Authentische und zuverlässige Mobilkommunikation für sicherheitsrelevante Anwendungen

Teil II: Systemarchitektur und Einbettung in GSM

Authentic and Reliable Mobile Communication for Safety-Related Applications
Part II: System Architecture and Adaptation to GSM

Von Bernd Friedrichs

Fortsetzung aus Heft 1–2/1995

Übersicht:

Als Beispiel einer sicherheitsrelevanten Anwendung wurde in Teil I eine auf das GSM-Mobilfunksystem gestützte Kommunikation zur Steuerung und Kontrolle von Zügen eingeführt. Zur Gewährleistung der Integrität und Authentizität sind kryptographische und codierungstheoretische Schutzmechanismen erforderlich, die in Abstimmung mit der Übertragungstechnik, dem Kommunikationsnetzwerk und den Anforderungen des Dienstes entwickelt werden müssen.

Der Message Authentication Code als wesentliches Schutzverfahren für ein einzelnes Telegramm wurde in Teil I informationstheoretisch analysiert und dimensioniert. In Teil II werden nun Verfahren zur Sicherheit des gesamten Kommunikationsprozesses einschließlich des Verbindungsmanagements diskutiert. Schwerpunkte sind dabei die Integration aller Verfahren zu einem Gesamtsystem in Form einer geschichteten Architektur, eine geeignete Schlüsselhierarchie und kryptographische Protokolle sowie die Einbettung in das GSM-Mobilfunksystem.

Abstract:

A communication system for train control based on the GSM mobile radio standard was introduced in Part I. Cryptographical and error control mechanisms are required to ensure integrity and authentication and have to be developed in accordance with the transmission standard, communication network and service definition.

The message authentication code as the main security component for a single data block was analyzed and dimensioned by means of information theory in Part I. Methods for the security of the entire communication process including link management are discussed in Part II. Topics are the integration of the system components to achieve a general concept in the form of a layered architecture, an appropriate key management and cryptographical protocols as well as the adaptation to the GSM system.

Für die Dokumentation:

Kryptographie / Authentifikation / Schlüsselhierarchie / Protokolle / Schichtenmodell / Zugbeeinflussung / GSM-Mobilfunk

1. Einführung

In Teil I [1] wurde die Funk-Zugbeeinflussung (FZB) im Projekt Dienste integrierender Bahnmobilfunk (DIBMOF) eingeführt als Beispiel einer auf das GSM-Mobilfunksystem gestützten sicherheitsrelevanten Kommunikation. Verschiedenartige potentielle Bedrohungen wie Manipulationen und Störungen erfordern Schutzmechanismen, die mit Verfahren aus den Bereichen Kryptographie und Kanalcodierung realisiert werden. Ziel ist eine gleichermaßen sichere und zuverlässige Kommunikation.

Kryptographische Verfahren sind notwendig zur *Erkennung* von Manipulationen und Störungen, die ansonsten zum Verlust der Integrität und Authentizität führen würden. Als Kern der kryptographischen Verfahren wurde in Teil I der Message Authentication Code (MAC) behandelt. Bei der Erkennung stochastischer Störungen kann der MAC in gewissem Umfang algebraische Fehlererkennungscodes (EDC, error detection code) ersetzen. *Sicherheit* liegt definitionsgemäß dann vor, wenn die Erkennung von Manipulationen und Störungen nur mit extrem geringer Wahrscheinlichkeit versagt.

Gleichzeitig sollte die Kommunikation auch hohe *Zuverlässigkeit* aufweisen, d. h. frei von Manipulationen und Störungen sein. Stochastische Störungen treten bei einer Mobilfunk-Übertragung in erheblichem Umfang auf. Diese Störungen können größtenteils durch entsprechend dimensionierte Übertragungsverfahren und Funkfeldplanung vermieden werden. Eine zentrale Rolle spielt dabei die *Korrektur* von Störungen durch hochentwickelte algebraische Fehlerkorrekturcodes (ECC, error correction code).

Kryptographische Methoden sind auch erforderlich, um die Vertraulichkeit einer sicherheitsrelevanten Kommunikation zu gewährleisten sowie zur Authentifizierung im Zusammenhang mit dem Verbindungsmanagement. Mit kryptographischen Verfahren wird prinzipiell immer auch ein Schlüsselmanagementsystem erforderlich, das hier aber nur in Teilen behandelt wird.

2. Geschichtete Architektur sicherheitsrelevanter Kommunikation

Das Architekturmodell für eine sichere Kommunikation unter Berücksichtigung aller in Teil I aufgeführten Bedrohungen wird anhand von Bild 1 erklärt, wobei im wesentlichen der Darstellung aus [2] gefolgt wird. Anschließend erfolgt eine detaillierte Begründung dieser Anordnung sowie wichtiger Details.

2.1 Prinzipielles Schichtenmodell

In **Bild 1** zeigt eine Aufgliederung des gesamten Kommunikationssystems in drei Schichten: Applikationsschicht, Sicherungsschicht und Übertragungsschicht. Die Datenblöcke zwischen Applikations- und Sicherungsschicht werden als *ungesicherte Telegramme* bezeichnet und die Datenblöcke zwischen Sicherungs- und Übertragungsschicht entsprechend als *gesicherte Telegramme*.

Für die Übertragungsschicht wird auch der Ausdruck *Bedrohter Kanal* verwendet, da hierin alle auftretenden bzw. denkbaren Bedrohungen zusammengefaßt werden. Außerhalb davon treten keine Bedrohungen auf. Per Definition werden also im Sende- und Empfangszweig sowohl die Applikationsschicht wie die Sicherungsschicht als bedrohungsfrei vorausgesetzt – das bedeutet beispielsweise eine virusfreie Software und fehlerfreie oder zumindest fehlertolerante Rechnersysteme („Sichere Rechner"). Damit werden sehr aufwendige Entwurfs- und Realisierungsverfahren erforderlich, die aber nicht Thema dieses Artikels sind.

Als wichtige Konsequenz daraus sind die Verfahren innerhalb der Sicherungsschicht möglichst schlank zu halten. Alles was nicht unbedingt für die Sicherheit erforderlich ist, wird logisch dem bedrohten Kanal zugeordnet, auch wenn die entsprechenden Verfahren physikalisch am Ort der Sicherungsverfahren realisiert werden. Genauer wird das mit folgenden Prinzipien deutlich:

- Die wichtigste Aufgabe der Sicherungsverfahren besteht in der Erkennung möglichst aller Fehler und Manipulationen – und zwar unabhängig von der übertragungstechnischen Güte des Kanals. Die Sicherungsverfahren müssen also manipulationssicher und störungsfrei realisiert werden.
- Maßnahmen zur Steigerung der Zuverlässigkeit wie beispielsweise durch einen ECC müssen dagegen logisch dem bedrohten Kanal zugeordnet werden, da ein Versagen der Fehlerkorrektur zwar die Zuverlässigkeit mindert, aber nicht die Sicherheit beeinflußt.
- Der bedrohte Kanal inklusive dem GSM-Mobilfunksystem ist als ein möglichst zuverlässiger Kanal zu entwerfen. Methoden dazu sind neben ECC insbesondere auch eine geeignete übertragungstechnische Einbettung in GSM sowie eine geeignete Funkfeldplanung.

  Unabhängig davon muß sich aber die Auslegung der Sicherungsverfahren an einem extrem unzuverlässigen Kanal orientieren.

Die Sicherungsschicht besteht wie in Bild 1 angegeben aus drei Subschichten, die klar voneinander getrennt sind. Von außen nach innen sind dies:

1. Die im Sender erzeugten Telegramme werden mit Protokolldaten ergänzt, die im Empfänger entsprechend überwacht werden. Ziel ist hierbei eine eindeutige Kennzeichnung und Verkettung der Telegramme, um beispielsweise den Replay-Attack [1] abzuwehren (siehe Abschnitt 4.2).
2. Eine Chiffrierung zur Vertraulichkeit kann optional vorgesehen werden, obwohl das für die definierte Sicherheit nicht unbedingt erforderlich ist. Vertraulichkeit und Authentizität sind unabhängige Attribute, die mit unabhängigen Verfahren zu realisieren sind. Zur Kombination von Vertraulichkeit und Authentizität siehe Abschnitt 2.4.
3. Kern der Sicherungsschicht ist die Chiffrierung zur Authentizität und Integrität, die in Form des MAC-Verfahrens realisiert wird. Die Einzelheiten wurden in Teil I dargestellt. Ein sehr wichtiges Problem ist dabei die vertrauliche Verteilung der Schlüssel (siehe Abschnitte 3 und 4.4).

   Auch die Erkennung stochastischer Fehler kann mit dem MAC-Verfahren erfolgen wie in Teil I dargestellt – entweder nur mit einem MAC oder in Kombination mit einem EDC. Die Kombinationsmöglichkeiten werden in Abschnitt 2.4 behandelt.

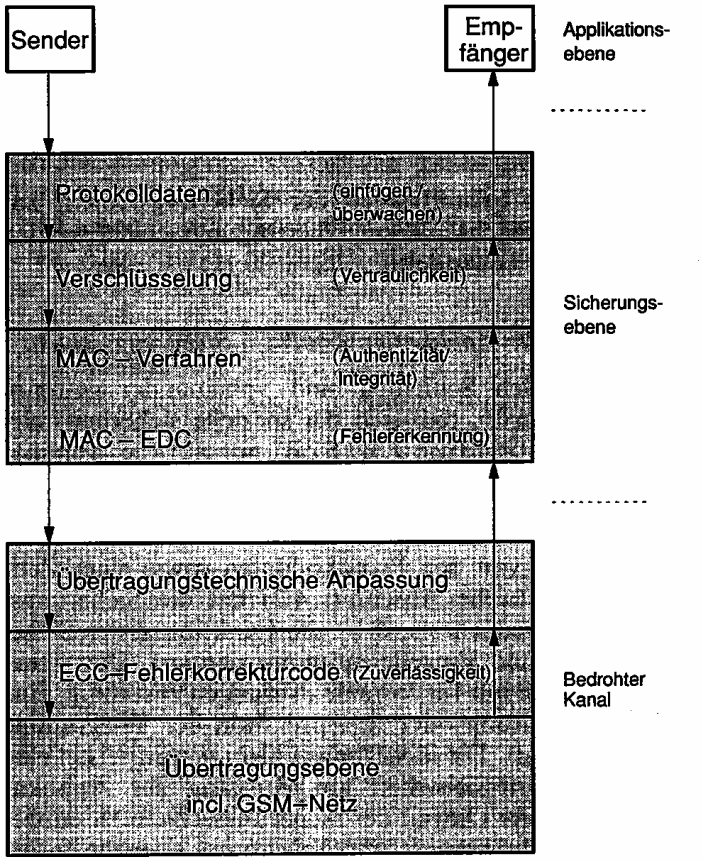

Bild 1: Detaillierte Architektur für sicherheitsrelevante Kommunikation

Auch die Übertragungsschicht bzw. der bedrohte Kanal zerfällt wie in Bild 1 dargestellt in drei Subschichten. Von innen nach außen sind dies:

1. Ganz innen finden sich die in Teil I genannten drei Netze CIRnet, ISDN-Bahn und das GSM-Netz „D3".
2. Der Fehlerkorrekturcode (ECC) ist direkt an die Übertragungseigenschaften des GSM-Systems anzupassen und dient der Erhöhung der Zuverlässigkeit.
3. Die übertragungstechnische Anpassung enthält u.a. die Synchronisation sowie das Schnittstellen- und Ver-

bindungsmanagement. Auch die Umsetzung einer eventuell ereignisgesteuerten Übertragung der gesicherten Telegramme zur konstanten und transparenten Übertragung in CCITT- bzw. ISDN-Norm ist hier zu realisieren.

Die beiden Schnittstellen der Sicherungsschicht zur Applikationsschicht und zur Übertragungsschicht werden nun gesondert behandelt.

2.2 Schnittstelle Applikationsschicht – Sicherungsschicht

Diese beiden Schichten sind voneinander getrennt durch das Prinzip, daß sich die spezielle sicherheitsrelevante Applikation (wie z. B. FZB) nur auf die Applikationsschicht, aber nicht auf die Sicherungsschicht auswirken darf.

Abgesehen von den Protokolldaten sowie einer Zeitüberwachung (siehe Abschnitt 4.2) hat die Sicherungsschicht kein Gedächtnis, d. h. alle Funktionen der Sicherungsschicht sind Einzeltelegramm-orientiert. Die Sicherungsschicht ist nur für formale Prüfungen zuständig; eine inhaltliche Prüfung oder Interpretation der Telegramme findet nicht statt. Die Sicherungsschicht gewährleistet eine Einzeltelegramm-Sicherheit am Ausgang zur Applikationsschicht. Der Output der Sicherungsschicht ist entweder das als richtig eingestufte Telegramm oder die Information, daß das Telegramm als falsch bzw. manipuliert eingestuft wurde.

Allerdings wird ein als richtig eingestuftes Telegramm in der Applikationsschicht nochmals auf Plausibilität geprüft werden, indem eine inhaltliche Interpretation stattfindet. Wenn beispielsweise eine offensichtlich unsinnige Information im Telegramm enthalten ist, dann wird dieses Telegramm auch in der Applikationsschicht noch als falsch eingestuft.

Wenn ein Telegramm als falsch erkannt wird, ist eine Wiederholung erforderlich. Dieser Mechanismus sowie eventuelle weitere übergeordnete Quittierungs- und Überwachungsmechanismen müssen also von der Applikationsschicht in Form eines Kommunikationsprotokolls verwaltet werden. Anhand einiger Beispiele wird deutlich, daß dabei ganz unterschiedliche Arten von Telegrammen zu berücksichtigen sind.

Betriebsfreigebende Telegramme. Dies ist der kritischste Fall, da hier unerkannte Fehler unbedingt zu vermeiden sind. Beispielsweise kann das Telegramm mehrfach gesendet werden mit einem empfangsseitigen Vergleich in der Applikationsschicht. Erst bei Übereinstimmung mehrerer Telegramme erfolgt die Freigabe der Befehle zur Ausführung.

Betriebshemmende Telegramme. Dieser Fall ist von der Sicherheit her unkritisch, da auch bei Zweifel an der Richtigkeit das Telegramm sofort zur Ausführung freigegeben wird.

Kritisch ist hier aber die Zuverlässigkeit, denn bei Störungen oder Manipulationen kommen die betriebshemmenden Telegramme in der empfangsseitigen Applikationsschicht gar nicht an. Deshalb ist für die maximale Ausfallzeit eine Obergrenze zu setzen, bei deren Überschreiten prinzipiell so reagiert werden muß, als wenn zwischenzeitlich ein betriebshemmendes Telegramm übertragen worden wäre.

„Kontinuierliche" Telegramme (z. B. Befehle zur Geschwindigkeit). Dieser Fall ist unkritisch, da die Befehle sich hier inhaltlich nur wenig in kurzen Zeitintervallen ändern, so daß Verluste einzelner Telegramme sich kaum auswirken.

2.3 Schnittstelle Sicherungsschicht – Bedrohter Kanal

Diese beiden Schichten sind voneinander getrennt durch das Prinzip, ob Manipulationen an Software oder Hardware kritisch oder unkritisch sind. Ferner muß eine vollständige Entkopplung der Sicherungsverfahren vom spezifischen Übertragungssystem gewährleistet werden. Ein Wechsel des Übertragungssystems soll keine Rückwirkungen auf die Sicherungsschicht haben.

Mit der übertragungstechnischen Anpassung wird gewährleistet, daß auf das GSM-System nur über eine standardisierte Schnittstelle gemäß CCITT- oder ISDN-Norm zugegriffen wird. Die gesicherten Telegramme werden von der Sicherungsebene als Datenblöcke asynchron oder synchron abgegeben, während das GSM-System nur eine „Bit-pipe" zur Verfügung stellt, d. h. einen konstanten Datenstrom mit konstanter Verzögerung. Empfangsseitig ist dann z. B. eine Rahmenerkennung und eine Rahmensynchronisation erforderlich. Da eine falsche Rahmensynchronisation als systematischer Fehler problemlos erkannt wird, sind die Mechanismen zur Anpassung und Einbettung in das Übertragungssystem nicht sicherheitsrelevant. Die übertragungstechnische Anpassung ist wie erwähnt auch für das Verbindungsmanagement zuständig.

Nach Bild 1 ist der ECC im bedrohten Kanal angeordnet, während der EDC zur Sicherungsschicht gehört. Es gibt zwar, wie in Teil I erwähnt, besonders leistungsfähige algebraische Codes, bei denen Fehlerkorrektur und Fehlererkennung effektiv kombiniert werden können. Diese Verfahren sind hier leider nicht anwendbar. Auch eine gemeinsame Optimierung von ECC und MAC ist unmöglich (dies gilt sogar für EDC und MAC). Eine derartige Optimierung ist auch wegen der unterschiedlichen Ziele der beiden Verfahren unmöglich:

- EDC und MAC müssen robust sein gegenüber den verschiedenen Fehlerszenarien und dürfen keineswegs auf ein spezielles Fehlerszenario ausgelegt werden. Damit wird die Sicherheit gewährleistet.
- Der ECC zur Erhöhung der Zuverlässigkeit wird natürlich auf die physikalisch zu erwartenden Fehlerstrukturen hinter dem GSM-Empfänger ausgelegt, d. h. auf einen Bündelfehlerkanal entzerrt mit der MLSE-Methode (Maximum Likelihood Sequence Estimation), versehen mit Faltungscodierung und Interleaving.

Der ECC wird direkt an den GSM-Funkkanal angepaßt, weil dort die meisten und gravierendsten Fehler entstehen. Eine Anpassung an den gesamten bedrohten Kanal wäre nur dann sinnvoll, wenn außerhalb des Funkkanals in den leitungsgebundenen Netzen ebenfalls Fehler in beträchtlicher Anzahl und von korrigierbarer Art entstehen würden.

2.4 Wichtige Details der Sicherungsschicht

1) *Anordnung der Verschlüsselung in der Sicherungsschicht.* Dazu gibt es die beiden in **Bild 2** dargestellten Möglichkeiten. Mit *X* werden die Klartext-Telegramme

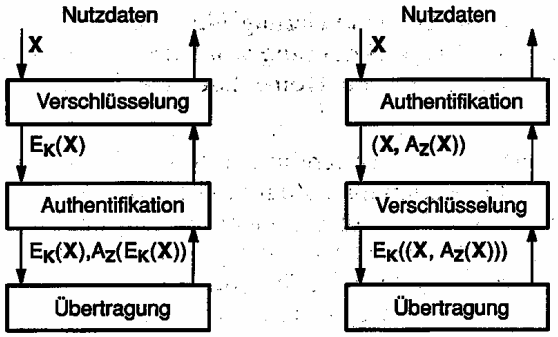

Bild 2: Alternativen zur Kombination der Chiffrierung zur Vertraulichkeit (Schlüssel K) und zur Authentizität (Schlüssel Z)

inklusive der Protokolldaten bezeichnet. Die Blockchiffrierung zur Vertraulichkeit wird über den Schlüssel K gesteuert und E_K bezeichnet den Verschlüssler. Die Authentifikationsprozedur wird mit dem Schlüssel Z gesteuert, und A_Z bezeichnet die Bildung des MAC.

Im linken Teil wird erst E_K-chiffriert und dann wird dazu der MAC gebildet, d.h. es wird der Chiffretext mit dem MAC zum Chiffretext übertragen. Im rechten Teil wird erst der MAC gebildet und dann werden Klartxt und MAC gemeinsam E_K-chiffriert.

Zum Vergleich der beiden Anordnungen. Wenn die Blockchiffrierung dem Diffusions-Prinzip [1] genügt, dann werden aus wenigen Übertragungsfehlern bei der rechten Anordnung nach der Blockdechiffrierung sehr viele Fehler, die mit hoher Wahrscheinlichkeit erkannt werden. Aber eine Kombination MAC-EDC zur garantierten Erkennung aller Fehler bestimmten Gewichts funktioniert bei der rechten Anordnung nicht, wohl aber bei der linken Anordnung, die aus diesem Grund in Bild 1 enthalten ist.

Die rechte Anordnung hat allerdings den Vorteil, daß nach der Blockdechiffrierung alle Fehlermuster die gleiche Wahrscheinlichkeit haben. Als Folge davon ist P_{ue} besonders einfach berechenbar [1].

Die beiden vorangehenden Argumente kehren sich allerdings in ihr Gegenteil um, wenn zur Vertraulichkeit eine Stromchiffrierung [5] verwendet wird. Da ein derartiges Verfahren fehlertransparent ist, ändert sich dadurch die Fehlermuster-Verteilung nicht.

2) *Kombination von MAC und EDC.* Die verschiedenen Alternativen werden in [2] verglichen mit dem Fazit, daß nur marginale Unterschiede bestehen. Vorzugsweise sollten der MAC und der EDC getrennt aus den Nutzdaten berechnet werden.

3) *Dimensionierung der erforderlichen MAC-Länge.* Jeder Zug empfängt bzw. sendet ca. 1 Telegramm pro Sekunde. Die Anzahl der Züge in Europa beträgt ca. 10000. Innerhalb von 1000 Jahren werden dann insgesamt

$$10000 \cdot 1000 \cdot 3600 \cdot 24 \cdot 365 \approx 2^{48} \qquad (1)$$

Telegramme empfangen. Wenn hierbei höchstens 1 unerkannter Fehler erlaubt wird, ist eine Sicherheit von $P_{ue} \approx 2^{-48}$ erforderlich. Nach Teil I kann das mit einer MAC-Länge von $L_{mac} = 64$ erreicht werden. Auch der Impersonation Attack bei einer MAC-Schlüssellänge von $L_z = 56$ ergibt eine entsprechend kleine Wahrscheinlichkeit P_I für den Impersonation Attack. Aufgrund der in Teil I genannten Gründe ist aber dennoch $L_z \geq 112$ vorzuziehen.

3. Schlüsselmanagement

Mit der Verwendung kryptographischer Verfahren werden unmittelbar Verfahren zur Organisation der Schlüssel erforderlich. Die wesentlichen Aufgaben des sogenannten Schlüsselmanagements sind die Erzeugung, Verteilung, Aufbewahrung und Vernichtung von Schlüsseln. Wie in Teil I schon erwähnt kann die Qualität aller kryptographischen Algorithmen prinzipiell nur so gut wie die Qualität der Schlüsselvereinbarung sein.

Prägend für das Schlüsselmanagement sind sowohl das Kommunikationsnetz wie die kryptographischen Bedrohungsszenarien wie auch die Anforderungen der Applikation. Dieser „interdisziplinäre" Komplex kann zum kompliziertesten Thema des Gesamtsystems werden, da hier gleichermaßen die bahnspezifische Sicherheitstechnik, die Übertragungstechnik und die Netzarchitektur betroffen sind.

3.1 Schlüsselhierarchie KK–KS

Für jede zulässige Kommunikationsbeziehung wird ein individueller Schlüssel vorgesehen, der als KK (Authentifikationsschlüssel, Schlüsselverteilschlüssel, Key Encryption Key) bezeichnet wird. Es werden nur symmetrische Verfahren angewendet, bei denen auf beiden Seiten der gleiche geheime Schlüssel verwendet wird. Der KK für die Kommunikation zwischen A und B wird als KK_{AB} bezeichnet. Diese KK sind unbedingt geheimzuhalten, weil damit die gegenseitige Authentifizierung erfolgt.

Aus dem KK wird ein weiterer symmetrischer Schlüssel KS (Sitzungsschlüssel, Kommunikationsschlüssel, Session Key) abgeleitet, der dem in Teil I für die MAC-Bildung benutzten Schlüssel entspricht: $Z = KS_{AB}$. Der KS ist nicht nur von KK abhängig, sondern auch von Zufallszahlen, damit ohne KK-Wechsel immer wieder neue KS erzeugt werden können. Im Detail wird die Ableitung von KS aus KK in den Abschnitten 4.4 und 4.5 beschrieben.

Die Lebensdauer der Authentifikationsschlüssel KK ist lang (Jahre) und die der Sitzungsschlüssel KS ist kurz (Sekunden bis Stunden). Der KS wird häufig gewechselt, um Manipulationen und Kryptoanalysen zu erschweren. Auch der KK darf nur so angewendet werden, daß sie keine wesentlichen Ansatzpunkte zur Kryptoanalyse ergeben.

KK und KS bilden also eine zweistufige Schlüsselhierarchie. Alle Operationen basieren auf dem DES-Algorithmus, weshalb die Länge aller Schlüssel als Vielfaches von 56 bzw. 64 vorgesehen wird. Die Aufbewahrung von KK und KS und die Berechnung von KS findet in der Sicherungsschicht statt.

3.2 Verwaltung der Authentifikationsschlüssel KK

Für den Bereich der Deutschen Bahn gilt momentan (in Klammern eine Schätzung für die zukünftigen Werte in Europa):

Anzahl Streckenzentralen : $N_Z = 12$ (200)
Anzahl LZB-Triebfahrzeuge : $N_F = 300$ (6000).

Theoretisch können also $(N_Z + N_F) \cdot (N_Z + N_F - 1)/2$ Kommunikationsbeziehungen bestehen. Allerdings ist nach Teil I für die FZB weder eine Kommunikation

zwischen den Zügen noch zwischen den Streckenzentralen vorgesehen, so daß nur $N_Z \cdot N_F$ Kommunikationsbeziehungen zwischen Zentrale und Fahrzeug bestehen.

Die KK werden nur für diese Kommunikationsbeziehungen vergeben. Jedes Fahrzeug muß also nur N_Z KK-Schlüssel abspeichern und jede Streckenzentrale nur N_F KK-Schlüssel. Damit sind Vor- und Nachteile verbunden:

- Nachteilig ist, daß bei der Einrichtung einer neuen Streckenzentrale die KK-Listen in allen Triebfahrzeugen und bei der FZB-Aufrüstung eines Triebfahrzeuges die KK-Listen in allen Streckenzentralen aktualisiert werden müssen.
- Vorteilhaft ist freilich, daß das Bekanntwerden einer KK-Liste nur begrenzte Auswirkungen hat. Wird aus dem Triebfahrzeug die Liste entwendet, so wird damit nur dieses Fahrzeug lahmgelegt. Wird aus einer Streckenzentrale die Liste entwendet, so ist nur im Bereich dieser Zentrale kein FZB-Betrieb mehr möglich.

Dennoch sollte natürlich möglichst sichergestellt werden, daß die KK nicht unentdeckt aus der Streckenzentrale oder dem Fahrzeug entwendet werden können. Falls eine Entwendung nicht prinzipiell verhindert werden kann, so muß die Entwendung zumindest unbedingt entdeckt werden. Ansonsten könnte der Angreifer eine falsche Identität beweisen (Maskerade). Insbesondere muß also die Verteilung der KK vertraulich und authentisch erfolgen, d.h. keinesfalls ungeschützt über das normale Kommunikationsnetz. Alternativen zur KK-Verteilung sind entweder die manuelle Verteilung mit speziellen Chips oder mit sogenannten Schlüsseltransportgeräten (tamper proofed boxes) [9] oder eine kryptographisch gesicherte Verteilung mit übergeordneten Systemschlüsseln [4], wobei sowohl symmetrische Secret-Key- wie asymmetrische Public-Key-Verfahren angewendet werden können.

Da die KK determiniert vergeben werden, kann die Vergabe gleicher KK für verschiedene Kommunikationsbeziehungen ausgeschlossen werden. Ferner können die schwachen und semi-schwachen Schlüssel vermieden werden.

3.3 Kryptographische Identität

Prinzipiell ist die Vergabe von Schlüsseln natürlich an Identitäten gebunden. Der KK ist theoretisch der Identität *Fahrzeug* bzw. *eindeutige Loknummer* zugeordnet. Tatsächlich ist der KK aber in einem *Fahrzeugrechner* abgespeichert, der im Falle eines Defektes natürlich austauschbar sein muß, ohne daß sich dadurch der KK ändert. Damit ist eine weitere Schlüsselebene erforderlich, in der der KK aus einem komponentenspezifischen Schlüssel abgeleitet wird. Natürlich muß die Vergabe dieser Schlüssel beim Hersteller der Komponenten auch wieder vertraulich und authentisch erfolgen.

Damit und auch durch andere hier uninteressante betriebliche Anforderungen ergibt sich eine erhebliche Ausweitung der Schlüsselhierarchie. Ferner sind weitere Schlüssel für die Erzeugung von Zufallszahlen notwendig, die bei der Ableitung von KS aus KK benötigt werden (siehe Abschnitt 4.4).

Im GSM-System ist die kryptographische Identität an die SIM-Karte (Subscriber Identity Module) bzw. an die IMSI (International Mobile Subscriber Identity) gebunden, während die Adressierung über die ISDN-Rufnummer erfolgt. Die Verknüpfung von IMSI und Rufnummer erfolgt bekanntlich im Home Location Register (HLR) [10].

Innerhalb der Anwendung erfolgt die Adressierung über die fahrplanmäßige Zugnummer, da Zug und Triebfahrzeug einander natürlich nicht fest zugeordnet sind. In einer Datenbank erfolgt dann die Umsetzung auf die Rufnummer des Mobilgerätes des Fahrzeugs, wobei die verschiedenen Konzepte dafür aber nicht Thema dieses Artikels sind.

4. Sicherheit des Kommunikationsprozesses

Der Kommunikationsprozeß umfaßt eine ganze Reihe von Operationen, die für eine sichere Kommunikation zwischen den Teilnehmern Zentrale und Fahrzeug durchgeführt werden müssen. Das betrifft sowohl das Verbindungsmanagement und die Authentifikation beim Verbindungsaufbau, den Verbindungsabbau und natürlich die Kommunikation selbst [8].

4.1 Übertragungsmodus

Da der Verbindungsaufbau von beiden Partnern initiiert werden kann, sind Zentrale und Fahrzeug gleichberechtigte Partner in symmetrischer Beziehung (siehe auch Bild 2 aus Teil I), die deshalb nachfolgend auch nur als A, B bezeichnet werden. Der Übertragungsmodus ist also richtungsunabhängig, und für die Authentifikationsschlüssel gilt $KK_{AB} = KK_{BA}$.

Prinzipiell ist zwischen zwei Betriebsarten der FZB zu unterscheiden.

Zyklischer Betrieb; es werden ständig Telegramme in gleichmäßigem Abstand gesendet (synchron).

Ereignisgesteuerter Betrieb; es werden Telegramme in ungleichmäßigem Abstand gesendet (asynchron).

Bei einem MAC-gesicherten Telegramm ist die Integrität und Authentizität gewährleistet, und Impersonation wie Substitution Attack sind theoretisch bzw. praktisch unmöglich [1], d.h. der Angreifer kann nicht selbst gültige Telegramme erzeugen. Dennoch hat ein Angreifer wesentliche Möglichkeiten zum Stören bzw. Manipulieren, die mit dem MAC-Verfahren allein nicht erkannt werden, sofern nicht zwischenzeitlich der Sitzungsschlüssel gewechselt wird:

- Replay-Attack, d.h. Wiedereinspielen von abgehörten und aufgezeichneten Telegrammen.
- Verzögerung, Vertauschung und Unterdrückung von Telegrammen.

Beim ereignisgesteuerten Betrieb sind noch besondere Vorkehrungen zu treffen, um die Unterdrückung von Telegrammen sofort zu bemerken und nicht erst dann, wenn „mal wieder" ein Telegramm beim Empfänger ankommen sollte. Klar ist natürlich, daß hierfür eine Duplex-Übertragung mit Quittierungsmechanismen erforderlich ist. Bei einer Simplex-Übertragung kann die Unterdrückung von Telegrammen prinzipiell nicht sofort bemerkt werden.

Zur Abwehr dieser Angriffe sind zusätzliche Maßnahmen erforderlich. Entweder wird permanent der Sitzungsschlüssel gewechselt (siehe Abschnitt 4.5), oder der Sender

muß die Nutzdaten des Telegramms um zusätzliche Redundanz bzw. Zusatzdaten erweitern, mit denen folgende Attribute zu gewährleisten sind:

Eindeutigkeit der Telegramme. Alle während der Lebensdauer eines Sitzungsschlüssels erzeugten Telegramme müssen sich voneinander unterscheiden.

Verkettung der Telegramme. Im Empfänger muß feststellbar sein, ob ein Telegramm neu ist und ob bei einer Folge von Telegrammen die Reihenfolge erhalten blieb.

4.2 Protokolldaten zur eindeutigen Kennzeichnung und Verkettung

Zur Gewährleistung von Eindeutigkeit und Verkettung der Telegramme sind folgende Methoden zu vergleichen:

Zufallszahlen. Das Telegramm wird sendeseitig mit einer Zufallszahl versehen. Die Wiederholung von Telegrammen wird erkannt, sofern der Empfänger alle bisher empfangenen Zufallszahlen abspeichert und die neu empfangene Zufallszahl mit dieser Liste vergleicht. Voraussetzung ist ferner, daß der Sender stets verschiedene Zufallszahlen wählt.

Fazit: Diese Methode ist aufwendig und ungeeignet. Beim ereignisgesteuerten Betrieb wird die Unterdrükkung von Telegrammen nie bemerkt.

Zeitstempel mit absoluter Zeit. Das Telegramm wird sendeseitig mit der Uhrzeit und dem Datum versehen. Empfangsseitig wird das Telegramm nur akzeptiert, wenn die eingestempelte Zeit von der tatsächlichen Zeit nur geringfügig abweicht. Von dieser zulässigen Abweichung hängt die erforderliche Genauigkeit (Granularität) der Zeitdarstellung ab.

Fazit: Beim zyklischen Betrieb ist diese Methode zur Abwehr aller Angriffe geeignet. Beim ereignisgesteuerten Betrieb wird die Unterdrückung von Telegrammen dagegen nie bemerkt. Nachteilig ist die Notwendigkeit synchronisierter Uhren.

Zeitstempel mit relativer Zeit. Hierbei wird die Zeit mit der Vereinbarung des Sitzungsschlüssels von Null gestartet. Es sind keine synchronisierten Uhren erforderlich, sondern lediglich eine gewisse Ganggenauigkeit während der Lebensdauer des Sitzungsschlüssels.

Fazit: Wie beim Zeitstempel mit absoluter Zeit.

Sequenznummer. Die Telegramme werden der Reihe nach durchnumeriert, wobei der Zähler mit der Vereinbarung des Sitzungsschlüssels von Null gestartet wird.

- Beim zyklischen Betrieb ist die entsprechende gleichmäßige Inkrementalisierung der Sequenznummer zu bekannten Zeiten leicht kontrollierbar. Somit ist diese Methode zur Abwehr aller Angriffe geeignet.
- Beim ereignisgesteuerten Betrieb werden die Sequenznummern zu Transaktionsnummern. Die Unterdrückung von Telegrammen wird erst dann bemerkt, wenn „mal wieder" ein Telegramm ankommt. Eine Verzögerung von Telegrammen bis zu diesem Zeitpunkt wird überhaupt nicht bemerkt.

Fazit: Beim zyklischen Betrieb der FZB sind die Sequenznummern eine geeignete und vergleichsweise wenig aufwendige Methode zur Abwehr aller Angriffe.

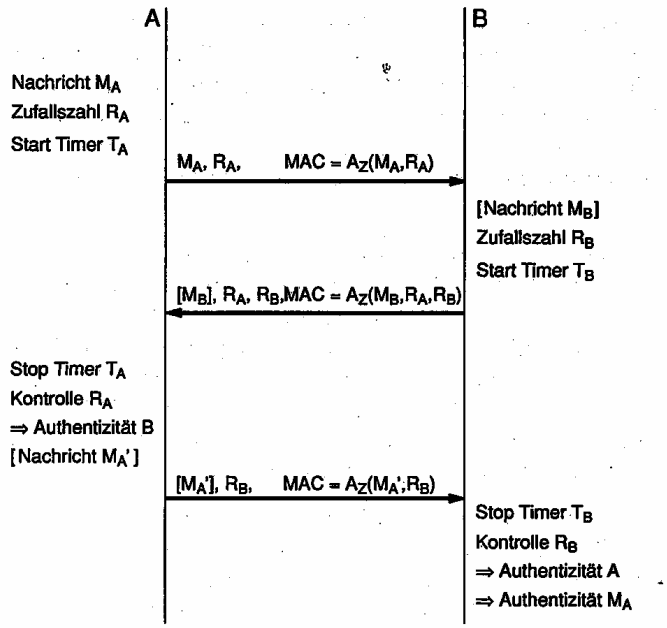

Bild 3: Protokoll zur Authentizität beim ereignisgesteuerten Betrieb

Beim ereignisgesteuerten Betrieb versagen die oben diskutierten Methoden. Das ist freilich selbstverständlich, da ein Verlust durch den Zeitstempel und eine Verzögerung durch die Sequenznummer nicht bemerkt wird. Wenn sowohl Zeitstempel wie Sequenznummer verwendet werden, wird der Verlust eines Telegramms dennoch nicht sofort bemerkt. Somit ist prinzipiell eine Form von Quittierung erforderlich und damit eine Duplex-Verbindung. Ein mögliches Verfahren basierend auf Zufallszahlen zeigt **Bild 3** [4, 7]:

Von A nach B soll die Nachricht $\boldsymbol{M}_A$ übermittelt werden. Zunächst wählt A eine Zufallszahl $\boldsymbol{R}_A$ und überträgt $\boldsymbol{M}_A$ und $\boldsymbol{R}_A$ mit dem entsprechenden MAC versehen nach B. Nun wählt B eine Zufallszahl $\boldsymbol{R}_B$ und überträgt $\boldsymbol{R}_A$ und $\boldsymbol{R}_B$ (und eventuell eine Nachricht $\boldsymbol{M}_B$) mit dem entsprechenden MAC versehen an A. Jetzt kontrolliert A, ob die empfangene Zahl $\boldsymbol{R}_A$ mit der gesendeten Zahl $\boldsymbol{R}_A$ übereinstimmt. Falls das der Fall ist, sendet A die Zahl $\boldsymbol{R}_B$ (und eventuell eine Nachricht $\boldsymbol{M}_A'$) mit dem entsprechenden MAC versehen an B. Jetzt kontrolliert B, ob die empfangene Zahl $\boldsymbol{R}_B$ mit der gesendeten Zahl $\boldsymbol{R}_B$ übereinstimmt. Falls das der Fall ist, wird die Nachricht $\boldsymbol{M}_A$ als authentisch angesehen und zur Ausführung freigegeben.

Überwacht wird dieser Dialog mit Timern T_A und T_B, so daß Verluste von Telegrammen sofort bemerkt werden. Aufgrund der MAC-Sicherung ist keine Fälschung möglich, sondern der Angreifer kann lediglich alte aufgezeichnete Telegramme wiederholen.

Wenn das erste Telegramm eine Wiederholung ist, bemerkt B das zwar nicht sofort, aber bei der Kontrolle stellt A einen Fehler in $\boldsymbol{R}_A$ fest – vorausgesetzt natürlich, daß A nicht mehrfach die gleichen Zufallszahlen verwendet. Wenn das zweite Telegramm eine Wiederholung ist, wird auch das erkannt, da $\boldsymbol{R}_A$ und $\boldsymbol{R}_B$ (sofort bzw. mit dem dritten Telegramm) kontrolliert werden. Wenn beispielsweise das erste und zweite Telegramm zusammenpassende Wiederholungen aus einem alten Protokoll sind, wird zwar A getäuscht, aber nicht B.

Anstelle der Zufallszahlen können auch Sequenznummern verwendet werden, da es nicht primär auf die Zufälligkeit ankommt, sondern nur darauf, daß keine alten Werte wiederholt werden.

Nach Ablauf dieses Protokolls ist garantiert, daß auf dem Übertragungsweg von A nach B keine gefälschten oder alten Nachrichten untergeschoben werden können, daß die Nachricht aktuell ist und daß ein Verlust der Nachricht sofort bemerkt wird. Selbst wenn alle drei Telegramme unterdrückt werden, wird dies zumindest von A bemerkt.

Allerdings weiß A nach Ablauf dieses Protokolls nicht, ob die Nachricht M_A bei B angekommen ist. Falls nämlich das dritte Telegramm unterdrückt wird oder bei Einspielung eines alten Telegramms die Kontrolle von R_B in B einen Fehler anzeigt, so wird B die Nachricht M_A nicht als authentisch ansehen und nicht ausführen. Dafür wäre dann ein viertes Telegramm von B nach A (und eventuell sogar ein fünftes Telegramm von A nach B) erforderlich.

Die Sicherheit dieses Protokolls zum ereignisgesteuerten Betrieb basiert natürlich darauf, daß nur die beiden Kommunikationspartner A und B den Sitzungsschlüssel kennen, d.h. $Z = KS_{AB}$ ist spezifisch für (A, B). Zwar könnte in den Protokolldaten auch die Sender- und Empfänger-Adresse enthalten sein, um beispielsweise falsche Verbindungen direkt zu erkennen. Allerdings wären diese Daten kryptographisch ohne Relevanz, da die Adressen einem potentiellen Angreifer bekannt sind; durch das Verheimlichen irgendwie codierter Adressen ergibt sich kein beweisbarer Sicherheitsgewinn.

4.3 Kanalüberwachung

Bei betriebshemmenden Telegrammen ergibt sich eine sicherheitskritische Situation dann, wenn ein solches Telegramm übertragen werden soll, aber die Verbindung unbemerkt unterbrochen ist. Natürlich kann eine derartige unbemerkte Unterbrechung nur beim ereignisgesteuerten Betrieb auftreten.

Somit ist eine Überwachung des Kanals bzw. der Übertragungsschicht erforderlich, um Ausfälle zu bemerken. Da dies eine sicherheitsrelevante Prozedur ist, sind die entsprechenden Verfahren in der Sicherungs- oder in der Applikationsschicht anzuordnen. Keinesfalls genügt die GSM-interne Messung der Kanalqualität.

Das Überwachungsverfahren kann wie folgt realisiert werden. In einem gewissen Abstand, der höchstens der maximal zulässigen Ausfallzeit entspricht, werden Leertelegramme übertragen, sofern keine tatsächlichen Nutztelegramme anliegen. Nutztelegramme werden also nicht durch Leertelegramme verdrängt. Die gesicherten Leertelegramme werden von der Sicherungs- oder Applikationsebene organisiert. Wenn der derart überwachte Kanal innerhalb der maximal zulässigen Ausfallzeit zu keinem gültigen Telegramm beim Empfänger führt, so reagiert der Empfänger in gleicher Weise, als wenn er einen Nothalt bzw. ein betriebshemmendes Telegramm bekommen hätte.

Zur Verhinderung des Replay-Attacks müssen die Leertelegramme entweder per Sequenznummer untereinander bzw. mit den Nutztelegrammen verkettet werden oder entsprechend Bild 3 quittiert werden.

Mit diesem Verfahren wird immer eine Reaktion zur sicheren Seite garantiert. Jedoch liegt auch hier eine Verkopplung mit der Zuverlässigkeit vor, denn bei schlechter Übertragungsqualität würde die Kanalüberwachung sehr oft ansprechen, was natürlich den Eisenbahnbetrieb stark beeinträchtigen würde.

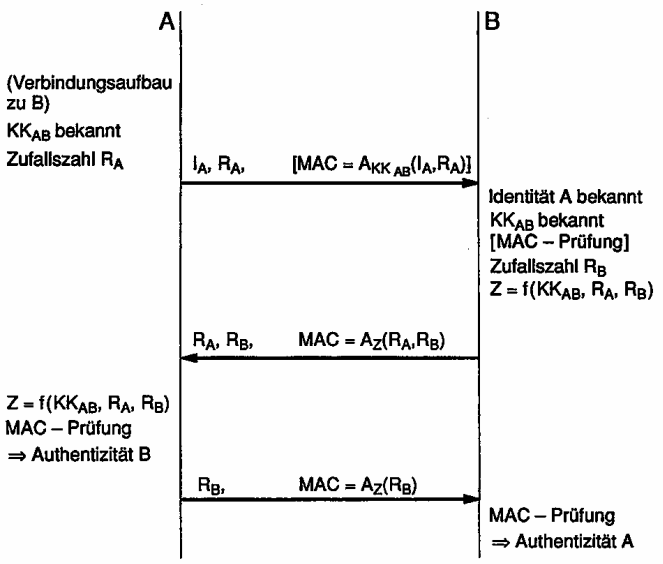

Bild 4: Protokoll zur Authentifikation und KS-Vereinbarung

4.4 Authentifikation und Vereinbarung des Sitzungsschlüssels KS

Der Sitzungsschlüssel KS wird jeweils nur kurzzeitig (Sekunden bis Stunden) verwendet, um die Kryptoanalyse zu erschweren. Beispielsweise kann bei jeder Einfahrt in den Bereich einer neuen Streckenzentrale ein neuer KS vergeben werden. Auch während der aktiven Kommunikation im Bereich einer Streckenzentrale kann der KS nach einer gewissen Zeit gewechselt werden, im Extremfall sogar bei jedem Telegramm. Für beide Fälle werden identische Prozeduren verwendet.

Während der Lebensdauer eines KS müssen die Telegramme beim zyklischen Betrieb eindeutig durch die Sequenznummer gekennzeichnet sein. Die Aufbewahrung der KS ist wegen ihrer kurzen Lebensdauer viel weniger kritisch als bei den KK.

Zur Vereinbarung bzw. Etablierung des KS dienen Schlüsselaustauschprotokolle. Dabei wird der KS allein durch A und B, also allein durch Fahrzeug und Zentrale bestimmt und somit ohne zentrale Instanzen. Dabei kann nicht determiniert verhindert werden, daß beispielsweise zwei Fahrzeuge (sogar innerhalb des Bereiches einer Streckenzentrale) den gleichen KS verwenden – allerdings kommt das nur mit geringer Wahrscheinlichkeit bei ausreichend großen Schlüssellängen vor.

Bild 4 zeigt ein Protokoll zur Vereinbarung des KS in Kombination mit einem Dialog zur Identifikation und Authentifikation (I&A-Dialog).

Von A geht die Initiative zur Kommunikation mit B aus. Damit kennt A natürlich KK_{AB}. A wählt eine Zufallszahl R_A und sendet diese zusammen mit der A-Identität I_A an B, wobei die MAC-Sicherung mit KK_{AB} erfolgt. Mit I_A ist dann auch in B der KK_{AB} bekannt, so daß B den MAC überprüfen kann. B wählt eine Zufallszahl R_B und sendet diese an A. Die MAC-Sicherung erfolgt dabei mit dem Sitzungsschlüssel Z, der aus KK_{AB} und den beiden Zufallszahlen berechnet wird. Nach Empfang von R_B in diesem Telegramm kann auch A den Sitzungsschlüssel Z berechnen und kann damit die Authentizität von B feststellen. Damit auch B die Authentizität von A feststellen kann, wird im dritten Telegramm R_B mit MAC-Sicherung von A nach B übertragen.

Die Authentizität wird also dadurch verifiziert, daß nur der berechtigte Partner im Besitz des Authentifikationsschlüssels KK sein kann. Das Protokoll aus Bild 4 ist wie das Protokoll aus Bild 3 sicher gegen Manipulationen und Replay-Attacks. Die MAC-Sicherung im ersten Telegramm aus Bild 4 kann auch entfallen. Das gilt allerdings nicht bei Bild 3, da sonst dort $\boldsymbol{M}_A$ per Substitution Attack manipuliert werden könnte.

Die Berechnung von KS erfolgt über eine Funktion f aus KK und den beiden von den Kommunikationspartnern gewählten Zufallszahlen:

$$\boldsymbol{Z} = \boldsymbol{KS}_{AB} = f(\boldsymbol{KK}_{AB}, \boldsymbol{R}_A, \boldsymbol{R}_B). \tag{2}$$

Dabei muß für f das Diffusions- und Konfusions-Prinzip [1] gelten, beispielsweise muß die Änderung eines Bits in KK oder in den Zufallszahlen zu einer Änderung von rund 50% der Bits in KS führen. Eine Wahlmöglichkeit für die Funktion f auf DES-Basis ist beispielsweise

$$\boldsymbol{Z} = DES_{\boldsymbol{KK}_{AB}}(\boldsymbol{R}_A) + DES_{\boldsymbol{KK}_{AB}}(\boldsymbol{R}_B) \tag{3}$$

siehe [3].

Dabei hat KS zunächst 64 Bits, womit eine Kürzung auf 56 Bits erforderlich wird. Ein doppelt so langer KS ergibt sich beispielsweise durch

$$\boldsymbol{Z} = (DES_{\boldsymbol{KK}_{AB}}(\boldsymbol{R}_A), DES_{\boldsymbol{KK}_{AB}}(\boldsymbol{R}_B)). \tag{4}$$

Längere KK auf DES-Basis können beispielsweise entsprechend dem Triple-DES-Prinzip [5] verarbeitet werden.

Natürlich darf ein Partner von seinem Gegenüber nicht die gleiche Zufallszahl akzeptieren, da sonst ein potentieller Angreifer $\boldsymbol{Z} = \boldsymbol{0}$ gemäß (3) erreichen kann. Ganz unkritisch ist auch die Wahl der Funktion f nicht. Zwar erfüllt auch

$$\boldsymbol{Z} = DES_{\boldsymbol{KK}_{AB}}(\boldsymbol{R}_A + \boldsymbol{R}_B) \tag{5}$$

das Diffusions- und Konfusions-Prinzip, aber dennoch ist hier ein spezieller Angriff möglich. Falls sich ein Angreifer für B ausgibt, und zwar nicht $\boldsymbol{KK}_{AB}$ kennt, wohl aber $DES_{\boldsymbol{KK}_{AB}}(\boldsymbol{R}_0)$ für ein spezielles $\boldsymbol{R}_0$, so gelingt mit $\boldsymbol{R}_B = \boldsymbol{R}_0 - \boldsymbol{R}_A$ ein erfolgreicher Substitution Attack.

Durch simple Modifikationen der Funktion f kann auch eine Richtungsabhängigkeit erreicht werden: $\boldsymbol{KS}_{AB} \neq \boldsymbol{KS}_{BA}$.

In Teil I wurde die Bestimmung von KS aus der Beobachtung der MAC-gesicherten Telegramme analysiert mit dem Fazit $L_{mac} = 64$, $L_z = L_{ks} = 112$. Das Protokoll aus Bild 4 vermittelt nun dem Abhörer Informationen über den Authentifikationsschlüssel KK, und somit ergibt sich das Problem, wie die Länge L_{kk} von KK vernünftig gewählt werden soll. Nach Formel (30) aus Teil I gilt (zur Erinnerung: L_{mac} ist die Länge von $A_{\boldsymbol{Z}}(.)$)

$$H(\boldsymbol{Z}|A_{\boldsymbol{Z}}(\boldsymbol{X}), \boldsymbol{X}) = H(\boldsymbol{Z}|\boldsymbol{Y}) = \max\{L_{ks} - L_{mac}, 0\}. \tag{6}$$

In direkter Analogie gilt für die Entropie von KK bei abgehörtem Protokoll aus Bild 4

$$H(\boldsymbol{KK}_{AB}|\boldsymbol{Z}, \boldsymbol{R}_A, \boldsymbol{R}_B) = H(\boldsymbol{KK}_{AB}|f(\boldsymbol{KK}_{AB}, \boldsymbol{R}_A, \boldsymbol{R}_B), \boldsymbol{R}_A, \boldsymbol{R}_B) = \max\{L_{kk} - L_{ks}, 0\}. \tag{7}$$

Bei $L_{kk} \leq L_{ks}$ ist also der KK durch Abhören des I&A-Protokolls theoretisch eindeutig bestimmt. Allerdings ist der KK auch bei $L_{kk} \gg L_{ks}$ theoretisch eindeutig bestimmt, wenn mehrere Protokolle abgehört werden können. Somit ist die notwendige Länge von KK eine Ermessensfrage. Einerseits sollte KK besonders gut geschützt bzw. schwierig zu ermitteln sein. Andererseits ist der praktische Aufwand zur Ermittlung von KK proportional zu $2^{L_{kk}}$ und nicht zu $2^{\max\{L_{kk} - L_{ks}, 0\}}$.

Die Kryptoanalyse ist übrigens theoretisch unabhängig davon, ob die Zufallszahlen im Klartext oder verschlüsselt übertragen werden. Lediglich der praktische Aufwand zur Ermittlung von KK kann eventuell linear mit der Anzahl der DES-Operationen in f gesteigert werden.

Wenn die Zufallszahlen gleichmäßig verteilt sind, so ist damit auch der KS gleichmäßig verteilt, so daß mit einer geringen Wahrscheinlichkeit auch die schwachen Schlüssel ausgewählt werden. Ferner können bei zwei verschiedenen Kommunikationsbeziehungen mit Wahrscheinlichkeit $2^{L_{ks}}$ zufällig identische Sitzungsschlüssel ausgewählt werden.

Die Erzeugung der Zufallszahlen kann beispielsweise durch den OFB-Modus [5] eines Blockverschlüsslers erfolgen, also beispielsweise durch den DES mit teilnehmerindividuellen Schlüsseln $\boldsymbol{KR}_A$ und $\boldsymbol{KR}_B$ (KR, Random Number Generator Key).

4.5 Wechsel des Sitzungsschlüssels KS ohne Authentifikation

In diesem Abschnitt wird ein kryptographisches Protokoll dargestellt, mit dem der KS gewechselt werden kann, ohne daß eine Unterbrechung der Kommunikation durch den I&A-Dialog erforderlich ist. Im Extremfall kann der KS mit jedem Telegramm gewechselt werden.

Die beiden Kommunikationspartner A bzw. B verwalten jeweils aktiv Sequenznummern S_A bzw. S_B, die im Telegramm (als Teil der Nutzdaten) mit übertragen werden, so daß A bzw. B auch Kenntnis von S_B bzw. S_A haben. Mit Beginn des I&A-Dialogs wird $S_A = 0$ und $S_B = 0$ gesetzt. Anschließend werden die Sequenznummern mit jedem gesendeten Telegramm inkrementiert. Die im I&A-Dialog ausgetauschten Zufallszahlen werden bei beiden Partnern bis zum nächsten I&A-Dialog gespeichert. Dann kann zu jedem beliebigen Zeitpunkt unabhängig für die beiden Übertragungsrichtungen ein neuer KS in Erweiterung von (3) berechnet werden:

$$\boldsymbol{Z} = DES_{\boldsymbol{KK}_{AB}}(\boldsymbol{R}_A + S_A) + DES_{\boldsymbol{KK}_{AB}}(\boldsymbol{R}_B + S_B). \tag{8}$$

Auch ein Wechsel zu zufällig gewählten Zeitpunkten ist möglich, wenn die Sequenznummer des Wechselzeitpunktes vorher mehrfach angekündigt wird. Der KS-Wechsel funktioniert dann sogar beim Verlust einiger Telegramme.

Welchen Sinn hat nun der KS-Wechsel, und gibt es eine „optimale" Wechselfrequenz? Der KS sollte so oft gewechselt werden, daß eine rechentechnische Ermittlung von KS aus den MAC's während der KS-Gültigkeitsdauer unmöglich ist. Damit ist ein relativ kurzer KS möglich. Die häufige Ableitung von KS aus KK vereinfacht die

Ermittlung von KK nur unwesentlich, so daß ein langer KK praktisch extrem sicher ist. Die theoretische Kryptoanalyse ist allerdings unabhängig von der Wechselfrequenz. Eine praktisch optimale Wechselfrequenz kann kaum definiert werden, da hier sehr viele Randbedingungen eingehen.

4.6 Reaktion bei Fehlerentdeckung

Wenn bei der MAC-Kontrolle ein fehlerhaftes Telegramm entdeckt wird, so muß der Empfänger angemessen reagieren. Eine Unterscheidung zwischen zufälligen Fehlern aufgrund schlechter Übertragungsqualität oder einem kryptographischen Angriff ist einerseits nicht möglich und andererseits bei einem prinzipiell als sehr zuverlässig angestrebten Kanal auch nicht erforderlich.

Die geeignete Reaktion findet in der Applikationsschicht statt, und zwar in Abhängigkeit vom Typ der Telegramme (siehe Abschnitt 2.2), vom Quittierungsmodus und von der Anzahl der fehlerhaften Telegramme während gewisser Zeiträume. Falls mit einer Wiederholung des fehlerhaften Telegramms (aufgrund ausbleibender Quittung oder expliziter Rückmeldung) reagiert wird, so findet die Wiederholung innerhalb der Applikationsschicht statt, d. h. in der Sicherungsschicht wird die Nutzinformation mit der inkrementierten Sequenznummer zu einem geänderten MAC führen. Keinesfalls werden also gleiche Nutzdaten mit gleichem MAC wiederholt, da dies der Empfänger nicht von einem Replay-Attack unterscheiden kann.

5. Einbettung in GSM

Im Projekt DIBMOF werden neben der FZB noch andere Mobilkommunikationsdienste für die Integration in das GSM-System untersucht, eine Übersicht dazu gibt beispielsweise [11].

Der Datenfluß bei der Anwendung FZB ist selbst für Mobilfunkverhältnisse relativ gering. Bei der zyklischen Betriebsart der FZB ist ein gesichertes Telegramm von etwa 256 Bits Länge pro Sekunde zu übertragen. Bei der ereignisgesteuerten Betriebsart der FZB können die Telegramme wesentlich länger sein (bis zu 8000 Bit), aber ohne strenge Anforderungen an die Übertragungszeit.

Für die FZB-Kommunikation können prinzipiell folgende Verbindungstypen verwendet werden, um über die übertragungstechnische Anpassung auf die transparente und synchrone GSM-Luftschnittstelle zuzugreifen.

Transparent / Verbindungsorientiert. Vorzugsweise wird hier der Halbraten-Datenkanal TCH/H2.4 mit 2400 Bit/s verwendet, dessen Übertragungsrate allerdings bei der zyklischen Betriebsart um den Faktor 10 zu hoch ist.

Somit können sehr leistungsfähige ECC-Verfahren mit Coderaten im Bereich von 0.1 bis 0.2 angewendet werden. Falls dennoch bei sehr schlechten Übertragungsabschnitten die Fehlerkorrekturfähigkeit überschritten wird, so werden die verbleibenden Fehler vom ECC oder vom MAC-EDC erkannt. Eventuelle Wiederholungen werden außerhalb des bedrohten Kanals organisiert.

Non-Transparent / Verbindungsorientiert. Vorzugsweise wird hier der Halbraten-Datenkanal TCH/H4.8 (NT) bzw. TCH/H2.4 (NT) mit 4800 bzw. 2400 Bit/s in Verbindung mit dem GSM Radio Link Protocol (RLP) verwendet [10]. An den Endpunkten der GSM-Verbindung, also in der Network Interworking Function (IWF, in der MSC) und in der Terminal Adaptation Function (TAF, im Mobilgerät), wird dabei ein ARQ-Protokoll (automatic repeat request) verwaltet, das bei (durch einen EDC) erkannten Übertragungsfehlern selbständig Wiederholungen vornimmt. Als Konsequenz ist die Übertragungsgüte konstant und unabhängig von der Qualität des Funkkanals, aber der Durchsatz und die Übertragungsverzögerung sind sehr stark von der Kanalqualität abhängig. Dieses Verfahren wird also durch das GSM-System und somit innerhalb des bedrohten Kanals organisiert, so daß sich daraus keine Rechenbelastungen für die Sicherungs- und die Applikationsschicht ergeben.

Allerdings ist diese Methode für die Anwendung FZB ungeeignet, da das ARQ-Protokoll von der Anwendung nicht direkt beeinflußt werden kann. Beispielsweise könnte es vorkommen, daß ein unwichtiges Telegramm immer wieder übertragen wird, während gleichzeitig ein wichtiges Telegramm höherer Priorität dadurch blockiert wird.

Schließlich sind bei dieser Methode auch ECC-Verfahren zur Erhöhung der Zuverlässigkeit unmöglich, so daß die Gesamteffizienz ungünstig bleibt.

Paketorientiert. Ein derartiger Verbindungstyp wird eventuell in einem erweiterten GSM-Standard verfügbar sein (GPRS, General Packet Radio Service), so daß verschiedene Benutzer den gleichen GSM-Kanal benutzen können.

Nachfolgend wird aber nur noch der transparente Halbraten-Datenkanal mit 2400 Bit/s betrachtet, weil hier die Wiederholungsverfahren direkt in der Anwendung organisiert werden und damit direkt kontrollierbar und steuerbar sind.

Mit Reed-Solomon-Codes zwischen der übertragungstechnischen Anpassung und dem GSM-Netz kann nicht nur die normale Fehlerrate der GSM-Kanäle reduziert werden, sondern es kann auch das gravierende Problem bei der Einbettung der FZB-Kommunikation in GSM gemindert werden, nämlich die durch die Inband-Signalisierung bei Handover (Zellenwechsel) verursachten Unterbrechungen. Die Unterbrechungszeit (von HO.COMMAND bis HO.COMPLETE, siehe [10]) liegt im fehlerfreien Fall im Bereich 150 bis 1000 ms (Mittelwert 300 bis 400 ms) – abhängig von den Randbedingungen wie Typ des Handovers (Intracell, Intercell, External), Synchronisationsmodus, Frequency Hopping und dem Nutzkanal-Typ. Je nach Clusterfaktor bzw. C/I-Wert an der Zellgrenze sowie des Handover-Managements kommt noch mit einer gewissen Verteilung ein Abschnitt von bis zu 1000 ms hinzu, in dem Unterbrechungen und stark erhöhte Fehlerraten auftreten. Bekanntlich erlauben (n, k)-RS-Codes die fehlerfreie Rekonstruktion des Informationswortes, wenn mindestens k beliebig verteilte Stellen im Codewort unverfälscht sind [6]. Allerdings sind mit dieser Methode natürlich Übertragungszeiten bzw. Aktualitätsverluste verbunden, die für die Anwendung noch akzeptabel sein müssen.

Ein Mobilfunknetz mit linien- statt flächenförmiger Ausleuchtung erlaubt auch eine besondere Funkplanung. Durch geeignete Standorte für die Basisstationen sowie

durch Richtantennen und aufgrund der ziemlich gerade verlaufenden Hochgeschwindigkeitsstrecken lassen sich sehr gute Ausleuchtungen mit hohen Rice-Faktoren erzielen [12, 13], die zu sehr zuverlässigen Kanälen auch bei Hochgeschwindigkeiten von 500 km/h führen.

6. Zusammenfassung

Die vorgestellten Sicherungsverfahren ermöglichen eine sicherheitsrelevante Kommunikation bei höchsten Anforderungen an Sicherheit und Zuverlässigkeit auch dann, wenn das Übertragungssystem relativ unzuverlässig ist und vielfältigen potentiellen Bedrohungen unterliegt. Die diskutierten Algorithmen basieren zwar auf bekannten Verfahren, aber bei der Kombination zu einem Gesamtverfahren und insbesondere bei der informationstheoretischen Analyse des Message Authentication Code treten doch vollkommen neue Fragestellungen auf.

Bei der Dimensionierung der kryptographischen Verfahren, insbesondere bei den Längen des Message Authentication Code und der verschiedenen Schlüssel, ist eine Abwägung zwischen dem theoretischen und praktischen Sicherheitsniveau erforderlich, die letztlich nur von Seiten der Anwendung erfolgen kann.

Die Einbettung der FZB-Kommunikation in das GSM-System erweist sich als abhängig von verschiedenen Details der FZB. Im Rahmen des Projektes DIBMOF wird auch die Funk-Zugbeeinflussung selbst neu konzipiert, so daß hier die möglichen Alternativen noch nicht weiter konkretisiert werden können.

Diese Arbeit entstand im Rahmen des Forschungs- und Entwicklungsvorhabens DIBMOF Phase II, gefördert durch das Bundesministerium für Forschung und Technologie und die Senatsverwaltung für Arbeit und Betriebe, Berlin (Förderkennzeichen TV 9211 B).

Der Autor möchte allen Beteiligten der Firmen AEG Mobile Communication, Alcatel-SEL, Detecon, Deutsche Bahnen und Siemens in der Arbeitsgruppe AG4 des vorgenannten Projektes für viele hilfreiche Diskussionen danken, die wesentlich zu den Ergebnissen aus Teil II beigetragen haben.

Literatur:

[1] Friedrichs, B.: Authentische und zuverlässige Mobilkommunikation für sicherheitsrelevante Anwendungen. Teil I: Sicherheitsanforderungen und grundlegende Verfahren. Frequenz 49 (1995) S. 17—27.
[2] Friedrichs, B.: Sicherungsverfahren für die Datenübertragung über „Bedrohte Kanäle" bei sicherheitsrelevanten Diensten. ANT Nachrichtentechnische Berichte (1993) 10, S. 47—63.
[3] Chudoba, C.; Weis, B. X.; Zeller, D.: Secure Communication for Traun Control. ITG/GI-Fachtagung Kommunikation in verteilten Systemen. München 1993.
[4] Davies, D. W.; Price, W. L.: Security for Computer Networks. New York: John Wiley 2. Ed. 1989.
[5] Fumy, W.; Rieß, H. P.: Kryptographie. München: R. Oldenbourg Verlag 1988.
[6] Blahut, R. E.: Theory and Practice of Error Control Codes. Reading: Addison-Wesley 1983.
[7] Beutelspacher, A.; Kersten, A.; Pfau, A.: Chipkarten als Sicherheitswerkzeug. Berlin: Springer 1991.
[8] Muftic, S.: Sicherheitsmechanismen für Rechnernetze. München: C. Hanser/Prentice-Hall 1992.
[9] Purser, M.: Secure Data Networking. Boston: Artech House 1993.
[10] Mouly, M.; Pautet, M. B.: The GSM System for Mobile Communications. Palaiseau, France 1992.
[11] Dreßler, H.-J.: GSM als zukünftiger UIC-Mobilfunkstandard. Signal + Draht 86 (1994) 1/2, S. 27—30.
[12] Bossert, M.; Hätty, B.; Klund, P.: GSM-Übertragungstechnik für Bahnanwendungen. Signal + Draht, 85 (1993) 12, S. 455—458.
[13] Fröhlingsdorf, G.; Göller, M.; Masur, K.-D.; Weber, U.: Meßergebnisse und Parameter zur Modellierung von Bahn-Mobilfunkkanälen im 900 MHz-Band. Nachrichtentechnik Elektronik 43 (1993) 6, S. 290—295.

Dr.-Ing. B. Friedrichs, ANT Nachrichtentechnik GmbH, Gerberstraße 33,
D-71522 Backnang
(Eingegangen am 11. 3. 1994)

Neues aus Forschung, Industrie und Wirtschaft

Videokonferenz vom Arbeitsplatz aus PC-Lösung von FUBA

Videokonferenzen sind ideales Mittel zur Verbesserung der internen und externen Kommunikation eines Unternehmens. Schnellere Entscheidungsfindung, Einsparung von Sach- und Dienstleistungen und der Wegfall von Reisezeiten machen die Videokonferenztechnik für den Anwender attraktiv.

Um Videokonferenzen direkt vom Arbeitsplatz aus durchführen zu können, hat FUBA das PC-gestützte System VS 1000 entwickelt, das die spontane, kostengünstige Videokonferenz ermöglicht. Über das System können Daten, Bilder und Sprache übertragen werden.

Eine spezielle Anwendungsform der Videokonferenztechnik stellt das FUBA-MEDKOM-System dar. Es wurde eigens für den Einsatz in Krankenhäusern, Universitätskliniken, Laboratorien und Arztpraxen entwickelt.

Züchtung versetzungsarmer Galliumarsenid-Kristalle

Unter der Leitung von Prof. Dr. Georg Müller (Institut für Werkstoffwissenschaften, Lehrstuhl VI, Martensstr. 7, 91058 Erlangen, Tel.: 09131/85-7636, Fax: 09131/85-8495) wird derzeit die Züchtung von weitgehend „fehlerfreien" Kristallen aus Galliumarsenid, die die Grundlage für langlebige Hochleistungslaser-Dioden bilden können, am Erlanger Kristallabor mittels eines noch wenig untersuchten, vielversprechenden Verfahrens erprobt. Das Forschungsvorhaben, das in Zusammenhang mit der Bergakademie Freiberg und dem Zentrum für Funktionswerkstoffe Göttingen durchgeführt wird, ist eines von sechs Projekten in einem Forscherbund zur Stärkung der Laserforschung in Deutschland. Im Juli 1994 konnte bereits ein erster Galliumarsenid (GaAs)-Einkristall mit Hilfe des Vertikalen Gradient-Freeze-Verfahrens gezüchtet werden.