege für die Nachrichten durch das Kommunikationsnetz möglich.

Deshalb soll in dieser Arbeit die zweite Möglichkeit des MIX-Netzes, die **MIX-Kaskade** gewählt deren. Dabei werden einzelne MIX-Knoten einer Kaskade fest zugeordnet. Alle von der Kaskade zu mixenden Nachrichten werden an den ersten MIX gesendet und dann automatisch, ohne Adressierung durch die gesamte MIX-Kaskade bearbeitet. Es gibt auch Mischformen beider Varianten des MIX-Netzes, im folgenden kommt aber das Prinzip der MIX-Kaskade zum Einsatz.

Außerdem kann man im Betreiben der MIXe zwischen **Pool- und Batch-(Schub)betrieb** wählen. Für diese Arbeit werden die MIX-Kaskaden im Schubbetrieb genutzt, um maximale Verzögerungszeiten garantieren zu können. Auch für die Realiserung der Unbeobachtbarkeit des physischen Sendens bietet sich die anschließende Verarbeitung der Nachrichten in MIX-Kaskaden im Schubbetrieb an, da alle Teilnehmer gleichzeitig senden sollen.

Im folgenden wird die Erklärung des **Grundprinzips der MIX-Kaskaden im Schubbetrieb** aus [PfPW_89] wiedergegeben, da dort die benötigten Grundlagen sehr gut beschrieben werden.

Möchte ein Sender S an einen Empfänger E eine Nachricht N senden und soll die Beziehung zwischen S und E verborgen werden, so sendet S seine Nachricht über eine fest vorgegebene Folge $M_1,...,M_m$ von m ausgezeichneten Stationen. Diese werden als MIXe, die Folge als MIX-Kaskade bezeichnet.

Der erste MIX M_1 faßt alle Nachrichten, die er in einem bestimmten Zeitraum erhalten hat, zu einem sogenannten Eingabeschub zusammen. Jede Nachricht des Schubs wird **umcodiert**, d.h. ihr Aussehen wird in einer Weise geändert, die für keinen möglichen Angreifer, außer für M_1, der die Umcodierung vornimmt, und denjenigen, der die Nachricht entsprechend vorbereitet hat, nachvollziehbar ist. Alle Ausgabenachrichten werden gegenüber der Reihenfolge im Eingabeschub (z.B. gemäß einer festen Ordnungsrelation) **umsortiert** und zu einem Ausgabeschub zusammengefaßt. Damit erhält ein Angreifer, der nicht von M_1 unterstützt wird, keine (zusätzliche) Information über die Zuordnung von nicht von ihm selbst vorbereiteten Nachrichten im Eingabeschub von M_1 zu Nachrichten im Ausgabeschub von M_1.

Das Verfahren wird durch jeden weiteren MIX wiederholt, d.h. der Ausgabeschub von M_i ist zugleich der Eingabeschub von M_{i+1}, i = 1 .. m-1 (siehe *Abb. 2.4.2.1*). Bereits ein einziger nicht den Angreifer unterstützender MIX gewährleistet die Unverkettbarkeit.

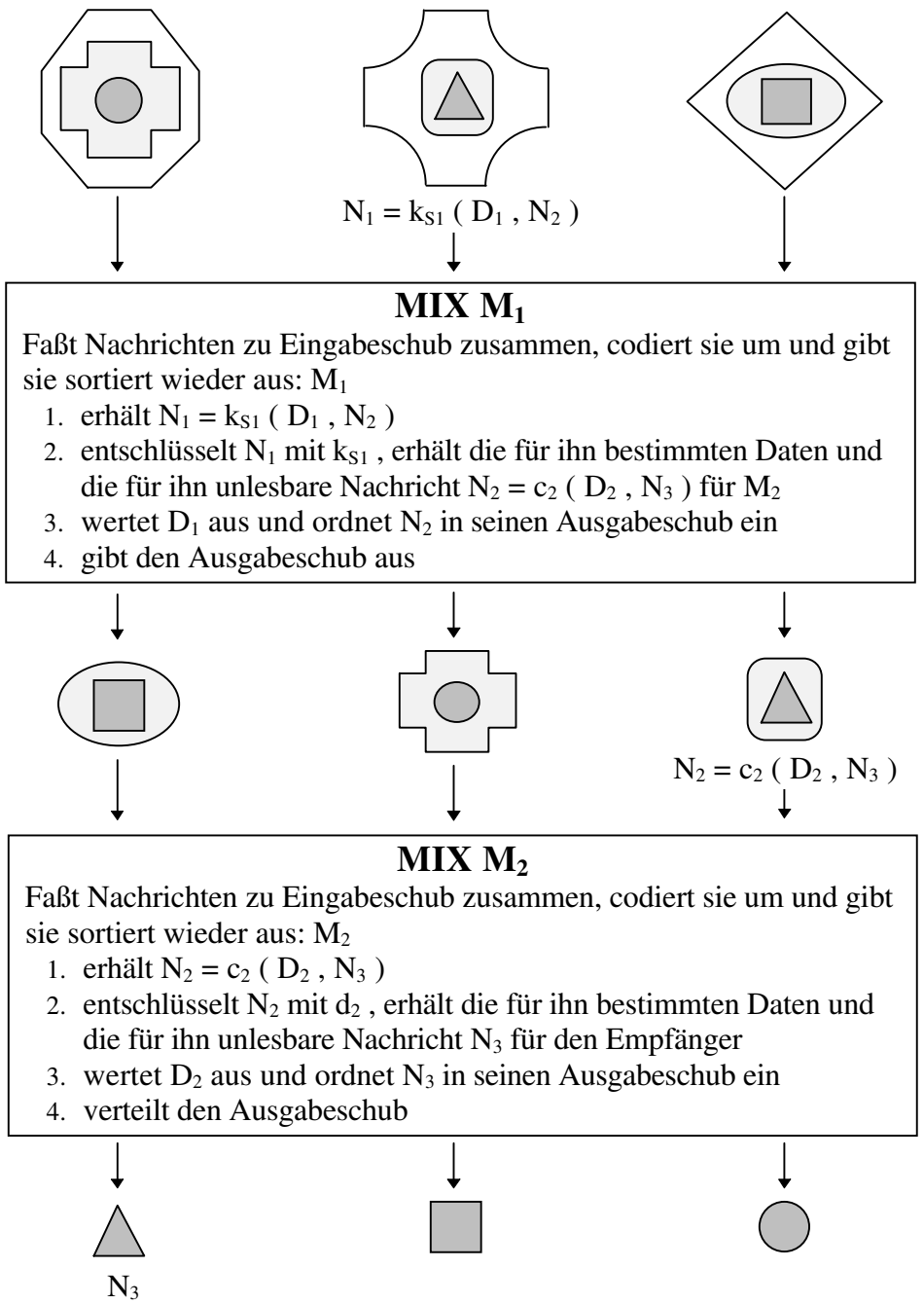


Abb. 2.4.2.1: MIX-Prinzip am Beispiel einer Kaskade mit 2 MIXen und einem Schub von 3 Nachrichten

Das Senden von Nachrichten bleibt beobachtbar. Daher kann der Empfänger einer Nachricht N die möglichen Sender von N auf diejenigen Teilnehmer begrenzen, die zum entsprechenden Zeitpunkt überhaupt etwas gesendet haben. Diese Beobachtungsmöglichkeit

wird beseitigt, indem alle Teilnehmer zu jedem möglichen Zeitpunkt gleichviel (notfalls bedeutungslose) Nachrichten zum Eingabeschub von M_1 beisteuern (**Dummy Traffic**).

Die Umcodierung wird im wesentlichen durch ein hybrides Kryptosystem realisiert (siehe *Abb 2.4.2.1*). Jeder MIX M_i, $i>1$[11], wählt sich ein Schlüsselpaar (c_i, d_i) des asymmetrischen Kryptosystems und gibt c_i öffentlich bekannt. In ISDN tauscht außerdem der MIX_1 mit jedem Netzabschluß S einen Schlüssel k_{S1} des symmetrischen Kryptosystems aus. Alle zu übermittelnden Nachrichten werden durch Auffüllen bzw. Aufspalten auf dieselbe Länge gebracht.

Angenommen ein Teilnehmer möchte über seinen Netzabschluß S die (bereits Ende-zu-Ende-verschlüsselte) Nachricht N an den Netzabschluß E eines anderen Teilnehmers senden, und zusätzlich jedem MIX M_i gewisse Daten D_i zukommen lassen[12]. Dann bildet er nacheinander die m+1 Nachrichten

$N_{m+1} := N$
$N_i := c_i^*(D_i , N_{i+1})$ für i = m, m-1, ..., 2
$N_1 := k_{S1}(D_1 , N_2)$ nur im ISDN, im GSM: $N_1 := c_1(D_1,N_2)$)

und sendet N_1 an M_1. N_1 wird als MIX-Eingabenachricht bezeichnet.

Jeder M_i erhält von M_{i-1} bzw. von S die Nachricht N_i, die Umcodierung von N_i besteht in der Entschlüsselung mit k_{S1} bzw. d_i und dem Beseitigen von D_i.

Die Verschlüsselungen mit c_i^* müssen **indeterministisch** sein, damit ein Angreifer nicht einfach die Nachrichten des Ausgabeschubs neu verschlüsseln und durch Vergleich mit den Nachrichten des zugehörigen Eingabeschubs die MIXe überbrücken kann.

Die Entschlüsselungsfunktion jedes MIXes ist zwangsläufig deterministisch. Würde eine Nachricht N_i zweimal von M_i gemixt, so erschiene daher auch N_{i+1} zweimal als Ausgabe von M_i. Durch **Wiederholung** von N_i und Vergleich der Ausgabeschübe könnte also ein Angreifer leicht N_i mit N_{i+1} in Verbindung bringen. Genauer genügt hierzu schon die Wiederholung des ersten Blockes der Nachricht. Wiederholungen von Nachrichten in verschiedenen Schüben können durch den Schub eindeutig charakterisierende Zeitstempel ausgeschlossen werden, die den MIXen in den D_i vom Sender mitgeteilt werden. Nachrichten mit ungültigen **Zeitstempeln** werden ignoriert. Schwerer zu vermeiden sind Wiederholungen in demselben Schub. Daher müssen innerhalb eines Schubes die MIXe Nachrichten mit gleichen Anfangsblöcken ignorieren.

Ebenfalls zu verhindern ist, daß der Angreifer durch Manipulationen an einer Nachricht N_i (z.B.Verdoppeln einzelner Blöcke) für ihn erkennbare Muster in der zugehörigen Nachricht N_{i+1} erzeugen kann. Eine Stromchiffre, die dies garantiert, ist die Pseudo-Vernamchiffre, d.h. man erzeugt zur Verschlüsselung einer Nachricht N eine pseudozufällige Bitfolge der Länge $|N|$ (z.B. aus einer Blockchiffre im OFB-Modus) und bildet das bitweise exklusive Oder der Nachricht N und der Bitfolge. Die Pseudo-Vernamchiffre erzeugt bei bitsynchroner Übertragung keine Fortpflanzung von Übertragungsfehlern und ist daher für das Folgende besonders geeignet.

Damit die Umcodierung sicher ist, sollte das asymmetrische Kryptosystem gegen aktive Angriffe sicher sein.

[11] Da im ISDN der Teilnehmerstandort stets gleich bleibt, kann jeder Teilnehmer mit dem ersten MIX bereits einen symmetrischen Schlüssel austauschen, bevor die Netznutzung beginnt. In GSM ist dies aufgrund der Teilnehmermobilität nicht möglich. Dort wird auch die Nachricht an den ersten MIX asymmetrisch mit c_{S1} verschlüsselt.

[12] Der Grund dafür wird wenige Zeilen später erklärt.

Zum Schutz des Empfängers vor Beobachtung durch den Sender (der ja die Nachricht N_{m+1} kennt, die der Empfänger erhalten soll) wird der Ausgabeschub von M_m **an alle Netzabschlüsse verteilt**. Damit wird zugleich unbeobachtbar, wann jemand überhaupt eine Nachricht empfängt. Um unnötigen Aufwand zu vermeiden, werden bedeutungslose Nachrichten vom Sender für M_m erkennbar (z.B. in D_m) als bedeutungslos gekennzeichnet und vor der Verteilung von M_m ausgesondert. Bis zu M_m müssen sie jedoch von echten Nachrichten ununterscheidbar sein.

Die **Verteilung** muß **zuverlässig** sein: Angenommen, die Nachricht N von S an einen Teilnehmer X wird nicht korrekt verteilt, sondern nur einem Netzabschluß E zugestellt. Erhält S auf N eine Antwort, so war E=X, sonst (was meist durch Zeitschranken entscheidbar ist) war B≠X, und S kann die Suche nach X fortsetzen [Waid_89, WaPf_89].

Soweit die Beschreibung des MIX-Grundprinzips aus [PfPW_89]. Die beschriebene MIX-Variante wird auch in dieser Arbeit eingesetzt, deshalb wurde die Erklärung zitiert.

Es werden also MIX-Kaskaden im Schubbetrieb verwendet, um die Unbeobachtbarkeit und Anonymität von Teilnehmern zu erreichen. Als nächstes muß die **Lage der MIX-Kaskaden** fixiert werden. Dafür bieten sich Ortsvermittlungsstellen und Verbindungen zwischen diesen an. Außerdem ist zu diskutieren, wieviele MIX-Kaskaden auf dem Weg vom Sender zum Empfänger durchlaufen werden sollen. Unter der Voraussetzung, daß die Teilnehmer die Netze sicher und dennoch möglichst effizient nutzen möchten, kann festgestellt werden, daß zwei MIX-Kaskaden ausreichend sind, wobei eine zum Schutz des Senders und die andere zum Schutz des Empfängers dienen soll. Wöllte man „nur“ die Kommunikationsbeziehung (wer mit wem) vor Outsidern schützen, würde sogar eine MIX-Kaskade ausreichend sein. Dann könnte aber der Sender als Angreifer den Empfänger einer Nachricht identifizieren, bzw. umgekehrt, je nachdem wer die MIX-Kaskade nutzt. Verwendet man zwei MIX-Kaskaden z.B. in den Ortsvermittlungsstellen, so werden zwar die Teilnehmer geschützt, es wird jedoch im Netz bekannt, welcher LE mit welchen LEs wie lange, wieviele Nutzkanalverbindungen unterhält. Da dadurch der Schutz der Teilnehmer nicht eingeschränkt wird, besteht darin allerdings kein Problem. Desweiteren sollten diese MIX-Kaskaden im LE angesiedelt werden, weil dadurch (zumindest im ISDN) **Anonymitätsgruppen** fester Größe entstehen. Aber auch im GSM bieten sich die MSCs für die MIX-Kaskaden an, denn ein weiterer Vorteil liegt in den geringeren Eingriffen, die im Fernnetz notwendig sind. Das komplette Routing der Nachrichten im Fernnetz, die Lastbalancierung und die Netzverwaltung brauchen nicht modifiziert zu werden.

Deshalb werden die MIX-Kaskaden im Schubbetrieb innerhalb der LEs bzw. MSCs angesiedelt.

2.4.3 Prinzip der MIX-Kanäle

Das in *Kapitel 2.4.2* vorgestellte Verfahren eignet sich im wesentlichen für die Versendung einzelner Nachrichten. Möchte man mehrere Nachrichten nacheinander übermitteln, so ist eine effizientere Verarbeitung in den MIXen notwendig.

Dazu wird die Idee der hybriden Verschlüsselung weiterentwickelt bzw. portiert. Bei der hybriden Verschlüsselung wird nur der erste Block der Nachricht asymmetrisch verschlüsselt. Darin wird dem Empfänger ein symmetrischer Schlüssel mitgeteilt, mit dem anschließend der Rest der Nachricht sehr effizient verschlüsselt wird.

Bezogen auf Kommunikationsnetze, bedeutet diese Idee, daß mit den Verbindungswunschnachrichten, die asymmetrisch verschlüsselt versendet werden müssen, effizient **symmetrisch arbeitende Kanäle** durch die MIX-Kaskaden aufgebaut werden, die während der weiteren Signalisierung und anschließenden Kommunikation symmetrisch und somit sehr schnell genutzt werden können.

Zum **Kanalaufbau** wird über den Signalisierungskanal eine MIX-Eingabenachricht N_1 gesendet, die den MIXen lediglich die **symmetrischen Schlüssel** für die anschließende hybride Verschlüsselung mitteilt. Jeder MIX merkt sich zusätzlich die **Zuordnung der Kanalaufbaunachricht** vom Eingabe- zum Ausgabeschub. Durch die Zuordnung der Nachrichten vom Eingabe- zum Ausgabeschub von M_i wird gleichzeitig auch die Vermittlung der Eingabe- auf die Ausgabekanäle von M_i festgelegt. Damit ist durch das Mixen einer Kanalaufbaunachricht ein Kanal durch alle MIXe definiert, auf dem anschließend die eigentlichen Nachrichten übermittelt werden könnten.

Eine Verteilung aller Kanäle an alle Netzabschlüsse zum Schutz des Empfängers ist nicht sinnvoll. Das Problem der Unbeobachtbarkeit des Empfängers vor dem Sender wird dadurch umgangen, indem der Empfänger dem Sender gleichgestellt wird. Ein aufgebauter Kanal kann als Sende- oder Empfangskanal genutzt werden.

Ein **Sendekanal** bildet das Analogon zur hybriden Verschlüsselung. Der Sender baut den Sendekanal, wie beschrieben auf und verschlüsselt anschließend die Informationen fortlaufend als $k_{S1}(k_{S2}(...k_{Sm}(N)...))$. In den MIXen wird der Nachrichtenstrom fortlaufend entschlüsselt und auf demselben Wege durch die MIX-Kaskade übermittelt. Der MIX M_m bildet durch seine Entschlüsselung am Ende den Klartextstrom N.

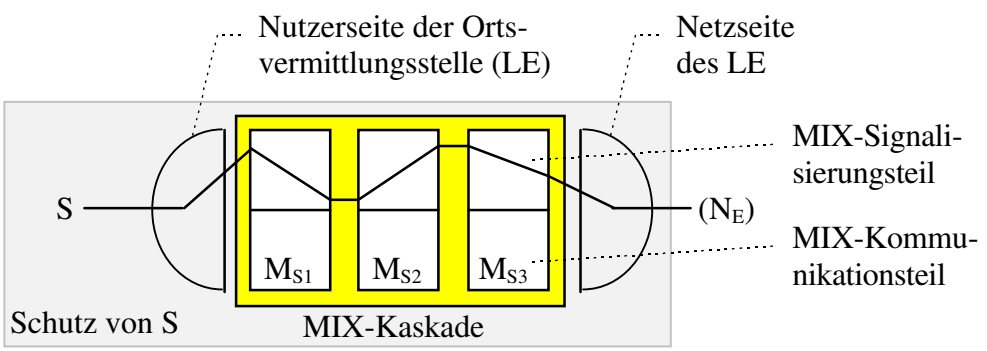
Ein **Empfangskanal** ist im wesentlichen ein in der entgegengesetzten Richtung betriebener Sendekanal. Der Empfänger muß den Empfangskanal zuvor mit der gleichen Art von Kanalaufbaunachricht aufbauen und der MIX M_m erhält vom Sender den Klartextstrom N, der in der MIX-Kaskade mit den verteilten symmetrischen Schlüsseln stufenweise verschlüsselt wird und anschließend in der Form $k_{E1}(k_{E2}(...k_{Em}(N)...))$ an den Empfänger übermittelt wird. Da der Empfänger alle verwendeten symmetrischen Schlüssel kennt, kann er daraus N berechnen.

Sende- und Empfangskanäle sind somit hinsichtlich ihrer Unbeobachtbarkeit völlig symmetrisch. Der Sender kann seinen Sendekanal nutzen, ohne daß der Empfänger ihn identifizieren kann. Ebenso ist der Empfänger eines Empfangskanals vor einer Identifizierung durch den Sender geschützt. Damit ein Teilnehmer sich in der Rolle als Sender und Empfänger schützen kann, benötigt er also für jede Kommunikation einen Sende- und einen Empfangskanal, die zusammen den MIX-Kanal (vollduplex) ergeben. Diese Sende- und Empfangskanäle des Senders und des Empfängers müssen jetzt noch entsprechend miteinander verknüpft werden. Dazu dient ein Kanalkennzeichen KKZ, das mit der Verbindungswunschnachricht ausgetauscht wird.

Da die Länge der zu mixenden Nachrichten den Aufwand der einzelnen MIXe entscheidend beeinflußt, ist es sinnvoll, die verschiedenen Nachrichtentypen separat zu mixen. Die Unbeobachtbarkeit wird dadurch nicht eingeschränkt und die Nachrichten brauchen nicht durch Auffüllen oder Aufspalten auf gleiche Länge gebracht werden. Deshalb werden im folgenden die MIXe in einen **Signalisierungsteil** (in Abbildungen oben) und einen **Kommunikationsteil** getrennt. Dennoch werden die beim Aufbau eines Sendekanals ausgetauschten symmetrischen Schlüssel und Kanalzuordnungen im Signalisierungs-MIX

während der Kommunikation auf dem Sendekanal im Kommunikations-MIX genutzt. Für den Empfangskanal eines Teilnehmers gelten dieselben Annahmen.

Abb. 2.4.3.1 zeigt den prinzipiellen **Aufbau von Sende- und Empfangskanälen mit 3 MIXen**. Der Teilnehmer sendet die Kanalaufbaunachricht auf dem exklusiv zugeordneten Signalisierungskanal an die Nutzerseite der Ortsvermittlungsstelle (LE). Dort wird die Nachricht an die MIX-Kaskade weitergegeben. Anschließend wird die MIX-Kaskade durchlaufen und die erforderlichen Zuordnungen und symmetrischen Schlüssel werden gespeichert. Während der letzte MIX M_m beim Aufbau eines Empfangskanals nur das Kanalkennzeichen erfährt, unter dem Informationen auf diesem Empfangskanal weitergeleitet werden sollen, erhält er beim Aufbau eines Sendekanals den zu verteilenden Verbindungswunsch. Dieser enthält die Adresse des LEs des Empfängers, eine Kennzeichnung des Verbindungswunsches als bedeutungslos oder bedeutungsvoll und die Verbindungswunschnachricht N_E an den Empfänger. Damit werden nur Verbindungswünsche im Ortsnetz des Empfängers verteilt, die keinen Dummy Traffic beinhalten.



Aufbau eines Sende- oder Empfangskanals

zu speichernde Informationen

LE-Nutzerseite	: D-Kanal$_S$	$\mapsto$ Nummer des Eingabeschubes (E-Nr.$_1$)von M_{S1}
M_{S1}	: E-Nr.$_1$	$\mapsto$ A-Nr.$_1$, k_{S1}
M_{S2}	: E-Nr.$_2$	$\mapsto$ A-Nr.$_2$, k_{S2}
M_{S3}	: E-Nr.$_3$	$\mapsto$ A-Nr.$_3$, k_{S3}
LE-Netzseite	: A-Nr.$_3$	$\mapsto$ KKZ, ($A_{LE(E)}$, Bv/Bl)

Abb. 2.4.3.1: Aufbau eines Sende- oder Empfangskanals

Nachdem der Empfänger durch die Verteilung der Nachricht N_E von dem Verbindungswunsch erfahren hat, baut er seinen Sende- und Empfangskanal mit den entsprechend von S gesendeten Kanalkennzeichen und der Zieladresse $A_{LE(S)}$ auf.

Abb. 2.4.3.2 zeigt die **Übermittlung einer Nutzkanalinformation** von S nach E über die bereits bestehenden Sende- und Empfangskanäle der Teilnehmer. Der Sender S nutzt seinen Sendekanal, um vom Empfänger nicht identifiziert zu werden, der MIX M_m des Senders kennt die Adresse der Ortsvermittlungsstelle des Empfängers und das Kanalkennzeichen des Empfangskanals dort. Die Daten werden im Fernnetz zur Ortsvermittlungsstelle übertragen, diese Kommunikation zwischen den Ortsvermittlungsstellen ist und bleibt beobachtbar. Die Netzseite des LEs von E gibt die Daten an die MIX-Kaskade und damit auf den Empfangskanal von E weiter und E muß die empfangenen Daten noch mit den symmetrischen Schlüsseln der MIXe entschlüsseln. Ein Duplexkanal entsteht durch zwei gegenlaufende Simplexkanäle und die Kommunikation in der Gegenrichtung funktioniert analog. Muß ein Teilnehmer Dummy Traffic senden, so verknüpft er seinen

Sendekanal mit seinem Empfangskanal und sendet den Dummy Traffic auf diesem Weg, ohne beobachtbar zu werden.

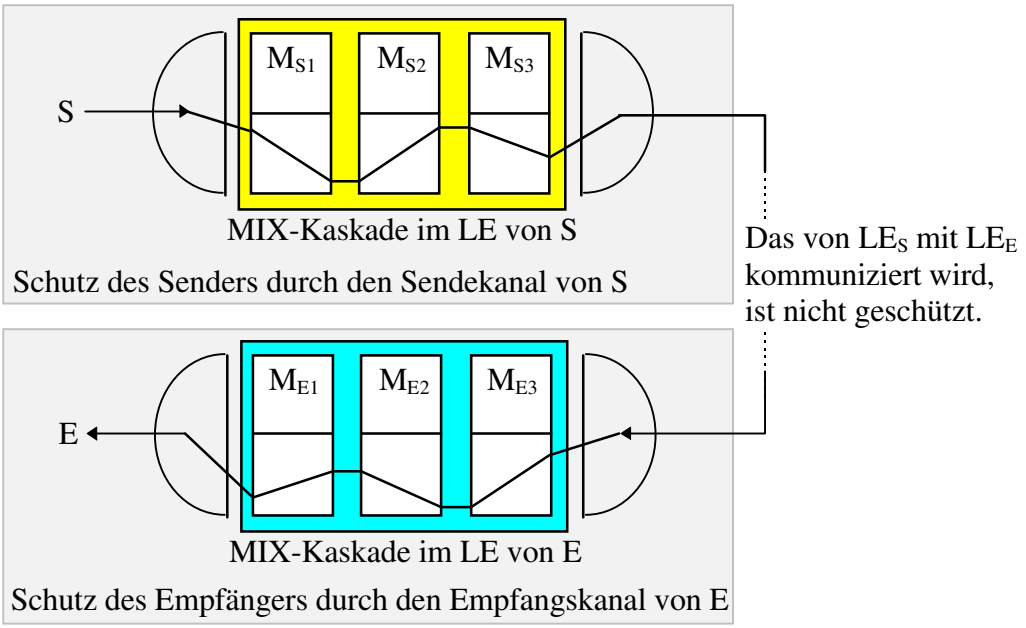


Abb. 2.4.3.2: Kommunikation vom Sender zum Empfänger über MIX-Kanäle

Festzuhalten bleibt außerdem, daß jeder Teilnehmer nicht nur zur **gleichen Zeit Sende- und Empfangskanäle aufbauen** muß, sondern daß er auch **jederzeit gleich viele Sende- und Empfangskanäle unterhalten** muß (notfalls Scheinkanäle). Wird auf einem Kanal nichts übertragen, so überbrückt jeder MIX die fehlenden Informationen durch bedeutungslose Daten. Dadurch wird z.B. verhindert, daß der Sender den Empfänger identifizieren kann, indem er auf seinem Sendekanal keine Informationen mehr überträgt und der Empfänger deshalb keine Informationen mehr erhält.

Das bis zu dieser Stelle beschriebene Verfahren kann allerdings so noch nicht eingesetzt werden. Damit die Aktionen der Teilnehmer nicht beobachtbar sind, mußten **Kanalaufbaunachrichten gleichzeitig** gesendet werden und gleich viele Kanäle belegt werden. Ein noch größeres Problem ist aber, daß **gleichzeitig aufgebaute Kanäle auch gleichzeitig wieder abgebaut** werden müssen, da die Nachrichten eines Schubes gleich lang sein müssen. Dadurch wird eine effektive Nutzung der zwei Nutzkanäle auch innerhalb einer kleineren Anonymitätsgruppe unmöglich. Deshalb wird in *Abschnitt 2.4.4* das Prinzip des getakteten Kommunikationssystems eingeführt.

2.4.4 Konzept des getakteten Kommunikationssystems

Durch die Einführung eines **Systemtaktes** (auch **Zeitscheibe** genannt) wird es für den Teilnehmer möglich, unbeobachtbare Verbindungen, also unbeobachtbare Ende-zu-Ende-Kanäle von beliebiger Dauer zu unterhalten, die trotzdem von jedem Kommunikationspartner regelmäßig abgebaut werden können.

Die im letzten Abschnitt aufgezeigten Probleme kann man lösen, indem beliebig lang andauernde Verbindungen auf mehrere **kurze** (ca. 1s) und **unmittelbar aufeinanderfolgende MIX-Kanäle**, im folgenden **Zeitscheibenkanäle** genannt, aufgeteilt werden. Zu Beginn jeder Zeitscheibe hat jeder Teilnehmer die Möglichkeit, eine neue Verbindung aufzubauen, oder eine bestehende abzubrechen.

Die Länge einer Zeitscheibe bzw. eines Systemtaktes sei z. Der **Systemtakt** erfolgt **synchron für alle Teilnehmer des gesamten Netzes**. Die Zeitscheibenkanäle werden im folgenden Zeitscheiben-Sende-(ZS)-Kanal und Zeitscheiben-Empfangs-(ZE)-Kanal genannt. Um Unbeobachtbarkeit zu gewährleisten, muß **jeder Netzabschluß in jeder Zeitscheibe für jeden Nutzkanal eine ZE- und eine ZS-Kanalaufbaunachricht** signalisieren und Informationen auf den belegten Nutzkanälen übermitteln (notfalls jeweils Dummy Traffic).

Der **Aufbau und die Nutzung unbeobachtbarer Kanäle muß parallel** erfolgen. Würde man zu Beginn jeder Zeitscheibe zuerst die Kanäle aufbauen und erst anschließend die Kanäle nutzen, so können zu Beginn jeder Zeitscheibe keine Nutzdaten gesendet werden. Dadurch könnte **kein isochroner Kommunikationsdienst** angeboten werden. Dieses Problem kann jedoch beseitigt werden. Man läßt die Zeitscheibe für die Nutzdaten erst beginnen, wenn die unbeobachtbaren Kanäle aufgebaut sind, d.h. man baut die unbeobachtbaren Kanäle auf und nutzt diese anschließend mit der vollen Zeitscheibenlänge, während parallel bereits die unbeobachtbaren Kanäle der nächsten Zeitscheibe aufgebaut werden. Vereinfacht bedeutet dies, das die **aufgebauten unbeobachtbaren Kanäle mit den ausgetauschten symmetrischen Schlüsseln stets erst während der nächsten Zeitscheibe genutzt** werden. In den folgenden Kapiteln wurde dieser Aspekt jedoch zur Vereinfachung der Darstellungen und Erklärungen nicht berücksichtigt.

Die Signalisierung erfolgt im wesentlichen über den eigenen **Signalisierungskanal**. Da dieser aber den **Hauptengpaß des Verfahrens** darstellt, wird ein Teil der Signalisierungsaufgaben auf den **Nutzkanal verlagert**. Der Auf- und Abbau von Verbindungen erfolgt, wie in *Abschnitt 2.4.3* beschrieben nun in jeder Zeitscheibe, deshalb soll an dieser Stelle auf eine nochmalige Darstellung verzichtet werden. Die technische Realisierung wird bezogen auf die jeweiligen Kommunikationsnetze in *Kapitel 3* detailliert beschrieben.

Die **Realisierung der Abrechnung** der Netz- und Dienstnutzung wird in dieser Arbeit nicht betrachtet. Für Gespräche innerhalb eines Ortsnetzes ist eine Abrechnung von Einzelgesprächen technisch sinnlos, da sie im Netz keinerlei zusätzlichen Aufwand verursachen und zudem völlig unbeobachtbar sind. Zur Abrechnung von Verbindungen, die das Fernnetz benutzen, können den Verbindungsaufbaunachrichten für den letzten MIX **Gebührenmarken** beigelegt werden. Einige ausführlichere Anmerkungen zur Abrechnung trotz unbeobachtbarer Netznutzung können in [PfPW_89] nachgelesen werden.

3. Realisierung von anonymer Signalisierung

3.1 Anonyme Signalisierung am Beispiel des ISDN-Festnetzes

3.1.1 Modifikation der Netzstruktur

Um für die Teilnehmer anonyme Signalisierung von Verbindungswunsch-, Kanalaufbau- und Kanalabbaunachrichten im ISDN gewährleisten zu können, ist die in *Abb. 2.3.1.1* dargestellte ISDN-Netzstruktur durch MIX-Kaskaden gemäß *Kapitel 2.4* zu erweitern. Dadurch werden die Teilnehmer mit ihren NTs einer Anonymitätsgruppe zugeordnet (siehe *Kapitel 2.4*). Diese umfaßt jeweils alle Teilnehmer einer Ortsvermittlungsstelle. Innerhalb seiner Anonymitätsgruppe ist jeder Teilnehmer unbeobachtbar und anonym. *Abb. 3.1.1.1* zeigt die modifizierte **Netzstruktur von ISDN**.

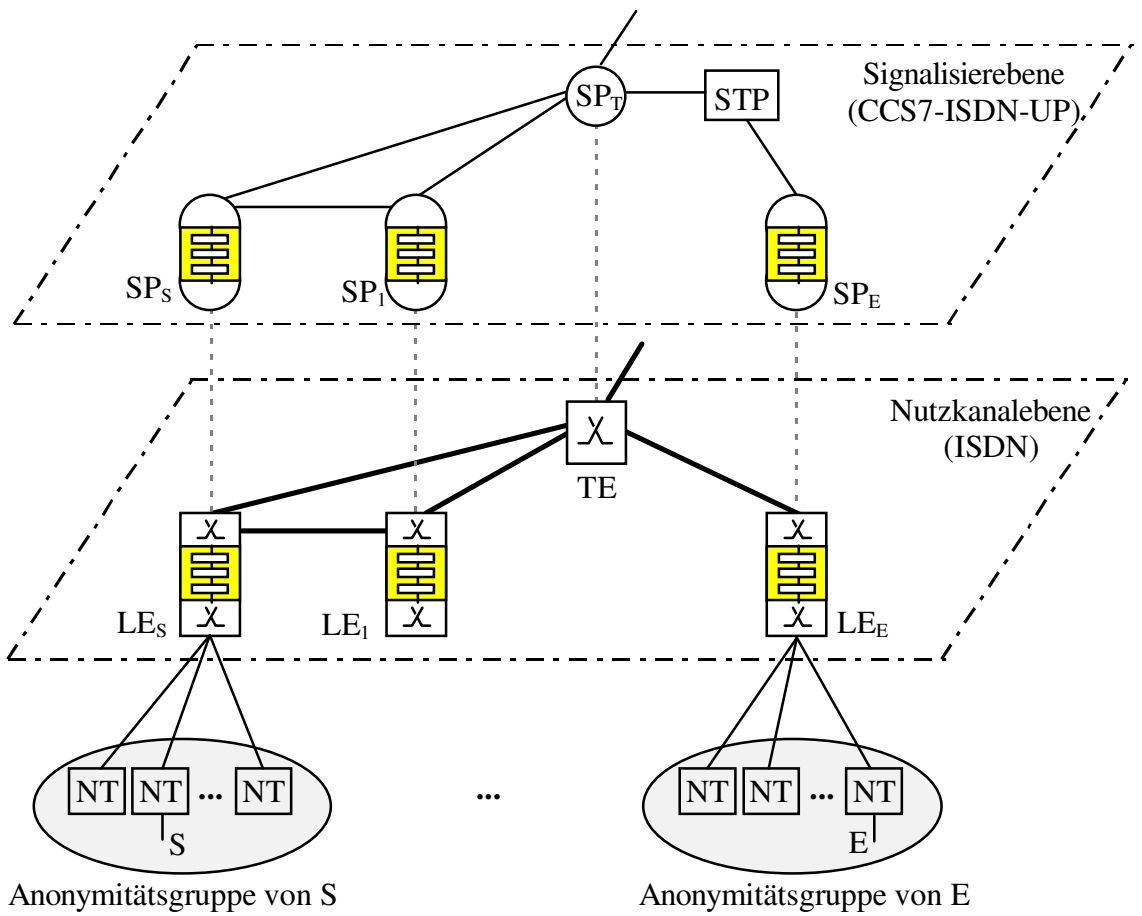


Abb. 3.1.1.1: Modifizierte ISDN-Netzstruktur

Man erkennt, daß nur die Ortsvermittlungsstellen und deren Signalisierungspunkte (SP), zum Schutz der daran angeschlossenen Teilnehmer, um MIX-Funktionalität erweitert werden müssen. Außerdem ist ersichtlich, daß verschiedene MIX-Kaskadentypen für die Signalisierung und für die Kommunikation benötigt werden. Diese benutzen paarweise gleiche symmetrischen Schlüssel und Schubzuordnungen (siehe *Abschnitt 2.4.3*).

Die **Nutzerseite einer Ortsvermittlungsstelle** erhält gemäß *Abschnitt 2.4.4* in jedem Takt des Kommunikationssystems von jedem angeschlossenen Teilnehmer sowohl

Nachrichten auf dem Signalisierkanal (D-Kanal), als auch auf den Datenkanälen (B-Kanäle). Diese Nachrichten sind ggf. bedeutungslos (Dummy Traffic). Das ist allerdings für die Nutzerseite einer Ortsvermittlungsstelle nicht erkennbar, so daß sie keine Rückschlüsse auf eine bestehende Kommunikationsbeziehung bestimmter Teilnehmer ziehen kann. Genau diese Beobachtungsmöglichkeiten der Nutzerseite einer Ortsvermittlungsstelle sind auch der in *Abschnitt 2.4.2* genannte Grund für die Notwendigkeit des Einsatzes von Dummy Traffic auf dem Weg zur Ortsvermittlungsstelle. Würden Teilnehmer nur im Bedarfsfall Daten auf den ihnen exklusiv zugeordneten Kanälen zur Ortsvermittlungsstelle senden bzw. signalisieren, so wäre dies von der Nutzerseite der Ortsvermittlungsstelle beobachtbar. Dadurch könnte die Ortsvermittlungsstelle die Anonymitätsgruppe verkleinern und Erkenntnisse zum Kommunikationsverhalten bestimmter Teilnehmer gewinnen, z.B. welcher Teilnehmer kommuniziert wann und wie lange.

Die **Netzseite der Ortsvermittlungsstelle** kann beobachten, wohin Nachrichten einer Anonymitätsgruppe signalisiert werden bzw. zu welchen Ortsvermittlungsstellen Kommunikationsbeziehungen aus der Anonymitätsgruppe heraus bestehen. Sie erhält aber auch nach Zusammenarbeit mit der Nutzerseite der Ortsvermittlungsstelle keine Information darüber, von welchem Teilnehmer diese Nachrichten stammen. Erkennbar ist aber, wie lange wird von welcher Ortsvermittlungsstelle mit welcher Ortsvermittlungsstelle kommuniziert und wann bzw. zu welcher Ortsvermittlungsstelle werden Verbindungswünsche signalisiert.

3.1.2 Modifikation des Signalisierungsprotokolles zum Verbindungsaufbau

Nach der Erweiterung der Ortsvermittlungsstellen und der zugehörigen Signalisierungspunkte um MIX-Kaskaden ist das Signalisierungsprotokoll aus *Abb. 2.3.1.2* zur Erfüllung der Datenschutzanforderungen aus *Abschnitt 2.1.2* mit den in *Kapitel 2.4* beschriebenen Methoden zu modifizieren.

Abb. 3.1.2.1 zeigt das modifizierte **Signalisierungsprotokoll zum Verbindungsaufbau**[13] . Zum Aufbau einer unbeobachtbaren Kommunikationsverbindung initiiert der Sender den Aufbau eines unbeobachtbaren Zeitscheiben-Empfangskanals (ZE-Kanal) durch die entsprechende Nachricht über den Signalisierungskanal. Außerdem baut er einen Zeitscheiben-Sendekanal (ZS-Kanal) für das unbeobachtbare Senden von Informationen auf. Die Netzseite der Ortsvermittlungsstelle des Senders erhält mit der ZS-Setup-Nachricht die im CCS7-Netz zu sendende Verbindungswunschnachricht und die Adresse der Ortsvermittlungsstelle des Empfängers und sendet eine Initial Address Message (IAM) ab. Mit der im CCS7-Netz zum Empfänger gerouteten IAM wird bereits ein Kommunikationskanal bis zur Ortsvermittlungsstelle des Empfängers belegt und geschaltet. Die mit der IAM in der Zielortsvermittlungsstelle eintreffende Nachricht an den Empfänger wird an alle angeschlossenen Teilnehmer der Ortsvermittlungsstelle verteilt. Der gewünschte Empfänger kann als einziger die empfangene Verbindungswunschnachricht korrekt entschlüsseln. In dieser Nachricht erhält der Empfänger alle notwendigen Informationen zum Aufbau der Verbindung (siehe *Kapitel 2.4*). Dieser muß jetzt selbst aktiv werden und einen ZE-Kanal sowie einen ZS-Kanal aufbauen. Dadurch wird die Verbindung durchgängig geschaltet. Um Bandbreite auf dem schmalbandigen Signali-

[13] Vereinfachend wurde nicht zwischen der NT_S und dem Teilnehmerendgerät unterschieden, ebenso wurden die LEs dargestellt, obwohl die Signalisierung über die zugehörigen SPs und nur die Kommunikation im Nutzkanal über die LEs übertragen wird.

sierungskanal zu sparen, wird der Zustand des Klingelns des Empfängertelefons mit der Alerting-Nachricht bzw. der Address Complete Message (ACM) bereits im Datenkanal übertragen. Sobald der Empfänger abhebt, wird dies mit der Connect-Nachricht bzw. Answer Message (ANM) dem Sender über den Datenkanal mitgeteilt. Die in Abb. *3.1.2.1* hellgrau hinterlegten Flächen gehören also bereits zum Datenkanal, wobei die eigentliche Datenübertragung in der Abbildung dunkelgrau dargestellt ist.

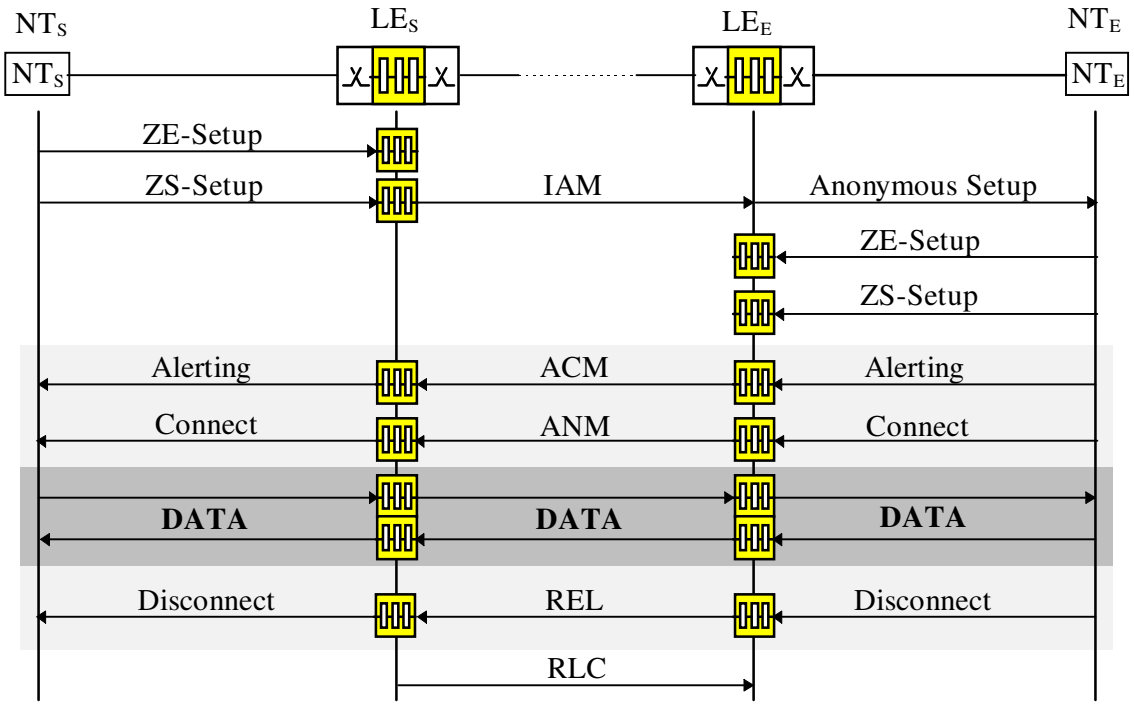


Abb. 3.1.2.1: Modifiziertes Signalisierungsprotokoll zum Verbindungsaufbau

Soll eine unbeobachtbare Verbindung nach einer erfolgten Kommunikation wieder abgebaut werden, so ist dies nur im Fernnetz nötig, da die Verbindung im Ortsbereich am Ende jeder Zeitscheibe automatisch abgebaut und am Beginn jeder Zeitscheibe im Bedarfsfall (sonst Dummy Traffic) auch automatisch wieder aufgebaut wird. Es wird also dem Gesprächsteilnehmer das Auflegen des Hörers im Datenkanal durch eine Disconnect-Nachricht bzw. Release Message (REL) mitgeteilt. Dieser legt nach Erhalt der Disconnect-Nachricht seinen Hörer auf und die Kommunikation ist beendet, da auch seine Verbindung im Ortsbereich automatisch beendet wird. Der B-Kanal im Fernnetz wird mit Erhalt der REL von den Vermittlungsstellen auf jedem Link separat abgebaut und dies mit Release Complete (RLC) anschließend signalisiert.

Die *Abb. 3.1.2.2* zeigt beispielhaft den **Ablauf eines Verbindungsaufbaus** in ISDN. Allerdings wird dies vereinfachend nur für einen B-Kanal dargestellt. Es sind 4 Systemtakte dargestellt, wobei die Aktionen der Senderseite links und die der Empfängerseite rechts angegeben werden. In jedem Systemtakt hat jeder Teilnehmer eine ZE-Setup- und eine ZS-Setup-Nachricht, sowie Daten auf dem geschalteten Datenkanal zu senden. Dabei erhält jeweils der letzte MIX Informationen zur Verknüpfung von Kommunikationskanälen.

So wird im **ZE-Setup** das aktuelle Kanalkennzeichen signalisiert, unter dem Daten auf dem Datenkanal entgegengenommen werden. Bei dieser Nachricht ist keine Unterscheidung von Dummy Traffic notwendig.

Im **ZS-Setup** wird die Adresse der Zielortsvermittlungsstelle und das dort aktuelle Kanalkennzeichen des ZE-Kanals mitgeteilt. Zusätzlich muß im ZS-Setup mitgeteilt werden, ob die Nachricht bedeutungsvoll oder bedeutungslos ist, um das Klingeln des Telefons während des Dummy Traffics zu verhindern. Handelt es sich bei der ZS-Setup-Nachricht um Dummy Traffic, so wird, wie in *Abschnitt 2.4.3* angegeben, der eigene ZE-Kanal als Empfänger adressiert und die Dummy-Verbindungswunschnachricht braucht nicht verteilt zu werden.

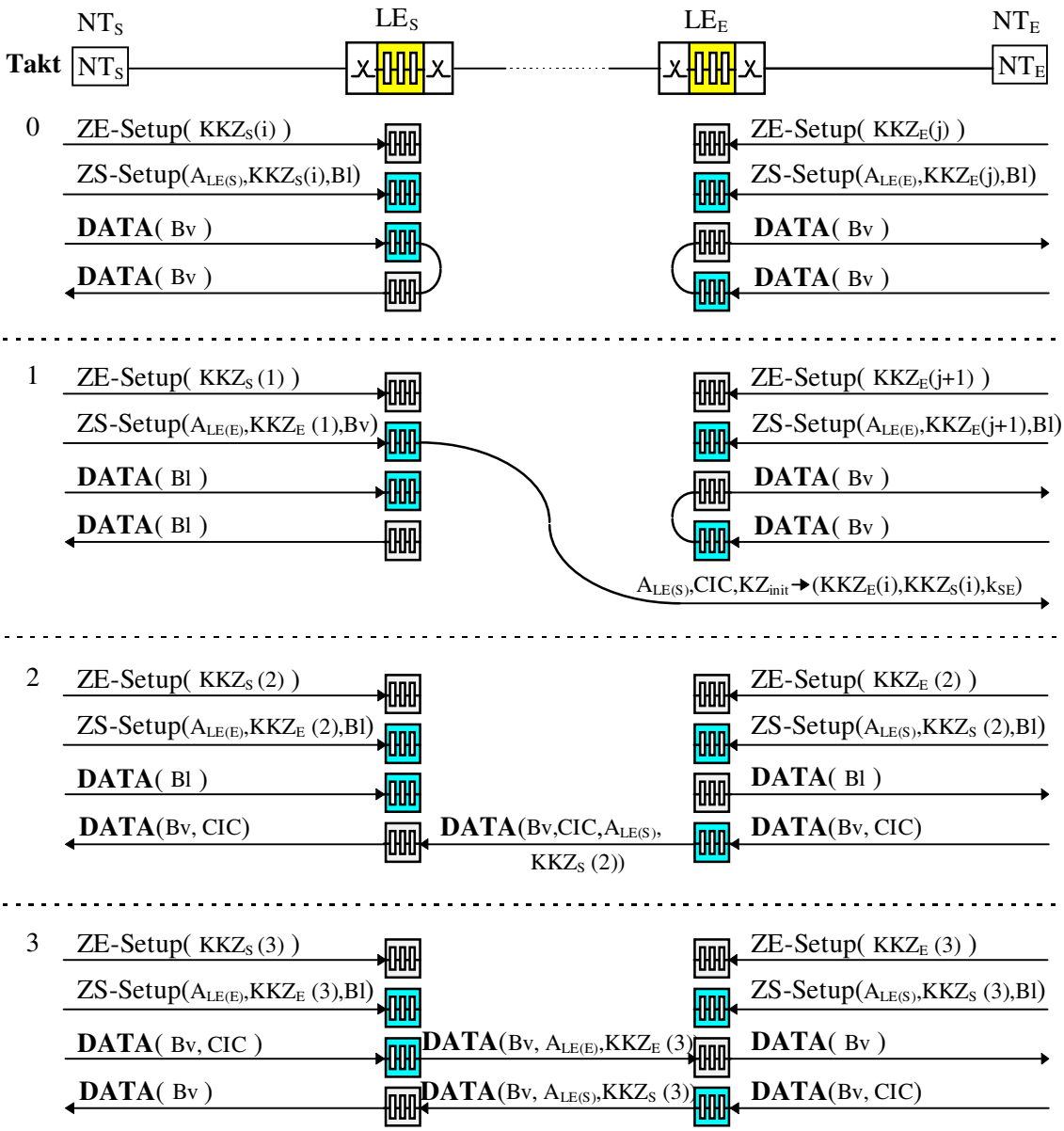


Abb. 3.1.2.2: Beispielszenario eines Verbindungsaufbaus

Daten werden auf dem ZS-Kanal gesendet und an den verknüpften ZE-Kanal weitergeleitet. Außerdem ist zu kennzeichnen, ob es sich um bedeutungsvolle (bv) oder bedeutungslose (bl) Nachrichten handelt. Die Daten werden folgendermaßen gekennzeichnet:

- während Dummy Traffic — bedeutungsvoll (oder bedeutungslos)
- während eines Verbindungsaufbaus — bedeutungslos
- während einer Verbindung — bedeutungsvoll

Während eines Verbindungsaufbaus sollten die Daten als bedeutungslos gekennzeichnet werden, damit diese von der Netzseite der Ursprungsortsvermittlungsstelle entfernt werden können und kein unnötiger Übertragungsaufwand im Fernnetz entsteht. Dadurch wird allerdings beobachtbar, wieviele Teilnehmer einer Ortsvermittlungsstelle eine Verbindung aufbauen möchten. Das hat wiederum Vor- und Nachteile, so könnte mit dieser Methode auch erkannt werden, wann Ortsgespäche[14] begonnen werden. Diese könnten dadurch mit einem festen Betrag unabhängig von der Länge abgerechnet werden. Soll diese Beobachtungsmöglichkeit im Ortsbereich verhindert werden, ist eine Kennzeichnung der Daten nicht mehr erforderlich, es entsteht aber zusätzlicher Aufwand im Fernnetz und Ortsgespräche können generell nicht mehr erkannt werden.

In *Abb. 3.1.2.2* ist folgender Ablauf des Verbindungsaufbaus dargestellt:

- **Takt 0:** Es wird von beiden Teilnehmern Dummy Traffic an sich selbst initiiert und gesendet. Die Kanalkennzeichen sind unabhängig voneinander von den Teilnehmern gewählt. Das ZS-Setup ist als bedeutungslos gekennzeichnet, so daß keine Verteilung eines Verbindungswunsches erfolgt. Die Daten werden als bedeutungsvoll an sich selbst gesendet.
- **Takt 1:** Der Sender S hat einen Verbindungswunsch an den Empfänger E. Er baut seinen ZE-Kanal auf und kennzeichnet die ZS-Setup-Nachricht als bedeutungsvoll. Damit wird der Verbindungswunsch durch das CCS7-Netz zur Zielvermittlungsstelle $A_{LE(E)}$ geroutet und dort an alle Teilnehmer verteilt. Darin teilt S den Initialwert KZ_{init} zur Berechnung gemeinsamer Kanalkennzeichen und eines Sitzungsschlüssels k_{SE} mit. Durch die Verbindungswunschnachricht wird bereits ein bidirektionaler Datenkanal im Fernnetz zwischen den beteiligten Ortsvermittlungsstellen allokiert und ein Kanalidentifikator (CIC[15]) dem Empfänger signalisiert. Die Daten von S werden während des Verbindungsaufbaus als bedeutungslos gekennzeichnet und in der Ursprungsortsvermittlungsstelle $A_{LE(S)}$ entfernt. Außerdem sendet die Ortsvermittlungsstelle (bzw. der erste MIX) auf dem ZE-Kanal des Senders Dummy Traffic solange E sich nicht meldet. Da E zu Beginn des Taktes 1 nichts von einem Verbindungswunsch für ihn weiß, sendet er auch in diesem Takt Dummy Traffic.
- **Takt 2:** Der Sender S wartet auf eine Antwort von E. S baut seinen ZE- und ZS-Kanal mit den weitergeschalteten Kanalkennzeichen auf und kennzeichnet seine ZS-Setup-Nachricht als Dummy Traffic. Außerdem sendet er weiterhin bedeutungslose Daten. E hat den Verbindungswunsch empfangen und antwortet bereits in diesem Takt (Optimalfall). Er baut seinen ZE- und ZS-Kanal mit den entsprechenden, aus dem Initialwert berechneten Kanalkennzeichen auf und kennzeichnet seine ZS-Setup-Nachricht ebenfalls als bedeutungslos. Im Datenkanal signalisiert er bedeutungsvoll Alerting und anschließend Connect an S. In der Alerting-Nachricht teilt E dem Sender den Kanalidentifikator CIC mit.
- **Takt 3:** Die Kommunikation ist angelaufen. Beide Teilnehmer bauen ihre ZE- und ZS-Kanäle mit entsprechend weiterberechneten Kanalkennzeichen auf und tauschen bedeutungsvolle Daten aus.

[14] Bei Ferngesprächen ist der Beginn und die Dauer in jedem Fall bekannt, da keine MIXe zwischen den Ortsvermittlungsstellen eingesetzt werden und der Schutz des einzelnen Teilnehmers dennoch gewährleistet ist.

[15] Der CIC bildet zusammen mit dem Originated Point Code (OPC) und dem Destination Point Code (DPC) ein netzweit eindeutiges Kennzeichen des Nutzkanals. Der OPC entspricht dem $A_{LE(S)}$ bzw $A_{MSC/VLR(S)}$ und der DPC dem $A_{LE(E)}$ bzw. $A_{MSC/VLR(E)}$.

Der Verbindungsabbau erfolgt anschließend, wie in *Abb 3.1.2.1* dargestellt.

In *Kapitel 3.1.3* wird beschrieben, welche Struktur die einzelnen Nachrichten haben und wie diese in DSS1 und CCS7 implementiert werden können.

3.1.3 Umsetzung der anonymen Signalisierung in DSS1 und CCS7

In diesem Kapitel werden die einzelnen Signalisierungsnachrichten und deren Modifikationen detailliert beschrieben. Außerdem werden die notwendigen Änderungen an den Datenstrukturen von DSS1 und CCS7 angegeben. Ausgangspunkt der Modifikationen sind die Angaben über die Signalisierungssysteme in den *Kapiteln 2.2.2* und *2.2.3*.

Die Protokolle werden entsprechend der Verwendungsreihenfolge betrachtet. So nutzt der Sender zuerst das DSS1-Protokoll zur Signalisierung von seinem Netzabschluß (NT) zur Teilnehmerseite seiner Ortsvermittlungsstelle, dort werden die Signalisierungsnachrichten in das MIX-Protokoll konvertiert und über die MIXe bis zur Netzseite der Ortsvermittlungsstelle übertragen. An dieser Stelle erfolgt anschließend die Konvertierung in das CCS7-Protokoll zur Übertragung im Fernnetz bis zur Netzseite der Zielortsvermittlungsstelle, wo die Nachrichten wieder ins MIX-Protokoll und danach ins DSS1-Protokoll konvertiert werden.

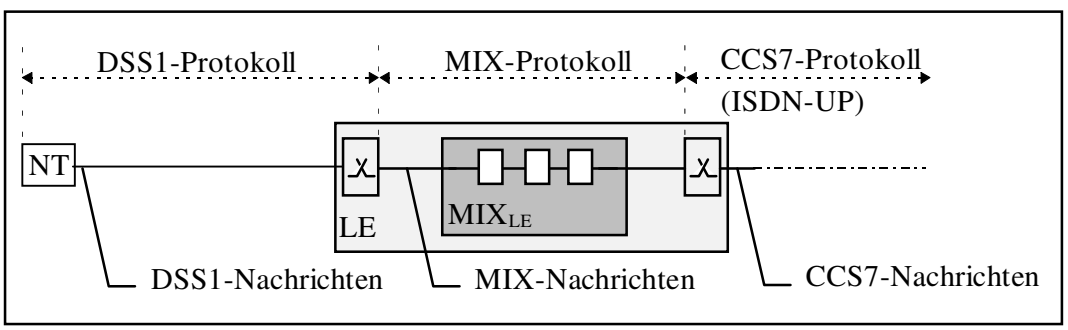


Abb. 3.1.3.1: Beschreibungspunkte der Nachrichteninhalte im ISDN

Abb. 3.1.3.1 zeigt die Lage der verwendeten Kommunikationsprotokolle. Außerdem wurden die Stellen besonders gekennzeichnet, an denen die Inhalte der jeweiligen Signalisierungsnachrichten in den folgenden Abschnitten detailliert beschrieben werden.

3.1.3.1 Signalisierungsnachrichten im DSS1-Protokoll

Signalisierungsnachrichten werden im folgenden im Index als Nachrichten des Senders bezeichnet, wenn sie im D-Kanal zwischen dem Sender und dessen Ortsvermittlungsstelle übertragen werden. Die Übertragungsrichtung wird bei der Erklärung nicht gesondert hervorgehoben, diese ist in *Abb. 3.1.2.1* dargestellt. Weiterhin werden hier nur die durch die Verwendung von unbeobachtbaren Zeitscheiben-Kanälen neu hinzukommenden I.E.´s angegeben. Die bestehenden und zu entfernenden I.E.´s werden bei der Änderung der Datenstrukturen des DSS1-Protokolls berücksichtigt.

Die **Setup**-Nachrichten: Diese Nachricht wird auf Senderseite aufgeteilt in eine ZE- und eine ZS-Setup-Nachricht, da die Empfangs- und Sendekanäle separat aufgebaut werden müssen (siehe *Abschnitt 2.4.3*). Die ZE-Setup-Nachricht endet in der Netzseite der Ortsvermittlungsstelle, während mit der ZS-Setup-Nachricht der Verbindungswunsch im Netz weitergeleitet wird. Auf Empfängerseite wird eine Anonymous Setup-Nachricht definiert, die an alle Teilnehmer der Ortsvermittlungsstelle

zu verteilen ist. Anschließend erfolgt auch beim Empfänger der getrennte Aufbau des unbeobachtbaren Empfangs- und des unbeobachtbaren Sendekanals.
Die Setup-Nachrichten enthalten folgende Informationen:

- **ZE-Setup**-Nachricht des Senders:
  $\mathbf{N_{ZE\text{-}Setup(S)}}$ $:= k_{S1}(D_{SE1}\ ,\ c_{S2}(D_{SE2}\ ,\ c_{S3}(D_{SE3}\ )\ )\ )$
  mit $\mathbf{D_{SE1}}$[16] $:= t_i$
  $\mathbf{D_{SE2}}$ $:= t_i,\ k_{SE2}$
  $\mathbf{D_{SE3}}$ $:= t_i,\ k_{SE3},\ KKZ_S(i)$[17]
  $|\mathbf{N_{ZE\text{-}Setup(S)}}| =$ 1954 Bit[18]
- **ZS-Setup**-Nachricht des Senders:
  $\mathbf{N_{ZS\text{-}Setup(S)}}$ $:= k_{S1}(D_{SS1}\ ,\ c_{S2}(D_{SS2}\ ,\ c_{S3}(D_{SS3}\ ,\ N_E\ )))$
  mit $\mathbf{D_{SS1}}$ $:= t_i$
  $\mathbf{D_{SS2}}$ $:= t_i,\ k_{SS2}$
  $\mathbf{D_{SS3}}$ $:= t_i,\ k_{SS3},\ A_{LE_E}\ ,\ KKZ_E(i)\ ,\ Bv/Bl$
  $\mathbf{N_E}$ $:= c_E\ (\ call_setup_msg\ ,\ t_i\ ,\ A_{LE_S}\ ,\ KZ_{init}\ )$
  $|\mathbf{N_{ZS\text{-}Setup(S)}}| =$ 2155 Bit
- **Anonymous Setup**-Nachricht zur Verteilung auf Empfängerseite:
  $\mathbf{N_{Anonymous\ Setup}}$ $:= c_E\ (call_setup_msg\ ,t_i\ ,A_{LE_S}\ ,KZ_{init}\ )$
  $|\mathbf{N_{Anonymous\ Setup}}| =$ 660 Bit (+ 12 Bit)
  Zusätzlich erhält der Empfänger mit dieser Nachricht den Kanalidentifikator CIC (Circuit Identification Code, 12 Bit) der Fernnetzverbindung. Diese Nachricht ist von der Ortsvermittlungsstelle, **ohne MIXe zu durchlaufen**, an alle angeschlossenen Teilnehmer zu **verteilen**.
- **ZE-Setup**-Nachricht des Empfängers:
  $\mathbf{N_{ZE\text{-}Setup(E)}}$ $:= k_{E1}(D_{EE1}\ ,\ c_{E2}(D_{EE2}\ ,\ c_{E3}(D_{EE3}\ )\ )\ )$
  mit $\mathbf{D_{EE1}}$ $:= t_i$
  $\mathbf{D_{EE2}}$ $:= t_i,\ k_{EE2}$
  $\mathbf{D_{EE3}}$ $:= t_i,\ k_{EE3},\ KKZ_E(i)$
  $|\mathbf{N_{ZE\text{-}Setup(E)}}| =$ 1954 Bit
- **ZS-Setup**-Nachricht des Empfängers:
  $\mathbf{N_{ZS\text{-}Setup(E)}}$ $:= k_{E1}(D_{ES1}\ ,\ c_{E2}(D_{ES2}\ ,\ c_{E3}(D_{ES3}\ )\ )\ )$
  mit $\mathbf{D_{ES1}}$ $:= t_i$
  $\mathbf{D_{ES2}}$ $:= t_i,\ k_{ES2}$
  $\mathbf{D_{ES3}}$ $:= t_i,\ k_{ES3},\ KKZ_S(i)$
  $|\mathbf{N_{ZS\text{-}Setup(E)}}| =$ 1954 Bit[19]

Sobald der Empfänger seinen unbeobachtbaren Sendekanal aufgebaut hat, ist die Kommunikation über die B-Kanäle möglich und wird nachfolgend bereits zur Signalisierung genutzt. Damit fallen aber auch bereits Gesprächskosten für die Teil-

[16] D_{SE1} bedeutet: Daten des Senders S für den im Empfangskanal genutzen MIX_1.
[17] Im ISDN und GSM gilt generell: Die Teilnehmerseite eines LE kennt alle Informationen des ersten MIXes und die Netzseite alle Informationen des letzten MIXes. In GSM entspricht das MSC/VLR dem LE.
[18] Alle Nachrichtenlängen werden in *Abschnitt 4.1.1* berechnet. In Gleichungen und Abbildungen wird vereinfachend von der Verwendung von 3 MIXen ausgegangen, die Nachrichtenlänge wird für die Nutzung von 10 MIXen berechnet. Die Nachrichtenlängen werden in diesem Kapitel ausschließlich zur Veranschaulichung des Mehraufwands angegeben.
[19] Wird dem letzten MIX keine Zieladresse und kein bv/bl mitgeteilt, soll es sich um Dummy Traffic im Ortsbereich handeln. Da diese Nachricht aber ohnehin auf 2155 Bit aufgefüllt werden muß können diese Parameter auch generell angegeben werden, da dadurch kein Performanceverlust entsteht.

nehmer an. Bei der Realisiserung sollte diese ZS-Setup-Nachricht mit Informationen bis auf die Größe der ZS-Setup-Nachricht des Senders aufgefüllt werden, da für jedes Nachrichtenformat (unterschiedliche Größe u.ä.) separater Dummy Traffic durchgeführt werden müßte.

Die **Alerting**-Nachricht: Diese Nachricht wird aus Effizienzgründen bereits im Datenkanal übertragen. Der Sender erhält mit dieser Nachricht das Freizeichen und beim Empfänger klingelt das Telefon. Außerdem erhält nun auch der Sender den Kanalidentifikator CIC der Fernnetzverbindung. Zur Bearbeitung dieser Nachrichten ist es notwendig, daß die Ortsvermittlungsstellen auf dem Datenkanal mitlesen. Falls die Kommunikation auf dem Datenkanal nicht zur Signalisierung gedacht ist, wird sie mit dem ausgehandelten Sitzungsschlüssel k_{SE} verschlüsselt, so daß eine Ortsvermittlungsstelle nur Signalisierungsinformationen auf dem B-Kanal lesen kann. Eine Adressierung der Daten im B-Kanal ist nicht erforderlich, da der B-Kanal unter dem OPC,DPC,CIC zwischen den Ortsvermittlungsstellen geschaltet ist.
Die Alerting-Nachrichten enthalten folgende Informationen:

- **Alerting**-Nachricht des Empfängers:
  $\mathbf{N_{Alerting(E)}} := k_{E1}(t_i , k_{ES2}(t_i , k_{ES3}(\text{alerting_msg} , t_i , A_{LE_S} , \text{CIC})))$
  $|\mathbf{N_{Alerting(E)}}| = \underline{334 \text{ Bit}}$
- **Alerting**-Nachricht des Senders:
  $\mathbf{N_{Alerting(S)}} := k_{S1} (t_i , k_{SE2} (t_i , k_{SE3} (\text{alerting_msg} , t_i , \text{CIC})))$
  $|\mathbf{N_{Alerting(S)}}| = \underline{320 \text{ Bit}}$

Falls es zu keiner Kommunikation kommt, weil der Empfänger nicht abhebt, wird die Verbindung abgebaut, sobald S auflegt bzw. eine Wartezeitschranke überschritten ist.

Die **Connect**-Nachricht: Auch diese Nachricht wird, zur Einsparung von D-Kanal-Signalisierungsaufwand, im Datenkanal übertragen. Sie wird gesendet, wenn der Empfänger den Hörer abgehoben hat und die Kommunikation beginnen kann.
Die Connect-Nachrichten enthalten folgende Informationen:

- **Connect**-Nachricht des Empfängers:
  $\mathbf{N_{Connect(E)}} := k_{E1} (t_i , k_{ES2} (t_i , k_{ES3} (\text{connect_msg} , t_i , A_{LE_S} , \text{CIC})))$
  $|\mathbf{N_{Connect(E)}}| = \underline{334 \text{ Bit}}$
- **Connect**-Nachricht des Senders:
  $\mathbf{N_{Connect(S)}} := k_{S1} (t_i , k_{SE2} (t_i , k_{SE3} (\text{connect_msg} , t_i)))$
  $|\mathbf{N_{Connect(S)}}| = \underline{308 \text{ Bit}}$

Die **Connect Acknowledge**-Nachricht kann entfallen, da die Verbindungen bereits mit den ZS-Setup-Nachrichten geschaltet werden und so keine Quittung auf die Connect-Nachricht gesendet werden muß. Falls der Sender den Verbindungswunsch beendet, bevor der Empfänger den Hörer abgehoben hat, so sendet der Sender im bereits existierenden B-Kanal die Disconnect-Nachricht, so daß das Telefon des Empfängers aufhört, zu klingeln.

Die **Disconnect**-Nachricht: Diese Nachricht wird ebenfalls über den B-Kanal übertragen und signalisiert die Beendigung der Kommunikation durch einen der Teilnehmer.
Die Disconnect-Nachrichten enthalten folgende Informationen:

- **Disconnect**-Nachricht des auflegenden Teilnehmers (z.B.: E):
  $\mathbf{N_{Disconnect(E)}} := k_{E1}(t_i , k_{ES2}(t_i , k_{ES3}(\text{disconnect_msg} , t_i , A_{LE_S} , \text{CIC})))$
  $|\mathbf{N_{Disconnect(E)}}| = \underline{334 \text{ Bit}}$

- **Disconnect**-Nachricht des anderen Teilnehmers, hier des Senders:
  $\mathbf{N_{Disconnect(S)}} := k_{S1} (t_i , k_{SE2} (t_i , k_{SE3} (\text{disconnect_msg} , t_i)))$
  $|\mathbf{N_{Disconnect(S)}}| = \underline{308 \text{ Bit}}$

Die **Release**- und die **Release Complete** Nachricht sind nicht mehr nötig, da alle bestehenden Verbindungen am Ende jeder Zeitscheibe (Systemtakt) automatisch abgebaut werden.

3.1.3.2 Änderungen der Datenstrukturen im DSS1-Protokoll

Ausgangspunkt der Modifikationen ist die *Abb. 2.2.3.1*. Dort wird der Nachrichtenaufbau einer DSS1-Signalisierungsnachricht auf Schicht 3 angegeben. Für neu hinzugekommene Nachrichten sind neue Nachrichtentypen (Message Type: MT) zu definieren und neue Informationselemente (I.E.) festzulegen. Zuerst sollen die Codierungen der Nachrichtentypen (siehe [BGGH_95] *Abb. 5.19*) und der I.E.´s (siehe [BGGH_95] *Abb. 5.20*) überarbeitet werden. Die modifizierten Codierungen sind in *Abb 3.1.3.2.1* und *Abb. 3.1.3.2.2* dargestellt.

Abb. 3.1.3.2.1 zeigt die überarbeitete Codierung der DSS1-Nachrichtentypen. Auf Quittungen, wie Call Proceeding, Connect Acknowledge und Setup Acknowledge kann verzichtet werden, da sie zur Funktion der Zeitscheibenkanäle nicht benötigt werden. Die Release und Release Complete Nachrichten sind ebenfalls entfallen, da B-Kanäle am Ende jeder Zeitscheibe automatisch abgebaut werden. Die Information-Nachricht wird nicht mehr benötigt, da alle Verbindungsinformationen bereits in den Setup-Nachrichten enthalten sein müssen. Die Nachrichten Progress und Notify sind ebenfalls nicht zwingend nötig und werden weggelassen. Ziel dieser Maßnahmen ist die Einsparung von Signalisierungsaufkommen auf dem D-Kanal, da für jede zusätzliche Nachricht im D-Kanal Dummy Traffic notwendig ist, um die gewinnbringende Beobachtung des physischen Sendens und Empfangens zu verhindern. Die Codierung bestehender Nachrichtentypen und I.E.´s wurde beibehalten und für hinzugekommene eine unbelegte bzw. frei gewordene Codierung gewählt.

Nachrichtentyp	Codierung
• <u>Nachrichten für den Verbindungsaufbau:</u>	000x xxxx
ZE-Setup	0 0101
ZS-Setup	0 1101
Anonymous Setup	0 0010
Alerting	0 0001
Connect	0 0111
• <u>Nachrichten für den Verbindungsabbau:</u>	010x xxxx
Disconnect	0 0101
• <u>Sonstige Nachrichten des Basisablaufes:</u>	011x xxxx
nicht benötigt bzw.	001x xxxx

Abb. 3.1.3.2.1: Modifizierte Codierung der DSS1-Nachrichtentypen des Basisablaufes

Abb. 3.1.3.2.2 zeigt die modifizierte Codierung der Informationselemente der verschiedenen Nachrichtentypen. Bei einigen I.E.´s ist statt der Codierung „B-Kanal“ vermerkt, d.h. diese I.E.´s gehören zu Signalisierungsnachrichten, die jetzt in den B-Kanal verlagert

wurden, wobei die I.E.´s weiterhin benötigt werden und diese deshalb in der Abbildung nicht fehlen sollten. Die I.E.´s Notification indicator, Display, Date/Time und Sending complete wurden entfernt, da sie nicht benötigt werden bzw. auch im heutigen ISDN der Deutschen Telekom nicht verwendet werden. Die I.E.´s Calling party number, Calling party subaddress, called party number und called party subaddress wurden dagegen entfernt, um die erreichte Unbeobachtbarkeit nicht aufzuheben.

Informationselement	Abkürzung	Codierung
Alerting-Information	AI	B-Kanal
Bearer capabilitiy	BC	0000 0100
Cause	CAU	B-Kanal
Channel identification	CHI	0001 1000
Connected-Information	CI	B-Kanal
Empfänger-Information	EI	0110 1100
High layer compatibility	HLC	0111 1101
Low layer compatibility	LLC	0111 1100
Progress indicator	PI	B-Kanal
Zeitscheiben-Empfangs-Information	ZEI	0110 1101
Zeitscheiben-Sende-Information	ZSI	0111 0000
Shift	SFT	1001 xxxx

Abb. 3.1.3.2.2: Modifizierte Codierung der DSS1-Informationselemente

Hinzugekommen ist das I.E. Zeitscheiben-Empfangs-Information. Dies enthält die Daten zum Aufbau von ZE-Kanälen. Analog beinhaltet das I.E. Zeitscheiben-Sende-Information die Daten zum Aufbau von ZS-Kanälen. Das I.E. Empfänger-Information enthält die an alle Teilnehmer zu verteilende Nachricht einer ankommenden Verbindung. Bei den I.E.´s Alerting Information bzw. Connected Information handelt es sich um die mit Alerting- bzw. Connect- und Disconnect-Nachrichten zu übertragenden MIX-Informationen. Bezüglich der zu beachtenden Codierungsregeln sei auf [BGGH_95] und [ETS_300_403-1] verwiesen.

Abb. 3.1.3.2.3[20] zeigt die Nachrichtenstruktur der ZE-Setup-Nachricht im DSS1. Die ersten 4 Byte (Oktetts) sind in allen DSS1-Nachrichten bedeutungsgleich. Die Bedeutung dieser 4 Oktetts ist in *Abschnitt 2.2.3* erklärt und ändert sich durch die Zeitscheiben-Kanäle nicht. Anschließend folgen die Informationselemente des jeweiligen Nachrichtentyps. Die in den jeweiligen DSS1-Nachrichten enthaltenen I.E.´s sind in [BGGH_95] in *Abb. 5.5* aufgeführt und erklärt. Bezüglich der zu beachtenden Codierungsregeln sei auch hier auf [BGGH_95] und [ETS_300_102-1] verwiesen. Aus *Abb. 3.1.3.2.3* ist die Nachrichtenstruktur aller anderen DSS1-Nachrichten des Signalisierungskanals ableitbar, da sich jeweils nur das letzte I.E. ändert, so daß hier auf weitere Darstellungen verzichtet werden soll. Die Signalisierungsnachrichten Alerting, Connect und Disconnect werden im Datenkanal übertragen. Deren Aufbau ist aufgrund der größeren Bandbreite des Datenkanals nicht kritisch. I.E.´s, die die Unbeobachtbarkeit des Teilnehmers gefährden

[20] Die folgenden Darstellungen des Aufbaus und Inhalts von Signalisierungsnachrichten wurden vereinfacht. Sie enthalten nur noch die Namen und Bedeutung der Parameter und deren Länge. Die Angabe der exakten Codierung, wie in *Abb. 3.1.3.2.3* ergibt keine weiteren Erkenntnisse über das Verfahren zur anonymen Signalisierung oder dessen Performance.

bzw. aufheben, müssen jedoch auch in diesen Signalisierungsnachrichten entfernt werden. Die detaillierte Codierung der I.E.´s ist in [ETS_300_102-1] angegeben.

Ein bisher nicht diskutiertes Problem ist die Länge der DSS1-Signalisierungsnachrichten. Die in *Abb. 3.1.3.2.3* dargestellte ZE-Setup-Nachricht ist 264 Byte lang. Nach [BGGH_95] wird die Länge einer Schicht-3-Nachricht im DSS1 begrenzt durch die in der Schicht 2 maximal nutzbare Rahmenlänge von 260 Byte. Falls längere Schicht-3-Nachrichten auftreten, müssen diese von der Schicht 3 in einzelne Nachrichtensegmente mit maximal 260 Byte aufgeteilt werden. [ETS_300_403-1] schreibt im Annex K vor, wie sich Sender und Empfänger einer segmentierten Nachricht zu verhalten haben, dies wird jedoch von den europäischen, öffentlichen Netzen zur Zeit nicht unterstützt. Die Lösung des Problems bietet entweder die Implementierung der Segmentierung auf Schicht 3 oder eine Optimierung der Länge der Signalisierungsnachrichten. So würde eine Reduzierung der verwendeten MIXe von 10 auf 8 bereits eine zufriedenstellende Lösungsalternative bieten, da sich dadurch die Länge einer ZE-Setup-Nachricht auf 224 Byte verringert und die längste Nachricht (ZS-Setup) 250 Byte benötigt (statt 290 Byte).

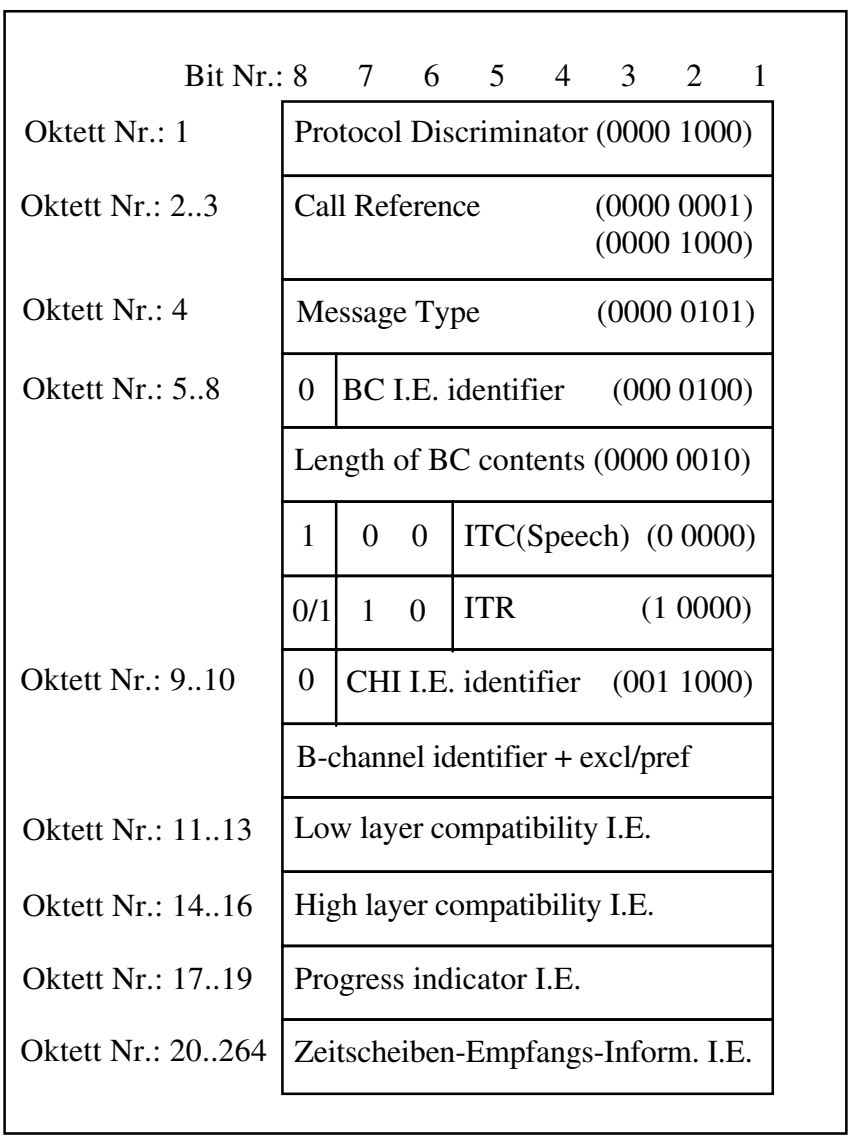


Abb. 3.1.3.2.3: Aufbau und Inhalt der ZE-Setup-Nachricht

3.1.3.3 Signalisierungsnachrichten im MIX-Protokoll

Die an der Teilnehmerseite einer Ortsvermittlungsstelle eintreffenden Signalisierungsnachrichten werden dort bearbeitet und anschließend in das MIX-Protokoll konvertiert und an die MIX-Kaskade der Ortsvermittlungsstelle weitergeleitet. Ein MIX-Protokoll existiert zur Zeit im ISDN nicht, so daß ein größerer Definitionsspielraum besteht. Der Signalisierungskanal sollte Informationen ebenfalls mit min. 16 kbps pro Teilnehmeranschluß übertragen können. Desweiteren sollen die Namen der Nachrichtentypen ZE-Setup und ZS-Setup im MIX-Protokoll nicht geändert werden. *Abb. 3.1.2.1* kann entnommen werden, daß keine weiteren Signalisierungsnachrichten in der MIX-Kaskade notwendig sind, da anschließend bereits der B-Kanal benutzt wird. Wie in *Kapitel 2.4* festgestellt, ist es sinnvoll für jeden Nachrichtentyp (unterschiedlicher Länge und Bedeutung) eine separate MIX-Kaskade zu implementieren. Im ISDN werden somit 4 MIX-Kaskadentypen benötigt, eine für ZE-Setup-Nachrichten, eine zweite für ZS-Setup-Nachrichten, eine dritte für die an der Ortsvermittlungsstelle ankommende- und eine vierte für die abgehende Datenkommunikation[21] .

Im folgenden werden die Datenstrukturen der Signalisierungsnachrichten angegeben, die die MIXe im Signalisierungskanal passieren.

- **ZE-Setup**-Nachricht des Senders:
  $\mathbf{N_{ZE\text{-}Setup(S)}} := k_{S1}(D_{SE1} , c_{S2}(D_{SE2} , c_{S3}(D_{SE3})))$ mit
  $\mathbf{D_{SE1}} := t_i$ $\mathbf{D_{SE2}} := t_i, k_{SE2}$ $\mathbf{D_{SE3}} := t_i, k_{SE3}, KKZ_S(i)$
  $|\mathbf{N_{ZE\text{-}Setup(S)}}| = \underline{1954 \text{ Bit}}$
- **ZS-Setup**-Nachricht des Senders:
  $\mathbf{N_{ZS\text{-}Setup(S)}} := k_{S1}(D_{SS1} , c_{S2}(D_{SS2} , c_{S3}(D_{SS3} , N_E)))$ mit
  $\mathbf{D_{SS1}} := t_i$ $\mathbf{D_{SS2}} := t_i, k_{SS2}$
  $\mathbf{D_{SS3}} := t_i, k_{SS3}, A_{LE_E} , KKZ_E(i)$, Bv/Bl
  $\mathbf{N_E} := c_B$ (call_setup_msg , t_i , A_{LE_S} , KZ_{init})
  $|\mathbf{N_{ZS\text{-}Setup(S)}}| = \underline{2155 \text{ Bit}}$
- **ZE-Setup**-Nachricht des Empfängers:
  $\mathbf{N_{ZE\text{-}Setup(E)}} := k_{E1}(D_{EE1} , c_{E2}(D_{EE2} , c_{E3}(D_{EE3})))$ mit
  $\mathbf{D_{EE1}} := t_i$ $\mathbf{D_{EE2}} := t_i, k_{EE2}$ $\mathbf{D_{EE3}} := t_i, k_{EE3}, KKZ_E(i)$
  $|\mathbf{N_{ZE\text{-}Setup(E)}}| = \underline{1954 \text{ Bit}}$
- **ZS-Setup**-Nachricht des Empfängers:
  $\mathbf{N_{ZS\text{-}Setup(E)}} := k_{E1}(D_{ES1} , c_{E2}(D_{ES2} , c_{E3}(D_{ES3})))$ mit
  $\mathbf{D_{ES1}} := t_i$ $\mathbf{D_{ES2}} := t_i, k_{ES2}$ $\mathbf{D_{ES3}} := t_i, k_{ES3}, KKZ_S(i)$
  $|\mathbf{N_{ZS\text{-}Setup(E)}}| = \underline{1954 \text{ Bit}}$[22]

Eine Codierung der Nachrichtentypen (MT) ist im MIX-Protokoll nicht erforderlich, da die im DSS1-Protokoll korrekt gekennzeichneten Nachrichtentypen zur Weiterleitung ausreichend sind. So werden die Nachrichten von der Teilnehmerseite der Ortsvermittlungsstelle (bei Daten auch von der Netzseite) auf dem Eingabekanal der entsprechenden, dem Nachrichtentyp zugeordneten, MIX-Kaskade gesendet. Auf der Netzseite der Ortsvermittlungsstelle kann anhand der verwendeten MIX-Kaskade erkannt werden, um welchen Nachrichtentyp es sich handelt. Durch diese Maßnahme erhöht sich die obenste-

[21] Dabei arbeiten jeweils 2 MIX-Kaskaden mit den gleichen Schlüsseln. Das sind die MIX-Kaskade der ZS-Setup-Nachrichten mit der MIX-Kaskade der abgehenden Datenkommunikation und die der ZE-Setup-Nachrichten mit der der ankommenden Nachrichten (siehe *Abschnitt 2.4.3*).

[22] Diese Nachricht wird bis auf 2155 Bit (Länge der ZS-Setup-Nachricht des Senders) aufgefüllt.

hende Nachrichtenlänge nicht. Die max. Rahmenlänge kann im MIX-Protokoll neu definiert werden. Sie sollte min. 270 Byte betragen, damit keine Nachrichtensegmentierung nötig ist. Auf die Codierung und Umcodierung der Nachrichten soll an dieser Stelle nicht eingegangen werden. Bezüglich eines Umcodierungsschemas für Senderanonymität bei Signalisierungsnachrichten im D-Kanal sei auf *Kapitel 2.5.2.2* in [Pfit_89] verwiesen. Eine längentreue Umcodierung ist nicht zwingend erforderlich, da alle Nachrichten die gleichen MIXe in der gleichen Reihenfolge durchlaufen. Für die Datenkommunikation wird ein Senderanonymitätsschema in der MIX-Kaskade auf Senderseite und ein Empfängeranonymitätsschema in der MIX-Kaskade auf Empfängerseite benötigt. Die Realisierung der Datenkommunikation ist nicht Bestandteil dieser Arbeit, deshalb sollen diese Angaben nicht vertieft werden.

Für die Realisierung und den Betrieb der MIX-Kaskaden gelten weiterhin die in *Kapitel 2.4* getroffenen Annahmen, so daß davon ausgegangen werden kann, daß die Teilnehmer- und die Netzseite einer Ortsvermittlungsstelle keine Nachrichten über die MIX-Kaskade verketten können. In der Netzseite der Ortsvermittlungsstelle werden die Signalisierungsnachrichten in das CCS7-Protokoll konvertiert, welches im folgenden Abschnitt beschrieben wird.

3.1.3.4 Signalisierungsnachrichten im CCS7-Protokoll

Das CCS7-Protokoll kommt zwischen den Netzseiten der Ortsvermittlungsstellen der beiden an der Kommunikation beteiligten Teilnehmer zum Einsatz. Das CCS7-Signalisiernetz routet Verbindungswünsche in den gewünschten Teilnehmeranschlußbereich. Diese Funktionalität wird durch den Einsatz von unbeobachtbaren Zeitscheibenkanälen nicht verändert. Zu modifizieren ist ausschließlich die Struktur der CCS7-Signalisierungsnachrichten im ISDN-UP[23] , nicht die Wegewahl, Lastbalancierung oder Netzmanagement. Die Grundlagen des CCS7 sind in *Kapitel 2.2.2* beschrieben und in *Abb. 3.1.2.1* sind u.a. die zu modifizierenden CCS7-Nachrichten dargestellt. Ein weiterer Vorteil für die Realisierung im CCS7-Netz ist, daß MIXe aus Effizienzgründen nur in den Ortsvermittlungsstellen eingesetzt werden, CCS7-Nachrichten also bis auf den veränderten Informationsinhalt im CCS7-Netz auf dem Weg zur Ortsvermittlungsstelle des Empfängers „normal“ behandelt werden können. Im folgenden werden nur die durch die Verwendung von unbeobachtbaren Zeitscheiben-Kanälen neu hinzukommenden I.E.´s angegeben. Beibehaltene und zu entfernende Parameter werden bei der Änderung der Datenstrukturen berücksichtigt.

Die **IAM**-Nachricht: Diese Nachricht wird durch die DDS1-ZS-Setup-Nachricht ausgelöst und signalisiert den Verbindungswunsch des Senders der Ortsvermittlungsstelle des Empfängers. In der Verbindungswunschnachricht ist lediglich die Ortsvermittlungsstelle des Empfängers adressiert, ein Empfänger kann erst erkennen, daß ein Verbindungswunsch für ihn ist, wenn er die N_E-Nachricht der DSS1-Anonymous-Setup-Nachricht korrekt entschlüsseln konnte.

- **IAM**-Nachricht:
  $\mathbf{N_{IAM}} := \mathbf{N_E} = c_B (\text{call_setup_msg} , t_i , A_{LE_S} , KZ_{init}) , A_{LE_E}$
  $|\mathbf{N_{IAM}}| = \underline{674 \text{ Bit}}$

[23] Alle Modifikationen im CCS7-Netz sind ausschließlich in dem Anwenderteil ISDN-User-Part nötig, der MTP liefert unverändert das Transportsystem der Signalisierungsnachrichten. Darin besteht ein großer Vorteil des CCS7-Signalisierungsnetzes.

Die **ACM**-Nachricht: Diese Nachricht wird aus Effizienzgründen bereits im Datenkanal übertragen. Ausgelöst wird diese Nachricht durch die DSS1-Alerting-Nachricht auf dem Datenkanal. Sie überträgt also die Information, daß der Verbindungswunsch durchgeschaltet wurde und das Telefon des Empfängers klingelt. Die Empfänger-Ortsvermittlungsstelle hat mit der Alerting-Nachricht den CIC des Datenkanals erhalten und weiß damit, welcher Fernnetzdatenkanal zu nutzen ist. Außerdem sendet sie mit den Daten die für den ZE-Kanal des Senders gespeicherte Zielinformation (Adresse der Ortsvermittlungsstelle des Senders und Kanalkennzeichen des Empfangskanals des Senders)

- **ACM**-Nachricht:
  $\mathbf{N_{ACM}}$:= acm_msg , t_i , A_{LE_S} , $KKZ_S(i)$, A_{LE_E} , CIC
  $|\mathbf{N_{ACM}}|$ = 106 Bit

Die **ANM**-Nachricht: Auch diese Nachricht wird aus Effizienzgründen im B-Kanal übertragen. Ausgelöst wird diese Nachricht durch die DSS1-Connect-Nachricht. Die ANM-Nachricht signalisiert, daß der Empfänger den Hörer abgenommen hat und die Kommunikation beginnen kann.

- **ANM**-Nachricht:
  $\mathbf{N_{ANM}}$:= anm_msg , t_i , A_{LE_S} , $KKZ_S(i)$, A_{LE_E} , CIC
  $|\mathbf{N_{ANM}}|$ = 106 Bit

Die **REL**-Nachricht: Auch diese Nachricht wird aus Effizienzgründen im B-Kanal übertragen. Ausgelöst wird diese Nachricht durch die DSS1-Disconnect-Nachricht. Die REL-Nachricht signalisiert, daß der Kommunikationspartner den Hörer aufgelegt hat und die Kommunikation beendet wird. Dadurch weiß zum einen der Teilnehmer, daß er seinen Hörer auch auflegen kann, zum anderen erfahren die Vermittlungsstellen, daß der Datenkanal im Fernnetz abgebaut werden soll.

- **REL**-Nachricht:
  $\mathbf{N_{REL}}$:= rel_msg , t_i , A_{LE_S} , $KKZ_S(i)$, A_{LE_E} , CIC
  $|\mathbf{N_{REL}}|$ = 106 Bit

Die **RLC**-Nachricht: Diese Nachricht teilt der Vermittlungsstelle, welche die REL-Nachricht gesendet hat, mit, daß der B-Kanal abgebaut wurde. Diese Nachricht wird durch das vorgestellte Verfahren nicht geändert.

3.1.3.5 Änderungen der Datenstrukturen im CCS7-Protokoll

Ausgangspunkt der Modifikationen ist hier der ISDN-User Part (ISDN-UP), dessen Nachrichtenaufbau in *Abb. 2.2.2.2* dargestellt wird. Der prinzipielle Nachrichtenaufbau bleibt bestehen, ebenso wie die Nachrichten des ISDN-UP und deren Codierung, da durch die Realisierung der unbeobachtbaren Zeitscheiben-Kanäle keine neuen CCS7-Nachrichten benötigt werden. *Abb. 3.1.3.5.1* zeigt die Codierung der CCS7-Nachrichtentypen (nach [ITU_Q.763], *Tabelle 4*).

Nachrichtentyp	Codierung
• Nachrichten für den Verbindungsaufbau:	
IAM	0000 0001
ACM	0000 0110
ANM	0000 1001
• Nachrichten für den Verbindungsabbau:	
REL	0000 1100
RLC	0001 0000

Abb. 3.1.3.5.1: Codierung der CCS7-Nachrichtentypen (ISDN-UP)

Abb. 3.1.3.5.2 zeigt die Codierung der CCS7-Informationselemente der verwendeten Nachrichten, wobei die Codierung bestehender I.E.´s aus [ITU_Q.763] (*Tabelle 5*) übernommen wurde und hinzugekommenen I.E.´s „freie" Codierungen zugewiesen wurden.

Informationselement	Abkürzung	Codierung
Access Transport	AT	0000 0011
Automatic Congestion Level	ACL	B-Kanal
Backward Call Indicator	BCI	B-Kanal
Call History Information	CHINF	B-Kanal
Cause Indicators	CAU	B-Kanal
Connection Request	CR	0000 1101
Echo Control Information	ECI	B-Kanal
Forward Call Indicators	FCI	0000 0111
Generic Notification	GN	0010 1100
Kanalkennzeichen	KKZ	B-Kanal
Nature of Connection Indicators	NOI	0000 0110
Optional Backward Call Indicators	OBCI	B-Kanal
Originated ISC Point Code	OISCPC	0010 1011
Parameter Compatibility Info	PCI	0011 1001
Propagation Delay Counter	PDC	0011 0001
Systemtakt	ST	B-Kanal
Transmission Medium Requirement	TMR	0000 0010
Transmission Medium Requirement Prime	TMRP	0011 1110
Transmission Medium Used	TMU	B-Kanal
User Service Information	USI	0001 1101
User Service Information Prime	USIP	0011 0000
User Teleservice Info	UTI	0011 0100
User to User Indicator	UTUI	B-Kanal
User to User Information	UUI	0010 0000

Abb. 3.1.3.5.2: Modifizierte Codierung des CCS7-Informationselemente (ISDN-UP)

Ein wichtiger Unterschied in der Funktion der CCS7-Nachrichten besteht allerdings in der symmetrischen Durchschaltung des Nutzkanals. Bisher wurde mit Aussendung der IAM der Nutzkanal belegt und durchgeschaltet, und zwar bei allen Transitvermittlungsstellen (TE) in Sende- und Empfangsrichtung, bei der Ursprungsvermittlungsstelle zunächst jedoch nur in Empfangsrichtung (asymmetrische Durchschaltung), damit Ansagen für den Sender sofort hörbar sind, aber die Verbindung erst voll genutzt werden kann,

wenn auch Gebühren eingenommen werden. Die Senderichtung des Nutzkanals wurde somit erst mit Empfang der ANM-Nachricht geschaltet. Für die Umsetzung der anonymen Signalisierung wird eine sofortige symmetrische Durchschaltung des Nutzkanals mit der IAM benötigt, damit die ACM und ANM aus Effizienzgründen bereits im Datenkanal übertragen werden können.

Da der Signalisierungskanal im CCS7-Netz nicht so stark belastet ist, wie der DSS1-Signalisierungskanal (siehe *Kapitel 4.2*), wäre es möglich, die DSS1-Alerting- und die DSS1-Connect-Nachricht zwar im B-Kanal zu übertragen, die CCS7-ACM und -ANM dagegen weiterhin im Signalisierungskanal. Dann würden weiterhin Gebühren erst mit der Aufnahme der Kommunikation (im Fernnetz) anfallen, da Gespräche bzw. bestehende Datenkanäle im Ortsbereich bei Nutzung anonymer Signalisierung kostenlos sind, da im Ortsbereich völlig unbeobachtbar ist, ob eine sinnvolle oder bedeutungslose Kommunikation abläuft. Bei den Informationsparametern der Signalisierungsnachrichten kommt lediglich die Systemzeit t_i und das Kanalkennzeichen des ZE-Kanals hinzu.

Abb. 3.1.3.5.3 zeigt (in Anlehnung an [BGGH_95] *Abb. 6.58* und [ITU_Q.763] Tabelle 32) den Aufbau einer IAM. Der Parameter User-to-User Information wird benutzt, um die Verbindungswunschnachricht an den Empfänger zu übertragen. Er ist deshalb zum Pflichtparameter fester Länge (674 Bit) geworden. Entfernt wurden dagegen die Parameter Calling Party Category (8 Bit), Called Party Number (32-88 Bit), Calling Party Number (32-96 Bit), Redirecting Number (32-96 Bit), Redirection Information (24-32 Bit), Closed User Group Interlock Code (48 Bit), MLPP Precedence (8 Bit), Original Called Number (32-96 Bit), Generic Number (40-104 Bit) und Location Number (40-96 Bit), da sie die Unbeobachtbarkeit und Anonymität der Teilnehmer einschränken bzw. aufheben. Deshalb erhöht sich die Länge der Nachricht nur unwesentlich (ca. 200 Bit). Da im CCS7 außerdem Nachrichtensegmentierung implementiert ist, sollte dies kein Problem darstellen.

Die maximale Länge des Service Information Field (SIF), in dem die Parameter übertragen werden, beträgt 272 Byte. Sollte eine Nachrichtensegmentierung notwendig sein, so wird direkt nach der segmentierten Nachricht eine Segmentation-Nachricht (SGM) gesendet. Diese Segmentierung wird von dem ISDN-UP vorgenommen.

Parametername	**enthaltene Information**
Pflichtparameter fester Länge: - Nature of Connection Indicators (8 Bit) - Forward Call Indicators (16 Bit) - Transmission Medium Requirement (8 Bit) - User to User Information (674 Bit)	 Zahl der Satellitenabschnitte, Continuity Check erforderlich/durchgeführt?, abgehende Halbechosperre enthalten? Verfügbare Ende-zu-Ende-Methode, durchgehend ISDN-UP, welche Zeichengabe gefordert Geforderte Nutzkanaleigenschaften wie: Sprache, 3,1 kHz Audio, 64 kbps transparent oder höhere Bitraten Verbindungswunschnachricht N_E
Pflichtparameter variabler Länge:	keine
Optionale Parameter: - Connection Request (56-72 Bit) - Access Transport (>24 Bit) - User Service Information (32-104 Bit) - User to User Indicator (24 Bit) - Propagation Delay Counter (32 Bit) - User Service Information Prime (32-104 Bit) - Originated ISC Point Code (32 Bit) - User Teleservice Info (24 Bit) - Parameter Compatibility Info (>32 Bit) - Generic Notification (24 Bit) - Transmission Medium Requirement Prime (24 Bit)	 Anforderung einer Ende-zu-Ende-Verbindung mit Angabe der lokalen Referenz enthält Angaben des D-Kanal-Protokolls, werden im Netz transparent weitergegeben und nicht ausgewertet BC-Feld von D-Kanal User to User gefordert? welcher Service? Laufzeit des Nutzkanals Zusätzliches BC-Feld (für Rückfall) SPC der gehenden Auslandsvermittlungsstelle Kopie des BC-Feldes (für Leitwegelenkung) Behandlung unbekannter Parameter? Angaben für Dienstmerkmale wie HOLD ... Wie oben (Sprache ...) für eventl. Rückfall auf niederwertigen Dienst

Abb. 3.1.3.5.3: Aufbau der Initial Address Message

Abb. 3.1.3.5.4 zeigt (in Anlehnung an [BGGH_95] *Abb. 6.59* und [ITU_Q.763] Tabelle 21) den Aufbau einer ACM. Hinzugekommen sind die Parameter Systemtakt (30 Bit) und Kanalkennzeichen (28 Bit). Der Parameter User-to-User Information wird benutzt, um den Kanalidentifikator des Nutzkanals im Fernnetz an den Sender zu übertragen. Er ist deshalb zum Pflichtparameter fester Länge (12 Bit) geworden (statt 24-1048 Bit). Entfernt wurden dagegen die Access Delivery Information (24 Bit), Redirection Number (40-96 Bit), Call Diversion Information (24 Bit) und Redirection Number Restriction (24 Bit), da sie die Unbeobachtbarkeit und Anonymität der Teilnehmer einschränken bzw.

die Möglichkeit der Anrufweiterleitung trotz anonymer Signalisierung nicht untersucht wird. Diese Nachricht wird deshalb durch das Anonymitätsverfahren nicht länger.

Parametername	**enthaltene Information**
Pflichtparameter fester Länge: - Backward Call Indicator (16 Bit)	 gebührenpflichtig? Teilnehmer frei? Normalteilnehmer oder Münzer? Ende-zu-Ende-Verfahren verfügbar, welches? Durchgehend CCS7 oder Interworking? Durchgehend ISDN-UP, ISDN-Teilnehmer? Ankommende Halbechosperre enthalten?
- Systemtakt (30 Bit)	aktueller Takt t_i des Netzes
- Kanalkennzeichen (28 Bit)	Kanalkennzeichen des Empfangskanals an der Zielortsvermittlungsstelle
- User to User Information (12 Bit)	CIC_S wird dem Sender mitgeteilt
Pflichtparameter variabler Länge:	keine
Optionale Parameter: - Optional Backward Call Indicators (24 Bit)	 Nachricht segmentiert? Ton oder Ansage verfügbar?
- Cause Indicators (>32 Bit)	Grund, warum Verbindung nicht erfolgreich war, zusammen mit Ton oder Hinweisansage
- User to User Indicator (24 Bit)	*bereits erklärt*
- Access Transport (>24 Bit)	*bereits erklärt*
- Generic Notification (24 Bit)	*bereits erklärt*
- Transmission Medium Used (24 Bit)	tatsächlich verhandene Art des Nutzkanals
- Echo Control Information (24 Bit)	Angaben zur Echosperrensteuerung
- Parameter Compatibility Info (>32 Bit)	*bereits erklärt*

Abb. 3.1.3.5.4: Aufbau der Address Complete Message

Abb. 3.1.3.5.5 zeigt (in Anlehnung an [BGGH_95] *Abb. 6.60* und [ITU_Q.763] Tabelle 22) den Aufbau einer ANM. Hinzugekommen sind die Parameter Systemtakt (30 Bit) und Kanalkennzeichen (28 Bit). Entfernt wurden dagegen die Connected Number (32-96 Bit), Generic Number (32-96 Bit), User to User Information (32-1048 Bit), Access Delivery Information (24 Bit), Redirection Number (40-96 Bit), Call Diversion Information (24 Bit) und Redirection Number Restriction (24 Bit), da sie die Unbeobachtbarkeit und Anonymität der Teilnehmer einschränken bzw. aufheben. Diese Nachricht wird deshalb durch das Anonymitätsverfahren nicht länger.

Parametername	**enthaltene Information**
Pflichtparameter fester Länge: - Systemtakt (30 Bit) - Kanalkennzeichen (28 Bit)	 aktueller Takt t_i des Netzes Kanalkennzeichen des Empfangskanals an der Zielortsvermittlungsstelle
Pflichtparameter variabler Länge:	keine
Optionale Parameter: - Backward Call Indicator (32 Bit) - Optional Backward Call Indicators (24 Bit) - User to User Indicator (24 Bit) - Access Transport (>24 Bit) - Generic Notification (24 Bit) - Parameter Compatibility Info (>32 Bit) - Call History Information (32 Bit) - Transmission Medium Used (24 Bit) - Echo Control Information (24 Bit)	 *bereits erklärt* *bereits erklärt* *bereits erklärt* *bereits erklärt* *bereits erklärt* *bereits erklärt* liefert die Laufzeit einer Nutzkanalverbindung *bereits erklärt* *bereits erklärt*

Abb. 3.1.3.5.5: Aufbau der Answer Message

Abb. 3.1.3.5.6 zeigt (in Anlehnung an [BGGH_95] *Abb. 6.61* und [ITU_Q.763] Tabelle 33) den Aufbau einer REL. Hinzugekommen sind die I.E.´s Systemtakt (30 Bit) und Kanalkennzeichen (28 Bit). Entfernt wurden dagegen die User to User Information (24-1048 Bit), Redirection Number Restriction (24 Bit), User to User Indicator (24 Bit) und die Access Delivery Information (24 Bit).

Parametername	**enthaltene Information**
Pflichtparameter fester Länge: - Systemtakt (30 Bit) - Kanalkennzeichen (28 Bit)	 aktueller Takt t_i des Netzes Kanalkennzeichen des Empfangskanals an der Zielortsvermittlungsstelle
Pflichtparameter variabler Länge: - Cause Indicators (>24 Bit)	 Auslösegrund
Optionale Parameter: - Access Transport (>24 Bit) - Automatic Congestion Level (32 Bit) - Parameter Compatibility Info (>32 Bit)	 *bereits erklärt* Überlastschwellwerte *bereits erklärt*

Abb. 3.1.3.5.6: Aufbau der Release Message

Die RLC wird durch den Einsatz anonymer Signalisierung nicht verändert und soll deshalb nicht gesondert dargestellt werden(Aufbau siehe [ITU_Q.763] Tabelle 34). Sie enthält als einzigen Parameter den Cause Indicator mit dem Auslösegrund und ist Quittung der REL-Nachricht. Sie signalisiert, daß der belegte Nutzkanal für einen neuen Verbindungsaufbau belegbar ist.

Zusammenfassend kann bezüglich der Umsetzung der anonymen Signalisierung im DSS1-, MIX- und CCS7-Protokoll festgehalten werden, daß die Modifikationen am DSS1-Protokoll umfassender und einschneidender sind, als in CCS7. Der Grund liegt in den zu signalisierenden, asymmetrisch verschlüsselten Nachrichten zum Aufbau unbeobachtbarer ZE- und ZS-Kanäle. Dadurch erhöht sich der Signalisierungaufwand im D-Kanal beträchtlich. Deshalb wurde die Verlagerung von Signalisierungsnachrichten auf den B-Kanal notwendig, um die Performance des Verfahrens zu verbessern. Ein weiterer Flaschenhals ist die notwendige Verteilung der N_E-Nachricht im DSS1-Anonymous-Setup an alle Teilnehmer einer Ortsvermittlungsstelle. Das CCS7-Netz wird dagegen nur unwesentlich stärker belastet, da die Verbindungen zwischen zwei Ortsvermittlungsstellen nicht geschützt werden sollen. Jeder Teilnehmer bleibt trotz dieser im Netz verfügbaren Information innerhalb seiner Anonymitätsgruppe unbeobachtbar. Die Effizienz dieser Modifikationen wird anschließend im *Kapitel 4.2* untersucht und bewertet.

Zusatzfunktionen (Dienstmerkmale) des ISDN, wie Anklopfen, Anrufweiterleitung und Halten sollten ebenfalls mit anonymer Signalisierung realisierbar sein, dies wird im Rahmen dieser Arbeit jedoch nicht untersucht. Fraglich ist allerdings, ob sich alle existierenden Dienstmerkmale auf anonyme Signalisierung portieren lassen.

3.2 Anonyme Signalisierung am Beispiel des GSM-Mobilfunknetzes

3.2.1 Modifikation der Netzstruktur

Um Anonymität und Unbeobachtbarkeit der Teilnehmer bei der Signalisierung auch für ein Mobilkommunikationssystem, wie GSM, gewährleisten zu können, ist nicht nur der Verbindungswunsch und der Kanalauf- bzw. -abbau zu schützen, sondern auch der Aufenthaltsort eines Mobilteilnehmers. Ausgangspunkt der Modifikationen ist die Netzstruktur eines GSM-Netzes aus *Abb. 2.3.2.1.* Die *Abb. 3.2.1.1* zeigt die modifizierte **GSM-Netzstruktur**. Man erkennt, daß auch bei GSM die Ortsvermittlungsstellen (MSC) und deren Signalisierungspunkte um MIX-Funktionalität erweitert werden müssen. Die Anonymitätsgruppe eines Mobilteilnehmers besteht demzufolge aus allen Mobilteilnehmern, die sich zur Zeit in einem Location Area (LA) aufhalten, das von demselben MSC verwaltet wird. Die Anonymitätsgruppengröße ist aufgrund der Teilnehmerbewegungen dynamisch. Die MIXe im MSC schützen also den Aufenthaltsort des Teilnehmers innerhalb eines MSC-Bereiches, d.h. ein MSC sollte möglichst viele verschiedene LAs verwalten. Außerdem werden durch diese MIXe bestehende Kommunikationsbeziehungen geschützt.

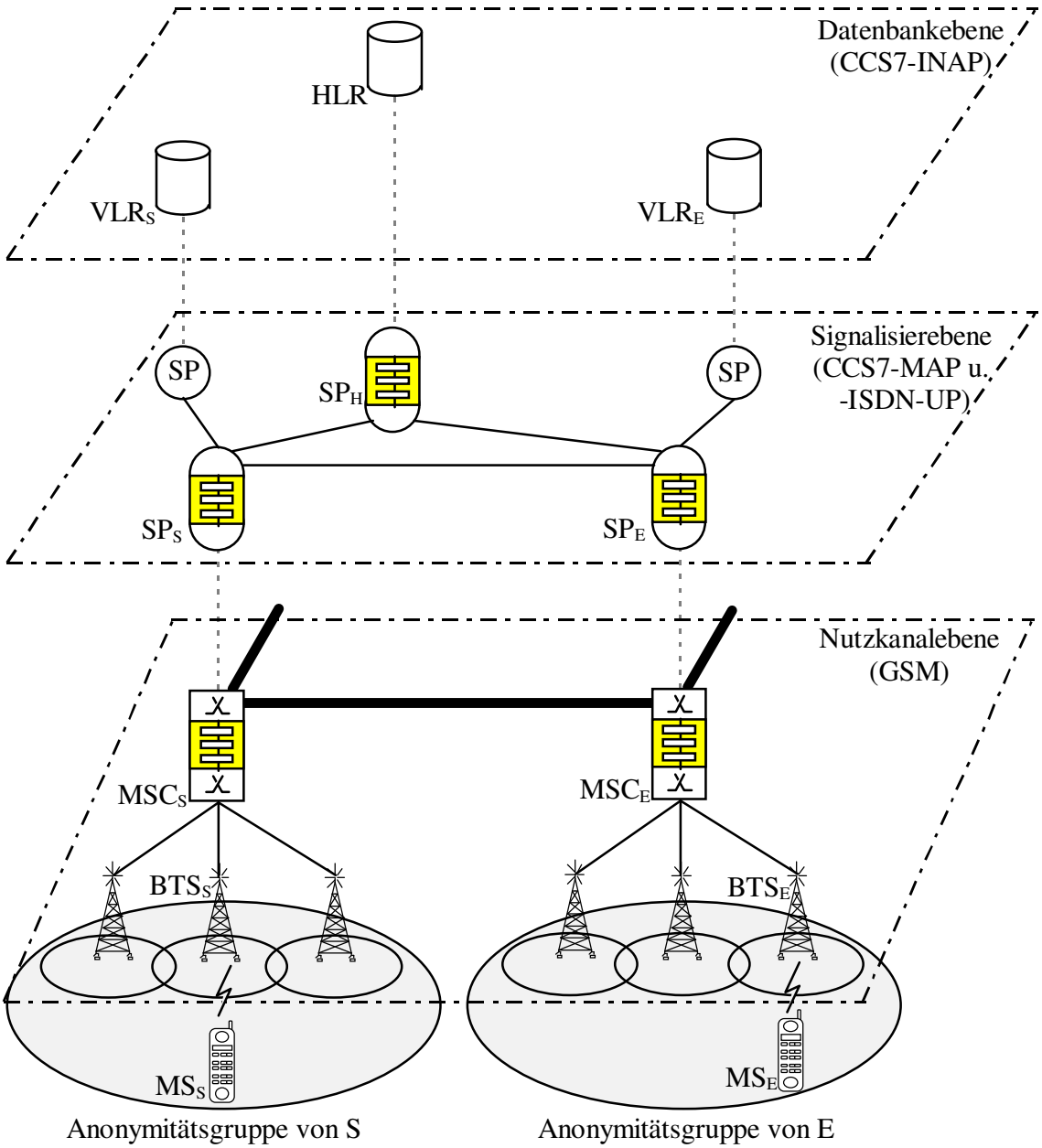


Abb. 3.2.1.1: Modifizierte GSM-Netzstruktur

Dieser Schutz ist in einem Mobilkommunikationssystem allerdings nicht ausreichend. Deshalb wird der Signalisierungspunkt des HLRs zusätzlich um MIX-Funktionalität erweitert. Dadurch wird bei einem Location Update geschützt, aus welchem MSC-Bereich Änderungen vorgenommen werden und bei einem Verbindungswunsch wird verborgen, in welchen MSC-Bereich der Verbindungswunsch zum Empfänger geroutet wird. Eine zweite Anonymitätsgruppe, bezüglich der Aufenthaltsorte, besteht demzufolge aus allen MSCs, die einem HLR zugeordnet sind. Die Beziehung zwischen einem MSC und dessen VLR ist dagegen zur Zeit nicht durch MIXe zu schützen, da es sich um eine 1:1 Beziehung handelt. Sollten jedoch zukünftig mehrere MSCs zu einem VLR zugeordnet werden, sollte auch diese Kommunikationsbeziehung analog der MSC-HLR-Beziehung durch MIXe im SP des VLRs geschützt werden. Der Aufenthaltsort von kommunizierenden Teilnehmern ist demzufolge mit MSC-Genauigkeit bekannt. An dieser Stelle soll jedoch auf die stets existierende Möglichkeit der Peilung und Ortung

einer sendenden Mobilstation hingewiesen werden, die man auch durch DS/SS (siehe [FeTh_95]) nicht ganz verhindern kann.

Die Verfahren des Location Managements und des Verbindungsaufbaus werden in den folgenden Abschnitten diskutiert, ebenso verschiedene Angriffsmöglichkeiten und das erreichbare Wissen eines Angreifers. Einschränkungen bezüglich der Unbeobachtbarkeit von Mobilteilnehmern wird es im Mobilfunk allerdings stets durch die geringe Bandbreite auf der Funkschnittstelle geben. Außerdem kann man von akkugetriebenen Mobilstationen keine Aussendung von Dummy Traffic erwarten. Aus diesen Gründen läßt sich bei Mobilfunksystemen nie der gleiche Schutz erreichen, der in Festnetzen, wie ISDN, möglich ist.

Wie die Signalisierungsprotokolle des Location Managements zur Realisiserung der zusätzlichen Anforderungen modifiziert werden müssen, wird in *Kapitel 3.2.2* beschrieben.

3.2.2 Modifikation des Authentikationsprotokolls

Die Authentikation erfolgt in GSM zur Zeit mit einem symmetrischen Challenge-Response-Verfahren[24] , wobei sich nur der Teilnehmer gegenüber dem Netzbetreiber authentisieren muß. Dies ist jedoch für ein mehrseitig sicheres System nicht ausreichend. Deshalb soll im folgenden eine gegenseitige Authentikation vorgeschlagen werden.

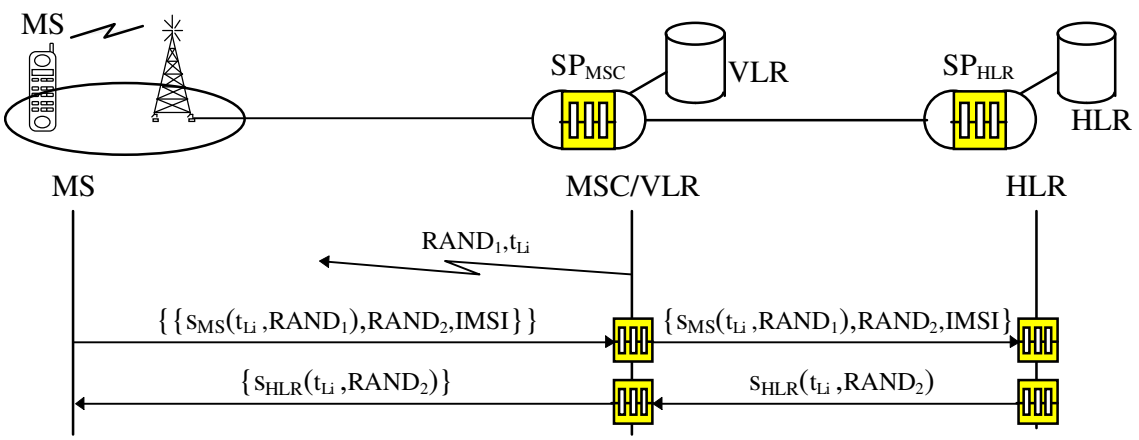


Abb. 3.2.2.1: Modifizierte Authentikationsprozedur

Da für den Einsatz von MIXen auf jeden Fall asymmetrische Kryptographie implementiert werden muß, wird im folgenden ein asymmetrisches Challenge Response Authentikationsverfahren vorgeschlagen, das nur zwei 2 Protokollschritte benötigt. In dieses Verfahren kann auch das Setzen eines Verschlüsselungsmodus integriert werden, dies wird jedoch in *Abb 3.2.2.1* nicht dargestellt. *Abb. 3.2.2.1* stellt das Grundprinzip der vorgeschlagenen **gegenseitigen Authentikation** dar. Jede BTS broadcastet in jedem LUP-Takt die vom Authentikation Center (AuC) signierte Challenge ($RAND_1$) und den Takt t_{Li}[25] .

[24] Dazu wird der MS eine Zufallszahl RAND (128 Bit) gesendet. In der MS wird RAND und der geheime Schlüssel k_i mit dem Algorithmus A3 bearbeitet und das Ergebnis SRES* wird dem Netz als Response gesendet. Dort wird SRES des Authentikationssets (aus dem AuC) mit SRES* verglichen. Genauere Informationen sind in [GSM_3.20] im *Kapitel 3.2* zu finden.

[25] Das LUP muß, ebenso wie der Verbindungsaufbau getaktet werden. Allerdings kann die Zeitscheibenlänge verschieden sein. Für LUPs ist einer längerer LUP-Takt von unter 10s ausreichend, da die Bewegung nicht so schnell erfolgt und Zellgrenzen sich überlappen. Bei einem Verbindungswunsch wäre eine Zeitscheibenlänge von ca. 10s dagegen nicht akzeptabel.

- **Schritt 1:** Die MS sendet an das MSC/VLR eine verdeckte Authentikationsnachricht {{N}} für das HLR. Diese enthält die signierte Challenge und den LUP-Takt, sowie die Challenge $RAND_2$ für das HLR. Außerdem muß die IMSI als Teilnehmeridentifikator gesendet werden. Für das MSC/VLR ist der Nachrichteninhalt der Nachricht N_{AuC} an das HLR nicht erkennbar.
  $\mathbf{N_{MSC/VLR}} := c_{V1}(D_{V1} , c_{V2}(D_{V2} , c_{V3}(D_{V3} , N_{AuC})))$
  mit $\mathbf{D_{V1}} := t_{Li}, k_{V1}$
  $\mathbf{D_{V2}} := t_{Li}, k_{V2}$
  $\mathbf{D_{V3}} := t_{Li}, k_{V3}, KKZ_V(Li)$
  $\mathbf{N_{AuC}} := c_{A1}(D_{A1} , c_{A2}(D_{A2} , c_{A3}(D_{A3} , s_{MS}(t_{Li},RAND_1), IMSI , RAND_2)))$
  mit $\mathbf{D_{A1}} := t_{Li}, k_{A1}$
  $\mathbf{D_{A2}} := t_{Li}, k_{A2}$
  $\mathbf{D_{A3}} := t_{Li}, k_{A3}, KKZ_A(Li)$
  $|\mathbf{N_{AuC}}| = \underline{2082 \text{ Bit}}$
  $|\mathbf{N_{MSC/VLR}}| = \underline{3690 \text{ Bit}}$
  Das HLR kann nun die Signatur des Teilnehmers (IMSI) prüfen und so die Teilnehmer-Netz-Authentikation vernehmen.

- **Schritt 2:** Das HLR signiert die Challenge $RAND_2$ für die Netz-Teilnehmer-Authentikation. Anschließend übergibt es die Daten mit dem Kanalkennzeichen $KKZ_A(Li)$ der HLR-MIX-Kaskade. Dort wird die Nachricht schrittweise verschlüsselt und zum MSC/VLR übertragen. Im MSC/VLR ist der Inhalt dieser Nachricht nicht erkennbar. Anschließend wird die Nachricht mit dem $KKZ_V(Li)$ über die MSC-MIX-Kaskade dem Teilnehmer signalisiert, so daß dieser die Netzauthentizität überprüfen kann.
  $\mathbf{N_{AuC}}^* := k_{A1}(t_{Li} , k_{A2}(t_{Li} , k_{A3}(t_{Li} , s_{HLR} (t_{Li} , RAND_2))))$
  $|\mathbf{N_{AuC}}^*| = \underline{500 \text{ Bit}}$
  $\mathbf{N_{MSC/VLR}}^* := k_{V1}(t_{Li},k_{V2}(t_{Li},k_{V3}(t_{Li},k_{A1}(t_{Li} ,k_{A2}(t_{Li},k_{A3}(t_{Li}, s_{HLR}(t_{Li} , RAND_2)))))))$
  $|\mathbf{N_{MSC/VLR}}^*| = \underline{800 \text{ Bit}}$

Durch das beschriebene Authentikationsprotokoll erfolgt die Authentikation ausschließlich zwischen der MS und dem HLR. Eine Authentikation zwischen dem diensterbringenden MSC/VLR und der MS wäre deutlich komplizierter und aufwendiger, da dem MSC/VLR die Identität der MS nicht bekannt werden darf, also nur das HLR die MS authentisieren kann. Demzufolge müßte das HLR dem MSC/VLR das Ergebnis der Teilnehmer-Authentikation unbeobachtbar mittteilen. Diese Unbeobachtbarkeit müßte auch dann noch gewährleistet sein, wenn MSC/VLR und HLR gemeinsam als Angreifer auftreten. Dieses Problem ließe sich mit zusätzlichen Protokollschritten zwar lösen, würde aber zu einem sehr aufwendigen und damit unpraktikablen Verfahren führen und soll deshalb im folgenden nicht genauer betrachtet werden.

Diese Nachrichten werden anschließend in die notwendigen Nachrichten des LUPs und des Call Setups integriert, um ohne zusätzliche Nachrichten und entsprechenden zusätzlichen Dummy Traffic eine gegenseitige Authentikation zu ermöglichen.

3.2.3 Modifikation der Signalisierungsprotokolle zum Location Management

Nach den Modifikationen der GSM-Netzstruktur ist das Signalisierungsprotokoll des Location Updates (LUP) ebenfalls zu modifizieren. Optimierungskriterium ist diesbezüglich die Anzahl und die Länge der Nachrichten auf der Funkschnittstelle. *Abb. 3.2.3.1* zeigt das entsprechend modifizierte Signalisierungsprotokoll des LUP.

Die Mobilstation (MS) nutzt die MIX-Kaskade des MSCs, um eine anonyme Rückadresse {LAI,IAdr}[26] unbeobachtbar im VLR abzulegen. Durch die anonyme LUP-Request-Nachricht wird ein unbeobachtbarer Empfangskanal für die anschließende Quittung des Netzes aufgebaut. Der anonyme LUP-Request enthält außerdem Authentikationsdaten und die LUP-Nachricht an das HLR.

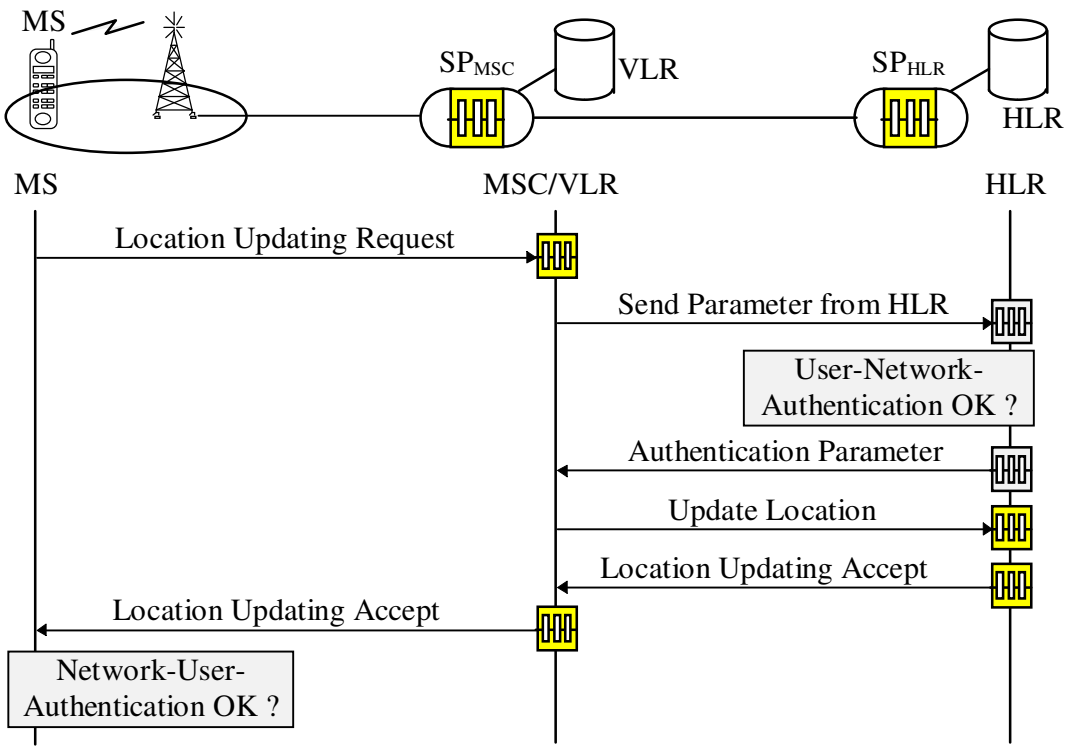


Abb. 3.2.3.1: Modifiziertes Signalisierungsprotokoll des LUP

Das MSC/VLR leitet die Authentikationsdaten nach Erhalt zuerst unbeobachtbar an das HLR weiter. Dazu wird die MIX-Kaskade beim HLR verwendet, an die alle MSC/VLRs ihre Anfragen richten. Das MSC/VLR erhält als Antwort die verdeckten Authentikationsdaten des HLRs über den anonymen Empfangskanal, der mit der Anforderung aufgebaut wurde. Anschließend wird die anonyme Rückadresse {LAI,IAdr} im VLR gespeichert und die LUP-Nachricht unbeobachtbar an das HLR gesendet. Verwendet wird dafür wiederum eine MIX-Kaskade beim HLR. Damit wird im HLR die anonyme Rückadresse {VLR,P} eingetragen. Sobald die Antwort des HLRs im MSC/VLR eingetroffen ist, leitet es die verdeckten Authentikationsdaten des HLRs innerhalb der anonymen LUP-Accept-Nachricht auf der Funkschnittstelle an den Teilnehmer weiter. Damit kann abschließend auch der Mobilteilnehmer die Authentizität die Netzes prüfen. Normalerweise sollte eine gegenseitige Authentikation vor der Netznutzung erfolgen, also bevor der Teilnehmer Informationen über sich preisgibt. Aus Effizienzgründen auf der Funkschnittstelle wurde die Authentikation hier nicht über separate Nachrichten vor dem LUP abgewickelt. Eine Abmeldung im alten VLR erfolgt aus Effizienzgründen nicht mehr. Der Eintrag dort verfällt nach einer festzulegenden Zeitschranke, von beispielsweise 10 Minuten, d.h. jede akkubetriebene Mobilstation muß mindestens alle 10 Minutem ein

[26] Die anonyme Rückadresse [LAI,IAdr} wird im VLR abgelegt und schreibt die Nutzung der MIX-Kaskade des MSCs bei der Übermittlung eines Verbindungswunsches vor. Diese Rückadresse wird in der MIX-Kaskade stufenweise entschlüsselt und gibt am Ende unverkettbar den Aufenthaltsort LAI des Teilnehmers und dessen dortige Kennung IAdr für eine Signalisierung bekannt.

LUP durchführen, um erreichbar zu bleiben. Dies ist im bestehenden GSM-Netz ähnlich gelöst.

3.2.4 Modifikation des Signalisierungsprotokolles zum Verbindungsaufbau

Das Signalisierungsprotokoll des Verbindungsaufbaus (Call Setup) wird bei GSM in zwei Teile geteilt. Der erste Teil ist das Mobile Originated Call Setup (MOC-Setup), ein von der MS ausgehender Ruf, und der zweite Teil ist das Mobile Terminated Call Setup (MTC-Setup), ein die MS erreichender Ruf.

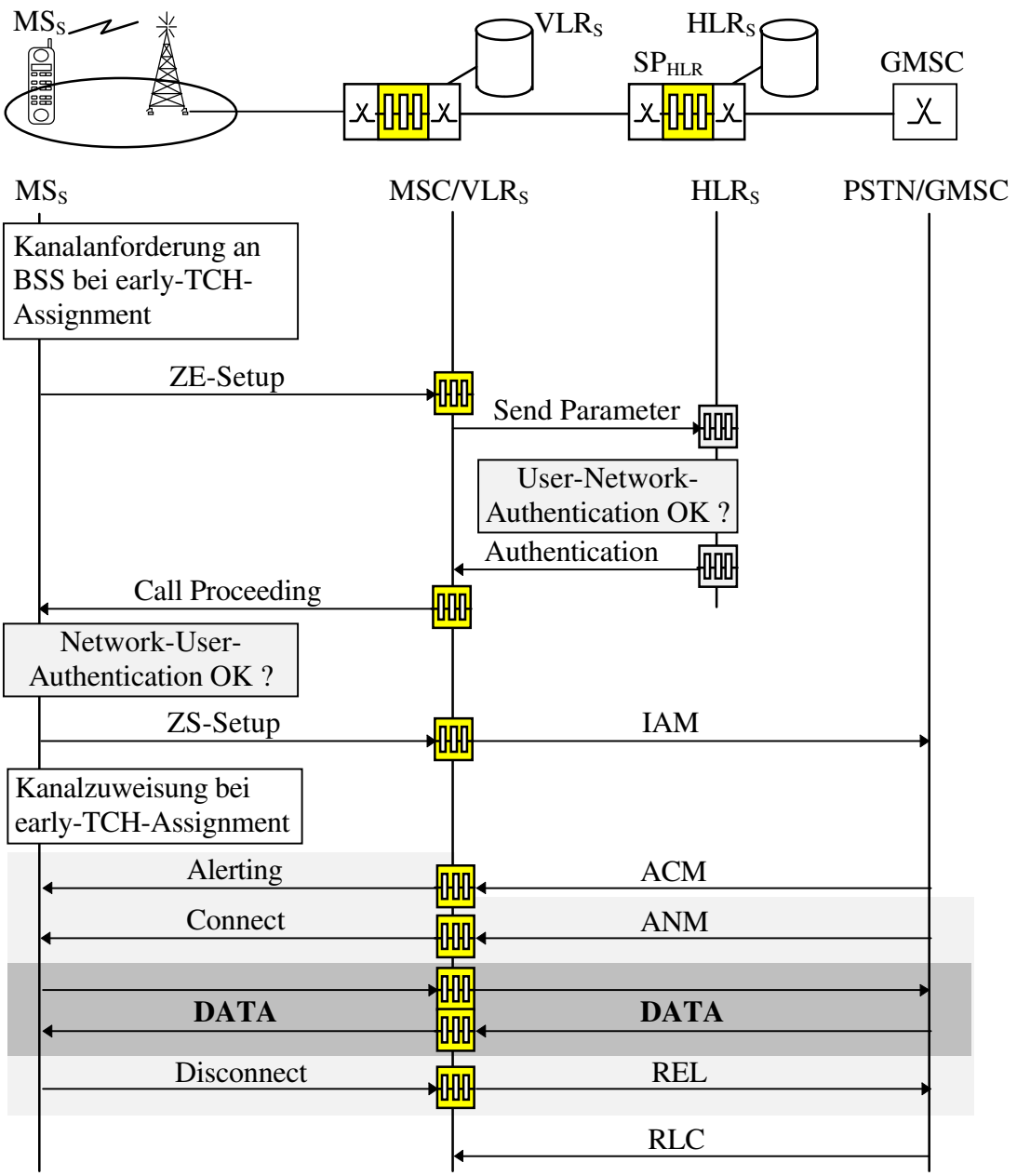


Abb. 3.2.4.1: Modifiziertes Signalisierungsprotokoll des Mobile Originated Calls

Entsprechend dieser Einteilung zeigt *Abb. 3.2.4.1* das modifizierte MOC-Setup-Protokoll. Weiterhin werden bei GSM zwei Arten des Call Setups entsprechend des Zeitpunkts der Nutzkanalanforderung unterschieden. Dabei handelt es sich um das early-TCH-Assignment, die zeitige Anforderung und Zuweisung eines Traffic Channels

(TCH), und um das Off Air Call Setup (OACSU). Bei der anonymen Signalisierung wurde das early-TCH-Assignment gewählt, damit schon frühzeitig ein Nutzkanal verfügbar ist.

Zuerst wird beim MOC ein Nutzkanal angefordert. Anschließend baut der Sender einen unbeobachtbaren ZE-Kanal über die MIX-Kaskade des MSC/VLR auf. Diese Nachricht enthält außerdem Authentikationsdaten für die Teilnehmer-Netz-Authentikation. Diese erfolgt, wie in *Kapitel 3.2.2* beschrieben. Anschließend erhält der Teilnehmer die Call-Proceeding-Nachricht mit den Daten des Nutzkanals auf der Funkschnittstelle und Angaben zur Netz-Teilnehmer-Authentikation. Der Sender baut anschließend den ZS-Kanal mit den Informationen über den Verbindungswunsch auf. Das MSC/VLR sendet darauf die IAM an das HLR des Empfängers. Dort wird die anonymen Rückadresse {VLR,P} des Empfängers ermittelt und die IAM mit dieser Rückadresse über die MIX-Kaskade des HLRs gesendet. Nach dieser MIX-Kaskade wird die IAM durch die in {VLR,P} enthaltenen Informationen zum VLR des Empfängers geroutet. Dabei kann noch kein Nutzkanal reserviert werden, da die MIX-Kaskade des HLRs nicht auf dem direkten Weg zum gewünschten VLR liegt und die spätere Nutzkanalkommunikation einen kürzestmöglichen Weg im Fernnetz nehmen soll. Nun muß der Sender warten, bis der Empfänger, wie im MTC beschrieben, aktiv wird und eine ACM auf dem direkten Weg sendet. Mit dieser Nachricht wird der bidirektionale Nutzkanal vollständig geschaltet und im Netz wird bekannt, welches MSC/VLR mit welchem MSC/VLR kommuniziert. Die beteiligten Teilnehmer bleiben innerhalb der verwalteten Aufenthaltsgebiete unbeobachtbar. Nachdem die ACM bzw Alerting-Nachricht vom Sender empfangen wurde, wartet dieser noch auf die ANM bzw. Connect-Nachricht im Nutzkanal, die signalisiert, daß der Empfänger den Hörer abgenommen hat. Nach erfolgter Kommunikation wird der Kanal im Fernnetz entsprechend der ISDN-Lösung abgebaut.

Abb. 3.2.4.2 zeigt das Gegenstück des Verbindungsaufbaus, das MTC-Setup. Die im HLR des Empfängers eintreffende IAM bildet den Ausgangspunkt eines MTC-Setups. Vom HLR des Empfängers wird die IAM mit der anonymen Rückadresse {VLR,P} über die MIX-Kaskade des HLRs gesendet und von dort zum VLR des Empfängers weitergeleitet. Dort ist der Empfänger mit dem Pseudonym P angemeldet und hat eine weitere anonyme Rückadresse hinterlegt, welche an die MIX-Kaskade im MSC des Empfängers zusammen mit dem Paging-Request signalisiert wird. Der letzte MIX dieser Kaskade erhält die Location Area Identification (LAI) des LAs, in dem der Paging-Request auszusenden ist. Der Empfänger erkennt an der signalisierten impliziten Adresse (IAdr), ob ein Verbindungswunsch für ihn ist. Ist dies der Fall, baut er, wie der Sender auch, den unbeobachtbaren ZE- und ZS-Kanal einschließlich Authentikation auf. Er sendet anschließend die ACM direkt zum ZE-Kanal im MSC/VLR des Senders und schaltet damit den Nutzkanal auch im Fernnetz auf dem direkten Weg. Wenn der Empfänger den Hörer abhebt folgt die Connect-Nachricht bzw. ANM bereits im Nutzkanal und die Kommunikation beginnt. Der Abbau erfolgt, wie bei ISDN beschrieben.

Durch diesen Verbindungsaufbau wird erst bei einer erfolgten Nutzkanalkommunikation bekannt, welches MSC/VLR mit welchem MSC/VLR eine Kommunikationsbeziehung unterhält. Während der Aufbauphase einer Verbindung bzw. wenn diese nicht angenommen wird, erfährt ein Angriffer nichts über den ungefähren Aufenthaltsort (MSC/VLR-Bereich) des Empfängers. Bekannt ist im Netz lediglich, daß ein Teilnehmer aus dem MSC/VLR-Bereich des Senders einen der Teilnehmer erreichen möchte, die im HLR des Empfängers eingetragen sind.

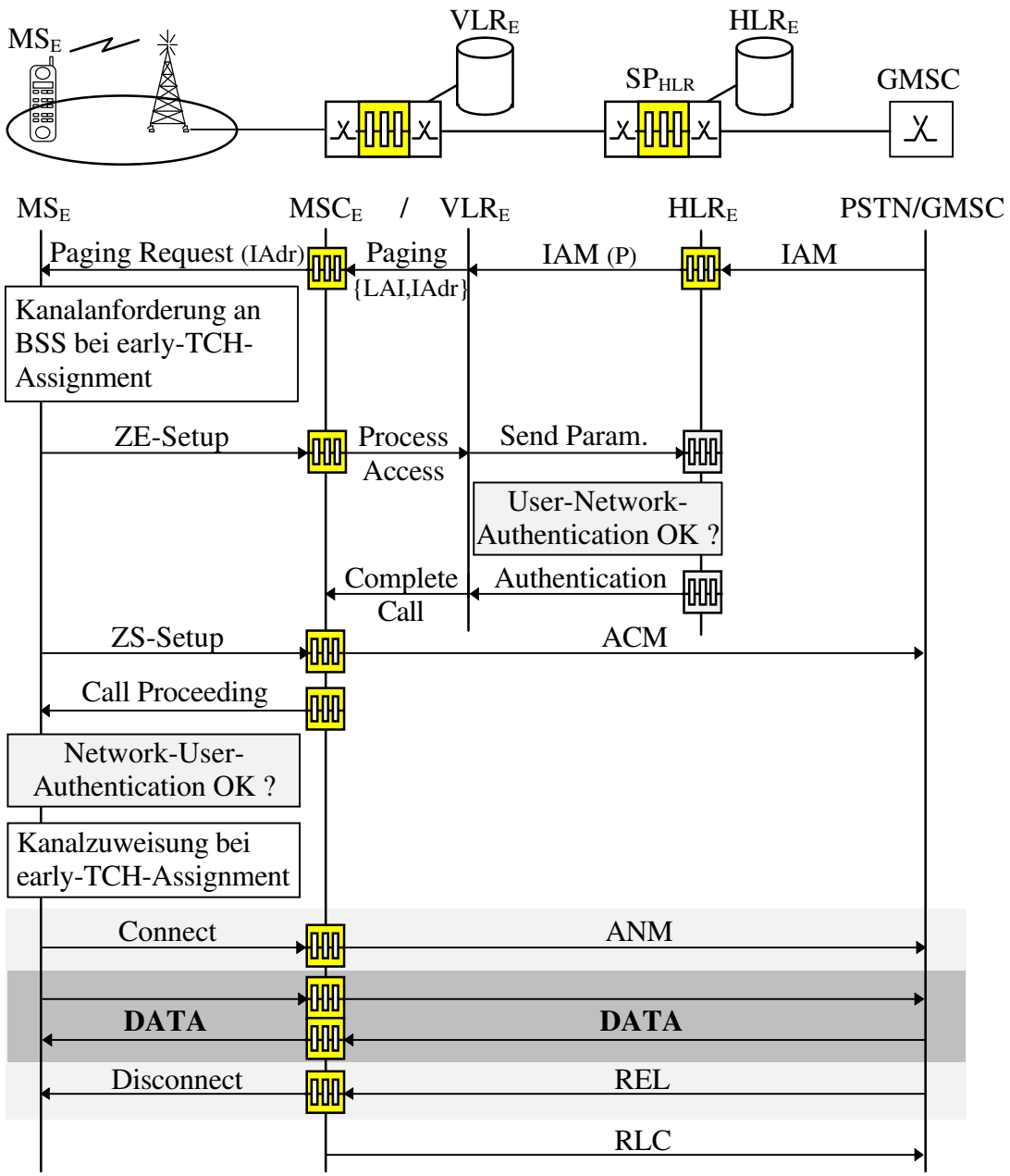


Abb. 3.2.4.2: Modifiziertes Signalisierungsprotokoll des Mobile Terminated Calls

Der Aufwand an Dummy Traffic, den eine anonyme Signalisierung erfordert, ist in GSM beträchtlich. Hauptproblem ist der Bandbreiteengpaß auf der Funkschnittstelle und der Einsatz von Dummy Traffic bei den Mobilstationen. Diese können sich nur an dem Dummy Traffic zum Schutz aller Teilnehmer eines MSC/VLR-Bereiches beteiligen, wenn sie nicht mit Akku betrieben werden. Den fehlenden Dummy Traffic aus einem LA gleicht die empfangende BTS aus. Dadurch entsteht im MSC/VLR kein zusätzliches Wissen, die BTS allerdings hat genauere Informationen über die Teilnehmer einer Anonymitätsgruppe und als Angreifer damit bessere Chancen zur Deanonymisierung einzelner Teilnehmer. Die Möglichkeit der Deanonymisierung von Mobilteilnehmern durch Peilung und Ortung ihrer sendenden MS wird dabei in dieser Arbeit nicht gesondert betrachtet. Dieser Angriff ist auch trotz anonymer Signalisierung möglich und wird in [FeTh_95] ausführlicher diskutiert.

3.2.5 Umsetzung der anonymen Signalisierung in RIL3 und CCS7

Das Radio Interface Layer 3-Protokoll (RIL3) wird auf dem Weg von der MS bis zum MSC verwendet. Es existiert weiterhin das Base Station Subsystem Management Part-Protokoll (BSSMAP), welches zwischen dem BSS und dem MSC für das Radio Ressource (RR)-Management und Handover (HOV) genutzt wird. Deshalb soll es hier nicht näher betrachtet werden. Im GSM-Festnetzbereich wird der CCS7-Mobile Application Part (MAP) für die Signalisierung genutzt. Der MAP ist Anwender des Transaction Capability Application Part TCAP). Zur Umsetzung der Verfahren zur anonymen Signalisierung ist jedoch nur eine Modifikation des RIL3 und des CCS7-MAP notwendig, welche in den folgenden Abschnitten beschrieben wird.

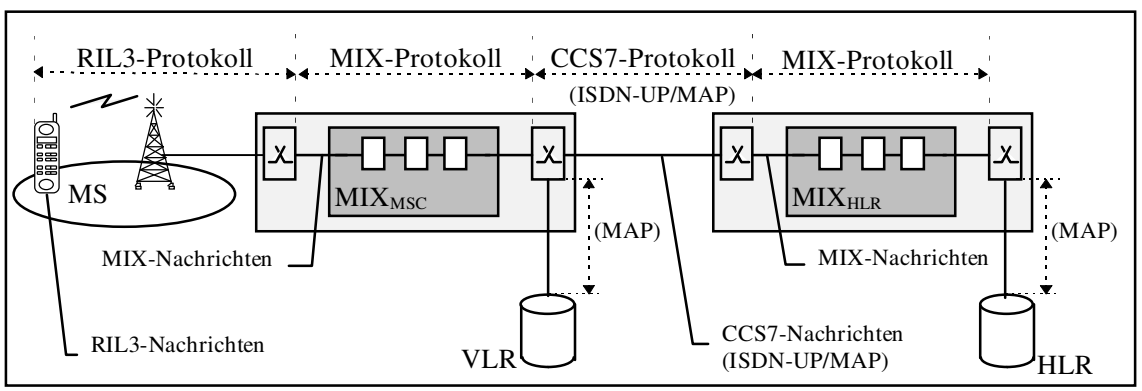


Abb. 3.2.5.1: Beschreibungspunkte der Nachrichteninhalte im GSM

Abb. 3.2.5.1 zeigt die Lage der verwendeten Kommunikationsprotokolle. Außerdem wurden die Stellen besonders gekennzeichnet, an denen die Inhalte der jeweiligen Signalisierungsnachrichten in den folgenden Abschnitten detailliert beschrieben werden.

3.2.5.1 Signalisierungsnachrichten im RIL3-Protokoll

Das RIL3-Protokoll besteht aus verschiedenen Teilen. So wird der Teil RIL3-Call Control (CC) und der Teil RIL3-Mobility Management (MM) bis zum MSC/VLR signalisiert und dort in das MAP-Protokoll konvertiert. Der Teil RIL3-Radio Ressource (RR) wird bereits in der BTS in das Radio Subsystem Management-Protokoll (RSM) konvertiert, im BSC in das BSSMAP und im ersten MSC in das MAP-Protokoll bis zum MSC/VLR. RR-Funktionen müssen zur Umsetzung anonymer Signalisierung allerdings nicht modifiziert werden, deshalb soll im folgenden dieser Teil nicht ausführlicher betrachtet werden.

Zuerst sollen die Nachrichten des Location Updates beschrieben werden. Bei den Zeitangaben der LUP-Nachrichten ist zu beachten, daß es sich um einen vom Systemtakt verschiedenen LUP-Takt handelt, wobei ein LUP-Takt deutlich länger als ein Systemtakt ist[27].

Die **Location Updating Request**-Nachricht: Mit der Aussendung dieser Nachricht signalisiert die MS eine Registrierungs-Aufforderung ihres neuen Aufenthaltsortes. Sie enthält die im VLR zu speichernden Lokalisierungsdaten, Authentikationsdaten und Lokalisierungsinformationen für das HLR. Die symmetrischen Schlüssel $k_{SE1..3}$ werden in der MIX-Kaskade im MSC für den Empfang der LUP-Quittung, ähnlich einem ZE-Kanal benutzt. Ebenso werden die Schlüssel $k_{A1..3}$ in der MIX-Kaskade

[27] Die Größen werden im *Kapitel 4.2* berechnet.

des HLRs benutzt. Das VLR erhält das Kanalkennzeichen $KKZ_S(Li)$ und das HLR $KKZ_A(Li)$ für die Antwort. Die anonyme Rückadresse {VLR,P} schreibt die Verwendung der MIX-Kaskade des HLRs vor und die {LAI, IAdr}-Rückadresse nutzt die MIX-Kaskade im aktuellen MSC. Dabei werden die Schlüssel $k_{H1..3}$ und $k_{S1..3}$ zum Verschlüsseln der Nachricht benutzt, die mittels der anonymen Rückadressen übertragen werden soll. Dabei handelt es sich in der Regel um einen Verbindungswunsch.

Die Location Updating Request-Nachricht enthält folgende Informationen:

- **Location Updating Request**-Nachricht des Teilnehmers S:

  $\mathbf{N_{LUP\text{-}Request}} := c_{S1}(D_{SE1}, c_{S2}(D_{SE2}, c_{S3}(D_{SE3}, N_{VLR})))$

  mit $\mathbf{D_{SE1}} := t_{Li}, k_{SE1}$

  $\mathbf{D_{SE2}} := t_{Li}, k_{SE2}$

  $\mathbf{D_{SE3}} := t_{Li}, k_{SE3}, KKZ_S(Li)$

  $\mathbf{N_{VLR}} := c_{MSC/VLR}(lup_msg, t_{Li}, P, \{LAI, IAdr\}, Bv/Bl, N_{AuC}, N_{HLR}^*)$

  $\mathbf{N_{AuC}} := c_{A1}(D_{A1}, c_{A2}(D_{A2}, c_{A3}(D_{A3}, s_{MS}(t_{Li}, RAND_1), IMSI, RAND_2)))$

  mit $\mathbf{D_{A1}} := t_{Li}, k_{A1}$

  $\mathbf{D_{A2}} := t_{Li}, k_{A2}$

  $\mathbf{D_{A3}} := t_{Li}, k_{A3}, KKZ_A(Li)$

  $\mathbf{N_{HLR}^*} := c_{H1}(D_{H1}, c_{H2}(D_{H2}, c_{H3}(D_{H3}, N_{HLR})))$

  mit $\mathbf{D_{H1}} := t_{Li}, k_{H1}$

  $\mathbf{D_{H2}} := t_{Li}, k_{H2}$

  $\mathbf{D_{H3}} := t_{Li}, k_{H3}, KKZ_{HLR}(Li)$

  $\mathbf{N_{HLR}} := k_{HLRS}(lup_msg, Bv/Bl, t_{Li}, IMSI, \{VLR,P\})$

  $\mathbf{\{VLR,P\}} := c_{H3}(k_{H3}, c_{H2}(k_{H2}, c_{H1}(k_{H1}, A_{VLR}, P)))$

  $\mathbf{\{LAI,IAdr\}} := c_{S3}(k_{S3}, c_{S2}(k_{S2}, c_{S1}(k_{S1}, LAI, IAdr)))$

  $|\mathbf{N_{LUP\text{-}Request}}| = \underline{9188\ Bit}$

Die **Location Updating Accept**-Nachricht: Diese Nachricht wird als Bestätigung eines LUPs vom MSC/VLR signalisiert. Sie enthält die Authentikationsdaten und die LUP-Quittung des HLRs.

Die Location Updating Accept-Nachricht enthält folgende Informationen:

- **Location Updating Accept**-Nachricht an den Teilnehmer S:

  $\mathbf{N_{LUP\text{-}Accept}} := k_{SE1}(t_{Li}, k_{SE2}(t_{Li}, k_{SE3}(t_{Li},$
  $(lup_acc_msg, k_{A1}(t_{Li}, k_{A2}(t_{Li}, k_{A3}(t_{Li}, s_{HLR}(t_{Li}, RAND_2)))), N_{HLR}^*)))$

  $\mathbf{N_{HLR}^*} := k_{H1}(t_{Li}, k_{H2}(t_{Li}, k_{H3}(t_{Li}, lup_acc_msg)))$

  $|\mathbf{N_{LUP\text{-}Accept}}| = \underline{1116\ Bit}$

Die folgenden Signalisierungsnachrichten gehören zum Call Setup. Deren Zugehörigkeit zum MOC- bzw. MTC-Setup wird für die Beschreibung der Nachrichteninhalte nicht gesondert angegeben, da dies aus *Abb. 3.2.4.1* und *3.2.4.2* ersichtlich ist. Es werden auch hier jeweils nur die hinzugekommenen I.E.´s angegeben, bestehende und zu entfernende I.E.´s werden im *Kapitel 3.2.5.2* beschrieben.

Die **Setup**-Nachrichten: Diese Nachricht teilt sich auch in GSM jeweils auf Sender und Empfängerseite in eine ZE-Setup-Nachricht zum Aufbau eines unbeobachtbaren Empfangskanals und eine ZS-Setup-Nachricht zum Aufbau eines unbeobachtbaren Sendekanals. Mit der ZE-Setup-Nachricht werden zusätzlich Authentikationsdaten des Teilnehmers signalisiert. Die ZS-Setup-Nachricht des Senders beinhaltet den Verbindungswunsch und damit die Daten der IAM und die ZS-Setup-Nachricht des Empfängers die Daten des ACM.

Die Setup-Nachrichten enthalten folgende Informationen:

- **ZE-Setup**-Nachricht des Senders:
  $\mathbf{N_{ZE\text{-}Setup(S)}}$:= $c_{S1}(D_{SE1}, c_{S2}(D_{SE2}, c_{S3}(D_{SE3}, N_{AuC}))$
  mit $\mathbf{D_{SE1}}$:= t_i, k_{SE1}
  $\mathbf{D_{SE2}}$:= t_i, k_{SE2}
  $\mathbf{D_{SE3}}$:= $t_i, k_{SE3}, KKZ_S(i)$
  $\mathbf{N_{AuC}}$:= $c_{A1}(D_{A1},c_{A2}(D_{A2},c_{A3}(D_{A3},s_S(t_i,RAND_1),IMSI_S, RAND_2)))$
  mit $\mathbf{D_{A1}}$:= t_i, k_{A1}
  $\mathbf{D_{A2}}$:= t_i, k_{A2}
  $\mathbf{D_{A3}}$:= $t_i, k_{A3}, KKZ_A(i)$
  $|\mathbf{N_{ZE\text{-}Setup(S)}}|$ = 3690 Bit
- **ZS-Setup**-Nachricht des Senders:
  $\mathbf{N_{ZS\text{-}Setup(S)}}$:= $c_{S1}(D_{SS1}, c_{S2}(D_{SS2}, c_{S3}(D_{SS3}, c_{HLR}(t_i,MSISDN_E,N_E)))$
  mit $\mathbf{D_{SS1}}$:= t_i, k_{SS1}
  $\mathbf{D_{SS2}}$:= t_i, k_{SS2}
  $\mathbf{D_{SS3}}$:= $t_i, k_{SS3}, A_{HLR_E}, KKZ_E(i)$, Bv/Bl
  $\mathbf{N_E}$:= c_E (call_setup_msg , t_i , A_{MSC/VLR_S} , KZ_{init})
  $|\mathbf{N_{ZS\text{-}Setup(S)}}|$ = 2501 Bit
- **ZE-Setup**-Nachricht des Empfängers:
  $\mathbf{N_{ZE\text{-}Setup(E)}}$:= $c_{E1}(D_{EE1}, c_{E2}(D_{EE2}, c_{E3}(D_{EE3}, N_{AuC}))$
  mit $\mathbf{D_{EE1}}$:= t_i, k_{EE1}
  $\mathbf{D_{EE2}}$:= t_i, k_{EE2}
  $\mathbf{D_{EE3}}$:= $t_i, k_{EE3}, KKZ_E(i)$
  $\mathbf{N_{AuC}}$:= $c_{A1}(D_{A1},c_{A2}(D_{A2},c_{A3}(D_{A3},s_{MS}(t_i,RAND_1),IMSI_E, RAND_2)))$
  mit $\mathbf{D_{A1}}$:= t_i, k_{A1}
  $\mathbf{D_{A2}}$:= t_i, k_{A2}
  $\mathbf{D_{A3}}$:= $t_i, k_{A3}, KKZ_A(i)$
  $|\mathbf{N_{ZE\text{-}Setup(E)}}|$ = 3690 Bit
- **ZS-Setup**-Nachricht des Empfängers:
  $\mathbf{N_{ZS\text{-}Setup(E)}}$:= $c_{E1}(D_{ES1}, c_{E2}(D_{ES2}, c_{E3}(D_{ES3}, N_S))$
  mit $\mathbf{D_{ES1}}$:= t_i, k_{ES1}
  $\mathbf{D_{ES2}}$:= t_i, k_{ES2}
  $\mathbf{D_{ES3}}$:= $t_i, k_{ES3}, A_{MSC/VLR_S}$, $KKZ_S(i)$, Bv/Bl
  $\mathbf{N_S}$:= alerting_msg, t_i , A_{MSC/VLR_E}
  $|\mathbf{N_{ZS\text{-}Setup(E)}}|$ = 2082 Bit
  Bei der Realisiserung sollte diese ZS-Setup-Nachricht mit Informationen bis auf die Größe der ZS-Setup-Nachricht des Senders aufgefüllt werden, da für jedes Nachrichtenformat (unterschiedliche Größe u.ä.) separater Dummy Traffic durchgeführt werden muß.

Die **Paging Request**-Nachricht: Mit dieser Nachricht wird der Verbindungswunsch im entsprechenden LA ausgesendet. Nur der adressierte Empfänger kann diesen Verbindungswunsch korrekt entschlüsseln. Durch Vergleich der IAdr braucht er allerdings nicht jede Paging-Nachricht entschlüsseln und spart Akkukapazität.
Die Paging Request-Nachricht enthält folgende Informationen:

- **Paging Request**-Nachricht an den Empfänger:
  $\mathbf{N_{Paging\ Request}}$:= IAdr, $k_{E1}(t_i, k_{E2}(t_i, k_{E3}(t_i, k_{H1}(t_i, k_{H2}(t_i, k_{H3}(t_i,$

$c_E(call_setup, t_i, A_{MSC/VLR_S}, KZ_{init})))))))$

$|\mathbf{N_{Paging\ Request}}| = \underline{1388\ Bit}$

Die **Call Proceeding**-Nachricht: Mit dieser Nachricht erhält der Teilnehmer die Bestätigung, daß die Teilnehmer-Netz-Authentikation erfolgreich war und der Verbindungswunsch bearbeitet wird. Außerdem sendet das Netz die Authentikationsdaten zur Netz-Teilnehmer-Authentikation.

Die Call Proceeding-Nachrichten enthalten folgende Informationen:

- **Call Proceeding**-Nachricht an den Sender:

  $\mathbf{N_{Call\ Proceeding(S)}} := k_{SE1}(t_i , k_{SE2} (t_i , k_{SE3} (t_i , call_pro_msg, k_{A1}(t_{Li} , k_{A2}(t_{Li} , k_{A3}(t_{Li} , s_{HLR} (t_{Li} , RAND_2)))))))$

  $|\mathbf{N_{Call\ Proceeding(S)}}| = \underline{808\ Bit}$
- **Call Proceeding**-Nachricht an den Empfänger:

  $\mathbf{N_{Call\ Proceeding(E)}} := k_{EE1}(t_i , k_{EE2} (t_i , k_{EE3} (t_i , call_pro_msg, k_{A1}(t_{Li} , k_{A2}(t_{Li} , k_{A3}(t_{Li} , s_{HLR} (t_{Li} , RAND_2)))) , CIC))$

  $|\mathbf{N_{Call\ Proceeding(E)}}| = \underline{820\ Bit}$

Die **Alerting**-Nachricht: Mit dieser Nachricht wird dem Sender die durchgeschaltete Verbindung signalisiert. Außerdem erhält der Empfänger die Informationen über den belegten Nutzkanal im Fernnetz (CIC). Diese Nachricht wird auf der Funkschnittstelle bereits im Nutzkanal übertragen.

Die Alerting-Nachricht enthält folgende Informationen:

- **Alerting**-Nachricht an den Sender:

  $\mathbf{N_{Alerting}} := k_{SE1}(t_i,k_{SE2}(t_i,k_{SE3}(alerting_msg, t_i, A_{MSC/VLR_E}, CIC)))$

  $|\mathbf{N_{Alerting}}| = \underline{334\ Bit}$

Die **Connect**-Nachricht: Mit dieser Nachricht wird das Zustandekommen der Kommunikationsverbindung auf dem Nutzkanal signalisiert.

Die Connect-Nachrichten enthalten folgende Informationen:

- **Connect**-Nachricht des Empfängers:

  $\mathbf{N_{Connect}} := k_{ES1}(t_i,k_{ES2}(t_i,k_{ES3}(connect_msg, t_i, A_{MSC/VLR_S}, CIC)))$

  $|\mathbf{N_{Connect}}| = \underline{334\ Bit}$
- **Connect**-Nachricht an den Sender:

  $\mathbf{N_{Connect}} := k_{SE1}(t_i , k_{SE2} (t_i , k_{SE3} (connect_msg, t_i)))$

  $|\mathbf{N_{Connect}}| = \underline{308\ Bit}$

Die **Disconnect**-Nachricht: Mit dieser im Datenkanal übertragenen Nachricht wird die Beendigung der Kommunikation durch einen der Teilnehmer signalisiert.

Die Disconnect-Nachrichten enthalten folgende Informationen:

- **Disconnect**-Nachricht des auflegenden Teilnehmers (z.B. E):

  $\mathbf{N_{Disconnect}} := k_{ES1}(t_i,k_{ES2}(t_i,k_{ES3}(disconnect_msg, t_i, A_{MSC/VLR_S}, CIC)))$

  $|\mathbf{N_{Disconnect}}| = \underline{334\ Bit}$
- **Disconnect**-Nachricht des anderen Teilnehmers, hier des Senders:

  $\mathbf{N_{Disconnect}} := k_{SE1}(t_i , k_{SE2} (t_i , k_{SE3} (disconnect_msg, t_i)))$

  $|\mathbf{N_{Disconnect}}| = \underline{308\ Bit}$

Die **Release**- und die **Release Complete** Nachricht sind nicht mehr nötig, da alle bestehenden Verbindungen am Ende jeder Zeitscheibe (Systemtakt) automatisch abgebaut werden.

3.2.5.2 Änderungen der Datenstrukturen im RIL3-Protokoll

In *Abb. 3.2.5.2.1* wird der allgemeingültige **Aufbau einer Radio Interface Layer 3 Message** (RIL3) dargestellt. Der Nachrichtenkopf ist stets 16 Bit groß, anschließend folgen die Informationselemente, nach Pficht- und Wahlparametern sortiert. Auch für RIL3-Nachrichten ist in GSM eine maximale Länge der I.E.´s angegeben. Diese beträgt abhängig vom benutzten Signalisierungskanal 144 Bit im SACCH, 160 Bit im FACCH, SDCCH und 184 Bit im BCCH, AGCH und PCH, d.h. es muß für die Kanalnutzung ebenfalls eine Nachrichtensegmentierung implementiert werden.

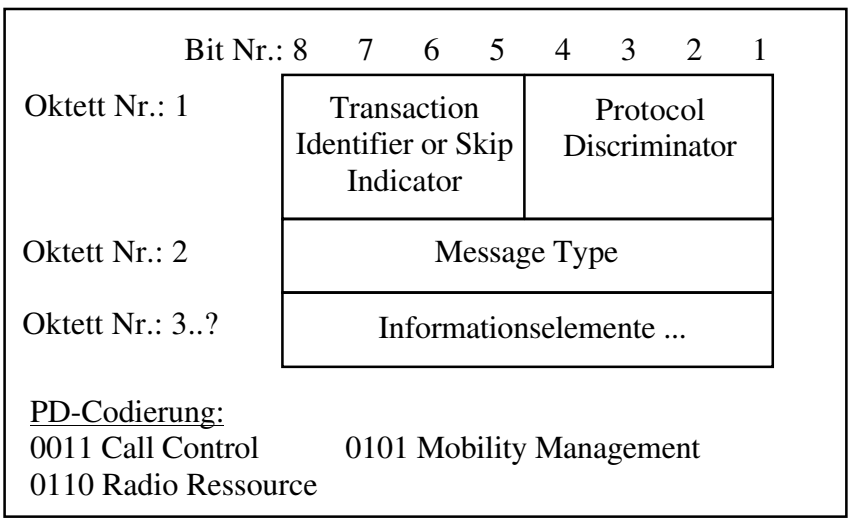


Abb. 3.2.5.2.1: Aufbau einer RIL3-Signalisierungsnachricht

Abb. 3.2.5.2.2 zeigt die modifizierte Codierung der benötigten RIL3-Nachrichtentypen. Ausgangspunkt dieser Darstellung ist die *Tabelle 10.1* in [GSM_4.08]. Nicht mehr benötigt werden die Ciphering Messages (Ciphering Mode Command und Ciphering Mode Complete), die Paging Response Message, die Call Confirmed Message, die Connect Acknowledge und die Call Clearing Messages (Release und Release Complete). Neu hinzugekommen sind die Nachrichtentypen ZE- und ZS-Setup für den Nachrichtentyp Setup.

Nachrichtentyp	Codierung
• Paging Messages:	0010 0xxx
Paging Request Type 1	0001
Paging Request Type 2	0010
Paging Request Type 3	0100
• Registration Message:	0x00 xxxx
Location Updating Accept	0010
Location Updating Request	1000
• Call Establishment Messages:	0x00 xxxx
Alerting	0011
Call Proceeding	1011
Connect	0111
ZE-Setup	0101
ZS-Setup	0110
• Call Clearing Messages:	0x10 xxxx
Disconnect	0101

Abb. 3.2.5.2.2: Modifizierte Codierung der RIL3-Nachrichtentypen des Basisablaufes

Die Signalisierung der Alerting-, Connect- und Disconnect-Nachricht erfolgt auch in GSM aus Performancegründen im Nutzkanal, deren Nachrichtenfunktionalität bleibt davon jedoch unverändert, da alle Switches unverschlüsselte Nachrichten im Nutzkanal auswerten.

Informationselement	Abkürzung	Codierung
Authentication Information	AI	0000 0010
Bearer Capability	BC	0000 0100
Cause	CAU	0000 1000
Channels Needed Indication	CNI	1110 - - - -
High Layer Compatibility	HLC	0111 1101
Location Information	LI	0000 0001
Low Layer Compatibility	LLC	0111 1100
Paging Information	PI	0000 0101
Page Mode	PM	1xxx - - - -
Proceeding Information	PRI	0000 0111
Repeat Indicator	RI	101x xxxx
Setup Information	SI	0000 0011
Signal	S	0011 0100

Abb. 3.2.5.2.3: Modifizierte Codierung der RIL3-Informationselemente

Abb 3.2.5.2.3 zeigt die modifizierte Codierung der Informationselemente. Die angegebene Codierung der I.E.´s ist jedoch nicht vollständig, sie enthält nur die I.E.´s, die in den betrachteten Signalisierungsnachrichten aus *Abb. 3.2.5.2.2* enthalten sind.

Nachfolgend wird der Nachrichteninhalt aller modifizierten Signalisierungsnachrichten angegeben, wobei die gewählte Darstellung deren exakte Codierung nicht wiedergibt, sondern nur den Namen, die Bedeutung und die Länge der Informationselemente. Die Codierung der vorhandenen I.E.´s wird im *Kapitel 10.5* in [GSM_4.08] erläutert.

Parametername	**enthaltene Information**
- Location Information (9188 Bit)	enthält die Lokalisierungsdaten für das VLR und das HLR, sowie Authentikationsdaten

Abb. 3.2.5.2.4: Aufbau der Location Updating Request-Nachricht

Abb. 3.2.5.2.4 zeigt den Inhalt der Location Updating Request-Nachricht. Entfernt wurden Location Update Type (8 Bit), Ciphering Key Sequence Number (8 Bit), Location Area Identification (48 Bit), Mobile Station Classmark (16 Bit) und Mobility Identity (24-80 Bit). Neu hinzugekommen ist das I.E. Location Information, welches die verschlüsselten Daten der $N_{LUP\text{-}Request}$ enthält. Die Länge dieser Nachricht nimmt demzufolge um ca. 9050 Bit zu. Damit stellt diese Signalisierungsnachricht, neben dem Dummy Traffic, das größte Problem bei der Realisierung eines solchen Verfahrens dar (siehe *Kapitel 4.3*).

Parametername	**enthaltene Information**
- Authentication Information (1116 Bit)	enthält die Authentikationsdaten und die LUP-Quittung des HLRs

Abb. 3.2.5.2.5: Aufbau der Location Updating Accept-Nachricht

In *Abb. 3.2.5.2.5* wird der Aufbau einer Location Updating Accept-Nachricht dargestellt. Entfernt wurden in dieser Nachricht die I.E.´s Location Area Identification (48 Bit), Mobile Identity (24-80 Bit) und Follow on Proceed (8 Bit). Hinzugekommen ist das I.E. Authentication Information, welches die Authentikationsdaten des Netzes gegenüber dem Teilnehmer enthält. Durch diese zusätzliche Funktionalität vergrößert sich die Nachricht um ca. 1000 Bit.

Parametername	**enthaltene Information**
- BC Repeat Indicator (8 Bit)	legt die Interpretierung von wiederholten I.E.´s fest
- Bearer Capability 1 (24-80 Bit)	enthält Informationen über den Trägerservice (Radio Channel, Coding Standard, Transfer mode ... siehe *Abb. 10.71ff.* in [GSM_4.08]
- Bearer Capability 2 (24-80 Bit)	*bereits erklärt*
- Low Layer Compatibility I (16-120 Bit)	Kompatibilitätsprüfung
- High Layer Compatibility I (16-40 Bit)	Kompatibilitätsprüfung
- Setup Information (3690 bzw. 2501 Bit)	enthält die Setup Informationen zum Aufbau eines ZE- bzw. ZS-Kanals

Abb.: 3.2.5.2.6: Aufbau der MOC ZE- bzw. ZS-Setup-Nachrichten

In *Abb. 3.2.5.2.6* wird der Aufbau einer ZE- bzw. ZS-Nachrichten für den MOC dargestellt. Entfernt wurden in dieser Nachricht die I.E.´s Facility (>24 Bit), Calling Party Subaddress (16-184 Bit), Called Party BCD Number (24-104 Bit), Called Party Subaddress (16-184 Bit), LLC Repeat Indicator (8 Bit), Low Layer Compatibility II (16-120 Bit), HLC Repeat Indicator (8 Bit), High Layer Compatibility II (16-40 Bit), User User (24-280 Bit), SS Version Indicator (>16 Bit), CLIR Suppression (8 Bit) und CLIR Invocastion (8 Bit).

Parametername	**enthaltene Information**
- BC Repeat Indicator (8 Bit)	legt die Interpretierung von wiederholten I.E.´s fest
- Bearer Capability 1 (24-80 Bit)	enthält Informationen über den Trägerservice (Radio Channel, Coding Standard, Transfer mode ... siehe *Abb. 10.71ff.* in [GSM_4.08]
- Bearer Capability 2 (24-80 Bit)	*bereits erklärt*
- Signal (16 Bit)	legt Art des Signaltones beim Teilnehmer fest
- Low Layer Compatibility I (16-120 Bit)	Kompatibilitätsprüfung
- High Layer Compatibility I (16-40 Bit)	Kompatibilitätsprüfung
- Setup Information (3690 bzw. 2501 Bit)	enthält die Setup Informationen zum Aufbau eines ZE- bzw. ZS-Kanals

Abb.: 3.2.5.2.7: Aufbau der MTC ZE- bzw. ZS-Setup-Nachrichten

In *Abb. 3.2.5.2.7* wird der Aufbau einer ZE- bzw. ZS-Nachrichten für den MTC dargestellt. Entfernt wurden in dieser Nachricht die I.E.´s Facility (>24 Bit), Progress Indicator (32 Bit), Calling Party BCD Number (24-112 Bit), Calling Party Subaddress (16-184 Bit), Called Party BCD Number (24-104 Bit), Called Party Subaddress (16-184 Bit), LLC Repeat Indicator (8 Bit), Low Layer Compatibility II (16-120 Bit), HLC Repeat Indicator (8 Bit), High Layer Compatibility II (16-40 Bit) und User User (24-280 Bit).

Parametername	**enthaltene Information**
- Page Mode (4 Bit)	Normal-, Erweitert- o. Reorganisation-Mode
- Channels Needed for Mobiles 1 and 2 (4 Bit)	zu benutzender Kanal (SDCCH, TCH/F oder TCH/H) von der MS
- Paging Information (1388 Bit)	enthält die Teilnehmerkennung IAdr und die Verbindungswunschnachricht N_E

Abb.: 3.2.5.2.8: Aufbau der Paging Request-Nachricht

In *Abb. 3.2.5.2.8* wird der Aufbau einer Paging Request-Nachricht dargestellt. Dieser Nachricht ist als erster Parameter die RIL2-Pseudo-Länge (8 Bit) vorangestellt, anschließend folgt der RIL3-Kopf und die RIL3-I.E.´s. Zu verwenden ist im Rahmen dieser Arbeit stets der Paging Request vom modifizierten Type 1. Dieser ist nur an genau einen Teilnehmer gerichtet. Entfernt wurden in dieser Nachricht die I.E.´s Mobile Identity 1 (16-72 Bit) und Mobile Identity 2 (24-80 Bit). In GSM ist eine Paging-Nachricht bisher

immer 176 Bit lang. Diese Länge reicht bei Anwendung der anonymen Signalisierung nicht aus. Die Paging-Nachricht hat dann eine Länge von 1404 Bit.

Parametername	**enthaltene Information**
- BC Repeat Indicator (8 Bit) - Bearer Capability 1 (24-80 Bit) - Bearer Capability 2 (24-80 Bit) - Proceeding Information (808 bzw. 820 Bit)	*bereits erklärt* *bereits erklärt* *bereits erklärt* Netz-Teilnehmer-Authentikation und beim Empfänger zusätzlich Nutzkanalkennung

Abb.: 3.2.5.2.9: Aufbau der Call Proceeding-Nachricht

In *Abb. 3.2.5.2.9* wird der Aufbau einer Call Proceeding-Nachricht dargestellt. Entfernt wurden in dieser Nachricht die I.E.´s Facility (>16 Bit) und Progress Indicator (32 Bit).

Alle anderen Signalisierungsnachrichten (Alerting, Connect und Disconnect) werden im Datenkanal übertragen. Deren Aufbau ist aufgrund der größeren Bandbreite des Datenkanals nicht kritisch. I.E.´s, die die Unbeobachtbarkeit des Teilnehmers gefährden bzw. aufheben, müssen jedoch auch in diesen Signalisierungsnachrichten entfernt werden.

3.2.5.3 Signalisierungsnachrichten im MIX-Protokoll

Auch bei der Realiserung im GSM wird das aus der ISDN-Umsetzung bekannte MIX-Protokoll verwendet. Die Signalisierungsdaten werden in den MSCs vom RIL3-Protokoll in das MIX-Protokoll und nach der MIX-Kaskade in das CCS7-MAP-Protokoll konvertiert bzw. bei dem MIX des HLRs vom CCS7-MAP- ins MIX- und anschließend zurück ins CCS7-MAP-Protokoll. Auch wenn die MIX-Kaskade des HLRs organisatorisch in der Signalisierungsebene liegt, existiert auf der Nutzkanalebene ein Switch, der die Konvertierungen vor und nach der MIX-Kaskade vornimmt. Dieser Switch hat aber keine vollständige MSC-Funktionalität, d.h. ihm sind keine BSSs und kein VLR zugeordnet, es handelt sich vergleichsweise um eine Transitvermittlungsstelle (TE).

Im folgenden werden die Datenstrukturen der Signalisierungsnachrichten, die vom RIL3- über das MIX- ins MAP-Protokoll zu konvertieren sind, angegeben und die Bezeichnungen der MIXe, die diese durchlaufen.

- **Location Updating Request**-Nachricht des Teilnehmers S:
  (MIX-Kaskade im MSC/VLR des Senders für LUP-Request)
  $\mathbf{N_{LUP\text{-}Request}} := c_{S1}(D_{SE1}, c_{S2}(D_{SE2}, c_{S3}(D_{SE3}, N_{VLR}))))$ (siehe *3.2.5.1*)
  $|\mathbf{N_{LUP\text{-}Request}}| = \underline{9188 \text{ Bit}}$
- **Location Updating Accept**-Nachricht an den Teilnehmer S:
  (MIX-Kaskade im MSC/VLR des Senders für LUP-Accept)
  $\mathbf{N_{LUP\text{-}Accept}} := k_{SE1}(t_{Li},k_{SE2}(t_{Li},k_{SE3}(t_{Li}(lup_acc_msg,k_{A1}(t_{Li},k_{A2}(t_{Li},k_{A3}(t_{Li},$
  $s_{HLR}(t_{Li},RAND_2)))),N_{HLR}^*))))$ (siehe *3.2.5.1*)
  $|\mathbf{N_{LUP\text{-}Accept}}| = \underline{1116 \text{ Bit}}$
- **ZE-Setup**-Nachricht des Senders:
  (MIX-Kaskade im MSC/VLR des Senders für ZE-Setup)
  $\mathbf{N_{ZE\text{-}Setup(S)}} := c_{S1}(D_{SE1}, c_{S2}(D_{SE2}, c_{S3}(D_{SE3}, N_{AuC}))))$ (siehe *3.2.5.1*)
  $|\mathbf{N_{ZE\text{-}Setup(S)}}| = \underline{3690 \text{ Bit}}$
- **ZS-Setup**-Nachricht des Senders:
  (MIX-Kaskade im MSC/VLR des Senders für ZS-Setup)

$\mathbf{N_{ZS\text{-}Setup(S)}}$:= $c_{S1}(D_{SS1}, c_{S2}(D_{SS2}, c_{S3}(D_{SS3}, c_{HLR}(t_i, MSISDN_E, N_E))))$ (siehe *3.2.5.1*)

$|\mathbf{N_{ZS\text{-}Setup(S)}}|$ = 2501 Bit

- **ZE-Setup**-Nachricht des Empfängers:
  (MIX-Kaskade im MSC/VLR des Empfängers für ZE-Setup)
  $\mathbf{N_{ZE\text{-}Setup(E)}}$:= $c_{E1}(D_{EE1}, c_{E2}(D_{EE2}, c_{E3}(D_{EE3}, N_{AuC})))$ (siehe *3.2.5.1*)
  $|\mathbf{N_{ZE\text{-}Setup(E)}}|$ = 3690 Bit
- **ZS-Setup**-Nachricht des Empfängers:
  (MIX-Kaskade im MSC/VLR des Empfängers für ZS-Setup)
  $\mathbf{N_{ZS\text{-}Setup(E)}}$:= $c_{E1}(D_{ES1}, c_{E2}(D_{ES2}, c_{E3}(D_{ES3}, N_S)))$ (siehe *3.2.5.1*)
  $|\mathbf{N_{ZS\text{-}Setup(E)}}|$ = 2082 Bit
- **Paging Request**-Nachricht an den Empfänger:
  (MIX-Kaskade im MSC/VLR des Empfängers für Paging Request)
  $\mathbf{N_{Paging\ Request}}$:= IAdr, $k_{E1}(t_i, k_{E2}(t_i, k_{E3}(t_i, k_{H1}(t_i, k_{H2}(t_i, k_{H3}(t_i,$
  $c_E(\text{call_setup}, t_i, A_{MSC/VLR_S}, KZ_{init}))))))$
  $|\mathbf{N_{Paging\ Request}}|$ = 1388 Bit
- **Call Proceeding**-Nachricht an den Sender:
  (MIX-Kaskade im MSC/VLR des Senders für Call Proceeding)
  $\mathbf{N_{Call\ Proceeding(S)}}$:= $k_{SE1}(t_i, k_{SE2}(t_i, k_{SE3}(t_i,$
  $\text{call_pro_msg}, s_{MSC/VLR}(t_i, RAND_2)))$
  $|\mathbf{N_{Call\ Proceeding(S)}}|$ = 808 Bit
- **Call Proceeding**-Nachricht an den Empfänger:
  (MIX-Kaskade im MSC/VLR des Empfängers für Call Proceeding)
  $\mathbf{N_{Call\ Proceeding(E)}}$:= $k_{EE1}(t_i, k_{EE2}(t_i, k_{EE3}(t_i,$
  $\text{call_pro_msg}, s_{MSC/VLR}(t_i, RAND_2), CIC))$
  $|\mathbf{N_{Call\ Proceeding(E)}}|$ = 820 Bit

Im folgenden werden die Datenstrukturen der Signalisierungsnachrichten, die vom MAP- über das MIX- ins MAP-Protokoll zu konvertieren sind, angegeben und die Bezeichnungen der MIXe, die diese durchlaufen.

- **Send Parameter form HLR**-Nachricht an das HLR:
  (MIX-Kaskade im HLR für Send Parameter)
  $\mathbf{N_{AuC}}$:= $c_{A1}(D_{A1}, c_{A2}(D_{A2}, c_{A3}(D_{A3}, s_{MS}(t_{Li}, RAND_1), IMSI, RAND_2)))$
  $|\mathbf{N_{AuC}}|$ = 2082 Bit
- **Authentication Parameter**-Nachricht vom HLR:
  (MIX-Kaskade im HLR für Authentication Parameter)
  $\mathbf{N_{AuP}}$:= $k_{A1}(t_{Li}, k_{A2}(t_{Li}, k_{A3}(t_{Li}, s_{HLR}(t_{Li}, RAND_2))))$
  $|\mathbf{N_{AuP}}|$ = 500 Bit
- **Update Location**-Nachricht an das HLR:
  (MIX-Kaskade im HLR für Update Location)
  $\mathbf{N_{HLR}}^*$:= $c_{H1}(D_{H1}, c_{H2}(D_{H2}, c_{H3}(D_{H3}, N_{HLR})))$ (siehe *3.2.5.4*)
  $|\mathbf{N_{HLR}}^*|$ = 3519 Bit
- **Location Updating Accept**-Nachricht vom HLR:
  (MIX-Kaskade im HLR für Updating Accept)
  $\mathbf{N_{HLR}}^*$:= $k_{H1}(t_{Li}, k_{H2}(t_{Li}, k_{H3}(t_{Li}, \text{lup_acc_msg})))$
  $|\mathbf{N_{HLR}}^*|$ = 308 Bit

- **IAM**-Nachricht an das VLR des Empfängers:
  (MIX-Kaskade im HLR für IAM)
  $\mathbf{N_{IAM}}$:= A_{VLR} , P , k_{H1}(t_i , k_{H2} (t_i , k_{H3} (t_i , N_E) (siehe *3.2.5.4*)
  $|\mathbf{N_{IAM}}|$ = 1102 Bit

Diese Auflistung der zu mixenden Signalisierungsnachrichten verdeutlicht, daß die Anzahl der MIX-Kaskadentypen im GSM aufgrund der verschiedenen Signalisierungsnachrichten deutlich größer ist als im ISDN. Dennoch sollte weiterhin für jeden Nachrichtentyp, der eine MIX-Kaskade durchläuft, ein MIX-Kaskadentyp implementiert werden, da im GSM größter Wert auf kurze Signalisierungsnachrichten, zumindest auf der Funkschnittstelle, gelegt werden muß um die schmalbandigen Signalisierungskanäle nicht unnötig zu belasten. Zählt man die benötigten MIX-Kaskadentypen zusammen, erhält man 13 verschiedene Typen, 2 für die Kommunikation, 6 im MSC und 5 im HLR. Bei der Realisierung des MIX-Protokolls gelten auch im GSM die in *Kapitel 3.1.3.3* getroffenen Aussagen bezüglich ISDN-Realisierung.

3.2.5.4 Signalisierungsnachrichten im CCS7-Protokoll

Das CCS7-Protokoll kommt auch im GSM zwischen den Netzseiten der MSCs der beiden an der Kommunikation beteiligten Teilnehmer und bei den Datenbankabfragen (VLR,HLR) im Fernnetz zum Einsatz. Das CCS7-Signalisiernetz routet Verbindungswünsche in den gewünschten MSC-Bereich. Außerdem wird das CCS7-Netz bei jeder Aktualisierung des Aufenthaltsortes für die Signalisierung zwischen dem MSC,VLR und HLR verwendet. Für die Modifikationen zur Realisierung anonymer Signalisierung bietet sich der Mobile Application Part (MAP) an, der in GSM die entsprechende Funktionalität hat, die im ISDN der ISDN-UP erfüllt. Zu modifizieren ist ausschließlich die Struktur der CCS7-MAP-Signalisierungsnachrichten. Die Grundlagen des CCS7 sind in *Kapitel 2.2.2* beschrieben.

Im folgenden wird der Inhalt der MAP-Nachrichten mit neu hinzugekommenen I.E.´s beschrieben. Die Änderungen der kompletten Datenstrukturen einschließlich der zu entfernenden Informationselemente ist in *Kapitel 3.2.5.5* angegeben.

Die **Send Parameter from HLR**-Nachricht: Die Aufgabe dieser Nachricht ändert sich durch die unbeobachtbaren Zeitscheibenkanäle, der Name wurde jedoch beibehalten. Bisher wurden mit dieser Nachricht die Authentikationsdaten des Teilnehmers beim HLR angefordert, um die Teilnehmerauthentikation durchzuführen. Beim Einsatz von anonymer Signalisierung kann nur das HLR die Teilnehmerauthentisierung vornehmen, damit der MSC/VLR-Bereich nicht in den Besitz der Teilnehmeridentität gelangt. Mit dieser vom Teilnehmer vorbereiteten Nachricht wird die Signatur des Teilnehmers dem HLR verdeckt zur Prüfung gesendet. Das HLR kann die Signatur testen, kennt aber nicht den Aufenthaltsort des Teilnehmers.
Die Send Parameter from HLR-Nachricht enthält folgende Informationen:

- **Send Parameter from HLR**-Nachricht:
  $\mathbf{N_{AuC}}$:= $c_{A1}(D_{A1},c_{A2}(D_{A2},c_{A3}(D_{A3},s_{MS}(t_{Li},RAND_1),IMSI, RAND_2)))$
  mit $\mathbf{D_{A1}}$:= t_{Li}, k_{A1}
  $\mathbf{D_{A2}}$:= t_{Li}, k_{A2}
  $\mathbf{D_{A3}}$:= t_{Li}, k_{A3}, $KKZ_A(Li)$
  $|\mathbf{N_{AuC}}|$ = 2082 Bit

Die **Authentication Parameter-**Nachricht: Die Aufgabe dieser Nachricht ändert sich durch die Einführung unbeobachtbarer Zeitscheibenkanäle ebenfalls. Bisher wurden

mit dieser Nachricht die Authentikationsdaten des Teilnehmers vom HLR gesendet, jetzt erfolgt mit dieser Nachricht die Netz-Teilnehmer-Authentikation. Die Kommunikationsbeziehung zum HLR wird durch die MIXe $M_{A1..3}$ geschützt, so daß ein Angreifer nicht feststellen kann, in welchem MSC/VLR-Bereich sich der Teilnehmer gerade aufhält, dessen Authentikation das HLR vorgenommen hat, vorausgesetzt es existiert stets genügend Traffic bzw. Dummy Traffic. Vor dem MSC/VLR muß der Inhalt der Authentikationsnachricht des HLRs verborgen bleiben, damit auch MSC/VLR und HLR als gemeinsame Angreifer den Aufenthaltsort des Teilnehmers nicht ermitteln können. Die Zuordnung von Anfrage und Antwort erfolgt im MSC/VLR über die Position im Batch des aus Sicht des MSC/VLR ersten verwendeten MIXes.

Die Authentication Parameter-Nachricht enthält folgende Informationen:

- **Authentication Parameter**-Nachricht eines Teilnehmers:
  $\mathbf{N_{AuP}} := k_{A1}(t_{Li} , k_{A2}(t_{Li} , k_{A3}(t_{Li} , s_{HLR} (t_{Li} , RAND_2))))$
  $|\mathbf{N_{AuP}}| = \underline{500 \text{ Bit}}$

Die **Update Location**-Nachricht: Mit dieser Nachricht wird die anonyme Rückadresse {VLR,P} unbeobachtbar im HLR hinterlegt. Diese Nachricht, die vom MSC/VLR über die MIX-Kaskade des HLRs zum HLR gesendet wird, wird vom Teilnehmer zu dessen Schutz vorbereitet und mit der Location Update Request-Nachricht an das MSC/VLR gesendet.

Die Update Location-Nachricht enthält folgende Informationen:

- **Update Location**-Nachricht:
  $\mathbf{N_{HLR}}^* := c_{H1}(D_{H1} , c_{H2}(D_{H2} , c_{H3}(D_{H3} , N_{HLR})))$
  mit $\mathbf{D_{H1}} := t_{Li}, k_{H1}$
  $\mathbf{D_{H2}} := t_{Li}, k_{H2}$
  $\mathbf{D_{H3}} := t_{Li}, k_{H3}, KKZ_{HLR}(Li)$
  $\mathbf{N_{HLR}} := k_{HLRS}(lup_msg,Bv/Bl,t_{Li},IMSI,\{VLR,P\})$
  $\mathbf{\{VLR,P\}} := c_{H3}(k_{H3} , c_{H2}(k_{H2} , c_{H1}(k_{H1} , A_{VLR} , P)))$
  $|\mathbf{N_{HLR}}^*| = \underline{3519 \text{ Bit}}$

Die **Location Updating Accept**-Nachricht: Mit dieser Nachricht wird die Speicherung der anonymen Rückadresse {VLR,P} im HLR bestätigt. Diese Nachricht wird über den unbeobachtbaren Kanal durch die MIX-Kaskade des HLRs, der mit der Update Location-Nachricht aufgebaut wurde, an das MSC/VLR gesendet und von dort an den Teilnehmer weitergeleitet.

Die Location Updating Accept-Nachricht enthält folgende Informationen:

- **Location Updating Accept**-Nachricht:
  $\mathbf{N_{HLR}}^* := k_{H1}(t_{Li} , k_{H2} (t_{Li} , k_{H3} (t_{Li} , lup_acc_msg)))$
  $|\mathbf{N_{HLR}}^*| = \underline{308 \text{ Bit}}$

Die **IAM**-Nachricht: Diese Nachricht wird vom MSC/VLR des Senders direkt zum HLR des Empfängers gesendet. Dort wird die Nachricht entschlüsselt und der Empfänger ermittelt. Das HLR sendet anschließend die Nachricht N_E mit der zur $MSISDN_E$ gespeicherten anonymen Rückadresse {VLR,P} über die MIX-Kaskade des HLRs zum in der anonymen Rückadresse enthaltenen VLR des Empfängers. Dabei wird noch kein Nutzkanal belegt.

Die IAM-Nachricht enthält folgende Informationen:

- **IAM**-Nachricht auf dem Weg zum HLR:
  $\mathbf{N_{IAM}} := c_{HLR}(t_i , MSISDN_E , N_E)$

$\mathbf{N_E}$:= c_E (call_setup_msg , t_i , A_{MSC/VLR_S} , KZ_{init})

$|\mathbf{N_{IAM}}|$ = 878 Bit

- **IAM**-Nachricht auf dem Weg zum VLR:

  $\mathbf{N_{IAM}}$:= A_{VLR} , P , k_{H1}(t_i , k_{H2} (t_i , k_{H3} (t_i , N_E)

  $\mathbf{N_E}$:= c_E (call_setup_msg , t_i , A_{MSC/VLR_S} , KZ_{init})

  $|\mathbf{N_{IAM}}|$ = 1102 Bit

Die **Paging**-Nachricht: Mit dieser Nachricht wird der Verbindungswunsch vom VLR des Empfängers zum MSC des Empfängers weitergeleitet. Dort durchläuft die Nachricht unter Verwendung der anonymen Rückadresse {LAI,IAdr} aus dem VLR die MIX-Kaskade des MSCs.
Die Paging-Nachricht enthält folgende Informationen:

- **Paging**-Nachricht auf dem Weg zum HLR:

  $\mathbf{N_{Paging}}$:= $c_{E3}(k_{E3},c_{E2}(k_{E2},c_{E1}(k_{E1},LAI,IAdr))),t_i,k_{H1}(t_i,k_{H2}(t_i,k_{H3}(t_i,N_E)))$

  $\mathbf{N_E}$:= c_E (call_setup_msg , t_i , A_{MSC/VLR_S} , KZ_{init})

  $|\mathbf{N_{Paging}}|$ = 2802 Bit

Die **Process Access**- und die **Complete Call**-Nachricht unterscheiden sich im Nachrichteninhalt nicht von der **Send Information from HLR-** und der **Authentication Information**-Nachricht. Sie heißen lediglich auf der MSC-VLR-Schnittstelle anders, als auf der VLR-HLR-Schnittstelle. Auf die detaillierte Angabe des Nachrichteninhaltes dieser Nachrichten kann deshalb verzichtet werden.

Die **ACM**-Nachricht: Mit dieser Nachricht wird der Nutzkanal im Fernnetz belegt und den Teilnehmern der Kanalidentifikator CIC mitgeteilt. Außerdem erfährt der Sender, daß sein Verbindungswunsch zum Empfänger vermittelt wurde und dessen Telefon jetzt klingelt.
Die ACM-Nachricht enthält folgende Informationen:

- **ACM**-Nachricht:

  $\mathbf{N_{ACM}}$:= acm_msg , t_i , A_{MSC/VLR_S} , $KKZ_S(i)$, A_{MSC/VLR_E} , CIC

  $|\mathbf{N_{ACM}}|$ = 106 Bit

Die **ANM**-Nachricht: Mit dieser Nachricht wird bereits im Datenkanal das Zustandekommen der Kommunikation dem Sender angezeigt, d.h. der Empfänger hat den Hörer abgenommen und ist zur Kommunikation bereit.
Die ANM-Nachricht enthält folgende Informationen:

- **ANM**-Nachricht:

  $\mathbf{N_{ANM}}$:= connect_msg , t_i , A_{MSC/VLR_S} , $KKZ_S(i)$, A_{MSC/VLR_E} , CIC

  $|\mathbf{N_{ANM}}|$ = 106 Bit

Die **REL**-Nachricht: Mit dieser Nachricht zeigt ein Teilnehmer das Ende der Kommunikationsbeziehung an. Diese Nachricht wird aus Effizienzgründen noch über den Datenkanal übertragen.
Die REL-Nachricht enthält folgende Informationen:

- **REL**-Nachricht:

  $\mathbf{N_{REL}}$:= disconnect_msg , t_i , A_{MSC/VLR_S} , $KKZ_S(i)$, A_{MSC/VLR_E} , CIC

  $|\mathbf{N_{REL}}|$ = 106 Bit

Die **RLC**-Nachricht ändert sich durch die Einführung anonymer Signalisierung auch im GSM nicht. Mit dieser Nachricht werden Nutzkanäle zwischen den MSCs abgebaut.

Ausgelöst wird die RLC- von der REL-Nachricht und die Verbindung wird auf jedem Link separat abgebaut und der Nutzkanal freigegeben.

3.2.5.5 Änderungen der Datenstrukturen im CCS7-Protokoll

In diesem Abschnitt werden die Änderungen der Datenstrukturen im CCS7-Protokoll beschrieben. Zu beachten ist dabei, daß zwischen dem MSC und VLR sowie zwischen dem MSC und HLR das MAP-Protokoll zum Einsatz kommt und das zwischen den MSCs der ISDN-UP bzw. TUP genutzt wird, wobei in dieser Arbeit von der Verwendung des ISDN-UPs ausgegangen werden soll. Nachfolgend werden zuerst die MAP-Signalisierungsnachrichten erklärt.

Die Codierung der MAP-Nachrichtentypen wird in [GSM_09.02] nicht definiert, so daß ein Systementwickler deren Codierungen frei festlegen kann. Gleiches gilt für die Codierungen der I.E.´s, so daß hier auf eine Beispielcodierung verzichtet werden kann.

Abb. 3.2.5.5.1. zeigt den Inhalt der Send Information from HLR-Nachricht. Diese Nachricht wird auf den MAP_Send_Identification Service Request abgebildet. Entfernt wurden die I.E.´s Invoke ID (16 Bit) und TMSI (32 Bit). Neu hinzugekommen ist das I.E. Authentication Information, welches die verschlüsselten Daten der N_{AuC} enthält.

Parametername	**enthaltene Information**
- Authentication Information (2082 Bit)	Nachricht an das HLR mit Authentikations-informationen des Teilnehmers

Abb. 3.2.5.5.1: Aufbau der Send Information from HLR-Nachricht

Abb. 3.2.5.5.2 zeigt den Inhalt der Authentication Parameter-Nachricht. Diese Nachricht wird auf den MAP_Send_Identification Service Response abgebildet. Entfernt wurden die I.E.´s Invoke ID (16 Bit), IMSI (60 Bit), Authentication Set (224 Bit) und User Error (8 Bit). Neu hinzugekommen ist das I.E. Authentication Result, welches die Daten der Netz-Teilnehmer-Authentikation des HLRs enthält.

Parametername	**enthaltene Information**
- Authentication Result (500 Bit)	Authentikation des HLRs

Abb. 3.2.5.5.2: Aufbau der Authentication Parameter-Nachricht

Abb. 3.2.5.5.3 zeigt den Inhalt der Update Location-Nachricht. Diese Nachricht wird auf den MAP_Update Location Service Request abgebildet. Entfernt wurden die I.E.´s Invoke ID (16 Bit), IMSI (60 Bit), MSC Address (14 Bit) und VLR-Number (14 Bit). Neu hinzugekommen ist das I.E. Location Information, welches die Nachricht N_{HLR} mit der anonymen Rückadresse {VLR,P} für das HLR enthält.

Parametername	**enthaltene Information**
- Location Information (3519 Bit)	Nachricht an das HLR mit verdecktem VLR-Aufenthaltsort des Teilnehmers

Abb. 3.2.5.5.3: Aufbau der Update Location-Nachricht

Abb. 3.2.5.5.4 zeigt den Inhalt der Updating Location Accept-Nachricht. Diese Nachricht wird auf den MAP_Update_Location Service Response abgebildet. Entfernt wurden die I.E.´s Invoke ID (16 Bit), HLR Number (14 Bit) und User Error (8 Bit). Neu hinzugekommen ist das I.E. Location Accept, welches den Empfang der letzten Nachricht und die Speicherung der Lokalisierungsinformationen bestätigt.

Parametername	**enthaltene Information**
- Location Accept (308 Bit)	Quittung der erfolgten Speicherung

Abb. 3.2.5.5.4: Aufbau der Updating Location Accept-Nachricht

Abb. 3.2.5.5.5 zeigt den Inhalt der Paging-Nachricht. Diese Nachricht wird auf den MAP_Page Service Request abgebildet. Entfernt wurden die I.E.´s Invoke ID (16 Bit), IMSI (60 Bit), Stored LAI (48 Bit) und TMSI (32 Bit). Neu hinzugekommen ist das I.E. Call Information, welches die auszusendende Nachricht N_E an Empfänger enthält.

Parametername	**enthaltene Information**
- Call Information (2802 Bit)	Verbindungswunschnachricht an den User

Abb. 3.2.5.5.5: Aufbau der Paging-Nachricht

Abb. 3.2.5.5.6 zeigt den Inhalt der Process Access-Nachricht. Diese Nachricht wird auf den MAP_Process_Access_Request Service Request abgebildet. Entfernt wurden die I.E.´s Invoke ID (16 Bit), Current LAI (48 Bit), TMSI (32 Bit), Cksn (8 Bit), IMSI (60 Bit) und IMEI (64 Bit). Neu hinzugekommen ist das I.E. Access Information, welches die Authentikationsdaten enthält.

Parametername	**enthaltene Information**
- CM Service type (8 Bit)	kennzeichnet Service Typ (Notruf,MOC,...)
- Access Connection Status (8 Bit)	kennzeichnet Status (Authentikation, Verschlüsselungsmodus,...)
- Access Information (2282 Bit)	Authentikationsdaten für das HLR

Abb. 3.2.5.5.6: Aufbau der Process Access-Nachricht

Abb. 3.2.5.5.7 zeigt den Inhalt der Complete Call-Nachricht. Diese Nachricht wird auf den MAP_Process_Access_Request Service Response abgebildet. Entfernt wurden die I.E.´s Invoke ID (16 Bit), IMSI (60 Bit), IMEI (64 Bit), MSISDN (60 Bit) und User Error (8 Bit). Neu hinzugekommen ist das I.E. Authentication Information, welches das Ergebnis der Authentikation enthält..

Parametername	**enthaltene Information**
- CM Service type (8 Bit)	*bereits erklärt*
- Access Connection Status (8 Bit)	*bereits erklärt*
- Call Information (201 Bit)	Authentikationsergebnis vom HLR

Abb. 3.2.5.5.7: Aufbau der Complete Call-Nachricht

Die Länge der I.E.´s Invoke ID, User Error, CM Service type und Access Connection Status wurde nicht explizit festgelegt, deshalb wird die Länge für diese Arbeit aufgrund der Aufgaben der I.E.´s abgeschätzt und zur weiteren Berechnung genutzt.

Die in GSM zwischen den MSCs verwendeten Signalisierungsnachrichten des ISDN-UPs (IAM,ACM,ANM,REL,RLC) beinhalten die gleichen I.E.´s, wie in der ISDN-Realisierung. Lediglich das I.E. User to User Information der IAM muß in der GSM-Lösung 1102 Bit lang gewählt werden, um die notwendigen Informationen des Verbindungswunsches übertragen zu können. Außerdem kann die IAM nicht direkt an das HLR des Empfängers gesendet werden, da diese Nachricht des ISDN-UPs nur zwischen MSCs verwendet wird. Deshalb muß diese Nachricht in dem GMSC, das die Anfrage beim HLR steuert, in das MAP-Protokoll konvertiert werden. Dann wird die MAP-Nachricht an das HLR gesendet und dort in das MIX-Protokoll konvertiert. Nach der MIX-Kaskade des HLRs wird die Nachricht wieder im MAP-Protokoll codiert und die Anfrage beim HLR ausgelöst. Die Antwort nimmt denselben Weg bis zum GMSC und wird dort in die ISDN-UP-Signalisierungsnachricht IAM zurückgewandelt und anschließend mit den neuen Zielinformationen zum VLR des Empfängers geroutet. Dieses Realisierungsdetail wird in den Darstellung zur Vereinfachung nicht angegeben.

3.3 Interworking bei unbeobachtbarer Signalisierung

Beim Interworking sind grundsätzlich zwei Fälle zu unterscheiden. Falls die beteiligten Kommunikationsnetze beide das Verfahren zur anonymen Signalisierung implementiert haben, erfolgen die Konvertierungen wie bisher an den entsprechenden Netzübergangsvermittlungsstellen. Hinzukommen durch die Einführung der anonymen Signalisierung einerseits einige Informationselemente bei den Signalisierungsnachrichten, deren Konvertierung keine Probleme bereiten sollte aber andererseits unter Umständen auch Synchronisationsprobleme. Für den Teilnehmer entsteht dadurch allerdings maximal eine größere Verzögerung, da die Nachrichten in den Netzübergangsvermittlungsstellen auf die jeweils nächste Zeitscheibe des anderen Netzes warten müssen, in der sie weitervermittelt werden können.

Der Netzübergang zu einem Kommunikationsnetz, in dem die anonyme Signalisierung nicht implementiert ist, gestaltet sich schwieriger. Verfügt nur die Ortsvermittlungsstelle des Sender über MIX-Funktionalität, so muß der letzte MIX der letzten erweiterten Ortsvermittlungsstelle die Rolle eines Umsetzers übernehmen. Dem letzten MIX werden dann die Daten, bis auf die Calling Party Number usw. die den Sender identifizieren würden, signalisiert, die nach dem bisherigen Schema für einen Verbindungsaufbau nötig sind. Außerdem erhält der MIX dann die Informationen zur Verknüpfung des normalen Kommunikationskanals mit den Zeitscheibenkanälen des Senders. Die Unbeobachtbarkeit des Senders wird dadurch nicht eingeschränkt und der Empfänger bleibt genauso beobachtbar, wie bisher. Verfügt dagegen nur die Ortsvermitlungsstelle des Empfängers über eine MIX-Kaskade, so ist in erster Linie die Frage der geeigneten Adressierung interessant. Wird wie in heutigen Systemen die Rufnummer des Empfängers direkt signalisiert ist natürlich auch die Unbeobachtbarkeit des Empfängers verloren. Daher sollte man für solche Verbindungen implizite Adressen vorsehen, dieser Fall soll allerdings nicht weiter betrachtet werden.

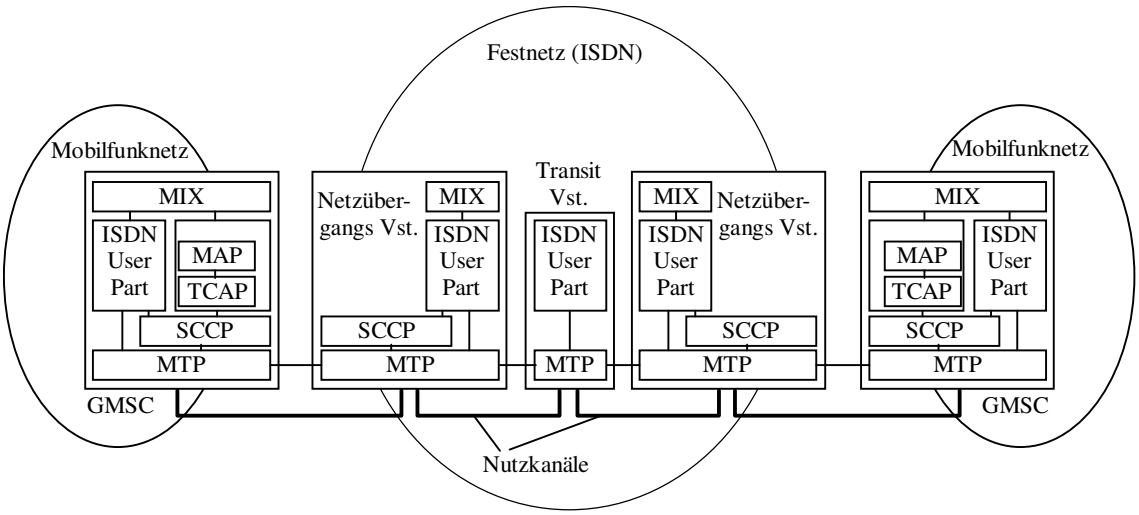


Abb. 3.3.1: Interworking zwischen Netzen mit anonymer Signalisierung

Abb. 3.3.1 zeigt das Interworking zwischen verschiedenen (z.B. nationalen) Mobilfunknetzen (GSM) über ein Festnetz (ISDN) für den Fall, daß die anonyme Signalisierung in allen Netzen möglich ist. Die gegenüber den bisherigen Netzen hinzugekommene MIX-Funktionalität setzt auf die Anwenderteile ISDN-UP und MAP auf. In den Transitvermittlungsstellen ist keine MIX-Funktionalität implementiert. Da stets nur die MIX-Kaskaden in den lokalen Vermittlungsstellen der beiden Kommunikationspartner genutzt werden, sind die MIX-Kaskaden in den Netzübergangsvermittlungsstellen zwar vorhanden (falls an diese Netzübergangsvermittlungsstellen Nutzer angeschlossen sind), werden jedoch in dem in *Abb. 3.3.1* dargestellten Beispiel nicht genutzt.

4. Effizienzbetrachtungen

4.1 Voraussetzungen zur Leistungsbewertung

4.1.1 Berechnung der Länge einer MIX-Eingabenachricht

Um Effizienzbetrachtungen durchführen zu können, muß als erstes die Länge der modifizierten Signalisierungsnachrichten berechnet werden. Dazu sind einige Festlegungen bezüglich der eingesetzten Kryptosysteme nötig. Bei der im *Kapitel 3* beschriebenen Realisierung anonymer Signalisierung wird symmetrische und asymmetrische Kryptographie eingesetzt. Dabei soll es sich bei dem symmetrischen Verschlüsselungsalgorithmus um eine Stromchiffre mit 128 Bit Schlüssellänge (s_{sym}) und bei dem asymmetrischen System um eines Blockchiffre mit einer Blocklänge von 660 Bit (b_{asym}) handeln. Außerdem wird, um Übertragungskapazität zu sparen, hybrid verschlüsselt, d.h. es wird von der zu verschlüsselnden Nachricht stets ein möglichst großer Teil N* des Klartextes N in den ersten, asymmetrisch verschlüsselten Block hineingezogen und außerdem ein symmetrischer Schlüssel k_{SE} ausgetauscht, mit dem der Rest N** effizient symmetrisch verschlüsselt werden kann, d.h. es gilt:

$$c_E^*(N) := \begin{cases} c_E(N) & \text{falls } |N| \le b_{asym} \\ c_E(k_{SE}, N^*) \,,\, k_{SE}(N^{**}) & \text{sonst.} \end{cases}$$

Dabei ist zu beachten, daß bei Nachrichten, die von MIXen asymmetrisch entschlüsselt und anschließend vor Verlassen des MIXes nicht symmetrisch verschlüsselt werden, der asymmetrische Algorithmus indeterministisch verschlüsseln muß, damit ein Angreifer diesen MIX nicht durch erneutes Verschlüsseln mit dem öffentlichen Schlüssel des MIXes und Vergleichen mit den Eingangsnachrichten überbrücken kann. Für den Indeterminismus werden zufällige 128 Bits in jeden asymmetrischen Block codiert. Diese kann man als symmetrischen Schlüssel der hybriden Verschlüsselung verwenden. Eine ausführlichere Beschreibung erfolgt in [PfPW_89].

Damit ergibt sich für die Länge einer hybrid verschlüsselten Nachricht:

$$|c_E^*(N)| = \max(b_{asym} \,,\, |N| + s_{sym})$$

Für die Länge einer MIX-Eingabenachricht gilt gemäß *Kapitel 2.4.2*:

$$|N_1| \le |D_1| + |N_2|$$

$$|N_i| = \max(b_{asym} \,,\, |D_i| + |N_{i+1}| + s_{sym}) \qquad \text{für } i := 2 \,..\, m.$$

Da die Nachricht N_{i+1} für $i<m$ mindestens aus einem asymmetrisch verschlüsselten Block besteht, gilt stets $|N_{i+1}| \ge b_{asym}$. Deshalb folgt nach Auflösung der obigen rekursiven Gleichungen:

$$|N_1| = \sum_{j=1}^{m-1} |D_j| + (m-2) \cdot s_{sym} + \max(b_{asym} \,,\, |D_m| + |N_{m+1}| + s_{sym})$$

Diese Gleichung wird im folgenden zur Berechnung der Länge von MIX-Eingabenachrichten verwendet. Werden allerdings Signalisierungsnachrichten betrachtet, so muß zu

der Länge der MIX-Eingabenachricht noch die Länge der anderen Signalisierungsparameter addiert werden.

4.1.2 Länge der Parameter in den verwendeten Kommunikationsnetzen

In diesem Abschnitt wird die Länge aller Parameter angegeben, die zur Berechnung der Länge von MIX-Eingabenachrichten notwendig sind. Die Länge der anderen Signalisierungsparameter wird jeweils bei der Codierung der Signalisierungsnachrichten aufgeführt. Die Größe der ISDN-Parameter wurde [BGGH_95] und die Größe der GSM-Parameter [GSM_04.08, GSM_09.02 und GSM_09.10] entnommen. Allerdings wurden für die IMSI (24-64 Bit) und die MSISDN (8-72 Bit) Durchschnittswerte von 60 Bit angenommen.

Parametername	Abkürzung	Länge
• allgemeine Parameter:		
Zeitscheibennummer	t	30 Bit
Kanalkennzeichen	KKZ	28 Bit
Initialwert des Kanalkennzeichens	KZ_{init}	128 Bit
Block des asymmetrischen Systems	b_{asym}	660 Bit
Schlüssel des symmetrischen Systems	s_{sym}	128 Bit
digitale Signatur	$s_{MS}(N)$	200 Bit
Nutzkanalidentifikator im Fernnetz	CIC	12 Bit
Anzahl der MIXe	m	10 Stück
bedeutungsvoll/bedeutungslos Kennzeichen	bv/bl	1 Bit
• ISDN-Parameter:		
Adresse einer Ortsvermittlungsstelle	A_{LE}	14 Bit
• GSM-Parameter:		
International Mobile Subscriber Identity	IMSI	60 Bit
International Mobile Equipment Identity	IMEI	64 Bit
Temporary Mobile Subscriber Identity	TMSI	32 Bit
Mobile Subscriber ISDN-Number	MSISDN	60 Bit
Location Area Identifikation	LAI	48 Bit
Pseudonym	P	128 Bit
Implizite Adresse	IAdr	128 Bit

Abb. 4.1.2.1: Länge der Parameter in den Kommunikationssystemen

4.2 Leistungsbewertung für das ISDN-Festnetz

4.2.1 Länge der ISDN-Signalisierungsnachrichten im Vergleich

Im folgenden sollen die Längen der ISDN-Signalisierungsnachrichten vor und nach der Modifikation gegenübergestellt werden. Zuvor wird beispielhaft die Länge zweier MIX-Eingabenachrichten mit der allgemeinen Formel aus *Abschnitt 4.1.1* berechnet.

- **ZE-Setup**-Nachricht des Senders:
  Nachrichteninhalt:
  $\mathbf{N_{ZE\text{-}Setup(S)}} := k_{S1}(D_{SE1}, c_{S2}(D_{SE2}, c_{S3}(D_{SE3}))))$
  mit $\mathbf{D_{SE1}} := t_i$, $\mathbf{D_{SE2}} := t_i, k_{SE2}$, $\mathbf{D_{SE3}} := t_i, k_{SE3}, KKZ_S(i)$
  Nachrichtenlänge:

$|\mathbf{D_{SEm}}|$ = 30 Bit + 128 Bit + 28 Bit = 186 Bit
$|\mathbf{D_{SEi}}|$ = 30 Bit + 128 Bit = 158 Bit für i = 2 .. m-1
$|\mathbf{D_{SE1}}|$ = 30 Bit
$|\mathbf{N_{m+1}}|$ = 0 Bit
$|\mathbf{N_m}|$ = 186[28] Bit $\Rightarrow$660 Bit (da < b_{asym})
$|\mathbf{N_{ZE\text{-}Setup(S)}}|$ = $(m-1)\cdot$ (30 Bit + 128 Bit) - 128 Bit[29] + 660 Bit = <u>1954 Bit</u>

- **<u>ZS-Setup</u>**-<u>Nachricht des Senders:</u>
  Nachrichteninhalt:
  $\mathbf{N_{ZS\text{-}Setup(S)}}$:= k_{S1}(D_{SS1} , c_{S2}(D_{SS2} , c_{S3}(D_{SS3} , N_E)))
  mit $\mathbf{D_{SS1}}$:= t_i , $\mathbf{D_{SS2}}$:= t_i, k_{SS2} , $\mathbf{D_{SS3}}$:= t_i, k_{SS3}, A_{LE_E} , $KKZ_E(i)$, Bv/Bl
  $\mathbf{N_E}$:= c_E (call_setup_msg , t_i , A_{LE_S} , KZ_{init})
  Nachrichtenlänge:
  $|\mathbf{D_{SSm}}|$ = 30 Bit + 128 Bit + 14 Bit + 28 Bit + 1 Bit = 201 Bit
  $|\mathbf{D_{SSi}}|$ = 30 Bit + 128 Bit = 158 Bit für i = 2 .. m-1
  $|\mathbf{D_{SS1}}|$ = 30 Bit
  $|\mathbf{N_{m+1}}|$ = 8 Bit + 30 Bit + 14 Bit + 128 Bit = 180 Bit $\Rightarrow$660 Bit (da < b_{asym})
  $|\mathbf{N_m}|$ = $|D_m|$ + $|N_{m+1}|$ + s_{sym} = 201 Bit + 660 Bit = 861 Bit
  $|\mathbf{N_{ZS\text{-}Setup(S)}}|$ = $(m-1)\cdot$ (30 Bit + 128 Bit) - 128 Bit + 861 Bit = <u>2155 Bit</u>

Analog kann die Länge aller MIX-Eingabenachrichten bzw. der kompletten Signalisierungsnachrichten berechnet werden. *Abb. 4.2.1.1* zeigt eine Gegenüberstellung aller modifizierten Signalisierungsnachrichten. Dort wird die Länge der Signalisierungsnachrichten bisher, mit 5 und mit 10 eingesetzten MIXen angegeben. In der letzten Spalte wird zum Vergleich die Länge der durch den MIX-Einsatz neu hinzugekommenen I.E.´s angegeben. Die bisherige Länge der DSS1-Signalisierungsnachrichten wurde aus [ETS_300_403-1] ermittelt, wobei I.E.´s mit einer variablen Länge innerhalb bestimmter Grenzen (z.B. HLC 16 - 40 Bit) mit ihrem Mittelwert und I.E.´s mit variabler Länge (z.B. Network Specific Facility >16 Bit) mit dem Doppelten (hier 32 Bit) angenommen wurden. Außerdem wurden auch optionale I.E.´s als vorhanden zur Längenberechnung als vorhanden eingestuft, so daß die Performance in der Praxis besser sein sollte, als im Rechenbeispiel beschrieben. Die bisherige Länge der ISDN-UP-Signalisierungsnachrichten wurde aus [ITU_Q.763] entnommen.

	bisherige Länge	Länge mit 5 MIXen	Länge mit 10 MIXen	Länge der neuen I.E.´s bei 10 MIXen
Setup	1084 Bit	—	—	—
Setup Acknowledge	204 Bit	—	—	—
ZE-Setup	—	1532 Bit	2322 Bit	1954 Bit
ZS-Setup	—	1733 Bit	2523 Bit	2155 Bit
Anonymous	—	1040 Bit	1040 Bit	672 Bit

[28] Da ohnehin ein symmetrischer Schlüssel verteilt wird, existiert s_{sym} nicht extra, da dieser Schlüssel für die hybride Verschlüsselung genutzt werden kann.
[29] Da für den ersten MIX im ISDN schon ein symmetrischer Schlüssel k_{S1} ausgetauscht wurde.

Setup				
Alerting	296 Bit	484 Bit	632 Bit	334 Bit
Call Proceeding	296 Bit	—	—	—
Connect	404 Bit	556 Bit	706 Bit	334 Bit
Connect Acknowledge	36 Bit	—	—	—
Disconnect	204 Bit	392 Bit	542 Bit	334 Bit
Information	432 Bit	—	—	—
Progress	296 Bit	—	—	—
Release	180 Bit	—	—	—
Release Complete	180 Bit	—	—	—
IAM	976 Bit	1166 Bit	1166 Bit	674 Bit
ACM	1076 Bit	470 Bit	470 Bit	106 Bit
ANM	1216 Bit	478 Bit	478 Bit	106 Bit
REL	912 Bit	374 Bit	374 Bit	106 Bit

Abb. 4.2.1.1: Länge der modifizierten ISDN-Nachrichten im Vergleich

4.2.2 Minimale Dauer des Systemtaktes

Um Unbeobachtbarkeit des physischen Sendens zu erreichen, mußte die Taktung des Kommunikationssystems eingeführt werden, wobei jeder Teilnehmer für jeden Systemtakt und jeden zur Verfügung stehenden Nutzkanal (im ISDN zwei 64 kbps Kanäle) eine ZE- und eine ZS-Setup-Nachricht signalisieren muß. Außerdem müssen auf dem 16 kbps Signalisierungskanal von ISDN die Verbindungswunschnachrichten Anonymous Setup an alle Teilnehmer einer Ortsvermittlungsstelle verteilt werden. Da es sich jedoch bei dem Signalisierungskanal um einen Vollduplexkanal handelt, hat die Verteilung der Verbindungswünsche keinen Einfluß auf die Größe der Zeitscheibe. Da ein Teil der 16 kbps des Signalisierungskanals zur Sicherung der Daten, für einige schmalbandige Dienste und weitere I.E´s der Signalisierungsnachrichten benötigt wird, soll im folgenden lediglich von einer verfügbaren Bandbreite von 12 kbps für die, durch den MIX-Einsatz, neu hinzukommenden I.E.´s in beiden Richtungen ausgegangen werden.

Ein Netzabschluß muß also in der Lage sein, über seinen Signalisierungskanal in jedem Systemtakt $2 \cdot (|N_{ZE\text{-}Setup}| + |N_{ZS\text{-}Setup}|)$ Bit zu übertragen, d.h. es gilt:

$$z \geq \frac{2 \cdot \left(\left| N_{ZE-Setup} \right| + \left| N_{ZS-Setup} \right| \right)}{12 kbps}$$

Bei einem Einsatz von 10 MIXen pro Kaskade erhält man:

$$z \geq \frac{2 \cdot (1954 Bit + 2155 Bit)}{12000 \, Bit/s} = 0{,}6848 s$$

In der Realsierung könnte man demzufolge den Systemtakt z.B. auf 0,7 Sekunden festlegen. Verwendet man dagegen nur 5 MIXe in jeder Kaskade erhält man nach obiger Formel z≥0,4215s. Die Einführung eines Taktes von 0,7 s (bei 10 MIXen) bedeutet für den Teilnehmer, daß er nur zum Beginn jedes Taktes Verbindungswünsche absenden kann, im Mittel also 0,35 s warten muß. In *Abb. 4.2.2.1* ist die Abhängigkeit der minimalen Zeitscheibe von der Anzahl der verwendeten MIXe dargestellt. Die Verwendung von nur einem MIX pro Kaskade wäre in der Praxis unsinnig, da man diesem vollständig vertrauen müßte. Diese Darstellung soll verdeutlichen, in welchem Maße der Aufwand, bezogen auf die minimal mögliche Zeitscheibenlänge, bei der Erhöhung der MIX-Anzahl pro Kaskade steigt.

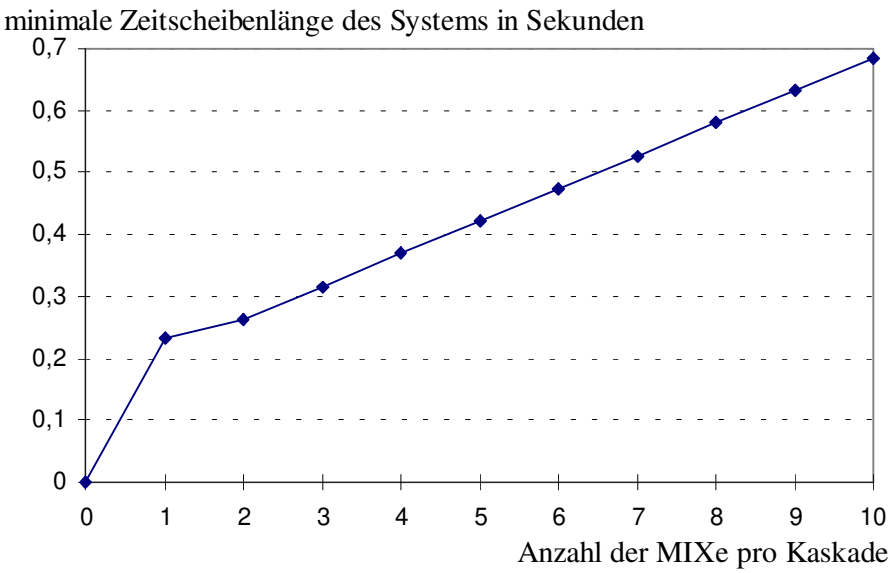


Abb. 4.2.2.1: Abhängigkeit der Zeitscheibenlänge von der MIX-Anzahl

4.2.3 Maximale Anzahl der von einer MIX-Kaskade bedienbaren Netzabschlüsse

Die maximale Anzahl von einer Ortsvermittlungsstelle bedienbarer Teilnehmer wird im wesentlichen durch die Verteilung der Verbindungswunschnachrichten an alle angeschlossenen Netzabschlüsse begrenzt. Den größten Einfluß hat dabei die Verkehrsstatistik, d.h. wieviele Verbindungswünsche startet ein Teilnehmer und wieviele erreichen ihn. Für die Beispielrechnung sollen hier die Werte aus [PfPW_89] verwendet werden. Dort wird von einer maximalen Ankunftsrate von 12 Verbindungswunschen pro Teilnehmer und Stunde (λ =1/300 /s) in Stoßzeiten ausgegangen. Dieser Wert ist bewußt sehr hoch gewählt, in der Literatur findet man beispielsweise durchschnittliche Werte von 2 pro Stunde (in [PoMG_95]) bis 0,8 pro Stunde (in [FuBr_94]. Außerdem ist für die Realisierung von anonymer Signalisierung nur die Rate ankommender Verbindungswünsche interessant.

Jede Anonymous Setup-Nachricht hat im ISDN eine Länge von 1040 Bit, unabhängig von der Anzahl der verwendeten MIXe. Es können maximal $\mu := b/N_{\text{Anonymous Setup}}$ Verbindungswunschnachrichten pro Sekunde verteilt werden. Geht man von b = 12 kbps aus so erhält man $\mu = 11{,}54$ /s. In [PfPW_89] wurde die Gleichung zur Berechnung der Zeit T_V, die ein Verbindungswunsch im Mittel benötigt, um bei den Netzabschlüssen einzutreffen, aus [Klei_75] entnommen, diese soll auch in dieser Arbeit verwendet werden:

$$T_V = \frac{2 \cdot \mu - n \cdot \lambda}{2 \cdot \mu \cdot (\mu - n \cdot \lambda)}$$

Daraus ergibt sich für n:

$$n = \frac{\mu}{\lambda} \cdot \frac{\mu \cdot T_v \cdot -1}{\mu \cdot T_v - 0{,}5}$$

Für $T_v \leq 0{,}5s$ erhält man somit $n \leq 3133$ Teilnehmer pro Ortsvermittlungsstelle. Geht man von nur 5 Verbindungswünschen pro Teilnehmer und Stunde (λ=1/720 /s) in Stoßzeiten aus, könnte man bereits 7520 Teilnehmer an jede Ortsvermittlungstelle und deren MIX-Kaskade anschließen. In *Abb. 4.2.3.1* ist dieser Zusammenhang zwischen der Verkehrsstatistik (Anzahl der Verbindungswünsche in Stoßzeiten) und der damit maximal möglichen Anzahl der Teilnehmer dargestellt, die an eine Ortsvermittlungstelle angeschlossen werden können und damit einer Anonymitätsgruppe angehören.

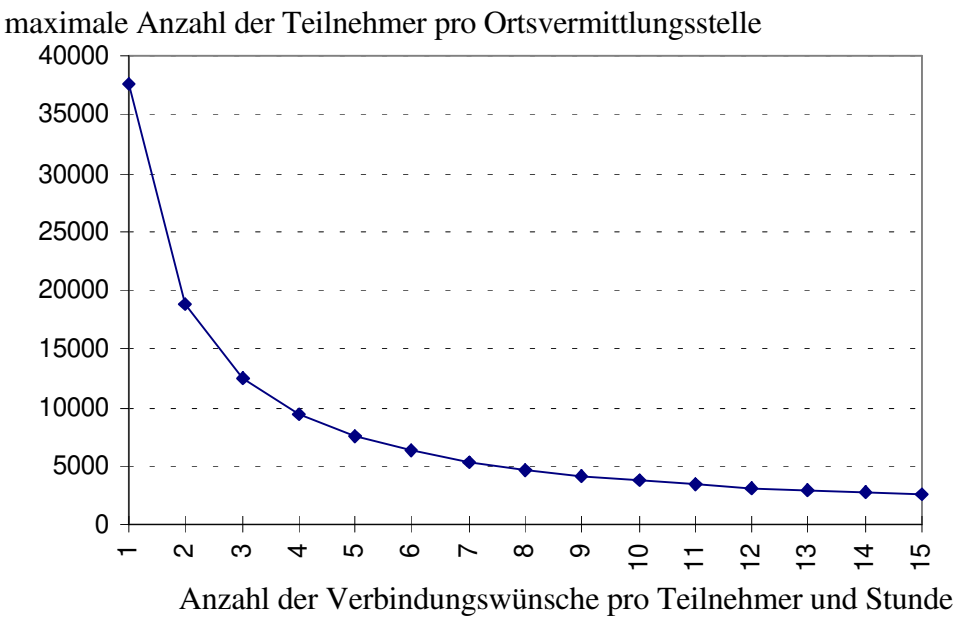


Abb. 4.2.3.1: Abhängigkeit der Teilnehmeranzahl von der Verbindungswunschrate

4.2.4 Berechnungsaufwand der Netzabschlüsse und MIXe

Für die Netzabschlüsse besteht der zusätzliche Berechnungsaufwand hauptsächlich aus dem Anwenden kryptographischer Verfahren, wie dem Ver- und Entschlüsseln von Nachrichten, den Signieren und Testen von Nachrichten und dem Vorbereiten der MIX-Nachrichten. Da aber die Verschlüsselungsraten der symmetrischen und asymmetrischen Verfahren deutlich über der Übertragungsrate von 12 kbps im Signalisierungskanal bzw. 2*64 kbps im Nutzkanal liegen, stellen diese Verfahren kein Performanceproblem dar. In der Literatur [Bras_88] findet man[30] für gute Hardwareimplementierungen des symmetrischen Kryptoverfahrens DES Ver- und Entschlüsselungsraten von 20 Mbps. Für das asymmetrische Verfahren RSA wird in [Sedl_88][31] eine Hardwareimplementierung mit einer Ver- und Entschlüsselungsgeschwindigkeit von ca. 200 kbps bei einer Moduluslänge von 660 Bit angegeben.

[30] nach [PfPW_89]
[31] nach [PfPW_89]

Der Berechnungsaufwand der MIXe besteht im wesentlichen aus dem Ver- und Entschlüsseln der MIX-Nachrichten, dem Puffern und Umsortieren der Nachrichten, sowie dem Testen der Zeitstempel. Dies betrifft in jedem Systemtakt 2 Signalisierungseingabeschübe und 2 Dateneingabeschübe mit je höchstens 3133 Nachrichten (siehe *Abschnitt 4.2.3*). Setzt man in jedem MIX spezielle Hardware (für massiv-parallele Abarbeitung) ein, ist es nach [PfPW_89] möglich, Verarbeitungszeiten (v) von weniger als 0,01 s pro MIX zu erreichen. Generell sollten verschiedene Nachrichten bzw. Nachrichten innerhalb einer MIX-Kaskade pipelineartig verarbeitet werden, d.h. die Zeitscheiben bei den verschiedenen MIXen zu unterschiedlichen, definierten Zeitpunkten beginnen können.

4.2.5 Verbindungsaufbauzeit

Die Berechnung der Verbindungsaufbauzeit wurde aus [PfPW_89] entnommen. Sie setzt sich im wesentlichen zusammen aus

- dem Warten auf die Übermittlung des Verbindungswunsches durch die MIX-Kaskade der Ortsvermittlungsstelle des Senders ($\leq$z),
- der Verzögerungszeit der MIX-Kaskade der Senderortsvermittlungsstelle ($m \cdot 0{,}01$ s),
- der Laufzeit des Verbindungswunsches im Fernnetz ($\leq$0,2 s),
- dem Warten auf die Verteilung an den Empfänger (in Stoßzeiten im Mittel $T_V \leq 0{,}5$ s),
- dem Warten auf das Aufbauen des ZS-Kanals durch den Empfänger ($\leq$z, wenn der Empfänger sofort antwortet) und
- der Verzögerungszeit der MIX-Kaskade der Empfängerortsvermittlungsstelle ($m \cdot 0{,}01$ s).

Daraus ergibt sich eine Zeit von $2 \cdot (z + m \cdot 0{,}01s) + T_V + 0{,}2s$, bei den obigen Werten (z = 0,7s) also ca. 2,3s, wobei die Verbindungsaufbauzeit im Mittel nur etwa halb so groß sein wird.

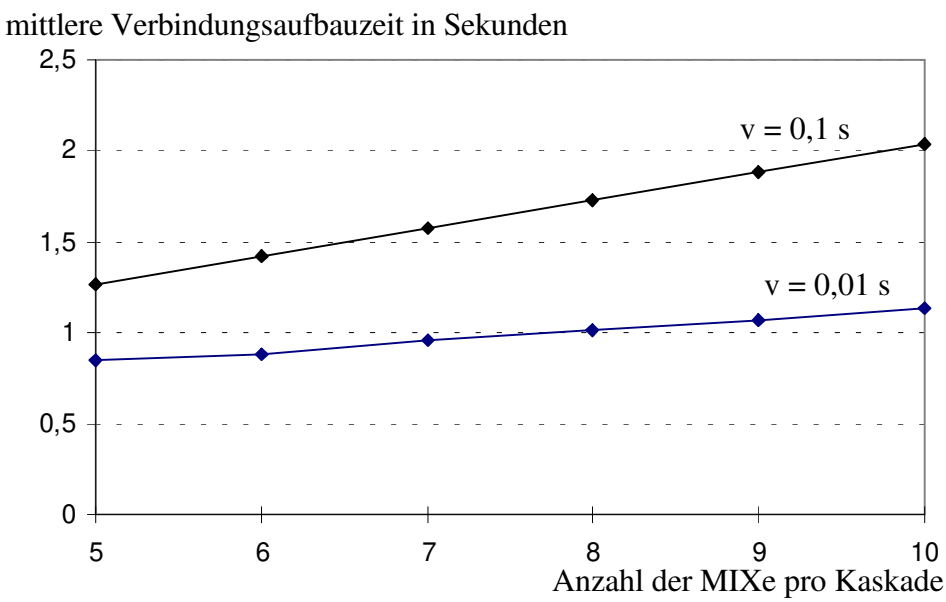


Abb. 4.2.5.1: Abhängigkeit der Verbindungsaufbauzeit von der MIX-Anzahl und der MIX-Verarbeitungszeit

Abb. 4.2.5.1 zeigt die Abhängigkeit der mittleren Verbindungsaufbauzeit von der Anzahl der MIXe pro Kaskade und der Verarbeitungszeit pro MIX. Die Darstellung verdeutlicht besonders die große Bedeutung der MIX-Verarbeitungszeit. Ohne den Einsatz von spezieller Hardware sind nur unzureichende Verarbeitungszeiten möglich, die den Verbindungsaufbau extrem verzögern.

4.3 Leistungsbewertung für das GSM-Mobilfunknetz

4.3.1 Länge der GSM-Signalisierungsnachrichten im Vergleich

Im folgenden sollen die Längen der GSM-Signalisierungsnachrichten vor und nach der Modifikation gegenübergestellt werden. Zuvor wird auch hier beispielhaft die Berechnung einer MIX-Eingabenachricht nach der Formel aus *Abschnitt 4.1.1* erklärt.

- **Location Updating Request**-Nachricht des Teilnehmers S:

  Nachrichteninhalt:

  $\mathbf{N_{LUP\text{-}Request}} := c_{S1}(D_{SE1}, c_{S2}(D_{SE2}, c_{S3}(D_{SE3}, N_{VLR}))))$

  mit $\mathbf{D_{SE1}} := t_{Li}, k_{SE1}$, $\mathbf{D_{SE2}} := t_{Li}, k_{SE2}$, $\mathbf{D_{SE3}} := t_{Li}, k_{SE3}, KKZ_S(Li)$

  $\mathbf{N_{VLR}} := c_{MSC/VLR}(lup_msg, t_{Li}, P, \{LAI, IAdr\}, Bv/Bl, N_{AuC}, N_{HLR}^*)$

  $\mathbf{N_{AuC}} := c_{A1}(D_{A1}, c_{A2}(D_{A2}, c_{A3}(D_{A3}, s_{MS}(t_{Li}, RAND_1), IMSI, RAND_2)))$

  mit $\mathbf{D_{A1}} := t_{Li}, k_{A1}$, $\mathbf{D_{A2}} := t_{Li}, k_{A2}$, $\mathbf{D_{A3}} := t_{Li}, k_{A3}, KKZ_A(Li)$

  $\mathbf{N_{HLR}^*} := c_{H1}(D_{H1}, c_{H2}(D_{H2}, c_{H3}(D_{H3}, N_{HLR}))))$

  mit $\mathbf{D_{H1}} := t_{Li}, k_{H1}$, $\mathbf{D_{H2}} := t_{Li}, k_{H2}$, $\mathbf{D_{H3}} := t_{Li}, k_{H3}, KKZ_{HLR}(Li)$

  $\mathbf{N_{HLR}} := k_{HLRS}(lup_msg, Bv/Bl, t_{Li}, IMSI, \{VLR, P\})$

  $\mathbf{\{VLR,P\}} := c_{H3}(k_{H3}, c_{H2}(k_{H2}, c_{H1}(k_{H1}, A_{VLR}, P))))$

  $\mathbf{\{LAI,IAdr\}} := c_{S3}(k_{S3}, c_{S2}(k_{S2}, c_{S1}(k_{S1}, LAI, IAdr))))$

  Nachrichtenlänge:

  - Länge der anonymen Rückadresse {LAI,IAdr}:

    $|\mathbf{N_{m+1}}| = 60 \text{ Bit} + 128 \text{ Bit} = 188 \text{ Bit}$

    $|\mathbf{N_m}| = 128 \text{ Bit} + 188 \text{ Bit} = 316 \text{ Bit} \Rightarrow 660 \text{ Bit}$ (da $< b_{asym}$)

    $|\mathbf{\{LAI,IAdr\}}| = (m-1) \cdot (128 \text{ Bit}) + 660 \text{ Bit} = 1812 \text{ Bit}$

  - Länge der anonymen Rückadresse {VLR,P}:

    $|\mathbf{N_{m+1}}| = 14 \text{ Bit} + 128 \text{ Bit} = 142 \text{ Bit}$

    $|\mathbf{N_m}| = 128 \text{ Bit} + 142 \text{ Bit} = 270 \text{ Bit} \Rightarrow 660 \text{ Bit}$

    $|\mathbf{\{VLR,P\}}| = (m-1) \cdot (128 \text{ Bit}) + 660 \text{ Bit} = 1812 \text{ Bit}$

  - Länge der Nachricht an das HLR:

    $|\mathbf{N_{m+1}}| = 8 \text{ Bit} + 1 \text{ Bit} + 30 \text{ Bit} + 60 \text{ Bit} + 1812 \text{ Bit} = 1911 \text{ Bit}$

    $|\mathbf{N_m}| = 30 \text{ Bit} + 128 \text{ Bit} + 28 \text{ Bit} + 1911 \text{ Bit} = 2097 \text{ Bit}$

    $|\mathbf{N_{HLR}^*}| = (m-1) \cdot (30 \text{ Bit} + 128 \text{ Bit}) + 2097 \text{ Bit} = 3519 \text{ Bit}$

  - Länge der Authentificationnachricht an das HLR:

    $|\mathbf{N_{m+1}}| = 200\text{Bit} + 30\text{Bit} + 60\text{Bit} + 128\text{Bit} = 418\text{Bit}$

    $|\mathbf{N_m}| = 30 \text{ Bit} + 128 \text{ Bit} + 28 \text{ Bit} + 418 \text{ Bit} = 604 \text{ Bit} \Rightarrow 660 \text{ Bit}$

    $|\mathbf{N_{AuC}}| = (m-1) \cdot (30 \text{ Bit} + 128 \text{ Bit}) + 660 \text{ Bit} = 2082 \text{ Bit}$

  - Länge der Nachricht an das VLR:

    $|\mathbf{N_{m+1}}| = 8\text{Bit} + 30\text{Bit} + 128\text{Bit} + 1812\text{Bit} + 1\text{Bit} + 2082\text{Bit} + 3519\text{Bit} = 7580\text{Bit}$

    $|\mathbf{N_m}| = 30 \text{ Bit} + 128 \text{ Bit} + 28 \text{ Bit} + 7580 \text{ Bit} = 7766 \text{ Bit}$

    $|\mathbf{N_{LUP\text{-}Request}}| = (m-1) \cdot (30 \text{ Bit} + 128 \text{ Bit}) + 7766 \text{ Bit} = \underline{9188 \text{ Bit}}$

	bisherige Länge	Länge mit 5 MIXen	Länge mit 10 MIXen	Länge der neuen I.E.´s bei 10 MIXen
Location Updating Request	148 Bit	5554 Bit	9204 Bit	9188 Bit
Location Updating Accept	124 Bit	832 Bit	1132 Bit	1116 Bit
Setup	853 Bit	—	—	—
ZE -Setup	—	2334 Bit	3914 Bit	3690 Bit
ZS-Setup	—	1935 Bit	2725 Bit	2501 Bit
Call Proceeding	195 Bit	648 Bit	948 Bit	820 Bit
Paging Request	176 Bit	1120 Bit	1420 Bit	1388 Bit
Alerting	280 Bit	232 Bit	382 Bit	334 Bit
Connect	448 Bit	232 Bit	382 Bit	334 Bit
Disconnect	416 Bit	232 Bit	382 Bit	334 Bit
Send Parameter from HLR	64 Bit	1308 Bit	2098 Bit	2082 Bit
Authentication Parameter	324 Bit	366 Bit	516 Bit	500 Bit
Send Routing Information	248 Bit	—	—	—
Information Acknowledge	240 Bit	—	—	—
Update Location	120 Bit	2105 Bit	3535 Bit	3519 Bit
Location Updating Accept	54 Bit	174 Bit	324 Bit	308 Bit
Paging	172 Bit	2028 Bit	2818 Bit	2802 Bit
IAM	976 Bit	1444 Bit	1594 Bit	1102 Bit
ACM	1076 Bit	470 Bit	470 Bit	106 Bit
ANM	1216 Bit	478 Bit	478 Bit	106 Bit
REL	912 Bit	374 Bit	374 Bit	106 Bit

Abb. 4.3.1.1: Länge der modifizierten GSM-Nachrichten im Vergleich

Analog kann die Länge aller MIX-Eingabenachrichten bzw. der kompletten Signalisierungsnachrichten berechnet werden. *Abb. 4.3.1.1* zeigt eine Gegenüberstellung aller modifizierten Signalisierungsnachrichten. Die bisherige Länge der RIL3-Signalisierungsnachrichten wurde aus [GSM_04.08], die bisherige Länge der MAP-Nachrichten aus

[GSM_09.02] und die Länge der ISDN-UP-Signalisierungsnachrichten wurde aus [ITU_Q.763] entnommen.

4.3.2 Minimale Dauer des Systemtaktes

Eine Unbeobachtbarkeit des physischen Sendens zu erreichen, ist in GSM deutlich schwieriger als in ISDN, da akkubetriebene Mobilstationen sich nicht am Dummy Traffic beteiligen können. Dieser und weitere in der Realisierung diskutierte Gründe, die zu einer eingeschränkten Unbeobachtbarkeit führen, sollen in diesem Abschnitt nicht im Vordergrund stehen, sondern die Berechnung der minimalen Taktung des Kommunikationssystems. In GSM muß jeder Teilnehmer, dem dies möglich ist, für jeden Systemtakt eine ZE- und eine ZS-Setup-Nachricht signalisieren. Außerdem erhält er eine Call Proceeding-Nachricht. Für die Signalisierung vom Teilnehmer zum Netz (BTS) wird für Verbindungswünsche ein Stand-Alone Dedicated Control Channel (SDCCH) vergeben. Dieser verfügt über eine Bandbreite von 0,782 kbps (vollduplex) und ist nur für sehr kurze Signalisierungsnachrichten verwendbar. Außerdem wird einem SDCCH ein Slow Associated Control Channel (SACCH) zugeordnet, die über eine Bandbreite von 0,391 kbps verfügt. Für die zusätzliche Signalisierung soll vorerst lediglich der SDCCH verwendet werden, der Rest steht für weitere I.E.´s und Management- bzw. Sicherungsaufgaben zur Verfügung. Ein Teil der 0,782 kbps wird jedoch außerdem für Location Updates (LUP) benötigt, so daß zur Signalisierung von Verbindungswünschen nur eine Bandbreite von 0,6 kbps genutzt werden kann. Mit diesen Werten errechnet sich nach der untenstehenden Formel eine unzumutbare Zeitscheibenlänge von 10,32 s. Deshalb soll hier eine Modifikation vorgeschlagen werden. Neben dem SACCH existiert ein Fast Associated Control Channel (FACCH), der mit einer Bandbreite von 4,6 kbps (Halfrate) bzw 9,2 kbps (Fullrate) (jeweils vollduplex) einem Nutzkanal zugeordnet wird. Durch Modifikationen in der Kanalvergabe kann man bei Early TCH-Assignment, diesen FACCH bereits für die Signalisierung nutzbar machen. Dann kann der SDCCH ebenfalls andere Aufgaben übernehmen. Im Berechnungsbeispiel sollen die 4,6 kbps des FACCH/H verwendet werden. 1,1 kbps werden für das LUP reserviert und so stehen für den Verbindungsaufbau 3,5 kbps zur Verfügung.

Eine Mobilstation muß also in der Lage sein, über ihren Signalisierungskanal in jedem Systemtakt $|N_{ZE\text{-}Setup}| + |N_{ZS\text{-}Setup}|$ Bit zu übertragen, d.h. es gilt:

$$z \geq \frac{\left|N_{ZE-Setup}\right| + \left|N_{ZS-Setup}\right|}{3{,}5kbps}$$

Bei einem Einsatz von 10 MIXen pro Kaskade erhält man:

$$z \geq \frac{3690Bit + 2501Bit}{3500\,Bit/s} = 1{,}769s$$ [32]

In der Realsierung könnte man demzufolge den Systemtakt z.B. auf 1,8 Sekunden festlegen. Verwendet man dagegen nur 5 MIXe in jeder Kaskade, erhält man mit der Formel $z \geq 1{,}092s$. Die Einführung eines Taktes von 1,8 s bedeutet für den Teilnehmer, daß er zum Beginn jedes Taktes Verbindungswünsche absenden kann, im Mittel also 0,9 s warten muß.

[32] Die Signalisierung vom Netz zum Teilnehmer ($N_{Call\text{-}Proceeding}$) verursacht weniger Aufwand, als die Gegenrichtung und hat deshalb keinen Einfluß auf die minimale Zeitscheibenlänge.

In *Abb. 4.3.2.1* ist die Abhängigkeit der minimalen Zeitscheibe von der Anzahl der verwendeten MIXe und der verwendeten Signalisierungskanäle dargestellt. Die Verwendung von nur einem MIX pro Kaskade wäre in der Praxis unsinnig, da man diesem vollständig vertrauen müßte. Diese Darstellung soll verdeutlichen, in welchem Maße der Aufwand, bezogen auf die minimal mögliche Zeitscheibenlänge, bei der Erhöhung der MIX-Anzahl pro Kaskade steigt. Außerdem soll gezeigt werden, wie wichtig ein leistungsfähiger Signalisierungskanal im GSM auch für zukünftige Dienste ist.

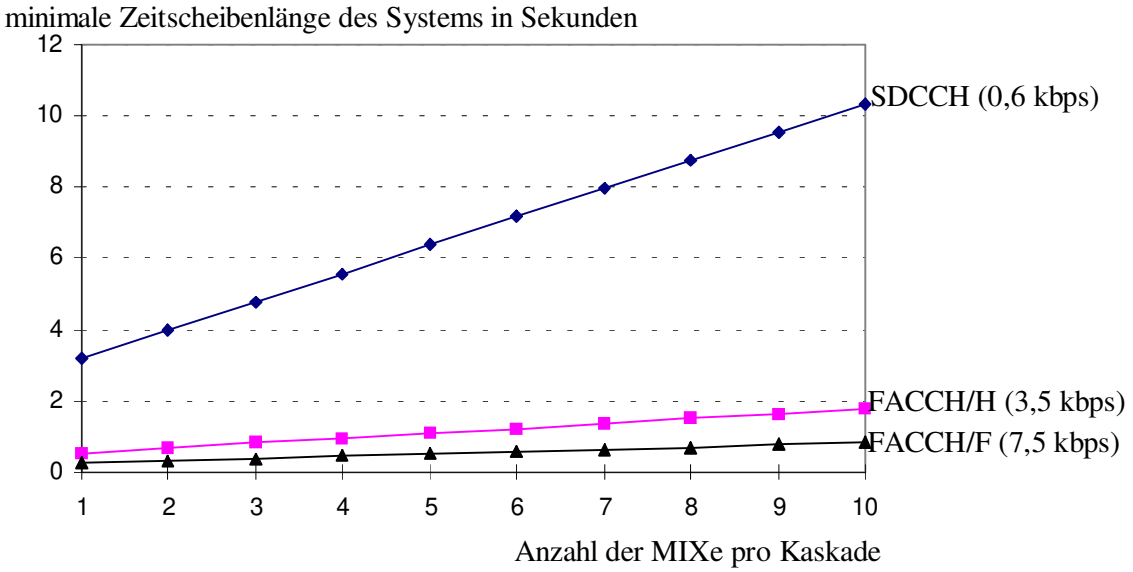


Abb. 4.3.2.1: Abhängigkeit der Zeitscheibenlänge von der MIX-Anzahl

Außerdem ist zu beachten, daß auch die Authentikationschallenges innerhalb der Zeitscheibe signalisiert werden müssen. Dafür wird der Broadcast Control Channel (BCCH) verwendet, der eine Bandbreite von 0,782 kbps (simplex von der BTS zur MS) hat. Die Länge des Authentikationschallenge ist $RAND_1 + t_i + s_{AuC}(RAND_1,t_i) = 358$ Bit. Wenn für diesen Broadcast 0,25 kbps des BCCH dauerhaft genutzt werden können, kann man diese Nachricht in 1,43s signalisieren. Damit braucht der Systemtakt von 2s nicht weiter erhöht werden.

4.3.3 Minimale Dauer des Location-Update-Taktes

Für die in Bewegung befindlichen Mobilteilnehmer ist ein Location Update mit einer bestimmten Häufigkeit nötig. Diese LUP-Häufigkeit hängt von mehreren Faktoren ab, z.B. von der Durchschnittsgeschwindigkeit v der MS, dem Radius r der Funkzellen und der Anzahl der Funkzellen pro Location Area N_{LA}. In [FuBr_94] wird für die durchschnittliche Anzahl von LUPs λ_{LUP} pro MS während der Stoßzeiten

$$\lambda_{LUP} = \frac{v}{\pi \cdot r} \cdot \left(1 - \frac{N_{LA} - 1}{2 \cdot N_{LA}}\right)$$

angegeben. Abb. 4.3.3.1 zeigt die durchschnittliche LUP-Rate in Abhängigkeit von dem Zellradius und der Anzahl der Funkzellen pro LA. Dabei wird von einer Durchschnittsgeschwindigkeit analog zu [FuBr_94] von 15 km/h ausgegangen.

Bei einem LUP muß die MS in der Lage sein, die LUP-Request-Nachricht abzusenden und die LUP-Accept-Nachrichten zu empfangen. Zur Verfügung stehen dafür dieselben

Kanäle, wie beim Verbindungsaufbau. Wird also nur der SDCCH mit 0,18 kbps für die LUP Signalisierung genutzt, so erhält man für die minimale LUP-Zeitscheibe nach untenstehender Formel einen Wert von $z_{LUP} \leq 51{,}1s$. Ein Teilnehmer kann demzufolge pro Stunde 70 LUPs durchführen, muß aber im Mittel 25,5s darauf warten. Auch hier verursacht die Signalisierung vom Teilnehmer zum Netz den größeren Aufwand und bildet deshalb das entscheidende Kriterium für die minimale Länge des LUP-Taktes. Auch hier soll der FACCH/H genutzt werden, um den SDCCH zu entlasten und bessere Ergebnisse zu erzielen. Dadurch hat man einen Bandbreite von 1,1 kbps statt 0,18 kbps für das Location Update zur Verfügung.

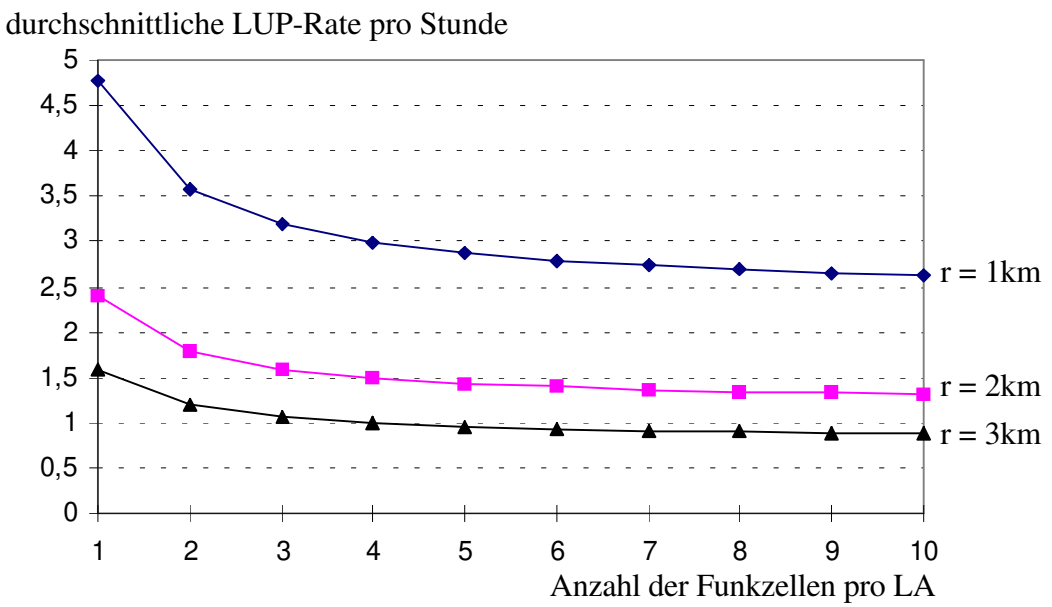


Abb. 4.3.3.1: durchschnittliche LUP-Rate in GSM

Die minimale LUP-Zeitscheibenlänge berechnet sich dann:

$$z_{LUP} \leq \frac{\left| N_{LUP-\mathrm{Re}\,quest} \right|}{1{,}1kbps}$$

Bei einem Einsatz von 10 MIXen pro Kaskade erhält man:

$$z_{LUP} \leq \frac{9188Bit}{1100\,Bit/s} = 8{,}353s$$

In *Abb. 4.3.3.2* ist die Abhängigkeit der minimalen LUP-Zeitscheibe von der Anzahl der verwendeten MIXe und der verwendeten Signalisierungskanäle dargestellt. Diese Darstellung soll verdeutlichen, in welchem Maße der Aufwand, bezogen auf die minimal mögliche LUP-Zeitscheibenlänge, bei der Erhöhung der MIX-Anzahl pro Kaskade steigt. Außerdem soll gezeigt werden, wie wichtig ein leistungsfähiger Signalisierungskanal GSM auch für das LUP ist.

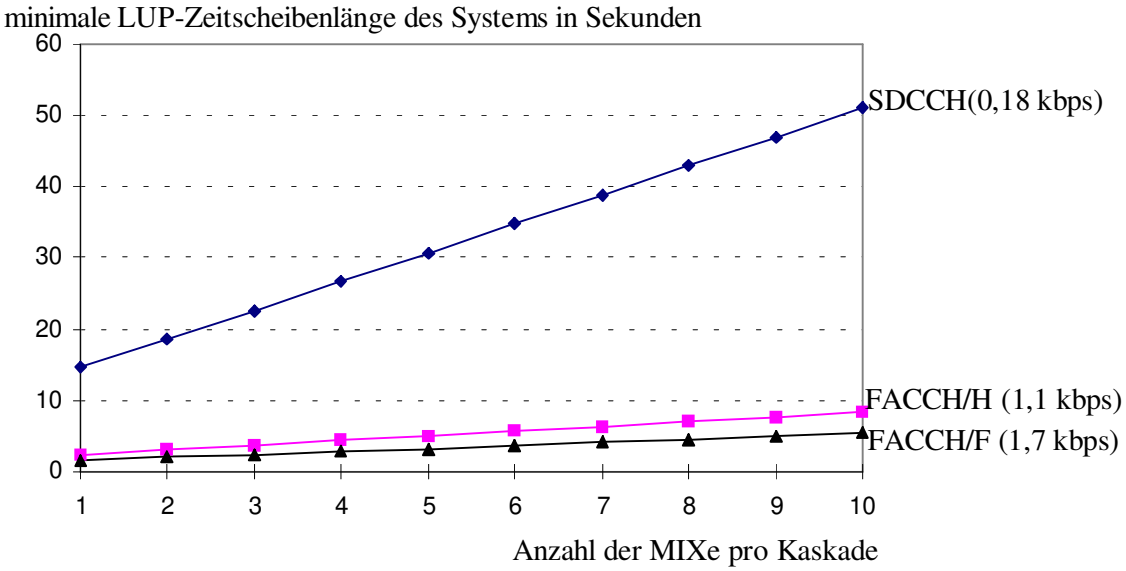


Abb. 4.3.3.2: Abhängigkeit der LUP-Zeitscheibenlänge von der MIX-Anzahl

4.3.4 Maximale Anzahl der von einer Funkzelle bedienbaren Mobilstationen

Ein weiterer Parameter des Kommunikationssystems muß Beachtung bei der Leistungsbewertung der unbeobachtbaren Zeitscheibenkanäle finden, das Paging. Die Paging Request-Nachricht wird bei einem MTC von der BTS ausgesendet, um den Empfänger eines Verbindungswunsches davon zu unterrichten. Diese Nachricht ist 2818 Bit lang. Verwendung findet der Paging Channel, der über eine Bandbreite von 0,782 kbps (simplex von der BTS zur MS) verfügt. Wenn für die zusätzlichen Paging-Informationen davon 0,7 kbps genutzt werden können, dauert die Übermittlung einer Verbindungswunschnachricht 4,03s. Die durchschnittliche Anzahl notwendiger Paging-Nachrichten in einer Funkzelle hängt wiederum von verschiedenen Größen ab. In [FuBr_94] wird für die durchschnittliche Paging Request-Rate

$$\lambda_{PAGING} = N_{MS} \cdot \lambda_{MTC} \cdot \left(A_P \cdot \left(N_{LA} - 1 \right) + 1 + \frac{\left(A_F - 1 \right) \cdot P_{KF}}{1 + P_{KF} + P_{KA}} \right)$$

angegeben, wobei

- N_{MS} die durchschnittliche Anzahl der Mobilteilnehmer pro Funkzelle,
- λ_{MTC} die durchschnittliche Anzahl der ankommenden Verbindungswünsche,
- A_F die maximale Anzahl der Paging Request Versuche pro MTC in der besuchten Funkzelle (A_F=2),
- A_P die Anzahl der Paging Request Versuche in jeder anderen Funkzelle des besuchten LAs (A_P=2),
- N_{LA} die Anzahl der Funkzelle pro LA ist (N_{LA}=3),
- P_{KF} die Wahrscheinlichkeit ist, daß kein Funkkontakt möglich ist (P_{KF}=0,4) und
- P_{KA} die Wahrscheinlichkeit ist, daß eine MS nicht antwortet (P_{KA}=0,3).

Abb. 4.3.4.1 zeigt die Anzahl der notwendigen Paging Requests innerhalb einer Funkzelle in Abhängigkeit von der Anzahl der Mobilteilnehmer pro Funkzelle und deren Verkehrscharakteristik λ_{MTC}. Da die Übermittlung einer Paging Request-Nachricht 4,03s dauert, können in einer Stunde nicht mehr als 893 Paging-Nachrichten signalisiert wer-

den. Dadurch wird auch die maximale Anzahl von versorgbaren Mobilteilnehmern begrenzt, wobei deren Verkehrsstatistik und die Anzahl der Funkzellen pro LA sowie deren Durchmesser ebenfalls diese Größe beeinflussen.

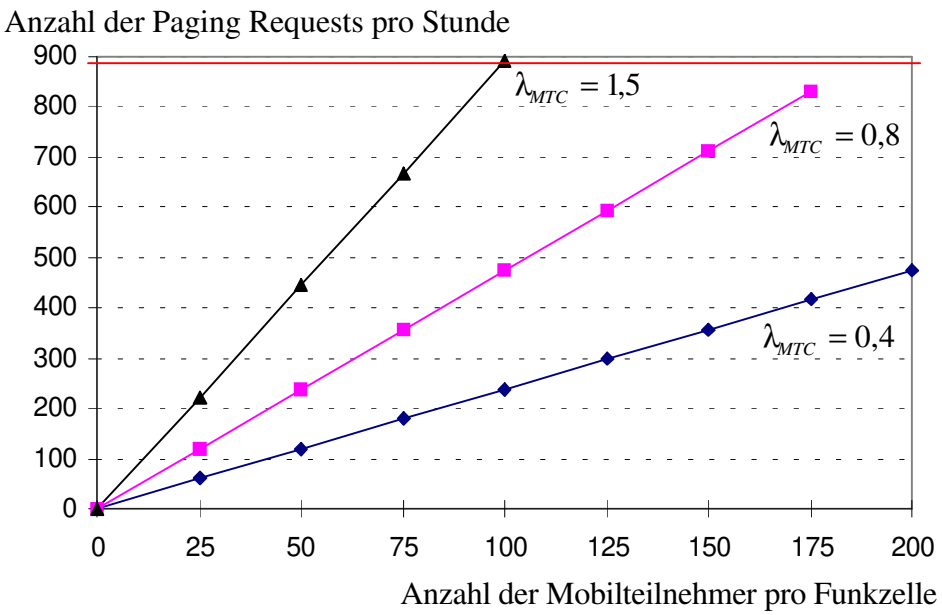


Abb. 4.3.4.1: Paging Request-Rate in Abhängigkeit von der Teilnehmeranzahl pro Funkzelle

4.3.5 Berechnungsaufwand der Mobilstationen und MIXe

Für die Mobilstationen besteht der zusätzliche Berechnungsaufwand auch in GSM hauptsächlich aus dem Anwenden kryptographischer Verfahren, wie dem Ver- und Entschlüsseln von Nachrichten, dem Signieren und Testen von Nachrichten und dem Vorbereiten der MIX-Nachrichten. Da in GSM mehrere MIX-Kaskaden durchlaufen werden, steigt der Berechnungsaufwand zum Berechnen der MIX-Nachrichten. Allerdings ist die Übertragungsbandbreite deutlich geringer, statt 144 kbps nur ca. 30 kbps. Dadurch ist der Berechnungsaufwand der Mobilstationen in der Summe niedriger als im ISDN.

Der Berechnungsaufwand der MIXe besteht auch im GSM im wesentlichen aus dem Ver- und Entschlüsseln der MIX-Nachrichten, dem Puffern und Umsortieren der Nachrichten, sowie dem Testen der Zeitstempel. Dies betrifft in jedem Systemtakt 6 Signalisierungseingabeschübe im MSC, 5 Signalisierungseingabeschübe im HLR und 2 Dateneingabeschübe mit höchstens $N_{MS} \cdot N_{LA} \cdot N_{MSC}$ Nachrichten[33] im MSC. Die maximale Anzahl der Mobilteilnehmer, die einem HLR zugeordnet werden und über dessen MIX-Kaskade kommunizieren, hängt von den MIX-Implementierungen ab. Setzt man in jedem MIX spezielle Hardware ein, ist es nach [PfPW_89] möglich, Verarbeitungszeiten (v) von weniger als 0,01 s pro MIX bei ca. 27000 angeschlossenen Teilnehmern (Schubgröße) zu erreichen. Generell sollten verschiedene Nachrichten bzw. Nachrichten innerhalb einer MIX-Kaskade pipelineartig verarbeitet werden, d.h. die Zeitscheiben bei den verschiedenen MIXen zu unterschiedlichen, definierten Zeitpunkten beginnen können.

[33] N_{MSC} ist die Anzahl der LAs pro MSC.

4.3.6 Verbindungsaufbauzeit

Die Berechnung der Verbindungsaufbauzeit wird entsprechend der ISDN-Lösung vorgenommen. Sie setzt sich im wesentlichen zusammen aus

- der gegenseitigen Authentikation von Sender und Netz ($\leq$z),
- dem Warten auf die Übermittlung des Verbindungswunsches durch die MIX-Kaskade des MSCs des Senders ($\leq$z)[34],
- der Verzögerungszeit der MIX-Kaskade des MSCs des Senders ($m \cdot 0{,}01$ s),
- der Laufzeit des Verbindungswunsches im Fernnetz zum HLR des Empfängers ($\leq 0{,}2$ s),
- dem Warten auf die Übermittlung des Verbindungswunsches durch die MIX-Kaskade des HLRs des Empfängers ($\leq$z),
- der Verzögerungszeit der MIX-Kaskade im HLR des Empfängers ($m \cdot 0{,}01$ s),
- der Laufzeit des Verbindungswunsches im Fernnetz zum VLR der Empfängers ($\leq 0{,}2$ s),
- dem Warten auf die Übermittlung des Verbindungswunsches durch die MIX-Kaskade des MSC/VLRs des Empfängers ($\leq$z),
- der Verzögerungszeit der MIX-Kaskade im MSC/VLR des Empfängers ($m \cdot 0{,}01$ s),
- dem Warten auf die Verteilung an den Empfänger (in Stoßzeiten im Mittel $T_V \leq 5$ s),
- der gegenseitigen Authentikation von Empfänger und Netz ($\leq$z),
- dem Warten auf das Aufbauen des ZS-Kanals durch den Empfänger ($\leq$z, wenn der Empfänger sofort antwortet) und
- der Verzögerungszeit der MIX-Kaskade des MSCs des Empfängers ($m \cdot 0{,}01$ s).

Daraus ergibt sich eine Zeit von $4 \cdot (z + m \cdot 0{,}01) + 2 \cdot z + 2 \cdot 0{,}2 + T_V$, bei den obigen Werten (z = 1,8s) also ca. 16,6s, wobei die Verbindungsaufbauzeit im Mittel nur etwa halb so groß sein wird. Dieser Wert zeigt deutlich, daß die Bandbreite auf den Signalisierungskanälen in GSM erhöht werden müßte, so würde die Verbindungsaufbauzeit bei Verwendung von 5 MIXen und einer verfügbaren Bandbreite von 7,5 kbps für Verbindungswünsche (siehe *Abschnitt 4.3.2*) und 3 kbps für den PCH nur ca. 4,8s betragen, im Mittel also weniger als 2,5s.

[34] Der Aufbau von zugeordneten Signalisierungs- und Nutzkanälen auf der Funkschnittstelle gehört zu diesem Punkt.

5. Zusammenfassung und Ausblick

Das Ziel dieser Arbeit war es, aufzuzeigen, daß sich Unbeobachtbarkeit und Anonymität bei der Signalisierung von Verbindungswünschen und Location Updates bereits mit den Bandbreitemöglichkeiten der bestehenden Kommunikationsnetze realisieren läßt. Für die Erklärung der Verfahren zur Erreichung von Teilnehmerunbeobachtbarkeit und der beispielhaften technischen Realisierung wurden das Festnetz ISDN und das Mobilfunknetz GSM (D1, D2, E-plus) gewählt.

Im ISDN wurden, ausgehend von der Idee der Telefon-MIXe aus [PfPW_89], die Netzstruktur und die Protokolle entsprechend modifiziert und die notwendigen Änderungen der Signalisierungsnachrichten detailliert dokumentiert. Außerdem wurde in den Effiziensbetrachtungen nachgewiesen, daß sich Teilnehmerunbeobachtbarkeit bei der Signalisierung von Verbindungswünschen mit vertretbarem Aufwand erreichen läßt. Es wurden allerdings nur die Basisabläufe des Verbindungsaufbaus untersucht und modifiziert. Zusatzdienste von ISDN, wie Anrufweiterleitung, Anklopfen und Halten, wurden nicht analysiert. Es ist allerdings zu erwarten, daß sich ein großer Teil der Zusatzdienste auch trotz Unbeobachtbarkeit und Anonymität der Nutzer realisieren läßt. An diesem Punkt besteht jedoch weiterer Forschungsbedarf. Außerdem können die hier vorgestellten Prinzipien weiter verbessert werden, so kann man im Festnetz z.B. eine offene implizite Adresse des Senders in der Verbindungswunschnachricht signalisieren, wenn die beiden Teilnehmer bereits einmal kommuniziert haben. Diese reicht aus, damit der Empfänger den Sender erkennen kann und dessen gespeicherte Daten (z.B. LE_S, Kz_{init}) zum Verbindungsaufbau wiederverwenden kann. Bei einander bekannten Teilnehmern kann ebenfalls sofort symmetrische Ende-zu-Ende-Verschlüsselung eingesetzt werden, wodurch weiterer Aufwand gespart wird. Die hier vorgestellte Realisierung ist jedoch praktikabel und ausbaufähig.

In GSM mußten die Verfahren zum Schutz der Signalisierungsbeziehungen an die Teilnehmermobilität angepaßt werden. Auch für GSM wurden Modifikationen der Netzstruktur und der Verbindungsaufbau- bzw. Location Update-Protokolle entwickelt und diskutiert, wobei durch die schmalbandigen Signalisierungskanäle nicht die Leistungsfähigkeit erreicht werden konnte, wie im ISDN. Außerdem können sich akkubetriebene Mobilstationen nicht am notwendigen Dummy Traffic auf der Funkschnittstelle beteiligen. Dadurch verringert sich die erreichbare Unbeobachtbarkeit erheblich, da eine BTS als Angreifer mehr Informationen erhält. Hinzu kommt, daß die Mobilteilnehmer der BTS vertrauen müssen, daß diese den notwendigen Dummy Traffic im Festnetz erzeugt. Das Problem der Peil- und Ortbarkeit von sendenden Mobilstationen wurde in dieser Arbeit nicht untersucht, es sei auf die in der Literatur existierenden Lösungen [FeTh_95] verwiesen. In der Leistungsbewertung wurde ermittelt, daß die Realisierung zu spürbaren Einbußen in der Dienstqualität führt. Die Wartezeiten können allerdings durch die beschriebene modifizierte Kanalvergabe und -verwendung deutlich reduziert werden, so sich auch diese Lösungen praktizieren läßt. Des weiteren kann man auch diese Protokolle noch optimieren. Faßt man beispielsweise bei einem Location Update die Authentikationsnachrichten (Send Parameter ...) und die Nachrichten zur Speicherung des Aufenthaltsortes (Update Location ...) zusammen, so spart man ca. 2000 Bit an zu signalisierenden Informationen. Nicht untersucht wurde in GSM das Handover und die Zusatzdienste.

Die Methode zum Schutz der Signalisierungsbeziehungen wurde zu Beginn dieser Arbeit allgemeingültig beschrieben, so daß eine Adaption auf andere Kommunikationsnetze, wie Asynchronous Transfer Mode (ATM) im Festnetzbereich oder Universal Mobile Telecommunication System (UMTS) im Mobilkommunikationsbereich auf Grundlage dieser Arbeit möglich ist.

Somit bleibt festzuhalten, daß bei der rasanten Entwicklung neuer Kommunikationstechnologien und -dienste die Privatsphäre der Nutzer und deren informationelle Selbstbestimmung nicht vernachlässigt werden sollte. Diese Arbeit soll mit den dargestellten Konzepten ihren Teil dazu beitragen.

Ein besonderer Dank geht an dieser Stelle an Dipl.-Inform. Hannes Federrath, Dipl.-Inform. Anja Jerichow und Prof. Dr. Andreas Pfitzmann, die durch ihre permanente Diskussionsbereitschaft und ihr kritisches Hinterfragen viel zu dieser Arbeit beigetragen haben.

6. Abkürzungsverzeichnis

A3	Algorithmus zur Authentikation in GSM
ACM	Address Complete Message
A_F	max. Anzahl der Paging-Versuche in der besuchten Funkzelle
AI	Alerting-Information
A_{LE_E}	Adresse des LEs von E
ANM	Answer Message
A_P	Anzahl der Paging-Versuche in anderen Funkzellen eines LAs
AuC	Authentication Center
ATM	Asynchronous Transfer Mode
b_{asym}	Blocklänge des asymmetrischen Kryptosystems
BC	Bearer Capability
BCCH	Broadcast Control Channel
BSC	Base Station Controler
BSS	Base Station Subsystem
BSSMAP	BSS-Management Part
BTS	Base Transceiver Station
Bv/Bl	Kennzeichnung Bedeutungsvoll/Bedeutungslos
CAU	Cause
CC	Call Control
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CCS7	Common Channel Signalling System CCITT No. 7
CHI	Channel Identification
CI	Connected-Information
CIC	Circuit Identification Code
CR	Call Reference
c_S	asymmetrischer öffentlicher Schlüssel von S
d_S	asymmetrischer geheimer Schlüssel von S
D_{SE1}	Daten von S für den MIX_1 im Empfangskanal
DPC	Destination Point Code
DSP	Destination Signalling Point
DSS1	Digital Subscriber Signalling System No. 1
E	Empfänger
EI	Empfangs-Information
EIR	Equipment Identity Register
FACCH/F	Fast Associated Control Channel/ Fullrate
FACCH/H	Fast Associated Control Channel/ Halfrate
GMSC	Gateway-MSC
GSM	Global System for Mobile Communication, Groupe Spéciale Mobile
HLC	High Layer Compatibility
HLR	Home Location Register
HOV	Handover
IAdr	impizite Adresse
IAM	Initial Address Message
IN	Intelligent Network
INAP	Intelligent Network Application Part
ISDN	Integrated Services Digital Network

ISDN-UP	ISDN-User Part
ISO/OSI	International Standardisation Organisation/ Open Systems Interconnection
ITC	Information Transfer Capability
ITR	Information Transfer Rate
IWF	Interworking Functions
I.E.	Informationselement
kbps	kBit/s
k_c	Sitzungsschlüssel für Verbindungsverschlüsselung in GSM
k_i	„geheimer“ Schlüssel des GSM-Teilnehmers
KKZ	Kanalkennzeichen
KZ_{init}	Kanalzeicheninitialwert
k_{SE}	symmetrischer Schlüssel von S und E
LA	Location Area
LAI	Location Area Identification
LE	Local Exchange
LLC	Low Layer Compatibility
LUP	Location Update
m	Anzahl der MIXe in einer Kaskade
MAP	Mobile Application Part
MM	Mobility Management
MOC	Mobile Originated Call
MS	Mobile Station
MSC	Mobile Switching Center
MT	Message Type
MTC	Mobile Terminated Call
MTP	Message Transfer Part
N	Nachricht
|N|	Länge der Nachricht N
N_i	Nachricht i bzw. Nachricht an i
N_{LA}	Anzahl der Funkzellen pro LA
N_{MS}	Anzahl der MSen pro Funkzelle
NT	Network Termination
OACSU	Off Air Call Setup
OPC	Originated Point Code
OSP	Originated Signalling Point
P	Pseudonym
PD	Protokoll Diskriminator
PI	Progress Indicator
P_{KA}	Wahrscheinlichkeit, daß eine MS nicht antwortet
P_{KF}	Wahrscheinlichkeit, daß kein Funkkontakt möglich ist
PSTN	Public Switched Telephone Network
r	Radius einer Funkzelle
{R}	anonyme Rückadresse mit Inhalt R
RAND	Zufallszahl für GSM-Authentikation
REL	Release Message
RIL3	Radio Interface Layer 3
RLC	Release Complete Message
RR	Radio Ressource
RSM	Radio Subsystem Management

S	Sender
SACCH	Slow Associated Control Channel
SCCP	Signalling Connection Control Part
SDCCH	Stand-Alone Dedicated Control Channel
SFT	Shift
SGM	Segmentation Message
SL	Signalling Link
SMS	Short Message Service
SP	Signalling Point
SRES	Authentikationsresponse in GSM
s_{sym}	Schlüssellänge des symmetrischen Kryptosystems
STP	Signalling Transfer Point
TC	Transaction Capabilities
TCAP	Transaction Capability Application Part
TCH	Traffic Channel
TCU	Transaction Capability User
TE	Transit Exchange
t_i	Systemzeit im i-ten Takt
TUP	Telephone User Part
T_v	Signalisierzeit eines Verbindungswunsches bis zum Teilnehmer
UMTS	Universal Mobile Telecommunication System
UPT	Universal Personal Telecommunications
v	Geschwindigkeit einer Mobilstation
v	Verabreitungszeit einer MIX-Kaskade
VLR	Visitor Location Register
z	Länge einer Zeitscheibe
ZE-Kanal	Zeitscheiben-Empfangskanal
ZEI	Zeitscheiben-Empfangs-Information
ZS-Kanal	Zeitscheiben-Sendekanal
ZSI	Zeitscheiben-Sende-Information
λ	Ankunftsrate
μ	Bearbeitungsrate

7. Abbildungsverzeichnis

Abb. 2.2.2.1: Funktionale Struktur des CCS7 11
Abb. 2.2.2.2: Generelles Nachrichtenformat des ISDN-UP 12
Abb. 2.2.3.1: Aufbau einer DSS1-Nachricht der Schicht 3 13
Abb. 2.3.1.1: ISDN-Netzstruktur 14
Abb. 2.3.1.2: Signalisierungsprotokoll des Verbindungsaufbaus 15
Abb. 2.3.2.1: GSM-Netzstruktur 16
Abb. 2.4.2.1: MIX-Prinzip am Beispiel einer Kaskade mit 2 Mixen und einem Schub von 3 Nachrichten 18
Abb. 2.4.3.1: Aufbau eines Sende- oder Empfangskanals 22
Abb. 2.4.3.2: Kommunikation vom Sender zum Empfänger über MIX-Kanäle 23
Abb. 3.1.1.1: Modifizierte ISDN-Netzstruktur 25
Abb. 3.1.2.1: Modifiziertes Signalisierungsprotokoll zum Verbindungsaufbau 27
Abb. 3.1.2.2: Beispielszenario eines Verbindungsaufbaus 28
Abb. 3.1.3.1: Beschreibungspunkte der Nachrichteninhalte im ISDN 30
Abb. 3.1.3.2.1: Modifizierte Codierung der DSS1-Nachrichtentypen des Basisablaufes 33
Abb. 3.1.3.2.2: Modifizierte Codierung der DSS1-Informationselemente 34
Abb. 3.1.3.2.3: Aufbau und Inhalt der ZE-Setup-Nachricht 35
Abb. 3.1.3.5.1: Codierung der CCS7-Nachrichtentypen (ISDN-UP) 39
Abb. 3.1.3.5.2: Modifizierte Codierung des CCS7-Informationselemente (ISDN-UP) .. 39
Abb. 3.1.3.5.3: Aufbau der Initial Address Message 41
Abb. 3.1.3.5.4: Aufbau der Address Complete Message 42
Abb. 3.1.3.5.5: Aufbau der Answer Message 43
Abb. 3.1.3.5.6: Aufbau der Release Message 43
Abb. 3.2.1.1: Modifizierte GSM-Netzstruktur 45
Abb. 3.2.2.1: Modifizierte Authentikationsprozedur 46
Abb. 3.2.3.1: Modifiziertes Signalisierungsprotokoll des LUP 48
Abb. 3.2.4.1: Modifiziertes Signalisierungsprotokoll des Mobile Originated Calls 49
Abb. 3.2.4.2: Modifiziertes Signalisierungsprotokoll des Mobile Terminated Calls 51
Abb. 3.2.5.1: Beschreibungspunkte der Nachrichteninhalte im GSM 52
Abb. 3.2.5.2.1: Aufbau einer RIL3-Signalisierungsnachricht 56
Abb. 3.2.5.2.2: Modifizierte Codierung der RIL3-Nachrichtentypen des Basisablaufes. 57
Abb. 3.2.5.2.3: Modifizierte Codierung der RIL3-Informationselemente 57

Abb. 3.2.5.2.4: Aufbau der Location Updating Request-Nachricht..... 58
Abb. 3.2.5.2.5: Aufbau der Location Updating Accept-Nachricht 58
Abb.: 3.2.5.2.6: Aufbau der MOC ZE- bzw. ZS-Setup-Nachrichten 58
Abb.: 3.2.5.2.7: Aufbau der MTC ZE- bzw. ZS-Setup-Nachrichten..... 59
Abb.: 3.2.5.2.8: Aufbau der Paging Request-Nachricht..... 59
Abb.: 3.2.5.2.9: Aufbau der Call Proceeding-Nachricht 60
Abb. 3.2.5.5.1: Aufbau der Send Information from HLR-Nachricht 65
Abb. 3.2.5.5.2: Aufbau der Authentication Parameter-Nachricht..... 65
Abb. 3.2.5.5.3: Aufbau der Update Location-Nachricht..... 65
Abb. 3.2.5.5.4: Aufbau der Updating Location Accept-Nachricht 66
Abb. 3.2.5.5.5: Aufbau der Paging-Nachricht 66
Abb. 3.2.5.5.6: Aufbau der Process Access-Nachricht 66
Abb. 3.2.5.5.7: Aufbau der Complete Call-Nachricht..... 66
Abb. 3.3.1: Interworking zwischen Netzen mit Anonymer Signalisierung..... 68
Abb. 4.1.2.1: Länge der Parameter in den Kommunikationssystemen..... 70
Abb. 4.2.1.1: Länge der modifizierten ISDN-Nachrichten im Vergleich 72
Abb. 4.2.2.1: Abhängigkeit der Zeitscheibenlänge von der MIX-Anzahl 73
Abb. 4.2.3.1: Abhängigkeit der Teilnehmeranzahl von der Verbindungswunschrate 74
Abb. 4.2.5.1: Abhängigkeit der Verbindungsaufbauzeit von der MIX-Anzahl und der MIX-Verarbeitungszeit..... 75
Abb. 4.3.1.1: Länge der modifizierten GSM-Nachrichten im Vergleich..... 77
Abb. 4.3.2.1: Abhängigkeit der Zeitscheibenlänge von der MIX-Anzahl 79
Abb. 4.3.3.1: Durchschnittliche LUP-Rate in GSM..... 80
Abb. 4.3.3.2: Abhängigkeit der LUP-Zeitscheibenlänge von der MIX-Anzahl..... 81
Abb. 4.3.4.1: Paging Request-Rate in Abhängigkeit von der Teilnehmeranzahl pro Funkzelle..... 82

8. Literaturverzeichnis

Axla_95 Jörgen Axland: Fax- und Sprachverschlüsselung für jedermann; Siemens Zeitschrift SPECIAL FuE; Frühjahr 1995.

AzDi_94 Ashar Aziz, Whitfield Diffie: Privacy and Authentication for Wireless Local Area Networks; IEEE Personal Communications, First Quarter 1994, Page 25-31.

BGGH_95 Gerhard Bandow, Hubert Gottschalk, Dieter Gehrmann, Walter Hlavac, Heinz Koch, Werner Müller, Dieter Schwetje: Zeichengabesystems – Eine neue Generation für ISDN und intelligente Netze; L.T.U.-Vertriebsgesellschaft, Bremen, 1995.

Bial_94 Jacek Biala: Mobilfunk und intelligente Netze; Vieweg; Braunschweig/ Wiesbaden; 1994.

Bras_88 Gilles Brassard: Modern Cryptology - A Tutorial; LNCS 325, Springer-Verlag, Berlin 1988.

Chau_81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; CACM 24/2 (1981), Page 84-88.

Chau_88 David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability; Journal of Cryptology 1/1 (1988), Page 65-75.

ETS_300_102-1 ETSI: ISDN, User-network interface layer 3, Specifications for basic call control; December 1990.

ETS_300_343 ETSI: ISDN, Signalling interworking specification for ISDN User Part, Version 1; July 1994.

ETS_300_403-1 ETSI: ISDN, DSS1 protocol, Signalling network layer for circuit-mode basic call control, Part 1 Protocol specification; November 1995.

Fede_95 Hannes Federrath: Technischer Datenschutz in der Mobilkommunikation - Analyse von Sicherheitsproblemen in existierenden Netzen; Arbeitspapier, Dezember 1995.

FeJP_96 Hannes Federrath, Anja Jerichow, Andreas Pfitzmann: MIXes in mobile communication systems: Location management with privacy; Workshop on Information Hiding, Cambridge (UK), June 1996.

FeTh_95 Hannes Federrath, Jürgen Thees: Schutz der Vertraulichkeit der Aufenthaltsortes von Mobilfunkteilnehmern; Datenschutz und Datensicherung, DuD 6/95, Seite 338-348.

FFJM_97 Hannes Federrath, Elke Franz, Anja Jerichow, Jan Müller, Andreas Pfitzmann: Ein Vertraulichkeit gewährendes Erreichbarkeitsverfahren - Schutz des Aufenthaltsortes in künftigen Mobilkommunikationssystemen; KiVS 97, GI/ITG Fachtagung Kommunikation in Verteilten Systemen, Braunschweig, Februar 1997.

Frey_94 L. Frey: The Possible Use of Public Key Cryptosystems for UMTS; RACE Mobile Telecommunications Workshop, Amsterdam, May 1994, Page 364-368.

FuBr_94 Woldemar F. Fuhrmann, Volker Brass: Performance Aspects of the GSM Radio Subsystem; Proceedings of the IEEE, Vol. 82, No. 9, September 1994.

GSM_03.20 ETSI: ETSI/TC GSM: 03.20 Security Related Network Functions; Version 4.3.1; September 1994.

GSM_04.03 ETSI: ETSI/TC GSM: 04.03 MS-BS Interface - Channel Structures and Access Capabilities; Version 3.0.3; November 1988.

GSM_04.06 ETSI: ETSI/TC GSM: 04.06 MS-BSS Interface Data Link Layer Specification; Version 4.4.0; 1994.

GSM_04.08 ETSI: ETSI/TC GSM: 04.08 Mobile Radio Interface Layer 3 Specification; Version 4.10.1; February 1995.

GSM_09.02 ETSI: ETSI/TC GSM: 09.02 Mobile Aplication Part (MAP) specification; Version 4.9.1; February 1995.

GSM_09.10 ETSI: ETSI/TC GSM: Information element mapping between MS - BSS and BSS-MSC Signalling procedures and the MAP; Version 4.2.2; February 1995.

ITU_Q.700 ITU-T: Q.700 Specification of Signalling System No. 7, Introduction to CCITT Signalling System No. 7; 1994.

ITU_Q.701 ITU-T: Q.701 Specification of Signalling System No. 7, Functional Description of the Message Transfer Part (MTP) of Signalling System No. 7; 1994.

ITU_Q.711 ITU-T: Q.711 Specification of Signalling System No. 7, Functional Description of the Signalling Connection Control Part (SCCP); 1994.

ITU_Q.763 ITU-T: Q.763 Specification of Signalling System No. 7, Formats and Codes of the ISDN User Part of Signalling System No. 7; March 1993.

Jabb_92 Bijan Jabbari: Intelligent Network Concepts in Mobile Communications; IEEE Communications Magazine, February 1992, Page 64-69.

KaKö_91 Andreas Kanbach, Andreas Körber: ISDN-Technik; Hüthig Buch Verlag; Heidelberg; 1991.

KeMe_90 Timothy J. Kearns, Maureen C. Mellon: The Role of ISDN Signalling in Global Networks; IEEE Communications Magazine Vol. 28, No. 7, July 1990, Page 36-43.

KiOg_90 Kenichi Kitami, Kazuhiko Ogawa: Current Role and Future Evolution of the ISDN Signalling System in NTT´s Network; IEEE Communications Magazine Vol. 28, No. 7, July 1990, Page 78-83.

Klei_75 Leonard Kleinrock: Queueing Systems - Volume 1: Theory; Wiley, New York 1975.

MoPa_92 Michel Mouly, Marie-Bernadette Pautet: The GSM System for Mobile Communications; published by M. Mouly, M.-B. Pautet; 1992.

MoSk_90 Abdi R. Modarressi, Ronald A. Skoog: Signalling System No. 7: A Tutorial; IEEE Communications Magazine Vol. 28, No. 7, July 1990, Page 19-35.

Pfit1_83 Andreas Pfitzmann: Ein dienstintegrierendes digitales Vermittlungs-/ Verteilnetz zur Erhöhung des Datenschutzes; Fakultät für Informatik, Interner Bericht 18/83, Universität Karlsruhe 1983.

Pfit_89 Andreas Pfitzmann: Dienstintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; Universität Karlsruhe; Fakultät für

Informatik; Dissertation; Feb. 1989; IFB 234; Springer Verlag; Heidelberg; 1990.

Pfit_93 Andreas Pfitzmann: Technischer Datenschutz in öffentlichen Funknetzen; Datenschutz und Datensicherung, DuD 17/8, 1993, Seite 451-463.

PfPf_89 Andreas Pfitzmann, Birgit Pfitzmann: How to Break the Direct RSA-Implementation of MIXes; Eurocrypt ´89, LNCS, Springer-Verlag, Berlin, 1989.

PfPW_88 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Datenschutz garantierende offene Kommunikationsnetze; Informatik Spektrum 11/3, 1988, Seite 118-142.

PfPW_89 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2•64+16)-kbit/s-Teilnehmeranschluß; Datenschutz und Datensicherung DuD, Nr. 12/1989, Seite 605-622.

PfPW_91 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes-Untraceable Communication with Very Small Bandwidth Overhead; Proc. Kommunikation in Verteilten System, IFB 267, Springer Verlag, Heidelberg 1991, Seite 451-463.

PoMG_95 Gregory P. Pollini, Kathleen S. Meier-Hellstern, David J. Goodman: Signalling Traffic Volume Generated by Mobile and Personal Communications; IEEE Communications Magazine, June 1995, Page 60-65.

Sedl_88 H. Sedlak: The RSA cryptography processor; Eurocrypt ´87, LNCS 304, Springer Verlag, Berlin 1988, Page 95-105.

Siem_89 Siemens Topic 8: Zentrales Zeichengabesystem Nr. 7 (CCS7); Herausgegeben vom Bereich Öffentliche Kommunikationsnetze; München; 1989.

Stol_92 Helmut Stolz: Kommunikationssicherheit für Fax- und Voice-Anwendung; aus Kommunikation und Sicherheit; TeleTrust Deutschland e.V.; Bad Vilbel - Darmstadt; 1992

Tele_95 Deutsche Telekom: Telesec - Das neue System für authentische und vertrauliche Kommunikation; Siegen; 3/1995

Waid_89 Michael Waidner: Unconditional Sender and Recipient Untraceability in spite of Active Attacks; Eurocrypt ´89, LNCS, Springer-Verlag, Berlin 1989.

WaPf1_89 Michael Waidner, Birgit Pfitzmann: The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability; Eurocrypt ´89, LNCS, Springer-Verlag, Berlin 1989.

WaPf_89 Michael Waidner, Birgit Pfitzmann: Unconditional Sender and Recipient Untraceability in spite of Active Attacks - Some Remarks; Fakultät für Informatik, Interner Bericht 5/89, Universität Karlsruhe 1989.

WiKü_90 Gert Willmann, Paul J. Kühn: Performance Modeling of Signalling System No. 7; IEEE Communications Magazine Vol. 28, No. 7, July 1990, Page 44-56.

WiSc1_94 Gert Willmann, Michael Schopp: Protokolle der Signalisierungssystems CCITT Nr. 7: Übersicht; Unterlagen zum Hochschulkolleg ISDN-Protokolle; Universität Stuttgart; Institut für Nachrichtenvermittlung und Datenverarbeitung; 1994.

WiSc2_94 Gert Willmann, Michael Schopp: Protokolle der Signalisierungssystems CCITT Nr. 7: Signalling Connection Control Part (SCCP); Unterlagen zum Hochschulkolleg ISDN-Protokolle; Universität Stuttgart; Institut für Nachrichtenvermittlung und Datenverarbeitung; 1994.

WiSc3_94 Gert Willmann, Michael Schopp: Protokolle der Signalisierungssystems CCITT Nr. 7: Message Transfer Part (MTP); Unterlagen zum Hochschulkolleg ISDN-Protokolle; Universität Stuttgart; Institut für Nachrichtenvermittlung und Datenverarbeitung; 1994.

WiSc4_94 Gert Willmann, Michael Schopp: Protokolle der Signalisierungssystems CCITT Nr. 7: Transaction Capabilities (TC); Unterlagen zum Hochschulkolleg ISDN-Protokolle; Universität Stuttgart; Institut für Nachrichtenvermittlung und Datenverarbeitung; 1994.

WiSc5_94 Gert Willmann, Michael Schopp: Protokolle der Signalisierungssystems CCITT Nr. 7: ISDN User Part (ISDN-UP); Unterlagen zum Hochschulkolleg ISDN-Protokolle; Universität Stuttgart; Institut für Nachrichtenvermittlung und Datenverarbeitung; 1994.

Erklärung:

Hiermit erkläre ich, daß ich die vorliegende Arbeit selbstständig angefertigt sowie keine anderen als die angegebenen Hilfsmittel verwendet habe.

Dresden, den 28. Februar 1997

_____

Jan Müller