Königsbach-Stein, im Juni 1997

Standards kommerzieller mobiler Funknetze - Eine Übersicht

Dipl.-Ing. Erich H. Franke, DK6II
Lenaustraße 20
D-75203 Königsbach-Stein 2
FAX: 07232-1647
Dk6ii@afusoft.de

Skriptum zum Vortrag anläßlich der 42. UKW-Tagung in Weinheim

DECT, GSM, TETRA, GPS, MODACOM und INMARSAT. Ob terrestrisch oder satellitengestützt, digitale Kommunikations-, Navigations- und Funkmeldesysteme sind in aller Munde. Der Bedarf an mobiler Sprach- und Datenkommunikation hat zusammen mit dem rasanten Fortschritt in der Miniaturisierung komplexer analoger und digitaler Komponenten diese Entwicklung möglich gemacht. Ein Übriges hierzu trägt die internationale Standardisierung bei. Wie sind diese Standards zustandegekommen? Wie funktionieren die Systeme prinzipiell? Diese Fragen sind nicht immer ganz einfach zu beantworten. Der folgende Beitrag will helfen, ein wenig Licht in das Dunkel zu bringen.

1 Einführung

In den vergangenen Jahren hat sich das Gesicht des ehemaligen 'öffentlichen' und 'nicht-öffentlichen, beweglichen Landfunkdienstes' (öBL, nöBL) entscheidend verändert.

Zu diesen Diensten zählte man beispielsweise das 'klassische' Autotelefon, die Funkdienste von Polizei und Feuerwehr bis hin zu Funkrufsystemen, die man heute gemeinhin unter dem Begriff 'Pager' kennt. Der Oldtimer 'Eurosignal' gehört in diese Kategorie.

Jahrzehntelang wurden diese Mobilfunk-Dienste praktisch ausschließlich von analog arbeitenden Funkübertragungssystemen beherrscht. Der Trend bei neuen Systemen geht jedoch eindeutig zur digitalen Übertragungstechnik.

Als Relikte der analogen Ära existieren heute auf diesem Gebiet nur noch der VHF- und UHF-Amateurfunk, sowie die sogenannten Behörden und Organisationen mit Sicherheitsaufgaben (BOS), also beispielsweise Polizei, Feuerwehren und Rettungsdienste, die nach wie vor offene, unverschlüsselte und damit für jedermann zugängliche Übertragungsverfahren benutzen.

Im folgenden wollen wir uns einzelne ausgewählte Dienste der digitalen Fraktion in ihren technischen Parametern näher betrachten. Wir werden ebenfalls deren Vor- und Nachteile, sowie die Grenzen und Risiken der Digitalisierung analysieren.

Wir wollen überdies ein klein wenig die möglichen Auswirkungen dieser digitalen Technologien auf den Amateurfunk streifen, da diese inzwischen fast ausschließlich auf international wirksamen Standards beruhen.

Ich denke, es ist nur noch eine Frage der Zeit, bis wir beispielsweise die erste Amateurfunk-Relaisstelle auf Basis des DECT-Standards haben werden. Nur so zum Versuch. Wir sind doch schließlich noch immer ein experimenteller Funkdienst. Also Leute! Wer macht mit?

2 Systeme, die in Frage kommen

Im nun folgenden Text wollen wir beispielhaft die digitalen Mobiltelefon-Systeme **DCS-1800** und **GSM**, die in Deutschland in den Netzen E-Plus, D1 und D2 von privaten Providern betrieben werden, betrachten und gegen deren ältere, zumeist analog arbeitenden Schwestern B und C der ehemaligen Deutschen Bundespost stellen.

Interessant sind darüberhinaus die Standards moderner schnurloser Telefone für den Privatbereich (**CTx**), bei denen im Augenblick allerdings nur noch der europäische **DECT**-Standard eine Rolle spielt.

Als modernster Vertreter des privaten Funkbereiches (Taxi, Fuhrunternehmen) gilt heute, also 1997, der digitale Bündelfunk mit dem in Entstehung befindlichen Standard **TETRA**.

Zur Abrundung wollen wir uns noch Funkruf-Systeme (Pager) am Beispiel der Standards **ERMES** und **POCSAC** ansehen. Ein System der letztgenannten Art ist in Deutschland unter dem Namen Cityruf bekannt.

3 Grundlegende Fragen der Digitalisierung

Wie so häufig, hatte die stürmische Verbreitung digitaler Funkübertragungssysteme rein kommerzielle und ökonomische Gründe. Fast könnte man sagen, daß es gerade die Privatisierung dieser Dienste war, die die Entwicklung deutlich vorangetrieben hat. Vielleicht ist es eine gewagte Theorie, doch es scheint, daß die Digitalisierung der Mobiltelefon-Netze (Beispiel GSM) und des Bündelfunks (Beispiel TETRA) einen weitaus höheren Stellenwert hatte wie beispielsweise die der Funknetze der Polizei, obgleich diese Nutzer eigentlich einen deutlichen Bedarf an Übertragungssicherheit haben müßten.

Nun, hier haben vermutlich die leeren öffentlichen Kassen die Prioritäten entscheidend beeinflußt. Doch wieder zurück zur Technik.

Einer der zentralen Gründe der Digitalisierung kommerzieller Netze lag sicherlich in der **Gebührenerfassung**. Genauer gesagt, im **Zugriffsschutz**. Ziel ist es, nur befugten Teilnehmern den Zugriff auf das System zu ermöglichen, also in der Regel denen, die ihre Gebühren bezahlt haben. Man spricht hierbei auch von **Authentisierung**.

Digitale Funksysteme lassen sich wesentlich leichter gegen unbefugte Benutzung schützen als ihre analogen Schwestern. Wie wir alle wissen, genügt lediglich die Kenntnis der Ein- und Ausgabefrequenzen einer Amateur-Relaisfunkstelle, um über diese Funkverkehr abzuwickeln. Und wie zahlreiche Relaisbenutzer aus leidvoller Erfahrung berichten können, gehört nicht viel Verstand dazu, den Betrieb einer derartigen Relaisfunkstelle zu stören.

Über die Verhältnisse bei den nicht-öffentlichen Diensten der Polizei oder Feuerwehren möchte ich an dieser Stelle aus begreiflichen Gründen überhaupt nicht eingehen. Sie sind an anderer Stelle aussagekräftig beschrieben, z.B. in [DigPol].

Denkt man weiterhin an die Zeiten der veralteten analogen 'Autotelefon'-Netze B oder gar A zurück, so erinnert man sich vielleicht an die unzähligen Fälle des Mißbrauchs.

Im B-Netz genügten beispielsweise neben der Sende- und Empfangseinrichtung lediglich elementare Kenntnisse der analog gestalteten 'Zutrittsprozedur', um an diesem Dienst teilnehmen zu können.

Will man Presseberichte Glauben schenken, so scheint auch der halb-digitale C-Netz-Standard auf seiner Funkschnittstelle nicht sicher vor unbefugter Verwendung./1/

Gleiches gilt beispielsweise für den US-amerikanischen Mobiltelefon-Standard AMPS, dessen Schutz lediglich aus 'geheimen' Tonsignalisierungen besteht. Der zweite Schutz liegt beim amerikanischen Gesetzgeber, der in den USA den Handel mit Scanner-Empfängern verbietet, die auf den 'Cellular'-Frequenzen (900 MHz-Bereich) empfangsbereit sind. Ein wahrlich wirksamer Schutz, oder?

Erst die rein digital arbeitenden Mobilfunknetze, wie GSM (in Deutschland D-Netz) oder DCS-1800 (in Deutschland E-Netz) gelten was ihre 'Luftschnittstelle' betrifft, zumindest im Jahre 1997 als einigermaßen sicher gegen Mißbrauch.

Bei GSM sorgt ein mehrstufiges voll digital arbeitendes Verschlüsselungsverfahren dafür, daß nur ein autorisierter Teilnehmer Zugang zu der Überleiteinrichtung (Base-Station) erhält und Telefonverkehr abwickeln kann.

Auch bei der, 1997 noch immer laufenden Verhandlung über den digitalen Bündelfunk-Standard TETRA steht die Gebührenerfassung, das 'Billing' und der Zugriffsschutz als zentrales Thema im Vordergrund.

Bei den Vorläufer-Systemen, beispielsweise dem analog arbeitenden Taxifunk oder den Systemen privater Nutzer ('Kies-Kutscher') wurden die Nutzungsgebühren von der Fernmeldeverwaltung pauschal erhoben, da eine von der Nutzungsdauer abhängige Erfassung schlichtweg nicht möglich war. Lediglich zum Zwecke der Mehrfachnutzung der dafür vorgesehenen Funkkanäle wurde ein analog arbeitendes **Selektivruf**-System, der sogenannte Fünfton-Folgeruf nach CEPT eingesetzt. Hiermit konnten auf einfache Weise Benutzergruppen unterschieden werden. Ein Schutz vor Mißbrauch bestand jedoch keinesfalls.

Auch das im Behördenfunk eingesetzte Funk-Meldesystem FMS benutzt Tonfolgen, die gemäß CEPT standardisiert sind. Auch hierbei bestand (und besteht) kein wesentlicher Schutz gegen mißbräuchliche Verwendung (siehe auch [DigPol]).

Bei TETRA hingegen wird ein als recht sicher geltendes, sogenanntes 'Challenge-Response'-Verfahren zur Authentisierung benutzt, bei dem niemals eine abhörbare Klarinformation über Funk übertragen wird.

Deshalb kann die Authentisierungsinformation auch zum Zwecke der Gebührenerfassung herangezogen werden, denn TETRA wird zeitgemäß sicherlich von privaten Betreibern ('Providern') betrieben werden.

Selbst bei schnurlosen Telefonen hat die Authentisierung inzwischen Einzug gehalten. Bei den alten, meist unzulässig betriebenen 'Cordless Phones' aus Importquellen war es durchaus nicht unüblich, daß sich der Nachbar mit seinem gleichermaßen unzulässigen 'Schnurlosen' zufällig oder absichtlich am heimischen Telefonaufkommen beteiligen konnte. Das lag an den sehr laxen bzw. nicht vorhandenen Authentisierungsverfahren dieser Billigprodukte.

Bei den standardisierten Systemen wurden mehr und mehr digitale Kennungen eingeführt, die jedoch noch immer nicht 'fälschungssicher' waren. Durch Eingriffe in die Software der Handsets und Kenntnis der 24-Bit-Kennung, die meist sogar auf dem Typenschild der Basisstation aufgedruckt war, konnte das System noch immer umgangen werden.

Beim DECT-Standard hingegen wird ein sehr aufwendiges Authentisierungsverfahren zum Zeitpunkt der Erstinbetriebnahme verwendet, das recht sicher ist, da es auf einer willkürlich auszuführenden 'Initialisierungssequenz' beruht.

Wer's genauer wissen will, der lese die Bedienungsanleitung seines DECT-Telefones und suche nach Themen wie 'Einbuchen eines Zweithörers' oder ähnlich. Für den weniger technisch orientierten Benutzer wird diese Erstinitialisierung erfreulicherweise meist vom Gerätehersteller selbst durchgeführt und braucht vom Normalbenutzer während der Lebensdauer der Geräte nicht wiederholt zu werden.

Ähnliche Überlegungen wie für den Schutz gegen mißbräuchliche Benutzung gelten auch für das unerlaubte **Abhören** dieser Systeme. Hieran haben vor allem die Nutzer ein Interesse. Die Diensteanbieter kommerzieller Systeme müssen jedoch alleine aus Wettbewerbsgründen eine geeignete Verschlüsselung anbieten, um nicht potentielle Kunden an die verschlüsselnde Konkurrenz zu verlieren.

Analog arbeitende Funkübertragungssysteme lassen sich jedoch nur ungenügend gegen unbefugte Lauscher absichern. Den Versuchen, mit analogen Methoden eine **Verschleierung** der Nutzinformation, mithin also der übertragenen Sprachinformation zu erzielen, sind naturgemäß enge Grenzen gezogen.

Der klassische Vetreter hierfür ist das sogenannte 'Inversband-Verfahren'. Dabei wird eine für Funkamateure wohlbekannte Art der Einseitenband-Auf- und Abbereitung nach der Filter-Methode verwendet, um im analogen Sprachbereich 300 Hz bis 3400 Hz die spektrale Energieverteilung umzukehren.

Der Lauscher hört mit unbewaffnetem Ohr also quasi das falsche Seitenband. Ein zweiter, gleichartiger Inverter macht dabei die Umkehrung wieder rückgängig. Man sagt, daß geübte Lauscher die so verschleierte Sprachinvertierung auch ohne Decoder aufnehmen könnten.

Will man dem Fernsehen Glauben schenken, so arbeitete früher die Polizei mit einer derartigen Verschleierung [Isar]. Tatsache ist, daß das C-Netz eine ähnliche Technik als Abhörschutz benutzt. Wer's genauer wissen will, der lese die 'gelben Seiten' einschlägiger Fachzeitschriften wie der cqDl.

Bei den schnurlosen Telefonen liegen die Verhältnisse zum Teil noch extremer. Die meisten der älteren, in Deutschland nicht zugelassenen schnurlosen Telefone besitzen überhaupt keine Sprachverschlüsselung. Das selbe gilt für die älteren zugelassenen Systeme, die am oberen Ende des 800 MHz-Bereiches arbeiten. Die Sprache wird hierbei in analoger Frequenzmodulation übertragen und der einzige Schutz gegen unbefugtes Abhören besteht in einem mehr oder minder seltenen Frequenzwechsel. Im Zeitalter frei erwerbbarer Scanner-Empfänger ein wahrlich minderwertiger Schutz.

Wesentlich betriebssicherer sind digital arbeitende **Verschlüsselungsverfahren**, beispielsweise auf Basis von Pseudo-Zufallsfolgen, wie sie beispielsweise für die Nachrichtenverschlüsselung bei GSM, TETRA und DECT verwendet werden.

Ich würde hier die Aussage wagen, daß unter Berücksichtigung der dort benutzten Schlüssellängen ein Abhören für das breite Publikum mit vertretbarem Aufwand nicht mehr möglich ist. Anderes könnte vielleicht für Personengruppen gelten, für die vielzitierte 'vertretbare Aufwand' keine Rolle spielt. Auf diese Thematik wollen wir an dieser Stelle jedoch nicht näher eingehen.

Ein weiterer, kommerzieller, beziehungsweise wettbewerbstechnischer Grund hat die Digitalisierung noch weiter vorangetrieben. Es handelt sich um die Integration von Sprache und Daten.

In früheren Systemen spielte die mobile Datenübertragung meist nur eine nachrangige Rolle. Dies war zumindest in zivil genutzten Systemen der Fall. Die

Polizei benutzte zwar bereits recht früh mobile Datenterminals, diese arbeiteten jedoch mit analogen Modems, um die Kompatibilität mit den analogen Polizeifunkgeräten zu ermöglichen.

Heute ist die Datenübertragung für viele Mobiltelefonbesitzer bereits zum Standard geworden. Auch bei dem Bündelfunk, beispielsweise TETRA ist die Fähigkeit zur Datenübertragung fest verankert und wird beispielsweise im Flottenmanagement benutzt.

Selbst an den schnurlosen Telefonen im Heimbereich ist die Datenübertragung nicht vorbeigegangen. Inzwischen werden auf DECT basierende LAN-Systeme angeboten, die beispielsweise zur portablen Lagerbestandserfassung verwendet werden.

4 Diskussion der einzelnen Systeme

4.1 Mobiltelefon-Netze

4.1.1 C-Netz

Das C-Netz soll hier nur am Rande gestreift werden, handelt es sich hierbei um ein 'halb-digitales' Netz. Es handelt sich um ein rein nationales Mobiltelefon-Netz, das im Gegensatz zu GSM-Netzen (D-Netze in Deutschland) nicht auf internationalen Standards beruht. Daher werden die Systemkomponenten auch mit interessanten deutschsprachigen Abkürzungen bezeichnet. Als Beispiel soll 'FuFSt' für 'Funk-Feststation' dienen, was der 'Base-Station' bei GSM entspricht.

Nichts desto trotz ist es in Deutschland flächendekend ausgebaut und versorgt ca. 1 Million Teilnehmer.

Das System nutzt 287 Duplex-Kanäle im 70cm-Band. Die Verbindung vom Mobilteilnehmer zur 'FuFSt', also der 'Uplink' benutzt Frequenzen zwischen 451 und 455,74 MHz. Der Downlink arbeitet auf 461 bis 465,74 MHz, jeweils im 20 kHz-Kanalraster. Der Weichenabstand, d.h. die Frequenzdifferenz zusammengehörender Kanäle beträgt 10 MHz.

Die Funktelefone dürfen Leistungen bis zu 20 Watt aussenden.

Wir haben das C-Netz als 'halb-digital' bezeichnet, denn nur die Signalisierungsinformation wird digital übertragen. Die Sprachinformation wird analog in Phasenmodulation mit 4 kHz Hub ausgesendet.

Die Datenübertragung erfolgt in FSK mit einem Hub von ±5 kHz und einer Bitrate von ca. 5,28 kBit/s.

Im Ruhezustand, d.h. ohne laufendes Gespräch wird ein synchrones Zeitschlitzverfahren mit einer Gesamtrahmenlänge von 2,4 Sekunden angewandt. Alle Basisstationen (FuFSt) werden streng synchron betrieben. Dabei werden alle Teilnehmer in regelmäßigen Zeitabständen abgefragt. Die Antwortsendungen werden dazu herangezogen, den Standort der Teilnehmergeräte mittels Hyperbelortungsverfahren zu bestimmen. Auf diese Weise wird diejenige FuFSt zur Überleitung bestimmt, die dem Mobilteilnehmer am nächsten ist, in der Hoffnung, die Funkverbindung zu optimieren. Manchmal klappt das sogar.

Die Übertragung der Steuerdaten erfolgt blockweise in Blöcken zu jeweils 37,5 ms, entsprechend 198 Bit. Von diesen werden jeweils sieben zu Beginn und am Ende des Blockes als Schutzzeit freigehalten, so daß eine effektive Datenblocklänge von 184 Bit übrig bleibt. Effektiv übertragen werden allerdings nur 70 Bit (acht Mal 8 Bit plus ein Mal 6 Bit). Der Rest dient der Synchronisation und Redundanz.

Auch während der Übertragungsphase werden digitale Signalisierungen ausgetauscht. Zu diesem Zweck wird die Sprache analog komprimiert. Hierdurch entstehen alle 12,5 ms Lücken von ca. 1,136 ms, in die vier Datenbit eingeblendet werden. Diese Datenbit werden gesammelt, bis nach 46 dieser 12,5 ms-Blöken ein Datenrahmen von 184 Bit aufgenommen werden kann.

4.1.2 GSM

GSM ist das im Moment weltweit wohl am weitesten verbreitete Mobiltelefonsystem. Der Name stammt ursprünglich von einem frankophonen, europäischen Normengremium, der 'Groupe Speciale Mobile'. Heute verwendet man gerne den Marketing-Anglismus 'Global Standard for Mobile communication'.

Neben den bereits erwähnten Verschlüsselungs- und Authentisierungsverfahren liegt der größte Vorteil des Systems in seiner internationalen Verfügbarkeit. Mit einem Telefon kann man in zahlreichen Ländern im Prinzip telefonieren, sofern der eigene Provider mit dem jeweiligen Gastland einen sogenannten Roaming-Vertrag abgeschlossen hat und man selbst bereit ist, die zum Teil haarsträubenden Gebühren hierfür zu entrichten.

Auf die Gebührensituation will ich hier erst garnicht eingehen. Ich empfehle hierbei einfach, Kontakt zu einem der zahlreichen Providern aufzunehmen. Man bekommt dort jede Menge Informationen - zumindest als Neukunde.

Schauen wir uns statt dessen lieber die Technik an: 'In

der Luft' benutzt GSM weltweit 124 Duplexkanäle mit einer Bandbreite von jeweils 200 kHz.

Die Uplink-Frequenzen, auf der die Verbindung von den Mobiltelefonen zur Basis-Station läuft liegt zwischen 890 und 915 MHz. Der Downlink, also die Sendefrequenz der Basis-Station liegt zwischen 935 und 960 MHz. Der Weichenabstand beträgt demnach 45 MHz.

Auf jedem Träger wird jeweils ein Zeitmultiplex-Signal mit acht nutzbaren Zeitschlitzen ausgesendet. Die Rahmenlänge beträgt 4,6 ms. Jeder Zeitschlitz ist demnach 577µs lang. Auf jedem Frequenzkanal (Träger) können also bis zu acht Gespräche gleichzeitig abgewickelt werden.

Der Zeitschlitz selbst enthält 148 Bit, die mit einer Rate von 270,833 kBit/s übertragen werden. Wer genauer hinsieht, stellt fest, daß die Rechnung nicht ganz aufgeht. Es bleibt ein Rest von ca. 30,5 µs, der nicht durch übertragene Bits belegt ist. Dieser Zeitabschnitt am Ende des Zeitschlitzes dient als Schutzzeit (Guard Time) und hilft, den im Mobilbetrieb unvermeidlichen Zeit-Jitter aufzufangen.

Auch das Mobilgerät sendet während der Gesprächsphase synchron Bursts aus, wobei der Burst auf dem Uplink gegenüber dem dazugehörenden Zeitschlitz im Downlink um drei Schlitzbreiten hinterherhinkt. Die Basisstation bestimmt also den Takt und der soeben erwähnte Zeitabstand erlaubt es dem Mobilteilnehmer auch bei reflexionsbedingtem Jitter auf das Raster 'aufzuspringen'.

Fügt man nun alle Zeitschlitze mit gleicher Nummer aneinander, so entsteht eine Art von logischem Kanal auf dem die Informationsübertragung stattfinden kann. Pro Träger sind dies bereits acht, und wenn man bedenkt, daß eine Base-Station mehrere Hochfrequenz-Träger aussendet, so erkennt man, daß pro Base-Station 32 oder mehr derartiger 'logischer' Kanäle zur Verfügung stehen können.

Es ist sogar so, daß ein logischer Kanal sich über mehrere HF-Kanäle erstrecken kann. Man spricht dabei von 'Frequency Hopping'. Ähnlich wie bei militärisch genutzten Frequenzsprung-Systemen dient das 'Hopping' hier der Erhöhung der Störresistenz, insbesondere dem Ausgleich von Störungen durch Mehrwegeausbreitung.

Der GSM-Standard definiert verschiedene Arten logischer Kanäle: Signalisierungskanäle (Control Channel, CCH) und Verkehrskanäle (Traffic Channels, TCH). Zu Ersteren gehören beispielsweise die Bakensignale (Broadcast Channel, BCCH) an Hand deren der Mobilteilnehmer eine Base-Station identifizieren kann.

Andere CCH's dienen dem Aufbau von Verbindungen sowie der Sendung von Kurztelegrammen (Short Message Service, SMS). Für die Dauer einer Telefonverbindung werden dynamisch die Verkehrskanäle zugeordnet. Es können also weit mehr Teilnehmer an einer Base-Station eingebucht sein, wie gleichzeitig sprechen können. Bei Überlast-Situationen muß das Teilnehmergerät auf eine andere Base-Station ausweichen.

4.1.3 DCS-1800

Im Gegensatz zu GSM wird das DCS-1800-Telefonsystem auf 1,8 GHz betrieben. In Deutschland sind dies die E-Netze (E2 ist derzeit im Aufbau).

Die Nutzung des höheren Frequenzbereiches hat eine Verringerung der Reichweite des DCS-1800 im Vergleich zu einem vergleichbaren GSM-Netz zur Folge. Als Zellendurchmesser sind 300 m bis ca. 9 km vorgesehen.

Auch DCS-1800 benutzt zwei Frequenzgruppen, 1710-1885 MHz im Uplink und 1805-1880 MHz im Downlink. Es stehen demnach 375 Kanäle im 200 kHz-Raster mit einem Weichenabstand von 95 MHz zur Verfügung. Derzeit ist jedoch nur ein Teilbereich für die Nutzung durch E-Plus (E1) freigegeben.

Als Sendeleistung der Mobilgeräte wurde 1 Watt vorgesehen. Sie kann bedarfsweise bis auf ca. 20 mW reduziert werden.

Wie bei GSM wird als Modulationsart GMSK verwendet.

4.2 Bündelfunk-Systeme

4.2.1 TETRA

Das Trans European Trunked Radio System, kurz TETRA genannt stellt ein sogenanntes 'Bündelfunk-System' dar.

Seine Aufgabe soll sein, die Frequenzökonomie bei privaten Mobilfunkstellen des 'öffentlichen Landfunks' (öBL), also beim Taxifunk, Transportunternehmen und ähnlichen Nutzern zu erhöhen, die sich bislang die Funkkanäle durch Nutzung analoger Selektivrufsysteme teilten.

Wie jeder weiß, mußte jede Benutzergruppe eine

eigene Funkzentrale unterhalten, mit Sendern, Antennen etc. Entsprechend war die Reichweite dieser Systeme auf die VHF-Reichweite begrenzt. In früherer Zeit wurden viele Amateurfunkgeräte aus dem Bestand ehemaliger öBL-Geräte rekrutiert (z.B. BOSCH KF-T 166)

Bei TETRA geht man nun einen völlig anderen Weg [Tetra]. Anstatt daß jede Nutzergruppe eine eigene Funkzentrale unterhält, werden bundes- bzw. europaweit sogenannte Basis-Stationen aufgestellt, die über öffentliche Netze (z.B. ISDN) zugänglich sind.

Die Base-Stations und die Netzzugänge werden von Diensteanbietern (Service Providern) verwaltet, ähnlich wie beim Mobiltelefon-Dienst.

Im Gegensatz zum klassischen Mobiltelefon ist jedoch die Betriebsweise dem Funkverkehr ähnlicher. Auch die Gebührenstruktur ist anders, so daß gerade für lokal operierende Unternehmen (Taxen o.ä.) diese Bündelfunk-Systeme gegenüber dem Autotelefon 'rechnen'.

In jüngster Zeit ist TETRA auch als möglicher Kandidat für die Ablösung des Polizeifunks im Gespräch. Als offener, europäischer Standard scheint er gerade im Europa der offenen Grenzen adäquat (Siehe dazu auch TETRAPOL).

Nun, wie funktioniert das Ganze? Zunächst muß sich ein potentieller Teilnehmer an einer Base-Station einbuchen. Um die notwendige Sicherheit gegen Mißbrauch zu gewährleisten, wird ein sogenanntes Challenge-Response-Verfahren benutzt. Hierzu sendet die Base-Station ein zufällig generiertes Datenwort aus. Der Mobilteilnehmer antwortet mit dem verschlüsselten Text.

Die Base-Station verschlüsselt ebenfalls das Datenwort und vergleicht das eigene mit dem, welches sie vom Mobilteilnehmer erhalten hat. Nur wenn beide Werte zueinander passen, wird der Zugang freigegeben. Der Vorteil liegt nun darin, daß in der Luft keine für einen Lauscher verwertbare Information vorliegt.

Für die Anmelde- und Nutzungsphase werden insgesamt drei verschiedene Schlüsselsysteme benutzt. Diese können zudem 'over-the-air' ausgetauscht werden (Remote Krypto Management). Für Hacker gibt es also viel Arbeit...

Die Datenübertragung hält sich übrigens an das OSI-7-Schichten-Modell, wobei wie gehabt die Netzwerk-Dienste die Schichten 1 bis 3 beinhalten. Schicht vier bis sieben werden als Endbenutzer-Funktionen betrachtet und können je nach geünschter Funktionalität ausgelegt werden.

À propos, Layer 1: TETRA benutzt zweifrequenz-Duplex für Up- und Downlink mit einem Weichenabstand von 10 MHz bzw. 45 MHz, abhängig vom Frequenzbereich.

Dabei können die Mobilgeräte durchaus auch im Simplex-Betrieb eingesetzt werden (Semi-Duplex, ähnlich Relaisfunkstellen). Dies erlaubt einfache, preisgünstige Endgeräte. Die Base-Station muß vollduplex-fähig sein.

Das Modulationsschema von TETRA ist ausgelegt für Nutzung zwischen ca 150 MHz und 900 MHz. Von CEPT sind drei Frequenzbänder empfohlen worden:

410-420 MHz / 420-430 MHz
450-460 MHz / 460-470 MHz
870-888 MHz / 915-993 MHz

Darüberhinaus wurde Ende 1995 der Bereich 410-420 MHz / 420-430 MHz für Nutzer mit Sicherheitsaufgaben freigegeben.

Der Kanalabstand beträgt 25 kHz. Es kommt pi/4-DQPSK bei 36 kBaud/s Schrittgeschwindigkeit zum Einsatz.

Eine Base-Station muß auf mehreren Frequenzen gleichzeitig senden können. Einer der Frequenzen istr fest als Organisationskanal zugeordnet.

Auf allen HF-Trägern wird in TDMA gearbeitet. Jeder TDMA-Rahmen enthält vier Zeitschlitze zu jeweils 56.67 ms. Jeder ist also ca. 14.167 ms lang und enthält 510 'modulation bits'.

Die TDMA-Rahmen werden in einer 1.02 Sekunden langen Überstruktur von 17 Nutz- und einem Steuerrahmen (control frame) zusammengefaßt. Jeweils sechzig dieser multiframes bilden zusammen einen ca 61.2 Sekunden langen, 60 Multiframes umfassenden, sogenannten 'Hyperframe'.

Die Datenstruktur innerhalb der Rahmen und das zugrunde liegende Datenmodell ist recht komplex und ist in dem entsprechenden Standard beschrieben. Es trägt insbesondere den Ausbreitungseigenschaften und dem Bitfehlermodell der Funkkanäle in dem zugeordneten Frequenzbereich Rechnung.

Interessant ist noch, daß innerhalb der TDMA-Frames die zusammengehörende Duplex-Information um zwei Slots verschoben gesendet bzw. empfangen wird. Dies erlaubt wiederum einfache, billige Mobilgeräte, da die Anforderungen an die Umstimmzeit gering gehalten

wird.

TETRA enthält zahlreiche Dienste wie z.B. Gruppenruf, um Quasi-Duplex-Funkgespräche zwichen mehreren Mobilteilnehmern zu ermögliche, ohne daß hierzu allzuviele Resourcen der Basisstation belegt werden. Dies wird dadurch erreicht, daß ja bereits alle Mobilteilnehmer synchron im Zeitraster arbeiten.

Details hierzu sind [Tetra] zu entnehmen.

4.2.2 TETRAPOL

Im Gegensatz zu dem auf europäischer Ebene offen standardisierten TETRA handelt es sich bei **TETRAPOL** um einen reinen Firmenstandard, der von MATRA für den Einsatz bei der französischem Polizei und Gendamerie entwickelt worden ist.

Daher sind nähere Angaben zu den technischen Parametern hier nicht möglich. Es darf jedoch getrost angenommen werden, daß es sich bei der Namens-Ähnlichkeit mit dem europaweiten TETRA-Standard durchaus nicht um einen Zufall handelt, denn MATRA und deren deutsche Tochter AMC versuchen, das System auch in Deutschland im BOS-Bereich anzubieten.

4.3 Schnurlose Telefone

4.3.1 CTx

Mit Ausnahme der völlig un-standardisierten schnurlosen Telefonen aus dem Ex- und Import-Bereich gab es in der Prä-DECT-Ära die Cordeless Telephone Standards CT1 bis CT3.

Obgleich manchmal auch von **CT0** gesprochen wird, handelt es sich hierbei nicht um einen Standard. Man bezeichnet hiermit die unstandardisierten, rein analog arbeitenden vollduplex-Geräte kleiner Leistung, deren Arbeitsfrequenz häufig im Bereich um 40 MHz lag. Dieser Bereich ist (war) in den USA und Japan für diese Nutzung vorgesehen. 'CT0'-Geräte sind als Billig-Importware zu uns gekommen.

CT1 wurde bereits in den neunziger Jahren durch CEPT definiert, um die Frequenznutzung zu kanalisieren. Es handelte sich dabei um ein rein analog arbeitendes System für das zwei Frequenzbänder definiert wurden. Zwischen 914.0125 und 914.9875 MHz sendeten die Mobilgeräte, wobei die Basisgeräte zwischen 959.0125 und 959.9875 MHz arbeiteten. Es stehen somit insgesamt 40 Duplex-Kanäle im 20-kHz-Frequenzraster zur Verfügung. Die analoge Frequenz-, bzw. Phasenmodulation läßt lediglich Frequenzduplex zur Anwendung kommen. Der Weichenabstand beträgt 45 MHz.

In einer Ausbaustufe wurden unter dem Arbeitstitel CT1+ weitere 40 Kanäle zugewiesen. Die neuen Achzigkanalgeräte arbeiten also auf 885,0125 bis 886,9875 MHz (Sendefrequenz Mobilteil) und 930,0125 bis 931,9875 MHz (Sendefrequenz Fest-Teil).

Im Gegensatz zum rein analogen CT1 handelt es sich bei **CT2** um einen echten digitalen Standard. Das System benutzt Zeit-Duplex im Gegensatz zum Frequenzduplex. Das bedeutet, daß die Mobilstation und die Feststation zeitversetzt auf dem gleichen Frequenzkanal senden.

Hierzu stehen wiederum vierzig Kanäle zur Verfügung. Festgelegt wurden 864,150 bis 868,050 MHz mit einem Kanalabstand von 100 kHz. Aus Gründen der Störsicherheit wurde Breitband-FSK mit einem Hub vom ±20 kHz gewählt.

Die 'Over-the-air'-Bitrate beträgt 72 kBit/s. Als Modulationsart kommt aus spektralen Gründen GMSK zur Anwendung.

Sowohl Sprache als auch die Signalisierungsinformation wird digital übertragen. Die Sprache wird dabei mit 32 kBit/s ADPCM codiert und in Bursts übertragen.

Das CT2-System hat sich als öffentliches Kleinzellen-System unter dem Namen 'Birdy' in einem Feldversuch in München einen Namen gemacht.

Die Geräte nach **CT3** besitzen bereits alle Merkmale der DECT-Geräte, also Zeitmultiplex, digitale Übertragung von Sprache und Signalisierungsinformationen sowie die Verschlüsselungs und Authentisierungsverfahren. Nur eben ein wenig anders als bei DECT.

Seit dem Aufkommen des DECT-Standards sind diese Geräte jedoch am Markt praktisch nicht mehr verfügbar.

4.3.2 DECT

Als Standard für schnurlose Telefone ist der europäische DECT-Standard derzeit state-of-the art.

Das System arbeitet voll digital und benutzt Zeitmultiplex für die Trennung zwischen Up- und Downlink. Derzeit sind zehn Frequenzkanäle zur Nutzung durch DECT-Telefone vorgesehen: 1880.064 MHz bis 1897,344 MHz. Aus unerfindlichen Gründen sind dabei die Kanalnummern nach *absteigender* Frequenz sortiert.

Bedingt durch die hohe Funkbitrate von 1,152 MBit/s wurde ein Kanalabstand von 1,728 MHz festgelegt

Zur Anwendung kommt wiederum GMSK mit einem Frequenzhub vom ±144 kHz. Der Standard sieht eine Sendeleistung von maximal 250 mW vor.

Wie bereits erwähnt handelt es sich um ein Zeitschlitz-System, das im Zeitmultiplex betrieben wird. Pro HF-Träger werden vierundzwanzig Zeitschlitze (Full Slots, s.u.) verwendet, von denen die ersten 12 den 'Downlink' von der Feststation zum mobilen Teilnehmer belegen. Die zweiten 12 Zeitschlitze werden von den mobilen Teilnehmern belegt.

Die Rahmenlänge, bestehend aus eben diesen vierundwanzig Zeitschlitzen beträgt 10 Millisekunden. Jeweils 16 dieser Rahmen bilden einen sogenannten 'Multiframe' von 160 ms Dauer.

Demnach dauert ein 'Full Slot', also ein Zeitschlitz ca. 416µs und enthält 480 Bit. Schutzzeiten von jeweils 50 µs dienen dem Ausgleich des Jitters aus dem mobilen Einsatz.

4.4 Funkrufdienste (Pager)

4.4.1 POCSAC

Das von der britischen Post Office Coded Standardisation Advisory Group (POCSAG) definierte Einwege-Protokoll ist die Basis für den deutschen Personenrufdienst Cityruf.

Es ist vielleicht interessant, daß der Zeitablauf bzw. die späte Liberalisierung der mobilen Telekommunikationsdienste in Deutschland dazu geführt hat, daß sich dieserorts die sogenannten 'Pager'-Dienste gegenüber dem boomenden GSM nicht in der gleichen Weise durchsetzen konnten wie beispielsweise in den USA.

Gerade im Land der unbegrenzten Möglichkeiten machten Wildwuchs bei den Mobiltelefon-Anbietern, die unübersichtliche Gebührenstruktur und der Wirrwar bei den Roamingabkommen die Pagerdienste attraktiv.

In Deutschland hingegen finden die Pager erst allmählich ihren Markt, insbesondere, seit es Diensteanbieter gibt, die den Service ohne Grundgebühren anbieten und so die Rufempfänger für Schüler etc. erschwinglich machen. Insgesamt ein interessantes Stück Marketing und Zielgruppenfindung.

Der POCSAG bzw. Cityruf unterscheidet sich dabei grundlegend von dem älteren, analog arbeitenden EUROSIGNAL-Dienst, der als Beipack die UKW-Rundfunksender benutzt und seine Rufinformation in Form von Fünftonfolge-Sendungen ausstrahlt. Einige Jahre ist es her, da veröffentlichte eine große deutsche Zeitschrift der Funktechnik eine Methode, diese Aussendungen zu decodieren. Findige Leute waren so in der Lage, mittels UKW-Radio und einem EMUF die Grundbegühren zu umgehen, was natürlich strengstens verboten war...

Heute ist die 'piratenmäßige' Nutzung von Cityruf nicht mehr attraktiv, da die Telekom die Gebühren vom Anrufer kassiert. Der gerufene Teilnehmer trägt keine Gebühren.

Im Gegensatz zu Eurosignal benutzt POCSAG bzw. Cityruf hingegen Frequenzen im 70 cm-Band (450 bis 470 MHz) im 20 kHz-Kanalraster für die Aussendungen. POCSAG definiert drei Typen von Empfängern. Die sogenannten Nur-Ton-Empfänger erlauben die Anzeige von vier Tönen. Daneben gibt es Empfänger, die Nachrichten als Ziffernfolgen (mit einigen wenigen Sonderzeichen) bzw. als alphanumerischen Text erlauben.

Die Datenübertragung erfolgt mit einer Datenrate von 512 Bit/s in Form sogenannter 'Batches', also Informationsgruppen, von denen je einer einen Pager anspricht. In den Batches wiederum ist die Information hineincodiert.

POCSAG wird in Europa viel genutzt. Die British Telecom hat in Zusammenarbeit mit Ericsson beispielsweise gerade ein satellitengestütztes Verteilsystem in Dienst gestellt.

4.4.2 ERMES

ERMES ist die europäische Antwort auf POCSAG und Cityruf. 1990 fertiggestellt, hat er heute (d.h. 1997) noch keine kommerziell verwertbare 'critical mass' in Europa erzielen können [EuroT].

ERMES benutzt eine wesentlich höhere Funkbit- bzw. -symbolrate von 3,125 Symbole/Sekunde (Baud). Das System benutzt eine vierstufige FSK, wodurch eine Bitrate von 6,25 kBit/s erzielt wird.

Das System nutzt europaweit Frequenzen im VHF-Bereich. Hier sind sechzehn Kanäle zwischen 169,4125 und 169,8125 MHz im 25 kHz-Kanalraster festgelegt.

Das System arbeitet zeitsynchron, wobei eine Übertragungssequenz 60 Minuten dauert. Hier hinein sind wiederum die 'Batches' codiert, die jeweils 750 ms lang sind. Dieses Schema erlaubt jedem Pager sich auf das System aufzusynchronisieren und um je nach gewünschtem Batch-Typ genügend Chancen zu haben, eine an ihn gerichtete Meldung auch wirklich zu empfangen.

Die Frequenzauswahl der Empfänger erfolgt ebenfalls zeitsynchron, damit diese den jeweiligen Aussendefrequenzen folgen können.

5 Ausblick:

Es besteht keinerlei Zweifel. Die digitalen Mobiltelefonsysteme werden die älteren, analogen Systemen im Verlauf der nächsten Zeit komplett ablösen.

Und es wird deutlich weitergehen. Bereits heute sind satellitengestützte Mobiltelefonsysteme im Einsatz auf die wir im vorangegangenen Text nur ganz knapp eingegangen sind. Spätestens seit dem Golfkrieg gehören Satellitentelefone zur Standardausrüstung vieler Auslandskorrespondenten. Auch auf diesem Markt dominieren private Provider, meistens Konsortien. INMARSAT, NorTel Data und wie sie alle heißen mögen.

Leute, die etwas auf sich halten, ordern bereits heute sogenannte Dual-Mode-Terminals (Insider sagen nicht mehr 'Handy' zum Handtelefon. Das ist vulgär! Sie sagen jetzt 'Terminal'). Diese Geräte erlauben den Zugriff auf terrestrische Netze, also GSM, DCS-1800 oder ähnliches, können aber gleichzeitig auf satellitengestützte Systeme zugreifen. Hier sind bereits zwei Systeme zumindest teilweise in Betrieb, nämlich das von Alcatel betriebene GlobalStar-System sowie das von dem Motorola-Konsortium propagierte IRIDIUM-System. Sicherlich werden andere folgen. Immerhin munkelt man, daß auch Microsoft plant in diesen lukrativen Geschäftszweig einzusteigen.

Die Satelliten umlaufen die Erde in niederen Flugbahnen (LEO) und sind in sechs 'Abstandskäfigen' ähnlich dem Raumsegment des GPS-Navigationssystems angeordnet und treten in wahren Rudeln auf. Um eine möglichst lükenlose Versorgung zu gewährleisten, benötigt das IRIDIUM-System beispielsweise mindestens 66 Satelliten, jeweils 11 in den schon erwähnten Abstandskäfigen.

Wohin der digitale Zug bei den Organisationen mit Sicherheitsaufgaben (BOS) geht, ist heute noch nicht abzusehen. Da es sich bei den weiter oben betrachteten Mobilfunksystemen um privat, d.h. marktwirtschaftlich betriebene Systeme handelt, kämpfen die verschiedenen Diensteanbieter derzeit erbittert um Marktanteile auf diesem Gebiet. Immerhin wären an der Polizei als Kunden erhebliche Beträge alleine an auflaufenden Gebühren zu verdienen. Allerdings würde dann auch für eine ganze Reihe neugieriger Zeitgenossen der Nervenkitzel entfallen, Ringfahndungen oder saftige Unfallberichte quasi live zu erhalten. Doch vielleicht lassen sich im Zeitalter leerer Kassen die für eine derartige Investition notwendigen Mittel auch gar nicht so schnell aufbringen.

Und dann die Frage: Quo vadis, Amateurfunk. Nun, ich will die Hoffnung nicht aufgeben, daß sich hier etwas tut. Zumindest können wir auf die Erfolge bei der flächendekenden Einführung von Packet Radio stolz sein, die sich in 1985, als ich zusammen mit DL5UY (ex DB3IG) in DL erste Versuche mit TAPR 6809-Boards angestellt habe, noch garnicht absehen ließen.

Es muß ja nicht gleich GSM sein, aber vielleicht packt es ja den einen oder anderen und probiert ein DECT-Relais auf Basis der am Markt inzwischen von mehreren Firmen leicht erhältlichen Chipsets aus. Möglicherweise beschäftigt sich gerade in diesem Moment, in dem ich diese Zeilen schreibe, jemand mit diesem oder einem ähnlichen Thema. Ich würde mich in jedem Fall über eine Mail freuen und bin gerne bereit, das eine oder andere darüber auf meiner Homepage zu veröffentlichen. Also dann, bis bald!

6 Kontakte

Der Autor kann über die email-Adresse *dk6ii@afusoft.de* erreicht werden. Das Manuskript zu diesem Vortrag wie auch die Skripten zu älteren Vorträgen von UKW-Tagungen, Ham Radio etc. können über folgende URL aus dem World Wide Web abgerufen werden: *http://www.afusoft.de*

7 Glossar:

AMPS	American Mobile Phone Standard
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
CCITT	Commitée Consultative Internationale de Télephone et Télegraphe
CELP	Codebook Excited Linear Prediction, modernes Digitalisierungsverfahren für Sprache. Siehe hierzu auch [SprCod]
CEPT	Commitée Europen de poste et télecommunication
CNR	Combat Net Radio. Allg: Militärisches Funkgerät
CNRI	Combat Net Radio Interface. Bezeichnung für eine Funk-/Draht-Überleiteinrichtung für militärische Funkgeräte
cqDl	Verbandszeitschrift des DARC
CTx	Cordless Telephone (standard) x, d.h. CT0, CT1, CT2 usw. Ältere, zumeist analoge Standards für schnurlose Telefone.
DARC	Deutscher Amateur Radio Club e.V.
DECT	Digital European standard for Cordless Telephones
DQPSK	Differential Quadrature Phase Shift Keying
EPPA	European Public Paging Association
ETSI	European Telecommunications Standard Institute
FMS	Funk-Meldesystem
FSK	Frequency Shift Keying
GMSK	Gaussian Minimum Shift Keying
GPS	Global Positioning System. Satellitengestütztes Navigationssystem
GSM	'Global Standard for Mobile communication' oder 'Groupe spéciale mobile'. Digitaler Mobiltelefonstandard (entspricht D-Netz in Deutschland)
IMEI	International Mobile Equipment Identity
ERMES	European Radio Message System
LAN	Local Area Network
LEO	Low Earth Orbit, Bezeichnung für Satelliten auf einer 'niederen' Erdumlaufbahn
nöbL	'nicht-öffentlicher, beweglicher Landfunkdienst'
öbL	'öffentlicher beweglicher Landfunkdienst'
OSI	Open Systems Interconnect
PCS	Personal Communication Standard
PIN	Personal Identification Number
POCSAG	(British) Post Office Coded Standardisation Advisory Group
RPE-LPT	Regular Pulse Excited, Long-Term Prediction; Sprachcodierungsverfahren, das bei GSM im 13 kBit/s 'full rate' Mode angewandt wird.
TAPR	Tucson Amateur Packet Radio (Group)
TDMA	Time Division Multiple Access; Zeitmultiplex
TETRA	Trans European Trunked Radio Access
WWW	World Wide Web

8 Literatur

[BOS]	Marten	"BOS-Funk"
[DigP]	Schiffhauer, N.	"Auch Polizei und Feuerwehr wollen digital kommunizieren"; Frankfurter Allgemeine Zeitung, 15.4.97, Nr. 87/Seite T1.
[EuroT]		"European Paging Operators want freedom of choice"; Eurotrade Magazine 6/97."
[GPS]	Franke, E. H.	"Das GPS-Satelliten-System"; 37. UKW-Tagung, Weinheim
[GSM]	ETSI	"GSM"; Doc 145/90
[Isar]	ARD	"ISAR 12"; Fernsehserie aus den sechziger Jahren
[Sign]	Gabler;	"Signalisierungs- und Meßverfahren im modernen Mobilfunk"; Franzis'; ISBN 3-7723-4951-X
[SprC]	Franke, E. H.	"Digitale Sprachcodierung und -übertragung"; 39. UKW-Tagung, Weinheim
[Tetra]	ETSI	"TETRA Voice+Data, Designer's Guide"; RES06(95)034; ETSI Technical Report; V0.0.10, 4.Jan 1996