

FUNK- UND

TELEKOMMUNIKATIONSSICHERHEIT

**DLBCSEEMT01\_E**

A black background with white text

Description automatically generated with low confidence

# ÜBERGEORDNETE LERNZIELE

Die Zahl der Geräte, die sich drahtlos mit Netzwerken verbinden können, hat bereits heute die Zahl der Desktop- und Laptop-Computer überholt, die über ein Kabel mit einem lokalen Netzwerk verbunden sind. Vor allem Handys und Tablets, die mit drahtlosen Telekommunikationsnetzen verbunden sind, dominieren den Markt. Aber es gibt auch viele andere Formen der drahtlosen Kommunikation, die Geräte nutzen. Die Besonderheiten dieser Funksysteme müssen verstanden werden, um sie in ein umfassendes Sicherheitskonzept integrieren zu können. Funkprotokolle zwingen die Benutzer:innen oft, sich auf ein System zu verlassen, das sie möglicherweise überhaupt nicht verstehen. Dieser Kurs zum Thema **Funk- und Telekommunikationssicherheit** bringt Licht ins Dunkel.

Wir werden uns mit den Grundlagen von Funksignalen bei der Datenübertragung beschäftigen und lernen, die verschiedenen Arten von Funknetzwerken zu erkennen und ihre Unterschiede zu verstehen. Wir behandeln die Terminologie der Telekommunikation und vergleichen sie mit der IT-Terminologie. Dieses Studienskript stellt dar, wie sich die Architekturen der wichtigsten drahtlosen Telekommunikationssysteme analysieren lassen. Wir werden die Bedrohung durch Angriffsvektoren auf Handys und Geräte sowie auf das Kernnetz erläutern. Schließlich besprechen wir noch andere Arten von Netzwerken und wie diese verwendet werden.

**12 PREVIEW-PDF, erzeugt: 2023-05-04T11:56:31.658+02:00**

# LEKTION 1

## FUNKPROTOKOLLE – EIN ÜBERBLICK

###### LERNZIELE

Nach der Bearbeitung dieser Lektion …

* kennen Sie die Unterschiede zwischen den verschiedenen Arten von Funknetzen basierend auf ihrem jeweiligen Abdeckungsbereich.
* können Sie die verschiedenen Normen für Funknetze des Institute of Electrical and Electronics Engineers (IEEE) 802.11 in Bezug auf Wireless Fidelity (Wi-Fi) und seine Entwicklung umreißen.
* sind Sie in der Lage, Weitverkehrsnetzwerkprotokolle und ihre wichtigsten Eigenschaften (Durchsatz, Abdeckung und Skalierbarkeit) zu analysieren.
* können Sie die wichtigsten Konzepte der Kryptografie anwenden und die Sicherheit von Wi-Fi analysieren.

### 1. FUNKPROTOKOLLE – EIN ÜBERBLICK

#### Einführung

Wenn Sie dieses Studienskript online auf Ihrem PC oder Laptop lesen, nutzen Sie wahrscheinlich eine drahtlose Verbindung – und somit eine Funkverbindung–, um die Informationen abzurufen. In diesem Fall nutzen Sie die Norm IEEE 802.11 (Institute of Electrical and Electronics Engineers), allgemein bekannt als Wi-Fi, um sich per WLAN mit Ihrem Router und über diesen schließlich mit dem Internet zu verbinden. Bevor Sie sich auf den Kurs vorbereitet haben, haben Sie sich vielleicht mit Ihrem Handy in sozialen Netzwerken umgesehen, und Ihr Handy war möglicherweise auch drahtlos mit dem Internet verbunden, allerdings über einen anderen drahtlosen Kommunikationsstandard: das Mobilfunknetz.

Die Funkkommunikation hat sich für zahlreiche Anwendungen und Szenarien zur wichtigsten Art der Konnektivität entwickelt. Sie spielt eine entscheidende Rolle bei der Kommunikation zwischen Menschen, Geräten, Sensoren und Aktoren. Anhand ihrer Reichweite (d. h. der Entfernung, über die zwei Geräte miteinander kommunizieren können) können Funknetze in drei Hauptgruppen eingeteilt werden:

1. Wireless Personal Area Networks (WPAN) mit einer Reichweite von bis zu mehreren Metern
2. Wireless Local Area Networks (WLAN) mit einer Reichweite von mehreren Metern bis zu mehreren 100 Metern
3. Wide Area Networks (WAN) mit Reichweiten von mehreren Kilometern

Während Wireless Personal Area Networks (WPANs) für die Kommunikation zwischen Geräten verwendet werden, die wir direkt bei uns tragen (z. B. Bluetooth-Headsets, NFC-Uhren), werden Wireless Local Area Networks und Wide Area Networks für die Kommunikation zwischen Mensch und Maschine eingesetzt (z. B. Wi-Fi für die Kommunikation zwischen Computern, Mobiltelefone für die Kommunikation zwischen Menschen und Satellitennetze für die Kommunikation in abgelegenen Gebieten). In den folgenden Unterabschnitten werden die wichtigsten Funkprotokolle und ihre Eigenschaften für jede Art von Funknetz vorgestellt.

#### WPAN-Protokolle (Bluetooth, RFID, NFC und mehr)

WPANs (Wireless Personal Area Networks) werden für die Kommunikation über kurze Entfernungen verwendet. Die Hauptmerkmale dieser Technologien sind der Betrieb in ISM-Frequenzbändern (ISM: Industrial, Scientific and Medical; Industrie, Wissenschaft, Medizin), niedrige Kosten (< 2 €/Chip), Datenraten von einigen hundert Kilobyte pro Sekunde (KBps) bis zu mehreren Megabyte pro Sekunde (MBps) und ein niedriger Stromverbrauch zur Verlängerung der Lebensdauer. Diese Technologien werden hauptsächlich für die Kommunikation mit niedriger Datenrate und über kurze Entfernungen eingesetzt, z. B. für drahtlose Lautsprecher, drahtlose Headsets, die Kommunikation bei Kartenzahlungen oder auch für die Steuerung von LED-Leuchten. Einige der hier diskutierten Technologien sind Bluetooth, IEEE 802.15.4, Near Field Communication (NFC) und RFID.

##### Bluetooth

Die Bluetooth-Funktechnologie wurde 1994 von Ericsson als Kurzstreckentechnologie entwickelt, um die kabelgebundene Kommunikation für Sprache und Daten zu ersetzen. Später, im Jahr 1998, wurde die Bluetooth Special Interest Group (BT SIG) gegründet, der IBM, Nokia, Intel und Ericsson angehören, um offene Spezifikationen für die drahtlose Kommunikation im Nahbereich zu standardisieren (Tanenbaum, 2021). Die erste Version von BT wurde 1999 veröffentlicht und verwendete 79 Kanäle mit einer Breite von 1 MHz und Channel Hopping. Im Jahr 2004 wurde die neue Version von Bluetooth, BT 2.0, veröffentlicht, die höhere Datenraten von bis zu 3 Mbps bietet und den EDR-Mechanismus (EDR: Enhanced Data Rate) verwendet. Seitdem ist die Steigerung des Datendurchsatzes die Haupttriebfeder für die Weiterentwicklung von BT. Im Jahr 2009 wurde die Version BT 3.0 und im Jahr 2010 die Version BT 4.0, die als Bluetooth Low Energy (BLE) bekannt ist, veröffentlicht. BLE standardisiert den völlig neuen Protokollstapel von der Bitübertragungsschicht bis zur Anwendungsschicht und strebt einen sehr geringen Stromverbrauch an, bei dem die Funkeinheit mit Knopfzellen betrieben wird.

Bluetooth wird im 2,4 GHz-Band zwischen 2400 und 2483,5 MHz mit einem Kanalabstand von 1 MHz betrieben. Die Mittenfrequenz des ersten Kanals liegt bei 2402 MHz und die des letzten bei 2480 MHz. Bluetooth hat insgesamt 79 Kanäle. BLE, die neueste Version von Bluetooth, verwendet die gleichen Frequenzen, aber mit einem Kanalabstand von 2 MHz, was zu 40 nutzbaren Kanälen führt. Von diesen 40 Kanälen werden drei (37, 38 und 39) als primäre Advertising-Kanäle (*advertising* im Sinne von *Aufmerksamkeit*) verwendet, während 37 andere Kanäle für die verbindungsorientierte Kommunikation genutzt werden, wie in der Abbildung unten zu sehen ist. Die Advertising-Kanäle werden so ausgewählt, dass sie die Wi-Fi-Kommunikation nicht stören, da sie sich zwischen den Wi-Fi-Kanälen befinden.

Abbildung 1: BLE-Kanäle und ihre Frequenzen

A picture containing text, screenshot, number

Description automatically generated

Quelle: Jetmir Haxhibeqiri (2023).

BLE verwendet zwei verschiedene Betriebsarten zwischen Geräten: den Advertising-Modus (etwa: Aufmerksamkeitsmodus) und den verbindungsorientierten Modus, wie in der Abbildung „BL- Betriebsarten: Der Advertising-Modus und der verbindungsorientierte Modus“ dargestellt. Im Advertising-Modus senden ein oder mehrere Geräte regelmäßig in bestimmten Intervallen Informationen auf drei Advertising-Kanälen. Diese Geräte übernehmen die Advertiser-Rolle. Andere Geräte scannen die drei Advertising-Kanäle, einen nach dem anderen, in unterschiedlichen Intervallen für ein bestimmtes Scanfenster, um die Advertising-Informationen zu erfassen. Diese Geräte übernehmen die Scanner- oder Beobachter-Rolle. Das Advertising-Intervall und das Scan-Intervall müssen nicht identisch sein. Im Gegensatz zu Bluetooth Low Energy (BLE) unterstützt Bluetooth nur Punkt-zu-Punkt-Netzwerktopologien, während BLE Punkt-zu-Punkt-, Broadcast- und Mesh-Topologien unterstützt.

Abbildung 2: BLE-Betriebsarten: Der Advertising-Modus und der verbindungsorientierte Modus

A picture containing circle, screenshot, diagram

Description automatically generated

Quelle: Jetmir Haxhibeqiri (2023).

Im verbindungsorientierten Modus wird ein Gerät als Master (zentrales Gerät) ausgewählt, das dann die Verbindungen mehrerer Peripheriegeräte verwaltet. Das zentrale Gerät verwaltet und synchronisiert die Peripheriegeräte, und jede Verbindung verwendet ein Frequenzsprungverfahren, um Robustheit zu gewährleisten. Mittels Time Division Multiple Access (TDMA) werden verschiedene Verbindungen zu unterschiedlichen Zeiten organisiert.

##### IEEE 802.15.4

In vielen Sensornetzwerken, die zur Steuerung und Überwachung eingesetzt werden, ist die Lebensdauer der batteriebetriebenen Geräte eine der Hauptbeschränkungen für den Netzwerkeinsatz. Die Datenrate, die bei diesen Anwendungen verwendet wird, ist gering. Es werden nur wenige Pakete pro Stunde gesendet. Weitere Merkmale, die berücksichtigt werden müssen, sind die Komplexität der Endgeräte, die Kosten pro Endgerät, der Stromverbrauch und die Selbstheilung sowie Mesh-Netzwerke.

Als Alternative zu IEEE 802.11 wurde 2003 IEEE 802.15.4 eingeführt, um Mesh-Sensornetzwerke mit geringerer Komplexität, niedrigeren Kosten und geringerem Stromverbrauch zu ermöglichen. IEEE 802.15.4 definiert nur den Standard für die Bitübertragungs- und MAC-Schicht (MAC: Media Access Control) für die Realisierung von drahtlosen Sensor- und Aktornetzwerken (WSAN: Wireless Sensor and Actuator Networks). Es bildet die Grundlage für verschiedene andere Netzwerkstacks, die oberhalb der IEEE 802.15.4 MAC-Schicht definiert sind, z. B. Zigbee, WirelessHRT und ISA 100.11a. Es spezifiziert zwei verschiedene Bitübertragungsschichten: eine, die im 2,4-GHz-Band unter Verwendung von Direct Sequence Spread Spectrum (DSS) mit einer erreichbaren Datenrate von 250 kbit/s arbeitet, und eine, die im 868/915-MHz-Band mit wesentlich niedrigeren Datenraten von 40 kbit/s bzw. 20 kbit/s arbeitet (Adams, 2006). Im 2,4-GHz-Band werden 16 Kanäle mit einer Breite von 2 MHz und einem Abstand von 5 MHz für die Kommunikation verwendet, von denen die ersten 15 weltweit verfügbar sind, wie in der Abbildung „IEEE 802.15.4 Kanalverwendung“ dargestellt.

Abbildung 3: IEEE 802.15.4 Kanalverwendung

A picture containing text, screenshot, font, line

Description automatically generated

Quelle: Jetmir Haxhibeqiri (2023).

Für den Zugriff auf das Übertragungsmedium sind zwei Mechanismen vorgesehen. Für den Betrieb ohne Beacon wird das CSMA/CA-Verfahren (Carrier Sense Multiple Access with Collision Avoidance) verwendet. Beim Beacon-basierten Medienzugriff sendet der Netzwerkkoordinator in regelmäßigen Abständen Beacons, die den Kommunikations-Superframe definieren. Der Kommunikations-Superframe ist weiter unterteilt in die Contention-Access-Periode (in der die Knoten das CSMA/CA-Verfahren für den Zugriff auf das Medium verwenden) und die Contention-Free-Access-Periode, in der bestimmten Knoten bestimmte Guaranteed Time Slots (GTS) zugewiesen werden. Hinsichtlich der Netzwerktopologien können Peer-to-Peer-Kommunikation und sternförmige Kommunikationstopologien unterstützt werden. Bei der Peer-to-Peer-Kommunikation wird eine Ad-hoc-Kommunikation zwischen zwei Kommunikationsgeräten aufgebaut, während bei der Sterntopologie ein PAN-Koordinator den Kanalzugriff für andere Knoten koordiniert, die Beacons aussenden.

##### RFID- und NFC-Technologie

Die RFID-Technologie (Radio Frequency ID) wird heute für die Zugangsverwaltung und die Verfolgung von Waren, Personen, Tieren usw. eingesetzt. Sie nutzt Funkfrequenzen, um Transponder (sogenannte *Tags*) auch ohne Sichtverbindung zu identifizieren. Das RFID-Konzept ist simpel und besteht aus einem RFID-Lesegerät, das den Funkimpuls zum Abfragen der Tags erzeugt, und einem RFID-Tag, das mit digitalen Daten antwortet, die die Tag-ID kodieren.

RFID-Systeme verwenden verschiedene Frequenzbänder, die die Reichweite der Kommunikation bestimmen, z. B. 433 MHz: Reichweite 1-100 m, ISM-Bänder 2,4 und 5 GHz: Reichweite 1-2 m. Basierend auf den Arten von Tags und Lesegeräten können die RFID-Systeme in die folgenden Systeme unterteilt werden (Want, 2006):

* passives Lesegerät und aktives Tag: Das Tag sendet, während das Lesegerät nur empfängt.
* aktives Lesegerät und passives Tag: Das Lesegerät kann das Tag abfragen und empfängt die Identifikation vom Tag selbst.
* aktives Lesegerät und aktives Tag: Das Lesegerät kann das aktive Tag abfragen, indem es dieses mit Funksignalen aktiviert.

Ähnlich wie bei der RFID-Technologie werden bei der Near Field Communication (NFC) elektromagnetische Wellen zur Datenübertragung und zur Stromversorgung passiver Tags verwendet. Die Lesereichweite von NFC ist mit bis zu 10 cm deutlich geringer als die von RFID und funktioniert nur bei Sichtkontakt (Thanpal, 2017). Die Datenraten reichen von 106 kbps bis 424 kbps.