Proc. Verläßliche IT-Systeme (VIS'97), DuD Fachbeiträge, Vieweg 1997, 191-210.

Unbeobachtbarkeit in Kommunikationsnetzen

Hannes Federrath, Anja Jerichow, Jan Müller, Andreas Pfitzmann
Technische Universität Dresden, Institut für Theoretische Informatik, 01062 Dresden
{federrath@, jerichow@, jm4@, pfitza@}inf.tu-dresden.de

Zusammenfassung

Es wird ein Verfahren zum Schutz der Vermittlungsdaten vorgestellt, das es den Nutzern von Kommunikationsnetzen ermöglicht, diese Netze unbeobachtbar und anonym zu nutzen. Dieses Verfahren der getakteten Mix-Kanäle [PfPW_89] basiert auf dem Mix-Netz, einer Methode für anonyme Kommunikation von D. Chaum. Die Realisierung dieses Konzeptes wird für die Kommunikationsnetze ISDN und GSM angegeben. Durch die beschriebenen Modifikationen ist eine anonyme und unbeobachtbare Netznutzung ohne Einbußen bei der Datenrate des Nutzkanals trotz Echtzeitanforderungen möglich. Die Effizienz des beschriebenen Verfahrens wird untersucht.

1. Motivation

Das schnelle Wachstum der Kommunikationsnetze erfordert eine ständige Auseinandersetzung mit neuen Anforderungen an die Technik. Die Gewährleistung von Datenschutz für die Nutzer der Systeme rückt immer mehr in den Mittelpunkt. Sensible, durch die Netznutzung entstehende, personenbezogene Daten sollen nicht mißbraucht werden können. Dazu gehört nicht nur der Schutz der Nutzdaten (z.B. Bild, Ton und Text), der durch Ende-zu-Ende Verschlüsselung gewährleistet werden kann, sondern auch der Schutz der Vermittlungsdaten (z.B. Adressen der Kommunikationspartner, Beginn, Dauer und Dienstart). Es wird gezeigt, daß sich Unbeobachtbarkeit und Anonymität von Teilnehmern bei der Signalisierung von Verbindungswünschen, Location Updates und anschließender Kommunikation bereits mit der zur Verfügung stehenden Bandbreite bestehender Kommunikationsnetze realisieren läßt.

Die bekanntesten Techniken für anonyme Kommunikation sind Mixe [Chau_81] und DC-Netze [Cha8_85, Chau_88]. Da das DC-Netz es erfordert, daß jeder Netzabschluß im physikalischen Sinne mindestens halb soviel sendet, wie alle Netzabschlüsse zusammen im logischen Sinne senden, ist dieses Konzept auf den existierenden schmalbandigen Signalisierungskanälen nicht realisierbar. Unter der gesetzten Zielstellung, vorhandene Netze zu modifizieren und nicht neue Netze zu entwerfen, kommt (entsprechend [PfPW_89]) nur das Mix-Netz in Frage.

Kapitel 2 stellt das Prinzip der getakteten Mix-Kanäle in allgemeingültiger Form vor. Anschließend wird in Kapitel 3 und 4 die Realisierung von anonymer Signalisierung am Beispiel von ISDN und GSM beschrieben. Die dafür notwendigen Modifikationen der Netzstrukturen, Signalisierungsprotokolle und Signalisierungsnachrichten werden in dieser Arbeit angegeben. In Kapitel 5 erfolgen Effizienzuntersuchungen zum beschriebenen Verfahren für ISDN und GSM.

2. Einführung der getakteten Mix-Kanäle

Die Kenntnis des Grundprinzips eines Mix-Netzes [Chau_81], mit den Verbesserungen aus [PfPW_89] zur Vermeidung der Angriffsmöglichkeiten aus [PfPf_89] wird in dieser Arbeit vorausgesetzt. Annahmen zum genutzten Mix-Netz:

- Es werden Mix-Kaskaden im Schubbetrieb genutzt. Diese können am einfachsten innerhalb der Vermittlungsstellen (Vst) des Kommunikationsnetzes implementiert werden.
- Alle Teilnehmer, die an dieselbe Vst angeschlossen sind, bilden dadurch eine Anonymitätsgruppe. Teilnehmeraktionen lassen sich nur einer Anonymitätsgruppe zuordnen, keinem einzelnen Teilnehmer.
- Für alle Mix-Nachrichten, die auf Teilnehmern exklusiv zugeordneten Kanälen übertragen werden, wird Dummy Traffic eingeführt, damit das physische Senden und Empfangen unbeobachtbar ist.

Das Mix-Netz eignet sich in dieser Form besonders für die unbeobachtbare Übertragung einzelner Nachrichten. Da für Telefonie-Dienste aber unbeobachtbare Kommunikationskanäle mit strengen Echtzeitanforderungen benötigt werden, muß das Mix-Konzept modifiziert werden. Analog der *hybriden Verschlüsselung* sollen im folgenden symmetrische unbeobachtbare Kanäle (Mix-Kanäle) durch eine asymmetrische Setup-Nachricht aufgebaut werden (siehe Abb. 2.1). Vollduplex-Kanäle werden im folgenden als zwei gegenlaufende Simplex-Kanäle betrachtet. Jeder Teilnehmer muß sowohl als Sender *S* als auch als Empfänger *E* in einer Kommunikationsbeziehung unbeobachtbar sein. Aus diesem Grund muß jeder Teilnehmer vor einer Kommunikation für sich einen unbeobachtbaren Sendekanal (ZS-Setup) und einen unbeobachtbaren Empfangskanal (ZE-Setup) aufbauen. Dadurch wird nicht nur die Unbeobachtbarkeit gegenüber Dritten gewährleistet, es bleiben auch beide Kommunikationspartner voreinander unerkannt.

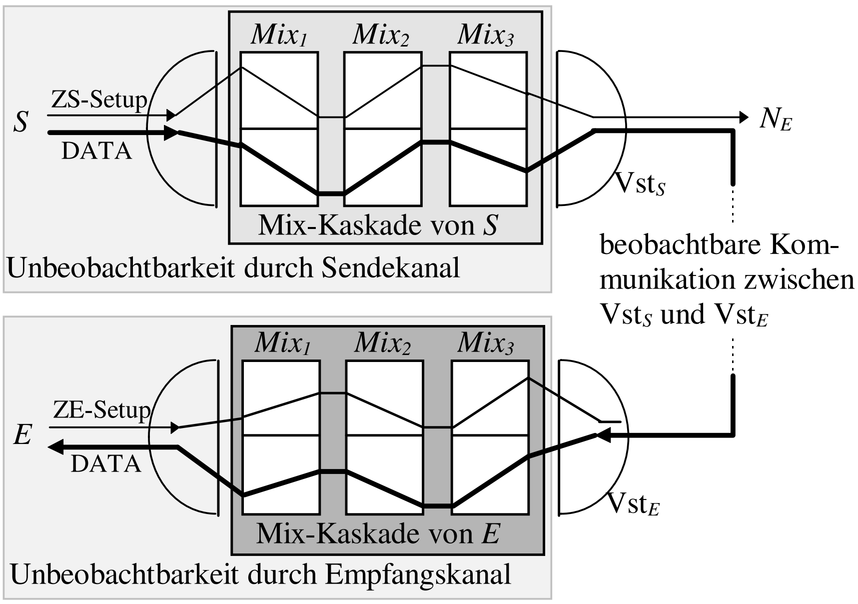

Abb. 2.1: Prinzip der Mix-Kanäle am Beispiel eines Simplex-Kanals von *S* nach *E*

Eine *Kanalaufbaunachricht* wird mit den öffentlichen Schlüsseln c_j der Mixe M_j der Kaskade der nächsten Vst asymmetrisch verschlüsselt. Mit dieser Nachricht wird jedem Mix M_j ein vom Teilnehmer gewählter symmetrischer Schlüssel k_{xyj} (x Sender/Empfänger, y Sende-/Empfangskanal, j Nummer des Mixes) für die folgende Signalisierung und Kommunikation übergeben. Außerdem speichert jeder Mix die Position dieser Nachricht in seinem Eingabeschub zusammen mit der Position dieser Nachricht im Ausgabeschub (nach der Umsortierung). Diese Zuordnung bleibt dann, ebenso wie der symmetrische Schlüssel, während der Kommunikation gleich.

Das bis zu dieser Stelle beschriebene Verfahren kann allerdings in dieser Form noch nicht eingesetzt werden. Forderungen an die Kanalaufbaunachrichten:

- Damit die Aktionen der Teilnehmer nicht beobachtbar sind, müssen Kanalaufbaunachrichten gleichzeitig gesendet werden und gleich viele Kanäle belegt werden.
- Außerdem müssen gleichzeitig aufgebaute Kanäle auch gleichzeitig wieder abgebaut werden, da die Nachrichten eines Schubes gleich lang sein müssen. Dadurch wird eine effektive Nutzung der zwei Nutzkanäle (ISDN) auch innerhalb einer kleineren Anonymitätsgruppe unmöglich.

Deshalb wird ein Systemtakt t_i (auch Zeitscheibe genannt) eingeführt. Der Systemtakt ermöglicht den Teilnehmern, unbeobachtbare Verbindungen, also unbeobachtbare Ende-zu-Ende-Kanäle von beliebiger Dauer zu unterhalten, die trotzdem von jedem Kommunikationspartner regelmäßig abgebaut werden können. Durch die Einführung der Zeitscheiben werden beliebig lang andauernde Verbindungen auf mehrere kurze (ca. 1s) und unmittelbar aufeinanderfolgende Mix-Kanäle, im folgenden *Zeitscheibenkanäle* genannt, aufgeteilt. Zu Beginn jeder Zeitscheibe hat jeder Teilnehmer die Möglichkeit, eine neue Verbindung aufzubauen, oder eine bestehende abzubrechen. Dieser Systemtakt erfolgt synchron für alle Teilnehmer des gesamten Netzes. Die Zeitscheibenkanäle werden im folgenden Zeitscheiben-Sende-(ZS)-Kanal und Zeitscheiben-Empfangs-(ZE)-Kanal genannt.

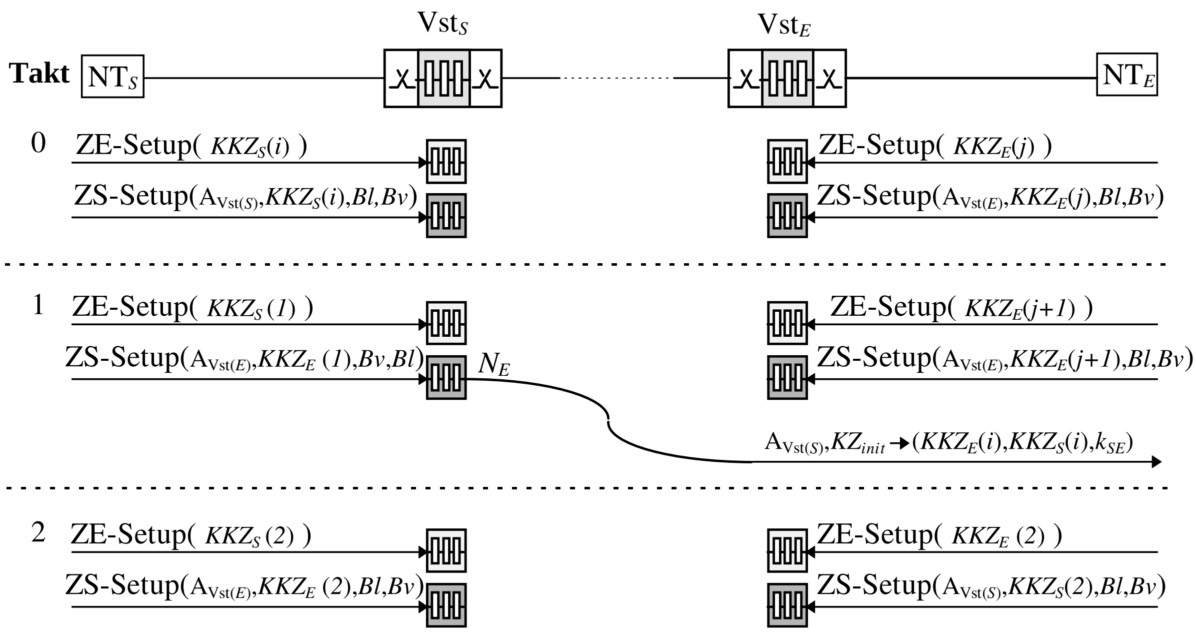

Abb. 2.2: Vereinfachter Beispielablauf eines Verbindungsaufbaus

Abb. 2.2 zeigt den vereinfachten Ablauf eines Verbindungsaufbaus. 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).[1]

Mit dem Einsatz dieses Verfahrens muß außerdem die Übermittlung der Verbindungswunschnachricht N_E verändert werden, damit dadurch keine Beobachtungsmöglichkeiten entstehen. N_E ist so in die ZS-Setup-Nachricht codiert, daß sie erst auf der Netzseite der Vst im „Klartext" vorliegt. Anschließend kann diese Nachricht, wie bisher, zur Vst des Empfängers signalisiert werden. Dort muß sie allerdings an alle Teilnehmer einer Anonymitätsgruppe zuverlässig verteilt werden, damit das Empfangen der Verbindungswunschnachricht keine Beobachtungsmöglichkeiten bietet (Takt 1). Diese Nachricht kann nur der „gewünschte" Empfänger korrekt entschlüsseln. Die darin enthaltenen Informationen benötigt der Empfänger zum Aufbau seiner unbeobachtbaren Sende- und Empfangskanäle, z.B. Angaben (Kanalkennzeichen (*KKZ*)) zur Verkettung der unbeobachtbaren Kanäle beider Teilnehmer. Für jeden Sendekanal wird die Zieladresse $A_{Vst(x)}$ und das KKZ_x des dortigen Empfangskanals beim Kanalaufbau in der Netzseite der Vst gespeichert, für einen Empfangskanal wird nur das aktuelle *KKZ* gespeichert. Für diese *KKZs* wird zu Beginn ein Initialwert KZ_{init} ausgetauscht, aus dem die *KKZ* der beiden Empfangskanäle berechnet werden. Diese werden mit einem Pseudozufallsgenerator in jedem Takt „weitergeschaltet".

Damit nicht beobachtbar ist, wann ein Teilnehmer einen Verbindungswunsch hat, muß auch für die Verbindungswunschnachricht Dummy Traffic signalisiert werden. Dieser sollte für die Netzseite einer Vst (vorher jedoch auf keinen Fall) als Dummy Traffic erkennbar sein (erste *Bv*/*Bl*-Kennzeichnung in ZS-Setup), damit solche Verbindungswünsche nicht verteilt werden müssen. Außerdem sollte eine analoge Kennzeichnung in der ZS-Setup-Nachricht für die übertragenen Nutzdaten erfolgen (zweite *Bv*/*Bl*-Kennzeichnung in ZS-Setup). Während eines Verbindungsaufbaus wird das Fernnetz dann nicht unnötig belastet. Wenn ein Teilnehmer einen Kommunikationskanal nicht benötigt, baut er mit Dummy Traffic eine Verbindung zu seinem eigenen Empfangskanal auf und sendet Dummy Traffic-Daten an sich selbst (Takt 0).

Kommunikationskanäle im Fernnetz werden nicht in jeder Zeitscheibe auf- und abgebaut. Einmal zum Beginn der Kommunikation belegt, werden sie erst am Ende wieder freigegeben. Dadurch wird lediglich beobachtbar, wieviele Kommunikationsbeziehungen zwischen verschiedenen Anonymitätsgruppen bestehen.

Zur Gewährleistung isochroner Kommunikationsdienste muß der Aufbau und die Nutzung unbeobachtbarer Kanäle parallel erfolgen. Diese werden mit den ausgetauschten symmetrischen Schlüsseln stets erst während der nächsten Zeitscheibe genutzt.

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

---

[1] siehe Mix-Grundprinzip.

zur Abrechnung bei unbeobachtbarer Netznutzung können in [PfPW_89] nachgelesen werden.

3. Realisierung getakteter Mix-Kanäle in ISDN

Um für die Teilnehmer anonyme Signalisierung von Verbindungswunsch-, Kanalaufbau- und Kanalabbaunachrichten im ISDN gewährleisten zu können, muß die Netzstruktur, wie in Abb. 3.1 beschrieben, modifiziert werden:

- In den Ortsvermittlungsstellen (LE: Local Exchange) sind Mix-Kaskaden nötig.
- Ein Teil der Mix-Kaskade liegt in der Signalisier- und der andere Teil liegt in der Nutzkanalebene.

Die Nutzerseite einer LE erhält in jedem Takt des Kommunikationssystems von jedem angeschlossenen Teilnehmer (NT: Network Termination) sowohl Nachrichten auf dem Signalisierungskanal (D-Kanal) mit 16kbit/s, als auch auf den 2 Datenkanälen (B-Kanäle) mit je 64kbit/s. Diese Nachrichten sind ggf. bedeutungslos (Dummy Traffic). Für die Nutzerseite einer LE ist das allerdings nicht erkennbar. Sie kann keine Rückschlüsse auf eine bestehende Kommunikationsbeziehung bestimmter Teilnehmer ziehen.

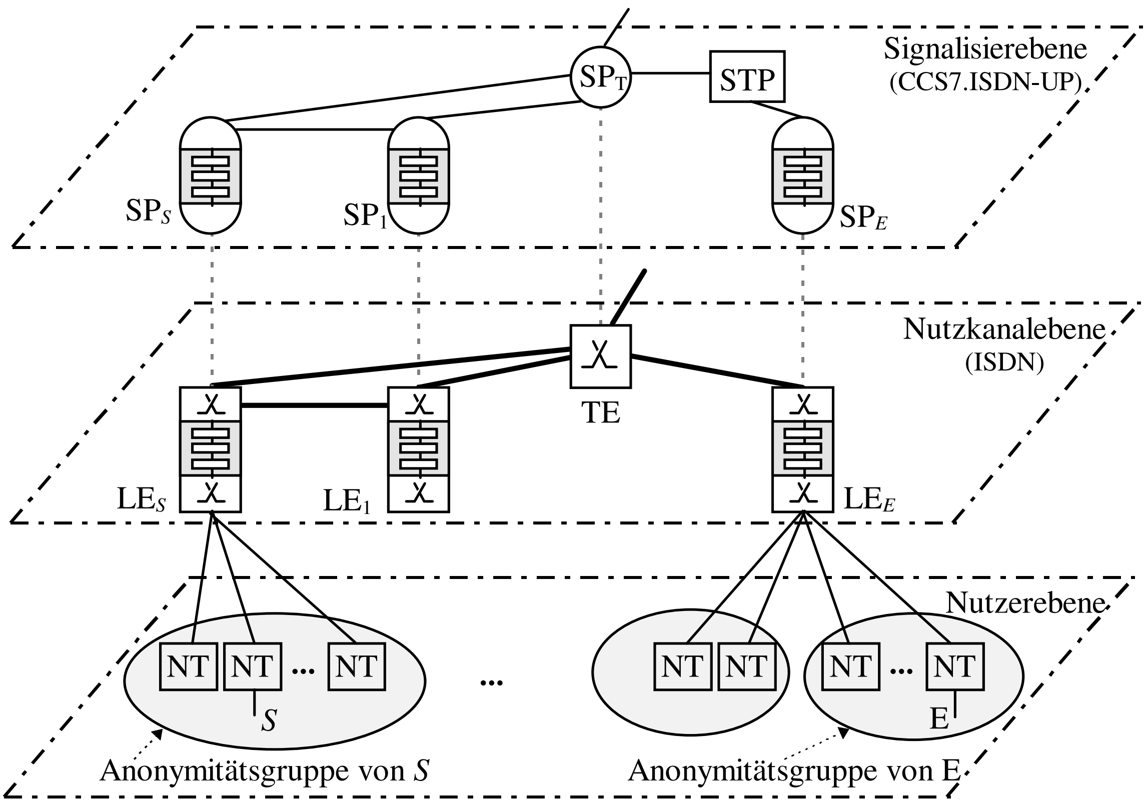

Abb. 3.1: Modifizierte Netzstruktur von ISDN

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

Neben der Netzstruktur von ISDN sind folgende Modifikationen des Signalisierungsprotokolls zum Verbindungsaufbau notwendig (siehe Abb. 3.2):

- Modifikation des Digital Subscriber Signalling System No. 1 (DSS1)-Protokolls zwischen den NTs und der LE.
- Einführung eines Mix-Protokolls innerhalb der Mix-Kaskade.
- Modifikation des Common Channel Signalling System No. 7 (CCS7)-ISDN-User Part (UP)-Protokolls zwischen den LEs.

Zum Aufbau einer unbeobachtbaren Kommunikationsverbindung initiiert der Sender S den Aufbau eines unbeobachtbaren ZE-Kanals durch die entsprechende DSS1-Nachricht über den Signalisierungskanal. Außerdem baut er einen ZS-Kanal für das unbeobachtbare Senden von Informationen auf. Die Netzseite der LE des Senders erhält mit der ZS-Setup-Nachricht die im CCS7-Netz zu sendende Verbindungswunschnachricht und die Adresse $A_{LE(E)}$ und sendet eine Initial Address Message (IAM) ab. Mit der im CCS7-Netz zum Empfänger gerouteten IAM wird bereits ein Kommunikationskanal bis zur LE_S belegt und geschaltet. Die mit der IAM im LE_E eintreffende Nachricht an den Empfänger E wird an alle angeschlossenen Teilnehmer der LE mittels einer DSS1-incoming call-Nachricht verteilt.

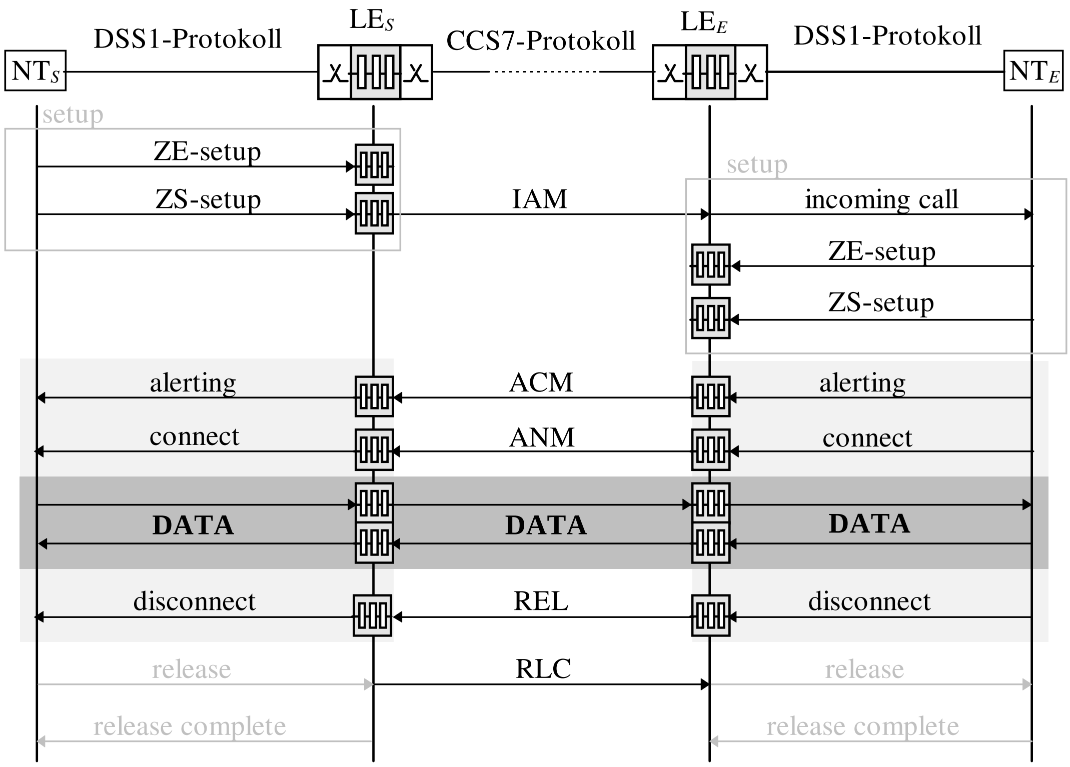

Abb. 3.2: Modifiziertes Protokoll des Verbindungsaufbaus in ISDN

Der gewünschte E kann als einziger die empfangene Verbindungswunschnachricht korrekt entschlüsseln. In dieser Nachricht erhält E alle notwendigen Informationen zum Aufbau der Verbindung. Dieser muß jetzt selbst aktiv werden und einen entsprechenden ZE-Kanal sowie ZS-Kanal aufbauen. Dadurch wird die Verbindung durchgängig geschaltet. Um Bandbreite auf dem schmalbandigen Signalisierungskanal zu sparen, wird der Zustand des Klingelns des Empfängertelefons mit der Alerting-Nachricht bereits im Datenkanal übertragen. Sobald der Empfänger abhebt, wird dies mit der Connect-Nachricht dem Sender über den Datenkanal mitgeteilt. Im Fernnetz werden die Signalisierungsnachrichten weiterhin im Signalisierungskanal übertragen. Die in Abb. 3.2 hellgrau hinterlegten Flächen gehören also bereits zum Datenkanal, wobei die eigentliche Datenübertragung in der Abbildung dunkelgrau dargestellt ist. Außerdem verdeutlichen die hellgrau geschriebenen Nachrichten den ursprünglichen Protokollablauf.

Durch Änderung des Protokolls ändert sich auch der Inhalt der Signalisierungsnachrichten. In dieser Arbeit sollen die notwendigen Modifikationen nur am Beispiel der ZS-Setup-Nachricht des Senders für eine Mix-Kaskade mit 3 Mixen angegeben werden.[2]

$$N_{\text{ZS-Setup}(S)} := k_{S1}(t_i,\ c_2(t_i,\ k_{SS2},\ c_3(t_i,\ k_{SS3},\ \mathrm{A}_{\mathrm{LE}(E)},\ KKZ_E(i),\ Bv/Bl,\ Bv/Bl,\ N_E)))$$

$$\text{mit}\quad N_E := c_E\,(\text{call\_setup\_msg},\ t_i,\ \mathrm{A}_{\mathrm{LE}(S)},\ KZ_{init})$$

Zur Vereinfachung hat jeder Teilnehmer mit dem ersten Mix bereits einen symmetrischen Schlüssel k_{S1} fest vereinbart, da diesem Mix ohnehin bekannt ist, wer sendet. Durch diese Modifikationen ändert sich die Länge der Signalisierungsnachrichten. Hinzu kommt, daß in jeder Zeitscheibe jeder Teilnehmer signalisieren und Daten senden muß (notfalls Dummy Traffic). Dadurch ändert sich die Performance im ISDN beträchtlich. In Kapitel 5 werden die notwendigen Effizienzuntersuchungen durchgeführt, und es wird nachgewiesen, daß sich dieses Verfahren ohne Einbußen bei der Datenrate auf dem Nutzkanal realisieren läßt.

4. Realisierung getakteter Mix-Kanäle in GSM

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. In GSM sind für die Realisierung des Verfahrens folgende Annahmen nötig (siehe Abb 4.1):

- Eine Erweiterung der Ortsvermittlungsstellen (MSC: Mobile Switching Center) und deren Signalisierungspunkte um Mix-Funktionalität ist notwendig.
- Die Größe der Anonymitätsgruppe eines Mobilteilnehmers ist dynamisch. Sie besteht aus allen Mobilteilnehmern, die sich zur Zeit in einem Location Area (LA) aufhalten, das von demselben MSC verwaltet wird.
- Die Mixe im MSC schützen den Aufenthaltsort des Teilnehmers innerhalb eines MSC-Bereiches, d.h. ein MSC sollte möglichst viele verschiedene LAs verwalten.
- Durch diese Mixe werden außerdem bestehende Kommunikationsbeziehungen geschützt.
- Zusätzlich muß in GSM der Signalisierungspunkt des HLRs um Mix-Funktionalität erweitert werden. Dadurch wird bei einem Location Update geschützt, aus welchem MSC-Bereich Änderungen vorgenommen werden. Bei einem Verbindungswunsch

---

[2] In [Müll_97] sind die Modifikationen der Nachrichteninhalte mit den notwendigen Änderungen der Protokolle im DSS1 und CCS7 detailliert beschrieben.

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.[3]

An dieser Stelle soll jedoch auf die stets existierende Möglichkeit der Peilung und Ortung einer sendenden Mobilstation hingewiesen werden, die auch durch DS/SS (siehe [FeTh_95]) nicht ganz verhindert werden kann.

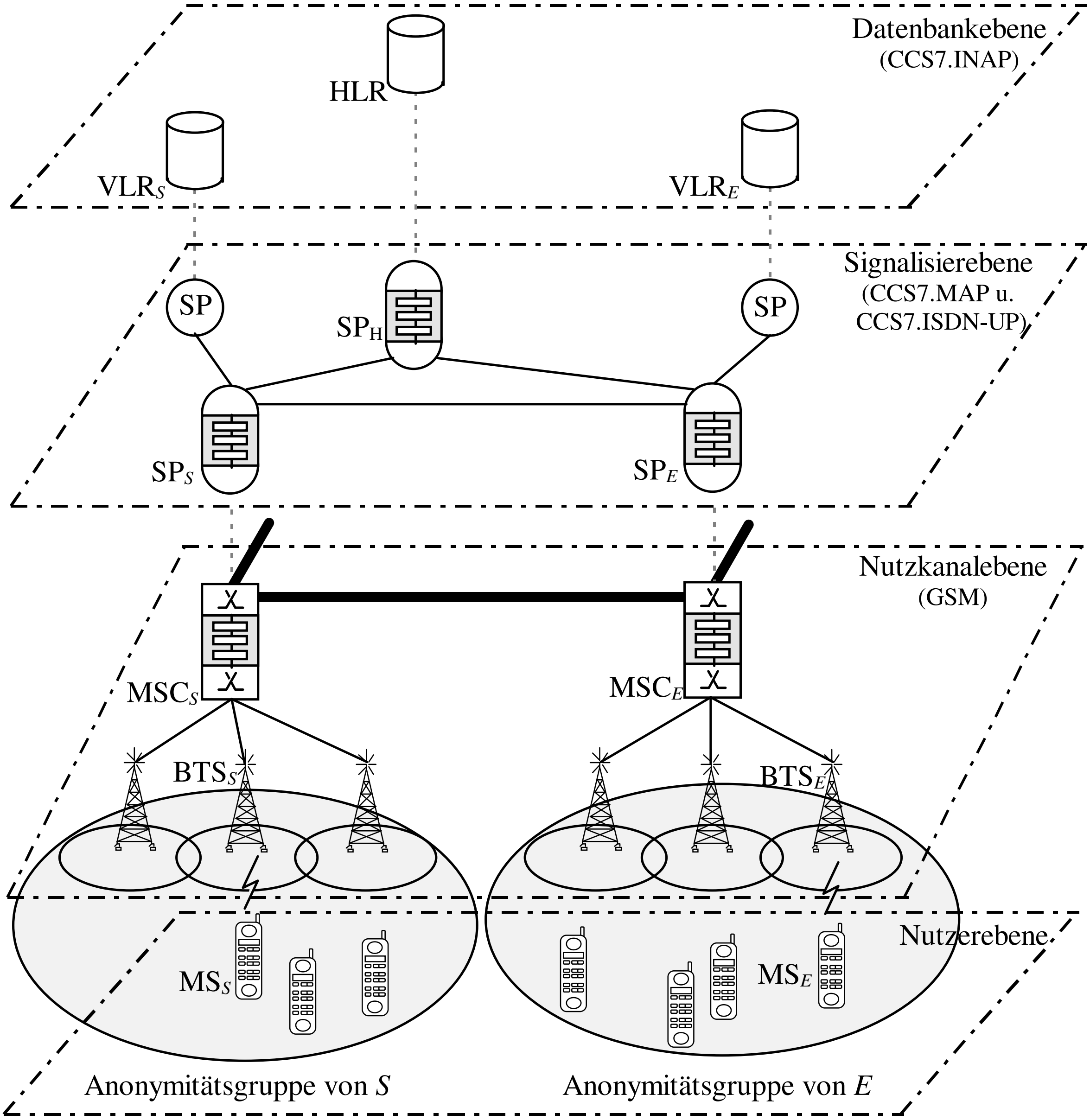

Abb. 4.1: Modifizierte Netzstruktur von GSM

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 Unbeobachtbar-

---

[3] 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.

keit 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.

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 (siehe Abb. 4.2). Auch diese Nachrichten müssen aus den in Kapitel 2 genannten Gründen getaktet werden. Allerdings kann dieser LUP-Takt deutlich länger (ca. 10s) sein, da LUPs nicht so häufig notwendig sind.

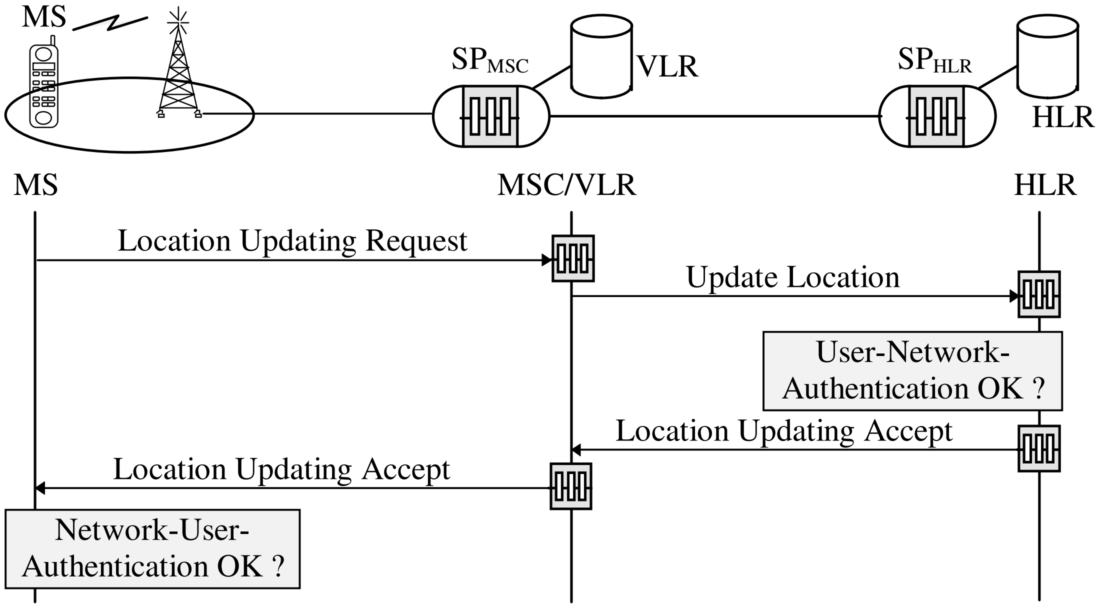

Abb. 4.2: Modifiziertes Protokoll des Location Updates

Die Mobilstation (MS) nutzt die Mix-Kaskade des MSCs, um eine anonyme Rückadresse {LAI,IAdr}[4] 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. Dem HLR wird diese vorbereitete Nachricht über dessen Mix-Kaskade signalisiert. Im HLR wird die Authentikation des Teilnehmers durchgeführt und anschließend dessen verdeckte Aufenthaltsinformation {VLR,P} gespeichert. Die Quittung kann anschließend symmetrisch verschlüsselt zum MSC/VLR und weiter zum Teilnehmer signalisiert werden. Die Einzelheiten der verbesserten gegenseitigen Authentikation sind in [Müll_97] beschrieben.

Das Signalisierungsprotokoll des Verbindungsaufbaus (Call Setup) wird bei GSM in zwei Teile geteilt. Der erste Teil ist das Mobile Originated Call Setup (MOC-Setup),

---

4 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.

ein von der MS ausgehender Ruf, und der zweite Teil ist das Mobile Terminated Call Setup (MTC-Setup), ein die MS erreichender Ruf.

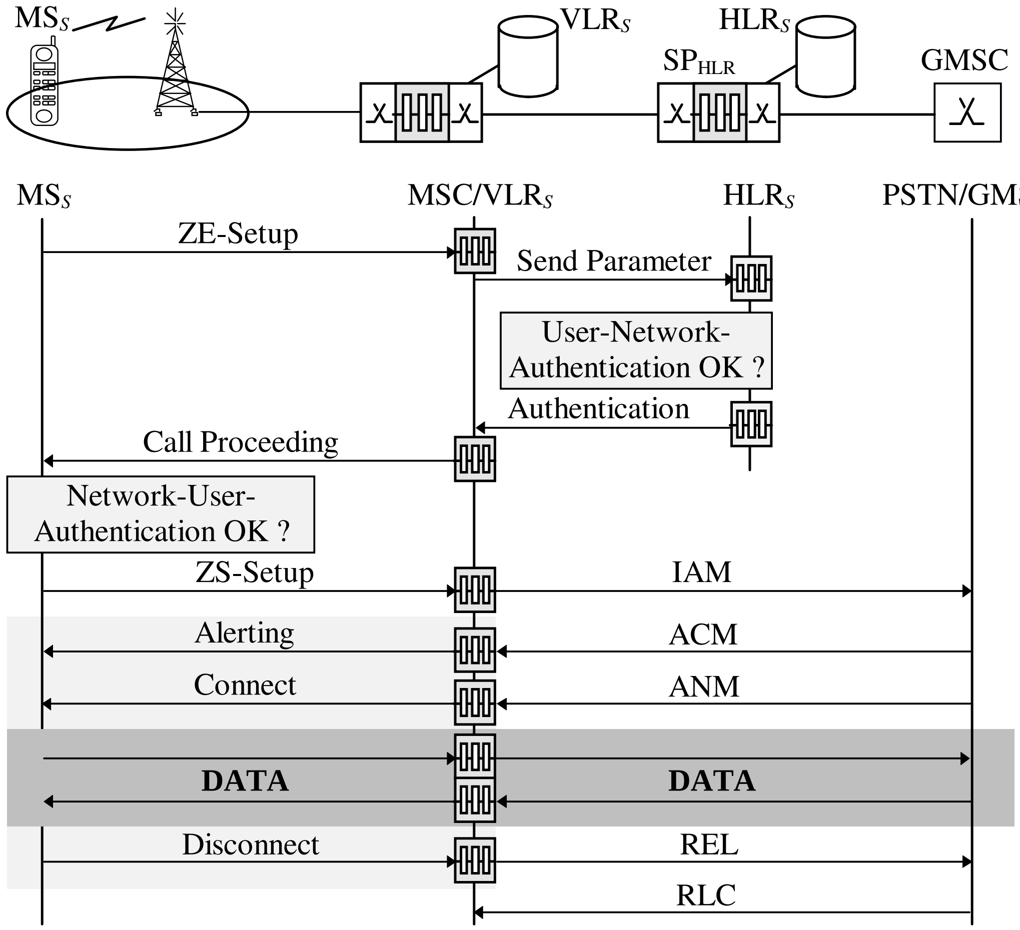

Abb. 4.3: Modifiziertes Protokoll des Mobile Originated Call Setup

Im folgenden sollen nur die Änderungen des MOC-Setup-Protokolls aus Abb. 4.3 beschrieben werden. Auch hier ist eine gegenseitige Authentikation vorgesehen (siehe [Müll_97]). Zuerst wird von *S* ein Signalisierungskanal (SDCCH) angefordert und ein ZE-Kanal über die Mix-Kaskade des MSC/VLR aufgebaut. Anschließend baut *S* den ZS-Kanal mit den Informationen über den Verbindungswunsch auf. Das MSC/VLR sendet darauf die IAM an das HLR_E. Dort wird die anonyme Rückadresse $\{VLR,P\}_E$ ermittelt und die IAM mit dieser Rückadresse über die Mix-Kaskade des HLRs gesendet und durch die in $\{VLR,P\}_E$ enthaltenen Informationen zum VLR_E 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 eine ACM auf dem direkten Weg sendet, wie anschließend im MTC beschrieben. Mit dieser Nachricht wird der bidirektionale Nutzkanal vollständig geschaltet. Im Netz wird bekannt, welches MSC/VLR mit welchem MSC/VLR kommuniziert. Die beteiligten Teilnehmer bleiben innerhalb der verwalteten Aufenthaltsgebiete unbeobachtbar. Während der Aufbauphase einer Verbindung bzw. wenn diese abgewiesen wird, erfährt ein Angreifer nichts über den ungefähren Aufenthaltsort

(MSC/VLR-Bereich) von *E*. Bekannt ist im Netz lediglich, daß ein Teilnehmer aus dem MSC/VLR-Bereich von *S* einen der Teilnehmer erreichen möchte, die im HLR_E eingetragen sind.

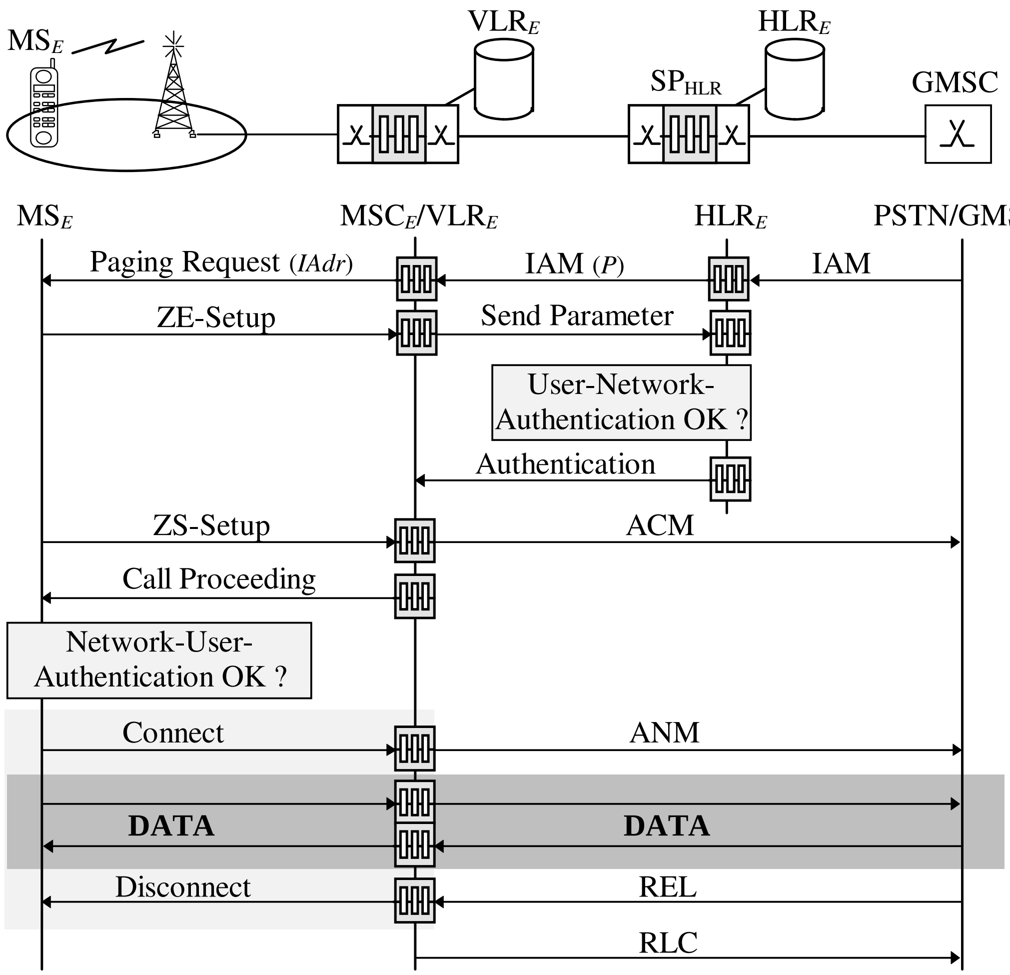

Abb. 4.4: Modifiziertes Protokoll des Mobile Terminated Call Setup

Abb. 4.4 zeigt das modifizierte Gegenstück des Verbindungsaufbaus, das MTC-Setup. Vom HLR_E wird die IAM mit der anonymen Rückadresse $\{VLR,P\}_E$ zum VLR_E weitergeleitet. Dort ist *E* 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 entsprechenden 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.

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.

Auch für GSM soll beispielhaft nur die Modifikation einer komplexen Signalisierungsnachricht mit 3 Mixen angegeben werden (ausführlicher in [Müll_97]).

$$\begin{aligned}
N_{\text{LUP-Request}} &:= c_1(t_{Li}, k_{SE1}, c_2(t_{Li}, k_{SE2}, c_3(t_{Li}, k_{SE3}, KKZ_S(Li), N_{\text{VLR}})))\\
N_{\text{VLR}} &:= c_{MSC/VLR}(\text{lup_msg}, t_{Li}, P, \{\text{LAI}, IAdr\}, Bv/Bl, N_{\text{HLR}})\\
N_{\text{HLR}} &:= c_{H1}(t_{Li}, k_{H1}, c_{H2}(t_{Li}, k_{H2}, c_{H3}(t_{Li}, k_{H3}, KKZ_{HLR}(Li), N_{\text{HLR}}*)))\\
N_{\text{HLR}}* &:= k_{HLRS}(\text{lup_msg}, s_{MS}(t_{Li}, RAND_1), \text{IMSI}, RAND_2, Bv/Bl, t_{Li}, \{\text{VLR}, P\})\\
\{\text{VLR}, P\} &:= c_{H3}(k_{H3}, c_{H2}(k_{H2}, c_{H1}(k_{H1}, \text{A}_{\text{VLR}}, P)))\\
\{\text{LAI}, IAdr\} &:= c_3(k_{S3}, c_2(k_{S2}, c_1(k_{S1}, \text{LAI}, IAdr)))
\end{aligned}$$

Die Länge dieser LUP-Request-Nachricht erhöht sich bei der Realisierung in GSM am meisten, da der Teilnehmer diese Nachricht für die Benutzung von zwei Mix-Kaskaden vorbereiten und zwei anonyme Rückadressen für Verbindungswünsche in dieser Nachricht übertragen muß. Dennoch läßt sich das Verfahren mit geringen Modifikationen bei der Kanalvergabe und -nutzung (siehe Kapitel 5) effizient realisieren.

5. Performance-Betrachtungen

5.1 Voraussetzungen der Performanceanalyse

Festlegungen bezüglich der eingesetzten Kryptosysteme:

- Einsatz einer symmetrischen Stromchiffre,
- Einsatz einer asymmetrischen Blockchiffre,
- Einsatz von hybrider Verschlüsselung.[5]

Abb. 5.1 faßt die benötigten Parameter von ISDN und GSM zusammen. Diese wurden aus [BGGH_95] für ISDN und [GSM_04.08, GSM_09.02 und GSM_09.10] für GSM entnommen.

Parametername	Abk.	Länge	Parametername	Abk.	Länge
allgemeine Parameter:			Nutzkanalidentifikator	CIC	12 Bit
Zeitscheibennummer	t	30 Bit	Kanalkennzeichen	*KKZ*	28 Bit
Initialwert des Kanalkennzeichens	KZ_{init}	128 Bit	Block des asym. Systems	b_{asym}	660 Bit
Schlüssel des symmetrischen Systems	s_{sym}	128 Bit	digitale Signatur	$s_{MS}(N)$	200 Bit
bedeutungsvoll/-los Kennzeichen	*bv/bl*	1 Bit	Anzahl der MIXe	*m*	10 Stück
ISDN-Parameter:			Adresse eines Local Exchanges	A_{LE}	14 Bit
GSM-Parameter:			Implizite Adresse	*IAdr*	128 Bit
International Mobile Subscriber Identity	IMSI	60 Bit	Intern. 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

Abb. 5.1: Länge der Parameter in den Kommunikationsnetzen

Abb. 5.2 zeigt die Länge der Signalisierungsnachrichten bisher, sowie die berechnete Länge der modifizierten Nachrichten mit 10 eingesetzten Mixen pro Kaskade für ISDN

[5] Bei hybrider Verschlüsselung 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.

und GSM. Die bisherige Länge im DSS1 wurde aus [ETS_300_403-1] ermittelt, im CCS7-ISDN-UP aus [ITU_Q.763], im RIL3[6] aus [GSM_04.08] und im CCS7 Mobile Application Part (MAP) aus [GSM_09.02]. Parameter mit einer variablen Länge innerhalb bestimmter Grenzen mit ihrem Mittelwert und solche mit variabler Länge wurden mit dem Doppelten der Mindestlänge angenommen. Außerdem wurden auch optionale Parameter zur Längenberechnung als vorhanden eingestuft, so daß die Performance in der Praxis stets besser sein sollte, als im in Abb. 5.2 dargestellt.

Signalisier-system	**Nachrichten**	**ISDN**		**GSM**	
		bisher	**10 Mixe**	**bisher**	**10 Mixe**
DSS1 bzw. RIL3	Location Updating Request	—	—	148 Bit	7578 Bit
	Location Updating Accept	—	—	124 Bit	824 Bit
	Setup	1084 Bit	—	853 Bit	—
	ZE -Setup	—	2322 Bit	—	3914 Bit
	ZS-Setup	—	2536 Bit	—	2738 Bit
	Incoming Call	—	1040 Bit	—	—
	Call Proceeding	296 Bit	—	195 Bit	948 Bit
	Paging Request	—	—	176 Bit	1420 Bit
	Alerting	296 Bit	458 Bit	280 Bit	356 Bit
	Connect	404 Bit	530 Bit	448 Bit	356 Bit
	Disconnect	204 Bit	366 Bit	416 Bit	356 Bit
CCS7. ISDN-UP	IAM	976 Bit	1166 Bit	976 Bit	1594 Bit
	ACM	1076 Bit	470 Bit	1076 Bit	470 Bit
	ANM	1216 Bit	478 Bit	1216 Bit	478 Bit
	REL	912 Bit	374 Bit	912 Bit	374 Bit
CCS7. MAP	Send Parameter from HLR	—	—	64 Bit	2098 Bit
	Authentication Parameter	—	—	324 Bit	516 Bit
	Update Location	—	—	120 Bit	3863 Bit
	Location Updating Accept	—	—	54 Bit	324 Bit

Abb. 5.2: Länge der modifizierten Signalisierungsnachrichten im Vergleich

5.2 Minimale Dauer des Systemtaktes

Jeder Teilnehmer muß für jeden Systemtakt und jeden zur Verfügung stehenden Nutzkanal eine ZE- und eine ZS-Setup-Nachricht signalisieren. Da es sich bei dem Signalisierungskanal in ISDN und GSM um einen Vollduplexkanal handelt, hat die Verteilung der Verbindungswünsche keinen Einfluß auf die Größe der Zeitscheibe. Ein Teil des Signalisierungskanals wird zur Sicherung der Daten, für einige schmalbandige Dienste benötigt. Daher soll im folgenden stets von einer etwas geringeren Datenrate ausgegangen werden. Die minimale Zeitscheibenlänge z berechnet sich wie folgt:

$$z \geq \frac{Anz_{Nutzkanäle} \cdot \left(\left| N_{ZE-Setup} \right| + \left| N_{ZS-Setup} \right| \right)}{Signalisierungskapazität}$$

Bei einem Einsatz von 10 Mixen pro Kaskade erhält man für ISDN (2 Nutzkanäle, 12kbit/s) $z \geq 0{,}81$s und für GSM (1 Nutzkanal, 0,6kbit/s) $z \geq 11{,}09$s.

In GSM existieren zur Signalisierung von Verbindungswünschen und LUPs zwei Signalisierungskanäle (SDCCH mit 0,782kbit/s und SACCH mit 0,391kbit/s). Der

---

6 Radio Interface Layer 3 Protokoll auf der Funkschnittstelle in GSM.

SDCCH soll mit 0,6kbit/s für den modifizierten Verbindungsaufbau und mit 0,18kbit/s für das modifizierte LUP genutzt werden. Der SACCH bleibt für die übrigen Signalisierungsaufgaben frei. Zur Verbesserung der Performance werden folgende Modifikationen in der Kanalvergabe und -nutzung vorgeschlagen: Der Signalisierungskanal FACCH wird bisher in GSM nur Nutzkanälen zugeordnet. Bei Aerly-TCH-Assignment wird der FACCH belegt, jedoch bisher nicht für die Signalisierung zum Verbindungsaufbau verwendet. Die Modifikation besteht darin, den ungenutzten FACCH zum Verbindungsaufbau zu verwenden. Der FACCH kann als Halfrate- (/H) mit 4,6kbit/s bzw. als Fullrate-Kanal (/F) mit 9,2kbit/s betrieben werden, wobei wiederum eine Aufteilung in Verbindungsaufbau und LUP erfolgt. Da der FACCH diese Aufgaben übernimmt, steht der SDCCH für andere Aufgaben zur Verfügung. Es wird folgende Aufteilung angenommen: FACCH/H 3,5kbit/s für Verbindungsaufbau und 1,1kbit/s für LUP bzw. FACCH/F 7,5kbit/s und 1,7kbit/s. Für letzteres beträgt die minimale Zeitscheibenlänge $z \geq 0{,}89$s.

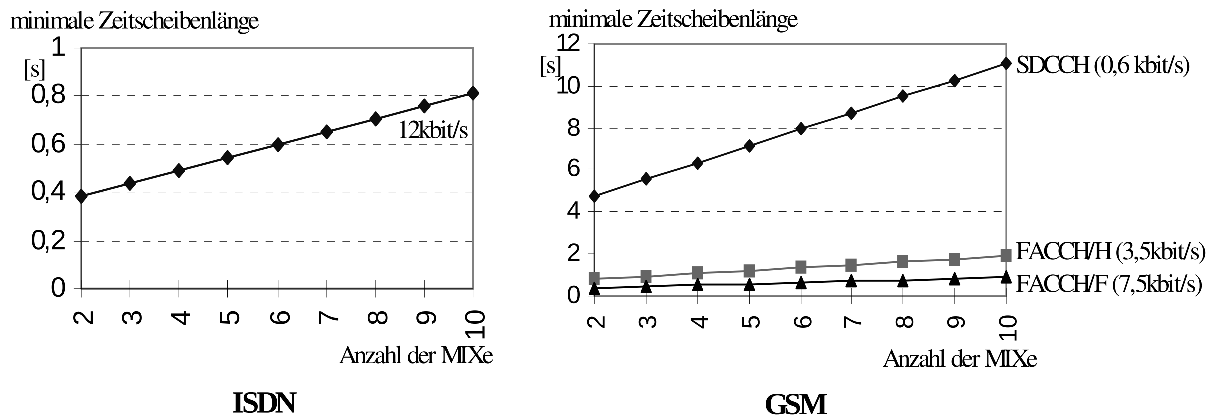

Abb. 5.3: Abhängigkeit der Zeitscheibenlänge von der Mix-Anzahl

In GSM muß zusätzlich die minimale Länge des LUP-Taktes z_{LUP} berechnet werden. Die 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

$$\lambda_{LUP} = \frac{v}{\pi \cdot r} \cdot \left(1 - \frac{N_{LA} - 1}{2 \cdot N_{LA}}\right) \text{angegeben. Es gilt } z_{LUP} \leq \frac{\left|N_{LUP-\mathrm{Re}\,quest}\right|}{Signalisierungskapazit\ddot{a}t\, t_{LUP}}.$$

Abb. 5.4 links 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.

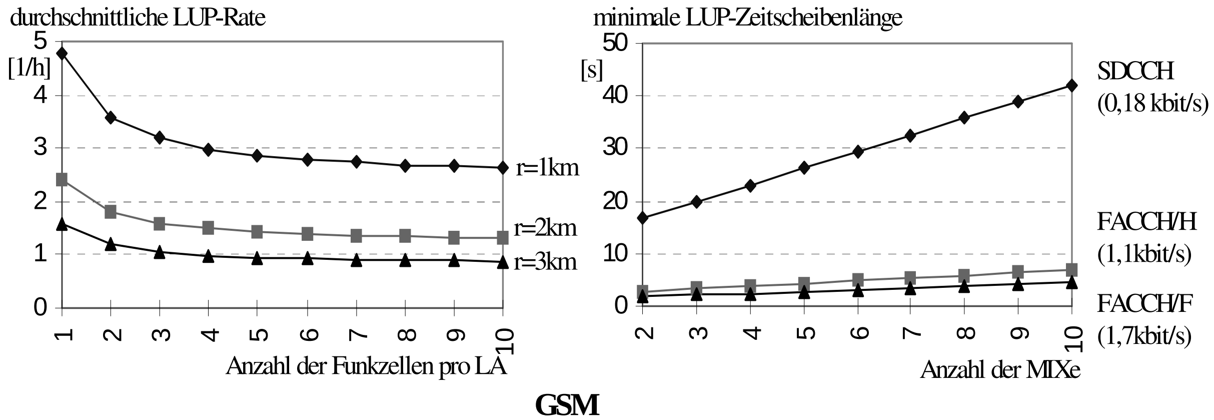

Abb. 5.4: Abhängigkeit der LUP-Zeitscheibenlänge von der Mix-Anzahl

Würde man nur den SDCCH mit 0,18 kbit/s für die LUP Signalisierung nutzen, so erhielte man für die minimale LUP-Zeitscheibe nach obenstehender Formel einen Wert von $z_{LUP} \leq 42{,}1$s. Ein Teilnehmer könnte demzufolge pro Stunde 85 LUPs durchführen, müßte aber im Mittel 21s darauf warten. Da aber in der modifizierten Variante der FACCH genutzt werden soll, kann von einer minimalen LUP-Zeitscheibenlänge von $z_{LUP} \leq 4{,}46$s ausgegangen werden.

5.3 Maximale Anzahl der von einer Mix-Kaskade bedienbaren Teilnehmer

ISDN: Die maximale Anzahl von einer Mix-Kaskade bedienbarer Teilnehmer wird durch die Verteilung der Verbindungswunschnachrichten an alle angeschlossenen Teilnehmer 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 Verbindungswünschen pro Teilnehmer und Stunde (λ =1/300 /s) in Stoßzeiten ausgegangen. Dieser Wert ist sehr hoch gewählt, in der Literatur findet man beispielsweise auch 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.

Es können maximal $\mu := b/N$ Verbindungswunschnachrichten pro Sekunde verteilt werden. Für ISDN (b=12kbit/s, N=1040Bit) erhält man $\mu = 11{,}54$ /s. T_V ist die Zeit, die ein Verbindungswunsch im Mittel benötigt, um bei den Netzabschlüssen einzutreffen (nach [PfPW_89] aus [Klei_75]), und berechnet sich wie folgt:

$$T_V = \frac{2 \cdot \mu - n \cdot \lambda}{2 \cdot \mu \cdot (\mu - n \cdot \lambda)}.\ \text{Daraus ergibt sich für n:}\quad n = \frac{\mu}{\lambda} \cdot \frac{\mu \cdot T_v \cdot -1}{\mu \cdot T_v - 0{,}5}.$$

Für $T_v \leq$ 0,5s erhält man $n \leq 3133$ Teilnehmer pro Mix-Kaskade. Geht man von nur 5 Verbindungswünschen pro Teilnehmer und Stunde (λ=1/720 /s) in Stoßzeiten aus, könnte man bereits 7520 Teilnehmer an jede Mix-Kaskade anschließen.

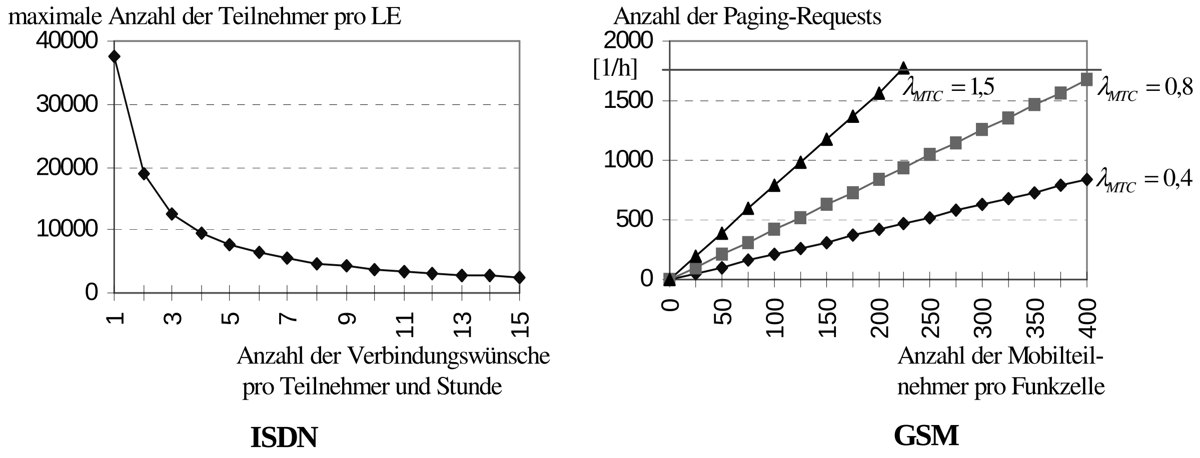

Abb. 5.5: Anzahl der bedienbaren Teilnehmer

GSM: In GSM wird die Aussendung eines Verbindungswunsches Paging genannt. Die Paging Request-Nachricht wird bei einem MTC von der BTS ausgesendet, um den Empfänger eines Verbindungswunsches davon zu unterrichten. Diese Nachricht ist 1420 Bit lang. Es wird der Signalisierungskanal PCH (0,782kbit/s simplex downlink) verwendet. Wenn davon 0,7 kbit/s genutzt werden können, dauert die Übermittlung einer Verbindungswunschnachricht 2,03s. 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) und N_{LA} die Anzahl der Funkzellen pro LA ist (N_{LA}=3). P_{KF} ist die Wahrscheinlichkeit, daß kein Funkkontakt möglich ist (P_{KF}=0,4) und P_{KA} die Wahrscheinlichkeit, daß eine MS nicht antwortet (P_{KA}=0,3).

In Abb. 5.5 rechts wird die Anzahl der notwendigen Paging Requests innerhalb einer Funkzelle in Abhängigkeit von der Anzahl der Mobilteilnehmer pro Funkzelle und deren Verkehrscharakteristik λ_{MTC} gezeigt. Da die Übermittlung einer Paging Request-Nachricht 2,03s dauert, können in einer Stunde nicht mehr als 1773 Paging-Nachrichten signalisiert werden. Dadurch wird auch die maximale Anzahl der versorgbaren Mobilteilnehmern begrenzt, wobei deren Verkehrsstatistik und die Anzahl der Funkzellen pro LA sowie deren Durchmesser ebenfalls diese Größe beeinflussen.

5.4 Verbindungsaufbauzeit

ISDN: Die Berechnung der Verbindungsaufbauzeit für ISDN 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 (≤0,2 s),
- dem Warten auf die Verteilung an den Empfänger (in Stoßzeiten im Mittel T_V≤0,5 s),
- dem Warten auf das Aufbauen des ZS-Kanals durch den Empfänger (≤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 = 0,8s) also ca. 2,5s, wobei die Verbindungsaufbauzeit im Mittel nur etwa halb so groß sein wird.

GSM: Die Berechnung der Verbindungsaufbauzeit wird für GSM entsprechend vorgenommen und setzt sich im wesentlichen zusammen aus:

- der gegenseitigen Authentikation von Sender und Netz (≤z),
- dem Warten auf die Übermittlung des Verbindungswunsches durch die Mix-Kaskade des MSCs des Senders (≤z),[7]
- der Verzögerungszeit der Mix-Kaskade des MSCs des Senders ($m \cdot 0{,}01$ s),
- der Laufzeit des Verbindungswunsches im Fernnetz zum HLR des Empfängers (≤0,2 s),
- dem Warten auf die Übermittlung des Verbindungswunsches durch die Mix-Kaskade des HLRs des Empfängers (≤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 (≤0,2 s),
- dem Warten auf die Übermittlung des Verbindungswunsches durch die Mix-Kaskade des MSC/VLRs des Empfängers (≤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≤5 s),
- der gegenseitigen Authentikation von Empfänger und Netz (≤z),
- dem Warten auf das Aufbauen des ZS-Kanals durch den Empfänger (≤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=0,9s) also ca. 11,2s, 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.

6. Ausblick

Bereits mit den Bandbreitemöglichkeiten der bestehenden Kommunikationsnetze läßt sich Unbeobachtbarkeit und Anonymität bei der Signalisierung von Verbindungswünschen und Location Updates realisieren. Im Nutzkanal entstehen keine Datenrateeinbußen. Für die Erklärung der Verfahren zur Erreichung von Teilnehmerunbeobachtbar-

---

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

keit 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, die Netzstruktur und die Protokolle entsprechend modifiziert. In den Effizienzbetrachtungen wurde 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, 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.

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. LUP-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 MS der BTS vertrauen muß, daß diese den notwendigen Dummy Traffic im Festnetz erzeugt. 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 daß sich auch diese Lösungen praktizieren lassen. Nicht untersucht wurde in GSM das Handover und die Zusatzdienste.

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

Die hier dargestellten Konzepte zeigen Möglichkeiten, die Privatsphäre der Nutzer und deren informationelle Selbstbestimmung zu gewährleisten. Dies sollte bei der rasanten Entwicklung neuer Kommunikationstechnologien und -dienste nicht vernachlässigt werden.

Literaturverzeichnis

BGGH_95 Gerhard Bandow et.al.: Zeichengabesystems – Eine neue Generation für ISDN und intelligente Netze; L.T.U.-Vertriebsgesellschaft, Bremen, 1995.

Chau_81 D. Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 84-88.

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

Cha8_85 D. Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044.

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

FeTh_95 Hannes Federrath, Jürgen Thees: Schutz der Vertraulichkeit der Aufenthaltsortes von Mobilfunkteilnehmern; Datenschutz und Datensicherung, DuD 6 (1995) 338-348.

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_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.

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

Müll_97 Jan Müller: Anonyme Signalisierung in Kommunikationsnetzen; Diplomarbeit, TU Dresden, Institut für Theoretische Informatik, 1997.

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

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, 12 (1989) 605-622.

PoMG_95 Gregory P. Pollini, Kathleen S. Meier-Hellstern, David J. Goodman: Signalling Traffic Volume Generated by Mobile and Personal Communications; IEEE Communications Magazine, 6 (1995) 60-65.