erschien in: Datenschutz und Datensicherung DuD 17/8 (1993) 451-463

Technischer Datenschutz in öffentlichen Funknetzen

Andreas Pfitzmann
Institut für Informatik, Universität Hildesheim,
Postfach 101 363, W-3200 Hildesheim

Gliederung

1 Problemanalyse ... 2
1.1 Entwicklung der öffentlichen Funknetze ... 3
1.2 Technische Datenschutzanforderungen ... 3
1.3 Datenschutzdefizite der bestehenden öffentlichen Funknetze ... 4
1.4 Weiterer Aufbau: Welche Datenschutzanforderungen werden wo behandelt? ... 5
2 Schutz der Nutzdaten ... 6
3 Schutz der Verkehrsdaten ... 7
3.1 Anwendbarkeit der für leitungsgebundene Netze bekannten Grundverfahren ... 7
3.1.1 Schutz des Empfängers (Verteilung) ... 7
3.1.2 Schutz des Senders ... 8
3.1.2.1 Unbeobachtbarkeit angrenzender Leitungen und Stationen sowie digitale Signalregenerierung ... 8
3.1.2.2 Überlagerndes Senden (DC-Netz) ... 8
3.1.3 Schutz der Kommunikationsbeziehung (MIX-Netz) ... 8
3.1.4 Vergleich von Stärke und Aufwand von RING-, DC- und MIX-Netz ... 10
3.2 Adaption für Funknetze: Funk-MIXe ... 11
3.2.1 Defensive Annahme: Stationen sind peil- und identifizierbar, wenn sie senden ... 11
3.2.2 Funk-MIXe ... 12
4 Schutz vor Belästigung und vor Ermittlung des Aufenthaltsortes mittels unerwünschtem Anruf ... 15
4.1 Generierung kurzer offener impliziter Adressen, Filterung unerwünschter Verbindungswünsche und Verkleinerung der Broadcastgebiete durch ortsfeste Teilnehmerstation ... 15
4.1.1 Generierung kurzer offener impliziter Adressen spart Bandbreite im Broadcast-Signalisierungskanal und Aufwand bei der Adreßerkennung ... 15
4.1.2 Filterung unerwünschter Verbindungswünsche durch ortsfeste Teilnehmerstation ... 16
4.1.3 Verkleinerung der Broadcast-Gebiete: Eigene ortsfeste Teilnehmerstation weiß ungefähren Aufenthaltsort des mobilen Teilnehmers ... 17
4.2 Beliebige, auch nichtanonyme Kommunikationsformen auf Netzen mit Schutz der Verkehrsdaten ... 18
5 Entgeltabrechnung ... 19
6 Fehlertoleranz zur Steigerung der Verfügbarkeit ... 20
7 Nachweis der Praktikabilität der Funk-MIXe ... 20
8 Anwendung auf Verkehrsleitsysteme ... 22
9 Forschungs-, Normungs- und Entwicklungsbedarf ... 22
Ein Dankeschön ... 23
Stichwörter ... 23
Literaturverzeichnis ... 23

Zusammenfassung

Eine gründliche Analyse der Datenschutzprobleme in öffentlichen Funknetzen ergibt 8 technische Datenschutzforderungen. Nach dem Aufzeigen der erheblichen und tiefliegenden Datenschutzdefizite der bestehenden öffentlichen Funknetze wird unter defensiven Annahmen über die Peil- und Identifizierbarkeit von Funkstationen grundlegend geklärt, wie weit und wie nicht nur die **Nutzdaten**, sondern auch die **Verkehrsdaten**, insbesondere der momentane **Ort** mobiler Teilnehmer(stationen), überprüfbar geschützt werden können.

Das hierzu entwickelte Verfahren der **Funk-MIXe** wird danach um die Funktionalität des „digitalen Kommunikationsleibwächters“ erweitert, um die Teilnehmer vor Belästigung und vor Ermittlung ihres Aufenthaltsortes mittels unerwünschter Anrufe zu schützen.

Möglichkeiten zur datenschutzgerechten Entgeltabrechnung und Fehlertoleranz werden erläutert.

Danach wird mittels eines einfachen Leistungsmodells die Praktikabilität des Verfahrens der Funk-MIXe demonstriert: Selbst in der für Schutz der Verkehrsdaten extrem ungünstigen Funkzellenstruktur des D-Netzes läßt sich das Verfahren der Funk-MIXe ohne neue Frequenzzuweisung realisieren. Verbindungswünsche können innerhalb von mehr als 5 Millionen Teilnehmern verteilt werden, so daß der momentane Ort eines empfangsbereiten Teilnehmers dem Netz nicht bekannt zu sein braucht.

Überlegungen zum Forschungs-, Normungs- und Entwicklungsbedarf schließen die Arbeit ab.

1 Problemanalyse

Als Ergänzung des zügigen Ausbaus der öffentlichen Kommunikationsnetze zwischen ortsfesten, durch Leitungen verbundenen Teilnehmerstationen erfolgt ein geradezu stürmischer Ausbau der öffentlichen Funknetze zwischen mobilen Teilnehmerstationen. Deshalb muß dringend gründlich untersucht werden, wie die hierbei auftretenden Datenschutzprobleme gelöst oder zumindest erträglich klein gehalten werden können.

Hierbei kann auf Erfahrung bei der Lösung des Datenschutzproblems in Kommunikationsnetzen zwischen ortsfesten Teilnehmern zurückgegriffen werden [Chau_81, Cha8_85, Chau_88, Pfi1_83, PfPW_88, PfPW1_89, PfPW5_91, Pfit_90]. Die Unterschiede zwischen diesen und Funknetzen sind:

- Übertragungsbandbreite ist und *bleibt* bei Funknetzen sehr knapp, da das elektromagnetische Spektrum im freien Raum „nur einmal“ vorhanden ist.
- Der mobile Teilnehmer muß unterwegs „gefunden“ werden.
- Nicht nur die üblichen Daten (technisch gesehen die Nutz- und Vermittlungsdaten bzw. inhaltlich gesehen die Inhalts-, Interessens- und Verkehrsdaten [PfPW_88]) weisen einen Personenbezug auf und müssen deshalb geschützt werden, sondern auch der *momentane Ort* der mobilen Teilnehmerstation bzw. des sie benutzenden Teilnehmers.

Die erste Begrenzung 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.

Der Rest dieser Problemanalyse besteht aus vier Teilen:

1. Zuerst wird die *Entwicklung* der öffentlichen Funknetze in der Bundesrepublik Deutschland knapp beschrieben, insbesondere ihre bzgl. technischem Datenschutz wesentlichen Eigenschaften.
2. Danach werden *technische Datenschutzanforderungen* aufgestellt: Welche Daten sind vor wem wogegen zu schützen?
3. Anschließend werden die *Defizite* der beschriebenen öffentlichen Funknetze kurz aufgezeigt.
4. Zuletzt wird der weitere *Aufbau dieses Papieres* beschrieben: insbesondere, in welchen der folgenden Kapitel welche der aufgestellten Datenschutzanforderungen behandelt werden.

1.1 Entwicklung der öffentlichen Funknetze

In der Vergangenheit waren öffentliche Funknetze *dienstespezifisch* und oftmals auch *geographisch* sowie bzgl. der Zahl der Teilnehmer stark *eingeschränkt*: Vom Rheinfunk-Dienst für Flußschiffer über Telefongespräche in Zügen mit vergleichsweise wenig Sprechstellen bis zum boomenden *Zellularfunknetz C* der DBP Telekom erfolgt die Sprachübertragung mittels ***analoger* Signale**.

Mit ***digitaler* Übertragungstechnik** arbeiten Spezialnetze [Tele6_90] zur Übermittlung von Piepstönen (*Eurosignal* in ganz Mitteleuropa, *Cityruf* in einigen Regionen der Bundesrepublik), kurzer Texte (*Cityruf* mit entsprechendem Empfänger) oder beliebig langer Daten (*Modacom* in einigen Regionen der Bundesrepublik) und die 1992 in Betrieb gegangenen *Zellularfunknetze D1* der DBP Telekom und *D2* der Mannesmann-Mobilfunk GmbH. Letztere werden europaweit betrieben, so daß gegenüber regionalen Netzen am Wohnort der momentane Aufenthaltsort innerhalb eines weit größeren Gebietes verfolgt werden kann. D1- und D2-Netz sind als *universell einsetzbare* öffentliche Funknetze konzipiert.

1.2 Technische Datenschutzanforderungen

Geordnet nach den Schutzzielen *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* bestehen insbesondere bei für universelle Nutzung gedachten öffentlichen Funknetzen folgende **technische Datenschutzanforderungen**:

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[1]. Umgekehrt kann der Netzbetreiber nur für korrekt erbrachte Dienstleistungen Entgelte fordern.

Zugegeben, die letzten drei Schutzziele unter Integrität zu fassen, ist etwas gezwungen. Alternativ müßten weitere Schutzziele eingeführt werden, was leicht ins Uferlose ausartet.[2] i4 könnte allerdings auch unter Verfügbarkeit eingeordnet werden.[3]

Schutzziel Verfügbarkeit (availability)

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

Diese Datenschutzanforderungen können durch juristische Mittel allein nicht gewährleistet werden – und nicht durchgesetzte, insbesondere also alle nicht durchsetzbaren Rechtsvorschriften haben auf Dauer einen negativen Einfluß auf die Gesetzestreue aller. Die Gefährdung der Demokratie durch mangelhaften oder auch nur mangelhaft überprüfbaren Datenschutz ist in [Pfit_90] ausführlich dargelegt.

Deshalb genügt es nicht, bzgl. Funknetzen nur zu diskutieren, wer wie lange welche Daten speichert [Alke_88, Alke_92, Cott_92, Luka_92]. Vertraulichkeitseigenschaften müssen durch **Verhinderung der Erfassungsmöglichkeit** durchgesetzt werden [Chau_81, PfPW_88, Pfit_90], da anders Schutz beispielsweise auch gegen Betreiber und Entwerfer von Netzkomponenten nicht zu erreichen ist. Letztere könnten etwa *universelle transitive Trojanische Pferde* implementiert haben [Pfit1_90].

1.3 Datenschutzdefizite der bestehenden öffentlichen Funknetze

Analoge Übertragung verhindert oder *erschwert* zumindest den Einsatz von *Verschlüsselung*, ohne den weder die Vertraulichkeitsanforderungen c1, c2, noch die Integritätseigenschaften i1, i2, i3 realisierbar sind. Folglich ist in den entsprechenden, oben genannten Funknetzen bisher kein Schutz der Nutzdaten durch Verschlüsselung vorgesehen. Sie sind also auch in dem Sinne öffentliche Netze, daß alles in ihnen Übertragene öffentlich ist, da jeder Interessierte mit einem Budget von einigen hundert DM mithören kann – auch wenn beim C-Netz die Sprache in verschleierter Form übertragen wird [Tele7_90]. Früher war dieses Mithören verboten, seit dem 12. August 1992 ist der Besitz und Betrieb passender Empfänger praktisch freigegeben [Oste_92].

Digitale Übertragung ermöglicht den *preiswerten Einsatz sicherer Verschlüsselung* der Nutzdaten. Verschlüsselung wird jedoch nur bei den D-Netzen und dort auch nur zur Sicherung der Funkstrecke [Mich_91] und in zweifelhafter Qualität verwendet, da *geheimgehaltene* Kryptosysteme eingesetzt werden. Die Nutzdaten sind also insbesondere bei der Übermittlung im leitungsgebundenen Netz weder vor unbefugter Kenntnisnahme noch vor unerkannter Veränderung geschützt. Eurosignal und Cityruf sind momentan, da auf Verschlüsselung verzichtet wird, auch öffentliche Netze im doppelten Sinne des Wortes.

---

1 Diese Forderung ist stärker als das, was ein öffentliches Funknetz unbedingt leisten muß. Es würde reichen, daß der Netzbetreiber die korrekte Erbringung von Dienstleistungen *beweisen* kann. Ob und wie unter Vorlage dieser Beweise dann Geldflüsse außerhalb des öffentlichen Funknetzes erzwungen und realisiert werden, müßte hier eigentlich nicht betrachtet werden. Da aber die Vertraulichkeitsforderung c2 das Eintreiben von Entgeltforderungen zu erschweren scheint, wird hier die stärkere Forderung erhoben. In Kap. 5 wird dann gezeigt, wie auch sie erfüllt werden kann.

2 Die kanadischen Kriterien zur Bewertung der Sicherheit von IT-Produkten (The Canadian Trusted Computer Product Evaluation Criteria, CTCPEC) führen ein viertes Schutzziel, Zurechenbarkeit (accountability), ein [PfRa_93 Seite 178], das für i2, i3 und i4 gut paßt.

3 Dies gilt bei der Einteilung in die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit. Nimmt man noch als viertes Schutzziel Zurechenbarkeit hinzu, gilt dies weniger.

Außer beim Telefonieren mit *Münzen* oder *Wertkarten* in Zügen ist die **Entgeltabrechnung** in allen erwähnten Funknetzen *personenbezogen*. Dies ist nicht nur unnötig (siehe Kap. 5), sondern widerspricht auch der Datenschutzforderung c2. Außerdem ist der Funknetz-Benutzer kaum oder überhaupt nicht in der Lage, sich vor unberechtigten Entgeltforderungen des Funknetz-Betreibers zu schützen. Lediglich bei der ausschließlichen Verwendung von Münzen und Wertkarten ist sein finanzielles Risiko wenigstens begrenzt.

Auch die **Verfügbarkeitsanforderung** wird nur unbefriedigend erfüllt:

Einerseits sind alle genannten Funknetze leicht störbar, da weder Verfahren zum *Frequenzbandwechsel* noch *Spreizbandtechniken* (spread spectrum) etc. implementiert sind. Die genannten Funknetze ermöglichen Kommunikation also nur, wenn leicht durchführbare aktive Angriffe unterbleiben.

Andererseits ermöglichen die genannten Funknetze nicht nur Kommunikation zwischen Partnern, die dies wünschen, sondern erlauben auch die *Belästigung* des Empfängers mit Nachrichten von unerwünschten Kommunikationspartnern, da keine der in [Pfit_90 Seite 290f, Raub1_92] genannten Mechanismen zum Schutz vor unerwünschten Anrufen implementiert sind, vgl. Kap. 4.

1.4 Weiterer Aufbau: Welche Datenschutzanforderungen werden wo behandelt?

In den folgenden Kapiteln 2-7 wird untersucht, wie weit die Datenschutzanforderungen des Abschnitts 1.2 bei öffentlichen Funknetzen erfüllt werden können. Der weitere Aufbau dieses Papieres orientiert sich dabei nicht an der dortigen Gliederung der Anforderungen, sondern an den *Klassen der zu schützenden Daten* oder – was auf dasselbe hinausläuft – den einzusetzenden Schutzmechanismen, vgl. Bild 1.

In Kap. 2 wird der Schutz der *Nutzdaten* behandelt, was den Anforderungen c1, i1, i2 und i3 entspricht.

Kap. 3 ist dem Schutz der *Verkehrsdaten* gewidmet, der zur Realisierung der Anforderungen c2 und c3 nötig ist und die Realisierung der Anforderung i4 unterstützt.

Vom Schutz vor *Belästigung* und vor Ermittlung des *Aufenthaltsortes* mittels unerwünschtem Anruf handelt Kap. 4. Die hier genannten Verfahren unterstützen die Erfüllung der Anforderungen c3 und a1.

Kap. 5 ist der *Entgeltabrechnung* und damit zentral der Anforderung i4 gewidmet.

Kap. 6 skizziert, welche bisher nicht vorgesehenen Maßnahmen zur Fehlertoleranz sinnvoll sind, um die *Verfügbarkeit* des Funknetzes insbesondere in kritischen Situationen zu verbessern und damit die Datenschutzanforderung a1 wenigstens näherungsweise zu verwirklichen.

In Kap. 7 wird zum Nachweis der *Praktikabilität* des zuvor entwickelten Verfahrens der Funk-MIXe ein einfaches Leistungsmodell entwickelt.

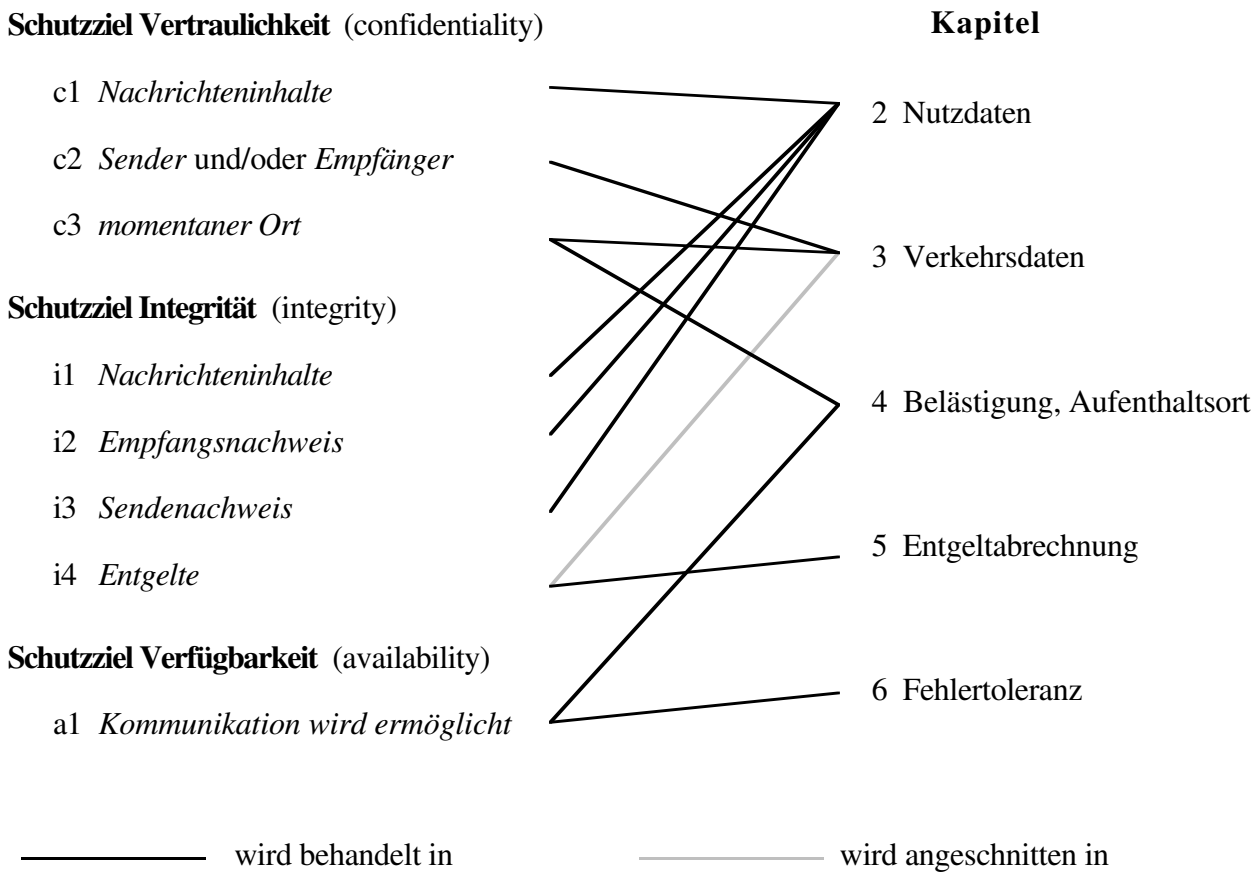


Bild 1: Zuordnung zwischen technischen Datenschutzanforderungen und Kapiteln

2 Schutz der Nutzdaten

Die Datenschutzanforderung c1 ist nach dem gegenwärtigen Stand von Wissenschaft und Technik ohne **Verschlüsselung** nicht realisierbar – bei *analoger* Übertragung muß die Nutzinformation also erst *digitalisiert*, dann *verschlüsselt* und danach für die analoge Übertragung *moduliert* werden. Je nach Dienst ist dies vergleichsweise einfach oder auch nahezu unmöglich – letzteres etwa, wenn der Dienst den analogen Übertragungskanal sehr gut ausnutzt und eine auch nur leichte Qualitätsverschlechterung des Dienstes unakzeptabel ist. Auch kann ohne den Einsatz von **Authentikationscodes** oder **digitalen Signaturen** die Fälschung von Nachrichteninhalten (i1) nicht sicher erkannt werden. Für i2 ist eine digitale Signatur des Absenders unter die Nachricht nötig, für i3 eine digital unterschriebene Empfangsquittung des Empfängers und ersatzweise des Nachrichtenübermittlungssystems.

Digitale Übertragung ermöglicht den preiswerten Einsatz sicherer Verschlüsselung, Authentikationscodes und digitaler Signatursysteme. Da alle zukünftigen öffentlichen Funknetze mit digitaler Übertragungstechnik geplant werden, gibt es für die Realisierung der Datenschutzanforderungen c1, i1, i2 und i3 zukünftig also keine ernsthaften technischen Hindernisse.

Allerdings sei erwähnt, daß für den Einsatz von Kryptographie in öffentlichen Netzen eine **Normierung der kryptographischen Systeme** sehr wünschenswert ist. Leider wurde sie aus politischen Gründen innerhalb ISO gestoppt – als ob das organisierte Verbrechen oder feindliche Staaten nicht

Experten zum Lesen der öffentlichen Literatur und zur Realisierung der ausgewählten Verfahren (etwa als Programm für Laptops) anstellen könnten [WaPP_87].

3 Schutz der Verkehrsdaten

In diesem Kapitel wird untersucht, inwieweit und wie die Datenschutzanforderungen c2 und c3 erfüllt werden können. Hierzu wird zunächst die Anwendbarkeit der für leitungsgebundene Netze bekannten Grundverfahren untersucht (Kap. 3.1). Danach wird das einzige für öffentliche Funknetze sinnvoll anwendbare Verfahren adaptiert (Kap. 3.2). Es ist dies das Verfahren der umcodierenden MIXe.

Dem eiligen oder an der Zwangsläufigkeit der Lösung nicht interessierten Leser sei empfohlen, Kapitel 3.1 vollständig zu überspringen und bei der Lektüre von Kap. 3.2.2 die Erläuterung von MIXen in Kapitel 3.1.3 und von Verteilung in Kap. 3.1.1 nachzuschlagen.

Es sei angemerkt, daß die Realisierung von c2 (und ggf. von c3) die Datenschutzanforderung i4 unterstützt, weil ein Netzbetreiber (oder – via Trojanischer Pferde – ein Netzkomponentenhersteller) die Opfer überzogener Entgeltforderungen nicht gezielt auswählen kann.

3.1 Anwendbarkeit der für leitungsgebundene Netze bekannten Grundverfahren

Nach einer kurzen Beschreibung der bekannten Grundverfahren zum Schutz der Verkehrsdaten geordnet nach ihrem Schutzziel (Schutz des *Empfängers*, Schutz des *Senders*, Schutz der *Kommunikationsbeziehung*) werden sie bzgl. Stärke und Aufwand verglichen. Für ausführlichere Erläuterungen sei auf [PfPW_88] oder [Pfit_90] verwiesen.

In Funknetzen sind nur die Grundverfahren zum Schutz des Empfängers und zum Schutz der Kommunikationsbeziehung anwendbar – was nach und nach begründet wird.

3.1.1 Schutz des Empfängers (Verteilung)

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.

3.1.2 Schutz des Senders

Neben dem Senden *bedeutungsloser Nachrichten* (aufwendig und nur sehr bedingt wirkungsvoll) sind *zwei Grundverfahren* bekannt, die im folgenden kurz beschrieben werden.

3.1.2.1 Unbeobachtbarkeit angrenzender Leitungen und Stationen sowie digitale Signalregenerierung

Das Netz wird so gebaut, daß es für jeden Angreifer genauso aufwendig wie Individualüberwachung ist, alle Ein- und Ausgänge einer Teilnehmerstation zu beobachten [Pfi1_83]. Dann genügt **digitale Signalregenerierung** [Pfit_90] zur Schaffung von Unbeobachtbarkeit, die etwa durch Zugriffsverfahren erhalten werden muß. Das bekannteste Beispiel ist das **RING-Netz**, bei dem die Teilnehmerstationen ringförmig verbunden sind.

3.1.2.2 Überlagerndes Senden (DC-Netz)

Auf einem beliebigen Bitübertragungsnetz, das an beliebig vielen Stellen abgehört und manipuliert werden kann, wird **überlagerndes Senden** (nach einem Beispiel von David Chaum **DC-Netz** genannt [Chau_88]) implementiert: Die Teilnehmerstationen haben paarweise miteinander Schlüssel ausgetauscht, deren Werte vor den anderen Teilnehmern (und erst recht Außenstehenden) geheim gehalten werden. Jede Station addiert (in einer endlichen abelschen Gruppe) zeichenweise ihre Nachricht (eine echte Nachricht oder die leere Nachricht) und alle ihr bekannten Schlüssel. Das *lokale Ergebnis* gibt jede Station aus, so daß die *globale Summe* aller lokalen Summen berechnet werden kann. Damit sich hierbei die paarweisen Schlüssel gegenseitig wegheben, verwendet jeweils einer, etwa der, der den Schlüssel generiert hat, bei der Bildung seiner lokalen Summe das additive Inverse des Schlüssels. Dann ist die globale Summe, die alle Stationen erhalten, die Summe aller echten Nachrichten.

Anonyme Zugriffsverfahren erlauben es den Stationen sehr effizient, ihre Nachrichten einzeln zu übermitteln.

Für das überlagernde Senden ist folgendes bewiesen: Hängen Stationen durch Schlüssel zusammen, deren Werte ein Angreifer *A* nicht kennt, so erfährt *A*, wenn er alle lokalen Summen erfährt, über die von diesen Stationen gesendeten Nachrichten nicht mehr, als wenn er nur die globale Summe erfährt. Abhören aller Leitungen liefert ihm also keine zusätzliche Information – das Senden im DC-Netz ist beweisbar anonym.

Vertiefungen sind in [Pfit_90, LuPW_91, PfWa1_91] nachzulesen.

3.1.3 Schutz der Kommunikationsbeziehung (MIX-Netz)

Um die Kommunikationsbeziehung zwischen Sender und Empfänger zu schützen, werden Nachrichten nicht direkt, sondern über **MIXe** geschickt. Damit die Wege der Nachrichten weder anhand ihres äußeren Erscheinungsbildes (also ihre 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, vgl. Bild 2.

Das Umcodieren erfolgt durch Ent- oder Verschlüsseln mittels eines Kryptosystems.

Die zusammen gemixten, d.h. zusammen gepufferten (oder erzeugten), umcodierten und umsortiert ausgegebenen Nachrichten werden als ein *Schub* bezeichnet.

Zusätzlich muß jeder MIX darauf achten, daß er *jede Nachricht nur einmal mixt* – oder, anders herum gesagt, daß er Nachrichtenwiederholungen ignoriert.

Würde nämlich 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.

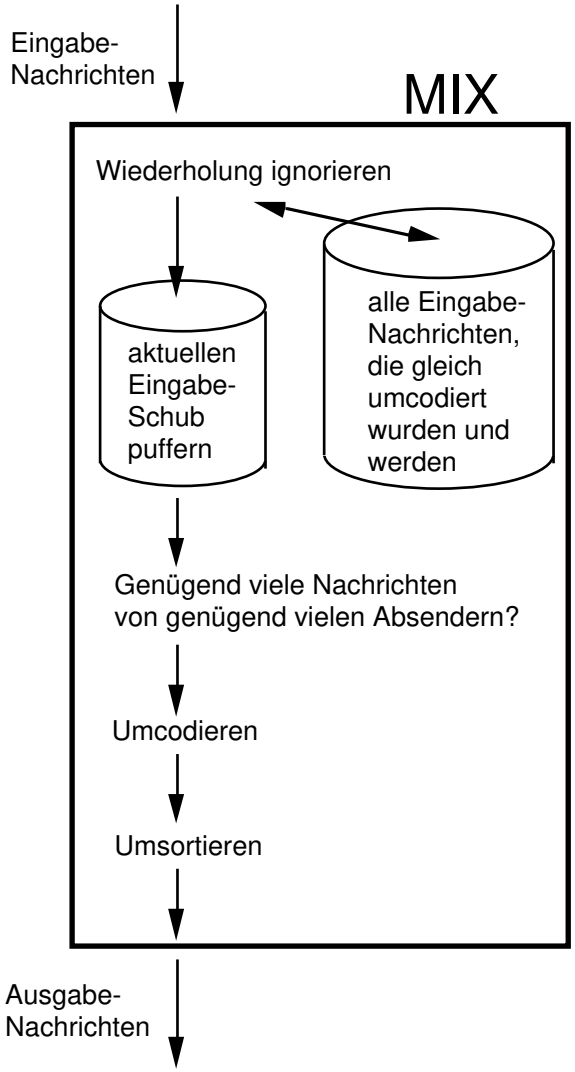


Bild 2: Grundfunktionen eines MIXes

In Bild 3 ist das Zusammenspiel mehrerer MIXe gezeigt, die die Nachrichten jeweils mit einem asymmetrischen Konzelationssystem umcodieren. Die von den Nachrichten durchlaufenen MIXe sollten möglichst *unabhängig entworfen und hergestellt* sein [Pfit_86 Seite 356] sowie *unabhängige Betreiber* haben [Chau_81, Cha1_84 Seite 99]. Denn andernfalls gibt es doch wieder einzelne Personen oder Organisationen, die den Schutz der Kommunikationsbeziehung allein aufheben können.

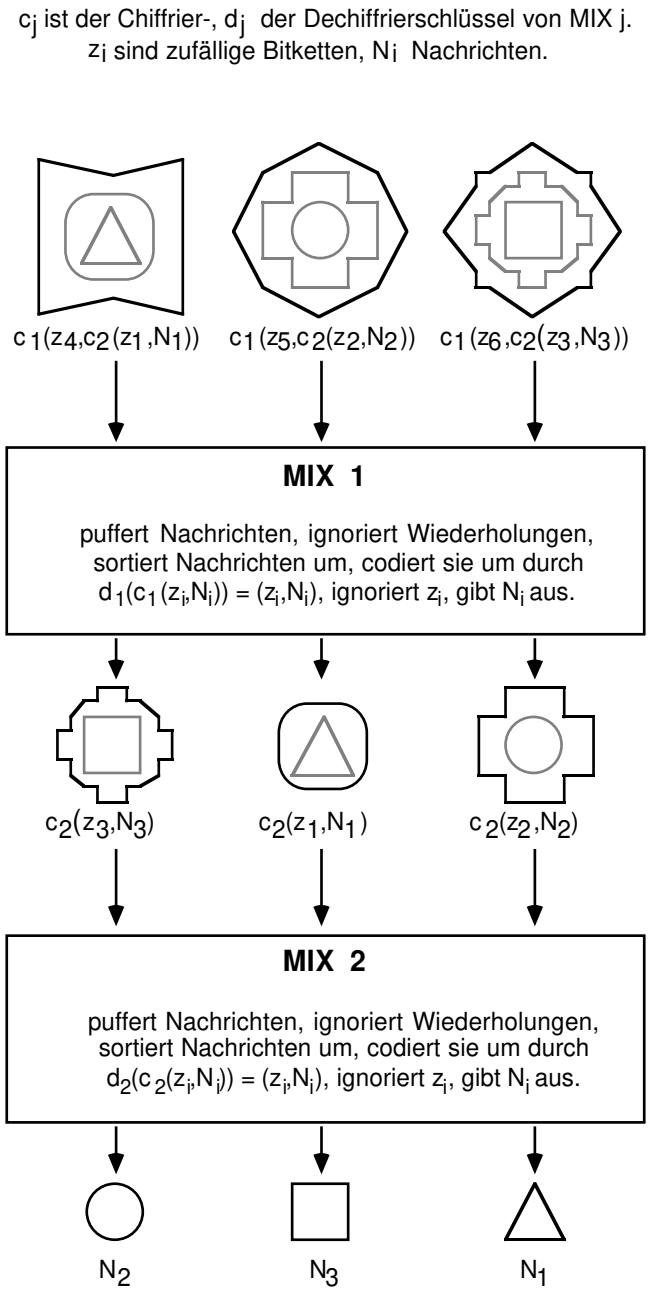


Bild 3: MIXe verbergen den Zusammenhang zwischen ein- und auslaufenden Nachrichten

3.1.4 Vergleich von Stärke und Aufwand von RING-, DC- und MIX-Netz

Um die Stärke der skizzierten Verfahren und ihren Aufwand zu vergleichen, ist die folgende Tabelle hilfreich. Man sieht, daß das DC-Netz zwar stärkeren Angreifern als das MIX-Netz widersteht. Dafür ist der Aufwand des MIX-Netzes signifikant geringer. Da Bandbreite in Funknetzen notorisch knapp ist (vgl. Kap. 1), ist letzteres dort besonders wichtig. Physisch beschränkte Angreifer, die wie beim RING-Netz nicht alle Übertragungswege abhören können, sind bei Funknetzen eine unrealistische Annahme. Das MIX-Netz dürfte daher am ehesten für die Lösung der Anforderung c2 in öffentlichen Funknetzen geeignet sein.

	Unbeobachtbarkeit angrenzender Leitungen und Stationen sowie digitale Signalregenerierung, z.B. RING-Netz	DC-Netz	MIX-Netz
Angreifermodell	physisch beschränkt	informationstheoretisch bzgl. Vertraulichkeit informationstheoretisch, bzgl. Diensterbringung komplexitätstheoretisch beschränkt	komplexitätstheoretisch beschränkt
Aufwand pro Station und pro Bit	Übertragung: $O(n)$ (genauer: $\geq \frac{n}{2}$)	polynomial in n, aber unpraktikabel Übertragung: $O(n)$ (genauer: $\geq \frac{n}{2}$) Schlüsselaustausch: $O(k \bullet n)$	Übertragung im Teilnehmeranschlußbereich: $O(k)$, praktisch: ≈ 1; Übertragung im Innern des Netzes, insgesamt: $O(k^2)$, praktisch: $\approx k$

n = Teilnehmerzahl k = Zusammenhang Schlüsselgraph DC-Netz, bzw. Anzahl MIXe

Tabelle: Aufwand der Grundverfahren

3.2 Adaption für Funknetze: Funk-MIXe

Funk-MIXe sind eine Adaption der umcodierenden MIXe für Funknetze:

In Kap. 3.2.1 wird kurz begründet, welche Annahmen über die Peil- und Identifizierbarkeit von Funkstationen sinnvoll sind.

Danach wird in Kap. 3.2.2 das Grundkonzept für den Schutz von Sender, Empfänger und momentanem Ort des Teilnehmers (c2, c3) in öffentlichen Funknetzen entwickelt. Dieses Grundkonzept – Funk-MIXe genannt – wird in Kap. 4 dann bzgl. c3 weiter verfeinert.

3.2.1 Defensive Annahme: Stationen sind peil- und identifizierbar, wenn sie senden

Wie bereits in [Pfi1_83 Seite 17, Pfit_90 Seite 101] erläutert wurde, ist es zumindest bezüglich technisch versierter Angreifer unrealistisch zu fordern, daß Signale, die von verschiedenen Stationen gesendet werden, nicht unterschieden werden können: Wegen der analogen Charakteristika des Senders und der bei jedem Produktionsprozeß unvermeidbaren Streuung dieser Charakteristika wäre dies praktisch und wegen der Änderung des Signals bei seiner Ausbreitung (Dispersion) bei kontinuierlichem Senden auch theoretisch nicht erfüllbar.

Dennoch sollten Hochfrequenztechniker das Funksystem so auslegen, daß Identifikation und Peilung der mobilen Teilnehmerstationen möglichst schwierig ist. Zusätzlich kann man hoffen, daß

bei manchen Anwendungen dem Angreifer unbekannte, die Signalausbreitung beeinflussende Umgebungen eine Identifikation praktisch sehr erschweren.

Trotzdem gehe ich im folgenden vorsichtshalber davon aus, daß eine **mobile Teilnehmerstation immer identifizierbar und peilbar ist, wenn sie sendet**. Daß dies keine exotische Annahme ist, möge folgendes Zitat belegen [BMI_89 Seite 297]: „Computergesteuerte Empfangs- und Auswerteeinrichtungen erlauben es der Fernmeldeaufklärung, aus einer Vielzahl von Signalen die Signale einzelner Geräte (jedes Einzelgerät weist besondere Charakteristiken auf) zu selektieren.“[4]

Im Gegensatz dazu gehe ich im folgenden davon aus, daß Teilnehmerstationen so ausgelegt werden können, daß sie **nicht identifizierbar und peilbar sind, wenn sie nur (passiv) empfangen**.

3.2.2 Funk-MIXe

Das Grundkonzept zum Schutz von Sender, Empfänger und momentanem Ort des Teilnehmers in Funknetzen, Funk-MIXe genannt, ist eine Kombination mehrerer Maßnahmen:

Funk-MIXe = Ende-zu-Ende-Verschlüsselung +
Verbindungs-Verschlüsselung zwischen mobiler und ortsfester Teilnehmerstation +
ortsfeste umcodierende MIXe +
Verteilung gefilterter Verbindungswünsche.

Diese Maßnahmen werden nun der Reihe nach erläutert.

Da Funkverkehr auch durch Außenstehende sehr leicht abhörbar ist, ist neben der immer notwendigen **Ende-zu-Ende-Verschlüsselung** auch **Verbindungs-Verschlüsselung** zwischen der mobilen Teilnehmerstation und der (aus ihrer Sicht) ersten ortsfesten Station angebracht, sofern die Protokollinformation der Schichten 1 bis 3 des ISO OSI Referenzmodells irgendeinen Personenbezug aufweist, vgl. [Pfit_90 Kap. 2.6].

Wegen der Knappheit der Übertragungsbandbreite und einer ansonsten jederzeit möglichen Identifikation und Peilung der mobilen Teilnehmerstation sind die in Abschnitt 3.1.2 beschriebenen Möglichkeiten zum Schutz des Senders („bedeutungslose Nachrichten“, „Unbeobachtbarkeit angrenzender Leitungen und Station sowie digitale Signalregenerierung“, „überlagerndes Senden“) weder anwendbar noch empfehlenswert. Auch die direkte Anwendung des Verfahrens der Telefon-MIXe [PfPW1_89, PfPW5_91] ist nicht möglich, da es MIXe und bedeutungslose Nachrichten über den Teilnehmeranschluß kombiniert.

Somit müssen Maßnahmen zum Schutz der Verkehrs- und Interessensdaten im wesentlichen im ortsfesten Teil des Kommunikationsnetzes abgewickelt werden. Folgendes Vorgehen bietet sich an (Bild 4):

Sofern die Codierung der Nutzdaten in mobilen genauso wie in ortsfesten Teilnehmerstationen erfolgt, kann das Verfahren der **umcodierenden MIXe** direkt angewendet werden, sofern die mobilen Teilnehmerstationen über genügend Verschlüsselungskapazität verfügen.

Ist die Codierung der Nutzdaten in mobilen Teilnehmerstationen anders als in ortfesten, beispielsweise um Übertragungsbandbreite zu sparen (z.B. 13 kbit/s Sprachkanal statt 64 kbit/s), so könnten der Empfänger und das Kommunikationsnetz dies zur Unterscheidung zweier Klassen von Sprachkanälen verwenden. In diesem Fall sollte, zumindest solange mobile Teilnehmerstationen nur einen

---

[4] Bei den D-Netzen ist solch Aufwand nicht einmal nötig, da jedes Gerät eine eindeutige Nummer hat und diese auch übermittelt. Dies ist gedacht, um durch Abgleich mit einer „schwarzen Liste“ gestohlene Geräte wiederzufinden oder aber zumindest von der weiteren Benutzung auszuschließen. Natürlich wären auch mit den technischen Datenschutzanforderungen c2 und c3 verträgliche Diebstahlsicherungen möglich – die Normer hätten nur rechtzeitig darüber nachdenken müssen.

sehr kleinen Teil aller Teilnehmerstationen bilden, von der mobilen Teilnehmerstation ein **Verbindungs-verschlüsselter Kanal zu einer ortsfesten Teilnehmerstation (möglichst des gleichen Teilnehmers)**[5] hergestellt, das Signal dort an die übliche Signalcodierung angepaßt und von dort mit den üblichen Verfahren zum Schutz der Verkehrsdaten weiterübertragen werden. Entsprechendes gilt, wenn zwar die Codierung der Nutzdaten in mobilen genauso wie in ortsfesten Teilnehmerstationen erfolgt, die mobilen Teilnehmerstationen aber nicht über genügend Verschlüsselungskapazität für die bei Verwendung von MIXen nötige Mehrfachverschlüsselung verfügen.

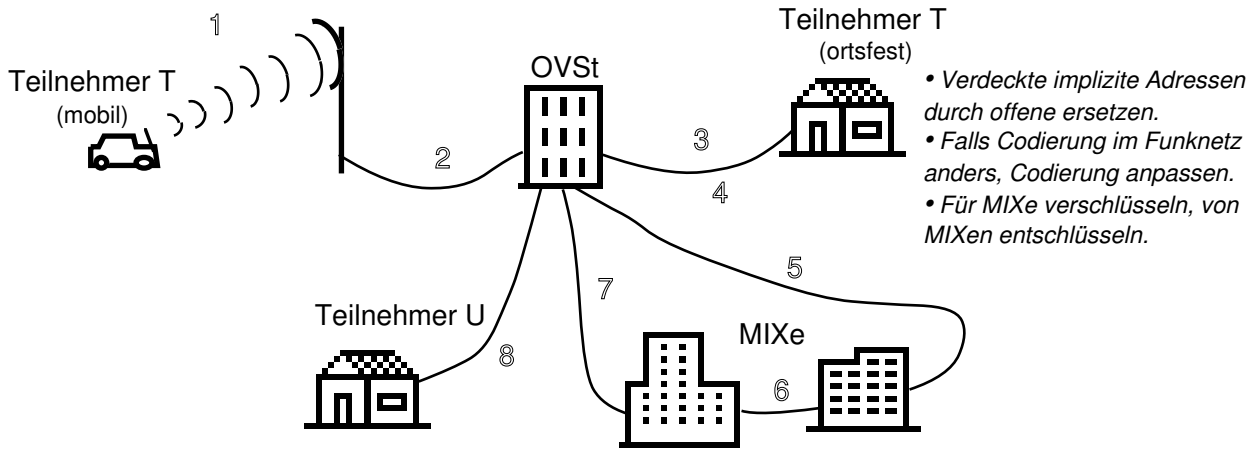
Während eine mobile Teilnehmerstation nur (passiv) empfängt, sollte sie (auch bei Zellularfunksystemen) vom Kommunikationsnetz nicht lokalisiert werden können. Liegt für sie ein Verbindungswunsch oder eine lange Nachricht vor, so sollte eine entsprechende **implizite Adresse im ganzen Funknetz** (und nicht nur in einer Funkzelle) **verteilt** werden, worauf sich die mobile Teilnehmerstation (aktiv) meldet und dadurch (gemäß der Annahme in Abschnitt 3.2.1) lokalisierbar ist. Da solche Verbindungswunschnachrichten nur wenige Bytes umfassen müssen, ist der Aufwand für diese Datenschutzmaßnahme gering – falls sie bei geeigneter Frequenzzuteilung nicht sogar zu einer Aufwandssenkung führt, da die Verwaltung eines Zellularfunksystems erheblich vereinfacht wird. Wie für diesen Zweck besonders kurze implizite Adressen verwendet werden können und durch Filterung unerwünschter Verbindungswünsche sowohl Bandbreite gespart wie auch eine unnötige Lokalisierung der mobilen Teilnehmerstation verhindert wird, wird in Kap. 4.1 beschrieben.

---

5 Um die Erklärungen nicht unnötig zu komplizieren, wird im folgenden jeweils davon ausgegangen, daß jeder Mobilfunkteilnehmer *genau eine* orstfeste Teilnehmerstation besitzt.

Besitzt der Mobilfunkteilnehmer *mehrere* ortsfeste Teilnehmerstationen, kann er die Aufgaben einer von ihnen statisch zuweisen oder aber – etwa um Übertragungsgebühren zu sparen – dynamisch jeweils der Teilnehmerstation, die räumlich gerade besonders günstig liegt.

Besitzt der Mobilfunkteilnehmer *keine* ortsfeste Teilnehmerstation, kann er die in den Erklärungen seiner orstfesten Teilnehmerstation zugedachten Aufgaben einer beliebigen ortsfesten Teilnehmerstation „seines Vertrauens“ übertragen. Solche Vertraulichkeitsdienste könnten von den unterschiedlichsten Firmen, Organisationen, staatsbürgerlichen Vereinigungen, etc. angeboten werden. Erhalten Großeinkäufer von Übertragungskapazität Mengenrabatte, kann aus der (datenschützerischen) Not sogar eine (kostensparende) Tugend werden.



Die Zahlen 1-8 geben die Reihenfolge der Übertragungsabschnitte von der Mobilstation des Teilnehmers T zum Teilnehmer U an. (Ohne Funk-MIXe würden nur die Abschnitte 1, 2 und 8 benötigt. Sind Mobilstation und ortsfeste Station des Teilnehmers T sowie Teilnehmer U nicht im selben Ortsnetz, so muß man sich statt einer Ortsvermittlungsstelle (OVSt) jeweils durch ein Fernnetz verbundene OVSts vorstellen.)

Verteilung von Verbindungswunschnachrichten erfolgt auf dem Abschnitt 1, sofern T der gerufene Teilnehmer ist.

Ende-zu-Ende-Verschlüsselung erfolgt durchgehend auf den Abschnitten 1-8.

Verbindungs-Verschlüsselung erfolgt durchgehend auf den Abschnitten 1-3.

Schutz der Verkehrsdaten mittels ortsfester umcodierender MIXe erfolgt auf den Abschnitten 4-8. Hier kann und sollte das Verfahren der Telefon-MIXe angewendet werden.

Bild 4: Funk-MIXe: Anschluß von Funk-Teilnehmern an ein MIX-Netz

Leider hat das beschriebene Verfahren der Funk-MIXe eine **prinzipielle Schwäche**. Diese Schwäche haben aber wohl alle Verfahren, die unter den Randbedingungen von Funknetzen arbeiten müssen:

Im Kommunikationsnetz (Übertragungsabschnitte 1-3 in Bild 4) ist beobachtbar, wann genau die Mobilstation sendet. Für interaktive Dienste mit unterschiedlicher Länge von Kommunikationsbeziehungen, beispielsweise Telefongespräche, könnte der Kommunikationspartner eines Funknetz-Teilnehmers in Zusammenarbeit mit dem Netzbetreiber (oder auch nur durch Abhören der Funkkanäle) die ihm bekannten Anfangs- und Endezeitpunkte „seines“ Gespräches mit denen der im Funknetz beobachtbaren Zeitpunkte vergleichen und so mit einer gewissen Wahrscheinlichkeit seinen Gesprächspartner identifizieren.

Diese Schwäche, die beim Verfahren der Telefon-MIXe durch das fortwährende Senden ggf. bedeutungsloser Zeitscheibenkanäle vollständig vermieden werden konnte [PfPW1_89, PfPW5_91], ist in Funknetzen nicht grundsätzlich behebbar. Einerseits fehlt heutzutage die Bandbreite im Funknetz, um alle Teilnehmer fortwährend mit ihrer maximalen Bandbreite senden zu lassen. Andererseits sollte „unnötiges“ Senden gerade vermieden werden, um die Zeiten der Peilbarkeit von Mobilstationen zu minimieren, vgl. Kap. 3.2.1. Es bleibt nur die Wahl eines Kompromisses: Beginn und Dauer von Telefongesprächen werden gerastert. Beispielsweise könnten sie alle 30 Sekunden beginnen und ein Vielfaches einer Minute dauern (wobei der Teilnehmer natürlich zu jedem Zeitpunkt auflegen kann – nur seine Station läßt die Verbindung ggf. noch etwas stehen). Dann kann man hoffen, daß immer genügend viele Gespräche gemeinsam beginnen und enden.

Eine von den bisher beschriebenen Maßnahmen zum Schutz der Verkehrsdaten unabhängige ist, den **Benutzer gegenüber seiner Sendestation anonym** zu halten. Dies macht immer dann Sinn, wenn

Sendestationen Benutzern nicht fest zugeordnet sind, wie dies etwa in den D-Netzen (GSM Zellularfunknetz) vorgesehen ist. In ihnen kann jeder Teilnehmer eine Chipkarte (SIM = Subscriber Identity Module) erhalten, mit der er jede Sendestation mit Chipkartenleser benutzen kann[6]. Ein Beispiel einer Anwendung wäre ein Mietwagen, wobei weder Funknetz noch Sendestation des Mietwagens erfahren sollten, wer die Sendestation gerade benutzt. Diese Anonymisierungsmaßnahme entspricht der in [PfPW_88 Kap. 2.1.1, Pfit_90 Kap. 2.4.1] diskutierten Benutzung öffentlicher Anschlüsse. Benutzer gegenüber ihrer Sendestation anonym zu halten, ist als alleinige Maßnahme zur Realisierung der technischen Datenschutzanforderungen c2 und c3 allerdings genauso unzureichend wie die ausschließliche Benutzung öffentlicher Anschlüsse, vgl. [Pfit_90 Kap. 2.4.1].

4 Schutz vor Belästigung und vor Ermittlung des Aufenthaltsortes mittels unerwünschtem Anruf

In diesem Kapitel wird zunächst die *Generierung kurzer offener impliziter Adressen* durch die ortsfeste Teilnehmerstation des gerufenen Teilnehmers beschrieben. Sie reduziert die zur Verteilung der Verbindungswunschnachrichten nötige Bandbreite, die bei der heutigen Frequenzzuteilung knappste Ressource in öffentlichen Funknetzen, auf ein Zehntel. Zusätzlich wird hierdurch die *Filterung unerwünschter Verbindungswünsche* leicht durchsetzbar: Die Generierung kurzer offener impliziter Adressen erfolgt durch die ortsfeste Teilnehmerstation des gerufenen Teilnehmers, also durch eine Station desjenigen, der geschützt werden soll.

Danach wird erläutert, wie beliebige, auch nichtanonyme Kommunikationsformen auf Netzen mit Schutz der Verkehrsdaten realisiert werden können. Wichtig für Datenschutz und Komfort des Teilnehmers ist die Realisierung eines „*digitalen Kommunikationsleibwächters*“.

4.1 Generierung kurzer offener impliziter Adressen, Filterung unerwünschter Verbindungswünsche und Verkleinerung der Broadcastgebiete durch ortsfeste Teilnehmerstation

Bereits in Kap. 3.2.2 wurde darauf hingewiesen, daß **Anrufe über die** (oder bei mehreren: eine) **ortsfeste Teilnehmerstation des Gerufenen geleitet** werden sollten, um

- im Funknetz mit **kurzen offenen impliziten Adressen** auszukommen und
- Anrufe nach einer vom Gerufenen frei festlegbaren Strategie **filtern** zu können.

Zusätzlich erlaubt das Einschalten einer ortsfesten Station des gerufenen Teilnehmers eine

- Verkleinerung der Gebiete, in denen die offenen impliziten Adressen verteilt werden müssen.

Dies wird nun der Reihe nach genauer begründet und erklärt.

4.1.1 Generierung kurzer offener impliziter Adressen spart Bandbreite im Broadcast-Signalisierungskanal und Aufwand bei der Adreßerkennung

Damit implizite Adressen für Unbeteiligte nicht miteinander verkettbar sind, müssen zumindest für die erste Nachricht zwischen zwei Teilnehmern *verdeckte* implizite Adressen verwendet werden, da im allgemeinen eine *öffentliche* Adresse verwendet werden muß, vgl. Bild 5 und Kap. 3.1.1, sowie [PfPW_88, Pfit_90]. Leitet man Anrufe über eine ortsfeste Teilnehmerstation des gerufenen Teilneh-

---

6 Im GSM-Standard ist auch die Möglichkeit vorgesehen, daß SIMs in Sendestationen fest eingebaut sind. Mit solchen Geräten ist die hier beschriebene Maßnahme nicht ohne weiteres praktikabel.

mers und läßt man diese die vom Sender verwendete, *öffentliche verdeckte* implizite Adresse durch eine *private offene* implizite Adresse zwischen ortsfester und mobiler Teilnehmerstation ersetzen, so spart dies erheblich Übertragungsbandbreite im **Broadcast-Signalisierungskanal**, in dem die Verbindungswunschnachrichten verteilt werden.

Die Ersparnis ergibt sich aus folgenden Eigenschaften impliziter Adressen: Aus kryptographischen Gründen müssen öffentliche verdeckte implizite Adressen heutzutage mindestens 500 Bit lang sein, während private offene schon mit etwa 50 Bit realisiert werden können. Dies liegt daran, daß öffentliche verdeckte implizite Adressen mittels eines asymmetrischen Konzelationssystems gebildet werden und keine sicheren asymmetrischen Konzelationssysteme bekannt sind, die kürzere Schlüsseltexte als 500 Bit erzeugen können. Zusätzlich bewirkt der technologische und algorithmische Fortschritt, daß diese kürzestmögliche Länge langsam steigt. Private offene implizite Adressen können hingegen als (im Prinzip beliebig kurze) Zufallszahlen realisiert werden. Hier muß lediglich die Wahrscheinlichkeit, daß mehrfach die gleiche Zufallszahl als Adresse verwendet wird, hinreichend klein sein. Dies ist bei einer Länge der Zufallszahlen von 50 Bit sicherlich der Fall.

		Adreßverwaltung	
		öffentliche Adresse	private Adresse
implizite Adresse	verdeckt	sehr aufwendig, für Kontaktaufnahme nötig	aufwendig
	offen	abzuraten	nach Kontaktaufnahme ständig wechseln

Bild 5: Kombinationen von Adressierungsart und Adreßverwaltung und vorgeschlagene Ersetzung

Zusätzlich spart die Ersetzung von verdeckten durch offene implizite Adressen bei Verbindungswünschen erhebliche Berechnungsfähigkeiten bei den mobilen Stationen ein: Die Erkennung von verdeckten impliziten Adressen erfordert im wesentlichen die Entschlüsselung in einem asymmetrischen Konzelationssystem, während die Erkennung von offenen impliziten Adressen mittels *Assoziativspeicher* und damit um viele Größenordnungen effizienter erfolgen kann [Pfit_90 Seite 65].

4.1.2 Filterung unerwünschter Verbindungswünsche durch ortsfeste Teilnehmerstation

Zusätzlich zur in Abschnitt 4.1.1 beschriebenen Aufwandsreduktion kann durch diese Adreßersetzung in der ortsfesten Teilnehmerstation verhindert werden, daß eine Filterung einfach umgangen werden kann. Die mobile Teilnehmerstation sollte nur auf die von der ortsfesten generierten Verbindungswunschadressen reagieren. Anderenfalls hätte man eine einfache Möglichkeit zur Ermittlung des Aufenthaltsortes aller im Funknetz erreichbaren Teilnehmer: Man schicke ihnen einfach einen Verbindungswunsch zu und beobachte, was im Netz passiert.

Um mißbräuchliche Ermittlung des Aufenthaltsortes von Teilnehmern auf das für die Diensterbringung unumgängliche Maß zu begrenzen und um den Broadcast-Signalisierungskanal sparsam zu nutzen, sollten vom Teilnehmer nicht gewünschte Gespräche nicht erst von der mobilen Teilnehmerstation, sondern bereits von einer ortsfesten abgelehnt werden. Hierzu sollte der rufende Teilnehmer

seiner Nachricht ggf. eine bereits von der ortsfesten Teilnehmerstation des Gerufenen interpretierbare *Dringlichkeit* („Priorität“, „zu erledigen bis“, etc.) und *Absenderangabe* (siehe Abschnitt 4.2) mitgeben.

Um einer mißbräuchlichen Verwendung von Dringlichkeiten entgegenzuwirken, kann mit jeder Priorität ein Geldbetrag (siehe Kap. 5) verknüpft werden, der vom Anrufer beim Kommunikationsnetz hinterlegt werden muß, damit dieses den Anruf weiterübermittelt. Fühlt sich der Gerufene von der angegebenen Priorität hereingelegt, nachdem er den Anruf akzeptiert hat, so fällt ihm das hinterlegte Geld zu, ohne daß er dies rechtfertigen müßte. Andernfalls wird das Geld vom Kommunikationsnetz an den Rufer zurückübereignet.

4.1.3 Verkleinerung der Broadcast-Gebiete: Eigene ortsfeste Teilnehmerstation weiß ungefähren Aufenthaltsort des mobilen Teilnehmers

Bei der Generierung der offenen impliziten Adresse kann die *ortsfeste Teilnehmerstation* gleichzeitig das in ihr – und nicht etwa im Kommunikationsnetz – vorhandene *Wissen über den momentanen Aufenthaltsort des Teilnehmers nutzen*, um der nur begrenzte Zeit gültigen (sonst wären Angriffe durch nochmaliges Aussenden schwer zu vereiteln) offenen impliziten Adresse eine Beschreibung einer geeignet großen Region mitzugeben, in der sich der Teilnehmer garantiert befindet. Auch dies spart erheblich Bandbreite im Broadcast-Signalisierungskanal: Verbindungswunschnachrichten müssen nicht mehr im ganzen Funknetz verteilt werden.

Hierbei steht der ortsfesten Teilnehmerstation möglicherweise nicht nur das (bei perfekter Auswertung aller analoger Funksignale gemäß der defensiven Annahme in Abschnitt 3.2.1 auch im Funknetz erfaßbare) Wissen zur Verfügung, wo und wann sich der Teilnehmer zum letzten Mal gemeldet hat. Der Teilnehmer kann und sollte ihr auch mitteilen, von wann bis wann er wo erreichbar sein wird. Hierdurch entsteht kein zusätzliches Datenschutzproblem, da die ortsfeste Teilnehmerstation für den Teilnehmer vertrauenswürdig ist. Umgekehrt stellt sich natürlich auch die Frage, wie der Teilnehmer seiner ortsfesten Station seine Reisepläne möglichst bequem mitteilen kann – und was überhaupt seine Motivation hierfür sein soll. Ersteres lasse ich bis auf die Anmerkung, daß Reiseplanung mittels „digitaler persönlicher Assistenten“ dieses Problem evtl. löst, als Forschungsfrage offen. Letzteres kann dadurch gelöst werden, daß die Verteilung der Nachrichten je nach Größe der Region, in der verteilt wird, unterschiedlich teuer ist. Hierbei ist allerdings darauf zu achten, daß die Systemgestaltung und Tarifierung nicht einen Verzicht auf Datenschutz belohnt, sondern die aktive Mitarbeit des Teilnehmers – denn Grundrechtsschutz sollte keine Einkommensfrage sein.

Sollte, aus welchen Gründen auch immer, die für die Verteilung der Verbindungswunschnachricht gewählte Region „falsch“ sein, muß die Verbindungswunschnachricht ggf. noch in weiteren Regionen verteilt werden. Im schlimmsten Fall – wenn etwa die Teilnehmerstation momentan nicht empfangsbereit ist – ergibt sich der Aufwand aus Abschnitt 3.2.2: Verteilung im ganzen Funknetz.

Die gerade beschriebene Verkleinerung der Broadcastgebiete für offene implizite Adressen schwächt die Erfüllung der technischen Datenschutzanforderung c3 genau dann nicht ab, wenn die gerufene mobile Teilnehmerstation auf die verteilte implizite Adresse zur Erbringung des Dienstes reagieren muß und dies auch tatsächlich tut: Nach den Annahmen in Abschnitt 3.2.1 ist sie dann (und nur dann) sowieso identifizier- und peilbar.

Die in diesem Abschnitt beschriebene Maßnahme sollte also nur bei Zweiwegkommunikationsdiensten und nur dann angewendet werden, wenn die Erreichbarkeit der gerufenen Mobilstation mit hoher Wahrscheinlichkeit gegeben ist.

Anmerkung:

Statt daß die ortsfeste Teilnehmerstation jedes Teilnehmers seinen ungefähren Aufenthaltsort kennt und den von ihr generierten privaten offenen impliziten Adressen **senderseitig** ihr Verteilgebiet mitgibt, kann dual dazu **empfängerseitig** die Verteilung von Verbindungwünschen folgendermaßen gesteuert werden:

1. Die zwischen ortsfester Teilnehmerstation und Mobilstation verwendeten privaten offenen impliziten Adressen werden *zeitintervallabhängig* gemacht.
2. Jede *Mobilstation sendet* der ihr gerade zugeordneten (d.h. am nächsten liegenden) Ortsvermittlungsstelle die im folgenden Zeitintervall für sie *gültigen privaten offenen impliziten Adressen* (die ansonsten nur sie und die entsprechende ortsfeste Teilnehmerstation kennen). Die Ortsvermittlungsstelle verteilt dann im jeweiligen Zeitintervall in ihrem Gebiet nur solche Verbindungswünsche, deren offene implizite Adresse sie von einer Mobilstation in ihrem Gebiet erhalten hat.

Analyse:

Der Vorteil der empfängerseitigen Steuerung ist, daß der Aufenthaltsort der mobilen Teilnehmer(stationen) genauer (sowohl räumlich wie zeitlich) bekannt ist, so daß durch Verkleinerung der Verteilgebiete mehr Bandbreite eingespart werden kann. Zusätzlich ist weniger Kommunikation mit der teilnehmereigenen ortsfesten Station nötig, was Fernverkehr(sentgelte) spart.

Ein Nachteil besteht darin, daß Teilnehmerstationen mehr senden müssen, nämlich ihre temporären privaten offenen impliziten Adressen. Damit dies nicht gemäß Abschnitt 3.2.1 die Erfüllung der technischen Datenschutzforderungen c2 und c3 deutlich abschwächt, sollte diese Mitteilung der temporären privaten offenen impliziten Adressen nur dann erfolgen, wenn die Teilnehmerstation sowieso senden muß.

4.2 Beliebige, auch nichtanonyme Kommunikationsformen auf Netzen mit Schutz der Verkehrsdaten

Auf einem Schutz der Verkehrsdaten durch *Anonymität*, *Unbeobachtbarkeit* und *Unverkettbarkeit* [Pfit_90] anbietenden Kommunikationsnetz sind beliebige, auch nicht anonyme Kommunikationsformen ohne Leistungseinbuße realisierbar.

Fast alle Verfahren, sich über ein Netz einander zu erkennen zu geben (d.h. sich zu identifizieren und authentisieren) oder seine Autorisation nachzuweisen, machen bereits heute keinen Gebrauch davon, daß das sendende oder empfangende Endgerät oder gar der es gerade benutzende Teilnehmer dem Kommunikationsnetz gegenüber identifizierbar ist. Zum Beispiel erkennt man Telefonpartner an ihrer Stimme und Sprechweise sowie ihrem Wissen, Briefpartner an ihrer (Unter-)Schrift. Fortschritte der Sprachsynthese machen die Erkennung von Telefonpartnern an ihrer Sprechweise und Stimme [Diff_82], Fortschritte in der Mustererkennung und Robotik die Erkennung anhand einer (Unter-)Schrift jedoch immer unzuverlässiger. Da es für beides jedoch digitale Entsprechungen gibt (digitale Signatursysteme), können übliche Identifikations- und Authentisierungsprotokolle weiterverwendet werden [DaPr_84].

Deren routinemäßiger Einsatz bei allen Diensten, bei denen dies wünschenswert ist, ist preiswert und praktisch ohne Manipulationschance möglich – sogenannte (externe) „Hacker“ sind also eigentlich kein Problem. Insbesondere ist es sowohl unsinnig als auch weitgehend erfolglos, mangelhafte Identifikations-, Authentisierungs- oder Autorisationsprüfung in Teilnehmerendgeräten (z.B. Mobiltelefonen, Rechenzentren, Datenbanken etc.) durch globale Beobachtung und Protokollierung im öffentlichen Kommunikationsnetz ausgleichen zu wollen: Dann „gehen Hacker“ eben durch ausländische Kommunikationsnetze und – ggf. dort – von der „Hackergemeinde“ betriebene MIXe, und

hinterher ist nichts beweisbar. Im übrigen ist vielfach auch ein Beweis gegen den Täter zur Schadensbewältigung nutzlos, beispielsweise wenn vertrauliche Information bekannt wurde.

Nach diesem Beispiel der anonymen oder eine falsche Benutzeridentität vortäuschenden Belästigung von Rechnern noch eins von Personen: Fühlt sich beispielsweise ein Teilnehmer durch nächtliche anonyme Anrufe belästigt, so kann er seine Teilnehmerstation instruieren, ihm Anrufe zwischen beispielsweise 21.00 und 8.00 Uhr nur dann zu signalisieren, *nachdem* sich der Anrufer dem Teilnehmerendgerät gegenüber identifiziert und dieses die *Identifikation gespeichert* hat. Wer will kann diesen „**digitalen Kommunikationsleibwächter**“ natürlich rund um die Uhr in Betrieb lassen. Analog kann jeder Netzteilnehmer den *Personenkreis*, für den er während gewisser Zeiten erreichbar ist, *einschränken*. Dies kann er mit den in Kap. 4.1.2 eingeführten *Dringlichkeiten* kombinieren.

Für manche Dienste (z.B. Kontaktanzeigen) können Möglichkeiten interessant sein, daß sich Teilnehmer *gleichzeitig* identifizieren [Gol2_83, Gol1_85].

5 Entgeltabrechnung

Bei einem öffentlichen Kommunikationsnetz muß ggf. eine komfortable und sichere Abrechnung der Kosten für die Netznutzung mit dem Netzbetreiber möglich sein (i4). Bei der Organisation der Abrechnung muß darauf geachtet werden, daß Anonymität, Unbeobachtbarkeit und Unverkettbarkeit im Kommunikationsnetz durch Abrechnungsdaten nicht verloren gehen (c2, c3).

Prinzipiell hat man dabei zwei Möglichkeiten: **Individuelle** Abrechnung nach Einzelnutzung (oder auch für Abonnements u.ä.) mit Verfahren, bei denen der bezahlende Teilnehmer anonym ist oder **generelle**, d.h. von allen Netzteilnehmern zu leistende, pauschale Bezahlung, die nicht anonym erfolgen muß, da dabei keine interessanten Abrechnungsdaten entstehen.

Für individuelle Abrechnung können entweder

- nicht manipulierbare Zähler [Pfi1_83 Seite 36f] oder
- anonyme digitale Zahlungssysteme

verwendet werden.

Die **nicht manipulierbaren Zähler** werden bei ortsfesten Teilnehmeranschlüssen zweckmäßigerweise im *Netzabschluß* [Pfit_90] oder bei mobilen in einem *SIM* (Subscriber Identity Module), beispielsweise einer *Chipkarte*, untergebracht. Sie entsprechen in ihrer Funktion den heutigen Elektrizitätszählern, nur daß sie über das Kommunikationsnetz ausgelesen werden können. Sind die Zähler technisch so gestaltet, daß dieses Auslesen nur in großen Zeitintervallen, z.B. alle Monate einmal, geschehen kann, geben diese Zähler nur sehr wenig personenbezogene Information ab, so daß zwischen Netzbetreiber und Teilnehmern über deren Zählerstände nichtanonym abgerechnet werden kann. Dies kann entweder – wie heute bei Elektrizitätszählern – durch **Rechnungstellung** der verbrauchten Einheiten geschehen (was für den Diensterbringer das Risiko der Illiquidität des Kunden birgt) oder mittels **vorausbezahlter Einheiten**, wie heute bei den Telefonwertkarten.

Hauptvorteil der Abrechnung mittels nicht manipulierbarer Zähler ist, daß im Kommunikationsnetz so gut wie kein Aufwand für Abrechnungszwecke getrieben werden muß. Hauptnachteile sind, daß ein Umgehen des Zählers durch Umgehen des Netzabschlusses oder des SIM genauso verhindert oder zumindest entdeckt werden muß wie eine Manipulation am Zählerstand. Beide Nachteile sind allerdings nicht sehr schwerwiegend, da (im Gegensatz zu allgemein verwendeten Zahlungsmitteln) mit diesen Zählern nur die Bezahlung einer einzigen Dienstleistung von – zumindest bei Privatleuten – üblicherweise eher geringem Wert möglich ist. (Auch heute sind Briefmarken wesentlich leichter zu fälschen als Geldscheine.) Die Abrechnung von Mehrwertdiensten hohen Wertes kann und sollte mittels der nachfolgend beschriebenen anonymen digitalen Zahlungssysteme erfolgen.

Bei Verwendung von **anonymen digitalen Zahlungssystemen** müssen die genauen Abrechnungsprotokolle so entworfen werden, daß von vornherein niemand betrügen kann, da bei ihnen die Anonymität, Unbeobachtbarkeit und Unverkettbarkeit eine nachträgliche Strafverfolgung generell be- oder gar verhindert [WaPf_85, PWP_90, BüPf_90]. Dies ist beim Abrechnungsproblem der Netznutzung sehr einfach zu erreichen: Der ersten aller verkettbaren Informationseinheiten (z.B. den die Adresse und die ersten Amplitudenwerte codierenden Bytes eines Telefongespräches) wird jeweils ein digitales, d.h. durch eine binäre Nachricht repräsentiertes Zahlungsmittel vorangestellt. Den Wert dieser „**digitalen Briefmarke**“ läßt sich der Netzbetreiber gutschreiben, bevor er die verkettbaren Informationseinheiten weiterbefördert und damit die Verbindung herstellt.

Hauptvorteil dieses Verfahrens der „digitalen Briefmarken“ ist, daß es ohne nicht umgehbare und nicht manipulierbare Zähler auskommt und bei einem „guten“ anonymen Zahlungssystem keinerlei personenbezogene Information anfällt. Hauptnachteil ist der nötige Kommunikationsaufwand. Um ihn erträglich und insbesondere die Verzögerungszeit kurz zu halten, sollte der Netzbetreiber die Funktion der „Bank“ im digitalen Zahlungssystem übernehmen.

Wünscht der Teilnehmer einen Einzelentgeltnachweis, so kann diesen je nach Funktionsverteilung entweder das Teilnehmerendgerät, der Netzabschluß oder das SIM erstellen – jedoch nur für ihn und nicht etwa auch dem Netzbetreiber zur Kenntnis.

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 zu erwarten ist (vgl. Kap. 1), ist z.B. ein pauschales Entgelt an den Netzbetreiber möglich.

6 Fehlertoleranz zur Steigerung der Verfügbarkeit

Zum Schluß sei noch daran erinnert, daß die mobilen Teilnehmerstationen so konzipiert werden sollten, daß sie in Katastrophensituationen (Naturkatastrophen, beispielsweise Überschwemmung eines Stadtviertels, oder massive Sabotageakte, seien sie physischer Natur oder via Trojanischer Pferde, die Übertragungsleitungen oder ortsfeste Vermittlungseinrichtungen weitgehend unbrauchbar machen) ohne den ortsfesten Teil des Kommunikationsnetzes in der näheren Umgebung auskommen und zusätzliche, normalerweise für Unterhaltung (Rundfunk) verwendete Frequenzen nach Erhalt einer „Freigabenachricht“ für Notrufe verwenden können [Pfit_90 Kapitel 5 und 6.1]. Dies unterstützt die Datenschutzanforderung „Ermöglichung der Kommunikation“ (a1).

Bei solchen Katastrophen muß und kann (da anonyme Notrufe von geheimgehaltenen Orten aus wenig Sinn machen und es wegen der Aufregung der Menschen bei Katastrophen sowie der daraus häufig resultierenden Unvollständigkeit der Absender- und Ortsangabe sogar zweckmäßig ist, diese Angaben automatisch zu übertragen) auf die Erfüllung der technischen Datenschutzanforderungen c2 und c3 verzichtet werden. Selbstverständlich sollte dies den Teilnehmern angezeigt werden.

7 Nachweis der Praktikabilität der Funk-MIXe

Für die Praktikabilität des in den Kapiteln 3.2 bis 5 beschriebenen Verfahrens der Funk-MIXe ist entscheidend, ob die (ggf. netzweite) Verteilung der Verbindungswunschnachrichten möglich ist. Im folgenden wird anhand eines einfachen **Leistungsmodells** für die Verteilung der Verbindungswunschnachrichten im D-Netz gezeigt, daß dies möglich ist. Damit steht einer Realisierung der Funk-MIXe technisch nichts im Wege.

Die Beispielrechnung basiert auf Zahlen, die ich [Hoff1_90, Pott_92] entnommen bzw. errechnet habe:

Im D-Netz gibt es in einer Funkzelle etwa 320 Kanäle zu je 22,8 kbit/s, in denen bisher jeweils ein Fernsprechkanal und die gesamte Signalisierung für diesen Kanal untergebracht ist.

Angenommen, wir könnten von den 22,8 kbit/s je 3 kbit/s als Broadcast-Signalisierungskanal zum Teilnehmer nutzen, so stünden in jeder Funkzelle

$$b = 320 \bullet 3 \text{ kbit/s} = 960 \text{ kbit/s}$$

zur Verfügung.

Die Anzahl n der via Verbindungswunsch-Verteilung bedienbaren Mobilfunkstationen wird im wesentlichen durch die Verteilung der Verbindungswunschnachrichten begrenzt: Jedem Netzabschluß steht anteilig lediglich ein Empfangskanal von je b/n zur Verfügung.

Wie stark diese Begrenzung ist, hängt von der Verkehrsstatistik ab. Vereinfachend wird angenommen, daß das Verteilnetz ein M/D/1-System sei [Klei_75], wobei λ die maximale mittlere Rate sei, mit der jeder der n Teilnehmer Verbindungswünsche erhält. Als Wert wird

$$\lambda = \frac{1}{300} \frac{1}{\text{s}}$$

angenommen, d.h. in Stoßzeiten im Mittel zwölf Verbindungswünsche je Teilnehmer und Stunde.

(Dieser Wert für λ ist sicher ausreichend, eher sogar zu hoch: Laut Fernsprechstatistik [SIEM_90] wurden 1988 in der Bundesrepublik *im Mittel* weniger als 3 Gespräche je Hauptanschluß und *Tag* geführt. Vertraut man den Erwartungen von Siemens, so dürfte der Wert λ = 1/300 1/s auch für Spitzenzeiten eher zu hoch sein: Laut [SIEM_88] verarbeitet der leistungsfähigste Vermittlungsrechner von Siemens im Endausbau 4,8 Vermittlungsversuche je Teilnehmer und Stunde. Außerdem interessieren beim Verfahren der Funk-MIXe für λ sogar nur die ankommenden Gespräche.)

Jede verteilte Verbindungswunschnachricht besteht aus B = 50 Bit, so daß maximal

$$\mu = \frac{b}{B} = \frac{960 \text{ kbit/s}}{50 \text{ Bit}} = 19200/\text{s}$$

Verbindungswunschnachrichten verteilt werden können.

Ist T_v die mittlere Systemzeit, d.h. die Zeit, die ein Verbindungswunsch im Mittel benötigt, um bei den Netzabschlüssen einzutreffen, so gilt nach [Klei_75 § 5.5, insbesondere (5.74)] in Stoßzeiten im Mittel

$$T_v = \frac{2 \bullet \mu - n \bullet \lambda}{2 \bullet \mu \bullet (\mu - n \bullet \lambda)}.$$

Hieraus ergibt sich

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

Für λ = 1/300 1/s, $T_v \le 0{,}5$ s, b = 960 kbit/s und B = 50 Bit ergibt dies

$$n \le 5\,759\,699.$$

Die M/D/1-Annahme ist, wie erwähnt, natürlich etwas vereinfachend. Allerdings schadet dies hier fast nichts: Die Ankünfte der Verbindungswunschnachrichten sind näherungsweise „gedächtnislos“, da eine Wahlwiederholung durch nochmalige Übertragung der Verbindungswunschnachricht nicht notwendig ist: Die Mobilstationen können, wenn sie einen Verbindungswunsch nicht sofort akzeptieren, die verteilte Verbindungswunschnachricht speichern und so bei nächster Gelegenheit einen Rückruf durchführen. Die Bedienzeit ist tatsächlich deterministisch, bis auf seltene, aufgrund von Fehlern notwendige Wiederholungen.

Die Beispielrechnung zeigt, daß selbst innerhalb der für das D-Netz vorgesehenen Übertragungsbandbreite und Struktur eine Verteilung der Verbindungswunschnachrichten zumindest innerhalb der gesamten Bundesrepublik möglich ist, wo momentan für ca. 2 Millionen Mobilfunkteilnehmer geplant wird.

Noch mehr, nämlich dreimal so viele Teilnehmer kann das geplante E-Netz verkraften, insgesamt also mehr als 17 Millionen nach obigem Leistungsmodell.

Das Beispiel sollte nicht als Empfehlung für das Beibehalten der Funkzellenstruktur zur Verteilung von Verbindungswunschnachrichten verstanden werden. Für zukünftige Netze erscheint es eher sinnvoll, für die Verteilung der Verbindungswunschnachrichten größere Regionen als kleinste adressierbare Einheiten zu definieren und die Frequenz(en) passend zu wählen. Auch bestehende Netze (etwa das D-Netz) könnten durch einen solchen zusätzlichen Verteilkanal vom Netz zur Teilnehmerstation nachgerüstet werden. Will man beispielsweise Verbindungswunschnachrichten europaweit verteilen und nimmt man für Europa einen Endausbau von maximal 60 Millionen Teilnehmern an, so müßte der Verteilkanal nach obiger Rechnung etwa 10 Mbit/s umfassen, was bereits bei heutiger Technologie keineswegs exorbitant viel ist. Würde solch eine Festlegung bald getroffen, so könnten die Mobilstationen der Teilnehmer gleich „ab Werk“ passend ergänzt werden – bisher wurden nämlich noch so gut wie keine D-Netz-Mobilstationen produziert.

8 Anwendung auf Verkehrsleitsysteme

Das über öffentlichen mobilen Funk Gesagte ist auch bei der Gestaltung von **Verkehrsleitsystemen** zu beachten: Es ist bezüglich Datenschutz unkritisch, Informationen an Fahrzeuge zu verteilen. Es ist sehr kritisch, wenn Fahrzeuge Informationen dauernd oder sehr oft senden müssen, wie dies im Projekt PROMETHEUS [FO_87, Walk_87] vorgesehen ist.

Wie in Abschnitt 1.2 dargelegt, sollten Verkehrsleitsysteme aus Datenschutzgründen zusätzlich so entworfen werden, daß Sensoren zwar Fahrzeuge erkennen, aber weder Fahrzeugtypen noch gar Fahrzeugexemplare unterscheiden können – anderenfalls entstehen Bewegungsbilder, die genausowenig geschützt werden können wie die in dieser Arbeit behandelten Verkehrsdaten.

9 Forschungs-, Normungs- und Entwicklungsbedarf

Ergänzend zu den in dieser Arbeit beschriebenen „digitalen“ Verfahren sollte erforscht werden, welche **Funkverfahren zur Erschwerung der Peil- und Unterscheidbarkeit von Funkstationen** eingesetzt werden können. Wichtige Fragen dabei sind:

- Was sind ihre Kosten?
- Wieviel Aufwand müßte ein Angreifer investieren, um trotz dieser Verfahren Funkstationen zu peilen und zu unterscheiden?

Nach Beantwortung dieser Fragen in einer für die öffentliche Forschung befriedigenden Weise sollte die defensive Annahme aus Kap. 3.2.1 überdacht und ggf. modifiziert werden.

Die beschriebenen Verfahren müssen in der Fachwelt dringend diskutiert, ggf. modifiziert und selbstverständlich noch genauer ausgearbeitet werden. Danach sollten sie unmittelbar in der **Normung** aufgegriffen und so ein möglichst breiter technischer, juristischer und sozialer Konsens zügig erreicht werden. In jedem Monat, der ungenutzt verstreicht, wird überprüfbarer Datenschutz in öffentlichen Funknetzen erheblich teurer.

Schließlich müssen die Normen in **Produkte** umgesetzt werden. Dies sollte in einem geradezu explodierenden Markt auch Marktneulingen erlaubt werden. Es könnte für sie sehr interessant sein, wenn

die bisherigen Lieferanten der Betreiber öffentlicher Funknetze mit ähnlicher Begeisterung wie bei der Realisierung von überprüfbarem Datenschutz in leitungsgebundenen öffentlichen Kommunikationsnetzen zu Werke gehen. Dort wird *jetzt* diskutiert, wie teuer *zukünftig* die Realisierung der bereits *1985* in den Grundzügen publizierten Verfahren [Pfit_85] geworden sein wird. Alles deutet auf ein bzgl. der Verwirklichung von Grundrechten, Erschließung neuer Produkte und Märkte sowie der damit verbundenen Technologiepolitik weitgehend verschenktes Jahrzehnt hin. Wird sich dies bei öffentlichen Funknetzen wiederholen?

Ein Dankeschön

an zahllose anonyme Mitreisende in europäischen Bahnen, daß sie mich weitgehend ungestört mit dem PowerBook schreiben ließen, alle FreundInnen und KollegInnen, die mich während der fraglichen Zeiten nicht erreichen (und auch nicht lokalisieren) konnten (denn ein Funktelefon hatte ich nicht dabei) für Ihre Geduld sowie *Birgit Pfitzmann* und *Kai Rannenberg* zusätzlich für beharrliche und konstruktive Kritik an mitgebrachten Textversionen!

Stichwörter

Technischer Datenschutz, überprüfbarer Datenschutz, vorbeugender Datenschutz, Unbeobachtbarkeit, Anonymität, Bewegungsprofile, Massenüberwachung, Fernmeldenetze, öffentliche Funknetze, Zellularfunknetz, Peilbarkeit, Nutzdaten, Verkehrsdaten, Verteilung, implizite Adresse, MIX-Netz, Funk-MIXe, Filterung von Verbindungswünschen, digitaler Kommunikationsleibwächter, Verschlüsselung, Entgeltabrechnung, digitale Briefmarke, Verkehrsleitsysteme

Literaturverzeichnis

Alke_88 Horst Alke: DATENSCHUTZBEHÖRDEN: Alles registriert – nur beim Autotelefon? Registrierung durch die DBP beim "normalen Telefon"; Vollspeicherung beim Autotelefondienst; Datenschutz und Datensicherung DuD /1 (1988) 4-5.

Alke_92 Horst Alke: Beitrag zur Podiumsdiskussion "Datenschutz in der Mobilkommunikation"; Dokumentation des ITG-Forums "Gestaltungsfelder beim Mobiltelefon", 12. Mai 1992, Frankfurt am Main, 29-31.

BMI_89 Bundesministerium des Inneren: Rahmenkonzept zur Gewährleistung der Sicherheit bei Anwendung der Informationstechnik; Datenschutz und Datensicherung DuD /6 (1989) 292-299.

BüPf_90 Holger Bürk, Andreas Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) 715-721.

Cha1_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.

Cha8_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.

Cott_92 Michael Cotta: Beitrag zur Podiumsdiskussion "Datenschutz in der Mobilkommunikation"; Dokumentation des ITG-Forums "Gestaltungsfelder beim Mobiltelefon", 12. Mai 1992, Frankfurt am Main, 13-15.

DaPr_84 D. W. Davies, W. L. Price: Security for Computer Networks, An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer; John Wiley & Sons, New York 1984.

Diff_82 Whitfield Diffie: Cryptographic Technology: Fifteen Years Forecast; ACM SIGACT News 14/4 (1982) 38-57.

FO_87 FO: Ein Fall für Prometheus; ADAC motorwelt /4 (1987) 50-53.

Gol1_85 Oded Goldreich: On Concurrent Identification Protocols; Eurocrypt '84, LNCS 209, Springer-Verlag, Berlin 1985, 387-396.

Gol2_83 Oded Goldreich: On Concurrent Identification Protocols; Laboratory for Computer Science, Massachusetts Institute of Technology, MIT/LCS/TM-250, December 1983.

Hoff1_90 Gerd E. Hoffmann: Europaweit GSM – Funktelefone für jedermann; Nachrichtentechnische Zeitschrift ntz 43/10 (1990) 748-753.

Klei_75 Leonard Kleinrock: Queueing Systems - Volume I: Theory; John Wiley and Sons, New York 1975.

Luka_92 Jörg Lukat: Flüsse und Spuren teilnehmerbezogener Daten im D1-Netz; Beitrag zur Podiumsdiskussion "Datenschutz in der Mobilkommunikation"; Dokumentation des ITG-Forums "Gestaltungsfelder beim Mobiltelefon", 12. Mai 1992, Frankfurt am Main, 8-12.

LuPW_91 Jörg Lukat, Andreas Pfitzmann, Michael Waidner: Effizientere fail-stop Schlüsselerzeugung für das DC-Netz; Datenschutz und Datensicherung DuD 15/2 (1991) 71-75.

Mich_91 Uwe Michel: Sicherheitsfunktionen im paneuropäischen Mobilfunknetz; Proc. Verläßliche Informationssysteme (VIS'91), März 1991, Darmstadt, Informatik-Fachberichte 271, Springer-Verlag, Heidelberg 1991, 133-145.

Oste_92 Thomas Osterkorn: Vorsicht, Nachbar hört mit!; Stern /46 (1992) 278-283.

Pfi1_83 Andreas Pfitzmann: Ein dienstintegriertes digitales Vermittlungs-/Verteilnetz zur Erhöhung des Datenschutzes; Fakultät für Informatik, Universität Karlsruhe, Interner Bericht 18/83, Dezember 1983.

Pfit_85 Andreas Pfitzmann: Technischer Datenschutz in diensteintegrierenden Digitalnetzen - Problemanalyse, Lösungsansätze und eine angepaßte Systemstruktur; Proceedings der 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, München, Oktober 1985, herausgegeben von P.P.Spies, IFB 113, Springer-Verlag, Berlin 1985, 96-112.

Pfit_86 Andreas Pfitzmann: Die Infrastruktur der Informationsgesellschaft: Zwei getrennte Fernmeldenetze beibehalten oder ein wirklich datengeschütztes errichten ?; Datenschutz und Datensicherung DuD 10/6 (1986) 353-359.

Pfit_90 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz; IFB 234, Springer-Verlag, Heidelberg 1990.

Pfit1_90 Andreas Pfitzmann: Entwicklungslinien der Informationstechnik und Informatik und ihre Auswirkungen auf rechtliche Beherrschung; Datenschutz und Datensicherung DuD 14/12 (1990) 620-627.

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

PfPW1_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 13/12 (1989) 605-622.

PfPW5_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.

PfRa_93 Andreas Pfitzmann, Kai Rannenberg: Staatliche Initiativen und Dokumente zur IT-Sicherheit – Eine kritische Würdigung; Computer und Recht 9/3 (1993) 170-179.

PfWa1_91 Birgit Pfitzmann, Michael Waidner: Unbedingte Unbeobachtbarkeit mit kryptographischer Robustheit; Proc. Verläßliche Informationssysteme (VIS'91), März 1991, Darmstadt, Informatik-Fachberichte 271, Springer-Verlag, Heidelberg 1991, 302-320.

Pott_92 Robin Potter: Implementation of PCNs Using DCS1800; IEEE Communications Magazine 30/12 (1992) 32-36.

PWP_90 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.

Raub1_92 Eckart Raubold: Computer persönlich, persönlicher, am persönlichsten?; PIK, Praxis der Informationsverarbeitung und Kommunikation 15/3 (1992) 134-135.

SIEM_88 SIEMENS: Vermittlungsrechner CP 113 für ISDN; SIEMENS telcom report 11/2 (1988) 80.

SIEM_90 SIEMENS: 1990 Internationale Fernmeldestatistik; International Telecom Statistics; Statistique internationale des télécommunications; Estadística internacional de telecomunicaciones; Status: January 1, 1989; SIEMENS Aktiengesellschaft ÖN ÖV Marketing, Postfach 70 00 73, D-8000 München 70, May 1990.

Tele6_90 Telekom Deutsche Bundespost: Das Mobilfunkssystem der Telekom. Information kann viele Wege gehen.; Telekom Deutsche Bundespost (November 1990) 1-35.

Tele7_90 Telekom Deutsche Bundespost: Komfort von der Telekom: das C-Netz; Telekom Deutsche Bundespost, September 1990.

Walk_87 Bernhard Walke: Über Organisation und Leistungskenngrößen eines dezentral organisierten Funksystems; Kommunikation in Verteilten Systemen; Anwendungen, Betrieb, Grundlagen; GI/NTG-Fachtagung, Aachen, Februar 1987, IFB 130, herausgegeben von N. Gerner und O. Spaniol, Springer-Verlag, Heidelberg, 578-591.

WaPf_85 Michael Waidner, Andreas Pfitzmann: Betrugssicherheit trotz Anonymität. Abrechnung und Geldtransfer in Netzen; 1. GI Fachtagung Datenschutz und Datensicherung im Wandel der Informationstechnologien, IFB 113, Springer-Verlag, Berlin 1985, 128-141; Überarbeitung in: Datenschutz und Datensicherung DuD 10/1 (1986) 16-22.

WaPP_87 Michael Waidner, Birgit Pfitzmann, Andreas Pfitzmann: Über die Notwendigkeit genormter kryptographischer Verfahren; Datenschutz und Datensicherung DuD /6 (1987) 293-299.