Abiturjahrgang 2012/14

# SEMINARARBEIT

## Kryptographie

## Verschlüsselung und Technik mobiler Telekommunikations-systeme am Beispiel Terrestrial Trunked Radio

# Inhaltsverzeichnis

# 1 Mobilfunknetze, Entwicklung und Überblick

Als Horaz um das Jahr 23 v. Chr. seine Lobeshymne[1] auf den römischen Götterboten Mercurius (griechisch: Hermes) dichtete, hat er wohl nicht damit gerechnet, dass dessen Arbeit als Bote zwischen Göttern und Menschen heute längst durch moderne Telekommunikationssysteme überholt wurde, denn heute würden die antiken Götter wohl eher zum bequemen Mobiltelefon greifen.

Als erstes Telekommunikationssystem wurde seit 1793 Telegraphie verwendet [12], danach seit 1860 Festnetz-Telefonie [13] und seit 1896 Sprechfunk in Form von Morsezeichen [14].

Erst 1958 begann in Deutschland mit dem sogenannten **A-Netz** der Betrieb des ersten öffentlichen Mobilfunknetzes, mit dem man sich ohne Bindung an einen Standort über größere Entfernungen verständigen konnte. Das von der Bundespost unter dem Namen "öffentlich beweglicher Landfunkdienst (öbL)" betriebene Netz bildete das Gegenstück zu dem vor allem für Behörden oder Verkehrsgesellschaften vorgesehenen "Nichtöffentlichen mobilen Landfunk (NömL)" und stellte ein analog übertragenes, nationales System dar, das auf einem weitgehend flächendeckenden System basierte [4].

Das A-Netz zählte genau wie die Nachfolger B- und C-Netz zur ersten Generation der Mobilfunksysteme. Da es technisch veraltet und zudem überlastet war, wurde es 1977 abgeschaltet [8].

Vorteil des seit 1972 betriebenen B-Netzes war vor allem der automatisierte Verbindungsaufbau. Außerdem war es möglich, in kompatible Netze zum Beispiel in Österreich, den Niederlanden oder Großbritannien zu telefonieren. Dagegen brachte das B-Netz auch Nachteile, so war es beispielsweise nicht möglich, das Gespräch bei einem Wechsel der Funkzelle[2] fortzusetzen (sog. Handover). Weiterhin musste der Bereich kannt sein, in dem sich der angerufene Teilnehmer befand [4].

Die meisten dieser Probleme wurden mit dem nächsten, ebenfalls analogen Standard der ersten Generation behoben, dem sogenannten **C-Netz**, das von 1985 bis 2000 von DeTeMobil unter dem Namen "C-Tel" betrieben wurde [8]. Es war jetzt möglich, "den Aufenthaltsort eines mobilen Teilnehmers im Netz zu speichern und mit jedem Funk-

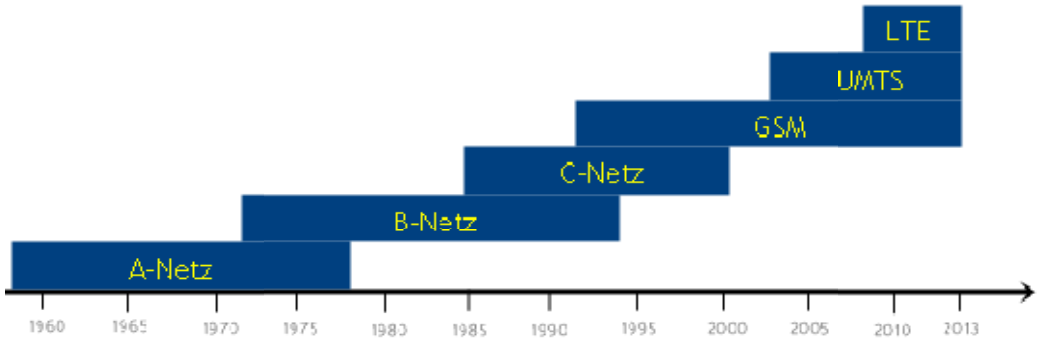


**Abbildung 1** Zeitliche Übersicht der Entwicklung des öffentlichen Mobilfunks in Deutschland

[1] Q. Horatii Flacci: carmina, carmen 1,10: Hymnus auf Mercurius, liber primus http://www.gottwein.de/Lat/hor/horc110.php

[2] Geographischer Bereich, in dem die Funkkommunikation stattfindet [4, S. 382]

zellenwechsel zu aktualisieren" [4, S. 434]. Auch die Handover-Funktion wurde erfunden und ermöglichte es, während eines Gesprächs die Funkzelle zu wechseln. Eine weitere neue Entwicklung neben der automatischen Standortbestimmung durch die Laufzeitunterschiede zwischen Mobiltelefon und Funkmasten war der Einsatz einer Chipkarte, eine Art Vorläufer der heute gängigen SIM-Karte [2], [1]. Außerdem wurde im Gegensatz zum A- und B-Netz mit C-Tel mit der sogenannten Verschleierungsfunktion[3] erstmalig eine annähernd sichere Übertragung privater Gespräche ermöglicht [8].

Wegen technischer Überholung wurde C-Tel im Jahr 2000 vom Netz genommen.

Es existieren in anderen Ländern Systeme wie Nordic Mobile Telephone (NMT, v.a. Skandinavien), Advanced Mobile Phone System (AMPS, v.a. USA) und japanische Vertreter der ersten Generation [4], auf die an dieser Stelle jedoch nicht näher eingegangen werden soll, vielmehr wird nur die Entwicklung in Deutschland betrachtet.

Einen großen Meilenstein in der Geschichte des öffentlichen Mobilfunks erreichten die **CEPT**[4] und später das **ETSI**[5] um 1991 mit der Entwicklung des **Global System for Mobile Communications (GSM)** [9], [1]. Mit diesem erstmals digitalen Mobilfunkstandard der sogenannten zweiten Generation wurde der Grundstein für die meisten nachfolgenden Systeme gelegt.

Die digitale Übertragung ermöglichte vor allem eine schnellere Übermittlung nicht nur von Sprache, sondern auch von Text und Datenpakten, die später zur Erfindung der SMS (Short Message Service) führte. Weiterhin war es jetzt möglich, wesentlich bessere Verschlüsselungstechniken einzusetzen [8].

Vertreter von GSM bilden in Deutschland die Systeme GSM900 unter dem Namen D1 und D2 und das als E-Netz bezeichnete DCS1800[6] [1].

Mit dem Ziel, neue Erfindungen wie höhere Übertragungsgeschwindigkeiten zu erzielen, wurde GSM später an das **3GPP**[7] übergeben. GSM wird noch immer weiterentwickelt, sodass schnellere Systeme wie zum Beispiel GPRS[8] entstanden [2].

Der auf dem Mobilfunkmarkt
de Konkurrenzdruck führte dazu, dass Mobiltelefone über massiv nachlassende Preise, mit wiederum für die Wirtschaft förderlichen Auswirkungen, für die breite Bevölkerung erschwinglich wurden. 2006

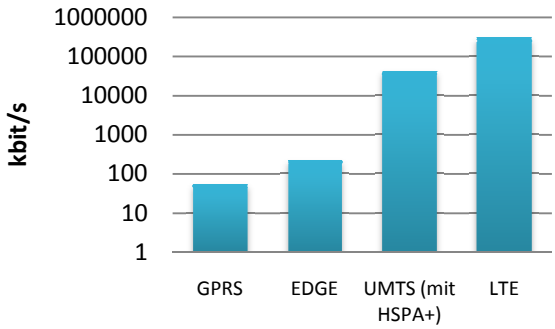


**Abbildung 2** Übertragungsgeschwindigkeiten unterschiedlicher Mobilfunkstandards. Logarithmische Darstellung. Daten aus [11]

[3] Das analoge Signal wird stark verzerrt übertragen, nur der berechtigte Empfänger erhält ein verständliches Sprachsignal.
[4] Conférence Européenne des Administrations des Postes et des Télécommunications, deutsch: Europäische Konferenz der Verwaltungen für Post und Telekommunikation. Organisation für Zusammenarbeit von Regulierungsbehörden (z.B. Bundesnetzagentur).
[5] European Telecommunications Standards Institute, deutsch: Europäisches Institut für Standardisierung in der Telekommunikation.
[6] Prinzipiell handelt es sich um den gleichen Standard, allerdings verwendet GSM900 den 900 MHz-Frequenzbereich, während DCS1800 bei 1800 MHz angesiedelt ist.
[7] 3rd Generation Partnership Project, Kooperationsprojekt von Standardisierungs-Organisationen. Mitglieder: ARIB, TTC (Japan), ETSI (Europa), ATIS (USA), TTA (Korea).
[8] General Packet Radio System, GSM-Paketdatendienst

zählte das Global System for Mobile Communications mit weltweit 1,7 Milliarden Kunden als meistgenutztes Mobilfunksystem [43]. GSM ist auch heute noch im Einsatz.

Als Übergang von der zweiten zur dritten Generation ist insbesondere **EDGE** zu nennen, Enhanced Data for Global Evolution. Es handelt sich dabei um eine Erweiterung von GSM, die vor allem größere Übertragungsgeschwindigkeiten und eine effektivere Frequenzökonomie bietet, d.h., kleinere Frequenzbereiche effizienter nutzen kann, da diese als knappe Ressource gelten [15].

Ungefähr seit 2003 ist mit **UMTS** (Universal Mobile Telecommunications System) die dritte Generation der öffentlichen Mobilfunkstandards in Deutschland vertreten. Neben verbesserten Sicherheitsmerkmalen bietet UMTS durch mehrere Erweiterungen wie z.B. das sogenannte HSPA+ (High Speed Packet Access Plus) vor allem wesentlich höhere Übertragungsraten (Abb. 2), die beispielsweise mobiles Internet ermöglichen. In der Folge wurden und werden sogenannte Smartphones mit Internet-Applikationen entwickelt, die dem Nutzer eine große Vielfalt an Diensten anbieten.

Ende 2008 wurde die Entwicklung von **LTE** (Long Term Evolution) abgeschlossen, einem Mobilfunk- und Netzwerk-Standard, der auf dem prinzipiell gleichen Grundschema wie UMTS basiert und bereits zur vierten Generation gezählt wird. Für Mobiltelefone bietet es eine noch höhere Übertragungsrate, die vor allem wegen der zunehmenden Bedeutung des mobilen Internets eine große Rolle spielt [16]. Die Protokollerweiterung **LTE-Advanced** ermöglicht mit Bandbreiten von bis zu 1000 Megabit pro Sekunde höhere Datenübertragungsraten und soll in Deutschland ab 2014 realisiert werden [17].

Die oben beschriebenen Systeme sind für die Öffentlichkeit bestimmt. Parallel dazu entwickelte sich wegen anderer Anforderungen der Anwender der **nicht-öffentliche Mobilfunk**, auch als privates Netz bezeichnet, das nur einem internen Kreis von Teilnehmern zugänglich ist, so zum Beispiel Mitarbeitern eines Unternehmens oder von Behörden [1].

Im Mobilfunk unterscheidet man zwischen **analogen** und **digitalen** Übertragungsverfahren: Während in einem analogen Netz "Signale zeit- und wertkontinuierlich übertragen [werden]" [1, S. 4-3], arbeitet ein digitales System binär, d.h. über den Wert "Strom an" bzw. "Strom aus" und kann so, weitgehend unabhängig von analogen Faktoren, nahezu verzerrungsfrei Daten übermitteln [1].

Mobilfunknetze werden auch nach Netzarchitektur unterschieden, von denen man die zellulare Struktur am häufigsten findet[9].

Neben diesen Kategorien unterteilt man Funknetze weiterhin nach Übertragungsmedium, z.B. Funkrufsystemen, Satellitensystemen, kabelverbundenen Systemen, Richtfunk oder Mobilfunk [1], wobei an dieser Stelle nicht näher auf diese einzelnen Medien eingegangen werden soll, sondern speziell auf den nicht-öffentlichen Mobilfunk.

Nachfolgend wird der Schwerpunkt auf das nicht-öffentliche Bündelfunksystem TETRA (Terrestrial Trunked Radio) gelegt, das in Deutschland auch als "Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BOS)" bezeichnet wird.

[9] Erläuterungen siehe unten.

# 2 Terrestrial Trunked Radio (TETRA)

Im folgenden soll das Bündelfunksystem TETRA (Terrestrial Trunked Radio, deutsch: irdischer Bündelfunk) zunächst definiert und dann nach technischen und sicherheitstechnischen Aspekten näher beleuchtet werden. Im Anschluss wird beispielhaft auf den aktuellen Stand des nicht-öffentlichen digitalen Bündelfunks in Deutschland eingegangen werden.

## 2.1 Definition

Terrestrial Trunked Radio (TETRA) ist der am weitesten verbreitete europäische Standard der zweiten Generation für digitalen Bündelfunk[10]. Dieser allgemein auch als Digitalfunk bezeichnete Standard wird im mobilen Betriebsfunk und als sichere Kommunikationstechnik für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) angewandt [3].

### 2.1.1 Der Standard


**Abbildung 3** Logo von TETRA [29]

Die in Deutschland verwendete Systemtechnik ist nach dem TETRA 25-Standard in den 1990er Jahren vom ETSI entwickelt worden [19] und soll für "professionelle Mobilfunkanwender wie Militär, Behörden, Sicherheitsdienste, Verkehrsgesellschaften und Energieversorgung" [5, S. 13] eingesetzt werden. Ziel war es, einen europaweiten Standard zu entwerfen, der zudem mit PMR-Systemen[11] interagieren kann. TETRA bietet vor allem eine verbesserte Sprachqualität sowie bessere Sicherheitsmerkmale als analoge Systeme, eine effizientere Frequenz-Ökonomie, und hat unterschiedliche Möglichkeiten zur Datenübertragung, neben Sprache können beispielsweise auch Text- und Bildnachrichten gesendet und empfangen werden [5], [20].

### 2.1.2 Klassifikation und Einordnung

Bei TETRA handelt es sich um ein nicht-öffentliches System, das vor allem von Behörden und industriellen Anwendern verwendet wird. Weiterhin ist es ein digitales Netz, das im Gegensatz zu analogem Funk eine verbesserte Sprachqualität und die Möglichkeit der Verschlüsselung mit sich bringt. Die Endgeräte sind zumeist mobil. Außerdem erfolgt die Datenübertragung durch das Prinzip des Bündelfunks, während die Netzarchitektur ähnlich wie beim GSM der eines zellularen Systems entspricht[12] [4].

[10] siehe Abschnitt 2.3.1: Technik, Bündelfunksystem und Übertragung
[11] Private Mobile Radio, "Jedermann-Funk" im Frequenzbereich 446.000 - 466.100 MHz
[12] siehe Abschnitt 2.3: Technik

## 2.2 Bedeutung und Anwendung

Derzeit wird in Deutschland TETRA unter dem Namen **Digitalfunk** für die Behörden und Organisationen mit Sicherheitsaufgaben (**BOS**)[13] eingeführt. Bundesweit sollen 500.000 Nutzer an das neue, abhörsichere Netz angeschlossen werden, womit es zum weltweit größten seiner Art würde [5].

### 2.2.1 Entwicklung von TETRA in Deutschland

1990 verpflichteten sich die Schengen-Staaten, ein länderübergreifendes Kommunikationssystem zu errichten. Aufgrund mehrerer Beschlüsse der Innenministerkonferenzen der Länder wurden Projektgruppen ins Leben gerufen, die sich mit dem Aufbau eines digitalen, bundesweit einheitlichen Sprech- und Datenfunksystems befassen sollten. Mitte 2001 wurde ein zweijähriger Pilotversuch in Aachen durchgeführt. Daraufhin einigten sich Bund und Länder auf einen Mindeststandard und setzten das Ziel, bis Ende 2010 das bundeseinheitliche Digitalfunksystem einzuführen.

Im April 2007 nahm die neu gegründete Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (**BDBOS**) ihre Arbeit auf. Diese Behörde nimmt Aufgaben wie die Einrichtung, Verwaltung und Überwachung der Sicherheit des Digitalfunks wahr. Im Anschluss wurde die Finanzierung des Funknetzes und die Beteiligung der einzelnen Länder geregelt. Im Juni 2007 wurde das digitale Funknetz in sechs deutschen Städten in Betrieb genommen [5].

### 2.2.2 TETRA weltweit

121 Staaten nutzten weltweit Ende 2010 TETRA-Systeme, so zum Beispiel zahlreiche asiatische Staaten und fast alle europäischen Länder [21]. Dabei verwenden hauptsächlich Behörden, Industrie und Transportgesellschaften diesen Standard. Auf dem Markt sind mehrere Anbieter vertreten, da TETRA ein offener Standard ist.

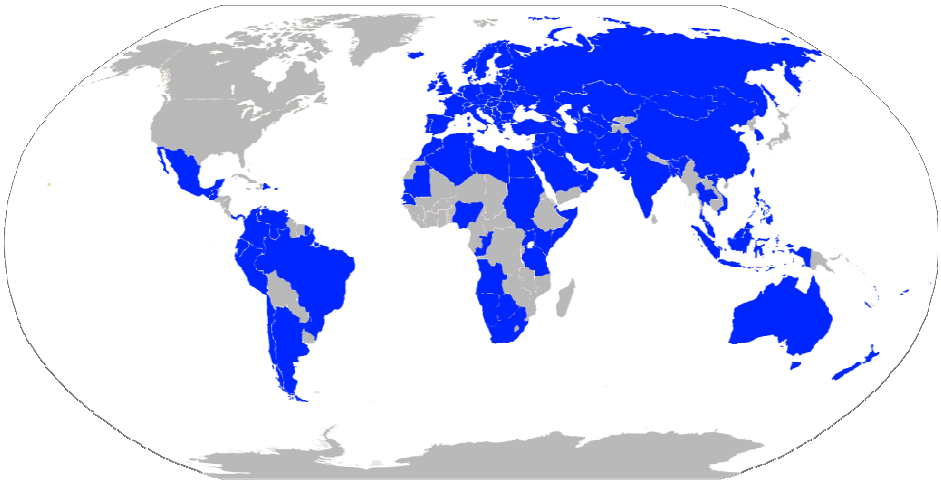

**Abbildung 4** Nutzung von TETRA weltweit. In den USA und anderen Ländern wird geplant, das System ebenfalls einzuführen. Daten von [21]

[13] Z.B. Polizei, Feuerwehr, Rettungsdienst

# 2.3 Technik

Obwohl TETRA einige Elemente des GSM übernahm, wurde dennoch ein enormer Technologiesprung vollzogen. Mit der Ablösung des analogen durch den digitalen Funk werden gleichzeitig mehrere neue Entwicklungen der letzten Jahre integriert wie zum Beispiel neue Übertragungsverfahren, verbesserte Gerätetechnik und die Digitalisierung von Sprache und Daten.

## 2.3.1 Bündelfunksystem, Übertragung

Der bisher von vielen Unternehmen verwendete Analogfunk bringt viele Nachteile mit sich: Die Funkkanäle sind überlastet, durch Empfangsstörungen entsteht eine schlechte Sprachqualität [4] und Nachrichten können zudem ohne nennenswerten Aufwand abgehört werden. Daher wird das alte, analoge System zunehmend durch digitale Systeme ersetzt.

Hierbei bieten sich digitale Bündelfunksysteme der zweiten Generation an, zu denen auch TETRA gehört. Als bekanntester Vertreter der analogen ersten Generation sei "Chekker" genannt, ein im Betriebsfunk eingesetztes System [1].

Die "Idee des Bündelfunks [...] besteht darin, dass unterschiedliche Benutzergruppen auf gemeinsamen Frequenzen zusammengefasst werden und diese durch den Bündelungseffekt besser ausgenutzt werden" [4, S. 455]. Ergebnis dieses Effektes ist eine erhöhte Frequenzökonomie, die zur Verfügung stehenden Funkfrequenzen werden besser ausgenutzt, denn diese gelten als knappe Ressource. Funkkanäle werden im Gegensatz zum Analogfunk gleichmäßig genutzt und nicht überlastet, außerdem kommt es nicht zu Qualitätsverlusten, wenn auf nahe beieinander liegenden Kanälen gesendet wird [5].

TETRA basiert auf einem **Multiplexverfahren**, einem Verfahren, das "einem Übertragungskanal mehrere Signale zur gleichzeitigen Übertragung [zuweist]" [5, S. 26]. Es werden viele voneinander unabhängige Signale binär codiert, innerhalb eines zeitlichen Fensters (einem sog. *Zeitschlitz*) übertragen und von den Empfängern wieder in Kanälen aufgelöst [22].

Durch das Multiplexverfahren ergeben sich (im Netzbetrieb[14]) zusätzliche Kanäle, obwohl die Kanalbandbreite dieselbe ist: Einem physikalischen Kanal sind mehrere logische Kanäle zugeordnet [1]. Damit können auf jeder TETRA-Frequenz mehrere Teilnehmer gleichzeitig Daten senden. "Die Zuordnung der Daten zu den Teilnehmern und die Synchronisation der Zeitschlitze übernimmt hierbei die zentrale Netzsteuerung" [5, S. 28].

TETRA nutzt ähnlich dem Analogfunk Frequenzen im Unterband ("Uplink", 380-385 MHz) und Oberband ("Downlink", 390-395 MHz). Dabei überträgt das Mobilfunkgerät im Unterband zur Basisstation. Im Oberband wird die Mitteilung an die anderen Gesprächsteilnehmer verstärkt ausgestrahlt (vgl. auch Abb. 5).

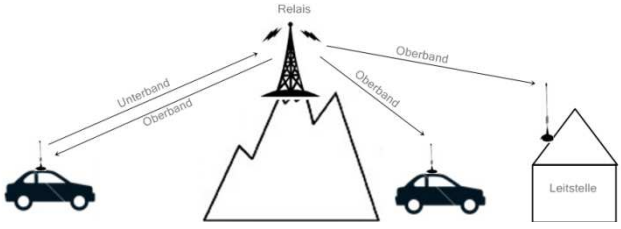


**Abbildung 5** Netzarchitektur des analogen BOS-Funks. Ein Funkteilnehmer, z.B. ein Fahrzeug, sendet eine Sprachnachricht im Unterband an die nächstgelegene Relaisstation. Diese verstärkt das analoge Signal und strahlt es im Oberband an sämtliche Teilnehmer des Sprechfunkverkehrskreises aus, die denselben Kanal eingestellt haben.

[14] siehe 2.3.4.1: Netzbetrieb (Trunked Mode Operation, TMO)

## 2.3.2 Netzarchitektur

Beim Analogfunk besteht eine örtlich begrenzte Infrastruktur, die aus mehreren zusammengeschalteten **Relaisstellen** aufgebaut ist (Abb. 5). Jede Organisation nutzt eine eigene Infrastruktur mit einem eigens zugeteilten Funkkanal (z.B. Kanäle für Polizei, Feuerwehr, Rettungsdienst, etc.) [5].

TETRA hingegen weist dem GSM-System ähnliche Netzkomponenten auf [4], so wird zum Beispiel auch hier auf die zellulare Struktur zurückgegriffen (Abb. 6), indem jede der Zellen von einer **Basisstation** versorgt wird und die jeweiligen Nachbarzellen unterschiedliche Frequenzen nutzen, um gegenseitige Störungen zu verhindern. Dadurch ergibt sich die Möglichkeit, gleiche Frequenzen mehrfach zu verwenden, wenn sie eine ausreichende Distanz aufweisen [5]. Verlässt ein Gesprächsteilnehmer eine Funkzelle, bleibt die Verbindung dennoch bestehen (**Handover**: eine bestehende Verbindung wird bei Funkzonenwechsel automatisch nachgeführt [2]).

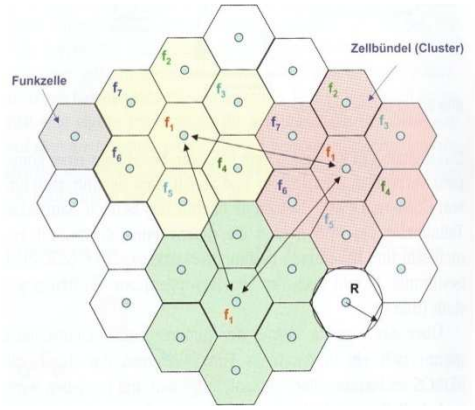


**Abbildung 6** Zellenstruktur im TETRA-System. Bei hexagonalen Zellen werden aus sieben benachbarten Zellen sogenannte **Cluster** (Zellbündel) gebildet. Zellen, die mit derselben Zahl beschriftet sind, nutzen identische Frequenzen. Das Versorgungsgebiet einer Zelle (R) wird durch geographische und technische Gegebenheiten festgelegt [5].

Es bestehen allerdings einige Unterschiede zu der GSM-Netzarchitektur. So gibt es bei TETRA die Teilsysteme **Mobile Station** (MS), **TETRA-Basisstation** (TBS) und **Vermittlungsstellen** (DXT: Digital Exchange for TETRA), die über mehrere Schnittstellen miteinander verbunden sind [5].

Als Mobilstation wird die Ausrüstung des Teilnehmers (z.B. Funkgerät) mit der zugehörigen Schnittstelle bezeichnet, mit der der Benutzer auf die Dienste (z.B. Datenübertragung) zugreift [3].

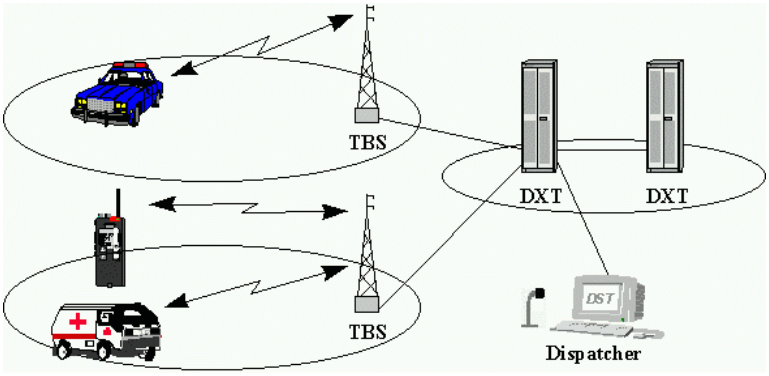


**Abbildung 7** Die TETRA-Architektur [23]

Die TETRA-Basisstation hat die Aufgabe, die "Funkkommunikation in die Festnetzinfrastruktur überzuleiten" [5, S. 36], enthält also eine Sende- und Empfangseinheit und stellt damit eine Schnittstelle zur Festnetzinfrastruktur dar.

Die DXT ist eine logische Datenbank, die Teilnehmerprofile speichert. Der oft auch als Switching & Management Infrastructure (**SwMI**) bezeichnete Verbindungsvermittler regelt auch die Authentifizierung der Teilnehmer [3], [5].

Die Leitstelle (in der Abbildung "Dispatcher", deutsch: Disponent) ist für die Dokumentation des Funkverkehrs, die Teilnehmerverwaltung, Kurzdatendienste (z.B. Statusmeldungen) und die Alarmierung zuständig.

Die zwei wichtigsten, standardisierten Funkschnittstellen sind das **Air Interface** (AI), welches die "Grundlage für die Kommunikation der Mobilstationen mit der festen Netzinfrastruktur" [4, S. 456] darstellt, und das **AI Direct Mode Operation**

($AI_{DMO}$), das die "Funkschnittstelle für die direkte Kommunikation zwischen Mobilstationen" [4, S. 456] bildet.

### 2.3.3 Digitalisierung

Beim analogen Funk werden Signale kontinuierlich übertragen und sind durch eine bestimmte physikalische Größe gekennzeichnet und messbar.

Moderne Mobilfunksysteme dagegen übertragen Signale ausschließlich digital. Dadurch entstehen einige Vorteile, beispielsweise ist die Übertragung weniger fehleranfällig, kann digital gespeichert werden und bietet die Möglichkeit, Verschlüsselung einzusetzen.

Zur Umsetzung des akustischen Signals der menschlichen Sprache in ein Digitalsignal wird ein **Analog-Digital-Umsetzer** (ADU) verwendet [5].

### 2.3.4 Betriebsfunktionen und Dienste

Um die gesamte Bandbreite der TETRA-Dienste nutzen zu können, sind die Funkgeräte im Gegensatz zum analogen System in einem Netzbetrieb integriert. Sie behalten sich aber die Möglichkeit vor, z.B. bei Störungen in einen direkten Modus zu wechseln [5].

#### 2.3.4.1 Netzbetrieb (Trunked Mode Operation, TMO)

Um im Netzbetrieb (englisch: Trunked Mode Operation, **TMO**) arbeiten zu können, muss das Funkgerät sich authentifizieren, d.h. bei Inbetriebnahme wird die nächstgelegene Basisstation kontaktiert und mit der Vermittlungsstelle (DXT) die Schlüsselinformation ausgetauscht. Erst dann ist das Gerät im gesamten Netz zu erreichen.

TMO stellt mehrere Betriebsfunktionen zur Verfügung:

- **Notruf**: Alle Funkgeräte verfügen über eine Notruf-Taste, die als Ziel entweder die Leitstelle oder eine vorher definierte Gruppe hat. Der Notruf erhält Priorität, d.h., andere Verbindungen werden im Bedarfsfall unterbrochen.
- **Telefonanruf**: Es können Gespräche im **Gegensprechmodus**[15] geführt werden. Dabei sind auch Verbindungen in andere Funk- und Telefonnetze möglich.
- **Gruppenruf**: Im Digitalfunknetz können statisch (im Gerät gespeichert) oder dynamisch (über das Netzmanagement/Luftschnittstelle) Gruppen gebildet werden. Damit sind die Gruppen unabhängig von physikalischen Frequenzen, d.h., bei Anwahl einer Gruppe werden alle darin definierten Geräte kontaktiert.
- **Einzelruf**: Im Gegensatz zum Telefonat sprechen die Teilnehmer abwechselnd miteinander (**Wechselsprechen**), nachdem das Netzmanagement die Verbindung zugelassen hat [5].

[15] Die Gesprächsteilnehmer können gleichzeitig miteinander reden und müssen nicht warten, bis der andere die Sprechtaste freigibt.

### 2.3.4.2 Direktbetrieb (Direct Mode Operation, DMO)

Falls keine Verbindung zur Verfügung steht oder benutzt werden soll, kann am Funkgerät der Direktbetrieb gewählt werden (engl.: Direct Mode Operation, **DMO**). Die Endgeräte funktionieren dann ohne physikalisches Netz, d.h., innerhalb eines durch die Sendeleistung vorgegebenen Radius. Alle Geräte, die auf dieselbe Frequenz eingestellt sind, können erreicht werden (Abb. 8).

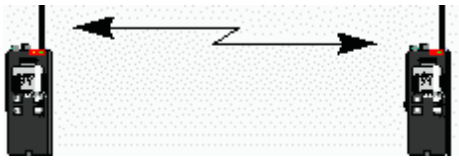

**Abbildung 8** Einfaches DMO-Gespräch zwischen zwei Funkgeräten [23]

Um die Reichweite zu erhöhen, kann ein **Repeater** eingesetzt werden, d.h., ein in einem Fahrzeug installiertes Endgerät wird zwischengeschaltet und reicht das Signal weiter (Abb. 9).


**Abbildung 9** Erhöhung der Reichweite durch Repeater-System [23]

Wenn das TETRA-Netz nicht erreichbar ist (z.B. Einsatz in einem Gebiet, das in einem Funkschatten liegt), kann ein Fahrzeug als **Gateway** verwendet werden. Das heißt, die Verbindung zwischen dem DMO- und dem TETRA-Netz wird somit überbrückt (Abb. 10).

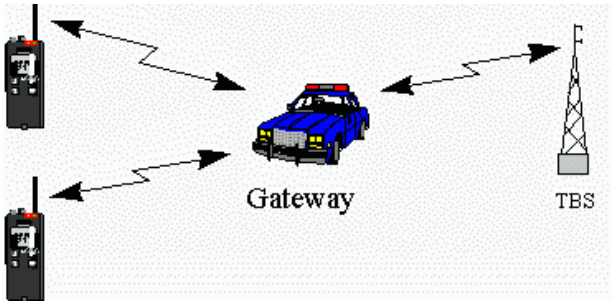


**Abbildung 10** Verbindung in das TETRA-Netz mittels Gateway [23]

### 2.3.4.3 Datendienste

Im Analogfunk ist es möglich, mittels **FMS** (Funkmeldesystem) **Statusmeldungen** zwischen Fahrzeug und Leitstelle zu versenden, zum Beispiel, um einen Notruf abzusetzen oder sich einsatzbereit zu melden. Für die Leitstelle ergibt sich damit die Möglichkeit, den Überblick über den Einsatz-Status der Fahrzeuge zu behalten, außerdem wird der Funkverkehr entlastet [24].

TETRA übernimmt die Möglichkeit, Statusmeldungen zu versenden [3]. Anders als beim Analogfunk sind die meisten nicht festgelegt und können je nach Organisation frei definiert werden, z.B. "Frei auf Funk" oder "Patient aufgenommen".

Neu ist auch die Übermittlung von Kurztextdaten (SDS, **Short Data Service**). Diese sind mit der aus dem öffentlichen Mobilfunk bekannten SMS vergleichbar. Sie können aber auch "an Gruppen, die Leitstelle oder andere EDV-Anwendungen verschickt werden" [5, S. 78].

Außerdem können größere Datenmengen wie zum Beispiel Fahndungsbilder oder Notarzt-Protokolle aus Rettungsmitteln übermittelt werden [7]. Da hierbei große Bandbreiten

nötig sind, werden die Informationen wie beim Internet nach dem **TCP/IP-Protokoll**[16] in Datenpakete aufgeteilt und diese nacheinander verschickt [5].

## 2.4 Kommunikationssicherheit

Die Hauptanforderung an das digitale Funksystem der BOS stellt die sichere Kommunikation dar. Ziel soll es sein, nur autorisierten Personen/Organisationen Zugriff zu ermöglichen, außerdem soll das System gegen Manipulationen und Störungen geschützt und die Authentizität der Informationen gewährleistet sein [26].

### 2.4.1 Allgemeines

Wird ein mobiles Endgerät eingeschaltet, erfolgt in zwei Richtungen zunächst die Authentifizierung: Das Netz überprüft auf Basis von Geräteadressen, ob das Funkgerät eine Berechtigung besitzt, und das Funkgerät prüft, ob das Netz verifiziert ist. Erst dann wird die Verbindung hergestellt und je nach verwendeter Sicherheitsklasse wird der Schlüssel berechnet [26].

### 2.4.2 Teilnehmer-Adressierung

Damit die in einem Netz angemeldeten Geräte unterschieden und zugeordnet werden können, sind ihnen zur Identifikation individuelle Nummern zugewiesen. Bei TETRA besitzt jedes Gerät mindestens eine **TSI** (TETRA Subscriber Identity), die fest auf dem Gerät gespeichert ist und nicht verändert werden kann.

Die TSI wird nach **ITSI** (Individual TSI) und **GTSI** (Group TSI) unterschieden. Erstere weist dem Gerät eine individuelle Rufnummer zu, die zum Beispiel für Anrufe genutzt wird. Letztere wird für Gruppenrufe benötigt [27].

Die TSI besteht aus drei Teilen (Abb.11): dem Mobile Country Code (MCC), dem Mobile Network Code (MNC) und der Short Subscriber Identity (SSI). Der dreistellige MCC dient zur Identifikation des Herkunftslandes (z.B. 262: Deutschland [19]), der MNC Kennzeichnung von Netzen innerhalb eines Landes. Es werden vier Typen von SSI unterschieden:

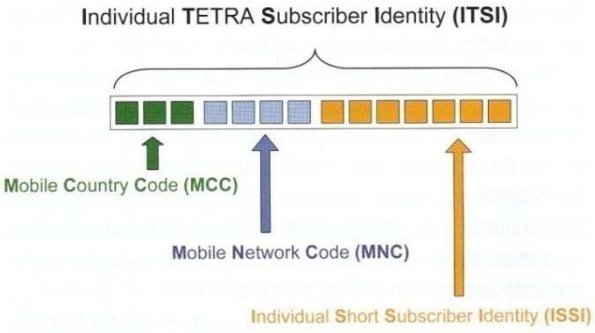


**Abbildung 11** Zusammensetzung der Individual TETRA Subscriber Identity (ITSI) [5]

- ISSI (Individual Short Subscriber Identity): Verwendung in der ITSI. Sie kennzeichnet ein Funkgerät innerhalb eines Netzes eindeutig.
- GSSI (Group Short Subscriber Identity): Verwendung in der GTSI. Mit ihr können Gesprächsgruppen identifiziert werden.
- ASSI (Alias Short Subscriber Identity): Adressierung fremder Netzteilnehmer.
- TETRA-Systemadressen [27].

[16] Transmission Control Protocol/Internet Protocol, Protokoll-Gruppe für die Vermittlung und den Transport von Datenpaketen in einem Netzwerk [25]

Statt der "Funkrufnamen" im Analogfunk (z.B. "Stephan 12/1") werden andere Teilnehmer im Digitalfunknetz an der **Operativ-Taktischen Adresse (OPTA)** erkannt, die bei jeder Funkverbindung automatisch vom Sender zum Empfänger übertragen wird. Sie umfasst maximal 24 Zeichen (Abb. 12). Die ersten beiden Ziffern kennzeichnen das Bundesland, die folgenden drei die Behörde bzw. Organisation, die nächsten drei die Region und die restlichen Zeichen enthalten je nach Organisation weitere Zuordnungsziffern wie z.B. Funkrufname, Ortsverband/Wache oder Funktionszuordnung. Es ist zu unterscheiden zwischen dem gesprochenen Rufnamen, der OPTA und der Darstellung des Senders im Display.


**Abbildung 12** Zusammensetzung der Operativ-Taktischen Adresse (OPTA) [5]

Wird zum Beispiel ein Teilnehmer per Funk angesprochen, erscheint die OPTA des Senders im Display des Empfängers (z.B. Sender: "Stephan 12/1", OPTA wie in Tab. 1) [28].

| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | Y | P | O | L | B | A | | S | T | E | P | H | A | N | | 1 | 2 | / | 0 | 1 | | | |

**Tabelle 1** Beispiel für eine OPTA von "Stephan 12/1", einem Einsatzfahrzeug der Polizei Bamberg/Bayern

## 2.4.3 Authentifizierung

TETRA unterstützt die **gegenseitige Authentifizierung** von Mobiler Station (MS) und dem Netzwerk – so kann das TETRA-System unberechtigten Zugriff verhindern, und die MS überprüfen, ob das Netzwerk verifiziert ist. Damit kann zum Beispiel einem sog. Man-in-the-Middle-Angriff vorgebeugt werden. Bei diesem Angriff wird eine modifizierte Funkstation präpariert, in die sich die MS einloggt, die Verschlüsselung wird ausgehebelt und ein Angreifer kann mithören oder in den Funkverkehr eingreifen. Bei GSM sind solche Täuschungen möglich, da nur einseitig "kontrolliert" wird, TETRA dagegen verhindert dies durch die gegenseitige Überprüfung der Berechtigung.

Erst nach erfolgter Authentifizierung kommt die Verbindung zustande.

DMO nutzt keine Authentifizierung, da die MS in diesem Fall keine Verbindungen in das Netz aufnehmen [26].

## 2.4.4 Schlüsselbildung und –management

Nachdem die Verbindung zwischen MS und Netz hergestellt ist, wird mit dem TETRA Authentication Algorithm 1 (TAA 1) der Schlüssel für die **Funkschnittstellenverschlüsselung** (engl.: Air Interface (AI) Encryption) gebildet.

Dabei gibt kommen **drei Sicherheitsklassen** zur Anwendung:

- Klasse 1: Keine AI-Verschlüsselung
- Klasse 2: Statischer Schlüssel (SCK, Static Cipher Key)

- Klasse 3: Dynamischer Schlüssel (DCK, Derived Cipher Key) [26], [6].

Im deutschen BOS-Funk wird grundsätzlich Sicherheitsklasse 3 eingesetzt. Klasse 1 und 2 werden v.a. von anderen professionellen Anwendern (Sicherheitsdienste, Verkehrsgesellschaften, Energieversorger, etc.) benutzt, da die Implementierung der bei Klasse 3 verwendeten Technologie komplex ist [30].

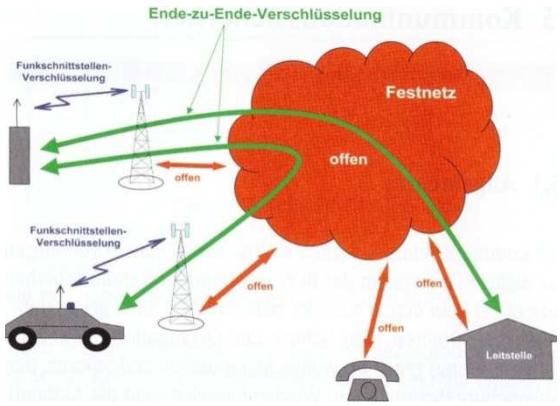


**Abbildung 13** Verschlüsselung an den Funkschnittstellen [5]

Speziell im deutschen Digitalfunk besitzt jedes Gerät eine **BOS-Sicherheitskarte** (ähnlich SIM-Karte, Abb. 14), um die Ver- und Entschlüsselung in den Geräten zu gewährleisten. "Die Daten und notwendigen Algorithmen befinden sich als zusätzliche Applikation auf der BOS-Sicherheitskarte" [5, S. 101]. Es wurde ein Schlüssel-Management entwickelt, das auf der Basis von Zertifikaten den Endteilnehmer berechtigt, Schlüssel anzufordern und weiterzuleiten. Vom Bundesamt für Sicherheit in der Informationstechnik (BSI) werden die Kryptoalgorithmen und Registrierungsdaten in die Sicherheitskarten geladen (**Initialisierung**). Die Sicherheitskarten werden anschließend einem Funkgerät oder einer Person mobil oder fest zugeordnet (**Personalisierung**). Erst mit einer freigeschalteten Sicherheitskarte kann der Benutzer sich in das TETRA-Netz einwählen. Zusätzlich können Daten wie z.B. Gruppenadressen, SDS-Nachrichten oder DMO-Frequenzen sicher gespeichert werden. Ähnlich wie beim GSM-Netz verwendet die BOS-Sicherheitskarte die PIN/PUK-Funktion[17]. Außerdem ist die OPTA auf der Karte gespeichert. Gestohlene oder verlorene Geräte können anhand der fest zugewiesenen Nummern deaktiviert bzw. gesperrt werden.


**Abbildung 14** BOS-Sicherheitskarte [7]

Nach einem Beschluss von Bund und Ländern sind alle Daten im Digitalfunknetz **Ende-zu-Ende zu verschlüsseln** (das entspricht Sicherheitsstufe 3).

Voraussetzung für die Verschlüsselung stellt das Vorhandensein eines digitalen Signals dar. Dazu wird zunächst das analoge Sprachsignal digitalisiert (siehe 2.3.3: Digitalisierung). Diese Daten werden mit generierten Schlüsseldaten der Sicherheitskarte verschlüsselt [5].

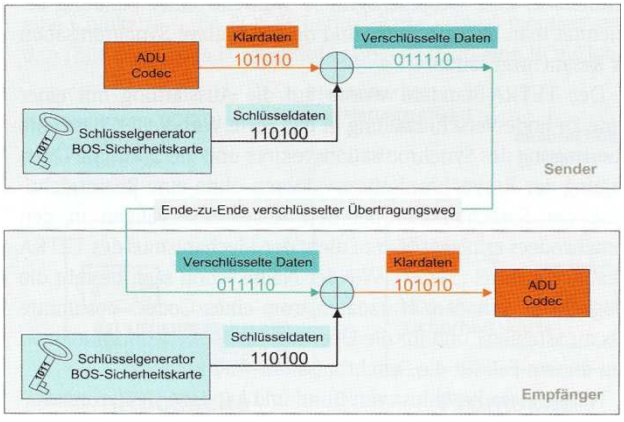


**Abbildung 15** Prinzip der Verschlüsselung [5]

In Schengen-Staaten wird dazu von Behörden der Verschlüsselungsalgorithmus

[17] PIN: Personal Identification Number, PUK: Personal Unblocking Key. Beim Einschalten fordert das Gerät eine PIN, mit der sich der Nutzer freischalten muss. Bei mehrmalig falscher Eingabe wird die PUK abgefragt.

**TEA2** (TETRA Encryption Algorithm 2) verwendet [6]. Viele Sicherheitsbehörden nutzen auf ihre Bedürfnisse zugeschnittene Algorithmen für die Luftschnittstellenverschlüsselung. Für die Ende-zu-Ende-Verschlüsselung sind mehrere Methoden möglich: Eine Organisation kann ein eigenes Kryptographie-Modell anwenden oder öffentlichen Standards folgend diese kryptographischen Funktionen mit dem IDEA[18]- oder AES-Algorithmus[19] individuell realisieren[20] [26].

Anschließend werden die doppelt verschlüsselten Datenpakete an den Empfänger übertragen.

Dieser kann mit dem auf der Schlüsselkarte gespeicherten Schlüsselgenerator die Datenpakete wieder entschlüsseln und damit das Signal wieder in akustischen oder optischen Klartext übertragen.

Die Schlüssel werden von den Leitstellen verwaltet, zugewiesen und regelmäßig gewechselt [5].

## 2.5 TETRA in Deutschland

"Ursprünglich hätte der Digitalfunk bereits bundesweit zur Fußball-Weltmeisterschaft im Jahr 2006 in Betrieb gehen sollen. Die Kosten sind mittlerweile auf mehr als 900 Millionen Euro gestiegen", schrieben die Nordbayerischen Nachrichten am 15. März 2012.

Das Digitalfunknetz der BOS wird in Deutschland derzeit aufgebaut. Es sind 4500 Basisstationen geplant, von denen Anfang Juni 2013 3210 in das Netz integriert worden waren. Das Netz ist in den meisten Bundesländern bereits etabliert, der Aufbau ist jedoch noch nicht vollständig abgeschlossen [31].

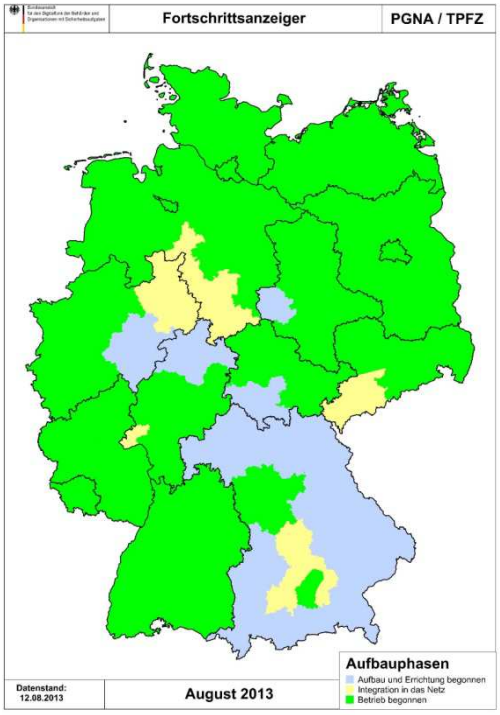


**Abbildung 16** Fortschritt des Netzausbaus in Deutschland im August 2013 [31]

### 2.5.1 Hintergrund der Einführung des Digitalfunks für die Behörden und Organisationen mit Sicherheitsaufgaben

Allen Behörden und Organisationen mit Sicherheitsaufgaben (BOS) soll das neue TETRA-Netz bundesweit zur Verfügung stehen. Die Zusammenarbeit der Organisationen z.B. bei Großschadenslagen soll vereinfacht werden. Durch die Struktur gäbe es ein flächendekkendes Netz.

Das Netz ist außerdem gegen unberechtigten Zugriff und Manipulationen geschützt, da

[18] International Data Encryption Algorithm: Verschlüsselungsalgorithmus, der lange Zeit als sicher angesehen wurde.
[19] Advanced Encryption Standard: Patentfrei verfügbarer Verschlüsselungsalgorithmus, der ein hohes Maß an Sicherheit bietet.
[20] Über die in Deutschland verwendeten Verschlüsselungsmethoden liegen keine Informationen vor.

es neben der Funkschnittstellenverschlüsselung zusätzlich eine Ende-zu-Ende-Verschlüsselung nutzt.

Das TETRA-Netz ermöglicht sowohl Einzel- als auch Gruppenkommunikation, es können einsatzbezogene Gruppen gebildet werden.

Durch das Bündelfunk-Verfahren werden Frequenzen ohne Verluste bei der Sprachqualität ökonomischer genutzt.

Ein weiteres Kennzeichen ist die Einführung der Notruftaste, womit sofort vorrangig die Leitstelle kontaktiert wird. Je nach Ausstattung der Endgeräte ist es zum Beispiel möglich, Positionsdaten zu übermitteln, Bilder zu versenden oder Statusmeldungen abzusetzen [31].

Das Netz ist unabhängig von Netzbetreibern und damit gebührenfrei im Netzbetrieb [32].

### 2.5.2 Nachteile, Kritik und Widerstand

In Deutschland werden sowohl durch die Bevölkerung als auch von Anwendern Argumente gegen den Digitalfunk angebracht.

Das Hauptargument gegen TETRA stellt die Gefährdung der Gesundheit dar. Durch die Anwendung von relativ niedrigen Frequenzen werden eine Vielzahl von Symptomen und unterschiedlichen Krankheitsbildern postuliert, die mittlerweile in mehreren Studien untersucht wurden, bislang jedoch noch keine konkreten Ergebnisse nachweisen konnten, die möglicherweise erst in prospektiven Langzeitstudien präzisiert werden können [34].

Ein weiteres Argument von Kritikern ist die Finanzierung des TETRA-Projektes. Oft wird die Frage gestellt, ob ein Ausbau des Analogfunks kostengünstiger gewesen wäre, da die genaue Entwicklung der Kosten unklar ist, bislang existieren nur grobe Schätzungen über die finanziellen Aufwendungen des Projektes und über die noch ausstehenden Kosten für den bundesweiten, flächendeckenden Einsatz und den Erhalt und Ausbau der vorhandenen Infrastruktur [35].

Es wird über unterschiedliche systembedingte Ausfälle berichtet, ein konkretes Problem stellen die durch die geographischen Gegebenheiten bedingten noch vorhandenen regionalen Funkschatten dar [36].

Im Vergleich zu anderen Systemen wie LTE oder UMTS sind die Übertragungsgeschwindigkeiten bei TETRA eher niedrig. So kann es dazu kommen, dass das Netz bei der Übertragung großer Datenmengen wie z.B. von Bildern überlastet wird und so der normale Funkverkehr eingeschränkt wird [33]. Eine Neukonfiguration von Gruppen, wie sie beispielsweise bei Katastrophen erforderlich wäre, ist zeitintensiv und kann zu Verzögerungen führen [37].

Es werden zudem Zweifel an der Sicherheit des bereits in den 1990er-Jahren entwickelten TETRA-Systems angebracht. Zwar wird in Deutschland zusätzlich die Ende-zu-Ende-Verschlüsselung eingesetzt, doch es könnte in naher Zukunft möglich sein, mit leistungsstarken Computern das System zu manipulieren [30].

# 3 Fazit

Mit welchem Funknetz die antiken Götter kommunizieren würden, wissen nur sie selbst, doch es existiert ein großes Repertoire an öffentlichen und nichtöffentlichen Lösungen für den Mobilfunk, das sich auch stetig weiterentwickelt.

Auf dem Markt für den öffentlichen Mobilfunk erscheinen ständig neue Technologien, die immer schneller und leistungsfähiger werden. So wird bereits über den Nachfolger von LTE und der Erweiterung LTE-Advanced spekuliert, obwohl LTE sich noch im Netzaufbau befindet [38].

Der Trend geht nach wie vor weg vom klassischen Personal Computer hin zu Smartphones und Tablet-Computern. Für die mobilen Geräte werden immer mehr Applikationen und Dienste entwickelt, die höhere Übertragungsgeschwindigkeiten erfordern [39].

Die größte Schwachstelle der mobilen Geräte stellt aber immer noch die Stromversorgung dar: Hochauflösende Displays und schnelle Rechenleistung benötigen viel Energie.

Smartphones haben dennoch ihren Platz im Alltag gefunden, da man überall erreichbar ist, jederzeit Zugriff auf das World Wide Web hat, damit navigieren kann oder einkaufen, Filme ansehen oder Spiele konsumieren und eine Vielzahl weiterer Optionen in Anspruch nehmen kann. Vor zehn Jahren wurden Postkarten geschickt, vor fünf Jahren E-Mails oder SMS gesendet und diese werden nun zunehmend durch soziale Netzwerke wie beispielsweise "Facebook" oder "Twitter" abgelöst. Mit den miniaturisierten Geräten, den "Computern für die Hosentasche", hat man überall und jederzeit Zugriff auf Anwendungen aller Art.

Die Frage, ob nicht auch Behörden und Organisationen mit Sicherheitsaufgaben (BOS, z.B. Polizei, Feuerwehr) die vielfältigen Möglichkeiten der öffentlichen Mobilfunksysteme nutzen sollten, ist daher berechtigt.

Die speziell von professionellen Mobilfunknutzern gestellten Anforderungen setzen ihren Schwerpunkt auf ein hohes Maß an Abhörsicherheit, welche momentan nur von UMTS und LTE garantiert wird. Das System TETRA hingegen bietet durch die Möglichkeit einer implementierten BOS-Sicherheitskarte andere wichtige Merkmale.

In der Praxis werden beim Einsatz der BOS vor allem viele kurze Mitteilungen gesendet, die einen schnellen Gesprächsaufbau bedingen: Der nach wie vor erforderliche Wahlvorgang beim Gebrauch des öffentlichen Mobilfunknetzes verkürzt sich in der Anwendung des BOS-Funks auf die Betätigung der Sprechtaste, die sofort eine Verbindung aufbaut.

Nur das TETRA-Netz ist in der Lage, dynamische Einsatz-Gruppen zu bilden, um alle beteiligten Kräfte schnell informieren zu können. Ein BOS-spezifisches Netz soll beispielsweise die Möglichkeit bieten, alle Kräfte in einem Funkverkehrsbereich gleichzeitig über eine Fahndung zu informieren.

Den Leitstellen fällt dabei eine Schlüsselrolle zu, da sie Einsätze und Gruppen koordinieren und mit Hilfe von Funkmeldesystemen Statusmeldungen verwalten. Die Leitstelle hat eine Vorrangfunktion vor anderen Funkteilnehmern und empfängt übergeordnete Not-

rufe.

Systeme wie TETRA bieten die Möglichkeit, netzunabhängig eine lokale Einsatzgruppe einzurichten, um beispielsweise auch in einem Katastrophenfall in einem entlegenen Gebiet trotzdem eine stabile Kommunikation zu gewährleisten [40].

TETRA ist zwar in der Lage, Bilddateien und größere Datenpakete zu übertragen, allerdings nur unter Beanspruchung einer sehr hohen Netzkapazität. Deswegen weichen Einsatzkräfte zur Vermeidung zeitlicher Verluste häufig auf Mobiltelefone aus.

Die TETRA-Endgeräte können nicht auf vorhandene Datenbanken und Informationssysteme, z.B. der Polizei, zugreifen und müssen nach wie vor die Leitstelle konsultieren. Deshalb werden von verschiedenen Organisationen Einsatzfahrzeuge mit speziellen Computern ausgestattet, die beispielsweise über LTE eine Anbindung an diese Datenbanken ermöglichen. Dadurch werden Betriebsabläufe zeitlich und personell optimiert, da dies zu einer Entlastung der Leitstellen führt und den Einsatzkräften vor Ort sofort die gewünschte Information zur Verfügung steht [41].

Das in Deutschland eingeführte TETRA-Netz bietet Funktionen, die für professionelle Anwender elementar sind und die von öffentlichen Netzen nicht unterstützt werden. Dennoch erscheint es sinnvoll, sich nicht vollständig auf ein System zu verlassen, sondern auch die Vorteile anderer Techniken zu nutzen. So können zum Beispiel umfangreiche Daten wie Bilddateien über leistungsstarke öffentliche Netze übertragen werden, während mobile Computersysteme Datenbankanfragen durchführen.

Die am TETRA-System geäußerte Kritik gilt es ernst zu nehmen, aufzuarbeiten und offen zu diskutieren. Daher sollten Bürger und Anwender detailliert informiert werden und insbesondere sind prospektive, wissenschaftlich abgesicherte Untersuchungen zu fördern, um ein mögliches Gefährdungspotential für die Gesundheit auf ein Minimum zu reduzieren.

Es wird bereits an einer Weiterentwicklung von TETRA gearbeitet, die mit LTE verknüpft ist. Zielführend steht dabei eine Steigerung der Übertragungsgeschwindigkeiten im Vordergrund. Der dazu erforderliche zeitliche Rahmen, um die dazu erforderlichen Technologien zu entwickeln, ist zur Zeit noch umgewiss, da zunächst eine Einigung auf einen geeigneten Frequenzbereich getroffen werden muss, der möglichst europaweit genutzt werden kann [42].

Mit TETRA wird ein Technologiesprung vollzogen, der der Entwicklung der Technik in den letzten Jahren gerecht wird. Doch es ist auch notwendig, mit dem Fortschritt der Kommunikationssysteme mitzuhalten und bestehende Technologien stetig weiterzuentwickeln. Besonders Anwender der BOS, aber auch Vertreter aus Industrie und Verkehrsbetrieben brauchen ein modernes und zuverlässiges Kommunikationssystem, das ihnen Protektion für sensible Informationen und einen effektiven Schutz vor Angriffen bietet. Die einsatzspezifischen Funktionen müssen auf dem aktuellsten Stand der Technik gehalten werden, damit weiterhin ein störungsfreier Ablauf in den vorhandenen Infrastrukturen gegeben ist, und unsere Sicherheit gewährleistet bleibt.

# Anhang A: Quellen und Abbildungen, Abkürzungen, CD-ROM

## A.1 Literaturverzeichnis


[1] *V. Jung/H.-J. Warnecke (Hrsg.)*: Handbuch für die Telekommunikation, 1. Auflage, Springer 1998

[2] *B. Walke*: Mobilfunknetze und ihre Protokolle Band 1. Grundlagen, GSM, UMTS und andere zellulare Mobilfunknetze, 2. Auflage, Teubner 2000

[3] *B. Walke*: Mobilfunknetze und ihre Protokolle Band 2. Bündelfunk, schnurlose Telefonsysteme, W-ATM, HIPERLAN, Sattelitenfunk, UPT, 2. Auflage, Teubner 2000

[4] *F. Bergmann/H.-J. Gerhardt (Hrsg.):* Taschenbuch der Telekommunikation, Leipzig 1999

[5] *P. Hartl/G. Merzbach*: Digitalfunk, 2. Auflage, Kohlhammer 2010

[6] *ETSI EN 300 392-7*: Terrestrial Trunked Radio; Voice plus Data; Part 7: Security, V2.1.1, European Telecommunications Standards Institute 2001


## A.2 Internetquellen


[7] *Christiansen, Jens* (2012): "TETRA (Terrestrial Trunked Radio)", www.digitaler-bos-funk.de (Aufruf: 18.08.2013)

[8] (o.J.): "Daten und Fakten zu Mobilfunk in Deutschland". www.mobilfunk-geschichte.de (Aufruf: 01.07.2013)

[9] *Wikipedia* (Hrsg., 2013): "Global System for Mobile Communications". de.wikipedia.org/wiki/GSM (Aufruf: 03.07.2013)

[10] *ETSI* (Hrsg., o.J.): "Mobile technologies GSM". www.etsi.org/technologies-clusters/technologies/mobile/gsm (Aufruf: 03.07.2013)

[11] *Wikipedia* (Hrsg., 2013): "Universal Mobile Telecommunications System", de.wikipedia.org/wiki/Universal_Mobile_Telecommunications_System (Aufruf: 04.07.2013)

[12] (o.J.): "Mediengeschichte des 19. und frühen 20. Jahrhunderts: Telegrafie". www.kreimeier-online.de/Mediengeschichte_05.htm (Aufruf: 04.07.2013)

[13] *Wikipedia* (Hrsg., 2013): "Telefonie". de.wikipedia.org/wiki/Telefonie (Aufruf: 04.07.2013)

[14] *Wikipedia* (Hrsg., 2013): "Funktechnik". de.wikipedia.org/wiki/Funktechnik (Aufruf: 04.07.2013)

[15] *3GPP* (Hrsg., o.J.): "About 3GPP", www.3gpp.org/About-3GPP (Aufruf: 04.07.2013)

[16] *3GPP* (Hrsg., o.J.): "LTE", www.3gpp.org/LTE (Aufruf: 04.07.2013)

[17] *3GPP* (Hrsg., Mai 2012): "LTE-Advanced", www.3gpp.org/LTE-Advanced (Aufruf: 04.07.2013)

[18] *Wikipedia* (Hrsg., 2013): "Long Term Evolution", de.wikipedia.org/wiki/LTE (Aufruf: 14.08.2013)

[19] *Wikipedia* (Hrsg., 2013): "Terrestrial Trunked Radio" de.wikipedia.org/wiki/TETRA (Aufruf: 14.08.2013)

[20] *The TETRA + Critical Communications Association* (Hrsg., o.J.): www.tandcca.com/about/page/12320 (Aufruf: 20.07.2013)

[21] *TETRA Industry Group* (2013), www.tetrahealth.info/worldCountries.htm

[22] (o.J.): "Zeitmultiplexverfahren". www.uni-protokolle.de/Lexikon/Zeitmultiplexverfahren.html (Aufruf: 16.08.2013)
[23] *Janne Tervonen*, Übersetzung aus dem Finnischen: Einführung in TETRA (24.05.1998), www.intellectics.com/tetra.html (Aufruf: 20.07.2013)
[24] *Feuerwehrverband Ostfriesland e.V.* (Hrsg., April 2007): "Die Ausbildung zum Sprechfunker". www.ostfriesische-feuerwehren.de/pdf-Dateien/Sprechfunker.pdf (Aufruf: 20.07.2013)
[25] *Elektronik Kompendium* (Hrsg., o.J.): "TCP/IP". www.elektronik-kompendium.de/sites/net/0606251.htm (Aufruf: 18.08.2013)
[26] *TETRA MoU Association* (Hrsg., Februar 2006): TETRA Security, www.tandcca.com/Library/Documents/About_TETRA/TETRA%20Security%20pdf.pdf (Aufruf: 24.07.2013)
[27] *Wipperfürth, Detlef* (02.05.2013): "TETRA (Terrestrial Trunked Radio)". funkfrequenzen01.de/index002.htm (Aufruf: 05.05.2013)
[28] *Ausschuss für Informations- und Kommunikationswesen des Arbeitskreises V der Ständigen Konferenz der Innenminister und Senatoren der Länder* (Hrsg., 08.03.2010): Richtlinie für die operativ-taktische Adresse (OPTA) im Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben, www.idf.nrw.de/projekte/ardini/dokumente/opta_richtlinie_mrz2010_20100408.pdf (Aufruf: 17.08.2013)
[29] www.trunking.nu/tetra-logo.jpg
[30] *Rettungsdienst.de* (Hrsg., Juni 2011): "Hacker knackt Tetra-Digitalfunk". www.rettungsdienst.de/nachrichten/hacker-knackt-tetra-digitalfunk-23556 (Stand: Juni 2011)
[31] *Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben* (Hrsg., 2013), www.bdbos.bund.de/cln_329/nn_1358092/DE/Bundesanstalt/Projekt__Digitalfunk/Netzaufbau__Roll__out/Fortschrittsanzeiger/fortschrittsanzeiger__roll__out__node.html?__nnn=true (Aufruf: 19.08.2013)
[32] (2009): "Vorteile und Nachteile von TETRA Funk". www.vkd-gmbh.de/Fernwirken/Tetra-Funk/Tetra_Vor-_und_Nachteile/tetra_vor-_und_nachteile.html (Stand: 2009)
[33] *Wikipedia* (Hrsg., 2013): "Terrestrial Trunked Radio". en.wikipedia.org/wiki/Terrestrial_Trunked_Radio (Aufruf: 18.08.2013)
[34] *Ronny Weikl* (Mai 2013): "Was ist TETRA-Funk?". www.stoppt-tetrafunk.de/was_ist_tetrafunk.php (Aufruf: 19.08.2013)
[35] *Diagnose Funk* (Hrsg., 06.05.2013): "TETRA: Ein finanzieller Blindflug". diagnose-funk.org/themen/behoerdenfunk/tetra/tetra-veraltete-technik-und-finanzieller-blindfl.php (Aufruf: 19.08.2013)
[36] *Garmatter, Ralf* (Januar 2011): "'Viele Argumente sprechen gegen Tetra-Funk' – Informationsveranstaltung am Mittwoch in Kirchberg/Jagst". www.hohenlohe-ungefiltert.de/?p=9643 (Aufruf: 19.08.2013)
[37] *Diagnose*-Funk (Hrsg., 15.12.2011): "Faktensammlung TETRA – Digitaler BOS-Funk". diagnose-funk.org/assets/df_tetra-fakten.pdf (Aufruf: 19.08.2013)
[38] *Chip-Online* (Hrsg., 21.01.2013): Mobilfunk der Zukunft: LTE-Advanced und 5G". business.chip.de/artikel/Mobilfunk-der-Zukunft-LTE-Advanced-und-5G-4_59986470.html (Stand: 21.01.2013)
[39] *Telecom Handel* (Hrsg., 09.07.2013): "Smartphone-Technologie: Das bringt die Zukunft". www.telecom-handel.de/Marktreports/Mobilfunk/Smartphone-Technologie-Das-bringt-die-Zukunft (Aufruf: 20.08.2013)
[40] *Horst Beckebanze* (o.J.): "Warum setzen die BOS nicht einfach auf öffentliche

Mobilfunknetze?". www.pfa.nrw.de/PTI_Internet/pti-intern.dhpol.local/Funk/Aufsatz_UMTS.pdf.html (Aufruf: 20.08.2013)
[41] *Invidis* (Hrsg., 04.07.2013): "Bayerns Polizei wrackt CarPCs ab – und schafft CarPads an". invidis.de/2013/07/tablets-bayerns-polizei-wrackt-carpcs-ab-und-schafft-carpads-an/ (Aufruf: 20.08.2013)
[42] *Behördenspiegel* (September 2011): Breitbandkommunikation – Die Zukunft des BOS-Digitalfunks. solutions.3mdeutschland.de/3MContentRetrievalAPI/BlobServlet?lmd=1330345042000&locale=de_DE&assetType=MMM_Image&assetId=1319216259175&blobAttribute=ImageFile (Aufruf: 20.08.2013)
[43] *Wikipedia* (Hrsg., 2013): "Global System for Mobile Communications". de.wikipedia.org/wiki/GSM (Aufruf: 01.07.2013)

## A.3 Abbildungsverzeichnis



## A.4 Tabellenverzeichnis



## A.5 Abkürzungsverzeichnis

| | |
|---|---|
| 3GPP | 3rd Generation Partnership Project, Kooperationsprojekt von Standardisierungs-Organisationen |
| ADU | Analog-Digital-Umsetzer |
| AI | Air Interface, Funkschnittstelle |
| $AI_{DMO}$ | Air Interface Direct Mode Operation |
| ARIB | Association of Radio Industries and Business, japanische Standardisierungsorganisation und Mitglied des 3GPP |

| | |
|---|---|
| ATIS | Alliance for Telecommunications Industry Solutions, US-amerikanische Standardisierungsorganisation und Mitglied des 3GPP |
| BDBOS | Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben |
| BOS | Behörden und Organisationen mit Sicherheitsaufgaben, z.B. Feuerwehr, Polizei, Rettungsdienst |
| CEPT | Conférence Européenne des Administrations des Postes et des Télécommunications, deutsch: Europäische Konferenz der Verwaltungen für Post und Telekommunikation. Organisation für Zusammenarbeit von Regulierungsbehörden (z.B. Bundesnetzagentur) |
| DCK | Derived Cipher Key, Dynamischer Schlüssel |
| DCS1800 | Digital Cellular System at 1800 MHz, GSM-Frequenzband |
| DMO | Direct Mode Operation, Direktbetrieb zwischen Mobilstationen |
| DXT | Digital Exchange for TETRA, Datenbank |
| EDGE | Enhanced Data rates for Global Evolution, Verbesserung von GSM für schnellere Übertragungsraten |
| ETSI | European Telecommunications Standards Institute, deutsch: Europäisches Institut für Standardisierung in der Telekommunikation |
| FMS | Funkmeldesystem, System für Statusmeldungen im Analogfunk |
| GPRS | General Packet Radio System, GSM-Paketdatendienst |
| GSM | Global System for Mobile Telecommunications |
| GSSI | Group Short Subscriber Identity, Teil der GTSI |
| GTSI | Group TETRA Subscriber Identity, Teilnehmer-Adressierung |
| HSPA+ | High Speed Packet Access, UMTS-Erweiterung für höhere Übertragungsraten |
| ISSI | Individual Short Subscriber Identity, Teil der ITSI |
| ITSI | Individual TETRA Subscriber Identity, Teilnehmer-Adressierung |
| LTE | Long Term Evolution |
| MCC | Mobile Country Code, Teil der TSI |
| MNC | Mobile Network Code, Teil der TSI |
| MS | Mobile Station |
| NömL | Nichtöffentlicher mobiler Landfunk |
| öbL | öffentlicher beweglicher Landfunkdienst |
| PMR | Private Mobile Radio, "Jedermann-Funk" |
| SCK | Static Cipher Key, Statischer Schlüssel |
| SDS | Short Data Service, Kurznachrichten-Dienst |
| SIM | Subscriber Identity Module, Chipkarte zur Identifikation eines Mobilfunk-Teilnehmers |
| SMS | Short Message Service, Kurznachrichten-Dienst |
| SSI | Short Subscriber Identity, Teil der TSI |
| SwMI | Switching & Management Infrastructure, verwaltet TBS |
| TBS | TETRA Base Station, leitet die Funkkommunikation |
| TCP/IP | Transmission Control Protocol/Internet Protocol, Internet-Übertragungsprotokoll |
| TEA | TETRA Encryption Algorithm, Verschlüsselungs-Algorithmus |
| TETRA | Terrestrial Trunked Radio |
| TMO | Trunked Mode Operation, Netzbetrieb |
| TSI | TETRA Subscriber Identity, Teilnehmer-Adressierung |
| TTA | Telecommunications Technology Association of Korea, koreanische Standardisierungsorganisation und Mitglied des 3GP |
| TTC | Telecommunication Technology Committee, japanische Standardisie- |

| | |
|---|---|
| | rungsorganisation und Mitglied des 3GPP |
| UMTS | Universal Mobile Telecommunications System |

## A.6 CD-ROM

# Erklärung

Ich erkläre hiermit, dass ich die Seminararbeit ohne fremde Hilfe angefertigt und nur die im Literaturverzeichnis angeführten Quellen und Hilfsmittel verwendet habe. Insbesondere versichere ich, dass ich alle wörtlichen und sinngemäßen Übernahmen aus anderen Werken als solche kenntlich gemacht habe.

, den _____ _____