



Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte



Bundesamt für Sicherheit in der Informationstechnik
Projektgruppe „Local Wireless Communication“

Das gesamte Dokument (62 Seiten) siehe:
<http://www.bsi.de/literat/doc/drahtloskom/drahtloskom/pdf>

Die aktuellen Systeme nach Standard 802.11b verwenden nur das DSSS Verfahren. Die zu übertragene Daten werden mit einem festen Code gespreizt, um die Übertragung unempfindlicher gegen Störung zu machen. Der Zugriff auf den Funkkanal erfolgt, wie bei allen Systemen der 802.11 Standards, nach einem zufallsgesteuerten Verfahren, genannt Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Die Brutto-Datenübertragungsrate beträgt bei 802.11b maximal 11 Mbit/s. Die Übertragungsraten können, wie bei allen Systemen der 802.11 Standards, nicht garantiert werden, sie hängen ab von der Anzahl der Clients und der Qualität der Funkübertragungsstrecke.

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 können jedoch nur maximal 3 Kanäle gleichzeitig überlappungsfrei genutzt werden, beispielsweise die Kanäle 2, 7 und 12 (siehe Abb. 3).

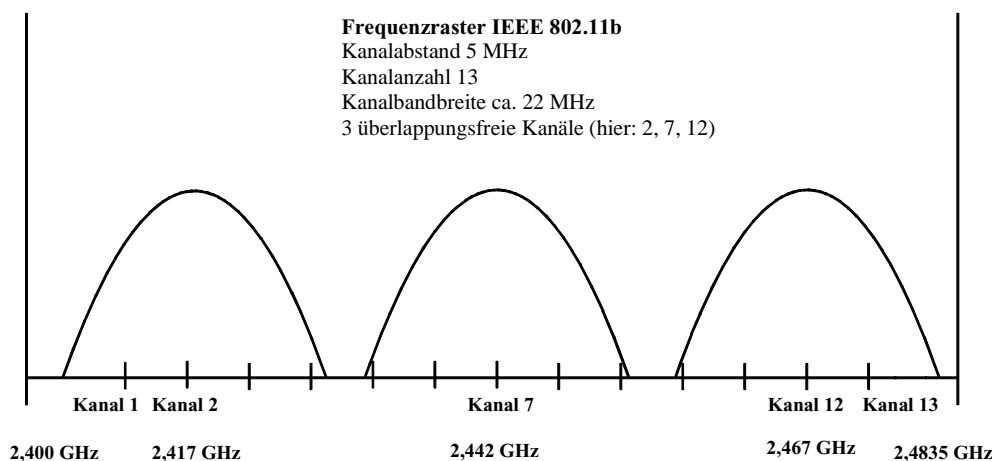


Abb. 3: 802.11b Kanalaraster, überlappungsfreie Kanäle

Neben den 802.11b Systemen werden nun auch 802.11a und 802.11g Systeme angeboten und weitere Standards wie 802.11h stehen vor der Fertigstellung. Alle drei Standards definieren gegenüber 802.11b eine unterschiedliche physikalische Übertragungstechnik zur Realisierung höherer Übertragungsraten von bis zu 54 Mbit/s (brutto).

802.11g Systeme arbeiten im gleichen Frequenzbereich wie 802.11b, sodass auch hier nominell 13 Kanäle in Deutschland zur Verfügung stehen. Bei einer Bandbreite der Funksignale von 20 bzw. 22 MHz können maximal 4 Kanäle gleichzeitig in räumlicher Nähe betrieben werden ohne sich gegenseitig zu stören.

802.11a und zukünftige 802.11h Systeme nutzen den 5 GHz-Bereich. Im Frequenzbereich von 5,15 bis 5,35 GHz und bei 5,47 bis 5,725 GHz sind in Deutschland insgesamt 19 Kanäle in einem Abstand von 20 MHz unter Auflagen freigegeben worden [REGTP]. Bei einer Kanalbandbreite von 20 MHz werden direkt benachbarte Kanäle hier nicht gestört.

1.3 Sicherheitsmechanismen

Die Sicherheitsmechanismen aller 802.11 kompatiblen Systeme sind im Standard 802.11 definiert. Die Erweiterungen a, b, g und h des Standards bieten keine zusätzlichen Sicherheitsmechanismen, erst die Erweiterung i wird neue Sicherheitsmechanismen definieren. Die zurzeit in 802.11 definierten Mechanismen dienen ausschließlich zur Sicherung der Funkstrecke zwischen den Clients und Access-Points. Darüber hinaus lässt der Standard aber auch Freiraum für proprietäre Erweiterungen.

Sämtliche Sicherheitsmechanismen des Standards 802.11, die im Folgenden dargestellt werden, sind überwindbar und bieten keinen verlässlichen Schutz für sensible Informationen.

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.

Wie erwähnt und in Abbildung 4 dargestellt, verschlüsselt WEP die übertragenen Nutzdaten und die Integritätschecksumme. Management- und Steuersignale (Management- und Control-Frames) werden auf der Funk-Schnittstelle jedoch nicht verschlüsselt.

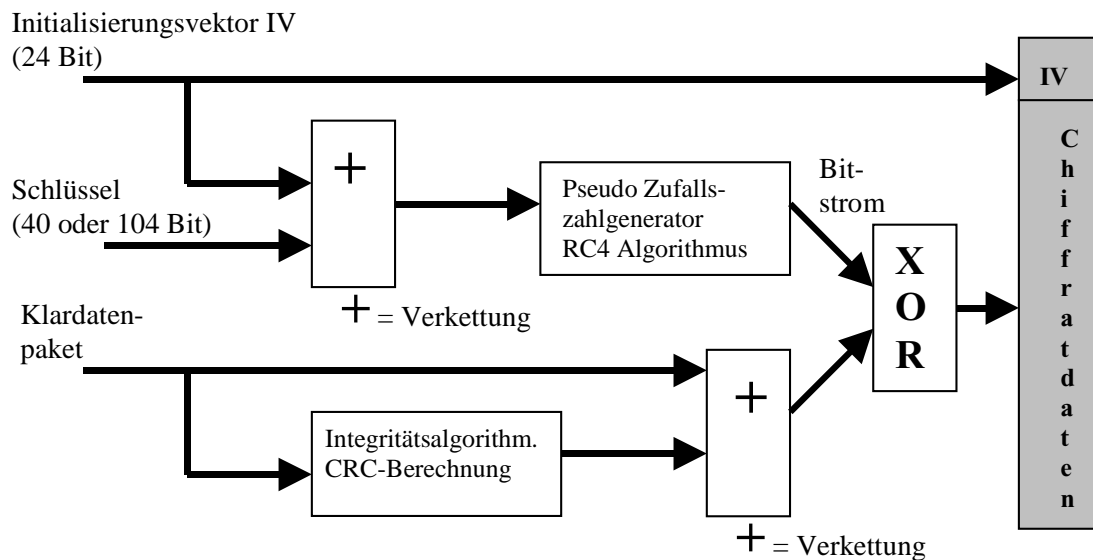


Abb. 4: Blockschaltbild von WEP

2 Sicherheitsprobleme

Die aktuellen standardkonformen Funk-LAN-Systeme bergen bzgl. der Sicherheit große Schwachstellen, die aktive wie passive Angriffe erlauben und damit zu einem Verlust von Vertraulichkeit, Integrität und Verfügbarkeit führen können. Im Folgenden werden mögliche Sicherheitsprobleme beim Einsatz dieser Technologie exemplarisch aufgeführt.

2.1 Sicherheitskritische Grundeinstellung

Im Auslieferungszustand sind die Funk-LAN Komponenten häufig so konfiguriert, dass keine oder nur einige der zudem schwachen Sicherheitsmechanismen aktiviert sind.

2.2 SSID Broadcast

Einige Access-Points bieten die Möglichkeit, das Senden der SSID im Broadcast zu unterbinden, um das Funk-LAN vor Unbefugten zu verstecken (so genanntes "Closed System"). Dieser Schutz wirkt gegen diverse frei verfügbare Tools wie z. B. Netstumbler, jedoch kann mittels Funk-LAN-Analysatoren auch in diesem Falle die SSID aus anderen Management- und Steuersignalen ermittelt werden.

IEEE favorisiert die port-basierte Authentisierung nach dem Standard IEEE 802.1X, der auf dem Extensible Authentication Protocol (EAP, RFC2284) basiert. EAP stellt einen Rahmen für verschiedene Authentisierungsmethoden wie z. B. EAP-MD5, EAP-TLS, EAP-TTLS, PEAP, etc. zur Verfügung. Beim Einsatz von 802.1X ist eine Authentisierungsmethode zu wählen, die tatsächlich eine gegenseitige Authentisierung durchführt (z. B. EAP-TLS). Weiterhin ist zu beachten: 802.1X bietet nur Authentisierung (und ggf. Schlüsselverteilung) und stellt daher keine integrierte Sicherheitslösung dar. 802.1X ist ohne passende Verschlüsselung / Integritätssicherung sogar unsicher [MA02]. Daher muss 802.1X zusammen mit z. B. TKIP / Michael verwendet werden, wie es in WPA bzw. 802.11i der Fall ist (vgl. Kapitel Ausblick).

Insgesamt bietet es sich an, eine Sicherheitslösung auf Basis von digitalen Zertifikaten und ggf. einer PKI-Infrastruktur zu nutzen. Dadurch wird zum einen das Schlüsselmanagement besser integriert und zum anderen können die Sperrlisten der PKI genutzt werden, um die Authentisierung zusätzlich abzusichern.

B2: Abschottung des drahtgebundenen Firmen-/Behördennetz durch Firewall und Intrusion Detection System

Das drahtgebundene Firmen-/Behördennetz sollte durch eine Firewall mit Intrusion Detection System (IDS) gegen die Access-Points des Funknetzes abgeschottet werden.

Mittlerweile sind neben leitungsgebundenen IDS auch spezielle funkbasierte IDS auf dem Markt verfügbar, die mit Funksensoren das Frequenzspektrum des Funk-LANs überwachen und sicherheitsrelevante Anomalien, wie z. B. falsche APs und unbekannte Clients, entdecken und melden. In bestimmten Szenarien ist der Einsatz solcher Systeme als Alternative bzw. Ergänzung zu leitungsgebundenen IDS empfehlenswert.

B3: Absicherung der Clients

Insbesondere bei mobilen Clients, die sich in verschiedene Funk-LANs einbuchen können, sollten weitere lokale Schutzmaßnahmen implementiert werden, wie z. B.: Zugriffsschutz, Benutzerauthentisierung, Virenschutz, Personal Firewall, restriktive Datei- und Ressourcenfreigabe auf Betriebssystemebene, lokale Verschlüsselung, etc.[GSHB].

3.3 Organisatorische Maßnahmen

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

C1: Sicherheitsrichtlinien aufstellen

Für den Einsatz von Funk-LAN-Komponenten in Behörden und Unternehmen sollten individuelle Sicherheitsrichtlinien aufgestellt werden. Diese Funk-LAN spezifischen Sicherheitsrichtlinien sollten konform zum generellen Sicherheitskonzept der Behörde bzw. des Unternehmens sein und regelmäßig auf Aktualität überprüft und ggf. angepasst werden. Typische Punkte einer Funk-LAN Sicherheitsrichtlinie findet man z. B. in [NIST]. Nutzer der Funk-LANs sollten sensibilisiert werden für Gefährdungen sowie für Inhalte und Auswirkungen der Richtlinie.

C2: Einhaltung der Sicherheitsrichtlinien überprüfen

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

- C2.1 Regelmäßige Kontrollen der Access-Points und Clients mittels Funk-LAN-Analysator und Netzwerk-Sniffer
- C2.2 Auswertung der Protokolldatei (Log) des Access-Points - falls technisch möglich - und Überprüfung der an einem Access-Point angemeldeten Clients

► Authentisierung und Schlüsselmanagement

Diese Protokolle werden auf dem Standard IEEE 802.1X basieren.

Die Herstellervereinigung Wi-Fi-Alliance hat Ende 2002 bekannt gegeben, TKIP und 802.1X, basierend auf den Drafts von IEEE 802.11i, unter dem Namen Wi-Fi Protected Access (WPA) zu unterstützen. WPA stellt eine zu IEEE 802.11i aufwärtskompatible Zwischenlösung dar. Es soll demnächst möglich sein, Wi-Fi zertifizierte Funk-LAN-Komponenten durch Firmware-Update auf WPA aufzurüsten. Dabei ist 802.1X optional für die Benutzerauthentisierung und das Schlüsselmanagement bei großen Funk-LAN-Installationen vorgesehen, während kleinere Funk-LANs weiterhin mit manuell verteilten Schlüsseln arbeiten. TKIP verwendet weiterhin WEP, jedoch werden zur Behebung der größten Schwächen sicherheitsrelevante Veränderungen eingeführt. Diese sind ein erweiterter Initialisierungsvektor IV, eine dynamische Schlüsselerzeugung pro Datenpaket und ein kryptographischer Message Integrity Check (MIC), genannt "Michael". Michael wird zusätzlich zum CRC zur Integritätssicherung eingesetzt.

Auch bei WPA sind bereits mögliche neue Schwachstellen bekannt geworden: Entdeckt der Access-Point einen aktiven Angriff in Form von gefälschten Paketen, werden alle Verbindungen getrennt und der Access-Point wird für eine Minute inaktiv. Durch diese Gegenmaßnahme kann ein Angreifer das drahtlose Netzwerk unbrauchbar machen, indem er einfach gefälschte Pakete sendet (Denial of Service Angriff). Da diese zusätzliche Gegenmaßnahme oft kritisiert wurde, wird sie möglicherweise aus dem endgültigen Standard wieder entfernt.

Eine weitere Schwachstelle von WPA ist der mögliche Kompatibilitätsbetrieb eines Access-Points, sowohl mit WPA als auch mit WEP. In diesem Kompatibilitätsbetrieb werden zwar prinzipiell alle WPA-fähigen Clients mit dem Access-Point über WPA kommunizieren, 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.

Aus diesen Gründen sollte der Kompatibilitätsbetrieb möglichst nicht verwendet werden, d. h. wenn alle Clients auf WPA umgestellt wurden, sollte der Access-Point ebenfalls so konfiguriert werden, dass ausschließlich WPA Verbindungen akzeptiert werden.

Das Sicherheitsniveau von WPA ist - bei Kenntnis der genannten Schwachstellen und Berücksichtigung der o.g. Empfehlung - wesentlich stärker einzustufen als das des Standards IEEE802.11.

5 **Fazit**

Die Sicherheitsmechanismen des Standards IEEE 802.11 (und damit auch von IEEE 802.11b, a, h und g) erfüllen nicht die Anforderungen für eine Nutzung in sensitiven Bereichen. Trotz der dargestellten Sicherheitsprobleme sollten jedoch die im Standard definierten elementaren Schutzmaßnahmen im Funk-LAN aktiviert werden.

Für höhere Sicherheitsanforderungen sind zusätzliche Maßnahmen über den Standard 802.11 hinaus dringend erforderlich. Zurzeit sind im Wesentlichen nur proprietäre Erweiterungen, die untereinander meist nicht kompatibel sind, sowie WPA verfügbar. Neue Vorgaben hierzu wird der zukünftige Standard 802.11i voraussichtlich zum Ende des Jahres 2003 liefern. Bis zur Einführung der neuen Sicherheitsarchitektur ist WPA als Zwischenlösung zu empfehlen.

Aufgrund der gravierenden Schwächen von WEP bleibt abzuwarten, dass zügig mit der Integration von WPA und insbesondere von 802.11i in die Produkte begonnen wird. Hierbei ist die korrekte Implementierung von besonderer Bedeutung, damit keine neuen Angriffsmöglichkeiten entstehen.

Die höchste Sicherheit bei der Anbindung eines Funk-Clients an ein Firmen-/ Behördennetz bietet gegenwärtig ein korrekt implementiertes VPN, z. B. auf IPSEC oder SSL Basis.

3.3 Weitere Schutzmaßnahmen

Über die in 3.1 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

usw.

Informationen hierzu findet man im IT-Grundschutzhandbuch des BSI [5].

Als Schutzmaßnahme gegen das Abhören von Raumgesprächen ist ein Verbot des Einbringens von Funktechnik in den zu schützenden Raum zu empfehlen (vgl. auch [8]).

3.4 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 (vgl. 2.5) kann nicht verhindert werden.
- ▶ Die Gefährdung der Verfügbarkeit (vgl. 2.6) ist ebenfalls nicht vermeidbar.
- ▶ **Man-in-the-Middle-Angriffe (vgl. 2.2) 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 SSL) oder direkt auf Anwendungsebene (Ende-zu-Ende-Sicherheit).**

4 Ausblick

Für 2003 ist die Veröffentlichung der Bluetooth-Spezifikation Version 1.2 geplant.

Zukünftige Versionen des Bluetooth-Standards werden die Verwendung des Geräteschlüssels als Verbindungsschlüssel nicht mehr erlauben. Zusätzlich wird das Konzept der Gruppenschlüssel eingeführt. Gruppenschlüssel sollen Roaming ermöglichen, so dass ein Gruppenschlüssel nicht verbindungsindividuell zwischen zwei Geräten ausgehandelt wird, sondern dienstindividuell.

Es ist ebenfalls davon auszugehen, dass die Erstellung eines Kombinationsschlüssels nicht mehr ausschließlich durch die Eingabe einer PIN gesichert wird. Anstelle dessen wird der Kombinationsschlüssel über das Diffie-Hellmann-Verfahren vereinbart. Bei diesem Protokoll wird der Schlüssel über ein asymmetrisches kryptographisches Verfahren berechnet. Die PIN dient nur noch zur Kontrolle, ob die Berechnung nicht manipuliert wurde.

Das Erstellen von Bewegungsprofilen soll durch den neuen Standard erschwert werden, indem die feste Geräteadresse durch temporäre Adressen ersetzt wird. Die feste Geräteadresse wird dann nur noch zum Verbindungsaufbau verwendet.