

TETRA und seine Anwendung bei Behörden und Organisationen mit Sicherheitsaufgaben

Daniel Baumann

Betreuer: Stephan Günther

Hauptseminar - Innovative Internettechnologien und Mobilkommunikation WS2011

Lehrstuhl für Netzarchitekturen und Netzdienste

Fakultät für Informatik, Technische Universität München

Email: daniel.baumann@in.tum.de

KURZFASSUNG

Dieses Paper behandelt den Bündelfunk-Standard TETRA und seine Anwendung bei Behörden und Organisationen mit Sicherheitsaufgaben. Dabei wird TETRA beschrieben und auf Layer 3 Nachrichten eingegangen, welche bei einem Gespräch entstehen. Des Weiteren werden Gründe diskutiert, weswegen der Analogfunk nicht mehr dem Stand der Technik entspricht und welche Vor- und Nachteile diese Techniken haben. Zudem werden Messergebnisse dargestellt, welche die Dauer eines Handovers und den Gesprächsablauf verdeutlichen.

1. EINLEITUNG

Bei Behörden und Organisationen mit Sicherheitsaufgaben (BOS) wird die Analogfunktechnik für die Kommunikation verwendet. Bei dieser Technik wird das Sprachsignal auf ein Trägersignal aufmoduliert und über Funk auf einer reservierten und zugeteilten Frequenz übertragen und ausgegeben. Der größte Vorteil ist, dass die Technik sehr einfach im Verhältnis zum neuen Digitalfunk ist. Aufgrund dieser simpleren Technik gibt es aber auch Einschränkungen. So ist es beim Analogfunk nicht möglich die Daten zu verschlüsseln oder über bestimmte Funknetzgrenzen hinweg zu kommunizieren, denn beim Analogfunk gibt es meist pro Landkreis ein Gebiet, dem eine gewisse Frequenz zugeteilt wird. Diese Frequenz stellt dann den Kommunikationskanal dar, auf dem die Organisation in diesem Landkreis kommuniziert. Es ist daher nicht möglich, über diesen Kanal mit einer Organisation in einem anderen Landkreis zu kommunizieren. Aufgrund dieser und weiterer Nachteile, welche die Kommunikation über Regierungsgrenzen erschwert, wurde 1995 der TETRA-Standard standardisiert. Im Kapitel 3 wird daher auf die schon angesprochenen Vor- und Nachteile auch im Bezug zur TETRA Digitalfunktechnik eingegangen. Das darauf folgende Kapitel 4 behandelt TETRA und gibt Einblicke in die Funktionsweise. Im Kapitel 5 wird die Umsetzung des TETRA Standards auf das deutsche Digitalfunknetz der BOS dargestellt. Danach wird im Kapitel 6 auf Messungen, welche mittels zwei TETRA-Mobiles und einer Messsoftware von Rohde und Schwarz¹ durchgeführt wurde, eingegangen.

2. VERWANDTE ARBEITEN

Diese Arbeit bezieht sich hauptsächlich auf das Buch „Aufbau und Technik des digitalen BOS-Funks“ von Christof

¹Elektronikkonzern mit Sitz in München (www.rohde-schwarz.de).

Linde[9] und auf die Dissertation Dimensionierung und Leistungsbewertung von TETRA-Bündelfunksystemen von Peter Sievering[10]. Zudem wurden genauere Details zum TETRA Standard aus dem Buch „Digital Mobile Communication and the TETRA System“[8] entnommen. Dieses Buch gibt einen umfangreicheren Einblick in den TETRA Standard. [9] gibt dagegen einen Einblick in den Digitalfunk aus Sicht der BOS und betrachtet somit eher eine abstrakte Sichtweise von TETRA.

3. DIGITALFUNK IM VERGLEICH ZUM ANALOGFUNK

Beim Analogfunk werden mehrere Funknetze für die verschiedenen BOS benötigt. Ein Grund dafür ist zum Beispiel, dass die Feuerwehr nicht die Gespräche der Polizei mithören kann oder deren Kanäle belegt. Durch die Analogfunktechnik sind aber meist die Funknetze auch auf Landkreisgrenzen beschränkt. Dies führt dazu, dass die Kommunikation von einem zum anderen Landkreis nicht einfach ist. Der Digitalfunk bietet dagegen allen BOS ein einheitliches, flächendeckendes Netz. Dadurch haben alle BOS in Deutschland neue Kommunikationsmöglichkeiten, welche die Zusammenarbeit vereinfachen und beschleunigen. Bei Großveranstaltungen oder Großschadenslagen können durch TETRA dynamische Gruppen erstellt werden, welche zum Beispiel Einheiten der Polizei und Feuerwehr auf die gleiche Kommunikations-Gruppen legt.[5]

Des Weiteren bietet der TETRA-Standard Abhörsicherheit, indem die Datenübertragung zwischen Endgerät und Basisstation (Luftschnittstelle) verschlüsselt wird. Zudem gibt es noch eine Ende-zu-Ende-Verschlüsselung, welche die Datenübertragung auch auf der restlichen Netzinfrastruktur schützt. Beim Analogfunk kann dagegen die Kommunikation, zum Beispiel der Polizei, mit der richtigen Frequenzwahl abgehört werden.[5]

Ein sehr wichtiger Punkt ist auch die Verbesserung der Sprach- und Empfangsqualität. Durch die Digitalisierung können Hintergrundgeräusche herausgefiltert werden und dies führt somit zu einer verbesserten Empfangsqualität. Beim Analogfunk werden keine Hintergrundgeräusche herausgefiltert und somit sind Gesprächspartner, welche in der Nähe von Maschinen wie zum Beispiel einem Löschfahrzeug stehen, sehr schwer zu verstehen.[5]

Da durch die Bündelfunktechnik² mehrere Gruppen die gleiche Frequenz verwenden können, besteht eine höhere Frequenzökonomie. Somit sind die Funkkanäle auch nur dann belegt, wenn sie tatsächlich genutzt werden. Mit „belegt“ ist hier die feste Zuordnung von Organisationen zu Frequenzbereichen gemeint. Dabei kann dieser Frequenzbereich zu einer bestimmten Zeit nicht verwendet werden, allerdings kann auch keine andere Organisation auf diese Frequenzen zugreifen, da diese fest zugeordnet sind. Beim Analogfunk werden im Moment parallel bis zu sechs voneinander unabhängige analoge Funknetze (Polizei, Bundespolizei, Feuerwehr, Rettungsdienst, THW, Katastrophenschutz und Zoll), jeweils im 2- und im 4-Meter-Bereich³ betrieben[1]. Zudem beansprucht dort jeder Kanal permanent einen Frequenzbereich. Daher kommt es bei Großschadenslagen auch regelmäßig zu Überlastungen. Alle Feuerwehren des Landkreises München haben zum Beispiel einen Kanal, auf dem diese mit der Leitstelle und untereinander kommunizieren können. Kommt es nun in Garching und Unterschleißheim zu einem Einsatz, bekommt jede der beiden Feuerwehren die Kommunikation der anderen mit und stören sich somit gegenseitig. Im schlimmsten Fall muss eine Feuerwehr mit der Nachforderung von Einsatzkräften warten, bis der andere sein Gespräch beendet hat. Mit TETRA könnte die Leitstelle beide auf verschiedene Kommunikations-Gruppen legen.[5]

Zudem bietet TETRA auch die Möglichkeit der Einzelkommunikation, welche es ermöglicht gezielt mit einem einzelnen Teilnehmer ein Funkgespräch zu führen. Beim Analogfunk können immer nur die Geräte erreicht werden, welche im gleichen Funknetz auf der gewählten Frequenz liegen. Durch die Wahl dieser Frequenz können somit auch immer beliebig viele Teilnehmer das Gespräch mitverfolgen. Somit ist eine Einzelkommunikation derzeit über Analogfunk nicht möglich.[5]

Eine sehr nützliche Funktion des Digitalfunks ist die Notruftaste. Durch das Drücken dieser Taste an den Endgeräten wird unter anderem ein Rufaufbau mit höchster Priorität zur Leitstelle veranlasst, welcher, falls das Funkgerät auch eine GPS-Empfänger hat, die aktuelle Position übermittelt und somit die Suche der verunglückten Einsatzkraft beschleunigt.[5]

4. TETRA

Das Kommunikationsnetz der BOS wurde 1995 aufgrund der europäischen Vereinheitlichung standardisiert. Dies geschah durch eine Projektgruppe des Europäischen Instituts für Telekommunikationsnormen (ETSI), welche ein einheitliches Funknetz für die europäischen Sicherheitsbehörden definieren sollte. Das Ergebnis war der dem Digitalfunknetz zugrunde liegende Standard TETRA. TETRA stand zu Beginn für

²Der Bündelfunk ist eine Mobilfunkanwendung für Sprach- oder Datenübertragung mit einer oder mehreren Versorgungszellen. In jeder Zelle sind mehrere Übertragungskanäle verfügbar, von denen einer dynamisch zugewiesen wird, wenn ein Verbindungswunsch signalisiert wird. Durch diese dynamische Kanaluweisung und durch die Bündelung mehrerer Kanäle werden eine sehr effiziente Frequenzausnutzung und eine hohe Verfügbarkeit gewährleistet.[6]

³Bei der Feuerwehr spricht man von der Wellenlänge statt Frequenz. Daher entspricht Fahrzeugfunk, welcher im 4-Meter-Bereich ist, dem 80-MHz-Bereich.

Trans European Trunked Radio. Allerdings wurde dieser Begriff später aus kommerziellen Gründen in Terrestrial Trunked Radio geändert. Durch diese Bündelfunktechnik ist es möglich vielen Teilnehmern bzw. Gruppen gemeinsam ein Kanalbündel zur Verfügung zu stellen. Es besteht somit eine logische Zuordnung zu Gesprächsgruppen, die nicht über Frequenzen definiert werden müssen. Der TETRA Standard wird nicht nur von Behörden verwendet sondern auch von Industrie- und Nahverkehrsbetrieben, wie zum Beispiel den Stadtwerke München(SWM).

4.1 TopLevel-Beschreibung

Im Folgenden wird TETRA aus TopLevel Sicht beschrieben. Dabei werden die zwei Betriebsarten, Trunked Mode Operation und Direct Mode Operation, und der funktionale Aufbau des digitalen Mobilfunknetzes TETRA dargestellt.

4.1.1 Trunked Mode Operation (TMO)

Die normale Betriebsart ist TMO, bei der die Mobilgeräte die Netzinfrastruktur nutzen, um eine Kommunikation mit anderen Funkgeräten aufzubauen. Zwei Modi, die im Trunked Mode zur Verfügung stehen, sind der TETRA Voice + Data (TETRA V+D) Mode und Packet Data Optimized Mode (TETRA PDO). Allerdings wird bei den BOS bisher nur TETRA V+D verwendet, welcher der gleichzeitigen Übertragung von Sprache und Daten dient.[9]

TETRA V+D bietet kanalvermittelte Sprach- und Datendienste sowie einen Kurzdatendienst für Status- und Textnachrichten sowie einen Paketdatendienst für IP.[10]

Die Sprachdienste haben folgende Verbindungsarten: Der **TMO-Gruppenruf** dient zur Kommunikation zwischen mehr als zwei Gesprächspartnern und ist somit eine Punkt-zu-Multi-Punkt Verbindung. Im analogen Sprechfunk entspricht der Gruppenruf der hauptsächlichen Kommunikation. Daher ist diese Verbindungsart eine der Wichtigsten. Der Gruppenruf erfolgt im Halb-Duplex Modus. Dabei kann nur ein Gruppenmitglied senden und alle anderen Gruppenmitglieder empfangen auf dem gleichen Kanal. Durch die Nutzung des gleichen Downlink-Kanals ist dies auch eine effiziente Nutzung der Funkressourcen. Dieses Leistungsmerkmal besitzt GSM zum Beispiel nicht und ist daher einer der Gründe, warum man nicht GSM anstelle von TETRA verwendet.[9]

Beim **TMO-Einzelruf** wird eine Punkt-zu-Punkt Verbindung zwischen zwei Mobilteilnehmern aufgebaut. Dabei können beide Teilnehmer gleichzeitig empfangen und senden. Somit erfolgt die Kommunikation im Vollduplexmodus, welcher jeweils einen Uplink- und Downlink-Zeitschlitz benötigt. Der Kommunikationsaufbau entspricht dabei einem normalen Telefongespräch, bei dem man hier die Aliasnummer des Gesprächspartners wählt und dieser das Gespräch mit einem Knopfdruck annehmen muss.[9]

Des Weiteren gibt es im TMO Betrieb auch einen **Telefonruf**. Dieser ist vergleichbar mit dem TMO-Einzelruf mit der Erweiterung, dass man eine Verbindung in ein anderes Telekommunikationsnetz aufbauen kann.[9]

Beim Mobilfunknetz TETRA gibt es allerdings noch Prioritäten auf die Kommunikation. So können Gespräche, welche höhere Prioritäten haben, abhängig von Gruppen und Gerä-

ten, andere Gespräche mit niedrigeren Prioritäten verdrängen, falls alle verfügbaren Zeitschlitzte ausgelastet sind. Der **Notruf** hat immer die höchste Priorität.[9]

4.1.2 Direct Mode Operation (DMO)

Bei DMO wird die Netzinfrastruktur nicht benötigt. Durch DMO ist es somit möglich bei einer Überlastung des Netzes noch in einem Gebiet zu kommunizieren. Des Weiteren kann man so auch unabhängige Gesprächsgruppen erstellen, welche das Netz nicht belasten. Um den Direct Mode verwenden zu können, müssen alle Gesprächsteilnehmer ihr Funkgeräte manuell auf Direct Mode umschalten. Da nun die Frequenz und Zeitschlitzwahl nicht mehr durch die Netzinfrastruktur vorgegeben werden kann, müssen alle den gleichen Kanal selbst wählen. Die Kommunikation kann hier nur im Halb-Duplex Modus durchgeführt werden, da der DMO-Master prüft, ob auf der gewählten Frequenz jemand sendet. Falls dies nicht der Fall ist, kann er senden.[9]

Der **DMO-Einzelruf** entspricht dem **DMO-Gruppenruf** mit einem statt mehreren Empfängern. Bei beiden kann nur über Halb-Duplex kommuniziert werden.[9]

Bei besonderen Ereignissen kann es sinnvoll sein eine DMO-Gruppe einzusetzen, obwohl das TMO-Netz zur Verfügung steht. Hierbei ist es gerade für Führungskräfte von Vorteil, wenn sie gleichzeitig im TMO und DMO Betrieb kommunizieren können. Daher gibt es Geräte, welche die **Dual Watch** Betriebsart unterstützen, bei der sie periodisch eine DMO-Frequenz und den Organisationskanal einer Basisstation überwachen.[9]

Beim Einsatz von Handfunkgeräten ist durch die Baugröße die Reichweite deutlich geringer als bei Fahrzeugfunkgeräten. Durch **DMO-Repeater** kann aber die Reichweite vergrößert werden. DMO-Repeater nehmen dabei das Signal vom Sender auf und senden dieses auf einem anderen Kanal oder Zeitschlitz weiter. Als DMO-Repeater können insbesondere Fahrzeugfunkgeräte eingesetzt werden, da diese aufgrund ihrer Bauart auch eine größere Sendeleistung als Handfunkgeräte haben.[9]

Ein weitere Betriebsart ist die **DMO-Gateway**. Falls ein Handfunkgerät beim Betrieb aufgrund der Sendeleistung nicht in der Lage wäre eine Basisstation zu erreichen, aber es ein Fahrzeugfunkgeräte in der Nähe gibt, welches eine Verbindung zur Basisstation hat, besteht noch die Möglichkeit über DMO eine Verbindung zu einem Fahrzeugfunkgerät aufzubauen, welches als DMO-Gateway dient und aufgrund der größeren Sendeleistung die Basisstation erreicht.[9]

4.1.3 Funktionaler Aufbau des TETRA-Systems

Der Aufbau des TETRA-Systems ist ähnlich zu GSM. Es besteht aus einer Mobile Station (MS), Line Station (LS) sowie einer Switching and Management Infrastructure (SwMI).[10]

Die Mobile Station verfügt über eine eindeutige Kennung, die TETRA Subscriber Identity (TSI) (vgl. Abb. 1), welche aus dem Mobile Country Code (MCC), Mobile Network Code (MNC) und der Short Subscriber Identity (SSI) besteht. Der MCC beinhaltet die Länderkennung (262 für Deutschland). Der MNC bezeichnet das entsprechende TETRA-Netz, zum Beispiel 1001 für BDBOS. Die SSI steht für den Teilnehmer.

Wenn man eine Verbindung zu einem bestimmten Funkgerät im Heimnetz aufbaut, wird nur die SSI als Adresse verwendet. Zudem gibt es noch für jede Mobile Station die TETRA Equipment Identity (TEI), welche gerätespezifisch ist. Diese Nummer wird vom Betreiber vergeben.[10]

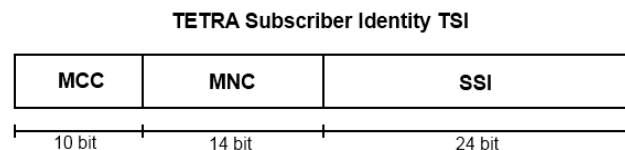


Abbildung 1: TETRA Subscriber Identity

Die Line Station bietet die gleichen Funktionen und Dienste wie die Mobile Station, ist allerdings über ISDN mit der Netzinfrastruktur verbunden. Die Leitstelle ist zum Beispiel eine Line Station. Diese hat auch den Zugang zu Datenbanken der Verwaltungsinfrastruktur.[10]

Die Switching and Management Infrastructure beinhaltet Basisstationen, Vermittlungsstellen (auch Main Switching Center (MSC) genannt), Transitvermittlungstellen und das Netzverwaltungszentrum (NMC), welche die Kommunikation zwischen Mobile Stationen und Line Stations herstellen und überwachen. Des Weiteren übernimmt das SwMI Aufgaben, welche unter anderem das Zuteilen von Kanälen und das Vermitteln von Verbindungen sind. Die Authentifizierung wird durch die SwMI durchgeführt und verfügt somit auch über die Home Data Base (HDB) und Visited Data Base (VDB).[10]

Die HDB enthält alle administrativen Informationen über jeden Mobilteilnehmer, der im Netz registriert ist. Die VDB enthält eine Teilmenge der HDB Daten, welche für die Rufüberwachung und das interne Routing im jeweils überwachten Bereich notwendig sind.[9]

Wie die HDB und VDB in den SwMI Komponenten verteilt sind, ist nicht Bestandteil des TETRA-Standards.[8]

4.2 LowLevel-Beschreibung

In diesem Abschnitt wird TETRA durch die unteren drei OSI-Schichten beschrieben. In Tabelle 1 sind die wichtigsten Parameter von TETRA aufgelistet.

4.2.1 Bitübertragungsschicht

Die Bitübertragungsschicht ist bei TETRA V+D zum einen für die Burstbildung verantwortlich. Bei der Burstbildung wird ein Burst auf eine Trägerfrequenz aufmoduliert. Der TETRA-Burst ist somit der Inhalt eines definierten Zeitschlitzes[9]. Das hierbei verwendete Modulationsverfahren ist $\pi/4$ Differential Quaternary Phase-Shift Keying (DQPSK), welches eine Modulationsbitrate von 36kBit/s hat.[10]

Bei TETRA gibt es verschiedene Basisstrukturen für einen Burst. Diese dienen zum einen der Datenübertragung aber auch der Synchronisierung und Änderung der Sendeleistung. Ein normaler Burst besteht aus zwei Blöcken mit je 216 Bit Nutzdaten, womit der Burst einem Zeitschlitz des Frames entspricht.[10]

Tabelle 1: Technische Daten von TETRA

Parameter	Wert
Frequenzen (MHz)	UL:380-390 DL:390-400 UL:410-420 DL:420-430 UL:450-460 DL:460-470 UL:870-888 DL:915-933 (UL:Uplink, DL:Downlink)
Frequenzen BOS (MHz)	UL:380-385 DL:390-395 (UL:Uplink, DL:Downlink)
Kanalbandbreite	25 kHz
Duplexabstand	10 MHz
Rufaufbauzeit	<300 ms
Modulationsverfahren	$\pi/4$ Differential Quaternary Phase Shift Keying (DQPSK)
Modulationsbitrate	36 kbit/s
Mehrfachzugriff	TDMA mit 4 Zeitschlitz pro Träger
Sprachcodec	Algebraic Code Excited Linear Predictive (ACELP) (4,56 kbit/s)
Nutzdatenrate (kbit/s)	hoch geschützt: 9,6 geschützt: 19,2 ungeschützt: 28,8

Zudem sind Modulation und Demodulation, Frequenz- und Symbolsynchronisation und Auswahl der Frequenzbänder und Sendeleistung Aufgaben dieser Schicht. Die Symbolsynchronisation wird durch eine Trainingssequenz erreicht, die in allen Bursts enthalten ist. Somit ist das Erkennen von Grenzen der Bursts möglich. In Europa sind die Frequenzbänder 410-420 MHz, 450-470 MHz, 870-876 MHz und 915-921 MHz reserviert. Der Duplexabstand zwischen Uplink- und Downlink-Trägerfrequenzen soll 10 MHz betragen. In Deutschland ist der Bereich 380-385 MHz als Uplink und 390-395 MHz als Downlink der BOS zugeteilt. Dabei entspricht ein Kanal der Bandbreite von 25 kHz und hat einen Schutzabstand von 25 kHz. Zudem messen Mobile Station den Empfangspegel des verwendeten Frequenzkanals um anhand der Werte einen Zellwechsel einzuleiten.[10]

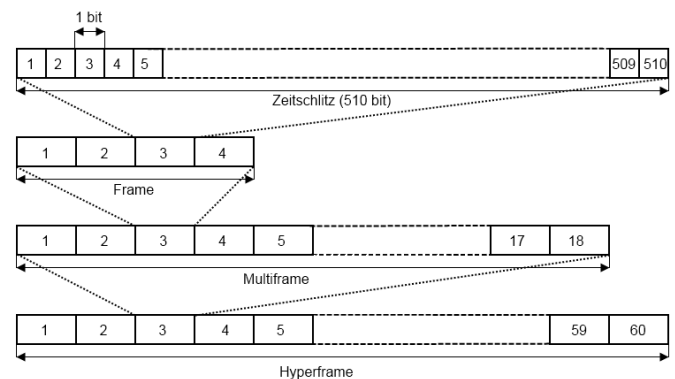
4.2.2 Sicherungsschicht

Diese Schicht ist in die Teilschichten Medium Access Control (MAC) und Logical Link Control (LLC) aufgeteilt. Dabei gelangen die Daten von der Bitübertragungsschicht zuerst zur MAC-Teilschicht und dann über die LLC-Teilschicht zur Vermittlungsschicht.

Die MAC-Teilschicht umfasst die Funktionen der Kanalcodierung und Kanalzugriffssteuerung.[10]

TETRA verwendet als Multiplexverfahren Time Division Multiple Access (TDMA), welches jede Trägerfrequenz in vier Zeitschlitz der Größe von 510 Bit einteilt. Ein TDMA-Rahmen hat daher eine Größe von 255 Byte. Achtzehn Rahmen werden zu einem Multirahmen zusammengefasst, der 4590 Byte groß ist. Ein Hyperrahmen besteht aus 60 aufeinander

folgenden Multirahmen, mit der Größe von ca. 269 kB. In Abbildung 2 ist die Rahmenstruktur dargestellt.[10]

**Abbildung 2: TETRA-Rahmenstruktur**

Die LLC-Teilschicht ist für die Datenübertragung, Übertragungswiederholung und Segmentierung zuständig und stellt so der Vermittlungsschicht fehlerfreie Daten zur Verfügung.[8]

4.2.3 Vermittlungsschicht

Diese stellt Funktionen zur Verfügung um Verbindungen zwischen mobilen Teilnehmern, Teilnehmern an Line Stations und Teilnehmern in anderen Netzen aufzubauen.[10]

Der Layer 3 ist in die Teilschichten Mobile Link Entity (MLE), Circuit Mode Control Entity (CMCE), Mobilitätsmanagement (MM) und Subnetwork Dependent Convergence Protocol (SNDP) unterteilt.[10]

- Die Aufgabe der Mobile Link Entity-Teilschicht ist das Herstellen und Aufrechterhalten der Funkverbindung zwischen Mobile- und Basisstation. Daher entscheidet auch die MLE-Teilschicht wann und ob sie die Funkzelle wechselt. Die MLE besteht wiederum aus Komponenten, welche für die Überwachung der Funkkanalqualität, das Scannen und Bewerten von Nachbarzellen, das Durchführen von Zellwechselprozeduren und die Auswahl der LLC Dienste verantwortlich sind.[10]
- Die Circuit Mode Control Entity ist verantwortlich für die Rufsteuerung und Kurzdatendienste.[10]
- Das Mobilitätsmanagement (MM) besitzt die Aufgabe die Zuordnung von Mobile Stationen zu Aufenthaltsbereichen aktuell zu halten.[10]
- Das SNDP ist für die Einbindung von IP-Teilnetzen verantwortlich. So wird in dieser Schicht die Zuordnung von einer PDP-Adresse (z.B. IP-Adresse) zu einer Individual TETRA Subscriber Identity (ITSI) kontrolliert und verwaltet.[10]

4.2.4 Handover

In einem Netz aus vielen Funkzellen müssen die Funkverbindungen über die Dauer des gesamten Gesprächs auch beim Wechseln der Zelle aufrecht erhalten werden. Den Vorgang, bei dem ein Gespräch auf eine Frequenz in der nächsten Zelle weitergegeben wird, bezeichnet man als Handover. Dieser Handover kommt zustande, wenn die Kommunikationsbedingung einer benachbarten Zelle besser als die der eigenen ist. Wie die Kommunikationsbedingung der benachbarten Zellen sind, wird durch das Überprüfen der Control Channels⁴ der jeweiligen Basisstationen festgestellt.[9]

Beim Handover gibt es unterschiedliche Arten aufgrund der Netztopologie:

- 1) Die Umschaltung kann zwischen unterschiedlichen Basisstationen erfolgen, welche an der gleichen Vermittlungsstelle (MSC) angeschlossen sind. In diesem Fall kann die Vermittlungsstelle den Vorgang selbst verarbeiten.
- 2) Die Umschaltung kann auch zwischen unterschiedlichen Basisstationen, welche an unterschiedlichen Vermittlungsstellen (MSC) angeschlossen sind erfolgen. Beide Vermittlungsstellen sind allerdings an das selbe Transit Main Switching Center (Transit MSC) angeschlossen.
- 3) Zudem kann die Umschaltung zwischen unterschiedlichen Basisstationen erfolgen, welche an unterschiedlichen Main Switching Centers angeschlossen sind. Diese Form wird auch als externes Handover bezeichnet.[9]

Welche Nachrichten bei einem Handover auf Layer 3 Ebene entstehen, wird in Abschnitt 6 behandelt.

4.3 Sicherheit

TETRA hat drei Mechanismen um Daten sicher zu übertragen. Eine Sicherheitsvorkehrung ist die Luftschnittstellenverschlüsselung. Diese Verschlüsselung basiert auf den einzelnen Funkzellen. Beim TMO-Einzelruf handelt jeder Teilnehmer mit der Basisstation den jeweiligen Kommunikationsschlüssel einzeln aus. Dagegen verwenden beim TMO-Gruppenruf alle Gruppenmitglieder den gleichen Kommunikationsschlüssel. Beim DMO Betrieb werden weitere statische Kommunikationsschlüsseln eingesetzt, welche in den Geräten gespeichert sind.[9]

Des Weiteren gibt es noch eine Ende-zu-Ende Verschlüsselung, welche auch die Daten zwischen Basisstation und Leitstelle verschlüsselt. Im TETRA-Netz der BOS wird diese Sicherheit durch ein asymmetrisches Kryptosystem realisiert, bei der jede Mobile Station eine BSI-Kryptokarte benötigt. Diese entspricht einer intelligenten SIM Karte und enthält einen speziell für die Verschlüsselung optimierten Prozessor mit zugehörigem Datenspeicher[9]. Die BSI-Kryptokarte beinhaltet aber auch noch die operativ-taktische Adresse, durch die jedes Funkgerät eindeutig zuordenbar wird.[7]

5. TETRA BEI BOS

Das TETRA-Netz wird bei der BDBOS seit 2008 ausgebaut. Nach den Angaben von BDBOS soll die flächendeckende Infrastruktur voraussichtlich bis Ende 2012 aufgebaut sein.[3]

⁴Der Control Channel ist ein unidirektionaler Steuerkanal zwischen der Basis Station und den Mobile Stations. Über diesen Kanal werden Netzinformationen von der Basis Station übertragen.[9]

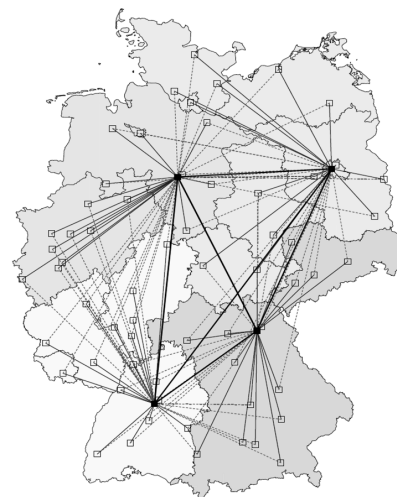


Abbildung 3: Funktionaler Aufbau des digitalen BOS-Netzes[2]

Zum funktionalen Aufbau des digitalen BOS Netzes (vgl. Abb. 3). Dieses besteht aus 45 Netzabschnitten. Es gibt in diesen Netzabschnitten 64 Vermittlungsstellen (MSC), welche mit den einzelnen Basisstationen über Kabel oder Richtfunk verbunden sind. Die Vermittlungsstellen sind wiederum mit zwei Transitvermittlungsstellen verbunden. Hiervon gibt es vier, welche vollvermascht vernetzt sind[2]. Somit sind die Vermittlungsstellen mit mehreren Transitvermittlungsstellen verbunden und beim Ausfall eines Knoten ist die Kommunikation noch über einen weiteren gewährleistet.[9]

Die gesamte Steuerung des Netzes erfolgt über zwei Netzverwaltungszentren (NMC). Diese befinden sich in Berlin und Hannover, um bei einem Störfall sich gegenseitig ersetzen zu können.[4]

Die Leitstellen sind über Kabel mit zwei unabhängigen Vermittlungsstellen verbunden. Durch diese Redundanz wird die Leitstelle bei einem Ausfall einer Leitung nicht funktionslos.[9]

6. TETRA MESSUNGEN

Aufgrund mehrerer Mitteilungen von Feuerwehrangehörigen, die besagen, dass man beim neuen BOS-Funk lange warten muss bis man sprechen kann oder beim Zellwechsel für mehrere Sekunden die Verbindung ausfällt, wurden einige Messungen durchgeführt, um festzustellen wie lang ein Verbindungsaufbau dauert und ein Handover an Zeit benötigt.

Diese Messungen konnte mit der Unterstützung von Rohde und Schwarz durchgeführt werden. Dabei kam die Messsoftware ROMES 4.63 und zwei Sepura TETRA-Mobiles zum Einsatz. Die Mobiles waren über USB mit dem PC verbunden, auf dem die ROMES lief. Über die SAIL Schnittstelle der Sepura Mobiles wurden dann die entsprechenden Daten ausgelesen. Eigentlich sollte die Messungen im Netz der BOS durchgeführt werden. Dafür wären allerdings Mobiles notwendig gewesen, welche im BOS-Netz eingebucht sind. Rohde und Schwarz hat allerdings nur zwei Mobiles, welche im Netz der Stadtwerke München eingebucht sind. Beim digitalen

BOS-Netz können sich die folgenden Zeiten somit unterscheiden, da dort eine andere und größere Netzinfrastruktur vorliegt. Bei der Messung befanden sich beide Mobiles im TMO Betrieb. In dieser Betriebsart hat das Mobile 2 mehrere Einzelrufe an Mobile 1 durchgeführt. Das Mobile 2 hat im Abstand von 60 Sekunden Mobile 1 angerufen und die Verbindung für 30 Sekunden gehalten.

Aus den Layer 3 Nachrichten in Abbildung 4 kann man den Verbindungsaufbau und Abbau erkennen. Die Zeitangaben der Layer 3 Nachrichten sind aus den Messprotokollen entnommen. Die Messsoftware ROMES protokolliert mit den Layer 3 Nachrichten auch den Zeitpunkt.

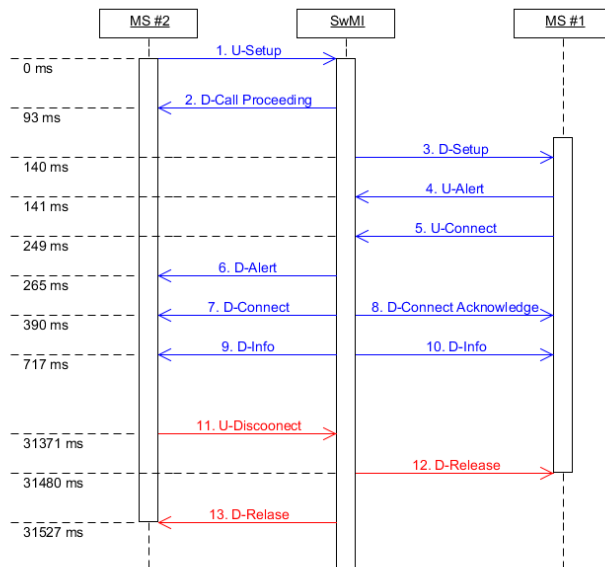


Abbildung 4: TETRA Call

Bei dieser Verbindung wird als erstes die Protocol Data Unit (PDU) U-Setup von MS2 an die SwMI geschickt um zu signalisieren, dass das MS2 eine Verbindung aufbauen will. Daraufhin erhält das MS2 vom SwMI als Bestätigung die PDU D-Call Proceeding, dass der Gesprächsaufbau fortgesetzt wird. Danach sendet die SwMI an das MS1 die PDU U-Setup, um diesem mitzuteilen, dass es von MS2 angerufen wird. Als Bestätigung erhält die SwMI das U-Alert. Sobald das MS1 bereit für die Verbindung ist, sendet dies U-Connect an die SwMI. Das MS2 erhält nun auch die PDU D-Alert als Bestätigung, dass das MS1 verfügbar ist. Nun sendet die SwMI die PDU D-Connect an MS2 und D-Connect Acknowledge an MS1 als Bestätigung, dass die Verbindung aufgebaut ist. Mit der PDU D-Info werden noch allgemeine Daten an die Mobiles geschickt. Nach den 30 Sekunden beendet MS2 mit der PDU U-Disconnect das Gespräch. Die SwMI schickt darauf an MS1 und MS2 D-Release um zu signalisieren, dass das Gespräch beendet wurde.

Bei einem Handover entstehen die in Abbildung 5 gezeigten Layer 3 Nachrichten.

Wenn das Mobile eine neue Zelle ausgewählt hat, schickt dies die PDU U-Prepare an die SwMI mit der gewählten Zelle als

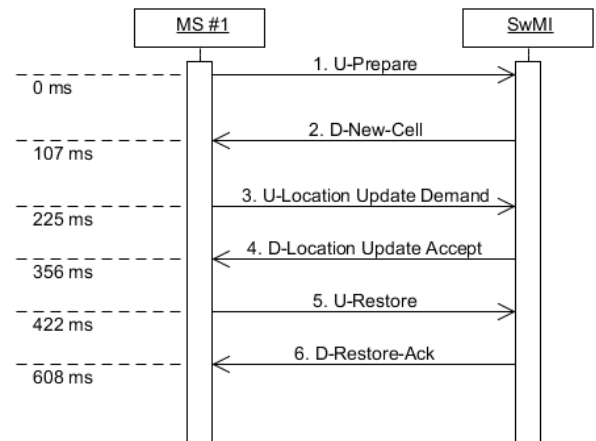


Abbildung 5: TETRA Handover

Information. Das SwMI antwortet darauf, indem es die PDU D-NEW-CELL schickt, um zu bestätigen, dass das Mobile in die gewünschte Zelle wechseln kann. Als nächstes sendet das Mobile die PDU U-Location Update Demand, um bei der SwMI eine Aktualisierung der Registrierungen zu veranlassen. Die SwMI schickt, sobald das Update durchgeführt wurde, die PDU D-Location Update Acceptet. Danach sendet das Mobile noch U-Restore, welches der SwMI signalisiert, dass das Mobile noch Informationen aufgrund des Zellwechsels aktualisiert. Die SwMI bestätigt dies mit D-Restore-Ack.

Aus diesen zwei Ausschnitten kann man aber nicht generell auf den zeitlichen Ablauf eines Gesprächs schließen. Somit können sich je nach Auslastung des Netzes oder auch des Mobiles diese Zeiten sehr unterscheiden. Auch die Frage, wie lang bei dem Handover aus Abbildung 5 die Tonübertragung unterbrochen war, konnte man mit diesen Layer 3 Nachrichten nicht zeigen. Vermutlich fällt die Übertragung der Sprache ab der PDU D-NEW-CELL bis U-RESTORE aus, was 315 ms⁵ entsprechen würde. Allerdings kann man hier gut erkennen wie die Kommunikation in TETRA abläuft.

7. ZUSAMMENFASSUNG UND ZUKUNFT VON TETRA

Zum einen wurde immer wieder bemängelt, dass der TETRA Standard schon wieder veraltet ist und die Übertragungsraten zu niedrig sind. Dies ist aber nur in einem gewissen Maß korrekt. Im Moment steht bei einer verschlüsselten Verbindung eine Übertragungsrate von 9,6 kbit/s zur Verfügung, was im Vergleich zu UMTS, mit zum Teil verfügbaren 7,2 Mbit/s, sehr gering ist. Allerdings sind diese 9,6 kbit/s nicht dem TETRA Standard an sich verschuldet sondern aufgrund der BDBOS Auslegung. So kann mit einem anderen Modulationsverfahren und größeren Kanalbandbreiten auch eine höhere Übertragungsrate erreicht werden. Zudem gibt es auch schon Erweiterungen von TETRA. Wie den TETRA Enhanced Data Service, mit dem eine Steigerung der Übertragungsrate mit bis zu 300 kBits/s möglich ist. Falls diese Datenrate nicht ausreicht, besteht immer noch

⁵time(„D-NEW-CELL“) - time(„U-RESTORE“) = 107 ms - 422 ms = 315 ms

die Möglichkeit LTE als Zusatz für die Datenübertragung zu verwenden. Diese höheren Datenraten sind vor allem auch nur für Datenübertragungen notwendig. Für die normale Sprachkommunikation reicht die Übertragungsrate von 9,6 kbit/s durch den Sprachcodec aus.

Die Frage stellt sich nun vielleicht, warum man nicht gleich einen Mobilfunkstandard wie LTE verwendet. Gründe warum man dies nicht machen sollte, sind zum einen, dass LTE, GSM usw. die Gruppenruffunktion und Verschlüsselung nicht unterstützen. Es wurde aber auch über die Nutzung des GSM Netzes nachgedacht. Allerdings hat ein eigenes Funknetz immer den großen Vorteil, dass dies auch noch funktionsfähig ist, wenn bereits andere Netze aufgrund von Überlastung ausgefallen sind. So ist es vor allem bei Massenveranstaltungen sinnvoll, ein eigenes Kommunikationsnetz zu haben, da dort öfters die Mobilfunknetze GSM bzw. UMTS überlastet sind.

Im großen und ganzen bringt die Einführung vom Digitalfunk den BOS eindeutig mehr Vorteile und wird somit der neue Kommunikationsstandard der BOS in Deutschland.

8. LITERATUR

- [1] Bayerisches Staatsministerium des Innern (StMI). Ablösung Analogfunk BOS-Digitalfunk - Einführung in Bayern. <http://www.stmi.bayern.de/sicherheit/digitalfunk/einfuehrung/detail/17342/>. 21.01.2011.
- [2] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben. Digitalfunk BOS Vorsorgemaßnahmen zur Energieversorgung. PowerPoint.
- [3] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS). Fortschrittsanzeiger: Der Aufbau des BOS-Digitalfunknetzes. http://www.bdbos.bund.de/cln_090/nn_1358092/DE/Bundesanstalt/Projekt__Digitalfunk/Netzaufbau__Roll__out/Fortschrittsanzeiger/fortschrittsanzeiger__roll__out__node.html?__nnn=true. 21.01.2011.
- [4] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS). Netzverwaltungszentren des BOS-Digitalfunknetzes in Betrieb. http://www.bdbos.bund.de/cln_090/nn_1358092/DE/Bundesanstalt/Projekt__Digitalfunk/Netzaufbau__Roll__out/Netzverwaltungszentren/netzverwaltungszentren__node.html?__nnn=true. 21.01.2011.
- [5] Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS). Warum eigentlich Digitalfunk BOS? http://www.bdbos.bund.de/cln_090/nn_421176/DE/Bundesanstalt/Projekt__Digitalfunk/Vorteile__des__Digitalfunks__BOS/vorteile__node.html?__nnn=true. 21.01.2011.
- [6] Bundesnetzagentur. Bündelfunk. http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/RegulierungTelekommunikation/Frequenzordnung/FrequenzzuteilungAntraege/Buendelfunk/Buendelfunk_node.html. 21.01.2011.
- [7] J. T. D. Christof Linde. *Digitalfunk*. ecomed SICHERHEIT, 2011.
- [8] J. I. John Dunlop, Demessie Girma. *Digital Mobile Communications and the TETRA System*. John Wiley and Sons Ltd, 1999.
- [9] C. Linde. *Aufbau und Technik des digitalen BOS-Funks*. Franzis Verlag, 2008.
- [10] P. Sievering. Dimensionierung und Leistungsbewertung von TETRA-Bündelfunksystemen. Dissertation, Dezember 2004.