

Seminar zum Thema Mobile Computing

Bluetooth

Thorge Wegers

WI 5047

Informatik Seminar FH Wedel

23.11.2004

Inhaltsverzeichnis

Inhaltsverzeichnis	II
Abbildungsverzeichnis	III
1. Einleitung	
1.1. Geschichte.....	1
1.2. Einsatzgebiete.....	1
1.3. Eigenschaften.....	2
2. Vernetzung	3
3. Der Bluetooth Protokollstapel	6
3.1. Bluetooth Radio und Baseband.....	7
3.1.1. Frequency Hopping.....	7
3.1.2. Synchrone und asynchrone Verbindungen.....	9
3.1.3. Paketformate.....	10
3.2. Link Manager.....	13
Betriebsmodi.....	14
3.3. L2CAP.....	15
3.4. SDP/RFCOMM/TCS BIN.....	17
4. Sicherheit in Bluetooth-Netzen	18
4.1. Schlüsselgenerierung.....	19
4.2. Authentifizierung.....	20
4.3. Verschlüsselung.....	21
4.4. Kritik am Sicherheitskonzept.....	22
Literaturverzeichnis	A

Abbildungsverzeichnis

Abbildung 1:	Bluetooth Netzwerk verbunden mit GSM-Netz.....	2
Abbildung 2:	Bildung eines Piconetzes.....	3
Abbildung 3:	Synchronisieren der internen Uhr.....	4
Abbildung 4:	Scatternetz.....	4
Abbildung 5:	Bluetooth Protokollstapel.....	6
Abbildung 6:	Bluetooth Leistungsklassen.....	7
Abbildung 7:	Kommunikation zwischen Master und Slave.....	7
Abbildung 8:	Kommunikation mit Multislotpaketen.....	8
Abbildung 9:	ACL- und SCO-Links.....	9
Abbildung 10:	Paketformat im Basisband.....	10
Abbildung 11:	SCO Pakettypen.....	10
Abbildung 12:	ACL Pakettypen.....	11
Abbildung 13:	Bluetooth Basisband Datenraten.....	12
Abbildung 14:	Bluetooth Betriebsmodi.....	15
Abbildung 15:	Logische Kanäle zwischen Geräten.....	16
Abbildung 16:	L2CAP Paketformate.....	16
Abbildung 17:	Generierung Initialization Key.....	19
Abbildung 18:	Authentifizierung.....	20
Abbildung 19:	Verschlüsselung.....	21

1. Einleitung

1.1 Geschichte

Die Geschichte von Bluetooth beginnt im 10. Jahrhundert als König Harald Gormsen, dessen Spitzname Blatand war, Dänemark und Norwegen vereinigt.

1994 startete die Firma Ericsson Forschungsarbeiten an einem „Multi-Communicator-Link“. Dieser Entwurf stellte eine Technologie dar, die Kabelverbindungen zwischen tragbaren Kommunikationsgeräten überflüssig machen soll. Das Projekt wurde sehr bald umbenannt. Namensgeber war ein Freund der Entwickler, welcher Wikingerfan war, und so wurde Bluetooth geboren.

Man setzte bei der Bluetooth-Technik auf die Funkübertragung, da Infrarotlicht stets eine Sichtverbindung benötigt und daher nicht in der Lage ist, Kleidung und andere Hindernisse zu durchdringen.

1998 schloss sich Ericsson mit den Firmen Intel, IBM, Nokia und Toshiba zur Bluetooth Special Interest Group (Bluetooth SIG) zusammen. Ihr Ziel war die Entwicklung einer billigen Ein-Chip-Lösung für eine drahtlose Netztechnik. Viele weitere Forschungseinrichtungen und Firmen sind schon bald der Bluetooth SIG beigetreten. Der erste Standard wurde im Juli 1999 mit der Version 1.0 verabschiedet.

Ende 2000 kamen dann die ersten Produkte auf den Massenmarkt.

Im März 2001 wurde der Bluetooth Standard v1.1 verabschiedet. Dieser wurde im Jahr 2002 als IEEE-Norm 802.15.1 übernommen.

1.2 Einsatzgebiete

Bluetooth ist für eine ganze Menge von Einsatzszenarien geeignet. Im folgenden werden einige kurz beschrieben.

Verbindung von Peripheriegeräten: Heute sind die meisten Peripheriegeräte wie Drucker, Lautsprecher, Kopfhörer, Modem usw. über Kabel mit dem Computer verbunden. Diese Technik hat einige Nachteile. Fast jedes Gerät hat seinen eigenen Kabel- und Steckertyp, die Leitungen benötigen Platz und sind oft genug einfach nur im Weg. Mit dem Einsatz von Bluetooth würden weder Kabel noch Stecker benötigt. Soll das Netzwerk allerdings wirklich drahtlos sein, muss die Stromversorgung über Batterien sichergestellt werden.

Verbindung verschiedener Netze: Als veranschaulichendes Beispiel kann man sich hier ein Handy mit Bluetoothchip vorstellen, welches als Brücke zwischen einem lokalen drahtlosen Netz und einem GSM Netz dient. Es wäre denkbar, dass ein eingeschaltetes Mobiltelefon über Bluetooth mit einem Laptop in Empfangsreichweite verbunden wird, und so der drahtlose Internetzugang ermöglicht wird.

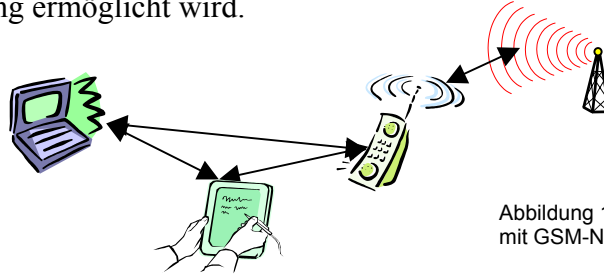


Abbildung 1: Bluetooth Netzwerk verbunden mit GSM-Netzwerk

Zwei-in-eins-Telefon: Integriert man in ein GSM Handy einen Bluetoothchip, so kann man es zusätzlich als schnurloses Telefon nutzen. Eine Bluetooth Basisstation dient dabei als Verbindung zum Festnetz.

Drahtloses Headset: Das Headset wird über Bluetooth mit dem Handy verbunden.

Grundsätzlich sind alle Anwendungsgebiete von Bluetooth auch mit anderen Techniken umsetzbar. Diese sind jedoch für eine Höhere Bandbreite und Reichweite entworfen worden und somit wesentlich teurer. Ferner arbeitet Bluetooth wesentlich energiesparender.

1.3 Eigenschaften

Bluetooth nutzt das lizenzfreie 2,4 GHz ISM Band, welches in 79 Kanäle mit einem Kanalabstand von 1MHz unterteilt wird. Der erste Kanal liegt bei 2402 MHz, der Kanal 79 bei 2480 MHz. In Frankreich, Spanien und Japan wird mit einem auf 23 Kanäle reduzierten Frequenzbereich gearbeitet.

Bei der Übertragung wird zwischen den Kanälen regelmäßig mit einer Geschwindigkeit von 1600 Sprüngen pro Sekunde gewechselt. Eine Frequenz wird somit für eine Dauer von 625 Millionstel Sekunden gehalten. Dieser Zeitraum wird auch als Slot bezeichnet.

Bluetooth unterstützt eine Bruttodatenrate von 1 MBit/s, wobei Entfernungen von bis zu zehn Metern überbrückt werden können (Leistungsklasse 3 im Indoorbereich).

Eingeschaltete Geräte in Kommunikationsreichweite werden automatisch verbunden. Als Verbindungen stehen sowohl Audio- als auch Datenkanäle zur Verfügung.

Die Ausgangsleistung von Bluetooth-Geräten ist ca. 800 mal kleiner als die von GSM-Telefonen.

2. Vernetzung

Bluetooth-Geräte, die sich in Kommunikationsreichweite befinden, können Verbindung zueinander aufbauen. Im ersten Schritt der Netzbildung sendet die zukünftige Leitstation, auch Master genannt, seine Geräteerkennung und den Wert seiner internen Uhr an andere Geräte. Das entstehende Netz nennt man Piconetz. An einem Piconetz nehmen genau eine Leitstation und bis zu sieben Folgestationen, auch Slaves genannt, teil.

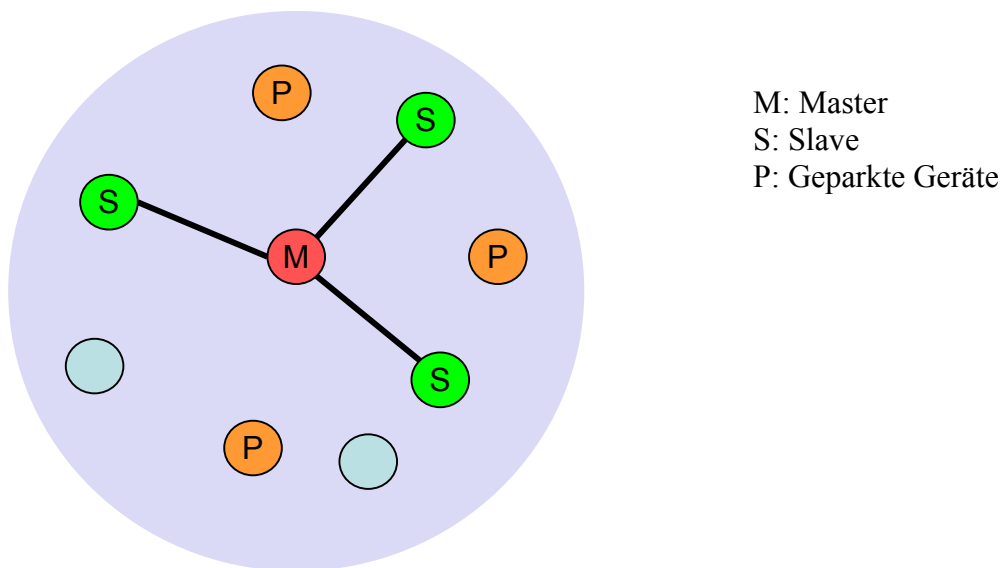


Abbildung 2: Bildung eines Piconetzes

Die Festlegung, ob ein Gerät Master oder Slave wird, erfolgt bei der ersten Kontaktaufnahme. Das die Verbindungsaufnahme einleitende Gerät wird Master, die reagierenden werden Slaves. Jedes Bluetooth-Gerät muss beide Rollen beherrschen. Ein Rollentausch während einer laufenden Verbindung ist dann möglich, wenn die beteiligten Geräte zustimmen. Alle Geräte in einem Piconetz sind auf die gleiche Sprungfolge synchronisiert. Diese Sprungfolge ist pseudozufällig und errechnet sich aus der weltweit eindeutigen 48 Bit Geräteerkennung des Masters (siehe auch 3.1.1 Frequency Hopping). Nachdem ein Gerät seine interne Uhr synchronisiert hat, kann es am Piconetz teilnehmen.

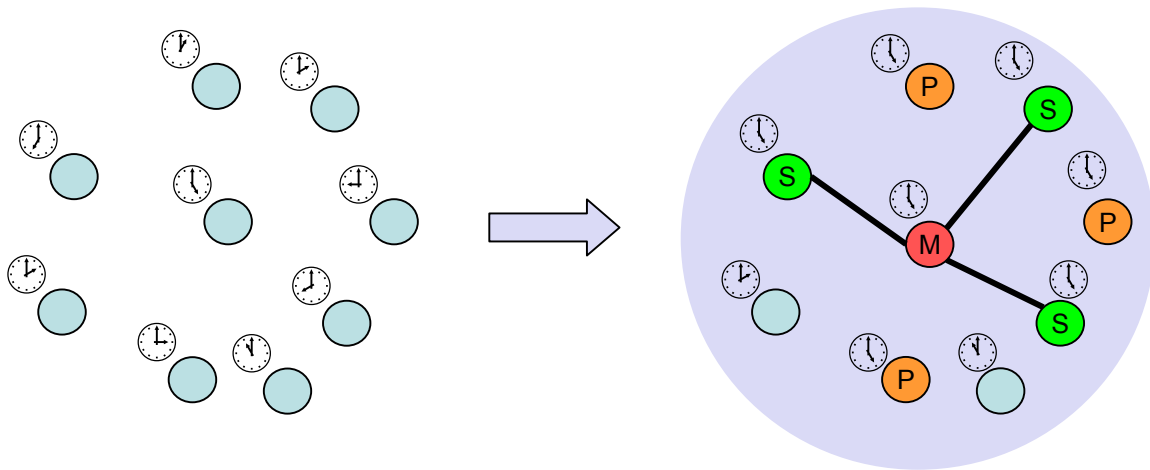


Abbildung 3: Synchronisieren der internen Uhr

Pikonetz/Scatternetz

Netzwerke aus zwei bis acht Bluetooth-Geräten nennt man Pikonetz. Es gibt genau einen Master und bis zu sieben mit dem Master verbundene Slaves. Eine direkte Kommunikation zwischen zwei Slaves ist nicht möglich. Aktive Geräte erhalten eine 3 Bit Active Member Adress (AMA), geparkte Geräte eine 8 Bit Parked Member Adress (PMA). Die 3 Bit AMA ist auch der Grund dafür, dass an einem Pikonetz nur acht Geräte aktiv teilnehmen können. Gibt es Geräte, die sich in mehreren Pikonetzen befinden, so spricht man von Scatternetzen.

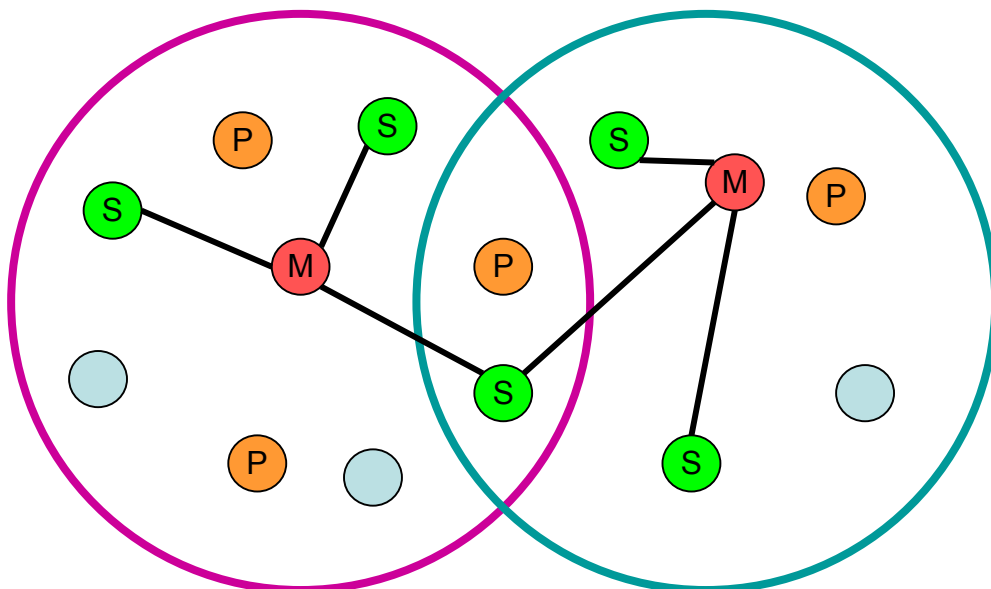


Abbildung 4: Scatternetz

Der Grund für die Bildung von Scatternetzen ist, den Datendurchsatz pro Nutzer hoch zu halten. Alle Teilnehmer eines Piconetzes folgen der gleichen Sprungsequenz, das heißt, sie teilen sich den gleichen 1 MHz Kanal. Je höher die Anzahl der Nutzer wird, desto weniger Daten kann der einzelne Nutzer senden. Daher werden nur 3 Bit Adressen vergeben, um die Anzahl der Teilnehmer klein zu halten. Um trotzdem große Netzstrukturen zu ermöglichen, gibt es die Idee der Gruppenbildung von Piconetzen, die sogenannten Scatternetze. Jedes Piconetz hat seine eigene Sprungfolge, da diese ausschließlich von der Geräteerkennung des Masters abhängt.

Will ein Slave an mehr als einem Piconetz teilnehmen, so synchronisiert er sich mit der Sprungfolge im neuen Piconetz. Vor dem Verlassen des alten Piconetzes teilt der Slave dem Master mit, dass er für eine Weile nicht erreichbar sein wird. Die Kommunikation der verbleibenden Geräte geht ganz normal weiter.

Auch ein Master kann an einem anderen Piconetz teilnehmen, dies aber nur als Slave, da die zwei Piconetze ansonsten exakt die selbe Sprungfolge hätten und somit zu einem großen würden. Eine geregelte Kommunikation wäre hier nicht mehr möglich, da uns nur eine 3 Bit Adresse zur Verfügung steht. Verlässt der Master ein Piconetz, um als Slave an einem anderen teilzunehmen, wird der Datenverkehr im alten Netz bis zur Rückkehr des Masters unterbrochen.

Die Kommunikation zwischen zwei oder mehr Piconetzen findet durch Geräte statt, die zwischen diesen Netzen hin und her springen. Es ist allerdings zu beachten, dass Scatternetze weder von allen Geräten unterstützt werden, noch die zugehörigen Verfahren vollständig spezifiziert sind.

3. Der Bluetooth Protokollstapel

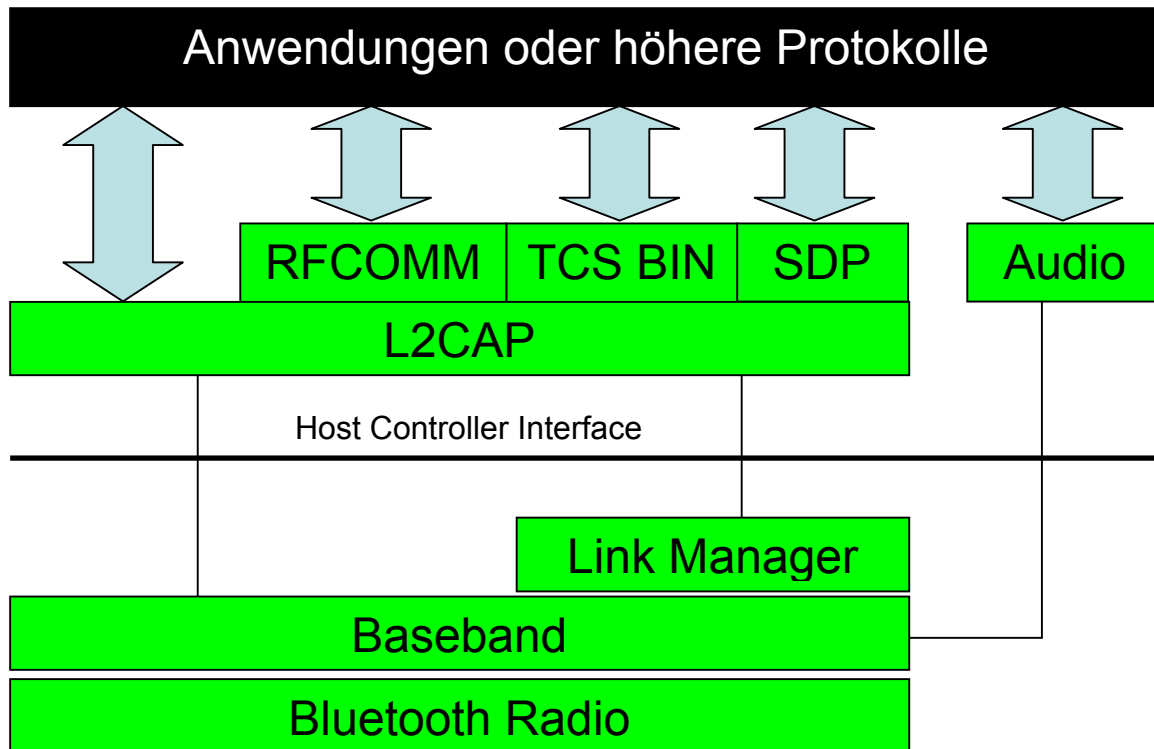


Abbildung 5: Bluetooth Protokollstapel

- Bluetooth Radio und Baseband: Diese Schichten stellen einen Zugriff von höheren Protokollschichten auf das Funkmedium bereit. Bluetooth Radio umfasst die Spezifikation der Luftschnittstelle (Sendeleistung, Frequenzen).
- Link Manager Protokoll (LMP): Diese Schicht kapselt Funktionen zum Verbindungsaufbau und zur Verbindungsverwaltung.
- Host Controller Interface (HCI): HCI ist eine Kommandoschnittstelle für höhere Schichten, zum Zugriff auf die Baseband-Funktionen.
- Logical Link and Adaption Protokoll (L2CAP): Anpassung der höheren Schichten an die Fähigkeiten des Basisbandes.
- Service Discovery Protocol (SDP): SDP ermöglicht die Suche nach Diensten anderer Bluetooth-Geräte.
- RFComm: RFComm emuliert serielle Schnittstellen als Ersatz für ein Kabel.
- Telephony Control Protocol Binary (TCS BIN): Bereitstellung von Funktionen zur Anrufkontrolle, wie sie bei Telefonen benötigt werden.
- Audio: Die Audioübertragung wird bei Bluetooth gesondert behandelt. Sie werden direkt der Baseband-Komponente übergeben und nicht wie Anwendungsdaten übertragen.

3.1 Bluetooth Radio und Baseband

Diese beiden untersten Schichten des Bluetooth Protokollstapels regeln den Verbindungsaufbau zwischen Bluetooth-Geräten und dienen der Übertragung von Daten über die Funkschnittstelle.

In der Spezifikation der Funkschnittstelle (Bluetooth Radio) sind unter anderem die folgenden 3 Leistungsklassen definiert:

Klasse	Sendeleistung	Outdoor Range	Indoor Range
1	1-100 mW	100-130 Meter	50-80 Meter
2	0,25-2,5 mW	25-35 Meter	20-30 Meter
3	n/a-1mW	10-18 Meter	8-12 Meter

3.1.1 Frequency Hopping

Bluetooth wechselt 1600 mal in der Sekunde die Frequenz. Jede Frequenz wird also exakt 625 Millionstel Sekunden gehalten. Diesen Zeitraum nennt man Slot. Damit jedes Gerät im Netz auch auf der aktuell gültigen Frequenz sendet, muss die Sprungfolge jedem bekannt sein. Man berechnet die Sprungfolge aus der Geräteadresse des Masters, da diese jedem Slave bekannt ist. Außerdem führt dieses Verfahren dazu, dass jedes Piconetz eine Individuelle Sprungfolge verwendet. Andere Piconetze benutzen andere Sprungfolgen, da sie andere Master haben. Dies hat den Vorteil, dass Kollisionen zwischen verschiedenen Piconetzen nur äußerst selten auftreten. Kollisionen innerhalb eines Piconetzes werden durch die Tatsache vermieden, dass ein Slave erst antworten darf, wenn er durch den Master dazu aufgefordert wurde. Der Master sendet hierbei grundsätzlich auf den Slots mit gerader Nummer, der Slave auf denen mit ungerader Nummer.

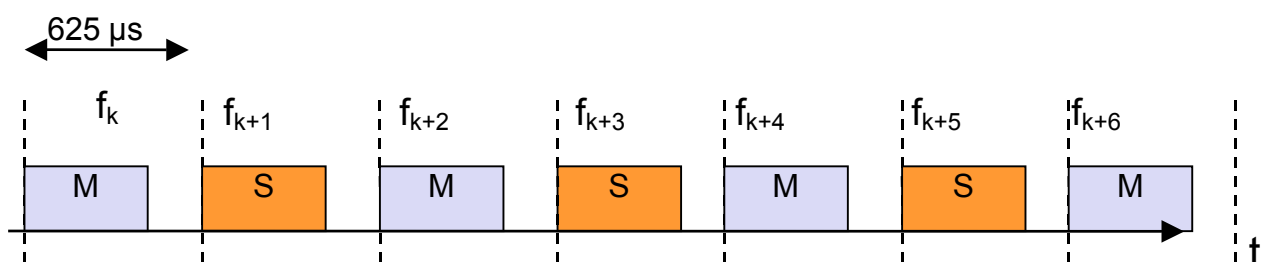


Abbildung 7: Kommunikation zwischen Master und Slave

In dem einfachen Beispielfall in Abbildung 7 werden nur Pakete versendet, deren Übertragung lediglich einen Zeitschlitz belegt. Es können aber auch Pakete versendet werden, die entweder 3 oder 5 Slots belegen. Der Sender verweilt hierbei auf der gleichen Frequenz. Innerhalb eines Paketes erfolgt also kein Frequenzwechsel. Die Antwort erfolgt auf der Frequenz, die bei einem Wechsel pro Slot gültig gewesen wäre. Dieses spezielle Sprungverfahren bei Multislotpaketen wird angewendet, um das Problem der versteckten Endgeräte zu lösen (siehe hierzu auch Vortrag von Björn Peters: Besonderheiten des mobilen Medienzugriffs, Folie 10). Slaves, die von der Übertragung nichts mitbekommen haben, fahren normal mit der Sprungfolge fort und sind so nach der Übertragung wieder auf der richtigen Frequenz.

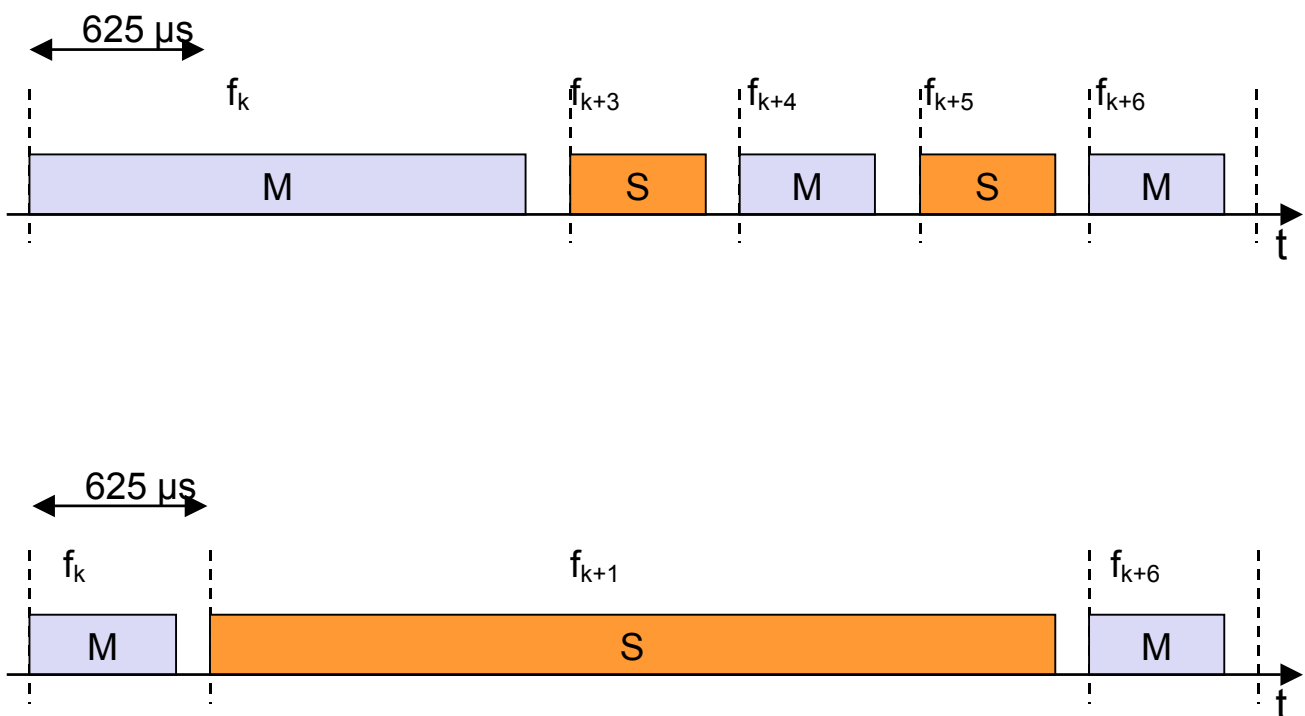


Abbildung 8: Kommunikation mit Multislotpaketen

Befinden sich mehrere Slaves in einem Piconetz, so schickt der Master abwechselnd zu den Slaves Pakete. Ein Slave darf erst antworten, wenn er dazu aufgefordert wurde. Hat ein Slave diese Aufforderung im Fehlerfall nicht erhalten, so darf er nicht einfach senden, nur weil er an der Reihe gewesen wäre.

3.1.2 Synchrone und Asynchrone Verbindungen

Bluetooth unterstützt zwei verschiedene Arten von Verbindungen zwischen den Geräten. Zum einen synchron verbindungsorientiert (Synchronus Connection-Oriented Link, kurz SCO) und asynchron verbindungslos (Asynchronus Connectionless Link, kurz ACL). SCO-Links werden von klassischen Sprachverbindungen über das Telefon benötigt. Bei diesen symmetrischen Punkt-zu-Punkt Verbindungen reserviert der Master zwei aufeinanderfolgende Zeitschlitze in festen Intervallen. Damit wird eine feste Bandbreite im Piconetz reserviert, was zur Folge hat, dass maximal 3 SCO Verbindungen pro Gerät zulässig sind. Der Master kann diese Verbindungen zu einem einzelnen oder auch mehreren Slaves herstellen. Ein Slave kann bis zu 3 SCO Links zu einem Master haben oder 2 Links zu verschiedenen Leitstationen betreiben. Es stehen 3 verschiedene Pakettypen zur Verfügung, die jeweils einen Slot belegen. Der Unterschied liegt in der Nutzlast (siehe auch 3.1.3 Paketformate). Die Datenrate beträgt 64 kBits/s in beide Richtungen. SCO Pakete werden im Fehlerfall nicht erneut übertragen.

ACL-Links werden für typische Datenanwendungen. Sie ermöglichen paketvermittelte Punkt-zu-Mehrpunkt Übertragungen inklusive der Möglichkeit eines Broadcasts. Es kann nur jeweils eine Verbindung zwischen Master und Slave geben. Um eine sichere Datenübermittlung anzubieten, stellt Bluetooth eine automatische Übertragungswiederholung (Automatic Repeat Request, ARQ) zur Verfügung.

Anders als bei SCO-Links erfolgt keine Reservierung von Zeitschlitzen. Es werden die Slots verwendet, die nicht von SCO-Links belegt sind.

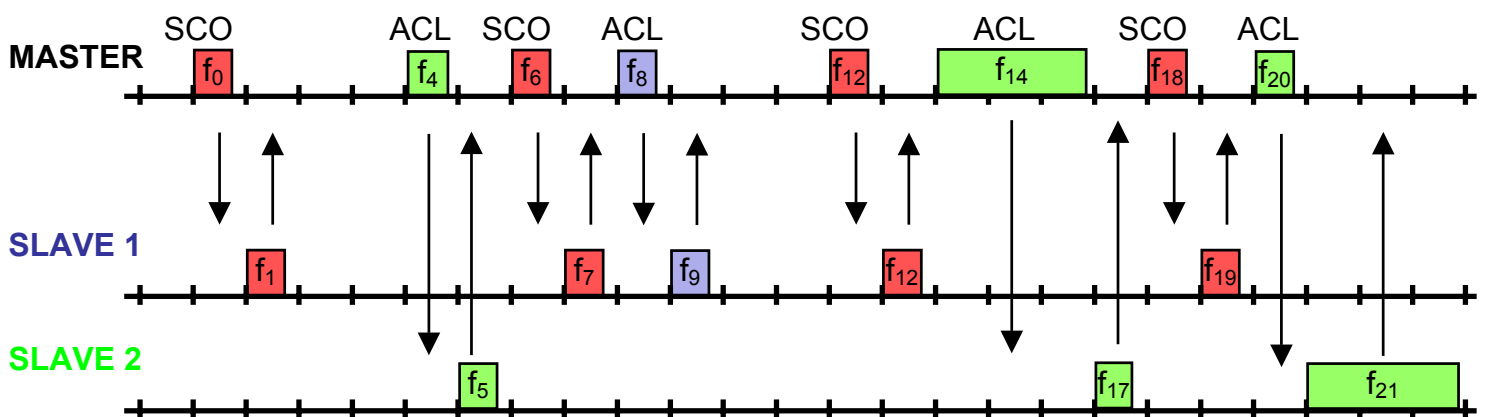


Abbildung 9: ACL- und SCO-Links

Zu *Abbildung 10*: Die SCO Verbindung belegt jeden sechsten Zeitschlitz und den Folgeslot. Die ACL Verbindungen nutzen die nicht belegten Slots. Der Slave antwortet nur, wenn er vom Master dazu aufgefordert wird.

3.1.3 Paketformate

Pakete im Bluetooth Basisband bestehen aus den 3 Feldern Zugriffscode, Paketkopf und Daten. Die verschiedenen Paketformate für ACL- und SCO-Links unterscheiden sich jedoch nur hinsichtlich des Feldes Daten.

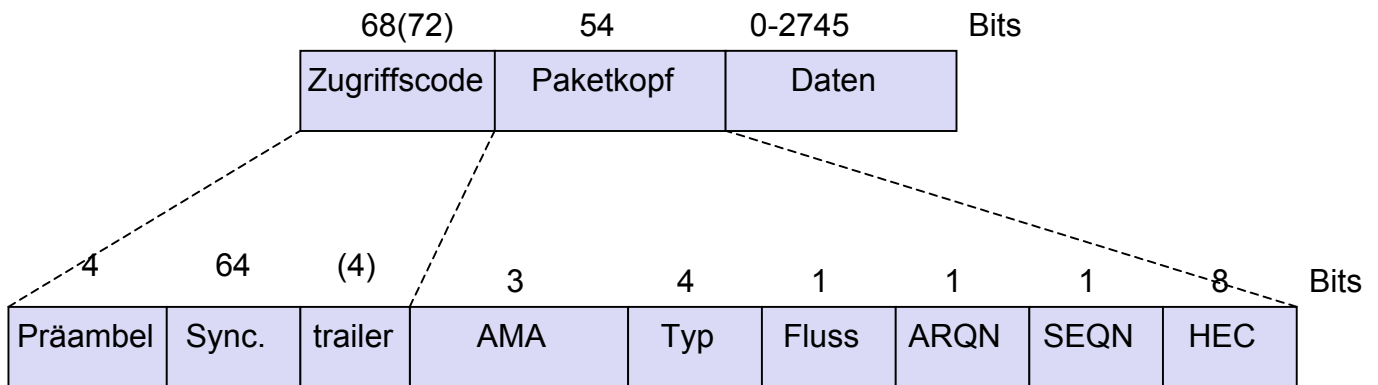


Abbildung 10: Paketformat im Basisband

Der Zugriffscode wird zur Synchronisation und Identifizierung des Piconetzes benötigt. Ist das Paket für ein Spezielles Gerät bestimmt, so wird hier zusätzlich die Adresse angegeben, welche sich aus der Geräteerkennung ableitet. Sollen andere beliebige Geräte gefunden werden, wird eine reservierte Adresse verwendet. Ist der Trailer mit angegeben, heißt dies, dass ein Paketkopf folgt.

Der Paketkopf definiert den Pakettyt und enthält Daten zur Flusskontrolle.

Im Feld AMA steht die lokale Piconetzadresse des Empfängers. Sendet der Master ein Paket an alle Slaves, so wird als Adresse die Null eingetragen. Sendet ein Slave an den Master, so trägt er seine eigene Adresse ein. HEC (Head Error Check) beinhaltet die Prüfsumme des Paketkopfes. Diese insgesamt 18 Bit werden mit einer Forward Error Check Rate (FEC Rate) von 1/3 versandt. Dies bedeutet, dass jedes Bit 3fach redundant Versandt wird.

Die Daten enthalten die eigentliche Nutzlast, welche abhängig vom Pakettyt ist.

Es gibt vier SCO-Pakettyten und sieben ACL-Pakettyten.

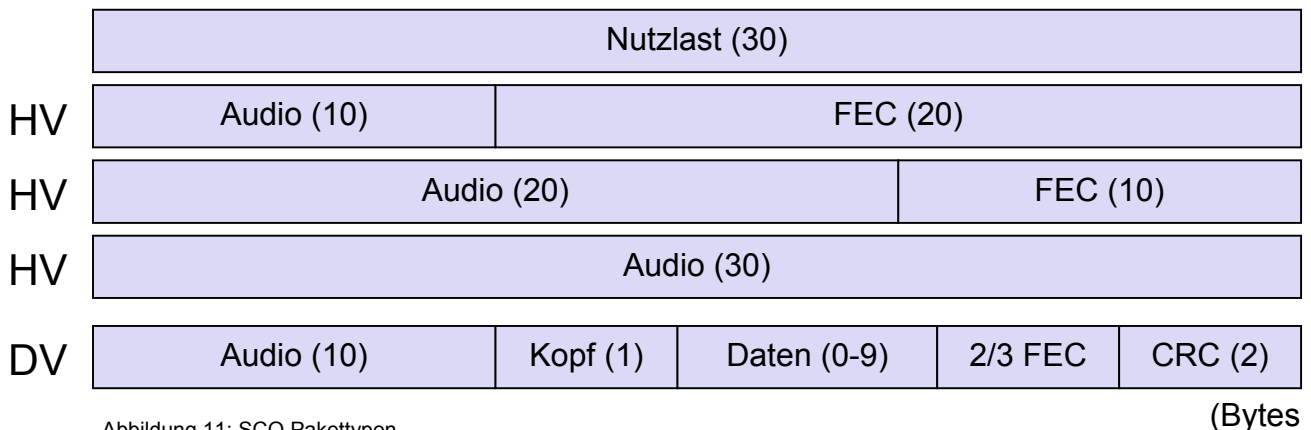


Abbildung 11: SCO Pakettyten

(Bytes)

Für die Audioübertragung stehen die vier Pakettypen HV1, HV2, HV3 und DV zur Verfügung. Jedes dieser Pakete belegt genau einen Slot und nutzt SCO-Links. Der Typ DV erlaubt neben 10 Byte Audiodaten, auch 1 bis 9 Byte Daten zu transportieren. Die Daten werden mit einer FEC Rate von 2/3 gesendet. Der Unterschied zwischen HV1,2 und 3 liegt in der Datenmenge pro Paket sowie in der FEC Rate. Den HV Paketen stehen reservierte Slots zur Verfügung (siehe 3.1.2, SCO-Links). Die Auswahl der FEC Rate erfolgt meist in Abhängigkeit von der Fehlerrate auf dem Kanal. Dies bedeutet zwar einen Mehraufwand, jedoch kann so mehrmaliges Übertragen der Daten verhindert werden. Die Nettodatenrate ist für alle Pakettypen gleich. Hohe Fehlertoleranz wird hier durch eine höhere Belegung der zur Verfügung stehenden Slots erkauft.

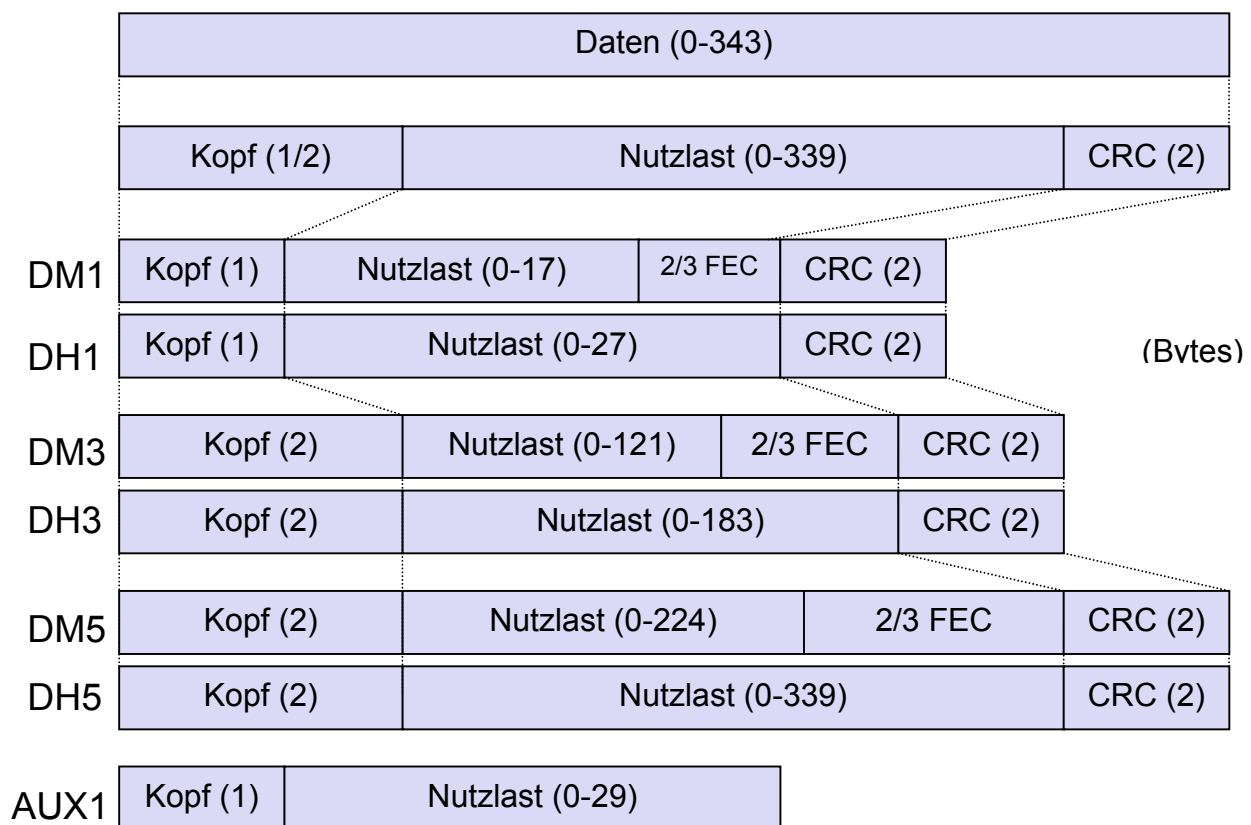


Abbildung 12: ACL Pakettypen

Für die Datenübertragung stehen 7 Pakettypen zur Verfügung, die alle ACL-Links nutzen. Bis auf den Typ AUX1 verwenden die Pakettypen eine 2 Byte Prüfsumme (CRC). Der DM Typ (Data Medium Rate) sichert den Datenblock mit einer 2/3 FEC Rate. Die Data High Rate (DH) nutzt kein FEC, wodurch mehr Daten übertragen werden können. AUX1, DM1 und DH1 belegen einen Slot, DM3 und DH3 belegen 3 Slots und DM5, DH5 belegen 5 Slots.

Aus dem Paketaufbau resultieren auch die maximalen Datenraten von Bluetooth:

- Für asynchronen Datentransport ergeben sich 723,2 kBits/s für die eine Richtung und 57,6 kBits/s für die Gegenrichtung
- Für den synchronen Datentransport ergeben sich 433,9 kBits/s in beide Richtungen
- Für Audioübertragungen erreicht man maximal 64 kBits/s in beide Richtungen

ACL	Typ	Paketkopf [Byte]	Nutz- last [Byte]	FEC	CRC	Datenrate (symmet- risch) [kBit/s]	Datenrate (asymmetrisch)	
							vorwärts [kBit/s]	rückwärts [kBit/s]
1 Zeit- schlitz	DM1	1	0-17	2/3	ja	108,8	108,8	108,8
	DH1	1	0-27	keine	ja	172,8	172,8	172,8
3 Zeit- schlitze	DM3	2	0-121	2/3	ja	258,1	387,2	54,4
	DH3	2	0-183	keine	ja	390,4	585,6	86,4
5 Zeit- schlitze	DM5	2	0-224	2/3	ja	286,7	477,8	36,3
	DH5	2	0-339	keine	ja	433,9	723,2	57,6
SCO	AUX1	1	0-29	keine	nein	185,6	185,6	185,6
	HV1	-	10	1/3	nein	64	-	-
	HV2	-	20	2/3	nein	64	-	-
	HV3	-	30	keine	nein	64	-	-
	DV	1 D	10 + (0-9)D	2/3 D	Ja D	64 + 57,6 D	-	-

Abbildung 13: Bluetooth Basisband Datenraten

3.2 Link Manager

Das Protokoll für die Verbindungsverwaltung (Link Manager Protocol, LMP) erweitert die Baseband Schicht um zusätzliche Funktionen. Die Baseband Schicht wird nicht vollkommen abgedeckt vom LMP, so dass höhere Schichten weiter auf die Baseband Funktionen zugreifen können.

LMP Pakete werden über ACL-Links übertragen. Ihre Verarbeitung erfolgt direkt in der LMP Schicht des Empfängers. Um die Pakete als LMP Pakete zu identifizieren, erhalten sie einen Eintrag im Paketheader.

Die Verbindungsverwaltung bietet eine Vielzahl von Funktionen an. Die wichtigsten werden im folgenden kurz beschrieben:

- Authentifizierung und Verschlüsselung: Das LMP nimmt sowohl bei der Verschlüsselung als auch bei der Authentifizierung eine indirekte Rolle ein. Es steuert den Austausch von Zufallszahlen und signierten Antworten. Ferner setzt das LMP den Verschlüsselungsmodus sowie die Schlüssellänge und den Startwert für den Verschlüsselungsprozess fest. In erster Linie dient dies zum Schutz vor dem Eingriff Dritter in die Kommunikation zwischen zwei Geräten.
- Synchronisierung: Eine exakte Zeitmessung ist bei Bluetooth extrem wichtig, um beispielsweise den Anfang eines Slots exakt ermitteln zu können. Jedes Bluetooth-Gerät verfügt über eine interne Uhr. Die verschiedenen Uhren der Teilnehmer eines Piconetzes werden mit der des Masters abgeglichen. Die Uhren werden hierzu nicht geändert, sondern es wird ein Offset berechnet, welcher zu der aktuellen Zeit addiert wird.
- Verbindungsüberwachung: Nach dem Verbindungsaufbau zwischen Geräten existiert zunächst nur ein ACL-Link. Das LMP ist in der Lage SCO-Links auf- und auch abzubauen.
- Leistungssteuerung: Ein Bluetooth-Gerät kann jederzeit die Stärke des empfangenen Signals messen. Ist das Signal zu stark bzw. zu schwach, so wird der Sender angewiesen, seine Signalstärke anzupassen.
- Dienstgüteaushandlung: Dieses Feature ermöglicht es, durch eine Vielzahl von Funktionen auf die Übertragungsqualität zu reagieren. Sollte etwa die Fehlerrate ansteigen, so kann dies durch die Wahl eines Pakettyps mit höherer FEC Rate kompensiert werden. Der Master kann seine eigene Sendebandbreite auch erhöhen, indem er die Anzahl der Slots, die einem Slave für eine Antwort zur Verfügung stehen, begrenzt.

- Tausch der Master/Slave Rollen: Sollte es für bestimmte Anwendungen nötig sein, so regelt LMP den Rollentausch des Masters mit einem Slave.
- Ändern der Verbindungszustände: LMP Funktionen ermöglichen den Wechsel zwischen verschiedenen Betriebszuständen.

Betriebsmodi

Man unterscheidet bei Bluetooth insgesamt acht verschiedene Verbindungsmodi.

Wird ein Bluetooth-Gerät eingeschaltet, so befindet es sich im Bereitschaftszustand (*Standby*). In diesem Zustand hat es noch keine Verbindung zu anderen Geräten. Er zeichnet sich durch einen geringen Stromverbrauch aus, da lediglich die innere Uhr weiterbetrieben wird. Es folgt nun der Erkundigungszustand (*Inquiry*). Das Gerät sucht in diesem Zustand nach anderen Bluetooth-Geräten, die sich in Kommunikationsreichweite befinden. Hierbei wird der Datenverkehr auf 32 standardisierten Frequenzen nach dem Inquiry Access Code abgehört, den jedes Gerät zyklisch aussendet. Suchende Geräte erhalten so die Geräteadressen von erreichbaren Geräten.

Falls die Erkundigung nach anderen Geräten erfolgreich war, wechselt das Gerät in den Ausrufen-Zustand (*page*). Es erfolgt die eigentliche Kontaktaufnahme.

Ein Bluetooth-Gerät begibt sich zyklisch in den Zustand *Page Scan*. Der Nachrichtenverkehr wird abgehört. Wird ein Paket mit der eigenen Geräteadresse entdeckt, so erfolgt der Kontaktaufbau.

Ist ein Gerät mit einem Piconetz verbunden, so kann in Abhängigkeit von der eigenen Kommunikationsaktivität zwischen 4 Verbindungszuständen gewählt werden:

- Active Mode: In diesem Modus befinden sich normal verbundene Geräte. Der Slave hört die Übertragungen vom Master ständig ab und sendet nach Aufforderung Pakete an den Master, auch wenn keine Daten übertragen werden müssen.
- Sniff Mode: Der Modus ist für Slaves gedacht, bei denen kein großes Kommunikationsaufkommen erwartet wird. Der Master kontaktiert den Slave wesentlich seltener mit Sendeanforderungen. Der Slave muss also nicht mehr ständig den Datenverkehr abhören. Dies hat jedoch auch zur Folge, dass der Slave weniger Gelegenheit hat, Daten an den Master zu übertragen.
- Hold Mode: Falls gerade keine Daten übertragen werden, kann ein Gerät seinen Stromverbrauch weiter reduzieren.

- Park Mode: In diesem Zustand weißt ein Gerät die wenigsten Aktivitäten auf. Das Gerät kommuniziert nicht mehr aktiv, bleibt aber hinsichtlich seiner Sprungsequenz synchronisiert. Zu bestimmten Zeitpunkten wacht es auf, um sich erneut zu synchronisieren. Mit diesem Modus kann die Grenze von 8 Geräten pro Piconetz umgangen werden.

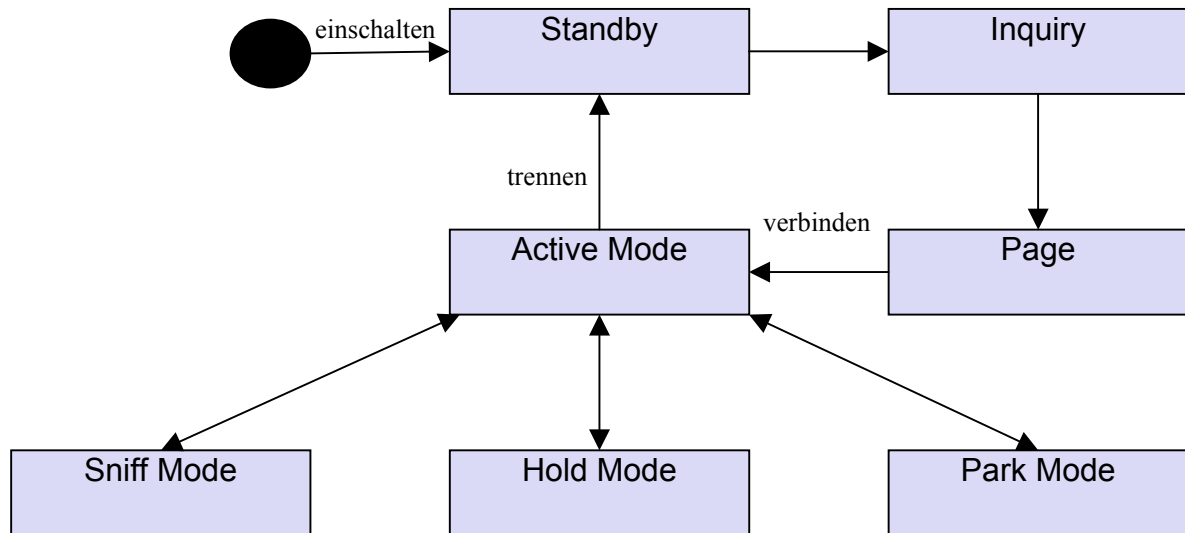


Abbildung 14: Bluetooth Betriebsmodi

Sniff, Hold und Park Mode sind Energiesparzustände. Im Sniff und Hold Mode behalten die Slaves ihre Active Member Adress (AMA). Im Park Mode hingegen wird die AMA abgegeben und der Slave erhält eine PMA (Park Member Adress). Insgesamt können sich 255 Geräte im Park Mode aufhalten.

3.3 L2CAP

Das Logical Link Control and Adaption Protocol (L2CAP) liegt oberhalb der Baseband Schicht. Seine wichtigste Funktion ist die Bereitstellung mehrerer logischer Kanäle über eine bestehende ACL Verbindung zwischen Master und Slave. Es gibt 3 Typen logischer Kanäle:

- Verbindungslos: Diese unidirektionalen Kanäle werden vom Master typischerweise für Rundrufe verwendet. Mit einem verbindungslosen Kanal kann der Master beliebige Slaves erreichen. Meist wird dieser Kanal jedoch mit allen Slaves im Piconetz verknüpft.
- Verbindungsorientiert: Diese bidirektionalen Kanäle stellen eine Datenverbindung zwischen genau zwei Geräten zur Verbindung.
- Signalisierung: Dieser Kanal wird von der L2CAP Schicht benutzt, um weitere logische Kanäle einzurichten.

Jeder logische Kanal wird eindeutig durch einen Channel Identifier (CID) identifiziert. Der CID-Wert 1 ist hierbei für die Signalisierungskanäle reserviert, CID-Wert 2 kennzeichnet die verbindungslosen Kanäle. Der CID-Wert 2 ist allerdings nur auf der Empfängerseite verpflichtend. Die CID-Werte von 3-63 sind reserviert. Die L2CAP Schicht eines Gerätes kann die Identifier für verbindungsorientierte Kanäle aus einem Intervall von 64 bis 65535 frei wählen.

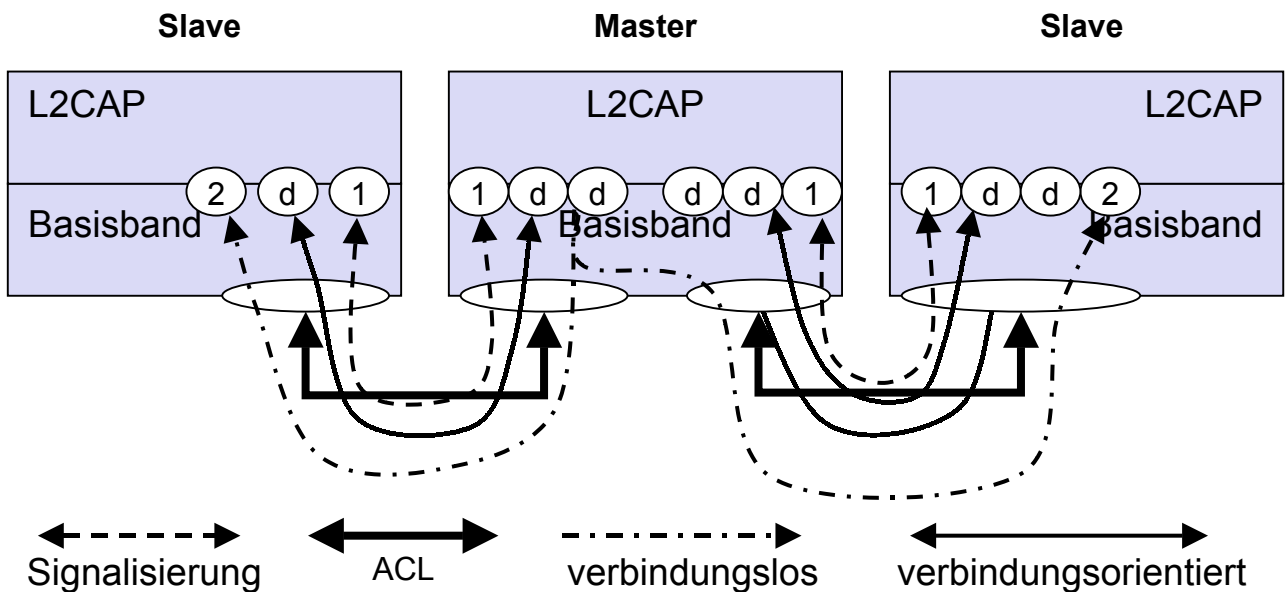


Abbildung 15: Logische Kanäle zwischen Geräten

Zu jeder Art logischer Kanäle gehört ein spezieller Typ Datenpaket. Das Paketfeld ‚Länge‘ gibt die Länge der Nutzlast an. Die Nutzlast der Signalisierungspakete enthält zusätzlich Befehle. Diese werden beispielweise für Verbindungsanforderungen benötigt.

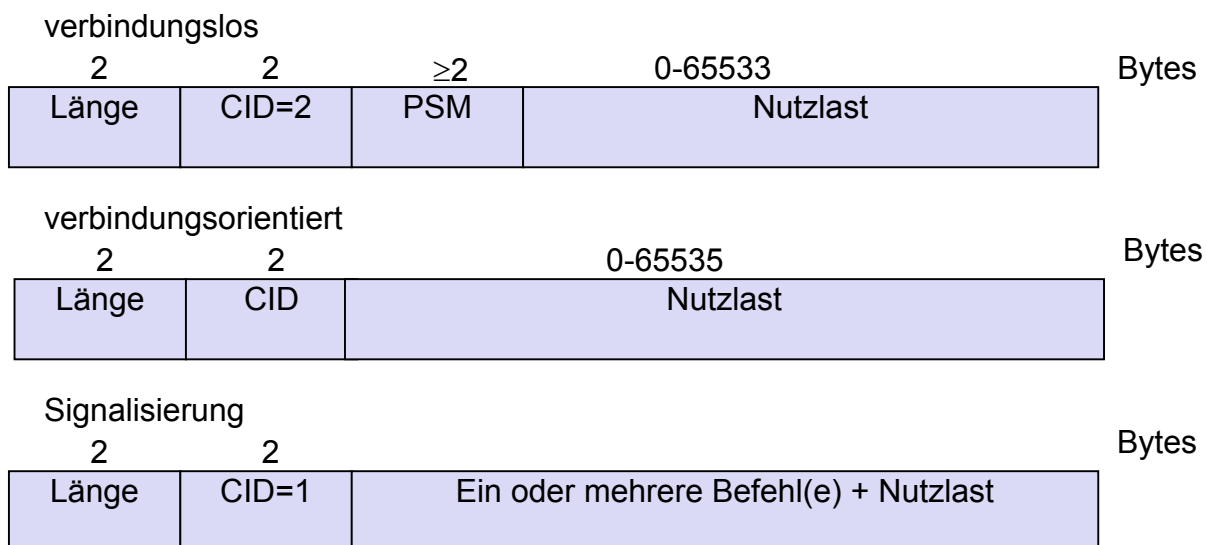


Abbildung 16: L2CAP Paketformate

Die L2CAP Pakete haben eine Größe von 64 KByte. Die Baseband Schicht kann hingegen nur sehr viel kleinere Pakete (unter 0,4 KByte) transportieren. L2CAP hat die zweite wichtige Funktion die großen Pakete für den Transport in mehrere kleinere zu zerlegen, dabei werden jeweils nur Teile eines Paketes hintereinander über die Verbindung versendet. So wird sichergestellt, dass auf Empfängerseite ein Paket komplett rekonstruiert werden kann, bevor Teile eines anderen Paketes eintreffen.

3.4 SDP/RFCOMM/TCS BIN

SDP

Ein wichtiger Bestandteil von Bluetooth ist, dass die Geräte in vorher unbekanntem Umgebungen spontan mit anderen Geräten in Kontakt treten sollen. Es ist daher notwendig zu wissen, welche Geräte sich in Kommunikationsweite aufhalten, genauer gesagt, welche Dienste diese Geräte anbieten. Zur Suche von Diensten wurde in Bluetooth das *Service Discovery Protocol* (SDP) spezifiziert. Geräte, die Dienste anbieten, müssen einen SDP-Server installieren. Geräte, die lediglich Dienste nutzen wollen, müssen einen SDP-Client installieren. SDP stellt lediglich Informationen über Dienste zur Verfügung, die Dienstonutzung ist allerdings nicht Bestandteil des Protokolls.

Momentan gibt es noch keine Verfahren, Geräte über neu hinzugefügte oder entfernte Dienste zu benachrichtigen. Weiterhin wird keine Zugriffskontrolle unterstützt, das heißt jedes Gerät kann alle Dienste nutzen. Auch erlaubt SDP keine Weitervermittlung von Diensten. All diese Funktionen könnten jedoch in Zukunft implementiert werden.

RFCOMM

RFCOMM emuliert serielle Schnittstellen. Mit Hilfe dieses Protokolls können die Kabel für eine serielle Verbindung zwischen zum Beispiel einem Handy und einem Laptop entfallen, wobei aber weiterhin alle bisherigen Protokolle und Anwendungen, nun aber über Bluetooth, verwendet werden können.

Mit Hilfe weiterer Protokolle, welche auf RFCOMM aufsetzen, können sogar die Protokolle TCP und UDP genutzt werden. Damit ist es möglich, Internetverbindungen über Bluetooth herzustellen.

TCSBIN

Das *Telephony Control Protocol Specification Binary* beschreibt zur Steuerung typischer Telefonfunktionen ein Bit orientiertes Protokoll. Bluetooth Geräte können so beispielsweise als schnurlose Telefone betrieben werden.

4. Sicherheit in Bluetooth-Netzen

Bluetooth bietet ein sehr einfaches Sicherheitskonzept an. Ein Bluetooth-Gerät kann seine Sendeleistung so vermindern, dass möglichst nur der gewünschte Kommunikationspartner erreicht wird. Damit ist auf einfache Weise ein Schutz gegen Abhören gegeben.

Da dieser Schutz natürlich nicht optimal ist, wurde ein umfangreiches Sicherheitskonzept integriert, welches die Authentifizierung von Geräten und die Verschlüsselung von Nutzdaten umfasst. Es werden drei Sicherheitsmodi unterschieden:

Modus 1 (keine Sicherheit): Dieser Modus ist für den Fall gedacht, dass eine Verschlüsselung unerwünscht oder auch nicht nötig ist.

Modus 2 (Sicherheit auf Dienstebene): Die Sicherheitsbedingungen werden erst nach dem Aufbau der Verbindung eingerichtet.

Modus 3 (Sicherheit auf Verbindungsebene): Der Modus stellt eine Art Grundsicherheit bei jeder Art von Kommunikation zwischen zwei Geräten dar. Die Sicherheitsbedingungen werden für jede Verbindung neu festgelegt.

Das Sicherheitskonzept im Modus 3 benutzt die folgenden Bestandteile:

- kryptografische Funktionen: Diese werden im folgenden mit E0, E1, E21, E22 und E3 bezeichnet. Ihre Funktionsweise wird nicht genauer betrachtet.
- Zufallszahlengenerator: Der Generator ist nicht weiter spezifiziert. Seine Implementierung wird den Geräteherstellern überlassen.
- Geräteadresse: Jedes Gerät erhält eine weltweit eindeutige 48 Bit Geräteerkennung. Die Adresse ist nicht geheim und kann von anderen Geräten erfragt werden.
- Geheimzahl: Die PIN wird für den erstmaligen Verbindungsaufbau zweier Geräte benötigt. Idealerweise wird diese vom Benutzer eingegeben, bei einigen Geräten ist diese aber auch fest in dem Gerät gespeichert.
- Zwei Schlüssel: Für die Verschlüsselung der Daten wird ein Encryption Key verwendet. Er wird aus einem Link Key generiert, welcher zur gegenseitigen Authentifizierung verwendet wird.

4.1 Schlüsselgenerierung

Soll eine gesicherte Verbindung zwischen zwei Geräten eingerichtet werden, so prüfen diese zuerst, ob sie schon einmal miteinander eine gesicherte Verbindung aufgebaut haben und daher schon über einen Link Key verfügen. Ist dies nicht der Fall, so muss zunächst ein gemeinsamer Link Key generiert werden. Mit Hilfe dieses Link Key authentifizieren sich die Geräte gegenseitig.

Um einen Link Key zu erzeugen, benötigt man zu aller erst einen Initialization Key.

Hierzu muss der Benutzer auf beiden Geräten dieselbe PIN eingeben. Ist eine Eingabe nicht möglich, so muss zumindest dieselbe PIN gespeichert sein. Ein Gerät erzeugt jetzt eine Zufallszahl, welche dem anderen übermittelt wird. Aus der PIN und der Zufallszahl erzeugt die Funktion E22 den Initialization Key. Beide Geräte erzeugen den gleichen geheimen Initialization Key.

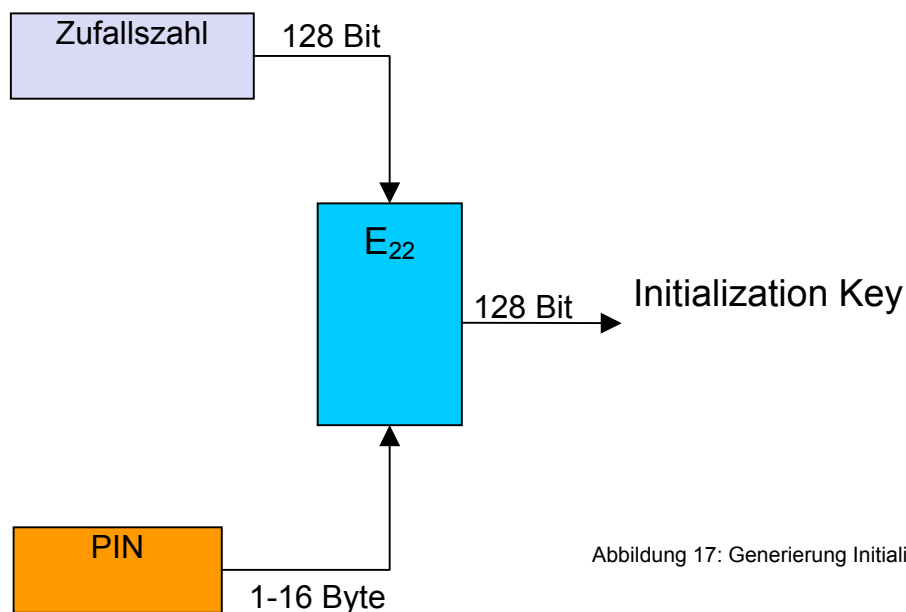


Abbildung 17: Generierung Initialization Key

Der Link Key wird aus einer Zufallszahl und dem Initialization Key mit der kryptischen Funktion E21 erzeugt.

4.2 Authentifizierung

Nach der Vereinbarung eines Link Keys, authentifizieren sich die Geräte gegenseitig.

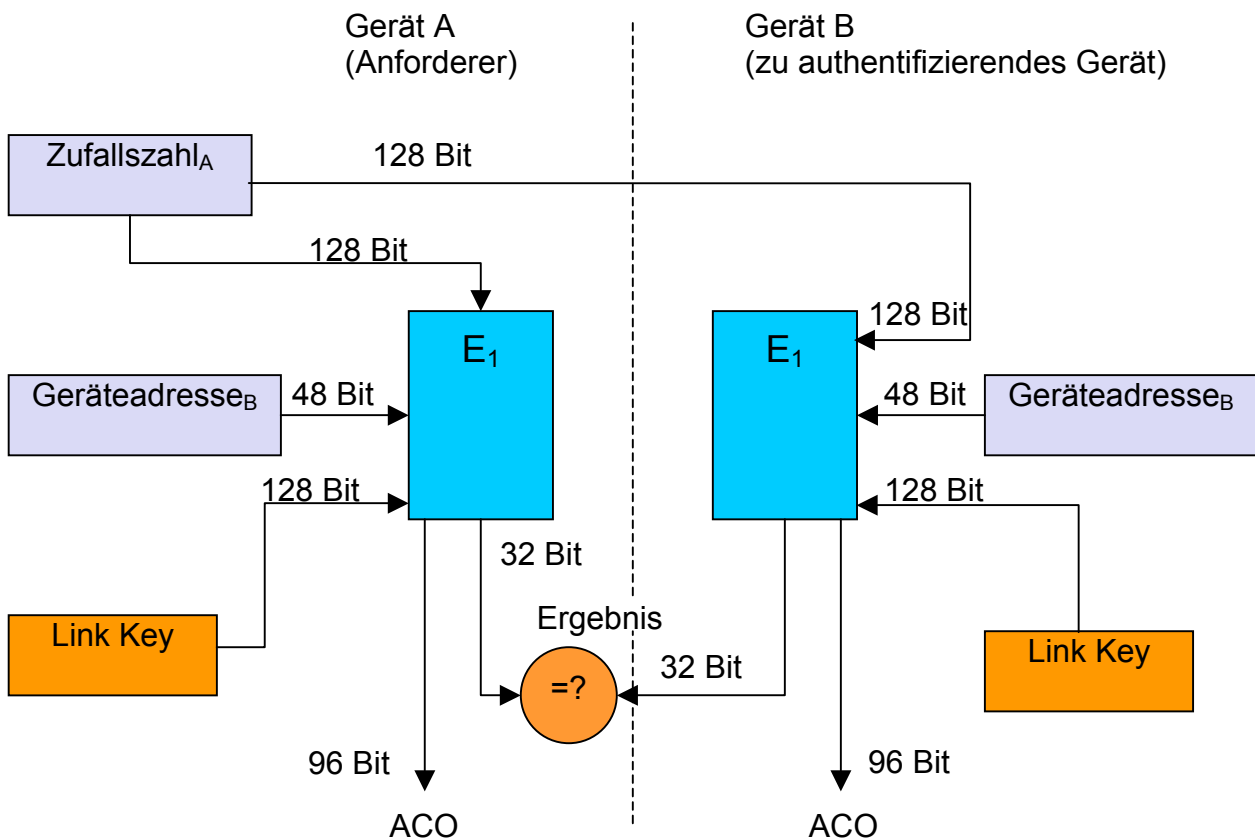


Abbildung 18: Authentifizierung

Gerat A (Anforderer) fordert Authentifizierung von Gerat B an. Das anfordernde Gerat erzeugt eine Zufallszahl und sendet sie ans andere Gerat. Die Funktion E₁ findet Anwendung. In deren Berechnung flieen die Zufallszahl, die Geratekennung von Gerat B und der geheime Link Key ein. Nur wenn beide Gerate den gleichen Link Key besitzen, erhalten sie ein identisches Ergebnis. Das Ergebnis wird an das anfordernde Gerat ubertragen, welches beide Ergebnisse vergleicht. Sind beide Ergebnisse gleich, so ist die Authentifizierung positiv. E₁ berechnet zusatzlich zum eigentlichen Ergebnis einen Wert ACO, der fur die spatere Verschlusselung benotigt wird.

4.3 Verschlüsselung

Im ersten Schritt der Verschlüsselung wird über die Funktion E3 ein Encryption Key gebildet. Beide Geräte einigen sich vorher auf eine Schlüssellänge zwischen 8 und 128 Bit. Diese Variable Schlüssellänge ist auch der Grund dafür, dass man nicht gleich den Link Key verwendet. Neben einer Zufallszahl und dem Link Key fließt in die Berechnung des Encryption Key der Wert COF ein. Dieser wurde aus dem Wert ACO (siehe 4.2 Authentifizierung) gebildet.

Der Encryption Key wird an die Funktion E0 übergeben, welche als weitere Parameter eine Geräteadresse und eine zwischen beiden Geräten synchronisierte Uhrzeit erwartet. E0 erzeugt eine Bitfolge, die mit den Nutzdaten XOR verknüpft werden.

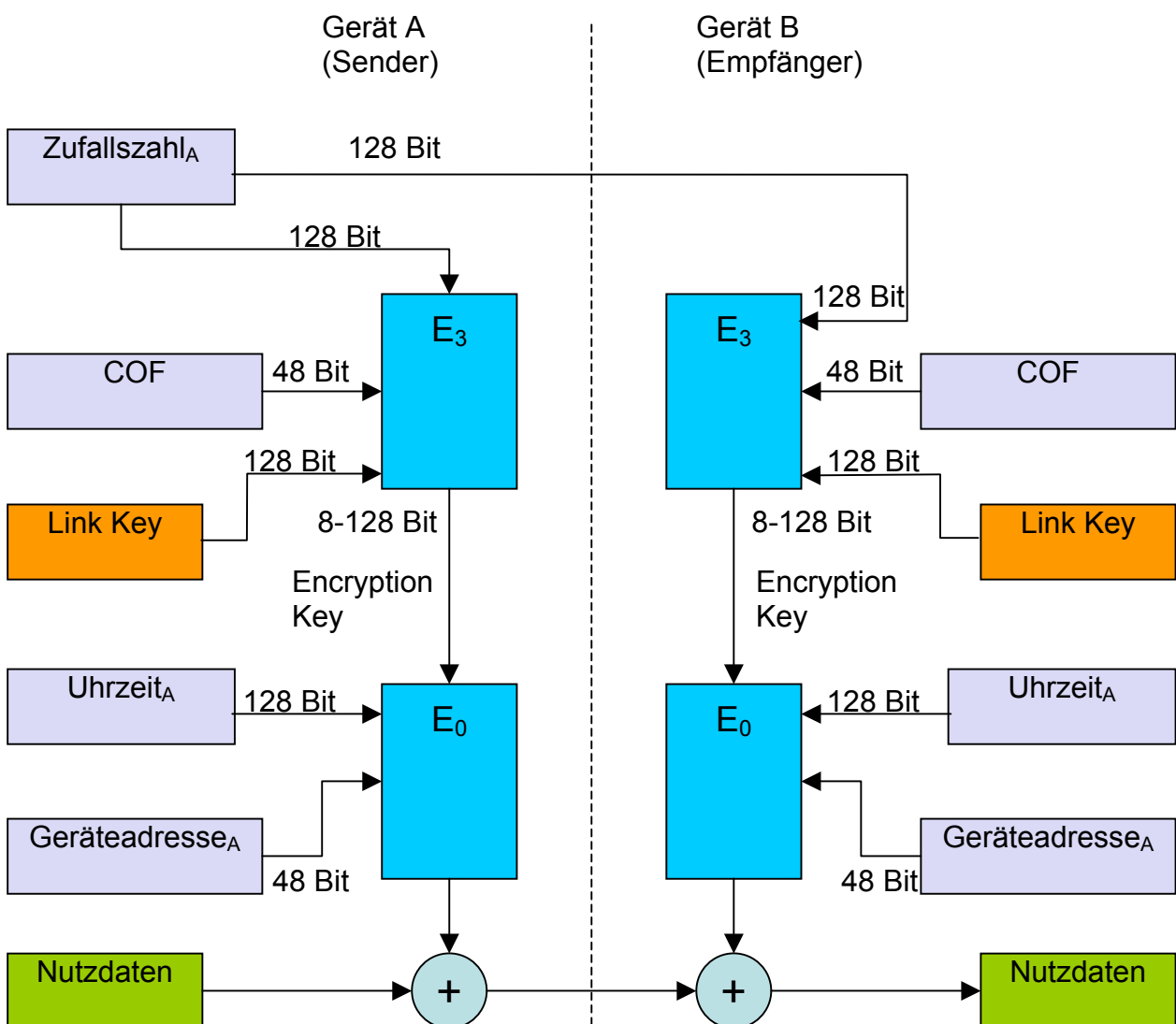


Abbildung 19: Verschlusselung

4.4 Kritik am Sicherheitskonzept

Generell bietet das Bluetooth Sicherheitskonzept mit seinen Bestandteilen Authentifizierung und Verschlüsselung einen ausreichenden Schutz. Es gibt allerdings ein paar Kritikpunkte. An den Zufallszahlengenerator wird in der Bluetoothspezifikation keinerlei Anforderung gestellt. Sind die Ergebnisse des Generators vorhersehbar, so würde die Sicherheit von Verschlüsselung und Authentifizierung beeinträchtigt, da der Schutz vor statistischen Angriffen nicht mehr gewährleistet wäre.

Ein anderer Kritikpunkt ist die PIN. Kann diese in Erfahrung gebracht werden, so lassen sich Link Key und Encryption Key rekonstruieren. Einfache Geräte erlauben häufig nur vierstellige PIN, welche ein austesten der Zahlenkombination sehr vereinfachen. Bei Geräten ohne Eingabemöglichkeit für PINs wird diese vom Hersteller oftmals mit „0000“ fest vorgegeben. Hiermit ist jedes weitere Sicherheitskonzept sehr fragwürdig.

Aufgrund der ständigen Kommunikationsbereitschaft der Bluetooth-Geräte ist es ein einfaches Bewegungsprofile zu erstellen. In einem Kaufhaus könnten Geräte fest platziert werden, welche ständig in Erfahrung bringen, welche anderen Geräte sich in der Umgebung befinden. Einige Geräte bieten hierfür den Non Discoverable Mode an. In diesem Modus reagiert ein Bluetooth-Gerät nicht auf Suchanfragen anderer Geräte.

Literaturverzeichnis

Bücher:

Jochen Schiller: Mobilkommunikation, Pearson 2003, ISBN 3-8273-7060-4

Jörg Roth: Mobile Computing, dPunkt-Verlag 2002, ISBN 3-89864-165-1

Arno Kral, Heinz Kreft: Wireless LANs Networker's Guide, ISBN 3-8272-6329-8

Internetquellen:

<http://www.bluetooth.com/about>

<http://www.heise.de/mobil/artikel/50853>

<http://www.heise.de/mobil/artikel/50888>

<http://www.heise.de/ct/01/09/100/default.shtml>

<http://www.teltarif/i/bluetooth.html>