Wireless Networks

Funknetzwerke auf Basis von IEEE 802.11b

Töns Büker
Senior Consultant
e-trend Media Consulting GmbH
toens.bueker@e-trend.de

Übersicht

- **Einleitung**
- **Begriffsbestimmung „IEEE 802.11b“**
- **Aufbau von Funknetzwerken**
  - Komponenten
  - Anwendungsszenarien
  - Sicherheit
- **Ausblick**

Begriffsbestimmung „IEEE 802.11b“
Standard unter vielen

- **Standards im Bereich Datenfunk:**
  - GSM, GPRS, HSCSD, UMTS, i-mode, Bluetooth, DIRC, DECT, DAB, HomeRF, UWB, HiperLAN, etc.
- **IEEE (Institute of Electrical and Electronics Engineers):**
  - eine Organisation, die Standards erarbeitet und herausgibt
  - Mitglieder sind sowohl Forscher als auch Produkthersteller
- **IEEE 802.11**
  - Die Arbeitsgruppe (Working Group) „Wireless LAN“ des IEEE, deren Sub-Arbeitsgruppen (Task Groups) an verschiedenen Verbesserungen und Erweiterungen des Standards arbeiten:
  - 802.11a: Development of Physical Layer (PHY) to operate in the UNII Band
  - 802.11b: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz Band
  - 802.11c: Media Access Control (MAC) Bridges
  - 802.11d: Extensions for Operation in Additional Regulatory Domains (Countries)
  - 802.11e: MAC Enhancements for Quality of Service
  - 802.11f: Recommended Practice for Inter Access Point Protocol
  - 802.11g: Standard for Higher Rate (20+ Mbps) Extensions in the 2.4 GHz Band
  - 802.11h: SMa – Spectrum Managed 802.11a
  - 802.11i: MAC Enhancements for Enhanced Security

Begriffsbestimmung „IEEE 802.11b“
Standard unter vielen

- **IEEE 802.11b:**
  - arbeitet auf dem ISM (Industrial, Scientific, Medical) Band bei 2,4 GHz
  - Störungen durch andere Sender auf gleicher Frequenz sind möglich (z. B. durch HomeRF, DECT, Bluetooth oder Mikrowellengeräte)
  - verwendet Complementary Code Keying (CCK) als Modulation
  - Reichweite variiert von 30 m bis zu mehreren Kilometern (mit Sichtkontakt)
  - verspricht Übertragungsraten von 1, 2, 5 und 11 MBit/s half-duplex (600 kbyte/s netto max.)
  - unterstützt Multi-Channel-Roaming, welches die gleichzeitige Benutzung von drei verschiedenen Funkkanälen erlaubt um die vorhandene Bandbreite besser zu verteilen
  - bietet Wireless Equivalent Privacy (WEP) – Verschlüsselung mit 40 und 104 bit Schlüssellänge, die sich aber inzwischen als unsicher erwiesen hat
- **Wireless Fidelity (WiFi)**
  - ein Standard der Wireless Ethernet Compatibility Alliance (WECA) – Mitglieder sind z. B. 3com, Cisco, Apple, Compaq, Dell, Elsa, IBM, HP, Intel, Intersil, Texas Instruments, etc.
  - WiFi-zertifizierte Produkte sollen interoperabel sein – eine Liste mit zertifizierten Produkten ist unter www.wi-fi.org aufgeführt.

Aufbau von Funktnetzwerken

- **Komponenten**
  - Basisstationen
  - Netzwerkadapter
  - Software
- **Anwendungsszenarien**
  - im öffentlichen Bereich
  - im Unternehmen und im privaten Bereich
- **Sicherheit**
  - Angriffe
  - Gegenmaßnahmen

Basisstationen (Access Points)
Brücke zwischen Funk und Kabel

Apple Airport

Cisco Aironet Basisstation

- **Verbindung zwischen kabelgebundenem Netz und Funknetz**
- **Bridge zum Teil mit Router-Eigenschaften**
- **Je nach Hersteller und Firmware-Version verschiedenste Funktionen (SNMP, Firewall, etc.)**
- **Erweiterbar durch externe Antennen**
- **Verschiedene Bauformen**

Netzwerkadapter
Sender/Empfänger für Laptop und PC

PC-Card

PCI-Bus Kartenadapter

- **PC- bzw. PCMCIA-Karten für Laptops**
- **PCI-Adapter für „normale“ PCs**
- **In Laptops der aktuellen Generation meist bereits eingebaut**
- **Robuste Ausführung**
- **Erweiterbar durch externe Antennen**
- **Im Ad-Hoc Modus kann von Karte zu Karte gefunkt werden**

Software
Klebstoff für die Einzelteile

- **Firmware für den Betrieb von Basisstationen und Netzwerkadaptern**
  - zusätzliche Funktionen und Protokolle
  - verbesserte Sicherheitsmechanismen
  - verbesserte Interoperabilität

- **Treibersoftware für das eingesetzte Betriebssystem**
  - Konfiguration des Netzwerkadapters (z. B. Kanalauswahl, WEP-Key Eingabe, etc.)
  - Anzeige der Signalqualität, des verwendeten Kanals, etc.
  - Debug-Informationen (z. B. verlorene Pakete, verbundene Basisstation, etc.)

- **Zentrale Netzwerkdienste**
  - Authentisierung (z. B. via RADIUS)
  - Vergabe von IP-Adressen (z. B. via DHCP)
  - Verschlüsselung (z. B. via IPSec, Kerberos oder SSL)
  - Abrechnung (z. B. durch geeignete Back-End Systeme auf Basis von RADIUS-Logfiles)

Anwendungsszenarien
Flexibel einsetzbar

- **im öffentlichen Bereich:**
  - Betrieb von Public Spots, Hot Spots:
    - Hotels
    - Flughäfen
    - Bahnhöfe
  - Abrechnungsmodelle:
    - Volumenabhängige Abrechnung
    - Zeitabhängige Abrechnung
    - Pauschal / Pre-Paid (Verkauf von Kontingenten)
    - Provisions- und Werbeumsätze über Zwangshomepages

- **im Unternehmen und im privaten Bereich:**
  - Vernetzung auch in denkmalgeschützten Gebäuden
  - einfache Vernetzung von Gebäuden an entfernten Lokationen
  - einfache Vernetzung von Außenbereichen oder Lagerhallen
  - hohe Investitionssicherheit und extrem schneller Aufbau

Sicherheit
Funknetzwerke sind unsicher

- **Angriffsszenarien:**
  - WEP-Verschlüsselung kann durch passives Abhören gebrochen werden – der Zeitraum bis zur Entschlüsselung hängt nur vom Verkehr im Funknetz ab (je mehr Verkehr, desto eher)
  - Erweitern des Netzwerkes durch nicht autorisierte Basisstationen (z. B. mit höherer Sendeleistung) oder Netzwerkkarten
  - Mitlesen und Analyse von Netzwerkverkehr, Fälschen von Netzwerkverkehr, um sensitive Informationen (z. B. Passwörter) zu gewinnen und SSL- bzw. SSH-Verbindungen zu übernehmen („Man-in-the-Middle“ Angriff)
  - ARP-Spoofing/ARP-Poisoning, um Verkehr aus dem Kabel auch über das Funknetzwerk zu leiten und so obige Aktivitäten durchzuführen

- **Gegenmaßnahmen:**
  - Fehlkonfigurationen (z. B. Werkseinstellungen) vermeiden
  - Einsatz von Client-Zertifikaten (bei SSL) und StrictHostKeyChecking (bei SSH)
  - Access-Listen (für MAC-Adressen) verwenden
  - Starke Verschlüsselung auf IP-Level einsetzen (z. B. IPSec)
  - Einsatz von Access Points mit IPSec-Funktion (wenn verfügbar)
  - Das Funknetzwerk muß immer als unsicheres Netzwerk betrachtet werden und ist deshalb vor der Firewall anzusiedeln
  - Der Zugriff auf Unternehmensresourcen darf vom Funknetz aus nur authentisiert und verschlüsselt möglich sein

Ausblick

- **IEEE 802.11a:**
  - verwendet das Unlicensed National Information Infrastructure (UNII) Band ab 5 GHz
  - verspricht bis zu 54 Mbit/s Übertragungsrate durch Orthogonal Frequency Divison Multiplexing (OFDM) Modulation bei geringerer Reichweite als IEEE 802.11b
  - nicht kompatibel zu IEEE 802.11b
- **IEEE 802.11g:**
  - verwendet das 2,4 GHz Band und auch CCK Modulation – ist deshalb abwärtskompatibel zu IEEE 802.11b
  - verspricht bis zu 54Mbit/s Übertragungsrate durch andere Modulation (OFDM oder PCBB)
  - „vorläufiger Standard“ bis zur Ratifizierung – Herstellerinteressen sind der Grund
- **Netzwerke für Jedermann/frau:**
  - Initiativen zur privaten Funkvernetzung in größeren Städten und Ballungsräumen
  - Keine Übertragungskosten, Gelegenheitsnutzer können sich einen ADSL-Anschluß teilen
- **Sicherheit bleibt ein Problem:**
  - Hersteller adressieren das Problem bisher zu wenig