Methoden zum Schutz von Verkehrsdaten in Funknetzen

Jürgen Thees, Hannes Federrath
TU Dresden, Institut Theoretische Informatik, 01062 Dresden

23. September 1994

Zusammenfassung

Die stürmische Entwicklung der öffentlichen Funknetze, insbesondere der digitalen Mobilfunknetze, ermöglicht es immer mehr Teilnehmern, auf komfortable Weise ortsunabhängig zu kommunizieren. Die Verwendung elektromagnetischer Wellen für die Übertragung der Daten im freien Raum bringt jedoch Probleme bezüglich des Datenschutzes mit sich.

Das vorliegende Papier sucht unter dem Aspekt des technischen Datenschutzes nach Möglichkeiten, die Peilung von aktiven Sendeeinrichtungen zu verhindern. Das angestrebte Ziel ist, die Nichtortbarkeit einer Mobilstation und damit den Schutz des Aufenthaltsortes eines Teilnehmers zu gewährleisten.

Die Untersuchungen ergeben ein Modell, bei dem unter Ausnutzung eines Geheimnisses die unbeobachtbare Kommunikation zwischen Sender und Empfänger möglich ist. Die gefundenen Erkenntnisse werden auf eine bestehende Konzeption zum Schutz von Verkehrsdaten angewendet. Für Probleme beim Einsatz des Verfahrens werden Lösungsmöglichkeiten aufgezeigt und die sich ergebenden Änderungen bezüglich ihrer Eignung bewertet.

Einige Überlegungen zu Aufwand und Realisierbarkeit in derzeitigen und künftigen Netzen schließen die Arbeit ab.

1 Einführung

Elektromagnetische Wellen tragen neben den Nutzdaten Richtungsinformationen in sich und können somit von jedermann zur Ortsbestimmung einer Sendestation eingesetzt werden. Bereits einfachste Peiltechniken ermöglichen einen Zugriff zu solchen Ortsinformationen und damit auch die Erstellung von Bewegungsprofilen. Die Kenntnis dieses Problems führte zu einem verstärkten Nachdenken darüber, wie die bestehende Situation entschärft werden kann. Grundlage der Untersuchungen bildeten dabei erste Gedanken in [Pfit93]. Darin werden prinzipielle Vorschläge zum Schutz der Verkehrsdaten unter den speziellen Bedingungen von Funknetzen gemacht. Das dort verwendete Angreifermodell geht von der Annahme aus, daß eine sendende Mobilfunkstation in jedem Falle peilbar ist. Mit der vorliegenden Arbeit soll nun untersucht werden, ob es Möglichkeiten gibt, diese Annahme abzuschwächen. Ziel war es dabei, Verfahren zu finden, welche die Gewinnung von Richtungsinformationen aus elektromagnetischen Wellen stark erschweren oder unmöglich machen.

2 Peilung und Ortung

Elektromagnetische Wellen besitzen eine elektrische und eine magnetische Feldkomponente. Die Feldstärkevektoren stehen senkrecht aufeinander und senkrecht auf dem Ausbreitungsvektor. Jede Form elektromagnetischer Ausstrahlung trägt in ihrer Erscheinungsform also auch eine Richtungsinformation. Der mit Lichtgeschwindigkeit fortschreitenden Wellenfront kann diese unter Einsatz geeigneter Meßverfahren entnommen werden. Orts- und Richtungsbestimmungen erfordern eine bestimmte Modellvorstellung. Im einfachsten Fall kann dies die Entstehung und Ausbreitung von Wellen im freien Raum sein.

Die an einem Ort vorgenommene Bestimmung der hier vorherrschenden Ausbreitungsrichtung elektromagnetischer Wellen nennt man **Peilung**. Grundlage hierfür ist die Eigenschaft elektromagnetischer Wellen, sich von der Quelle aus geradlinig auszubreiten. Daraus kann man die Parameter Ausbreitungsrichtung und Laufzeit einer Wellenfront ermitteln. Die Peilung einer einzelnen Peilstelle liefert dabei eine Standlinie, auf der sich der gesuchte Ort befindet.

Die so ermittelten Standlinien können dann zur **Ortung** genutzt werden. Der Schnittpunkt dieser Standlinien ist der gesuchte Standort. Diese kurzen Erläuterungen zeigen, daß zu jeder elektromagnetischen Welle eine Bestimmung der Ausbreitungsrichtung und des Quellortes auf einfache Art und Weise möglich ist. Dabei wird allerdings immer davon ausgegangen, daß die zu analysierende Welle eine ausreichende Feldstärke besitzt und zeitlich unbegrenzt zur Verfügung steht.

3 Ansätze zur Verhinderung von Peilung

Um die Peilung elektromagnetischer Wellen zu erschweren, bietet es sich an, Störungen bei deren Ausbreitung zu nutzen. In der Praxis treten solche Störungen durch Inhomogenitäten und Diskontinuitäten im Ausbreitungsmedium auf, und widersprechen damit dem Modell der geradlinigen Wellenausbreitung.

Neben diesen Ausbreitungsproblemen ergeben sich jedoch auch Störungen der zu peilenden Wellen durch andere Wellen im gleichen Frequenzbereich. Diese Mehrwellenproblematik ist technisch nur sehr schwer aufzulösen. Kann eine derartige Auflösung nicht erfolgen, so besteht auch keine Möglichkeit, die Ausbreitungsrichtung der am Signalgemisch beteiligten Wellen zu ermitteln. Bei einer großen Senderdichte wird neben diesem Problem eine Identifizierung des richtigen Senders notwendig.

Eine weitere Peilfehlerquelle und ein Problem bei der allgemeinen Verarbeitung elektromagnetischer Wellen stellt das **Rauschen** dar. Beim Rauschen handelt es sich um eine kontinuierliche Spannung, die in nicht vorhersagbarer Weise schwankt und das Ergebnis innerer und äußerer statistischer Störungen ist. Das Rauschen trägt eine gewisse Energie in sich, die ein zu verarbeitendes Signal verfälscht. Wesentliche Anteile des Rauschens, vor allem das thermische Rauschen, sind mit gleicher Leistungsdichte über das gesamte Frequenzspektrum verteilt.

Trotz all dieser Probleme ist eine Peilung und damit auch eine Ortung von Funksendern immer noch möglich. Es ist jedoch zu beachten, daß die Bestimmung einer Standlinie einen bestimmten Zeitaufwand erfordert, der nicht beliebig verringert werden kann. Des weiteren muß die Welle als solche erkennbar sein, das heißt, ihr Signal/Rausch-Verhältnis muß einen bestimmten Wert überschreiten. Die Kenntnis dieser Bedingungen führte zur Entwicklung eines Kommunikationsmodells, das im folgenden vorgestellt werden soll.

Neben dem Schutz vor Peilung muß das Verfahren auch gewährleisten, daß ein legitimer Empfänger das Signal trotzdem auswerten kann. Der Grundgedanke besteht nun darin, daß Sender und Empfänger ein gemeinsames Geheimnis haben, welches nur ihnen die Kommunikation ermöglicht.

Zur Realisierung eines Verfahrens wird aus den Parametern elektromagnetischer Wellen einer ausgewählt, dessen Veränderung in einem großen Bereich auf einfache Art und Weise möglich ist. Hintergrund dafür ist die Notwendigkeit eines großen Schlüsselraumes, um ein bestimmtes Sicherheitsniveau zu ermöglichen. Die Frequenz scheint hier den größten Spielraum zu bieten. Statt des bisherigen einzelnen Kanals sollen ab jetzt n mögliche Sendekanäle zur Verfügung stehen. Ein Zeichen wird nun nicht mehr nur auf einem Kanal gesendet, sondern die Sendeenergie auf m Kanäle verteilt.

Die Zahl m der notwendigen Sendekanäle ist abhängig von der Energieveränderung, die im einzelnen Kanal vorgenommen werden soll. Diese darf nur so groß sein, daß sie im Bereich statistischer Schwankungen des Rauschens liegt. Damit wird sichergestellt, daß die Beobachtung eines einzelnen Kanals keine Aussagen liefert. Erst die Beobachtung aller m Kanäle gibt Aufschluß über das gesendete Zeichen. Die Auswahl der m Kanäle erfolgt pseudozufällig und wird vom geheimen Schlüssel der Kommunikationspartner gesteuert. Ein Testen aller Möglichkeiten wird durch die kombinatorische Explosion verhindert, die bei größeren Werten von m und n entsteht. Selbst wenn der Angreifer in der Lage ist, alle Kombinationen durchzuprobieren, fehlt ihm jedoch ein Entscheidungskriterium dafür, wann er die richtige Kombination gefunden hat.

Das vorgestellte Modell zeigt erst einmal nur die Grundkonzepte aus kryptographischer Sicht auf. Für den praktischen Einsatz ist natürlich noch die Vorstellung eines technisch durchführbaren Verfahrens notwendig.

4 Die Realisierung

Die Forderung nach Nutzung mehrerer Kanäle oder allgemein eines breiteren Frequenzbereiches wird von den **Bandspreizverfahren** (*spread spectrum systems*) realisiert. Sie benutzen eine Bandbreite, die viel höher ist, als die zu übertragende Information es erfordert. Zur Verteilung der Energie auf das zur Verfügung stehende Frequenzband verwenden sie Funktionen (meist Codesequenzen), die von der zu übertragenden Information unabhängig sind, und beeinflussen damit Parameter im Zeit- oder Frequenzbereich.

Die Bandspreizverfahren basieren auf dem Grundsatz der Nachrichtentheorie, daß es bei der Übertragung eines digitalen Zeichens nicht darauf ankommt, welche Form es besitzt, sondern nur auf seinen Energieinhalt, d.h. die Fläche, die sein Spektrum besitzt. Wie sich die Signalenergie dabei auf die Frequenzachse verteilt ist unerheblich. Wird also durch ein geeignetes Modulationsverfahren die Signalleistungsdichte nun so breit verteilt, daß sie wesentlich kleiner als die Rauschleistungsdichte ist, so ist dennoch eine Informationsübertragung möglich. Die benötigte Bandbreite kann unter Zuhilfenahme der Shannonschen Formel für die Kanalkapazität

$$C = B \, \log_2 \left(1 + \frac{S}{N}\right)$$

berechnet werden, mit der Kanalkapazität C, der Bandbreite B, der Signalenergie S und der Rauschenergie N. Für betragsmäßig kleine Werte[1] von $x := \frac{S}{N}$ gilt die Beziehung $\log_2(1+x) \approx \frac{x}{\ln 2}$. Da dies aber die interessanten Werte für $\frac{S}{N}$ in einem Bandspreizsystem sind, kann die Formel auf einfache Art und Weise nach B umgestellt und für ein gegebenes

[1] Nur für $x \leq 0,1$ kann der Logarithmus so einfach aufgelöst werden.

Signal/Rausch-Verhältnis sowie eine geforderte Kanalkapazität die erforderliche Bandbreite ermittelt werden:

$$B \approx \ln 2 \cdot C \cdot \frac{N}{S}$$

Die spektrale Spreizung wird durch Multiplikation eines auf konventionelle Weise modulierten, relativ schmalbandigen Signals mit einer breitbandigen Spreizfunktion erreicht, die von den zu sendenden Daten unabhängig ist. Als Spreizfunktion dient meist eine Pseudozufallszahlenfolge sehr langer Periode, die eine schnell abklingende Autokorrelationsfunktion besitzt und rauschähnliches Verhalten zeigt. Aufgrund ihrer Eigenschaften wird sie **Pseudorausch- (*pseudonoise* PN-) Code** genannt. Im Rhythmus dieses Digitalsignals wird entweder die Phase (*phase shift keying* PSK) oder die Frequenz des Nachrichtensignals umgetastet. Die Rückgewinnung der Information kann in beiden Fällen nur dann erfolgen, wenn die bei der Modulation verwendete Codesequenz bekannt ist. Mit der spektralen Spreizung ergibt sich gleichzeitig eine Verringerung der spektralen Leistungsdichte.

Als konkretes Verfahren scheint die **direkte Spreizung** (*direct sequence spread spectrum* DS) am Besten geeignet. Dabei wird die Energie der Sendung durch Multiplikation mit der digitalen Zufallszahlenfolge kontinuierlich über das zur Verfügung stehende Spektrum verteilt: Die zu übertragenden Daten werden zunächst auf einen Träger in herkömmlicher Weise aufmoduliert. Das entstehende, relativ schmalbandige Signal wird dann in einem zweiten Modulationsschritt mit einem breitbandigen binären PN-Code, der rauschähnliches Verhalten zeigt, moduliert.

Die Erzeugung des PN-Codes geschieht unter Zuhilfenahme eines PN-Generators aus dem PN-Key, welcher das Geheimnis von Sender und legitimen Empfänger darstellt. Es entsteht ein Signal geringer Leistungsdichte, das von einer Antenne abgestrahlt werden kann und ähnliche Merkmale wie „weißes Rauschen“ aufweist.

Auf der Empfängerseite wird der PN-Code nachgebildet. Durch erneute Multiplikation des empfangenen Signals mit diesem Code wird die Spreizung wieder zurückgenommen und der modulierte Träger liegt in seiner ursprünglichen Form vor. Aus ihm können nun die Daten zurückgewonnen werden (Bilder 1 und 2).

Das gesendete DS-Signal besitzt eine große Unempfindlichkeit gegen Störungen. Mehrere Nutzer können so auf dem gleichen Frequenzband arbeiten, wenn sie orthogonale Codes benutzen. Das bedeutet, daß die PN-Codes nur geringe Kreuzkorrelationen aufweisen dürfen, um die gegenseitige Beeinflussung so klein wie möglich zu halten. Wird der PN-Code zusätzlich nach kryptologischen Gesichtspunkten gebildet, so bewirkt das zugleich eine Verschlüsselung der Sendung.

Wie in Bild 3 zu sehen ist, werden von der Empfangsantenne natürlich neben dem gewünschten Signal auch andere Signale sowie Rauschen und Störsignale aufgenommen. Im Mischer wird nun die spektrale Spreizung des gewünschten Signals mittels des synchronisierten PN-Codewortes zurückgenommen. Bei diesem Vorgang werden alle unerwünschten Signale spektral gespreizt (Bild 4) und können danach mit entsprechenden Filtern eliminiert werden. Aus diesem Entspreizvorgang ergibt sich ein Systemgewinn, der dem Verhältnis von Bandbreite des gespreizten Signals zu Signalbandbreite $B/\Delta B$ entspricht. Dies ist auch der Grund, warum DS-Signale nur ein so geringes Signal/Rausch-Verhältnis haben müssen. Die Übertragungsqualität eines DS-Signals wird also wesentlich vom Verhältnis Bandbreite des Datensignals zu Bandbreite des Pseudorauschsignals bestimmt, dem sogenannten Spreizfaktor. Dieser liegt im Normalfall in der Größenordnung von einigen hundert und bestimmt zugleich den Grad der Absenkung (bzw. Anhebung auf der Senderseite) des Signals.

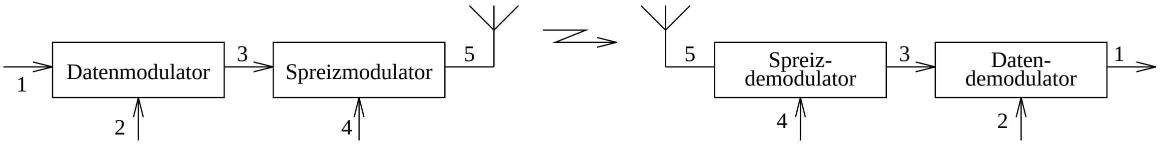

Abbildung 1: Modulation eines Trägers mit den zu übertragenden Daten

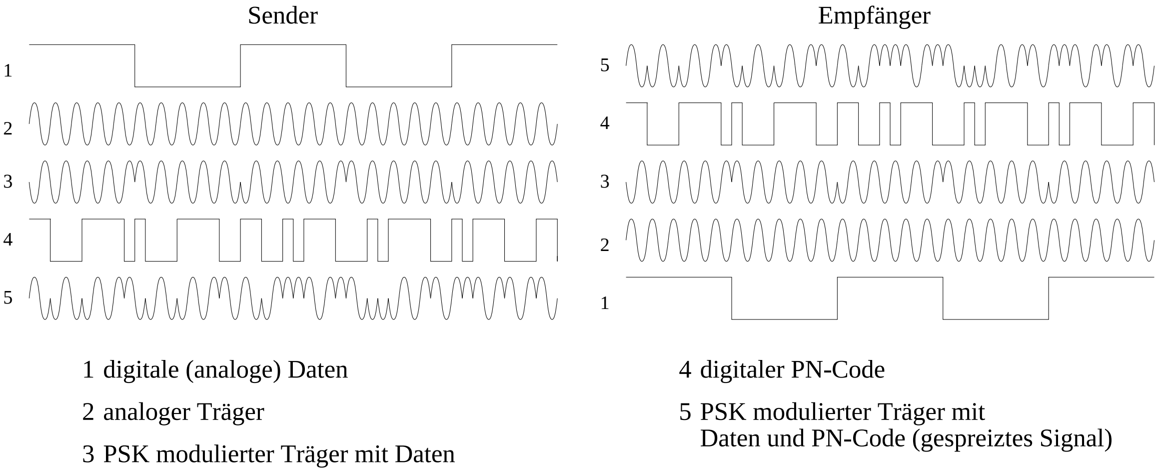

Abbildung 2: Signalformen bei der Trägermodulation mit den zu übertragenden Daten

5 Erkennung bandgespreizter Signale

Bei bekanntem PN-Code können DS-Signale sehr gut zur Peilung und Ortsbestimmung eingesetzt werden ([Dixo84] S. 306ff). Sie sind relativ unempfindlich gegen Störungen, aber die Synchronisation der PN-Codereferenz mit dem empfangenen Signal muß sehr genau erfolgen. Daraus ergibt sich die Möglichkeit, das Signal an zwei Antennen zu empfangen, deren genauer Abstand bekannt ist. Wird an beiden Empfängern die PN-Codesequenz durch Korrelation synchronisiert, so ist ein zeitlicher Versatz zwischen den beiden Empfängern ermittelbar, der ein Maß für die relative Entfernung der Antennen zum Sender darstellt. Durch diese Laufzeitpeilung (*time of arrivel direction finding* TOA-DF) erhält man eine Standlinie, auf der sich der Sender befindet. Das kann hilfreich sein, wenn der Standort eines Nutzers ermittelt werden muß, z.B. in einem Notfall. Dieser kann dann einen Notfallcode benutzen, der den entsprechenden Stationen bekannt ist, und mit dessen Hilfe sie eine Ortung vornehmen können.

Wenn die Signale im Vergleich zum thermischen oder Umgebungsrauschen eine geringere spektrale Dichte haben und wenn sich diese in Abhängigkeit von der Frequenz nur sehr langsam ändert (was bei Verwendung von PN-Codes maximaler Länge der Fall ist), sind DS-Signale bei unbekanntem PN-Code mit konventionellen Mitteln wie Spektrumanalysatoren nicht zu entdecken (LPI-Signale: *low probability of intercept*). Trotzdem existieren zwei prinzipielle Möglichkeiten, das im Rauschen versteckte Signal zu erkennen:

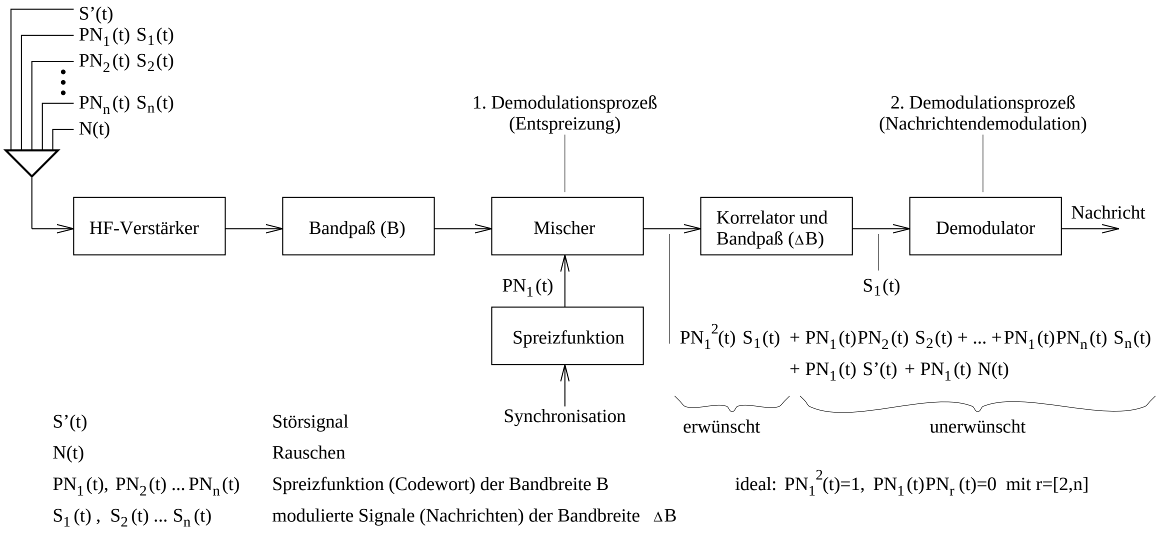

Abbildung 3: Verarbeitung von direkt gespreizten Signalen

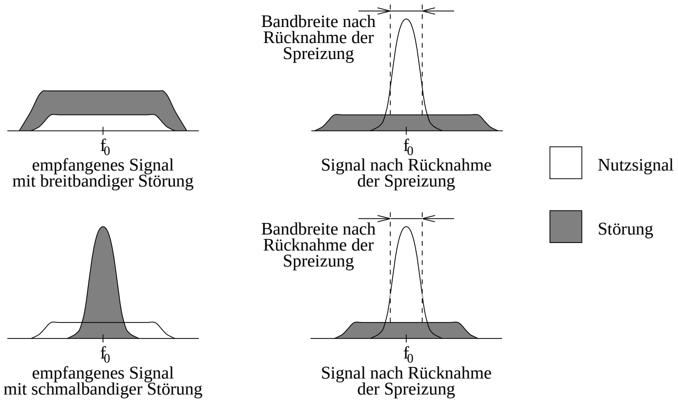

Abbildung 4: Einfluß von Störungen auf direkt gespreizte Signale

5.1 Integration des vorhandenen Rauschens

Hintergrund dieses Verfahrens ist die Tatsache, daß jede Aussendung eines Signals und damit von elektromagnetischen Wellen zu einer Erhöhung des Energieniveaus im jeweiligen Frequenzbereich führt. Bei der direkten Spreizung ist diese Erhöhung natürlich sehr gering im Vergleich zum Rauschpegel. Um die Erhöhung feststellen zu können, wird eine Anordnung benutzt, die man **Radiometer** nennt. Den Aufbau eines solchen Gerätes zeigt Bild 5.

Die Ausgabe X des Integrators wird mit einem festgelegten Schwellwert S verglichen und in Abhängigkeit des Ergebnisses auf die Existenz ($X > S$) oder Nichtexistenz ($X < S$) eines Signals geschlossen. Die Rauschenergie kann jedoch aufgrund verschiedenster Einflüsse (Antennenrauschen abhängig vom Wetter; nur endliche Mittelwertbildung bei Messungen; nichtstationäres Rauschen im Kanal usw.) nicht unendlich genau bestimmt werden. Es kann lediglich eine obere Grenze für das benötigte Signal/Rausch-Verhältnis ermittelt werden, ungeachtet der Sendezeit. Der Grund dafür ist, daß das Radiometer nur auf Veränderungen

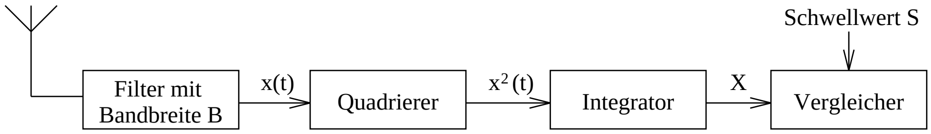

Abbildung 5: Aufbau eines Radiometers

in der gesamten empfangenen Energie reagiert, diese sich aber zum größten Teil aus Rauschenergie zusammensetzt. Die zur Berechnung notwendigen Formeln sind in [SoFi92] zu finden.

Selbst wenn das Radiometer ein Signal erkannt hat, gibt es danach keine Möglichkeit, dieses Signal zu peilen. Auch ist eine Unterscheidung, ob es sich um ein oder mehrere Signale handelt, nicht möglich. Diese Begrenzungen des Radiometers sind der Grund, warum hier keine tiefere theoretische Behandlung sondern nur ein Verweis auf die entsprechende Literatur erfolgt.

5.2 Korrelationsanalyse

Die Korrelationsanalyse kann genutzt werden, um deterministische Signale unterhalb des Rauschpegels zu erkennen. Die **Autokorrelationsfunktion** (*autocorrelation function* ACF)

$$\psi(\tau) = \lim_{T \to \infty} \frac{1}{2T} \int_{-T}^{+T} x(t)\, x(t+\tau)\, dt$$

ist ein Maß für den deterministischen Zusammenhang des Signalverhaltens zu unterschiedlichen Zeitpunkten. Hat die Funktion $\psi(\tau)$ die Form eines Impulses, so wird die Zeitdauer des Impulses die Korrelationszeit des Signals genannt. Die ACF hat ihren Maximalwert bei $\tau = 0$ und zeigt in Abhängigkeit der Periode ein charakteristisches Verhalten. Gegen diese Detektion periodischer Vorgänge kann man sich jedoch ganz einfach schützen, indem man die Periode des verwendeten PN-Codes so groß wählt, daß er sich während einer Sendung nicht wiederholt.

Bliebe noch die Möglichkeit einer Kreuzkorrelationsanalyse. Dabei wird nicht das gleiche Signal zeitlich versetzt, sondern ein Signal verwendet, von dem man annimmt, daß es mit dem Gesuchten stark korreliert. Die **Kreuzkorrelationsfunktion** (*crosscorrelation function* CCF) berechnet sich nach

$$\psi_{xy}(\tau) = \lim_{T \to \infty} \frac{1}{2T} \int_{-T}^{+T} x(t)\, y(t+\tau)\, dt$$

und hat ein Maximum, wenn die korrelierenden Signale zeitsynchron sind. Für das Finden eines DS-Signals wäre ein solches korrelierendes Signal der PN-Code, mit dem es erzeugt wurde.

Die CCF wird bei einem Verfahren benutzt, das mit der Laufzeitpeilung bei bekanntem PN-Code vergleichbar ist. Verwendet werden zwei oder mehrere zeitsynchronisierte, örtlich verteilte Empfangsstationen mit bekanntem Abstand. Dieser muß so groß gewählt sein, daß das Rauschen an beiden unkorreliert ist. Wie bei der Laufzeitpeilung wird der Zeitunterschied des Eintreffens eines bestimmten Merkmals an den Empfangsstationen ermittelt. Dazu wird die Kreuzkorrelationsfunktion der Empfangssignale zweier Stationen gebildet.

Die empfangenen Signale enthalten beide Rauschen und das darin versteckte Signal. Das Rauschen ist aufgrund der Entfernung der Empfangsstationen aber unkorreliert, und leistet so keinen Beitrag. Die Kreuzkorrelationsfunktion wird also ein Maximum haben, wenn beide Signale zeitsynchron sind. Die dazu notwendige Verzögerung des einen Signals um $\Delta t = \tau$ liefert aber wie bei der Laufzeitpeilung eine Standlinie, auf der sich der Sender befinden muß. Somit ist auch hier eine prinzipielle Möglichkeit gegeben, die Einfallsrichtung des Signals zu ermitteln.

Bei dem beschriebenen Vorgehen gibt es jedoch keine Möglichkeit, ein gewünschtes Signal zu selektieren. Deshalb würde das gesamte, an den Antennen empfangene, Signalgemisch bei der Kreuzkorrelationsanalyse verwendet. Das Ergebnis wäre eine Vielzahl von lokalen Maxima bei unterschiedlichen Verzögerungszeiten ($\rightarrow$ Richtungen), womit die angestrebte Richtungsbestimmung für ein bestimmtes Signal unmöglich wird. Bei der hohen Sensitivität des Verfahrens für Signale weit unter dem Rauschpegel kann man sich vorstellen, daß aus nahezu allen Richtungen Signale von Stationen empfangen werden, selbst wenn sie aufgrund der hohen Entfernung nur sehr schwach sind.

5.3 Schlußfolgerungen

Zusammenfassend kann so folgendes festgestellt werden:

Die direkte Spreizung erfüllt die Forderungen nach Nichtortbarkeit eines Senders. Unter den bisher bekannten und untersuchten Methoden gibt es kein Verfahren, mit dem DS-Signale ohne Kenntnis des PN-Codes peilbar wären, und deshalb auch keine Möglichkeit, die Ortung des Senders vorzunehmen.

Ausgenutzt werden also Probleme, die sich bei der Trennung von Signalgemischen ergeben. Schon bei Energiedichten weit über dem Rauschpegel ist eine Trennung von Signalgemischen nicht immer möglich. Beispielsweise können zwei Signale, die aus der gleichen Richtung kommen und auf der gleichen Frequenz liegen, nicht mehr getrennt werden. Dies gilt sowohl für einen potentiellen Angreifer als auch den legitimen Empfänger. Bei der direkten Spreizung kommt für den Angreifer aufgrund des niedrigen Signalpegels zusätzlich das Rauschen als Störquelle hinzu, der legitime Empfänger dagegen hat mittels des PN-Codes die Möglichkeit, das Signalgemisch zu trennen.

Das bisher verwendete Peilungsmodell geht vom theoretischen Fall des Vorhandenseins nur *eines* zu analysierenden Signals aus. Die Erweiterung des Modells auf mehrere trennbare und damit analysierbare Signale hat zunächst keinen Einfluß auf die Aussagen über Peilbarkeit.

Zusätzlich kommt für einen Angreifer das Problem hinzu, jedem Signal eine Sendestation und dieser wiederum einen Benutzer zuzuordnen. Diese Aufgabe wird im allgemeinen durch Analyse der Inhaltsdaten oder Verkettung von Informationen vorgenommen. Werden die Möglichkeiten eines potentiellen Angreifers in dieser Richtung eingeschränkt, so trägt das in einem Mehrsignalumfeld wesentlich zur Verringerung der Ortungswahrscheinlichkeit eines Nutzers bei. Diese Bemerkung soll zeigen, daß die Grundannahmen der bisherigen Untersuchungen defensiver sind als eigentlich notwendig, damit aber eine gute obere Schranke bilden.

6 Konsequenzen und Auswirkungen

Während bisher, das heißt in [Pfit93], davon ausgegangen wurde, daß eine Mobilstation (*mobile station* MS) immer peilbar ist, wenn sie sendet, kann diese Annahme jetzt abgeschwächt werden. Nach den neuen Erkenntnissen ist bei Verwendung der direkten Spreizung eine Mobilstation nur noch dann peilbar, wenn der Angreifer über den zur Spreizung verwendeten PN-Code verfügt.

Das ursprünglich angestrebte Ziel ist allerdings noch nicht vollständig erreicht. Zwar kann ohne Kenntnis des PN-Codes nach den bisherigen Untersuchungen niemand die Mobilstation peilen, der autorisierte Empfänger muß allerdings zum Empfang der Sendung im Besitz des PN-Codes sein und hat so auch die Möglichkeit, die Position des Senders zu ermitteln. Die direkte Spreizung eines Signals bildet damit ein Analogon zur Verbindungsverschlüsselung in der Kryptographie, bei der auch der im Besitz des Schlüssels befindliche Empfänger die Nachricht entschlüsseln kann, jeder andere dagegen nicht. Von der elektrotechnischen Seite bestehen hier jedoch keine Möglichkeiten mehr, die Peilung auch für einen im Besitz des PN-Codes befindlichen Kommunikationspartner zu verhindern. An dieser Stelle muß mittels sicherheitstechnischer Verfahren und Protokolle eine Lösung gefunden werden.

Das veränderte Angreifermodell bringt natürlich die Notwendigkeit mit sich, die gemachten Aussagen zum Schutz der Verkehrsdaten noch einmal zu überprüfen und wo sich durch die neue Situation Änderungen ergeben, diese darzulegen. Grundlage bei allen bisherigen Betrachtungen war der Artikel [Pfit93], in dem prinzipielle Vorschläge zum Datenschutz in Funknetzen gemacht werden. Das darin vorgestellte Verfahren ist eine aufgrund der Bedingungen bei Funknetzen (begrenzte Übertragungsbandbreite; mögliche Identifikation und Peilung) abgewandelte Variante der Telefon-MIXe [PfPW89].

Das Verfahren und die dazu gemachten Aussagen können auch beim geänderten Angreifermodell vollständig weiterbenutzt werden. Vereinfachungen ergeben sich jedoch bei der Verschlüsselung zwischen mobiler und ortsfester Teilnehmerstation. Auf der Funkstrecke wird sie im wesentlichen schon durch die Anwendung der direkten Spreizung realisiert (Schutz der Inhaltsdaten durch Verwendung des PN-Codes). Wenn das Empfangsspektrum, wie in Kapitel 6.2 vorgeschlagen, bis zur ortsfesten Teilnehmerstation des „Adressaten" verteilt wird, sind dann keine zusätzlichen Schutzmaßnahmen mehr notwendig.

Weiterhin können ab jetzt alle Angreifer außerhalb des Kommunikationsnetzes von den Betrachtungen bezüglich Peilung ausgenommen werden. Ihnen wird wegen der Unkenntnis des PN-Codes eine Ortsbestimmung des Senders durch Peilung der von ihm ausgestrahlten elektromagnetischen Wellen unmöglich gemacht. Sie als einzig mögliche Angreifer anzusehen ist aber wahrscheinlich eine zu schwache Forderung, denn alle Angriffe, die bisher über das Netz oder vom Netz ausgehend möglich waren, sind dies auch jetzt noch.

Die wichtigste Veränderung aufgrund des neuen Angreifermodells ist damit die Möglichkeit, die Betrachtungen zur Peilung auf das Kommunikationsnetz einzuschränken. Um den vollständigen Schutz des Standortes eines Senders zu gewährleisten, müssen Mittel gefunden werden, die eine Peilung durch das Netz unmöglich machen. Aus sicherheitstechnischer Sicht scheint die Suche nach Verhinderung der Peilung für das Kommunikationsnetz allerdings weniger erfolgversprechend, als die Forderung, nur mit vertrauenswürdigen Partnern zu kommunizieren, die eine gewonnene Ortsinformation nicht oder nur in einem vom Sender gewünschten Sinne weitergeben. Das hört sich zunächst nach einer starken Einschränkung der Kommunikationsmöglichkeiten an. Für die Realisierung sollen hier zwei Möglichkeiten vorgestellt werden:

6.1 Informationstechnische Kapselung der Stationen

Die direkte Spreizung des Signals zur Verhinderung der Peilung ist nur auf dem Funkweg notwendig. Die Entspreizung des Signals kann also prinzipiell schon im Empfangsturm der Basisstation (*base transceiver station* BTS) vorgenommen werden. Dazu muß der PN-Code dort bekannt sein. Durch die Kenntnis des PN-Codes hat die BTS aber die Möglichkeit zur Peilung. Die Grundidee der informationstechnischen Kapselung besteht nun darin, die BTS aus sicherheitstechnischer Sicht vertrauenswürdig zu konstruieren. Das bedeutet, die BTS haben zwar die Möglichkeit zur Peilung, geben diese Information aber nicht weiter bzw. ermitteln sie gar nicht erst (Bild 6). Das Einbringen eines trojanischen Pferdes in eine solche BTS könnte diese Maßnahme gefährden. Der Vorteil von BTS gegenüber gewöhnlichen Vermittlungsrechnern ist aber ihre geringere Komplexität einserseits und die starke Hardwareabhängigkeit der Peilung andererseits. Die Untersuchung der BTS auf derartige Sicherheitslücken und die Erkennung von Manipulationen sollte deshalb einfacher möglich sein. Um den BTS den Status eines vertrauenswürdigen Partners zuerkennen zu können, muß deren informationstechnische Kapselung bezüglich der Ortsinformationen natürlich nachgewiesen sein. Weitere Bemerkungen zu Kriterien, Eigenschaften und Realisierungsmöglichkeiten der Kapselung von IT-Komponenten finden sich in [WaPf87].

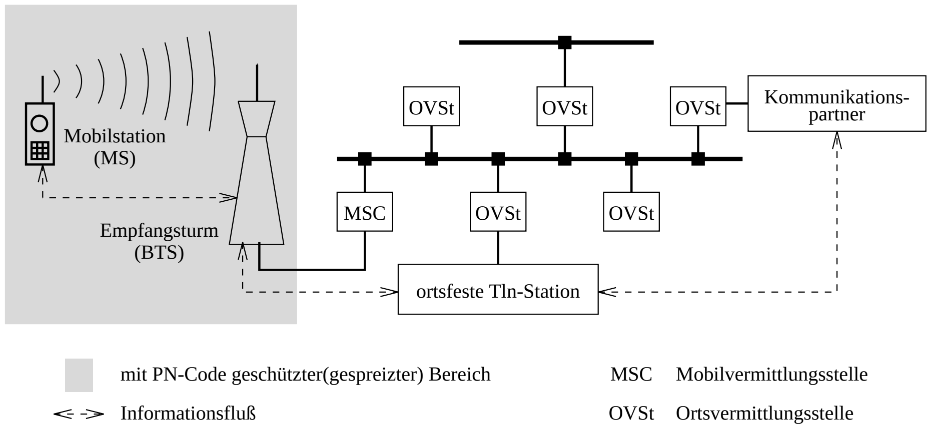

Abbildung 6: Informationstechnische Kapselung der BTS

6.2 Verlagerung der Detektionsfunktion an eine vertrauenswürdige Stelle

Eine Verlagerung der Detektionsfunktion bedeutet, daß das an einem Empfänger vorhandene Signalgemisch aus bandgespreizten Signalen, Rauschen und Störsignalen unverändert, also in gespreizter Form mit der vollen Bandbreite, zu einer entfernten Station gelangt. Dort ist der zur Spreizung verwendete PN-Code bekannt, und so ist nur diese Station in der Lage, das gewünschte Signal zu entspreizen. Diese für den Sender vertrauenswürdige Station kann z.B. seine ortsfeste Teilnehmerstation mit Festnetzanbindung sein (Bild 7). Der gewünschte Frequenzbereich wird dazu vom Empfangsturm des Funknetzes aus über das Festnetz an diese Station weitergeleitet. Dabei ergeben sich einige Probleme, die im folgenden näher beleuchtet werden sollen.

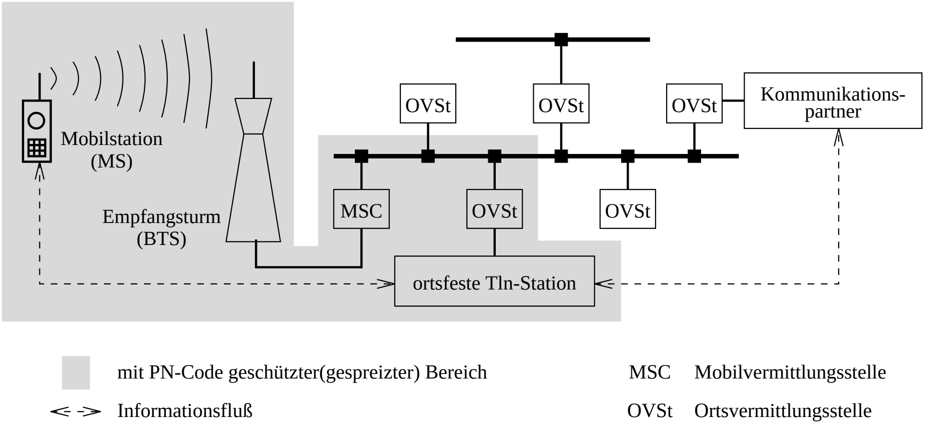

Abbildung 7: Verlagerung der Detektionsfunktion in die ortsfeste Teilnehmerstation

6.2.1 Bandbreite

Das erste und offensichtlichste ist der Bandbreitebedarf im Festnetz, der notwendig ist, um die elektromagnetische Information in unveränderter Form an die jeweiligen ortsfesten Teilnehmerstationen zu verteilen. Die notwendige Bandbreite errechnet sich aus der Bandbreite des zu übertragenden Signals multipliziert mit dem Spreizfaktor. Der Spreizfaktor ist von verschiedenen Faktoren wie der Sendeleistung, dem Signal/Rausch-Verhältnis nach der Spreizung und der damit in Zusammenhang stehenden Erkennungswahrscheinlichkeit des Signals abhängig. Für ihn können deshalb ohne Kenntnis oder Festlegung dieser Unbekannten keine konkreten Werte angegeben werden. Sie ergeben sich aber beim konkreten Entwurf eines Systems neben den vorgegebenen Begrenzungen und geforderten Parametern durch eine Optimierung zwischen der mit zunehmenden Sicherheitsanforderungen steigenden Bandbreite (→ größerer Spreizfaktor) und den daraus resultierenden Kosten für die Übertragung im ortsfesten Netz.

In der Literatur ([PiSM82],[SoFi92]) werden für den Spreizfaktor Werte zwischen 20dB (100) und 30dB (1000) angegeben. Für einen GSM-Kanal von 22,8 kBit/s beispielsweise würde sich im gespreizten Zustand somit eine minimal[2] zu übertragende Bandbreite im Festnetz von 2,28 MBit/s bis 22,8 MBit/s ergeben. Das klingt zunächst sehr viel, stellt aber bei den derzeit absehbaren Entwicklungen auf dem Netzmarkt, wo die Vermittlung von hochauflösenden Fernsehprogrammen geplant ist, sicher kein unlösbares Problem dar.

Für die Übertragung des benötigten Frequenzbereiches an die jeweilige ortsfeste Teilnehmerstation gibt es zwei verschiedene Möglichkeiten. Sie kann, wie dies bei derzeitigen Fernsehprogrammen geschieht, an alle ortsfesten Teilnehmerstationen *verteilt* werden. Dazu müssen alle relevanten Frequenzbereiche der einzelnen Empfangstürme zusammenführt werden, um sie dann gemeinsam und gleichzeitig zu allen ortsfesten Teilnehmerstationen zu verteilen. Das Ergebnis wären sehr hohe Bandbreiteanforderungen an das Festnetz im Teilnehmeranschlußbereich, hervorgerufen durch die Vielzahl der Empfangstürme und die so parallel zu verteilende Bandbreite.

Eine zweite, aus Sicht der Netzbelastung im Teilnehmeranschlußbereich günstigere Variante, ist die *Vermittlung* der benötigten Frequenzbereiche. Diese werden von der ortsfesten Teilnehmerstation aus beim jeweiligen Empfangsturm angefordert, und dann auf dem glei-

[2] Minimal deshalb, weil sicherlich noch ein gewisser Aufwand an Verwaltungsdaten hinzukommt.

chen Wege wie bei der Telefonie über Vermittlungsstellen zu den ortsfesten Teilnehmerstationen geliefert. Wenn die Vermittlung der Frequenzbereiche darüberhinaus so erfolgt, daß diese nur einmal über eine Fernstrecke übertragen werden, auch wenn sie in der gleichen Zielvermittlungsstelle öfter benötigt werden, so führt das zusätzlich zu einer Verminderung des Bandbreitebedarfs auf den Fernstrecken.

Eine Verringerung der zu übertragenden Bandbreite des einzelnen Kanals scheint beim verwendeten Verfahren der direkten Spreizung nicht möglich. Dazu wäre eine teilweise Entspreizung des Signals in der BTS notwendig, die nur mittels eines in der Bandbreite reduzierten PN-Codes vorgenommen werden könnte. Dieser PN-Code muß, um seine Funktion korrekt zu erfüllen, zwangsläufig mit dem ursprünglich zur Spreizung verwendeten PN-Code in weiten Teilen korrelieren. Damit erhielte die BTS allerdings wieder Informationen, welche es ihr mittels des in Kapitel 5.2 dargestellten Vorgehens erlauben, den Sender zu peilen.

6.2.2 Auswahl des richtigen Empfangsturms

Bei einer Entspreizung an dezentraler Stelle besteht neben der eigentlichen Übertragung des ungespreizten Signals noch das Problem, daß die Quelle bestimmt werden muß, von der das Signal stammen soll. Diese Information ist mit dem Aufenthaltsgebiet des Senders identisch und darf nur der ortsfesten Teilnehmerstation bekannt sein, um dem Kommunikationsnetz keine Möglichkeit zu geben, an derartige Informationen zu gelangen. Die Verwaltung des Aufenthaltsorts durch die ortsfeste Teilnehmerstation bedeutet aber auch, daß diese die Koordination bei Änderung des Senderstandortes übernehmen muß. Das beinhaltet unter anderem die Nachführung des Empfangsturms, von dem das ungespreizte Signal empfangen werden soll. Hilfreich kann hier die in Kapitel 5 vorgestellte Möglichkeit zur Ortung einer Mobilstation durch die ortsfeste Teilnehmerstation sein.

6.2.3 Verschleiern des Aufenthaltsortes

Die dezentral verwalteten Aufenthaltsinformationen zwingen die ortsfesten Stationen, die ungespreizten Signale des Empfangsturms anzufordern, in dessen Erfassungsgebiet der Sender liegt. Die Analyse dieser Anforderungen eröffnet jedoch eine weitere, wenn auch gröbere Möglichkeit für das Kommunikationsnetz, den Standort des Senders zu bestimmen. Abhilfe könnte hier die *intelligent koordinierte Bestellung der Signale* von mehreren Empfangstürmen schaffen, so daß das Kommunikationsnetz durch Beobachtung der Bestellungen keinen wesentlichen Informationszuwachs erreicht. Der Grenzfall wäre die bereits besprochene Variante der Verteilung der Frequenzbereiche aller Empfangstürme, welche in dieser Beziehung sehr vorteilhaft erscheint. Bei diesen Überlegungen ist allerdings die Erhöhung der notwendigen Übertragungskapazität zur ortsfesten Teilnehmerstation zu beachten, da natürlich alle Signale gleichzeitig dort hingelangen müssen.

Werden die Frequenzbereiche *vermittelt*, besteht aber auch die Möglichkeit, die anfallenden Verkehrsdaten (in diesem Falle insbesondere wer welchen Frequenzbereich anfordert) durch MIXe zu schützen. Der Schutz des Empfängers kann auf die gleiche Weise wie bei der Telefonie im Festnetz geschehen. Vorschläge zu dieser Methode finden sich in [PfPW89] in Kapitel 2.2.3 unter dem Stichwort **anonyme Rückadressen**. Der zusätzliche Aufwand besteht dann nur im Einrichten der MIXe und dem Ausrüsten der ortsfesten Teilnehmerstationen mit einer entsprechenden asymmetrischen Verschlüsselungskapazität. Die Vorteile gegenüber der Verteilung liegen in den geringeren Anforderungen an die Netzkapazität gerade im Teilnehmeranschlußbereich. Als nachteilig ist allerdings die zeitliche Beobachtbarkeit der Kommunikation eines Teilnehmers zu nennen. Sie könnte in diesem Fall durch senden bedeutungsloser Nachrichten, wenn keine bedeutungsvollen zu übertragen sind, sog. *dummy-traffic*, gelöst werden. Ein Senden bedeutungsloser Nachrichten auf der Funkstrecke verbietet sich einerseits aufgrund des dort herrschenden Mangels an Übertragungskapazität. Andererseits ist die Akkukapazität einer Mobilstation zu begrenzt, um ständig zu senden. Es spricht jedoch nichts dagegen, wenn die ortsfeste Teilnehmerstation einen Frequenzbereich bestellt, auch wenn die Mobilstation gar nicht sendet. Das zeitliche Kommunikationsprofil des Teilnehmers kann so verborgen werden. Aus Sicht der Netzbelastung trägt diese Maßnahme nur zu einem Ansteigen der mittleren Anzahl zu vermittelnder Kommunikationswünsche bei und ist so akzeptabler als Verteilung.

7 Verbindungsaufnahme

Der Verbindungsaufbau wird bei Verwendung des Verfahrens der direkten Spreizung zum Schutz vor Peilung stark erschwert, da kein Signal von einer Mobilstation aus ungespreizt gesendet werden darf, vor Beginn der Sendung aber der zu benutzende PN-Code ausgetauscht werden muß. Bei dezentraler Verwaltung der Aufenthaltsinformationen kommt für die ortsfeste Teilnehmerstation die Aufgabe hinzu, den Aufenthaltsort der Mobilstation bei deren Neueinbuchung zu ermitteln. Diese Probleme sollen in den folgenden Abschnitten behandelt werden.

7.1 Austausch der Schlüssel zur Erzeugung des PN-Codes

Entscheidend dabei ist, wer aufgrund eines Kommunikationswunsches die Initiative ergreift. Alle Maßnahmen zum *Verbindungsaufbau vom Festnetz* (bzw. der ortsfesten Station)[3] *zur mobilen Station*, die von Festnetzseite aus initiiert werden (*mobile terminated*), sind dabei relativ unproblematisch. Für sie brauchen keine Maßnahmen zum Schutz vor Peilung angewendet zu werden (die Standorte der Sendetürme sind sowieso bekannt), so daß nur eine einfache Verschlüsselung zwischen Festnetz und mobiler Teilnehmerstation notwendig wird. Der Schutz des Aufenthaltsortes der Mobilstation kann dabei, wie in [Pfit93] vorgeschlagen, durch Verteilung mit entsprechender Filterung unerwünschter Verbindungswünsche erfolgen.

Kritischer ist die Situation, wenn die Kontaktaufnahme *von einer mobilen Station aus mit dem Festnetz* (*mobile originated*) erfolgen soll. In jedem Fall muß die mobile Station, bevor sie senden kann, im Besitz eines Schlüssels (PN-Key) sein.

Das einfachste und eleganteste Verfahren scheint hier das von Rabin vorgeschlagene sogenannte **Leuchtturmprinzip** [Rabi81] zu sein. Die eine Kommunikation wünschenden Partner vereinbaren dabei eine Blockchiffre (BC) und einen nur ihnen bekannten Schlüssel K_i. Ein zentraler, von allen zu empfangender Funksender[4] (Leuchtturm), verteilt laufend Zufallszahlen ZZ (siehe Bild 8). Diese verschlüsseln die Kommunikationspartner unter Zuhilfenahme der Blockchiffre mit dem vereinbarten Schlüssel K_i und erhalten beide so den PN-Key K_{PN}, mit dem die Kommunikation zwischen ihnen geschützt werden soll. Mit einem entsprechenden PN-Code-Generator kann daraus der PN-Code erzeugt werden. Eine

[3] Im folgenden ist unter Festnetz je nach dem Zielort der gespreizten Signale entweder ein Empfangsturm des Funknetzes oder die ortsfeste Teilnehmerstation zu verstehen.

[4] In einem Mobilfunknetz kann diese Aufgabe durch einen speziellen Signalisierungskanal übernommen werden.

abgewandelte Variante des Verfahrens besteht darin, die Zufallszahlen nicht zu verteilen, sondern Uhrzeit und Datum, beruhend auf einer genauen Zeitbasis, als solche zu verwenden.

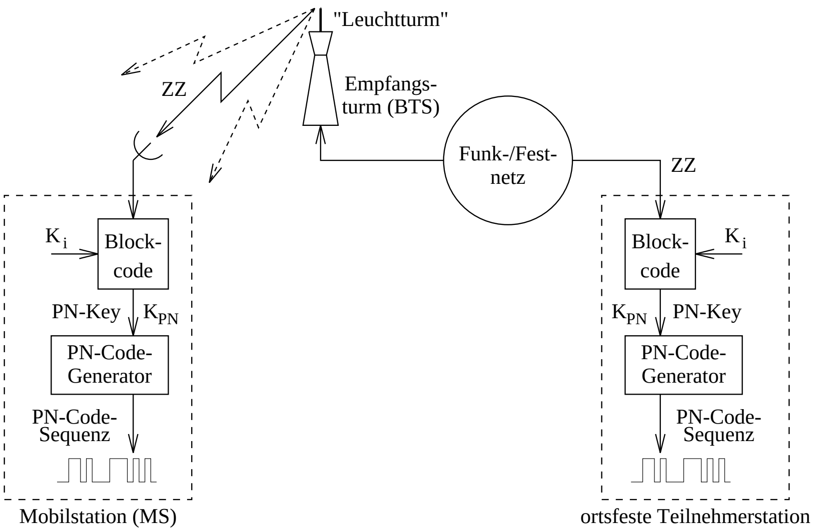

Abbildung 8: Verwendung eines *Leuchtturmes* zur Verteilung von Schlüsseln

Der mobilen Station steht somit zu jedem Zeitpunkt ein Schlüssel zur Verfügung, mit dem sie gespreizt senden kann und der auch dem Festnetz bekannt ist, um es in die Lage zu versetzen, die Sendung wieder entspreizen zu können. Wann welcher Schlüssel verwendet wird und wie lange er gültig sein soll, ist dann eine Vereinbarungsfrage oder Definitionsfrage und kann in Abhängigkeit anderer Faktoren (Synchronisationszeiten usw.) angepaßt werden.

7.2 Ermitteln des Aufenthaltsortes der mobilen Station

Bei Verwaltung der Aufenthaltsinformationen einer Mobilstation in der zugehörigen ortsfesten Teilnehmerstation muß diese auch die Koordination des Informationsflusses von und zur Mobilstation übernehmen. Das beinhaltet sowohl die Weiterleitung von Verbindungswünschen in das momentane Aufenthaltsgebiet der Mobilstation als auch die Bestellung des Frequenzbereiches beim jeweiligen Empfangsturm, um die Kommunikation von der Mobilstation zur ortsfesten Teilnehmerstation zu sichern. Solange die beiden Stationen in Kontakt stehen, kann eine ständige Aktualisierung des Aufenthaltsortes der Mobilstation vorgenommen werden. Reißt dieser Kontakt aus irgendeinem Grund ab, z.B. vollständiges Abschalten der Mobilstation, und bewegt sich die Mobilstation aus ihrem Aufenthaltsgebiet heraus, so erhält die ortsfeste Teilnehmerstation keine Informationen mehr über diese Veränderung. Sie erkennt allerdings, daß die Mobilstation nicht mehr auf ihre Rufe reagiert, kann also diesen Zustand gesondert behandeln.

Eine Möglichkeit, den aktuellen Standort zu ermitteln, wäre die Einrichtung eines Sonderkanals, der im gesamten Festnetz (→ an alle ortsfesten Teilnehmerstationen) verteilt wird. Auf ihm könnten alle Mobilstationen, die im Moment keine Verbindung zu ihren ortsfesten Teilnehmerstationen mehr haben, eine kurze Nachricht mit dem derzeitigen Aufenthaltsort an diese schicken. Die ortsfeste Teilnehmerstation kann daraufhin die Ortsinformationen auf den neuesten Stand bringen und ihre Aktivitäten auf dieses neue Gebiet richten. Die Sendung auf dem Sonderkanal muß natürlich in gespreizter Form erfolgen. Der Kanal kann aber im Zeitmultiplex von mehreren Stationen genutzt werden, so daß die

Netzbelastung durch die Verteilung an alle ortsfesten Teilnehmerstationen gering gehalten wird.

8 Zusammenfassung und Bewertung

In den vorangegangenen Abschnitten wurde ein prinzipielles Modell entwickelt, bei dem unter Ausnutzung eines Geheimnisses das „Verbergen“ elektromagnetischer Wellen und damit die unbeobachtbare Kommunikation zwischen Sender und Empfänger realisierbar scheint.

Die vorliegende Arbeit suchte in erster Linie nach einer Möglichkeit zur Verhinderung der Ortung von sendenden Mobilstationen. Dabei ging es um das Finden und Untersuchen prinzipieller Verfahren und weniger vordergründig um die direkte Umsetzbarkeit in bestehenden Netzen. Das gefundene Verfahren der direkten Spreizung bietet neben der geforderten Nichtortbarkeit der Mobilstationen als einen weiteren Schritt zur Vervollkommnung des Schutzes der Verkehrsdaten auch andere Vorteile. Die gute Selbstortungsmöglichkeit im Notfall (siehe Kap. 5) beispielsweise ist ein wesentlicher Punkt auf dem Weg zum dezentralen Erreichbarkeitsmanagement. Weiterhin macht die vorgeschlagene dezentrale Verwaltung der Erreichbarkeitsinformationen deren Speicherung im HLR/VLR (*home location register/ visitor location register*) überflüssig, womit diese Datenbanken als Unsicherheitsfaktor beim Schutz von Verkehrsdaten wegfallen. Die Konzeption zielt also im wesentlichen darauf ab, das Netz als ein abstraktes Transportmedium zu betrachten, das vom Betreiber bereitgestellt wird, ohne daß dieser Einfluß oder Zugriff auf die darauf transportierten Daten hat. Die Organisation des Erreichbarkeitsmanagements und der Ablaufsteuerung übernimmt dann die ortsfeste Teilnehmerstation in Zusammenarbeit mit der zugehörigen mobilen.

All diese Möglichkeiten lassen sich jedoch, wie bereits erwähnt, nicht ohne Probleme in derzeit existierende Netzkonzepte integrieren. Zunächst ist aufgrund der Bandbreiteanforderungen beim Einsatz der direkten Spreizung auf der Funkstrecke ein vollständiger Umbau der Multiplexgestaltung der Kanäle hin zum Codemultiplex erforderlich. Die Anzahl gleichzeitig arbeitender Nutzer bei synchronen Betrieb ist nach [PiSM82] allerdings bei den unterschiedlichen Multiplexverfahren gleich groß, so daß ein vorgegebener Frequenzbereich mit der gleichen Effektivität ausgenutzt wird.

Bei einer Verlagerung der Detektionsfunktion an eine vertrauenswürdige Stelle kommt es zusätzlich zu Kapazitätsengpässen im Festnetzbereich. Im momentanen Ausbauzustand des Netzes ist diese Methode deshalb nicht realisierbar. Die Ursache hierfür ist aber weniger das Vorhandensein natürlicher Begrenzungen als mehr die Kosten, die ein entsprechender Ausbau des Festnetzes mit der derzeitigen Technologie verursachen würde. Notwendig wäre nämlich nicht nur eine hohe Kapazität zwischen den Vermittlungsstellen, sondern auch eine Breitbandverkabelung im Teilnehmeranschlußbereich.

Die Einführung einer ortsfesten Teilnehmerstation als koordinierendes System scheint in diesen Zusammenhang weniger problematisch, da innerhalb der natürlichen Erneuerungsperiode von ortsfesten Telefonen ein Umstieg auf ein integriertes System Telefon/ortsfeste Teilnehmerstation ohne weiteres möglich sein sollte.

Die Integration der vorgestellten Möglichkeiten zur Realisierung der technischen Datenschutzforderungen wird also wahrscheinlich eine Kostenfrage sein. Der hohe Aufwand für den Schutz der Verkehrsdaten im Vergleich zum Schutz der Inhaltsdaten sollte aber nicht zu dem Schluß führen, daß man sich einen Schutz der Verkehrsdaten nicht leisten kann. Bei der derzeitigen stürmischen Entwicklung gerade auf dem Netzsektor ist es von entscheidender Bedeutung, schon sehr frühzeitig im Entwurfsstadium solche, zur Zeit nicht realisierbar erscheinende Ideen und Vorschläge in zukünftige Konzeptionen einzubringen. Es könnte sonst passieren, daß die Forderung nach entsprechenden Maßnahmen die technische Entwicklung überholt. Weitere Arbeiten auf diesem Gebiet sollten also Möglichkeiten der Realisierung des schrittweisen Übergangs zu der vorgestellten Konzeption bei im Moment in der Planung befindlichen Netzen überprüfen. Das derzeit noch vorhandene, und bei solchen Überlegungen meist hinderliche Mißverhältnis von Schutzbedarf und Schutzbedürfnis muß durch eine Sensibilisierung der Nutzer für Fragen des Datenschutzes ausgeglichen werden.

Wir danken Prof. Dr. Andreas Pfitzmann und Dr. Herbert Klimant für die Anregungen, die sie uns bei der Bearbeitung der Problematik gaben. Weiter danken wir der Gottlieb Daimler- und Karl Benz- Stiftung Ladenburg für die freundliche Unterstützung.

Eine ausführlichere Beschreibung der Zusammmenhänge zur Peilung und Ortung sowie Bewertung verschiedener Spreiztechniken ist in [Thees94] zu finden und kann bei den Autoren angefordert werden.

Literatur

[Dixo84] Dixon, Robert C.: *Spread Spectrum Systems.* John Wiley & Sons, New York 1984

[PfPW89] Pfitzmann, A.; Pfitzmann B.; Waidner M.: *Telefon-MIXe: Schutz der Vermittlungsdaten für zwei 64-kbit/s-Duplexkanäle über den (2*64+16)-kbit/s-Teilnehmeranschluß.* Datenschutz und Datensicherung (1989) № 12 pp.605-622

[Pfit93] Pfitzmann, Andreas: *Technischer Datenschutz in öffentlichen Funknetzen.* Datenschutz und Datensicherung (1993) № 8 pp.451-463

[PiSM82] Pickholtz, Raymond L.; Schilling, Donald L.; Milstein, Laurence B.: *Theory of Spread-Spectrum Communications - A Tutorial.* IEEE Transactions on Communications (1982) volume 30 № 5 pp.855-878

[Rabi81] Rabin, Michael O.: *Transaction Protection by Beacons.* Technical Report TR-29-81, November 1981, veröffentlicht in: Journal of Computer and System Sciences (1983) № 27 pp.256-267

[SoFi92] Sonnenschein, Alexander; Fishman, Philip M.: *Radiometric Detection of Spread-Spectrum Signals in Noise of Uncertain Power.* IEEE Transactions on Aerospace and Electronic Systems (1992) volume 28 issue 3 pp.654-660

[Thees94] Thees, Jürgen: *Konkretisierung der Methoden zum Schutz von Verkehrsdaten in Funknetzen.* Diplomarbeit, TU Dresden, Inst. Theoretische Informatik, 1994

[WaPf87] Waidner, Michael; Pfitzmann, Birgit: *Anonyme und verlusttolerante elektronische Brieftaschen.* Universität Karlsruhe, Fakultät für Informatik, Institut für Rechnerentwurf und Fehlertoleranz, Interner Bericht 1/87