

Bluetooth

Informatik Seminar

WS 2004/2005

Thorge Wegers

- Einleitung
- Vernetzung
- Der Bluetooth Protokollstapel
- Sicherheit in Bluetooth-Netzen

- Einleitung
 - Geschichte
 - Einsatzgebiete
 - Eigenschaften
- Vernetzung
- Der Bluetooth Protokollstapel
- Sicherheit in Bluetooth-Netzen

- 1994 untersucht Ericsson Alternativen zur kabelgebundenen Verbindung von Geräten
- 1998 erfolgt Gründung der Bluetooth SIG
 - Gründungsmitglieder sind Ericsson, Intel, IBM, Nokia und Toshiba
 - Weitere Firmen treten Bluetooth SIG bei
 - 2004 hat die SIG ca. 3750 Mitglieder

- Im Juli 1999 wird der erste Bluetooth Standard mit Version 1.0 verabschiedet
- Im März 2001 folgt Version 1.1
- Übernahme des Standard v 1.1 als IEEE-Norm 802.15.1

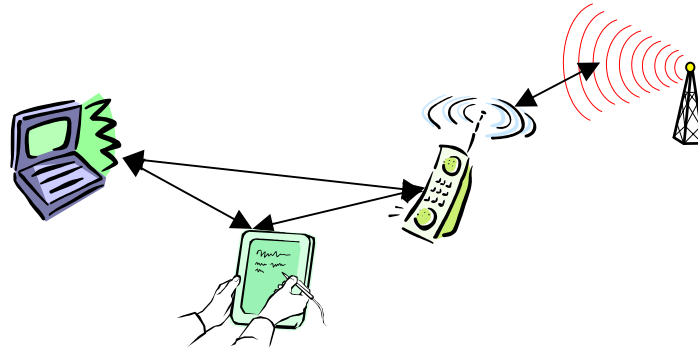


Harald "Blåtand" Gormsen



- Verbinden von Computer und Peripheriegeräten
Problem: Stromversorgung
- Drahtloses Headset
- Schnurloses Telefon

- Verbinden verschiedener Netze




- Realisierung ist auch mit anderen Techniken möglich
- Aber: Bluetooth arbeitet energiesparender und ist kostengünstiger

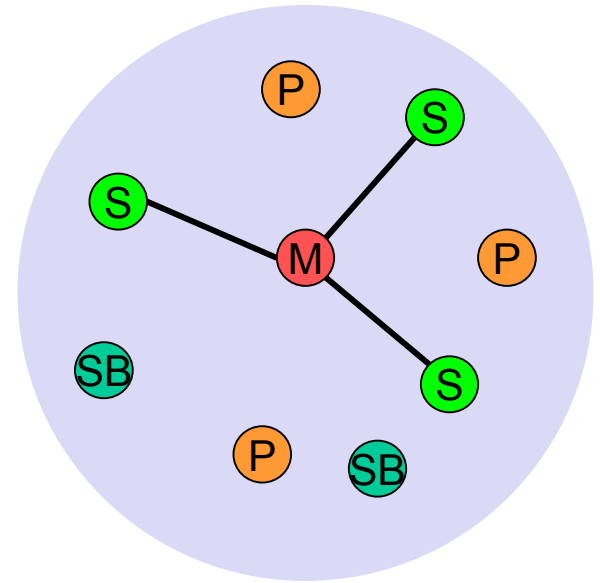
- Universelles Funksystem für drahtlose Verbindungen
- Lizenzfrei im 2,4 GHz ISM Band
- 79 (23) Kanäle mit 1 MHz Kanalabstand
 - Kanal 1: 2402 MHz ... Kanal 79: 2480 MHz
- Frequenzwechsel mit 1600 Sprüngen pro Sekunde
 - Jede Frequenz wird genau 625 μ s gehalten
 - Die Sprungfolge ist pseudozufällig, vorgegeben durch den Master

- Bruttodatenrate beträgt 1MBit/s
- Geräte in Kommunikationsreichweite werden automatisch verbunden
- Sowohl Audio- als auch Datenkanäle
- Ausgangsleistung von Bluetooth-Geräten ca. 800 mal kleiner als die von GSM-Telefonen

- Einleitung
- Vernetzung
 - Piconetz
 - Scatternetz
- Der Bluetooth Protokollstapel
- Sicherheit in Bluetooth-Netzen

- Master: Leitstation, leitet die Verbindungsaufnahme ein
- Slave: Folgestation, reagierendes Gerät
- Master sendet Geräteerkennung und Wert seiner internen Uhr an Slaves
- Slaves synchronisieren sich  Piconetz
- Kommunikation zwischen Slaves nicht möglich

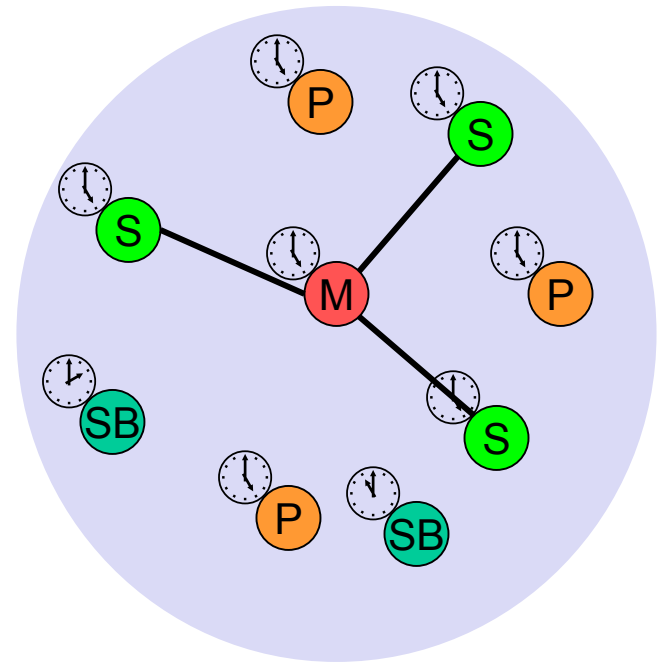
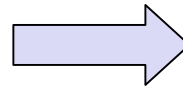
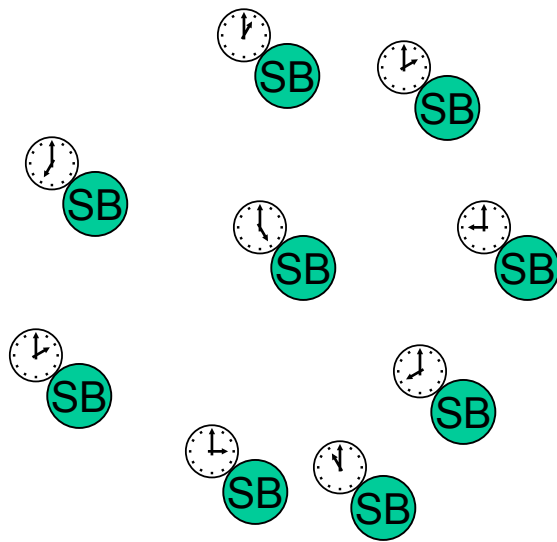
- Netzwerk aus 2 bis 8 Geräten
- Genau ein Master pro Pikonetz
 - Bestimmt die Sprungfolge, Slaves müssen sich synchronisieren



- Jedes Pikonetz hat eindeutige Sprungfolge
- Teilnahme am Pikonetz = synchronisieren auf Sprungfolge

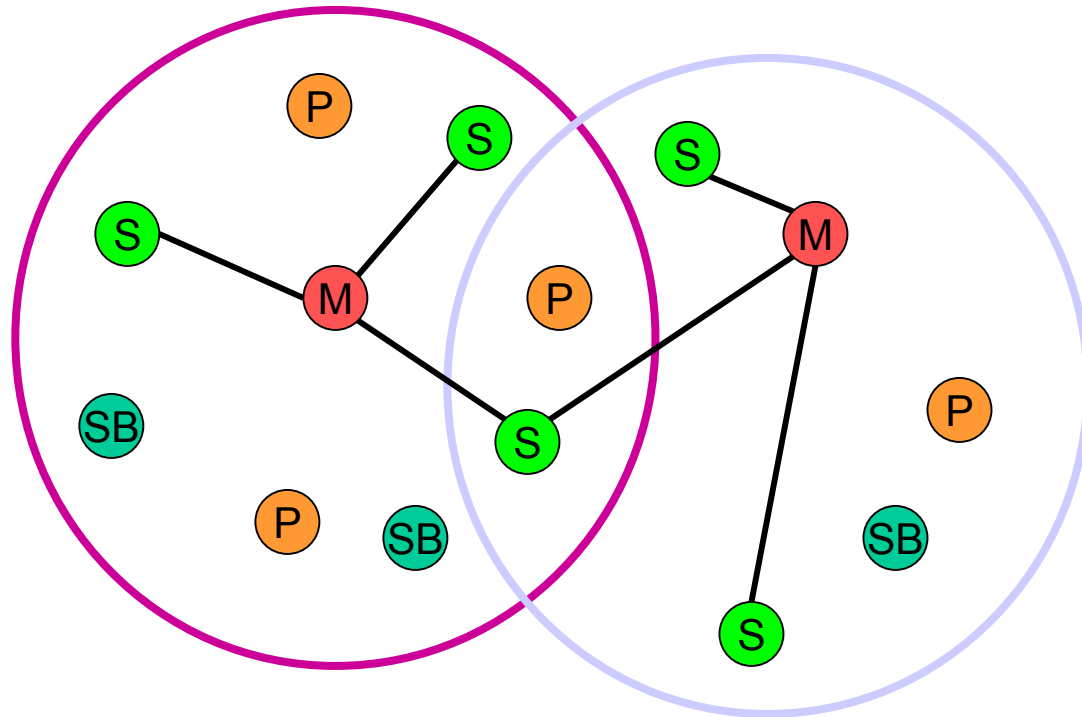
- Alle Geräte springen synchron:
 - Sprungfolge bestimmt durch Geräteerkennung des Masters
 - Phase in der Sprungfolge bestimmt durch Uhrzeit
- Aktive Geräte: 3 Bit AMA (Active Member Adress)
 - Folge: maximal 8 aktive Geräte pro Netz
- Passive Geräte: 8 Bit PMA (Parked Member Adress)
 - Über 200 passive Geräte pro Netz

Synchronisieren der internen Uhr



Scatternetze entstehen durch sich überlappende Piconetze, d.h. es gibt Geräte, die sich in mehreren Piconetzen befinden.

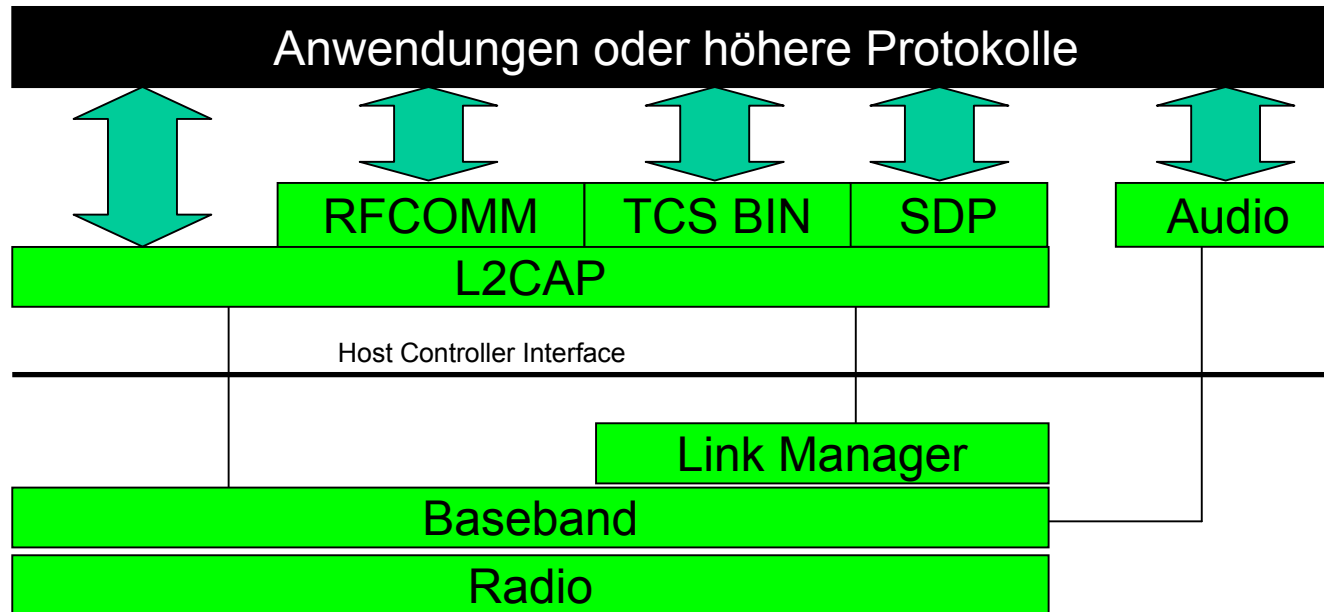
M=Master
S=Slave
P=Parked
SB=Standby



- Vorteile Scatternetze:
 - Möglichkeit großer Netzstrukturen
 - Hoher Datendurchsatz pro Nutzer
- Kommunikation zwischen Piconetzen erfolgt durch Geräte, welche zwischen den Piconetzen hin und her springen
- Master kann nur in einem Piconetz Leitstation, nimmt er an anderem Piconetz teil, so ist er dort Slave

- Einleitung
- Vernetzung
- Der Bluetooth Protokollstapel
 - Bluetooth Radio und Baseband
 - Frequency Hopping
 - Verbindungstypen
 - Paketformate
 - Link Manager
 - Betriebsmodi
 - L2CAP
 - SDP/RFCOMM/TCSBIN
- Sicherheit in Bluetooth-Netzen

Der Bluetooth Protokollstapel



- Radio und Baseband: stellt Zugriff auf Funkmedium bereit
- Link Manager: Funktionen zum Verbindungsaufbau und zur Verbindungsverwaltung
- L2CAP: Anpassung höherer Schichten an Baseband-Funktionen

- SDP: ermöglicht die Suche nach Diensten
- RFCOMM: emuliert serielle Schnittstelle
- TCS BIN: Funktionen zur Anrufkontrolle
- Audio: Übertragung von Audio

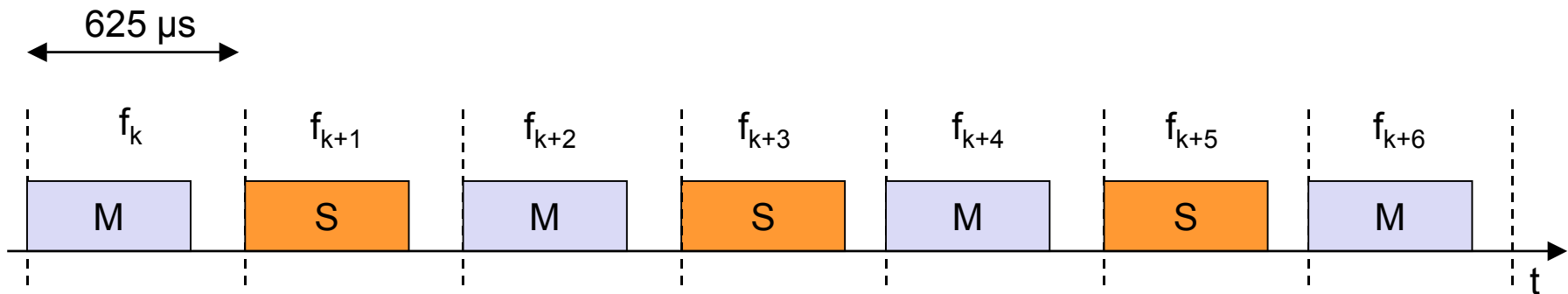
- Regelung des Verbindungsaufbaus
- Datenübertragung über die Funkschnittstelle
- 3 Leistungsklassen

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

- 1600 Frequenzwechsel pro Sekunde
- Jede Frequenz wird 625 μs gehalten
 - Zeitraum wird als Slot bezeichnet
- Sprungfolge wird abgeleitet aus Geräteadresse des Masters
- Jedes Piconetz benutzt individuelle Sprungfolge

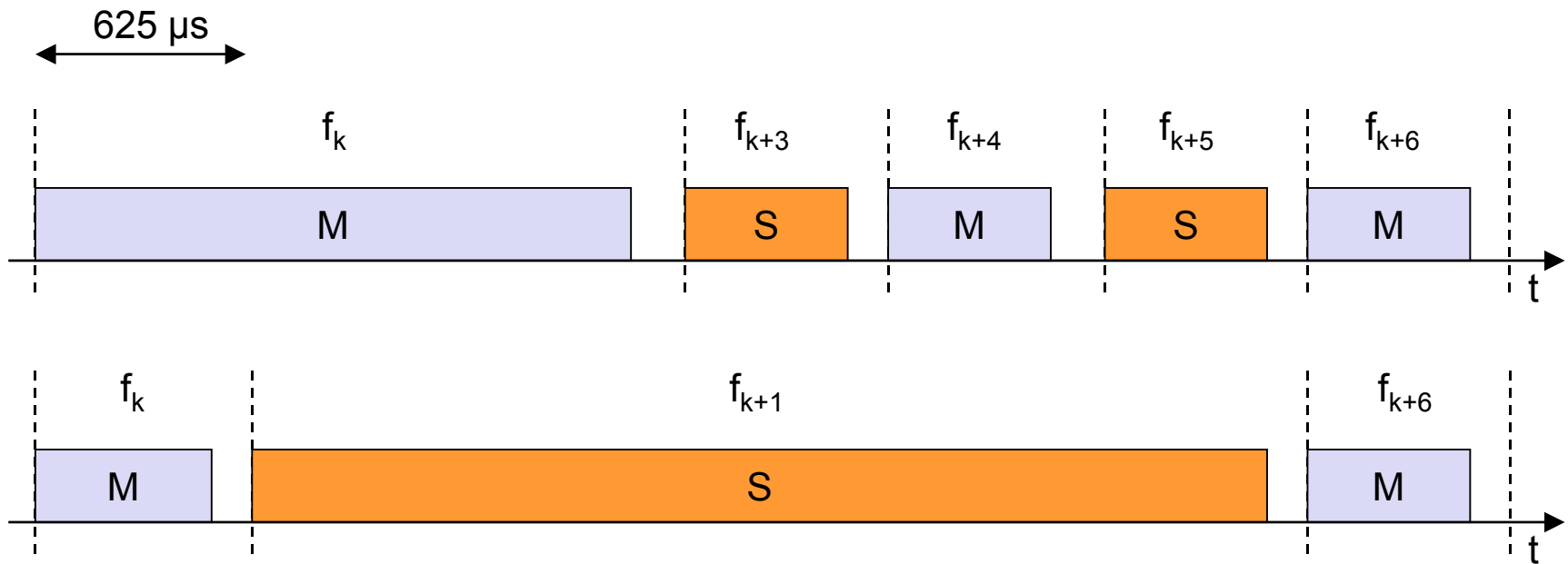
Frequency Hopping

- Unterschiedliche Sprungfolgen schützen vor Kollisionen zwischen Piconetzen
- Kollisionsvermeidung im Piconetz:
 - Master sendet auf geraden Slots
 - Slaves senden auf ungeraden Slots
 - Slave antwortet nur ,wenn der Master ihn auffordert



Frequency Hopping

- Pakete können 1, 3 oder 5 Slots belegen
- Sender verweilt auf gleicher Frequenz
- Innerhalb eines Paketes kein Frequenzwechsel



- Antwort auf Multislotpakete erfolgt auf der Frequenz, die bei einem Wechsel je Slot gültig gewesen wäre.
- Versteckte Endgeräte fahren mit normaler Sprungfolge fort
- Alle Geräte sind nach der Übertragung wieder auf der richtigen Frequenz

Unterstützt werden 2 Verbindungstypen:

- Synchron verbindungsorientiert
(Synchronus **C**onnection-**O**riented Link, SCO)
- Asynchron verbindungslos
(A)synchronus **C**onnectionless Link, ACL)

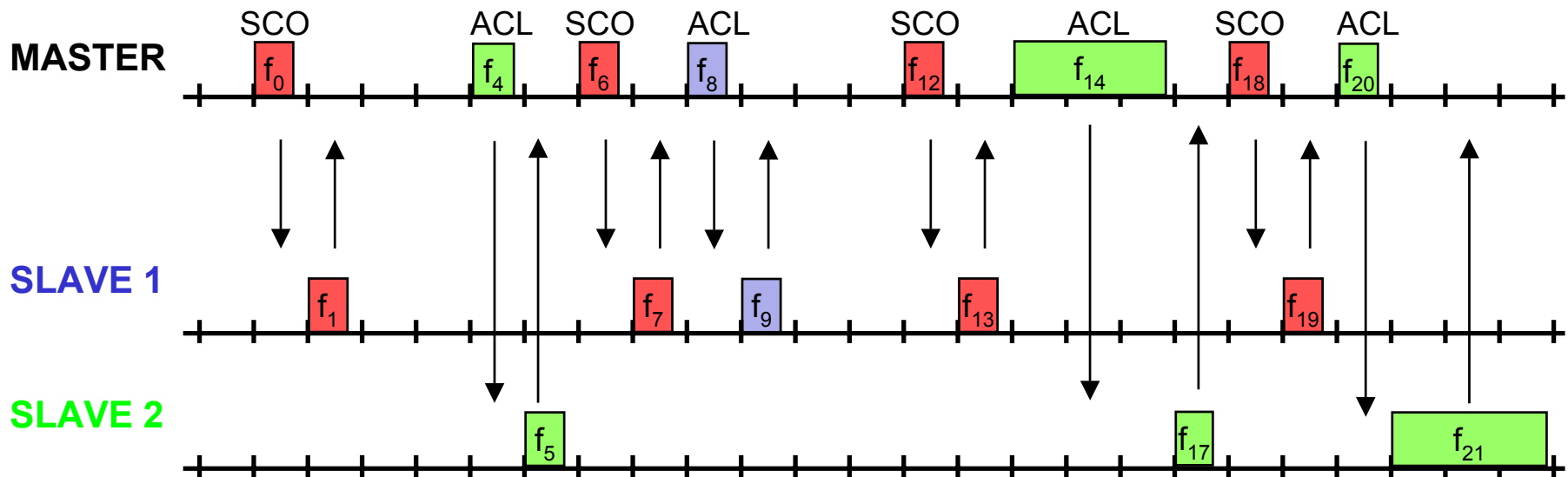
- Symmetrische Punkt-zu-Punkt Verbindung
- Benötigt für klassische Sprachverbindungen
- Pakete im Fehlerfall nicht erneut übertragen
- Datenrate: 64 kBits/s in beide Richtungen

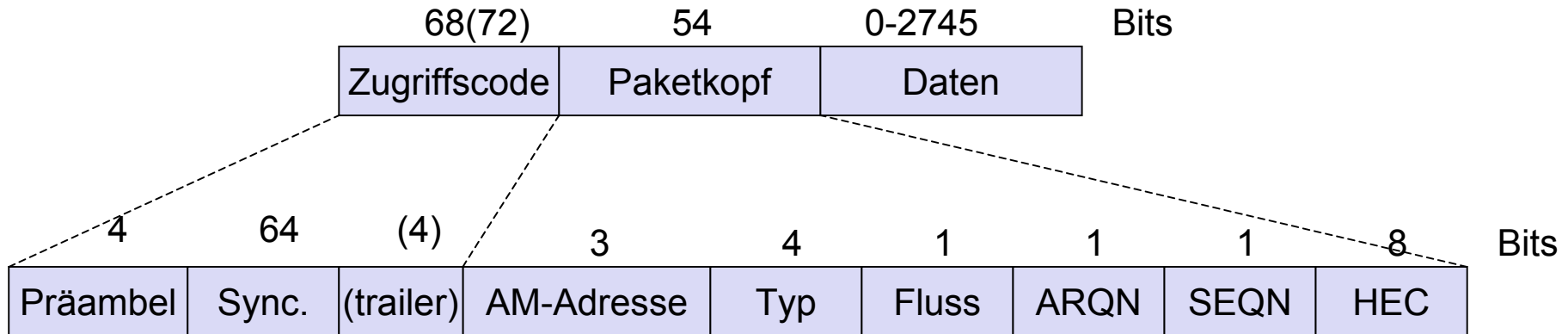
- Bei Einrichtung eines SCO-Links wird feste Bandbreite reserviert
 - Konsequenz: maximal 3 Verbindungen pro Gerät
- Der Master kann bis zu 3 SCO-Links zu einem oder mehreren Slaves herstellen
- Ein Slave kann 3 Links zu einem Master oder 2 zu verschiedenen Leitstationen herstellen

- Benötigt für typische Datenverbindungen
- Ermöglichen Punkt-zu-Mehrpunkt Übertragungen
- Genau eine Verbindung zwischen Master und Slave
- Maximale Datenrate 723,2 kBits/s in die eine Richtung und 57,6 kBits/s in die Gegenrichtung

- Automatische Übertragungswiederholung (ARQ) steht zur Verfügung
- Keine Reservierung von Slots
- Nutzung der Slots, die nicht von SCO-Links belegt sind

ACL-/SCO-Links

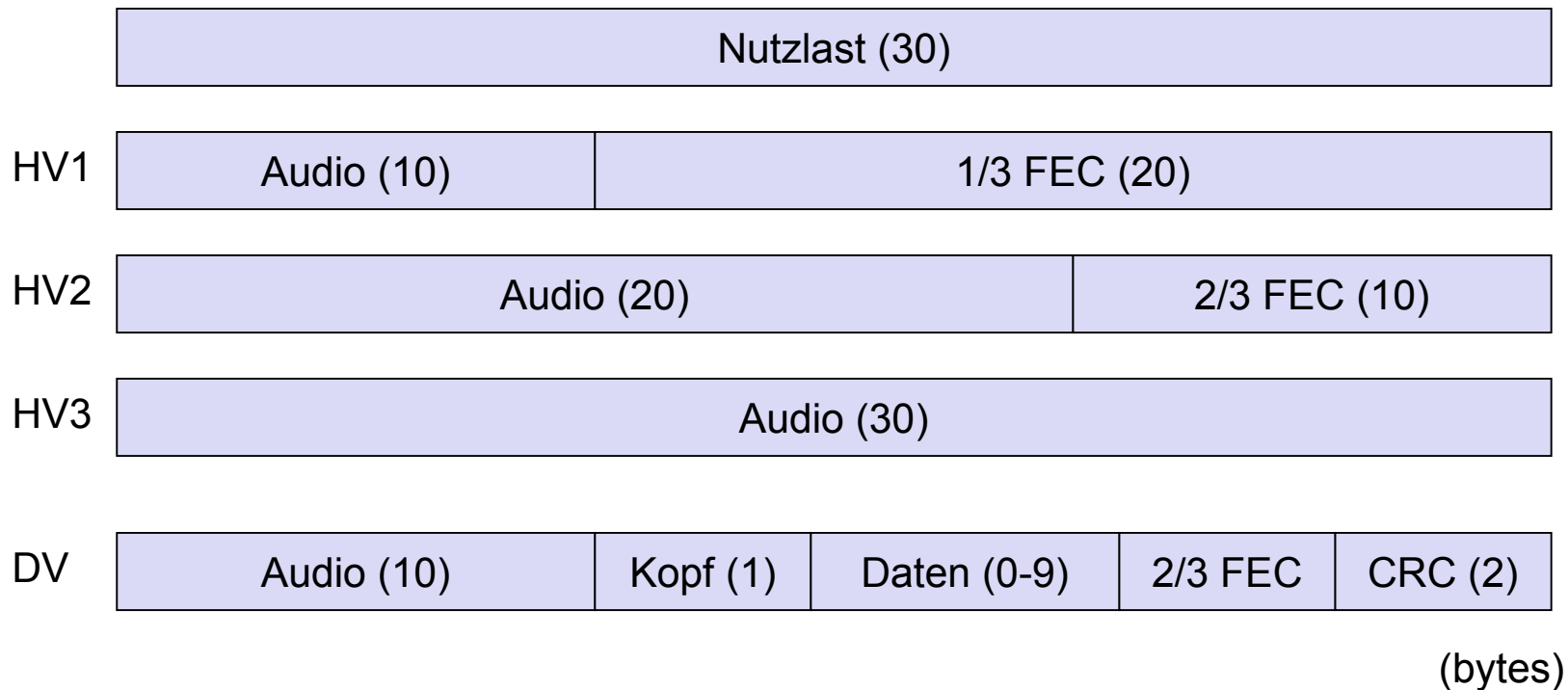




- Zugriffscode: zur Synchronisierung und Identifikation des Piconetzes
- Paketkopf: definiert Pakettyp
 - FEC Rate $\frac{1}{3}$

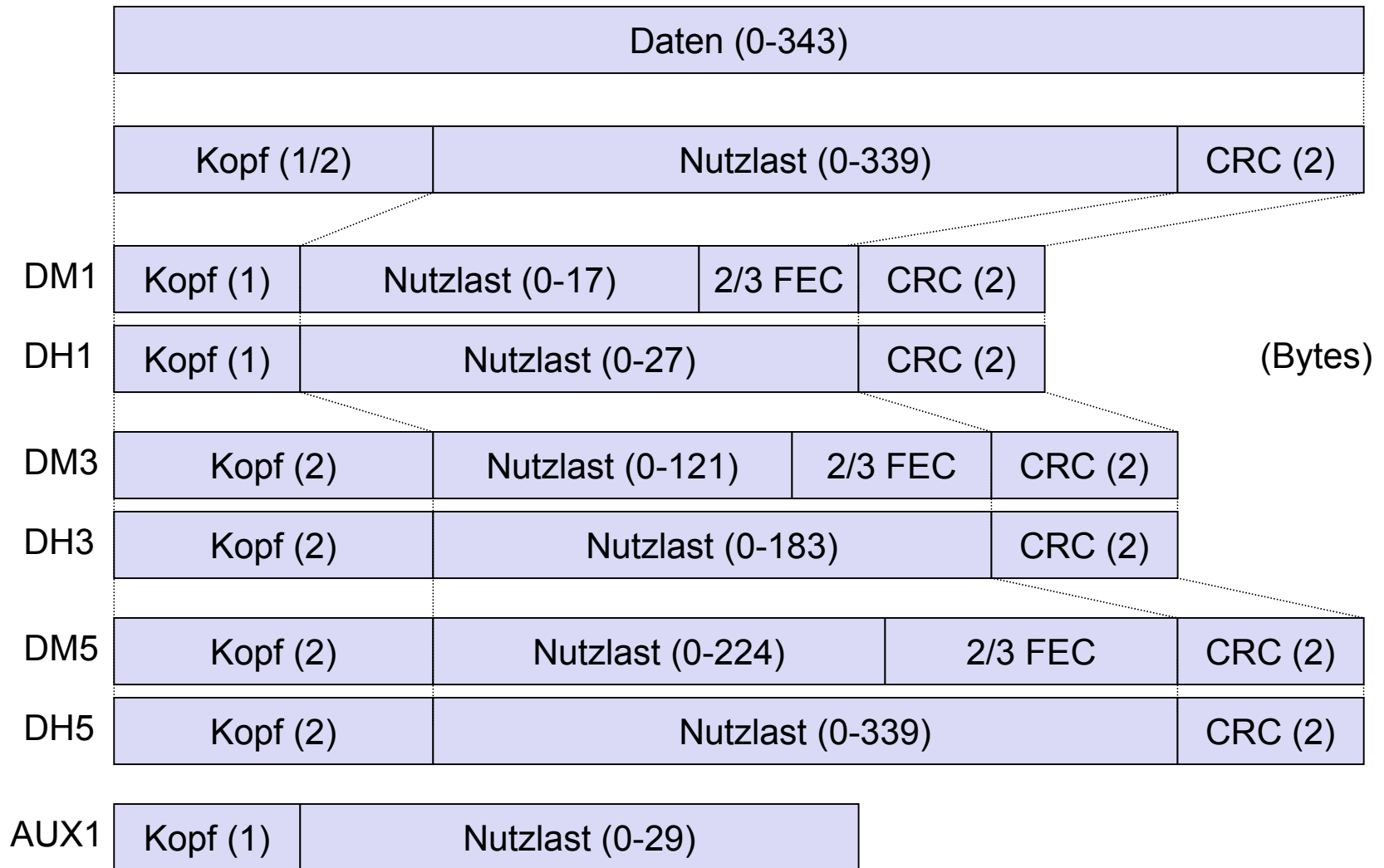
- Daten: enthalten eigentliche Nutzlast
- Nutzlast ist abhängig vom Pakettyp
 - 4 SCO-Pakettypen
 - 7 ACL-Pakettypen

- Pakete belegen genau einen Slot
- Versand über reservierte Slots



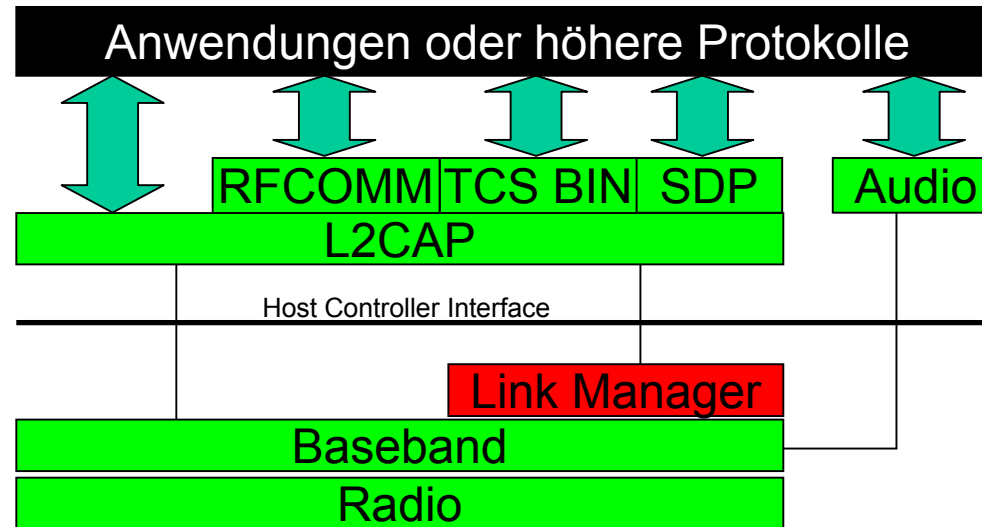
- Auswahl der FEC-Rate in Abhängigkeit von der Fehlerrate auf dem Kanal
- Nettodatenrate für alle Pakettypen gleich
- Fehlertoleranz erkaufte durch höhere Belegung der verfügbaren Slots

ACL-Pakettypen



- Data Medium Rate (DM) sichert Datenblock mit $\frac{2}{3}$ FEC-Rate
- Data High Rate (DH) nutzt kein FEC
==> mehr Daten übertragbar
- Paketlänge 1, 3 bzw. 5 Slots

ACL	Typ	Nutzlast	Nutzlast	FEC	CRC	Symmetrisch	Asymmetrisch
		Kopf [byte]	Daten [byte]			max. Rate [kbit/s]	max. Rate [kbit/s] Forward Reverse
1 Zeit- schlitz	DM1	1	0-17	2/3	yes	108.8	108.8 108.8
	DH1	1	0-27	no	yes	172.8	172.8 172.8
3 Zeit- schlitze	DM3	2	0-121	2/3	yes	258.1	387.2 54.4
	DH3	2	0-183	no	yes	390.4	585.6 86.4
5 Zeit- schlitze	DM5	2	0-224	2/3	yes	286.7	477.8 36.3
	DH5	2	0-339	no	yes	433.9	723.2 57.6
SCO	AUX1	1	0-29	no	no	185.6	185.6 185.6
	HV1	na	10	1/3	no	64.0	
	HV2	na	20	2/3	no	64.0	
	HV3	na	30	no	no	64.0	
	DV	1 D	10+(0-9) D	2/3 D	yes D	64.0+57.6 D	



- Erweiterung der Baseband Schicht um weitere Funktionen
- LMP Paketübertragung über ACL-Links
- LMP Pakete erhalten zur Identifizierung einen Eintrag im Paketheader

- Authentifizierung und Verschlüsselung
 - Indirekte Rolle des Link Managers
 - Steuert Austausch von Zufallszahlen
 - Festsetzen von Verschlüsselungsmodus und Schlüssellänge
- Tausch der Master und Slave Rollen

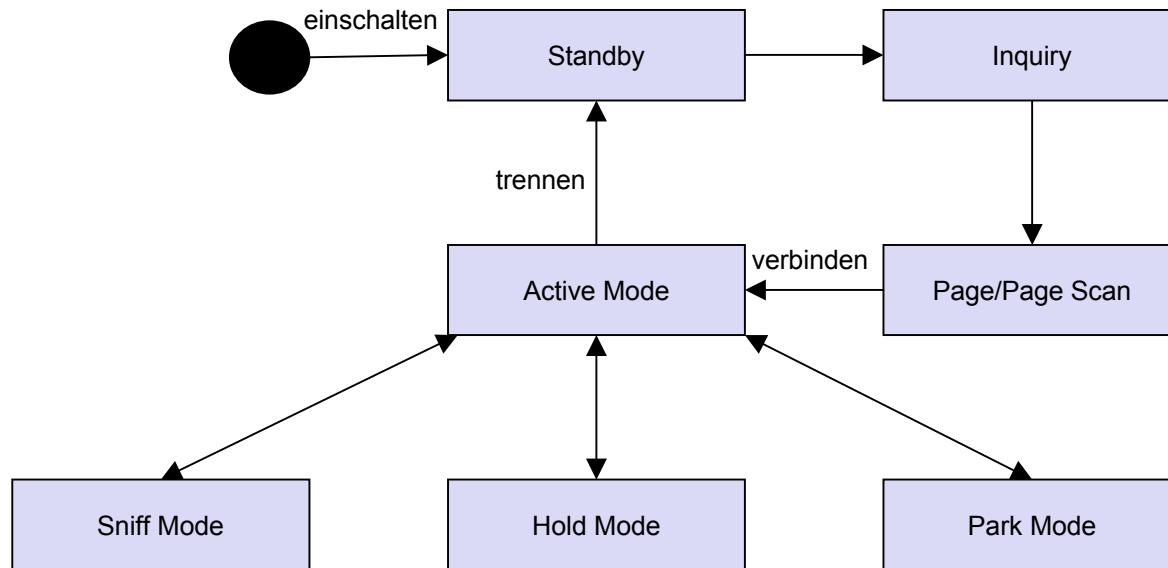
- Synchronisierung der internen Uhr
 - Abgleich der internen Uhr mit der des Masters
 - Berechnung eines Offsets, welcher zu der aktuellen Zeit addiert wird
 - Wichtig, um Anfang eines Slots exakt zu ermitteln
- Verbindungsüberwachung
 - Auf- und Abbau von SCO-Links

- Dienstgüteaushandlung
 - Funktionen, um auf Übertragungsqualität zu reagieren
- Leistungssteuerung
 - Signalstärke des empfangenen Signals messen
 - Sender anweisen, diese evtl. zu korrigieren
- Wechsel zwischen verschiedenen Betriebszuständen

Bluetooth unterscheidet 8 Verbindungszustände

- Standby: Bereitschaftszustand
 - Zustand nach dem einschalten
 - Keine Verbindungen zu anderen Geräten
 - Lediglich innere Uhr weiterbetrieben
 - Geringer Stromverbrauch
- Inquiry: Erkundigungszustand
 - Suche nach anderen Bluetooth-Geräten
 - Abhören des Datenverkehrs

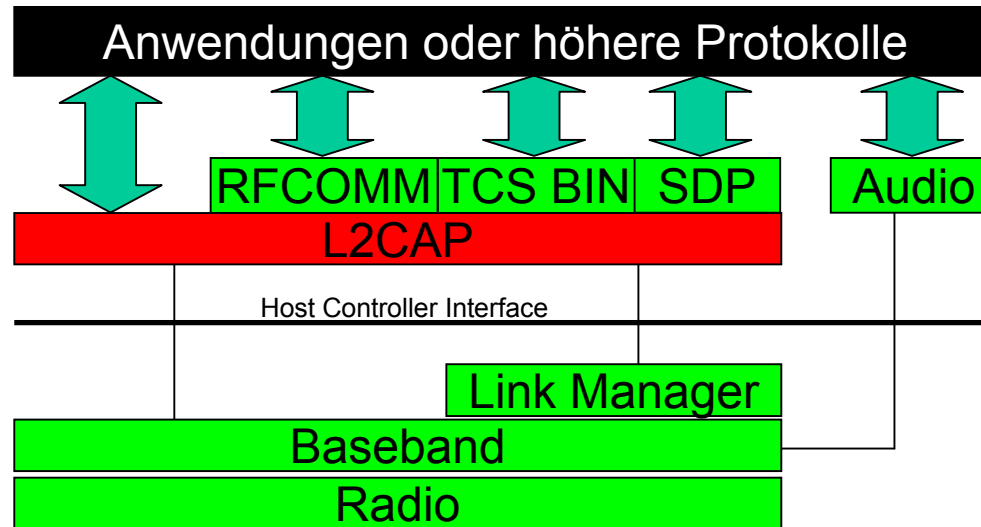
- Page: Ausrufen Zustand
 - Suche nach anderen Geräten war erfolgreich
 - Eigentliche Kontaktaufnahme
- Page Scan:
 - Abhören des Datenverkehrs
 - Wird Paket mit eigener Geräteadresse gefunden, so erfolgt der Kontaktaufbau



Ist das Gerät mit einem Piconetz verbunden, so kann zwischen 4 Verbindungszuständen gewählt werden.

- Active Mode: Gerät ist normal verbunden
 - Ständiges abhören der Datenübertragungen des Masters
 - Senden nach Aufforderung, auch falls keine Daten gesendet werden müssen
- Sniff Mode:
 - Kein wesentliches Kommunikationsaufkommen erwartet
 - Slave wird seltener mit Sendeanforderungen kontaktiert
 - Datenverkehr muss nicht ständig abgehört werden
 - Wenig Gelegenheit, selbst Daten zu senden

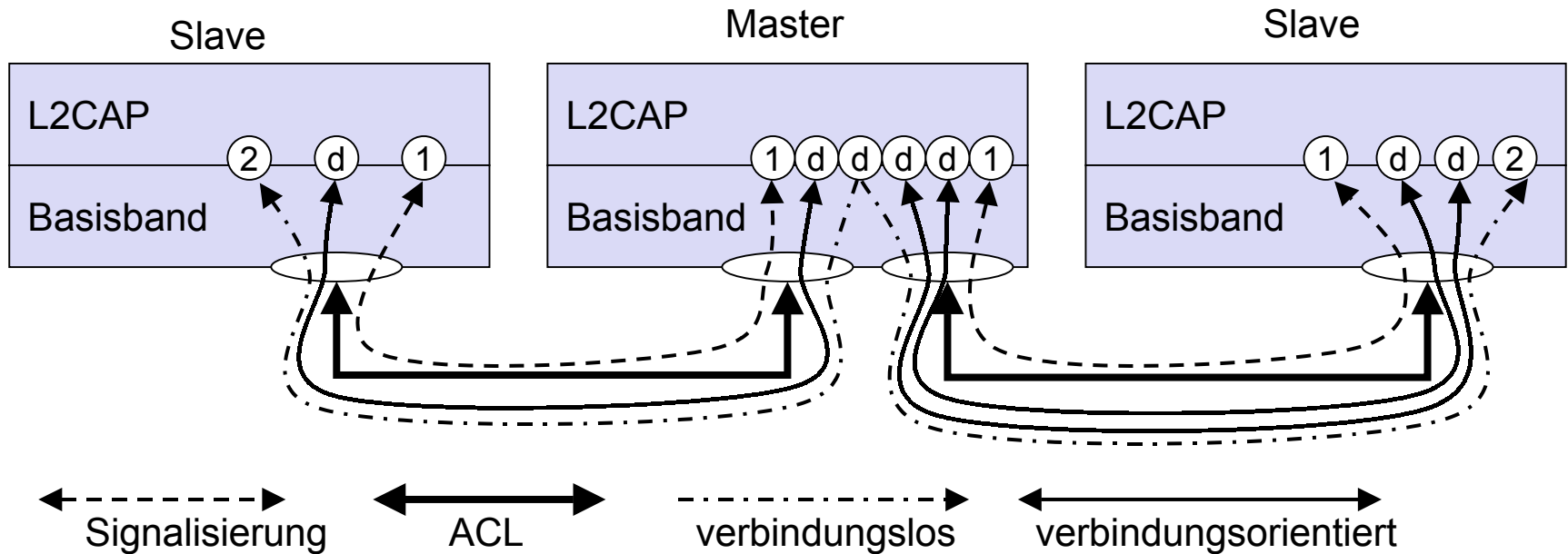
- Hold Mode:
 - Momentan keine Daten zu übertragen
 - Stromverbrauch wird stark reduziert
- Park Mode:
 - Modus mit den wenigsten Aktivitäten
 - Keine aktive Kommunikation
 - Gerät bleibt auf Sprungfolge synchronisiert
 - AMA wird abgegeben, Gerät erhält PMA
 - Umgehen der Grenze von 8 Geräten pro Piconetz



- Wichtigste Funktion: Bereitstellung mehrerer logischer Kanäle über eine bestehende ACL Verbindung zwischen Master und Slave

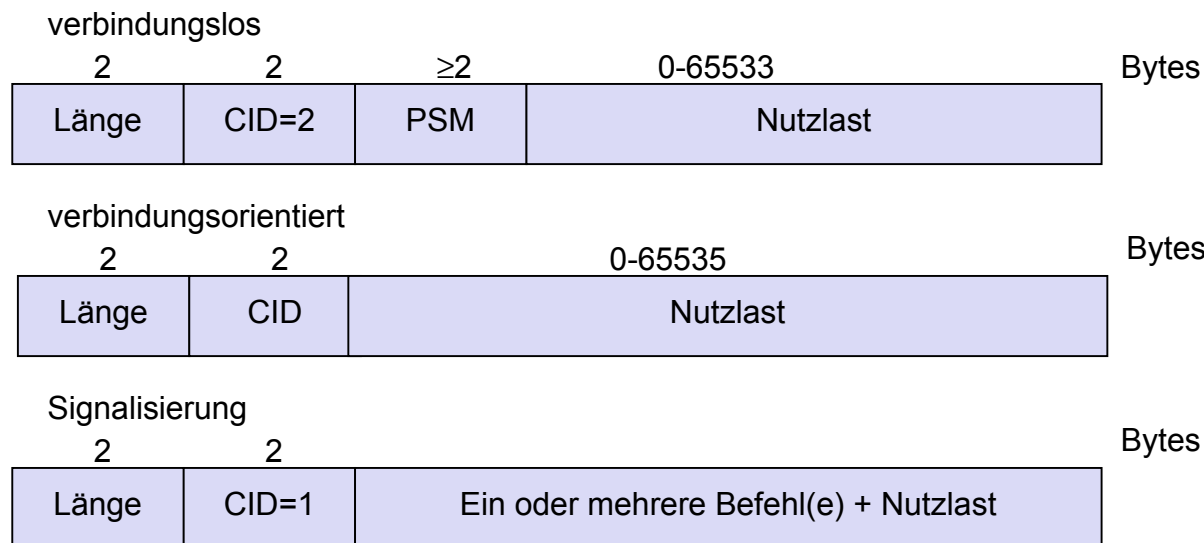
- Signalisierung:
 - zum Einrichten weiterer logischer Kanäle
- Verbindungslos:
 - Unidirektionaler Kanal
 - Typischerweise für Rundrufe verwendet
 - Master kann Kanal für beliebige Slaves einrichten, meist wird ein Kanal jedoch mit allen Slaves im Piconetz verknüpft
- Verbindungsorientiert:
 - Bidirektionaler Kanal zwischen genau 2 Geräten

- Channel Identifier (CID) identifiziert Kanal
- CID-Wert 1 für Signalisierungskanäle
- CID-Wert 2 kennzeichnet verbindungslose Kanäle
- CID-Werte von 3-63 sind reserviert
- CID-Wert für verbindungsorientierte Kanäle frei wählbar (64-65535)



L2CAP-Paketformate

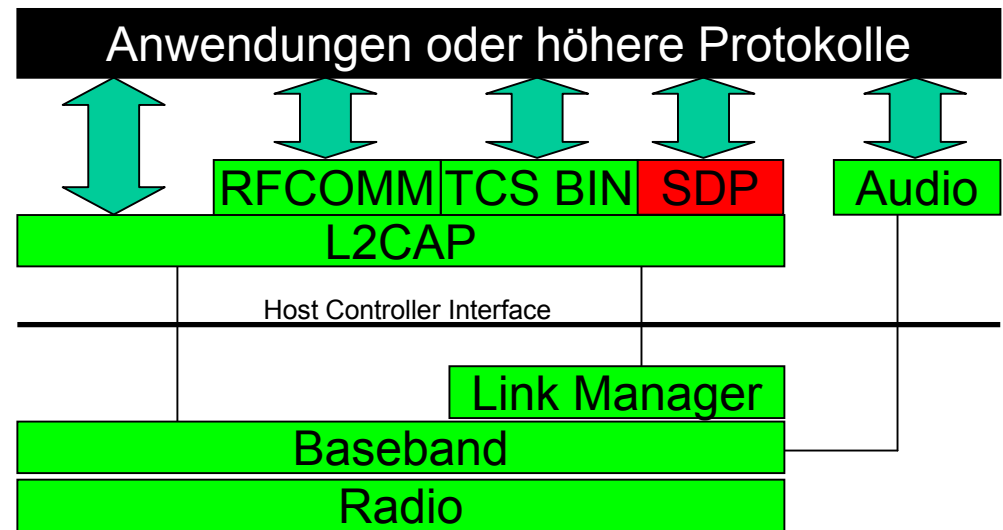
- L2CAP definiert 3 Paketarten (64KByte)
- Feld „Länge“ gibt die Länge der Nutzlast an
- Befehle werden bspw. Für Verbindungsanforderungen benötigt



- Zweite wichtige Funktion: große Pakete für den Transport über Baseband zerlegen
- Teile eines Paketes werden hintereinander gesendet
=> Paket kann auf Empfängerseite komplett rekonstruiert werden, bevor Teile anderer Pakete eintreffen

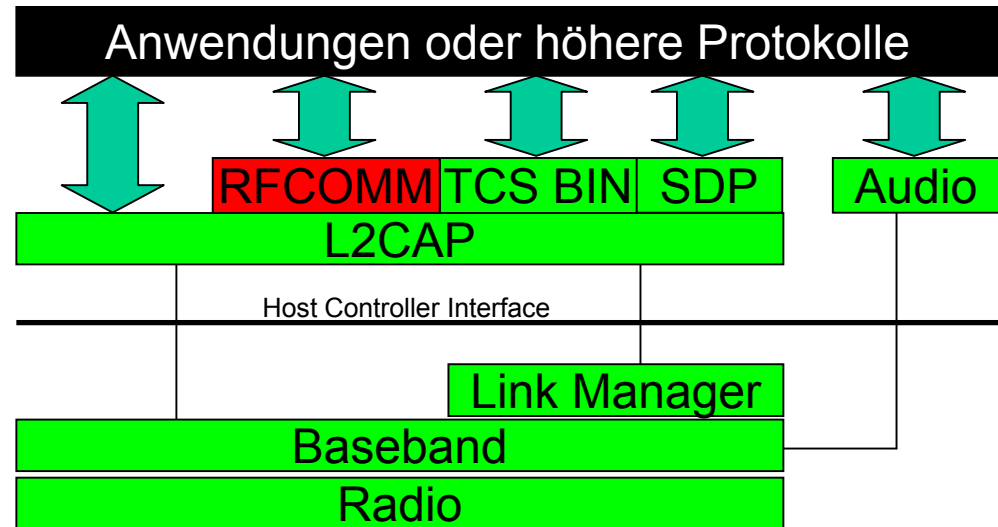
Service Discovery Protocol

- Bluetooth-Geräte sollen spontan untereinander kommunizieren
- Wichtig ist hierbei das Wissen über Geräte in Kommunikationsreichweite, besser gesagt über angebotene Dienste
- SDP wurde zur Suche von Diensten spezifiziert

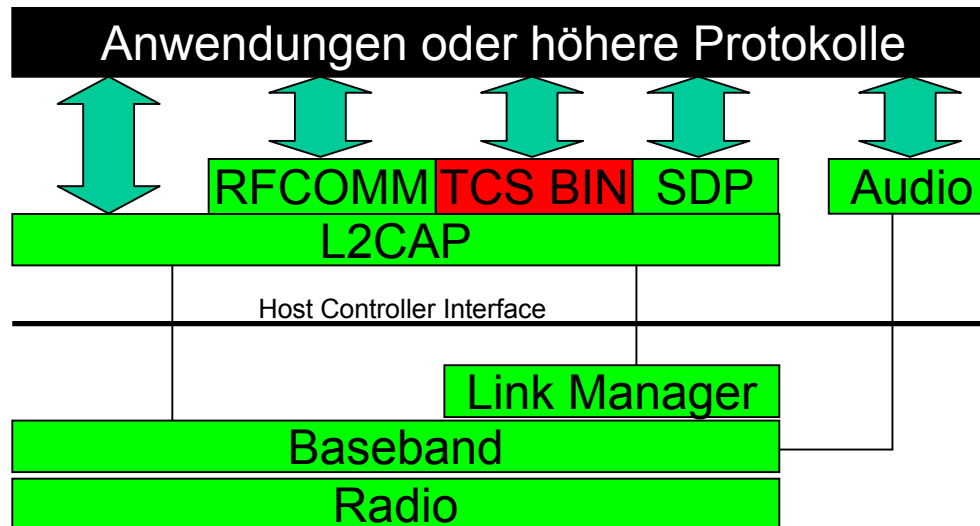


- Dienstanbieter benötigen SDP-Server
- Dienstanutzer installieren einen SDP-Client
- Dienstanutzung ist nicht Bestandteil von SDP
- Keine Zugriffskontrolle: Jedes Gerät kann jeden Dienst nutzen
- Keine Weitervermittlung von Diensten

- emuliert serielle Schnittstellen.
- Kabel für serielle Verbindungen können entfallen
- Bisherige Protokolle weiterhin verwendbar, nun aber über Bluetooth
- Beispiel: Nutzung von TCP und UDP für Internetverbindungen über Bluetooth



- Telephony Control Protocol Specification Binary
- Bit orientiertes Protokoll zur Steuerung von Telefonfunktionen



- Einleitung
- Vernetzung
- Der Bluetooth Protokollstapel
- Sicherheit in Bluetooth-Netzen
 - Schlüsselgenerierung
 - Authentifizierung
 - Verschlüsselung
 - Kritik

- Einfachstes Sicherheitskonzept:
vermindern der Sendeleistung
- Schutz nicht optimal
- Daher: Einführung von Authentifizierung
und Verschlüsselung

Unterschieden werden 3 Sicherheitsmodi:

- Modus 1: keine Sicherheit
 - Falls Verschlüsselung unnötig oder nicht erwünscht
- Modus 2: Sicherheit auf Dienstebene
 - Sicherheitsbedingungen erst nach Verbindungsaufbau eingerichtet
- Modus 3: Sicherheit auf Verbindungsebene
 - Grundsicherheit für jede Art von Kommunikation
 - Sicherheitsbedingungen Für jede Verbindung neu festgelegt

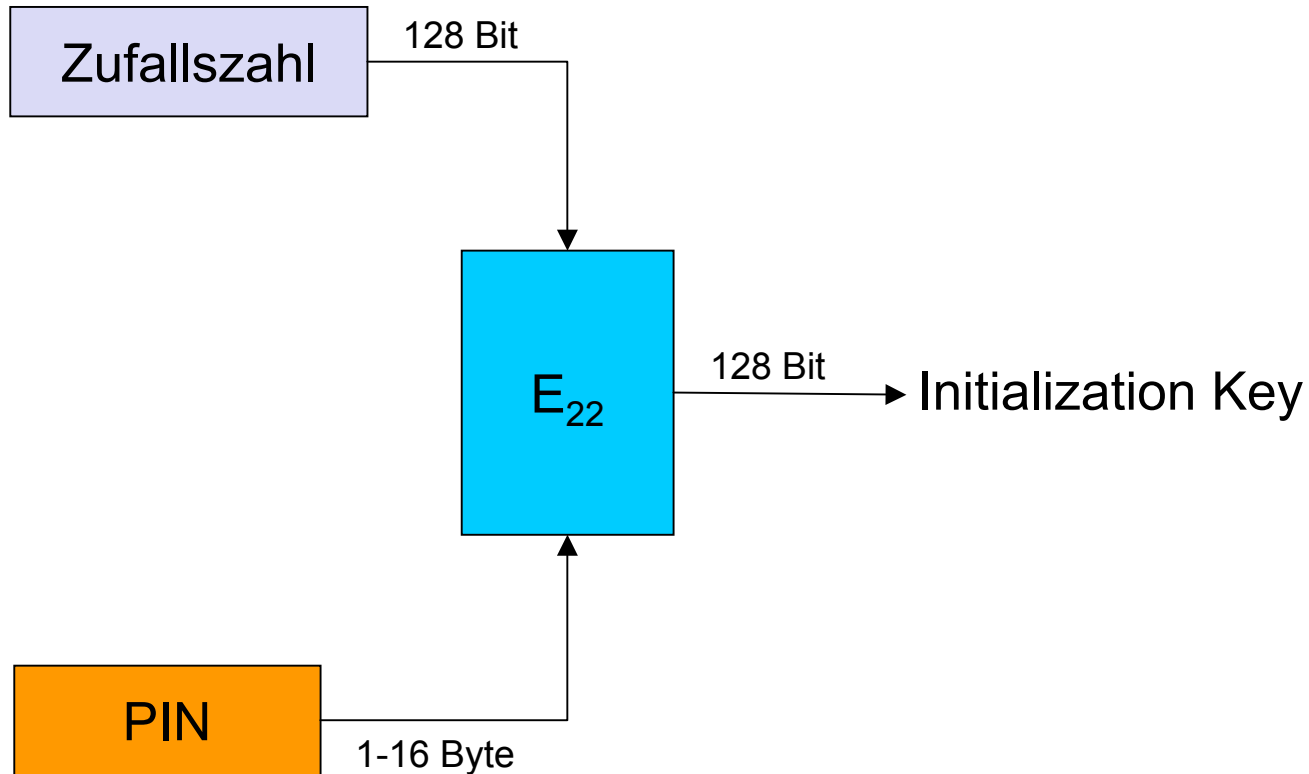
Sicherheitsmodus 3

Bestandteile:

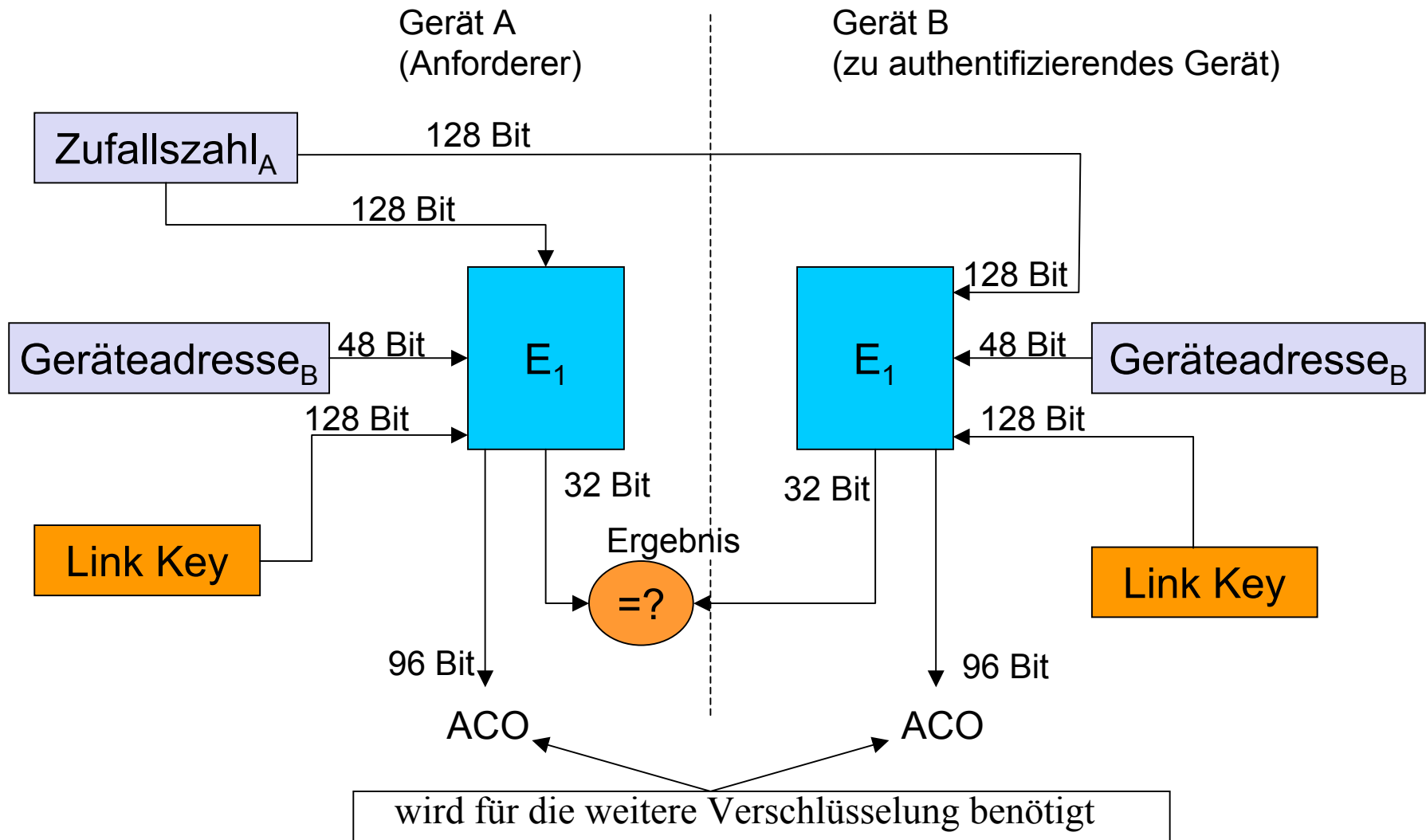
- Kryptografische Funktionen (E0,E1,E21,E22,E3)
- Zufallszahlengenerator (nicht spezifiziert)
 - Implementierung wird Herstellern überlassen
- Geräteadresse: von anderen Geräten erfragbar
- Geheimzahl:benötigt für erstmaligen Verbindungsaufbau zweier Geräte
 - Idealerweise wird sie eingegeben, teils fest im Gerät gespeichert
- Zwei Schlüssel: Encryption Key zur Datenverschlüsselung, wird generiert aus Link Key

- Geräte benötigen Link Key zur gegenseitigen Authentifizierung
- Link Key wird aus Initialization Key erzeugt mit Hilfe der Funktion E21
- Benutzer muss auf beiden Geräten PIN eingeben
- Initialization Key wird aus PIN und Zufallszahl generiert

Schlüsselgenerierung

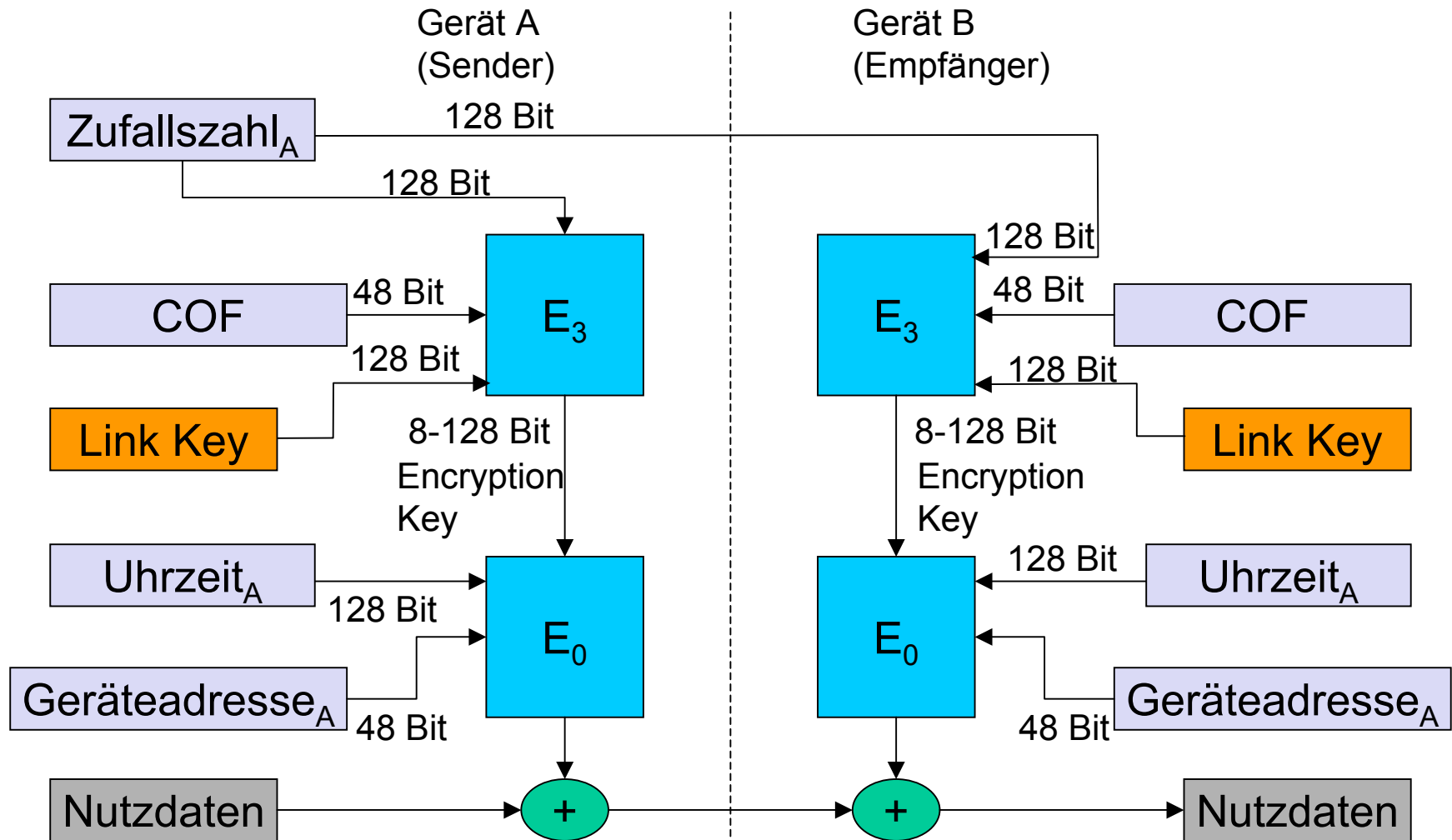


Authentifizierung



- Bildung eines Encryption Key
 - Länge frei wählbar (8 bis 128 Bit)
- Link Key, Zufallszahl und COF (berechnet aus ACO) fließen in die Berechnung des Encryption Key mit ein
- Aus Encryption Key, Uhrzeit und Geräteadresse wird eine Bitfolge erzeugt
- Die Bitfolge wird mit den Nutzdaten XOR verknüpft

Verschlüsselung



- Keine Anforderungen an den Zufallszahlengenerator
 - Bei Vorhersehbarkeit der Ergebnisse ist Schutz vor statistischen Angriffen nicht gewährleistet
- PIN: wird sie in Erfahrung gebracht, so lassen sich die verwendeten Schlüssel rekonstruieren
 - Viele Geräte erlauben nur 4stellige PIN
 - Bei Geräten ohne Eingabemöglichkeit ist die PIN oft mit „0000“ voreingestellt

Hiermit ist jedes weitere Sicherheitskonzept überflüssig

- Ständige Kommunikationsbereitschaft der Bluetooth-Geräte erlaubt Erstellung von Bewegungsprofilen
 - Einige Geräte bieten zur Lösung des Problems einen Non Discoverable Modus an (Gerät reagiert nicht auf Suchanfragen)