in: Wissenschaftliche Zeitschrift der TU Dresden, 44 (1995) Heft 6

Technischer Datenschutz in öffentlichen Mobilkommunikationsnetzen

Hannes Federrath[1], Anja Jerichow[1], Dogan Kesdogan[2], Andreas Pfitzmann[1]

[1]TU Dresden, Institut für Theoretische Informatik, 01062 Dresden
[2]RWTH Aachen, Informatik IV, 52056 Aachen

Zusammenfassung

Ausgehend von den schärfsten bisher formulierten Datenschutzforderungen für öffentliche Funknetze werden Datenschutzdefizite von bestehenden öffentlichen sowie geplanten Mobilkommunikationsnetzen aufgezeigt. Es wird erklärt, wie weit und wie eine Umsetzung der Datenschutzforderungen erfolgen kann. Bereits bekannte Verfahren werden vorgestellt sowie Vorschläge erörtert, die den Stand der gegenwärtigen Forschung repräsentieren.

1 Einführung

Zunächst geben wir eine Einführung, wie die Grundstruktur künftiger Mobilkommunikationsnetze aussehen wird. Ausgehend von den in solchen Netzen anfallenden Daten werden Datenschutzforderungen erhoben — unseres Wissens die schärfsten bisher formulierten.

1.1 Struktur künftiger Mobilkommunikationsnetze

Das *Universal Mobile Telecommunication System* (UMTS) wird als allgemeines Mobilkommunikationssystem der Zukunft bezeichnet. In UMTS ist die Schaffung einer gemeinsamen Plattform für existierende Systeme der zweiten Generation, beispielsweise Mobilkommunikationssysteme der Standards GSM, DECT, DCS-1800, ERMES, sowie die Integration neuer Systeme geplant. Parallel zu UMTS, das europaweit entwickelt wird, erfolgt eine weltweite Standardisierung als *Future Public Land Mobile Telecommunication System* (FPLMTS).

Die Gestaltung von UMTS ist noch nicht fest definiert. Als Basis kann eine Struktur aus den drei Komponenten Luftschnittstelle für die Mobilübertragung (*access network*), Festnetz (*core network*), welches Funktionen für die Zusammenarbeit verschiedener Netze bereitstellt, sowie IN-(*intelligent network*)-Funktionen betrachtet werden. Durch IN-Funktionen soll mehr Flexibilität erreicht werden. Das IN-Konzept kommt insbesondere den Dienstanbietern zugute, da schnell neue Dienste definier- und implementierbar sind. In UMTS werden die notwendigen Mobilitätsprozeduren (wie handover, location update u.a.) vorrangig durch IN-Funktionen realisiert.

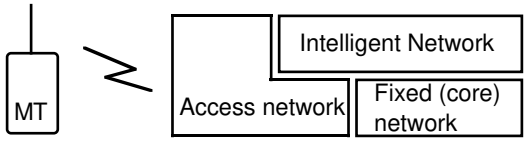

Abbildung: *Die Grundstruktur von UMTS nach [MITT 94]*

Als Festnetz-Basis soll Breitband-ISDN dienen. Das bringt den Vorteil, daß teure Netzwerkressourcen gemeinsam genutzt werden können. Ergänzend zu den terrestrischen Funknetzen ist – überlagernd – der Einsatz von Satelliten geplant.

Bei dem geradezu stürmischen Ausbau bereits standardisierter öffentlicher Funknetze sowie den neueren Projekten wie UMTS/FPLMTS muß dringend gründlich untersucht werden, wie hierbei auftretende Datenschutzprobleme gelöst oder zumindest erträglich klein gehalten werden können.

Hierbei kann auf Erfahrungen bei der Lösung von Datenschutzproblemen in Kommunikationsnetzen zwischen ortsfesten Teilnehmern zurückgegriffen werden [Chau 81, Cha 85, Chau 88, PfPW 91]. Die Unterschiede zwischen diesen und Mobilnetzen sind:

1. Übertragungsbandbreite ist und *bleibt* bei Funknetzen sehr knapp, da das elektromagnetische Spektrum im freien Raum „nur einmal“ vorhanden ist.
2. Der mobile Teilnehmer muß unterwegs „gefunden“ werden.
3. Nicht nur die üblichen Daten (technisch gesehen die Nutz- und Vermittlungsdaten bzw. inhaltlich gesehen die Inhalts-, Interessens- und Verkehrsdaten, vgl. Abschnitt 1.2) weisen einen Personenbezug auf und müssen deshalb geschützt werden, sondern auch der *momentane Ort* der mobilen Teilnehmerstation bzw. des sie benutzenden Teilnehmers.

Das erste Problem wird gemindert, indem der freie Raum in viele Funkzellen aufgeteilt wird und so in nicht aneinandergrenzenden Funkzellen Teile des elektromagnetischen Spektrums erneut genutzt werden können. Diese Lösung des ersten Problems verschärft das zweite und dritte, da nun scheinbar zwangsläufig die momentane Funkzelle und damit der momentane Ort einer mobilen Teilnehmerstation bzw. des sie benutzenden Teilnehmers dem Zellularfunknetz bekannt, zumindest aber jederzeit leicht ermittelbar sein muß.

1.2 Nutzdaten und Vermittlungsdaten

Die bei der Kommunikation anfallenden Daten lassen sich aus technischer Sicht in Nutzdaten und Vermittlungsdaten unterteilen. Nutzdaten sind die zu übertragenden Daten, Vermittlungsdaten die zum Verbindungsaufbau notwendigen.

Die so anfallenden Daten ermöglichen Rückschlüsse auf die Interessen von Netzbenutzern und geben Auskunft darüber, wer mit wem, wann und wie lange kommuniziert. Mit Hilfe von Verkehrsdaten sind Bewegungsprofile erstellbar.

1.3 Datenschutzforderungen

Wir sehen es als eine Einengung und Verletzung der Privatsphäre der Menschen, daß Daten über sie erfaßbar (und auswertbar) sind, zumal es technische Möglichkeiten gibt, Systeme so zu gestalten, daß dies verhindert wird.

Bei für universelle Nutzung gedachten öffentlichen Mobilkommunikationsnetzen sollen aus unserer Sicht die folgenden **technischen Datenschutzforderungen** gelten [Pfit 93]:

Schutzziel Vertraulichkeit (confidentiality)

- c1 *Nachrichteninhalte* sollen vor allen Instanzen außer dem Kommunikationspartner vertraulich bleiben.
- c2 *Sender* und/oder *Empfänger* von Nachrichten sollen voreinander *anonym* bleiben können, und *Unbeteiligte* (inkl. Netzbetreiber) sollen *nicht in der Lage* sein, sie *zu beobachten*.
- c3 Weder potentielle Kommunikationspartner noch Unbeteiligte (inkl. Netzbetreiber) sollen ohne Einwilligung den *momentanen Ort* einer mobilen Teilnehmerstation bzw. des sie benutzenden Teilnehmers ermitteln können.

Schutzziel Integrität (integrity)

- i1 Fälschungen von *Nachrichteninhalten* (inkl. des *Absenders*) sollen erkannt werden.
- i2 Gegenüber einem Dritten soll der Empfänger *nachweisen* können, daß Instanz *x* die Nachricht *y gesendet hat*.
- i3 Der Absender soll das *Absenden* einer Nachricht mit korrektem Inhalt *beweisen* können, möglichst sogar den Empfang der Nachricht.
- i4 Niemand kann dem Netzbetreiber *Entgelte* für erbrachte Dienstleistungen vorenthalten. Umgekehrt kann der Netzbetreiber nur für korrekt erbrachte Dienstleistungen Entgelte fordern.

Schutzziel Verfügbarkeit (availability)

- a1 Das Netz ermöglicht Kommunikation zwischen allen Partnern, die dies *wünschen* (und denen es nicht verboten ist).

Solche Datenschutzforderungen können gewöhnlich durch juristische Mittel allein nicht gewährleistet werden. Insbesondere haben nicht durchgesetzte bzw. nicht durchsetzbare Rechtsvorschriften auf Dauer einen negativen Einfluß auf die Gesetzestreue aller. Vertraulichkeitseigenschaften müssen also möglichst durch **Verhinderung der Erfassungsmöglichkeit personenbezogener Daten** durchgesetzt werden [siehe z.B. Chau 81], da Schutz beispielsweise auch gegen Betreiber und Entwerfer von Netzkomponenten anders nicht zu erreichen ist. Im folgenden soll gezeigt werden, wie durch technischen Datenschutz Sicherheit im Sinne der Menschen und nicht nur der Netzbetreiber erreicht werden kann.

2 Umsetzung der Datenschutzforderungen

Wie und an welchen Stellen kann man ansetzen, um den Datenschutzforderungen gerecht zu werden? Der Mobilitätsaspekt bringt einige Faktoren mit sich, die einerseits eine Übertragung der aus dem Festnetz bekannten Verfahren erschweren oder unmöglich machen, andererseits treten neue Probleme auf, zu deren Lösungsmöglichkeiten ebenfalls einige Ideen aufgezeigt werden.

2.1 Bereits bekannte Verfahren

Mit Hilfe bekannter Verfahren wie Ende-zu-Ende-Verschlüsselung, Verbindungsverschlüsselung, Schutz der Verkehrsdaten über Teilnehmer durch bestimmte Adressierungsarten, Verteilung (*broadcast*), MIXe oder überlagerndes Senden konnten bisher die Probleme im Festnetz weitgehend analysiert und Vorschläge zur Lösung von Datenschutzproblemen gegeben werden.

2.1.1 Schutz der Nutzdaten

Vertraulichkeit nach c1 bedeutet, daß es den Endteilnehmern sowohl innerhalb eines Netzes als auch zwischen Netzen möglich sein muß, vertraulich zu kommunizieren. Dies gilt ebenfalls für die Integritätssicherung nach i1, i2 und i3. Durch den Einsatz von Verschlüsselung, digitalen Signaturen und Authentikationscodes kann dies erreicht werden. Die Datenschutzanforderung c1 läßt sich durch Ende-zu-Ende-Verschlüsselung erreichen. Für i1 und i2 wird die Nachricht vom Absender digital signiert. Für i3 dient eine digital unterschriebene Empfangsquittung des Empfängers oder ersatzweise des Nachrichtenübermittlungssystems.

Damit die Anwendung von Kryptographie möglich wird, müssen eine Reihe von Anforderungen erfüllt sein:

Die in den Endgeräten verwendeten kryptographischen Verfahren (Bausteine) und Protokolle für verschiedene Dienste und verschiedene Netze müssen aufeinander abgestimmt sein. Bei der zunehmenden „Internationalisierung“ von Kommunikation ist das allerdings eher ein juristisches (politisches) und wirtschaftliches als technisches Problem.

Die Nutzkanäle (bezogen auf das 7-Schichtenmodell der ISO mindestens die Transportschicht 4 oder höher) müssen bittransparent sein, d.h. die zu übertragenden Bits dürfen auf dem Signalweg nicht verändert oder gestört werden. Jede Bitveränderung auf dem Signalweg könnte sonst einen Verlust von Integrität bedeuten. Außerdem wird bei kryptographischen Systemen gewöhnlich eine starke Abhängigkeit zwischen mehreren Bits hergestellt, so daß die Änderung eines Bits eine Fehlerfortpflanzung in viele Bits zur Folge hat.

Allein diese Bittransparenz ist in bereits realisierten und standardisierten Netzen nicht immer vorhanden. So ist in Netzen nach dem GSM-Standard [GSM 93] kein bittransparenter Sprachkanal vorhanden. Andere Netze, z.B. das ISDN, stellen bittransparente Kanäle zur Verfügung. Bei der Integration von Netzen und Diensten sind deren Übergänge unter diesem Aspekt sorgfältig zu planen.

2.1.2 Schutz der Verkehrsdaten

Die hier geschilderten Grundverfahren sollen exemplarisch zeigen, daß es möglich ist, datenschutzgerechte Netze zu bauen.

2.1.2.1 Verbindungs-Verschlüsselung

Durch Ende-zu-Ende-Verschlüsselung auf ISO-Schicht 4 ist die Vertraulichkeit aller Nutzdaten und Protokollinformationen der Schichten 4 bis 7 gesichert. Enthalten aber die Protokollinformationen der Schichten 1 bis 3 personenbezogene Daten, so sollten diese Informationen außerdem durch Verbindungs-Verschlüsselung geschützt werden. Solche Informationen sind z.B. die Adressen der Endgeräte bzw. der Chipkarten von Teilnehmern, die meist verkettet werden können mit ihrem Nutzer, da es sich oft um persönliche Einrichtungen handelt, die der Mobilteilnehmer wohl nicht nach jedem Gespräch auswechselt!

In GSM-Netzen wird Verbindungs-Verschlüsselung auf der Funkschnittstelle angewendet, um den Schutz der Nutzdaten und teilnehmerspezifischen Verbindungsdaten im freien Raum zu gewährleisten. Da ansonsten alle Daten unverschlüsselt übertragen werden, hat zumindest der Netzbetreiber die Möglichkeit, Inhalts- und Interessensdaten aus den Nutzdaten zu erhalten.

Die verwendeten Verschlüsselungsalgorithmen sind *nicht* öffentlich bekannt. Daher kann man darüberhinaus *nicht* davon ausgehen, daß deren Verwendung für Ende-zu-Ende-Verschlüsselung vertrauliche Kommunikation zwischen Endteilnehmern ermöglicht. Außerdem erzeugt der Netzbetreiber die Schlüssel!

2.1.2.2 Schutz des Empfängers durch Verteilung und schutzgerechte Adressierungsarten

Schutz des Empfängers von Nachrichten wird durch **Verteilung** der (ggf. Ende-zu-Ende-verschlüsselten) Nachrichten an alle potentiellen Empfänger erreicht.

Damit die Nachrichten vom intendierten Adressaten erkannt werden können, werden sie mit **impliziten Adressen** versehen. *Implizite* Adressen kennzeichnen im Gegensatz zu *expliziten* weder einen Ort im Netz noch eine Station, sondern sie sind nur ein ansonsten bedeutungsloses und mit nichts anderem in Beziehung zu setzendes Merkmal für den Empfänger. Er kann daran erkennen, ob eine Nachricht für ihn bestimmt ist.

Offene implizite Adressen können von Unbeteiligten auf Gleichheit getestet werden. Eine geeignete Realisierung sind Zufallszahlen, die vom Empfänger mittels eines Assoziativspeichers, in den alle für die Station gerade gültigen impliziten Adressen geschrieben werden, sehr effizient erkannt werden können.

Verdeckte implizite Adressen können außer vom Adressaten von niemand auf Gleichheit getestet werden. Der Test auf Gleichheit durch den Adressaten stellt damit zwangsläufig eine kryptographische Operation dar und ist deshalb auch für den Adressaten deutlich aufwendiger als bei offenen impliziten Adressen.

2.1.2.3 Schutz des Senders durch DC-Netze oder umcodierende MIXe

Auf einem beliebigen Bitübertragungsnetz, das an beliebig vielen Stellen abgehört und manipuliert werden kann, kann man **überlagerndes Senden**, nach einem Beispiel von David Chaum **DC-Netz** genannt [Chau 88], implementieren: Die Teilnehmerstationen haben paarweise miteinander Schlüssel ausgetauscht, deren Werte vor den anderen Teilnehmern (und erst recht Außenstehenden) geheim gehalten werden. Anonyme Zugriffsverfahren erlauben es den Stationen sehr effizient, ihre Nachrichten einzeln zu übermitteln. Für das überlagernde Senden ist bewiesen, daß das Senden im DC-Netz **anonym** ist, wenn Stationen über Schlüssel zusammenhängen, die der Angreifer nicht kennt.

Eine Möglichkeit, die Kommunikationsbeziehung zwischen Sender und Empfänger zu schützen ist, die Nachrichten nicht direkt, sondern über sog. **MIXe** zu schicken. Damit die Wege der Nachrichten weder anhand ihres äußeren Erscheinungsbildes (also ihrer Länge und Codierung) noch anhand zeitlicher oder räumlicher Zusammenhänge verfolgt werden können, *puffern* die MIXe Nachrichten gleicher Länge von vielen Sendern, *codieren* sie um und geben sie *umsortiert* aus. Das Umcodieren erfolgt durch Ent- oder Verschlüsseln mittels eines Kryptosystems.

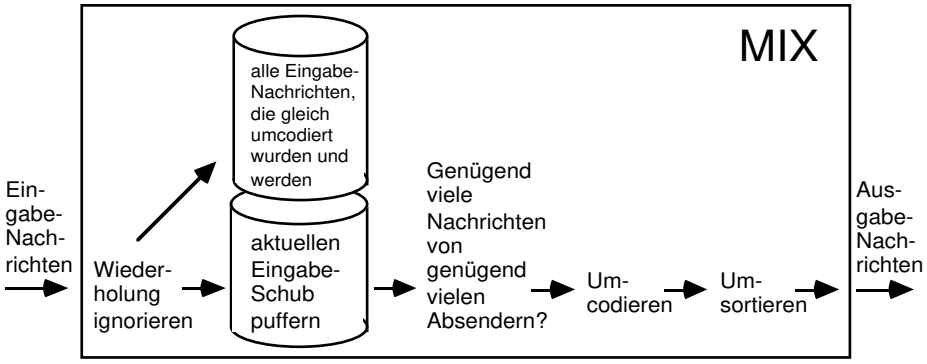

Abbildung: *Grundfunktionen eines MIXes*

Ein MIX muß darauf achten, daß er jede Nachricht nur einmal mixt, d.h. Nachrichtenwiederholungen ignoriert. Würde eine Nachricht innerhalb *eines* Schubes mehrfach bearbeitet, so entstünden über die Häufigkeiten der Eingabe- und Ausgabe-Nachrichten dieses Schubes unerwünschte Entsprechungen: Einer Eingabe-Nachricht, die *n*-mal auftritt, entspricht eine Ausgabe-Nachricht, die ebenfalls *n*-mal auftritt. Treten alle Eingabe-Nachrichten eines Schubes verschieden häufig auf, so schützt das Umcodieren dieses Schubes also überhaupt nicht. Gleiches gilt über mehrere Schübe hinweg, solange die Umcodierungsfunktion, gegeben durch den Chiffrierschlüssel eines Kryptosystems, nicht gewechselt wird.

Der Schutz der Kommunikationsbeziehung wird erreicht durch das Zusammenspiel mehrerer MIXe, die möglichst *unabhängig entworfen und hergestellt* sein sollen sowie *unabhängige Betreiber*

haben [Chau 81, Cha 84]. Denn andernfalls gibt es doch wieder einzelne Personen oder Organisationen, die den Schutz der Kommunikationsbeziehung allein aufheben können, sobald sie alle MIXe beherrschen, die eine Nachricht durchläuft.

Eine Methode, den Zeitpunkt des Sendens einer Nachricht zu verschleiern, ist **dummy-traffic**, d.h. das Senden bedeutungsloser Nachrichten, wenn keine bedeutungsvollen zu senden sind.

Leider lassen sich die hier beschriebenen Verfahren im mobilen Bereich, d.h. auf der Funkschnittstelle, nicht oder nur bedingt anwenden. Z.B. scheidet dummy-traffic auf der Funkschnittstelle allein schon wegen der Knappheit an Akkukapazität und Bandbreite auf der Funkschnittstelle aus. Man könnte jedoch einen wesentlichen Teil der Maßnahmen zum Schutz der Verkehrs- und Interessensdaten im ortsfesten Teil des Kommunikationsnetzes abwickeln, wie in Abschnitt 2.2.2 beschrieben.

2.1.3 Anonyme, sichere Abrechnungsverfahren

Bei einem öffentlichen Kommunikationsnetz sollte eine komfortable und sichere Abrechnung der Kosten für die Netznutzung mit dem Netzbetreiber möglich sein (i4). Sie sollte so organisiert sein, daß Anonymität, Unbeobachtbarkeit und Unverkettbarkeit im Kommunikationsnetz trotz Abrechnungsdaten erhalten bleiben (c2, c3).

Prinzipiell hat man dabei zwei Möglichkeiten: *Individuelle Abrechnung* nach Einzelnutzung mit Verfahren, bei denen der bezahlende Teilnehmer anonym ist oder von allen Netzteilnehmern zu leistende, *pauschale Bezahlung*, die nicht anonym erfolgen muß, da dabei keine interessanten Abrechnungsdaten entstehen oder nötig sind.

Bei Verwendung von **Pauschalzahlungen** vermeidet man alle Probleme bezüglich Betrugssicherheit und fast den gesamten Aufwand des Abrechnungsverfahrens. Sobald genügend Bandbreite zur Verfügung steht, was allerdings nur für leitungsgebundene Netze und im Nahbereich zu erwarten ist, wäre ein pauschales Entgelt an den Netzbetreiber möglich.

Individuelle Abrechnung könnte zum Beispiel erreicht werden durch Installation **nicht manipulierbarer Zähler**, im ortsfesten Bereich beim Teilnehmer im Netzabschluß und im mobilen Bereich in einem SIM (*Subscriber Identity Module*), der ohnehin schon vorhandenen persönlichen Chipkarte des Teilnehmers. Die Bezahlung könnte dann entweder per Abrechnung verbrauchter Einheiten erfolgen oder, wie heute von den Telefonkarten her bekannt, durch Vorbezahlung evtl. wieder aufladbarer Wertkarten. Hauptvorteil der Abrechnung mittels nicht manipulierbarer Zähler ist, daß im Kommunikationsnetz so gut wie kein Aufwand für Abrechnungszwecke getrieben werden muß. Hauptnachteile sind, daß sowohl ein Umgehen des Zählers durch Umgehen des Netzabschlusses oder des SIM verhindert oder zumindest entdeckt werden muß, als auch eine Manipulation am Zählerstand.

Eine weitere Möglichkeit der individuellen Abrechnung ist die Verwendung von **anonymen digitalen Zahlungssystemen** [BüPf 89]. Sie gewährleisten Anonymität, Unbeobachtbarkeit und Unverkettbarkeit. Die notwendigen Abrechnungsprotokolle müssen natürlich so entworfen sein, daß von vornherein niemand betrügen kann, da eine nachträgliche Strafverfolgung generell be- oder gar verhindert wird.

2.2 Neuere Ideen

Faktoren wie die Knappheit an Bandbreite auf der Funkschnittstelle, die Peilbarkeit von Sendeanlagen bedingt durch die physikalischen Ausbreitungseigenschaften elektromagnetischer Wellen, die Erhebung von Lokalisierungsinformation, das Streben nach Kompaktheit mobiler Endgeräte und der

daraus resultierenden Knappheit an Energie erfordern neue technische Datenschutzmethoden. Die folgenden Vorschläge sollen deshalb zur Diskussion gestellt werden.

2.2.1 Sendeverfahren, die Peilbarkeit einschränken

Elektromagnetische Wellen tragen neben den zu übertragenden Daten Richtungsinformationen in sich und können somit zur Ortsbestimmung einer Sendestation eingesetzt werden. Bereits einfachste Peiltechniken ermöglichen einen Zugriff zu solchen Ortsinformationen und damit auch die Erstellung von Bewegungsprofilen. Um die Peilung elektromagnetischer Wellen zu erschweren, bietet es sich an, Störungen bei deren Ausbreitung zu nutzen.

Ein Problem bei der Verarbeitung elektromagnetischer Wellen stellt das *Rauschen* dar. Rauschen ist eine kontinuierliche Spannung, die in nicht vorhersagbarer Weise schwankt und das Ergebnis innerer und äußerer statistischer Störungen ist. Wesentliche Anteile des Rauschens sind mit gleicher Leistungsdichte über das gesamte Frequenzspektrum verteilt.

Will man eine Welle peilen, muß sie als solche erkennbar sein. Das bedeutet, ihr Signal/Rausch-Verhältnis muß einen bestimmten Wert überschreiten. Die Kenntnis dieser Bedingungen führt zu Sendeverfahren für mobile Stationen, die **Bandspreizverfahren** (*spread spectrum systems*) genannt werden. Bandspreizverfahren basieren auf dem Grundsatz der Nachrichtentheorie, daß es bei der Übertragung eines digitalen Zeichens nicht darauf ankommt, welche Form es besitzt, sondern nur auf seinen Energieinhalt, d.h. die Fläche, die sein Spektrum besitzt. Wird durch ein geeignetes Modulationsverfahren die Signalleistung nun so breit verteilt, daß sie wesentlich kleiner als die Rauschleistungsdichte ist, so ist dennoch eine Informationsübertragung möglich. Als konkretes Verfahren scheint die *direkte Spreizung* (**direct sequence spread spectrum** DS) am besten geeignet: Die zu übertragenden Daten werden zunächst auf einen Träger in herkömmlicher Weise aufmoduliert. Das entstehende, relativ schmalbandige Signal wird dann in einem zweiten Modulationsschritt mit einer breitbandigen binären Pseudozufallszahlenfolge, dem PN-Code (*pseudonoise code*), der rauschähnliches Verhalten zeigt, moduliert. Die Erzeugung des PN-Codes geschieht unter Zuhilfenahme eines PN-Generators aus dem PN-Key, welcher das Geheimnis von Sender und legitimem Empfänger darstellt. Es entsteht ein Signal geringer Leistungsdichte, das von einer Antenne abgestrahlt werden kann und ähnliche Merkmale wie „weißes Rauschen“ aufweist.

Auf der Empfängerseite wird der PN-Code nachgebildet. Durch erneute Multiplikation des empfangenen Signals mit diesem Code wird die Spreizung wieder zurückgenommen und der modulierte Träger liegt in seiner ursprünglichen Form vor. Aus ihm können nun die zu übertragenden Daten zurückgewonnen werden.

Durch Verwendung orthogonaler PN-Codes ist es möglich, mehrere Nutzer im selben Spektrum senden zu lassen. Die Auslastung ist ebenso hoch wie bei schmalbandiger Mehrfachnutzung des Spektrums durch Frequenz- (*frequency division multiplex*) oder Zeitmultiplexverfahren (*time division multiplex*).

Wenn die Signale im Vergleich zum thermischen oder Umgebungsrauschen eine geringere spektrale Dichte haben und wenn sich diese in Abhängigkeit von der Frequenz nur sehr langsam ändert, sind DS-Signale bei unbekanntem PN-Code mit konventionellen Mitteln wie Spektrumanalysatoren nicht zu entdecken. Lediglich mit einem *Radiometer*, d.h. durch Integration des vorhandenen Rauschens in einem Spektrum über einen längeren Zeitraum, könnte ein Signal entdeckt werden. Mit Radiometer erkannte Signale sind jedoch nicht peilbar. Nähere Informationen finden sich in [Torr 92] und [PiSM 82].

Ansätze, wie die Struktur vorhandener zellularer Mobilfunknetze modifizierbar wäre, finden sich in [ThFe 95].

2.2.2 Speicherung der Lokalisierungsinformationen

Soll ein mobiler Teilnehmer eines zellularen Mobilfunknetzes erreichbar sein, muß dem Netz Lokalisierungsinformation bekannt sein. Gewöhnlich wird Lokalisierungsinformation in Datenbanken (*home location register* HLR, *visitor location register* VLR) *im* Netz abgelegt und dort ständig aktualisiert. Dadurch ist es einem Angreifer, der ja auch der Netzbetreiber sein kann, möglich, Bewegungsprofile zu erstellen, was gegen die Datenschutzforderung c3 verstößt.

Wenn man nun die Lokalisierungsinformation in einem vertrauenswürdigen Bereich abspeichert und diese dem Netz nur zum Verbindungsaufbau zur Verfügung stellt, so ist das Problem entschärft. Könnte man sogar das gesamte Lokalisierungsmanagement in einem solchen vertrauenswürdigen Bereich abwickeln und würde man die Kommunikationsbeziehnungen im Netz z.B. über MIXe schützen, so wäre die Erstellung von Bewegungsprofilen durch das Netz nicht mehr oder nur noch mit extrem hohem Aufwand möglich.

Ein solcher vertrauenwürdiger Bereich könnte z.B. eine Station des Teilnehmers im Festnetz sein. Diese Station muß in der Lage sein z.B. Verschlüsselungs-, Rechen- und Managmentfunktionen auszuführen. Wir wollen diese Station **ortsfeste Teilnehmerstation** oder **HPC** (*home personal computer*) nennen. Diese Station muß nicht notwendigerweise beim Nutzer selbst lokalisiert sein. Die Aufgaben des HPC könnten ebenso von vertrauenswürdigen Organisationen, Firmen, Vereinigungen wahrgenommen werden. Auch wäre es denkbar, kooperativ mit dem Netzbetreiber beidseitig sichere Chips zu generieren, einen für den Nutzer, dem heutigen SIM-Modul (*subscriber identity module*) entsprechend, einen weiteren für den Netzbetreiber, die Funktionalität des HPC umfassend.

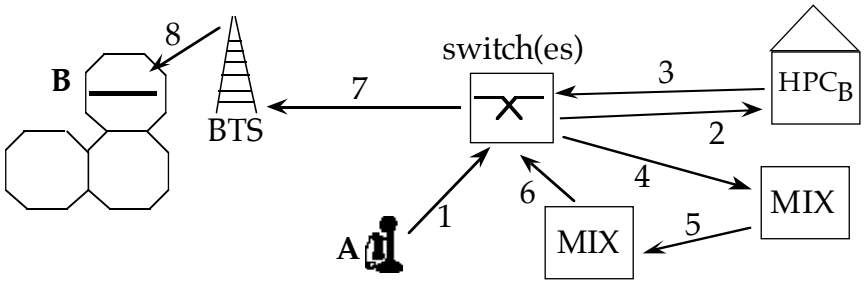

Abbildung: *Vertrauenswürdige Speicherung von Lokalisierungsinformation im HPC und Signalisierung über ein MIX-Netz*

Will z.B. ein Teilnehmer A eine Verbindung zum mobilen Teilnehmer B aufbauen, so erreicht er über Vermittlungsstellen (und evtl. über MIXe) die ortsfeste Station HPC_B von B. HPC_B kennt den Aufenthaltsbereich von B und kann damit den Verbindungswunsch über MIXe zur Basisstation BTS (*base transceiver station*) leiten. Warum ist der Schutz der Kommunikationsbeziehung (durch MIXe) zwischen HPC_B und BTS notwendig? Der Netzbetreiber könnte sonst über Verkehrsdatenanalyse feststellen, daß HPC_B und BTS miteinander kommuniziert haben. Der Netzbetreiber weiß aber damit, daß sich B im Versorgungsbereich von BTS befindet. Damit ist wieder die Datenschutzforderung c3 verletzt.

2.2.3 Ausnutzung hierarchischer Zellbereiche bei der Signalisierung

Die Integration der verschiedenen Kommunikationssysteme in UMTS kann günstige Ansatzpunkte für die Realisierung datenschutzfreundlicher Systeme bieten, insbesondere für den Schutz des Aufenthaltsortes des Teilnehmers. Dieser ist am besten dadurch gegeben, daß weder der Netzbetreiber

noch eine vertrauenswürdige, ortsfeste Teilnehmerstation genaue Lokalisierungsinformation speichern müssen.

Um einen Verbindungswunsch zum mobilen Teilnehmer signalisieren zu können, muß dieser im Aufenthaltsgebiet des mobilen Teilnehmers verteilt werden (*broadcast*).

Je größer das Verteilungsgebiet der Verbindungswunschnachricht ist, umso gröber darf die über den Teilnehmer vorhandene Lokalisierungsinformation sein.

Besitzt man in Datenbanken detaillierte und aktuelle Lokalisierungsinformationen, z.B den BTS-Bereich eines Teilnehmers, kann man den Broadcastbereich klein halten. Es sind jedoch Protokolle erforderlich, welche die Lokalisierungsinformationen in den Datenbanken stets aktualisieren (*location update*), wenn sich ein Teilnehmer bewegt.

In der Zukunft erwartet man in Richtung UMTS die Integration verschiedener Zellnetze mit ihren verschiedenen Zellradien: Picocells (<100 m), Microcells (<1 km) und Macrocells (<35 km) [Evci 92]. Als Ergänzung dieser terrestrischen Systeme sollen Satellitensysteme (z.B. LEO-Satelliten, *low earth orbit*) zum Einsatz kommen. Das bekannteste Projekt dafür ist Iridium von Motorola. Es soll 1998 mit 66 Satelliten in Betrieb gehen [Floh 94]. Die Iridium LEO-Satelliten werden flächendeckend und weltumspannend eingesetzt. Ein einziger LEO-Satellit deckt dabei eine Overlayzelle mit einem Radius von ca. 2000 km, gebildet durch 48 sog. Spot-Beams, ab.

Die Zellen der verschiedenen in UMTS integrierten Systeme überlagern sich also teilweise und bilden eine „Abdeckungs-Hierarchie".

Je größer die sich überlagernden Zellen werden, die man zu Broadcastgebieten „macht" (der Ausdruck „macht" deshalb, weil sie in diesem Sinne eigentlich nicht dafür gedacht waren), desto unpräziser wird der exakte Ort eines Teilnehmers. Voraussetzung ist natürlich, daß der Teilnehmer über Technik, Signale „anderer" Netze bzw. Netzstandards zu empfangen, verfügt. Je größer jedoch ein Broadcastgebiet ist, umso größer ist auch sein Anonymitätsbereich. Daraus folgt: Eine Signalisierung zum mobilen Teilnehmer sollte über ein möglichst großes Broadcastgebiet erfolgen. Eine Signalisierung **„von groß nach klein"** liegt also nahe. Ein Beispiel soll das verdeutlichen:

Eine Signalisierung zu einem mobilen Teilnehmer B könnte über LEO-Satelliten erfolgen. Signale von LEO-Satelliten sind mit den im Mobilfunk üblichen Kurzantennen empfangbar. Das bedeutet, zum Erreichen von B sind keine oder nur sehr grobe Aufenthaltsinformationen nötig.

Hat B das Signal erhalten, kann er entsprechend reagieren, ggf. eine Verbindung aufbauen und die Nutzkanäle etablieren. Es ist klar, daß der mobile Teilnehmer auf die für ihn günstigste Art, z.B. die akkusparsamste und/oder kostengünstigste (wenn *er* bezahlen muß) Art kommunizieren möchte. Von solchen Faktoren sowie den örtlichen Gegebenheiten, z.B. erreichen nicht alle Netze Flächendeckung, kann abhängen, ob und wie er reagiert. Gewöhnlich wird also die nächste verfügbare Funkzelle im kleinstzelligsten Netz benutzt. Diese Art des Verbindungsaufbaus wollen wir deshalb **„von klein nach groß"** nennen.

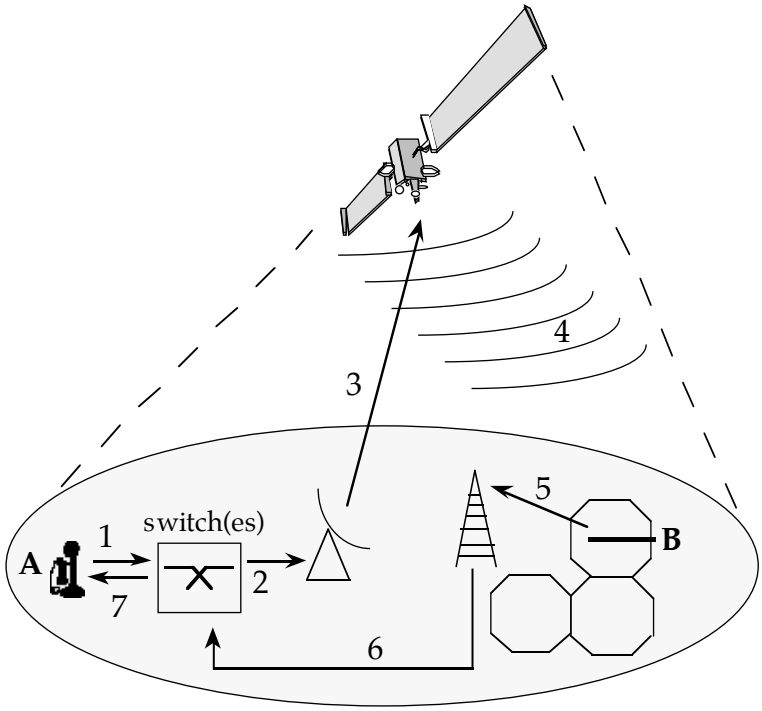

Abbildung: *Signalisierung und Verbindungsaufbau zur mobilen Station*

In der Abbildung wird der Satellit vereinfachend als Sternknoten mit einem Ausleuchtgebiet (ovale Fläche) dargestellt. Durch die Verteilung der Nachricht innerhalb eines großen Broadcastgebietes ist eine perfekte informationstheoretische Anonymität des Empfängers gegeben [Pfit 89].

Ein passiver Angreifer kann dann durch Beobachtung des Netzes nicht entscheiden, wer auf welchen Anruf reagiert. Ein aktiver Angreifer könnte die konsistente Verteilung der Nachricht verhindern, indem er die über Satellit gesendeten Signale (zer)stört. Bei Verwendung von Bandspreizverfahren könnte dies jedoch sehr erschwert werden, da sie recht störsicher sind.

Problematisch bei der Broadcast-Signalisierung über LEO-Satelliten ist die kurze Aufenthaltsdauer eines Satelliten in einem Versorgungsgebiet. Dies ist bedingt durch die hohe Relativgeschwindigkeit zwischen Erdoberfläche und Satellit. In Abhängigkeit von der Bahnhöhe (von 500 km bis 2000 km) beträgt die Sichtverbindung an einem fixen Punkt der Erde zu einem LEO-Satelliten nur wenige Minuten [DoZM 93]. Über eine Koordinationszentrale muß also das Mapping des Broadcastgebietes auf die entsprechenden LEO-Satelliten vorgenommen werden. Um ein großes Broadcastgebiet zu versorgen, z.B. europaweit, müssen mehrere LEO-Satelliten eingesetzt werden. Wenn ein aktiver Angreifer über die Koordinationszentrale die Konsistenz der Verteilung in einem Gebiet stört, z.B. gezielt mit einzelnen LEO-Satelliten Signalisierungswünsche für eine bestimmte mobile Station absetzt, könnte das zur Aufdeckung des Aufenthaltsgebietes des Teilnehmers führen. Denn der Angreifer kann das (kleinere) Signalisierungsgebiet und das Reagieren (oder Nicht-Reagieren) der Mobilstation verknüpfen und somit detailiertere Aufenthaltsinformation über den Teilnehmer erhalten. Eine mögliche Gegenmaßnahme zu diesem aktiven Angriff ist die digitale Signierung der verteilten Signale mit einem Zeitstempel durch den Satelliten, so daß ein späteres Aufdecken des Angriffs möglich ist.

2.2.4 Erreichbarkeitsmanagement

Durch die erhöhte technische Erreichbarkeit eines Mobilteilnehmers ist ein Management seiner persönlichen Erreichbarkeit wünschenswert. Wenn ein Mobilteilnehmer in seinen verschiedenen Rollen

(z.B. privat, dienstlich) gar nicht die Wahl hat, ob er ein Kommunikationsmedium verwenden will, so muß ihm die Möglichkeit des Filterns unerwünschter Verbindungswünsche möglich sein. Ein technisches System, das Kommunikationswünsche entgegennimmt und behandelt, bildet dann die Schnittstelle zwischen dem zu schützenden Teilnehmer und dem Netz. Ein Erreichbarkeitsmanager vollzieht damit einen wesentlichen Teil der Aufgaben eines digitalen Assistenten.

Die im Erreichbarkeitsmanager abgespeicherten Erreichbarkeitsprofile enthalten personenbezogene Daten, die einerseits Daten über andere Teilnehmer enthalten können, andererseits aber auch Daten über die eigene zu schützende Situation. Nach c2 sind also Erreichbarkeitsprofile schützenswert und sollten daher in einem vertrauenswürdigen Bereich, z.B. dem HPC (siehe Abschnitt 2.2.2), abgespeichert und gemanagt werden [FKPS 94]

3 Schlußfolgerungen

Die Ausführungen zeigen, daß es Konzepte gibt, wie man technischen Datenschutz in öffentlichen Kommunikationsnetzen realisieren kann. Weiterhin wurde gezeigt, daß durch den Mobilitätsaspekt bekannte Verfahren überdacht und weiterentwickelt werden müssen, aber auch neue Verfahren nötig sind.

In der Phase der Standardisierung künftiger Mobilfunknetze ist es noch möglich, Sicherheit als festen Bestandteil solcher Systeme einzubringen. Es könnte sonst geschehen, daß die Forderung nach entsprechenden Maßnahmen die technische Entwicklung überholt.

Das Verfahren der direkten Spreizung ist unseres Erachtens ein notwendiger Schritt zur Nichtortbarkeit von Mobilstationen und damit zum Schutz der Verkehrsdaten. Die vorgeschlagene dezentrale Verwaltung der Erreichbarkeitsinformation macht deren Speicherung in Datenbanken überflüssig, womit diese Datenbanken als Unsicherheitsfaktor beim Schutz von Verkehrsdaten wegfallen. Die Einführung einer ortsfesten Teilnehmerstation als koordinierendes System scheint in diesen Zusammenhang weniger schwierig, da innerhalb der natürlichen Erneuerungsperiode von Telefonen ein Umstieg auf ein integriertes System Telefon/ortsfeste Teilnehmerstation/Erreichbarkeitsmanager ohne weiteres möglich sein sollte.

4 Literatur

BüPf 89 Holger Bürk, Andreas Pfitzmann: Digital Payment Systems Enabling Security and Unobservability; Computers & Security 8/5 (1989) 399-416.

Cha 84 David Chaum: A New Paradigm for Individuals in the Information Age; 1984 IEEE Symposium on Security and Privacy, IEEE Computer Society Press, Washington 1984, 99-103.

Cha 85 David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044.

Chau 81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 84-88.

Chau 88 David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability; Journal of Cryptology 1/1 (1988) 65-75.

DoZM 93 Frederic Dosiere, Tarif Zein, Gerard Maral: A Model for the Handover Traffic in Low Earth Orbiting (LEO) Satellite Networks for Personal Communications; International Journal of Satellite Communications, Vol. 11 (1993) 145-149.

Evci 92 Cengiz Evci: Race-UMTS for third generation wireless communications, ANN. TÉLÉCOMMUN., 47, Nr. 7-8, 1992.

FKPS 94 Hannes Federrath, Dogan Kesdogan, Andreas Pfitzmann, Otto Spaniol: Erreichbarkeitsmanagement und Notrufdienst auf der Basis datensparsamer Adressierung. Arbeitspapier zum Kolleg „Sicherheit in der Kommunika-

tionstechnik“ der Gottlieb Daimler - und Karl Benz - Stiftung Ladenburg, April 1994.

Floh 94 Udo Flohr: Trabanten im All, iX 12/1994.

GSM 93 ETSI: GSM Recommendations: GSM 01.02 - 12.21; February 1993, Release 92.

Mitt 94 Hakan Mitts: Universal Mobile Teecommunication System – Mobile access to Broadband ISDN; Broadband Islands '94: Connecting with the End-User; W. Bauerfeld, O. Spaniol, F. Williams (Editors), Elsevier Science B.V. 1994, 203-209.

Pfit 89 Andreas Pfitzmann: Diensteintegrierende 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) 451-463.

PfPW 91 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes – Untraceable Communication with Very Small Bandwidth Overhead; Proc. IFIP/Sec'91, May 1991, Brighton, North-Holland, Amsterdam 1991, 245-258.

PiSM 82 R.L. Pickholtz, D.L. Schilling, L.B. Milstein: Theory of Spread-Spectrum-Communications – A Tutorial. IEEE Transactions on Communications (1982) vol. 30, No.5, 855-878.

ThFe 95 Jürgen Thees, Hannes Federrath: Methoden zum Schutz von Verkehrsdaten in Funknetzen; Proc. Verläßliche Informationssysteme (VIS'95), Vieweg 1995, 181-192.

Torr 92 D.J. Torrieri: Principles of Secure Communication Systems (Second Edition); Artech House, Boston, London, 1992.