Datenschutz und Datensicherheit DuD 21/6 (1997) 328-333.

Ende-zu-Ende-Verschlüsselung in GSM-Mobilfunknetzen*

Hannes Federrath, Jan Müller

TU Dresden, Institut für Theoretische Informatik, 01062 Dresden

Zusammenfassung. Aufgrund des Fehlens von Bittransparenz der Sprechkanäle in Mobilfunknetzen nach dem GSM-Standard ist weder Ende-zu-Ende-Verschlüsselung der Sprache zwischen Teilnehmern des GSM-Mobilfunknetzes noch zu bzw. von Teilnehmern des Festnetzes oder anderer Mobilfunknetze möglich. Es werden Vorschläge gemacht, wie diesem Datenschutzdefizit entgegengetreten werden kann.

Dipl.-Inform. Hannes Federrath, seit 1994 wissenschaftlicher Mitarbeiter an der TU Dresden, Institut für Theoretische Informatik. Arbeitsgebiete: Sicherheit in verteilten Systemen, Technischer Datenschutz in Mobilkommunikationssystemen.

Dipl.-Inform. Jan Müller, 1992-1997 Studium der Informatik an der TU-Dresden, seit 1997 bei der Dresdner Bank AG Frankfurt, Konzernstab Organisation, IT-Sicherheit/Datenschutz, Arbeitsgebiet: Sicherheit in verteilten Systemen.

Stichworte: Mobilfunk, GSM, Ende-zu-Ende-Verschlüsselung.

1. Einführung

1.1. Motivation

Bei der Realisierung von Mobilfunknetzen nach dem GSM-Standard (Global System for Mobile Communication) [GSM_93] war aufgrund des hohen Konkurrenzdruckes durch außereuropäische Anbieter Zeit ein wichtiger Erfolgsfaktor. Man war sich wohl darüber einig, daß Sicherheit ein nicht zu vernachlässigender Aspekt sein dürfte. So wurde selbstverständlich Verschlüsselung angewendet, um nachher werbewirksam ankündigen zu können, das Netz sei abhörsicher [Tele_95, Mann_95]. Zwar ist das richtig, wenn sich die Abhörsicherheit auf die über die Luft übertragenen Daten bezieht, sobald aber die Daten ins Festnetz gelangen, werden sie entschlüsselt und dort weiterverarbeitet.

Im Juli 1995 existierten nach [Stat_95] in 35 europäischen Staaten öffentliche Mobilkommunikationsnetze, die von ca. 19 Millionen Menschen genutzt wurden, davon allein 3 Millionen (D-Netze, E-Netz und C-Netz zusammen) in Deutschland. Eine Reihe von Arbeiten (z.B. [Bath_92, FJKP_95, MüSt_95, Pfit_93, Walk_94]) beschäftigten sich mit Sicherheitsproblemen im GSM und deren Beseitigung. Die Hauptkritikpunkte sind dabei aus Sicherheitssicht:

* Diese Arbeit wurde finanziell unterstützt von der Gottlieb-Daimler- und Karl-Benz-Stiftung Ladenburg und der Deutschen Forschungsgemeinschaft. Wir danken Andreas Pfitzmann für Anregungen und Diskussionen, insbesondere zu Abschnitt 3.2.

- ständige Lokalisierbarkeit der Teilnehmer durch den Netzbetreiber,
- Intransparenz, was die Güte der eingesetzten Kryptoalgorithmen betrifft,
- Implementierung einseitiger Authentikationsprotokolle anstelle gegenseitiger Authentikation,
- fehlende Ende-zu-Ende-Dienste, insbesondere Verschlüsselung und Authentikation.

Dieses Papier beschäftigt sich mit der nachträglichen und weitgehend mit dem Standard verträglichen Implementierung von Ende-zu-Ende-Verschlüsselung im GSM. Für das ISDN (Integrated Services Digital Network) sind entsprechende Lösungen bereits bekannt (z.B. [Axla_95]).

1.2. Angreifermodell und Sicherheitsanforderungen

Es wird nur der Schutz der Nutzdaten (Sprache) untersucht, also nicht die Vertraulichkeit von Vermittlungsdaten. Diese können durch Ende-zu-Ende-Verschlüsselung nicht geschützt werden. Ebenfalls nicht betrachtet werden die Schutzziele Integrität, Verfügbarkeit, Unbeobachtbarkeit und Anonymität.

Außerdem werden die Teilnehmerendgeräte, also die Mobilstation und das Teilnehmerendgerät im Festnetz als vertrauenswürdige Bereiche betrachtet. Zusätzlich haben die Teilnehmer bereits die notwendigen Schlüssel nach einem sicheren Verfahren ausgetauscht. Ob dies symmetrische oder asymmetrische Schlüssel sind, ist im Kontext dieser Arbeit belanglos. Das ende-zu-ende eingesetzte Verschlüsselungsverfahren wird als kryptographisch sicher angenommen. Aus Effizienzgründen bzgl. der Schlüsselverteilung könnten asymmetrische Verfahren eingesetzt werden, mit denen ein symmetrischer Session Key zwischen den Teilnehmern ausgetauscht wird. Der Schutz der eigentlichen Nutzdaten erfolgt dann mit einem symmetrischen Verschlüsselungsverfahren.

Aus dem Angreifermodell können folgende Sicherheitsanforderungen abgeleitet werden:

1. Die Inhaltsdaten müssen während der Funkübertragung verschlüsselt sein.
2. Die Inhaltsdaten müssen zwischen den vertrauenswürdigen Bereichen der Teilnehmer ständig verschlüsselt sein.

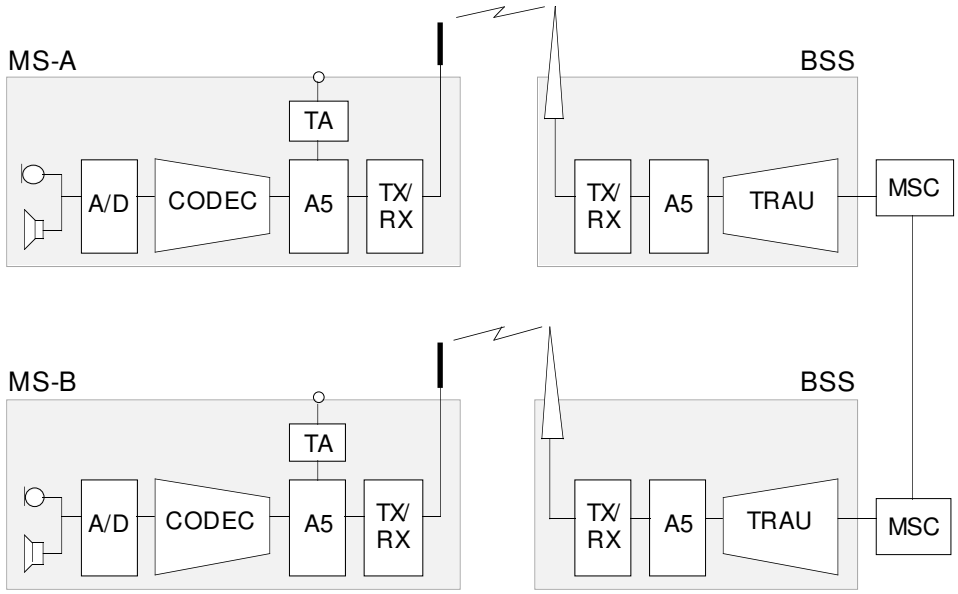
Diese Sicherheitsanforderungen kann man durch sichere Ende-zu-Ende-Verschlüsselung erfüllen, womit sich die Arbeit im weiteren beschäftigt.[1]

---

[1] Weiterhin muß natürlich gelten, daß die Teilnehmerendgeräte frei von Trojanischen Pferden sind, wenn sie in Betrieb genommen werden. Diese Kontrolle sollte entwicklungs- und produktionsbegleitend sein. Der nachträgliche Einbau von Trojanischen Pferden (z.B. während einer Fernwartung) in die Teilnehmerendgeräte muß ebenfalls ausgeschlossen werden können.

2. Der bestehende GSM-Standard

2.1. Sprachübertragung im GSM-Mobilfunknetz



MS	Mobile Station	A5	Verbindungsverschlüsselung
BSS	Base Station Subsystem	TX/RX	Transmitter/Receiver
A/D	Analog-Digital-Umsetzer	TRAU	Transcoder/Rate Adaption Unit
CODEC	Sprachcodierbaustein	MSC	Mobile Switching Centre
TA	Terminal Adaption		

Abb. 1: Übertragungsweg im GSM-Mobilfunknetz (schematisch)

Abb. 1 zeigt die Sprachübertragung im GSM-Mobilfunknetz am Beispiel eines Gespräches zwischen zwei Mobilteilnehmern A und B. Die einzelnen Komponenten werden nachfolgend näher betrachtet.

Bei der Sprachübertragung wird die Sprache zuerst im A/D-Wandler digitalisiert und mit einer Datenrate von 104 kbps (kBit/s) im Sprachkomprimierer (CODEC) verlustbehaftet bis auf 13 kbps komprimiert.

Die hohe Komprimierung der Sprache ist durch Redundanzreduktion und Irrelevanzreduktion [Heut_94] möglich. Beim Dekomprimiervorgang werden nicht die ursprünglich digitalisierten Wellen zurückgewonnen, sondern nur eine Annäherung der Wellen, die zur Sprachverständlichkeit und Sprechererkennung ausreichen. Der dadurch entstandene Informationsverlust ist für das menschliche Ohr wenig oder nicht hörbar.

Die Komprimierung ist notwendig, damit durch sparsame Ausnutzung der Bandbreite auf der Funkschnittstelle möglichst viele Gespräche innerhalb einer Funkzelle parallel geführt werden können. Anschließend werden die Daten mit dem Verschlüsselungsalgorithmus A5 verschlüsselt. Dabei handelt es sich um eine *Verbindungsverschlüsselung*, da die Daten bereits im nächstgelegenen Base Station

Subsystem (BSS) wieder entschlüsselt und unverschlüsselt im Klartext weiter übertragen werden.

Durch die verlustbehaftete Komprimierung in CODEC entsteht ein *nicht bittransparenter Sprachkanal*. Man bezeichnet einen Übertragungskanal als bittransparent, wenn er alle gesendeten Bitfolgen unverändert bis zum Empfänger überträgt. Durch das Fehlen von Bittransparenz wird der Einsatz von Ende-zu-Ende-Verschlüsselung erheblich erschwert, da ein um wenige Bits veränderter Schlüsseltext bei der Entschlüsselung je nach verwendetem Verfahren einen stark bzw. völlig veränderten Klartext erzeugt.

Bevor die Daten von der Mobilstation (MS) gesendet werden können, wird eine Kanalkodierung durchgeführt, um den Einfluß von Fehlern, die auf der Funkstrecke auftreten, zu minimieren. Durch diese Kodierung erhöht sich die Bitrate von 13 kbps auf 22,8 kbps.

Die TRAU (Transcoder/Rate Adaption Unit) im BSS (Base Station Subsystem) ist für die Umkodierung der Daten zur Übertragung innerhalb des GSM-Netzes oder bis zum Netz des Empfängers (bei einem ortsfesten Teilnehmer) verantwortlich. Dabei wird beim Sprachdienst mit dem im TRAU enthaltenen netzseitigen CODEC (dort Transcoder genannt) die Sprache auf maximal 64 kbps dekomprimiert, während beim Datendienst in der Rate Adaption Unit nur Datenratenanpassungen vorgenommen werden. Über die MSCs (Mobile Switching Centres) wird die Gesprächsverbindung vom BSS des Rufenden zum BSS des Gerufenen vermittelt.

GSM verfügt neben dem nicht bittransparenten Sprachkanal mit 13 kbps noch über einen bittransparenten Datendienst mit einer Datenrate von 9,6 kbps. Die Daten werden dabei zuerst über eine Terminal Adaption (TA) auf eine Datenrate von 12 kbps aufgefüllt und anschließend mit A5 verschlüsselt. Die weitere Verarbeitung der Daten verläuft bis auf die beschriebenen Unterschiede im TRAU analog der Sprachdatenverarbeitung.

In den bestehenden GSM-Mobilfunknetzen werden die Inhaltsdaten (Sprache, Daten) nur auf der Funkstrecke verschlüsselt. Bezüglich der aufgestellten Sicherheitsanforderungen muß man feststellen, daß Forderung 1 (aus Abschnitt 1.2) von der Stärke des verwendeten Kryptoalgorithmus abhängt, und Forderung 2 leider nicht berücksichtigt ist.

2.2. Sicherheitsalgorithmen

In GSM unterscheidet man 3 Sicherheitsalgorithmen. Der Algorithmus A3 dient zur Authentikation, A5 zur Verschlüsselung und A8 zur Schlüsselgenerierung (siehe auch [Pütz_97]). Im Rahmen dieser Arbeit und des aufgestellten Angreifermodells ist also nur der Algorithmus A5 von Interesse, da die Schlüssel als zuvor sicher ausgetauscht und Teilnehmer als zuvor beidseitig sicher authentisiert betrachtet werden. Der Klartextstrom wird mit einem pseudozufälligen Bitstrom bitweise XOR verknüpft. Dieser Bitstrom wird in A5 erzeugt. A5 ist europa- bzw. weltweit (Algorithmus A5X) standardisiert. Über seine kryptographischen Eigenschaften ist nichts bekannt. Der Algorithmus generiert alle 4,615 ms – das ist die Länge eines TDMA-(Time Division Multiple

Access)-Frames – eine Folge von 114 pseudozufälligen Bits. Die Rahmennummer dient der Synchronisation zwischen Mobilstation und BSS, wo netzseitig der gleiche Algorithmus angewendet wird. Über die Stärke des Algorithmus ist bekannt, daß sich der pseudozufällige Bitstrom erst nach ca. 209 Minuten wiederholt, da sich dann die Rahmennummer wiederholt.

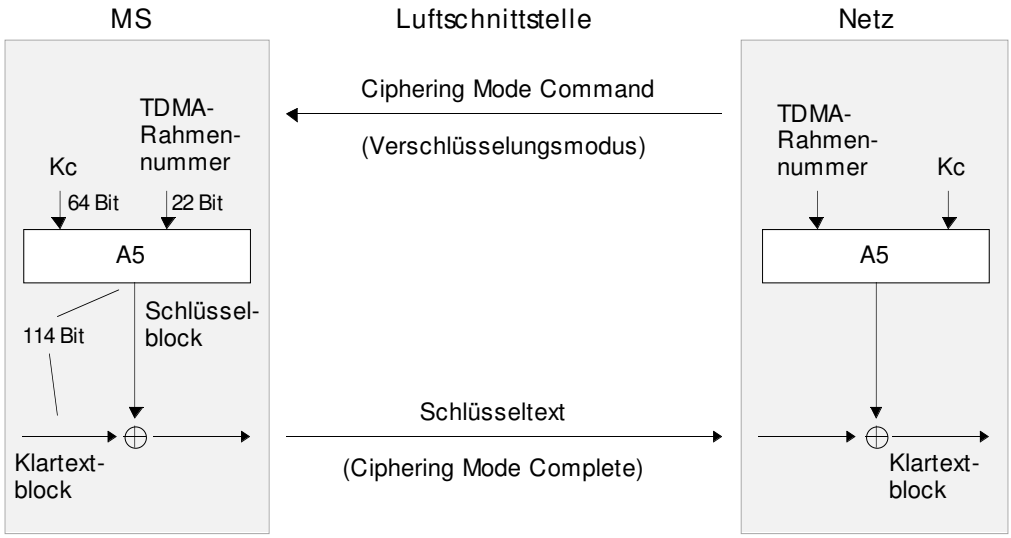


Abb. 2: Verbindungsverschlüsselung auf der Luftschnittstelle

3. Lösungsansätze für Ende-zu-Ende-Vertraulichkeit im GSM

Um Ende-zu-Ende-Vertraulichkeit zu erreichen, sind prinzipiell mehrere Wege möglich.

1. Man kann das Problem des nicht bittransparenten Sprachkanals umgehen, indem man den vorhandenen bittransparenten Datenkanal, wie unter 3.1 beschrieben, nutzt.
2. Einen zweiten Weg stellen Eingriffe in den nicht bittransparenten Sprachkanal, wie unter 3.2 beschrieben, dar, um diesen für die Teilnehmer bittransparent zu machen, wobei das Verfahren aus 3.3 im Prinzip eine Mischform aus beiden darstellt.
3. Eine dritte Möglichkeit wäre die Erarbeitung einer neuen, vom GSM-Standard abweichenden Architektur, die einen bittransparenten Sprach- und einen bittransparenten Datenkanal bietet, in denen die hier aufgestellten Forderungen des Datenschutzes realisiert sind. Dieser Weg wird in dieser Arbeit nicht näher betrachtet. Zweifellos wäre dies aber die Lösungsmöglichkeit mit den wenigsten Kompromissen.

Bei den folgenden Lösungsvorschlägen ist es unwesentlich, welcher Verschlüsselungsalgorithmus zum Einsatz kommt. Zweckmäßigerweise wählt man asymmetrische Verfahren zum Austausch eines Sitzungsschlüssels und verwendet anschließend symmetrische Verfahren, um die Echtzeitforderungen zu erfüllen. In den

folgenden Lösungsansätzen wird der Ende-zu-Ende-Verschlüsselungs-/Entschlüsselungsbaustein mit E/D (Encrypt/Decrypt) bezeichnet.

Die folgenden Verfahren sind jeweils für eine Kommunikation zweier mobiler Teilnehmer beschrieben. Für eine Kommunikation zwischen einen Mobilteilnehmer und einem Festnetzteilnehmer eignen sich diese mit geringfügigen Anpassungen ebenfalls.

3.1. Nutzung des bittransparenten Datenkanals

In Abb. 3 ist der prinzipielle Aufbau zur Erreichung von Ende-zu-Ende-Vertraulichkeit zweier mobiler Teilnehmer unter Nutzung des bittransparenten Datenkanals beschrieben. Da dieser 9,6 kbps-Kanal bittransparent ist, kann man Ende-zu-Ende-Verschlüsselung einfach hinzufügen. Man benötigt allerdings zusätzlich einen verbesserten CODEC, hier bezeichnet mit CODEC*, der das eingehende digitalisierte Sprachsignal von 104 kbps auf 9,6 kbps, statt der bisher 13 kbps, komprimiert.

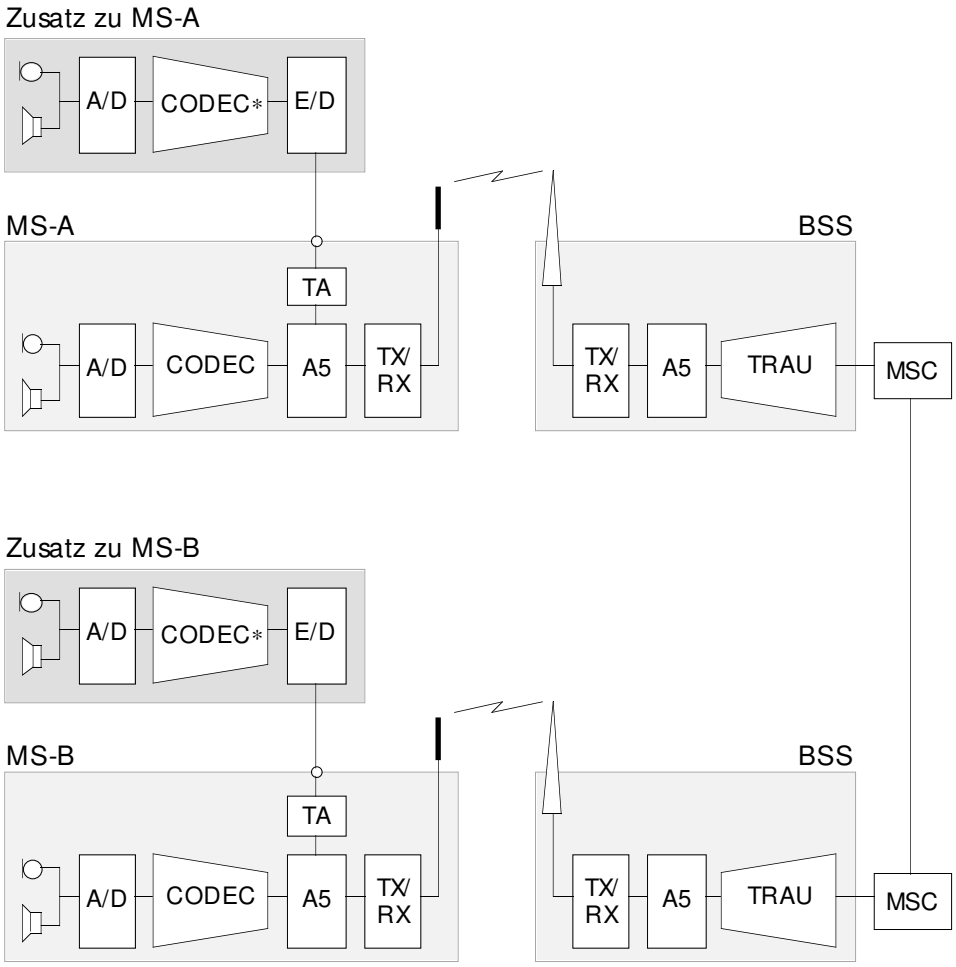


Abb. 3: Nutzung des bittransparenten Datenkanals mit 9,6 kbps

Diese Reduzierung der nutzbaren Datenrate von 13 kbps auf 9,6 kbps ist auch der Nachteil des Verfahrens. Dieser Nachteil ist aber aufgrund neuer Entwicklungen und

Implementierungen gering. So ist Half-Rate GSM (siehe [GSM_06.20]) bereits verfügbar und komprimiert die Sprache auf 6,5 kbps. Außerdem existieren Lösungen für CODEC-Bausteine mit Datenraten bis zu 2,4 kbps und darunter (siehe [AtKE_95]).

Als weiterer Nachteil können sich die hohen Anforderungen an die Echtzeit der Übertragung erweisen. Die Daten werden im Fehlerfall erneut übertragen (ARQ, Automatic Request Forretransmission). Bei der Sprachübertragung über den Datenkanal ist eine daraus resultierende Verzögerung nicht tolerierbar, deshalb müßte man durch Messungen den Einfluß solcher Fehler bestimmen und entsprechend reagieren.

Möchte ein Teilnehmer ende-zu-ende-vertraulich kommunizieren, so benötigt er ein Mobiltelefon, das die Datenübertragung unterstützt und ein Zusatzgerät. Diese „Set-Top-Box„ enthält dann außerdem Funktionen des Schlüsselmanagements und der Authentikation, die hier nicht betrachtet werden.

Die Nutzung des bittransparenten Datenkanals stellt also durchaus eine praktikable Lösung des Problems der Ende-zu-Ende-Vertraulichkeit dar, wenn man den Echtzeitanforderungen genügen kann. Der Nachteil der Reduzierung der Datenrate macht sich lediglich in einem leicht erhöhten Hintergrundrauschen bemerkbar, das tolerierbar ist.

Damit die nachfolgenden Lösungsvorschläge sinnvoll sind, sollten sie sich also durch eine höhere nutzbare Datenrate oder geringeren Realisierungsaufwand auszeichnen.

3.2. Ergänzung des Signallaufes durch Modems

Eine andere Möglichkeit für sichere Ende-zu-Ende-Kommunikation stellen Veränderungen des Sprachkanals dar. Ziel solcher Modifikationen muß es sein, den vorhandenen nicht bittransparenten 13-kbps-Sprachkanal bei möglichst hoher Datenrate bittransparent zu machen. Der Einsatz von Modems ist eine Alternative. Diese müssen möglichst genau an den Übertragungskanal angepaßt werden, damit der mit den Modems entstehende bittransparente Kanal noch über eine ausreichend hohe nutzbare Datenrate verfügt.

Abb. 4 zeigt den Signalverlauf bei Verwendung von Modems für vertrauliche Ende-zu-Ende-Kommunikation. Zur besseren Übersicht wurde das BSS weggelassen.

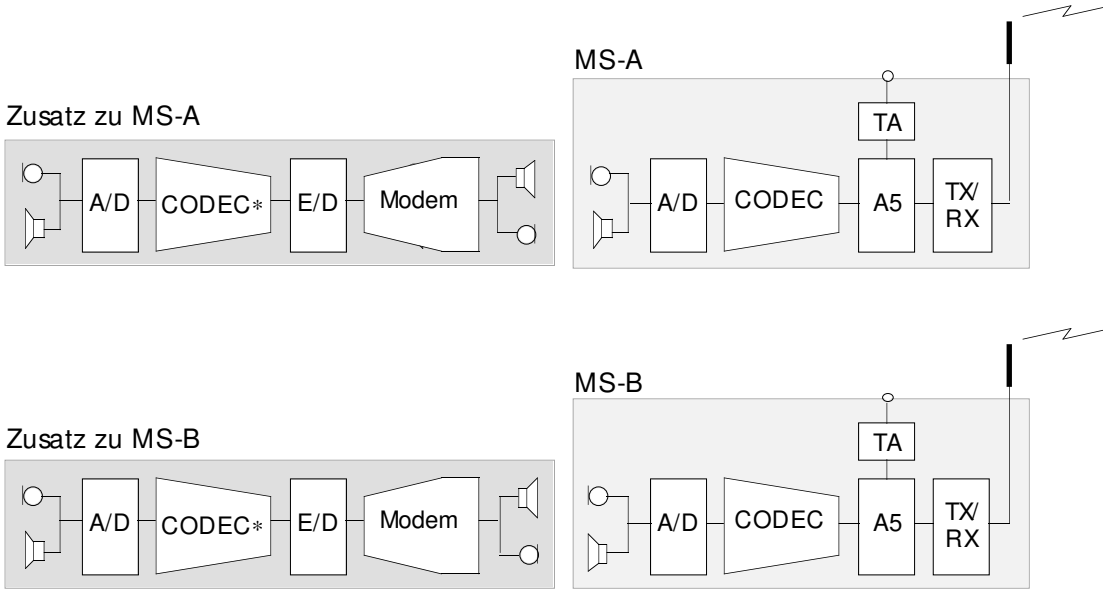


Abb. 4: Ergänzung des Signallaufes durch Modems

Im folgenden wird beschrieben, wie man diese Modems bezüglich des verwendeten Kanals anpassen muß. Dabei wird der Übertragungskanal nur noch mit den CODECs und A/D-Wandlern dargestellt, da dies die interessanten Bausteine für die Bittransparenz des Kanals sind (Abb. 5).

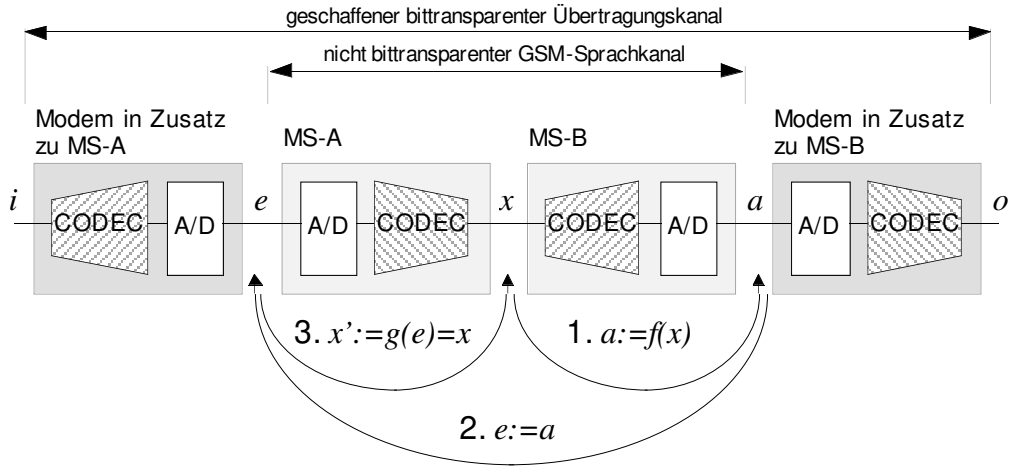


Abb. 5: Kanalanpassung der Modems

Dabei müssen folgende Voraussetzungen erfüllt sein:

1. Zu jeder Bitkombination des Übertragungssignals *x* gehört (genau) ein anderes analoges Ausgangssignal *a*.
2. Wird ein Ausgangssignal *a* wieder als Eingangssignal *e* verarbeitet, so überträgt der Kanal wieder dieselbe Bitkombination des Übertragungssignals *x*.

3. Das Übertragungssignal *x* bleibt auf der Übertragungsstrecke durch das Netz konstant.

Vernachlässigt man weiterhin die Verluste bei der Analog/Digital-Umsetzung, so erhält man aus dem nicht bittransparenten 13 kbps Kanal zwischen den Punkten *e* und *a* einen bittransparenten 13 kbps Kanal zwischen den Punkten *i* und *o*.

Es ist also unter den gegebenen Voraussetzungen möglich, das Modem des Teilnehmers B so zu bauen, daß es die Funktionalität des CODECs der Mobilstation des Teilnehmers A enthält und umgekehrt und dadurch eine gute Anpassung an den vorhandenen Kanal zu erreichen (Bausteine mit der gleichen Schraffur sind identisch).

In der Praxis sind solche Umwandlungen aber verlustbehaftet. Deshalb wird zusätzlich eine fehlerkorrigierende Kanalkodierung benötigt. Dadurch verringert sich die Datenrate des bittransparenten Sprachkanals je nach Fehlerrate auf Werte deutlich unter 13 kbps. Außerdem muß man bei dieser Lösung den Spezialisierungsgrad des CODECs beachten, da dieser im GSM sprachoptimiert ist. Sendet man diesem CODEC nicht-sprachliche Signale, so leidet seine Performance darunter beträchtlich (siehe [GSM_06.10]).

Weiterer Forschungsbedarf besteht darin festzustellen, ob der vorhandene Kanal in GSM den aufgestellten Voraussetzungen für den effektiven Einsatz von Modems genügt.

In der Praxis ist bei diesem Verfahren u.U. mit deutlichen Datenrateeinbußen zu rechnen, so daß die verfügbare Datenrate unter den 9,6 kbps des bittransparenten Datenkanals liegen kann. Erfüllt der GSM-Sprachkanal nicht die oben aufgestellten Forderungen, so wird so viel Redundanz bei der Kanalanpassung nötig, daß diese Lösung gänzlich unattraktiv wird.

Der Teilnehmer benötigt auch für diese Variante ein Mobiltelefon, und ein Zusatzgerät. Diese Set-Top-Box enthält außerdem wieder Funktionen des Schlüsselmanagements und der Authentikation, die hier nicht betrachtet werden. Man könnte eine solche Set-Top-Box vom Äußeren beispielsweise mit dem Zusatzgerät zur Fernabfrage von Anrufbeantwortern bei Telefonen im Festnetz vergleichen.

3.3. Modifizierung des Signallaufes durch Protokolländerungen

Die Grundidee dieser Variante besteht darin, den Signallauf innerhalb der MS gemäß GSM durchzuführen und durch die Änderung von Protokollinformationen zu erreichen, daß netzseitig im BSS der CODEC „übergangen„ und das redundanzreduzierte und verschlüsselte Sprachsignal bis zum Endteilnehmer durchgeschleift wird. Der Vorteil besteht darin, daß man die Sprache mit 12 kbps bittransparent übertragen kann (entsprechend der Datenrate des Datendienstes nach der TA, siehe Abschnitt 2.1).

Abb. 6 zeigt noch einmal den bestehenden GSM-Kanal vor den Veränderungen. Der Detaillierungsgrad wurde dabei so gewählt, daß die relevante Funktionalität der TRAU schematisch dargestellt wird, da die modifizierte Signalisierung hier später eine Veränderung des Signallaufs bewirkt. Zur Vereinfachung wurde nur der Informationsfluß von MS-A zu MS-B dargestellt.

Die Art der Information (Daten, Sprache) wird im GSM-Netz „in band,, signalisiert, d.h. die übertragenen Informationen beinhalten eine Vielzahl von Attributen zur Signalisierung. Das sind z.B. die Art der zu übermittelnden Informationen (Sprache, Daten unterschiedlicher Übertragungsrate) und die zu verwendenden Fehlerkorrekturverfahren.

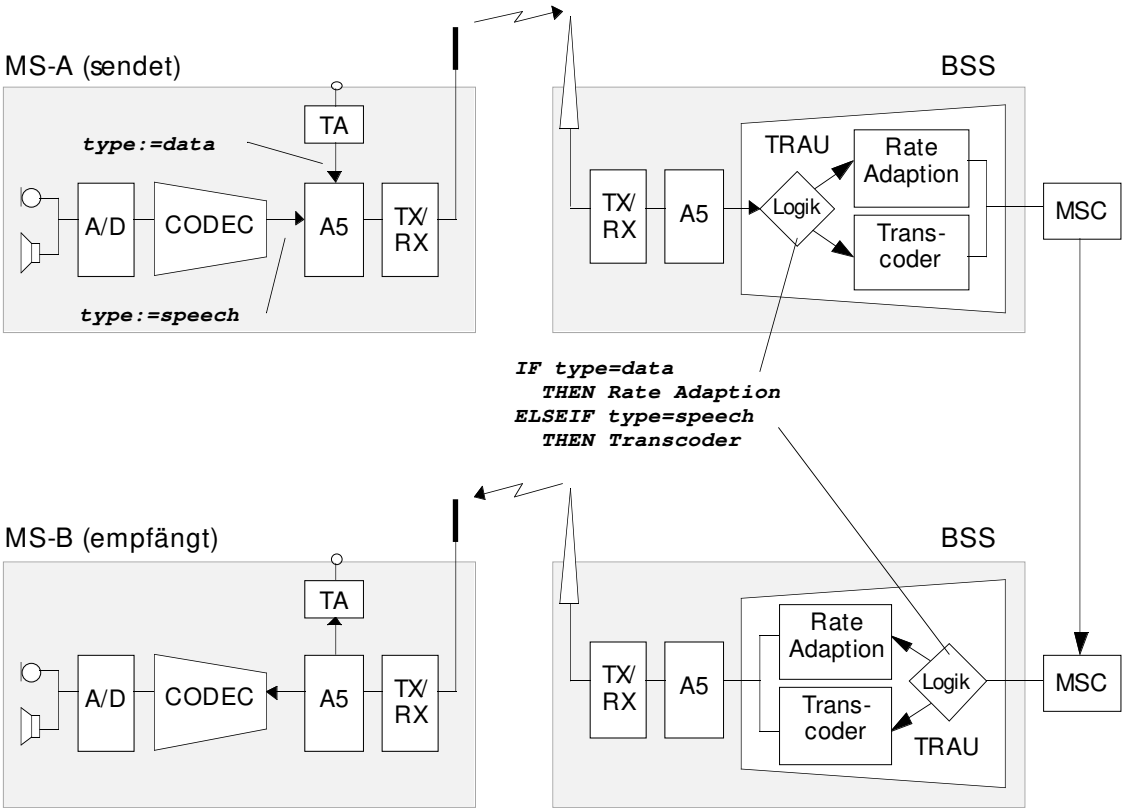


Abb. 6: Signalisierung des Datentyps (Sprache, Datendienst) im GSM (schematisch)

Die Aufgabe besteht darin, die Mobilstationen so zu erweitern, daß sie den nötigen Encrypt/Decrypt-Baustein (E/D) enthalten, und daß sie in der Lage sind, in einem zusätzlichen Signalisierungsattribut der Mobilstation des Kommunikationspartners zu signalisieren, das sie verschlüsselte Sprache senden. Dem GSM-Netz wird die verschlüsselte Sprache dagegen als Daten signalisiert.

Man muß für diesen Vorschlag zwar die Mobiltelefone modifizieren, braucht aber keine Veränderung am bestehenden GSM-Netz bzw. seinem Standard vorzunehmen, lediglich eine Erweiterung des Standards ist nötig.

Abb. 7 zeigt die nötigen Modifikationen zur Realisierung dieser Variante. Die MS signalisiert dem Netz im Falle einer ende-zu-ende-verschlüsselten Sprachübertragung Daten (`type:=data`). Ein neu hinzukommendes Attribut wird zur Unterscheidung zwischen einer „echten,, Datensendung und verschlüsselter Sprache verwendet (`edtype:=encrypted_speech`). In der BSS wird das Attribut `edtype` übergangen, während die verschlüsselte Sprache durch das Attribut `type` einer Ratenanpassung ausgesetzt wird, die aber nicht zu einem Verlust der Bittransparenz führt.

In der empfangenden MS wird das Attribut `edtype` zusätzlich ausgewertet und die Daten entweder an TA oder E/D weitergegeben.

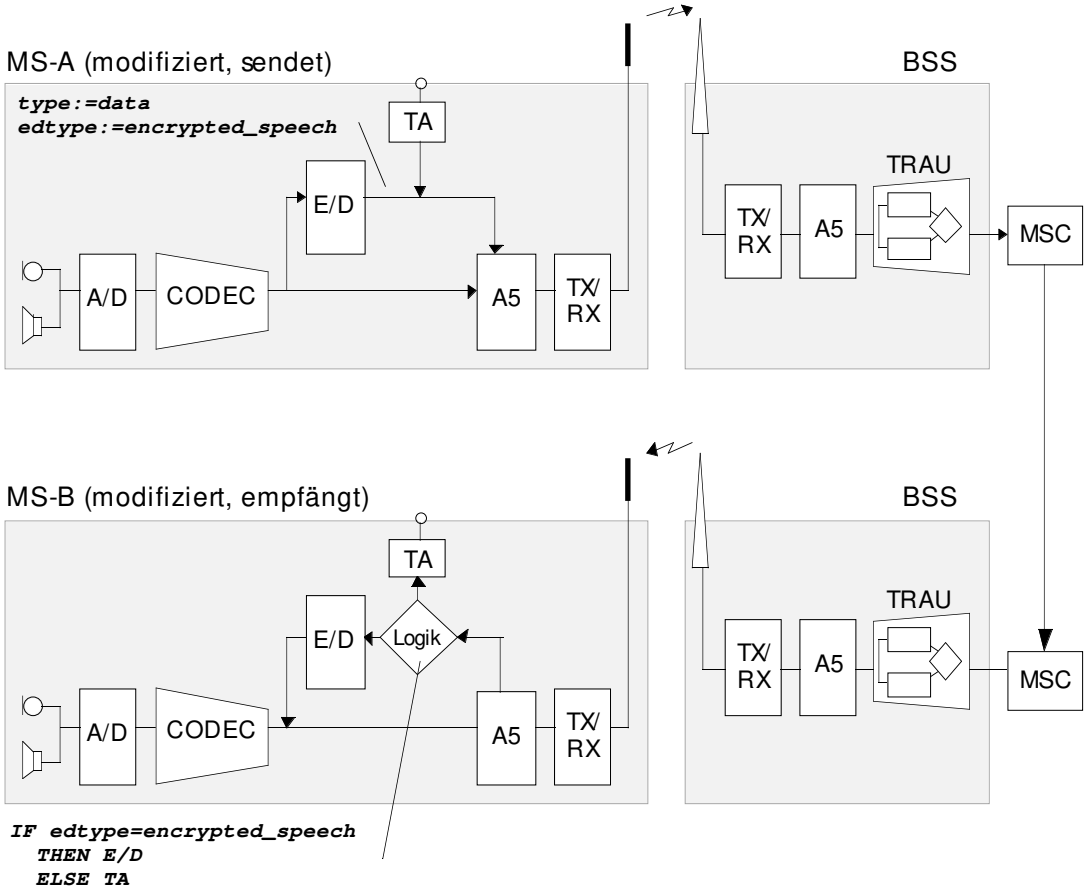


Abb. 7: Sprachübertragung im GSM mit modifizierten Mobilstationen

Mit dieser Lösungsvariante ist theoretisch eine Datenrate von knapp unter 12 kbps zu erreichen. Dies wird möglich, da TA nicht durchlaufen werden muß und die Daten im Netz bittransparent vermittelt werden. Damit bietet diese Alternative zwar die höchste nutzbare Datenrate, ist aber in der Realisierung aufwendiger, da die Mobilstationen der Teilnehmer speziell für dieses Verfahren modifiziert werden müssen. Ein Vorteil ist aber dennoch, daß die bestehende GSM-Netzstruktur und Administration nicht geändert werden muß.

Bei einer Mobilnetz-Festnetz-Kommunikation ist der Aufbau ähnlich, deshalb wird hier auf eine Darstellung verzichtet. Bei dem Gesprächsteilnehmer aus dem Festnetz wird während des Empfangs zuerst die Ratenanpassung rückgängig gemacht. Anschließend kann die Sprache entschlüsselt und im CODEC dekomprimiert werden. Der Teilnehmer im Festnetz benötigt also auch ein modifiziertes Endgerät, das in der Lage ist, die signalisierte verschlüsselte Sprache korrekt zu erkennen und zu bearbeiten. Spricht der Teilnehmer ins Mobilfunknetz, erfolgt der Ablauf in umgekehrter Reihenfolge.

Auch bei dieser Variante ist allerdings noch gesondert zu untersuchen, ob man mit dem Datendienst den Echtzeitforderungen genügen kann.

4. Ausblick

Die in diesem Papier diskutierten Realisierungsvorschläge für ende-zu-ende-vertrauliche Kommunikation lassen sich in zwei Gruppen gliedern. Die Verfahren aus 3.1 und 3.3 nutzen den vorhandenen bittransparenten Datenkanal zur Sprachübertragung. Das in 3.2 vorgestellte Verfahren soll dagegen den nicht bittransparenten Sprachkanal bei möglichst hoher nutzbarer Datenrate bittransparent machen.

Die dabei entstehenden Probleme unterscheiden sich ebenfalls. So sind bei der Nutzung des Datenkanals die Echtzeitbedingungen für die Sprachübertragung die größte Schwierigkeit. Falls es allerdings in der Praxis mit dem Datenkanal gelingt, den Anforderungen für Sprachübertragung zu genügen, so bieten die in 3.1 und 3.3 beschriebenen Verfahren eine gute Alternative zu der unsicheren Kommunikation über den vorhandenen GSM-Sprachkanal. Diese beiden Verfahren unterscheiden sich dann nur im Realisierungsaufwand und der dadurch erreichbaren Datenrate. So kommt man bei dem Verfahren aus 3.1 mit einem Zusatzgerät aus, über das beide Teilnehmer verfügen müssen, wogegen das Verfahren aus 3.3 eine Modifikation der Mobilstationen und eine Erweiterung des GSM-Standards erfordert. Durch diesen Mehraufwand erhöht man die nutzbare Datenrate auf dem bittransparenten Kanal von 9,6 kbps auf ca. 12 kbps.

Das in 3.2 vorgestellte Verfahren läßt sich dagegen nur dann effektiv realisieren, wenn der vorhandene GSM-Sprachkanal den unter 3.2 aufgestellten Voraussetzungen genügt, da sonst die nutzbare Datenrate auf dem entstehenden bittransparenten Sprachkanal beträchtlich sinkt und den praktischen Einsatz dieses Verfahrens unmöglich macht.

Es sei hier noch erwähnt, daß zur Zeit die Nutzung des Datendienstes in allen deutschen GSM-Netzen (D1-, D2- und E-Netz) mit einer zusätzlichen monatlichen Grundgebühr verbunden ist. Die Verbindungskosten unterscheiden sich bei Sprach- und Datenübertragungen nicht.

Für die Zukunft der GSM-Netze wäre es wünschenswert, daß die Netzbetreiber Dienste für vertrauliche Ende-zu-Ende-Kommunikation anbieten, und die Gerätehersteller entsprechende Mobiltelefone auf den Markt bringen. Letztere arbeiten zur Zeit an solchen Lösungen, wie der Artikel [Koll_96] hoffen läßt.

Beim viel diskutierten Mobilfunknetz der 3. Generation — UMTS (Universal Mobile Telecommunication System, siehe auch [Pütz2_97]) sollte man bereits zu Beginn bittransparente Übertragungskanäle für Sprach- und Datenübertragung vorsehen, um sichere Ende-zu-Ende-Kommunikation zu ermöglichen.

5. Literatur

AtKE_95 I. A. Atkinson, A. M. Kondoz, B. G. Evans: Time Envelope Vocoder, a New LP Based Coding Strategy for Use at Bit Rates of 2,4 kb/s and Below; IEEE Journal on selected Areas in Communications; Vol. 13; No. 2; February 1995

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

Bath_92 Beate Bathe-Peters: Lösungsansätze für Datenschutzprobleme beim Mobiltelefon. Dokumentation des ITG-Forums "Gestaltungsfelder beim Mobiltelefon, 12. Mai 1992, Frankfurt am Main, 93-96.

FJKP_95 Hannes Federrath, Anja Jerichow, Dogan Kesdogan, Andreas Pfitzmann: Security in Public Mobile Communication Networks. Proc. of the IFIP TC 6 International Workshop on Personal Wireless Communications, Verlag der Augustinus Buchhandlung Aachen, 1995, 105-116.

GSM_06.10 ETSI: ETSI/TC GSM: 06.10 GSM full rate speech transcoding; Version 3.2.0; July 1989

GSM_06.20 ETSI: ETSI/TC GSM: 06.20 GSM Digital Speech Compression; Version 4.0.0; 1992

GSM_93 GSM Recommendations: GSM 01.02 - 12.21; February 1993; Release 92.

Heut_94 Ulrich Heute: Sprachkodierung: Ansätze, Tendenzen, Standardisierungen. ITG-Fachbericht 130, VDE-Verlag, Berlin, Offenbach,1994, 437-448.

Koll_96 Sabine Koll: Neue Mehrwertdienste, Geräte und Produkte zur Datenübertragung angekündigt — Die deutsche Mobilfunkszene wartet auf die ersten Dual-Mode-Handys; Computer Zeitung; 14.03.1996; Seite 50

Mann_95 Mannesmann Mobilfunk GmbH: D2-Info-Box; Werbezeitschrift für das D2-Netz; Düsseldorf; 8/1995

MüSt_95 Günter Müller, Frank Stoll: Der Freiburger Kommunikationsassistent - Sicherheit in multimedialen Kommunikationsnetzen durch nutzerbezogene Dezentralisation. Dokumentation zum Symposium "Multimedia und Datenschutz" des Berliner Datenschutzbeauftragen, Internationale Funkausstellung Berlin, August 1995, 1-16.

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

Pütz1_97 Stefan Pütz: Zur Sicherheit digitaler Mobilfunksysteme, in diesem Heft.

Pütz2_97 Stefan Pütz: Mobilfunksysteme, Gateway, in diesem Heft.

Stat_95 Statistics: European Cellular Subscribers, Analogue & Digital (PCN, GSM) Mobile Communications International; December 1995/ January 1996

Tele_95 Deutsche Telekom: Werbeanzeige für das D1-Netz; Sächsische Zeitung; 21.12.1995; Seite 22

Walk_94 Bernhard Walke: Technik-Akzeptanz und -Verträglichkeit von mobilen Kommunikationsnetzen. ITG-Fachtagung "Herausforderung Informationstechnik", VDE-Verlag, München, 18.-20.Oktober 1994.