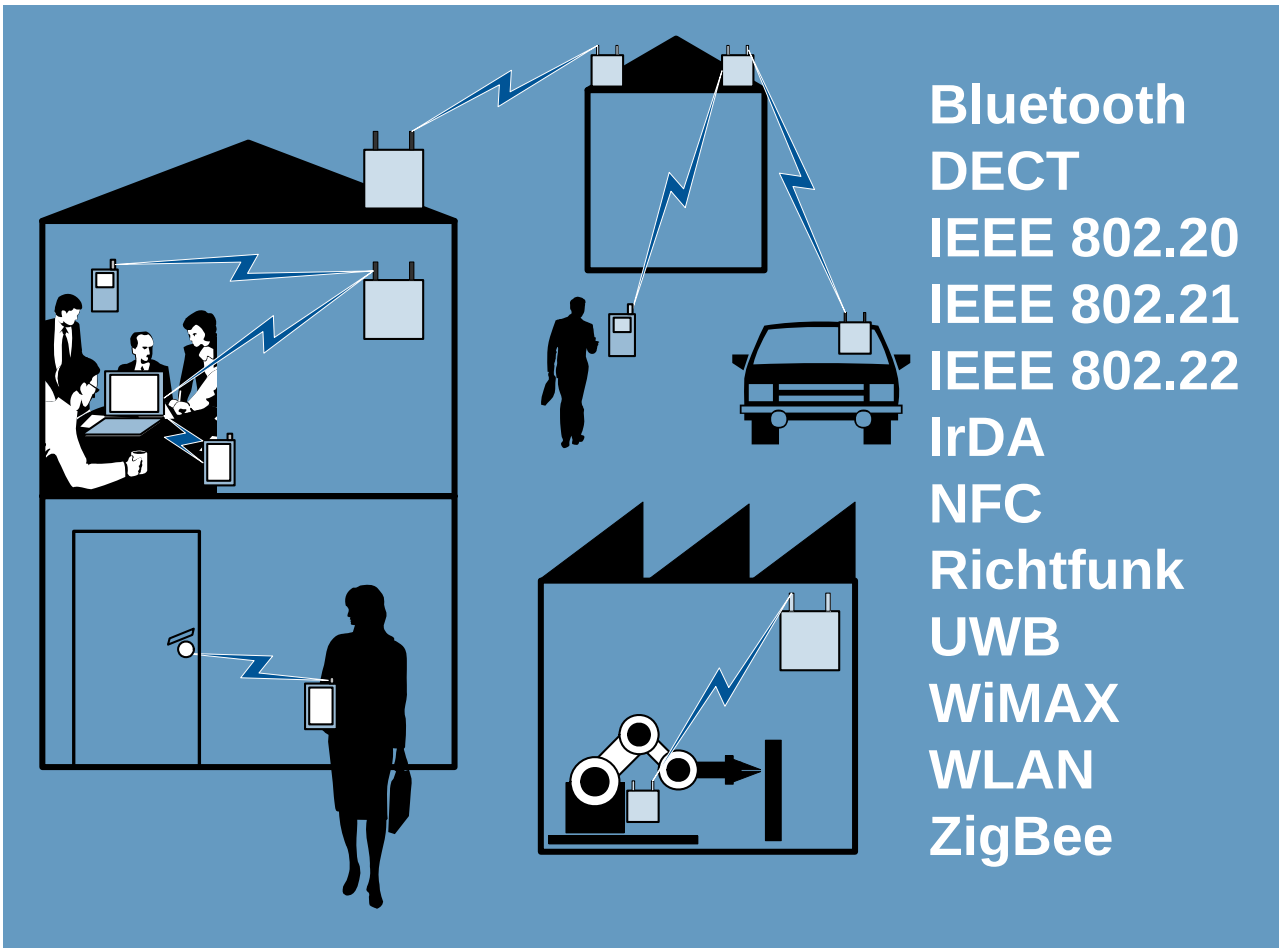
Bundesamt für Sicherheit in der Informationstechnik

Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte



Bundesamt für Sicherheit in der Informationstechnik

Diese Broschüre soll die Funktionsweise von drahtlosen Kommunikationssystemen darstellen, mögliche Gefährdungen der Informationssicherheit bei Nutzung dieser Systeme beschreiben sowie geeignete Schutzmaßnahmen aufzeigen. Das Dokument reflektiert den Stand der Technik bis Mai 2006.

An der Erstellung waren folgende Mitarbeiter des BSI beteiligt: Heinz Gerwing, Dr. Wilhelm Pütz, Guido Reckhaus, Berthold Ternes. Weiterhin haben folgende Mitarbeiter der ComConsult Beratung und Planung mitgewirkt: Oliver Flüs, Dr. Simon Hoff, Hartmut Kell, Dr. Jochen Wetzlar.

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 (0) 1888 95820
E-Mail: lwc@bsi.bund.de
Internet: http://www.bsi.bund.de

Gliederung des Dokumentes

A. Wireless LAN, IEEE 802.11

B. Bluetooth

C. DECT

D. WiMAX, IEEE 802.16

E. Richtfunktechniken

F. ZigBee, IEEE 802.15.4

G. IrDA

H. Drahtlose Tastaturen, Mäuse und andere Eingabegeräte

I. UWB

J. Neuere Entwicklungen

Einleitung

Drahtlose Kommunikationssysteme finden bei zunehmender Produktvielfalt eine immer größere Verbreitung. Die Funkanbindung von stationären wie mobilen Endgeräten an das Telefonnetz, das Internet oder das lokale Netz in einem Unternehmen oder einer Behörde bietet neue Freiheiten bei der Nutzung der Netze und deren Dienste. Drahtlose Netze können ein effizienter Ersatz sein für ein aufwändiges Verlegen von Kabeln; Ad-hoc-Vernetzung per Funk ermöglicht den spontanen und mobilen Datenaustausch. Kabellose Eingabegeräte erhöhen den Bedienkomfort der IT-Systeme. Mit heute verfügbarer drahtloser Technik sind viele Mobilitätsansprüche der Nutzer von IT-Technik realisierbar.

Die wichtigsten technischen Systeme hierzu sind zurzeit:

- Wireless LANs nach den Standards der Serie IEEE 802.11 als Ergänzung der kabelbasierten lokalen Netze (Local Area Networks, LANs)
- Bluetooth zur Übertragung von Sprache und Daten in der unmittelbaren persönlichen Umgebung
- Sprach- und Datenkommunikationssysteme nach dem DECT-Standard (Digital Enhanced Cordless Telecommunications)
- WiMAX (Worldwide Interoperability for Microwave Access) zur Anbindung von Feststationen und für mobile Endgeräte,
- Richtfunk-Techniken zur drahtlosen Überbrückung größerer Entfernungen zwischen Gebäuden
- ZigBee, basierend auf IEEE 802.15.4, für Sensor- und Steuernetzwerke
- Infrarot-Module nach IrDA zur Kommunikation mit Peripheriegeräten
- Drahtlose Tastaturen, Mäuse und andere Eingabegeräte
- UWB (Ultra-wideband) zur Anbindung von Peripheriegeräten mit hohen Datenraten

Außerdem zeichnen sich bereits künftige Entwicklungen ab, die beispielsweise eine mobile Breitbandkommunikation mit Fahrzeugen gestatten (Mobile Broadband Wireless Access, MBWA) oder über eine Kommunikation im unmittelbaren Nahbereich z.B. drahtlose Bezahlsysteme ermöglichen.

Alle diese Systeme bieten einen Gewinn an Komfort und Mobilität, jedoch birgt die Nutzung der drahtlosen Technik auch zusätzliches Gefährdungspotential für die Sicherheit der Informationen. Diese Gefährdungen sind bedingt durch die spezielle drahtlose Kommunikationstechnik, durch Schwächen der zugrunde liegenden Protokolle sowie durch falsche Konfiguration und Benutzung der Systemkomponenten.

Drahtlos heißt, dass Informationen mittels elektromagnetischer Wellen wie Funk oder Infrarot-Licht zwischen den Kommunikationspartnern übertragen werden. Hier fehlt also der physikalische Schutz des Mediums, den eine Leitung – sei es Kabel, Draht oder Lichtwellenleiter – bietet. Dies führt praktisch bei allen drahtlosen Kommunikationssystemen zu typischen Problemen:

Interferenzen und stark schwankende Kanalbedingungen können bis zum Verlust der Verfügbarkeit der Kommunikationsfähigkeit des Systems führen. Darüber hinaus können die ausgesendeten elektromagnetischen Wellen aber auch von Dritten empfangen, aufgezeichnet, ausgewertet und ggf. manipuliert werden. Mit Hilfe von leistungsfähiger Empfangstechnik, z.B. mit Richtantennen oder empfindlichen Empfängermodulen sind der Empfang und die Aufzeichnung der Informationen auch weit über die normale Nutzreichweite der funkbasierten Kommunikationssysteme möglich.

Damit die übertragenen Informationen vertraulich bleiben, sind sichere Verschlüsselungsverfahren notwendig, starke Authentisierungsverfahren sollen dem nicht autorisierten Dritten den Zutritt zum drahtlosen Kommunikationssystem verwehren, und Integritätsschutzmechanismen sollen dafür Sorge tragen, dass ausgesendete Informationen unverfälscht den Empfänger erreichen.

Im Folgenden werden in separaten autarken Kapiteln die wichtigsten drahtlosen Kommunikationssysteme dargestellt, mögliche Gefährdungen der Informationssicherheit bei Nutzung dieser Systeme beschrieben und ggf. geeignete Schutzmaßnahmen aufgeführt. Diese Informationsschrift möchte Administratoren, Sicherheitsbeauftragten und Endbenutzern drahtloser Kommunikationssysteme eine Hilfestellung zur Bewertung und sicheren Nutzung dieser Systeme bieten.

A. Wireless LAN, IEEE 802.11

Inhaltsverzeichnis des Abschnitts

1. Grundlagen und Funktionalität

Wireless LANs (WLANs, manchmal auch als Funk-LAN bezeichnet), die auf dem 1997 vom Institute of Electrical and Electronics Engineers (IEEE) definierten Standard IEEE 802.11 basieren, findet man mittlerweile als drahtlose Erweiterung eines traditionellen LAN (Local Area Network) sowohl in den Bereichen Büro, Produktion, Logistik und Medizin als auch zunehmend im privaten Bereich. Sie erlauben den immer wichtiger werdenden mobilen Zugang zu allen benötigten Informationen unabhängig vom aktuellen Aufenthaltsort.

Aufgrund der einfachen Installation werden WLANs auch für temporär zu installierende Netze (z.B. auf Messen) verwendet. Darüber hinaus besteht die Möglichkeit, an öffentlichen Plätzen wie Flughäfen oder Bahnhöfen Netzwerkzugänge, so genannte Hot Spots anzubieten, um den mobilen Benutzern Verbindungen in das Internet und hierüber z.B. per Virtual Private Network (VPN) einen Zugriff auf die heimatliche IT-Infrastruktur zu ermöglichen.

Die Kommunikation erfolgt bei WLANs über Funk, was aufgrund der damit verbundenen Eigenschaft eines Shared Medium immer die Gefahr der Abhörbarkeit, die Möglichkeit des unerlaubten Zugangs zum WLAN und die mögliche Störbarkeit von Übertragungen (beabsichtigt oder nicht) birgt.

Bereits Mitte 2001 sind massive Sicherheitslücken im Standard IEEE 802.11 bekannt geworden, die zu großen Sicherheitsproblemen führen können. Die ursprünglich spezifizierten kryptographischen Mechanismen sind unzulänglich: der verwendete Verschlüsselungsalgorithmus kann in kürzester Zeit gebrochen werden. Der Zugang zu fremden WLANs wird außerdem noch durch frei verfügbare Werkzeugen erleichtert. Mittlerweile gibt es von der IEEE allerdings mit IEEE 802.11i eine Erweiterung des Standards, die deutlich verbesserte Sicherheitsmaßnahmen spezifiziert.

Bis heute basieren praktisch alle am Markt verfügbaren WLAN-Systeme auf dem genannten Standard IEEE 802.11 und seinen Ergänzungen, die im Folgenden kurz vorgestellt werden[1]. Eine besondere Rolle nimmt dabei die Hersteller-Vereinigung Wi-Fi Alliance ein, die basierend auf IEEE 802.11 mit Wi-Fi einen Industriestandard geschaffen hat. Dabei bestätigt die Wi-Fi Alliance mit dem Wi-Fi-Gütesiegel, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat (z.B. Wi-Fi Protected Access, WPA).

1.1 Architekturen

WLANs können in zwei verschiedenen Architekturen betrieben werden.

Im Ad-hoc-Modus kommunizieren zwei oder mehr mobile Endgeräte (Clients), die mit einer WLAN-Karte ausgestattet sind, direkt miteinander. WLANs im Ad-hoc-Modus sind in der Praxis eher selten.

---

[1] Neben dem Standard IEEE 802.11 gibt es noch andere WLAN-Standards, die jedoch keine praktische Relevanz mehr haben, da keine Produkte am Markt verfügbar sind. Zu nennen sind hier HomeRF und HIPERLAN/2.

HomeRF (Home Radio Frequency) wurde 1999 für die drahtlose Vernetzung in privaten Haushalten zur Unterstützung für Daten- und Sprachdienste konzipiert und durch die HomeRF Working Group als Industriestandard veröffentlicht. Januar 2003 hat die HomeRF Working Group jedoch ihre Arbeit eingestellt und seitdem hat die Bedeutung von HomeRF rapide abgenommen.

HiperLAN/2 (High Performance Radio Local Area Network Type 2) wurde im Jahr 2000 als europäischer Standard für Funk-LANs von dem European Telecommunications Standards Institute (ETSI) spezifiziert. Erwähnenswert ist, dass Konzepte für Quality of Service (QoS) in HiperLAN/2 von Beginn an Bestandteil des Standards waren und nicht wie in IEEE 802.11 später mühevoll als Ergänzung aufgenommen wurden. In Prototypen konnte HiperLAN/2 zwar eine sehr gute Leistung demonstrieren, bislang sind aber keine Produkte am Markt verfügbar.

Detailliertere Beschreibungen beider Systeme können der ersten Auflage dieser Schrift entnommen werden, die auf der Web-Seite des BSI noch zum Download zur Verfügung steht.

Der größte Teil der WLAN-Installationen wird im Infrastruktur-Modus betrieben. Hier erfolgt die Kommunikation der Clients über eine zentrale Funkbrücke, den so genannten Access Point, über den auch die Anbindung an das kabelgebundene LAN erfolgt (siehe Abb. A-1).

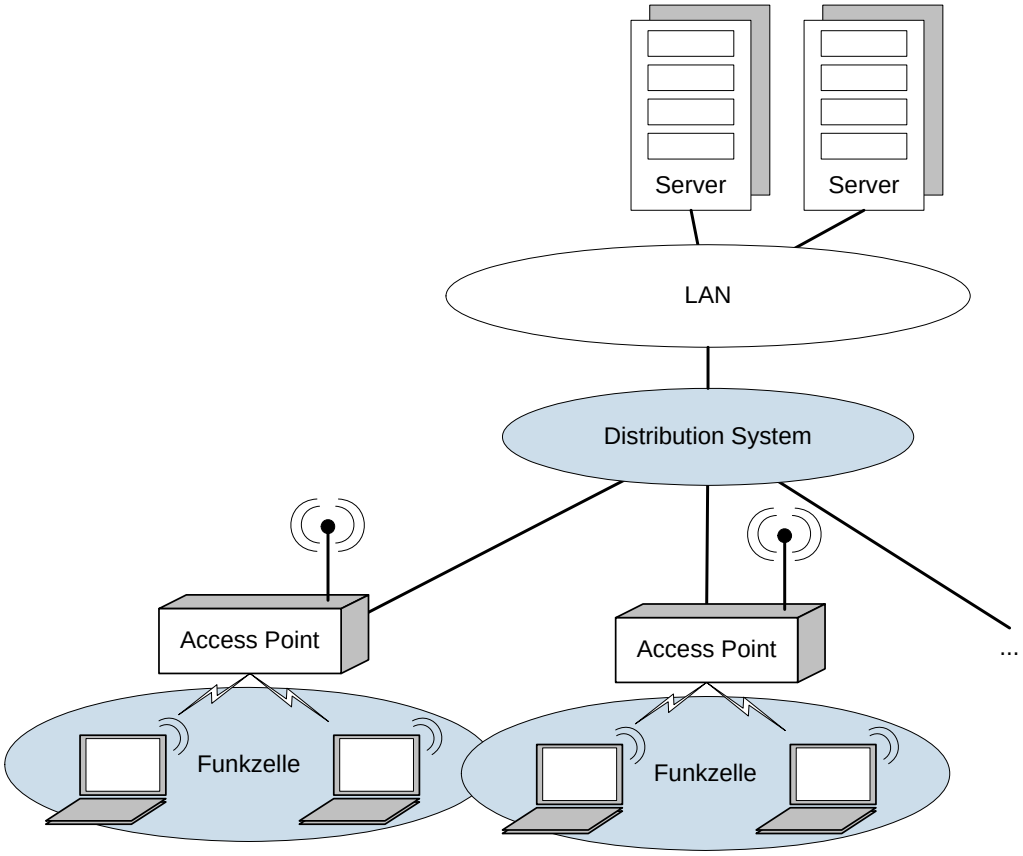


Abb. A-1: Infrastruktur-Modus- Erweiterung kabelbasierter LANs

Bei der Verwendung entsprechender Komponenten (Richtantennen) an den Access Points, die dann oft als Wireless Bridge bezeichnet werden, kann ein WLAN auch zur Kopplung kabelbasierter LAN-Segmente wie eine Richtfunkstrecke eingesetzt werden (siehe Abb. A-2).

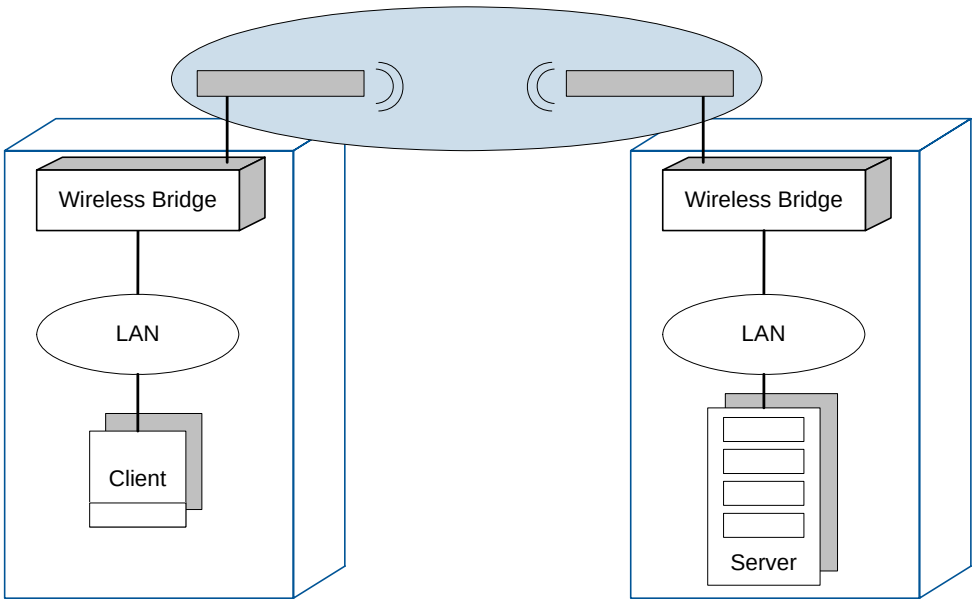


Abb. A-2: Infrastruktur-Modus - LAN-Kopplung

Der Standard verwendet die Bezeichnungen Independent Basic Service Set (IBSS) für Funk-Netzwerke im Ad-hoc-Modus und Basic Service Set (BSS) für Konstellationen im Infrastruktur-Modus mit einem Access Point. Mehrere gekoppelte BSS werden als Extended Service Set (ESS) bezeichnet, das koppelnde Netzwerk wird Distribution System (DS) genannt.

Es kann durchaus vorkommen, dass an einem Ort WLANs unterschiedlicher Betreiber empfangen werden können. Zur Identifikation wird für ein WLAN daher ein Name vergeben, der so genannte Service Set Identifier (SSID).

1.2 Funkschnittstelle

In IEEE 802.11 (siehe [IEEE99]) und seinen Erweiterungen werden sechs Varianten zur physikalischen Übertragung und ein gemeinsames Verfahren für den Kanalzugriff spezifiziert.

- Systeme des 1997 veröffentlichten Standards IEEE 802.11 übertragen die Daten mit einer Rate von 1 MBit/s oder 2 MBit/s mittels Bandspreizverfahren: entweder Frequency Hopping Spread Spectrum (FHSS) oder Direct Sequence Spread Spectrum (DSSS). Die Systeme nutzen das ISM-Frequenzband (Industrial, Scientific, and Medical) zwischen 2,4 und 2,48 GHz.

  Der Vollständigkeit halber sei erwähnt, dass IEEE 802.11 auch eine Infrarot-Übertragung definiert, die aber bisher in der Praxis bedeutungslos geblieben ist.
  DSSS-Systeme nach IEEE 802.11 mit maximal 2 MBit/s werden praktisch nicht mehr eingesetzt. FHSS-Systeme sind sehr robust gegenüber Störungen und daher noch vereinzelt in Produktionsbereichen oder medizinischen Bereichen zu finden.
- Die Systeme der 1999 veröffentlichten Ergänzung IEEE 802.11b (siehe [IEEE99b]) verwenden eine Erweiterung des DSSS-Verfahrens. Die Brutto-Datenübertragungsrate beträgt maximal 11 MBit/s. Es wird ebenfalls das ISM-Frequenzband bei 2,4 GHz genutzt.

  Mit IEEE 802.11b haben sich WLANs enorm verbreitet und auch heute werden Systeme nach IEEE 802.11b noch häufig eingesetzt.
- Um Datenraten bis zu 54 MBit/s und eine höhere Anzahl von parallel operierenden Systemen mit sich überlappenden Funkzellen anbieten zu können, verwenden Systeme nach der ebenfalls 1999 veröffentlichten Ergänzung IEEE 802.11a den 5-GHz-Bereich von 5,15 bis 5,35 GHz und von 5,47 bis 5,725 GHz (siehe [IEEE99a]). Als Übertragungstechnik wird Orthogonal Frequency Division Multiplexing (OFDM) genutzt.
- Systeme der im Juni 2003 veröffentlichten Ergänzung IEEE 802.11g operieren im ISM-Band bei 2,4-GHz und sind mit IEEE 802.11b abwärtskompatibel. Als Übertragungstechnik wird OFDM analog zu IEEE 802.11a verwendet, wodurch auch Datenraten bis 54 MBit/s möglich sind (siehe [IEEE03g]).

Im 2,4-GHz-Frequenzbereich stehen in Deutschland 13 Frequenzkanäle mit einem Frequenzabstand von 5 MHz für die Funkübertragung nach 802.11b zur Verfügung. Bei einer Kanalbandbreite von ca. 22 MHz für IEEE 802.11b können jedoch nur maximal 3 Kanäle gleichzeitig überlappungsfrei genutzt werden. Dies gilt auch für IEEE 802.11g.

Im 5-GHz-Bereich sind in Deutschland insgesamt 19 Kanäle in einem Frequenzabstand von 20 MHz unter Auflagen freigegeben worden. Bei einer Kanalbandbreite von 20 MHz stören sich direkt benachbarte Kanäle untereinander nicht.

Die Rahmenbedingungen und Parameter für den Betrieb von WLANs sind in Verfügungen der Bundesnetzagentur (vormals Regulierungsbehörde für Telekommunikation und Post) festgelegt, siehe [RegTP03] für den 2,4-GHz-Bereich und [RegTP/BNA] für WLANs bei 5 GHz.

Der Zugriff auf den Funkkanal (Medium Access Control, MAC) erfolgt bei allen Systemen einheitlich nach einem zufallsgesteuerten Verfahren, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), das einen Best-Effort-Dienst liefert. Die entsprechende Komponente des WLAN MAC Layer wird in der Terminologie von IEEE 802.11 als Distributed Coordination Function (DCF) be-

zeichnet. Der Standard spezifiziert auch eine optionale Polling-basierte deterministische Kanalvergabe (Point Coordination Function, PCF), die jedoch in den wenigsten Produkten implementiert ist.

Eine Auswahl der weiteren Ergänzungen des Standards IEEE 802.11, die auch für die Sicherheitsbetrachtung von WLANs wichtig sind, ist im Folgenden aufgelistet:

- IEEE 802.11h: Ergänzung zu IEEE 802.11a, verabschiedet im September 2003 (siehe [IEEE03h])

  Der 5-GHz-Bereich wird auch von militärischen und zivilen Radar- und Navigationsanwendungen genutzt. Um Störungen dieser Anwendungen durch ein WLAN zu vermeiden, darf das gesamte bei 5 GHz zur Verfügung stehende Spektrum nur dann durch ein WLAN genutzt werden, wenn im WLAN eine dynamische Frequenzwahl (Dynamic Frequency Selection, DFS) und eine Anpassung der Sendeleistung (Transmit Power Control, TPC) unterstützt wird. IEEE 802.11h spezifiziert die hierfür notwendige Erweiterung des MAC Layer. Seit Frühjahr 2005 zertifiziert die Wi-Fi Alliance auch Geräte bezüglich IEEE 802.11h.

- IEEE 802.11i: verabschiedet im Juni 2004 (siehe [IEEE04i])

  Hier werden verbesserte Sicherheitsmechanismen spezifiziert, die notwendig waren, weil sich die ursprünglich in IEEE 802.11 festgelegten Verfahren als unzulänglich erwiesen haben. Die Verbesserungen betreffen Verschlüsselung, Integritätsschutz und Authentisierung. Die Elemente von IEEE 802.11i und der entsprechenden Konzepte der Wi-Fi Alliance werden in den folgenden Kapiteln noch genauer beschrieben.

- IEEE 802.11e: verabschiedet im September 2005 (siehe [IEEE05e])

  Hier wird die MAC-Ebene von IEEE 802.11 um Dienstgütemechanismen (Quality of Service, QoS) erweitert, indem ein erweiterter Kanalzugriff spezifiziert wird, der unter anderem eine Priorisierung verschiedener Verkehrsklassen und eine durch den Access Point gesteuerte Kanalvergabe erlaubt.

- IEEE 802.11n: Verabschiedung geplant für Frühjahr 2007

  Hier soll dem WLAN-Nutzer durch entsprechende Erweiterungen der physikalischen Übertragung und Optimierung der Protokolle auf dem MAC Layer eine Leistung von mindestens 100 MBit/s geboten werden (im Sinne einer Nettodatenrate). Die physikalische Übertragung wird durch ein als Multiple Input Multiple Output (MIMO) bezeichnetes Verfahren geschehen, das es gestattet, mehrere parallele OFDM-Ströme sich überlagernd auf einem Frequenzkanal zu übertragen. Eine Einigung auf eine technische Lösung wurde Anfang 2006 erreicht.

- IEEE 802.11w: Verabschiedung geplant für Frühjahr 2008

  Ein Sicherheitsrisiko, das IEEE 802.11i nicht beseitigt, geht aktuell von der Übertragung ungesicherter Managementpakete aus, die nicht verschlüsselt und nicht hinsichtlich ihrer Authentizität und Integrität geprüft werden. Die Absicherung von Managementpaketen soll mit IEEE 802.11w möglich werden.

- IEEE 802.11s: Verabschiedung geplant für Sommer 2008

  Das Thema dieser Erweiterung sind so genannte Meshed Networks, d.h. Access Points kommunizieren untereinander über Funk. Pakete können auf diese Weise über mehrere solcher (als Hops bezeichneter) Funkstrecken an das Ziel gelangen. Dabei sind spezielle Routing-Verfahren notwendig, die für eine Paketübertragung aus der vermaschten Netzstruktur, welche sich aus der Vernetzung über Funk ergibt, geeignete Wege von Access Point zu Access Point ermitteln. Meshed Networks können als eine Verallgemeinerung des Prinzips einer Punkt-zu-Punkt-Verbindung über WLAN, wie sie bei einer LAN-Kopplung genutzt wird, verstanden werden. Meshed Networks eignen sich insbesondere für WLAN-Installationen, für die mit vertretbarem Aufwand kein (ausschließlich) kabelbasiertes Distribution System realisierbar ist.

In Arbeit sind noch weitere Erweiterungen, beispielsweise zur Verbesserung des Managements von WLAN-Stationen (IEEE 802.11k und IEEE 802.11v) oder IEEE 802.11r für einen schnelleren Wechsel der Funkverbindung bei der Bewegung eines Clients zwischen Funkzellen.

Abschließend zeigt Abb. A-3 die Struktur des Standards IEEE 802.11 und der verschiedenen angesprochenen Erweiterungen.

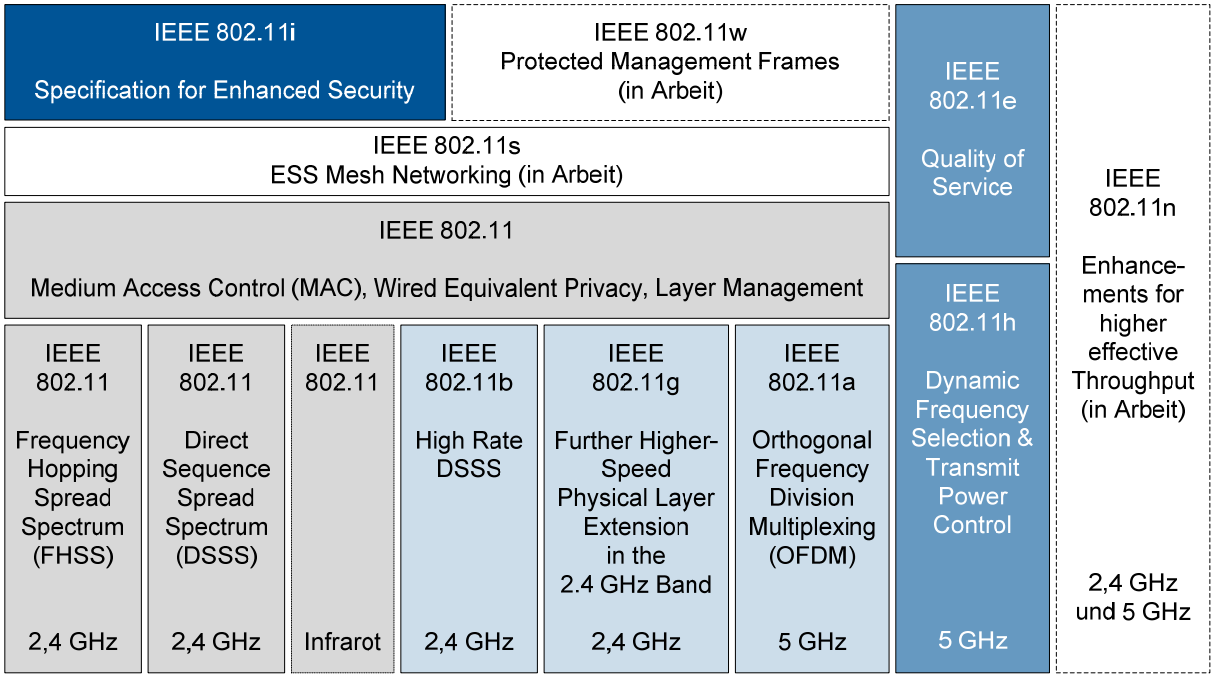


Abb. A-3: Ausschnitt der IEEE-802.11-Familie im Überblick

1.3 Wireless Switches und Thin Access Points

Unter Wireless Switches (auch als WLAN Controller oder Access Controller bezeichnet) versteht man Netzelemente, die gewisse Funktionen von Access Points zentral realisieren, eine entsprechende Schnittstelle für Management und Administration der Access Points bieten und dabei auch den Zugang zwischen Access Points und dem kabelbasierten LAN kontrollieren. Wireless Switches gibt es am Markt seit wenigen Jahren mit einer deutlich steigenden Produktvielfalt.

Access Points können produktabhängig direkt an einen Wireless Switch angeschlossen werden oder die Anbindung erfolgt über ein Netzwerk. In letzterem Fall findet die Kommunikation zwischen Access Points und Wireless Switch meist über Tunnelmechanismen statt. Dabei werden die Layer-2-Pakete von und zu den WLAN-Clients als Nutzlast über den Tunnel übertragen (siehe Abb. A-4).

Wird als Trägerprotokoll IP verwendet (was von den meisten Produkten unterstützt wird), entsteht ein virtuelles Distribution System und die zu Grunde liegende Netzstruktur zwischen Access Points und Wireless Switch wird transparent. Diese Konzepte führen zu einem WLAN-Design, das sich deutlich von dem Aufbau mit traditionellen Access Points unterscheidet. Im klassischen WLAN-Design ist das Distribution System meist ein flaches Layer-2-Netz, weil sich bei einem Layer-3-Netz Mobilitätseinschränkungen ergeben würden[2].

Dieses Problem kann durch den Einsatz von Tunnelmechanismen umgangen werden. Wird die Kommunikation eines Clients nämlich über das Distribution System getunnelt, merkt die Client-Applikation einen mobilitätsbedingten IP-Subnetzwechsel gar nicht, weil sie die zwischen Access Point und Wireless Switch liegende Netzstruktur nicht wahrnimmt.

[2] Auf Layer 3 bedingt ein Handover in ein anderes IP-Subnetz den Wechsel der IP-Adresse des Clients. Durch diesen Adresswechsel verliert der Client aber alle Kommunikationsbeziehungen, die auf seiner alten IP-Adresse beruhten. Dies macht gegebenenfalls den Neustart einer Anwendung oder sogar den Neustart des gesamten Client-Systems notwendig.

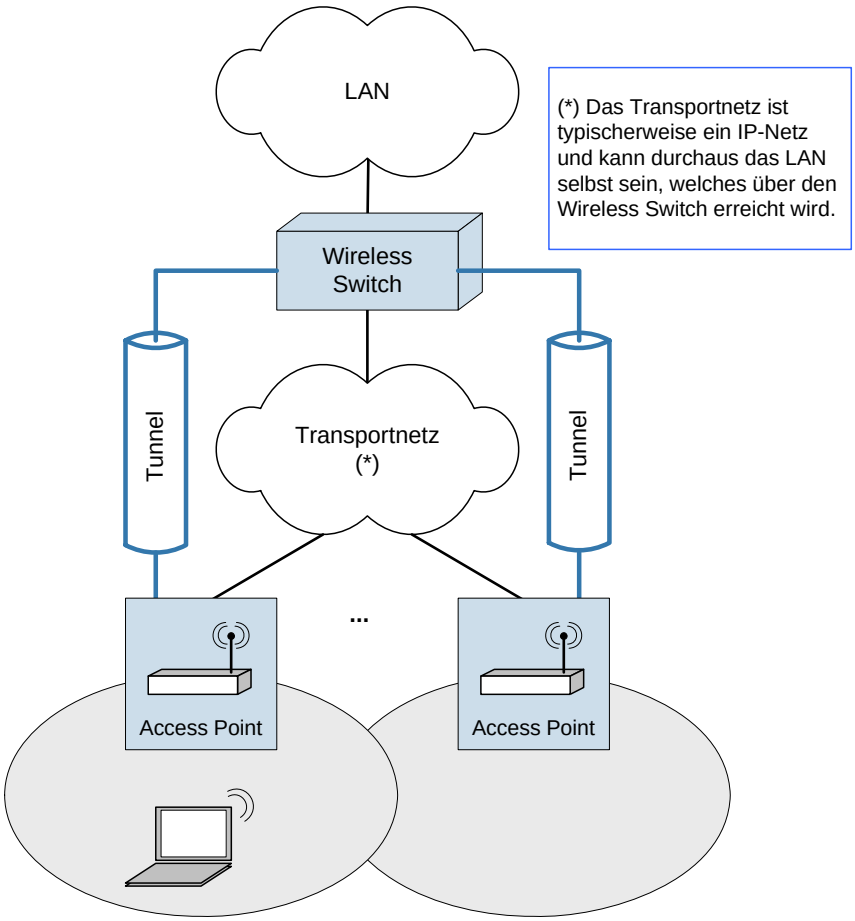


Abb. A-4: Tunnel zwischen Access Points und Wireless Switch

Wireless Switches können also insbesondere eingesetzt werden, um ein WLAN in eine (beliebige) Layer-3-strukturierte LAN-Infrastruktur zu integrieren bzw. um das Distribution System als Layer-3-Netz aufzubauen. Diese Anforderung hat verschiedene Gründe: Durch eine Strukturierung in mehrere Broadcast-Domänen reduziert sich die Broadcast-Last. Weiterhin können auf Layer 3 zuverlässige Redundanzmechanismen mit schnellen Failover-Zeiten eingesetzt werden, z.B. OSPF.

WLAN-Funktionen, die auf einem Wireless Switch zentralisiert werden, brauchen nicht mehr auf den Access Points implementiert zu werden. Die Access Points können also schlanker gestaltet werden. Als Konsequenz müssen der Wireless Switch als zentrale Steuerinstanz und die schlanken Access Points (Thin Access Points) aufeinander abgestimmt sein. Thin Access Points sind sogar meist nicht mehr in der Lage, ohne einen zugehörigen Wireless Switch zu funktionieren. Nach dem Anschluss eines Thin Access Point an ein LAN ist die erste Operation des Thin Access Point die Suche nach einem Wireless Switch. Der Wireless Switch versorgt den Thin Access Point zunächst mit einer WLAN-Konfiguration und gegebenenfalls mit einer neuen Firmware. Stand heute kommen daher Wireless Switches und Thin Access Points meist aus einer Hand.

Es gibt aber mit der IETF-Arbeitsgruppe CAPWAP (Control And Provisioning of Wireless Access Points) bereits erste Standardisierungsbemühungen für die Kommunikation zwischen Thin Access Points und Wireless Switches und für die Frage, welche Funktionen von einem Access Point auf einen Wireless Switch verlagert werden können (siehe [CAPW05]). Aktuell liegen die meisten Ergebnisse (insbesondere die Spezifikation desProtokolls zwischen Access Point und Wireless Switch, siehe [CAPW06]) allerdings nur als IETF Internet Draft vor.

Aus der Sicherheitsperspektive sind Wireless Switches aus folgenden Gründen interessant:

- Die Access Points erhalten ihre Konfiguration grundsätzlich vom Wireless Switch. Thin Access Points verfügen oft sogar über keinen eigenen permanenten Speicher für Konfigurationen. Es sind Systeme verfügbar, bei denen zusätzlich die Kommunikation zwischen (Thin) Access Point und

Wireless Switch eine gegenseitige Authentisierung erfordert und verschlüsselt werden kann. Auf diese Weise kann das System vor einem unberechtigten Zugriff auf einen Access Point oder auf die zwischen Access Point und Wireless Switch ausgetauschten Daten geschützt werden. Weiterhin ist das Risiko reduziert, dass ein Access Point mit unsicherer Default-Konfiguration versehentlich im Netz installiert ist.

- Die Zentralisierung von Sicherheitsfunktionen im Wireless Switch kann zu einer Leistungsverbesserung beitragen. Moderne Sicherheitsmechanismen für größere WLAN nutzen IEEE 802.1X für die Authentisierung und für die Verteilung von Sitzungsschlüsseln (siehe Kapitel 2.4). Bei jedem Wechsel einer Funkzelle würde IEEE 802.1X eine erneute Authentisierung anstoßen. Dieser Aufwand kann erheblich reduziert werden, wenn die Authentisierung zentral auf dem Wireless Switch, der ja mehrere Access Points (d.h. Funkzellen) bedient, durchgeführt wird.
- Durch die genannten Tunnelmechanismen wird auch die Kommunikation zwischen Clients zunächst zum Wireless Switch geleitet und kann dort gefiltert werden. Dies erschwert Angriffe von einem Client auf einen anderen Client.

1.4 Voice over IP über WLAN

Die Übertragung von Voice over IP (VoIP) über WLAN ist eine Anforderung, die durch den Standard IEEE 802.11 in seiner Version von 1999 nicht zufrieden stellend abgedeckt werden konnte.

Der Grund ist zunächst, dass der Kanalzugriff in einem WLAN nach IEEE 802.11 ein zufallsgesteuerter Mechanismus ist, der in seiner ursprünglichen Fassung weder eine Priorisierung unterschiedlicher Verkehrsklassen noch eine explizite Bandbreitenreservierung vorsieht. Als Konsequenz ist die Antwortzeit in einem WLAN nach IEEE 802.11 stets starken Schwankungen unterworfen. Diese Schwankungen sind neben der Qualität des Funkkanals abhängig von der Anzahl der Clients, die an einem Access Point assoziiert sind und vom Verkehrsverhalten (also von den Anwendungen) dieser Clients.

Für die Übertragung von Sprache und anderen Daten, die höhere Anforderungen an das Antwortzeitverhalten haben, ist IEEE 802.11 also zunächst eher ungeeignet. Es fehlen Mechanismen zur Zusicherung von Dienstgüte (Quality of Service, QoS). Neben VoIP over WLAN gibt es natürlich auch eine steigende Zahl von WLAN-Anwendungen in Produktions- und Logistikbereichen, die mit Anforderungen an das Antwortzeitverhalten gekoppelt sind und von QoS-Konzepten in WLAN ebenfalls unmittelbar profitieren würden. Weiterhin ist für die Übertragung von Video über WLAN bei Überwachungskameras der Einsatz von QoS interessant, falls das WLAN auch von anderen Geräten außer diesen Kameras genutzt wird.

Es gibt zwar schon seit mehreren Jahren Handsets für VoIP over WLAN, die jedoch zunächst proprietäre Verfahren einsetzen mussten, um zumindest eine Priorisierung des VoIP-Verkehrs zu ermöglichen. Client Adapter und Access Point mussten also hier besonders aufeinander abgestimmt sein. Inzwischen sind entsprechende WLAN-Standards verfügbar.

Nach ca. 5 Jahren Arbeit wurde im September 2005 mit IEEE 802.11e die QoS-Erweiterung des WLAN MAC Layer verabschiedet (siehe [IEEE05e]). Seit September 2004 gibt es aber auch Wi-Fi Multimedia (WMM) von der Wi-Fi Alliance. WMM basiert auf einem Draft zu IEEE 802.11e, und es sind bereits diverse Produkte WMM-zertifiziert.

Das Kernelement von IEEE 802.11e und WMM ist die abwärtskompatible Erweiterung der DCF um einen Priorisierungsmechanismus. Diese Funktion wird als Enhanced Distributed Channel Access (EDCA) bezeichnet. Hierzu gehört auch ein Burst-Modus, der es gestattet, für eine gewisse Zeit alleine über das Medium zu verfügen. Auf diese Weise können hochpriore Pakete schnell hintereinander übertragen werden und müssen nicht in einer Warteschlange auf einen nächsten Übertragungsversuch warten. In der EDCA bleibt der grundsätzliche Zufallsmechanismus erhalten.

Es werden vier Prioritätsklassen unterschieden: Voice Priority als höchste Priorität gefolgt von Video Priority, dann Best Effort Priority und schließlich Background Priority.

Möglichkeiten der Reservierung und Kontrolle eines Kommunikationskanals sind über den HCF Controlled Channel Access (HCCA) gegeben. Für Stationen, die keine QoS-Funktionen unterstützen bleibt die (optionale) PCF. Diese Funktionen (PCF, EDCA und HCCA) werden zur Hybrid Coordination Function (HCF) zusammengefasst. Abb. A-5 zeigt die Elemente des MAC Layer in IEEE 802.11e im Überblick.

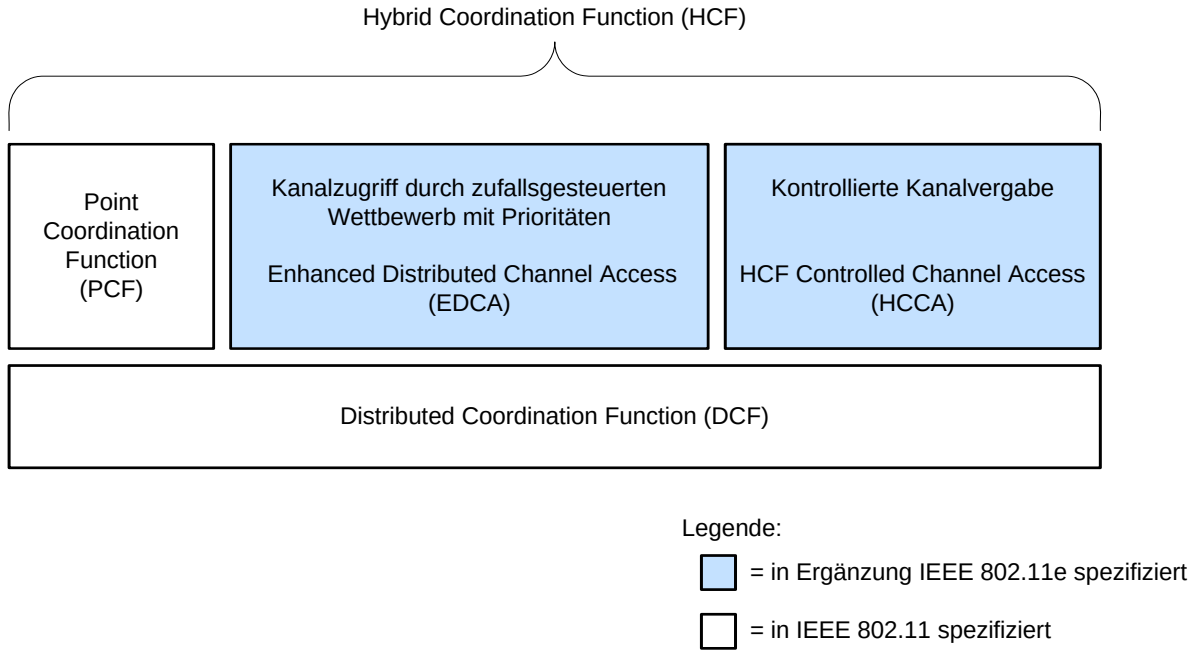


Abb. A-5: Erweiterung der DCF

Wird VoIP in einem flächendeckenden WLAN, bestehend aus mehreren überlappenden Funkzellen (Access Points) genutzt, bestehen hohe Anforderungen an den Zellwechsel (Handover). Gewisse Ausfallzeiten der Verbindung sind bei einem Handover unvermeidbar. Für VoIP müssen sich diese Ausfallzeiten in tolerablen, d.h. kaum wahrnehmbaren, Grenzen bewegen. Der Standard IEEE 802.11 und seine aktuellen Erweiterungen spezifizieren aber weder Verfahren noch Parameter für ein Handover. Die Implementierung eines Handover ist also derzeit noch vollständig herstellerspezifisch. In der „Task Group r“ wird allerdings bereits an schnellen Handover-Verfahren gearbeitet, die mit IEEE 802.11r standardisiert werden sollen.

1.5 Hotspots

Neben der Erweiterung der LAN-Infrastruktur im betrieblichen und privaten Umfeld haben sich relativ schnell öffentliche WLANs (Hotspots) als eine weitere Nutzungsform der WLAN-Technik etabliert.

Neben der Absicherung des Hotspot gegen einen unautorisierten Zugang, sind für einen Hotspot die Aufgabengebiete Teilnehmerverwaltung, Authentisierung des (zahlenden) Teilnehmers dem Netz gegenüber sowie Zahlungsabwicklung und Abrechnung zu betrachten. Da Hotspot-Anbieter im Sinne des Telekommunikationsgesetzes (TKG) als Telekommunikationsdienstleister auftreten, sind u.a. die Auflagen bzgl. Sicherheit der Abrechnungs- und Benutzerdaten (Datenschutz, Speicherung von Verbindungsdaten) zu berücksichtigen (siehe [TKG04]).

Ein Nutzer, der sich an einem Hotspot anmelden möchte, führt zunächst eine Assoziierung des Clients an einem entsprechenden Access Point des Hotspot durch. In der Regel erfolgt keine Verschlüsselung auf der Luftschnittstelle, um dem Client einen möglichst unproblematischen Netzzugang zu ermöglichen. Eine IP-Adresse erhält der Client automatisch über das Dynamic Host Configuration Protocol (DHCP). Wenn die Netzverbindung aufgebaut ist, startet der Nutzer einen Web-Browser und wird automatisch zur Startseite des Hotspot-Systems umgeleitet. Hier werden die Zahlungs- und Zugangs-

modalitäten geregelt. Die Zugangskontrolle an einem Hotspot erfolgt in den meisten Fällen durch Angabe eines Passworts in einem Feld einer Web-Applikation des Hotspot-Systems.

Leider ist bis heute keine einheitliche systemübergreifende Authentisierung, Anmeldung und Abrechnung für Hotspot-Systeme realisiert. Durch den Einsatz eines Clearing House oder durch direkte Kooperationen von Wireless Internet Service Providern (WISPs) kann dieses Problem inzwischen zwar deutlich gemildert werden, von der Umsetzung eines internationalen Standards ist man aber noch weit entfernt. Weiter zeichnet sich für größere Hotspot-Systeme der Trend ab, ein GSM- bzw. UMTS-Netz für Authentisierung und Abrechnung zu nutzen, da diese elementaren Funktionen hier bereits implementiert sind.

2. Sicherheitsmechanismen

In diesem Kapitel werden die wesentlichen Sicherheitsmechanismen vorgestellt, die zum Schutz der WLAN-Übertragung beitragen. Den Schwerpunkt bildet die Vorstellung der Ergänzung IEEE 802.11i (bzw. der entsprechenden Spezifikationen der Wi-Fi Alliance) und der Authentisierung über IEEE 802.1X. Weitere Sicherheitsmechanismen und detailliertere Ausführungen können dem Teil 1 der Technischen Richtlinie Sicheres WLAN entnommen werden (siehe [TR-S-W1]).

2.1 Netzwerkname (SSID)

Der Service Set Identifier (SSID) dient der Identifikation eines ESS, d.h. eines WLAN. Bei der Anmeldung an ein WLAN und beim Handover zwischen zwei benachbarten Funkzellen dient der SSID dazu, den nächsten Access Point zu finden. Die maximale Länge eines SSID beträgt 32 Byte. Der SSID wird auf Client und Access Point konfiguriert. Die Client-Software unterstützt meist verschiedene Profile, die es erlauben, mehrere WLANs (sprich: mehrere SSIDs) zu konfigurieren.

Die Übertragung des SSID geschieht auf Layer 2 als Parameter in einem speziellen, in regelmäßigen Abständen übertragenen Paket, dem so genannten Beacon Frame. Dieser Mechanismus wird auch als SSID Broadcast bezeichnet. In dem Beacon Frame übermittelt ein Access Point neben dem SSID die wesentlichen Übertragungsparameter inklusive der Sicherheitseinstellungen, wie z.B. das zu verwendende Verschlüsselungsverfahren.

Alternativ kann ein Client explizit erfragen, ob ein Access Point mit einem gewissen SSID erreichbar ist. Hierzu sendet der Client unter Angabe des gewünschten SSID ein spezielles Layer-2-Paket (Probe Request) und ein Access Point passender SSID antwortet mit einem Probe-Response-Paket. Verwendet der Client dabei den so genannten Broadcast SSID (ein SSID der Länge 0), bedeutet dies, dass der Client mit einem beliebigen Access Point kommunizieren möchte. Sofern es in der Konfiguration eines Access Point nicht unterdrückt wird, antwortet ein Access Point auf ein Probe Request mit Broadcast SSID durch ein Probe-Response-Paket mit dem SSID des Access Point.

Für nicht-öffentliche WLAN sollte an einem Access Point die Antwort auf eine Anfrage mit Broadcast SSID unterdrückt werden.

Da der SSID unverschlüsselt gesendet wird, kann ein Angreifer ihn mit einfachen Mitteln in Erfahrung bringen. Einige Access Points bieten die Möglichkeit, den SSID Broadcast zu unterbinden[3]. Ein Client muss den SSID dann, wie eben beschrieben, explizit erfragen. Bevor die Broadcast-Übertragung des SSID am Access Point unterbunden wird, sollte überprüft werden, ob alle Clients mit dieser Einstellung zurechtkommen, denn dies kann für manche Client-Systeme zu Beeinträchtigungen in der Netzauswahl kommen. Hierzu gehören z.B. Microsoft Windows-Systeme, die über die Funktion Wireless Zero Configuration (WZC) konfiguriert werden.

[3] Es erfolgt weiterhin eine periodische Übertragung durch den Access Point. In dem entsprechenden Paket ist der SSID des WLAN jedoch nicht mehr aufgeführt.

2.2 MAC-Adresse

Jede Netzwerkkarte verfügt über eine eindeutige Hardware-Adresse, die im Normalfall als MAC-Adresse (Media-Access-Control-Adresse) verwendet wird. Prinzipiell ist es möglich, an einem Access Point Listen anzulegen, in denen die MAC-Adressen derjenigen Clients eingetragen werden, denen es erlaubt ist, über den Access Point zu kommunizieren. Dieses Prinzip der Zugangssteuerung über eine Liste von MAC-Adressen wird auch als MAC-Adress-Authentisierung bezeichnet. Die MAC-Adresslisten müssen „von Hand“ gepflegt werden, d.h. der Aufwand wächst generell mit der Anzahl der zugelassenen Adressen.

Die meisten Access Points unterstützen die Verwendung des Remote Authentication Dial-In User Service (RADIUS, siehe [RADI00]). Die MAC-Adressen werden dann auf einem zentralen RADIUS-Server gepflegt und die Access Points fragen über RADIUS nach, ob eine angegebene Adresse verzeichnet ist.

Die Pflege von Adress-Listen auf den Access Points ist bereits bei wenigen Clients und Access Points sehr aufwändig. Dies ist meist nur für WLAN im Small-Office-Home-Office-Bereich eine mit vertretbarem Aufwand durchführbare Maßnahme. Für größere WLANs mit vielen Clients sind auch zentrale Listen unter Verwendung von RADIUS nur schwer zu verwalten.

Hinzu kommt, dass eine MAC-Adress-Authentisierung nur einen geringen Sicherheitsgewinn liefert.

Für einen Angreifer kann mit nicht nennenswertem Aufwand ein WLAN-Adapter auf eine andere MAC-Adresse umgestellt werden. Vermutet ein Angreifer, dass eine MAC-Adress-Authentisierung eingesetzt wird, beobachtet er einfach das WLAN, zeichnet die MAC-Adressen von erlaubten Clients auf und konfiguriert für einen Angriff den eigenen WLAN-Adapter mit einer der aufgezeichneten MAC-Adressen.

Die MAC-Adress-Authentisierung kann also lediglich als flankierende Maßnahme für kleine WLAN-Installationen gesehen werden, sofern der Aufwand akzeptabel ist.

2.3 Wired Equivalent Privacy

Vertraulichkeit, Integrität und Authentizität im WLAN wurden im ursprünglichen Standard IEEE 802.11 ohne die Erweiterung IEEE 802.11i durch einen als Wired Equivalent Privacy (WEP) bezeichneten Mechanismus gesichert. Allerdings ist WEP mittlerweile vollständig kompromittiert und für die Absicherung eines WLAN allein als ungenügend einzustufen (siehe auch Kapitel 3.10).

WEP basiert auf der Stromchiffre RC4, mit der Klardaten paketweise abhängig von einem Schlüssel und einem Initialisierungsvektor (IV) in Chiffratdaten umgewandelt werden. Der Schlüssel ist dabei eine Zeichenkette von wahlweise 40 oder 104 Bit und muss den am WLAN beteiligten Clients sowie dem Access Point vorab zur Verfügung gestellt werden. Dabei wird für das gesamte WLAN ein gemeinsamer Schlüssel verwendet. Der IV wird vom Absender gewählt und sollte für jedes übertragene Datenpaket unterschiedlich sein. Der IV wird dem verschlüsselten Datenpaket unverschlüsselt vorangestellt und über das WLAN übertragen.

Über WEP sollten folgendermaßen die Vertraulichkeit und die Integrität der übertragenen Daten gesichert sowie die Authentisierung des Endgerätes (nicht des Nutzers) durchgeführt werden:

- Vertraulichkeit: Aus dem Schlüssel und dem IV wird ein pseudozufälliger Bitstrom generiert. Die Chiffratdaten ergeben sich, indem die unverschlüsselten Daten bitweise mit dem Bitstrom XOR-verknüpft werden (XOR = exklusives Oder). Beim Empfänger werden die Klartextdaten wiederum aus den Chiffratdaten ermittelt, indem derselbe Bitstrom mit den Chiffratdaten XOR-verknüpft wird.
- Integrität: Für jedes zu übertragene Datenpaket wird eine 32-Bit CRC-Checksumme berechnet. Anschließend wird das Datenpaket und die angehängte Checksumme verschlüsselt. Der Empfänger entschlüsselt das Datenpaket und überprüft die Checksumme. Ist die Checksumme korrekt, wird das Datenpaket angenommen, andernfalls wird es verworfen. Das verwendete Verfahren

eignet sich zwar zur Erkennung von Bitfehlern durch Übertragungsstörungen, es ist jedoch für die Abwehr systematischer Paketfälschungen und damit für die Sicherstellung der Integrität ungeeignet. Dies ist eine weitere erhebliche Schwäche des WLAN-Standards von 1999.

- Authentisierung: In Verbindung mit der WEP-Verschlüsselung kann zwischen zwei Authentisierungsmodi gewählt werden: „Open“ (hierbei findet keine Authentisierung statt) und „Shared Key“. Für die Authentisierung im „Shared Key“-Modus wird ein so genanntes Challenge-Response-Verfahren durchgeführt: Der Access Point generiert 128 zufällige Bytes und sendet diese in einem Datenpaket unverschlüsselt an einen Client (Challenge). Der Client verschlüsselt das Datenpaket und sendet es zurück zum Access Point (Response). Der Client hat sich erfolgreich authentisiert, wenn der Access Point die Response zur Challenge entschlüsseln kann. Der Authentisierungsprozess ist nur einseitig: der Access Point muss sich gegenüber den Clients nicht authentisieren. Zum Authentisieren wird derselbe Schlüssel verwendet wie zur Verschlüsselung der Nutzdaten.

WEP verschlüsselt die übertragenen Nutzdaten und die Integritäts-Checksumme. Management- und Steuersignale (Management Frames und Control Frames) werden auf der Funk-Schnittstelle jedoch nicht verschlüsselt.

2.4 IEEE 802.11i

Die Erweiterung IEEE 802.11i entstand, um die aufgetretenen Sicherheitslücken von WEP zu schließen. IEEE 802.11i umfasst die Bereiche Verschlüsselung, Authentisierung und Schlüsselmanagement.

Da die in IEEE 802.11i verabschiedete Lösung abwärtskompatibel zu WEP sein musste, umfasst sie zwei verschiedene Verschlüsselungsverfahren:

- Temporal Key Integrity Protocol (TKIP) mit Integritätsprüfung Michael

  TKIP ist eine als Temporärlösung aufzufassende abwärtskompatible Lösung, die sich insbesondere zur verbesserten Absicherung bereits bestehender WLANs eignet.

- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)

  CCMP ist eine langfristige Lösung, die neue Hardware erfordert.

Die Authentisierung erfolgt entweder über IEEE 802.1X (in diesem Fall erfolgt das Schlüsselmanagement auch über IEEE 802.1X) oder Pre-Shared Keys.

Ein WLAN, das ausschließlich eine durch die in IEEE 802.11i spezifizierten Sicherheitsmechanismen geschützte Kommunikation erlaubt, wird durch den Standard als Robust Security Network (RSN) bezeichnet. Abb. A-6 zeigt die wesentlichen Bestandteile von IEEE 802.11i im Überblick.

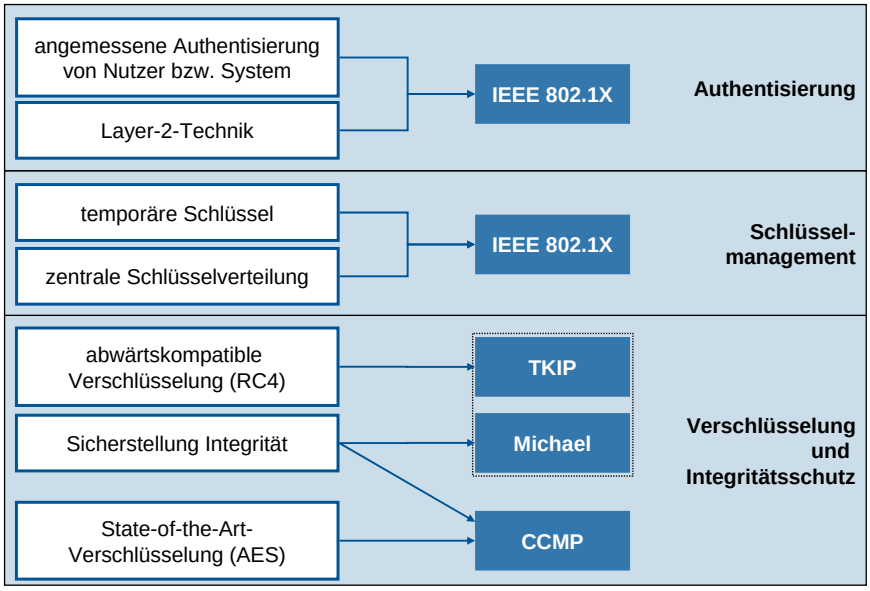


Abb. A-6: Bausteine von IEEE 802.11i im Überblick

2.4.1 TKIP und Michael

Die zu WEP abwärtskompatible Verschlüsselungsmethode ist das Temporal Key Integrity Protocol (TKIP), das die bisher bekannten Schwächen von WEP bei der Auswahl und Erzeugung der Startwerte von RC4 beseitigt. Die effektive Schlüssellänge bei TKIP liegt weiterhin bei 104 Bit, da als Basis WEP verwendet wird. In TKIP wird pro Paket ein neuer Schlüssel erzeugt, um die bisher statischen WEP-Schlüssel zu vermeiden. Ein solcher Schlüssel entsteht durch Anwendung einer Hash-Funktion auf einen geheimen symmetrischen Sitzungsschlüssel, den Initialisierungsvektor und eine Paketsequenznummer. Der Sitzungsschlüssel wiederum wird aus einem gemeinsamen Schlüssel – Pairwise Master Key (PMK) genannt – abgeleitet, der entweder als Pre-Shared Key (PSK) auf den WLAN-Systemen voreingestellt ist oder der im Rahmen der Authentisierung eines WLAN-Clients über IEEE 802.1X übermittelt wird (siehe Kapitel 2.4.3 und 2.4.4).

Für die Entschlüsselung muss zusätzlich zum Initialisierungsvektor für WEP ein weiterer Initialisierungsvektor übertragen werden, damit der Empfänger den vom Sender benutzten Paketschlüssel ebenfalls erzeugen kann.

Da TKIP auf der gleichen Hardware basiert, die auch WEP nutzt, sind wesentliche Funktionen von TKIP in Software realisiert, wodurch sich gegenüber WEP eine Reduzierung des Datendurchsatzes von 5% bis 10% ergeben kann.

Zur Beseitigung der mangelhaften Integritätsprüfung in WEP wird TKIP durch einen zusätzlichen Message Integrity Check (MIC, bezeichnet als „Michael“) ergänzt. Dieser berücksichtigt nicht nur die Nutzdaten, sondern auch die Paketsequenznummer sowie die Quell- und Zieladresse des MAC-Pakets und wird verschlüsselt übertragen. Beim Empfänger wird dann nach weitgehendem Ausschluss von zufälligen Übertragungsfehlern (korrekte CRC und passender Initialisierungsvektor) durch MIC die Integrität des Datenpakets bzw. des Absenders überprüft. Wenn Michael mehr als eine Integritätsverletzung pro Minute feststellt, werden alle Übertragungen von der zugehörigen Quelladresse für eine Minute ignoriert, die Schlüssel müssen neu ausgehandelt werden und der Angriffsversuch wird dem Netzmanagement gemeldet.

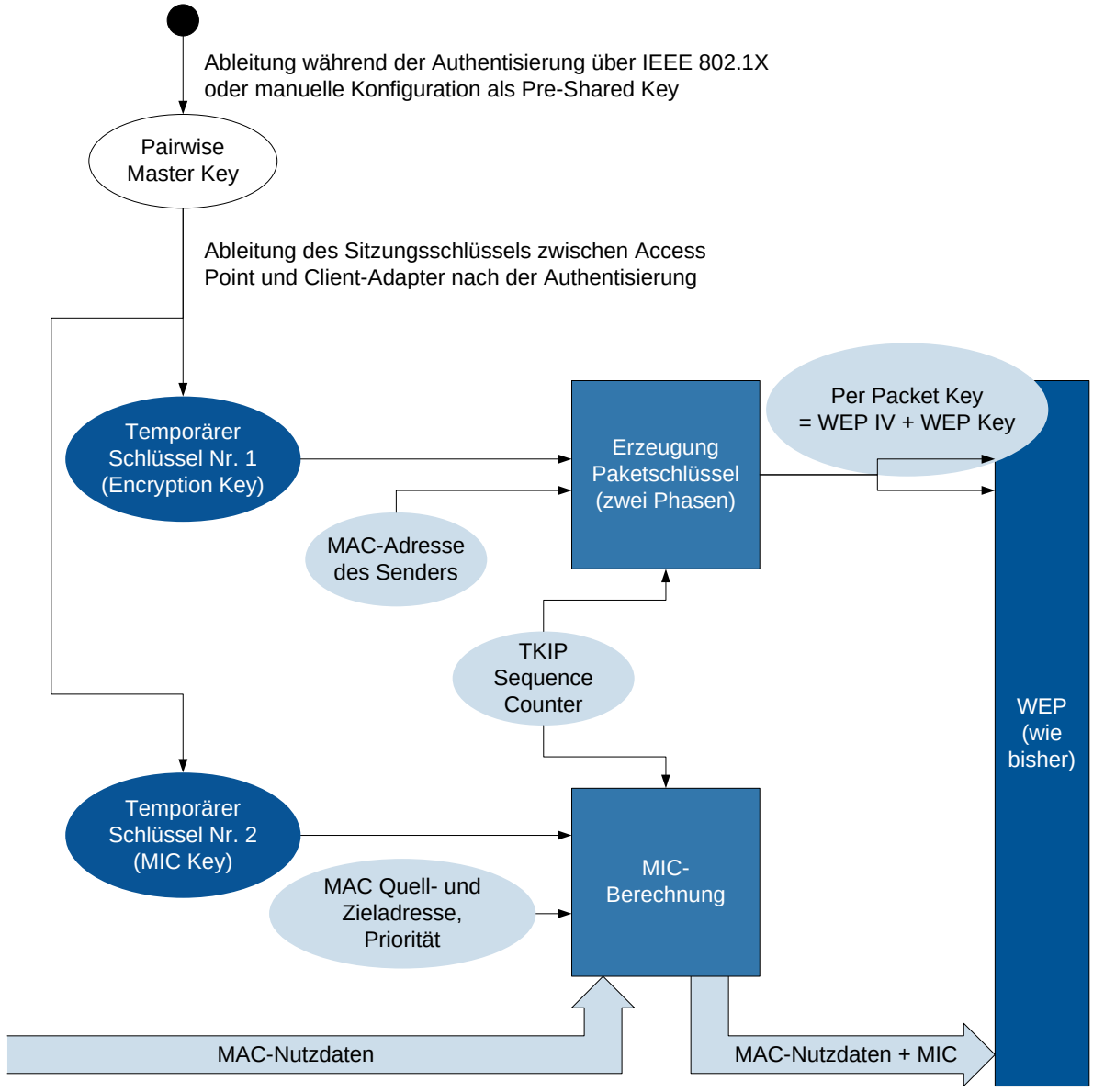


Abb. A-7: Aufbau von TKIP (vereinfacht)

2.4.2 CCMP

Im zweiten langfristig zu nutzenden Verschlüsselungsverfahren von IEEE 802.11i wird der Advanced Encryption Standard (AES) im speziellen Modus Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) genutzt. Hierbei wird nicht direkt der Klartext mit AES verschlüsselt, sondern der Wert eines Zählers. Das eigentliche Verschlüsselungsergebnis entsteht dann aus der XOR-Verknüpfung eines Blocks des Klartextes mit dem AES-verschlüsselten Zähler, wie in Abb. A-8 illustriert. Die Schlüssellänge beträgt 128 Bit. Die Bereitstellung des Schlüssels erfolgt über IEEE 802.1X oder über einen manuell konfigurierten Pre-Shared Key (siehe Kapitel 2.4.3 und 2.4.4). Die Integritätsprüfung geschieht durch die in CCMP genutzte Methode Cipher Block Chanining.

Generell ist der Einsatz von AES zu bevorzugen, da AES ein Verfahren auf dem Stand der Technik darstellt und hier alle wesentlichen Elemente des Verschlüsselungsverfahrens in Hardware realisiert sind.

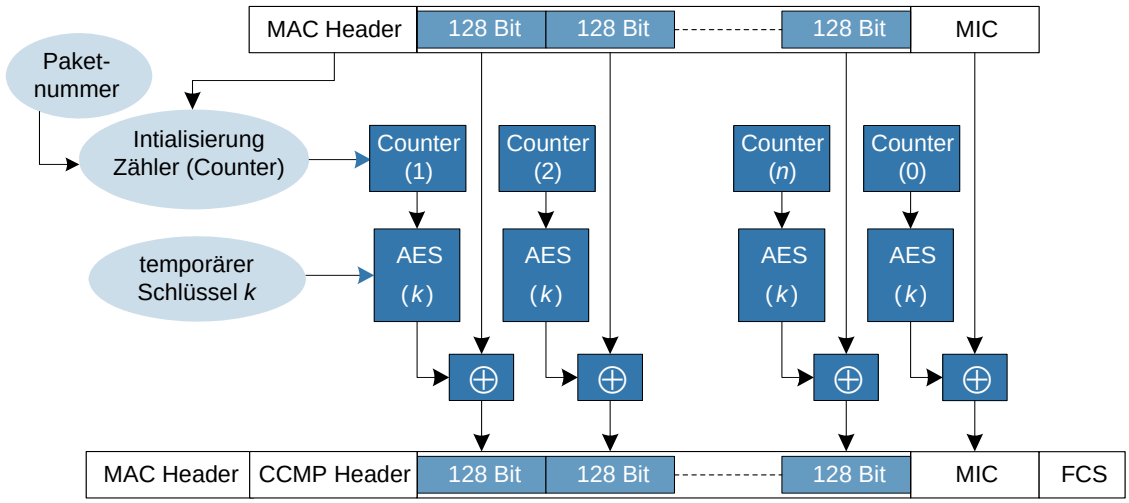


Abb. A-8: Verwendung von AES in IEEE 802.11i (vereinfacht)

2.4.3 IEEE 802.1X

IEEE 802.1X spezifiziert eine standardisierte Methode zur portbasierten Netzwerkzugangskontrolle für kabelbasierte LAN, die auf IEEE-802-Standards basieren, und für WLAN nach IEEE 802.11.

IEEE 802.1X spezifiziert verschiedene Rollen der beteiligten Netzelemente (siehe Abb. A-9):

- Der Supplicant ist eine Software-Komponente im (WLAN-) Client-System, die den Netzwerkzugang anfordert.
- Das Gerät, das den Netzwerkzugang herstellt und eine Schnittstelle für die Authentisierung anbietet, heißt Authenticator. Im WLAN wird diese Funktion vom Access Point wahrgenommen.
- Der Authentication Server ist das Gerät, welches den eigentlichen Authentisierungsdienst bereitstellt. Der Authenticator Server ist typischerweise ein RADIUS-Server (siehe [RADI03]).

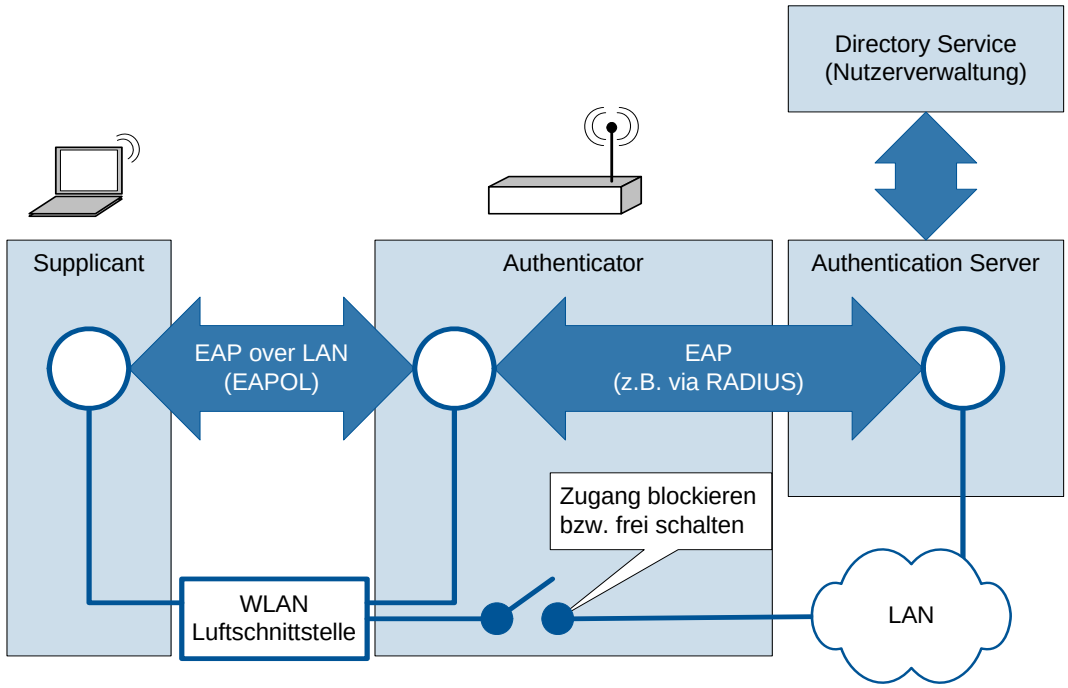


Abb. A-9: Funktionsweise von IEEE 802.1X

Die Authentisierung geschieht über das Extensible Authentication Protocol (EAP, siehe [EAP04]). Dabei erfolgt die Kommunikation über die LAN- bzw. WLAN-Schnittstelle zwischen Supplicant und Authenticator mit der Variante EAP over LAN (EAPOL). EAPOL gestattet die Übertragung von EAP-Nachrichten auf Layer 2. Auf diese Weise wird eine Authentisierung am Netzzugangspunkt ermöglicht, bevor eine Kommunikation auf IP-Ebene und höheren Protokollebenen stattfinden kann. Die Kommunikation zwischen Authenticator und Authentication Server geschieht (typischerweise) über RADIUS, wobei die EAP-Nachrichten als RADIUS-Attribute übertragen werden.

EAP ist modular und liefert einen Rahmen, in den die eigentlichen Authentisierungsverfahren, die so genannten EAP-Methoden, eingebettet werden können. Damit EAP-Methoden für die Anwendung im WLAN geeignet sind, müssen sie zusätzlich auch die Möglichkeit der Erzeugung und Verteilung von Schlüsselmaterial (siehe Kapitel 2.4.1 und 2.4.2) bieten. Es gibt eine ganze Reihe von EAP-Methoden. Im Folgenden werden die für die WLAN-Anwendung besonders relevanten Methoden beschrieben:

- EAP-TLS (RFC 2716)

  Diese EAP-Methode basiert auf der Authentisierung gemäß Transport Layer Security (TLS). Es wird eine beidseitige Authentisierung anhand von X.509-Zertifikaten durchgeführt. Das bedeutet, dass eine Public Key Infrastructure (PKI) zur Zertifikatsverteilung und Verwaltung der Zertifikate (Ausstellung, Rückruf, Erneuerung etc.) benötigt wird, die wiederum einer sorgfältigen Planung bedarf. Außerdem muss für jeden Client-Typ ein Zertifikat ausgestellt werden können.
  Bei EAP-TLS sendet der jeweils zu authentisierende Kommunikationspartner ein Zertifikat, das seinen öffentlichen Schlüssel enthält. Außerdem sendet er eine mit seinem privaten Schlüssel gebildete Signatur, so dass der Empfänger durch Anwendung des öffentlichen Schlüssels auf diese Signatur die Authentizität des Senders feststellen kann.
  Während der Authentisierungsphase wird auch vom Client ein Master Session Key (MSK) generiert, der dem Server verschlüsselt durch seinen öffentlichen Schlüssel übermittelt wird. Aus diesem Master Session Key können dann sowohl Server als auch Client die für die weitere Verschlüsselung der Kommunikation nötigen Schlüssel wie z.B. den PMK von TKIP ableiten.

- EAP-TTLS (IETF Internet Draft)

  Bei EAP-TTLS (Tunneled TLS) wird die unter EAP-TLS beschriebene Methode nur zur Authentisierung des Servers genutzt. Anschließend wird ein TLS-Tunnel zwischen Server und Client aufgebaut, in dem dann geschützt die Authentisierung des Clients durch andere Methoden erfolgt, wie z.B. über die EAP-Methode Generic Token Card (GTC) oder auch über ältere Standardprotokolle wie PAP, CHAP oder MSCHAP.
  Auch bei EAP-TTLS wird während der Authentisierungsphase ein MSK generiert, der für die Ableitung weiterer für die Verschlüsselung notwendiger Schlüssel genutzt wird.

- EAP-PEAP (IETF Internet Draft)

  EAP-PEAP (Protected EAP) funktioniert ähnlich wie EAP-TTLS, nur dürfen im Tunnelinneren nur EAP-Methoden zur Authentisierung des Clients angewendet werden. In den aktuell genutzten Implementierungen PEAPv0 und PEAPv1 werden MSCHAPv2 (siehe [KaPa04]) und EAP-GTC (Generic Token Card, siehe [EAP04]) als innere Authentisierungsmethoden unterstützt. Ein Beispiel ist die Kombination von EAP-PEAP mit der EAP-Methode EAP-MSCHAPv2, die auf der oft bei Windows-Clients genutzten PPP-Authentisierungsmethode MSCHAPv2 basiert. Über EAP-MSCHAPv2 können die für eine Domänenanmeldung üblichen Abfragen von Nutzername und Passwort geschehen, so dass diese Methode gut zur Benutzerverwaltung in Windows-Lösungen passt.

Wenn möglich, ist EAP-TLS den beiden anderen beschriebenen EAP-Methoden immer vorzuziehen, da durch die direkte gegenseitige Authentisierung von Server und Client auf jeden Fall ein höheres Sicherheitsniveau erreicht wird. Weiterhin ist EAP-TLS als RFC vergleichsweise solide standardisiert. EAP-TLS wird in den Tests für WPA/WPA2-Zertifizierungen (siehe Kapitel 2.5) als Referenzmethode benutzt und kann für WLAN daher durchaus als eine der am meisten getesteten EAP-Methoden be-

zeichnet werden[4]. EAP-TLS wird von praktisch allen Supplicants gängiger Betriebssysteme genauso wie von externen kommerziellen und Open Source Supplicants unterstützt. Die meisten modernen RADIUS-Server unterstützen EAP-TLS. Da auch auf der Seite der Netzbetriebssysteme eine geeignete Unterstützung der Verwaltung der Nutzerdaten vorliegt, ist EAP-TLS allgemein für WLAN im Behörden- und im Unternehmensbereich eine zu empfehlende Authentisierungsmethode, wenn WPA- bzw. WPA2-Enterprise genutzt werden soll.

2.4.4 Ableitung der Sitzungsschlüssel

Über die genutzte EAP-Methode wird zwischen Supplicant und Authentication Server ein gemeinsamer geheimer Master-Schlüssel (Pairwise Master Key, PMK) vereinbart. Der PMK wird vom Authentication Server zum Authenticator (Access Point) übertragen. Der PMK hat eine Länge von 256 Bit.

Über EAPOL (siehe Kapitel 2.4.3) können anschließend die verwendeten Sitzungsschlüssel ausgehandelt werden. Dabei werden Schlüsselinformationen zum Supplicant übertragen (Group Temporal Key, GTK) und es wird ein gemeinsamer Schlüssel zwischen Supplicant und Authenticator abgeleitet (Pairwise Transient Key, PTK). Aus GTK und PTK werden dann die eigentlichen temporären Schlüssel für die Verfahren TKIP bzw. CCMP konstruiert. Die Länge dieser letztendlich verwendeten Schlüssel beträgt 128 Bit. Der GTK ist dabei die Grundlage für die Verschlüsselung von Broadcasts und Multicasts, während der PTK als Basis für die Verschlüsselung von Unicasts dient.

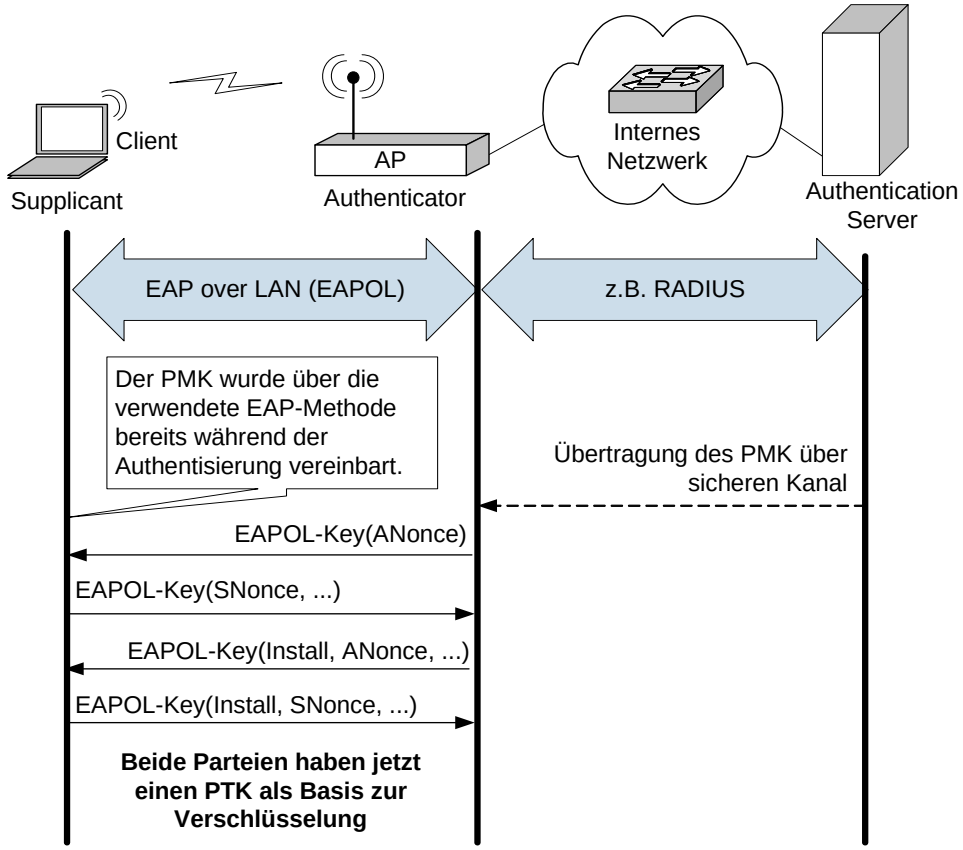


Abb. A-10: PTK-Schlüsselgenerierung über EAPOL Key Exchange

[4] Die Wi-Fi Alliance bietet seit April 2005 auch die Möglichkeit an, EAP-Methoden zu zertifizieren. Zu den Methoden, die zertifiziert werden können, gehören unter anderem auch EAP-TTLS und EAP-PEAP.

Die Master-Schlüssel können auch als Pre-Shared Keys (PSKs) manuell (WPA-Personal bzw. WPA-PSK) auf den Komponenten konfiguriert werden. Bei Verwendung von PSKs wird die EAP-Authentisierung nicht genutzt, EAPOL kommt aber für die Ableitung von transienten Schlüsseln (PTK, GTK) weiterhin zum Einsatz.

Dieser Austausch von Schlüsselinformationen geschieht durch die in Abb. A-10 gezeigte EAPOL-Key-Sequenz. Bei diesem so genannten 4-Way-Handshake werden insbesondere zwei Pseudozufallszahlen (ANonce für den Authenticator und SNonce für den Supplicant) über EAPOL ausgetauscht, die als sitzungsspezifische Parameter in die Funktion zur Ableitung der PTK einfließen. Dies ist für eine sichere WLAN-Kommunikation bei IEEE 802.11i erforderlich, um einen statischen Schlüssel wie bei WEP zu vermeiden.

Bei lang andauernden WLAN-Sitzungen ist es sinnvoll, den PMK „aufzufrischen“. Hierzu sieht IEEE 802.1X die Funktion der regelmäßigen Re-Authentisierung (Reauthentication) vor.

2.5 Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) ist ein im ersten Quartal 2003 veröffentlichter Standard der Wi-Fi Alliance (siehe [WPA04]), der auf einem Draft zu IEEE 802.11i basiert (siehe Abb. A-11) und aufwärtskompatibel zu IEEE 802.11i ist. Bereits seit Ende August 2003 ist WPA Bestandteil der Wi-Fi-Interoperabilitätstests.

WPA nutzt wie IEEE 802.11i TKIP und unterstützt somit die hierfür benötigten Erweiterungen, bietet aber noch nicht die Variante der AES-Verschlüsselung über CCMP. Es gibt zwei Varianten von WPA: WPA-Enterprise für größere WLAN-Installationen, das für die Authentisierung und Schlüsselverwaltung IEEE 802.1X mit RADIUS nutzt, und WPA-Personal für kleinere WLAN-Installationen und den SOHO-Bereich, das mit Pre-Shared Keys (PSK) operiert[5].

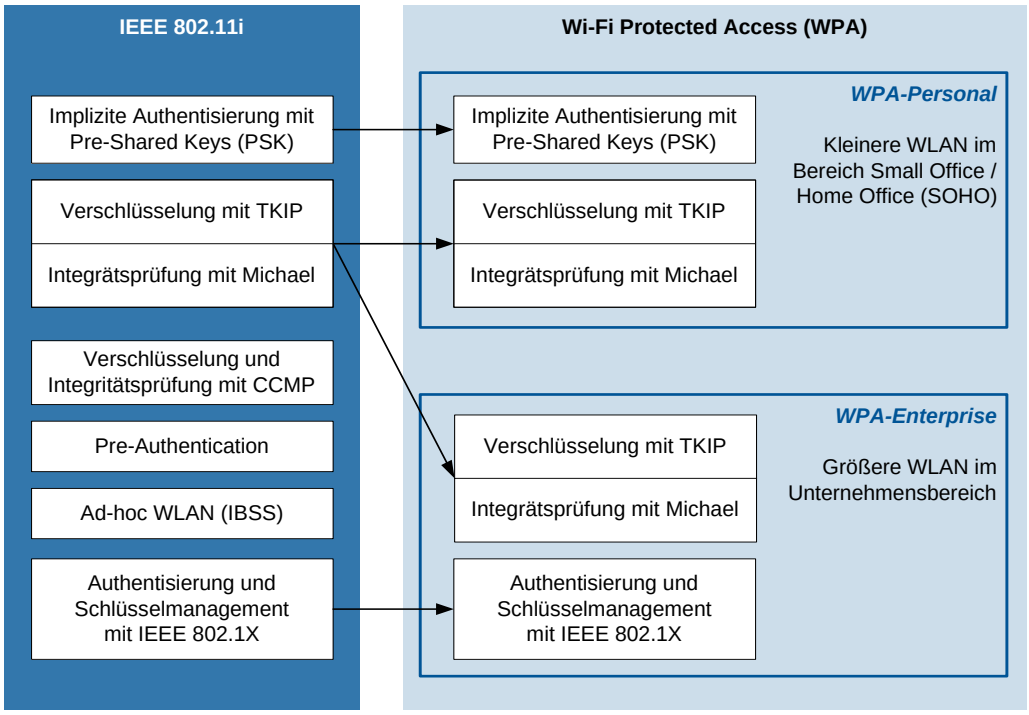


Abb. A-11: Zusammenhang zwischen WPA und IEEE 802.11i

5 WPA-Personal wird auch als WPA-PSK bezeichnet.

Im Jahr 2004 wurde WPA2, die Folgeversion von WPA, verabschiedet, und seit Sommer 2004 werden WLAN-Geräte nach WPA2 zertifiziert, wobei diese Zertifizierung bis September 2006 optional ist. WPA2 deckt alle zwingenden Anforderungen von IEEE 802.11i ab und unterstützt neben TKIP auch den AES-Modus CCMP, der allerdings nicht mehr abwärtskompatibel zu WEP ist. Analog zu WPA sind für WPA2 die beiden Profile WPA2-Enterprise und WPA2-Personal spezifiziert.

Eine genaue Prüfung von WPA durch die internationale Kryptoanalytiker-Gemeinde hat ergeben, dass bereits WPA bei einer geeigneten Konfiguration die bisher bekannten Schwachstellen von WEP behebt. Allerdings ist WPA2 mit der Nutzung von CCMP immer vorzuziehen, wenn keine Abwärtskompatibilität benötigt wird, weil hier mit AES ein moderneres Verschlüsselungsverfahren eingesetzt wird. Außerdem gestattet der Verzicht auf eine Abwärtskompatibilität ein einfacheres Design und damit eine geringere Anfälligkeit für Implementierungsfehler. Zudem kann durch den höheren Anteil an in Hardware realisierter Funktionen ein besserer Datendurchsatz erreicht werden.

Abschließend zeigt Tab. A–1 eine zusammenfassende Bewertung der Sicherheitselemente in IEEE 802.11i bzw. WPA und WPA2.

Funktion	Verfahren	Bewertung	Kommentar
Authentisierung	implizite Authentisierung durch Pre-Shared Key	**0**	Diese Bewertung gilt, sofern der Schlüssel zufällig gewählt ist bzw. aus einem Passwort hoher Komplexität mit einer Länge von mindestens 20 Zeichen erzeugt wird.
	IEEE 802.1X	**++**	Schlüsselmanagement und diverse Authentisierungmethoden werden unterstützt. Die verwendete Authentisierungmethode muss dem zu erreichenden Sicherheitsniveau angemessen gewählt sein. Nur für diesen Fall gilt die angegebene Bewertung.
Verschlüsselung (WPA)	TKIP	**+**	TKIP basiert auf WEP. Es erfolgt für jedes Paket eine kryptographische Erzeugung eines Schlüssels. Da TKIP in Software abläuft, kommt es zu Leistungseinbußen.
Integritätsprüfung (WPA)	Michael	**0**	DoS-Angriff ist möglich. Die Länge des MIC beträgt 64 Bit.
Verschlüsselung (WPA2)	CCMP	**++**	CCMP verwendet AES. AES erfordert entsprechende Hardware. Die verwendete Schlüssellänge beträgt 128 Bit. Nach dem Stand der Technik ist CCMP als sicheres Verfahren einzustufen.
Integritätsprüfung (WPA2)	CBC-MAC	**++**	Bestandteil von CCMP. Die Länge des MIC beträgt 64 Bit.
Legende: "++" = sehr gut, "+" = gut, "0" = akzeptabel, "-" = mangelhaft, "--" = ungenügend			

Tab. A–1: Bewertung der Elemente von IEEE 802.11i bzw. WPA und WPA2

3. Gefährdungen

Dieses Kapitel beschreibt typische Gefährdungen, denen ein WLAN ausgesetzt sein kann. Eine genauere Analyse der Gefährdungslage kann dem Teil 2 der Technischen Richtlinie Sicheres WLAN entnommen werden (siehe [TR-S-W2]).

3.1 Ausfall durch höhere Gewalt

Wie im kabelgebundenen LAN kann es auch im WLAN durch Überspannungen zum Ausfall von WLAN-Komponenten kommen. Außerdem sind Außeninstallationen von WLAN-Komponenten zur Versorgung von Außenbereichen (z.B. Antennen) durch Blitz und Witterungseinflüsse gefährdet.

3.2 Mangelhafte Planung

Planungsfehler stellen sich oft als besonders schwerwiegend heraus, da leicht flächendeckende Sicherheitslücken geschaffen werden können, deren Beseitigung mit hohen Kosten verbunden ist.

Beispiele sind:

- Durch eine mangelhafte Planung können sich z.B. Performance-Einbußen ergeben, die durch Störungen oder auch durch Funklöcher entstehen können. Im Außenbereich kann eine mangelhafte Planung die Gefährdung von WLAN-Komponenten durch Blitzschlag oder Witterungseinflüsse zur Folge haben.
- Erfolgt durch mangelhafte Planung am Übergabepunkt zwischen Distribution System und LAN keine geeignete Absicherung, kann zunächst die gesamte Broadcast-Domäne, in der sich der Access Point befindet, abgehört und die dadurch gewonnenen Informationen für einen Angriff auf das gesamte LAN genutzt werden. Dies erfordert allerdings eine Kompromittierung der Absicherung der Luftschnittstelle bzw. der Sicherheitseinstellungen auf dem Access Point.
- Sind Authentisierungsverfahren und Schutz der Authentisierungs-Informationen schlecht gewählt, kann dies ebenfalls zur Kompromittierung der internen LAN-Infrastruktur führen.

3.3 Fehlende Regelungen zur Nutzung von Frequenzen und unbeabsichtigte Störung durch Fremdsysteme

Ist die Nutzung des ISM-Bands bei 2,4 GHz nicht geregelt, und werden WLAN nach IEEE 802.11b bzw. IEEE 802.11g parallel zu anderen Funksystemen (wie z.B. Bluetooth[6], Bewegungsmeldern, Mikrowellenherden etc.) im selben Bereich genutzt, kann es zu signifikanten Störungen der Datenübertragung im WLAN kommen. Diese Störungen können auch durch einen anderen Nutzer (außerhalb der Behörde oder des Unternehmens) verursacht werden, der berechtigterweise ebenfalls im 2,4-GHz-Bereich operiert, und müssen dann hingenommen werden.

Für den 5-GHz-Bereich ist zu beachten, dass Radar-Anwendungen (z.B. von Einrichtungen der zivilen Luftfahrt und des Militärs) in diesem Frequenzband Primärnutzer sind und Vorrang vor WLAN-Anwendungen genießen.

---

[6] Mit Bluetooth 1.2 ist mit Adaptive Frequency Hopping (AFH) ein Mechanismus eingeführt worden, der die Koexistenz zwischen WLAN nach IEEE 802.11b bzw. IEEE 802.11g und Bluetooth verbessern soll. Bei manchen Bluetooth-Geräten kommt es aber trotz AFH noch zu signifikanten Störungen einer WLAN-Übertragung. Der Mischbetrieb zwischen Bluetooth und WLAN muss also bei Bedarf im Einzelfall getestet werden.

3.4 Unzureichende Regelungen zur Administration der WLAN-Infrastruktur

Aufgrund fehlender Regelungen zur Administration der WLAN-Infrastruktur kann es beispielsweise zu Fehlkonfigurationen der WLAN-Komponenten (z.B. Access Points) kommen. Probleme können sich auch ergeben, wenn es keine einheitliche Festlegung zur Dokumentation von Systemveränderungen gibt.

3.5 Fehlende Regelungen zur Überwachung der WLAN-Infrastruktur und zur Notfallbehandlung

Wurden hierzu keine Festlegungen getroffen und die entsprechenden finanziellen und personellen Ressourcen nicht bereitgestellt, werden Angriffe auf das WLAN unter Umständen nicht erkannt.

Sofern für den Betrieb des WLAN keine Festlegungen zur Notfallbehandlung erfolgt sind, kann es beispielsweise zu Datenabfluss oder zu Wurmattacken kommen, die gegebenenfalls bemerkt werden, gegen die aber Gegenmaßnahmen nicht zeitnah (innerhalb von Minuten) eingeleitet werden, da auf keine entsprechenden vorbereiteten Maßnahmenkataloge, geregelten Abläufe und Befugnisse zu notwendigen Eingriffen zurückgegriffen werden kann.

3.6 Sicherheitskritische Grundeinstellung

Im Auslieferungszustand sind die WLAN-Komponenten häufig so konfiguriert, dass keine oder nur einige der Sicherheitsmechanismen aktiviert sind. So kann schon ein einziger Access Point oder WLAN-Client, der nicht gemäß geltender Sicherheitsrichtlinie konfiguriert wurde, zu einer Kompromittierung des gesamten WLAN führen.

3.7 Fehlkonfiguration von WLAN-Komponenten

Mittlerweile bieten Access Points eine Vielzahl von Konfigurationseinstellungen, die insbesondere auch die Nutzung von Sicherheitsfunktionen betreffen. Werden hier falsche Einstellungen vorgenommen, ist entweder keine Kommunikation über den Access Point möglich oder die Kommunikation erfolgt ungeschützt bzw. mit einem zu geringen Schutzniveau, obwohl der Nutzer von einem vorhandenen Schutz ausgeht.

3.8 SSID Broadcast

Einige Access Points bieten die Möglichkeit, das Senden des SSID im Broadcast zu unterbinden, um das WLAN vor Unbefugten zu verstecken (oft als „Closed System“ bezeichnet). Dieser Schutz wirkt gegen diverse frei verfügbare Tools, jedoch kann mit einem WLAN-Protokoll-Analysator auch in diesem Falle der SSID aus anderen Management- und Steuersignalen ermittelt werden.

3.9 Manipulierbare MAC-Adressen

Die MAC-Adressen von WLAN-Stationen können relativ einfach abgehört werden und ein Angreifer kann durch Verwendung einer anderen MAC-Adresse eine fremde Identität vorspielen. MAC-Adressfilter, die in den Access Points zum Zweck des Zugriffsschutzes häufig unterstützt werden, sind daher leicht überwindbar.

3.10 Schwachstellen in WEP

Das Ziel mittels WEP Vertraulichkeit, Integrität und Authentizität im WLAN zu sichern, kann eindeutig als nicht erreicht eingestuft werden, denn WEP ist mittlerweile vollständig kompromittiert. Hierzu sei insbesondere auf die Arbeit von Fluhrer, Mantin und Shamir (siehe [FMS01]) hingewiesen, welche die Grundlage für die heute frei verfügbaren Angriffswerkzeuge auf WEP geschaffen hat. Diese Werkzeuge können mit einer guten Zuverlässigkeit den eigentlich geheimen WEP-Schlüssel aus aufgezeichneten verschlüsselten Paketen zurückrechnen. Es genügt schon oft die rein passive Aufzeichnung von etwa 75.000 Paketen (entspricht typischerweise ca. 100 MByte Daten), die beispielsweise bei der Übertragung von Daten zu einem WLAN-Drucker schnell erreicht werden.

Weiterhin kann durch so genannte Re-Injection-Angriffe das benötigte Verkehrsvolumen durch eine aktive Aktion des Angreifers aus wenigen aufgezeichneten Paketen künstlich erzeugt werden. Dabei wird zunächst versucht, aus den verschlüsselten Übertragungen spezielle Pakete z.B. durch einen Längenvergleich zu erraten (etwa einen ARP-Request[7]) und aufzuzeichnen. Dieser aufgezeichnete Verkehr wird wieder in das WLAN „injiziert“, der zugrunde liegende Protokollmechanismus wird erneut angestoßen, und Stationen im WLAN antworten (etwa mit einem ARP-Response).

Es existieren noch weitere Schwächen in WEP. Beispielsweise gestattet es der in WEP verwendete CRC-Mechanismus, dass Pakete „fast beliebig“ gefälscht werden können, ohne dass die Integritätsprüfung dies bemerkt.

Für die Absicherung eines WLAN ist WEP allein als ungenügend einzustufen. Ein WLAN nach IEEE 802.11 sollte immer mit zusätzlichen über den ursprünglichen Standard von 1999 hinausgehenden Mitteln abgesichert werden.

3.11 Probleme bei Mischbetrieb von WPA und WEP z.B. durch Migration

In Folge einer Migration muss ein Access Point oft im Kompatibilitätsbetrieb sowohl mit WPA als auch mit WEP betrieben werden, da einige WLAN-Clients schon auf WPA/WPA2 umgestellt sind, andere WLAN-Clients aber nur WEP unterstützen. In diesem Fall kommunizieren zwar prinzipiell alle WPA-fähigen Clients mit dem Access Point über WPA, es gibt jedoch einige Einschränkungen: Zum einen werden Multicast- und Broadcast-Nachrichten grundsätzlich mit WEP verschlüsselt, zum anderen sind nicht-WPA-fähige Clients in der Regel auch nicht 802.1X kompatibel. Dadurch kann die Authentisierung und der dynamische Schlüsselwechsel umgangen werden.

Hier ist (zumindest für die Dauer der Migration) eine Trennung der verschiedenen Nutzergruppen vorzunehmen, die es gestattet, zwei Sicherheitsmechanismen parallel zu verwenden, ohne dass es zu einer nicht akzeptablen Schwächung des stärkeren Sicherheitsmechanismus kommt.

3.12 Schwachstellen bei passwortbasierten Authentisierungsverfahren in WPA, WPA2 bzw. IEEE 802.11i

Werden für die Authentisierung in WPA, WPA2 bzw. IEEE 802.11i passwortbasierte Mechanismen genutzt, wie z.B. Pre-Shared Keys (PSKs) oder EAP-PEAP unter Verwendung von EAP-MSCHAPv2, ist eine Wörterbuch-Attacke möglich. Die Verwendung von WPA-Personal, bzw. WPA2-Personal gestattet sogar eine Offline-Attacke, bei der es genügt, auf der Luftschnittstelle die ersten zwei Pakete des in Kapitel 2.4.4 vorgestellten 4-Way-Handshake aufzuzeichnen. Anschließend kann man ohne Verbindung zum WLAN mögliche Passworte probieren. Allgemein spielt hierbei spielt natürlich die Komplexität der Passworte eine entscheidende Rolle.

---

[7] Das Address Resolution Protocol (ARP) dient zur Ermittlung der MAC-Adresse, an die ein IP-Paket in einer Broadcast-Domäne geschickt werden soll, d.h. der Abbildung einer IP-Adresse auf eine MAC-Adresse.

3.13 Bedrohung der lokalen Daten

Auf den Client-Rechnern entstehen durch die Teilnahme eines Clients am WLAN zusätzliche Bedrohungen für die lokalen Daten. Lokale Datei- bzw. Druckerfreigaben im Betriebssystem erlauben in der Grundeinstellung meist auch über das WLAN Zugriffe auf diese Ressourcen. Ebenso sind bei eingeschaltetem WLAN Angriffe auf den Rechner zu befürchten, die Schwachstellen des verwendeten Betriebssystems ausnutzen. Diese Gefahren bestehen insbesondere bei der Nutzung von Hotspots und in Ad-hoc-Netzwerken.

3.14 Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen der WLAN-Komponenten breiten sich auch über räumliche Grenzen des WLAN-Nutzungsbereichs aus. Dabei kann auch in nicht vom WLAN-Betreiber kontrollierten Bereichen ein Empfang möglich sein. Je nach Umgebungsbedingungen und Leistungsfähigkeit der verwendeten Empfangsgeräte (z.B. Richtantennen) besteht auch hier noch eine konkrete Abhörgefahr.

3.15 Abhören der WLAN-Kommunikation

Da es sich bei Funk um ein Shared Medium handelt, können die über das WLAN übertragenen Daten leicht aufgezeichnet werden. Dies ist mit frei im Internet erhältlicher Software möglich, welche die WLAN-Karte des Angreifers in den Promiscuous Mode schaltet. Aus den aufgezeichneten Daten können auch bei verschlüsselter Datenübertragung zumindest WLAN-Parameter wie SSID, genutzter Funkkanal und eingesetztes Verschlüsselungsverfahren sowie die MAC-Adressen der Kommunikationspartner im WLAN gewonnen werden.

Bei nicht genutzter oder schwacher Verschlüsselung können darüber hinaus auch die IP-Adressen und genutzten Ports der Kommunikationspartner sowie gegebenenfalls übertragene Nutzdaten abgehört werden, sofern diese nicht über IP-VPN, SSL oder Verschlüsselung auf Applikationsebene geschützt sind.

3.16 Bedrohung der Verfügbarkeit

WLANs übertragen Informationen mittels elektromagnetischer Funkwellen. Strahlen andere elektromagnetische Quellen im gleichen Frequenzspektrum Energie ab, können diese die WLAN-Kommunikation stören und im Extremfall den Betrieb des WLAN verhindern. Dies kann unbeabsichtigt durch andere technische Systeme (z.B. Bluetooth-Geräte, andere WLANs, Mikrowellenöfen, medizinische Geräte, Funk-Überwachungskameras, etc.) oder aber durch absichtliches Betreiben einer Störquelle (Jammer) als so genannter Denial-of-Service-Angriff (DoS-Angriff) erfolgen. Eine solche Störquelle kann sich bei ausreichender Sendeleistung auch außerhalb des Geländes befinden, auf dem das WLAN genutzt wird.

Darüber hinaus sind DoS-Angriffe auch möglich durch wiederholtes Senden bestimmter Steuer- und Managementsignale, z.B. Deauthentication- bzw. Disassociation-Attacken.

Zusammengefasst ist zu betonen, dass in WLAN Angriffe vom Typ DoS nie vermieden werden können, denn ein Störsignal kann wie eben geschildert einfach, effektiv und jederzeit erzeugt werden.

3.17 Unerlaubte Mitnutzung des WLAN

Eine WLAN-Installation (insbesondere im SOHO-Bereich), über die ein Internet-Zugang ermöglicht wird, ist der Gefahr der unerlaubten Mitnutzung ausgesetzt, wenn keine hinreichenden Authentisierungsmechanismen für den Zugang zum WLAN implementiert sind. Diese unerlaubte Mitnutzung

führt einerseits zur Reduzierung der zur Verfügung stehenden Bandbreite und Erhöhung der Antwortzeiten für autorisierte WLAN-Nutzer sowie andererseits zur unerlaubten und unbezahlten Mitnutzung des Internetzugangs. Bei der Mitnutzung des Internetzugangs ist natürlich auch ein Missbrauch nicht ausgeschlossen, z.B. durch Angriffe auf andere Systeme im Internet, die Verbreitung von Spam-Mails oder das Bereitstellen bzw. Laden von strafrechtlich relevanten Inhalten.

3.18 Diebstahl eines Access Points

Access Points stellen einen gewissen Wert dar, der zum Diebstahl verleiten kann.

Dabei ist der monetäre Wert der Access Points beinahe nachrangig: Der Dieb kann auch über den nun dauerhaften und unbeschränkten physikalischen Zugriff unbehindert und unbemerkt Basisinformationen für eine weitere Kompromittierung erlangen, z.B. auf dem Wege des Auslesens eines „Shared Secrets“ zur RADIUS-Authentisierung oder des verwendeten Schlüssels für WEP, WPA-Personal bzw. WPA2-Personal.

3.19 Vortäuschung eines gültigen Access Points

Durch Poisoning- / Spoofing-Methoden oder die Man-in-the-Middle-Technik täuscht der Angreifer eine falsche Identität vor bzw. lenkt den Netzwerkverkehr zu seinen eigenen Systemen um und kann so die Kommunikation belauschen und kontrollieren.

3.20 Schwachstellen beim administrativen Zugriff auf Access Points

Wird ein Access Point über die Funkschnittstelle über Klartext-Protokolle wie z.B. Telnet, HTTP oder SNMPv1/v2 administriert, können die über das WLAN übertragenen Administrations-Passwörter mitgelesen werden. Mit dieser Information kann ein Angreifer den Access Point umkonfigurieren.

3.21 Ungeschützte Übertragung von Management-Paketen

Ein generelles Problem besteht bei der WLAN-Kommunikation darin, dass die Management-Pakete zur Steuerung der Layer-2-Kommunikation ungesichert übertragen werden, d.h. hier fehlt der Schutz der Vertraulichkeit, Integrität und Authentizität. Dadurch ist es beispielsweise möglich, so genannte Deauthentication-Attacken über frei verfügbare Tools durchzuführen. Diese Attacken können sowohl in Richtung Access Point als auch in Richtung WLAN-Client erfolgen. Aufgrund dieser ungesicherten Management-Pakete besteht die Gefahr von DoS-Angriffen[8].

3.22 Ungeschützter LAN-Zugang am Access Point

Der kabelbasierte LAN-Zugang, über den ein Access Point an die Infrastruktur angeschlossen ist, stellt ein besonderes Risiko dar. Wenn ein Access Point sichtbar und ohne physischen Schutz montiert ist (speziell in einem öffentlich zugänglichen Bereich), kann ein Angreifer versuchen, über den LAN-Zugang des Access Points einen Zugriff auf Ressourcen der LAN-Infrastruktur zu erreichen.

Während der Zugang über die Luftschnittstelle mit IEEE 802.11i bzw. WPA und WPA2 geeignet abgesichert werden kann, besteht oft kein Schutz auf der Ethernet-Schnittstelle zum LAN.

---

8 Diese Schwachstelle soll durch die kommende Ergänzung IEEE 802.11w beseitigt werden.

Sofern in dieser Situation das Distribution System keine separate Infrastruktur ist, die durch eine Sicherheitsschleuse (Firewall oder zumindest Paketfilter) von der LAN-Infrastruktur getrennt ist, hat der Angreifer im schlimmsten Fall einen Zugriff auf die gesamte über das LAN erreichbare Infrastruktur.

Diese Gefährdung besteht insbesondere bei der Verwendung von Thin Access Points und Wireless Switches, denn der wesentliche Vorteil dieser Systeme ist ja gerade die Verwendung einer bestehenden LAN-Infrastruktur als Trägernetzwerk für ein WLAN. Zwar kann die Kommunikation zwischen Thin Access Point und Wireless Switch meist geschützt werden, dies ist aber nicht das einzige Angriffsziel. Über den Ethernet-Port, an den ein Thin Access Point angeschlossen ist, können eben nicht nur Wireless Switches erreicht werden, sondern oft auch andere Elemente der IT-Infrastruktur.

3.23 Erstellung von Bewegungsprofilen

Da die MAC-Adresse eines WLAN-Adapters, welche (sofern sie nicht explizit geändert wurde) die Hardware-Adresse der WLAN-Karte ist, bei jeder Datenübertragung mit versendet wird, ist ein eindeutiger Bezug zwischen MAC-Adresse des Funk-Clients, Ort und Uhrzeit der Datenübertragung herstellbar. Auf diese Weise können Bewegungsprofile über mobile Nutzer in einem Firmen- oder Behörden-WLAN erstellt werden[9].

4. Schutzmaßnahmen

Zur Erhöhung der Sicherheit beim Einsatz von WLAN-Komponenten sind abhängig vom Einsatzszenario und dem Schutzbedarf der Informationen mehrere Maßnahmen erforderlich. Die Maßnahmen sind in drei Kategorien unterteilt:

A. Konfiguration und Administration der Funkkomponenten

B. Zusätzliche technische Maßnahmen

C. Organisatorische Maßnahmen

Maßnahmen, die bei einem hohen Schutzbedarf **zusätzlich** ergriffen werden sollten, sind in Anlehnung an das IT-Grundschutzhandbuch im Folgenden mit dem Kürzel „HS“ gekennzeichnet. Diese Maßnahmen können aber durchaus im Einzelfall bereits bei einem mittleren Schutzbedarf in Betracht gezogen werden.

Eine detaillierte Betrachtung der Erstellung eines Maßnahmenkatalogs als Bestandteil eines umfassenden WLAN-Sicherheitskonzepts kann dem Teil 2 der Technischen Richtlinie Sicheres WLAN entnommen werden (siehe [TR-S-W2]).

4.1 Konfiguration und Administration der Funkkomponenten

Die im Folgenden beschriebenen Maßnahmen betreffen Access Points, WLAN Clients und die Übertragung auf der Funkstrecke.

A1: Sorgfältige Planung

A1.1 Festlegung eines Frequenzstandards und der Übertragungstechnik

Im Rahmen der WLAN-Planung ist zunächst eine Ist-Aufnahme durchzuführen, welche der von der Behörde bzw. dem Unternehmen betriebenen Systeme in das ISM-Band bei

[9] Dies ist speziell im Zusammenhang mit der Funktion der Lokalisierung von fremden WLAN Clients und Access Points zu sehen, die als Bestandteil des WLAN-Managements zunächst zum Schutz des WLAN beiträgt. Allerdings eignen sich die dabei verwendeten Techniken grundsätzlich auch für die Erstellung von Bewegungsprofilen von Clients im eigenen WLAN.

2,4 GHz sowie in das 5 GHz-Band abstrahlen. Nachdem diese Ist-Aufnahme abgeschlossen wurde, kann in einem Frequenzstandard festgelegt werden, in welchen Einsatzumgebungen solche Systeme erlaubt sind. Insbesondere wird dadurch eine „Eigenstörung“ des WLAN durch von der Behörde bzw. dem Unternehmen betriebene Systeme vermieden.

Des Weiteren muss in diesem Standard festgelegt werden, in welchen Bereichen (Gebäude, Flure, Hallen, Campus) der Behörde bzw. des Unternehmens die WLAN-Nutzung erlaubt ist und welches WLAN-System nach welchem Standard zum Einsatz kommen soll.

A1.2 Untersuchung der Einsatzumgebung auf mögliche Störungen des WLAN auf Funkebene (HS)

Sofern hohe Anforderungen an die maximal zulässige Störung der Funkübertragung im WLAN gestellt werden, sollten über einen Spektrumanalysator und über WLAN-Messprogramme mögliche Störquellen ermittelt und entsprechende Abhilfemaßnahmen festgelegt werden. Die Ergebnisse sind zu protokollieren.

A1.3 Festlegungen zum Aufbau des Distribution System

Generell ist eine Trennung der Verkehrsflüsse zwischen WLAN-Infrastruktur und kabelbasiertem LAN vorzunehmen.

Dabei ist zunächst die grundsätzliche Entscheidung zu treffen, ob ein Aufbau mit Thin Access Points und Wireless Switches geschehen soll oder, ob ein klassisches WLAN-Design mit intelligenten Access Points erfolgt.[10]

Weiterhin muss festgelegt werden, ob aus Sicherheitsgründen eine eigene Infrastruktur aufgebaut bzw. geschaltet wird und damit eine physikalische Trennung zur Infrastruktur des internen LAN ermöglicht wird. Andernfalls erfolgt eine logische Trennung zwischen WLAN und LAN durch die Konfiguration von VLAN auf den Access Switches des kabelbasierten LAN bzw. durch den Tunnelmechanismus zwischen Thin Access Points und Wireless Switches.

A1.4 Planung der zu verwendenden WLAN-Authentisierungsverfahren und deren Nutzung

Zur Authentisierung sollten nur als allgemein sicher anerkannte Verfahren eingesetzt werden. Zu empfehlen ist bei größeren WLAN die Verwendung von IEEE 802.1X im Rahmen von IEEE 802.11i bzw. von den Varianten WPA-Enterprise und WPA2-Enterprise. Als Authentisierungsverfahren kommt insbesondere EAP-TLS in Frage, da hier eine gegenseitige zertifikatsbasierte Authentisierung von Supplicant (WLAN Client) und Authentication Server durchgeführt wird. Andere Verfahren, die bei entsprechend geringerem Schutzbedarf verwendet werden können sind EAP-PEAP und EAP-TTLS.

A1.5 Erstellung eines Anforderungskatalogs für die WLAN-Beschaffung

Anhand der Ergebnisse der WLAN-Planung ist ein Anforderungskatalog zu erstellen. Darin sind auf Basis der laut Schutzbedarfsfeststellung umzusetzenden Sicherheitsmaßnahmen entsprechende Anforderungen an die von den WLAN-Komponenten zu leistenden Sicherheitsmerkmale beschrieben. Neben Anforderungen an Access Points und WLAN-Clients sind darin auch Anforderungen an ein WLAN-Management zu spezifizieren.

A1.6 Planung und Prüfung des Zusammenwirkens aller WLAN-Komponenten und der zugehörigen Infrastruktur

---

10 Der Einsatz von Wireless Switches gestattet den Aufbau der WLAN-Infrastruktur weitestgehend unabhängig von der Architektur des kabelbasierten LAN. Für den klassischen Aufbau mit intelligenten Access Points sind spezielle Rahmenbedingungen zu berücksichtigen (insbesondere hinsichtlich der Layer-3-Strukturierung des Netzes).

Im Rahmen der Beschaffung sollten Kriterien aufgestellt werden, welche die Kompatibilität und das korrekte Zusammenwirken aller WLAN-Komponenten überprüfen (siehe hierzu auch Teil 3 der Technischen Richtlinie Sicheres WLAN, siehe [TR-S-W3]). Bei der Beschaffung einer größeren WLAN-Installation sollten im Rahmen der Ausschreibung entsprechende Teststellungen gefordert werden. Mit Hilfe eines Prüfkatalogs kann die Erfüllung der technischen Anforderungen evaluiert werden.

A2: Schutzmaßnahmen aktivieren

A2.1 Verschlüsselung, Integritätsschutz und Authentisierung auf der Luftschnittstelle

Falls möglich, sollte Verschlüsselung und Integritätsschutz mit CCMP (gemäß WPA2 bzw. IEEE 802.11i) aktiviert werden, anderenfalls müssen zumindest TKIP-Verschlüsselung und Michael-Integritätsschutz (gemäß WPA bzw. IEEE 802.11i) genutzt werden.

In SOHO-WLAN und bei der Verwendung von WLAN zur LAN-Kopplung können Pre-Shared Keys (WPA2-Personal bzw. WPA-Personal) eingesetzt werden, da nur eine geringe Anzahl von WLAN-Stationen zu verwalten ist.

In allen anderen WLAN-Installationen sollte WPA2-Enterprise bzw. WPA-Enterprise mit Authentisierung und Schlüsselverwaltung über IEEE 802.1X eingesetzt werden. Hier ist dann als Authentisierungsmethode vorzugsweise EAP-TLS, mindestens aber EAP-TTLS oder EAP-PEAP zu verwenden.

Diese Anforderungen gelten unabhängig von den verwendeten WLAN-Endgeräten und WLAN-Anwendungen.

A2.2 Identifikations- und Passwortvorgaben ändern

- Der Standard SSID sollte an Access Points und bei allen Clients geändert werden. Dabei sollte der gewählte SSID keine Rückschlüsse auf die Firma bzw. die Behörde und auf das Netzwerk zulassen.
- Das Standard Passwort zur Konfiguration der Access Points muss geändert werden. Es ist als Mindestanforderung ein komplexes Kennwort zu wählen.

A2.3 SSID Broadcast am Access Point abschalten - falls technisch möglich

In der Default-Konfiguration eines Access Point wird in den periodischen Übertragungen der so genannten Beacon Frames der SSID übertragen. Viele Hersteller gestatten es, diese Übertragung zu unterdrücken. Nach Möglichkeit sollte diese Einstellung der SSID-Unterdrückung konfiguriert werden. Dies kann allerdings für manche Client-Systeme zu Beeinträchtigungen in der Netzauswahl führen.

A2.4 Assoziation via Broadcast SSID

Die Assoziation via Broadcast SSID muss am Access Point deaktiviert werden, damit der Client explizit den gewünschten SSID bei der Assoziierung angeben muss.

A2.5 MAC Adress-Filterung

Die Filterung von MAC-Adressen (MAC-Adress-Authentisierung) kann am Access Point eingeschaltet werden, sofern der Aufwand akzeptabel ist. Diese Maßnahme ist für den SOHO-Bereich sinnvoll.

A3: Schlüssel und Zugangspassworte von hoher Komplexität nutzen

Schlüssel und Zugangspassworte sollten entsprechend anerkannter Passwortgestaltungsregeln (z.B. gemäß [GSHB]) so gewählt werden, dass sie einen möglichst wirksamen Schutz gegen Angreifer bieten. Dazu gehört auch der regelmäßige Wechsel.

A4: Im Fall der Nutzung von Pre-Shared Keys (PSKs) den PSK regelmäßig wechseln

Der PSK sollte regelmäßig gewechselt werden (etwa alle drei bis sechs Monate). Außerdem sollte er möglichst zufällig gewählt oder aus einem Passwort hoher Komplexität mit mindestens 20 Zeichen gebildet werden. Keinesfalls dürfen Passworte aus bekannten, in Wörterbüchern vorhandenen, Zeichenkombinationen bestehen.

A5: Aufstellort und Antennencharakteristik der Access Points optimieren

Aufstellort und Antennencharakteristik der Access Points sollten so gewählt werden, dass möglichst nur das gewünschte Gebiet funktechnisch versorgt wird. Dabei ist zu beachten, dass sich die Funkwellen sowohl horizontal als auch vertikal ausbreiten.
Außerdem sollten die Access Points zugriffssicher (z.B. in Doppelböden, Zwischendecken oder Metallgehäusen) montiert werden, um Manipulationen direkt am Access Point bzw. am Ethernet-Anschluss zum LAN zu verhindern. Dies ist besonders wichtig, wenn keine physikalische Trennung zwischen WLAN Distribution System und dem internen LAN vorgenommen wird (wie es oft bei einem Aufbau mit Thin Access Points und Wireless Switches der Fall ist).
Die Außeninstallation von Access Points ist nach Möglichkeit zu vermeiden. Bei einer Antennenmontage im Außenbereich ist auf geeigneten Schutz gegen Blitzschlag und Witterungseinflüsse zu achten.

A6: Sendeleistung an den Access Points optimieren

Die Sendeleistung an den Access Points sollte - falls technisch möglich - reduziert werden, damit nach Möglichkeit nur das gewünschte Gebiet funktechnisch versorgt wird. Hierbei ist zu beachten, dass zur Erzielung der maximalen Datenübertragungsrate eine bestimmte Güte des Signals erforderlich ist.

A7: Regelmäßiges Einspielen von Firmware-Upgrades / Software-Updates auf den Access Points

Die Verfügbarkeit von Firmware-Upgrades für die WLAN-Komponenten sowie von Updates und Patches für die Software der Access Points und zugehörige Gerätetreiber der WLAN-Clients sollte regelmäßig überprüft werden. Neue Firmware- bzw. Software-Versionen oder Patches sollten allerdings erst nach einem angemessenen Test eingespielt werden, um den reibungslosen Betrieb im WLAN nicht zu gefährden. Hierbei ist außerdem zu beachten, dass Upgrades / Updates oft nur greifen, wenn sie auf allen beteiligten WLAN-Komponenten eingespielt werden.

A8: Konfiguration der Access Points nur über sichere Kanäle

Die Konfiguration und Administration der Access Points sollte nur über sichere Kanäle erfolgen, d.h. der administrative Zugriff über die Luftschnittstelle ist, soweit technisch möglich, zu deaktivieren.
Weiterhin sollten unsichere Administrationszugänge wie z.B. Telnet, SSHv1 und HTTP möglichst abgeschaltet werden. Ein administrativer Zugriff muss in jedem Fall über eine verschlüsselte Verbindung erfolgen, z.B. über HTTPS oder SSHv2.
Der physische Zugriff auf die Access Points sollte nur autorisierten Personen möglich sein.

A9: WLAN-Komponenten nur bei Gebrauch einschalten

Bei Nichtbenutzung der WLAN-Komponenten sollte deren Funktion deaktiviert werden. Dies gilt gleichermaßen für Access Points und Clients, bei letzteren insbesondere auch für den Ad-Hoc-Modus. Diese Maßnahme ist oft für SOHO-WLAN sinnvoll.

Zwischenfazit

Durch korrekte Konfiguration und Administration der Funkkomponenten des WLAN können viele Angriffe abgewehrt werden, die mit freiverfügbaren Tools durchführbar sind. Dadurch wird Schutz gegen unbeabsichtigtes Einloggen in ein WLAN und gegen Mithören des WLAN-Datenverkehrs erreicht. Die Verfügbarkeit des Systems kann mit diesen Maßnahmen gegebenenfalls erhöht werden, bleibt aber dennoch leicht angreifbar.

Zum Schutz von sensiblen Daten müssen mindestens Verschlüsselung und Integritätsprüfung mit TKIP und Michael (gemäß WPA bzw. IEEE 802.11i) oder besser CCMP (gemäß WPA2 bzw. IEEE 802.11i) genutzt werden. Eine Absicherung allein durch WEP reicht unter keinen Umständen aus. Bei größeren WLAN-Installationen ist eine geeignete Authentisierung mit zentraler Schlüsselverwaltung essentiell. Dazu wird IEEE 802.1X verwendet. Bei kleineren WLAN-Installationen im SOHO-Bereich und bei der LAN-Kopplung über WLAN können Pre-Shared Keys eingesetzt werden.

In Behörden- und Firmennetzen mit einer größeren Anzahl von Benutzern sind einige Maßnahmen (z.B. A2.5 und A4) nicht im erforderlichen Umfang praktikabel.

4.2 Zusätzliche technische Maßnahmen

Zur Erhöhung der Sicherheit können folgende zusätzliche technische Maßnahmen eingesetzt werden.

B1: Verwendung eines VPN zur Absicherung des WLAN (HS)

Genauso wie der Remote Access eines Clients über das Internet auf die eigene Infrastruktur mit einem Virtual Private Network (VPN) geeignet abgesichert werden kann, ist es möglich, die Kommunikation über ein WLAN zu schützen. Dies ist allerdings bei Nutzung von WPA2 oder zumindest WPA nur bei hohem Schutzbedarf nötig.
Grundsätzlich kann sowohl ein IP-VPN als auch ein SSL-VPN genutzt werden, allerdings ist im Fall eines WLAN ein IP-VPN vorzuziehen, da hier die gesamte über das VPN-Gateway abgewickelte Kommunikation geschützt ist. Übliche SSL-VPN schützen hingegen „nur“ die Kommunikation ausgewählter Applikationen.
Grundidee ist der Abschluss des Distribution Systems durch ein VPN-Gateway. Das WLAN bildet das unsichere Transportnetz, über das durch einen entsprechend verschlüsselten Tunnel zwischen Client und VPN-Gateway ein gesicherter Kommunikationskanal etabliert werden kann. Die Kommunikation über das WLAN hinaus mit der weiteren Infrastruktur geschieht ausschließlich über das VPN-Gateway. Der Aufbau des Tunnels muss dabei an eine geeignet starke Authentisierung der Kommunikationspartner geknüpft sein.

B2: Abschottung des drahtgebundenen Firmen-/Behördennetzes durch Firewall und Intrusion Detection System bzw. Intrusion Prevention System (HS)

Das drahtgebundene Firmen-/Behördennetz sollte durch eine Firewall gegen die WLAN-Clients (und allgemein gegen Zugriffe auf Access-Point-Ebene) abgeschottet werden. Hierzu kann das Firewall-System auch durch ein Intrusion Detection System (IDS) bzw. ein Intrusion Prevention System (IPS) ergänzt werden. Für den Einsatz von Firewalls und IDS/IPS müssen insbesondere auch Festlegungen zum Logging und zur Auswertung von Protokolldateien, zur Definition von Sicherheitsvorfällen und zu entsprechenden Reaktionen beim Eintreten eines solchen Sicherheitsvorfalls spezifiziert werden.

B3: Überwachung der Luftschnittstelle des WLAN durch ein Wireless Intrusion Detection System (HS)

Mittlerweile sind neben leitungsgebundenen IDS auch spezielle funkbasierte IDS auf dem Markt verfügbar (so genannte Wireless IDS), die mit Funksensoren oder mit den produktiv genutzten Access Points das Frequenzspektrum des WLAN überwachen und sicherheitsrelevante Anomalien (z.B. fremde bzw. unbekannte Access Points und Clients) entdecken und melden können. In bestimmten Szenarien ist der Einsatz solcher Systeme als Alternative bzw. Ergänzung zu leitungsgebundenen IDS empfehlenswert.
Hierfür ist eine sorgfältige Planung erforderlich. Bei der Überwachung des WLAN durch Funksensoren sind Anzahl und Aufstellungsort der Funksensoren zu planen. Bei der Verwendung der produktiven Access Points muss beachtet werden, dass die Überwachungsfunktion auf den Access Points zu Leistungseinbußen führen kann. Weiterhin müssen Festlegungen zum Logging, zur Definition von Sicherheitsvorfällen und zur entsprechenden Reaktionen beim Eintreten eines solchen Sicherheitsvorfalls getroffen werden.

B4: Schutz auf Anwendungs- und Server-Ebene

Sicherheitsmaßnahmen auf Anwendungs- und Server-Ebene sind insbesondere erforderlich, wenn im Rahmen einer Migration Client-Altlasten im WLAN eingesetzt werden müssen, die nicht gemäß A2.1 abgesichert werden können. Außerdem kommen die folgenden Maßnahmen zur Absicherung bei einem hohen Schutzbedarf in Frage:

Auf Anwendungsebene kann eine Authentisierung und eine Ende-zu-Ende-Verschlüsselung vorgenommen werden, sofern diese Funktionen von der Anwendung bzw. dem Client- und dem Server-System unterstützt werden. Die Anforderungen an die Güte der eingesetzten Verfahren unterscheidet sich nicht von der Absicherung der Luftschnittstelle mit IEEE 802.11i oder VPN (siehe A2.1 bzw. B1). Ein Beispiel in diesem Zusammenhang ist die Absicherung der Übertragung von VoIP über WLAN. Mechanismen hierzu werden in der Studie VoIPSEC des BSI behandelt (siehe [BSI05], etwa die Ende-zu-Ende-Absicherung der Übertragung von VoIP über WLAN mit dem Secure Realtime Transmission Protocol (SRTP).

B5: Einsatz eines zentralen WLAN-Management-Systems

Mit Hilfe eines zentralen WLAN-Management-Systems (gegebenenfalls auch WLAN-Management-Modul zu einem bereits eingesetzten Netzwerk-Management-System) sollten die folgenden Funktionen ermöglicht werden:

- Allgemeine Alarm- und Fehlerbehandlung im WLAN mit Schwellwertüberwachung, Auslösung von Maßnahmen, Auswertungen und Statistiken
- Erkennung und Lokalisierung von Fremdgeräten, insbesondere von fremden (rogue) Access Points und von Störsendern[11]
- Durchführung von Site Surveys
- Überwachung der Konfiguration von WLAN-Netzelementen
- Überwachung der Verfügbarkeit der Authentisierungs-Server
- Gegebenenfalls Wireless IDS zur Überwachung der Luftschnittstelle

Hierbei ist auch eine Spezifikation der Reaktion auf das Eintreten eines Sicherheitsvorfalls zu berücksichtigen.

B6: Absicherung der Clients

Insbesondere bei mobilen Clients, die sich in verschiedene WLANs einbuchen können, sollten weitere lokale Schutzmaßnahmen implementiert werden, wie z.B.: Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, restriktive Browser-Konfiguration, lokale Verschlüsselung etc. (siehe IT-Grundschutzhandbuch [GSHB], insbesondere Bausteine B 3.201 „Allgemeiner Client“, B 3.203 „Laptop“, B 3.208 „Internet-PC“, B 3.405 „PDA“ und B 4.4 „Remote Access Dienste“). Ein WLAN-Client sollte in diesem Sinne während der WLAN-Kommunikation keine weitere Netzverbindung aufbauen und auf der WLAN-Verbindung keine Netzwerk-Dienste als Server erbringen.
WLAN-Clients, die Daten mit hohem Schutzbedarf verarbeiten, sollten nicht in unsicheren Umgebungen betrieben werden, d.h. sie sollten nur in WLANs eingesetzt werden, die vertrauenswürdig sind bzw. vollständig unter eigener Kontrolle betrieben werden und einem hohen Schutzniveau genügen.

4.3 Organisatorische Maßnahmen

Diese nichttechnischen Maßnahmen dienen, in Kombination mit den Maßnahmen A und B, der Anhebung des Sicherheitsniveaus.

---

[11] Die Lokalisierung von Fremdgeräten gewinnt mit steigender WLAN-Flächendeckung an Bedeutung. Inzwischen sind erste Produkte verfügbar, die eine Lokalisierung von fremden WLAN-Geräten gestatten. Allerdings ist noch kein Standard für eine Lokalisierungsfunktion im WLAN in Sicht. Störsender stellen eine spezielle Bedrohung dar, denn sie sind oft nur durch einen Leistungseinbruch im WLAN detektierbar und können nur schwer (wenn überhaupt) mit WLAN-Mitteln lokalisiert werden, da sie nicht notwendig mit WLAN-Technik arbeiten müssen.

C1: Ermittlung des Schutzbedarfs der über das WLAN übertragenen Daten

Hierzu hat in einem WLAN-Konzept zunächst eine Erhebung der im WLAN übertragenen oder darüber erreichbaren Daten und Applikationen zu erfolgen (siehe auch [TR-S-WLAN]). Das Ergebnis der Schutzbedarfsfeststellung sollte in Form einer so genannten Datenschutzmatrix beschrieben werden.

C2: Sicherheitsrichtlinien aufstellen

Für den Einsatz von WLAN-Komponenten in Behörden und Unternehmen sollten individuelle Sicherheitsrichtlinien sowohl für Benutzer als auch für Administratoren aufgestellt werden. Diese WLAN-spezifischen Sicherheitsrichtlinien sollten konform zum generellen Sicherheitskonzept der Behörde bzw. des Unternehmens sein und regelmäßig auf Aktualität überprüft und gegebenenfalls angepasst werden. Typische Punkte einer WLAN-Sicherheitsrichtlinie findet man z.B. in Teil 2 der Technischen Richtlinie Sicheres WLAN (siehe [TR-S-W2]).
Nutzer eines WLAN sollten sensibilisiert werden für Gefährdungen sowie für Inhalte und Auswirkungen der Richtlinie.

C3: Einhaltung der Sicherheitsrichtlinien überprüfen

Die Einhaltung der Vorgaben sollte ständig kontrolliert werden. Mechanismen zur Überprüfung der Einhaltung sind z.B.:

C3.1 Regelmäßige Kontrollen der Access Points und Clients mittels Protokollanalysator für WLAN und kabelbasiertes LAN

C3.2 Regelmäßige, gegebenenfalls stichprobenweise Auswertung der Protokolldatei (Log) der Access Points und Überprüfung der an einem Access Point angemeldeten Clients

Diese Kontrollen und Auswertungen können durch ein zentrales WLAN-Management-System unterstützt werden.

C4: Gezielte Administratorschulungen

Der verantwortliche Betrieb eines WLAN, insbesondere auch der zugehörigen Sicherheitsmaßnahmen, erfordert den gezielten Aufbau des notwendigen Know-how. Hierfür sollten eine Grundlagenschulung zu den benutzten Mechanismen sowie eine produktspezifische Schulung zu Administrationsaufgaben erfolgen. Danach sollte eine Einweisung zu den Inhalten der WLAN-Sicherheitsrichtlinie erfolgen. Darüber hinaus ist noch eine entsprechende WLAN-spezifische Messtechnik-Schulung sinnvoll.

C5: Schulung der WLAN-Benutzer

Die Nutzer des WLAN sind zu den in der Benutzerrichtlinie aufgeführten Maßnahmen zu schulen. Hierzu gehören auch Hinweise auf die Nutzung komplexer Passwörter.

C6: Sensibilisierung des Objektschutzes zur WLAN-Problematik

Der Objektschutz (z.B. der Werkschutz) sollte dahingehend sensibilisiert werden, dass er darauf achtet, dass sich nicht über längere Zeit unbekannte Personen mit Notebook und gegebenenfalls sogar mit WLAN-Antennen in unmittelbarer Nähe des Liegenschafts- oder Betriebsgeländes aufhalten.

C7: Abnahme

Nach Abschluss der WLAN-Installation sollte anhand des Leistungsverzeichnisses eine Abnahme durchgeführt werden. Dabei sind die speziellen Eigenschaften eines WLAN besonders zu berücksichtigen, z.B. Schwankungen der Empfangsqualität und Mobilität zwischen Access Points. Die Abnahmetests und die zugehörigen Messverfahren sollten als Bestandteil der Planungs- bzw. Ausführungsunterlagen festgelegt sein.

C8: Pflege der Dokumentation

Wie für ein LAN ist auch für das gesamte WLAN eine Dokumentation zu führen, in der z.B. der Aufbau des Distribution Systems, Firm- und Softwarestände der WLAN-Komponenten, Konfigurationsdetails, Sicherheitskonfigurationen und eine Historie geführt werden.

Für den WLAN-Einsatz muss die Dokumentation zusätzlich solche bautechnischen Aspekte berücksichtigen, die Einschränkungen der Signalausbreitung auf Funkebene haben können. Diese können Relevanz für die Access-Point-Positionierung haben, sobald ein Bereich durch WLAN-Technik erschlossen werden soll.

C9: Sicherheitsrevision

Folgende Bereiche müssen regelmäßig kontrolliert werden:

C9.1 WLAN-Infrastruktur: Alle Komponenten der WLAN-Infrastruktur sind regelmäßig auf ihre korrekte Konfiguration zu überprüfen. Neben den Access Points zählen hierzu die Komponenten des Distribution System, die Elemente der Sicherheitsinfrastruktur (inklusive Authentication Server) und des Management-Systems.

Zur weitergehenden Verifikation der korrekten Konfiguration sollten zentrale Sicherheitssysteme, wie der Authentication Server oder das Koppelelement am Übergangspunkt zwischen Distribution System und LAN, Sicherheits-Scans unterzogen werden.

Insbesondere für Installationen in öffentlich zugänglichen Bereichen sollte eine stichprobenartige Prüfung im Hinblick auf gewaltsame Öffnungsversuche oder Manipulationsversuche (speziell für Access Points) durchgeführt werden.

C9.2 WLAN-Clients: Weiterhin müssen die WLAN-Clients regelmäßig überprüft werden. Bei einer größeren Anzahl sollte dies zumindest stichprobenweise geschehen.

C9.3 WLAN-Sicherheitskonzept: Zusätzlich sollte auch eine regelmäßige Revision des WLAN-Konzepts durchgeführt werden. Insbesondere sollte eine Bewertung erfolgen, ob die ergriffenen Maßnahmen zur Absicherung des WLAN noch dem Stand der Technik entsprechen und ob der zu Grunde gelegte Schutzbedarf nach wie vor gültig ist.

Sofern möglich, sollte das Sicherheitskonzept über das GS-Tool[12] des BSI dokumentiert und gegebenenfalls einer IT-Grundschutzzertifizierung zugeführt werden. Dadurch ist gewährleistet, dass zumindest alle 2 Jahre – im Rahmen der Re-Zertifizierung – ein umfassendes Audit der WLAN-Infrastruktur durchgeführt wird.

C10: Schutz personenbezogener Daten

Ein Nutzer von öffentlichen Hotspots sollte sich versichern, dass der von ihm gewählte Hotspot-Anbieter (Wireless Internet Service Provider, WISP) datenschutzkonform mit den personenbezogenen Daten umgeht.

4.4 Beispielszenarien zur Maßnahmenauswahl

Im Folgenden wird für drei typische Größenordnungen von WLAN-Installationen eine Auswahl der oben aufgeführten Sicherheitsmaßnahmen getroffen, die für das entsprechende Szenario einen niedrigen bis mittleren Schutz bzw. einen hohen Schutz bieten. Die aufgeführten Maßnahmen für den hohen Schutzbedarf sind als **zusätzliche Maßnahmen** zu den Basismaßnahmen für den niedrigen bis mittleren Schutzbedarf zu verstehen.

Betrachtet werden die drei Beispielszenarien

- kleine WLAN-Installation,
- große WLAN-Installation und
- SOHO-WLAN

sowie die Nutzung von Hotspots und die LAN-Kopplung.

---

[12] Mit der Entwicklung des BSI-Tool IT-Grundschutz (GS-Tool) stellt das BSI eine Software bereit, die den Anwender bei Erstellung, Verwaltung und Fortschreibung von IT-Sicherheitskonzepten entsprechend dem IT-Grundschutz effizient unterstützt.

Ein niedriger bis mittlerer Schutzbedarf bedeutet, dass die Schadensauswirkungen begrenzt und überschaubar sind. Bei einem hohen Schutzbedarf können die Schadensauswirkungen beträchtlich sein.

4.4.1 Kleine WLAN-Installation

Das Beispielszenario „Kleine WLAN-Installation“ umfasst maximal 10 Access Points, die von ca. 100 WLAN-Clients genutzt werden.

Lösungen für einen niedrigen bis mittleren Schutzbedarf

Für eine Basislösung sollten die folgenden Schutzmaßnahmen umgesetzt werden:

- A1.1: Festlegung eines Frequenzstandards und der Übertragungstechnik
- A1.2: Untersuchung der Einsatzumgebung auf mögliche Störungen des WLAN auf Funkebene
- A1.3: Festlegungen zum Aufbau des Distribution System

  Aus betrieblichen Gesichtspunkten und zur Realisierung einer klaren Unterscheidung der Infrastruktur des WLAN und der sonstigen IT-Umgebung wird empfohlen, die (maximal 10) Access Points möglichst auf einen eigenen Switch aufzuschalten, der exklusiv für das Distribution System genutzt wird und in einem zentralen Verteilerraum untergebracht sein sollte. Der Switch muss in ein zentrales Netzmanagement integriert werden können.
- A1.4: Planung der zu verwendenden WLAN-Authentisierungsverfahren und deren Nutzung
- A1.5: Erstellung eines Anforderungskatalogs für die WLAN-Beschaffung
- A1.6: Planung und Prüfung des Zusammenwirkens aller WLAN-Komponenten und der zugehörigen Infrastruktur
- A2.1: Für Verschlüsselung und Integritätsschutz sollte WPA2-Enterprise (CCMP und IEEE 802.1X) genutzt werden. Ist dies nicht möglich, muss zumindest WPA-Enterprise (TKIP + Michael und IEEE 802.1X) verwendet werden.

  Die Authentisierung geschieht mit IEEE 802.1X. Dabei können die EAP-Methoden EAP-PEAP oder EAP-TTLS genutzt werden.
- A2.2: Identifikations- und Passwortvorgaben ändern
- A2.3 / A2.4: SSID Broadcast am Access Point abschalten und Assoziation via Broadcast SSID deaktivieren
- A3: Schlüssel und Zugangspassworte von hoher Komplexität nutzen
- A5: Aufstellort und Antennencharakteristik des Access Points optimieren
- A6: Sendeleistung an den Access Points optimieren
- A7: Regelmäßiges Einspielen von Firmware-Upgrades / Software-Updates auf den Access Points nach ausführlichen Tests
- A8: Konfiguration der Access Points nur über sichere Kanäle
- B6: Absicherung der Clients
- C1: Ermittlung des Schutzbedarfs der über das WLAN übertragenen Daten
- C2 / C3: Sicherheitsrichtlinien aufstellen und deren Einhaltung überprüfen
- C4 / C5: Gezielte Administratorschulungen und Schulung der WLAN-Benutzer
- C7: Abnahme
- C8: Pflege der Dokumentation
- C9: Sicherheitsrevision

Diese Basislösung kann erweitert werden, indem zur Authentisierung die EAP-Methode EAP-TLS genutzt wird (anstelle von EAP-PEAP oder EAP-TTLS) und die Schutzmaßnahme B5, Einsatz eines zentralen WLAN-Management-Systems, umgesetzt wird.

Erweiterung der Lösungen für einen hohen Schutzbedarf

Für den hohen Schutzbedarf werden zwei Szenarien unterschieden: In Szenario 1 besteht ein hoher Vertraulichkeits- und Integritätsschutz. In Szenario 2 dagegen liegt der hohe Schutzbedarf in den hohen Verfügbarkeitsanforderungen begründet.

Bei Szenario 1 sollte die Basislösung um die Umsetzung der Schutzmaßnahme B1, Verwendung eines VPN zur Absicherung des WLAN, mit einer zugehörigen zertifikatbasierten Authentisierung ergänzt werden. Alternativ ist auch eine Absicherung des WLAN durch den ausschließlichen Einsatz von WPA2-Enterprise zusammen mit der EAP-Methode EAP-TLS zur Authentisierung möglich. Weiterhin ist meist auch der Einsatz von Firewall-Techniken zur Abschottung des drahtgebundenen Netzes (Bestandteil der Maßnahme B2) erforderlich. Die Anforderungen an das Firewall-System sind von dem konkreten Einsatzszenario des WLAN abhängig. Eine detailliertere Beschreibung hierzu kann [TR-S-W2] entnommen werden.

In Szenario 2 werden die hohen Verfügbarkeitsanforderungen durch ein Monitoring der Luftschnittstelle z.B. mit einem Wireless IDS erreicht.

4.4.2 Große WLAN-Installation

Dieses Szenario umfasst ca. 100 (oder mehr) Access Points, die von ca. 1000 WLAN-Clients genutzt werden. Es wird auch eine standortübergreifende WLAN-Nutzung betrachtet.

Lösungen für einen niedrigen bis mittleren Schutzbedarf

Für eine Basislösung gelten im Allgemeinen die Schutzmaßnahmen für die Basislösung in kleinen WLAN-Installationen. Allerdings müssen zwei Maßnahmen den geänderten Bedingungen angepasst werden:

- A1.3: Festlegungen zum Aufbau des Distribution System

  Auch hier ist aus Sicherheitsaspekten eine physikalische Trennung von Systemen unterschiedlichen Schutzbedarfs und Schutzniveaus zu bevorzugen, d.h. wenn möglich, sollten die Access Points auf Switches zusammengeführt werden, die nur für das WLAN-Distribution System und nicht für das kabelgebundene LAN bestimmt sind. Hiermit sind allerdings nicht unerhebliche Investitionen und zusätzliche Sicherheitsmaßnahmen verbunden.
  Alternativ ist auch die Konfiguration von VLAN ein gangbarer Weg, solange unter Verfügbarkeitsaspekten für die gesamte LAN- und WLAN-Infrastruktur nur ein mittlerer Schutzbedarf angestrebt wird (Ausfälle von mehr als 24 Stunden werden zugelassen).
- A2.1: Verschlüsselung, Integritätsschutz und Authentisierung auf der Luftschnittstelle

  Für Verschlüsselung und Integritätsschutz sollte möglichst WPA2-Enterprise (CCMP und IEEE 802.1X) genutzt werden. Ist dies nicht möglich, ist zumindest WPA-Enterprise (TKIP + Michael und IEEE 802.1X) zu verwenden.
  Die Authentisierung nach IEEE 802.1X sollte mit der EAP-Methode EAP-TLS geschehen.

Außerdem sollten zusätzlich die folgenden Schutzmaßnahmen umgesetzt werden:

- B5: Einsatz eines zentralen WLAN-Management-Systems
- C6: Sensibilisierung des Objektschutzes zur WLAN-Problematik

Diese Basislösung (siehe Abb. A-12) kann durch den Einsatz eines Wireless IDS erweitert werden.

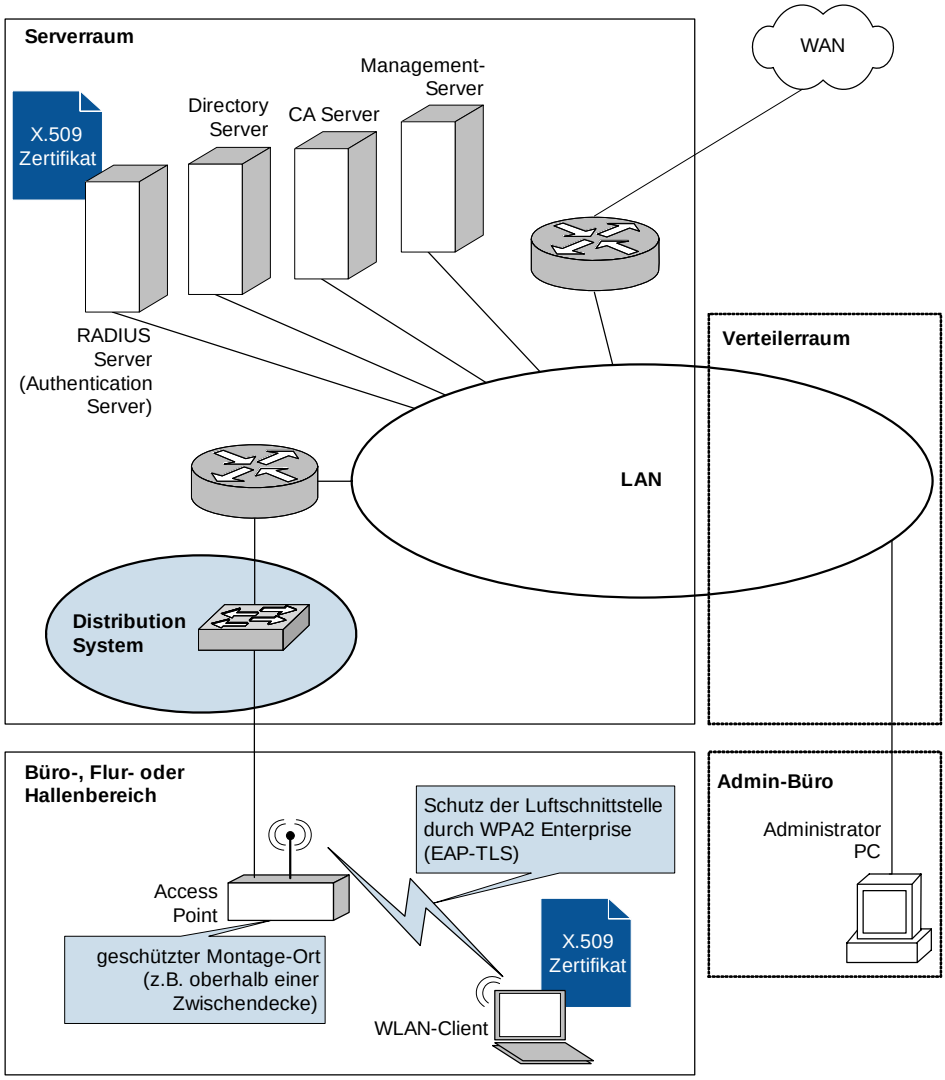


Abb. A-12: Netzplan des Grundkonzepts für eine große WLAN-Umgebung mit Clients, die einheitlich WPA2-Enterprise unterstützen

Erweiterung der Lösungen für einen hohen Schutzbedarf

Für den hohen Schutzbedarf werden zwei Szenarien unterschieden: In Szenario 1 besteht ein hoher Vertraulichkeits- und Integritätsschutz. In Szenario 2 dagegen liegt der hohe Schutzbedarf in den hohen Verfügbarkeitsanforderungen begründet.

Bei Szenario 1 muss die Basislösung um die Umsetzung der Schutzmaßnahme B1, Verwendung eines VPN zur Absicherung des WLAN, mit einer zugehörigen zertifikatbasierten Authentisierung ergänzt werden.

In Szenario 2 werden die hohen Verfügbarkeitsanforderungen zusätzlich zu den Maßnahmen für den niedrigen bis mittleren Schutzbedarf durch die Umsetzung der Schutzmaßnahme B3, Überwachung der Luftschnittstelle des WLAN durch ein Wireless Intrusion Detection System, inklusive einer Funktion zur Lokalisierung eines Sicherheitsvorfalls bzw. allgemein einer Störung, erreicht. Weiterhin ist die Umsetzung der Maßnahme B2, Abschottung des drahtgebundenen Firmen-/Behördennetzes durch Firewall und Intrusion Detection System bzw. Intrusion Prevention System, zu empfehlen. Auf diese Weise können unerlaubte Kommunikationsbeziehungen und Angriffsmuster, wie beispielsweise Port Scans, Buffer Overflows und das Verhalten vieler Würmer und Viren, festgestellt und blockiert werden.

4.4.3 SOHO-WLAN

Dieses Szenario spiegelt die Situation von Heimanwendern oder Freiberuflern wider: es umfasst einen Access Point, der von ca. 3 WLAN-Clients genutzt wird.

Lösungen für einen niedrigen bis mittleren Schutzbedarf

Für eine Basislösung sollten die folgenden Schutzmaßnahmen umgesetzt werden:

- A1.1: Festlegung eines Frequenzstandards und der Übertragungstechnik
- A1.2: Untersuchung der Einsatzumgebung auf mögliche Störungen des WLAN auf Funkebene
- A1.4: Planung der zu verwendenden WLAN-Authentisierungsverfahren und deren Nutzung
- A2.1: für Verschlüsselung und Integritätsschutz WPA2-Personal (CCMP und PSK) oder WPA-Personal (TKIP + Michael und PSK) nutzen[13]
- A2.2: Identifikations- und Passwortvorgaben ändern
- A2.3 / A2.4: SSID Broadcast am Access Point abschalten und Assoziation via Broadcast SSID deaktivieren
- A2.5: MAC Adressfilterung
- A3: Schlüssel und Zugangspassworte von hoher Komplexität nutzen
- A4: PSK regelmäßig wechseln
- A5: Aufstellort und Antennencharakteristik des Access Points optimieren
- A6: Sendeleistung an den Access Points optimieren
- A7: Regelmäßiges Einspielen von Firmware-Upgrades / Software-Updates auf den Access Points nach ausführlichen Tests
- A8: Konfiguration der Access Points nur über sichere Kanäle
- A9: WLAN-Komponenten nur bei Gebrauch einschalten
- B6: Absicherung der Clients
- C1: Ermittlung des Schutzbedarfs der über das WLAN übertragenen Daten
- C4 / C5: Gezielte Administratorschulungen und Schulung der WLAN-Benutzer

Erweiterung der Lösungen für einen hohen Schutzbedarf

Ein erhöhter Schutzbedarf besteht, wenn über das WLAN besonders zu schützende Daten, wie Patienten- oder Mandantendaten, die gegebenenfalls den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) unterliegen, auf den WLAN-Clients gespeichert und verarbeitet werden.

Bei einem hohen Schutzbedarf muss zusätzlich zu den für einen niedrigen bis mittleren Schutzbedarf genannten Maßnahmen zumindest WPA2-Personal mit CCMP unter Verwendung von PSK genutzt werden.

Ist der Einsatz von WPA2-Personal nicht möglich, kann alternativ auch ein VPN (Schutzmaßnahme B1) zur Absicherung des WLAN eingesetzt werden.

---

[13] Die Verwendung von PSK ist (unter der Voraussetzung einer genügenden Komplexität der zu Grunde liegenden Passphrase) akzeptabel, da im SOHO-WLAN nur wenige Stationen beteiligt sind und der Aufwand für eine manuelle und trotzdem effektive Schlüsselverwaltung überschaubar ist.

4.4.4 Hotspot-Nutzung

Öffentliche Hotspot-Systeme stellen dem Nutzer einen drahtlosen transparenten Internet-Zugang bereit. Sie sind nicht dazu gedacht, eine abgesicherte Einwahlplattform für den Remote Access (RAS) via Internet bereitzustellen. Im Hinblick auf eine sichere Hotspot-Nutzung sind folgende Grundprinzipien von Hotspot-Systemen relevant:

- Es gibt bis heute keine einheitliche systemübergreifende Authentisierung und Abrechnung für Hotspot-Systeme.
- In der Regel werden keine Verschlüsselungsmechanismen auf der Luftschnittstelle zur Verfügung gestellt.
- Die Anmeldung im Hotspot erfolgt meist an einem Web-Portal über eine Web-Applikation; diese muss für den Schutz der Anmelde-Information sorgen.

Auf Grund der vielfältigen Bedrohungen, denen ein WLAN-Client in einer Hotspot-Umgebung ausgesetzt ist, sind spezielle Konfigurationsvorgaben zur Absicherung des Clients notwendig.

Es ist zu beachten, dass ein Nutzer eines Hotspot-Systems lediglich auf die Konfiguration seines WLAN-Clients Einfluss nehmen kann. Auf die Absicherung der Luftschnittstelle und der Access Points sowie auf die Architektur und Absicherung des Distribution Systems, auf die benötigte Sicherheitsinfrastruktur und das WLAN-Management hingegen hat er keinerlei Einfluss.

Lösungen für einen niedrigen bis mittleren Schutzbedarf

Für einen mittleren Schutzbedarf sollten die folgenden Schutzmaßnahmen umgesetzt werden:

- A7: Regelmäßiges Einspielen von Firmware-Upgrades / Software-Updates (hier Updates und Patches für die Gerätetreiber der WLAN-Clients) nach ausführlichen Tests
- A9: WLAN-Komponenten (hier WLAN-Adapter) nur bei Gebrauch einschalten
- B6: Absicherung der Clients

  Die Verwendung des Hotspots wird nur für den Aufbau eines VPN-Tunnels gestattet. Dieser Tunnelaufbau sollte möglichst automatisch, unmittelbar nachdem eine Internet-Verbindung über den Hotspot hergestellt ist, erfolgen. Da kein Einfluss auf Sicherheitsmechanismen auf der Luftschnittstelle genommen werden kann, sind Maßnahmen auf höheren Netzwerkschichten notwendig, die sich nicht wesentlich von denen für einen Remote-Access-Client unterscheiden, auf Grund der WLAN-spezifischen Bedrohungen jedoch restriktiver gehandhabt werden müssen. Hierzu zählen unter anderem:

  - Einsatz einer Personal Firewall-Software
  - Entfernung von nicht benötigten Stamm-CA-Zertifikaten
  - Client-Systeme werden mit einem vorkonfigurierten Satz von Stamm-CA-Zertifikaten ausgestattet. Diese Liste muss auf das notwendige Minimum reduziert werden, um die Angriffsfläche für Man-in-the-Middle-Attacken gegen SSL-Sitzungen zu reduzieren.
  - Restriktive Browser-Konfiguration

    Siehe hierzu auch IT-Grundschutzhandbuch Baustein B 3.208 „Internet-PC“, M 5.93 „Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs“ und M 5.66 „Verwendung von SSL“ (siehe IT-Grundschutzhandbuch [GSHB]).
  - Virenschutz
  - Einrichtung einer eingeschränkten Benutzerumgebung
  - Zugriffsschutz (komplexe Kennwörter, besonders komplexe Administrator-Kennwörter)
  - Scannen und Patchen (d.h. Härtung) der WLAN-Clients
- C1: Ermittlung des Schutzbedarfs der über das WLAN übertragenen Daten

► C2 / C3: Sicherheitsrichtlinien (hier Benutzerrichtlinien für die Hotspot-Nutzung) aufstellen und deren Einhaltung überprüfen

In dieser Benutzerrichtlinie werden beispielsweise die folgenden Punkte für die Hotspot-Nutzung geregelt:

- Sensibilisierung zum Umgang mit SSL-Zertifikaten
- Beschreibung, wie eine Plausibilitätsprüfung des Zertifikats erfolgen kann (Fingerprint, Gültigkeitsdauer, Inhaber und Zertifizierungsinstanz des Zertifikates)
- Anweisung, dass WLAN-Adapter auszuschalten sind, wenn sie nicht in Benutzung sind
- Verhaltensweisen bei einer vermuteten Kompromittierung des WLAN-Clients
- Ggf. Verpflichtung des WLAN-Nutzers, den Hotspot-Zugang nur zur Etablierung der RAS-Verbindung zu nutzen

► C4 / C5: Gezielte Administratorschulung und Schulung der WLAN-Benutzer (hier insbesondere hinsichtlich der Hotspot-Nutzung)

Es sollte auch eine regelmäßige Nachschulung der Hotspot-Nutzer erfolgen.

Erweiterung der Lösungen für einen hohen Schutzbedarf

Für WLAN-Clients, die Daten mit hohem Schutzbedarf verarbeiten, werden zwei Alternativen vorgeschlagen, die im Rahmen der Schutzbedarfsfeststellung und einer Risikoanalyse zu bewerten sind:

► Empfohlen wird ein Verbot der Hotspot-Nutzung.

► Abweichend davon muss zumindest eine Einschränkung der Hotspot-Nutzung durch die folgenden Maßnahmen erfolgen, die zusätzlich zum Basisschutz (siehe Maßnahmen für den niedrigen bis mittleren Schutzbedarf) durchzuführen sind:

- C10: Es wird nur die Nutzung von vertrauenswürdigen Hotspots gestattet, zu deren Betreiber eine entsprechende vertragliche Beziehung besteht. Dabei muss in jedem Fall der Schutz personenbezogener Daten sichergestellt sein.
- Absicherung der Luftschnittstelle

  Es wird lediglich die Nutzung von Hotspots gestattet, die eine Absicherung der Luftschnittstelle mit WPA bzw. WPA2 unterstützen. Die Verwendung des Hotspots wird nur für den Aufbau eines VPN-Tunnels gestattet. Dieser Tunnelaufbau sollte möglichst automatisch, unmittelbar nachdem eine Internet-Verbindung über den Hotspot hergestellt ist, erfolgen. Dies beinhaltet auch die Forderung, dass jeglicher Datenverkehr nach Aufbau des VPN-Tunnels ausschließlich über diesen läuft und beispielsweise kein Internet-Zugang außerhalb des VPN-Tunnels erlaubt ist.
- Restriktivere Einstellung der Regelbasis der Personal Firewall
- Verschlüsselung der Daten auf der Festplatte
- Erhöhter Zugriffsschutz durch Zweifaktorauthentisierung (Wissen und Besitz) z.B. mit Chipkarten, Token etc.
- Unterbindung bzw. starke Einschränkung der Nutzung von Wechseldatenträgern

Abschließend sei auf die Konzeptarbeit des Department of Defense zum Thema „Secure Remote Access Service" hingewiesen (siehe [DOD05c]), die insbesondere für den Hotspot-Zugang einen umfangreichen Maßnahmenkatalog spezifiziert.

4.4.5 LAN-Kopplung

Bei einer LAN-Kopplung wird eine WLAN-Übertragung als verbindendes Medium zwischen zwei LANs genutzt. Die Koppelelemente werden als Wireless Bridges bezeichnet und haben, wie auch ein Access Point, auf der einen Seite eine Ethernet-Schnittstelle zur Anbindung an das kabelbasierte LAN und auf der anderen Seite eine WLAN-Schnittstelle.

Bei einer LAN-Kopplung fehlt das dynamische Element mobiler Clients. Die Kommunikation erfolgt statisch zwischen den beteiligten Wireless Bridges.

Bei der LAN-Kopplung werden oft hohe Anforderungen an die Verfügbarkeit gestellt. Die Erwartungshaltung des Nutzers ist eine Verfügbarkeit, die mindestens einer WAN-Verbindung entspricht. Diese Anforderung ist durchaus kritisch zu sehen, da im Außenbereich eine Funkverbindung stets durch die Umwelt oder Störungen beeinflusst wird.

Lösungen für einen niedrigen bis mittleren Schutzbedarf

Für einen niedrigen bis mittleren Schutzbedarf sollten die folgenden Schutzmaßnahmen umgesetzt werden:

- A1.1: Festlegung eines Frequenzstandards und der Übertragungstechnik
- A1.2: Untersuchung der Einsatzumgebung auf mögliche Störungen des WLAN auf Funkebene
- A1.4: Planung der zu verwendenden WLAN-Authentisierungsverfahren und deren Nutzung
- A2.1: Für Verschlüsselung und Integritätsschutz WPA2 (CCMP) nutzen

  Für eine LAN-Kopplung wird bei einem mittleren Schutzbedarf von der Nutzung von WPA (TKIP + Michael) abgeraten. Zur Authentisierung kann die Variante WPA2-Personal mit Pre-Shared Keys zum Einsatz kommen
- A2.2: Identifikations- und Passwortvorgaben ändern
- A2.3 / A2.4: SSID Broadcast am Access Point abschalten und Assoziation via Broadcast SSID deaktivieren
- A3: Schlüssel und Zugangspasswörter von hoher Komplexität nutzen
- A4: Im Fall der Nutzung von Pre-Shared Keys den PSK regelmäßig wechseln
- A5: Aufstellort und Antennencharakteristik der Wireless Bridges optimieren

  Die Montage der Wireless Bridges sollte möglichst in einem geschlossenen, geeignet klimatisierten Technikraum bzw. einem entsprechenden Schutzschrank erfolgen. Bei einer Außenmontage einer Wireless Bridge muss die Wireless Bridge entweder eine Außenmontage erlauben, d.h. das Gehäuse der Wireless Bridge ist geeignet gegen Wettereinflüsse (Hitze, Kälte, eindringende Feuchtigkeit etc.) geschützt. Andernfalls muss die Wireless Bridge in einen für den Außeneinsatz spezifizierten Schutzschrank montiert werden. Bei der Montage ist weiterhin zu beachten, dass die Wireless Bridge vor elektrischen Entladungen und unberechtigtem Zugriff geeignet geschützt ist. Speziell ist sicherzustellen, dass ein Schutz vor einem unberechtigten Zugriff auf die Kommunikationsschnittstellen (Ethernet, serielle Schnittstelle) besteht.
  Bei der Montage einer Außenantenne muss der Schutz vor elektrischen Entladungen berücksichtigt werden. Bei Anbringung von Antennen auf Gebäudedächern muss die Antenne gegen Blitzschlag gesichert werden. Antennen im Außenbereich, die möglicherweise von der Gefahr elektrischer Entladungen betroffen sind, sollten über einen speziellen Überspannungsschutz angeschlossen werden. Außenantennen sind geeignet gegen Schnee-Ablagerung zu schützen. Sie sind entweder windgeschützt anzubringen, oder die Anbringung muss auch bei hohen Windstärken so fest sein, dass sich die Antennenausrichtung nicht verstellt.
- A6: Sendeleistung an den Wireless Bridges optimieren

  Hier müssen in jedem Fall die Vorgaben der Bundesnetzagentur hinsichtlich der maximalen Strahlungsleistung berücksichtigt werden.
- A7: Regelmäßiges Einspielen von Firmware-Upgrades / Software-Updates auf den Access Points nach ausführlichen Tests (hier für die Wireless Bridges)
- A8: Konfiguration der Wireless Bridges bevorzugt nur über sichere Kanäle

  Diese Maßnahme wird für die LAN-Kopplung bewusst leicht abgeschwächt. Ein administrativer Zugriff auf eine Wireless Bridge sollte bevorzugt über die Ethernet-Schnittstelle bzw. die serielle Schnittstelle von dedizierten Management-Stationen aus erfolgen. Der administrative Zugriff über

die Luftschnittstelle sollte auf ein Minimum beschränkt werden und sich dabei möglichst nur auf einen lesenden Zugriff beschränken. Es sind sichere Managementprotokolle zu verwenden. Von der Nutzung Web-basierter Zugriffe wird abgeraten.

- Ggf. B1: Verwendung eines VPN zur Absicherung des WLAN

  Eine Wireless Bridge wird normalerweise möglichst in der Nähe der Außenantenne montiert, da das HF-Kabel zwischen Wireless Bridge und Antenne je nach verwendetem Kabeltyp das Signal unterschiedlich stark dämpft. In einer solchen Situation kann es vereinzelt vorkommen, dass eine geeignete räumliche Absicherung des Zugangs zur Wireless Bridge nicht vollständig umgesetzt werden kann. In dieser Situation kann bereits bei einem mittleren Schutzbedarf der Einsatz eines Site-to-Site IPSec VPN eine Option sein, wobei die beteiligten VPN-Gateways entsprechend gesichert aufgestellt sein müssen und der VPN-Tunnel die unsicheren Bereiche vollständig abdeckt.

- B2: Abschottung des drahtgebundenen Firmen-/Behördennetzes

  Die Kopplung zwischen einer Wireless Bridge und dem LAN erfolgt über eine Layer-3-Instanz. Die Wireless Bridges sind Bestandteil eines eigenen IP-Subnetzes (Transportnetz). Sofern die genutzten Dienste sinnvoll begrenzt werden können, ist eine ACL (Layer 3 und höher) auf der Routing-Instanz zu empfehlen.

- Ggf. B3 und B5: Überwachung der Luftschnittstelle des WLAN durch ein Wireless Intrusion Detection System und Einsatz eines zentralen WLAN-Management-Systems

  Werden nur wenige Wireless Bridges im Netzwerk eingesetzt, kann die Verwaltung über die vom Hersteller mitgelieferten Konfigurations-Tools durchgeführt werden.
  Allerdings ist eine effektive und effiziente Überwachung der Wireless Bridges nur über ein zentrales Management möglich. Eine solche kontinuierliche Überwachung der Luftschnittstelle kann bereits bei einem mittleren Schutzbedarf in Betracht gezogen werden.
  Für einen niedrigen bis mittleren Schutzbedarf kann prinzipiell auf ein Out-of-Band-Management verzichtet werden. Allerdings ist eine solche Einrichtung für das Management von Wireless Bridges in vielen Fällen technisch sinnvoll.

- C1: Ermittlung des Schutzbedarfs der über das WLAN übertragenen Daten

- C2 / C3: Sicherheitsrichtlinien aufstellen und deren Einhaltung überprüfen (hier keine Benutzerrichtlinie, sondern nur eine Administrationsrichtlinie erforderlich)

- C4: Gezielte Administratorschulungen

- C8: Pflege der Dokumentation

- C9: Sicherheitsrevision

Erweiterung der Lösungen für einen hohen Schutzbedarf

Für den hohen Schutzbedarf wird hier die Schaffung eines hohen Vertraulichkeits- und Integritätsschutzes betrachtet. Hierzu wird das Konzept um ein Site-to-Site-IP-VPN ergänzt. Die Kommunikation zwischen den VPN-Gateways wird über IPSec geschützt. Das VPN-Gateway kann als separate Komponente oder als Modul einer Firewall realisiert sein. Durch den Einsatz einer VPN-Lösung auf IPSec-Basis wird ein vergleichbar hohes Sicherheitsniveau wie bei der Verwendung eines VPN zur Kopplung von Standorten über das Internet erreicht. Die erreichte Schutzklasse der Daten und des LAN hängt primär von der Implementierung des VPN-Gateways ab.

Wenn auch ein hoher Schutzbedarf hinsichtlich der Verfügbarkeit besteht, müssen auch andere Übertragungsalternativen in Betracht gezogen werden. Neben der kabelbasierten Übertragung kann hier auch der Einsatz von Richtfunktechniken in Frage kommen.

4.4.6 Meshed Networks

Die im Kapitel 4.4.5 spezifizierten Maßnahmen gelten grundsätzlich auch für Meshed Networks, bei denen ein Wireless Distribution System über eine Funkvernetzung zwischen WLAN Access Points geschaffen werden kann.

Zu beachten ist allerdings, dass sich Meshed Networks durch eine größere Dynamik im Sinne wechselnder Übertragungswege im Netz und wechselnder Netzwerkknoten auszeichnen. Ein zentrales Netzmanagement und ein kontinuierliches Monitoring der Luftschnittstelle der beteiligten Stationen sind unabdingbar.

5. Ausblick

WLANs gehören zu den sich am dynamischsten entwickelnden Bereichen der Kommunikationstechnik und man muss sich stets auf Entwicklungen einstellen, die auch Auswirkungen auf die Sicherheit haben. An der kommenden Integration von WLAN und Mobilfunktechnik wird beispielsweise nicht mehr gezweifelt. Die Erwartung ist, dass zumindest ein Roaming zwischen GSM- bzw. UMTS-Netzen und Hotspots möglich sein wird und im Hotspot die Sprachkommunikation über VoIP geschehen wird. Wie dabei eine standardisierte Absicherung der WLAN-Übertragung in einem Hotspot stattfindet, ist aber noch nicht abschließend in allen Details geklärt. Erwähnenswert ist in diesem Zusammenhang, dass erste Mobiltelefone auf dem Markt verfügbar sind, deren WLAN-Komponente WPA- und sogar WPA2-Enterprise mit verschiedenen EAP-Methoden unterstützen.

Wireless Switches sind eine weitere Technik, die sich wahrscheinlich noch erheblich entwickeln wird. Die hiermit verbundenen Konzepte werden insbesondere im Rahmen der Implementierung von WLAN als natürlichem Bestandteil konvergenter Netze an Bedeutung gewinnen. WLAN werden vermehrt nicht mehr als separate Spezialnetze gesehen werden, sondern bilden zusammen mit den zugehörigen Sicherheitsmechanismen einen integralen Bestandteil der IT-Infrastruktur.

6. Fazit

Eine Datenübertragung über Funk muss stets durch eine entsprechende Kombination von Mechanismen zur Authentisierung, Verschlüsselung und Integritätsprüfung geeignet abgesichert werden. Der in IEEE 802.11 ursprünglich festgelegte Mechanismus WEP ist hierzu nur mangelhaft geeignet.

Mit der Erweiterung IEEE 802.11i bzw. mit WPA und WPA2 stehen inzwischen Bausteine zur Verfügung, die auf der Luftschnittstelle eine adäquate Absicherung eines WLAN hinsichtlich der Sicherheitsziele Vertraulichkeit und Integrität gestatten. Für größere WLAN und generell für WLAN mit höheren Sicherheitsanforderungen ist der Einsatz von IEEE 802.1X in Kombination mit einer angemessen hochwertigen EAP-Methode zur Authentisierung dringend zu empfehlen. Auf der Basis von WPA und WPA2 werden von der Wi-Fi Alliance WLAN-Produkte zertifiziert. Die Verfügbarkeit ist in WLAN ein grundsätzliches Problem des Übertragungsmediums Funk, da Störungen der Übertragung nicht ausgeschlossen bzw. nicht verhindert werden können. Das Netzmanagement muss daher diese und andere WLAN-spezifischen Eigenheiten berücksichtigen. Dies beinhaltet speziell auch die Erkennung von Fremdstationen (Access Points und Endgeräte) und deren geografische Lokalisierung.

Der hier vorgestellte Maßnahmenkatalog zur Absicherung eines WLAN macht deutlich, dass auch Maßnahmen notwendig sind, die über die Absicherung der Funkübertragung hinausgehen. Die Absicherung eines WLAN erfordert genauso die Betrachtung von Infrastrukturaspekten, wie den geeigneten Aufbau des Distribution System und des Übergabepunkts zur LAN-Infrastruktur.

Obwohl mit IEEE 802.11i eine deutliche Verbesserung der WLAN-Absicherung erreicht ist, gibt es noch offene Punkte, wie z.B. die ungesicherte Übertragung von Management Frames auf der MAC-Ebene. Hier ist mit IEEE 802.11w ein entsprechender Standard in Arbeit. Aktuell muss diese Sicherheitslücke aber noch hingenommen werden.

7. Literatur / Links

Ausführliche technische Informationen zur Funktionsweise der in WLAN eingesetzten Sicherheitsmechanismen können dem Teil 1 der Technischen Richtlinie Sicheres WLAN [TR-S-W1] entnommen werden. Bedrohungsanalyse und Sicherheitsmaßnahmen werden im Teil 2 vertieft [TR-S-W2]. Der dritte Teil dieser Richtlinie [TR-S-W3] spezifiziert Kriterien für die Auswahl von WLAN-Systemen die hierzu gehörenden Prüfkriterien. Ferner sind umfangreiche Publikation über das amerikanische National Institute of Standards and Technology (NIST) verfügbar, die sich mit Aufbau, Betrieb und speziell der Absicherung von WLAN befassen, siehe z.B. [DOD05a] und [DOD05b]. Einen sehr guten Überblick über die verschiedenen Aspekte der Absicherung von WLAN liefert [UNOFF].

Im Folgenden ist weiterhin die Liste der im Text referenzierten Titel aufgeführt. Diese Liste stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

[CAPW05] RFC 4118, „Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)“, Juni 2005, http://www.ietf.org/rfc/rfc4118.txt

[CAPW06] P. Calhoun et. al, „CAPWAP Protocol Specification“, Internet Draft, Februar 2006, verfügbar unter http://www.ietf.org

[DOD05a] Department of Defense, „Wireless Security Technical Implementation Guide“, Version 4, Release 1, Oktober 2005, verfügbar unter http://csrc.nist.gov/pcig/cig.html

[DOD05b] Department of Defense, „Wireless LAN Security Framework – Addendum to the Wireless Security Technical Implementation Guide”, Version 2, Release 1, Oktober 2005, verfügbar unter http://csrc.nist.gov/pcig/cig.html

[DOD05c] Department of Defense, „Secure Remote Access Service – Addendum to the Wireless Security Technical Implementation Guide”, Version 1, Release 0 (Draft), Februar 2005, verfügbar unter http://csrc.nist.gov/pcig/cig.html

[EAP04] RFC 3748, “Extensible Authentication Protocol (EAP)”, IETF, Juni 2004, http://www.ietf.org/rfc/rfc3748.txt

[FMS01] S. Fluhrer, I. Mantin und A. Shamir, Weaknesses in the Key Scheduling Algorithm of RC4. In Selected Areas in Cryptography - SAC 2001, Lecture Notes in Computer Science 2259, Springer-Verlag, Seiten 1-24.

[GSHB] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutzhandbuch – Standard-Sicherheitsmaßnahmen“, verfügbar unter http://www.bsi.bund.de/gshb

[IEEE99] ANSI/IEEE Std 802.11, „Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications“, 1999.

[IEEE99a] IEEE Std 802.11a, „High-speed Physical Layer in the 5 GHz Band“, 1999.

[IEEE99b] IEEE Std 802.11b, „Higher-Speed Physical Layer Extension in the 2.4 GHz Band“, 1999.

[IEEE03g] IEEE Std 802.11g, „Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications; Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band“, Juni 2003.

[IEEE03h] IEEE Std 802.11h, „Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications; Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe“, September 2003.

[IEEE04i] IEEE Std 802.11i, „Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Medium Access Method Control (MAC) Security Enhancements“, Juni 2004.

[IEEE04X] IEEE Std 802.1X, „Port-Based Network Access Control“, Dezember 2004 (Revision der ersten Auflage des Standards von 2001).

[IEEE05e] IEEE Std 802.11e, „Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications; Amendment: Medium Access Control (MAC) Quality of Service Enhancements“, September 2005.

[KaPa04] V. Kamath, A. Palekar, “Microsoft EAP CHAP Extensions“, Internet Draft, IETF, April 2004, http://www.ietf.org

[RADI00] RFC 2865, “Remote Authentication Dial In User Service (RADIUS)”, IETF, Juni 2000, http://www.ietf.org/rfc/rfc2865.txt

[RADI03] RFC 3579, “RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)”, IETF, September 2003, http://www.ietf.org/rfc/rfc3579.txt

[RegTP/BNA] Bundesnetzagentur (vorm. Reg TP) , Vfg 8/2006, „Allgemeinzuteilung von Frequenzen in den Bereichen 5150 MHz - 5350 MHz und 5470 MHz - 5725 MHz für Funkanwendungen zur breitbandigen Datenübertragung, WAS/WLAN (Wireless Access Systems including Wireless Local Area Networks)“, 2006; ersetzt Vfg 35/2002.

[RegTP03] Regulierungsbehörde für Post und Telekommunikation (jetzt: Bundesnetzagentur), Vfg 89/2003, „Allgemeinzuteilung von Frequenzen im Frequenzbereich 2400,0 – 2483,5 MHz für die Nutzung durch die Allgemeinheit in lokalen Netzwerken; Wireless Local Area Networks (WLAN- Funkanwendungen)“, 2003.

[TKG04] „Telekommunikationsgesetz (TKG)“, Bundesgesetzblatt Jahrgang 2004 Teil I Nr. 29, Juni 2004.

[TR-S-W1] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie Sicheres WLAN – Teil 1: Darstellung und Bewertung der Sicherheitsmechanismen“, SecuMedia Verlag, 2005.

[TR-S-W2] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie Sicheres WLAN – Teil 2: Vorgaben eines WLAN Sicherheitskonzepts“, SecuMedia Verlag, 2005.

[TR-S-W3] Bundesamt für Sicherheit in der Informationstechnik, „Technische Richtlinie Sicheres WLAN – Teil 3: Auswahl und Prüfung von WLAN-Systemen“, SecuMedia Verlag, 2005.

[UNOFF] “The Unofficial 802.11 Security Web Page”, http://www.drizzle.com/~aboba/IEEE/

[WPA04] Wi-Fi Alliance, „Wi-Fi Protected Access (WPA)“, Version 2.0, April 2003, http://www.wi-fi.org

8. Abkürzungen

ACL	Address Control List
AES	Advanced Encryption Standard
AFH	Adaptive Frequency Hopping
ARP	Address Resolution Protocol
BSS	Basic Service Set
CAPWAP	Control And Provisioning of Wireless Access Points
CBC-MAC	Cipher Block Chaining Message Authentication Code

CCK	Code Complementary Keying
CCMP	Counter mode with CBC-MAC Protocol
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DCF	Distributed Coordination Function
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DS	Distribution System
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
EAP-PEAP	Protected EAP
EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP Tunneled Transport Layer Security
EDCA	Enhanced Distributed Channel Access
ESS	Extended Service Set
ETSI	European Telecommunications Standards Institute
FHSS	Frequency Hopping Spread Spectrum
GSM	Global System for Mobile Communications
GTC	Generic Token Card
GTK	Group Temporal Key
HCCA	HCF Controlled Channel Access
HCF	Hybrid Coordination Function
HIPERLAN	High Performance Radio LAN
HS	Hoher Schutzbedarf
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP über SSL
IAPP	Inter Access Point Protocol
IBSS	Independent Basic Service Set
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IV	Initialisierungsvektor
LAN	Local Area Network
MAC	Medium Access Control
MIC	Message Integrity Check
MIMO	Multiple Input Multiple Output
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSK	Master Session Key
OFDM	Orthogonal Frequency Divison Multiplexing

PCF	Point Coordination Function
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PPP	Point to Point Protocol
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RSN	Robust Security Network
SNMP	Simple Network Management Protocol
SOHO	Small Office / Home Office
SRTP	Secure Realtime Transmission Protocol
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
TKG	Telekommunikationsgesetz
TKIP	Temporal Key Integrity Protocol
TLS	Transport-Layer Security
TPC	Transmit Power Control
UMTS	Universal Mobile Telecommunications System
VLAN	Virtual LAN
VoIP	Voice over IP
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WISP	Wireless Internet Service Provider
WLAN	Wireless LAN
WMM	Wi-Fi Multimedia
WPA	Wi-Fi Protected Access
WZC	Wireless Zero Configuration

9. Glossar

Access Control List (ACL)
: Zugriffskontrollliste für die Filterung von zugelassenen IP-/MAC-Adressen

Access Point
: Funkfeststation für den Client-Zugang in ein WLAN

Advanced Encryption Standard (AES)
: Symmetrisches Verschlüsselungsverfahren mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit. AES bietet ein sehr hohes Maß an Sicherheit. Das Verfahren wurde eingehenden kryptoanalytischen Prüfungen unterzogen.

Assoziation
: Anmeldevorgang eines Clients an einem Access Point

Authentisierung
: Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Gerätes. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist i. A. keine sinnvolle Autorisierung möglich.

Cyclic Redundancy Check (CRC)
: Prüfsumme über die zu übertragenden Daten, die in der Nachricht mitgeschickt wird und es dem Empfänger gestattet, Bitfehler, die auf dem Kommunikationskanal entstanden sind, zu erkennen

Denial of Service (DoS)
: Ein Angriff vom Typ Denial of Service hat zum Ziel die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr („Dummy Traffic“) oder die beabsichtigte Herbeiführung eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Dictionary-Attacke
: Siehe Wörterbuch-Attacke

Distribution System (DS)
: Netzwerk, das Access Points untereinander und mit der weiteren Infrastruktur verbindet. Kann als physikalisch separates LAN oder als VLAN in einer bestehenden LAN-Infrastruktur realisiert werden.

EAP over LAN (EAPOL)
: Verfahren zur Verwendung von EAP auf Layer 2 über Lokale Netzwerke (LANs) wie z.B. IEEE 802.3 („Ethernet“) oder IEEE 802.11 (WLAN)

EAP-Transport-Layer Security (EAP-TLS)
: EAP-Methode, die Zertifikate zur gegenseitigen Authentisierung benutzt

Extensible Authentication Protocol (EAP)
: Rahmen (Framework) für die Verwendung von Authentisierungsmethoden. Es wird u.a. für PPP oder auch in Verbindung mit EAPOL unter IEEE 802.1X verwendet.

Funkzelle
: Geographischer Bereich um einen Sender (z.B. Access Point) herum, in dem ein genügend guter Empfang besteht. Was als „genügend gut“ zu bezeichnen ist und was nicht, ist Festlegungssache. Die Empfangsqualität in einem WLAN hängt unter anderem vom verwendeten Übertragungsstandard, von der Qualität der Hochfrequenz-Hardware in den Geräten und von der Charakteristik der Antennen ab. Die Ausdehnung einer Funkzelle wird weiterhin durch den verwendeten Frequenzbereich, die Sendeleistung und insbesondere durch die jeweiligen Umgebungsbedingungen (z.B. Material von Wänden, Türen, Fenstern und Decken) beeinflusst.

Handover
: Wechsel von einem (physikalischen) Kommunikationskanal auf einen anderen unter Aufrechterhaltung der Ende-zu-Ende-Kommunikationsbeziehung. Beispiel: Bei einem Telefonat über VoIP over WLAN darf bei einem (mobilitätsbedingten) Wechsel von einer Funkzelle in eine andere das Gespräch nicht signifikant gestört werden oder sogar abreißen.

Hotspot
: Öffentlich zugänglicher Internet-Zugang über ein WLAN

Intrusion Detection System (IDS)
: Bietet die Möglichkeit unerwünschte Zugriffe, Inhalte und Angriffe zu erkennen. Sobald das IDS einen Verstoß gegen die vereinbarten Regeln erkennt, erfolgen eine Protokollierung und eine Meldung an den Administrator, dieser kann manuell Gegenmaßnahmen einleiten.

Intrusion Prevention System (IPS)
: Kann Angriffe nicht nur erkennen, sondern auch eine als Angriff erkannte Kommunikation unterbinden

ISM-Frequenzband
: Lizenzfrei nutzbare Frequenzbänder, die für industrielle, wissenschaftliche und medizinische Zwecke verwendet werden können (ISM = Industrial-Scientific-Medical)

Man in the Middle
: Der Angreifer positioniert sich zwischen zwei Kommunikationspartner und täuscht beiden Parteien vor, der jeweils erwartete eigentliche Partner zu sein. Dabei kann der Man in the Middle den Dialog zwischen den beiden Parteien belauschen oder auch verfälschen. Ziel ist oft die Ermittlung von Passwörtern.

Message Integrity Check (MIC)
: kryptographischer Integritätsschutzmechanismus

Michael
: Name des MIC, der bei WPA und TKIP Verwendung findet

Pre-Shared Key (PSK)
: Vorab vereinbarter bzw. verteilter Schlüssel, der bis zur Verteilung eines neuen PSK für jede Verbindung verwendet wird

Public Key Infrastructure (PKI)
: System zum Erstellen, Verteilen und Prüfen von digitalen Zertifikaten

Remote Authentication Dial-In User Service (RADIUS)
: Authentisierungs- und Überwachungsprotokoll auf Anwendungsebene für Authentisierung, Integritätsschutz und Accounting im Bereich Netzzugang

Robust Security Network (RSN)
: WLAN, das ausschließlich eine durch die in IEEE 802.11i spezifizierten Sicherheitsmechanismen geschützte Kommunikation erlaubt

Service Set Identifier (SSID)
: Durch den Netzadministrator vergebener Name des WLAN. Wird bei der Anmeldeprozedur und optional zyklisch in Beacon Frames (vom Access Point zyklisch übertragene Pakete, die Übertragungsparameter enthalten) übertragen.

Spoofing
: Untergrabung von Authentisierungs- und Identifikationsverfahren durch Methoden, die auf der Verwendung vertrauenswürdiger Adressen oder Hostnamen beruhen

Temporal Key Integrity Protocol (TKIP)
: Im Standard IEEE 802.11i spezifiziertes Protokoll zur Verschlüsselung und zum Integritätsschutz in WLAN; abwärtskompatibel zu WEP

Transport-Layer Security (TLS)
: Standardisiertes Verschlüsselungsprotokoll für Datenübertragungen im Internet; Weiterentwicklung von SSL (Secure Socket Layer)

Wi-Fi Alliance
: Vereinigung von Herstellern von WLAN-Komponenten nach IEEE 802.11

Wi-Fi Protected Access (WPA)
: Von der Wi-Fi Alliance veröffentlichter Standard, der auf einem Draft zu IEEE 802.11i basiert und aufwärtskompatibel zu IEEE 802.11i ist; die Folgeversion WPA2 deckt alle zwingenden Anforderungen von IEEE 802.11i ab

Wired Equivalent Privacy (WEP)
: Im Standard IEEE 802.11 spezifiziertes Protokoll zum Schutz von Vertraulichkeit, Integrität und Authentizität im WLAN; mittlerweile vollständig kompromittiert und für die Absicherung eines WLAN allein als ungenügend einzustufen

Wörterbuch-Attacke
: Eine Wörterbuch-Attacke (auch als Dictionary-Attacke bezeichnet) wird typischerweise zum Raten eines Passworts oder Schlüssels eingesetzt. Man geht bei dieser Methode davon aus, dass Passworte oder Schlüssel aus einer sinnvollen oder in Wörterbüchern bekannten Zeichenkombination bestehen. In diesem Falle kann das Verfahren schnell zum Erfolg führen.

Zelle
: Siehe Funkzelle

Zertifikat

Von einer Certificate Authority beglaubigter öffentlicher Schlüssel, der einer Person oder einem Objekt zugeordnet ist

B. Bluetooth

Inhaltsverzeichnis des Abschnitts

1. Grundlagen / Funktionalität

Bluetooth ist ein offener Industriestandard [IEEE02] für ein lizenzfreies Nahbereichsfunkverfahren zur kabellosen Sprach- und Datenkommunikation zwischen IT-Geräten (Kabelersatz und Ad-hoc-Networking).

Die Entwicklung von Bluetooth geht auf eine Initiative der so genannten Bluetooth Special Interest Group (Bluetooth SIG) im Jahre 1998 zurück, der eine große Zahl Hersteller angehört. Die derzeit aktuelle Version der Spezifikation ist V2.0 [BTSIG04]. Auf dieser basierende Produktangebote sind bereits verfügbar, es werden aber auch noch zahlreiche Geräte verwendet und angeboten, die auf einer der Vorgängerversionen 1.x basieren.

1.1 Technische Grundlagen

Bluetooth arbeitet im 2,4-GHz-ISM-Frequenzband auf 79 Kanälen im Frequenzbereich von 2400 bis 2483,5 MHz[1]. Der Kanalabstand beträgt 1 MHz; an den Bandgrenzen wurden 2 bzw. 3,5 MHz freigelassen, damit keine Störungen benachbarter Systeme auftreten.

Die Übertragung der Datenpakete erfolgt zeitschlitzgesteuert (TDD) in Verbindung mit einem Frequenzsprungverfahren (FHSS). Dies dient zur Reduzierung der Empfindlichkeit gegenüber Störungen. Die Zeitschlitzlänge beträgt 625µs, woraus eine Frequenzwechselhäufigkeit von bis zu 1600 pro Sekunde resultiert. Im Allgemeinen findet ein Frequenzsprung nach jedem versendeten Paket statt. Die Sprung-Sequenz ist pseudozufällig, deckt alle 79 Kanäle gleichmäßig in kurzen Zeitabständen ab und wiederholt sich erst nach Ablauf mehrerer Stunden. Die Bluetooth-Spezifikation 1.2 hat als wesentliche Neuerung ein adaptives Frequenzsprungverfahren (AFH) eingeführt, das die von der Sprungsequenz abgedeckten Kanäle auf freie, d.h. ungestörte Frequenzen beschränkt. Hierdurch soll ein störungsfreier Parallelbetrieb mit anderen Funkdiensten, die im selben Frequenzbereich operieren, insbesondere Wireless LAN, erreicht werden.

Als Modulationsverfahren wird eine Frequenz- bzw. Phasenmodulation angewandt. Dabei findet der Frequenz- bzw. Phasensprung grundsätzlich einmal pro Mikrosekunde statt; man spricht von einer Symbolrate von 1 MS/s (Megasymbols/s). Die resultierende Datenrate ergibt sich aus dem angewendeten Modulations-Verfahren, das die Zahl der pro Symbol übertragenen Bits bestimmt. Bluetooth kennt drei verschiedene Verfahren:

- Eine binäre Frequenzmodulation (GFSK), bei der ein Bit pro Symbol übertragen wird. Die resultierende Datenrate beträgt 1 MBit/s und wird als „Basic Rate“ bezeichnet. Dieses Verfahren wurde bereits in der ursprünglichen Bluetooth-Spezifikation 1.1 [IEEE02] veröffentlicht. Alle Bluetooth-Lösungen müssen dieses Verfahren unterstützen.
- Eine vierwertige Phasenmodulation (π/4-DQPSK), bei der zwei Bits pro Symbol übertragen werden. Die resultierende Datenrate, als „Enhanced Data Rate“ bezeichnet, beträgt 2 MBit/s. Dieses Verfahren ist Teil der Spezifikation Bluetooth Version 2.0 + EDR [BTSIG04].
- Eine achtwertige Phasenmodulation (8DPSK), bei der drei Bits pro Symbol übertragen werden. Die resultierende Datenrate, ebenfalls als „Enhanced Data Rate“ bezeichnet, beträgt 3 MBit/s. Auch dieses Verfahren ist Teil der Spezifikation Bluetooth Version 2.0 + EDR [BTSIG04].

Eine Kompatibilität von Stationen unterschiedlicher Bluetooth-Spezifikation wird dadurch erreicht, dass die Protokollinformation am Beginn eines jeden Pakets grundsätzlich mit der „Basic Rate“ ausgesendet wird. Erst zur Übertragung der Nutzdaten wird auf eine Variante von EDR umgeschaltet, sofern die Gegenstation dies unterstützt.

---

[1] Diese Angaben gelten für Deutschland und die meisten europäischen Länder.

Bluetooth nutzt zwei grundsätzlich verschiedene Modi der Datenübertragung:

- Asynchrone verbindungslose Übertragung (ACL): Datenpakete werden gesendet, sobald ein Freiraum (Slot) besteht. Jedes Paket trägt eine Zieladresse, anhand derer es an den Empfänger vermittelt wird. Das Verfahren gleicht der Übertragung in Wireless LAN.
- Synchrone verbindungsorientierte Übertragung (SCO): Datenpakete werden in einem festen Zeitraster zwischen Stationspaaren ausgetauscht. Das Verfahren entspricht der leitungsvermittelten Übertragung in einem Telefonnetz.

Die erzielbaren Brutto-Datenraten bei ACL betragen maximal 723 kBit/s in der einen und 58 kBit/s in der anderen Richtung (asymmetrisch) bzw. maximal 434 kBit/s in beide Richtungen (symmetrisch). Mit EDR lässt sich die 3fache Übertragungsrate erzielen, d.h. maximal 2,2 MBit/s in der einen und 177 kBit/s in der anderen Richtung (asymmetrisch) bzw. 1,3 MBit/s in beide Richtungen (symmetrisch).

SCO wird für die Übertragung von Sprache eingesetzt. Zu diesem Zweck stehen jeder Station drei Kanäle mit einer Bandbreite von je 64 kBit/s zur Verfügung. Die Kodierung der Sprache erfolgt unter anderem mit logarithmischen PCM-Codecs, die auch in der ISDN-Telefonie eingesetzt werden (ITU-T G.711 µ-law/a-law). Ab der Bluetooth-Spezifikation 1.2 stehen synchrone Kanäle mit höherer Bandbreite zur Verfügung, die mit „Extended SCO“ (eSCO) bezeichnet werden. Im Gegensatz zu SCO erlaubt eSCO eine Neuübertragung fehlerhaft empfangener Datenpakte, um die Dienstqualität auch unter ungünstigen Empfangsverhältnissen zu verbessern.

Bluetooth-Stationen werden bezüglich ihrer Sendeleistung klassifiziert. Klasse 1 hat eine maximale Sendeleistung von 100 mW, Geräte mit bis zu 2,5 mW werden in Klasse 2 eingeordnet, solche mit 1 mW in Klasse 3. Die Reichweite variiert von bis zu 10 Metern bei 1 mW bis zu ca. 100 Metern bei 100 mW Sendeleistung. Zur Senkung des Stromverbrauchs sind verschiedene Spar-Modi (Sniff-, Park- und Hold-Mode) und eine Sendeleistungsregelung (Power Control) spezifiziert.

1.2 Protokollarchitektur

Neben den hardwarenahen Protokollen (Funktechnik und Basisband) definiert die Spezifikation [IEEE02] für das Verbindungsmanagement eine Link-Schicht, die neben Fehlerkorrekturverfahren auch kryptographische Sicherheitsmechanismen bereitstellt. Zusätzlich verfügt sie über eine Host-Controller-Schnittstelle sowie diverse weitere Protokolle für unterschiedliche Applikationen. Eine ausführliche Beschreibung des Bluetooth Protokoll-Stacks findet man in der Literatur (z.B. in [WOLL01]).

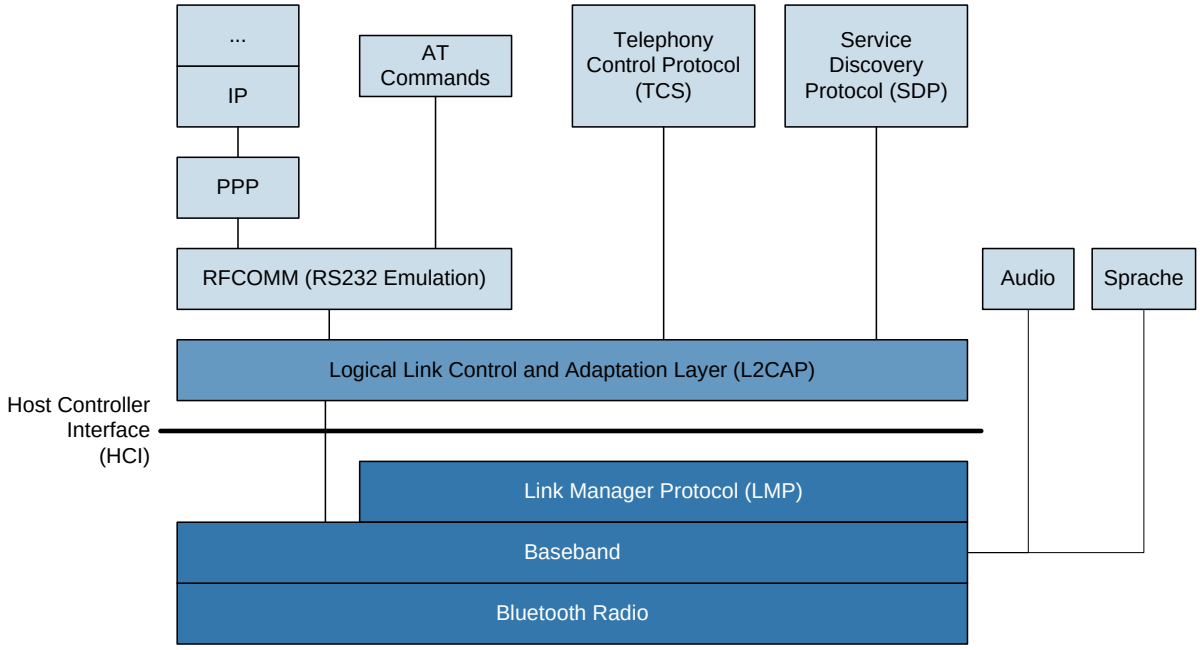


Abb. B-1: Bluetooth Protokoll-Stack

Um die Interoperabilität unterschiedlicher Geräte sicherzustellen, ohne dass in allen Geräten immer alle existierenden Protokolle implementiert sind, hat die Bluetooth SIG so genannte Anwendungs-Profile definiert. Einige häufig verwandte Profile sind:

- Generic Access Profile (GAP): GAP ist ein grundlegendes Profil zur herstellerübergreifenden Kommunikation von Bluetooth-Geräten. Auf GAP basieren viele Anwendungsprofile.
- Serial Port Profile: Serielle Kabelverbindungen (RS-232) zwischen zwei Geräten werden durch Bluetooth ersetzt; das entsprechende Protokoll heißt RFCOMM. Aus der Sicht der Anwendungsprogramme wird durch dieses Profil eine virtuelle serielle Schnittstelle bereitgestellt. Der im Vergleich mit anderen Funktechniken kostengünstige Ersatz serieller Leitungen durch Bluetooth spielt z.B. in der fertigenden Industrie eine Rolle, wo Leitungen häufig erhöhten Belastungen ausgesetzt sind (ständige Bewegung, Schmutz, usw.).
- Headset Profile und Handsfree Profile: Diese beiden Profile beschreiben Funktionen, die ein Mobiltelefon im Zusammenspiel mit einer Freisprecheinrichtung benötigt. Neben der reinen Übertragung von Sprache in beiden Richtungen spielt beim Handsfree Profil auch die Fernbedienung des Mobiltelefons eine Rolle.
- Human Interface Device Profile (HID Profile): Dieses Profil beschreibt die Protokolle und Funktionen, die zur drahtlosen Anbindung von Tastaturen, Zeigegeräten („Mäusen“) und Anzeigegeräten an Rechner benötigt werden. Das HID-Profil ersetzt die entsprechenden Funktionen des drahtgebundenen Universal System Bus (USB).
- Dialup Network Profile (DUN Profile) und Fax Profile: Diese Profile beschreiben Protokolle und Funktionen zur drahtlosen Anbindung von Modems oder Mobiltelefonen an Rechner mit dem Ziel, darüber Wählverbindungen zur Daten- oder Telefaxübertragung aufzubauen.
- File Transfer, Object Push und Synchronization Profile: Diese Profile werden zum Austausch von Dateien über Bluetooth genutzt. Wichtigste Anwendung ist die Synchronisierung von Kontakten, Terminen, Aufgaben und Mails zwischen tragbaren Geräten („Personal Information Manager“, PIM) und Servern. Die Profile basieren auf dem Protokoll OBEX.
- SIM Access Profile (SAP): Eine Bluetooth-Station greift auf Daten zu, die in der SIM-Karte einer anderen Station – typischerweise in einem Mobiltelefon – gespeichert sind. Ein typischer Anwendungsfall besteht in einem fest im Fahrzeug eingebauten Autotelefon, das keine eigene SIM-Karte

enthält. Stattdessen nimmt es Kontakt zu dem Mobiltelefon des Fahrers auf und meldet sich mit dessen Daten (und auf dessen Kosten) am Mobilfunknetz an.

1.3 Verbindungsaufbau und Netztopologien

Damit jedes Bluetooth-Gerät als Kommunikationspartner eindeutig zu identifizieren ist, verfügt es über eine 48 Bit lange öffentlich bekannte und weltweit eindeutige Geräteadresse, die so genannte Bluetooth Device Address.

Der Verbindungsaufbau erfolgt über die Prozeduren „Inquiry“ und „Paging“.

- Per Inquiry kann ein Bluetooth-Gerät feststellen, ob sich andere Geräte im Sendebereich befinden. Nach einem Inquiry liegen alle Geräteadressen und Zeittakte der gefundenen kommunikationsbereiten Geräte vor. Voraussetzung für das Auffinden eines Gerätes mittels Inquiry ist, dass dieses Gerät als erkennbar konfiguriert ist („discoverable“).
- Durch eine Paging-Anforderung kann eine Kommunikationsverbindung zu einem per Inquiry gefundenen Gerät aufgebaut werden. Das Gerät, das die Verbindung aufbaut, wird Master genannt, das andere Slave. Während des Pagings sendet der Master seine Geräteadresse und seinen Zeittakt an den Slave.

Neben einer Punkt-zu-Punkt-Verbindung zwischen zwei Bluetooth-Geräten unterstützt Bluetooth auch Punkt-zu-Mehrpunkt-Verbindungen. Bis zu 255 Bluetooth-Geräte (im Sonderfall auch mehr) können in einem so genannten Piconet als Slaves im Park-Mode mit einem Master vernetzt sein. Innerhalb eines Piconet können bis zu 7 Slaves gleichzeitig aktiv mit dem Master kommunizieren. Alle Geräte in einem Piconet folgen der gleichen Channel-Hopping-Sequence und dem Zeittakt des Masters. Prinzipiell sieht Bluetooth sogar die Möglichkeit einer Vernetzung von bis zu zehn Piconets zu einem so genannten Scatternet vor. Zur Bildung von Scatternetzen und zum anschließenden Datenaustausch in einem solchen Netz werden jedoch zusätzliche Protokolle benötigt, für die es derzeit nur Ideen, jedoch keine praktischen Implementierungen gibt.

2. Sicherheitsmechanismen

2.1 Kryptographische Sicherheitsmechanismen

Da Bluetooth ein funkbasierendes Verfahren ist, besteht grundsätzlich die Gefahr, dass "unberechtigte" Bluetooth-fähige Geräte die Bluetooth-Kommunikation mithören bzw. sich aktiv in die Kommunikationsverbindung einschalten. Die in der Bluetooth-Spezifikation vorgesehenen kryptographischen Sicherheitsmechanismen haben die Ausschaltung dieser beiden Bedrohungen zum Ziel. Diese Funktionen sind bereits auf Chip-Ebene implementiert und stehen auf der Link-Schicht einheitlich zur Verfügung.

Basis aller eingesetzten kryptographischen Verfahren sind Verbindungsschlüssel (Link Keys), die während der so genannten Paarung zwischen jeweils zwei Bluetooth-Geräten vereinbart werden.

Paarung (Pairing) und Verbindungsschlüssel

In der Regel wird beim Pairing zweier Bluetooth-Geräteein nur für die Verbindung dieser beiden Geräte genutzter, 128 Bit langer Kombinationsschlüssel (Combination Key) erzeugt und in jedem Gerät zur zukünftigen Nutzung als Verbindungsschlüssel (Link Key, LK) gespeichert.

Die Erzeugung des Kombinationsschlüssels (K(AB)) geht von einem Paar aus Geräteadresse (BD_ADDR) und Zufallszahl (LK_RAND) pro Gerät aus. Eine kryptographische Funktion mit der Bezeichnung E_{21} gemäß [IEEE02] wird angewandt, um jedes dieser Paare miteinander zu einem Wert

LK_K(A) bzw. LK_K(B) zu kombinieren. Beide LK_K werden in einer Exklusiv-Oder-Funktion miteinander verknüpft und ergeben den Kombinationsschlüssel (K(AB)) (siehe Abb. B-2).

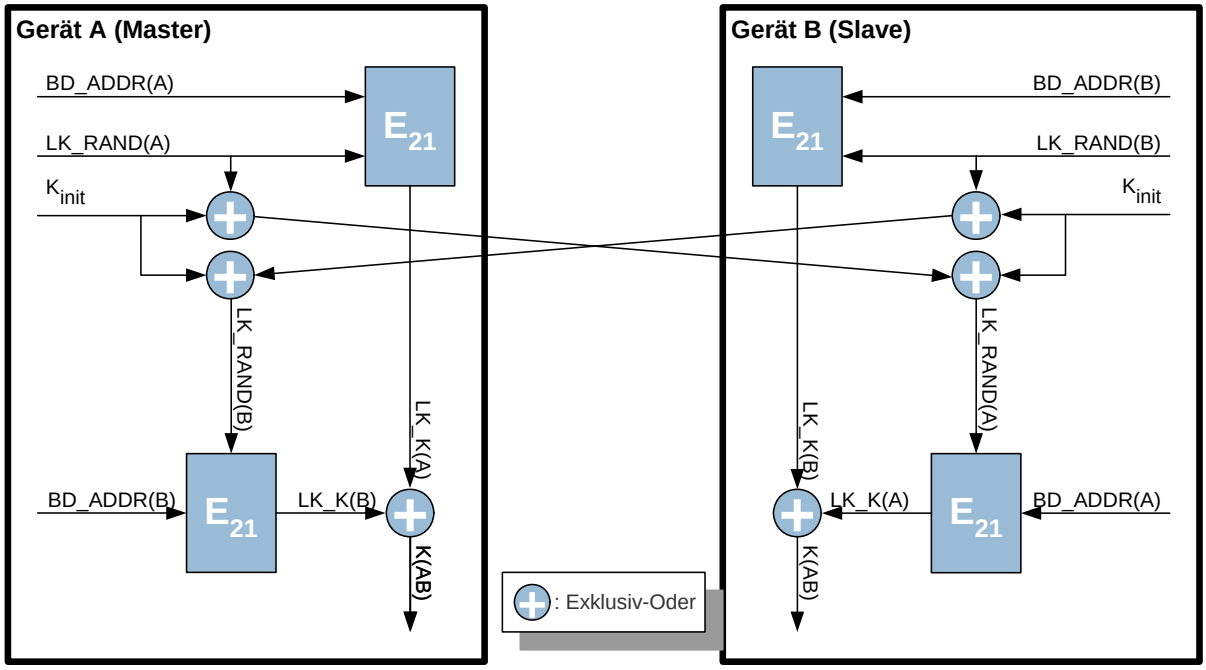


Abb. B-2: Erzeugen des Kombinationsschlüssels

Damit die genannten Verknüpfungen in beiden Geräten erfolgen können, ist die im Gerät erzeugte Zufallszahl LK_RAND auf das jeweils andere Gerät zu übertragen. Für die gesicherte Übertragung der Zufallszahlen wird ein Initialisierungsschlüssel K_{init} verwendet, der sich aus einer weiteren (öffentlichen) Zufallszahl, der Geräteadresse eines Teilnehmers und einer im Allgemeinen konfigurierbaren PIN berechnet. Die Berechnung erfolgt mittels einer kryptographischen Funktion mit der Bezeichnung E_{22} gemäß [IEEE02]. Eingangswerte sind neben der Zufallszahl RAND die mit der Geräteadresse BD_ADDR „verlängerte“ PIN sowie die Länge L’ der sich daraus ergebenden PIN’ (siehe Abb. B-3).

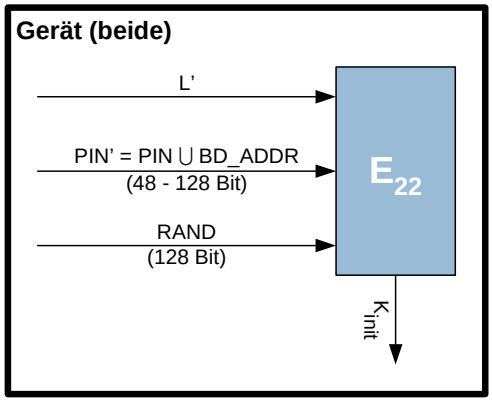


Abb. B-3: Erzeugen des Initialisierungsschlüssels

Für ein erfolgreiches Pairing muss in beide Geräte die gleiche PIN eingetragen werden. Die PIN kann 1 bis 16 Byte lang sein und ist entweder durch den Nutzer konfigurierbar oder fest voreingestellt. Verfügt eines der Geräte über eine feste PIN, so muss diese in das andere Gerät eingegeben werden.

Die Eingabe einer langen PIN an zwei Geräten durch den Nutzer ist fehleranfällig und kann zudem mit Zeitschranken für den Paarungs-Ablauf in Konflikt kommen. Zur Vermeidung dieses Problems schlägt der aktuelle Bluetooth-Standard 2.0 alternativ einen automatisierten Austausch zwischen den beiden

Bluetooth-Geräten vor, z.B. auf Basis des Diffie-Hellmann-Verfahrens. Dieser Austausch wäre jedoch durch eine Anwendungs-Software zu bewerkstelligen und ist nicht Teil des Standards.

Neben den Kombinationsschlüsseln erlaubt der Standard weitere Möglichkeiten für Link Keys:

- Geräteschlüssel (Unit Keys) können als Link Key genutzt werden. Der Geräteschlüssel wird bei der erstmaligen Verwendung eines Bluetooth-Gerätes erzeugt und normalerweise nicht mehr geändert. Geräteschlüssel werden beispielsweise verwendet, wenn ein Gerät nicht genügend Speicherplatz für weitere Schlüssel besitzt oder ein Gerät einer großen Gruppe von Nutzern zugänglich sein soll.
- Master-Schlüssel (Master Keys) können für die Dauer einer Bluetooth-Sitzung zwischen mehreren Geräten (temporär) vereinbart werden, wenn ein Master mehrere Geräte unter Verwendung desselben Verschlüsselungsschlüssels erreichen will. Master-Schlüssel werden nur bei Punkt-zu-Mehrpunkt-Verbindungen eingesetzt und über die aktuellen Link Keys gesichert vom Master an die Slaves übertragen.

Authentisierung

Zur Authentisierung wird ein Challenge-Response-Verfahren auf Basis eines symmetrischen Chiffrier-Verfahrens verwendet. Es wird grundsätzlich eine einseitige Authentisierung genutzt, d.h. ein Gerät (Claimant) authentisiert sich gegenüber einem anderen Gerät (Verifier). Wollen sich beide Geräte gegenseitig authentisieren, wird die Authentisierung mit vertauschten Rollen wiederholt.

Die Authentisierung läuft wie folgt ab (siehe Abb. B-4): Der Verifier sendet eine Zufallszahl (AU_RAND) an den Claimant. Dieser beweist, dass er als gemeinsames Geheimnis den Link Key (LK) kennt, indem er unter Benutzung dieses Geheimnisses aus der Zufallszahl und seiner eigenen Geräteadresse (BD_ADDR) eine 32 Bit lange Antwort (SRES) berechnet und zum Verifier zurücksendet. Der Verifier überprüft die Antwort, indem er die gleiche Berechnung durchführt. Sind die Ergebnisse identisch, ist der Claimant authentisiert, d.h. LK(A) ist gleich LK(B).

Gleichzeitig berechnen beide Geräte einen 96 Bit langen so genannten Authenticated Cipher Offset (ACO), der geheim gehalten wird und bei Bedarf der Erzeugung eines Verschlüsselungsschlüssels dient.

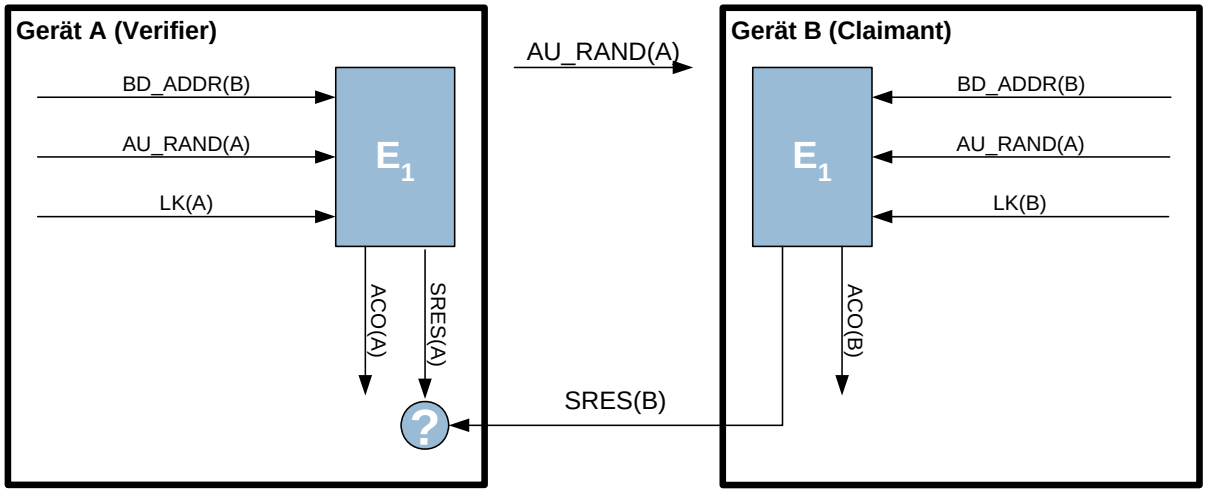


Abb. B-4: Authentisierung bei Bluetooth (vereinfacht)

Verschlüsselung

Die Verschlüsselung kann optional verwendet werden, wenn sich mindestens eines der beiden kommunizierenden Geräte gegenüber dem anderen authentisiert hat. Dabei kann die Verschlüsselung sowohl vom Master, als auch vom Slave beantragt werden. Die Verschlüsselung selbst wird jedoch immer vom Master gestartet, nachdem er die notwendigen Parameter mit dem Slave ausgehandelt hat.

Dazu einigen sich die beiden Geräte zunächst auf die Länge des zu verwendenden Schlüssels. Anschließend startet der Master die Verschlüsselung, indem er eine Zufallszahl an den Slave sendet. Der Verschlüsselungsschlüssel (K_C) berechnet sich in der Hash-Funktion E_3 aus dem Link Key (LK), einem Cipher Offset (COF) und einer Zufallszahl (EN_RAND), die vor Beginn der verschlüsselten Kommunikation im Klartext übertragen wird und somit den Kommunikationspartnern bekannt ist (siehe Abb. B-5).

Es stehen für die Verschlüsselung zwei Betriebsarten zur Verfügung: Punkt-zu-Punkt-Verschlüsselung und Punkt-zu-Mehrpunkt-Verschlüsselung. Bei der Punkt-zu-Punkt-Verschlüsselung wird der ACO des Authentisierungsprotokolls (siehe Abb. B-4) als COF verwendet. Bei der Punkt-zu-Mehrpunkt-Verschlüsselung wird dagegen die Geräteadresse des Masters als COF genutzt. Außerdem muss der Link Key durch einen Master-Schlüssel ersetzt werden, bevor die Verschlüsselung gestartet wird. Eine Punkt-zu-Mehrpunkt-Verschlüsselung wird z.B. in einem Piconetz benötigt, wenn der Master eine Nachricht an mehrere Slaves sendet (Multicast).

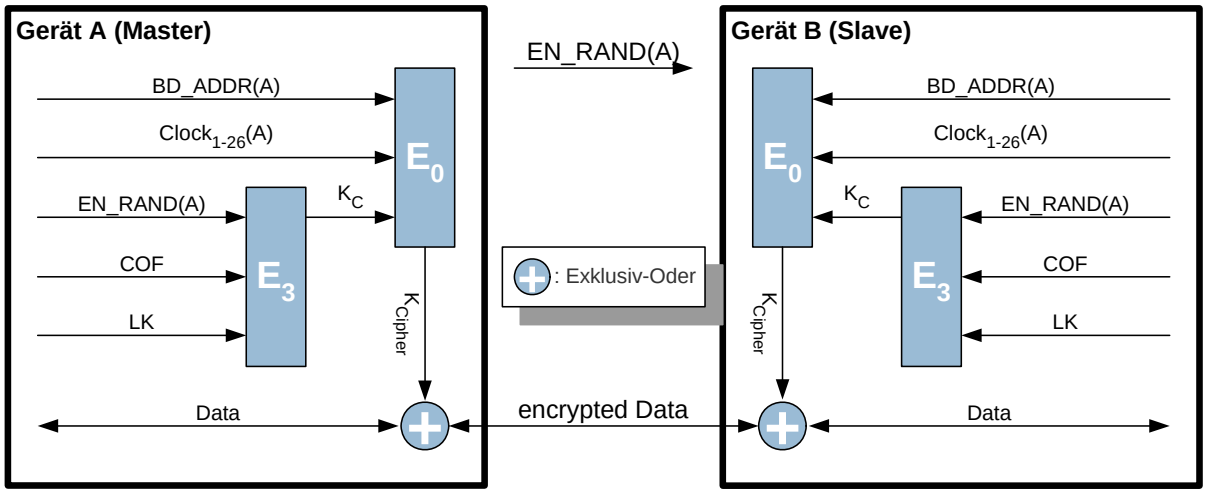


Abb. B-5: Verschlüsselung bei Bluetooth (vereinfacht)

Zum Verschlüsseln wird eine Stromchiffre (im Standard mit E_0 bezeichnet) eingesetzt. Für jedes Datenpaket wird dabei ein neuer Schlüsselstrom (K_{Cipher}) aus der Geräteadresse (BD_ADDR), dem Verschlüsselungsschlüssel (K_C) sowie 26 Bits aus dem Zeittakt des Masters ($Clock_{1-26}$) berechnet (siehe Abb. B-5). Verschlüsselt sind die Daten nur während des Transports per Funk. Vor der Aussendung bzw. nach Empfang liegen die Daten in den beteiligten Geräten unverschlüsselt vor; es handelt sich also nicht um eine Ende-zu-Ende-Verschlüsselung (d.h. Verschlüsselung der Daten von der Eingabe in Endgerät A bis zur Ausgabe bzw. Bearbeitung in Endgerät B).

2.2 Sicherheitsbetriebsarten

Die Spezifikation beschreibt im Generic Access Profile drei Sicherheitsmodi:

- **Sicherheitsmodus 1 („non-secure“)**: Das Bluetooth-Gerät initiiert selbst keine speziellen Sicherheitsmechanismen, reagiert aber auf Authentisierungsanfragen anderer Geräte.
- **Sicherheitsmodus 2 („service level enforced security“)**: Auswahl und Nutzung von Sicherheitsmechanismen werden abhängig vom Bluetooth-Gerät ("trusted" oder "non-trusted") und vom Dienst auf Anwendungsebene festgelegt. Das Gerät leitet erst dann Sicherheitsprozeduren ein, wenn es eine Aufforderung zum Verbindungsaufbau erhalten hat.
- **Sicherheitsmodus 3 („link level enforced security“)**: Es ist generell eine Authentisierung beim Verbindungsaufbau erforderlich; die Verschlüsselung der zu übertragenden Daten ist optional.

Darüber hinaus sind für die Erkennbarkeit von Bluetooth-Geräten beim Inquiry die Modi "non-discoverable" (Gerät antwortet nicht auf Inquiry) bzw. "limited discoverable" und "general discove-

rable" spezifiziert. Weiterhin gibt es die Betriebsmodi "non-connectable" (keine Reaktion auf Paging-Anforderungen) bzw. "connectable" sowie "non-pairable" (kein weiteres Pairing möglich) und "pairable".

3. Gefährdungen bei der Nutzung

Zu all den Gefährdungen, denen leitungsgebundene Netzwerke ausgesetzt sind (siehe [BSIGSH]), ergeben sich bei der Nutzung von Funknetz-Technik zusätzliche Gefährdungen, die insbesondere auf den Sicherheitsschwächen der verwendeten Protokolle sowie auf der unkontrollierten Ausbreitung der Funkwellen basieren.

3.1 Schwächen im Sicherheitskonzept des Standards

3.1.1 Verschlüsselung nicht vorgeschrieben

Unabhängig vom verwendeten Sicherheitsmodus ist die Verschlüsselung der übertragenen Daten optional und muss von den Anwendungen explizit beantragt werden.

3.1.2 Unsichere Voreinstellungen

Die Voreinstellungen sind von Seiten des Herstellers oft unsicher konfiguriert: Sicherheitsfunktionen wie Authentisierung und Verschlüsselung sind häufig abgeschaltet und PINs auf "0000" eingestellt. Wenn Geräte keine Eingabemöglichkeit besitzen (z.B. Headsets), ist eine Änderung der voreingestellten Werte gar nicht oder nur schwer möglich.

3.1.3 Erraten schwacher PINs

Wird bei der Gerätepaarung eine schwache PIN verwendet, kann ein Angreifer die PIN erraten und damit den aus der Paarung resultierenden Verbindungsschlüssel berechnen. Dazu muss der Angreifer nur die Paarung und die folgende Authentisierung abhören. Anhand der Aufzeichnungen der abgehörten Protokolle kann der Angreifer überprüfen, ob die PIN von ihm korrekt geraten wurde. Auf diese Weise ist es möglich, kurze oder triviale (z.B. "1234567890") PINs zu ermitteln.

Als sicherheitskritisch anzusehen ist, dass PINs als einzige geheime Parameter bei der Verbindungsschlüsselerzeugung eingehen. Erfahrungsgemäß lassen sich hier weit verbreitete Nutzer- bzw. Herstellergewohnheiten zu schwachen Sicherheitseinstellungen nur schwer durchbrechen.

Es ist festzuhalten, dass die Berechnung einer PIN nach Abhören des Paarungs- und Authentisierungsvorgangs keine rein theoretische Gefährdung ist. Die Autoren von [SHWO05] haben eine Methode beschrieben und auch praktisch implementiert, mit der beispielsweise 7-stellige PINs, die nur aus Ziffern bestehen, innerhalb von 77 Sekunden berechnet werden können[2]. Voraussetzung für die Durchführung dieser Angriffsmethode ist das vollständige Mitschneiden von Paarung und Authentisierung mit einem entsprechenden Werkzeug nebst Software zur Dekodierung der Paketinhalte (z.B. Bluetooth-fähiger Software-Analysator).

3.1.4 Unsichere Geräteschlüssel

Werden Geräteschlüssel von einem Gerät als Verbindungsschlüssel verwendet, so wird für jede Verbindung mit diesem Gerät immer der gleiche Schlüssel benutzt. Gelingt es dem Angreifer, eine Ver-

[2] Verwendete Rechner-Hardware: Pentium IV, 3 GHz

bindung mit diesem Gerät aufzubauen, ist er anschließend in der Lage, sich für dieses Gerät auszugeben oder jede Kommunikation mit diesem Gerät abzuhören.

Es handelt sich dabei nicht um eine theoretische Gefährdung. Diese Schwäche ist bei aktuellen Bluetooth-basierten Anwendungsformen vorzufinden. [TRIFORG] beschreibt unter der Bezeichnung „Car Whisperer“, wie besonders schwache Geräteschlüssel in manchen Herstellerlösungen dazu missbraucht werden können, einfach Zugriff auf Bluetooth-fähige Freisprecheinrichtungen oder Headsets in fremden Autos zu erhalten. Auf diese Weise können Gespräche im Fahrzeug abgehört oder den Fahrzeuginsassen Botschaften „eingeflüstert“ werden. Dieses Experiment wurde zum Nachweis der Praxisrelevanz der Sicherheitsschwachstelle „Geräteschlüssel mit schwachen oder gar bekannten Voreinstellungen“ durchgeführt und veröffentlicht.

3.1.5 Reinitialisierung Semi-permanenter Verbindungen

Der Bluetooth-Standard unterscheidet temporäre und semi-permanente Verbindungsschlüssel.

Temporäre Verbindungen benutzen den Verbindungsschlüssel als eine Art Einmal-Schlüssel, d.h. für jede neue Verbindung wird ein neuer Verbindungsschlüssel erzeugt (ein Paarungs-Vorgang je Verbindung). Dies ist aufgrund der Abhörbarkeit des Paarungsvorgangs sicherheitstechnisch ungünstig, da so die Wahrscheinlichkeit steigt, bei einem Abhörversuch Zeuge eines solchen Vorgangs zu werden und verwendete schwache PINs durch Berechnung ermitteln zu können.

Semi-permanente Verbindungsschlüssel werden von den beteiligten Bluetooth-Geräten nach Paarungs- und Authentisierungsvorgang in einem nichtflüchtigen Speicher festgehalten. Bei einer erneuten Verbindungsaufnahme entfällt somit die Paarung, die Authentisierung mehrerer aufeinander folgender Verbindungen zwischen den Geräten kann mit Hilfe der gespeicherten Verbindungsschlüssel vorgenommen werden. Die Häufigkeit von Paarungsvorgängen, die zur PIN-Ermittlung abgehört werden können, sinkt damit deutlich. Sie kann theoretisch auf gewollte Zeitpunkte, z.B. bewusste regelmäßige PIN-Wechsel durch den Nutzer reduziert werden.

Allerdings sieht die Bluetooth-Spezifikation neben einer solchen geplanten Ablösung semi-permanenter Verbindungsschlüssel auch den Fall des Informationsverlustes bei einem der beteiligten Geräte vor. Auf Grund verschiedener, in [SHWO05] beschriebener Anzeichen stellt das andere Gerät fest, dass der Partner nicht länger über den bisherigen semi-permanenten Schlüssel verfügt. Über eine neuerliche, automatisch initiierte Paarung wird dann von beiden ein neuer semi-permanenter Schlüssel generiert.

Die Anzeichen, die dieses Verhalten auslösen, bestehen in einer Abweichung innerhalb der Paketabfolge. Das Gerät, dem der bisherige Verbindungsschlüssel nicht länger bekannt ist, verhält sich bei der Authentisierung anders, als wenn es die Schlüsselinformation noch besäße.

Hierauf lässt sich eine weitere, in [SHWO05] beschriebene Angriffsmethode aufbauen: Ein Angreifer streut geschickt im passenden Moment ein entsprechendes, jedoch abweichendes Paket ein. Nötigenfalls wird dabei durch das Angreifer-Gerät die Adresse des Bluetooth-Geräts, dessen Schlüsselverlust simuliert werden soll, vorgespiegelt. Dies bedeutet: mit entsprechender Ausstattung lässt sich durch einen Angreifer bei Verwendung eines semi-permanenten Verbindungsschlüssels eine erneute Paarung provozieren, die dann abgehört werden kann.

Ein aufmerksamer Nutzer kann dies bemerken, wenn er ohne ersichtlichen Grund zur erneuten PIN-Eingabe aufgefordert wird. Ein entsprechend sensibilisierter Nutzer kann den Angriff scheitern lassen, indem er die PIN-Eingabe verweigert (kann dann aber vorübergehend seine Geräte nicht wie gewünscht verwenden). Bei Geräten, die keine PIN-Eingabe durch den Nutzer vorsehen, bleibt der Angriff völlig im Hintergrund. Außerdem sieht die Bluetooth-Spezifikation ausdrücklich die Möglichkeit vor, einen neuen Verbindungsschlüssel zu generieren, ohne eine PIN-Erneuerung vorzunehmen. Bei entsprechenden Implementierungen wird der Nutzer womöglich nur bei der ersten Paarung oder bei Abruf der Möglichkeit zur bewussten PIN-Änderung zur PIN-Eingabe aufgefordert.

3.1.6 Keine verbindliche Vorgabe einer ausreichenden Schlüssellänge

Während für Schlüssel, die zur Authentisierung benutzt werden, in der Bluetooth-Spezifikation eine Schlüssellänge von 128 Bit fest vorgeschrieben ist, kann die Länge des für die Verschlüsselung der weiteren Paketinhalte verwendeten Schlüssels variieren.

Nehmen Bluetooth-Geräte miteinander Verbindung auf und die Verwendung von Verschlüsselung ist vorgesehen, so handeln die beiden Geräte die tatsächlich genutzte Schlüssellänge aus. Die aktuelle Spezifikation Bluetooth v2.0 sieht hier eine Spannweite von 8 bis 128 Bit vor, d.h. eine minimale Schlüssellänge von 8 Bit kann verwendet werden, ohne gegen die Spezifikation zu verstoßen.

Dies wiegt umso schwerer, als dass eine Vorgabe der minimalen Schlüssellänge durch den Anwender ausdrücklich ausgeschlossen wird: die Spezifikation fordert, dass dies eine Fabrikeinstellung sein soll, die der Nutzer nicht überschreiben kann. Die Güte der erreichbaren Verschlüsselung ist damit allein abhängig von der Herstellerentscheidung. Als Nutzer kann man an dieser Stelle nur durch gezielte Wahl der eingesetzten Geräte Einfluss ausüben, vorausgesetzt, dass entsprechende Herstellerangaben zur eingestellten minimalen Schlüssellänge verfügbar sind. In allgemein zugänglichen Produktbeschreibungen fehlt eine solche Angabe oft völlig, oder es wird nur die maximale Schlüssellänge von 128 Bit angegeben.

3.1.7 Schwache Integritätssicherung

Zur Integritätssicherung wird ein Cyclic Redundancy Check (CRC, Verfahren zur Erkennung von Übertragungsfehlern anhand einer Prüfsumme) verwendet. Dadurch werden zwar mit hoher Wahrscheinlichkeit zufällige Störungen bei der Übertragung von Datenpaketen erkannt, aber gegen eine absichtliche Manipulation von Datenpaketen bieten CRC-Verfahren keinen Schutz.

3.1.8 Qualität des Zufallsgenerators

Zur Zufallserzeugung sind im Bluetooth-Standard keine Mechanismen festgelegt worden. Erfahrungsgemäß ist damit zu rechnen, dass die Güte der Zufallsgeneratoren hersteller- und implementierungsabhängig stark variiert.

3.2 Man-in-the-Middle-Angriffe

Ein weiteres Sicherheitsproblem von Bluetooth besteht darin, dass in bestimmten Konfigurationen so genannte "Man-in-the-Middle"-Angriffe möglich sind [KÜGL03].

Dabei schiebt sich ein Angreifer, der (unberechtigt) Zugriff auf ein Bluetooth-Gerät erhalten will, "mitten zwischen" zwei berechtigte Geräte. Anschließend kommunizieren die beiden Geräte über den Angreifer miteinander, der die Datenpakete abfängt und manipulieren kann. Folgende Szenarien sind denkbar:

- ► Der Angreifer baut aktiv eine Verbindung zu beiden Geräten auf.

  Der Angreifer verbindet sich mit beiden Geräten und gibt dabei vor, jeweils das andere Gerät zu sein. Sofern sich das Gerät des Angreifers gegenüber einem Gerät authentisieren muss, reicht es die Authentisierungsanfrage an das andere Gerät weiter und sendet die Antwort zurück. Anschließend kann der Angreifer mit dem Gerät beliebig interagieren. Als Voraussetzung für die erfolgreiche Durchführung dieses Angriffs müssen beide Geräte "connectable" sein (siehe Kapitel 2.2).
- ► Der Angreifer schaltet sich ein, während die Geräte mittels Pairing eine Verbindung aufbauen.

  Während des Verbindungsaufbaus müssen sich die Geräte auf die Sprungsequenz synchronisieren. Der Angreifer kann diese Synchronisation verhindern, so dass beide Geräte zwar die gleiche Sequenz, aber verschiedene Offsets in der Sequenz verwenden.

3.3 Probleme bei der Verschlüsselung

Die von Bluetooth optional verwendete Verschlüsselung hat einige Schwächen, die im Folgenden aufgeführt werden.

3.3.1 Sicherheit der Stromchiffre E_0

Obwohl E_0 Schlüssellängen von 1 bis 16 Bytes (8 - 128 Bit) akzeptiert, haben Fluhrer und Lucks gezeigt, dass die erreichbare Sicherheit je nach Stärke des Angreifers 73 bzw. 84 Bit nicht übersteigt [FLUH01].

3.3.2 Verkürzter Initialisierungsvektor

Jedes übertragene Datenpaket wird unter Verwendung eines neuen Initialisierungsvektors verschlüsselt. Dieser errechnet sich unter anderem aus dem Zeittakt des Masters. Es wird allerdings das höchstwertige Bit des Zeittaktes "vergessen". Diese Schwäche ist die Voraussetzung dafür, dass sich selbst bei eingesetzter Verschlüsselung Man-in-the-Middle-Angriffe (siehe Kapitel 3.2) durchführen lassen, da es immer zwei unterschiedliche Offsets in der Sprungsequenz zu einem Initialisierungsvektor gibt. Ein Man-in-the-Middle-Angriff auf verschlüsselte Verbindung erlaubt jedoch nur, den Datenstrom zu manipulieren (s.u.), nicht jedoch zu entschlüsseln.

3.3.3 Manipulation von verschlüsselten Daten

Aufgrund der Eigenschaften von Stromchiffren im Zusammenwirken mit dem zur Integritätssicherung eingesetzten CRC ist es möglich, Änderungen am Chiffrat dergestalt vorzunehmen, dass der Empfänger das Paket nach wie vor als gültig erkennt. So ist es beispielsweise im Rahmen eines Man-in-the-Middle-Angriffs möglich, IP-Header gezielt zu manipulieren.

3.4 Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen der Bluetooth-Komponenten breiten sich auch über räumliche Grenzen des Bluetooth-Nutzungsbereichs aus. Dabei kann auch in nicht vom Betreiber der Bluetooth-Geräte kontrollierten Bereichen ein Empfang möglich sein. Je nach Umgebungsbedingungen und Leistungsfähigkeit der verwendeten Empfangsgeräte (z.B. Richtantennen) besteht auch hier noch eine konkrete Abhörgefahr.

In der Sensibilisierung für die Praxisrelevanz von Bluetooth-Gefährdungen engagierte Fachleute (siehe [TRIFORG]) haben vorgeführt, dass sich mit entsprechend modifiziertem Gerät – inkl. Einsatz einer Richtantenne – die Bluetooth-Schnittstelle von Mobiltelefonen auf Entfernungen von nahezu 2 km erfolgreich angreifen lässt (z.B. Auslesen von gespeicherten Kontaktdaten).

3.5 Bewegungsprofile

Die eindeutigen Bluetooth-Geräteadressen können zum Verfolgen einzelner Geräte missbraucht werden. Auf diese Weise ist es möglich, Bewegungsprofile der Benutzer zu erstellen. Die Geräteadresse wird nicht nur zum Verbindungsaufbau verwendet, die Geräteadresse des Masters ist zum Teil (24 der 48 Bit) in jedem Datenpaket enthalten.

Ohne weiteres gelingt die Erkennung und Verfolgung von Bluetooth-Geräten mittels „Inquiry“, wenn diese als „discoverable“ konfiguriert sind (siehe Kapitel 1.3). Inzwischen hat man jedoch auch Methoden entwickelt, die Bluetooth-Geräte aufspüren, wenn sie auf „non discoverable“ eingestellt sind. Hierzu werden möglichen Bluetooth-Adressen durchprobiert. Ähnlich wie bei MAC-Adressen von Ethernet oder ähnlichen Verfahren ist auch bei Bluetooth der vordere Teil einer Bluetooth-Adresse

nicht willkürlich. Vielmehr beginnt eine solche Adresse generell mit einem herstellerspezifischen Präfix, wobei die entsprechend registrierten Abfolgen offen gelegt sind. In Kenntnis der in Frage kommenden Herstellerkennungen kann man einen Angriff erfolgreich durchführen, indem man alle möglichen Kombinationen der verbleibenden hinteren sechs Stellen durchprobiert und die so konstruierten Adressen gezielt anspricht.

3.6 Verfügbarkeitsprobleme

Die Verfügbarkeit kann unter anderem durch folgende Ursachen beeinträchtigt werden:

- Störung durch gezielt eingesetzte Störsender
- Denial-of-Service – Denkbar sind zum Beispiel Angriffe auf die Energiereserven einzelner Geräte durch Verhindern des Ruhe-Modus.
- Störungen durch andere Nutz-Anwendungen im gleichen ISM-Band

Prinzipiell verbessert die Einführung des Adaptive Frequency Hopping (AFH) mit Bluetooth 1.2 die Koexistenz von Bluetooth mit anderen Funkdiensten, indem die Nutzung belegter Kanäle vermieden wird. AFH ist jedoch nur während einer bestehenden Verbindung aktiv. Während der Verbindungsaufbauphase (Inquiry, Paging) werden dagegen feste Kanäle verwendet. Während dieser Phase besteht eine höhere Wahrscheinlichkeit der Störung durch andere Anwendungen im gleichen ISM-Band. Außerdem kann Bluetooth in dieser Phase störend auf andere Anwendungen – insbesondere WLAN – einwirken.

3.7 Implementierungsschwächen

Mit steigender Verbreitung von Bluetooth steigt auch die Wahrscheinlichkeit, dass Fehler in den Implementierungen der Hersteller auftreten, dass diese bekannt und schließlich für Angriffe ausgenutzt werden. Mittlerweile sind verschiedene Angriffsformen infolge fehlerhafter Implementierungen diskutiert und auch realisiert worden[3].

3.7.1 Ungeschützte Dienste

Voraussetzung für den Zugriff auf Dienste in Bluetooth-Geräten ist immer der erfolgreiche Abschluss des Pairing. Teil des Pairing ist generell eine Authentisierung anhand eines symmetrischen Schlüssels (PIN), die in Kapitel 2.1 beschrieben wurde. Ohne vorangegangenes Pairing lässt sich jedoch immer Kontakt zum Dienst „Service Discovery Protocol“ (SDP) aufnehmen, der dem Anwender die auf diesem Gerät zur Verbindung bereitstehenden Dienste mitteilt (siehe Abb. B-1).

In der Vergangenheit wurden jedoch Implementierungen bekannt, bei denen auch andere Dienste ohne vorangegangenes Pairing zugänglich waren. Die Hersteller hatten offensichtlich eine Art Hintertür geöffnet. Diese Dienste wurden jedoch vom SDP nicht bekannt gegeben, waren also für einen normalen Benutzer nicht sichtbar.

Auf Basis dieser Schwachstelle ließen sich unter anderem die folgenden Angriffe erfolgreich durchführen:

- Der Angreifer sendet so genannte AT-Kommandos an den ungeschützten Dienst RFCOMM und veranlasst so das Gerät zu den von ihm erwünschten Aktionen. Solche AT-Kommandos und die zugehörige Software-Schnittstelle sind eigentlich dazu gedacht, Telefonie-Geräte (Modems u.ä.) über serielle Verbindungen zu konfigurieren. Die entsprechenden Kommandos sind standardisiert und in [3GPP277] spezifiziert. Es lassen sich unter anderem Anruflisten von einem solchen Telefon kopieren sowie das Telefon vollständig fernsteuern (SMS-Versand oder SMS-Mitlesen, Ver-

[3] Z.B. BlueSnarf, BlueBug, Car Whisperer

änderung der Einstellungen, Nutzung des Telefons als Internet-Zugang, Änderung von Grundeinstellungen wie Rufweiterleitung, Provider-Voreinstellung usw.).

- Der Angreifer nutzt das Profil, das eigentlich für den einfachen Austausch von elektronischen Visitenkarten u. ä. vorgesehen ist (OBEX Push Profile). Dieser Dienst ist auf vielen Geräten nicht über Authentisierung gesichert. Da für Dateien wie Kalender oder Telefonbuch typischerweise Standardnamen verwendet werden, kann der Angreifer sich diese vom angegriffenen Gerät mit einem gezielten Befehl an diesen Dienst herunterladen. Unterstützt ein angegriffenes Bluetooth-Gerät nicht nur den einfachen OBEX Push-Dienst, sondern einen OBEX-basierenden FTP-Server, so kann ein Angreifer sogar unbefugt schreibenden Zugriff auf OBEX-Basis erhalten.

3.7.2 Denial of Service (DoS)

An Mobiltelefonen unterschiedlicher Hersteller wurden in der Vergangenheit fehlerhafte Implementierungen entdeckt, die es einem Angreifer ermöglichten, zeitweise den Bluetooth-Protokoll-Stack oder gar das gesamte Telefon lahm zu legen:

- Der Angreifer bombardiert ein fremdes Bluetooth-Gerät bis zur völligen Überlastung mit L2CAP echo requests.
- Bestimmte Mobiltelefone lassen sich mit einzelnen Bluetooth-Paketen außer Gefecht zu setzen, siehe [SOBS06].

3.8 Weitere Sicherheitsaspekte

Folgende Aspekte sind ebenfalls zu bedenken:

- Mobile Geräte sind gegenüber stationären Geräten einem höheren Diebstahlrisiko ausgesetzt.
- Authentisieren muss sich bei Bluetooth nur das Gerät gegenüber einem Kommunikationspartner, in der Regel aber nicht der Benutzer gegenüber dem Gerät. Bei Abhandenkommen mobiler, gepaarter Geräte sind diese also ohne weiteres im Herkunftsbereich durch unbefugte Dritte nutzbar.
- Bluetooth-Geräteadressen sind mit geeignetem Equipment manipulierbar (Flash-Memory).
- Auch in Ad-hoc-Netzwerken existiert die Gefahr der Verbreitung von Computer-Viren und trojanischen Pferden.
- Das Abhören bzw. Aufzeichnen von Raumgesprächen unter Verwendung von handelsüblichen oder speziell manipulierten Bluetooth-Geräten (z.B. Headset mit 100 mW Sendeleistung) ist grundsätzlich nicht auszuschließen (siehe hierzu auch [BSIGSM]).
- Generell kann man sich nicht vor Dritten sicher fühlen, nur weil zu diesen kein Sichtkontakt besteht (siehe 3.4).

4. Schutzmaßnahmen

Bluetooth-Geräte, die mindestens einen sicherheitsrelevanten Dienst anbieten, sollten Verschlüsselung mit Kombinationsschlüsseln unterstützen. Für eine maximale Sicherheit dürfen die Geräte keine Geräteschlüssel verwenden und müssen in geeigneter Weise abgesichert werden. Im Folgenden wird beschrieben, welche Maßnahmen ergriffen werden können und welche Rest-Risiken bestehen.

4.1 Absicherung von Bluetooth-Geräten

4.1.1 Gezielte Produktauswahl

Nach Möglichkeit sind keine Geräte einzusetzen, die mit Geräteschlüsseln arbeiten. Es sollte mindestens die Möglichkeit bestehen, Voreinstellungen zu überschreiben. Geräte mit möglichst guter minimaler Schlüssellänge für die Datenverschlüsselung sind zu bevorzugen.

4.1.2 Einspielen von Sicherheitspatches

Von den Geräteherstellern bereitgestellte Sicherheitspatches bzw. aktuellere Version der Firmware sollten nach Test und bei entsprechendem Sicherheitsbedarf eingespielt werden.

4.1.3 Allgemeine Konfiguration

Grundsätzlich ist es empfehlenswert, die vom Hersteller voreingestellte, oft unsichere Konfiguration zu überprüfen und wenn möglich zu ändern:

- Die Bluetooth-Geräten beiliegende Installations-Software versucht häufig, möglichst viele Dienste zu aktivieren, damit alle Möglichkeiten der Kommunikation mit anderen Geräten genutzt werden können. Nicht benötigte Dienste sollte der Anwender stets deaktivieren. Nur sporadisch benötigte Dienste sollten bei Bedarf gezielt aktiviert und danach wieder deaktiviert werden.
- Die Bluetooth-Schnittstellen der Geräte sollten bei Nichtbenutzung deaktiviert werden.
- Bluetooth-Geräte sollten möglichst wenig „offen“ konfiguriert werden. Es sind nach Möglichkeit die Betriebsmodi "non-discoverable", "non-connectable" und "non-pairable" einzustellen.
- Falls die Sendeleistung variabel ist, sollte sie so niedrig wie möglich und so hoch wie für die Funktionalität erforderlich eingestellt werden.
- Soweit möglich, sollten voreingestellte PINs sofort geändert werden.
- Als Default-PIN sollte eine möglichst lange und zufällig gewählte PIN verwendet werden (siehe Kapitel 4.2).
- Authentisierung und Verschlüsselung sind dem Schutzbedarf angemessen zu wählen.
- Für starke Verschlüsselung muss die Schlüssellänge mindestens 64 Bit betragen, und als Verschlüsselungsmodus darf nur Punkt-zu-Punkt-Verschlüsselung akzeptiert werden. Die Schlüssellänge sollte so groß wie möglich gewählt werden. Da sich die Länge des Verschlüsselungsschlüssels vom Benutzer nicht vorgeben lässt, sind nach Möglichkeit nur solche Geräte einzusetzen, die den genannten Anforderungen genügen (siehe Kapitel 3.1).

Darüber hinaus ist es empfehlenswert, Bluetooth-Geräte mit entsprechenden Hilfsmitteln[4] nach versteckten Diensten bzw. offenen Ports zu untersuchen.

4.1.4 Stationäre Geräte

Stationäre Geräte, bei denen Bluetooth als Kabelersatz - zum Beispiel zur Verbindung mit immer den gleichen Peripheriegeräten - verwendet wird, sollten in abhörgefährdeten Einsatzumgebungen mit Authentisierung und aktivierter Verschlüsselung betrieben werden. Die Länge der verwendeten PIN sollte über die minimal empfohlene PIN-Länge (siehe Kapitel 4.2) hinausgehen.

[4] Z.B. mittels „BT Audit“

4.1.5 Mobile Geräte

Bluetooth-Geräte, die mobil verwendet werden und mit fremden Geräten (d.h. Geräten unterschiedlicher Besitzer) kommunizieren, müssen besonders gesichert werden:

- ► Die Paarung zweier fremder Geräte sollte immer in abhörsicherer Umgebung durchgeführt werden. Die bei der Paarung verwendete PIN muss ausreichend lang sein (siehe Kapitel 4.2). Dabei ist zu beachten, dass Abhörsicherheit über die Möglichkeit des unbeobachteten Eindringens per Bluetooth von Außen zu beurteilen ist. Die Reichweite der eigenen Bluetooth-Geräte ist nicht alleine entscheidend.
- ► Jedes Gerät, das mehrere Dienste mit unterschiedlichen Sicherheitsniveaus anbietet, sollte in Sicherheitsmodus 2 (siehe Kapitel 2.2) betrieben werden. In diesem Fall ist darauf zu achten, dass die Sicherheitspolicies sorgfältig erstellt werden, d.h. unverschlüsselte Dienste sind nach Möglichkeit nicht zu verwenden.
- ► Geräte, die nur einen Dienst oder mehrere Dienste mit gleichem Sicherheitsniveau anbieten, sollten im Sicherheitsmodus 3 (siehe Kapitel 2.2) betrieben werden.
- ► Lösungen mit semi-permanenten Verbindungsschlüsseln sind zu bevorzugen. Wird bei einem solchen Paar zu einem unerwarteten Zeitpunkt vom Benutzer eine PIN-Eingabe verlangt, sollte dieser nach Möglichkeit darauf verzichten, bis er sich in abhörsicherer Umgebung befindet (entsprechende Nutzer-Einweisung oder -Schulung).
- ► Die Paarung sollte nur mit vertrauenswürdigen Geräten erfolgen.
- ► Bei Verlust/Diebstahl eines mobilen (bzw. stationären) Gerätes sollten alle zugehörigen Verbindungsschlüssel in den verbliebenen Geräten gelöscht werden.

4.2 Hinweise zur Wahl von PINs

PINs sollten eine möglichst zufällige Folge aus den verwendbaren Zeichen sein, triviale PINs wie "0000" oder "1234" sind unbedingt zu vermeiden (siehe [BSIGSH]). Für eine ausreichende Sicherheit bei der Paarung zweier Bluetooth-Geräte ist eine ausreichend lange PIN notwendig. Eine sichere PIN sollte mindestens eine Länge von 64 Bit aufweisen. PINs mit bis zu 40 Bit Länge können beispielsweise auf einem handelsüblichen, modernen PC gebrochen werden. Da es bei Bluetooth-Geräten nur möglich ist, PINs in Form von Ziffern bzw. alphanumerischen Zeichen einzugeben, gibt Tab. B–1 Empfehlungen für die Anzahl der zu verwendenden Zeichen.

Verwendete Zeichen	Min. empfohlene PIN-Länge	Minimale PIN Länge
0-9 (10 Zeichen)	19 Stellen (= 63 Bit)	12 Stellen (= 40 Bit)
0-9, A-Z (36 Zeichen)	12 Stellen (= 62 Bit)	8 Stellen (= 41 Bit)
0-9, A-Z, a-z (62 Zeichen)	11 Stellen (= 65 Bit)	7 Stellen (= 42 Bit)
(druckbares) ASCII (95 Zeichen)	10 Stellen (= 66 Bit)	6 Stellen (= 39 Bit)

Tab. B–1: Wahl von PINs

Beispiel: Akzeptiert das Gerät nur Ziffern und Großbuchstaben als PIN, sollte in jedem Fall eine PIN von mehr als 8 Stellen verwendet werden; empfohlen werden jedoch PINs mit mindestens 12 Stellen.

Anmerkung: Unter Umständen gibt es Geräte, bei denen sich 19-stellige PINs nicht eingeben lassen. Im diesem Falle ist eine nur aus Ziffern bestehende PIN nicht ausreichend, um das empfohlene Sicherheitsniveau zu erreichen.

4.3 Weitere Schutzmaßnahmen

Über die in Kapitel 4.1 genannten Maßnahmen hinaus sollten auf Bluetooth-Geräten – falls dies technisch möglich ist – weitere lokale Schutzmaßnahmen implementiert werden. Dazu zählen:

- Zugriffsschutz (materielle Sicherungsmaßnahmen)
- Benutzerauthentisierung
- Virenschutz
- Personal Firewall
- restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene
- lokale Verschlüsselung

Informationen hierzu findet man im IT-Grundschutzhandbuch des BSI [BSIGSH]. Im Zweifel orientiere man sich am Baustein „Internet-PC“ und wende die zugehörigen Maßnahmen sinngemäß an.

Als Schutzmaßnahme gegen das Abhören von Raumgesprächen ist ein Verbot des Einbringens von Funktechnik in den zu schützenden Raum zu empfehlen (siehe auch [BSIGSM]).

4.4 Rest-Risiko

Unabhängig von den beschriebenen Sicherheitsmaßnahmen sind mit der Verwendung von Bluetooth-Geräten immer folgende Rest-Risiken verbunden:

- Das Erstellen von Bewegungsprofilen mobiler Geräte (siehe Kapitel 3.5) kann nicht verhindert werden.
- Die Gefährdung der Verfügbarkeit (siehe Kapitel 3.6) ist ebenfalls nicht vermeidbar.
- Man-in-the-Middle-Angriffe (siehe Kapitel 3.2) sind auch bei optimal konfigurierten Geräten theoretisch möglich. Abhilfe ist nur durch die Verwendung zusätzlicher Sicherheitsmaßnahmen möglich, zum Beispiel durch die Verwendung von Sicherheitsdiensten in transportorientierten Schichten des ISO-Referenzmodells (z.B. IPSec) oder direkt auf Anwendungsebene (Ende-zu-Ende-Sicherheit).

5. Ausblick

Prognosen, dass Geräteschlüssel als Verbindungsschlüssel in Nachfolgeversionen von Bluetooth v1.1 verboten sein würden, haben sich leider nicht bestätigt. Hier wurde das Thema Abwärtskompatibilität offensichtlich höher eingestuft als die berechtigten Forderungen aus Sicherheitsgesichtspunkten.

Mittlerweile hält die Bluetooth-Technik auch Einzug in sensiblen Bereichen wie Autoelektronik und Fertigungssteuerung. Hierdurch erhalten die aufgezeigten Gefährdungen erhöhte Brisanz, nicht zuletzt auch die Gefahr des Einspielens von Viren nach erfolgreicher, unbefugter Verbindungsaufnahme. Generell wird das Virenthema auch für Bluetooth-fähige Geräte ständig an Bedeutung zunehmen. Mit zunehmender Intelligenz und Ressourcen-Ausstattung solcher Geräte werden diese im Nutzungsumfang den mobilen PCs immer ähnlicher, und damit auch die Bedrohungen für solche Geräte. Dies ist kein spezielles Bluetooth-Problem, jedoch bietet Bluetooth als drahtlose Technik eine erweiterte Angriffsfläche.

Zukünftig ist mit noch höheren Bandbreiten zu rechnen. So existiert bereits eine neue Arbeitsgruppe zu IEEE 802.15 (IEEE 802.15.3), die sich der Thematik höherer Bandbreiten für WPANs widmet. Darüber hinaus will die Bluetooth SIG die von der WiMedia Alliance vorgeschlagene Variante MB-OFDM [BTSIG06] für zukünftige Bluetooth-Systeme mit Ultra-Wide-Band-Technik (UWB) übernehmen.

6. Fazit

Bluetooth ist ein inzwischen weit verbreitetes Verfahren zur drahtlosen Kommunikation zwischen Mobiltelefonen, Personal-Computern und Peripheriegeräten. Eine Ausbreitung der Technik in neue Anwendungsfelder wie z.B. die industrielle Fertigung findet derzeit statt.

Das Sicherheitskonzept von Bluetooth sieht eine gegenseitige Authentisierung der Geräte sowie eine Verschlüsselung des Datenverkehrs vor. Für die Nutzung in Umgebungen mit niedrigem bis mittleren Schutzbedarf sind die von Bluetooth bereitgestellten kryptographischen Verfahren, insbesondere für die Verschlüsselung, angemessen. Dies gilt auch unter Berücksichtigung der bisher bekannt gewordenen Schwachstellen. Wird höherer Schutzbedarf gefordert, sind zusätzliche Maßnahmen, die über die Möglichkeiten von Bluetooth hinausgehen, zu treffen.

Im Gegensatz dazu wird die ausschließliche Verwendung im Gerät abgespeicherter symmetrischer Schlüssel („PINs“) als Basis für Authentisierung und Verschlüsselung zum Problem für den praktischen Einsatz von Bluetooth. Typische Gewohnheiten der Nutzer bei der Vergabe von Schlüsseln waren in der Vergangenheit häufig Ziele von Angriffen.

Die Absicherung der Kommunikation über Bluetooth kann somit technisch nicht erzwungen werden; sie wird stattdessen zu einer Aufgabe für den Nutzer. Dabei stehen sichere Konfiguration, Wahl komplexer PINs und umsichtiger Umgang mit der Technik im Vordergrund.

Vom Nutzer nicht zu beeinflussen ist dagegen eine nachlässige Implementierung der Bluetooth-Stacks durch die Hersteller. Zahlreiche in der Vergangenheit veröffentlichte Angriffs-Tools nutzten eben diese Schwächen aus, um vertrauliche Informationen aus Geräten auszulesen oder Geräte gar für ihre Zwecke zu missbrauchen. Hier hilft letztlich nur vollständiges Deaktivieren von Bluetooth – selbstverständlich unter Verzicht auf die Segnungen dieser drahtlosen Technik.

7. Literatur und Links

Informationen zum Grundverständnis in deutscher Sprache kann man unter anderem [GEIG04] entnehmen, weitere grundlegende deutschsprachige Informationen finden sich in den Büchern [WOLL01] und [MULL01]. Eine genauere Beschreibung der grundlegenden Bluetooth-Sicherheitsarchitektur ist zum Beispiel in [FOX02] enthalten. Aktuelle Informationen zu Bluetooth findet man unter [JAWE02] und [KAOW02], die aktuelle Spezifikation unter [BTSIG04]. Eine ausführliche Beschreibung verschiedener Schwächen im grundlegenden Sicherheitskonzept von Bluetooth findet sich in [FOX02]. Informationen zu konkreten, als praktikabel nachgewiesenen Angriffsformen finden sich unter [SHWO05].

Es gibt inzwischen zahlreiche Bücher und Publikationen zu Bluetooth. Die Liste der hier aufgeführten Titel und Links stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

[3GPP277] 3GPP TS 27.007: AT command set for User Equipment (UE), http://www.3gpp.org/ftp/Specs/html-info/27-series.htm, März 2005

[BSIGSH] Grundschutzhandbuch des BSI, http://www.bsi.bund.de/gshb

[BSIGSM] GSM-Mobilfunk, Gefährdungen und Sicherheitsmaßnahmen, http://www.bsi.bund.de/literat/doc/gsm/gsm.pdf, 2003

[BTSIG04] Specification of the Bluetooth System Version 2.0 + EDR, http://www.bluetooth.org/foundry/adopters/document/Core_v2.0_EDR/en/1/Core_v2.0_EDR.zip, November 2004

[BTSIG06] Bluetooth SIG selects WiMedia Alliance Ultra-Wideband Technology For High Speed Bluetooth® Applications, Pressemitteilung der Bluetooth SIG, http://www.bluetooth.com/Bluetooth/Press/SIG/BLUETOOTH_SIG_SELECTS_WIMEDIA_ALLIANCE_ULTRAWIDEBAND_TECHNOLOGY_FOR_HIGH_SPEED_BLUETOOTH_APPLICATION.htm, März 2006

[FLUH01] S. R. Fluhrer und S. Lucks: Analysis of the E_0 Encryption System, Selected Areas in Cryptography - SAC 2001, Lecture Notes in Computer Science 2259, Seiten 38-48, http://th.informatik.uni-mannheim.de/People/Lucks/papers/e0.ps.gz, Springer-Verlag, 2001

[FOX02] D. Fox: Bluetooth Security, http://www.secorvo.de/whitepapers/secorvo_wp05.pdf, Secorvo White Paper 2002

[GEIG04] J. Geiger, Bluetooth-FAQ, CHIP-online, http://www.chip.de/artikel/c1_artikel_12833263.html, September 2004

[IEEE02] Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), IEEE 802.15.1, Juni 2002

[JAWE02] M. Jakobsson und S. Wetzel: Security Weaknesses in Bluetooth. Progress in Cryptography - CT-RSA 2001, Lecture Notes in Computer Science 2020, Seiten 176-191, Springer-Verlag, 2001,

[KAOW02] T. Karygiannis und L. Owens: Wireless Network Security, http://www.csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf, National Institute of Standards and Technology (NIST) Nov. 2002

[KÜGL03] D. Kügler, "Man in the Middle" Attacks on Bluetooth, Financial Cryptography '03, Lecture Notes in Computer Science 2742, Seiten 149-161, Springer-Verlag 2003

[MULL01] N. J. Muller, Bluetooth, MITP-Verlag 2001

[SCHM03] Michael Schmidt: Angriffsmöglichkeiten bei Bluetooth, c't 11/2003

[SHWO05] Yaniv Shaked and Avishai Wool: Cracking the Bluetooth PIN http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/, Mai 2005

[SOBS06] Pierre Betouin, Version 0.6 de Bluetooth Stack Smasher, http://www.secuobs.com/news/05022006-bluetooth10.shtml, SecuObs.com, Februar 2006

[TRIFORG] Webseite der Trifinite Group, www.trifinite.org

[WOLL01] J. F. Wollert, Das Bluetooth-Handbuch, Franzis Verlag 2001

8. Abkürzungen

3GPP	3rd Generation Partnership Project
ACL	Asynchronous connection-less
ACO	Authenticated Cipher Offset
AFH	Adaptive Frequency Hopping
ASCII	American Standard Code for Information Interchange
BSI	Bundesamt für Sicherheit in der Informationstechnik
COF	Cipher Offset

CRC	Cyclic Redundancy Check
DPSK	Differential Phase Shift Keying, differentielle Phasenmodulation
DQPSK	Differential Quad Phase Shift Keying, vierwertige differentielle Phasenmodulation
DUN	Dial-up Network
EDR	Enhanced Data Rate
eSCO	extended SCO
FHSS	Frequency Hopping Spread Spectrum
GFSK	Gaussian Frequency Shift Keying
HID	Human Interface Device
IP	Internet Protocol
IPSec	Internet Protocol Security
ISM	Industrial, Scientific, Medical (2,4 GHz-Band)
ISO	International Organization for Standardization
IT	Information Technology
ITU-T	International Telecommunications Union, Telecommunication Standardisation Sector
L2CAP	Logical Link Control and Adaptation Protocol
LAN	Local Area Network
LK	Link Key
MB-OFDM	Multiband OFDM
OBEX	OBject EXchange protocol
OFDM	Orthogonal Frequency Division Multiplexing
PAN	Personal Area Network
PCM	Pulse Code Modulation
PIN	Personal Identification Number
RFCOMM	Serial Cable Emulation Protocol based on ETSI TS 07.10
SAP	SIM Access Profile
SCO	Synchronous connection-oriented
SDP	Service Discovery Protocol
SIG	(Bluetooth) Special Interest Group
SIM	Subscriber Identity Module
SMS	Short Message Service
SSL	Secure Sockets Layer
TDD	Time Division Duplex
UWB	Ultra Wide Band
WPAN	Wireless Personal Area Network

9. Glossar

Achtwertige Phasenmodulation (8DPSK, Differential Phase Shift Keying)
: Differentielle Phasenmodulation, bei der drei Bits pro Symbol übertragen werden, mit einer resultierenden Datenrate von 3 MBit/s.

adaptives Frequenzsprungverfahren (AFH)
: Verfahren, das die von der Sprungsequenz abgedeckten Kanäle auf freie, d.h. ungestörte Frequenzen beschränkt.

Ad-hoc-Netzwerke
: Drahtloses Netz zwischen zwei oder mehr mobilen Endgeräten, das ohne feste Infrastruktur auskommt; insbesondere verwendet bei Bluetooth, um die spontane Koppelung von Mobiltelefonen z.B. mit Headsets zu ermöglichen.

Anwendungs-Profil
: Definition von Untermengen der Bluetooth-Protokolle durch die Bluetooth SIG, um die Interoperabilität unterschiedlicher Geräte sicherzustellen, ohne dass in allen Geräten immer alle existierenden Protokolle implementiert sind, z.B. Serial Port Profile, Headset Profile

Asynchrone verbindungslose Übertragung (ACL)
: Übertragung, bei der die Datenpakete gesendet werden, sobald ein Freiraum (Slot) besteht; jedes Paket enthält eine Zieladresse, anhand derer es an den Empfänger vermittelt wird.

AT-Kommandos
: Quasi-Standard für Befehle zum Konfigurieren und Parametrieren von Modems und ähnlichen Geräten (AT steht für "attention"); Befehlssatz wurde teilweise von der ITU-T in die Empfehlung V.25ter umgesetzt; heutiger Name ist V.250.

Authentisierung
: Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Gerätes. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist im Allgemeinen keine sinnvolle Autorisierung möglich.

Binäre Frequenzmodulation (Gaussian Frequency Shift Keying , GFSK)
: Zwingend von Bluetooth-Implementierungen unterstützte Frequenzmodulation, bei der ein Bit pro Symbol übertragen wird, mit einer resultierenden Datenrate, „Basic Rate“, von 1 MBit/s.

Bluetooth Device Address
: 48 Bit lange öffentlich bekannte und weltweit eindeutige Geräteadresse

Bluetooth Special Interest Group (Bluetooth SIG)
: Interessengemeinschaft zahlreicher Unternehmen, die an der Entwicklung und Verbreitung der Bluetooth-Technologie interessiert sind; 1998 von Ericsson, IBM, Intel, Nokia und Toshiba gegründet; 1999 erweitert durch 3Com, Lucent, Microsoft und Motorola; Eigentümer des Bluetooth-Warenzeichens und Herausgeber der Bluetooth-Spezifikation.

Challenge-Response-Verfahren
: Sichere Authentisierung eines Endgerätes bei Kommunikationswunsch auf Basis von Wissen, welches beide Verbindungspartner besitzen (z.B. Passwort)

Channel-Hopping-Sequence
: Sprungsequenz

Chiffrat
: Verschlüsselte Form der Nachricht

Codec
: Es handelt sich um eine Wortkreuzung aus den englischen Begriffen „coder“ und „decoder“. Es bezeichnet ein Verfahren bzw. Programm, das Daten oder Signale digital codiert und decodiert.

Cyclic Redundancy Check (CRC)
: Prüfsumme über die zu übertragenden Daten, die in der Nachricht mitgeschickt wird und es dem Empfänger gestattet, Bitfehler, die auf dem Kommunikationskanal entstanden sind, zu erkennen

Denial of Service (DoS)
: Ein Angriff vom Typ Denial of Service hat zum Ziel die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr („Dummy Traffic“) oder die beabsichtigte Herbeiführung eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Extended SCO
: Synchrone Kanäle mit höherer Bandbreite, die eine Neuübertragung fehlerhaft empfangener Datenpakte erlaubt, um die Dienstqualität auch unter ungünstigen Empfangsverhältnissen zu verbessern.

Frequenzmodulation
: Modulationsverfahren, bei welchem die Trägerfrequenz durch das zu übertragende Signal beeinflusst wird.

Frequenzspreizung
: Verfahren in der drahtlosen Datenübertragung, bei dem ein schmalbandiges Signal in ein breitbandiges Signal umgewandelt wird; die Sendeenergie, die zuvor in einem kleinen Frequenzbereich konzentriert war, wird dabei auf einen größeren Frequenzbereich verteilt.

Frequenzsprungverfahren (FHSS)
: Frequenzspreizverfahren, bei dem die verfügbare Bandbreite auf viele Kanäle aufgeteilt wird, die nacheinander in einer regelmäßigen zyklischen Sprungsequenz genutzt werden.

Geräteschlüssel (Unit Keys)
: Intern, bei der ersten Verwendung eines Bluetooth-Gerätes erzeugter Schlüssel, der normalerweise nicht mehr geändert wird; kann als Link Key genutzt werden, wenn ein Gerät nicht genügend Speicherplatz für weitere Schlüssel besitzt oder einer großen Gruppe von Nutzern zugänglich sein soll.

Initialisierungsschlüssel
: Für die gesicherte Übertragung der Zufallszahlen für die Bluetooth-Paarung genutzter Schlüssel Kinit, der sich lokal mittels einer kryptographischen Funktion aus einer öffentlichen Zufallszahl, der Geräteadresse eines Teilnehmers und einer im Allgemeinen konfigurierbaren PIN berechnet.

ISM-Frequenzband
: Lizenzfrei nutzbare Frequenzbänder, die für industrielle, wissenschaftliche und medizinische Zwecke verwendet werden können (ISM = Industrial-Scientific-Medical)

Hold-Mode
: Stromsparmodus bei Bluetooth-Geräten

Kanalabstand
: Frequenzunterschiend zwischen zwei benachbarten Kanälen in einem Frequenzband. Innerhalb eines Frequenzbandes sind die Kanäle gleich breit.

Kombinationsschlüssel (Combination Key)
: Nur für die Verbindung zweier Geräte genutzter, 128 Bit langer Schlüssel, der in jedem Gerät als Verbindungsschlüssel (Link Key, LK) gespeichert wird und in Abhängigkeit von den Geräteadressen und einer Zufallszahl pro Gerät erzeugt wird.

Man in the Middle
: Der Angreifer positioniert sich zwischen zwei Kommunikationspartner und täuscht beiden Parteien vor, der jeweils erwartete eigentliche Partner zu sein. Dabei kann der Man in the Middle den Dialog zwischen den beiden Parteien belauschen oder auch verfälschen. Ziel ist oft die Ermittlung von Passwörtern.

Master-Schlüssel (Master Keys)
: Temporäre Schlüssel für die Dauer einer Bluetooth-Sitzung, falls ein Master mehrere Geräte unter Verwendung desselben Verschlüsselungsschlüssels erreichen will.

Modulationsverfahren
: Verfahren bei der drahtlosen Übertragung, mit dem die zu übertragenden Daten mit Signalen hoher Frequenz gemischt – moduliert – werden, da nur diese von einem Sender mit großer Reichweite abgestrahlt werden können.

PCM
: Verfahren zur Übertragung analoger Signale in binärer Form. Das analoge Signal wird hierbei mit einer bestimmten Frequenz in zeitgleichen Abständen abgetastet und anschließend mit einem Analog-Digital-Wandler in einen Zahlenwert umgewandelt. Der Zahlenwert wird binär codiert und übertragen.

Paarung bzw. Pairing
: Verfahren zu Beginn einer Verbindung zur Kommunikations-Absicherung zweier Bluetooth-fähiger Geräte, insb. Vereinbarung eines Verbindungsschlüssels.

Park-Mode
: Stromsparmodus bei Bluetooth-Geräten

Piconet
: Bluetooth-Netzwerk mit maximal acht ad-hoc verbundenen Endgeräten; auch PAN (Personal Area Network) genannt.

Personal Identification Number (PIN)
: Konfigurierbare, auf beiden Geräten gleiche Identifikation zur Erzeugung eines Initialisierungsschlüssels

Phasenmodulation
: Verfahren, mit dem ein Signal über einen Kommunikationskanal übertragen wird. Bei der Übertragung von digitalen Signalen wird die Phase einer Sinusschwingung (Träger) durch Phasenverschiebung moduliert.

Scatternet
: Gruppe von Piconets, die über gemeinsame Bluetooth-Geräte miteinander verbunden sind.

Sniff-Mode
: Stromsparmodus bei Bluetooth-Geräten

Sprungsequenz
: Regelmäßige Abfolge der Kanäle in einem Frequenzsprungverfahren.

Stromchiffre
: Symmetrische, kontinuierliche und verzögerungsfreie Ver- oder Entschlüsselung eines Datenstroms, bei der die Daten Bit für Bit bzw. Zeichen für Zeichen verschlüsselt werden.

Synchrone verbindungsorientierte Übertragung (SCO)
: Übertragungsmodus, bei dem Datenpakete in einem festen Zeitraster zwischen Stationspaaren ausgetauscht werden, entspricht. der leitungsvermittelten Übertragung in einem Telefonnetz.

Time Division Duplex (TDD)
: Zeitversetzte, in kurze Sequenzen aufgeteilte Übertragung der Daten , bei der Sende- und Empfangskanal die gleiche Frequenz nutzen, aber zeitlich voneinander getrennt sind.

Verbindungsschlüssel (Link Key, LK)
: Ein nur für die Verbindung zweier Geräte genutzter Schlüssel, 128 Bit langer Kombinationsschlüssel (Combination Key), Geräteschlüssel (Unit Key) oder Master-Schlüssel (Master Key)

Vierwertige Phasenmodulation (Differential Quad Phase Shift Keying, $\pi/4$-DQPSK)
: Differentielle Phasenmodulation, bei der zwei Bits pro Symbol übertragen werden, mit einer resultierenden Datenrate von 2 MBit/s.

C. DECT

Inhaltsverzeichnis des Abschnitts

1. Grundlagen und Funktionalität

DECT war ursprünglich die Abkürzung für „Digital European Cordless Telephone“ und wurde Ende der 80er Jahre als europaweit einheitlicher Standard konzipiert, der die bis dahin vorhandenen verschiedenen analogen schnurlosen Telefonsysteme (z.B. CT1, CT1+) ersetzen sollte. Heute steht DECT für „Digital Enhanced Cordless Telecommunications“, einen 1992 verabschiedeten Standard des European Telecommunications Standards Institute (ETSI), siehe [EN300175]. Der DECT-Standard spezifiziert ein vollständig digitales Mobilfunknetz zur Übertragung von Sprache und Daten, das sich im Vergleich zu analogen Schnurlostelefon-Standards durch eine hohe Sprachqualität und Optionen für eine höhere Abhörsicherheit auszeichnet. Als typische Einsatzorte von DECT sind in erster Linie Bürogebäude und Firmengelände sowie Heimbereiche zu nennen. Eine Verwendung als WLL-Technik (Wireless Local Loop) zur Überbrückung der letzten Meile zwischen einem Netzbetreiber und Kunden ist ebenfalls möglich, hat sich aber nicht durchsetzen können. Dagegen steht heute in sehr vielen Haushalten ein DECT-Telefon.

Im Folgenden werden Architektur, Protokolle und Sicherheitsmechanismen von DECT vorgestellt, mögliche Sicherheitslücken untersucht und entsprechende Sicherheitsmaßnahmen empfohlen.

1.1 Architektur

Mit DECT-Systemen können komplette schnurlose Nebenstellenanlagen aufgebaut werden. Neben den normalen Telekommunikationsverbindungen über einen Amtsanschluss können dann zwischen mehreren mobilen Endgeräten gebührenfrei interne Kommunikationsverbindungen über die DECT-Basisstation aufgebaut werden.

Bei einem schnurlosen Telefon für den Heimbereich, der am häufigsten anzutreffenden DECT-Anwendung, besteht das DECT-System aus einer Feststation, dem so genannten Fixed Part (FP), und einem oder mehreren Mobilstationen, den so genannten Portable Parts (PP).

Eine noch einfachere Systemkonfiguration ist der Direkt-Modus, bei dem zwei DECT-Endgeräte (PP) direkt miteinander kommunizieren. Im Direkt-Modus lässt sich z.B. fern von jeder DECT-Infrastruktur eine Datenfunkverbindung zwischen zwei mit Datenfunkmodulen ausgestatteten Laptops oder eine Walkie-Talkie-Verbindung zwischen zwei Sprachtelefonie-PPs realisieren.

DECT ist multizellenfähig und unterstützt Verfahren wie Roaming[1] und Handover[2]. Bei Mehr-Zellen-Systemen besteht ein DECT-Netz aus mehreren FPs, die an eine zentrale Vermittlungskomponente (DECT Fixed System, DFS) angeschlossen sind. Der abgedeckte Bereich kann durch überlappende Funkzellen flächendeckend versorgt werden. Das DFS verfügt hierzu über eine Datenbank zur Nutzer- bzw. Endgeräte-Verwaltung. Für den Anschluss an ein externes Telefonnetz gibt es im DFS eine so genannte Interworking Unit (IWU), die für die Anpassung der DECT-spezifischen Protokolle an die Protokolle des analogen Telefonnetzes bzw. des ISDN sorgt. Das DFS ist an eine Nebenstellenanlage (Private Branch Exchange, PBX) angeschlossen oder als Modul einer PBX realisiert. Zur Versorgung eines größeren Areals können mehrere DFSs und ggf. auch Nebenstellenanlagen eingesetzt und zu einem größeren Netz verbunden werden.

In einem kleinen DECT-System bestehend aus einem einzelnen FP (wie im Heimbereich üblich) werden die Funktionen des DFS im FP realisiert.

Zur Erweiterung eines DECT-Systems können auch so genannte Wireless Relay Stations (WRS), auch Relais oder Repeater genannt, eingesetzt werden. Als Relay-Station kommuniziert eine WRS sowohl mit PPs als auch mit einem FP.

---

1 Wechsel eines PP zwischen verschiedenen DECT-Netzen

2 Wechsel eines PP zwischen zwei benachbarten Funkzellen (d.h. den durch FPs versorgten Bereichen) unter Aufrechterhaltung der Ende-zu-Ende-Verbindung.

Mit einem PP bleibt ein Teilnehmer im gesamten Abdeckungsbereich des DECT-Netzes (z.B. einem Gebäude oder sogar auf einem größeren Gelände) unter seiner gewohnten Rufnummer erreichbar. Abb. C-1 zeigt den beschriebenen Aufbau eines DECT-Systems im Überblick.

Damit ein problemloses Zusammenspiel von PPs verschiedener Hersteller gewährleistet ist, gibt es das Generic Access Profile (GAP), das in [EN300444] spezifiziert ist und Minimalanforderungen für Fernsprechdienste festlegt. So genannte Interworking Profiles definieren die Schnittstellen zu anderen Netzen (z.B. ISDN). Weiterhin können auch schnurlose Datennetze mit entsprechenden Geräten auf DECT-Basis aufgebaut werden. In so genannten Application Profiles sind Kommunikationsdienste für spezielle Anwendungen spezifiziert.

Der DECT Packet Radio Service (DPRS, [EN300449]) und das DECT Multimedia Access Profile (DMAP, [EN300650]) ermöglichen beispielsweise Datenkommunikation mit höheren Datenraten (vergleichbar z.B. mit denen von Bluetooth). Mit einem Datenfunkmodul als PP lässt sich damit über ein entsprechend ausgestatteter FP beispielsweise auch ein drahtloser DECT-basierter Internet-Zugang realisieren. Ebenso ist die Kommunikation mit weiteren Datenfunkmodulen möglich, auf diese Weise ist beispielsweise der Datenaustausch zwischen PCs über eine DECT-Datenfunkverbindung machbar.

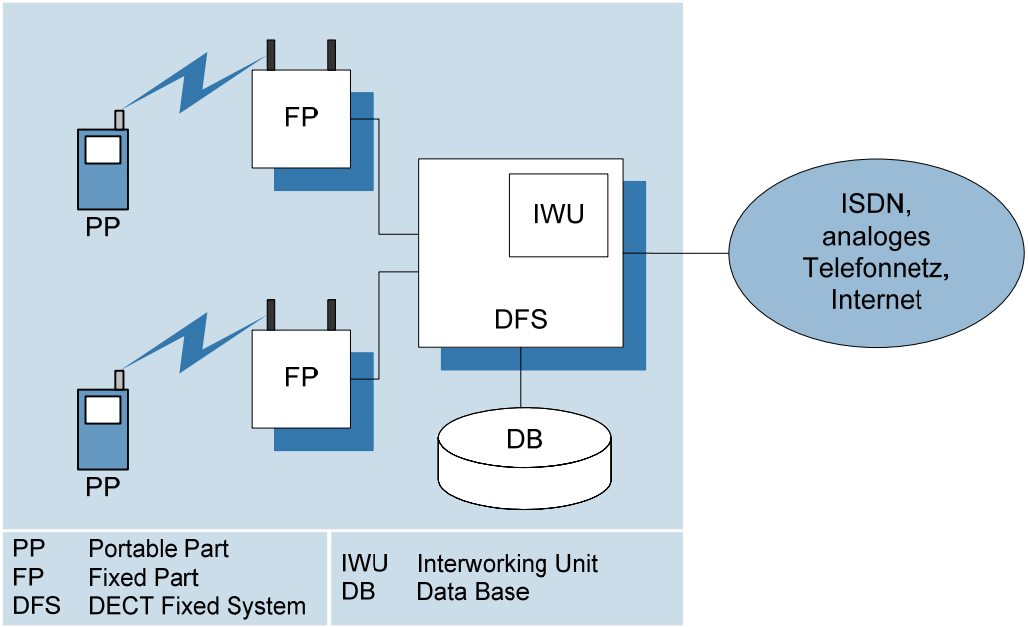


Abb. C-1: Vereinfachter Aufbau eines DECT-Systems

1.2 Funkschnittstelle

Die Übertragung auf der Funkschnittstelle geschieht ähnlich zu anderen Telekommunikationssystemen (z.B. ISDN) über zwei getrennte Protokoll-Stacks: einen für die Übertragung der Nutzer- bzw. Applikationsdaten (z.B. Sprache) und einen für die hierzu nötigen Signalisierungsdaten. Beide Protokoll-Stacks setzen auf einer gemeinsamen Kanalzugriffsebene (Medium Access Control, MAC) auf. Die Signalisierungsdaten beinhalten für den Austausch von Applikationsdaten Kontrollinformationen für Aufbau, Aufrechterhaltung und Abbau einer Verbindung. Abb. C-2 zeigt die Protokollarchitektur im Überblick.

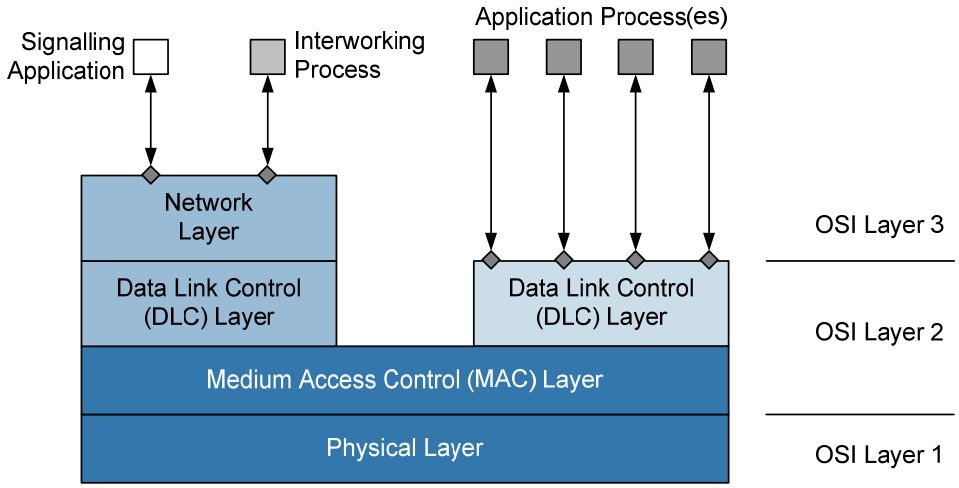


Abb. C-2: Protokolle auf der Luftschnittstelle (vereinfacht, siehe auch [EN300175])

1.2.1 Physikalische Übertragung und Kanalzugriff

DECT arbeitet in Europa im explizit reservierten Frequenzband zwischen 1880 MHz und 1900 MHz. Es stehen 10 Trägerfrequenzen im Abstand von 1,728 MHz (Frequency Division Multiplex, FDM), wie in Abb. C-3 gezeigt, zur Verfügung[3].

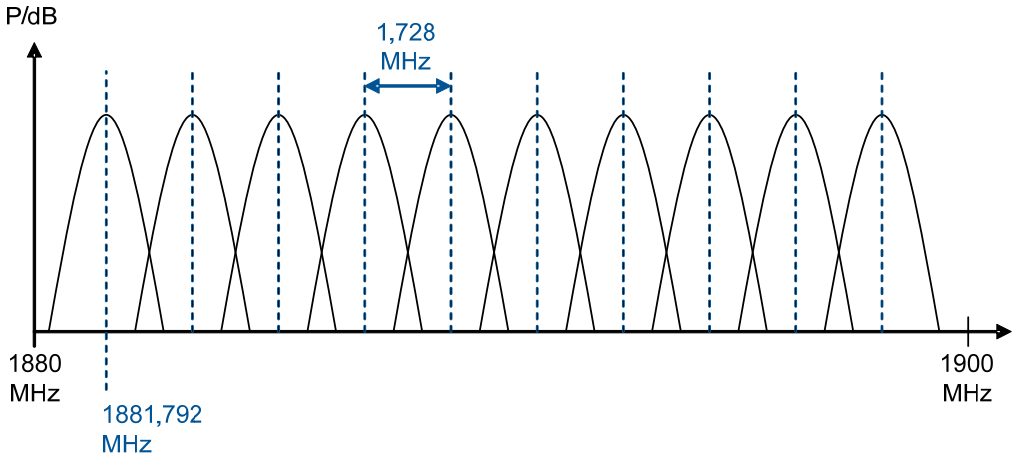


Abb. C-3: Trägerfrequenzen

Jeder Träger ist durch Zeitschlitze (Slots) in 24 Kanäle eingeteilt (Time Division Multiple Access, TDMA). Ein solcher aus 24 Slots bestehender Rahmen (Frame) ist 10 ms lang und wiederholt sich periodisch alle 10 ms. Der Duplexbetrieb erfolgt mittels Time Division Duplex (TDD). Dabei werden die ersten 12 Slots eines Rahmens im Downlink, d.h. in der Übertragungsrichtung vom FP zu den PPs, verwendet. Die zweiten 12 Slots bilden den Uplink, d.h. die Übertragungsrichtung von den PPs zum FP. Somit ergeben sich pro Träger 12 Duplexkanäle; auf den 10 Trägerfrequenzen stehen also insgesamt 120 Duplexkanäle zur Verfügung (siehe Abb. C-4). Ein für den DECT-Nutzer aufgebauter bidirektionaler Kommunikationskanal zwischen FP und PP belegt immer zwei Slots.[4]

---

[3] Die Trägerfrequenzen f berechnen sich wie folgt: $f = (1881{,}792 + k*1{,}728)$ MHz, für $k = 0, ..., 9$

[4] Bei der Verwendung eines WRS muss berücksichtigt werden, dass sich eine WRS einem FP gegenüber als PP verhält. Eine WRS sendet dann die so empfangenen Pakete in einem anderen Zeitschlitzpaar an einen PP weiter. Für jedes über eine WRS geführte Gespräch müssen somit insgesamt vier Zeitschlitze belegt werden.

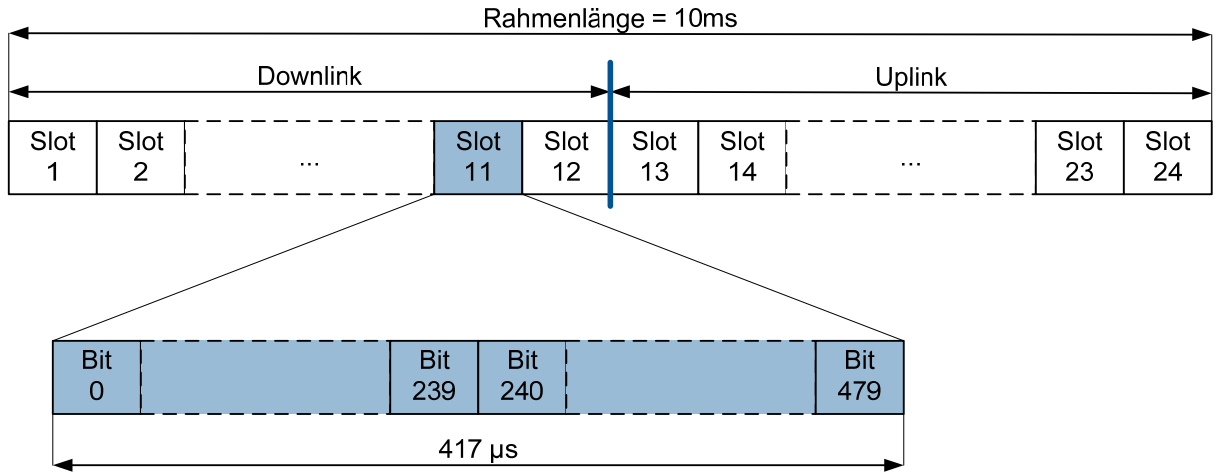


Abb. C-4: Zeitmultiplex

Zur Modulation wird bei DECT GMSK (Gaussian Minimum Shift Keying) verwendet. Mit dieser Modulationsart erreicht man hier eine maximale modulierte Gesamtbitrate von 1152 kBit/s auf jeder Trägerfrequenz. Jedes physikalische Datenpaket transportiert sowohl Signalisierungs- als auch Nutzdaten. Die Nutzdatenrate liegt bei maximal 32 kBit/s pro Kanal (Unprotected Mode). Um die Datenübertragung gegen Bitfehler zu schützen, können die Nutzdaten in Gruppen zu je 80 Bit aufgeteilt werden. Davon werden dann 64 Bit zur Datenübertragung und 16 Bit zur Fehlerkorrektur verwendet (Protected Mode). In diesem Fall sind pro Kanal effektiv 25,6 kBit/s möglich (siehe Abb. C-5). Im DECT-Standard sind verschiedene Übertragungsmodi spezifiziert, mit denen sich eine Vielzahl elementarer Kanäle (so genannte MAC-Bearer) aufbauen lassen, die sich bezüglich der Datenraten und Fehlerschutzmechanismen unterscheiden. MAC-Bearer lassen sich zum Erreichen höherer Datenraten auch kombinieren.

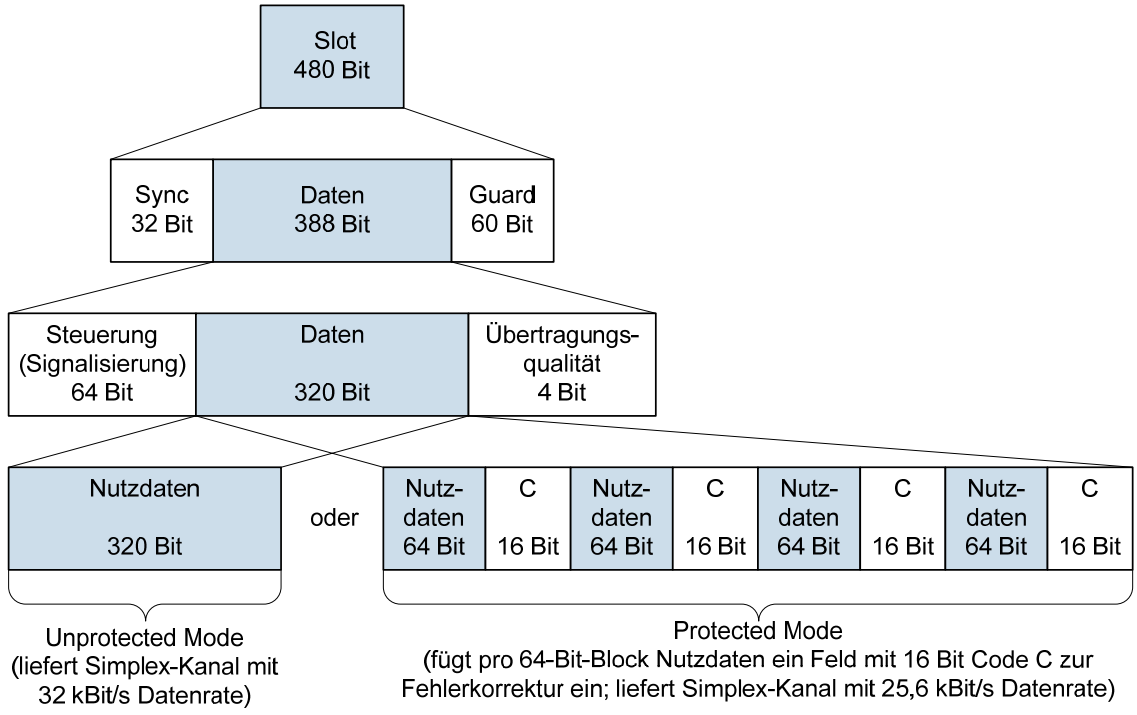


Abb. C-5: Format der Daten in einem Slot

Die maximale Sendeleistung beträgt 250 mW (bei mittlerer Sendeleistung von 10 mW), womit sich abhängig von den Funkausbreitungsbedingungen eine Reichweite (maximale Entfernung zwischen Basis- und Mobilstation) von bis zu 300 m im Freien und bis zu 50 m in Gebäuden ergibt. Mit Hilfe

von Richtantennen lässt sich die Reichweite auf bis zu 5 km erhöhen, solche Lösungen sind z.B. für stationäre WLL-Systeme praktikabel.

1.2.2 Höhere Protokollschichten

Oberhalb der MAC-Schicht ist in der DECT-Protokollarchitektur (siehe Abb. C-2) eine Sicherungsschicht (DLC) vorgesehen, die die Aufgabe hat, Daten aus höheren Schichten aufzubereiten, so dass sie mit der jeweils geforderten Qualität (Bitfehlerrate, Verzögerung usw.) über die MAC-Bearer übertragen werden können. Oberhalb der DLC-Schicht liegt die Netzwerk-Schicht, welche für Verbindungsauf- und -abbau sowie für das Mobilitätsmanagement zuständig ist; darüber liegen die Anwendungsschichten.

1.2.3 Übertragung der Nutzdaten

Sprache wird in DECT mittels Adaptive Differential Pulse Code Modulation (ADPCM) kodiert und über den Unprotected Mode mit 32 kBit/s oder über den Protected Mode mit 25,6 kBit/s übertragen. Zur Erzielung höherer Datenraten können mehrere Kanäle gebündelt werden. Die Duplexverbindungen können auch asymmetrisch ausgelegt sein, so dass für Hin- und Rückrichtung unterschiedliche Datenraten möglich sind. Durch DMAP [EN301650] wird der DECT-Standard diesbezüglich um zusätzliche Möglichkeiten erweitert.

1.3 Verbindungsaufbau

Jeder FP[5] sendet auf einem Kanal regelmäßig Bakensignale in Form der 40 Bit langen RFPI (Radio Fixed Part Identity) aus. Die der Funkzelle befindlichen PPs können diese RFPI dekodieren und können so die in ihrer Reichweite befindlichen FPs identifizieren. In den PPs sind Informationen über die jeweiligen Zugriffsrechte, so genannte PARKs (Portable Access Rights Keys), abgespeichert. Die Zugriffsrechte werden während einer Subscription (siehe Kapitel 2.5) vereinbart.

Nach dem Einschalten synchronisiert sich ein PP auf die in der Umgebung vorhandenen FPs auf, misst die jeweiligen Empfangspegel und dekodiert die Systeminformationen. Mit diesen Informationen wählt der PP aus den FPs, zu denen es Zugriffsrechte hat, den FP mit dem stärksten Empfangspegel aus und geht in Bereitschaft, in der ausgewählten Zelle Paging-Meldungen[6] zu empfangen und eine Verbindung aufzubauen. Bei Veränderung der Empfangsbedingungen findet erneut eine Zellauswahl statt.

Beim Einbuchen eines PP in einer Funkzelle erhält der PP vom FP eine eindeutige temporäre Kennung, die 20 Bit lange TPUI (Temporary User Identity). Mit dieser TPUI wird der PP bei einem ankommenden Anruf ausgerufen (Paging).

Ein Verbindungswunsch wird sowohl durch abgehende Anrufe als auch durch die Bereitschaft, einen eingehenden Anruf anzunehmen, ausgelöst. Eingehende Anrufe werden zuvor mittels Funkruf vom FP signalisiert. Für einen Verbindungsaufbau muss der PP geeignete Funkkanäle auswählen. Hierfür führt er auf allen verfügbaren Kanälen Empfangspegelmessungen durch und wählt die empfangsstärksten aus. Während einer laufenden Verbindung führt der PP weiterhin Pegelmessungen durch, um aus allen

---

5 Streng genommen ist es der so genannte Radio Fixed Part (RFP), der diese Funktion ausführt. Eine genauere Aufschlüsselung des Aufbaus eines DECT-Systems hätte jedoch den Rahmen dieser Broschüre gesprengt.

6 Wenn in einem Mobilfunknetz ein Ruf zu einem mobilen Teilnehmer vermittelt werden soll, muss das Mobilfunknetz zunächst die Funkzelle ermitteln, in der sich der Teilnehmer aktuell aufhält. Hierzu schickt das Mobilfunknetz in den Funkzellen, in denen es den Teilnehmer vermutet, spezielle Nachrichten aus, die den Teilnehmer auffordern, sich zu melden. Erst wenn dies geschieht, kann der Ruf zum Teilnehmer durchgestellt werden. Dieser Prozess des Ausrufs eines Teilnehmers mit der Bitte sich zu melden wird allgemein als Paging bezeichnet.

zur Verfügung stehenden Kanälen stets den nicht belegten mit der geringsten Störung auswählen zu können (dynamisches Kanalwahlverfahren). Die Entscheidung über den zu verwendenden Kanal trifft stets der PP. Das gleiche gilt übrigens auch für die Entscheidung über einen Handover bei Mehrzellenbetrieb. Der FP passt sich der vom PP gewählten Frequenz und dem gewählten Zeitschlitz an, weshalb für die Feststationen keine Frequenzplanung erforderlich ist.

1.4 Konvergenz von DECT und IP

Im Rahmen der Konvergenz von Sprache und Daten im Festnetz (Voice over IP, VoIP) ist generell die Frage von Interesse, wie drahtlose Techniken diesem Integrations- und Vereinheitlichungsprozess folgen können. Hier zeichnet sich allerdings bereits ein gewisser Trend in Richtung der Übertragung von VoIP über Wireless LAN ab. Zumindest während der Übergangszeit hin zu Voice over WLAN ist aber eine hybride Technik interessant, die es ermöglicht, in der Luftschnittstelle das DECT-Verfahren zu verwenden und auf der Leitung die VoIP-Technologie. Dies kombiniert den Funktionsumfang klassischer DECT-Lösungen mit den Einsparpotenzialen eines VoIP-Netzwerks. Hierzu werden DECT Access Points (DAPs) eingesetzt, die eine Ethernet-Schnittstelle haben und über das Ethernet-Netzwerk auch den Aufbau von größeren Sprachnetzen ermöglichen, ohne eine klassische TK-Anlage vorsehen zu müssen. Ein DAP-Controller übernimmt die Steuerung der DAPs und den Kontakt zu einem zentralen VoIP-Server (Protokollbasis ist z.B. das Session Initiation Protocol, SIP[7]). Remote-Standorte benötigen keine eigenen Kommunikationsserver, denn die Versorgung kann von einem zentralen Server aus erfolgen.

Es gibt weiterhin Geräte, die mehrere Funktechniken in einem Produkt integrieren. Beispiele sind ein DECT FP mit integriertem WLAN Access Point oder ein DECT PP mit integrierter Bluetooth-Schnittstelle. Der Anwender muss daher gegebenenfalls für mehrere Systeme eine Sicherheitsbetrachtung durchführen.

2. Sicherheitsmechanismen

Da DECT ein funkbasiertes Verfahren ist, besteht grundsätzlich die Gefahr, dass „unberechtigte“ DECT-fähige Geräte die DECT-Kommunikation mithören bzw. sich aktiv in die Kommunikationsverbindung einschalten. Neben nicht-kryptographischen Verfahren zum Schutz gegen Übertragungsfehler sieht die Spezifikation kryptographische Authentisierungs- und Verschlüsselungsalgorithmen vor. Die für die kryptographische Sicherheit verantwortlichen Parameter und Algorithmen sind in Abb. C-6 aufgeführt. In der Spezifikation sind viele Optionen beschrieben, die ein Hersteller von DECT-Systemen bei der Implementierung von Sicherheitsmechanismen verwenden kann. Die folgenden Beschreibungen beziehen sich auf die im Wesentlichen anzutreffenden Sicherheitsmechanismen gemäß GAP [EN300444].

[7] Das von der IETF in RFC 3261 spezifizierte Session Initiation Protocol (SIP) ist ein in der IP-Telefonie häufig eingesetztes Protokoll zum Aufbau und zur Verwaltung von Kommunikationssitzungen (Sessions) zwischen zwei und mehr Teilnehmern.

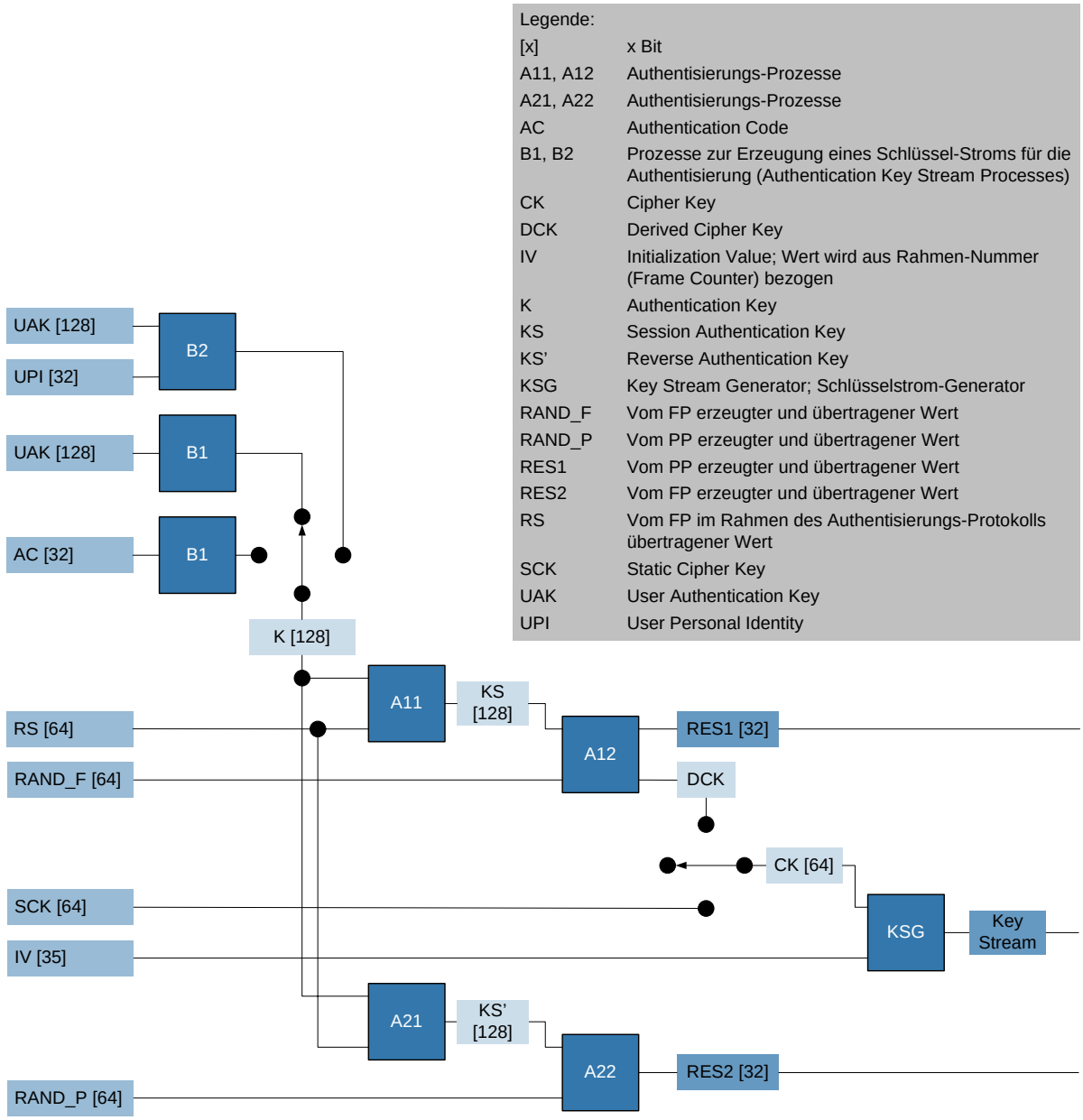


Abb. C-6: Kryptographische Sicherheitsmechanismen bei DECT (siehe [EN300175])

2.1 Authentisierung der Mobilstation

Jeder PP muss sich vor einem Verbindungsaufbau authentisieren. Hierdurch sollen unberechtigte Netzzugriffe verhindert werden. Die Authentisierung basiert auf einem so genannten Challenge-Response-Verfahren, wie in Abb. C-7 gezeigt.

Aus den vom FP gesendeten Zufallszahlen RAND_F und RS (Challenge) wird im PP unter Verwendung des Langzeitgeheimnisses UAK mit Hilfe der Prozesse A11 und A12 der Wert RES1 erzeugt und als Antwort (Response) über die Luftschnittstelle zum FP übertragen[8]. Bei korrekter Antwort RES1 gilt der PP als authentisiert. Gegebenenfalls wird neben dem Wert RES1 auch ein abgeleiteter

[8] Die Prozesse B1 und B2, die in Abb. C-6 gezeigt sind, dienen der Bereitstellung der Eingangsparameter für den Prozess A11.

Chiffrier-Schlüssel DCK (siehe Kapitel 2.3) generiert. Der DECT-Authentisierungsalgorithmus bestehend aus den Prozessen A11 und A12 ist nicht veröffentlicht.

Das Langzeitgeheimnis UAK (User Authentication Key) muss in beiden Geräten (Mobil- und Feststation) gespeichert sein (siehe Kapitel 2.5).

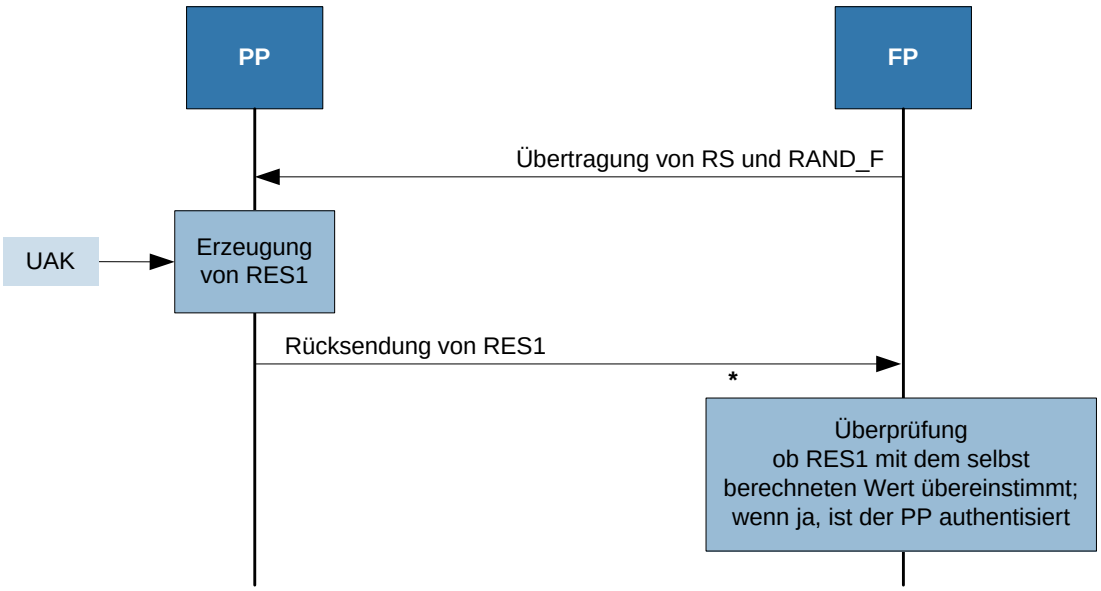


Abb. C-7: Authentisierung bei DECT

2.2 Authentisierung der Feststation

Die Authentisierung des FPs gegenüber dem PP zum Schutz der Mobilstation vor Verbindungen über unberechtigte Feststationen ist optional. Der Ablauf ist im Prinzip der gleiche wie bei der Authentisierung der Mobilstation, jedoch sind die Aufgaben von PP und FP vertauscht. Auch hier sind die verwendeten Algorithmen in den Prozessen A21 und A22 nicht veröffentlicht.

2.3 Verschlüsselung

Optional werden die Klardaten auf der Funkschnittstelle zum Schutz der Vertraulichkeit verschlüsselt übertragen. Die Verschlüsselung erfolgt auf Basis einer Stromchiffrierung, deren Schlüsselstrom (Key Stream) vom Schlüsselstromgenerator mit Hilfe des 64 Bit langen Chiffrier-Schlüssels CK (Cipher Key) und eines von der aktuellen Frame-Nummer abgeleiteten Initialisierungsvektors IV erzeugt wird. Der Schlüsselstrom sollte sich dabei in einem statistischen Sinne wie eine zufällige Bitfolge verhalten. Da der Schlüsselstrom jedoch systematisch erzeugt wird, spricht man auch von einem pseudozufälligen Bitstrom. Der Schlüssel CK kann ein statischer Chiffrier-Schlüssel (Static Cipher Key, SCK) sein, oder er ist der beim Verbindungsaufbau abgeleitete Chiffrier-Schlüssel (Derived Cipher Key, DCK).

Der Schlüsselstrom wird mit den Klardaten bitweise XOR-verknüpft (XOR = exklusives Oder). Auf diese Weise wird der Klartext quasi in dem pseudozufälligen Schlüsselstrom versteckt. Sofern der Schlüsselstrom sich statistisch mit genügender Qualität wie ein echter Zufall verhält, kann nur unter Kenntnis des Schlüsselstroms der Klartext wieder herausgefiltet werden. Dies geschieht auf der Empfängerseite einfach dadurch, dass der Empfänger seinerseits den Schlüsselstrom aus CK und IV erzeugt und die empfangenen verschlüsselten Daten bitweise mit dem Schlüsselstrom XOR-verknüft. Das Ergebnis sind die Klardaten.

Der verwendete Stromchiffrierer ist der so genannte DECT Standard Cipher (DSC). Dieser Algorithmus ist nicht veröffentlicht.

2.4 Authentisierung des Benutzers

Veränderungen wichtiger Einstellungen an DECT-Geräten erfordern in der Regel die Eingabe einer typischerweise 4- bis 8-stelligen Geheimnummer, der persönlichen Identifikationsnummer (PIN). Beispielsweise ist die PIN-Eingabe erforderlich, wenn an einem DECT-Telefon Nummernsperren o.ä. eingegeben werden sollen. Die PIN ist in der Regel änderbar, indem im entsprechenden Menü zuerst die aktuell gültige PIN eingegeben wird und dann die PIN, die zukünftig gültig sein soll.

2.5 Subscription

Als Subscription bezeichnet man die Anmeldung eines PP bei einem FP mit der Folge, dass dem PP fortan die Dienste des FP (und des damit verbundenen DECT-Netzwerks) zur Verfügung stehen. Auch bei der Subscription ist in der Regel die Eingabe einer PIN (siehe Authentisierung des Benutzers) erforderlich. Bei den meisten DECT-Telefonen für den Heimgebrauch wird die PIN im FP gespeichert und muss bei der Anmeldung eines PP auf diesem PP eingegeben werden, nachdem der FP durch Knopfdruck in einen Zustand versetzt wurde, der für eine begrenzte Zeit Anmeldungen neuer PPs zulässt. Während eines solchen Subscription-Prozesses wird für den PP ein Zugriffsrecht zum FP vereinbart und es wird bei FP und PP das Langzeitgeheimnis UAK für das Geräte-Paar (FP, PP) erzeugt. Dabei muss in beiden Geräten der gleiche Authentication Code (AC) vorhanden sein, denn der AC fließt in die Berechnung des neuen UAK ein[9]. Der UAK wird fortan bei jedem Verbindungsaufbau für die Authentisierung benutzt. Geräte, die dem Generic Access Profile (GAP, [EN300444]) genügen, unterstützen eine so genannte On-Air-Subscription. Dabei wird die für die Subscription benötigte Zufallszahl RS über die Luftschnittstelle übertragen.

3. Gefährdungen

Neben den Gefährdungen, denen leitungsgebundene Netzwerke ausgesetzt sind (siehe [GSHB]), ergeben sich bei der Nutzung von Funknetz-Technik zusätzliche Gefährdungen, die insbesondere auf den Sicherheitsschwächen der verwendeten Protokolle sowie auf der unkontrollierten Ausbreitung der Funkwellen basieren.

3.1 Unkontrollierte Ausbreitung der Funkwellen

Der Funkverkehr von DECT-Verbindungen kann mit Hilfe von DECT-Protokollanalysatoren passiv empfangen und aufgezeichnet werden. Alle Schichten des DECT-Protokoll-Stacks können offline betrachtet bzw. analysiert werden. Das Extrahieren und Mitlesen der übertragenen Nutzdaten ist bei fehlender Verschlüsselung möglich. Durch den Einsatz einer Antenne mit starker Richtcharakteristik und geeigneter Elektronik zur Verstärkung eines empfangenen DECT-Signals kann ein solcher „Lauschangriff“ auch noch in einer gegenüber der Reichweite normaler DECT-Geräte größeren Entfernung durchgeführt werden. Wünschenswert ist daher eine dynamische Anpassung der Sendeleistung der DECT-Geräte auf ein akzeptables Minimum, um den skizzierten Lauschangriff zumindest zu erschweren. Eine Sendeleistungsregelung ist allerdings optional und wird nicht von jedem DECT-Gerät unterstützt.

---

9 Der neue UAK entspricht dem bei der Authentisierung mit Verwendung von AC entstehenden KS´ in Abb. C-6

3.2 Schwächen im Sicherheitskonzept

3.2.1 Authentisierung und Subscription

Im Regelfall authentisiert sich nur der PP gegenüber dem FP, die Authentisierung des FP findet in der Regel nur bei der Subscription statt.

Der Authentisierungsalgorithmus benutzt ein 128 Bit langes Geheimnis, den UAK. Dieser Algorithmus (siehe Kapitel 2.1 und Kapitel 2.2) ist nicht öffentlich bekannt, so dass über dessen tatsächliche Stärke (genau 128 Bit oder deutlich weniger) nur gemutmaßt werden kann.

In der Implementierung des Schlüsselmanagements haben die Hersteller einige Freiheiten. Es ist in der Regel möglich, einen PP an einen FP neu anzumelden, auch wenn diese noch kein gemeinsames Geheimnis UAK besitzen (Subscription). Im GAP ist die Anmeldung über die Luftschnittstelle vorgesehen. Dabei werden ausschließlich der AC (32 Bit) und die Zufallszahl RS (64 Bit) benutzt, um den UAK zu erzeugen, so dass die kryptographische Stärke (Entropie) des UAK auf maximal 96 Bit beschränkt ist. In diesem Zusammenhang muss bei der On-Air-Subscription berücksichtigt werden, dass die Zufallszahl RS über die Luftschnittstelle ungesichert übertragen wird. Auch wenn die Zufallszahl RS selten übertragen werden muss, stellt dies eine Gefährdung dar, welche die kryptographische Stärke des UAK weiter reduzieren kann.

Der AC wird in der Regel aus der PIN generiert, indem die Ziffern mit jeweils 4 Bits codiert werden. Da bei dieser Codierung nicht alle Werte angenommen werden können, ist die Entropie des AC selbst bei 8-stelligen PINs auf maximal 27 Bit beschränkt, bei kürzeren PINs reduziert sie sich entsprechend weiter.

Die Qualität des implementierten Zufallsgenerators, der zur Erzeugung von RS dient, wirkt sich zusätzlich entscheidend auf die Entropie des UAK aus.

3.2.2 Verschlüsselung und Integritätsprüfung

In der Produktwerbung findet man gelegentlich die Behauptung, dass allein die Verwendung des digitalen DECT-Standards Abhörsicherheit garantiert. Für einen qualifizierten Angreifer stellt die digitale Übertragung allein jedoch kein Hindernis dar, wenn die Verschlüsselung in den DECT-Geräten nicht implementiert ist. Genau das ist aber bei vielen DECT-Geräten der Fall und diese Schwachstelle kann leicht ausgenutzt werden. Entsprechende Geräte zum Aufzeichnen der über die DECT-Luftschnittstelle übertragenen Protokoll- und Nutzdaten (Protokollanalysatoren) sind auf dem Markt ebenso verfügbar wie komplette Systeme zum Abhören unverschlüsselter DECT-Sprach-Telefonate. Wird an einem FP, der Verschlüsselung unterstützt, ein PP eingesetzt, der diese Funktion nicht bietet, wird typischerweise der PP nicht abgewiesen, sondern die Kommunikation findet automatisch unverschlüsselt statt. Daher muss der Anwender hier darauf achten, dass alle eingesetzten Geräte (insbesondere auch die PPs) eine Verschlüsselung unterstützen.

Ist die Verschlüsselung aktiviert, so wird für die Verschlüsselung ein 64 Bit langer Chiffrier-Schlüssel CK benutzt. Diese Schlüssellänge wird von Experten allenfalls für ein mittleres Sicherheitsniveau als ausreichend angesehen.

Der verwendete Verschlüsselungsalgorithmus DSC (DECT Standard Cipher) ist nicht öffentlich bekannt. Es gibt keine frei verfügbaren Forschungsergebnisse über die algorithmische Sicherheit des DSC, so dass darüber keine zuverlässige Aussage gemacht werden kann.

Da es sich bei DSC um eine Stromchiffrierung handelt, muss beachtet werden, dass bei Verwendung derartiger Chiffren sich der Schlüsselstrom nicht innerhalb kurzer Zeiträume wiederholen darf. Falls dies geschieht, entspricht die XOR-Summe der jeweiligen Chiffrate der XOR-Summe der zugehörigen Klartexte, da sich die identischen Bitströme der Schlüsselströme gegenseitig aufheben (dies wird auch als „In-die-Tiefe-Lesen“ bezeichnet). Je nach Redundanz der benutzten Klartexte erlaubt dies deren Rekonstruktion. Bei einem ausreichend großen Schlüsselraum und kryptographisch starken Schlüsselstromgenerator besteht hier keine Gefahr. Der DECT-Standard erlaubt jedoch die Nutzung eines stati-

schen Chiffrier-Schlüssels SCK. Da der SCK permanent beibehalten wird, hängt die Variation der Schlüsselströme ausschließlich vom Initialisierungsvektor IV ab. Die effektive Länge des IV beträgt 28 Bit. Da der IV im Wesentlichen der Frame-Nummer entspricht, die infolge des kontinuierlichen Sendens des FP alle 10 ms um 1 erhöht wird, sind nach ca. 1 Monat alle möglichen IV durchlaufen, so dass dann bei Nutzung des SCK identische Bitströme zum Verschlüsseln der Klartexte auftauchen.

Das „In-die-Tiefe-Lesen“ ist unter Umständen auch direkt möglich, wenn eine Kanalbündelung zum Erzielen höherer Datenraten so implementiert ist, dass auf allen Kanälen identische Initialisierungsvektoren verwendet werden, da dann die Schlüsselströme identisch sind. Dies gilt unabhängig davon, ob dabei der statische Schlüssel SCK oder der abgeleitete Schlüssel DCK verwendet wird.

Es gibt in DECT keine kryptographische Absicherung der Integrität der übertragenen Daten. Werden von einem Angreifer gezielt Bits in den Chiffratdaten gestört, so werden genau diese Bits in den Klardaten gestört. Auf diese Weise kann ein Angreifer gezielt Nachrichten manipulieren, wenn er gewisse Kenntnisse über den Nachrichtenaufbau hat.

3.2.3 Unsichere Voreinstellungen

Voreinstellungen sind von Seiten des Herstellers oft unsicher konfiguriert: PINs sind beispielsweise häufig auf „0000“ eingestellt. Auf diese Weise ungeschützte PPs könnten z.B. bei fremden FPs angemeldet werden, wenn der Angreifer kurzzeitig Zugang zum PP hat. Analog können an entsprechend ungeschützten FPs neue PPs unberechtigt angemeldet werden. Bei FPs einiger Hersteller genügt es, einen Knopf zu drücken, um die Bereitschaft für die Anmeldung neuer PPs herzustellen.

3.3 Weitere Gefährdungen

Folgende Aspekte sind ebenfalls zu bedenken:

- Die Verfügbarkeit einer DECT-Infrastruktur kann durch den Einsatz eines gezielt eingesetzten Störsenders beeinträchtigt werden. Durch das reservierte DECT-Frequenzband sind jedoch zufällige Störungen durch legal betriebene, mit anderen Funkstandards arbeitende Geräte ausgeschlossen.
- Handelsübliche oder speziell manipulierte DECT-Geräte können auch zum Abhören von Raumgesprächen oder zur missbräuchlichen Datenübertragung verwendet werden (siehe hierzu auch [BSI03]). Das Abhören von Raumgesprächen ist insbesondere mit solchen Geräten möglich, die eine so genannte Babyphon-Funktion unterstützen.
- Mit Hilfe von Protokollanalysatoren kann überwacht werden, ob und wie oft über einen bestimmten FP – verschlüsselt oder unverschlüsselt - telefoniert wird, somit können ggf. Kommunikationsprofile erstellt werden (siehe [BSI03] zum Thema Kommunikationsprofile).

4. Schutzmaßnahmen

4.1 Einsatz von Verschlüsselung durch gezielte Produktauswahl

DECT-Geräte, die mindestens einen sicherheitsrelevanten Dienst anbieten, sollten Verschlüsselung unterstützen. Es ist durch gezielte Produktauswahl darauf zu achten, dass Verschlüsselung nicht nur vom FP unterstützt wird, sondern auch von den PPs, da die Übertragung sonst unverschlüsselt erfolgt (siehe Kapitel 3.2.2). Hier kann der Benutzer meist nicht aktiv eingreifen und eine Konfiguration wählen, die einen PP, der keine Verschlüsselung unterstützt, abweist.

4.2 Überprüfung und Anpassung von Voreinstellungen

Grundsätzlich ist es empfehlenswert, die vom Hersteller voreingestellten, oft unsicheren Konfigurationen zu überprüfen und - wenn nötig und möglich - zu ändern. Insbesondere die PINs sollten nicht-trivial und mit größtmöglicher Länge gewählt werden.

4.3 Subscription in sicherer Umgebung vornehmen

Die On-Air-Subscription von PPs an die FPs sollte in einer gesicherten Umgebung vorgenommen werden, die einem Angreifer einen Lauschangriff zur Ermittlung der Subscriptions-Parameter möglichst nicht gestattet.

4.4 Gesicherte Montage bzw. Aufstellung eines FP

Um die Anmeldung fremder PPs an einem FP zu vermeiden, sind materielle Sicherungsmaßnahmen zu empfehlen, die den unautorisierten Zugriff auf einen FP verhindern.

Die gesicherte Montage eines FP ist weiterhin bei der Verwendung eines FP mit Ethernet-Anschluss (siehe Kapitel 1.4) sehr wichtig, da ein Zugriff auf den Ethernet-Anschluss einen Angriff auf die LAN-Infrastruktur gestattet, an die der FP angeschlossen ist.

4.5 Zusatzmaßnahmen bei Verwendung des Datenmodus

Über die bereits genannten Maßnahmen hinaus sollten für im Datenmodus arbeitende DECT-Geräte, falls dies technisch möglich ist, in Abhängigkeit des individuellen Schutzbedarfs weitere lokale Schutzmaßnahmen implementiert werden, wie z.B.

- Benutzerauthentisierung
- Virenschutz
- Personal Firewall
- restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene
- Einsatz von zusätzlicher Verschlüsselung und Integritätsschutz (unabhängig von den DECT-Mechanismen greifend, z.B. VPN-Tunnel)

Informationen hierzu findet man im IT-Grundschutzhandbuch des BSI [GSHB].

5. Ausblick

Die Nutzung von DECT für die reine Datenübertragung wird aufgrund der stark eingeschränkten Übertragungsrate zurückgehen. Hier ist eher mit der vollständigen Ablösung durch andere Techniken wie Bluetooth oder WLAN zu rechnen.

Es ist eine Zunahme von Kombigeräten festzustellen, die neben DECT auch weitere Schnittstellen wie z.B. Ethernet, WLAN oder Bluetooth besitzen. Solche Kombigeräte erfordern eine Sicherheitsanalyse, die über die hier beschriebene DECT-Technologie hinausgeht. Dabei ist jede Schnittstelle zunächst für sich zu betrachten und geeignet abzusichern. Weitergehend muss aber berücksichtigt werden, dass übergreifende Effekte entstehen können, die über eine Sicherheitslücke auf einer Schnittstelle einen Angriff auf einer anderen Schnittstelle ermöglichen. Beispielsweise könnte durch einen administrativen Eingriff über einen schlecht abgesicherten WLAN-Zugang auf einen FP die Konfiguration für die DECT-Kommunikation manipuliert werden.

6. Fazit

DECT bietet insgesamt einen wesentlich höheren Sicherheitsstandard als analoge Schnurlos-Standards, bei denen bereits ein Funkscanner zum Abhören der Telefonate ausreicht. Diese Aussage gilt insbesondere für solche DECT-Geräte, bei denen die im Standard optional vorgesehene Verschlüsselung implementiert ist.

Allerdings gibt es auf dem Markt auch zahlreiche Geräte, bei denen die DECT-Verschlüsselung überhaupt nicht implementiert ist.

Da die DECT-Algorithmen nicht öffentlich bekannt sind, kann über deren tatsächliche Stärke keine zuverlässige Aussage gemacht werden. Für hochsensible Anwendungen kann daher generell deren Einsatz allein nicht empfohlen werden. Für diesen Fall sind weitere Schutzmaßnahmen zu ergreifen.

7. Literatur / Links

Ausführliche Informationen zur DECT-Spezifikation in deutscher Sprache kann man u.a. dem Buch [Wa01] entnehmen. Eine gute Kurz-Beschreibung findet sich z.B. in [Lü01]. Es gibt zahlreiche Bücher und Publikationen zum Thema DECT. Die Liste der hier aufgeführten Titel und Links stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

Aktuelle Informationen zu DECT enthalten die Internet-Seiten [DECTWE] und [DECTFO].

Eine Diskussion verschiedener Schwächen im Sicherheitskonzept von DECT findet man auch in der Spezifikation [EN300175].

[BSI03] GSM-Mobilfunk, Gefährdungen und Sicherheitsmaßnahmen, BSI 2003, http://www.bsi.bund.de/literat/doc/gsm/gsm.pdf

[DECTFO] DECT-Forum http://www.dect.ch

[DECTWE] DECT-web http://www.dectweb.com

[EN300175] ETSI EN 300 175-1, 300 175-2 bis 300 175-8, European Standard (Telecommunications series), Digital Enhanced Cordless Telecommunications (DECT), Common Interface (CI), Part 1 bis Part 8

[EN300444] ETSI EN 300 444, Generic Access Profile (GAP)

[EN300449] ETSI EN 301 649, DECT Packet Radio Service (DPRS)

[EN301650] ETSI EN 301 650, DECT Multimedia Access Profile (DMAP)

[GSHB] Grundschutzhandbuch des BSI, http://www.bsi.bund.de/gshb

[Lü01] C. Lüders, Mobilfunksysteme, Würzburg: Vogel Verlag, 2001

[Wa01] B. Walke, Mobilfunknetze und ihre Protokolle – Band 2, Stuttgart: Teubner Verlag, 2001

8. Abkürzungen

AC	Authentication Code
ADPCM	Adaptive Differential Pulse Code Modulation
CK	Cipher Key
DAP	DECT Access Point
DB	Data Base
DCK	Derived Cipher Key

DECT	Digital Enhanced Cordless Telecommunications
DFS	DECT Fixed System
DLC	Data Link Control
DMAP	DECT Multimedia Access Profile
DPRS	DECT Packet Radio Service
DSC	DECT Standard Cipher
ETSI	European Telecommunications Standards Institute
FDM	Frequency Division Multiplex, Frequenzmultiplex
FP	Fixed Part, DECT-Feststation
GAP	Generic Access Profile
GMSK	Gaussian Minimum Shift Keying
IAP	ISDN Access Interworking Profile
IETF	Internet Engineering Task Force
IP	Internet Protocol
IT	Information Technology
IV	Initialisierungsvektor
IWU	Interworking Unit
LAN	Local Area Network
MAC	Medium Access Control
PARK	Portable Access Rights Key
PBX	Private Branch Exchange
PIN	Personal Identification Number
PP	Portable Part, DECT-Mobilstation
RFC	Request for Comment, Veröffentlichung der IETF
RFP	Radio Fixed Part
RFPI	Radio Fixed Part Identity
SCK	Static Cipher Key
SIP	Session Initiation Protocol
TDD	Time Division Duplex, Zeitduplex
TDMA	Time Division Multiple Access, Zeitmultiplex
TPUI	Temporary User Identity
UAK	User Authentication Key
VoIP	Voice over IP
VPN	Virtual Privat Network
WLAN	Wireless LAN
WLL	Wireless Local Loop
WRS	Wireless Relay Station, DECT-Repeater

9. Glossar

Chiffrier-Schlüssel (Cipher Key, CK)
: Dient zusammen mit einem Initialisierungsvektors zur Erzeugung eines Schlüsselstroms, mit dem der Klartext über ein XOR verknüpft und damit verschlüsselt wird

Downlink
: Frequenz-Zeit-Kanal, in dem der FP zum PP sendet

Fixed Part (FP)
: DECT-Feststation, die als Basisstation die Funkverbindung mit dem Portable Part und mit der Festnetzseite unterhält

Paging
: Ausruf eines Teilnehmers in einem Teil des Mobilfunknetzes, verbunden mit der Bitte, dass sich das Gerät des Teilnehmers meldet

Persönliche Identifikationsnummer (PIN)
: 4- bis 8-stelligen Geheimnummer, die zur Authentisierung des Benutzers dient

Portable Part (PP)
: DECT-Mobilstation

RAND_F, RAND_P
: Zufallswerte, die für Authentisierung und Subscription verwendet werden, dabei wird RAND_F vom FP erzeugt und RAND_P vom PP.

RS
: Zufallswert, der für Authentisierung und Subscription verwendet wird

Subscription
: Anmeldung eines PP bei einem FP

User Authentication Key (UAK)
: Langzeitgeheimnis für die Authentisierung

Uplink
: Frequenz-Zeit-Kanal, den der PP zum Senden an den FP verwendet

D. WiMAX, IEEE 802.16

Inhaltsverzeichnis des Abschnitts

1. Grundlagen und Funktionalität

WiMAX (Worldwide Interoperability for Microwave Access) ist ein Industriestandard, der auf den Standards der Serien IEEE[1] 802.16 und ETSI[2] HIPERMAN (High Performance Radio MAN[3]) basiert. Inhalt dieser Standards ist die Spezifikation eines drahtlosen Breitband-MAN. Das WiMAX-Forum ist verantwortlich für die WiMAX-Spezifikationen und unterstützt die Entwicklung von standardkonformen und interoperablen Produkten. Die Rolle des WiMAX-Forums ist vergleichbar mit der Rolle der Wi-Fi Alliance im WLAN-Bereich.

Der Standard IEEE 802.16 hat in der ersten veröffentlichten Version von 2001 unter dem Titel „Air Interface for Fixed Broadband Wireless Access System" lediglich eine Kommunikation zwischen ortsfesten Stationen beschrieben. Die Kommunikation erfolgt dabei zwischen einer zentralen Base Station und mehreren stationären Subscriber Stations. Ursprünglich wurde im Jahr 2001 diese Funkschnittstelle für Frequenzen zwischen 10 GHz und 66 GHz festgelegt. Problem dieses Frequenzbereiches ist es allerdings, dass eine Sichtverbindung (Line-of-Sight, LOS) zwischen Sender und Empfänger bestehen muss. Die Verbindung soll unter Idealbedingungen eine Datenrate von 70 MBit/s und Reichweiten von bis zu 50 km erreichen können. Es bestand jedoch ein größeres Interesse, den Frequenzbereich zwischen 2 GHz und 11 GHz für eine drahtlose MAN-Technik zu etablieren, da damit keine Sichtverbindung mehr erforderlich ist. Der daraus entstandene Standard ist IEEE 802.16-2004 und wird auch WiMAX Fixed genannt, da auch in diesem Standard nur ortsfeste Subscriber Stations beschrieben werden.

Die Erweiterung um die direkte Unterstützung mobiler Endgeräte ist in der Ergänzung IEEE 802.16e spezifiziert und ist im Februar 2006 veröffentlicht worden. Dieser Standard wird auch als WiMAX Mobile bezeichnet. Mobilität ist hier eher im Sinne von WLAN zu verstehen und nicht mit der Mobilität zu verwechseln, die Mobilfunksysteme wie GSM und UMTS bieten.

Bisher ist die WiMAX-Technik noch in der Erprobungsphase. Im Januar 2006 wurden die ersten Produkte für WiMAX Fixed durch das WiMAX-Forum zertifiziert.

Im Folgenden werden die beiden aktuellen Standards IEEE 802.16-2004 und IEEE 802.16e kurz vorgestellt. In den weiteren Kapiteln werden dann die spezifizierten Sicherheitsfunktionen beschrieben, mögliche Gefahren analysiert und entsprechende Gegenmaßnahmen empfohlen.

1.1 WiMAX Fixed (IEEE 802.16-2004)

WiMAX Fixed nach dem Standard IEEE 802.16-2004 dient primär zur Überbrückung der so genannten letzten Meile zum Teilnehmeranschluss und ist daher zunächst für Netzbetreiber von Interesse. Weiterhin kann WiMAX Fixed eine Alternative für Richtfunkstrecken sein, die beispielsweise zur Ankopplung von GSM/UMTS-Netzelementen verwendet werden. Für Unternehmen, die bereits über eigene Kabelnetze verfügen (z.B. Energieversorger und Stadtwerke) ist WiMAX als Redundanz interessant. Für Unternehmen, die grundstückübergreifend in einem Radius mehrerer Kilometer verschiedene Gelände vernetzen müssen, kann WiMAX eine Alternative zur Anbindung über ein öffentliches Netz sein. Außerdem kann WiMAX prinzipiell auch in Backbone-Netzen und als WLAN Distribution System eingesetzt werden.

WiMAX bietet die Möglichkeit flexible Bandbreiten für die angeschlossenen Geräte und QoS zu nutzen.

---

1 IEEE = Institute of Electrical and Electronics Engineers

2 ETSI = European Telecommunications Standards Institute

3 MAN = Metropolitan Area Network

1.1.1 Architektur

In WiMAX Fixed werden zwei Kommunikationsformen unterschieden:

- Point-to-Multipoint-Modus (siehe Abb. D-1)
- Mesh Modus (siehe Abb. D-2)

Im Point-to-Multipoint-Modus sendet die Base Station (Basisstation) über eine Sektorenantenne die Daten an alle Subscriber Stations in diesem Sektor[4]. Die Subscriber Stations übernehmen nur die Pakete, die für ihre Verbindung gültig sind. Auch Multicast (z.B. Video) oder Broadcast Verbindungen sind möglich. Die Kommunikation erfolgt immer zwischen der Base Station und den Subscriber Stations. Eine direkte Kommunikation zwischen verschiedenen Subscriber Stations ist nicht erlaubt. Dies ist dagegen im Mesh-Modus erlaubt. Eine Subscriber-Station im Mesh-Modus wird auch Mesh Subscriber Station genannt. Die Mesh Base Station ist diejenige Station, die eine direkte Verbindung zu Stationen außerhalb des Funknetzes hat. Die Kommunikation zu diesem externen Netz kann entweder direkt von den Mesh Subscriber Stations zur Mesh Base Station erfolgen, oder über mehrere Mesh Subscriber Stations geroutet werden. Auch eine direkte Kommunikation zwischen den Mesh Subscriber Stations ist möglich, ohne dass diese eine Verbindung zum externen Netz oder der Mesh Base Station haben.

Der IEEE Standard 802.16-2004 spezifiziert die physikalische Übertragung (Physical Layer) und den Kanalzugriff (Medium Access Control, MAC) zwischen Base Station und Subscriber Stations bzw. zwischen Subscriber Stations.

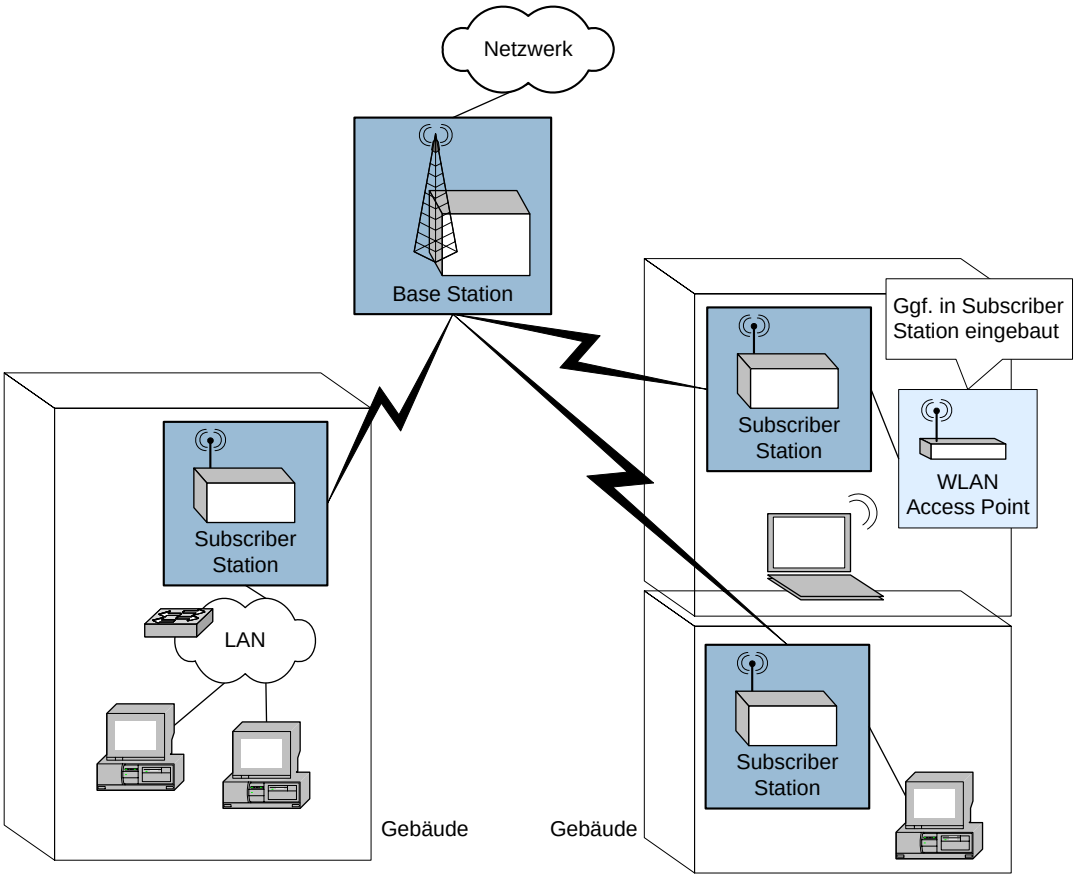


Abb. D-1: Point-to-Multipoint-Modus (Beispiel)

[4] Die Subscriber Station bildet den Teilnehmeranschluss mit einer WiMAX-Luftschnittstelle auf der einen Seite und beispielsweise einem oder mehreren Ethernet-Anschlüssen oder einem integrierten WLAN Access Point auf der anderen Seite.

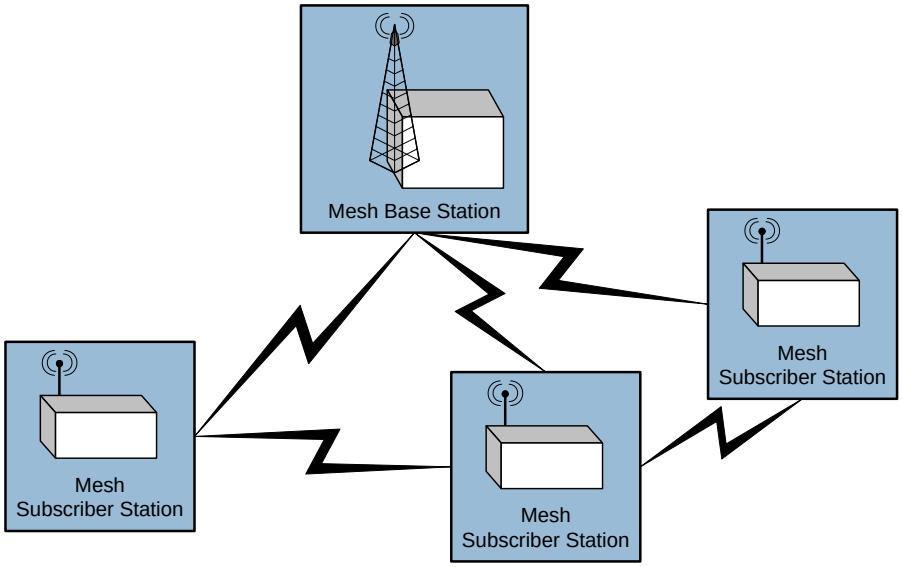


Abb. D-2: Mesh Modus (Beispiel)

1.1.2 Physikalische Übertragung

Der Standard spezifiziert verschiedene physikalische Übertragungsverfahren, die sich primär in der Nutzung der Frequenzbänder und der verwendeten Modulationsverfahren unterscheiden:

- WirelessMAN-SC[5]

  WirelessMAN-SC ist für die Nutzung von Frequenzen zwischen 10 GHz und 66 GHz spezifiziert worden. Dabei sollen unter Idealbedingungen (Sichtverbindung zwischen Sender und Empfänger, kurz: LOS[6]) Datenraten von 70 MBit/s und Reichweiten von bis zu 50 km erreicht werden können.

- WirelessMAN-SCa

  Dieses Übertragungsverfahren ist von WirelessMAN-SC abgeleitet und für die Nutzung von Frequenzen unter 11GHz ausgelegt. Damit sind dann auch NLOS-Verbindungen (Non-LOS-Verbindungen) möglich.

- WirelessMAN-OFDM

  Die Spezifikationen für WirelessMAN-OFDM beschreiben die Nutzung von Frequenzen unter 11 GHz. Auch hier sind damit NLOS-Verbindungen möglich. Als Modulationsverfahren kommt OFDM (Orthogonal Frequency Division Multiplexing) zum Einsatz.

- WirelessMAN-OFDMA

  Diese Variante basiert ähnlich zu WirelessMAN-OFDM auf OFDM und ist für Frequenzen unter 11 GHz und NLOS-Verbindungen geeignet. Darüber hinaus wird ein Mehrfachzugriff mit orthogonalen Unterträgern spezifiziert, d.h. die Aufteilung des Mediums auf mehrere Nutzer wird bei OFDMA durch die physikalische Übertragung (in Ergänzung zum MAC-Protokoll) unterstützt.

- WirelessHUMAN[7]

  WirelessHUMAN sieht die Nutzung des 5-GHz-Bereichs vor. Das Kanalraster wurde aus Interferenzgründen an die Frequenzen von WLAN nach IEEE 802.11a angepasst. Die sonstigen Spezifi-

---

5 SC = Single Carrier

6 LOS ist eine Abkürzung für Line-of-Sight. Sichtverbindung bedeutet hier stets eine funktechnische (nicht optische) Sichtverbindung. Dabei muss ein spezielles Ellipsoid mit einer gewissen Ausdehnung zwischen Sender und Empfänger weitestgehend frei von Hindernissen sein. Dies ist die sogenannte Fresnel-Zone.

7 HUMAN = High-speed Unlicensed MAN

kationen basieren entweder auf WirelessMAN-SCa oder WirelessMAN-OFDM oder Wireless-MAN-OFDMA.

In Deutschland regelt die Bundesnetzagentur die Vergabe der Frequenzen für WiMAX-Netze. Hier soll der Frequenzbereich zwischen 3410 MHz und 3694 MHz, der ursprünglich für Wireless Local Loop (WLL) vorgesehen war, für die WiMAX Nutzung verwendet werden.

1.1.3 MAC-Layer

Der MAC-Layer ist im WiMAX-Standard in drei Sublayer aufgeteilt:

- ► Der Service Specific Convergence Sublayer dient der Anpassung an verschiedene Netzwerkprotokolle, um beispielsweise eine Kompatibilität zu sowohl ATM-Netzen, als auch IP-Netzen zu gewährleisten.
- ► Der Common Part Sublayer enthält die eigentlichen Funktionen des MAC-Layers wie Bandbreiteneinteilung, Verbindungsaufbau und Verbindungshaltung.
- ► Die Sicherheitsfunktionen bilden den Security Sublayer. Diese werden im Kapitel 2.1 beschrieben.

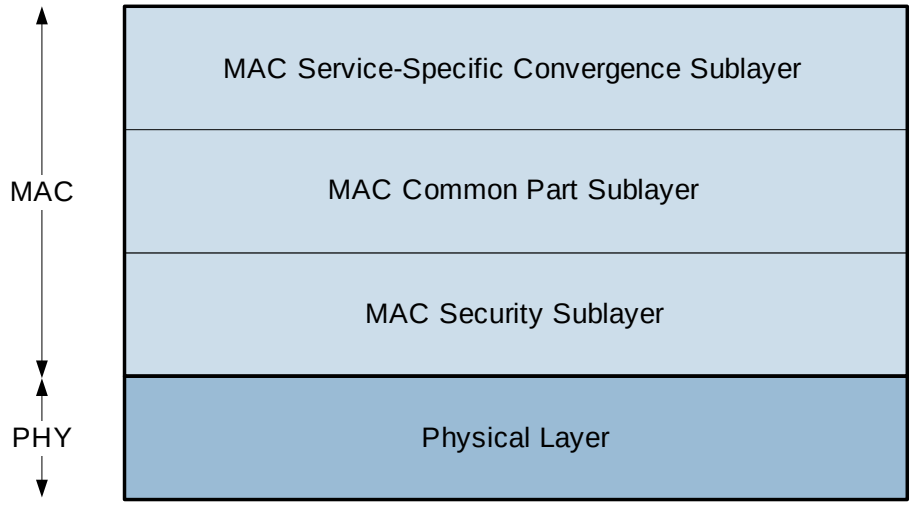


Abb. D-3: Struktur des MAC Layer

Jede Subscriber Station hat eine eindeutige 48-Bit lange MAC-Adresse. Jede Verbindung zwischen einer Subscriber Station und einer Base Station wird durch einen 16-Bit langen Connection Identifier bestimmt. Beim Aufbau einer Verbindung werden parallel zur eigentlichen Datenverbindung mehrere Management Verbindungen aufgebaut. MAC-Adressen werden unverschlüsselt übertragen.

1.2 WiMAX Mobile (IEEE802.16e)

Die als WiMAX Mobile bezeichnete Erweiterung IEEE 802.16e des WiMAX-Standards erlaubt die direkte Anbindung von mobilen Endgeräten. Im Unterschied zu WiMAX Fixed soll WiMAX Mobile ausschließlich Frequenzen in Bereichen unter 11 GHz nutzen. Um den Anforderungen an mobile Endgeräte gerecht zu werden, wurden zusätzliche Funktionen in den Standard aufgenommen. Dazu gehören beispielsweise:

- ► Sleep Mode, ein besonders Energie-sparender Betriebszustand
- ► Handover, die Möglichkeit der Bewegung eines Endgeräts zwischen dem Abdeckungsbereich von Base Stations unter Aufrechterhaltung der Ende-zu-Ende-Kommunikation (d.h. ohne signifikante Einbußen hinsichtlich der Qualität)

Weiterhin sind für die Unterstützung mobiler Endgeräte Anpassungen im gesamten Protokoll-Stack des Basis-Standards IEEE 802.16-2004 gemacht worden. Insbesondere wurden einige Sicherheitsfunktionen speziell für mobile Geräte spezifiziert bzw. adaptiert. Diese Funktionen werden in Kapitel 2.2 vorgestellt.

Mit ersten Produkten wird Ende 2006 gerechnet. Wie sich die Beziehung von WiMAX Mobile zu UMTS (insbesondere seit der Einführung von HSDPA[8]) entwickeln wird, bleibt abzuwarten. Es ist jedoch kein unrealistisches Szenario, dass sich WiMAX zu einer weiteren Zugangstechnik zum UMTS-Kernnetz entwickeln wird.

1.2.1 Architektur

Die Ergänzung IEEE 802.16e spezifiziert (wie auch der Basisstandard IEEE 802.16) die Protokollebenen zur physikalischen Übertragung und für den Kanalzugriff. Basierend auf IEEE 802.16e hat das WiMAX Forum ein so genanntes Profil für WiMAX Mobile spezifiziert, das neben einer Auswahl aus den verschiedenen in IEEE 802.16e spezifizierten Übertragungsmöglichkeiten auch Konzepte für den Aufbau von WiMAX-Mobile-Netzen festlegt (siehe [WiMAX]).

Neben der Luftschnittstelle (Air Interface) wird hierzu ein Roaming Interface definiert, über das die Anbindung der WiMAX-Infrastruktur an die IP-Infrastruktur eines Netzbetreibers geschieht. Über diese Schnittstelle kann ein mobiler Teilnehmer sich am Netz anmelden, die Informationen für eine Authentisierung werden bereitgestellt, und über Mobile IP wird dem Endgerät die Möglichkeit gegeben sich uneingeschränkt auch IP-Subnetz-übergreifend zu bewegen. Weiterhin werden über das Roaming Interface auch Funktionen zur Abrechnung der Dienstnutzung angestoßen. Abb. D-4 zeigt die vom WiMAX-Forum spezifizierte Architektur im Überblick.

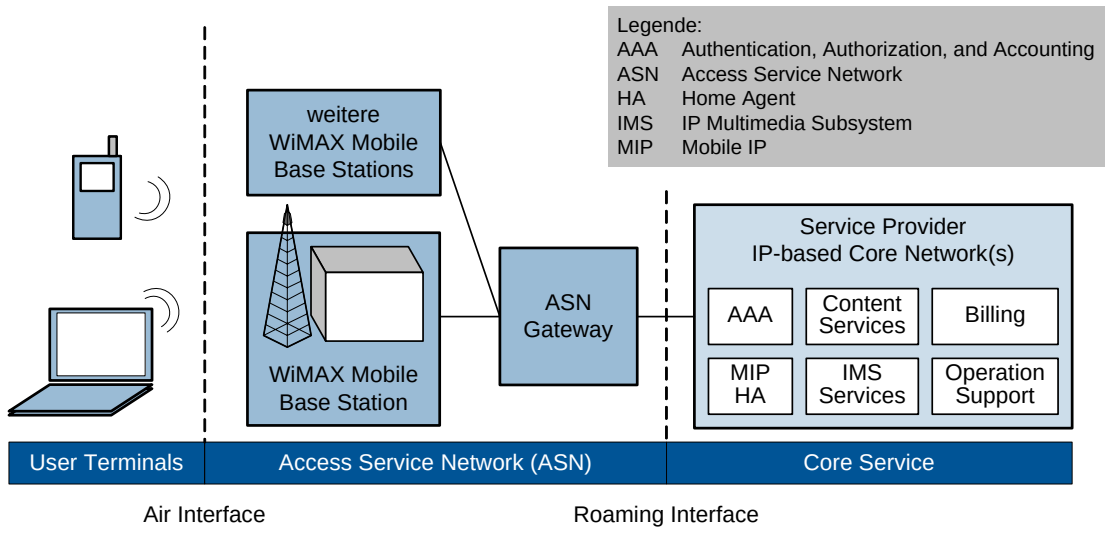


Abb. D-4: Architektur WiMAX Mobile (vereinfacht)

1.2.2 Physikalische Übertragung

In IEEE 802.16e sind folgende der in IEEE 802.16 spezifizierten physikalischen Übertragungsverfahren für die direkte Anbindung mobiler Endgeräte vorgesehen: WirelessMAN-SCa, WirelessMAN-OFDM und WirelessMAN-OFDMA (siehe Kapitel 1.1.2). Das WiMAX-Mobile-Profil des WiMAX-Forums konzentriert sich zunächst auf WirelessMAN-OFDMA.

---

8 HSDPA = High Speed Downlink Packet Access; neueres Übertragungsverfahren in UMTS, das eine Downlink-Datenrate von bis zu 14,4 Mbit/s ermöglichen soll.

Damit ist WiMAX Mobile zunächst auf lizenzierte Bänder festgelegt. Die diesbezügliche Regulierungslage für den Einsatz in Europa und speziell in Deutschland ist noch nicht geklärt.

1.2.3 MAC-Layer

Die wesentlichen Elemente zur Unterstützung mobiler Endgeräte, die auf dem MAC-Layer realisiert werden, sind eine Funktion zur dynamischen An- und Abmeldung von mobilen Endgeräten an einer Base Station und eine Handover-Funktion. Die Handover-Funktion muss dabei einen Wechsel zwischen benachbarten von Base Stations aufgespannten Funkzellen ermöglichen, ohne dass die Ende-zu-Ende-Kommunikation siginifkante Einbußen erfährt. Dabei müssen die ausgehandelten Dienstgüte- und Sicherheitseinstellung einer Verbindung bei einem Handover beibehalten werden. Je nach Anwendung (z.B. Voice over IP) muss ein Handover außerdem sehr schnell ablaufen, damit der Handover nicht spürbar ist. WiMAX Mobile legt hierzu spezifische Protokollmechanismen fest, wie in Abb. D-5 gezeigt wird.

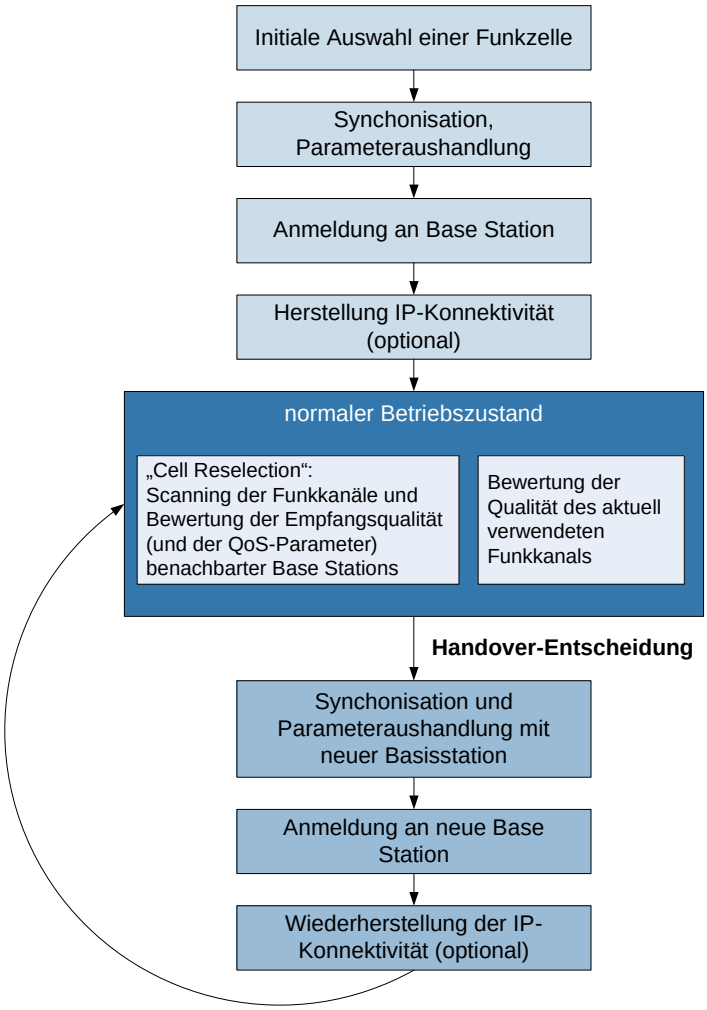


Abb. D-5: Ablauf von Anmeldung und Handover

2. Sicherheitsmechanismen

2.1 WiMAX Fixed (IEEE 802.16-2004)

Die MAC-Schicht der WiMAX-Spezifikation ist dreigeteilt. Den untersten, direkt auf die physikalische Schicht aufsetzenden Teil bildet der Security Sublayer. Der Security Sublayer stellt Sicherheitsmechanismen wie Authentisierung, sicheren Schlüsselaustausch und Verschlüsselung zur Verfügung.

Für diese Aufgabe sind zwei Protokolle spezifiziert:

- Das Encapsulation Protocol ermöglicht die Verschlüsselung der Datenpakete zwischen der Base Station und den Subscriber Stations. Hierfür werden so genannte Cryptographic Suites (Paare von Datenverschlüsselungs- und Authentisierungsmechanismen) und die Regeln für die Anwendung dieser Algorithmen auf die Datenpakete definiert.
- Das Key Management Protocol stellt einen Mechanismus für die sichere Verteilung von Schlüsselmaterial von der Base Station zu den Subscriber Stations bereit.

2.1.1 Security Associations und Schlüsselmaterial bei WiMAX Fixed

Sämtliche Verbindungen und Datenübertragungen zwischen einer Base Station und ihren Subscriber Stations werden so genannten Security Associations (SAs) zugeordnet. Eine SA ist ein Satz von Sicherheitsinformationen, die eine Base Station und eine Subscriber Station teilen, das heißt, alle zugeordneten Verbindungen werden entsprechend der in der SA genannten Sicherheitsmechanismen gesichert. Jede SA hat eine eindeutige Identifikation, den so genannten SAID (SA Identifier).

Während der Initialisierungsphase muss jede Subscriber Station eine primäre SA initiieren. Diese enthält mindestens die zwischen Base Station und Subscriber Station genutzte Cryptographic Suite der Subscriber Station und ggf. darüber hinaus Schlüsselmaterial und Initialisierungsvektoren.

Das Schlüsselmaterial für jede SA wird von der Base Station verwaltet und mit Hilfe des Key-Management-Protokolls (siehe Kapitel 2.1.2) mit den Subscriber Stations synchronisiert. Die folgenden Schlüsseltypen werden unterschieden:

- Authorization Key (AK)

  Der AK wird der Subscriber Station während der Authentisierung von der Base Station zugeteilt und ist eine bestimmte Zeitspanne gültig. Die Subscriber Station muss vor Ablauf der Gültigkeitsdauer einen neuen AK anfordern, wenn sie weiterhin mit der Base Station kommunizieren möchte. Jede Subscriber Station verfügt für alle ihre SAs nur über einen einzigen AK (bzw. während der Übergangsphase von einem bald ablaufenden zu einem neuen AK temporär über zwei AKs).
  Vom AK werden der Key Encryption Key (KEK) und die Message Authentication Keys abgeleitet.
- Traffic Encryption Key (TEK)

  Mit dem TEK wird der Datenverkehr zwischen einer Subscriber Station und der Base Station verschlüsselt. Eine Subscriber Station muss für jede SA einen TEK führen und ist dafür verantwortlich, vor dessen Gültigkeitsablauf einen neuen TEK bei der Base Station anzufordern, der dann mit dem Key Encryption Key verschlüsselt übertragen wird.
- Key Encryption Key (KEK)

  Der KEK wird vom AK abgeleitet und zur Verschlüsselung der TEKs während der Übertragung von der Base Station zur Subscriber Station verwendet.

- Message Authentication Keys

  Mit Message Authentication Keys werden Management-Nachrichten, z.B. zur Anforderung und Verteilung von TEKs, zwischen der Base Station und den Subscriber Stations signiert und verifiziert.

  Abb. D-6 zeigt den Aufbau einer SA und die Verwendung der verschiedenen Schlüsseltypen.

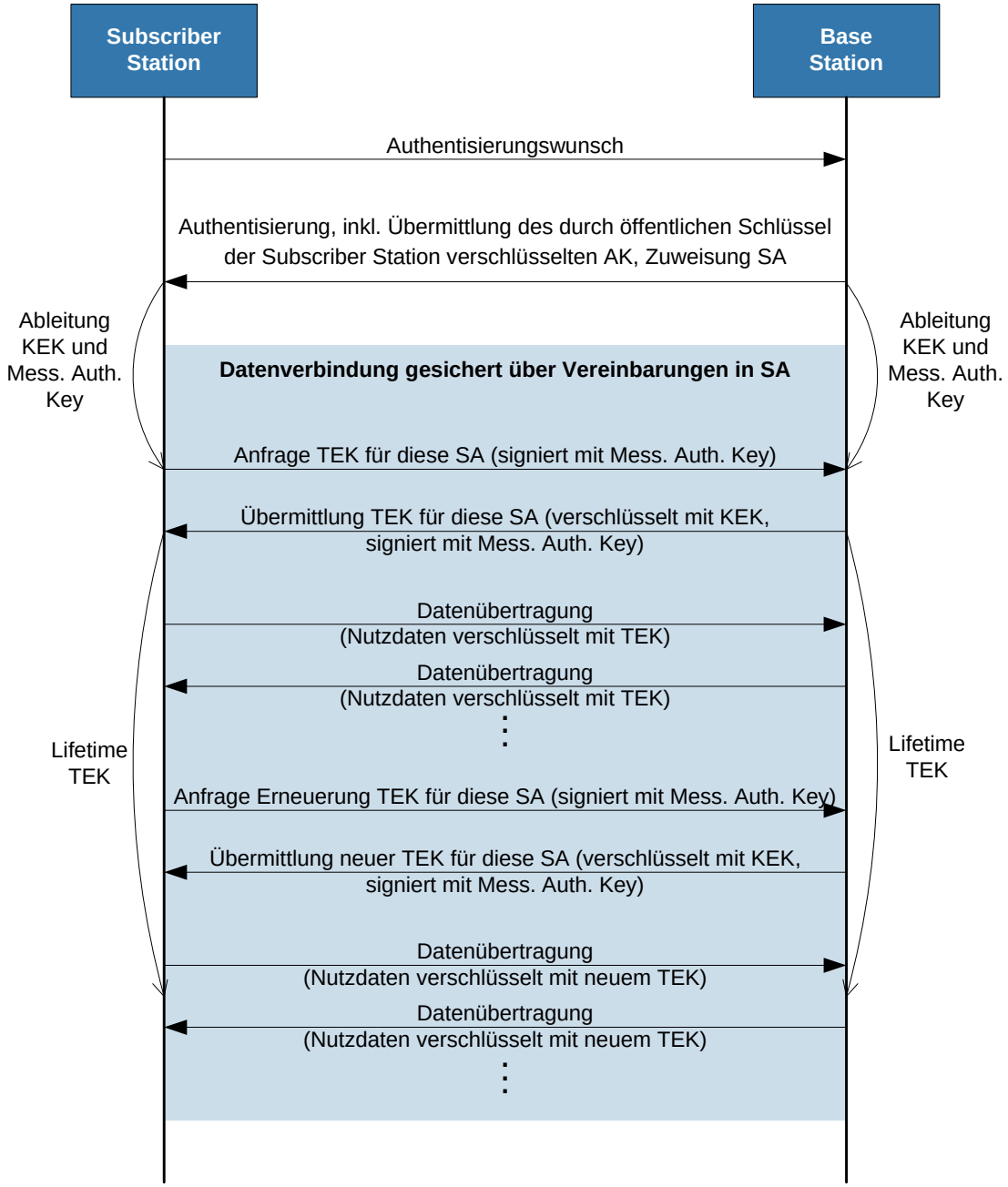


Abb. D-6: Verwendung von Schlüsseln in WiMAX Fixed

2.1.2 Privacy Key Management Protocol (PKM-Protokoll) bei WiMAX Fixed

Jede Subscriber Station verfügt über ein vom Hersteller ausgegebenes und installiertes digitales X.509-Zertifikat mit zugehörigem privatem Schlüssel und über das zugehörige X.509-Zertifikat des Herstellers.

Eine Subscriber Station beginnt den Authentisierungsprozess mit einer Authentication Information Message, in der sie der Base Station das Zertifikat des Herstellers übermittelt. Direkt danach sendet sie einen Authorization Request an die Base Station, der die folgenden Informationen enthält:

- ► das Zertifikat der Subscriber Station
- ► eine Liste von Cryptographic Suite IDs, die von der Subscriber Station unterstützt werden (siehe Kapitel 2.1.3)
- ► den Connection Identifier der Subscriber Station

Die Base Station prüft die Zertifikate und stellt fest, ob die Subscriber Station autorisiert ist, das WiMAX-basierte Netzwerk zu nutzen. Ist dies der Fall, erhält die Subscriber Station von der Base Station einen Authorization Reply mit den folgenden Informationen:

- ► einen Authorization Key (AK), der mit dem im Zertifikat übermittelten Public Key der Subscriber Station verschlüsselt wurde (siehe Abb. D-6)
- ► eine 4 Bit lange Key Sequence Number, durch die die einzelnen Schlüsselgenerationen unterschieden werden
- ► die Gültigkeitsdauer des AK
- ► die SAIDs und Informationen (Auswahl einer Cryptographic Suite und ggf. Traffic Encryption Keys und deren Gültigkeitsdauer) der primären und ggf. weiterer statischer SAs

Abb. D-7 zeigt den Ablauf der Authentisierung im Überblick.

Von dem AK werden dann sowohl von der Base Station als auch von der Subscriber Station nach einem vorgegebenen Algorithmus Key Encryption Key (KEK) und Message Authentication Keys abgeleitet, welche die weitere Anforderung und Übermittlung von Traffic Encryption Keys (TEK) absichern.

Sollen die Daten im WiMAX-basierten Netz verschlüsselt werden, muss die Subscriber Station immer vor Ablauf der Gültigkeitsdauer des verwendeten TEK einen neuen TEK anfordern. In der Point-to-Multipoint-Architektur startet sie dazu für jede ihrer SAs eine TEK State Machine, die für das regelmäßige Senden von Key Request Messages zuständig ist und somit das Schlüsselmaterial aktuell hält. Die Key Request Messages werden mit Message Authentication Keys signiert und der TEK wird mit dem Key Encryption Key verschlüsselt übermittelt.

In der Mesh-Architektur hingegen startet die Subscriber Station für jede Nachbarstation eine TEK State Machine, die regelmäßig Key Request Messages für TEKs für alle SAs sendet. Die Nachbarstationen übermitteln den aktuellen TEK der Base Station, der in dem Fall mit dem Public Key der Subscriber Station verschlüsselt wird.

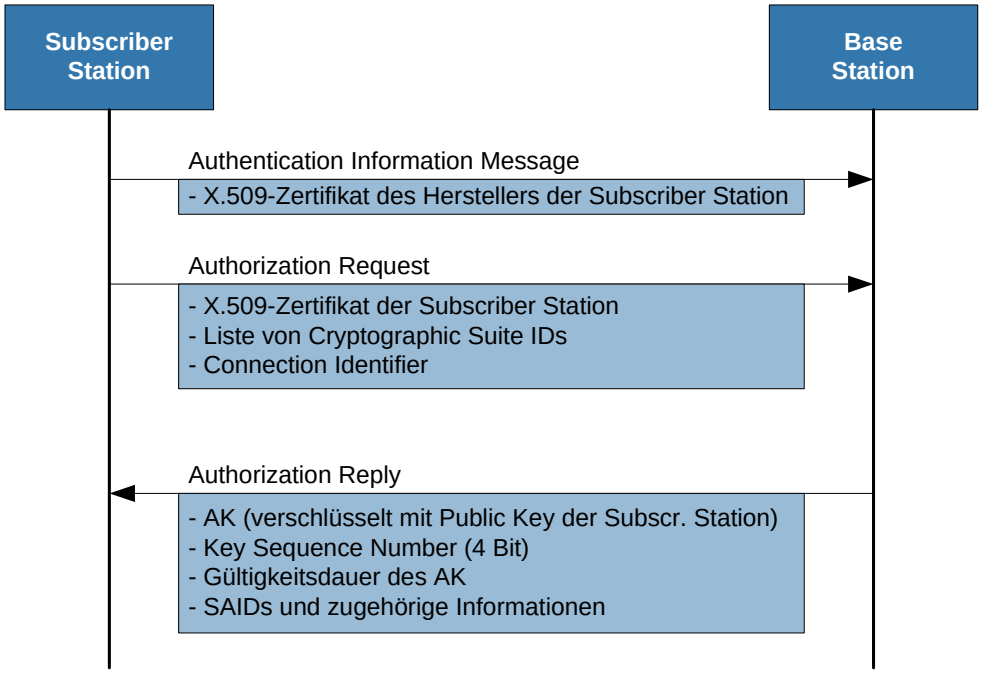


Abb. D-7: Authentisierung in WiMAX Fixed

2.1.3 Encapsulation Protocol bei WiMAX Fixed

Über das Encapsulation Protocol werden so genannte Cryptographic Suites festgelegt, welche die Fähigkeiten der Subscriber Station zur Verschlüsselung und Authentisierung spezifizieren. Jede Cryptographic Suite hat eine eindeutige Identifikation. Eine Liste dieser Identifikationen wird bei der Authentisierung der Subscriber Station an die Base Station übermittelt, die dann die erlaubten SAs ermitteln kann. Die Liste der Cryptographic Suites findet sich in Tab. D–1.

Cryptographic Suite ID	Beschreibung		
	Datenverschlüsselung	Daten-authentisierung	TEK-Verschlüsselung
0x000001	keine	keine	3DES im EDE-Modus mit 128-Bit-Schlüssel
0x010001	DES im CBC-Modus mit 56-Bit-Schlüssel	keine	3DES im EDE-Modus mit 128-Bit-Schlüssel
0x000002	keine	keine	RSA mit 1024-Bit-Schlüssel
0x010002	DES im CBC-Modus mit 56-Bit-Schlüssel	keine	RSA mit 1024-Bit-Schlüssel
0x020003	AES im CCM-Modus mit 128-Bit-Schlüssel	keine	AES im ECB-Modus mit 128-Bit-Schlüssel
Alle anderen Werte	Reserviert		

Tab. D–1: Cryptographic Suites für WiMAX Fixed

Für die Datenverschlüsselung können die folgenden Verschlüsselungsalgorithmen verwendet werden:

- Keine Verschlüsselung
- Data Encryption Standard (DES) im CBC-Modus[9] mit 56-Bit-Schlüssel
- Advanced Encryption Standard (AES) im CCM-Modus[10] mit 128-Bit-Schlüssel

Wenn eine Verschlüsselung erfolgen soll, wird grundsätzlich nur der Nutzdatenteil (Payload) der MAC PDU[11] verschlüsselt (siehe Abb. D-8). Der Generic MAC Header und die optionale CRC werden nicht verschlüsselt. Außerdem werden alle MAC Management-Nachrichten unverschlüsselt übertragen.

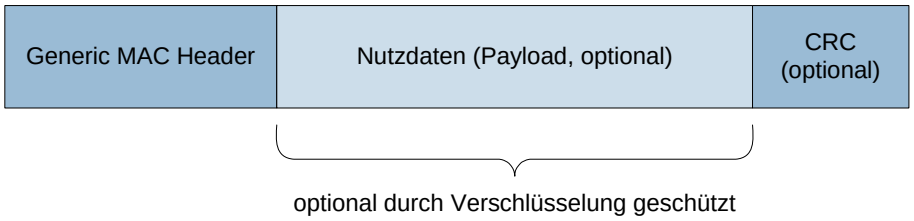


Abb. D-8: Verschlüsselter Bereich in einem MAC-Paket

Eine Datenauthentisierung im Sinne einer kryptographischen Integritätsprüfung ist im WiMAX-Fixed-Standard zunächst nicht vorgesehen (auch wenn CCM dies bereits unterstützt).

Der Traffic Encryption Key kann bei seiner Übermittlung an die Subscriber Station mit den folgenden Verschlüsselungsalgorithmen verschlüsselt werden:

- 3DES im EDE-Modus[12] mit 128-Bit-Schlüssel
- RSA[13] mit 1024-Bit-Schlüssel
- AES im ECB-Modus[14] mit 128-Bit-Schlüssel

2.2 WiMAX Mobile (IEEE802.16e)

Auch in der WiMAX-Mobile-Spezifikation ist die MAC-Schicht dreigeteilt. Hier heißt der für die Sicherheitsaufgaben zuständige Sublayer allerdings nicht mehr Security Sublayer, sondern Privacy Sublayer.

Es gibt ebenso die beiden Protokolle Encapsulation Protocol und Key Management Protocol, letzteres allerdings in zwei Versionen:

- PKMv1 ist vergleichbar mit PKM bei WiMAX Fixed
- PKMv2 bietet erweiterte Funktionen wie z.B. eine neue Schlüsselhierarchie, AES-CMAC, AES Key Wrap und Multicast-/Broadcast-Service

---

9 CBC = Cipher Block Chaining

10 CCM = Counter with CBC-MAC, CBC-MAC = CBC with Message Authentication Code; CCM ist eine generische Methode für die Verschlüsselung und Authentisierung von Daten, die für die Verwendung einer 128-Bit-Blockchiffrierung (z. B. AES) spezifiziert ist. Im WLAN-Kapitel dieses Dokuments ist diese Methode kurz beschrieben.

11 PDU = Protocol Data Unit

12 Bei 3DES (Triple DES) im EDE-Modus werden drei DES-Chriffrierer hintereinander geschaltet, wobei der mittlere DES-Chriffrierer invers eingebaut ist (Encrypt-Decrypt-Encrypt, kurz: EDE).

13 RSA ist ein populärer Public-Key-Algorithmus, der nach seinen Erfindern R. Rivest, A. Shamir und L. Adleman benannt ist.

14 ECB = Electronic Code Book

Die Authentisierung ist bei WiMAX Mobile nicht nur über Zertifikate wie in WiMAX Fixed, sondern auch über das Extensible Authentication Protocol (EAP) möglich[15].

2.2.1 Security Associations und Schlüsselmaterial bei WiMAX Mobile

Das Konzept der Security Associations (SAs) wurde vom WiMAX-Fixed-Standard übernommen. Allerdings gibt es im WiMAX-Mobile-Standard noch weitere SAs. Unterschieden werden:

- SAs für den Unicast-Verkehr, wie bereits in Kapitel 2.1.1 beschriebenen
- Group Security Association (GSA) für Multicast-Gruppen

  Multicast-/Broadcast-Service Group Security Association (MBS-GSA), für den Multicast-/Broadcast-Service

Für die beiden unterschiedlichen Authentisierungsverfahren gibt es bei WiMAX Mobile ein eigenes Schlüsselmaterial aus dem der Authorization Key (AK) jeweils abgeleitet werden kann:

- Pre-Primary Authorization Key (Pre-PAK)

  Der Pre-PAK wird bei der RSA-Authentisierung über Zertifikate an die Mobile Station übermittelt (verschlüsselt mit dem Public Key der Mobile Station). Aus dem Pre-PAK wird dann der Primary Authorization Key abgeleitet.
- Primary Authorization Key (PAK)

  Der PAK wird aus dem Pre-PAK abgeleitet und dient seinerseits zur Ableitung des Authorization Keys.
- Master Session Key (MSK)

  Der MSK wird bei der Authentisierung über EAP generiert. Aus ihm wird der Pairwise Master Key abgeleitet.
- Pairwise Master Key (PMK)

  Der PMK wird aus dem MSK abgeleitet und dient seinerseits zur Ableitung des Authorization Keys.
- Authorization Key (AK)

  Der AK wird vom PAK oder PMK abgeleitet und hat dieselbe Funktion wie bei WiMAX Fixed (siehe Kapitel 2.1.1)

Für die weiteren SAs, die in WiMAX Mobile spezifiziert sind, gibt es folgende Schlüssel:

- Group Key Encryption Key (GKEK)

  Der GKEK wird zufällig von der Base Station generiert und der Mobile Station mit dem KEK verschlüsselt übermittelt. Der GKEK dient zur Verschlüsselung der Group Traffic Encryption Keys bei der Übermittlung von der Base Station zu den Mobile Stations.
- Group Traffic Encryption Key (GTEK)

  Der GTEK für Multicast-Verkehr entspricht dem TEK für Unicast-Verkehr.
- MBS Traffic Key (MTK)

  Der MTK wird aus einem im WiMAX-Mobile-Standard nicht spezifizierten MBS Authorization Key (MAK) abgeleitet. Generierung und Übermittlung dieses MAK muss auf höheren Schichten geschehen. Mit dem MTK wird der MBS-Verkehr verschlüsselt.

Die übrigen in Kapitel 2.1.1 beschriebenen Schlüssel (TEK, KEK und Message Authentication Keys) werden genau so auch in WiMAX Mobile genutzt. Abb. D-9 zeigt den Aufbau einer SA und die Verwendung der verschiedenen Schlüsseltypen.

---

[15] EAP ist ein Authentisierungs-Framework, d.h. EAP spezifiziert eine generische Schnittstelle die von verschiedensten Authentisierungsmethoden (so genannte EAP-Methoden) genutzt werden kann. Eine Beschreibung einiger besonders wichtiger Authentisierungsmethoden kann dem WLAN-Kapitel dieses Dokuments entnommen werden.

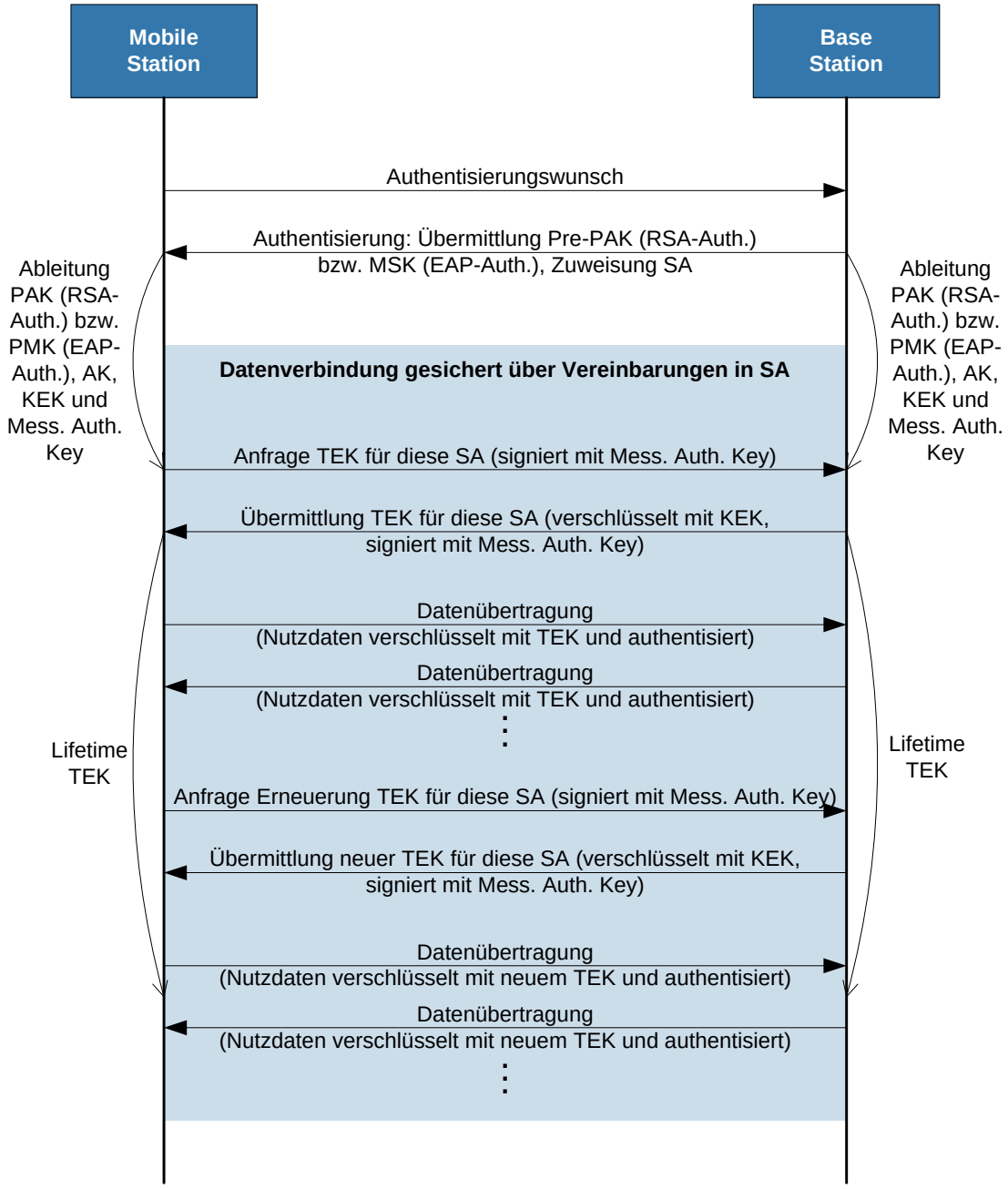


Abb. D-9: Verwendung von Schlüsseln in WiMAX Mobile

2.2.2 Key Management Protocol bei WiMAX Mobile

Wie schon erwähnt, gibt es bei WiMAX Mobile zwei Versionen des Privacy Key Management Protokolls: das mit PKM bei Fixed WiMAX vergleichbare PKMv1 und PKMv2 mit erweiterten Funktionen wie z.B. einer neuen Schlüsselhierarchie, AES-CMAC, AES Key Wrap und Multicast-/Broadcast-Service (siehe auch Kapitel 2.2.1).

Die Authentisierung ist bei WiMAX Mobile über zwei verschiedene Methoden möglich:

- RSA-Authentisierung über X.509-Zertifikate wie bei WiMAX Fixed

  Die RSA-Authentisierung läuft wie bei WiMAX Fixed ab (siehe Kapitel 2.1.2). Allerdings ist in PKMv2 auch eine beidseitige Authentisierung möglich, in dem die Base Station in ihrer Authorization Replay ihr Zertifikat an die Mobile Station sendet (siehe Abb. D-10).

Die RSA-Authentisierung muss in PKMv1 unterstützt werden (nur einseitige Authentisierung möglich) und ist in PKMv2 optional.

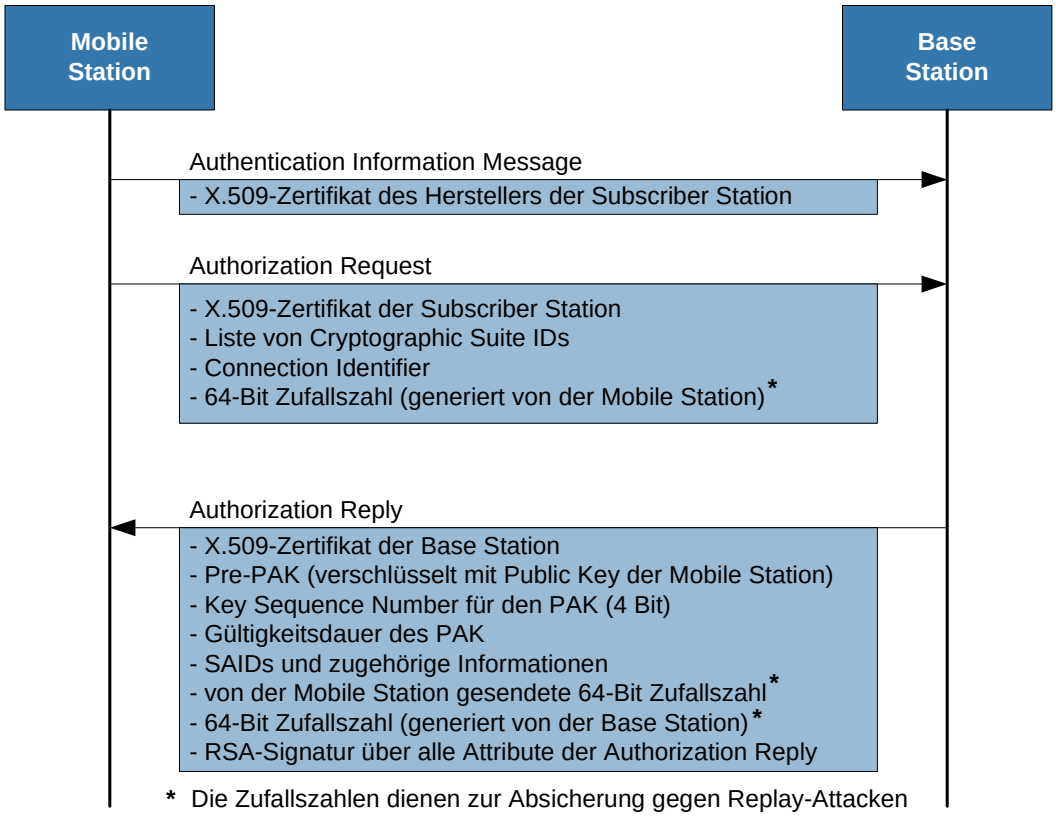


Abb. D-10: Beidseitige Authentisierung in WiMAX Mobile mit PKMv2

► Authentisierung über das Extensible Authentication Protocol (EAP) [IETF RFC 3748]

Bei der Authentisierung über EAP kann die EAP-Methode vom WiMAX-Netzbetreiber frei gewählt werden. Der genaue Vorgang der Authentisierung und die EAP-Methode werden im WiMAX-Mobile-Standard nicht spezifiziert, die EAP-Methode sollte aber die Pflichtkriterien des RFC 4017 Abschnitt 2.2 erfüllen:

- Generierung von symmetrischem Schlüsselmaterial
- Generierung von 128 Bit langen Schlüsseln, Generierung eines Master Session Keys (MSK) und eines Extended Master Session Keys (EMSK), beide mindestens 64 Bytes lang
- Unterstützung einer beidseitigen Authentisierung
- Widerstandsfähigkeit gegen Dictionary-Attacken
- Schutz gegen Man-in-the-Middle-Attacken
- Gesicherte Verhandlung von Folgeschlüsseln

Die EAP-Authentisierung ist in beiden PKM-Versionen optional.

Im WiMAX-Mobile-Standard ist eine Pre-Authentication möglich, um ein schnelleres Handover von einer Base Station zu einer benachbarten Base Station zu ermöglichen. Diese Pre-Authentication wird im WiMAX-Mobile-Standard allerdings nicht genauer spezifiziert.

2.2.3 Encapsulation Protocol bei WiMAX Mobile

Die Aufgabe des Encapsulation-Protokolls ist die gleiche wie bei WiMAX Fixed. Allerdings sind bei WiMAX Mobile weitere Verschlüsselungsmethoden erlaubt und auch eine Datenauthentisierung ist möglich. Eine Liste der zugelassenen Cryptographic Suites findet sich in Tab. D–2.

Für die Datenverschlüsselung sind die folgenden Verschlüsselungsalgorithmen zugelassen:

- Keine Verschlüsselung
- DES im CBC-Modus mit 56-Bit-Schlüssel
- AES im CCM-Modus mit 128-Bit-Schlüssel
- AES im CBC-Modus mit 128-Bit-Schlüssel
- AES im CTR-Modus mit 128-Bit-Schlüssel für Multicast-/Broadcast Services mit 8 Bit Rollover Counter

Auch hier wird grundsätzlich nur das MAC PDU Payload verschlüsselt. Der Generic MAC Header und die optionale CRC werden nicht verschlüsselt. Außerdem müssen alle MAC Management-Nachrichten unverschlüsselt übertragen werden.

Die Datenauthentisierung ist über AES im CCM-Modus mit 128-Bit-Schlüssel möglich.

Der Traffic Encryption Key / Group Traffic Encryption Key / MBS Traffic Encryption Key kann bei seiner Übermittlung an die Mobile Station mit den folgenden Verschlüsselungsalgorithmen verschlüsselt werden:

- 3-DES im EDE-Modus mit 128-Bit-Schlüssel
- RSA mit 1024-Bit-Schlüssel
- AES im ECB-Modus mit 128-Bit-Schlüssel
- AES Key Wrap mit 128-Bit-Schlüssel

Cryptographic Suite ID	Beschreibung		
	Datenverschlüsselung	Daten-authentisierung	TEK-Verschlüsselung
0x000001	keine	keine	3DES im EDE-Modus mit 128-Bit-Schlüssel
0x010001	DES im CBC-Modus mit 56-Bit-Schlüssel	keine	3DES im EDE-Modus mit 128-Bit-Schlüssel
0x000002	keine	keine	RSA mit 1024-Bit-Schlüssel
0x010002	DES im CBC-Modus mit 56-Bit-Schlüssel	keine	RSA mit 1024-Bit-Schlüssel
0x020103	AES im CCM-Modus mit 128-Bit-Schlüssel	AES im CCM-Modus mit 128-Bit-Schlüssel	AES im ECB-Modus mit 128-Bit-Schlüssel
0x020104	AES im CCM-Modus mit 128-Bit-Schlüssel	AES im CCM-Modus mit 128-Bit-Schlüssel	AES Key Wrap mit 128-Bit-Schlüssel
0x030003	AES im CBC-Modus mit 128-Bit-Schlüssel	keine	AES im ECB-Modus mit 128-Bit-Schlüssel
0x800003	AES im CTR-Modus mit 128-Bit-Schlüssel für Multicast-/ Broadcast Services mit 8 Bit Rollover Counter	keine	AES im ECB-Modus mit 128-Bit-Schlüssel
0x800004	AES im CTR-Modus mit 128-Bit-Schlüssel für Multicast-/ Broadcast Services mit 8 Bit Rollover Counter	keine	AES Key Wrap mit 128-Bit-Schlüssel
alle anderen Werte	reserviert		

Tab. D–2: Cryptographic Suites für WiMAX Mobile

3. Gefährdungen

Dieses Kapitel beschreibt typische Gefährdungen, denen ein WiMAX-basiertes Netz ausgesetzt sein kann. Eine detaillierte Analyse der Bedrohungen findet sich in [Barb05]. Da bisher nur eine punktuelle Versorgung durch WiMAX-Netze realisiert wurde und oft noch ein Testbetrieb erfolgt, gibt es nur wenig praktische Erfahrungen mit diesen Systemen.

3.1 Ausfall durch höhere Gewalt

Wie im kabelgebundenen LAN kann es auch in WiMAX-basierten Netzen durch Überspannungen zum Ausfall von Komponenten kommen. Außerdem sind Außeninstallationen (z.B. Antennen) durch Blitz und Witterungseinflüsse gefährdet.

3.2 Sicherheitskritische Einstellung

Der WiMAX-Standard bietet die Möglichkeit auf eine Verschlüsselung der Datenkommunikation zu verzichten bzw. nicht ausreichend sichere Verfahren (DES mit 56-Bit-Schlüssellänge) zu wählen. Für WiMAX Mobile muss zusätzlich berücksichtigt werden, dass EAP-Methoden frei gewählt werden können und speziell passwortbasierte Methoden durch Wörterbuchattacken angreifbar sind, was bei der Verwendung von schwachen Passworten eine Gefährdung darstellt.

3.3 Keine Datenauthentisierung bei WiMAX Fixed

Im WiMAX-Fixed-Standard ist keine Datenauthentisierung im Sinne einer kryptographischen Integritätsprüfung vorgesehen. Es kann also nicht unmittelbar festgestellt werden, ob die übermittelten Daten zwischen Sender und Empfänger manipuliert wurden.

3.4 Zum Teil nur einseitige Authentisierung

Sowohl bei WiMAX Fixed als auch bei der RSA-Authentisierung von WiMAX Mobile, wenn PKMv1 genutzt wird, wird nur eine einseitige Authentisierung durchgeführt. Dies bedeutet, dass sich zwar die Subscriber Station gegenüber der Base Station authentisieren muss, aber keine Authentisierung der Base Station gegenüber der Subscriber Station stattfindet.

Die Subscriber Station hat also keine Möglichkeit die Authentizität der Base Station zu überprüfen und kann somit eine falsche Base Station nicht erkennen. Dadurch ist prinzipiell ein Man-in-the-Middle-Angriff möglich. Die falsche Base Station übernimmt die Rolle einer richtigen Base Station und kann dann sämtlichen über sie laufenden Datenverkehr abgreifen. Wenn sie den Datenverkehr als Man in the Middle gleichzeitig auch an den Adressaten weiterleitet, können die Subscriber Stations den Angriff nicht bemerken. Da die Base Station auch die Schlüssel für die Datenverschlüsselung an die Subscriber Stations übermittelt, ist sie auch noch in der Lage, den abgegriffenen Datenverkehr zu entschlüsseln.

3.5 Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen der WiMAX-Komponenten breiten sich auch über räumliche Grenzen des WiMAX - Nutzungsbereichs aus. Dabei kann auch in nicht vom WiMAX-Betreiber kontrollierten Bereichen ein Empfang möglich sein. Je nach Umgebungsbedingungen und Leistungsfähigkeit der verwendeten Empfangsgeräte (z.B. Richtantennen) besteht auch hier noch eine konkrete Abhörgefahr.

3.6 Klartextübertragung von Management-Nachrichten

Sowohl bei WiMAX Fixed als auch bei WiMAX Mobile werden sämtliche Management-Nachrichten unverschlüsselt übertragen. Dadurch können Management-Nachrichten sehr leicht abgehört werden. Aus den abgefangenen Management-Nachrichten kann ein Angreifer Informationen über den Aufbau des Netzes erhalten.

3.7 Replay-Attacken

In WiMAX Fixed werden die Management-Nachrichten zwar authentisiert (Hashed Message Authentication Code, HMAC), diese Authentisierung gewährleistet aber keinen Schutz gegen so genannte Replay-Attacken. Hierbei werden die Management-Nachrichten abgefangen und zu einem späteren Zeitpunkt wieder an den Empfänger gesendet. Dies wird auch oft im Zusammenhang mit Man-in-the-Middle-Attacken benutzt.

Bei WiMAX Mobile kann auch eine andere Methode zur Authentisierunge der Management-Nachrichen genutzt werden (One-key Message Authentication Code, OMAC), die auf AES basiert und vor Replay-Attacken schützt.

Eine weitere Möglichkeit für Replay-Attacken wird durch die nur zwei Bit lange Key Sequence Number des TEK geboten. Hierdurch können abgefangene TEK-Übermittlungsnachrichten regelmäßig wieder eingespielt werden und der TEK wechselt immer zwischen den gleichen vier Werten, was einem Angreifer eine größere Möglichkeit zur Entschlüsselung des Datenverkehrs bietet.

3.8 Bedrohung der Verfügbarkeit

WiMAX-Netze übertragen Informationen mittels elektromagnetischer Funkwellen. Strahlen andere elektromagnetische Quellen im gleichen Frequenzspektrum Energie ab, können diese die WiMAX-Kommunikation stören und im Extremfall den Betrieb des WiMAX-Netzes verhindern. Dies kann unbeabsichtigt durch andere technische Systeme oder aber durch absichtliches Betreiben einer Störquelle (Jammer) als so genannter Denial-Of-Service-Angriff (DoS-Angriff) erfolgen. Eine solche Störquelle kann sich bei ausreichender Sendeleistung auch außerhalb des Bereiches befinden, in dem das WiMAX-Netz genutzt wird.

Weiterhin erfolgt in WiMAX die Übertragung von Management-Nachrichten unverschlüsselt. Dies kann grundsätzlich, wie es bei WLAN bereits der Fall ist, für DoS-Angriffe ausgenutzt werden.

3.9 Erstellung von Bewegungsprofilen

Mit WiMAX Mobile können sich Anwender frei bewegen. Da jedes WiMAX-Gerät eine eindeutige MAC-Adresse besitzt, kann so ein Bezug zwischen MAC-Adresse, Ort und Uhrzeit der Datenübertragung hergestellt werden. Auf diese Weise können Bewegungsprofile über mobile Nutzer in einem WiMAX-Netz erstellt werden.

4. Schutzmaßnahmen

4.1 Absicherung der Datenkommunikation

WiMAX-Netze sollten grundsätzlich mit Verschlüsselung betrieben werden. Die Geräte sollten immer die höchstmögliche Verschlüsselungsmethode nutzen. Für WiMAX Fixed ist für die Datenverschlüsselung beispielsweise die Verwendung von AES im CCM-Modus mit 128-Bit-Schlüssel zu empfehlen.

Wird WiMAX als Ersatz für DSL auf der letzten Meile im Rahmen eines RAS-Szenarios[16] eingesetzt, gelten für den Nutzer die entsprechenden GSHB-Empfehlungen (GSHB-Baustein B 4.4: Remote Access). Wird WiMAX als Backbone-Technik bzw. zur LAN-Kopplung eingesetzt und werden Daten mit einem mittleren oder sogar hohen Schutzbedarf übertragen, sollte seitens des Nutzers des WiMAX-Netzes zusätzlich eine VPN-Lösung mit adäquater Verschlüsselung und Authentisierung vorgesehen werden.

Weitere Schutzmaßnahmen gelten für den Anschluss eines Endgeräts an eine Subscriber Station. Dies beinhaltet insbesondere die geeignete Trennung des lokalen Systems von dem Funknetz durch den Einsatz von Firewall-Techniken und den Einsatz eines Virenschutzes für die lokal angeschlossenen Systeme.

Es gibt Subscriber Stations, die für den Anschluss von Endgeräten einen integrierten WLAN Access Point haben. Die Gefährdungslage und der empfohlene Maßnahmenkatalog entsprechen hier den Ausführungen in dem WLAN-Kapitel dieses Dokuments. Analoges gilt für Bluetooth.

4.2 Absicherung der Netzelemente

Netzelemente eines WiMAX-Systems sind geeignet zu härten, damit ein erfolgreicher Angriff über die Luftschnittstelle möglichst unwahrscheinlich ist. Dies gilt insbesondere für die Konfiguration der Subscriber Stations, denn wenn WiMAX den Massenmarkt erreicht, besteht gerade hier die Gefahr, dass Voreinstellungen unsicher sind, bzw. der Nutzer Fehleinstellungen vornehmen kann (z.B. die Abschaltung der Verschlüsselung).

4.3 Absicherung der Clients bei WiMAX-Mobile

Bei mobilen Clients, die sich direkt in ein WiMAX-Mobile-Netz einbuchen, sollten weitere lokale Schutzmaßnahmen implementiert werden, wie z.B.: Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, restriktive Browser-Konfiguration, lokale Verschlüsselung etc. (siehe [GSHB]).

4.4 Rest-Risiko

Unabhängig von den beschriebenen Sicherheitsmaßnahmen sind mit der Verwendung von WiMAX-Systemen immer folgende Rest-Risiken verbunden:

- Das Erstellen von Bewegungsprofilen mobiler Geräte (siehe Kapitel 3.9) kann nicht verhindert werden.
- Die Bedrohung der Verfügbarkeit (siehe Kapitel 3.8) ist ebenfalls nicht vermeidbar.

---

16 RAS = Remote Access Service

5. Ausblick

WiMAX-Systeme sind noch in der Testphase. Erste Produkte wurden vom WiMAX-Forum zertifiziert. Diese für WiMAX Fixed gedachten Geräte könnten eine gute Alternative für die „letzte Meile“ sein. Erste Testsysteme sind bei einigen Providern im Einsatz.

WiMAX Mobile steht in starker Konkurrenz zu UMTS- und speziell HSDPA-Systemen. Wann Geräte für WiMAX Mobile verfügbar sind, ist noch nicht abzusehen. Mit einer Einführung der Technik ist nicht vor 2007 zu rechnen. Ein wichtiger Schritt ist jedoch mit der Veröffentlichung des Standards schon getan.

6. Fazit

WiMAX spezifiziert die Ebenen 1 (Physical Layer) und 2 (MAC Layer) eines drahtlosen Breitbandzugangs im MAN-Bereich. Die Sicherheitsmechanismen konzentrieren sich daher auf die reine Absicherung der Funkübertragung. Übergeordnete Aspekte wie Teilnehmerauthentisierung oder die Kriterien für die Auswahl einer Cryptographic Suite sind bewusst in den Standards ausgeklammert.

Hier ist zunächst der Netzbetreiber durch Implementierung geeigneter Mechanismen bzw. Einsatz geeigneter Produkte gefordert eine angemessen sichere Infrastruktur zu schaffen. Außerdem sollte der Nutzer, der letztendlich über WiMAX kommuniziert, im Einzelfall prüfen, ob das angebotene Sicherheitsniveau auch zum Schutzbedarf der über WiMAX transportierten (bzw. erreichbaren) Daten passt. Ist dies nicht der Fall, muss er selbst weitere Sicherheitsmechanismen umsetzen, wie z.B. den Einsatz eines VPN im Fall einer LAN-Kopplung.

7. Literatur / Links

Diese Liste stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

[Barb05] Michel Barbeau, „WiMAX/802.16 Threat Analysis“, Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, Montreal, Kanada, 2005, verfügbar unter http://www.scs.carleton.ca/~barbeau/Publications/2005/iq2-barbeau.pdf

[GSHB] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutzhandbuch – Standard-Sicherheitsmaßnahmen“, verfügbar unter http://www.bsi.bund.de/gshb

[IEEE04] IEEE Std 802.16-2004, „Part 16: Air Interface for Fixed Broadband Wireless Access Systems“, 2004.

[IEEE06] IEEE Std 802.16e, „Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems - Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands “, 2006.

[RegTP05a] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Vfg. Nr. 95/2005, „Bereitstellen von Frequenzen für Funkanwendungen im Rahmen des Broadband Wireless Access (BWA); Zuteilung von Frequenzen im Bereich 3400-3600 MHz für breitbandige drahtlose Verteilsystem“, 2005

[RegTP05b] Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Vfg. 94/2005, „Bereitstellen von Frequenzen für Funkanwendungen im Rahmen des Broadband Wireless Access (BWA); Auswertung der Kommentare zum Zuteilungsverfahren für breitbandige drahtlose Verteilsysteme im Bereich 3400-3600 MHz“, 2005

[WiMAX] WiMAX Forum, http://www.wimaxforum.org

8. Abkürzungen

3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
AK	Authorization Key
ATM	Asynchronous Transfer Mode
CBC	Cipher Block Chaining
CBC-MAC	CBC with Message Authentication Code
CCM	Counter with CBC-MAC
CID	Connection Identifier
CMAC	Cipher-based Message Authentication Code
CPS	Common Part Sublayer
CRC	Cyclic Redundancy Check
CS	Convergence Sublayer
CTR	Counter
DES	Data Encryption Standard
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
ECB	Electronic Code Book
EDE	Encrypt-Decrypt-Encrypt
EMSK	Extended Master Session Key
ETSI	European Telecommunications Standards Institute
GKEK	Group Key Encryption Key
GSA	Group Security Association
GSM	Global System for Mobile Communications
GTEK	Group Traffic Encryption Key
HIPERMAN	High Performance Radio Metropolitan Area Network
HMAC	Hashed Message Authentication Code
HSDPA	High Speed Downlink Packet Access
HUMAN	High-speed Unlicensed MAN
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
KEK	Key Encryption Key
LAN	Local Area Network
LOS	Line-of-Sight
MAC	Medium Access Control
MAK	MBS Authorization Key
MAN	Metropolitan Area Network
MBS	Multicast-/Broadcast-Service
MSK	Master Session Key
MTK	MBS Traffic Key
NLOS	Non-Line-of-Sight
OFDM	Orthogonal Frequency Division Multiplexing

OMAC	One-key Message Authentication Code
PAK	Primary Authorization Key
PDU	Protocol Data Unit
PKM	Privacy Key Management
PMK	Pairwise Master Key
PMP	Point-to-Multipoint
PPP	Point to Point Protocol
QoS	Quality of Service
RAS	Remote Access Service
RFC	Request for Comments
RSA	Rivest, Shamir und Adleman
SA	Security Association
SAID	SA Identifier
SAP	Service Access Point
SC	Single Carrier
SFID	Service Flow Identifier
TEK	Traffic Encryption Key
UMTS	Universal Mobile Telecommunications System
VPN	Virtual Private Network
WiMAX	Worldwide Interoperability for Microwave Access
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN
WLL	Wireless Local Loop

9. Glossar

3DES
: Siehe Triple DES

Advanced Encryption Standard (AES)
: Symmetrisches Verschlüsselungsverfahren mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit. AES bietet ein sehr hohes Maß an Sicherheit. Das Verfahren wurde eingehenden kryptoanalytischen Prüfungen unterzogen.

Authentisierung
: Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Gerätes. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist i. A. keine sinnvolle Autorisierung möglich.

Cipher Block Chaining Mode (CBC)
: Betriebsart, in der Blockchiffrierungsalgorithmen arbeiten; vor dem Verschlüsseln eines Klartextblocks wird dieser erst mit dem im letzten Schritt erzeugten Geheimtextblock per XOR (exklusives Oder) verknüpft

Counter with CBC-MAC (CCM)
: CBC-MAC = Cipher Block Chaining with Message Authentication Code; CCM ist eine generische Methode für die Verschlüsselung und Authentisierung von Daten, die für die Verwendung einer 128-Bit-Blockchiffrierung (z.B. AES) spezifiziert ist.

Cyclic Redundancy Check (CRC)
: Prüfsumme über die zu übertragenden Daten, die in der Nachricht mitgeschickt wird und es dem Empfänger gestattet, Bitfehler, die auf dem Kommunikationskanal entstanden sind, zu erkennen

Data Encryption Standard (DES)
: Weit verbreiteter symmetrischer Verschlüsselungsalgorithmus; wird aufgrund der verwendeten Schlüssellänge von nur 56 Bit für viele Anwendungen als nicht ausreichend sicher erachtet. Die effektive Schlüssellänge kann durch Mehrfachanwendung des DES (siehe Triple DES, kurz 3DES) vergrößert werden.

Denial of Service (DoS)
: Ein Angriff vom Typ Denial of Service hat zum Ziel, die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr („Dummy Traffic“) oder die beabsichtigte Herbeiführung eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Dictionary-Attacke
: Eine Wörterbuch-Attacke (auch als Dictionary-Attacke bezeichnet) wird typischerweise zum Raten eines Passworts oder Schlüssels eingesetzt. Bei schwachen Passwörtern geringer Komplexität kann das Verfahren schnell zum Erfolg führen.

Electronic Code Book Mode (ECB)
: Betriebsart, in der Blockchiffrierungsalgorithmen arbeiten; einfachster und zugleich unsicherster Modus, denn dabei werden die Klartextblöcke nacheinander und unabhängig voneinander in den Geheimtextblock überführt

Extensible Authentication Protocol (EAP)
: Rahmen (Framework) für die Verwendung von Authentisierungsmethoden. Es wird u.a. für PPP oder auch in Verbindung mit EAPOL unter IEEE 802.1X verwendet.

Fresnel Zone
: Siehe LOS

Handover
: Wechsel von einem (physikalischen) Kommunikationskanal auf einen anderen unter Aufrechterhaltung der Ende-zu-Ende-Kommunikationsbeziehung.

LOS
: LOS ist eine Abkürzung für Line-of-Sight. Sichtverbindung bedeutet hier stets eine funktechnische (nicht optische) Sichtverbindung. Dabei muss ein spezielles Ellipsoid mit einer gewissen Ausdehnung zwischen Sender und Empfänger weitestgehend frei von Hindernissen sein. Dies ist die sogenannte Fresnel-Zone.

Man in the Middle
: Der Angreifer positioniert sich zwischen zwei Kommunikationspartner und täuscht beiden Parteien vor, der jeweils erwartete eigentliche Partner zu sein. Dabei kann der Man in the Middle den Dialog zwischen den beiden Parteien belauschen oder auch verfälschen. Ziel ist oft die Ermittlung von Passwörtern.

RSA
: RSA ist ein populärer Publik-Key-Algorithmus, der nach seinen Erfindern R. Rivest, A. Shamir und L. Adleman benannt ist.

Triple DES (3DES)
: Bei 3DES werden drei DES-Chriffrierer hintereinander geschaltet, wobei der mittlere DES-Chriffrierer invers eingebaut ist (Encrypt-Decrypt-Encrypt, kurz: EDE).

WiMAX Forum
: Vereinigung von Herstellern von WiMAX-Komponenten nach IEEE 802.16

Zertifikat
: Von einer Certificate Authority beglaubigter öffentlicher Schlüssel, der einer Person oder einem Objekt zugeordnet ist

E. Richtfunktechniken

Inhaltsverzeichnis des Abschnitts

1. Grundlagen und Funktionalität

Die Planer von modernen Kommunikationsanlagen mit lokal begrenzten Reichweiten, wie sie in einem Local Area Network (LAN) oder einem Metropolitan Area Network (MAN) vorzufinden sind, stehen bei der Planung eines gebäudeübergreifenden Primärnetzes immer wieder vor dem gleichen Hauptproblem: Wie kann zwischen zwei Gebäuden eine hohe Datenrate mit möglichst geringem Verkabelungsaufwand realisiert werden? Entspricht die Verkabelung nicht den Anforderungen bzw. sind die Betriebskosten von angemieteten Leitungen zu hoch, gibt es die Alternativen Neuverkabelung, Freiraumübertragung oder Nutzung des Internets mit Hilfe von VPN. Immer häufiger wird auch bei hochperformanten Verbindungen aus Kostengründen die Freiraumübertragung gewählt.

Bei der Freiraumübertragung wird unterschieden in

- Richtfunk in nicht genehmigungspflichtigen Frequenzbereichen (WLAN nach IEEE 802.11),
- genehmigungspflichtigen Richtfunk und
- anmeldepflichtigen optischen Richtfunk (Free Space Optics, FSO).

Streng genommen stellt die FSO-Übertragung eine Infrarot-Technik dar und ist damit im eigentlichen Sinne keine „Funktechnik". Da der allgemeine Sprachgebrauch jedoch auch den Begriff „Optischen Richtfunk" vorsieht, wird nachfolgend als Oberbegriff für die drei oben genannten Techniken der Begriff „Richtfunk" verwendet.

Alle betrachteten funkbasierenden Techniken werden in der klassischen Hochfrequenztechnik als „mikrowellenbasierend" bezeichnet, da sie in einem Frequenzbereich mit sehr kurzen Wellenlängen arbeiten. Da jedoch mit dem Begriff Mikrowellen-Richtfunk im Allgemeinen die Verwendung einer Übertragungstechnik mit Trägerfrequenzen oberhalb von 6 GHz assoziiert wird, ist auch im Folgenden mit diesem Begriff nur der genehmigungspflichtige Richtfunk und nicht WLANs nach IEEE 802.11 gemeint.

Richtfunksysteme mit WLAN-Technik nach IEEE 802.11 liefern in den meisten Fällen eine Ethernet-Schnittstelle (gemäß IEEE 802.3) zum Anschluss an das leitungsgebundene Netz. Weitergehende Informationen zur Verwendung von WLAN als Richtfunktechnik sind im Kapitel „Wireless LAN, IEEE 802.11" in diesem Dokument unter dem Stichwort LAN-Kopplung aufgeführt. Die Schnittstellen von Mikrowellen-Richtfunksystemen zum leitungsgebundenen Netz dagegen sind meistens anwendungsneutral, sie erlauben beispielsweise sowohl Übertragungen von Ethernet-Paketen als auch S_{2M}-Anwendungen. Derartige transparente Systeme bieten den Vorteil, dass an die Schnittstelle zum leitungsgebundenen Netz jede Übertragungstechnik angeschlossen werden kann. Das Richtfunk-System erkennt jeden beliebigen Bitstrom und überträgt ihn in den Freiraum. Damit besteht die Möglichkeit, die Schnittstelle zum leitungsgebundenen Netz für unterschiedlichste Übertragungsverfahren zu nutzen; bei Wechsel der leitungsgebundenen Übertragungstechnik muss das Mikrowellen-Richtfunksystem nicht ausgetauscht werden.

1.1 Mikrowellen-Richtfunksysteme

Abhängig von der zu überbrückenden Entfernung stehen bei Mikrowellen-Richtfunksystemen Außeneinheiten in verschiedenen genehmigungspflichtigen Frequenzbändern zur Verfügung. Die in Deutschland genutzten Trägerfrequenzen liegen bei 6, 7, 13, 15, 23, 26, 28, 32 und 38 GHz. Diese Frequenzen sind teilweise noch in weitere Frequenzbereiche unterteilt, die jeweils einen oder mehrere Kanäle der Richtfunkstrecke bilden. Die Übertragungsfrequenz bestimmt zusammen mit dem Antennendurchmesser und der Sendeleistung die maximal zu überbrückende Distanz; Reichweiten von mehr als 50 km mit einer Datenrate von bis zu 600 MBit/s sind nutzbar. Die Systeme arbeiten in von der Bundesnetzagentur koordinierten Frequenzbändern und weisen folgende Vorteile gegenüber den Frequenzbändern von WLAN-Systemen auf:

- ► Exklusive Zuweisung der Betriebsfrequenz an nur einen Nutzer
- ► Koordinierter Betrieb der Richtfunksysteme, dadurch keine Störungen durch andere Nutzer im selben Frequenzband

Die meisten Mikrowellen-Richtfunksysteme bestehen aus einer Innen- und einer Außeneinheit. Die Inneneinheit (Indoor Unit) enthält die Schnittstellenelektronik (z.B. Ethernet-Schnittstellen), den internen Multiplexer und die Stromversorgung für die Außeneinheit. Die Außeneinheit (Outdoor Unit) erzeugt das hochfrequente Sendesignal und gibt es an die Antenne ab. Diese wird zusammen mit der Antenne an einem Antennenträger auf dem Dach eines Gebäudes oder an einem Mast installiert. Sie enthält den Empfänger mit der zugehörigen Signalverarbeitung. Als Antennen werden Parabolantennen eingesetzt, die ein hohes Maß an Bündelung und Parallelität der Strahlen sicherstellen. Die Polarisation des Funkfeldes ist über eine Drehung der Antenne vertikal oder horizontal einstellbar. Mit Hilfe eines Koaxialkabels werden beide Einheiten miteinander verbunden; auch die Spannungsversorgung der Außeneinheit erfolgt über dieses Koaxialkabel.

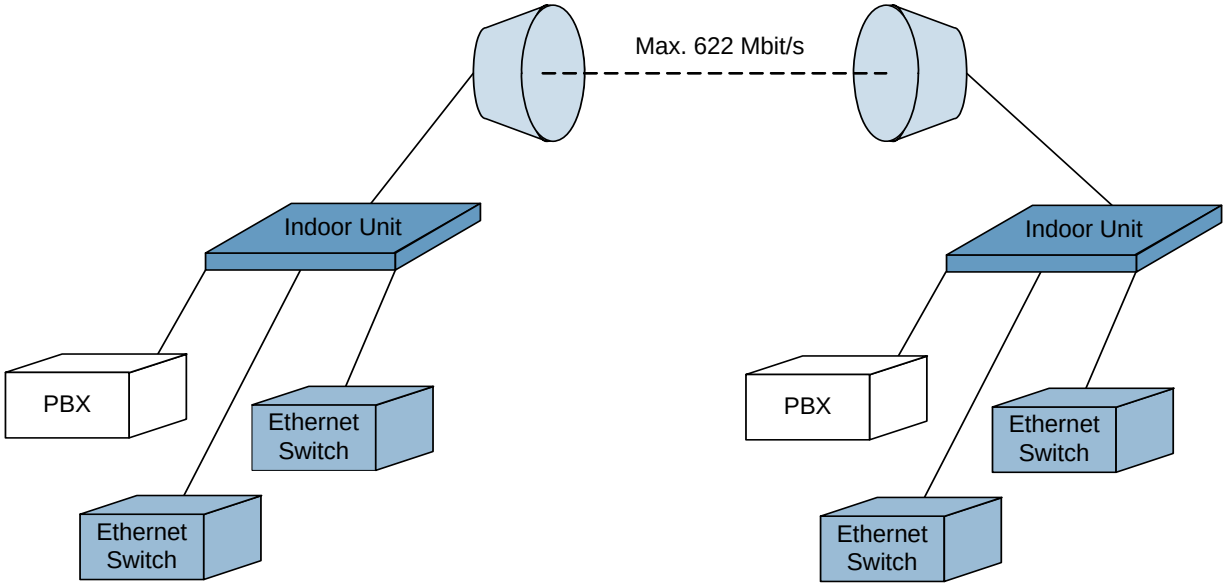


Abb. E-1: Komponenten eines Mikrowellen-Richtfunksystems

Falls zwischen den Endpunkten keine direkte Sichtverbindung besteht, lässt sich ein indirekter Weg über aktive oder passive Relaisstellen herstellen (Richtfunkrelais). Beispielsweise gibt es passive Umlenkantennen, d.h. direkt über Hohlleiter gekoppelte Antennen, die keine aktiven Elemente enthalten und demzufolge keinen Stromanschluss benötigen.

Mikrowellen-Richtfunksysteme werden grundsätzlich für Punkt-zu-Punkt-Verbindungen oder Punkt-zu-Mehrpunkt-Verbindungen verwendet. Die Punkt-zu-Punkt-Richtfunksysteme verbinden zwei Stationen über eine Richtfunkstrecke, sie werden häufig in Weitverkehrsnetzen und zur Überbrückung großer Distanzen verwendet.

Die Hersteller nutzen unterschiedliche Modulationsverfahren, so dass eine Kombination von verschiedenen Herstellern kaum möglich ist.

Die Datenübertragung in Richtfunksystemen geschieht typischerweise ausschließlich auf physikalischer Ebene, wobei die PDH-Hierarchie[1] mit Asynchron-Übertragung (kein identischer Takt) und die SDH-Hierarchie[2] mit Synchron-Übertragung arbeitet (Synchronisierung erfolgt über ein zentrales Taktsignal). Das PDH-Verfahren hat diverse Nachteile beim Multiplexen bzw. Demultiplexen, deshalb wird PDH zunehmend durch SDH abgelöst.

[1] PDH = Plesiochronous Digital Hierarchy

[2] SDH = Synchronous Digital Hierarchy

1.2 Optische Systeme

Im Unterschied zu Mikrowellen-Richtfunksystemen nutzen FSO-Systeme für die Übertragung im Freiraum Licht im infraroten Spektrum mit einer Wellenlänge zwischen 760 nm und 1550 nm. Der von einer Datenquelle wie z.B. einem Switch gelieferte Datenstrom wird mit Hilfe einer Strahlenquelle in Form einer Leuchtdiode oder Laserdiode direkt durch den Freiraum zu einer Empfangsstation gesendet. Im Empfänger befinden sich Fotodioden, welche die optischen Impulse in elektrische Impulse zurückverwandeln.

Dabei bedient man sich auf dem optischen Kanal eines einfachen binären Kodierungsverfahrens (das bedeutet tatsächlich die Verwendung eines „Licht an/Licht aus“-Schemas); der an- bzw. abgehende leitungsgebundene Kanal ist abhängig von dem verwendeten Übertragungsverfahren. Bei FSO-Systemen ist meistens nur die leitungsgebundene Schnittstelle standardisiert (z.B. 100BaseF), die Freiraumschnittstelle dagegen ist herstellerabhängig. Somit setzt der Aufbau von optischen Richtfunkstrecken derzeit immer zwei Geräte von einem Hersteller sowie aus der gleichen Produktreihe voraus.

Im Vergleich zu Mikrowellen-Richtfunksystemen zeichnen sich FSO-Systeme durch eine deutlich höhere nutzbare Datenrate aus, Systeme mit über 1 GBit/s sind auf dem Markt erhältlich. Dagegen ist die nutzbare Reichweite im Vergleich zu Funktechniken in genehmigungspflichtigen Frequenzbändern deutlich geringer: bei FSO-Technik können deutlich weniger als 5 km bereitgestellt werden (zum Vergleich: bei Mikrowellenrichtfunk 50 km und mehr).

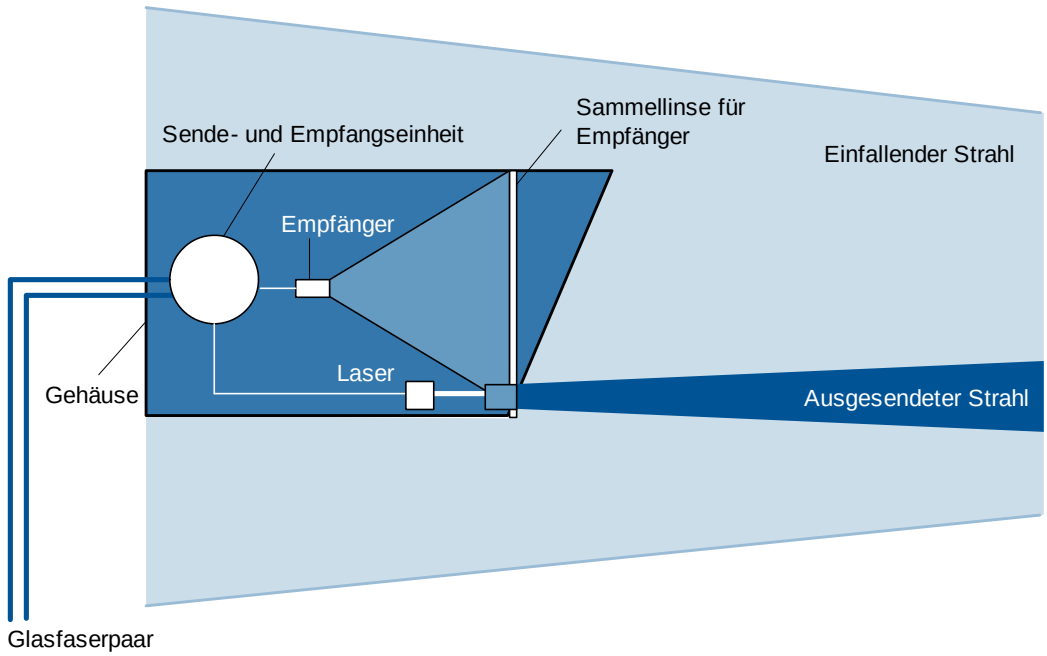


Abb. E-2: Aufbau eines optischen Richtfunksystems

Der Durchmesser eines Lichtstrahls hat die Eigenschaft, bei zunehmender Entfernung von der Lichtquelle größer zu werden, dies gilt auch für kohärentes Licht, wie es z.B. eine Laserquelle aussendet. Die übliche Aufweitung des Strahls am Sender von 2 bis 10 mrad führt z.B. bei einer Entfernung von ca. 1 km zu einer „ausgeleuchteten“ Kreisfläche von 2 bis 10 Meter Durchmesser; erhöht sich die Distanz auf z.B. 2 km, beträgt der Kreisdurchmesser 4 bis 20 Meter. Diese Strahlaufweitung (Divergenz) ist notwendig, um mögliche physikalische Schwankungen des Sendesystems, bedingt z.B. durch Windeinflüsse, auf der Empfangsseite kompensieren zu können.

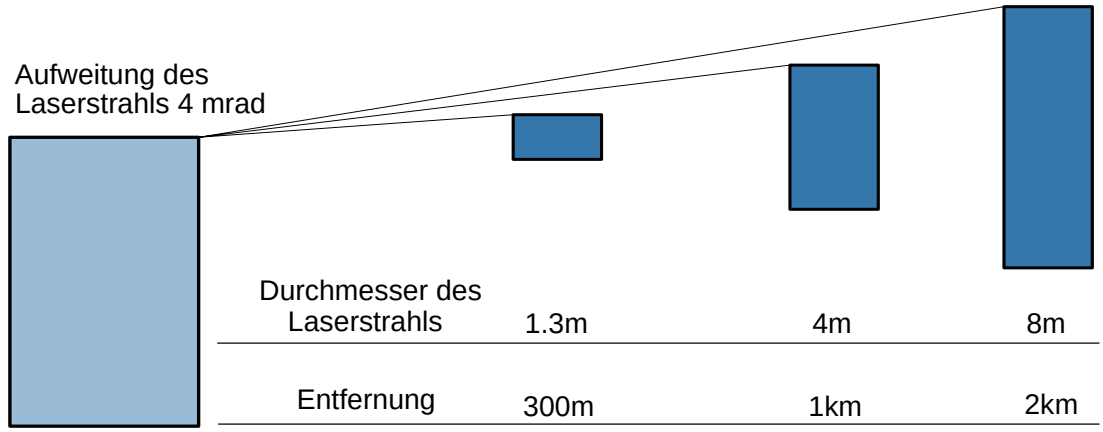


Abb. E-3: Aufweitung eines Laserstrahls

Alle Systeme überbrücken die Sichtweite auch bei Regen, Schneefall oder Dunst. Je nach Wetterlage kann es allerdings sein, dass die Bitfehlerrate ansteigt und im Extremfall die Verbindung vollkommen ausfällt. Als grober Richtwert für den Beginn eines Totalausfalls wird die Sichtweite des menschlichen Auges herangezogen: ist die Gegenstation nicht mehr zu sehen, so muss mit einer Kommunikationsunterbrechung gerechnet werden.

2. Sicherheitsmechanismen

Mikrowellen- und FSO-Richtfunksysteme haben ihre Wurzeln im Bereich der Telekommunikation auf der Ebene der physikalischen Übertragung. In diesem Sinne wird eine Richtfunkstrecke wie ein Kabel behandelt.

Daher werden von Anbietern auf Mikrowellen- oder FSO-Technik basierender Richtfunksystemen oft keine Mechanismen zur Absicherung der Kommunikation (Authentisierung, Verschlüsselung und Integritätsprüfung) eingesetzt. Wenn dennoch Sicherheitsmechanismen in den Produkten integriert sind, handelt es sich oft um proprietäre Eigenentwicklungen, deren Funktionsweise gar nicht oder nur sehr begrenzt offen gelegt wird.

Es wird bei diesen Richtfunksystemen also davon ausgegangen, dass eine höhere Protokollschicht die notwendigen Sicherheitsfunktionen implementiert.

3. Gefährdungen

3.1 Ausfall durch höhere Gewalt

Allgemein

Wie im kabelgebundenen LAN kann es auch im Richtfunk durch Überspannungen zum Ausfall von Richtfunk-Komponenten kommen.

Bei allen außen montierten Systemen ist darauf zu achten, dass Überspannungen in Folge eines direkten oder indirekten Blitzeinschlags zu einer Beschädigung der Systeme führen können. Neben der Beschädigung der Richtfunksysteme selber besteht zusätzlich die Gefahr, dass eine Überspannung ins Gebäude eintritt und dort weitere Schäden wie z.B. die Zerstörung der aktiven Netzwerkkomponenten anrichtet.

Mikrowellen-Richtfunk

Beim Mikrowellen-Richtfunk spielen Wettereinflüsse nur eine untergeordnete Rolle. Mit Ausnahme von extrem starkem Regen wird die Datenübertragung durch Wettereinflüsse nicht beeinflusst.

FSO-Systeme

Bei FSO-Systemen müssen witterungsbedingte Einflüsse von z.B. Regen, starkem Nebel oder Schneefall besonders berücksichtigt werden. Diese sind wiederum direkt abhängig von der Entfernung zwischen Sender und Empfänger.

3.2 Mangelhafte Planung

Da alle richtfunkbasierenden Systeme in einem verschalteten Netzwerk prinzipiell wie Kabelverbindungen einzustufen sind, müssen bei ring- oder maschenförmigen Topologien zusätzliche Mechanismen eingesetzt werden, um einen Loop zu verhindern. Durch Einsatz solcher Mechanismen wie z.B. Spanning Tree Protocol oder Routing Redundanzen können weitere Gefahren entstehen; zu nennen sind z.B. falsch konfigurierte Spanning Tree-Topologien, fehlerhafte Definitionen von Root Bridges etc.

3.3 Bedrohung der Verfügbarkeit

Mikrowellen-Richtfunk

Der Einsatz von Richtfunksystemen in genehmigungspflichtigen Frequenzbereichen bietet prinzipiell eine hohe Störunempfindlichkeit, da eine Nutzung der Frequenz nur nach Freigabe durch die Bundesnetzagentur möglich ist.[3]

FSO-Systeme

FSO-Systeme kommen – bezogen auf Störunempfindlichkeit – der leitungsgebundenen Übertragung am nächsten und können in vielen Fällen als Ersatz für Glasfaserverbindungen in Erwägung gezogen werden.

Kurze Unterbrechungen, beispielsweise durch Vögel, die den Strahl kreuzen, korrigiert das übergeordnete Protokoll oder bei Mehrkanalsystemen auch das FSO-System selber. Im ersten Fall werden die Daten automatisch erneut übertragen. Allerdings ist ein FSO-System sehr wetterempfindlich (siehe Kapitel 3.1).

Für FSO-Systeme besteht weiterhin für große Übertragungsstrecken ab 1000 m bei starkem Nebel die Gefahr einer Kommunikationsunterbrechung. Aus diesem Grunde bieten einige Hersteller funkbasierende Backup-Systeme, auf die automatisch umgeschaltet werden kann.

FSO-Systeme sind generell anfällig gegenüber Einflüssen durch das Wetter. Die Schwierigkeit der Einschätzung des Einflusses auf die Verfügbarkeit liegt insbesondere darin, dass die wetterabhängige Schwankungsbreite nicht verifizierbar und regional sehr unterschiedlich ist. Wer eine hohe Verfügbarkeit des Systems erreichen will oder muss, sollte mit geringeren Reichweiten kalkulieren.

Weiterhin muss der Wartungsaufwand von FSO-Systemen berücksichtigt werden, da diese Geräte zum Teil an sehr exponierten Stellen montiert werden und zur Wartung hohe Leitern oder gar Steiger notwendig sind. Dies muss in der Planung besonders berücksichtigt werden.

---

[3] Richtfunkvarianten in nicht genehmigungspflichtigen Frequenzbereichen haben den Nachteil, dass ihre Anfälligkeit gegen Störungen durch andere, im gleichen Frequenzbereich arbeitende Übertragungssysteme im Einzelfall sehr groß sein kann. Das 2,4-GHz-Band wird beispielsweise auch von privaten WLANs, Bluetooth, Bewegungsmeldern und weiteren Systemen genutzt.

3.4 Abhören

Allgemein

Eine Verschlüsselung der Luftschnittstelle ist mit Ausnahme der WLAN-Techniken bei den Richtfunktechniken weder vorgeschrieben noch standardisiert.

Mikrowellen-Richtfunk

Obwohl beim Mikrowellen-Richtfunk sehr stark bündelnde Parabolantennen eingesetzt werden, kann eine absolute Parallelität der Strahlen bedingt durch äußere Störeinflüsse nicht sichergestellt werden. Die daraus resultierende Streuung der Strahlen ermöglicht ein Belauschen der Verbindung, die keine Signalbeeinflussung zur Folge hat und demzufolge nur schwierig festgestellt werden kann. Allerdings muss der potentielle Lauscher zum Abhören neben der Sende- und Empfangsfrequenz auch die Polarisation, das Modulationsverfahren sowie Typ und Rahmenkodierung kennen.

FSO-Systeme

Generell erschweren optische Richtfunksysteme im Vergleich zu anderen funkbasierenden Systemen aus folgenden Gründen das Aufzeichnen eines Signalstroms:

- ► Der Strahlengang ist scharf gebündelt.
- ► Ein Abhören ist praktisch nur durch Unterbrechen bzw. Umlenken des Strahls möglich, dabei muss natürlich die weitere Kommunikation aufrechterhalten werden.
- ► Der Strahlenverlauf verläuft in der Regel in erheblicher Höhe über dem Erdboden.

Trotz der scharfen Bündelung des Strahls muss davon ausgegangen werden, dass sich der Strahl mit zunehmender Entfernung aufweitet. Es ist somit denkbar, dass insbesondere am Empfangspunkt ein Fremdsystem in den aufgeweiteten Strahl montiert wird und die Funkdaten ausliest, ohne dass die produktive Kommunikation unterbrochen und die Störung bemerkt wird.

FSO-Systeme mit automatischem Funk-Backup bei Wetterverschlechterung bergen das Risiko, dass für die Backup-Verbindung keine ausreichenden Maßnahmen zur Abhörsicherheit getroffen wurden. In diesem Fall ist dann ein gezieltes Aufzeichnen des Signalstromes und Mitlesen der Daten denkbar. Man kann sich ein Szenario vorstellen, bei dem z.B. durch gezielte Raucheinwirkung am Empfangsteil das sendende FSO-System zum Umschalten auf die nicht geschützte Funkstrecke gezwungen wird.

3.5 Verletzungsgefahr

Jeder Laser stellt insbesondere für das menschliche Auge eine Gefahrenquelle dar: Ist z.B. die Leistung des Lasers zu hoch, so besteht die Gefahr einer Verletzung der Netzhaut. Die unterschiedlichen Eigenschaften bezogen auf den Schutz der Augen wurden von internationalen Standardisierungsgremien durch Einführung von Laserleistungsklassen berücksichtigt (IEC 60825-1 und CDRH).

4. Schutzmaßnahmen

4.1 Sorgfältige Planung

Montage der Richtfunk-Systeme optimieren

Wichtigste Voraussetzung für den zuverlässigen Betrieb aller Systeme ist eine sichere Montage. Bereits bei der Planung des Standortes für Richtfunk-Systeme kann das Risiko einer Sabotage erheblich reduziert werden, indem – sofern möglich – die Systeme versteckt aufgestellt werden und damit nicht einfach zu entdecken sind. Beispielsweise erlauben FSO-Systeme auch eine Montage im Innenbereich hinter einem Fenster.

Außerdem sollten die Systemteile in Bereichen montiert werden, in denen ein unkontrollierter Zugang ausgeschlossen werden kann. Dies impliziert bei Einsatz von FSO-Systemen auch den Bereich des aufgeweiteten Lichtstrahls, auch hier sollte ein unautorisierter Zugang ausgeschlossen werden.

Schutz gegen Überspannungen durch Blitzeinschlag

Zum Schutz gegen Überspannungen durch Blitzeinschlag sind zwei wesentliche Maßnahmen zu treffen: Zum einen sind die Systeme durch Blitzfangstangen und weitere Maßnahmen gegen direkten Einschlag zu schützen. Zusätzlich ist durch geeignete Wahl der Datenleitungen (bevorzugt werden Lichtwellenleiter) oder Überspannungsschutzgeräte bei Kupferleitungen der Eintritt von Überspannungen ins Gebäude zu unterbinden (indirekte Blitzeinschlagwirkung). Dies gilt in gleicher Form für die Stromversorgung der Geräte.

Der kupferbasierende Datenanschluss eines außenmontierten Richtfunksystems ist nach Möglichkeit zu vermeiden, stattdessen sollten glasfaserbasierende Anschlüsse präferiert werden.

Welche Schnittstellen benötigt werden, hängt vom erwarteten Datenvolumen ab. In der Praxis gibt es inzwischen durchaus Anforderungen von 1000 MBit/s.

Untersuchung der Einsatzumgebung auf mögliche Störungen

Bei den meisten Richtfunk-Systemen benötigt man eine uneingeschränkte Sichtverbindung zwischen den beiden Standorten.

Im Falle einer Nutzung von mikrowellenbasierenden Techniken ist eine Abwesenheit von Hindernissen innerhalb der so genannten Fresnel-Zone[4] gefordert.

Planung von Backup-Mechanismen

Um bei wetterbedingten Verschlechterungen des Übertragungskanals einen alternativen Kommunikationskanal bereitzustellen, sollten Backup-Mechanismen eingeplant werden.

Bei optischen Systemen bieten sich nicht-optische, funkbasierende Backup-Lösungen an, sowohl herstellerspezifische als auch standardisierte WLAN-Lösungen. Alternativ können Backup-Lösungen durch Einsatz von terrestrischen Leitungen geschaffen werden. Hier ist möglicherweise ein geringerer Datendurchsatz zu berücksichtigen, z.B. beim Einsatz von ISDN-Leitungen.

Planung der rechtzeitigen Umschaltung auf Backup-Mechanismen

Um frühzeitig das wetterbedingte Absinken eines Signalpegels erkennen zu können und bereits vor dem Ausfall Vorbereitungen zu treffen, die z.B. eine Umschaltung auf alternative Verbindungen mög-

[4] Die Fresnel-Zone ist ein spezielles Ellipsoid mit einer gewissen Ausdehnung, der zwischen Sender und Empfänger weitestgehend frei von Hindernissen sein sollte, damit es nicht zu Verschlechterungen der Übertragungsqualität kommt.

lich machen (beispielsweise auf klassische terrestrische Leitungen), sollten die Systeme über integrierte Überwachungsfunktionen verfügen. Viele Systeme auf dem Markt bieten z.B. SNMP-Agenten an, die bei Unterschreitung eines zuvor definierten Schwellpegels einen Alarm generieren.

Die Überwachung der Systeme muss sich auf zwei Hauptaufgaben fokussieren: Kontrolle der Übertragungsqualität (z.B. Bitfehlerrate) und Kontrolle des Empfangspegels. Die ausschließliche Kontrolle der letztendlich relevanten Übertragungsqualität erlaubt dem Betreiber der Strecke ein Eingreifen erst bei beginnender Einbuße der Übertragungsqualität. Wird dagegen der Empfangspegel direkt überwacht, so kann mit entsprechender Schwellwertsetzung bereits vorher auf eine sich verändernde Wetterlage reagiert werden. Deshalb ist eine Pegelkontrolle mit automatischer Meldung bei Schwellwertunterschreitung ein absolutes Muss an Managementfunktionalität.

4.2 Überwachung der Systeme zur Erkennung von Lauschangriffen

Zur Erkennung eines Lauschangriffs auf eine Richtfunk-Verbindung kann insbesondere bei FSO-Systemen in Betracht gezogen werden, mit Hilfe einer Videokamera den Übertragungsweg permanent zu überwachen.

4.3 Zusätzliche Sicherheitsmechanismen

Die Möglichkeit einer Daten-Verschlüsselung wird durch die Systeme in der Regel nicht geboten und ein Abhören des Signalstroms kann nicht ausgeschlossen werden. Deshalb wird für alle beschriebenen Richtfunksysteme empfohlen, durch Zusatzmaßnahmen, wie beispielsweise durch die Nutzung eines VPN, für Authentisierung, Verschlüsselung und Integritätsschutz zu sorgen. Diese Verschlüsselung muss bereits im kabelbasierten Netz stattfinden, damit die Funksysteme ausschließlich verschlüsselte Informationen konvertieren und übertragen können.

4.4 Schutz vor Verletzungen

Für optische Freiraumsysteme wird in der Regel die Anforderung gestellt, Systeme zu spezifizieren, die für die Augen sicher sind und ohne zusätzliche Zugangs-Beschränkungen für nicht ausgebildetes Personal (wie z.B. Fensterputzer oder Wartungspersonal auf dem Dach) betrieben werden können. Dadurch reduzieren sich die in Frage kommenden Lasersicherheitsklassen nach IEC auf 2 Klassen:

- Klasse 1: Laser die unter normalen Umständen sicher zu benutzen sind und auch mit optischen Instrumenten zur Strahlverlaufverfolgung (Zielfernrohr, Fernglas oder Lupe) eingemessen werden können.
- Klasse 1M: Laser mit Wellenlängen von 302,5 nm bis 4000 nm, die ausreichend sicher sind, aber nicht mit optischen Instrumenten zur Strahlverfolgung ausgemessen werden können.

Dies bedeutet de-facto, dass bei beiden Typen für einen Menschen, der in einen Laserstrahl mit dem bloßen Auge hinein blickt, keine Gefahr besteht.

In Einzelfällen sind auch noch Systeme entsprechend der alten Laserklasse 3R im Einsatz. Geräte der Laserklasse 3R sind jedoch gefährlicher und sollten bei neuen Strecken nicht mehr zum Einsatz kommen.

5. Ausblick

Optische und Mikrowellen-Richtfunksysteme werden auch künftig eingesetzt werden, wenn ein Bedarf nach hohen Datenraten (100 MBit/s Full-Duplex und mehr) besteht. Da diese Richtfunksysteme rein auf der physikalischen Übertragungsebene arbeiten, sind standardisierte Sicherheitsmechanismen

zwischen den Sende- und Empfangseinheiten nicht zu erwarten. Die Hersteller von Richtfunksystemen werden auch in Zukunft eine Verschlüsselung des Datenstromes auf der leitungsgebundenen Eingangsseite der Richtfunksysteme voraussetzen, falls eine Abhörsicherheit im Freiraum gefordert wird.

6. Fazit

Die Nutzung der drahtlosen Techniken auf Basis von optischem und mikrowellenbasierendem Richtfunk stellen eine – unter Kenntnis der wetterbedingten Risiken – zuverlässige Technik zur Verbindung von Gebäuden dar. Vorteilhaft ist die Transparenz der Richtfunksysteme, welche die Nutzung durch unterschiedlichste Übertragungsverfahren gestattet. Durch die Bündelung der Funkwellen bzw. des Lichtstrahls wird das Aufzeichnen des Signalstroms im Vergleich zur WLAN-Technik zwar erschwert, kann aber dennoch nicht ausgeschlossen werden. Daher sind bei mittlerem und hohem Schutzbedarf zusätzliche Schutzmaßnahmen wie Verschlüsselung, Integritätssicherung und Authentisierung, z.B. durch VPN-Technik, notwendig. Diese Schutzmaßnahmen sind oft nicht Bestandteil des Richtfunksystems, das auf der physikalischen Ebene operiert, sondern müssen auf höheren Protokollebenen umgesetzt werden.

Die Verfügbarkeit von mikrowellenbasierenden Richtfunksystemen oder FSO-Systemen ist durch die Nutzung von genehmigungspflichtigen Frequenzbereichen bzw. der völligen Vermeidung von Funktechniken höher einzustufen als bei WLAN-basierenden Techniken. Im Vergleich der beiden vorgestellten Richtfunktechniken haben FSO-Systeme eine wesentliche Einschränkung gegenüber den mikrowellenbasierenden Technologien, denn sie sind witterungsabhängiger. Regen, Nebel oder Schneefall erhöhen die Dämpfung im Freiraum und die Reichweite der Systeme sinkt.

7. Literatur / Links

Eine genaue Beschreibung des Prinzips von Optischem Richtfunk ist z.B. in [WBG03] enthalten. Technische Details sind in der Regel herstellerspezifischen Quellen zu entnehmen.

Dokumente zu den Nutzungsbedingungen von regulierten Frequenzen können der Homepage der Bundesnetzagentur (http://www.bundesnetzagentur.de) entnommen werden.

Grundlegende Informationen zu Richtfunk finden sich bei Wikipedia (http://de.wikipedia.org/wiki/Richtfunk).

[WBG03] H. Willebrand, Baksheesh S. Ghuman, „Optischer Richtfunk“, Hüthig Verlag, 2003

8. Abkürzungen

CDRH	Center for Devices and Radiological Health
FSO	Free Space Optics
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
PDH	Plesiochronous Digital Hierarchy
SDH	Synchronous Digital Hierarchy
SNMP	Simple Network Management Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

9. Glossar

Divergenz
: Siehe Strahlaufweitung

Free Space Optics (FSO)
: Optischer Richtfunk, der für die Übertragung im Freiraum Licht im infraroten Spektrum nutzt

Indoor Unit (Inneneinheit)
: Die Indoor Unit des Mikrowellen-Richtfunksystems enthält die Schnittstellenelektronik, den internen Multiplexer und die Stromversorgung für die Außeneinheit.

Outdoor Unit (Außeneinheit)
: Die Outdoor Unit des Mikrowellen-Richtfunksystems enthält Sender und Empfänger mit der zugehörigen Signalverarbeitung. Sie wird zusammen mit der Antenne an einem Antennenträger auf dem Dach eines Gebäudes oder an einem Mast installiert.

Plesiochronous Digital Hierarchy (PDH)
: PDH ist eine international standardisierte Technik zum Multiplexen digitaler Datenströme für die Übertragung von annähernd synchronen Datenströmen (plesio = fast) auf Weitverkehrsstrecken. PDH definiert eine Hierarchie von unterstützten Bitraten (z.B. E1 mit 2 Mbit/s und E3 mit 34 Mbit/s´). Für Bitraten von mehr als 45 MBit/s verwendet man heute meist SDH.

Strahlaufweitung (Divergenz)
: Mit steigendem Abstand zwischen Sender und Empfänger eines FSO-Systems weitet sich je nach Einstellung am Sender der Strahl mehr oder weniger auf. Eine gewisse Strahlaufweitung ist notwendig, um mögliche physikalische Schwankungen des Sendesystems, bedingt z.B. durch Windeinflüsse, auf der Empfangsseite kompensieren zu können.

Synchronous Digital Hierarchy (SDH)
: SDH ist ein international standardisiertes synchrones Zeitmultiplex-Verfahren, das ähnlich zu PDH eine Multiplex-Hierarchie beinhaltet. Beispiele für die Hierarchie sind die Stufen STM-1 (155,52 MBit/s) und STM-16 (2.488,32 MBit/s). Die Daten werden transparent durch das SDH-Netz übertragen.

F. ZigBee, IEEE 802.15.4

Inhaltsverzeichnis des Abschnitts

1. Grundlagen und Funktionalität

ZigBee[1] ist ein Industriestandard für drahtlose Sensor- und Steuernetzwerke und stellt einen speziellen Typ von Wireless Personal Area Networks (WPANs) dar, zu denen Bluetooth und im weitesten Sinne auch WLAN zählen. ZigBee wird von dem im Jahr 2002 gegründeten Herstellerkonsortium ZigBee Alliance spezifiziert und basiert auf dem Standard IEEE 802.15.4, von dem die physikalische Übertragung und der Kanalzugriff übernommen wurde. ZigBee-Geräte sind für einen geringen Stromverbrauch ausgelegt, um batteriegetriebenen Endgeräten lange Laufzeiten zu ermöglichen. Hierzu operieren ZigBee und IEEE 802.15.4 (im Vergleich zu WLAN und Bluetooth) bewusst mit einer vergleichsweise geringen Datenrate. Weiterhin ist ein sehr kompakter kleiner Aufbau von ZigBee-Geräten möglich. Außerdem sollen ZigBee-Geräte zu einem niedrigen Preis hergestellt werden können.

Aktuelle Informationen zu ZigBee bietet die Internet-Seite der ZigBee Alliance (siehe [ZA04]).

Anwendungen von ZigBee liegen unter anderem in folgenden Bereichen:

- Automatisierungstechnik: z.B. Anlagensteuerung und Sensorabfrage
- Logistik: z.B. Barcode-Scanner und RFID-Lesegeräte
- Heim- und Gebäudeautomatisierung: z.B. Steuerung von Lichtschaltern, Türöffnern, Alarmierung durch Bewegungsmelder und Abfrage von Temperaturfühlern
- Medizintechnik: z.B. Steuerung, Alarmierung und Abfrage von medizinisch elektrischen Geräten
- Spielzeug: z.B. Vernetzung und Steuerung von Spielzeugelementen.

Die Kommunikation erfolgt bei ZigBee über Funk, und daher bestehen grundsätzlich die Gefahren der Abhörbarkeit, des unerlaubten Zugangs zum WPAN und der möglichen Störbarkeit von Übertragungen (beabsichtigt oder nicht). Da ZigBee zur Sensorabfrage und zu Steuerungszwecken eingesetzt werden soll, kommt der Forderung der Integrität der Daten (im Vergleich zu anderen Funknetzen) eine besonders hohe Bedeutung zu, da durchaus Szenarien denkbar sind, in denen manipulierte Steuerkommandos oder Messwerte zu einem erheblichen Schaden führen können.

1.1 Architektur

In der Architektur eines ZigBee-Systems werden die folgenden Schichten beschrieben (siehe auch Abb. F-1 und [ZA04]):

- Die physikalische Übertragung (**PHY Layer**) und der Kanalzugriff (Medienzugangssteuerung, Media Access Control Layer, kurz: **MAC Layer**) basieren auf der unter IEEE 802.15.4 beschriebenen Funkschnittstelle (siehe [IEEE03]).
- Das ZigBee **Network Layer (NWK)** dient der Bereitstellung einer Ende-zu-Ende-Kommunikation, die gegebenenfalls ein Routing über mehrere Zwischenknoten erfordern kann.
- Aufbauend auf dem Network Layer bietet das **Application Support Sub-Layer (APS)** einen Satz von allgemein verwendbaren Applikationselementen.

---

[1] Auf Englisch wird die Tanzsprache der Honigbiene, mit der Informationen über Futterquellen (wie Entfernung, Richtung und Ergiebigkeit) ausgetauscht werden, als ZigBee Principle bezeichnet, denn bei einer der beiden bekannten Tanzformen, dem so genannten Schwänzeltanz, verwendet die Biene ein zick-zack-förmiges (engl. zig-zag) Bewegungsmuster zur Informationskodierung.

Zur Namenswahl von ZigBee gibt auch die Homepage der Zigbee Alliance unter den Frequently Asked Questions (FAQ) Auskunft (siehe http://www.zigbee.org/en/about/faq.asp). Weitere Informationen zur Tanzsprache der Honigbiene findet man beispielsweise unter http://de.wikipedia.org/wiki/Tanzsprache.

- Geräte und Anwendungen werden als Objekte spezifiziert, d.h. sie werden über einen Satz von Attributen beschrieben, deren Zustand nur über die für das Objekt spezifizierte Schnittstelle geändert werden kann. **ZigBee Device Objects (ZDOs)** repräsentieren ZigBee-Geräte auf denen die eigentlichen Anwendungen laufen. Die Anwendungen werden als **Application Objects** dargestellt, die über die ZDOs kontrolliert und verwaltet werden. Das hierzu notwendige Rahmenkonzept (z.B. die Festlegung von Mechanismen zur Adressierung von Objekten) wird im ZigBee **Application Framework** bereitgestellt.

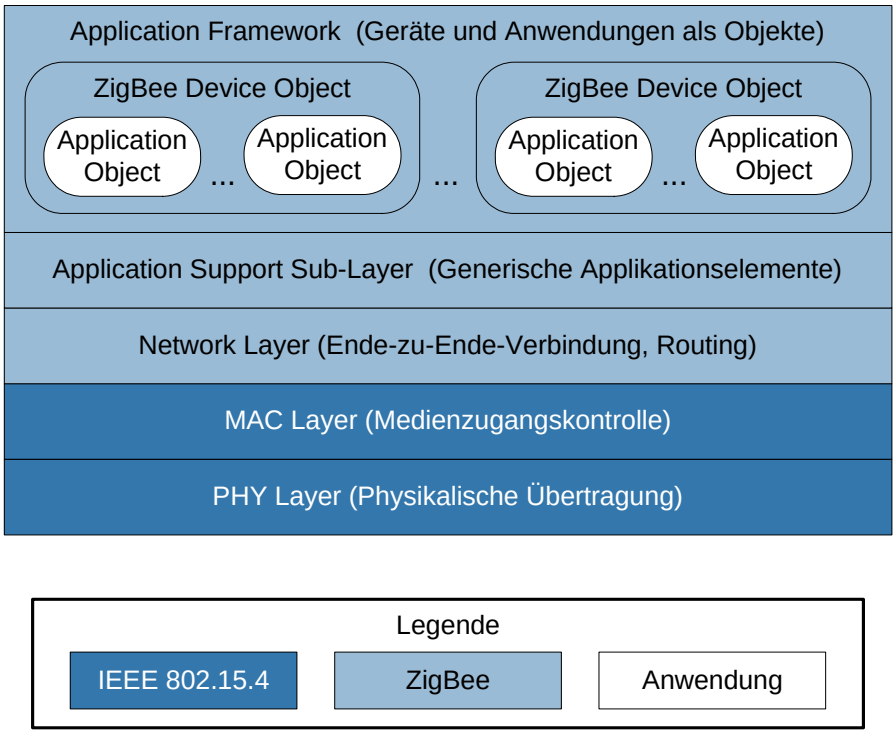


Abb. F-1: ZigBee-Architektur (vereinfacht)

1.2 IEEE 802.15.4

Für IEEE 802.15.4 werden drei Frequenzen vorgesehen (siehe auch Tab. F–1):

- Im weltweit verfügbaren ISM-Band bei 2,4 GHz können 16 Kanäle mit einem Kanalabstand von 5 MHz verwendet werden. Die Datenrate beträgt 250 kBit/s und die Modulation erfolgt mit einer Variante von QPSK (Quadrature Phase Shift Keying).
- In Europa ist im Frequenzbereich 868 MHz bis 868,6 MHz ein weiterer Kanal für IEEE 802.15.4 vorgesehen. Hier wird als Modulation BPSK (Binary Phase Shift Keying) verwendet. Die erreichbare Datenrate beträgt 20 kBit/s.
- In Amerika steht mit dem Frequenzbereich 902 MHz bis 928 MHz ein weiteres ISM-Band zur Verfügung, das 10 Kanäle für IEEE 802.15.4 bei einer Datenrate von 40 kBit/s unter Verwendung von BPSK liefert.

Frequenz	Verfügbarkeit	Datenrate	Anzahl Kanäle
2,4 – 2,4835 GHz (ISM)	weltweit	250 kBit/s	16
868 – 868,6 MHz	Europa	20 kBit/s	1
902 – 928 MHz (ISM)	Amerika	40 kBit/s	10.

Tab. F–1: Physikalische Übertragungsparameter

Um das System gegenüber schmalbandigen Störungen robust zu gestalten, werden zur Übertragung die Nutzdaten mit einer Spreizsequenz überlagert. Hierzu wird das zu übertragende Binärsignal mit einer Rate abgetastet (der so genannten Chiprate), die größer als die zugrunde liegenden Datenrate des Binärsignals ist. Dieses Signal wird mit einer anderen Bitfolge in der gegebenen Chiprate verknüpft, der so genannten Spreizsequenz. Dieses Verfahren wird als Direct-Sequence-Spread-Spectrum-Verfahren (DSSS) bezeichnet.

Der Standard IEEE 802.15.4 erwartet Sendeleistungen zwischen 0,5 mW bis 10 mW, wobei wahrscheinlich meist mit 1 mW operiert wird. Dabei kann eine Reichweite von ca.10 Metern (bei 1 mW Sendeleistung) bis ca. 70 Metern (unter idealen Bedingungen bei 10 mW Sendeleistung) erzielt werden.

IEEE 802.15.4 unterscheidet zwei Gerätetypen:

- Full Functional Device (FFD)
- Reduced Functional Device (RFD)

Eine FFD ist vereinfachend gesagt ein Gerät, das alle Betriebsfunktionen für ein WPAN implementiert hat und in diesem Sinne komplett ist, wohingegen ein RFD nur eingeschränkte Kommunikationsmittel hat. FFDs können unmittelbar miteinander kommunizieren, ein RFD kann dagegen nur mit einem FFD kommunizieren. RFDs sind für extrem einfache Applikationen gedacht, die nur geringe Datenvolumen übertragen müssen und nur bei Bedarf aktiv werden. Ein Beispiel ist ein über ZigBee gesteuerter Lichtschalter.

In einem WPAN nach IEEE 802.15.4 gibt es stets ein Gerät mit einer speziellen Rolle: den so genannten PAN Coordinator. Der PAN Coordinator ist stets ein FFD, die anderen Geräte im WPAN können FFDs oder RFDs sein. Typischerweise wird das erste aktive FFD automatisch zum PAN Coordinator. Der PAN Coordinator verwaltet die Identifikation des WPAN, koordiniert die Anmeldung weiterer Geräte (FFD oder RFD) an das WPAN und kann gewisse Parameter beim Kanalzugriff steuern.

In regelmäßigen Abständen senden Stationen, welche die Rolle eines so genannten Coordinators haben oder der PAN Coordinator selbst sind, ein spezielles Paket, das als Beacon Frame bezeichnet wird. In diesem Paket wird unter anderem die Identifikation des WPAN mitgeteilt[2]. Die Zeit zwischen zwei Beacon Frames wird in zwei Phasen eingeteilt: eine Phase, in der um den Funkkanal konkurriert wird (Contention Access Period) und eine optionale wettbewerbsfreie Phase (Contention Free Period). In der Contention Access Period erfolgt der Kanalzugriff über ein zufallsgesteuertes CSMA/CA-Verfahren[3].

---

2 Die Steuerung des Kanalzugriffs mittels Beacon Frames ist optional und kann in gewissen Situationen deaktiviert werden.

3 CSMA/CA ist die Abkürzung für Carrier Sense Multiple Access with Collision Avoidance.

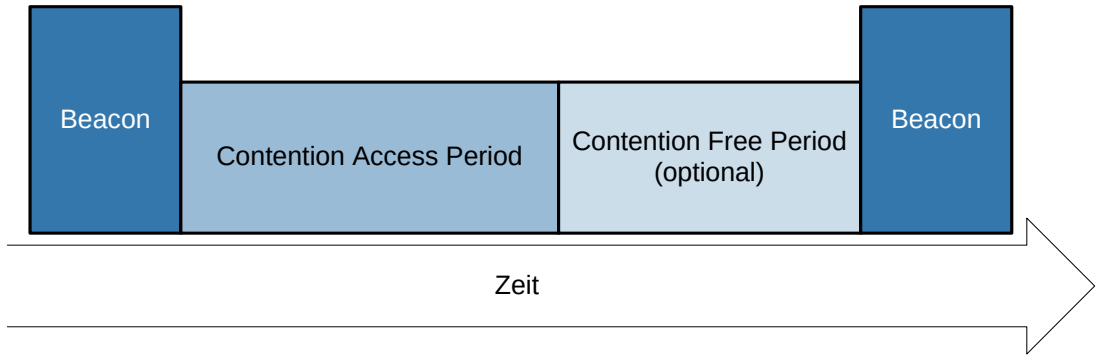


Abb. F-2: Aufteilung der Zeit für den Kanalzugriff

Eine Besonderheit des ZigBee-Kanalzugriffs ist, dass auf das Acknowledgement eines Pakets, welches von einem Gerät an den Coordinator geschickt wird, optional verzichtet werden kann. In diesem Fall erfährt ein Gerät nicht, ob ein gesendetes Paket angekommen ist oder auf dem Funkweg verloren gegangen ist, und es gibt keine Möglichkeit der Neuübertragung bei Paketverlust. Potenzielle Anwendung ist hier die periodische Übertragung von Nachrichten (z.B. Messwerten) bei denen es nichts ausmacht, wenn ein einzelnes Paket verloren geht, sofern früher oder später eine aktuelle Nachricht empfangen werden kann.

Eine weitere Besonderheit ist der richtungsabhängige Transfer von Daten, wie in Abb. F-3 gezeigt. Wenn ein Coordinator Daten zur Übertragung an ein spezielles Gerät vorliegen hat, zeigt der Coordinator dies im Beacon Frame an. Das durch die Parameter im Beacon Frame angesprochene Gerät fordert dann die Daten explizit vom Coordinator an. Auf diese Weise muss ein Gerät lediglich Beacon Frames verarbeiten und kann stromsparend alle anderen nicht für dieses Gerät bestimmte Pakete ignorieren. Weiterhin können ZigBee-Geräte in einen besonders energiesparenden Schlafzustand (Sleep Mode) versetzt werden, aus dem sie über das Netz wieder aufgeweckt werden können.

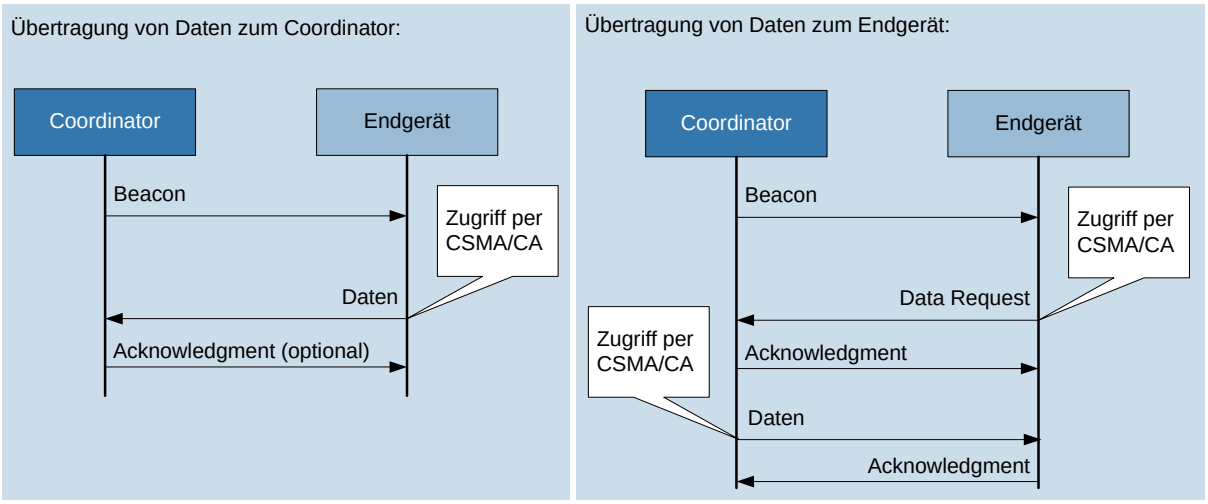


Abb. F-3: Richtungsabhängige Übertragung auf MAC Layer

1.3 Network Layer

Das ZigBee Network Layer stellt alle Grundfunktionen für ein sich selbst organisierendes Netzwerk bereit. Hierzu werden drei logische Gerätetypen (d.h. Rollen) unterschieden (siehe Abb. F-4):

- Der **ZigBee Coordinator** entspricht dem PAN Coordinator in IEEE 802.15.4 (muss daher ein FFD sein) und ergänzt diesen um Funktionen auf dem Network Layer.
- Ein FFD kann zusätzlich die Rolle eines **ZigBee Router** übernehmen, der Pakete zwischen ZigBee-Knoten vermittelt. Der logische Gerätetyp ZigBee Router entspricht dem Coordinator in IEEE 802.15.4.
- Ein **ZigBee End Device** ist ein reines Endgerät und kann sowohl FFD als auch RFD sein.

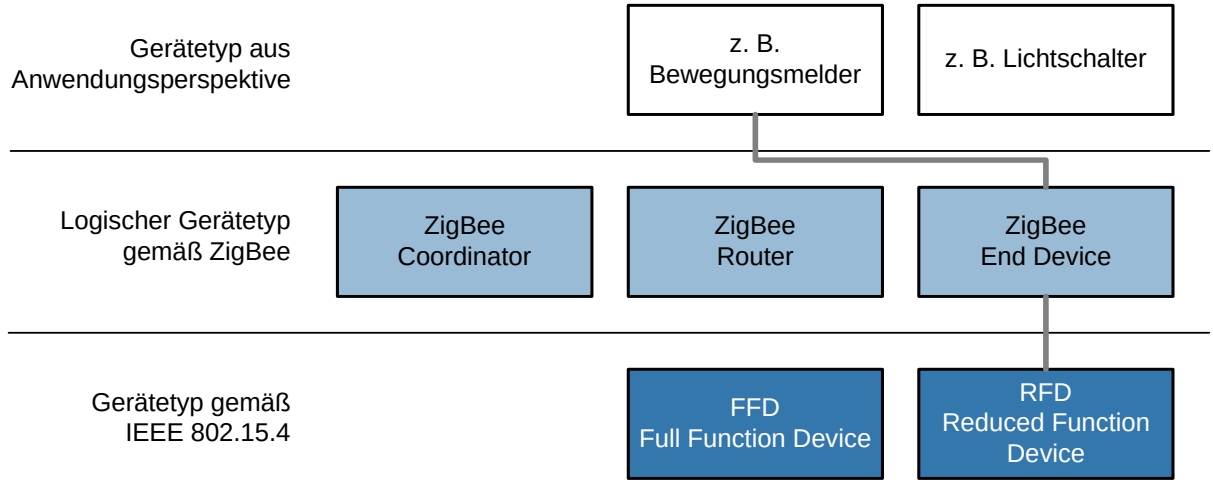


Abb. F-4: Gerätetypen

Dabei ergeben sich anwendungs- und gerätespezifische Profile, wie in der Abb. F-4 am Beispiel eines Bewegungsmelders skizziert.

Über die Mechanismen des Network Layer können unterschiedliche Topologien in einem ZigBee WPAN aufgebaut werden, wie in Abb. F-5 gezeigt. Dabei sind auch redundante Verbindungen möglich. Die Vermaschung kann sich dynamisch durch die Mobilität von Geräten ändern. ZigBee spezifiziert aber keine Mechanismen zur Aufrechterhaltung einer Ende-zu-Ende-Kommunikation bei einer durch Mobilität verursachten Konnektivitätsänderung.

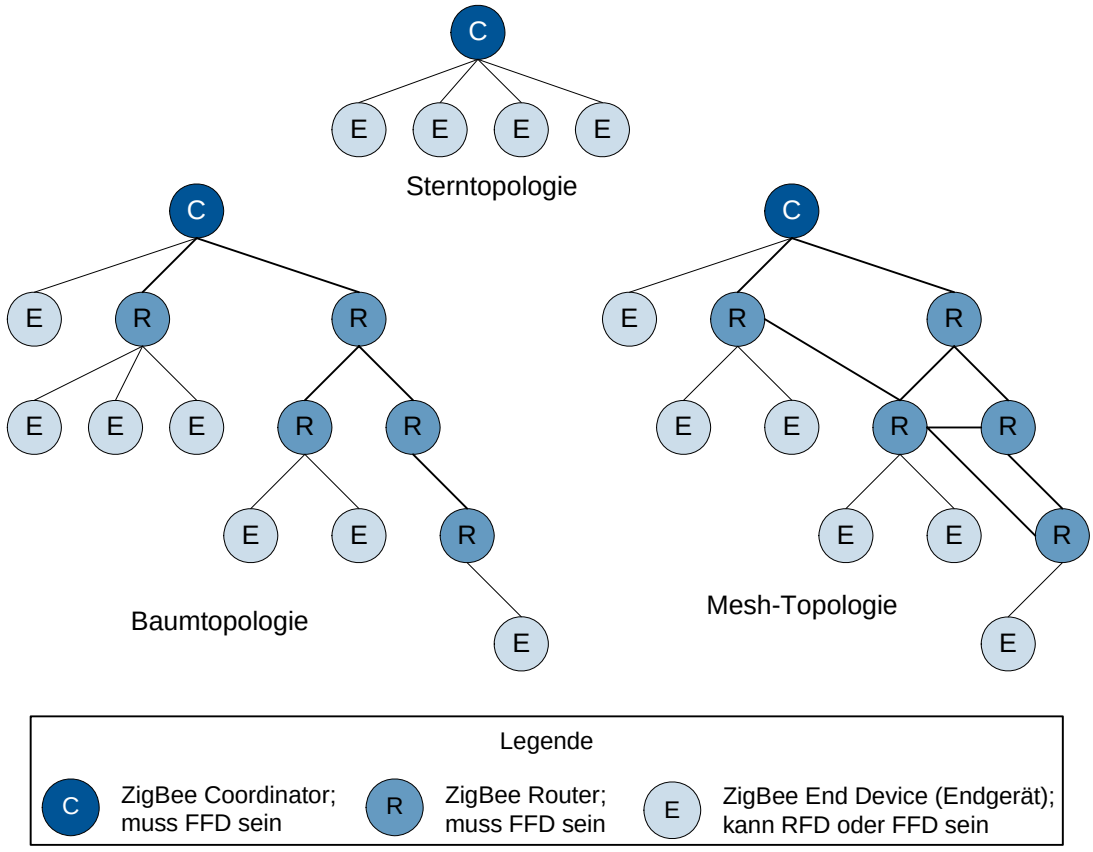


Abb. F-5: Mögliche Netz-Topologien

1.4 Application Layer

Das ZigBee Application Layer setzt sich aus dem Application Support (APS) Sub-Layer, den ZigBee Device Objects (ZDOs) und den außerhalb von ZigBee durch den Hersteller eines Gerätes definierten Application Objects zusammen.

Wenn ein Gerät eingeschaltet wird bzw. in ein ZigBee WPAN eingebracht werden soll, führt das APS Sub-Layer des Gerätes zunächst ein so genanntes Discovery aus. Dabei stellt das Gerät fest, welche anderen Geräte in der Nachbarschaft operieren, zu denen eine Verbindung aufgebaut werden kann. Das APS Sub-Layer übernimmt anschließend auch die Verwaltung der Liste der Geräte, zu denen eine Bindung (Binding) besteht, sowie die Verteilung von Nachrichten zwischen diesen Geräten.

Zu den Verantwortlichkeiten eines ZDO gehören die Festlegung der Rolle des Gerätes (z.B. Endgerät oder ZigBee Coordinator) sowie die Initiierung eines Binding bzw. die Antwort auf ein Binding Request. In dieser Phase werden auch die Parameter für eine gesicherte Kommunikationsbeziehung zwischen den Geräten festgelegt.

1.5 Verbindung zu anderen Netzwerken

Diverse ZigBee-Anwendungen benötigen neben der Funkvernetzung eine Anbindung an eine IP-basierte Infrastruktur. Hierzu dient das Konzept des ZigBee Gateway, welches auf der einen Seite über einen kompletten ZigBee-Protokoll-Stack als ZigBee Router die Verbindung zum ZigBee-Netz hält und über eine spezielle Anwendung auf der anderen Seite die Übertragung von Daten von und zur Infrastruktur durchführt (siehe Abb. F-6). Ein Beispiel ist die Abfrage des Zustands von ZigBee-Geräten und deren Konfiguration über eine zentrale Management-Konsole, die als Festnetzstation in

einem kabelbasierten LAN über IP mit einem ZigBee Gateway kommuniziert. In einem WPAN können durchaus mehrere ZigBee Gateways positioniert sein.

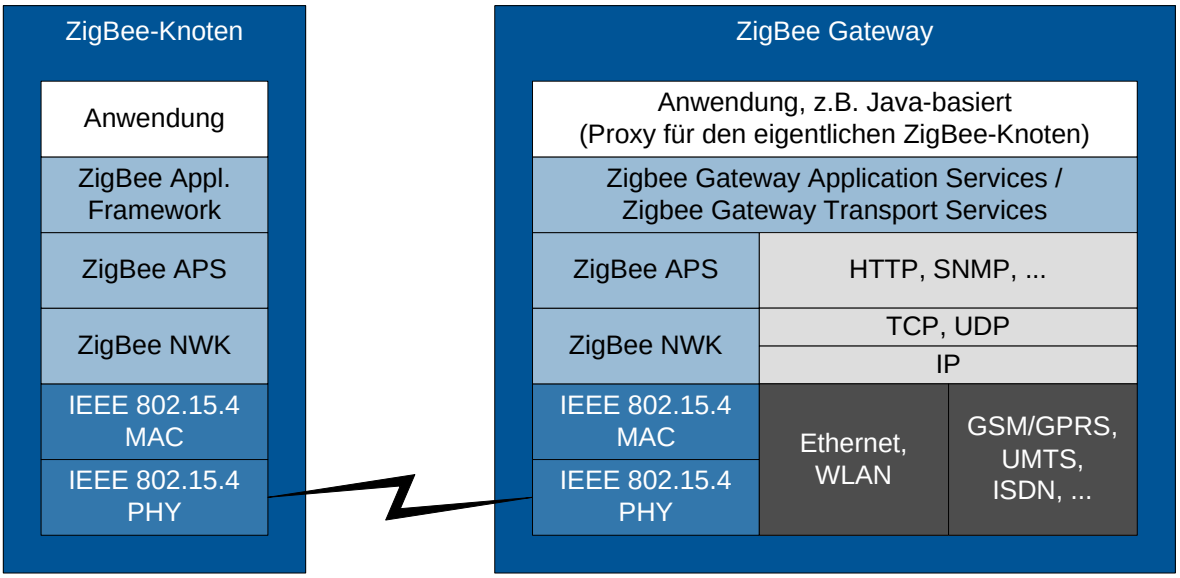


Abb. F-6: Anbindung an die Infrastruktur über ein ZigBee Gateway

2. Sicherheitsmechanismen

Die für ZigBee spezifizierten Sicherheitsmechanismen beinhalten Methoden für den Austausch von Schlüsselmaterial und für den Schutz der Nachrichten, die über ZigBee übertragen werden. Das dabei erreichbare Sicherheitsniveau hängt primär von der Sicherheit der verwendeten symmetrischen Schlüssel ab, d.h. ein Gerät muss entweder auf eine sichere Weise (bei der Herstellung des Gerätes oder manuell durch den Nutzer) mit einem Schlüssel vorkonfiguriert werden oder die Übertragung des Schlüsselmaterials muss geeignet abgesichert sein.

Dies ist allerdings nicht generell gewährleistet, da beispielsweise mit sehr einfachen Endgeräten zu rechnen ist, die eine manuelle Schlüsselkonfiguration nicht gestatten und für die ein initialer Schlüssel ungesichert über Funk übertragen werden muss. In diesem Fall ist das System für einen kurzen Moment sehr verwundbar.

In ZigBee gilt das Prinzip, dass diejenige Protokollebene, die ein Paket erzeugt, zunächst auch für die Absicherung des Pakets verantwortlich ist. Sicherheitsmechanismen werden in ZigBee auf mehreren Protokollebenen realisiert, wie im Folgenden kurz vorgestellt wird.

2.1 Schlüsselmanagement

Die Sicherheit in einem Netzwerk von ZigBee-Geräten basiert auf so genannten Link Keys (Verbindungsschlüssel) und einem Network Key (Netzwerkschlüssel). Die Unicast-Kommunikation zwischen zwei Applikations-Elementen (APL Peer Entities) wird unter Verwendung eines Link Keys abgesichert. Dieser symmetrische Schlüssel muss in den beiden APL Peer Entities vorliegen. Broadcasts werden mit dem Network Key verschlüsselt. Der Network Key ist allen ZigBee-Stationen im Netz bekannt. Alle Schlüssel haben eine Länge von 128 Bit.

Ein ZigBee-Gerät erhält einen Link Key entweder über eine Übertragung des Schlüssels oder durch die Ableitung des Schlüssels[4] oder der Schlüssel ist werksseitig oder manuell durch den Nutzer vorkonfiguriert.

Grundlage für die Ableitung eines Link Key ist ein Master Key, der seinerseits auf die ZigBee-Geräte durch eine Netzwerkübertragung oder eine Vorkonfiguration gelangt.

Der Network Key wird entweder übertragen oder er ist vorkonfiguriert. Der Network Key kann von jeder Protokollschicht, die Sicherheitsfunktionen beinhaltet, verwendet werden, d.h. von MAC, NWK und APL. Ein Link Key oder ein Master Key darf dagegen nur vom APS genutzt werden.

Für die Verteilung der Schlüssel ist in ZigBee ein so genanntes Trust Center verantwortlich, das außerdem Aufgaben im Bereich des Configuration Management auf Netzwerk- und Applikationsebene wahrnimmt. In einem abgesicherten ZigBee-Netzwerk ist genau ein Trust Center vorgesehen. Sofern nicht explizit auf den Geräten im Netzwerk anders vorkonfiguriert, übernimmt der PAN Coordinator auch die Rolle des Trust Centers. Alternativ kann der PAN-Coordinator diese Rolle auch an ein anderes Gerät delegieren.

Im Detail unterscheidet ZigBee hinsichtlich der Rolle des Trust Center zwischen zwei Modi, für die das Trust Center konfiguriert sein kann und denen auch unterschiedliche Sicherheitsniveaus zugeordnet sind: dem Commercial Mode, der meist für Applikationen, die hohe Sicherheitsanforderungen haben, genutzt wird und dem Residential Mode, der durch Anwendungen mit typischerweise geringeren Sicherheitsanforderungen charakterisiert ist.

2.2 Application Layer

Das APS bietet für die eigentlichen Anwendungsobjekte die zur Absicherung der Kommunikation notwendigen Dienste (Security Primitives) an. Dies beinhaltet Operationen für die sichere Übertragung, für den Empfang von abgesicherten Paketen sowie zur Etablierung und Verwaltung von Schlüsseln. Die Anwendungsobjekte sind verantwortlich für die Auswahl eines geeigneten Niveaus der Absicherung einer ausgehenden Übertragung.

Wenn ein Paket auf Anwendungsebene verschlüsselt werden soll, so geschieht dies durch AES-CCM*, einer Erweiterung von CCM, welche die Auswahl gestattet

- ein Paket nur zu verschlüsseln,
- für ein Paket nur eine Integritätsprüfung vorzunehmen
- oder beides zusammen durchzuführen.

CCM ist eine Abkürzung für Counter with CBC-MAC (CBC-MAC = CBC with Message Authentication Code, CBC = Cipher Block Chaining). CCM ist eine generische Methode für die Verschlüsselung und Authentisierung von Daten, die für die Verwendung einer 128-Bit-Blockchiffrierung spezifiziert ist. Hier wird AES als Blockchiffrierung benutzt. Im WLAN-Kapitel dieses Dokuments ist diese Methode kurz beschrieben. Abb. F-7 zeigt die in einem Paket auf dem Application Layer abgesicherten Bereiche.

[4] Der Link Key wird dazu nicht explizit übertragen, sondern Informationen aus denen ein gemeinsamer Schlüssel abgeleitet werden kann.

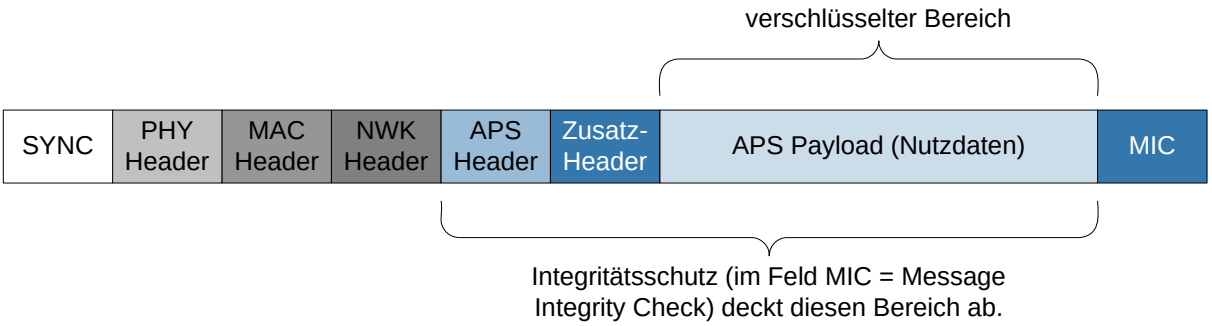


Abb. F-7: Abgesicherte Bereiche bei Verschlüsselung und Integritätsprüfung auf dem Application Layer

Der zur Ver- und Entschlüsselung notwendige symmetrische Schlüssel kann, wie in Abb. F-8 am vereinfachten Beispiel für eine Ende-zu-Ende-Schlüsselverteilung gezeigt, abgeleitet werden. Dabei wendet sich diejenige APS Entity, welche die Kommunikationsbeziehung initiiert (Initiator), zunächst an das Trust Center, um einen Schlüsseltransfer zu initiieren. Das Trust Center überträgt dann das gewünschte Schlüsselmaterial. Wenn es sich dabei um einen Master Key handelt, wird in einem zweiten Schritt der Sitzungsschlüssel im Rahmen des Protokolls Symmetric-Key Key Establishment (SKKE) vereinbart. Über das SKKE wird ein 4-Way-Handshake durchgeführt, ähnlich wie er auch in anderen Kommunikationssystemen (z.B. WLAN) für die Schlüsselaushandlung verwendet wird.

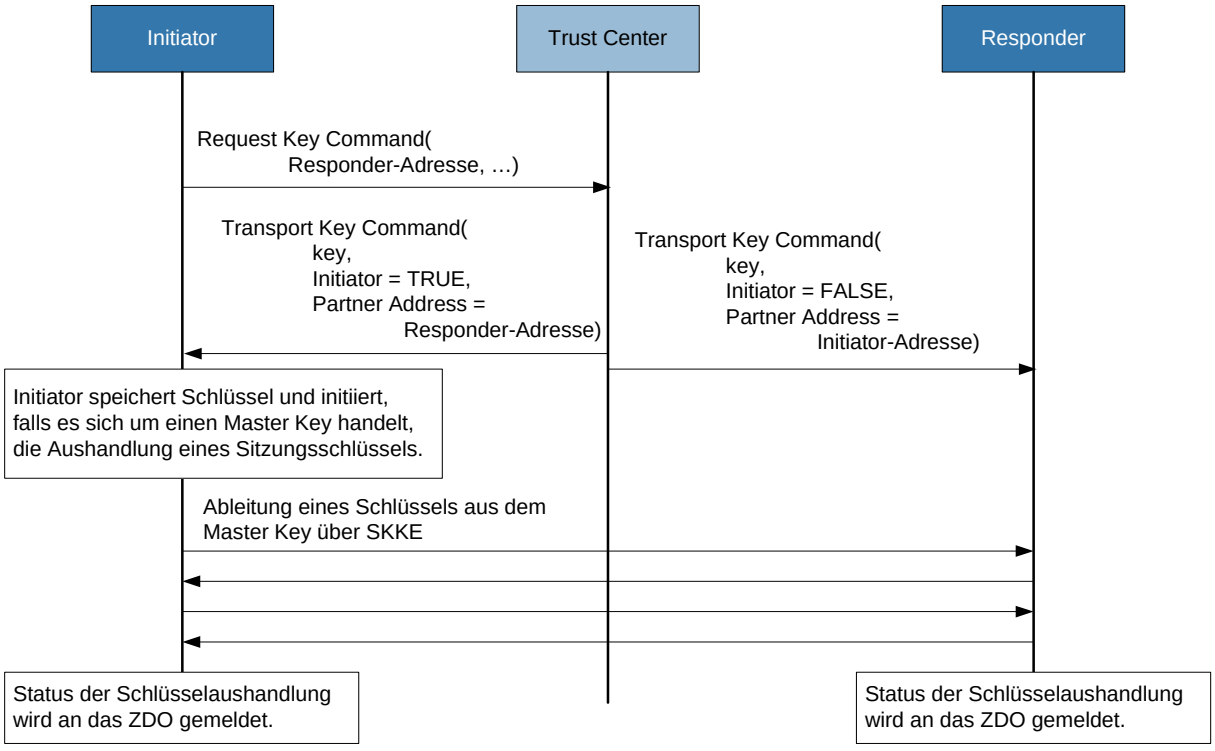


Abb. F-8: Beispiel für die Ende-zu-Ende-Ableitung eines Schlüssels auf Anwendungsebene

2.3 Network Layer

Für Pakete, die auf dem Network Layer verschlüsselt werden sollen, wird ebenfalls das Verfahren AES-CCM* verwendet. Die Anforderung zur Verschlüsselung auf Network Layer kann dabei beispielsweise vom Application Layer durch Angabe eines Parameters geschehen. Abb. F-9 zeigt die in einem Paket auf dem Network Layer abgesicherten Bereiche.

Eine Aufgabe des Network Layer ist das Routing von Nachrichten ggf. über mehrere Zwischenknoten (Hops) hinweg. Pakete des Routing-Protokolls (d.h. Signalisierungspakete zur Bestimmung und Auswahl des Übertragungswegs) beinhalten Broadcast- und Unicast-Nachrichten. Die Unicast-Nachrichten werden mit dem entsprechenden Link Key verschlüsselt, sofern dieser verfügbar ist. Zumindest wird für ein Paket der Network Key angewendet.

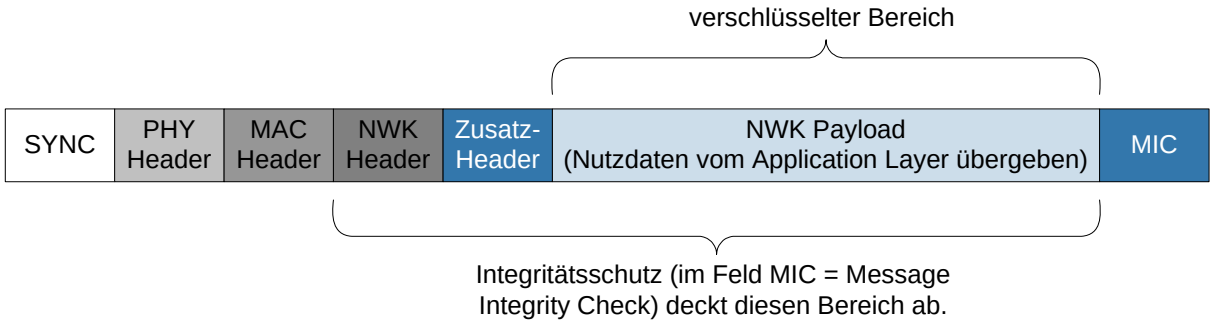


Abb. F-9: Abgesicherte Bereiche bei Verschlüsselung und Integritätsprüfung auf dem Network Layer

2.4 IEEE 802.15.4

Die MAC-Ebene von IEEE 802.15.4 bietet einen Satz von Basis-Sicherheitsdiensten bestehend aus den folgenden Elementen:

- Zugangskontrolle
- Verschlüsselung
- Integritätsprüfung
- Sequenzkontrolle

Diese Elemente werden in so genannten Security Suites zusammengestellt. Tab. F–2 zeigt die in IEEE 802.15.4 festgelegten Security Suites.

Identifikation	Name der Security Suite	Security Service			
		Zugangskontrolle	Verschlüsselung	Frame-Integritätsprüfung	Frame-Sequenzkontrolle (optional)
0x00	-				
0x01	AES-CTR	X	X		X
0x02	AES-CCM-128	X	X	X	X
0x03	AES-CCM-32	X	X	X	X
0x04	AES-CCM-64	X	X	X	X
0x05	AES-CBC-MAC-128	X		X	
0x06	AES-CBC-MAC-64	X		X	
0x07	AES-CBC-MAC-32	X		X	

Tab. F–2: Sicherheitsmechanismen in IEEE 802.15.4

Der Nutzer von IEEE 802.15.4 (also die höheren Protokollebenen, potenziell bis hin zum eigentlichen Nutzer des ZigBee-Systems) ist verantwortlich für die geeignete Auswahl und Nutzung der Security Suites. Dies beinhaltet insbesondere die sichere Übertragung und Ableitung bzw. Konfiguration von Schlüsselmaterial. Im Extremfall wird mit der Suite 0x00 kein Sicherheitsmechanismus eingesetzt.

Der Standard IEEE 802.15.4 legt für ein Gerät drei verschiedene Sicherheits-Modi fest:

- Im Unsecured Mode werden keine Sicherheitsmechanismen genutzt (entspricht der Security Suite 0x00)
- Im ACL Mode erfolgt lediglich eine Zugangskontrolle über eine Access Control List (ACL), siehe Kapitel 2.4.1.
- Nur im Secured Mode sind alle oben genannten Basis-Sicherheitsdienste verfügbar. Abb. F-10 zeigt die dabei in einem Paket auf der MAC-Ebene abgesicherten Bereiche.

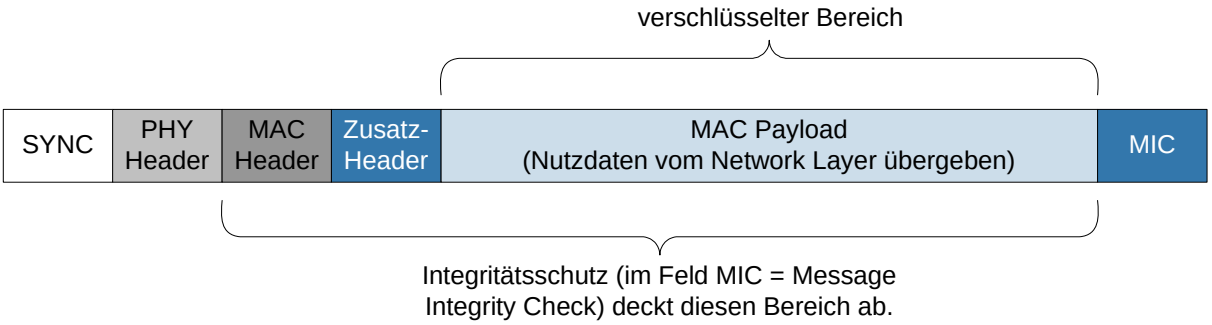


Abb. F-10: Abgesicherte Bereiche bei Verschlüsselung und Integritätsprüfung auf der MAC-Ebene

2.4.1 Zugangskontrolle

Die Zugangskontrolle ist ein Dienst, der einem Gerät die Auswahl des Kommunikationspartners ermöglicht. In einer Access Control List (ACL) werden im Sinne einer so genannten White List die MAC-Adressen derjenigen Stationen verzeichnet, mit denen eine Kommunikation gestattet ist. Empfängt eine Station ein Paket, wird geprüft, ob die Quell-MAC-Adresse in der ACL verzeichnet ist. Wenn nein, wird das Paket verworfen.

Dieser Mechanismus erscheint auf den ersten Blick sehr einfach, die Komplexität besteht allerdings in der Verwaltung der ACLs. Wenn beispielsweise ein Gerät oder der entsprechende Adapter ausgetauscht werden muss, ist es auch unmittelbar erforderlich, die zugehörigen Einträge der ACL(s) zu aktualisieren. Dies ist sehr fehleranfällig. Eine zentrale Verwaltung von MAC-Adressen wäre daher (speziell bei größeren Netzen) wünschenswert. Der Standard IEEE 802.15.4 gibt hierzu jedoch keine Empfehlungen.

2.4.2 Verschlüsselung

Zur Verschlüsselung sind zwei auf dem Advanced Encryption Standard (AES) basierende symmetrische Verfahren unter Verwendung einer Schlüssellänge von 128 Bit spezifiziert:

- AES-CTR: Im Counter (CTR) Mode wird der Wert eines Zählers mit AES verschlüsselt. Dieser verschlüsselte Zählerwert und ein entsprechend großer Block des Klartextes dienen dann als Eingabe in eine XOR-Operation, die dann das Verschlüsselungsergebnis liefert.
- AES-CCM: Siehe Kapitel 2.2.

Es ist grundsätzlich gestattet, dass eine Gruppe von mehr als zwei Stationen einen gemeinsamen Schlüssel verwendet. Mechanismen zum Schlüsselmanagement sind allerdings nicht Bestandteil von IEEE 802.15.4.

2.4.3 Integritätsprüfung

Die im vorangegangenen Kapitel 2.4.2 genannte Methode AES-CCM wird auch zur Integritätsprüfung verwendet. Bei Anwendung von AES-CCM erhält man neben dem verschlüsselten Text auch einen verschlüsselten Integritätscode. Der Standard IEEE 802.15.4 spezifiziert drei Längen für diesen Integritätscode: 32 Bit (AES-CCM-32), 64 Bit (AES-CCM-64) und 128 Bit (AES-CCM-128). Jede Implementierung, die den Secure Mode anbietet, muss zumindest AES-CCM-64 unterstützen.

Es sind auch Security Suites spezifiziert, die als kryptographische Mechanismen keine Verschlüsselung sondern lediglich eine Integritätsprüfung mit verschiedenen Längen für den Integritätscode unterstützen (32 Bit, 64 Bit und 128 Bit, siehe Tab. F–2). Dabei wird AES-CBC-MAC eingesetzt, d.h. AES dient hier nur zur Berechnung einer kryptographischen Prüfsumme der zu übertragenden Daten.

In diesem Zusammenhang ist es wichtig zu erwähnen, dass die ZigBee-Spezifikation in Ergänzung zu IEEE 802.15.4 zusätzlich auch für die MAC-Ebene die Unterstützung von AES-CCM* fordert.

2.4.4 Sequenzkontrolle

Die zu übertragenen Pakete werden nummeriert und die Paketnummer wird im Paket mit übertragen. Bei Empfang eines Pakets wird durch Betrachtung der Paketnummer geprüft, ob das Paket neuer ist als das zuvor empfangene Paket. Wenn nein, kann es sich um eine Replay-Attacke handeln und das entsprechende Paket sollte verworfen werden. Die Paketnummer wird verschlüsselt übertragen. Die Sequenzkontrolle ist optional und steht nur in den Security Suites zur Verfügung, die eine Verschlüsselung unterstützen.

3. Gefährdungen

Dieses Kapitel beschreibt typische Gefährdungen, denen ein ZigBee-System ausgesetzt sein kann. Da bisher kaum ZigBee-Geräte verfügbar sind, gibt es noch wenig Erfahrung.

3.1 Ausfall durch Umgebungseinflüsse

Wie in einem kabelgebundenen Netz kann es auch in einem ZigBee-Netz durch Überspannungen zum Ausfall von Netzkomponenten kommen. Insbesondere sind Außeninstallationen durch Blitz und Witterungseinflüsse gefährdet. In Produktions- und Logistikumgebungen können ZigBee-Komponenten in einer rauen Umgebung durch Staub und Feuchtigkeit beschädigt werden.

3.2 Mangelhafte Planung

ZigBee-Netze mit der Möglichkeit eines flexiblen Routing von Nachrichten über ZigBee Router können schnell eine Dimension erreichen, die eine sorgfältige Planung der Flächendeckung und der Länge möglicher Routing-Pfade erfordern. Folgende Beispiele illustrieren die Gefährdungen durch Planungsfehler:

- Durch eine mangelhafte Planung können sich z.B. Performance-Einbußen ergeben, die durch Störungen oder auch durch Funklöcher entstehen können.
- Die Anzahl der passierten ZigBee Router bis zur Auslieferung einer Nachricht an den Adressaten im ZigBee-Netz bzw. bis zum Erreichen eines ZigBee Gateway ist ein kritischer Parameter. Bei jeder Übertragung zum nächsten Hop über die störanfällige Funkstrecke steigt die Wahrscheinlichkeit eines Paketverlusts an und es kommt zu einer zusätzlichen Verzögerung. Ein Planungsfehler kann zu einer zu großen Anzahl von Hops führen, so dass als Folge Abstriche in der Verfügbarkeit und in der Dienstgüte hingenommen werden müssen.

► Im Rahmen der Netzplanung werden auch die eingesetzten Sicherheitsmechanismen festgelegt. Fehlerhafte Einschätzungen der Risikolage und Planungsfehler können dazu führen, dass ein unnötig geringes Sicherheitsniveau (z.B. der Verzicht auf Verschlüsselung und Integritätsprüfung) eingestellt wird oder beispielsweise Geräte eingesetzt werden sollen, die keine geeignete Absicherung unterstützen (beispielsweise weil sie die ungesicherte Übertragung eines Master Keys erfordern).

3.3 Fehlende Regelungen zur Nutzung von Frequenzen und Störung durch Fremdsysteme

Das ISM-Band bei 2,4 GHz, das für die ZigBee-Funkübertragung unter anderem in Frage kommt, wird von diversen Systemen genutzt (z.B. WLAN, Bluetooth, Bewegungsmeldern, Mikrowellenherden etc.). Wenn in dem Bereich, in dem ein ZigBee-Netz betrieben wird, keine Festlegungen hinsichtlich des Parallelbetriebs zu anderen Funksystemen getroffen werden, kann es zu signifikanten Störungen der Datenübertragung im ZigBee-Netz kommen. Werden diese Störungen durch einen anderen Nutzer (außerhalb der Behörde oder des Unternehmens) verursacht, der berechtigterweise ebenfalls im 2,4-GHz-Bereich operiert, müssen die Störungen sogar hingenommen werden.

3.4 Sicherheitskritische Einstellung

ZigBee überlässt die Wahl von Verschlüsselung und Integritätsprüfung der Applikation bzw. dem Nutzer. Im Extremfall kann der Benutzer selbst entscheiden, ob eine Übertragung gesichert wird oder nicht. Weiterhin können die Voreinstellungen des Herstellers eine unsichere Konfiguration bedeuten. Es besteht damit die Gefahr, dass Übertragungen unzureichend abgesichert sind.

3.5 Schwächen im Schlüsselmanagement

Schlüssel (insbesondere Master Keys) werden entweder vorkonfiguriert – manuell durch den Nutzer oder bei der Produktion des ZigBee-Gerätes – oder zu den ZigBee-Geräten übertragen. Damit besteht zunächst unmittelbar die Gefahr, dass Informationen über einen Master Key nach außen dringen. Ein manuell eingetragener Schlüssel kann (ggf. unbeabsichtigt) eine Systematik aufweisen, die ein Angreifer bei einer Brute-Force-Attacke im Sinne eines geschickten Ratens des Schlüssels ausnutzen kann.

Bei durch den Hersteller vorkonfigurierten Master Keys muss dem Hersteller vertraut werden, dass der Schlüssel einen genügend zufälligen Charakter aufweist.

Kritisch ist das Ausrollen neuer Master Keys, da der Standard hier keine Hilfsmittel spezifiziert. Manuelles Verteilen neuer Schlüssel kann zu Fehlkonfigurationen führen und sehr aufwändig sein. Dies birgt die Gefahr, dass Nutzer mit möglichst wenigen Master Keys arbeiten und die Master Keys weitestgehend über das ZigBee-Netz verteilen[5]. Weiterhin können Nutzer versucht sein, die regelmäßige Verteilung neuer Master Keys zu vermeiden, was automatisch mit dem Problem der Überalterung der Master Keys verbunden ist[6].

---

[5] Die Gefahr besteht dabei darin, dass je weniger Master Keys im Netz vorliegen, desto weniger Schlüssel muss ein Angreifer „erraten“, d.h. desto geringer ist der Aufwand für den Angreifer. Außerdem bedeutet jede Übertragung eines Master Keys die Gefahr, dass der Schlüssel von einem Angreifer abgefangen wird.

[6] Je seltener ein Master Key erneuert wird, desto mehr Zeit hat ein Angreifer, sich den Schlüssel durch geeignete Techniken zu beschaffen. Je länger ein bereits kompromittierter Schlüssel noch gültig ist, desto mehr Möglichkeiten hat ein Angreifer durch Abhören, Fälschen oder durch Zugriff auf Infrastruktur-Ressourcen Schaden zu stiften.

Das Schlüsselmanagement weist insgesamt die Schwäche auf, dass die Übertragung von Schlüsselmaterial nicht in eine Authentisierung eingebettet ist und durch die dabei eingesetzten kryptographischen Mittel geschützt ist. Trotz der Forderung der Unterstützung sehr einfacher Geräte, die keine komplexen Authentisierungsverfahren unterstützen, hätte dies nicht dagegen gesprochen, den ZigBee-Standard um ein weiteres Sicherheitsprofil zu erweitern, das eine Authentisierung mit integrierter Übertragung von Schlüsselmaterial unterstützt.

3.6 Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen der ZigBee-Komponenten breiten sich auch über räumliche Grenzen des ZigBee-Nutzungsbereichs aus. Hier ist dann eine Aufzeichnung grundsätzlich möglich. Werden Richtantennen für einen Lauschangriff verwendet, ist ein ZigBee-Netz trotz der üblicherweise sehr geringen Sendeleistungen seiner Komponenten auch über größere Entfernungen verwundbar.

3.7 Abhören der ZigBee-Kommunikation

Da es sich bei Funk um ein Shared Medium handelt, können die über ZigBee übertragenen Daten aufgezeichnet werden. Der Lauschangriff wird erleichtert, wenn keine Verschlüsselung verwendet wird, oder wenn es gelingt, einen Schlüssel zu kompromittieren. Weiterhin sind Daten, die beispielsweise mit dem im gesamten Netz identischen Network Key verschlüsselt werden, vergleichsweise schwach geschützt.

Die Gefährdung der Vertraulichkeit muss anwendungsspezifisch gewichtet werden. Die Übertragung von Statusinformationen oder Messergebnissen mag zwar in vielen Fällen (beispielsweise in Produktion und Logistik) nur geringe Anforderungen an die Vertraulichkeit stellen, werden dagegen in einer medizinisch-technischen Anwendung Daten übertragen, die auf das Krankheitsbild einer Person Rückschlüsse gestatten, ist der Schutz der Vertraulichkeit immens wichtig.

3.8 Replay und Manipulation von Nachrichten

Ein Angreifer kann zunächst Nachrichten von dem Shared Medium Funk aufzeichnen und wieder in das Netz einspielen. Weiterhin kann der Angreifer dabei Pakete manipulieren. Ohne einen geeigneten und aktivierten Integritätsschutz besteht eine hohe Wahrscheinlichkeit, dass Replay und Manipulation von Nachrichten unerkannt bleiben. Die Verletzung des Sicherheitsziels der Integrität der Nachrichten ist für ZigBee dabei besonders kritisch, da ZigBee zur Sensorabfrage und zu Steuerungszwecken eingesetzt werden soll. Fehlerhafte Messergebnisse oder Steuerkommandos können je nach Anwendung zu einem erheblichen Schaden führen.

3.9 Vortäuschen eines gültigen Netzelements

Sofern keine geeigneten Authentisierungsverfahren eingesetzt werden, kann im Netz eine Fremdstation nur schwer identifiziert werden. Die alleinige Verwendung einer MAC-Adresse für die Zugangskontrolle, wie in ZigBee vorgesehen, kann nicht verhindern, dass eine Station die MAC-Adresse einer anderen (aktuell nicht aktiven) Station übernimmt und sich als gültiges Netzelement ausgibt. Wenn in dieser Situation nicht vorkonfigurierte Schlüssel genutzt werden, kann es sogar passieren, dass eine solche Station mit Schlüsselmaterial versorgt wird und aktiv am Netz teilnehmen kann. Weiterhin ist zu bedenken, dass Multi-Hop-Netze generell eine gewisse Anfälligkeit gegenüber Man-in-the-Middle-Attacken haben. Denkbar ist, dass ein Angreifer einen ZigBee Router vortäuscht und versucht, einen gewissen Anteil des Netzverkehrs über sich zu leiten.

3.10 Bedrohung der Verfügbarkeit

Geräte, die in das Frequenzspektrum einstrahlen, in dem ein ZigBee-Netz operiert, können die Kommunikation empfindlich stören und im Extremfall unmöglich machen. Die Ursache können andere Funkgeräte sein. Speziell im ISM-Band bei 2,4 GHz gibt es diverse Systeme verschiedener Technologien, deren Parallelbetrieb zu massiven gegenseitigen Beeinflussungen führen kann.

Solche Störungen können bewusst durch einen Störsender erzeugt werden; generell können aber alle möglichen elektrischen Geräte Störstrahlungen aussenden. Dieser Faktor muss insbesondere in industriellen Umgebungen in Betracht gezogen werden, die ja eines der Einsatzbereiche von ZigBee ausmachen sollen. Prüfungen hinsichtlich der elektromagnetischen Verträglichkeit können lediglich die Wahrscheinlichkeit einer Störung reduzieren, ausschließen können sie eine Störung nicht. Eine solche Störquelle kann sich bei ausreichender Sendeleistung auch außerhalb des Geländes befinden, auf dem ZigBee genutzt wird.

Grundsätzlich können in Funknetzen Angriffe vom Typ Denial of Service nie ausgeschlossen werden. Ein Übertragungssystem, das robust gegenüber Störungen gestaltet ist, kann lediglich mildernd wirken.

3.11 Erstellung von Bewegungsprofilen

Da die MAC-Adresse eines ZigBee-Adapters, die normalerweise die Hardware-Adresse des Adapters ist, bei jeder Datenübertragung mit versendet wird, ist ein eindeutiger Bezug zwischen MAC-Adresse des Gerätes, Ort und Uhrzeit der Datenübertragung herstellbar. Auf diese Weise können grundsätzlich Bewegungsprofile über mobile Nutzer erstellt werden. Die Wertung dieser Eigenschaft von lokalen Funksystemen als Gefährdung ist anwendungsabhängig. Zunächst ist ein ZigBee-Gerät nicht notwendig mit einer Person assoziiert. Weiterhin gibt es Anwendungen, in denen die Lokalisierung eines Gerätes die Sicherheit von Arbeitsabläufen steigern kann. Das Wissen um die Position einer Person ist beispielsweise bei einem Unfall oft von entscheidender Bedeutung. Hier wäre es eher eine Gefahr, wenn die Lokalisierung nicht zuverlässig und genau genug ist.

4. Schutzmaßnahmen

ZigBee wird sich durch vielfältige und heterogene Anwendungen auszeichnen, verbunden mit einer großen Palette an unterschiedlich intelligenten Geräten. Es gibt also keine allgemeine Default-Empfehlung zur Absicherung, sondern die einzelne Anwendung (bzw. Anwendungsgruppe) muss betrachtet werden. In diesem Sinne ist ZigBee auch spezifiziert, denn jede Protokollschicht ist für die Absicherung eines in der entsprechenden Protokollschicht erzeugten Pakets zunächst selbst verantwortlich. Daher ist die Analyse des Schutzbedarfs der Anwendungen und der zugehörigen Daten eine fundamentale Grundlage.

4.1 Absicherung der Datenkommunikation

Generell gilt, dass jede Kommunikationsbeziehung in ZigBee immer die höchstmögliche anwendbare Absicherung verwenden sollte. ZigBee-Netze sollten dabei möglichst auf jeder Funkstrecke eine Verschlüsselung und eine Integritätssicherung verwenden. Die Priorisierung von Verschlüsselung und Integritätssicherung ist dabei anwendungsspezifisch am Schutzbedarf orientiert.

Auf die ungesicherte Übertragung von Master Keys sollte stets verzichtet werden. Sofern möglich, sollten Master Keys in regelmäßigen Abständen gewechselt werden. Die Häufigkeit muss im Einzelfall festgelegt werden.

Die Absicherung der zu übertragenden Pakete sollte möglichst bereits auf Anwendungsebene geschehen. Die Verschlüsselungsmechanismen der unteren Ebenen sollten nur zur Absicherung von Kontrollpaketen genutzt werden, die auf NWK Layer oder MAC Layer erzeugt werden. Auf diese Weise ist zugesichert, dass Nutzdaten auch bei der Übertragung über ZigBee Router stets gesichert sind.

4.2 Zugangskontrolle

Die Zugangskontrolle über ACLs aus MAC-Adressen gemäß IEEE 802.15.4 sollte für ZigBee Router und ZigBee Gateways genutzt werden. Auf diese Weise ist zunächst das Risiko minimiert, dass sich unbeabsichtigt eine Fremdstation in das Netz integriert. Außerdem kann durch MAC-Filter die Vielfalt der möglichen Netzverbindungen bewusst eingeschränkt und damit übersichtlich gehalten werden. Dies ist insbesondere für ZigBee Router wichtig.

Der effektive Sicherheitsgewinn durch eine Zugangskontrolle basierend auf MAC-Adressen ist allerdings eher gering.

4.3 Absicherung der ZigBee Gateways

Über ZigBee Gateways können sich prinzipiell Angriffe über Netze hinweg ausbreiten. Die Gefährdung besteht dabei in beiden Richtungen, denn auch ZigBee-Geräte können über ein Gateway angegriffen werden. Ein ZigBee Gateway kommuniziert allerdings auf Anwendungsebene und damit besteht die Möglichkeit – im Sinne eines Application Layer Gateway – hier ein hohes Niveau an Sicherheit zu schaffen. Dazu muss ein ZigBee Gateway entsprechend gehärtet sein, zumindest sofern auf dem Gateway ein Standard-Betriebssystem (z.B. Windows oder Linux) genutzt wird.

4.4 Planung der ZigBee Router

Die Verwendung eines ZigBee-Routers sollte mit Bedacht geplant werden, da jeder Hop die Gesamtverfügbarkeit reduziert. Die möglichen Kommunikationsbeziehungen zu anderen Routern sollten durch MAC ACLs gemäß IEEE 802.15.4 festgelegt werden (siehe auch Kapitel 4.2).

4.5 Nicht benötigte Funkschnittstellen deaktivieren

Bei Nichtbenutzung von ZigBee-Komponenten sollte deren Funktion deaktiviert werden bzw. zumindest in den Schlafzustand gewechselt werden.

4.6 Rest-Risiko

Unabhängig von den beschriebenen Sicherheitsmaßnahmen sind mit der Verwendung von ZigBee-Systemen immer folgende Rest-Risiken verbunden:

- ► Das Erstellen von Bewegungsprofilen mobiler Geräte (siehe Kapitel 3.11) kann nicht verhindert werden.
- ► Die Bedrohung der Verfügbarkeit (siehe Kapitel 3.1 und 3.10) ist ebenfalls nicht vermeidbar.

5. Ausblick

Es kann noch nicht abgeschätzt werden, wie stark sich ZigBee verbreiten wird. Zum Zeitpunkt der Erstellung dieses Dokuments sind zwar verschiedene ZigBee-Chipsätze, aber noch kaum Produkte verfügbar. Lücken in den Sicherheitsmechanismen und deren Implementierung zeigen sich meist erst bei entsprechender Verbreitung der Produkte. Hinsichtlich der Entwicklung der Gefährdungen und der Sicherheit ist ein weiterer Ausblick daher nicht möglich.

6. Fazit

ZigBee ist ein für Sensor- und Steuerungsaufgaben zugeschnittenes drahtloses Kommunikationssystem, das sowohl einen punktuellen als auch einen flächendeckenden Aufbau gestattet. ZigBee wird von der ZigBee Alliance als Industriestandard spezifiziert und nutzt auf den unteren beiden Protokollebenen den Standard IEEE 802.15.4.

Die Verschlüsselung und/oder die Integritätssicherung kann auf Application Layer, Network Layer und MAC Layer durchgeführt werden und setzt AES ein. Schlüssel werden vorkonfiguriert oder über das Netz übertragen. Das Schlüsselmanagement weist die Schwäche auf, dass die Schlüsselvereinbarung nicht in eine Authentisierung eingebettet ist und durch die dabei eingesetzten kryptographischen Mittel geschützt ist.

Unter der Annahme sicher konfigurierter Schlüssel gestattet ZigBee allerdings eine vergleichsweise solide Absicherung der Kommunikation (hinsichtlich des Sicherheitsziels der Vertraulichkeit). Voraussetzung ist, dass die im Standard unterstützten Mechanismen auch in den Produkten angeboten werden, der Einsatz dieser Mechanismen geeignet geplant und im Netz auch konfiguriert wird.

7. Literatur / Links

Ausführliche technische Informationen zur Funktionsweise von ZigBee können der Homepage der ZigBee Alliance (www.zigbee.org) entnommen werden. Neben der ZigBee-Spezifikation sind hier auch Präsentationen und White Papers verfügbar.

[IEEE03] IEEE Std 802.15.4, „Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)", Oktober 2003

[ZA04] ZigBee Alliance, „ZigBee Specification v1.0", Dezember 2004, verfügbar unter www.zigbee.org

8. Abkürzungen

ACL	Access Control List
AES	Advanced Encryption Standard
APS	Application Support Sub-Layer
BPSK	Binary Phase Shift Keying
CBC	Cipher Block Chaining
CBC-MAC	CBC with Message Authentication Code
CCM	Counter with CBC-MAC
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTR	Counter

DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
FFD	Full Functional Device
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISM	Industrial-Scientific-Medical
LAN	Local Area Network
MAC	Medium Access Control
NWK	Network Layer
PAN	Personal Area Network
QPSK	Quadrature Phase Shift Keying
RFD	Reduced Functional Device
RFID	Radio Frequency Identification
SKKE	Symmetric-Key Key Establishment
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
WLAN	Wireless LAN
WPAN	Wireless PAN
ZDO	ZigBee Device Object

9. Glossar

Access Control List (ACL)
: Zugriffskontrollliste für die Filterung von zugelassenen IP-/MAC-Adressen

Advanced Encryption Standard (AES)
: Symmetrisches Verschlüsselungsverfahren mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit. AES bietet ein sehr hohes Maß an Sicherheit. Das Verfahren wurde eingehenden kryptoanalytischen Prüfungen unterzogen.

Application Support Sub-Layer (APS)
: Bestandteil des ZigBee Application Layer, das aufbauend auf dem ZigBee Network Layer (NWK) einen Satz von allgemein verwendbaren Applikationselementen anbietet

Authentisierung
: Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Gerätes. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist i. A. keine sinnvolle Autorisierung möglich.

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
: Kanalzugriffsverfahren in ZigBee (und WLAN nach IEEE 802.11), welches auf dem Prinzip der zufälligen Verzögerung des Sendeversuchs und des Abhörens des Funkkanals vor einer Übertragung basiert. Erlaubt mehreren Stationen die simultane Nutzung des Shared Medium Funk mit einem vergleichsweise geringen Kollisionsrisiko.

Cipher Block Chaining Mode (CBC)
: Betriebsart, in der Blockchiffrierungsalgorithmen arbeiten können. Vor dem Verschlüsseln eines Klartextblocks wird dieser erst mit dem im letzten Schritt erzeugten Geheimtextblock per XOR (exklusives Oder) verknüpft

Counter with CBC-MAC (CCM)
: CBC-MAC = Cipher Block Chaining with Message Authentication Code; CCM ist eine generische Methode für die Verschlüsselung und Authentisierung von Daten, die für die Verwendung einer 128-Bit-Blockchiffrierung (z.B. AES) spezifiziert ist.

Denial of Service (DoS)
: Ein Angriff vom Typ Denial of Service hat zum Ziel die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr („Dummy Traffic“) oder die beabsichtigte Herbeiführung eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Dictionary-Attacke
: Eine Wörterbuch-Attacke, die typischerweise zum Raten eines Passworts oder Schlüssels eingesetzt wird. Bei kryptographischen Schwächen eines Verschlüsselungsverfahrens oder bei schwachen Passwörtern geringer Komplexität kann durch geschicktes Raten der Suchraum erheblich verkleinert werden und das Verfahren kann schnell zum Erfolg führen.

Full Functional Device (FFD)
: ZigBee-Gerät, das alle Betriebsfunktionen für ein WPAN implementiert (z.B. die Funktion eines PAN-Coordinators)

Funkzelle
: Geographischer Bereich um einen Sender herum, in dem ein genügend guter Empfang besteht. Was als „genügend gut“ zu bezeichnen ist und was nicht, ist Festlegungssache. Die Ausdehnung einer Funkzelle wird weiterhin durch den verwendeten Frequenzbereich, die Sendeleistung und insbesondere durch die jeweiligen Umgebungsbedingungen (z.B. Material von Wänden, Türen, Fenstern und Decken) beeinflusst.

ISM-Frequenzband
: Lizenzfrei nutzbare Frequenzbänder, die für industrielle, wissenschaftliche und medizinische Zwecke verwendet werden können (ISM = Industrial-Scientific-Medical)

Man in the Middle
: Der Angreifer positioniert sich zwischen zwei Kommunikationspartner und täuscht beiden Parteien vor, der jeweils erwartete eigentliche Partner zu sein. Dabei kann der Man in the Middle den Dialog zwischen den beiden Parteien belauschen oder auch verfälschen. Ziel ist oft die Ermittlung von Passwörtern.

Message Integrity Check (MIC)
: Kryptographischer Integritätsschutzmechanismus

PAN Coordinator
: Spezielle Rolle eines Full Functional Device in einem WPAN nach IEEE 802.15.4. Der PAN Coordinator verwaltet die Identifikation des WPAN, koordiniert die Anmeldung an das WPAN und kann gewisse Parameter beim Kanalzugriff steuern.

Personal Area Network (PAN)
: Netz, welches im Nahbereich (in einem Radius von wenigen Metern) operiert und Kleingeräte wie Drucker, PDAs oder Mobiltelefone untereinander oder mit einer Zentralstation (z.B. PC, Router) vernetzt. Dabei können verschiedene drahtgebundene Übertragungstechniken (z.B. USB oder FireWire) oder drahtloser Techniken, wie IrDA, Bluetooth oder ZigBee verwendet werden. Bei Verwendung drahtloser Techniken spricht man von einem Wireless PAN (WPAN).

Reduced Functional Device (RFD)
: ZigBee-Gerät mit eingeschränkten Kommunikationsmitteln. RFDs sind für einfache Applikationen gedacht (z.B. ein über ZigBee gesteuerter Lichtschalter).

Spoofing
: Untergrabung von Authentisierungs- und Identifikationsverfahren durch Methoden, die auf der Verwendung vertrauenswürdiger Adressen oder Hostnamen beruhen

Wireless PAN (WPAN)
: Siehe PAN

Zelle
: Siehe Funkzelle

ZigBee Device Object (ZDO)
: Modelliert auf Anwendungsebene ein ZigBee-Gerät. ZigBee Anwendungen werden als Application Objects dargestellt, die über die ZDOs kontrolliert und verwaltet werden.

ZigBee Coordinator
: Entspricht dem PAN Coordinator in IEEE 802.15.4 und ergänzt diesen um Funktionen auf dem Network Layer

ZigBee Router
: Spezielle Full Functional Device, die zusätzlich Pakete zwischen ZigBee-Knoten vermitteln kann. Der logische Gerätetyp ZigBee Router entspricht dem Coordinator in IEEE 802.15.4.

G. IrDA

Inhaltsverzeichnis des Abschnitts

1. Grundlagen / Funktionalität

Die Infrared Data Association (IrDA), eine 1993 gegründete Non-Profit-Organisation, hat 1994 die erste IrDA-Spezifikation veröffentlicht. In dieser werden die unteren Schichten eines Protokolls für eine Infrarot-Schnittstelle definiert, bei der Infrarotstrahlung (also Licht) als Träger für den Datenaustausch über kurze Distanzen verwendet wird. Mittlerweile stellt IrDA auch höhere Protokolle für unterschiedliche Einsatzbereiche zur Verfügung. IrDA wird heute von allen gängigen Betriebssystemen unterstützt, die Kommunikation von Geräten wie PDA und Mobiltelefon mit dem PC oder untereinander via Infrarot-Schnittstelle ist in der Praxis etabliert.

Die Infrarot-Schnittstelle wurde ursprünglich als kabelloser Ersatz der seriellen Schnittstelle konzipiert. Sie arbeitet bidirektional im Halbduplex-Verfahren mit Licht der Wellenlänge von 850 bis 900 Nanometer.

Heute wird grundsätzlich zwischen IrDA Data und IrDA Control unterschieden, wobei letzterem eine wesentlich geringere Bedeutung zukommt. Mit dem Begriff IrDA wird im Allgemeinen das IrDA Data Protokoll oder aber die IrDA-Organisation selbst bezeichnet.

1.1 IrDA Data

Der IrDA Data Standard wurde 1994 veröffentlicht und definiert in seiner ursprünglichen Version 1.0, die auch als Serial Infrared (SIR) bezeichnet wird, eine Datenrate von 2.400 Bit/s bis 115,2 kBit/s. In der Version 1.1 wurden 1995 höhere Datenraten von 1,152 MBit/s (Mid-Infrared = MIR) und 4 MBit/s (Fast-Infrared = FIR) spezifiziert, wobei die Kompatibilität zu SIR gewährleistet ist.

Die Versionen 1.2 und 1.3 beinhalten Low-Power-Versionen, die mit reduzierter Sendeleistung ebenfalls Datenraten bis zu 115,2 kBit/s (Version 1.2) bzw. 1,152 MBit/s und 4 MBit/s (Version 1.3) erreichen.

Die 1999 veröffentlichte Version 1.4 bietet durch ratenabhängige Kodierung der Datenbits Datenraten bis 16 MBit/s (Very Fast Infrared = VFIR).

Die Reichweite hängt von der abgestrahlten Leistung ab, sie beträgt in den Low-Power-Betriebsarten 20 Zentimeter, bei normaler Leistungsabgabe 1 bis 2 Meter. Der Abstrahlungswinkel beträgt ± 30°.

Um eine Verbindung aufzubauen, müssen zwei Geräte mit ihren Schnittstellen so aufeinander ausgerichtet werden, dass eine direkte Sichtverbindung zustande kommt. Hindernisse und größere Distanzen sind mit IrDA nicht zu überbrücken. Jedoch ergeben sich aus dieser Betriebsart auch Vorteile, da Störungen nur von sehr hellen Lichtquellen oder direkter Sonneneinstrahlung ausgehen.

Die Protokollarchitektur von IrDA Data ist in drei verbindliche und eine Reihe optionale Protokolle unterteilt (siehe Abb. G-1).

Zu den verbindlichen Protokollen gehören

- Physikalische Bitübertragungsschicht (IrPHY),
- IrDA Link Access Protocol (IrLAP),

  IrLAP setzt auf die physikalische Bitübertragungsschicht auf und ist für den Verbindungsaufbau zuständig.
  Es wird zwischen den zwei Betriebzuständen NDM (Normal Disconnected Mode) und NRM (Normal Response Mode) unterschieden. Im nicht verbundenen Modus (NDM) wird nach Signalen möglicher Kommunikationspartner gesucht und gleichzeitig ein Informationssignal mit 9600 Bit/s ausgesendet. Wird ein kommunikationsfähiges Gerät entdeckt, wird zwischen den zwei Geräten eine Verbindung hergestellt (NRM). Daraufhin werden die jeweiligen Leistungsdaten der Geräte ausgetauscht.
  IrLAP sichert die Verbindung mit Hilfe von Fehlerkorrektur (CRC-16 für Datenraten bis 1,152 MBit/s und CRC-32 für höhere Datenraten) und erneutem Senden von Daten im Bedarfsfall.

Details zum Verbindungsaufbau in IrDA können der IrDA-Spezifikation entnommen werden, die von der Infrared Data Association bezogen werden kann (siehe [IrDA]).

- IrDA Link Management Protocol (IrLMP)

  IrLMP setzt auf IrLAP auf und sorgt als nächst höhere Schicht für Mehrfachzugriff, Kanalbereitstellung für Dienste und das Informationsmanagement.

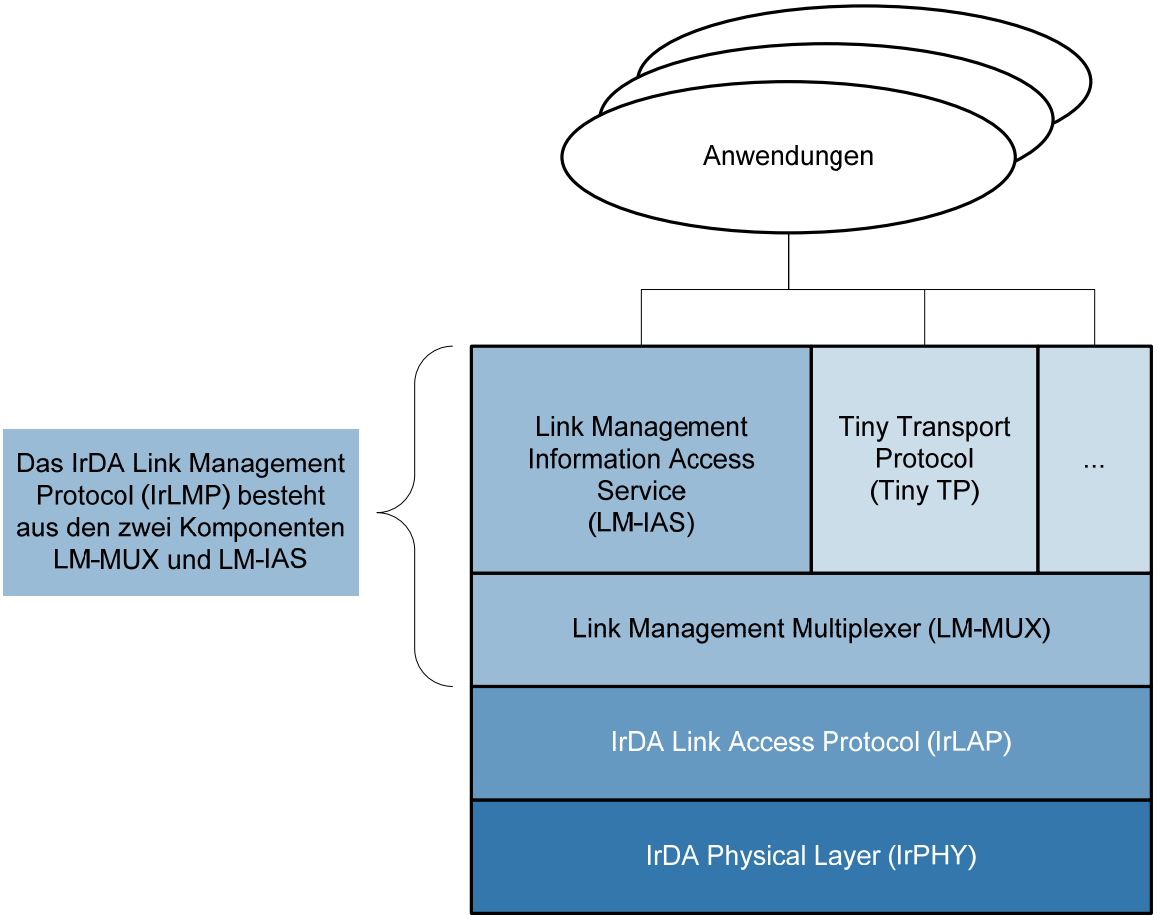


Abb. G-1: IrDA Protokoll-Stack

Neben diesen verbindlichen Protokollschichten existieren optionale Protokolle, die anwendungsspezifisch den Datenaustausch steuern. So gibt es beispielsweise

- Tiny Transport Protocol (TinyTP): bietet verbesserte Flusskontrolle und Segmentierung
- IrDA Infrared Communications Protocol (IrCOMM): emuliert serielle RS-232-Schnittstellen (EIA/TIA-232-E) und parallele Centronics Schnittstellen
- IrDA Local Area Network Access Protocol (IrLAN): erweitert das Link Management Protocol zur Einbindung von IrDA-Geräten in LANs
- IrDA Infrared Mobile Communications Protocol (IrMC): definiert einfachen Datenaustausch zwischen mobilen Geräten, z.B. Visitenkarten, Notizen, Kalendereinträge und Aufgabenlisten; außerdem definiert es eine Anrufkontrolle und Audiodatenübertragung zwischen Mobiltelefonen und Notebooks
- IrDA Object Exchange Protocol (OBEX): ermöglicht einfachen und schnellen Datenaustausch zwischen mobilen Geräten durch „Push“- und „Pull“-Funktion, z.B. Filetransfer, Bildübertragungen, Übertragung von Status- oder Diagnose-Informationen, etc.; ermöglicht auch Verbindungen über einen längeren Zeitraum mit mehreren Datenübertragungen und Idle-Zeiten

- ► IrDA Infrared Transfer Picture Specification (IrTran-P): spezifiziert Bildübertragungen für digitale Kameras
- ► IrDA Infrared for Wrist Watches (IrWW): stellt ein zeitbasiertes Datenkommunikationsschema für Armbanduhren zur Verfügung
- ► IrDA Financial Messaging (IrFM) Point and Pay: ermöglicht ein digitales Zahlungssystem

Eine Beschreibung der verschiedenen Protokolle findet sich unter [IrDA].

1.2 IrDA Control

IrDA Control ist ein Protokoll zur Kommunikation von Peripheriegeräten wie Tastaturen, Mäusen, Joysticks oder Fernbedienungen mit zentralen Hosts, wie z.B. PCs und Fernsehgeräten.

Für diese Infrarotübertragung ist eine andere physikalische Bitübertragungsschicht definiert, mit Datenraten bis 75 kBit/s und Reichweiten bis 5 Metern, so dass IrDA Data und IrDA Control zueinander nicht kompatibel sind. Um den Bewegungsraum zwischen Host und Peripheriegerät nicht unnötig einzuschränken, ist in der Spezifikation ein Arbeitswinkel von ± 50° vom Host angegeben.

IrDA Control arbeitet mit einem Zeitschlitzverfahren, so dass ein Host mehrere Peripheriegeräte gleichzeitig ansteuern kann.

Die Protokollarchitektur von IrDA Control umfasst die drei verbindlichen Protokollschichten

- ► Physical Layer (PHY)
- ► Media Access Control (MAC)
- ► Logical Link Control (LLC)

2. Sicherheitsmechanismen

Im IrDA Standard sind keine Sicherheitsmechanismen gegen ein Mithören des Datenverkehrs spezifiziert. Die Daten werden nur auf Protokollebene gegen Übertragungsfehler mittels CRC gesichert. Sicherheitsmechanismen wie Authentisierung, kryptographischer Integritätsschutz und Verschlüsselung sind nicht vorhanden. Diese müssen ggf. auf Applikationsebene implementiert werden.

In gewissem Rahmen wird die Übertragung zumindest bei IrDA Data durch die sehr eingeschränkte Reichweite der Infrarotstrahlen und die benötigte Sichtverbindung geschützt. Bei IrDA Control ist dagegen durch den größeren Streuwinkel und die größere Reichweite mehr Vorsicht geboten.

3. Gefährdungen

Da im Protokoll keine Authentisierung vorgesehen ist, kann ein beliebiger Partner Daten über die IrDA-Schnittstelle an ein Gerät senden. So nimmt beispielsweise ein Mobiltelefon mit aktivierter IrDA-Schnittstelle SMS-Mitteilungen zum Versand an. An einen PDA oder Laptop können auch Programme über IrDA geschickt werden, die Schadfunktionen enthalten können.

Die Einschränkungen bezüglich des Mithörens der Übertragung durch die geringe Streubreite bei der IrDA Data Spezifikation gelten nicht für die IrDA-Control-Spezifikation. Dies ist insbesondere beim Einsatz von Tastaturen mit Infrarotschnittstelle, die auf die IrDA Control Spezifikation zurückgreift, zu beachten.

4. Schutzmaßnahmen

Beim Betrieb von Geräten mit IrDA Schnittstelle ist darauf zu achten, dass diese nur im Bedarfsfall aktiviert wird: Da im Protokoll keine Authentisierung vorgesehen ist, kann ein beliebiger Partner Daten über die IrDA-Schnittstelle an ein Gerät senden. Außerdem belastet eine eingeschaltete IrDA-Schnittstelle die Batterie bzw. den Akku des mobilen Gerätes zusätzlich.

Da die Kopplung nur in einem sehr eingeschränkten Bereich möglich ist, ist ein Mithören der Kommunikation meist ausgeschlossen. Das bestehende geringe Restrisiko aufgrund der Streustrahlung der IrDA-Komponenten kann durch den Einsatz von zusätzlichen Sicherheitsmechanismen (z.B. Authentisierung und Verschlüsselung auf Applikationsebene) oder den Ersatz von IrDA durch leitungsgebundene Übertragung weiter minimiert werden.

5. Ausblick

Die Infrared Data Association hat Ende 2005 die IrDA-Spezifikation IrSimple Connect (IrSC) veröffentlicht. Dieses Protokoll bietet eine Datenübertragungsrate von 16 MBit/s, und eine Erweiterung auf 100 MBit/s ist in der Entwicklung. Die Übertragungszeit wird außerdem verkürzt, indem die Latenzzeit beim Verbindungsaufbau der Geräte, d.h. die Zeit bis zwei Geräte aufeinander eingestellt sind und die eigentliche Übertragung beginnen kann, verkürzt wurde.

IrSC kann laut IrDA über ein einfaches Update der bisherigen IrDA-Spezifikationen installiert werden und ist rückwärts kompatibel zu den bisherigen IrDA-Standards, so dass auch eine Kommunikation mit Geräten mit älteren IrDA-Spezifikationen möglich ist.

Durch diese Weiterentwicklung und vor allem die Aussicht auf eine Steigerung der Übertragungsrate auf 100 MBit/s werden sicherlich in nächster Zeit neue IrDA-Applikationen entwickelt.

6. Fazit

Durch die eingeschränkte Übertragungsreichweite und den relativ geringen Streuwinkel ist bei Infrarotübertragungen immer ein gewisser Grundschutz gegeben. Allerdings muss bei entsprechend höheren Sicherheitsanforderungen immer auf Sicherheitsmaßnahmen wie Authentisierung, Integritätssicherung und Verschlüsselung auf Applikationsebene zurückgegriffen werden, da die IrDA-Protokolle selbst keine Sicherheitsmaßnahmen bieten. Ist eine solche Sicherung auf Applikationsebene nicht möglich, muss gegebenenfalls auf den Einsatz von IrDA verzichtet werden.

7. Literatur / Links

[IrDA] Homepage der Infrared Data Association, http://www.irda.org

8. Abkürzungen

CRC	Cyclic Redundancy Check
FIR	Fast-Infrared
IrCOMM	IrDA Infrared Communications Protocol
IrDA	Infrared Data Association (IrDA)
IrFM	IrDA Financial Messaging
IrLAN	IrDA Local Area Network Access Protocol

IrLAP	IrDA Link Access Protocol (IrLAP),
IrLMP	IrDA Link Management Protocol
IrMC	IrDA Infrared Mobile Communications Protocol
IrPHY	IrDA Physikalische Bitübertragungsschicht
IrSC	IrDA-Spezifikation IrSimple Connect
IrTran-P	IrDA Infrared Transfer Picture Specification
IrWW	IrDA Infrared for Wrist Watches
LLC	Logical Link Control
MAC	Media Access Control
MIR	Mid-Infrared
NDM	Normal Disconnected Mode
NRM	Normal Response Mode
OBEX	IrDA Object Exchange Protocol
PC	Personal Computer
PDA	Personal Digital Assistant
PHY	Physical Layer
TinyTP	Tiny Transport Protocol
VFIR	Very Fast Infrared

9. Glossar

CRC
: Cyclic Redundancy Check: Prüfsumme über die zu übertragenden Daten, die in der Nachricht mitgeschickt wird und es dem Empfänger gestattet, Bitfehler, die auf dem Kommunikationskanal entstanden sind, zu erkennen

IrDA
: Infrared Data Association: Non-Profit-Organisation, die Spezifikationen für Infrarot-Schnittstellen erarbeitet; wird auch als Synonym für das von der Infrared Data Association spezifizierte IrDA Data Protokoll verwendet

IrLAP
: IrDA Link Access Protocol: für den Verbindungsaufbau zuständige Protokollschicht von IrDA Data

IrLMP
: IrDA Link Management Protocol: Protokollschicht von IrDA Data, die für Mehrfachzugriff, Kanalbereitstellung für Dienste und das Informationsmanagement zuständig ist. IrLMP besteht aus den beiden Komponenten LM-MUX und LM-IAS.

LM-IAS
: Der Link Management Information Service ist der Directory Service eines IrDA-Systems. LM-IAS stellt für ein Applikations-Element (Application Entity) die notwendigen Mittel zur Verfügung, um ein entsprechendes Gegenstück (Peer Entity) zu identifizieren und zu lokalisieren.

LM-MUX
: Der Link Management Multiplexer gestattet die simultane Nutzung der IrLAP-Verbindung durch mehrere Applikations-Elemente (Application Entity).

H. Drahtlose Tastaturen, Mäuse und andere Eingabegeräte

Inhaltsverzeichnis des Abschnitts

1. Grundlagen und Funktionalität

Drahtlose Tastaturen und Mäuse sind Peripheriegeräte, die kabellos über Funk- oder Infrarot-Schnittstellen mit einem Empfängermodul kommunizieren, das über einen COM-Port, eine PS2-Schnittstelle oder einen USB-Anschluss mit dem Rechner verbunden ist.

Da keine galvanische Verbindung zum Rechner besteht, müssen kabellose Eingabegeräte über eine eigene Spannungsversorgung in Form von Batterien oder Akkus verfügen. Für eine lange Betriebsdauer ist eine geringe Leistungsaufnahme dieser Geräte unumgänglich. Nach dem heutigen Stand der Technik haben Geräte mit Infrarot-Technik einen höheren Energieverbrauch als solche mit einer Funkschnittstelle. Inzwischen gibt es auch Geräte (speziell Mäuse), die ihre Energie drahtlos durch Induktion erhalten. Das Gerät wird dazu einfach auf ein spezielles Pad gelegt, das seinerseits konventionell mit Strom versorgt wird.

Die Betriebsfrequenzen der Systeme liegen ausschließlich in lizenzfreien ISM-Bändern. Die Mehrzahl der Funkmäuse und Funktastaturen sendet im 27 MHz-Band und verfügt über zwei Funkkanäle, einige kabellose Geräte arbeiten im 2,4-GHz-Bereich.

Die Reichweite der Funksysteme beträgt typischerweise 2 bis 5 Meter, die extrem abhängig von den Umgebungsbedingungen ist. Hier ist im Gegensatz zu Systemen auf Basis der Infrarot-Technik keine direkte Sichtverbindung zwischen Sender und Empfänger notwendig. Andere im gleichen ISM-Band sendende Geräte wie z.B. CB-Funkgeräte, Funkspielzeug, funkgesteuerte Antriebe für Garagentore oder WLAN Verbindungen im 2,4-GHz-Bereich können den Betrieb der Systeme empfindlich stören und die Reichweite reduzieren. Metallische Hindernisse (Stahlarmierungen, Stahlschränke und Ähnliches) können zum Versagen der Technik führen.

2. Sicherheitsmechanismen

Ein Problem der funkbasierten Eingabegeräte ist die mangelnde Abhörsicherheit. Die ausgesendeten Funksignale können von Dritten empfangen und aufgezeichnet werden. Sind diese Funksignale nicht sicher verschlüsselt, können diese Daten leicht ausgewertet werden. Es gibt auf dem Markt zahlreiche Funktastatursysteme, welche die aus den Tastenanschlägen resultierenden Signale völlig unverschlüsselt - und damit für Dritte abhörbar - übertragen. Hier reicht häufig schon ein zweiter Empfänger vom selben Hersteller aus, um die empfangenen Signale auf einem anderen Rechner sichtbar zu machen.

Hersteller von Funk-Anwendungen geben als Reichweite Entfernungen an, in denen die Datenübertragung ihrer Geräte sicher funktioniert. Diese Funktionsreichweite ist aber im Falle von Geräten, die nur mit billiger Empfangstechnik ausgestattet sind, meist kleiner als die Entfernung, in der die ausgesendeten Signale mit Hilfe von Richtantennen und hochwertiger Empfängerelektronik noch empfangen, aufgezeichnet und ausgewertet werden können. Eine Abhörgefährdung in einer größeren Entfernung als die Funktionsreichweite kann daher nicht ausgeschlossen werden.

Systeme, die auf Basis der Infrarot-Technik kommunizieren, verwenden meistens den IrDA-Standard (siehe Kapitel IrDA), der keinerlei Sicherheitsmechanismen unterstützt. Hier wird die benötigte Sichtverbindung zwischen Sender und Empfänger sowie die begrenzte Reichweite als Sicherheitsmerkmal genannt. Das Sicherheitsniveau solcher IrDa-Systeme liegt aufgrund der möglichen Streustrahlung trotzdem unter dem der kabelgebundenen Eingabegeräte.

Einige Hersteller bieten funkbasierte Produkte mit proprietären Sicherheitslösungen an. Über die Sicherheit solcher Lösungen kann keine Aussage getroffen werden, da die eingesetzten Algorithmen in der Regel von den Herstellern unter Verschluss gehalten werden.

Damit baugleiche Geräte nebeneinander betrieben werden können, haben die meisten Hersteller ihre Geräte mit verschiedenen Erkennungsnummern (IDs) ausgerüstet. Hierbei werden verschiedene Prinzipien verwendet, z.B. wird aus einem Pool von IDs ein bestimmter Wert fest für ein Gerät vergeben, oder es wird bei einem Batteriewechsel die ID durch die Software erneut zufällig bestimmt.

Auf dem Markt sind erste Produkte erhältlich, die mit Bluetooth-Funktechnik kommunizieren. Bei korrekter Implementierung und Konfiguration der Bluetooth-Sicherheitsmerkmale bieten diese im Allgemeinen einen höheren Schutz als Funksysteme mit proprietärer Technik. Eine Zusammenstellung der Gefährdungen und mögliche Sicherheitsmaßnahmen zum Thema Bluetooth findet man in Kapitel Bluetooth.

Abschließend sei erwähnt, dass bei Tastaturen durch die elektromagnetische Abstrahlung der Tastaturmatrix und des Verbindungskabels eine Abhörgefährdung besteht (siehe BSI-Faltblatt zur bloßstellenden Abstrahlung [BSIABSTR]). Dies gilt auch für kabellose Tastaturen. Im Allgemeinen ist die Abhörgefährdung bei kabelgebundenen Tastaturen wesentlich geringer als bei kabellosen Eingabegeräten.

3. Ausblick

In näherer Zukunft wird sich die Nutzung von drahtlosen Tastaturen und Mäusen weiter massiv ausbreiten. Auch in sensiblen Bereichen hält die Nutzung von drahtlosen Eingabegeräten verstärkt Einzug, wodurch die aufgezeigten Gefährdungen eine erhöhte Brisanz erhalten. Jedoch ist ein Trend zu Produkten, die auf der Bluetooth-Funktechnik basieren und damit einen höheren Schutz bieten, zu erkennen. Die potenzielle Nutzung von Eingabegeräten, die auf UWB-Funksystemen (ultra-wideband) basieren, ist zum jetzigen Zeitpunkt unklar, ein Trend in diese Richtung ist nicht erkennbar.

4. Fazit

Zahlreiche Funktastaturen und Funkmäuse senden ihre Informationen über Funk oder Infrarot-Licht ohne Sicherheitsvorkehrungen zu den Rechnern. Ohne großen Aufwand können diese Informationen von Dritten mitgelesen oder gegebenenfalls sogar manipuliert werden. Vom Einsatz solcher Systeme ist aus Sicht der IT-Sicherheit generell abzuraten.

Für Systeme mit proprietären Sicherheitsmaßnahmen, die kein Sicherheitszertifikat aufweisen, ist der Sicherheitswert nicht einschätzbar. Der Nutzer geht hierbei das Risiko ein, dass die nicht evaluierte Lösung des Herstellers nur eine minimale Sicherheit bietet, die aber bei weitem nicht ausreicht, um seine Daten effektiv zu schützen.

Drahtlose Systeme, die auf Standards wie Bluetooth basieren und bei denen die Sicherheitsmechanismen korrekt implementiert und aktiviert worden sind, können einen im Vergleich höheren Schutz bieten.

Bei Einsatz von Geräten mit einer Stromversorgung über Batterie- bzw. Akku kann die Nutzungsdauer von kabellosen Eingabegeräten einschränkt werden. Wird ein solches Gerät zur Bedienung von Geräten mit hoher Verfügbarkeitsanforderung wie z.B. einem Server zur Überwachung von Netzwerkkomponenten benutzt, so könnte es im Falle einer notwendigen schnellen Bedienung des Gerätes bei gleichzeitiger Unterbrechung der Eingabefunktionalität zu folgenschweren Ausfällen kommen.

In sensiblen Bereichen sollte man grundsätzlich keine Funk-Tastaturen, Funk-Mäuse und Infrarot-Produkte einsetzen.

5. Literatur / Links

[BSIABSTR] Bundesamt für Sicherheit in der Informationstechnik, Faltblatt „Bloßstellende Abstrahlung“, http://www.bsi.bund.de/literat/faltbl/012_blab.htm

6. Abkürzungen

ID	Identification, Erkennungsnummer
IrDA	Infrared Data Association
ISM	Industrial, Scientific and Medical
USB	Universal Serial Bus

I. UWB

Inhaltsverzeichnis des Abschnitts

1. Grundlagen / Funktionalität

Die staatliche US-Regulierungsbehörde FCC (Federal Communications Commission) hat im August 1998 auf eigenen Antrag Forschungen initiiert, die sich mit den Möglichkeiten einer unlizenzierten kommerziellen Nutzung von so genannten „ultra-wideband“ (UWB) Funksystemen beschäftigen [FCC98]. Der Begriff UWB bezeichnet Funksysteme, die – bezogen auf die Betriebsfrequenz – eine hohe Bandbreite nutzen. Im Allgemeinen belegt bei UWB das Spektrum der Aussendung eine Bandbreite, die mindestens 25% der Bandmittenfrequenz beträgt. Nach Ansicht der FCC eignet sich diese Technik für spezielle Radarsysteme sowie für bildgebende Verfahren in Bauwerken oder unter der Erde verborgene Objekte. Auch die Möglichkeit einer Modulation der Funksignale und Nutzung für die Datenübertragung wurde erwogen. Als besondere Eigenschaft der UWB-Systeme erkannte die FCC, dass sich die Sendeenergie auf einen sehr großen Frequenzbereich verteilt und somit für herkömmliche schmalbandige Empfangssysteme nur noch als Hintergrund-Rauschen wahrnehmbar ist oder gar vollständig hinter deren Eigenrauschen verschwindet. Somit wäre also ein ungestörter Parallelbetrieb herkömmlicher Funkanwendungen und UWB möglich.

Heute sieht man in UWB eine Technik, die zur Übertragung hoher Datenraten über kurze Entfernungen genutzt werden kann. Der Abstand zwischen Sender und Empfänger wird im Allgemeinen kleiner als 10 Meter sein. Auch im Hinblick auf eine lange Standzeit batteriebetriebener Geräte wird mit geringen Sendeleistungen gearbeitet. Die UWB-Technik ist letztlich vergleichbar mit Bluetooth, bietet jedoch eine erheblich höhere Bandbreite. Mögliche Anwendungen für UWB sind:

- schnelle Datenübertragung zu lokaler Videospeicherung in Audio- und Videogeräten für mobile Anwendungen
- genaue Standortverfolgung von Objekten in Lagern oder industriellen Umgebungen
- „drahtlose USB-Schnittstelle“ zur Verbindung von PCs und Peripheriegeräten in einem WPAN

Die Vorteile des UWB-Verfahrens werden in der Literatur wie folgt zusammengefasst:

- geringer Energieverbrauch, Voraussetzung für eine hohe Batterielebensdauer in mobilen Endgeräten
- skalierbare hohe Datenraten
- verbesserte Störfestigkeit
- robust gegen Mehrwegeausbreitung (Frequenz-Diversity)
- kleine, kostengünstige, skalierbare und flexible Chipsätze in CMOS-Technologie realisierbar

Die ersten Ansätze für UWB fußten auf so genannten gepulsten Signalen. Jeder Puls dauert dabei nicht länger als eine Milliardstel Sekunde (10^{-9} s) und ähnlich wie bei einem ultraschnellen Morsecode enthält die Abfolge der Pulse die zu übertragende Information.

In der Zwischenzeit haben sich zwei mögliche Varianten für eine technische Realisierung von UWB herauskristallisiert: Direct Sequence UWB (DS-UWB) und Multiband OFDM (MB-OFDM). Beide Verfahren wurden von der Task Group IEEE 802.15.3a [IEEE153a] diskutiert. Eine Einigung auf einen gemeinsamen Standard konnte die Task Group nicht erwirken, stattdessen löste sie sich im Januar 2006 auf. Die hinter den genannten Verfahren stehenden Konsortien bekräftigten jedoch ihr Interesse an einer weiteren Entwicklung der Technik. Es sind dies:

- Das UWB-Forum, das DS-UWB propagiert
- Die WiMedia Alliance (seit März 2005 verschmolzen mit der MBOA), die MB-OFDM propagiert

Die WiMedia Alliance erreichte in Zusammenarbeit mit der European Association for Standardizing Information and Communication Systems, kurz ECMA International, die Herausgabe eines Standards für UWB-Systeme auf der Basis von MB-OFDM. Die Spezifikation wurde als ECMA-368 veröffentlicht [ECMA05] und soll der ISO/IEC zur Verabschiedung vorgelegt werden. MB-OFDM wurde dar-

über hinaus im März 2006 von der Bluetooth Special Interest Group als Basis für zukünftige Bluetooth-Geräte ausgewählt [BTSIG06].

1.1 Direct Sequence UWB

Die nachfolgende Beschreibung basiert auf einem Vorschlag der IEEE 802.15.3a [DSU04], der vom UWB-Forum eingebracht wurde. Demnach arbeitet DS-UWB im Frequenzbereich von 3.1 bis 10.6 GHz, wobei zwischen einem Unterband (3.1 bis 4.85 GHz) und Oberband (6.2 bis 9.7 GHz) unterschieden wird. Je Band sind 6 Kanäle definiert; im Unterband beträgt der Kanalabstand 39 MHz, im Oberband 78 MHz. Die Kanaltrennung erfolgt letztlich über ein Code-Multiplexverfahren (CDMA). Dabei wird jedes zu übertragende Datenbit mit einem festen binären Muster multipliziert, der so genannten Spreizsequenz. Die bei DS-UWB verwendeten Spreizsequenzen sind zwischen 1 und 24 Bits lang; zur besseren Unterscheidung von den eigentlichen Datenbits werden die Bits der Spreizsequenz als „Chips“ bezeichnet. Bei DS-UWB wird eine Chip-Rate verwendet, die genau einem Drittel der verwendeten Sendefrequenz entspricht. Das Code-Multiplexverfahren ermöglicht eine gute Unterscheidung zwischen Signalen benachbarter Kanäle, obwohl sich die Spektren unterschiedlicher Kanäle infolge der hohen Bandbreite erheblich überlappen (siehe Abb. I-1).

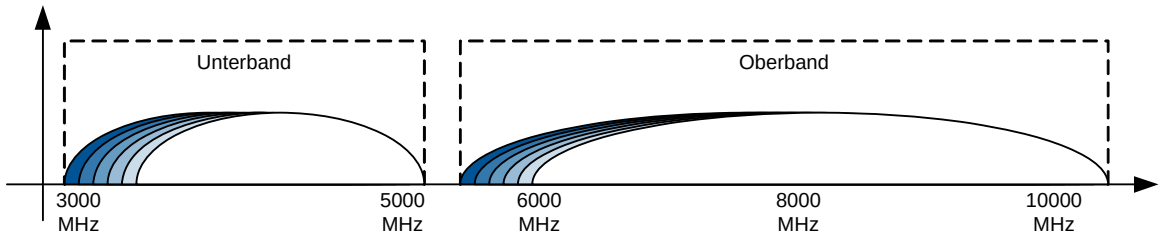


Abb. I-1: Vorgesehene Frequenzbänder bei DS-UWB gemäß [DSU04]

Die Modulation erfolgt wahlweise mit einem zweiwertigen (BPSK) oder einem vierwertigen Verfahren (4-BOK), entsprechend einem oder zwei Bits pro Symbol. Ein Symbol umfasst immer die Länge einer Spreizsequenz und wird auch als „Puls“ bezeichnet. Abhängig von der Sendefrequenz und der damit verknüpften Chip-Rate F_{chip} sowie der Länge der Spreizsequenz ergibt sich ein großer Bereich möglicher Bit-Raten.

Zur Verbesserung der Robustheit gegen Bitfehler wird die Verwendung eines Faltungscodes (Forward Error Correction, FEC) mit unterschiedlichen Code-Raten vorgeschlagen. Dabei wird die Gesamtzahl der versendeten Bits derart vergrößert, dass Redundanz entsteht. Sofern der Datenstrom auf der Übertragungsstrecke Bitfehler infolge von Störungen erleidet, kann der Empfänger die im Faltungscode enthaltene Redundanz dazu verwenden, die fehlerhaften Bits wieder herzustellen. Die Fähigkeit der Fehlerkorrektur wird umso besser, je mehr redundante Bits ausgesandt werden. Das Verhältnis der übertragenen Daten-Bits zu den tatsächlich übertragenen Bits wird als Code-Rate bezeichnet. Code-Rate ½ bedeutet demzufolge, dass für jedes Datenbit zwei Bits zu übertragen sind.

Die letztlich bereitstehende Datenrate ergibt sich also aus Bit-Rate[1] und verwendetem Faltungscode. Tab. I–1 nennt die möglichen Datenraten mit BPSK im Unterband. Im Gegensatz zu anderen Datenfunkverfahren wird die vierwertige Modulation nicht zu einer weiteren Erhöhung der Datenrate genutzt. Stattdessen verdoppelt man in diesem Falle die minimale Länge der Spreizsequenz und erhält dadurch eine größere Robustheit gegen Störungen. Gleiches gilt für den Betrieb im Oberband, wo infolge der doppelten Chip-Rate eine Verlängerung der minimalen Länge der Spreizsequenz erfolgt. Die maximale Datenrate beträgt 1320 MBit/s.

1 Das Produkt aus Symbol-Rate und Bits pro Symbol in Tab. I–1.

Datenrate	Code-Rate	Länge der Spreizsequenz	Bits pro Symbol	Symbol-Rate
28 MBit/s	½	24	1	$F_{chip}/24$
55 MBit/s	½	12	1	$F_{chip}/12$
110 MBit/s	½	6	1	$F_{chip}/6$
220 MBit/s	½	3	1	$F_{chip}/3$
500 MBit/s	¾	2	1	$F_{chip}/2$
660 MBit/s	1	2	1	$F_{chip}/2$
1000 MBit/s	¾	1	1	F_{chip}
1320 MBit/s	1	1	1	F_{chip}

Tab. I–1: Datenraten bei BPSK im Unterband

Beispiel (4. Tabellenzeile): Bei einer 3 Chips langen Spreizsequenz wird alle 3 Chips ein Symbol übertragen. Im Unterband beträgt die Sendefrequenz ca. 4000 MHz, die Chip-Rate F_{chip} beträgt demzufolge 1333 Megachips/s. Es ergibt sich eine Symbolrate von 444 Megasymbolen pro Sekunde. Pro Symbol wird bei BPSK ein mittels Faltungscode erzeugtes Bit übertragen, hier also 444 MBits/s. Bei einer Coderate von ½ ergibt sich eine tatsächlich nutzbare Datenrate von ca. 220 MBit/s.

1.2 Multiband-OFDM

Der Standard ECMA-368 [ECMA05] spezifiziert Multiband-OFDM im Frequenzbereich von 3.1 bis 10.6 GHz. Der Bereich ist in 14 Frequenzbänder mit einer Bandbreite von je 528 MHz unterteilt. Die Bänder werden in 4 Gruppen à 3 sowie einer Gruppe à 2 Bänder zusammengefasst (siehe Abb. I-2).

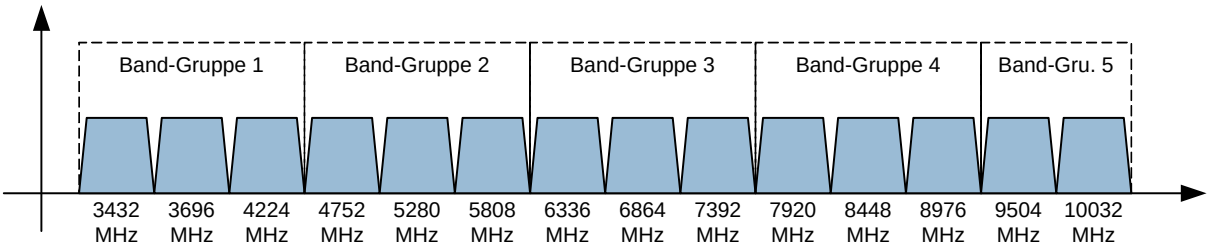


Abb. I-2: Geplante Frequenzbänder in MB-OFDM gemäß [ECMA05]

Jedes Band besteht aus 128 Unterkanälen, von denen 100 zur Datenübertragung genutzt werden. Die Symbolrate beträgt 3,2 Megasymbole pro Sekunde. Die Modulation erfolgt mit einem vierwertigen Verfahren (QPSK oder DCM, siehe [ECMA05]), entsprechend zwei Bits pro Symbol.

Zur Verbesserung der Robustheit gegen Bitfehler werden drei Verfahren vorgeschlagen:

- ► Verwendung eines Faltungscodes (Forward Error Correction, FEC) mit unterschiedlichen Code-Raten
- ► Aussenden gleicher Information auf zwei unterschiedlichen Unterträgern (Frequency-domain spreading, FDS)

► Aussenden desselben Symbols zweimal zu unterschiedlichen Zeiten (Time-domain spreading, TDS)

Insgesamt ergibt sich aus der Kombination dieser drei Parameter die in Tab. I–2 dargestellte Matrix der Datenraten.

Datenrate	Code-Rate	Modulation	FDS	TDS	Bits/Symbol
53,3 MBit/s	1/3	QPSK	Ja	Ja	50
80 MBit/s	1/2	QPSK	Ja	Ja	50
106.7 MBit/s	1/3	QPSK	Nein	Ja	100
160 MBit/s	1/2	QPSK	Nein	Ja	100
200 MBit/s	5/8	QPSK	Nein	Ja	100
320 MBit/s	1/2	DCM	Nein	Nein	200
400 MBit/s	5/8	DCM	Nein	Nein	200
480 MBit/s	3/4	DCM	Nein	Nein	200

Tab. I–2: Datenraten bei MB-OFDM

Beispiel (2. Tabellenzeile): Die OFDM ermöglicht in Kombination mit QPSK das gleichzeitige Übertragen von 200 Bits in einem Symbol. Wird FDS eingesetzt, halbiert sich diese Zahl auf 100, da immer zwei Unterträger für ein Bit benötigt werden. Infolge von TDS wird das gleiche Symbol zweimal ausgesandt, die Zahl halbiert sich zu 50 Bits pro Symbol. Bei 3,2 Megasymbolen pro Sekunde ergibt sich eine Bitrate von 160 MBit/s. Bei einer Coderate von ½ ergibt sich eine tatsächlich nutzbare Datenrate von ca. 80 MBit/s.

Die Unterscheidung verschiedener Kanäle geschieht mittels eines Frequenzsprungverfahrens. Dabei wird jedes Symbol in einem unterschiedlichen Band einer Band-Gruppe ausgesandt. In jeder der 4 unteren Bandgruppen sind 7 unterschiedliche Sprungsequenzen (Time-Frequency Codes, TFC) definiert, in der Bandgruppe 5 lediglich 2.

1.3 Regulierende Vorschriften für UWB

Die Untersuchungen der staatliche US-Regulierungsbehörde FCC hatten im Februar 2002 zu der Erteilung einer eingeschränkten kommerziellen Nutzungserlaubnis geführt, die aber bis heute nicht unumstritten ist [FCC02]. In erster Linie zweifeln Vertreter von Fluggesellschaften und Mobilfunkbetreiber sowie das US-Verteidigungsministerium an dieser Erlaubnis. Hervorgehoben werden immer wieder die möglichen Gefahren, die durch Interferenzen zwischen UWB und etablierten Drahtlos-Anwendungen (Mobilfunk, GPS, Radar) entstehen können. Vor allem deswegen hat die FCC ihre Erlaubnis zunächst auch eingeschränkt und die kommerzielle Nutzung der UWB-Technik nur für Anwendungen erlaubt, die unterhalb von 960 MHz und oberhalb von 3,1 GHz arbeiten.

Aufgrund neuerer Erkenntnisse hob die FCC im März 2003 die Nutzungseinschränkung aus [FCC02] auf. Die kommerzielle Nutzungserlaubnis für UWB gilt nunmehr für den gesamten Frequenzbereich [HEI03]. Die FCC teilte die Einwände von Fluggesellschaften und Netzbetreibern nicht mehr, dass es

zwischen herkömmlichen Funkanwendungen und UWB zu gefährlichen Interferenzen kommen könnte.

Entsprechend dem aktuellen Stand des Teil 15 der „Commission´s Rules“ [FCC05] ist UWB in den USA für verschiedene Anwendungsfälle zugelassen. Beispielhaft seien in der Tab. I–3 die Werte für Systeme im Innen-Bereich angegeben. Zu beachten ist, dass die Leistungswerte sich auf den Teil der Gesamtleistung beziehen, der innerhalb einer Bandbreite von 1 MHz um die betreffende Messfrequenz anfällt. Im für UWB vorgesehenen Frequenzbereich zwischen 3100 und 10600 MHz ist demzufolge eine Leistung[2] von 74 nW/MHz erlaubt. Auf den gesamten Frequenzbereich (7500 MHz) bezogen darf somit eine Leistung von 0,5 mW nicht überschritten werden[3].

Frequenz in MHz	EIRP in dBm pro MHz
960-1610	-75.3
1610-1990	-53.3
1990-3100	-51.3
3100-10600	**-41.3**
über 10600	-51.3

Tab. I–3: Leistungsgrenzen für UWB-System innerhalb von Gebäuden in den USA gem. [FCC05]

In Europa liegt derzeit noch keine Genehmigung für UWB vor. Die Britische Regulierungsbehörde Ofcom („Office of Communications“) hat jedoch im September 2005 ein Diskussionspapier für ein Meeting der entsprechenden Arbeitsgruppe bei CEPT vorgelegt. Ein Vorabversion harmonisierter Bedingungen für UWB-Geräte im Frequenzbereich unterhalb 10,6 GHz liegt den nationalen Behörden inzwischen zur Kommentierung vor.

2. Sicherheitsmechanismen

2.1 Kryptographische Sicherheitsmechanismen bei DS-UWB

Der vorliegende Vorschlag der IEEE 802.15.3a [DSU04] bezieht sich lediglich auf die physikalische Schnittstelle. Medienzugang und eventuelle Sicherheitsmechanismen sind bislang ungeklärt und keiner Standardisierung unterworfen.

2.2 Kryptographische Sicherheitsmechanismen bei MB-OFDM

Der ECMA-Standard [ECMA05] definiert zwei Sicherheitsebenen: keine Sicherheit und hohe Sicherheit. Geräte wählen zwischen den Ebenen abhängig von einem Sicherheitsmodus, in dem sie arbeiten:

► Security mode 0: Das Gerät verwendet grundsätzlich keine Sicherheit bei der Datenübertragung.

---

2 Hier ist die EIRP gemeint, d.h. die Sendeleistung, die man an eine isotrope Antenne einspeisen dürfte. In der Praxis sind der Gewinn der verwendeten Antenne und die Kabeldämpfung entsprechend zu berücksichtigen.

3 Diese Sendeleistung liegt in der Größenordnung der Bluetooth Klasse 3.

- Security mode 1: Das Gerät verwendet keine Sicherheit, wenn es mit Geräten des Modus 0 oder 1 kommuniziert. Bei Kommunikation mit Geräten im Modus 2 wird hohe Sicherheit eingesetzt.
- Security mode 2: Das Gerät verwendet grundsätzlich hohe Sicherheit und kommuniziert dem zufolge nur mit Geräten im Modus 1 oder 2.

Eine hohe Sicherheit wird erreicht durch starke Verschlüsselung, Integritätsprüfung und Schutz gegen Einspielen zuvor aufgezeichneter Frames („replay attack protection“). Dabei werden nicht nur Datenpakete geschützt, sondern auch ausgewählte Signalisierungspakete.

Ausgehend von einem symmetrischen geheimen Schlüssel (Pairwise Master Key, PMK) werden temporäre Schlüssel für die Punkt-zu-Punkt-Übertragung zwischen Stationspaaren (Pairwise Transient Key, PTK) sowie Schlüssel für die Multicast-Aussendung (Group Transient Key, GTK) abgeleitet. Zum Einsatz kommt ein Verfahren, das als 4-Way-Handshake bezeichnet wird. Es ähnelt dem gleichnamigen Verfahren bei Wireless LAN und ermöglicht das Generieren der temporären Schlüssel, ohne dass diese zwischen den Stationen übertragen werden müssten. Das Verfahren dient gleichzeitig der gegenseitigen Authentisierung der Kommunikationspartner, hier Initiator und Responder genannt.

Zu diesem Zweck tauschen Initiator und Responder je eine Zufallszahl (I-Nonce bzw. R-Nonce) aus. Beide Stationen bilden unter Zuhilfenahme der beiden Zufallszahlen, der Geräteadressen sowie dem PMK eine neue 256 Bit lange Pseudozufallszahl. Sofern beide PMK identisch waren, gilt dies auch für die Pseudozufallszahl, deren eine Hälfte (128 Bit) nun als PTK dient. Die andere Hälfte wird zur Errechnung eines Prüfwertes (PTK Message Integrity Code, PTK MIC) herangezogen, der an den jeweiligen Kommunikationspartner übertragen und dort zur Prüfung der Authentizität des Gegenübers verwendet wird. Abb. I-3 zeigt das vollständige Handshake.

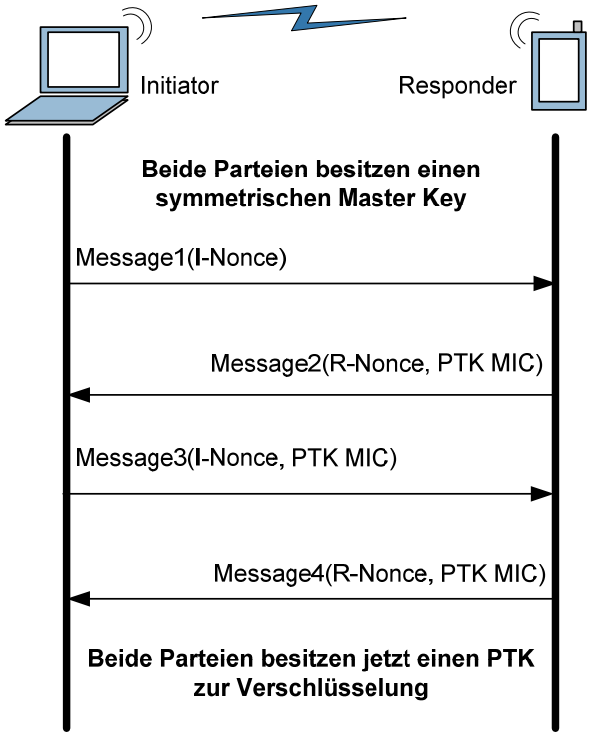


Abb. I-3: 4-Way-Handshake

Wie die Stationen in den Besitz des PMK gelangen, der als Basis für das 4-Way-Handshake dient, ist nicht Gegenstand des Standards.

Auf Basis der temporären Schlüssel erfolgt eine Verschlüsselung mittels Advanced Encryption Standard (AES) in einem speziellen Modus CCM (siehe Abb. I-4). CCM steht für CTR mode (Counter Mode) with CBC-MAC Protocol (Cipher Block Chaining Message Authentication Code). Hierbei wird nicht direkt der Klartext verschlüsselt, sondern ein Pseudozufallswert (Nonce), der unter anderem aus einem Paketzähler (Secure Frame Number, SFN) gebildet wird. Das eigentliche Verschlüsselungs-

ergebnis entsteht dann aus der XOR-Verknüpfung eines Blocks des Klartexts mit dem AES-verschlüsselten Nonce. Die Methode Cipher Block Chaining (CBC) wird zur Integritätssicherung der Daten verwendet; sie dient der Berechnung einer Prüfsumme (Message Integrity Code, MIC).

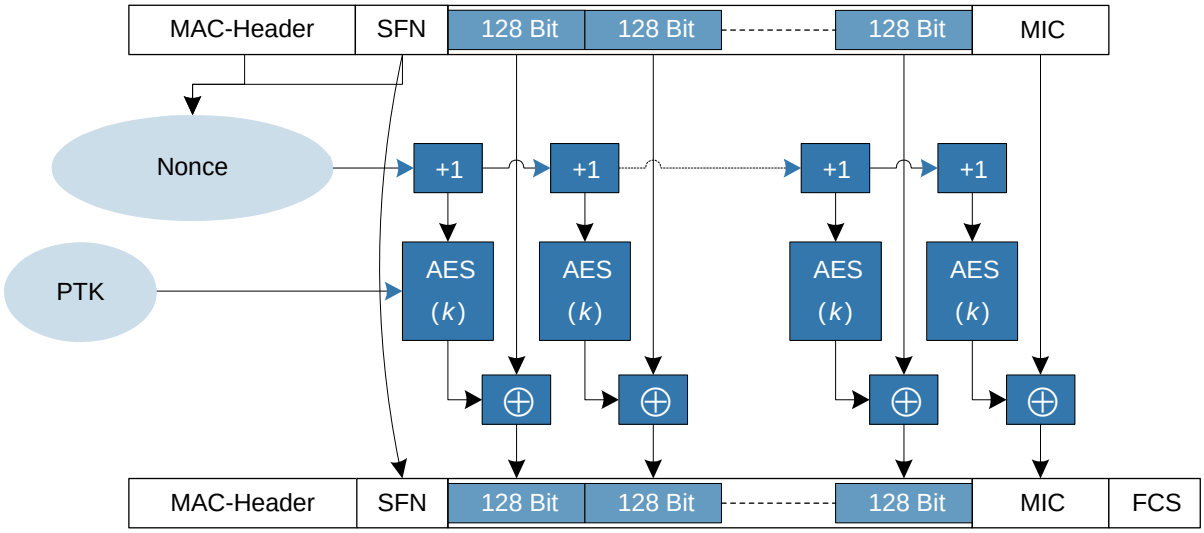


Abb. I-4: Verwendung von AES bei MB-OFDM (vereinfacht)

3. Gefährdungen bei der Nutzung von UWB

Dieses Kapitel beschreibt typische Gefährdungen, denen ein UWB-System ausgesetzt sein kann. Da bisher UWB nur in Prototypen eingesetzt wurde, gibt es keine praktischen Erfahrungen mit diesen Systemen. Darüber hinaus gibt es über die in Kapitel 2.2 genannten Verfahren keine stabilen Spezifikationen von Sicherheitsmechanismen.

3.1 Fehlende Regelungen zur Nutzung von Frequenzen

UWB-Systeme sind für den Einsatz parallel zu anderen Funksystemen prädestiniert. Die vorliegenden Regulierungen beschäftigen sich mit der Frage, inwieweit herkömmliche Systeme durch UWB beeinträchtigt werden. Dagegen ist ein Schutz von UWB-Systemen vor Störungen durch andere Funksysteme auf Basis einer Regulierung ebenso wenig möglich wie vorgesehen. Es ist somit beim Betrieb von Anwendungen auf der Basis von UWB grundsätzlich mit der Möglichkeit zu rechnen, dass Störungen auftreten. Eine Verfügbarkeit der Anwendungen kann unter diesen Bedingungen kaum garantiert werden (siehe auch Kapitel 3.2).

3.2 Bedrohung der Verfügbarkeit

UWB-Systeme übertragen Informationen mittels elektromagnetischer Funkwellen. Strahlen andere elektromagnetische Quellen im gleichen Frequenzspektrum Energie ab, können diese die UWB-Kommunikation stören und im Extremfall verhindern. Dies kann unbeabsichtigt durch andere technische Systeme oder aber durch absichtliches Betreiben einer Störquelle (Jammer) als so genannter Denial-of-Service-Angriff (DoS-Angriff) erfolgen. Eine solche Störquelle kann sich bei ausreichender Sendeleistung auch außerhalb des Gebäudes befinden, in dem UWB genutzt wird.

3.3 Schwachstellen bei passwortbasierten Authentisierungsverfahren

Die im ECMA-Standard vorgesehenen kryptographischen Sicherheitsmaßnahmen basieren auf einem symmetrischen Schlüssel (PMK), der allen beteiligten Komponenten bekannt sein muss (siehe Kapitel 2.2). Ein Verfahren zur Generierung und Verteilung des PMK ist nicht vorgegeben. Stattdessen muss man davon ausgehen, dass im vorgesehenen Einsatzbereich der UWB-Systeme die Implementierung einer Sicherheits-Infrastruktur – etwa auf Basis von EAP gem. IEEE 802.1X – weder technisch noch wirtschaftlich möglich sein wird. Stattdessen wird man dem Beispiel von Bluetooth folgen und PMK manuell eingeben.

Unter dieser Bedingung ist eine Wörterbuch-Attacke möglich. Zeichnet man den Informationsaustausch zur Ableitung eines Sitzungsschlüssels (PTK) auf der Luftschnittstelle auf, kann man anschließend ohne Verbindung zu den UWB-Systemen mögliche Passworte probieren. Hierbei spielt die Komplexität der Passworte eine entscheidende Rolle.

3.4 Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen der UWB-Systeme breiten sich auch über räumliche Grenzen des WPAN aus. Dabei kann auch in nicht vom WPAN-Betreiber kontrollierten Bereichen ein Empfang möglich sein. Durch die Verwendung einer Richtantenne lassen sich auch in größerer Entfernung schwache Signale empfangen und letztlich auswerten.

3.5 Diebstahl eines Endgeräts

Ein Dieb kann über die in dem gestohlenen Gerät enthaltenen Informationen ungehindert und unbemerkt Basisinformationen für eine weitere Kompromittierung erlangen, z.B. auf dem Wege des Auslesens des geheimen Schlüssels (PMK).

3.6 Erstellung von Bewegungsprofilen

Da die Geräte-Adresse eines UWB-Systems bei jeder Datenübertragung mit versendet wird, ist ein eindeutiger Bezug zwischen Geräte-Adresse des Funk-Clients sowie Ort und Uhrzeit der Datenübertragung herstellbar. Auf diese Weise können Bewegungsprofile über mobile Nutzer erstellt werden.

4. Schutzmaßnahmen

4.1 Absicherung von UWB

UWB-Systeme sollten grundsätzlich mit Verschlüsselung betrieben werden. Sofern Geräte gemäß ECMA-368 [ECMA05] zum Einsatz kommen, sollten diese in den Security Mode 2 versetzt werden, da sie nur unter dieser Bedingung jegliche unverschlüsselte Kommunikationsbeziehung ablehnen. Die Unterstützung des Security Mode 2 wird somit zu einem Auswahlkriterium für UWB-Systeme entsprechend ECMA-368.

Die UWB-Schnittstellen der Geräte sollten bei Nichtbenutzung deaktiviert werden.

4.2 Weitere Schutzmaßnahmen

Über die in Kapitel B.4.1 genannten Maßnahmen hinaus sollten auf UWB-Systemen – falls dies technisch möglich ist – weitere lokale Schutzmaßnahmen implementiert werden. Dazu zählen:

- Zugriffsschutz (materielle Sicherungsmaßnahmen)
- Benutzerauthentisierung
- Virenschutz
- Personal Firewall
- restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene
- lokale Verschlüsselung

Informationen hierzu findet man im IT-Grundschutzhandbuch des BSI [BSIGSH]. Im Zweifel orientiere man sich am Baustein „Internet-PC“ und wende die zugehörigen Maßnahmen sinngemäß an.

Als Schutzmaßnahme gegen das Abhören von Raumgesprächen ist ein Verbot des Einbringens von Funktechnik in den zu schützenden Raum zu empfehlen.

4.3 Rest-Risiko

Unabhängig von den beschriebenen Sicherheitsmaßnahmen sind mit der Verwendung von UWB-Systemen immer folgende Rest-Risiken verbunden:

- Das Erstellen von Bewegungsprofilen mobiler Geräte (siehe Kapitel 3.6) kann nicht verhindert werden.
- Die Bedrohung der Verfügbarkeit (siehe Kapitel 3.2) ist ebenfalls nicht vermeidbar.

5. Ausblick

Mittlerweile sind erste Prototypen für DS-UWB verfügbar. Tests der in einem „Entwickler-Kit“ genutzten Chipsätze ergaben eine nutzbare Datenrate von ca. 70 MBit/s bei 2 Meter Abstand [HaZi06]. Auch Chipsätze gemäß MB-OFDM sind in Vorbereitung. Offensichtlich versuchen die Hersteller anstelle einer Einigung auf einen gemeinsamen Standard nunmehr, ihre Produkte in den Markt zu bringen und diesen über den „besseren“ Standard entscheiden zu lassen. Die Adaption von MB-OFDM durch die Bluetooth SIG ist ein erster Schritt in Richtung eines allgemein verfügbaren Standards.

Über die zukünftige Implementierung von Sicherheitsmechanismen kann auf Grund der heute vorliegenden Prototypen keine Aussage getroffen werden.

6. Fazit

Funktechniken auf Basis von UWB (ultra-wideband) befinden sich bislang erst in der Entwicklung; serienreife Produkte sind noch nicht verfügbar. Die Standardisierung ist noch ebenso wenig abgeschlossen wie eine weltweite Regulierung ihrer Nutzung. Wegen der Vorteile des UWB-Übertragungsverfahrens (hohe Datenraten bei geringem Energieverbrauch) ist es unter anderem für zukünftige Generationen von WPAN attraktiv.

7. Literatur / Links

Die UWB-Technik befindet sich derzeit noch in einem frühen Entwicklungsstadium. Dementsprechend sucht man deutschsprachige Literatur, die eine leicht verständliche Einführung in das Thema gäbe, vergeblich. Stattdessen ist man auf Informationen in Zeitschriftenartikeln angewiesen, z.B. [HEI03] und [ZIBA05]. Eine komprimierte Beschreibung der physikalischen Schicht sowie des Medienzugangs bei MB-OFDM findet sich in [IEEE05]. Dort wird auch über Simulationsergebnisse berichtet. Ansonsten erhält man Informationen aus erster Hand in den entsprechenden Standards und Standard-Vorschlägen, z.B. [ECMA05] und [DSU04].

[BSIGSH] Grundschutzhandbuch des BSI, http://www.bsi.bund.de/gshb

[BTSIG06] Bluetooth SIG selects WiMedia Alliance Ultra-Wideband Technology For High Speed Bluetooth® Applications, Pressemitteilung der Bluetooth SIG, http://www.bluetooth.com/Bluetooth/Press/SIG/BLUETOOTH_SIG_SELECTS_WIMEDIA_ALLIANCE_ULTRAWIDEBAND_TECHNOLOGY_FOR_HIGH_SPEED_BLUETOOTH_APPLICATION.htm, März 2006

[DSU04] DS-UWB Physical Layer Submission to 802.15 Task Group 3a, ftp://ftp.802wirelessworld.com/15/04/15-04-0137-03-003a-merger2-proposal-ds-uwb-update.doc, Juli 2004

[ECMA05] High Rate Ultra Wideband PHY and MAC Standard, ECMA-368, http://www.ecma-international.org/publications/files/ECMA-ST/ECMA-368.pdf, Dezember 2005

[FCC98] Notice of Inquiry in the Matter of Revision of Part 15 of the Commission's Rules Regarding Ultra-Wideband, ET Docket No. 98-153, http://www.fcc.gov/Bureaus/Engineering_Technology/Notices/1998/fcc98208.txt, September 1998

[FCC02] New public safety applications and broadband Internet Access among uses envisioned by FCC Authorization of Ultra-Wideband-Technology, http://www.fcc.gov/Bureaus/Engineering_Technology/News_Releases/2002/nret0203.html, Februar 2002

[FCC05] Federal Comminications Commission, Part 15 of the Commission’s Rules, http://ftp.fcc.gov/oet/info/rules/part15/part15-91905.pdf, September 2005

[HaZi06] Dr. Till Harbaum, Dušan Živadinović, Weitsprung Ultrabreitbandfunk – erste Netzwerkkarten im Kurztest, c’t 7/2006, Seite 188, März 2006

[HEI03] Supermanns Röntgenblick für Notfallretter, Heise News, http://www.heise.de/newsticker/meldung/34548, Februar 2003

[IEEE05] Guido R. Hiertz, Yunpeng Zang, Jörg Habetha, Hanza Sirin, IEEE 802.15.3a Wireless Personal Area Networks - The MBOA Approach, In Proceedings of 11th European Wireless Conference 2005, Vol. 1, p.p. 204-210, April 2005

[IEEE153a] Webseite der IEEE 802.15 WPAN High Rate Alternative PHY Task Group 3a (TG3a), http://www.ieee802.org/15/pub/TG3a.htmlx

[OFC05] Ultra Wideband - An input document for discussion at the ECC TG3#11 preparation group, http://www.ofcom.org.uk/consult/condocs/uwb/uwb_statement/uwbstatement.pdf, September 2005

[ZIBA05] Dusan Zivadinovic, Oliver Bartels, Noch mehr Funk-Techniken auf dem Sprung in die Computer-Welt, c’t 2/2005, Seite 128, Februar 2005

8. Abkürzungen

4BOK	Quaternary Bi-Orthogonal Keying
AES	Advanced Encryption Standard
BPSK	Binary Phase Shift Keying
CBC	Cipher Block Chaining
CEPT	Conference European Des Administrations Des Postes Et Des Telecommunications
DCM	Dual Carrier Modulation
ECMA	European Association for standardizing Information and Communication Systems
EIRP	Equivalent Isotropically Radation Power, Strahungsleistung bezogen auf eine isotrope Antenne
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FDS	Frequency-domain spreading
FEC	Forward Error Correction
GPS	Global Positioning System
MBOA	Multiband OFDM Alliance
MB-OFDM	Multiband Orthogonal Frequency Division Multiplex
MIC	Message Integrity Code, Prüfsumme zur Integritätsprüfung
PAN	Personal Area Network
PMK	Pairwise Master Key, symmetrischer geheimer Schlüssel
PTK	Pairwise Transient Key, symmetrischer temporärer Schüssel
SFN	Secure Frame Number
TDS	Time-domain spreading
TFC	Time-Frequency Codes
USB	Universal Serial Bus
UWB	Ultra-wideband, neue drahtlose Breitband-Übertragungstechnik
WPAN	Wireless PAN

9. Glossar

Chip-Rate
: Siehe Spreizsequenz

Code-Rate
: Die Code-Rate ist ein Maß für die Redundanz, die ein FEC-Code den Nutzdaten hinzufügt und ist definiert als das Verhältnis von Informationsbits am Eingang eines Encoders zu den codierten Bits am Ausgang eines Encoders.

Faltungscode
: Ein Faltungscode ist ein spezieller FEC-Code, der sich insbesondere zur Kanalkodierung für stark störanfälligen Übertragungsmedien (z.B. drahtlose und mobile Kommunikationssysteme) eignet.

Forward Error Correction (FEC)
: Bei der Vorwärtsfehlerkorrektur kodiert der Sender die zu übertragenden Daten in redundanter Weise, so dass der Empfänger Fehler erkennen und korrigieren kann.

Orthogonal Frequency Division Multiplex (OFDM)
: OFDM ist ein Modulationsverfahren, das anstelle eines einzelnen Trägers eine große Zahl von Unterträgern gleichzeitig moduliert und parallel auf den Unterträgern (prinzipiell wie bei einer

parallelen Schnittstelle an einem PC) Daten überträgt. Die erreichbaren Datenraten hängen von der Anzahl der für die Datenübertragung verfügbaren Unterträger, von den verwendeten Modulationsverfahren auf den Unterträgern und von der Code-Rate des verwendeten FEC-Codes ab. Modulationsverfahren und Code-Rate werden oft dynamisch in Abhängigkeit von der Kanalqualität gewählt. OFDM wird beispielsweise auch in Wireless LAN verwendet.

Spreizsequenz

Bei Bandspreizverfahren wie Direct Sequence Spread Spectrum (DSSS) Code wird jedes einzelne Bit der zu übertragenden Nachricht mit einer Spreizsequenz multipliziert. Das Ergebnis ist ein Vielfaches der Spreizsequenz, das letzendlich über den Kanal übertragen wird. Hierdurch wird das Nutzdatensignal künstlich aufgeweitet, es entsteht ein „gespreiztes Spektrum“. Die Nutzbitrate ist damit stets kleiner als die Rate mit der das gespreizte Signal übertragen wird (Chip-Rate).

J. Neuere Entwicklungen

Inhaltsverzeichnis des Abschnitts

1. IEEE 802.20 – Mobile Broadband Wireless Access (MBWA)

Die Bereitstellung mobiler Breitbandnetze auf Basis drahtloser Technik wurde durch die IEEE zunächst im Rahmen der Arbeitsgruppe zu IEEE 802.16 WiMAX (Worldwide Interoperability for Microwave Access) behandelt. Der WiMAX-Standard dient dem Ziel, ein Breitbandnetz mit Metropolitan Area Network-Ausdehnung (MAN) zu schaffen. Dabei waren die Arbeiten der IEEE 802.16-Arbeitsgruppe allerdings zunächst nur auf stationäre Teilnehmer ausgerichtet. Erst im Januar 2006 folgte mit IEEE 802.16e eine Erweiterung der WiMAX-Ansätze für die mobile Nutzung.

Bereits im Dezember 2002 wurde der Zugriff auf Breitbandnetze durch drahtlose Teilnehmer (Mobile Broadband Wireless Access, MBWA) als neue Schwerpunktsetzung in eine eigene Arbeitsgruppe ausgegliedert. Diese IEEE 802.20-Arbeitsgruppe konzentriert sich seither auf die Definition einer standardisierten Luftschnittstelle, die für die Nutzung eines Breitbandangebots bei hoher Mobilität und als Basis für die Nutzung von IP-Netzwerken optimiert ist.

Schwerpunktmäßig wird auf Unterstützung solcher Netzzugänge nicht nur für Fußgänger (Fortbewegung mit ca. 3 km/h), sondern auch für höhere Mobilitätsklassen abgezielt, wobei Geschwindigkeiten bis zu 250 km/h unterstützt werden sollen. Damit zielt die Spezifikation insbesondere auf die Netzwerk-Nutzung aus Fahrzeugen ab. MBWA-Lösungen sollen unter allen Bedingungen eine ununterbrochene Konnektivität erlauben, wie man es von drahtgebundenen Systemen gewohnt ist.

Ursprünglich für Dezember 2004 geplant, ist die Fertigstellung der ersten verabschiedeten Standard-Version nunmehr für Ende 2006 vorgesehen (siehe [IEEE03]).

1.1 Grundlagen / Funktionalität gemäß IEEE 802.20

1.1.1 Technische Grundlagen

Die IEEE 802.20-Spezifikation beschreibt die grundlegenden technischen Merkmale eines MBWA-Systems, über das drahtlose Dienste für sich mit hoher Geschwindigkeit bewegende Teilnehmer zur Verfügung gestellt werden können.

MBWA ist für IP-basierte[1] Kommunikation optimiert und daher paketorientiert. Über entsprechende Quality of Service (QoS)-Mechanismen können auch Echtzeitdienste und IP-basierte Telefonie („Voice over IP“ VoIP) unterstützt werden[2]. Mit MBWA-Lösungen auf Basis von IEEE 802.20 soll weltweite Mobilität geboten werden, z.B. unter Nutzung von speziellen Lösungen wie Mobile IP. Mobile IP ermöglicht einem Teilnehmer, unter seiner ursprünglichen IP-Adresse erreichbar zu bleiben, obwohl er sich vorübergehend in einer fremden IP-Umgebung (Gastnetz) aufhält.

Das Grundmodell von IEEE 802.20 unterscheidet zwischen den folgenden Komponenten (siehe Abb. J-1):

- Access Terminal (AT): Schnittstelle mobiler Geräte zum MBWA Access Network
- Access-Netzwerk (AN): Komponenten, die den Access Terminals eine Verbindung mit einem IP-Netzwerk, typischerweise mit dem Internet, auf der Netzwerkebene (ISO-Layer 3) ermöglichen.
- Sektoren: Physikalische Kanäle zur Kommunikation zwischen AT und AN. Prinzipiell kann eine Basisstation mehrere Kanäle bereitstellen.

---

1 Wahlweise über IPv4 oder IPv6

2 Es besteht die Möglichkeit, für IP-Netze spezifizierte QoS-Steuerungsmechanismen wie Differentiated Services (DiffServ) und Resource Reservation Protocol (RSVP) geeignet abzubilden.

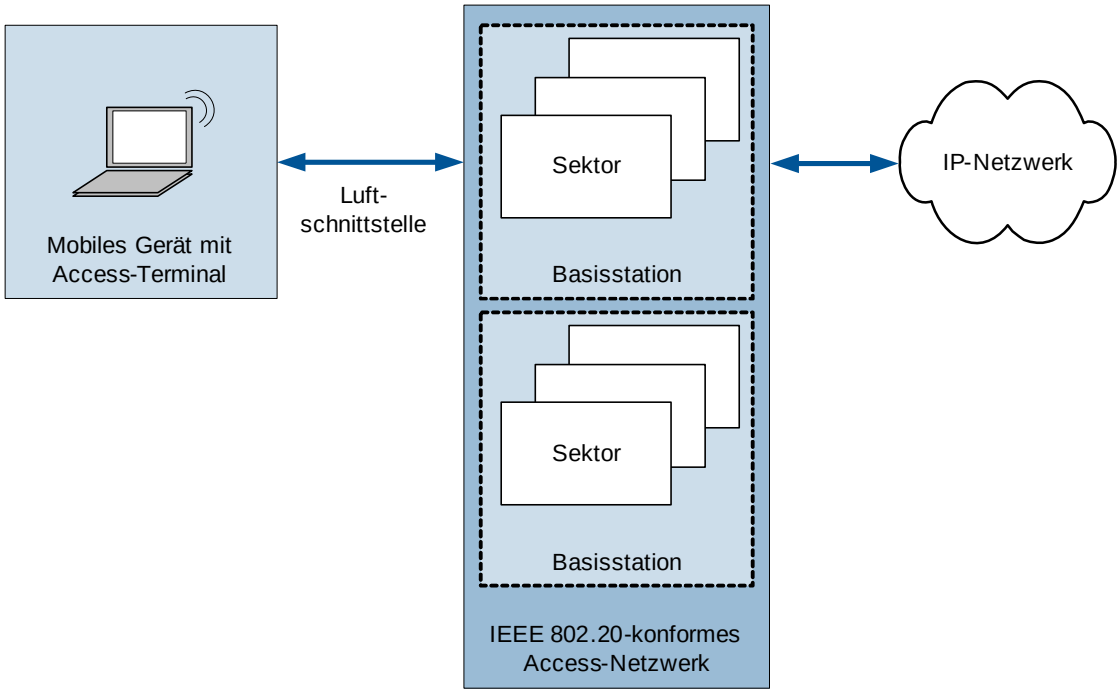


Abb. J-1: IEEE 802.20 - Referenz-Modell Netzwerk-Architektur

Implementierungen gemäß IEEE 802.20 arbeiten auf lizenzierten Frequenzen unterhalb 3,5 GHz. Derzeit gibt es zwei Vorschläge zur Implementierung von MBWA. Ein Breitbandverfahren (Wideband Mode) und eine schmalbandige Variante mit „Raummultiplexverfahren“ (625k-MC Mode).

Wideband Mode

Zur Datenübertragung wird ein breitbandiges Verfahren mit 5, 10 oder 20 MHz Bandbreite verwendet. Die Übertragung wird mittels OFDM auf so genannten Unterkanälen durchgeführt, die einen Abstand von je 9,6 kHz aufweisen. Dementsprechend stehen für die Übertragung 512, 1024 oder 2048 Unterkanäle zur Verfügung. Die Symbolrate entspricht genau dem Kanalabstand von 9,6 KHz. Bestimmte Steuerinformationen werden nicht mit dem beschriebenen OFDM-Verfahren versandt, sondern über ein Code-Multiplexverfahren (CDMA). Man will damit das Handover zwischen verschiedenen Sektoren vereinfachen, da das AT mittels CDMA gleichzeitig verschiedene Aussendungen auf derselben Frequenz unterscheiden und aufnehmen kann.

Die Modulation erfolgt je nach Qualität des Übertragungsweges mit 2- bis 64-wertigen Verfahren, entsprechend 1 bis 6 Bits pro Symbol. Zur Verbesserung der Robustheit gegen Bitfehler wird die Verwendung eines Faltungscodes (Forward Error Correction, FEC) mit Code-Raten 1/3 und 1/5 vorgeschlagen. Dabei wird die Gesamtzahl der versendeten Bits derart vergrößert, dass Redundanz entsteht.

Das Medienzugangsverfahren erfolgt entweder zeitschlitzgesteuert (Time Division Duplex, TDD) oder auf Basis eines Frequenzmultiplex-Ansatzes (Frequency Division Duplex, FDD). Beide Verfahren teilen ihre Aussendung in kurze „Rahmen“ mit vorgegebener Länge (8 Symbole) auf und ermöglichen so eine Übertragung mit vorhersagbarer Dauer.

AN und AT können jeweils mehrere Antennen einsetzen und ein MIMO-Verfahren anwenden. Dabei wird pro Antenne ein OFDM-Datenstrom auf derselben Frequenz ausgesandt. Da die Signale im Allgemeinen auf mehreren Wegen zum Empfänger gelangen (Mehrwege-Empfang) mischen sich die Symbole zeitversetzt und können, sofern sie auf Seiten des Empfängers ebenfalls von mehreren Antennen empfangen werden, mit Hilfe digitaler Signalverarbeitung wieder getrennt werden. MIMO erlaubt somit eine Vervielfachung der Übertragungsbandbreite ohne zusätzlichen Frequenzverbrauch.

Anhand von Simulationen hat man die im Wideband Mode möglichen Datenraten zu ca. 65 MBit/s in Richtung des AT und zu ca. 16 MBit/s in Richtung der Basisstation ermittelt.

625k-MC Mode

Neben den Varianten MBTDD und MBFDD ist eine Variante spezifiziert, die als MBTDD 625k-MC bezeichnet wird; zusätzlich findet man die erläuternde Bezeichnung Broadband MobilE SpaTial Wireless InterNet AccEss, kurz „BEST-WINE“. Hier wird ein mit 625 KHz vergleichsweise schmalbandiges Signal eingesetzt, das sich besonders gut für eine gerichtete Übertragung mittels „intelligenter“ Antennengruppen eignet. Durch die Verwendung solcher Richtantennen wird jeder Station ein separater Übertragungsweg bereitgestellt, der sich von den Übertragungswegen zu anderen Stationen lediglich durch die Abstrahlrichtung unterscheidet. Durch dieses so genannte Raummultiplexverfahren (Space Division Multiple Access, SDMA) wird eine hohe Ausnutzung der zur Verfügung stehenden Frequenzen erreicht. Auf derselben Sendefrequenz können mittels SDMA gleichzeitig mehrere Stationen bedient werden. Das Verfahren ist unter [ATIS05] (hier HC-SDMA genannt) näher beschrieben.

Bei MBTDD 625k-MC wird pro Kanal eine Unterteilung in drei Zeitschlitze vorgenommen. Pro Zeitschlitz lässt sich eine Datenrate von 500 KBit/s in Richtung des AT und von 190 KBit/s in Richtung der Basisstation erzielen. Es ist eine Parallelschaltung mehrerer Kanäle vorgesehen, so erreicht man beispielsweise mit 4 Kanälen downlink Datenraten von bis zu 2 MBit/s pro Slot. Die benötigte Bandbreite beträgt dann 2 MHz.

1.1.2 Protokollarchitektur

Die MBWA-Architektur gemäß IEEE 802.20 ist hinsichtlich der Protokollarchitektur bewusst mehrschichtig angelegt, obwohl sie sich auf die Layer 1 und 2 beschränkt. Neben den zuvor dargelegten Vorschriften für den physikalischen Layer (Kurzbezeichnung in der Spezifikation: PHY) existieren 3 Protokollebenen innerhalb des ISO-MAC-Layer, die unterschiedlichen Aufgaben dienen. Auf diesen Ebenen (Sublayer) wird unterschieden zwischen Transportprotokollen, die Beiträge zum Paketaufbau leisten, und reinen Steuerprotokollen. Die IEEE 802.20-Dokumente spezifizieren im Einzelnen:

- „Lower MAC Control Sublayer“ und „Lower MAC Sublayer“: Hier werden Verbindungen über die Luftschnittstelle aufgebaut und aufrechterhalten sowie die Schnittstelle zum physikalischen Layer realisiert.
- „Security Sublayer“: Er stellt die notwendigen Mechanismen zur Generierung der notwendigen Schlüssel sowie die Steuerung von Authentisierung und Verschlüsselung zur Verfügung.
- „Session Control Sublayer“: Er enthält die Intelligenz zur Steuerung der Datenkommunikation und verwaltet eindeutige, virtuelle Adressen für den Versand gerichteter Pakete (Unicast Access Terminal Identifier UATI). Darüber hinaus handelt er Protokolle aus und implementiert Dienste zur Statusverwaltung.
- „Convergence Sublayer“: Diese Ebene stellt insbesondere die Schnittstelle zum ISO Layer 3 und damit entsprechend der eindeutigen Ausrichtung von IEEE 802.20 zum Internet Protocol IP dar.

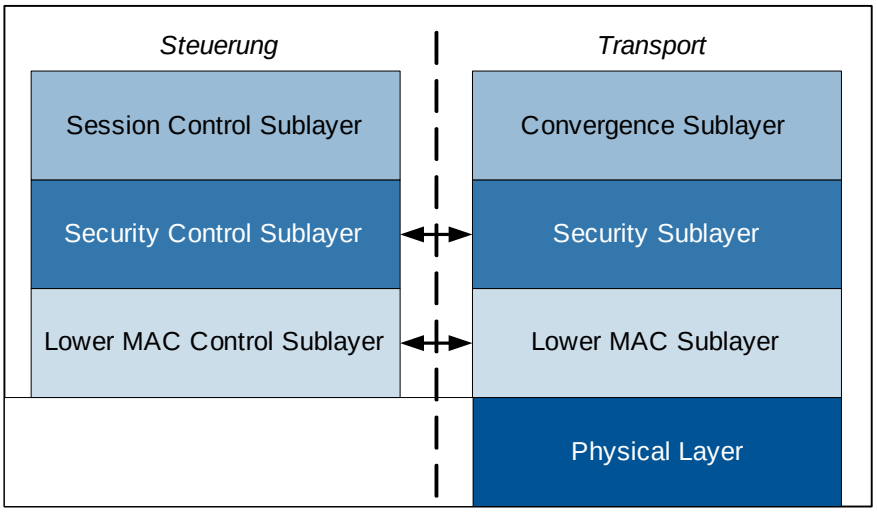


Abb. J-2: In IEEE 802.20 spezifizierte Protokolle und ihre Schichtung

Jeder (Sub-)Layer kann ein oder mehrere Protokolle bzw. Transportmechanismen mit zugehörigen Nachrichten-Formaten und Paket-Headern umfassen.

1.2 Sicherheitsmechanismen von IEEE 802.20

1.2.1 Temporäre Adressierung

Ein mit einem Access Network über die IEEE 802.20-Luftschnittstelle verbundenes Gerät besitzt drei Adressen auf Layer 2:

- Universal Access Terminal Identifier UATI: Ein UATI ist eine temporäre 128 Bit-Adresse, die dem Access Terminal vom AN (durch den Session Control Sublayer) zugeordnet wird. Hierüber wird das Access Terminal gezielt angesprochen (Unicast-Adresse). Die UATI wird ausdrücklich nicht aus einer Hardware-Adresse abgeleitet. Die UATI dient der „systemweiten“ Identifikation eines Geräts mit IEEE 802.20-Access Terminal, d.h. gilt Sektoren-übergreifend und ist netzwerkweit eindeutig.
- MAC ID: Über die 11 Bit-lange MAC ID wird ein Access Terminal innerhalb eines einzelnen Sektors eindeutig identifiziert und angesprochen. Ein mobiles Gerät mit IEEE 802.20-Access Terminal erhält somit eine MAC ID je Sektor, in dem es aktiv ist. Eine MAC ID ist nur innerhalb eines Sektors eindeutig. Auch die MAC ID wird unabhängig von der Gerätehardware erzeugt.
- Hardware-Adresse gemäß IEEE EUI-48 oder IEEE EUI-64: Diese wird dem Access-Terminal vom Hersteller im Zuge des Fertigungsvorgangs mitgegeben. Die Hardware-Adresse kann zur Verwaltung von Geräteinformationen durch das Netzwerk mit einem speziellen Befehl ausgelesen werden, dies aber nur über einen verschlüsselten Kanal nach Etablierung der vollen verfügbaren Systemsicherheit.

Die Kommunikation mit einem AT erfolgt somit ausschließlich über temporäre Adressen. Im Hinblick auf die potentielle Erstellung von Bewegungsprofilen ist dies als ein Sicherheitsmechanismus zu werten.

1.2.2 Kryptographische Sicherheitsmechanismen

Als funkbasiertes Verfahren ist IEEE 802.20 der Möglichkeit ausgesetzt, dass unbefugte Dritte unter Verwendung entsprechender Technik die MBWA-Kommunikation mithören bzw. den Versuch unternehmen, sich aktiv in Kommunikationsverbindungen einzuschalten.

Die IEEE 802.20-Spezifikation sieht zur Behandlung dieser Bedrohung innerhalb der mittleren MAC-Ebene (Security Control Sublayer und Security Sublayer) vor, die Datenübertragung zu verschlüsseln sowie über Prüfung der Authentizität eines Pakets die Integrität der Übertragungsinhalte zu sichern.

Die vorgesehenen Elemente der Sicherheitsschicht sind:

- Integritätssicherung für Pakete basierend auf dem durch die IETF in RFC 2104 spezifizierten HMAC-Algorithmus [HMARFC] sowie der SHA-256-Spezifikation (Secure Hash Algorithm) in [FIPS180-2]. Mit Hilfe des HMAC-Algorithmus wird die Authentizität eines Pakets auf Basis einer kryptographischen Hash-Funktion sichergestellt. Je nach Kontext werden im Falle der IEEE 802.20-Spezifikation hier verschiedene Schlüssel genutzt:
  - ein 128 Bit-langer MIC Key (für: Message Integrity Check) in der Phase eines als „Key Exchange“ bezeichneten vier-Wege-Handshake (s.u.)
  - im Weiteren ein 128 Bit-langer Authentication Key (für Nutzdaten- und Kontrollpakete mit Steuerinformationen, nach erfolgreichem Key Exchange)
- Verschlüsselung von Paketinhalten auf Basis des AES-128 Standards. Der dazu genutzte Schlüssel wird als „Encryption Key“ bezeichnet.

MIC Key, Authentication Key und Encryption Key werden aus einem so genannten Session Key abgeleitet. Grundlage für die Erzeugung des Session Key ist ein symmetrischer geheimer Schlüssel (Pairwise Master Key, PMK). Die IEEE 802.20-Spezifikation setzt die Existenz eines solchen PMK bei Access-Terminal und Access-Netzwerk voraus. Ein Schlüsselmanagement ist nicht spezifiziert; es wird lediglich auf „Aushandlung durch Protokolle höherer Layer“ verwiesen.

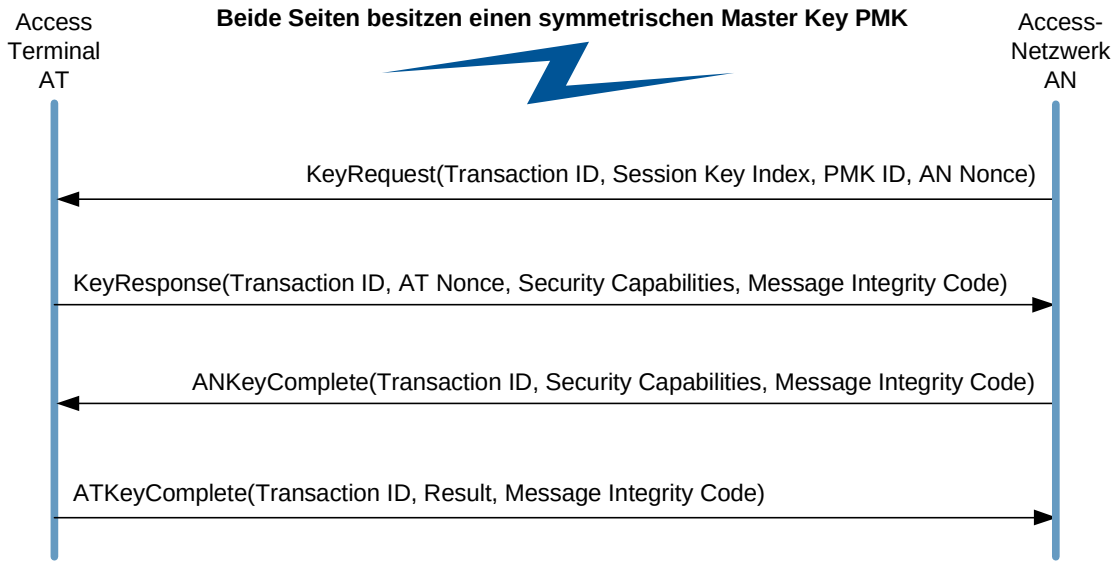


Abb. J-3: „4-Way-Key Exchange“ bei IEEE 802.20[3]

Verbindlich ist dagegen ein 4-Way-Key-Exchange wie in Abb. J-3 dargestellt. Es ähnelt dem gleichnamigen Verfahren bei Wireless LAN und ermöglicht das Generieren des Session Key, ohne dass

[3] Im Bild und innerhalb der folgenden Detailbeschreibung ist in der Praxis als „Access-Netzwerk“ letztlich die Basisstation zu sehen, über die als Zugangspunkt das Gerät mit betrachteter Access-Terminal-Implementierung die Erstverbindung zum Access-Netzwerk aufnimmt.

dieser zwischen den Stationen übertragen werden müsste. Das Verfahren dient gleichzeitig zur gegenseitigen Authentisierung von AT und AN.

Zu diesem Zweck tauschen AT und AN je eine Zufallszahl (AN Nonce bzw. AT Nonce) aus. Beide Stationen bilden unter Zuhilfenahme der beiden Zufallszahlen, dem PMK sowie nicht näher beschriebener Protokollinformation eine 384 Bit lange Pseudozufallszahl, die als Session Key dient. Sofern beide PMK identisch sind, gilt dies auch für den Session Key.

1.2.3 Sicherheitsbetriebsarten

Es werden zwei grundlegende Arbeitsmodi unterschieden:

- Modus ohne Security-Mechanismen
- „SecurityEnabled“-Modus.

Wird nicht der SecurityEnabled-Modus genutzt, fallen in den gesendeten Paketen Security-spezifische Teile weg, die vom Security Sublayer für Authentisierung bzw. Integritätssicherung benötigt werden, und die durch IEEE 802.20 spezifizierte Verschlüsselung kann nicht eingesetzt werden.

Der „SecurityEnabled“-Modus erlaubt beliebige Kombinationen der Sicherheitselemente Verschlüsselung und Integritätssicherung:

- Integritätssicherung, keine Verschlüsselung
- keine Integritätssicherung, Verschlüsselung
- Integritätssicherung, Verschlüsselung.

1.3 Gefährdungen bei der Nutzung von IEEE 802.20-Geräten

Zu all den Gefährdungen, denen leitungsgebundene Netzwerke ausgesetzt sind (siehe [GSHB]), ergeben sich bei der Nutzung von Funknetz-Technik zusätzliche Gefährdungen, die insbesondere auf eventuellen Sicherheitsschwächen der verwendeten Protokolle sowie auf der unkontrollierten Ausbreitung der Funkwellen basieren. Im Folgenden werden Überlegungen zur Gefährdungslage im Vorgriff auf die noch kommende Technik diskutiert.

1.3.1 Schwächen im Sicherheitskonzept des Standards

Bei den nachfolgenden Betrachtungen handelt es sich zurzeit noch um theoretische Gefährdungen. Zwar existieren Vor-Standard-Implementierungen von IEEE 802.20-artigen Lösungen, die sich jedoch vor allem auf die Optimierung der Signalisierung und ähnliche Aspekte konzentriert haben. Inwieweit der Gedanke der „Benutzerfreundlichkeit“ bzw. einer Minimierung des Herstellungsaufwands und resultierenden Preises womöglich zu unsicheren Produktlösungen führen wird, bleibt abzuwarten.

Die Nutzung des SecurityEnabled-Modus als Betriebsart ist nicht zwingend.

Eine Verschlüsselung bzw. Integritätssicherung für Pakete nach erfolgtem 4 Wege-Key Exchange ist nicht vorgeschrieben.

Grundsätzlich ist es möglich, mit der Sicherheitsbetriebsart SecurityEnabled wahlweise auf Verschlüsselung oder Integritätssicherung via paketweiser Authentizitätsprüfung zu verzichten.

Ausschlaggebend für das erreichte Sicherheitsniveau ist daher entweder eine pauschale Aktivierung beider Funktionalitäten als Standardeinstellung oder eine explizite Beantragung der Nutzung dieser beiden Sicherheitsoptionen durch die Anwendungen.

Unsichere Voreinstellungen sind nicht grundsätzlich ausgeschlossen.

Ähnlich wie bei anderen Lösungen zur drahtlosen Kommunikation muss auch im Falle von zukünftigen IEEE 802.20-Implementierungen damit gerechnet werden, dass ab Werk nicht „SecurityEnabled“

als Standardeinstellung (vorbehaltlich gezielter Abschwächung durch die einzelne Applikation) eingerichtet wird.

„Unsichere“ Lösungen der Verwaltung des PMK sind nicht ausgeschlossen.

Die konkret gewählte Methode zur „Aushandlung“ des PMK wird höheren Protokollschichten zugeordnet und offen gelassen. Die entsprechende Formulierung im Standard-Entwurf kann von Herstellern auch so ausgelegt werden, dass an Stelle automatisierter, abgesicherter Schlüsselverwaltung und -verteilung eine Schlüsseleingabe von Hand, etwa durch den Nutzer eines mobilen Geräts vorgesehen wird, was bekanntlich zu typischen Benutzerfehlern (schwache Schlüssel) führen kann.

1.3.2 Unkontrollierte Ausbreitung der Funkwellen

Die Funkwellen der MBWA-Komponenten breiten sich auch über räumliche Grenzen ihres Nutzungsbereichs aus. Dabei kann auch in nicht vom Betreiber kontrollierten Bereichen ein Empfang möglich sein. Je nach Umgebungsbedingungen und Leistungsfähigkeit der verwendeten Empfangsgeräte (z.B. Richtantennen) besteht auch hier noch eine konkrete Abhörgefahr.

1.3.3 Bewegungsprofile

Beim Einsatz von Funktechniken lassen sich prinzipiell Bewegungsprofile mobiler Teilnehmer erstellen. MBWA-Lösungen gem. IEEE 802.20 erschweren die Identifikation des beobachteten Geräts dadurch, dass die benutzten Adressen temporärer Natur sind und in keinem Zusammenhang zur Hardware-gebundenen Adresse stehen.

Ein rein passives Belauschen und Auswerten der IEEE 802.20-Header reicht daher zur Erstellung von Bewegungsprofilen nicht, sondern muss mit anderen Formen der unberechtigten Informationsbeschaffung kombiniert werden, um die temporären Layer 2-Adressen mit einem bestimmten Gerät in Verbindung bringen zu können.

1.3.4 Verfügbarkeitsprobleme

Die Verfügbarkeit kann unter anderem durch folgende Ursachen beeinträchtigt werden:

- ► Störung durch gezielt eingesetzte Störsender (Jammer).
- ► Denial-of-Service, zum Beispiel Angriffe auf die Energiereserven einzelner Geräte durch Abhalten vom Idle-Modus. Sofern nicht im SecurityEnabled-Modus die Authentizität entsprechender Pakete verifiziert wird, sind solche Angriffe prinzipiell denkbar.
- ► Mechanische Anfälligkeit intelligenter Antennen, die in miniaturisierter Form vom Anwender an mobilen Geräten in der Tasche transportiert werden.

1.3.5 Implementierungsschwächen

Wird IEEE 802.20-basierende Technik in ausreichendem Umfang angeboten und auch vom Markt angenommen, steigt auch die Wahrscheinlichkeit, dass Fehler in den Implementierungen einzelner Hersteller bekannt werden und schließlich für Angriffe ausgenutzt werden.

Der Nimbus der für potenzielle Angreifer mangels Verbreitung eher uninteressanten Technik wird beizeiten verloren gehen und damit das Risiko der Entwicklung gezielter Angriffsmethoden steigen.

1.3.6 Weitere Sicherheitsaspekte

Folgende Aspekte sind ebenfalls zu bedenken:

- ► Mobile Geräte sind gegenüber stationären Geräten einem höheren Diebstahlrisiko ausgesetzt.

► Das mobile Gerät authentisiert sich gegenüber dem Access-Netzwerk. Inwieweit eine Authentisierung eines Benutzers gegenüber dem Gerät notwendig ist, entscheidet der Hersteller. Es ist damit zu rechnen, dass mit dem Argument „Benutzerfreundlichkeit“ auf eine solche benutzerbezogene Authentisierung vor Zugriff auf das Gerät verzichtet wird. Bei Abhandenkommen mobiler Geräte sind diese leicht durch unbefugte Dritte zur Kommunikation oder zum Auslesen von lokal gespeicherten Informationen (z.B. des PMK) nutzbar.

1.4 Schutzmaßnahmen

Die nachfolgend benannten Schutzmaßnahmen basieren auf den bislang noch theoretischen Gefährdungsbetrachtungen. Eine Ergänzung bzw. Verschärfung kann notwendig werden, sobald nach Verabschiedung des Standards entsprechende Implementierungen konkrete Schwachstellen und hierauf abzielende Angriffsformen offenbaren.

IEEE 802.20-Geräte, die mindestens einen Dienst mit Schutzbedarf anbieten, sollten Verschlüsselung und Integritätssicherung unterstützen. Leicht kompromittierbare Formen zum Umgang mit dem PMK sind zu vermeiden. Außerdem müssen die Geräte in geeigneter Weise abgesichert werden. Im Folgenden wird beschrieben, welche Maßnahmen grundsätzlich ergriffen werden können.

Eine Benennung von Rest-Risiken ist nur bedingt möglich, da mögliche Schwachpunkte wie ungünstige Implementierung durch einen Hersteller oder sorgloser Umgang durch einen Nutzer mangels verfügbarer Produktrealisierungen noch nicht abschließend bewertet werden können.

1.4.1 Absicherung von IEEE 802.20-Geräten

Gezielte Produktauswahl

Nach Möglichkeit sollten keine Geräte eingesetzt werden, die mit Methoden zur Verwaltung des PMK arbeiten, die sich anderweitig bereits als problematisch herausgestellt haben.

Ab Werk erfolgte schwache Voreinstellungen sollten überschrieben werden können.

Einspielen von Sicherheitspatches

Von den Geräteherstellern bereitgestellte Sicherheitspatches bzw. eine aktuellere Version der Firmware sollten nach Test und bei Bedarf eingespielt werden.

Allgemeine Konfiguration

Grundsätzlich ist es empfehlenswert, die vom Hersteller voreingestellte Konfiguration auf Schwachstellen zu überprüfen und nötigenfalls zu ändern. Es ist mit üblichen, bei anderen Lösungen zur drahtlosen Kommunikation bereits zu beobachtenden Schwächen zu rechnen. Diesen sollte nach Möglichkeit gezielt begegnet werden, beispielsweise:

► Eine ab Werk eingestellte automatische Aktivierung möglichst vieler Dienste sollte unterbunden werden. Nicht benötigte Dienste sollten gezielt abgestellt werden.

► Die MBWA-Schnittstellen der Geräte sollten bei Nichtbenutzung deaktiviert werden.

► Falls die Sendeleistung variabel ist, sollte sie so niedrig wie möglich und so hoch wie für die Funktionalität erforderlich eingestellt werden. Sofern konfigurierbar, sollte für den Idle-Status ein zur typischen Erreichbarkeits-Dringlichkeit passender Paging-Zyklus eingestellt werden.

► Als Standardbetriebsmodus sollte SecurityEnabled eingestellt werden.

► Bei Verlust/Diebstahl eines mobilen (bzw. stationären) Gerätes sollte nach Möglichkeit die Löschung aller entsprechenden Schlüssel, inklusive PMK, veranlasst werden.

1.4.2 Weitere Schutzmaßnahmen

Generell sind alle Gefährdungen zu berücksichtigen, die für IP-basiert kommunizierende Geräte anfallen (man siehe hierzu insbesondere [BSIGSH]).

Über die in Kapitel B.4.1 genannten Maßnahmen hinaus sollten bei Verfügbarkeit von IEEE 802.20-basierten Geräten – falls dies technisch möglich ist – weitere lokale Schutzmaßnahmen berücksichtigt werden, z.B.

- ► Zugriffsschutz (materielle Sicherungsmaßnahmen)
- ► Benutzerauthentisierung
- ► Virenschutz
- ► Personal Firewall
- ► restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene
- ► lokale Verschlüsselung

Informationen hierzu findet man im IT-Grundschutzhandbuch des BSI [BSIGSH]. Im Zweifel orientiere man sich am Baustein „Internet-PC“ und wende die zugehörigen Maßnahmen sinngemäß an.

1.4.3 Rest-Risiko

Unabhängig von den beschriebenen Sicherheitsmaßnahmen sind mit der Verwendung zukünftiger IEEE 802.20-Geräte grundsätzlich immer folgende Rest-Risiken verbunden:

- ► Das Erstellen von Bewegungsprofilen mobiler Geräte (siehe Kapitel 1.3.3) kann nicht vollständig verhindert werden, sofern es einem Angreifer gelingt, über unbefugt erlangte Zusatzinformationen einen Zusammenhang zwischen den temporären Adressen (MAC ID, UATI) und dem zugehörigen Gerät herzustellen.
- ► Die Gefährdung der Verfügbarkeit (siehe Kapitel 1.3.4) ist nicht vollständig vermeidbar. Zwar erschweren die vorgesehenen Security-Funktionalitäten Angriffe über gezielte Pakete an die Adresse eines IEEE 802.20-Gerätes, und bei Verwendung intelligenter Antennentechnik, welche die Richtung des eingehenden Signals berücksichtigt, werden solche Pakete womöglich ausgefiltert. Ein genügend starker Störsender, der die Signale gewollter Kommunikation zwischen Access-Terminal und Access-Netzwerk überlagert, ist jedoch als Angriffsform gegen drahtlose Übertragung niemals völlig auszuschalten.

1.5 Ausblick

Inwieweit IEEE 802.20 tatsächlich praxisrelevant wird, hängt von verschiedenen Faktoren ab. Je nach angestrebter Nutzungsweise mobiler Geräte stehen verschiedene Alternativen als Konkurrenz im Raum, etwa die mobile Variante von WiMAX (IEEE 802.16e) oder Mobilfunktechnologien der dritten Generation.

Kommt der endgültige Standard nochmals verspätet, oder favorisieren die Produkthersteller im Bereich drahtloser Technik andere Lösungen und gehen eine Implementierung von IEEE 802.20 zögerlich an, so werden durch entsprechende Investitionen (Netzwerk-Betreiber) bzw. Sättigung des Markts Tatsachen geschaffen. Auch gegebenenfalls nachweislich vorhandene konzeptionelle und technische Vorteile von IEEE 802.20, etwa im Bereich der Sicherheit, würden hieran nichts zugunsten einer IEEE 802.20-Akzeptanz ändern.

Zum Teil sind die Auswirkungen der Herstellerstrategie auf die Einführungswahrscheinlichkeit schon in der Entstehungsgeschichte des Standards sichtbar. Die Verzögerung der Standardisierung um volle zwei Jahre ist mindestens zum Teil auf solche Einflüsse zurückzuführen.

Andererseits ist eine schnelle Umsetzung des Standards nach seiner Verabschiedung durch erste Produkte durchaus möglich, da für wesentliche Elemente der Konzeption bereits Vor-Standard-Lösungen existieren. Das Argument, der Standard komme in jedem Fall zu spät, kann also so pauschal nicht gelten gelassen werden.

1.6 Fazit

Noch ist MBWA auf Basis von IEEE 802.20 nicht verfügbar, und es können nur die Konzepte und Inhalte der Spezifikation bewertet werden.

Das Arbeiten mit einer MAC-Zwischenschicht, die Authentisierung, Verschlüsselung und Integritätssicherung für das einzelne Paket anbietet, ist zu begrüßen. Die hierzu verwendeten Methoden und kryptographischen Algorithmen sind etabliert und mit den vorgesehenen Schlüssellängen nach derzeitigem Stand auch geeignet, um hohem Schutzbedarf zu genügen.

Eine wesentliche Stärke in diesem Zusammenhang besteht neben den bereits erwähnten Sicherheitsfunktionalitäten in der Tatsache, dass die verwendeten Adressen temporärer Natur sind, also keinen unmittelbaren Rückschluss auf die Identität eines für einen Angreifer potentiell interessanten Geräts ermöglichen.

Nicht geklärt ist bisher die Verwaltung des geheimen Schlüsselmaterials. Die von einer MBWA-Lösung garantierte Sicherheit wird im Wesentlichen davon abhängen, wie der symmetrische Schlüssel PMK auf mobiles Gerät und Access Network verteilt wird.

1.7 Literatur / Links

Neben Veröffentlichungen der Hersteller, die vor-Standard-Implementierungen vorgenommen haben, sind entsprechend dem Status eines „Standards in Entwicklung“ (emerging standard) im Wesentlichen die Veröffentlichungen der zugehörigen IEEE-Arbeitsgruppe zu nennen. Eine vollständige Übersicht der allgemein zugänglichen Beiträge von Mitgliedern der jeweiligen Arbeitsgruppe findet sich unter [IEEE01] bzw. [IEEE02].

Weitere Literaturhinweise benennen Quellen mit überblicksartigem Inhalt oder Hintergrundliteratur.

Die Liste der hier aufgeführten Titel und Links stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

[ATIS05] High Capacity – Spatial Division Multiple Access (HC-SDMA) radio interface standard (ATIS-0700004-2005) for wireless wideband access, Alliance for Telecommunications Industry Solutions, http://www.atis.org, September 2005

[FIPS180-2] Federal Information Processing Standards Publication 180-2

[GSHB] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutzhandbuch – Standard-Sicherheitsmaßnahmen“, verfügbar unter http://www.bsi.bund.de/gshb

[HMARFC] RFC 2104 (informational)
“HMAC: Keyed-Hashing for Message Authentication”, Feb. 1997

[IEEE01] IEEE 802.20 Mobile Broadband Wireless Access (MBWA), “Contributions”
www.ieee802.org/20/Contributions.html

[IEEE02] IEEE 802.20 Mobile Broadband Wireless Access (MBWA),
“Working Group Permanent Documents / Working Group Documents”
http://www.ieee802.org/20/Documents.htm

[IEEE03] IEEE 802.20 Project Development Plan- 802.20-PD-07R1
www.ieee802.org/20/P_Docs/IEEE%20802.20%20PD-07r1.ppt, Nov. 2004

[IEEE04] Jim Tomcik, Radhakrishna Canchi:
MBFDD and MBTDD: Proposed Draft Air Interface Specification
www.ieee802.org/20/Contribs/C802.20-06-04.pdf, 06. Jan. 2006

[IEEE05] Jim Tomcik :
MBFDD and MBTDD Wideband Mode: Technology Overview
http://www.ieee802.org/20/Contribs/C802.20-05-68r1.pdf; 06. Jan. 2006

[IEEE06] System Requirements for IEEE 802.20 Mobile Broadband Wireless Access Systems – Version 14
http://www.ieee802.org/20/P_Docs/IEEE%20802.20%20PD-06r1.doc, 16. Jul. 2004

[IEEE07] Jim Tomcik:
MBTDD Wideband Mode Requirements Compliance Report
http://www.ieee802.org/20/Contribs/C802.20-05-65r1.pdf, 06. Jan. 2006

[IEEE08] Jim Tomcik:
MBFDD Requirements Compliance Report
http://www.ieee802.org/20/Contribs/C802.20-05-60r1.pdf

[IEEE09] Radhakrishna Canchi:
MBTDD 625k-MC *(BEST-WINE) System Requirements Compliant Report
http://www.ieee802.org/20/Contribs/C802.20-05-76r1.pdf, 06. Jan. 2006

[KACT05] Dr. Thomas Kaiser: Rudelfunk – Antennengruppen verbessern Funkverbindungen
c't 8/2005

1.8 Abkürzungen

625k-MC	625kiloHertz-spaced MultiCarrier
AES	Advanced Encryption Standard
AN	Access Network
AT	Access Terminal
BEST-WINE	Broadband MobilE SpaTial Wireless InterNet AccEss
BSI	Bundesamt für Sicherheit in der Informationstechnik
CDMA	Code Division Multiple Access
DiffServ	Differentiated Services
EUI-48	48-Bit Extended Unique Identifier
EUI-64	64-Bit Extended Unique Identifier
FDD	Frequency Division Duplexing
FEC	Forward Error Correction
FIPS	Federal Information Processing Standards
HC-SDMA	High Capacity-Space Division Multiple Access
HMAC	(keyed)Hash Message Authentication Code
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
MAC	Media Access Control

MAC ID	Media Access Control Identification
MAN	Metropolitan Area Network
MBFDD	Mobile Broadband Frequency Division Duplex
MBTDD	Mobile Broadband Time Division Duplex
MBWA	Mobile Broadband Wireless Access
MIC	Message Integrity Check
MIMO	Multiple Input - Multiple Output
OFDM	Orthogonal Frequency Division Multiple Access
QoS	Quality of Service
PHY	Kurzbezeichnung für den physikalischen Layer in der Spezifikation
PMK	Pairwise Master Key
RFC	Request for Comment, Veröffentlichung der Internet Engineering Task Force
RSVP	Resource Reservation Protocol
SDMA	Space Division Multiple Access
SHA	Secure Hash Algorithm
TDD	Time Division Duplex
UATI	Unicast Access Terminal Identifier
VoIP	Voice over IP
WiMAX	Worldwide Interoperability for Microwave Access

1.9 Glossar

Advanced Encryption Standard (AES)
: Symmetrisches Verschlüsselungsverfahren mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit. AES bietet ein sehr hohes Maß an Sicherheit. Das Verfahren wurde eingehenden kryptoanalytischen Prüfungen unterzogen.

Authentisierung
: Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Gerätes. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist i. A. keine sinnvolle Autorisierung möglich.

Code Division Multiple Access (CDMA)
: Beim Codemultiplexverfahren werden die Daten mehrerer Quellen oder Sender gleichzeitig auf derselben Frequenz übertragen. Die Unterscheidung der Signale erfolgt anhand einer pro Quelle eindeutigen Kodierung mit einer binären Sequenz, deren Bitrate (hier Chip-Rate genannt) ein Vielfaches der Datenrate beträgt.

Denial of Service (DoS)
: Ein Angriff vom Typ Denial of Service hat zum Ziel die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr („Dummy Traffic“) oder die beabsichtigte Herbeiführung eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Forward Error Correction (FEC)
: Bei der Vorwärtsfehlerkorrektur kodiert der Sender die zu übertragenden Daten in redundanter Weise, so dass der Empfänger Fehler erkennen und korrigieren kann.

Frequency Division Duplexing (FDD)
: Die Informationen werden für jede Richtung mit Hilfe einer anderen Trägerfrequenz übertragen. Dadurch wird ermöglicht, dass ein Gerät gleichzeitig senden und empfangen kann.

Message Integrity Check (MIC)
: kryptographischer Integritätsschutzmechanismus

Orthogonal Frequency Division Multiple Access
: Modulationsverfahren, das statt eines einzelnen Signalträgers eine große Zahl von Subträgern gleichzeitig moduliert. Jeder einzelne Träger ist phasen- und amplitudenmoduliert und kann daher die Information von mehreren Bits pro Symbol tragen.

Time Division Duplexing (TDD)
: Sende- und Empfangskanal nutzen die gleiche Frequenz sind aber zeitlich voneinander getrennt. Die Informationen werden mit Hilfe eines festgelegten Zeitgebers in kurzen Sequenzen zeitversetzt übertragen. Das Umschalten zwischen Sende- und Empfangsmodus geschieht so schnell, dass dem Nutzer die kurzzeitige Unterbrechung des Kanals nicht auffällt.

2. IEEE 802.21 – Media Independent Handover (MIH)

Nach erfolgreicher Beantragung zur Einsetzung der IEEE 802.21-Arbeitsgruppe im November 2003 hat diese im März 2004 die Arbeit aufgenommen. Ziel der Arbeitsgruppe ist die Spezifikation einer Möglichkeit zum Wechsel zwischen unterschiedlichen Netzwerk-Medienzugängen ohne Verlust der Sitzungen auf Nutzerebene. Ein derartiger Medien-unabhängiger Netzwechsel („Media Independent Handover“, MIH) soll prinzipiell zwischen verschiedensten Layer 1 / 2- Lösungen möglich sein, unabhängig davon, ob diese auf IEEE Standards basieren oder nicht. Ebenso soll ein Wechsel unabhängig davon möglich sein, ob das vernetzte Gerät mobil oder stationär eingesetzt wird.

Der Standard ist noch nicht verabschiedet. Gemäß ursprünglicher Zeitplanung soll eine vollständige Version im Mai 2006 zur abschließenden Revision eingereicht werden.

2.1 Grundlagen

Die grundlegende Aufgabenstellung für die IEEE 802.21-Spezifikation besteht darin, einen nahtlosen Medienwechsel auf Layer 1 / 2 zu erlauben, ohne dass hierdurch der Nutzer eines vernetzten Gerätes gezwungen ist, die Verbindungen zu von ihm genutzten Diensten neu zu etablieren.

Es ist nicht notwendig, dass der „nahtlose“ Medienwechsel für den Nutzer unbemerkt vonstatten geht. Jedoch sollen negative Übergangseffekte wie Datenverluste und Pausenzeiten minimiert werden, ohne dass der Nutzer des Geräts eingreifen muss.

Soweit genutzte Anwendungen QoS-Anforderungen aufweisen, soll die Möglichkeit bestehen, auf dasjenige verfügbare Netzwerk zu wechseln, mit dem diesen Anforderungen am ehesten entsprochen werden kann. Die in diesem Sinne notwendigen Funktionalitäten von IEEE 802.21 müssen insbesondere umfassen:

- Ermittlung verfügbarer Netzwerke im Bereich eines zu vernetzenden Geräts
- Gewinnung und Verwaltung von Informationen über die unterstützten Leistungsmerkmale je Netzwerk
- einheitliche Repräsentierung verschiedener Layer 1 / 2-Lösungen gegenüber den höheren Protokollschichten
- Erkennen der Notwendigkeit zum Netzwerk-Wechsel bei entsprechenden auslösenden Ereignissen

Zur Realisierung dieser Funktionalitäten beschreibt die IEEE 802.21-Spezifikation eine Art Zwischenschicht zwischen physikalischem Netzwerk und dessen Aktivierung („Data Link“) und Layer 3 bis 7. Beispielsweise wird im Falle eines Gerätes, das IP-basiert auf Grundlage eines IEEE 802.3-Netzwerks kommuniziert, eine IEEE 802.21-spezifische Zwischenschicht zwischen IP-Stack und Ethernet-

Kartentreiber einzufügen sein. Die Übergabepunkte der IEEE 802.21-Implementierung nach unten bzw. oben werden als Service Access Points (SAPs) bezeichnet, im Einzelnen als MIH_Link_SAP bzw. MIH_SAP.

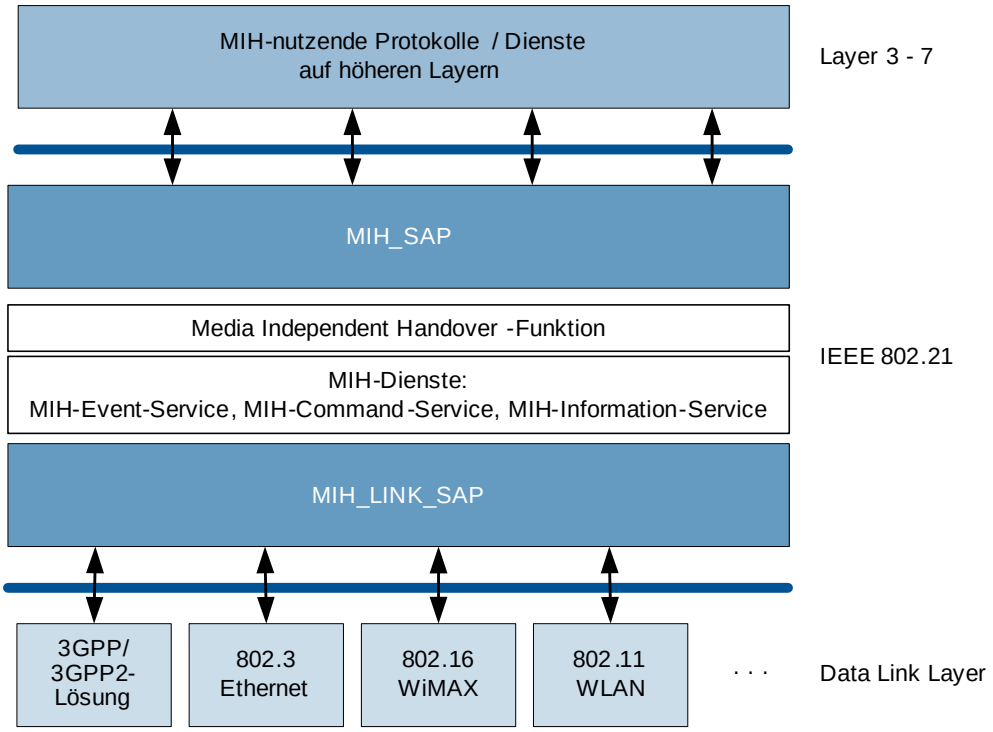


Abb. J-4: Generelles MIH-Referenzmodell bei IEEE 802.21

Die IEEE 802.21-Spezifikation beschreibt Funktionsweise, genutzte Nachrichtentypen und Kommandos in abstrakter Weise, macht aber gezielt keine weiteren Vorgaben für die Implementierung und nennt auch keine Präferenzen in diesem Sinne. Hier sind die Hersteller zukünftiger Lösungen gefragt.

Die notwendigen, im Referenzmodell bereits ersichtlichen IEEE-802.21-Dienste sind wie folgt zu charakterisieren:

- Media Independent Event Services (MIES): Die Spezifikation zu MIES definiert Ereignisse (Events) und Funktionen zur Reaktion auf diese. Ein Ereignis kennzeichnet eine Veränderung der Situation, die eine Revision der derzeitigen Netzwerkwahl nahe legt, diese erforderlich macht bzw. ihren Vollzug abschließt (Link up, Link down, Wechsel bei Leistungsparametern eines Links, Entdecken eines neuen Link, d.h. einer Netzwerk-Alternative, Verschlechterung des Zustands einer Layer 2-Verbindung mit drohendem Verlust, Abreißen einer Layer 2-Verbindung usw.).
- Media Independent Command Services (MICS): Die MICS steuern das Umsetzen von Kommandos, die über die MIH_SAP-Schnittstelle von höheren Protokollen und Diensten entgegen genommen werden. Die Liste der in der Spezifikation vorgesehenen Kommandos umfasst Statusabfragen, das Veranlassen eines Medienwechsels, konfigurierende Eingriffe auf den Data Link Layer und Schritte zur Begleitung des Medienwechsels.
- Media Independent Information Service (MIIS): Der MIIS ist die tragende Komponente der entstehenden Netzarchitekturen. Hier werden alle Informationen zusammengeführt und verwaltet, über die vorhandene Netze und ihre Zustände bzw. Merkmale beschrieben werden und gezielt als Kandidaten für aktive Verbindungen geprüft werden können. So lassen sich beispielsweise Informationen über die Betreiber eines Netzes, Roaming-Vereinbarungen und Kosten ermitteln, aber auch über die von einem Netz zur Verfügung gestellten Sicherheitsmechanismen.

2.2 Sicherheitsmechanismen gemäß IEEE 802.21

Spezielle Sicherheitsmechanismen sieht der Standard-Entwurf in der im März 2006 verfügbaren Version nicht vor. Eine Absicherung von Verbindungen zu Netzwerken vor dem vollständigen Verbindungsaufbau wird als nicht praktikabel eingestuft. Es wird auf eine Absicherung im Rahmen der beteiligten Netzwerk-Lösungen verwiesen. Der Media Independent Information Service nennt bereits vor dem Verbindungsaufbau zu einem Netz dessen unterstützte Sicherheitsmechanismen.

Diskussionsansätze zu Vorgaben hinsichtlich Authentisierung im Rahmen des Medienwechselvorgangs sind aufgekommen, jedoch bislang nur in Form erster Denkanstöße.

2.3 Gefährdungen bei der Nutzung von IEEE 802.21

Die wesentliche Gefährdung ist über den notwendigen Informationsdienst MIIS gegeben. Gelingt es einem Angreifer, gezielt auf diesen einzuwirken, so kann er wertvolle Hinweise für weiterführende Angriffsschritte erhalten, solche Angriffe durch Manipulation der verwalteten Informationen begünstigen oder über DoS-artige Angriffe die Verfügbarkeit des Informationsdienstes sabotieren und so den Medienwechsel unmöglich machen.

DoS-Angriffe sind ferner denkbar in einer Weise, dass durch Provokation bestimmter Ereignisse (Events) ein mobiles Gerät immer wieder dazu veranlasst wird, einen Medienwechsel durchzuführen. Eine produktive Nutzung der immer nur kurzzeitig etablierten Links wird dadurch unmöglich gemacht.

Man beachte, dass es sich bei diesen Betrachtungen zurzeit um rein theoretische Gefährdungen handelt, da noch keine Implementierungen zur Verfügung stehen.

2.4 Schutzmaßnahmen

Schutzmaßnahmen innerhalb des Geltungsbereichs von IEEE 802.21 sind derzeit nicht absehbar. Die dargestellten Gefährdungen müssen auf Ebene der genutzten Netzwerk-Lösungen mit Hilfe von Authentizitätssicherung und Verschlüsselung kritischer Informationen, etwa im Rahmen der MIIS-Nutzung, abgewendet werden.

2.5 Ausblick

Die Praxisrelevanz von IEEE 802.21 ist von einer geringeren Anzahl an Einflussgrößen abhängig. Hier kommt es im Wesentlichen darauf an, ob Hersteller einen ausreichend großen Markt sehen und die Vorleistung des Implementierungsaufwands eingehen. Die Akzeptanz auf Kundenseite wiederum wird sicherlich stark davon mitbestimmt werden, ob eine IEEE 802.21-Fähigkeit leicht, im Idealfall ohne Austausch bestehender Installationen von Software auf Layer 2 und 3, d.h. als reine Ergänzung nachgerüstet werden kann. Ob die Diskussionen zu Sicherheitselementen durch die IEEE 802.21-Arbeitsgruppe noch in die erste Standardversion einfließen werden, ist fraglich, sofern der aktuelle Terminplan eingehalten wird.

2.6 Fazit

IEEE 802.21 ist eine reine Verwaltungslösung, mit der Verbindungswechsel über die Grenzen der einzelnen Netzwerk-Technik hinaus möglich gemacht werden sollen. Prinzipiell ergeben sich hier keine zusätzlichen Aufgaben zur Absicherung, solange die für die so zusammengeführten Technologiealternativen bereits einzeln formulierten Empfehlungen zu Schutzmaßnahmen umgesetzt werden. Allerdings ist zu beachten, dass die Gewährleistung eines garantierten Mindestsicherheitsniveaus in

den entstehenden heterogenen Netzarchitekturen komplizierter wird: Das Sicherheitsniveau wird bestimmt durch die schwächste beteiligte Implementierung bzw. Konfiguration, die ein vernetztes Gerät über IEEE 802.21 auswählen kann. Sicherheitsanalysen werden komplexer, da Technikwechsel nicht länger auf definierte Übergabepunkte zwischen Netzwerken beschränkt bleiben, sondern „im multinetzwerkfähigen“ Endgerät selbst entschieden werden.

2.7 Literatur / Links

Neben Veröffentlichungen der Hersteller, die vor-Standard-Implementierungen vorgenommen haben, sind entsprechend dem Status eines „Standards in Entwicklung“ (emerging standard) im Wesentlichen die Veröffentlichungen der zugehörigen IEEE-Arbeitsgruppe zu nennen. Eine vollständige Übersicht der allgemein zugänglichen Beiträge von Mitgliedern der jeweiligen Arbeitsgruppe findet sich unter [IEEE10].

Die Liste der hier aufgeführten Titel und Links stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

[IEEE10] Web-Präsenz der IEEE 802.21-Arbeitsgruppe
http://www.ieee802.org/21/, insbesondere dort gelistete Links zu Verzeichnissen mit Dokumenten zu Konferenzen

[IEEE11] Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services IEEE P802.21/D00.01
http://www.ieee802.org/21/july05_meeting_docs/ 21-05-0308-00-0000-FT_comments_One_Proposal_Draft_Text.doc, Juli 2005

2.8 Abkürzungen

DoS	Denial of Service
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
MICS	Media Independent Command Services
MIES	Media Independent Event Services
MIH	Media Independent Handover
MIIS	Media Independent Information Service
QoS	Quality of Service
SAP	Service Access Point

2.9 Glossar

Authentisierung
: Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Gerätes. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist i. A. keine sinnvolle Autorisierung möglich.

Denial of Service (DoS)
: Ein Angriff vom Typ Denial of Service hat zum Ziel die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr („Dummy Traffic“) oder die beabsichtigte Herbeiführung eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Service Access Point (SAP)
: Schnittstelle zur Interaktion mit einer Kommunikationsschicht. Der Dienstbenutzer (die höhere Schicht) greift nur über den Service Access Point auf den Dienst der niedrigeren Schicht (den Diensteanbieter) zu.

3. IEEE 802.22 – Wireless Regional Area Network (WRAN)

Die IEEE 802.22 Arbeitsgruppe hat Stand Anfang 2006 ihre Arbeit gerade erst aufgenommen. Der Genehmigungsantrag für das zugehörige IEEE-Projekt wurde im März 2006 genehmigt und sieht die Einreichung einer ersten Version zur abschließenden Revision für Mai 2007 vor.

Entsprechend unklar ist die Sachlage hinsichtlich konkreter Ausprägung des zukünftigen Standards, was technische Vorgaben im Detail anbetrifft. Erste Unterlagen existieren im Zusammenhang der Arbeitsgruppen-Treffen, allerdings vorrangig in Form von Präsentationsmaterial, mit dem die verschiedenen ersten Ansätze vorgestellt und einer Auswahl unterzogen werden sollen. Dennoch hat sich in der Kürze der Zeit eine erste Straffung ergeben: ursprünglich mit getrennten Ansätzen angetretene Hersteller haben ihre Ideen dergestalt zusammengeführt, dass sich die Diskussionen auf das Abwägen zweier unterschiedlicher Vorschläge konzentrieren können. Die bis März 2006 erfolgten Arbeiten konzentrieren sich dabei vorrangig auf die Signalisierungstechnik.

Eine erste systematische Betrachtung der beabsichtigten Inhalte des Standards kann dennoch auf Basis der bisher vorliegenden Spezifikation funktionaler Anforderungen erfolgen.

3.1 Grundlagen

Gegenstand der Arbeitsgruppe IEEE 802.22 ist die Spezifikation einer Lösung zur regionalen drahtlosen Kommunikation im UHF/VHF-Bereich, soweit dieser im konkreten Fall nicht durch TV-Sendeaktivitäten oder andere Funkdienste belegt ist.

Ziel ist die drahtlose Versorgung von dünn besiedelten bzw. ländlichen Regionen (Wireless Regional Area Network, WRAN), bei denen ein Angebot an derzeit aktuellen kabelbasierten Breitband-Zugangsmöglichkeiten wie ADSL eher unwirtschaftlich ist, so dass mit entsprechenden Nachteilen bei der Versorgung solcher Regionen durch Dienstanbieter zu rechnen ist.

Das WRAN-System wird dabei als Teil der so genannten „Fixed Wireless Access“ (FWA)-Lösungen angesehen, die lokale Netzwerke an eine Gesamtinfrastruktur anschließen. IEEE 802.22-Kundenstationen sind also keine Endgeräte, die über eine Basisstation kommunizieren, sondern Punkte, an denen lokale Netze an überregionale Infrastrukturen angebunden werden können.

Angeboten werden soll ein Mindestdurchsatz von

- 1,5 MBit/s downlink (von der Basisstation zum Kundengerät (Customer Premises Equipment, CPE) und
- 384 kBit/s uplink.

Die tatsächlich unterstützten Datenraten bleiben offen, bis eine Einigung und Festschreibung hinsichtlich der gewählten Lösungen zu Signalisierung und Fehlerkorrektur erfolgt ist.

Der ursprüngliche Projektantrag sieht eine WRAN-Implementierung innerhalb des Bereichs zwischen VHF (54 MHz) bis UHF (862 MHz) vor. Eventuell wird eine Abwandlung des Projektantrags auf einen Rahmen von 47 – 910 MHz erfolgen.

Die Grundarchitektur von WRAN nach IEEE 802.22 basiert auf einer Basisstation, die mehrere stationäre Kundenstationen versorgen soll. Die Reichweite dieser Konstellation beträgt ca. 33 km. Über optionale Verstärker-Lösungen (Repeater-Funktion, RF) kann dies ausgeweitet werden.

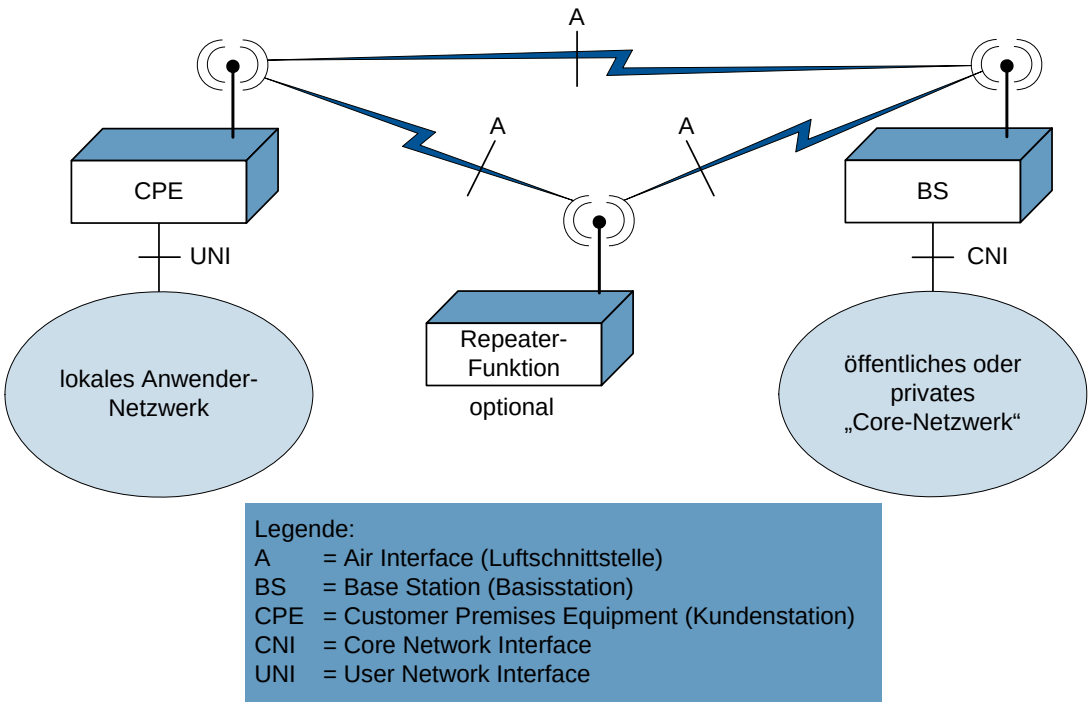


Abb. J-5: Netzwerkaufbau bei IEEE 802.22

Eine Kundenstation umfasst eine Außenantenne, für die eine Montage in ca. 10 m Höhe vorgesehen ist (Dach eines entsprechend hohen Gebäudes oder Antennenmast).

Der IEEE 802.22-Standard wird die drahtlose Kommunikation zwischen Basisstation und Kunden-Station auf physikalischer Ebene (PHY-Layer) und MAC-Layer regeln. Die Kommunikation ist verbindungslos angelegt (Paket-basierte Übertragung).

Der Basisstation obliegt dabei die vollständige Kontrolle der Kommunikation. Sie ist der „Master“ gegenüber den Verstärkern oder Kundenstationen („Slaves“). Insbesondere ist es Aufgabe der Basisstation, die Sendeaktivitäten so zu steuern, dass keine Konkurrenz zu TV-Übertragungen oder anderen Funkdiensten entsteht. Eine Kundenstation darf nur senden, wenn sie hierfür ein regelmäßig von der Basisstation gesendetes Freigabesignal erhält. Entdeckt die Basisstation andere Aktivitäten in ihrem Sendebereich, so wechselt sie auf einen noch freien Sendebereich.

Die IEEE 802.22-Spezifikation soll u.a. die Anforderungen gemäß Tab. J–1 erfüllen. Weitere Detailanforderungen können dem „Functional Requirements“-Dokument [IEEE13] entnommen werden.

Anforderungen	zwingend	optional
Unterstützung einer Mischung aus verschiedenen Kommunikationsflüssen wie Datenkommunikation, Voice over IP (VoIP) und Audio/Video-Anwendungen	X	
Unterstützung von Quality of Service (QoS) zwecks Erfüllung der jeweiligen Anforderungen unterschiedlicher paralleler Kommunikationsflüsse	X	
Unterstützung von IPv4 und IPv6 als Protokoll oberhalb der IEEE 802.22-MAC-Lösung	X	
Unterstützung von VoIP		X
Jitter nicht schlechter als 10 ms (VoIP-tauglich)		X
Unterstützung von QoS-Steuerung über IP Differentiated Services (RFCs 2474 und 2475)		X
konstante Bitrate	X	

Tab. J–1: Anforderungen an WRAN gemäß IEEE 802.22

3.2 Sicherheitsmechanismen von IEEE 802.22

Konkrete Spezifikationen von Sicherheitsmechanismen liegen noch nicht vor. Als funktionale Anforderungen werden jedoch Vorgaben an die auszuarbeitenden Spezifikationsinhalte formuliert, diese sind in Tab. J–2 dargestellt. Weiterhin wird von Arbeitsgruppenmitgliedern, die Vorschläge zur Spezifikation einreichen, gefordert, dass diese darstellen, wie die vorgeschlagene Lösung gegen Angriffe wie Denial of Service-Attacken geschützt werden kann bzw. welche Beiträge der Vorschlag hierzu beinhaltet.

Anforderungen	zwingend	optional
Lösung zur Authentisierung der Kundenstation bei Registrierung im Netzwerk	X	
Verschlüsselungsmöglichkeit	X	
Austausch von für die Verschlüsselungslösung relevanten Parametern innerhalb der IEEE 802.22-Lösung („over the air rekeying“, OTAR)	X	
Unterstützung einer paketweisen Authentizitätssicherung (Integritätssicherung)	X	
verschlüsselte und authentisierte Übertragung von Steuerungsinformationen über die Luftschnittstelle	X	

Tab. J–2: Sicherheitsmechanismen für WRAN gemäß IEEE 802.22

3.3 Schutzmaßnahmen

Aussagen zu konkreten Schutzmaßnahmen sind noch verfrüht. In anderen Fällen empfohlene Schutzmaßnahmen für Endteilnehmer oder Server (Virenschutz etc.) sind abhängig vom zugrunde liegenden Betriebssystem ebenfalls sinnvoll, können jedoch nur über die Produktauswahl beeinflusst werden, da IEEE 802.22-Kundenstationen Infrastrukturkomponenten sind.

Allerdings kann sich ein konkreter Bedarf für gezielte Schutzmaßnahmen unmittelbar aus der Art und Weise ergeben, wie die Spezifikation mit der Unverbindlichkeit der Forderung nach Regelung des Austausches von kryptographisch relevanten Informationen über die Luftschnittstelle umgeht. Eventuell lassen sich von anderen Luftschnittstellen-Spezifikationen bekannte Angriffsformen auf WRANs nach IEEE 802.22 übertragen, so dass die entsprechenden Gegenmaßnahmen zu ergreifen sind.

3.4 Ausblick

Auch bei WRAN gemäß IEEE 802.22 ist eine Prognose schwierig, wie sich die Praxisrelevanz darstellen wird und insbesondere, wie die Sicherheitsthematik gelöst wird.

Für alle diskutierten neueren Entwicklungen sollte man kritisch im Auge behalten, wie die noch ausstehenden Implementierungen mit dem Thema Sicherheit umgehen. In der Grundanlage gute und bewusst den Aspekt der Sicherheit berücksichtigende Standards können in der Praxis geschwächt werden, wenn die angebotenen Möglichkeiten zur Absicherung nicht konsequent genutzt oder durch Art und Weise der Lösung im Produkt verwässert werden.

3.5 Fazit

IEEE 802.22 befindet sich noch mitten in der Erarbeitung. Insbesondere existieren hinsichtlich der Sicherheit bislang nur funktionale Anforderungen, so dass eine Gefährdungsanalyse und Ableitung von Schutzmaßnahmen noch nicht durchgeführt werden kann.

3.6 Literatur / Links

Neben Veröffentlichungen der Hersteller, die vor-Standard-Implementierungen vorgenommen haben, sind entsprechend dem Status eines „Standards in Entwicklung“ (emerging standard) im Wesentlichen die Veröffentlichungen der zugehörigen IEEE-Arbeitsgruppe zu nennen. Eine vollständige Übersicht der allgemein zugänglichen Beiträge von Mitgliedern der jeweiligen Arbeitsgruppe findet sich unter [IEEE12].

Die Liste der hier aufgeführten Titel und Links stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

[IEEE12] Web-Präsenz der IEEE 802.22-Arbeitsgruppe http://www.ieee802.org/22/, insbesondere dort gelistete Links zu Verzeichnissen mit Dokumenten zu Konferenzen (Menüpunkt “Meeting Documents” http://www.ieee802.org/22/Meeting_documents/index.html) und Link auf Projektantrag (PAR http://www.ieee802.org/22/P802-22-1_PAR.pdf)

[IEEE13] Functional Requirements for the 802.22 WRAN Standard http://www.ieee802.org/22/Meeting_documents/2006_Jan/22-05-0007-47-0000_RAN_Requirements.doc, 29. Jan. 2006

3.7 Abkürzungen

ADSL	Asymmetric Digital Subscriber Line
CPE	Customer Premise Equipment
FWA	Fixed Wireless Access
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol

MAC	Media Access Control
OTAR	Over The Air Rekeying
QoS	Quality of Service
PHY-Layer	Physikalischer Layer
RF	Repeater-Funktion
RFC	Request for Comment, Veröffentlichung der Internet Engineering Task Force
UHF	Ultra High Frequency
VHF	Very High Frequency
VoIP	Voice over IP
WRAN	Wireless Regional Area Network

3.8 Glossar

Authentisierung
: Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Gerätes. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist i. A. keine sinnvolle Autorisierung möglich.

Ultra High Frequency (UHF)
: Frequenzband von 0,3 GHz bis 3 GHz

Very High Frequency (VHF)
: Frequenzbereich von 30 MHz bis 300 MHz (Ultrakurzwellen)

4. Near Field Communication (NFC)

Near Field Communication (NFC) ist eine Technik zur drahtlosen Kopplung von Geräten. Sie stellt eine Weiterentwicklung der RFID-Technik dar, bei der Daten auf einem Transponder berührungslos gelesen und gespeichert werden können. NFC erweitert die RFID-Technik um die Möglichkeit, zwei gleichberechtigte „intelligente“ Geräte miteinander verbinden zu können, wie beispielsweise bei Bluetooth. Wesentliches Merkmal ist jedoch die Einfachheit, mit der diese Kopplung geschieht. Sobald sich zwei Geräte in gegenseitiger Reichweite befinden, bauen sie in kürzester Zeit eine Verbindung auf. Die Reichweite wurde bei NFC bewusst auf max. 10 bis 20 cm begrenzt, damit der Anwender eine möglichst gute Kontrolle über die Kommunikation behält. Die geringe Reichweite vereinfacht nach Ansicht der Entwickler das Identifizieren der Kommunikationspartner [NFCFO06] und soll ein Sicherheitsmerkmal sein.

Die an der Entwicklung und Vermarktung der Technik beteiligten und interessierten Unternehmen haben sich im NFC-Forum zusammengeschlossen. Dabei steht die Anwendung der Technik in so genannten Consumer-Geräten im Vordergrund. Man verspricht sich von NFC neue Einsatzszenarien für mobile Geräte, wie beispielsweise Mobiltelefone, Digitalkameras oder PDAs. Auch an eine Verwendung von NFC als Vorstufe zu einer anschließenden Kommunikation mittels WLAN oder Bluetooth ist gedacht. In diesem Fall übernimmt NFC die Übertragung von Informationen, die zur Konfiguration von Bluetooth oder WLAN benötigt werden. So ist z.B. der selbsttätige Austausch einer Bluetooth PIN oder eines Schlüssels für die Absicherung einer WLAN-Kommunikation mittels NFC denkbar.

1. IEEE 802.20 – Mobile Broadband Wireless Access (MBWA)

Die Bereitstellung mobiler Breitbandnetze auf Basis drahtloser Technik wurde durch die IEEE zunächst im Rahmen der Arbeitsgruppe zu IEEE 802.16 WiMAX (Worldwide Interoperability for Microwave Access) behandelt. Der WiMAX-Standard dient dem Ziel, ein Breitbandnetz mit Metropolitan Area Network-Ausdehnung (MAN) zu schaffen. Dabei waren die Arbeiten der IEEE 802.16-Arbeitsgruppe allerdings zunächst nur auf stationäre Teilnehmer ausgerichtet. Erst im Januar 2006 folgte mit IEEE 802.16e eine Erweiterung der WiMAX-Ansätze für die mobile Nutzung.

Bereits im Dezember 2002 wurde der Zugriff auf Breitbandnetze durch drahtlose Teilnehmer (Mobile Broadband Wireless Access, MBWA) als neue Schwerpunktsetzung in eine eigene Arbeitsgruppe ausgegliedert. Diese IEEE 802.20-Arbeitsgruppe konzentriert sich seither auf die Definition einer standardisierten Luftschnittstelle, die für die Nutzung eines Breitbandangebots bei hoher Mobilität und als Basis für die Nutzung von IP-Netzwerken optimiert ist.

Schwerpunktmäßig wird auf Unterstützung solcher Netzzugänge nicht nur für Fußgänger (Fortbewegung mit ca. 3 km/h), sondern auch für höhere Mobilitätsklassen abgezielt, wobei Geschwindigkeiten bis zu 250 km/h unterstützt werden sollen. Damit zielt die Spezifikation insbesondere auf die Netzwerk-Nutzung aus Fahrzeugen ab. MBWA-Lösungen sollen unter allen Bedingungen eine ununterbrochene Konnektivität erlauben, wie man es von drahtgebundenen Systemen gewohnt ist.

Ursprünglich für Dezember 2004 geplant, ist die Fertigstellung der ersten verabschiedeten Standard-Version nunmehr für Ende 2006 vorgesehen (siehe [IEEE03]).

1.1 Grundlagen / Funktionalität gemäß IEEE 802.20

1.1.1 Technische Grundlagen

Die IEEE 802.20-Spezifikation beschreibt die grundlegenden technischen Merkmale eines MBWA-Systems, über das drahtlose Dienste für sich mit hoher Geschwindigkeit bewegende Teilnehmer zur Verfügung gestellt werden können.

MBWA ist für IP-basierte[1] Kommunikation optimiert und daher paketorientiert. Über entsprechende Quality of Service (QoS)-Mechanismen können auch Echtzeitdienste und IP-basierte Telefonie („Voice over IP“ VoIP) unterstützt werden[2]. Mit MBWA-Lösungen auf Basis von IEEE 802.20 soll weltweite Mobilität geboten werden, z.B. unter Nutzung von speziellen Lösungen wie Mobile IP. Mobile IP ermöglicht einem Teilnehmer, unter seiner ursprünglichen IP-Adresse erreichbar zu bleiben, obwohl er sich vorübergehend in einer fremden IP-Umgebung (Gastnetz) aufhält.

Das Grundmodell von IEEE 802.20 unterscheidet zwischen den folgenden Komponenten (siehe Abb. J-1):

- Access Terminal (AT): Schnittstelle mobiler Geräte zum MBWA Access Network
- Access-Netzwerk (AN): Komponenten, die den Access Terminals eine Verbindung mit einem IP-Netzwerk, typischerweise mit dem Internet, auf der Netzwerkebene (ISO-Layer 3) ermöglichen.
- Sektoren: Physikalische Kanäle zur Kommunikation zwischen AT und AN. Prinzipiell kann eine Basisstation mehrere Kanäle bereitstellen.

---

1 Wahlweise über IPv4 oder IPv6

2 Es besteht die Möglichkeit, für IP-Netze spezifizierte QoS-Steuerungsmechanismen wie Differentiated Services (DiffServ) und Resource Reservation Protocol (RSVP) geeignet abzubilden.

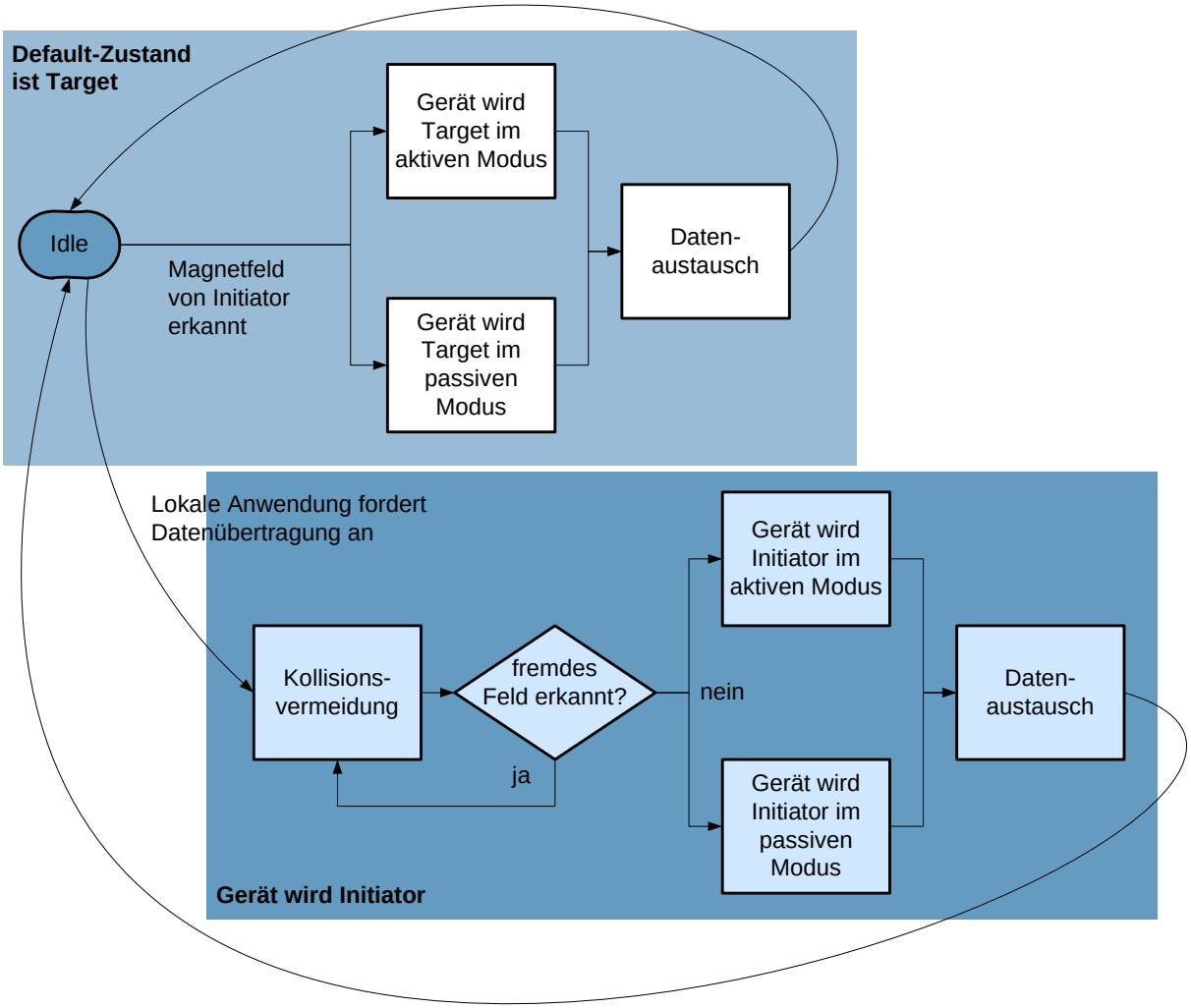


Abb. J-6: Kommunikation bei NFC (vereinfacht)

4.2 Sicherheitsmechanismen bei NFC

Der aktuelle Standard beschreibt keine Sicherheitsmechanismen. Im Gegenteil, der Verzicht auf Sicherheitsmechanismen und auf die damit verbundene Verwaltung entsprechender Parameter ist eine Voraussetzung für den unkomplizierten und schnellen Verbindungsaufbau zu jedem gewünschten Kommunikationspartner. Sicherheit entsteht nach Ansicht der Entwickler einzig durch die sehr geringe Reichweite des Verfahrens.

4.3 Gefährdungen beim Einsatz von NFC

Die folgenden Gefährdungen beim Einsatz von NFC sind denkbar:

- Fehlende Authentisierung und Verschlüsselung: Hier besteht die Gefahr, dass ein Target von einem fremden Initiator angesprochen wird und Daten preisgibt. Weiterhin kann auch bei den geringen Reichweiten eines NFC-Systems nicht ausgeschlossen werden, dass ein Dritter den Dialog zwischen Initiator und Responder belauscht. Verfahren zur Authentisierung und Verschlüsselung sind im Standard nicht vorgesehen und müssen von den Anwendungen bereitgestellt werden. Eine weitergehende Aussage über konkrete Gefährdungen ist zum heutigen Zeitpunkt noch nicht möglich.

- Unkontrollierte Ausbreitung der Funkwellen: Die von NFC-Geräten erzeugten hochfrequenten Magnetfelder lassen sich mit der in entsprechenden Chips vorgesehenen Empfangstechnik nur in einem Abstand von max. 20 cm wahrnehmen. Der Aufbau von Richtantennen mit hohem Gewinn, die einen Empfang der Signale aus größerer Entfernung ermöglichen, ist wegen der mit 22 m großen Wellenlänge nicht einfach zu bewerkstelligen. Insbesondere lassen sich solche Antennen wegen ihrer erheblichen Baugröße kaum verbergen. Darüber hinaus besteht bei NFC nicht die Möglichkeit, anhand von Kanälen oder Adressen zwischen verschiedenen Geräten zu unterscheiden. In einem kontrollierten Umfeld ist ein unbemerktes Abhören daher nur schwer möglich. Allerdings ist der Aufbau einer Abhöranlage (in Aktenkoffergröße), die das Mithören der NFC-Kommunikation in einem Abstand von mehr als einem Meter Abstand gestattet, nicht unrealistisch. Die NFC-Technik erschwert zwar das Abhören, schließt es aber nicht mit genügend hoher Wahrscheinlichkeit aus. Weiterhin sollen die für NFC vorgesehenen Anwendungen gerade in Umgebungen eingesetzt werden, die sich einer Kontrolle entziehen, z.B. in öffentlichen Verkehrsmitteln. Hier gibt es für einen Angreifer durchaus Möglichkeiten nahe genug an das Ziel heranzukommen und eine NFC-Kommunikation zu kompromittieren.
- Denial of Service (DoS): Die Kommunikation von NFC-Geräten lässt sich prinzipiell stören. Zum einen ist der Einsatz von Störsendern denkbar, die sich auch mit hohen Sendeleistungen auf einfache Weise beschaffen lassen. Die Antennentechnik ist jedoch mechanisch groß und kann nur schwer unauffällig installiert werden. Es können aber auch speziell programmierte NFC-Geräte als Störsender eingesetzt werden, die in unmittelbarer Nähe der zu störenden Systeme installiert werden, sofern die Umgebung dies unbemerkt zulässt.
- Erstellen von Bewegungsprofilen: Prinzipiell lassen sich auf mobilen NFC-Geräten implementierte Anwendungen dazu ausnutzen, Bewegungsprofile ihrer Benutzer zu erstellen.

Weitere Gefährdungen können sich aus den auf NFC basierenden Anwendungen ergeben. Hier ist insbesondere die oben genannte Möglichkeit der Übertragung von Schlüsselmaterial als Vorstufe für Bluetooth oder WLAN-Verbindungen zu nennen. Die in diesen Verfahren etablierten Sicherheitsmechanismen können durch eine Kompromittierung dieser Anwendungsform wirkungslos werden.

4.4 Schutzmaßnahmen beim Einsatz von NFC

Konkrete Schutzmaßnahmen lassen sich bisher nicht identifizieren, da diese wesentlich von den Anwendungen und Einsatzszenarien abhängen werden. Falls möglich, sollten mobile NFC-Geräte jedoch so lange vollständig deaktiviert bleiben, bis sie tatsächlich benötigt werden und sich die Einsatzumgebung vollständig kontrollieren lässt. Dies gilt insbesondere auch für den passiven Modus, bei dem ein Target im Normalfall inaktiv ist, bis es durch das Magnetfeld eines Initiators automatisch aufgeweckt wird. Dieser Aufweckvorgang muss deaktivierbar sein.

Die vorgesehenen Anwendungen und damit verbundene Sicherheitsmechanismen sollten vor ihrem Einsatz mit NFC einer Risikoanalyse unterzogen werden. Bei entsprechendem Schutzbedarf ist eine Authentisierung und Verschlüsselung auf Anwendungsebene erforderlich.

4.5 Ausblick

Die Möglichkeit, fast beliebige Geräte ohne vorangehende Konfiguration miteinander kommunizieren zu lassen, wird voraussichtlich zahlreiche neue Anwendungen für mobile Kleingeräte entstehen lassen. Gerätehersteller sehen diese Technik bereits heute als kostengünstigen Eintritt in den Markt der Smartcards an: Das Mobiltelefon wird zu einer kontaktlosen Smartcard, mit deren Hilfe man elektronische Sperren (etwa in der U-Bahn) überwindet, Eintrittsgelder bei Veranstaltungen bargeldlos entrichtet oder gar an der Supermarkt-Kasse bezahlt. Erste Ergebnisse entsprechender Feldversuche liegen bereits vor. Mit einer großen Verbreitung derartiger Anwendungen in der Gesellschaft wächst

naturgemäß die Gefahr von Angriffen auf die Vertraulichkeit und Integrität der übermittelten Daten mit kriminellem Hintergrund.

4.6 Fazit

NFC ist eine einfach zu handhabende Funktechnik, die sich nur auf wenigen Zentimetern einsetzen lässt. Damit verbunden ist zwar ein gewisser Schutz gegen Abhören und Störung, jedoch sind Angriffe auch nicht auszuschließen. Daher ist bei entsprechendem Schutzbedarf eine Absicherung auf Anwendungsebene unumgänglich, da aktuell für die NFC-Kommunikation selbst keine Sicherheitsmechanismen vorgesehen sind. Dem Nutzer der Technik ist es dann letztendlich überlassen, im Einzelfall zu prüfen, ob das so erreichte Sicherheitsniveau angemessen ist. Bei einer größeren Palette an Applikationen (von der bei NFC durchaus ausgegangen werden muss) kann ein Anwender hier schnell überfordert werden. Grundsätzlich ist es daher für drahtlose Kommunikationssysteme (auch für NFC) wünschenswert, dass Sicherheitsmechanismen einen integralen Bestandteil der drahtlosen Übertragungsdienste darstellen und zumindest optional aktiviert werden können. Auf diese Weise können Entwickler von NFC-Anwendungen einheitlich auf sichere Kommunikationsmittel zurückgreifen.

4.7 Literatur / Links

Diese Liste stellt nur eine wertungsfreie Auswahl ohne Anspruch auf Vollständigkeit dar.

[BSI04] Bundesamt für Sicherheit in der Informationstechnik, „Risiken und Chancen des Einsatzes von RFID-Systemen“, 2004, verfügbar unter http://www.bsi.bund.de/fachthem/rfid/RIKCHA.pdf

[Brow04] Eric S. Brown, „Wird das Handy zur universellen Smartcard“, Heise News, 2004, verfügbar unter http://www.heise.de/tr/artikel/51161

[ECMA340] ECMA International, Standard ECMA-340, „Near Field Communication Interface and Protocol (NFCIP-1) 2nd edition“, December 2004, verfügbar unter http://www.ecma-international.org/publications/standards/Standard.htm

[ECMA352] ECMA International, Standard ECMA-352, „Near Field Communication Interface and Protocol-2 (NFCIP-2)“, December 2003, verfügbar unter http://www.ecma-international.org/publications/standards/Standard.htm

[ECMA356] ECMA International, Standard ECMA-356, „NFCIP-1 - RF Interface Test Methods“, June 2004, verfügbar unter http://www.ecma-international.org/publications/standards/Standard.htm

[ECMA362] ECMA International, Standard ECMA-362, „NFCIP-1 - Protocol Test Methods 2nd edition“, December 2005, verfügbar unter http://www.ecma-international.org/publications/standards/Standard.htm

[ISO14443] International Organization for Standardization, Standard ISO/IEC 14443 Teile 1 bis 4,
„Part 1: Physical characteristics“, October 2003,
„Part 2: Radio frequency power and signal interface“, March 2006,
„Part 3: Initialization and anticollision“, March 2006,
„Part 4: Transmission protocol“, March 2006

[NFC06] “About Near Field Communication”, Webseite des NFC Forum, http://www.nfc-forum.org/aboutnfc

[Schu06] Jana Schudrowitz, „Freie Fahrt für Near Field Communication", 2006, verfügbar unter http://www.heise.de/newsticker/meldung/71940

4.8 Abkürzungen

ECMA	European Computer Manufacturers Association
ETSI	European Telecommunications Standards Institute
DoS	Denial of Service
ISO	International Organization for Standardization
NFC	Near Field Communication
OSI	Open Systems Interconnection
PDA	Personal Digital Assistant
PIN	Persönliche Identifikationsnummer
RFID	Radio-Frequency-Identification
WLAN	Wireless LAN

4.9 Glossar

Authentisierung
: Verifizierung der Identität einer Instanz, z.B. eines Benutzers oder eines Gerätes. Zweck ist oft die anschließende Autorisierung für Zugriffe. Ohne Authentisierung ist i. A. keine sinnvolle Autorisierung möglich.

Denial of Service (DoS)
: Ein Angriff vom Typ Denial of Service hat zum Ziel die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung eines Netzknotens durch unsinnigen Verkehr („Dummy Traffic“) oder die beabsichtigte Herbeiführung eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.

Radio-Frequency-Identification (RFID)
: Methode, um Daten auf einem Transponder berührungslos und ohne Sichtkontakt lesen und speichern zu können. Dieser Transponder kann an Objekten angebracht werden, welche dann anhand der darauf gespeicherten Daten automatisch und schnell identifiziert und lokalisiert werden können.

Smartcard
: Plastikkarten mit eingebautem Chip, der eine Hardware-Logik, Speicher oder auch einen Mikroprozessor enthält.

Tag
: Siehe Transponder

Transponder
: Der Transponder – auch als „Tag“ bezeichnet – fungiert als eigentlicher Datenträger. Er kann kontaktlos über Funktechnologie ausgelesen und je nach Technologie auch wieder beschrieben werden. Grundsätzlich setzt sich der Transponder aus einer integrierten Schaltung und einem Radiofrequenzmodul zusammen. Auf dem Transponder sind eine Identifikationsnummer und weitere Daten über den Transponder selbst bzw. das Objekt, mit dem dieser verbunden ist, gespeichert.