



Wireless LAN – Funknetzwerke

Anwendungsbereiche, Geschäftsmodelle, Funktionsweise und Sicherheitsaspekte

Lange standen sie im Ruf einer kostenintensiven und leistungsschwachen Nischentechnologie. Heute werden sie bereits als **Alternative zu UMTS** gehandelt: **Funknetzwerke auf Basis des IEEE 802.11b Standards**.

Wurde der europäische Markt 1999 noch auf 120 Millionen Dollar geschätzt, so sollen die **Umsätze im Jahr 2006** einer Studie von Frost & Sullivan zufolge auf **über 350 Millionen Dollar** ansteigen. Der anhaltende Boom bei der Mobil- und Funktechnologie hat sich dabei als bedeutender Wachstumsmotor erwiesen.

Über zwei Jahre hat es gedauert, bis die Komponenten für drahtlose Netzwerke so weit entwickelt waren, dass sie eine **echte Alternative zu konventionellen Netzwerken** auf Basis von Kupferkabeln darstellen. Die Produkte haben inzwischen einen Reifegrad erreicht, der ihren Einsatz beim **schnellen Aufbau von Netzwerken mit hoher Investitionssicherheit** attraktiv erscheinen lässt.

Anwendungsbereiche und Geschäftsmodelle

Funknetzwerke sind insbesondere **für Aufgaben interessant, die konventionellen Netzwerken** auf Grund der aufwändigen Installation **bisher verschlossen geblieben sind**. Die Presse berichtet zunehmend über Funknetzwerke, die beispielsweise an **Flughäfen** oder in **Hotels** in Betrieb genommen werden – Orte an denen Reisende im wesentlichen mit Warten beschäftigt sind. Der **Nutzwert** für die Reisenden ist **unübersehbar**: So kann während der Wartezeit schnell noch das elektronische Postfach überprüft werden. In letzter Zeit steigt zudem in Ballungsräumen die Zahl der Initiativen, die **Funknetzwerke für jedermann** bereitstellen. Die so entstehenden "Funknetzwerk-Inseln" lassen sich innerhalb einer Stadt durch geschickte Platzierung der Basisstationen (Access Points) untereinander vernetzen. Zusätzlich bauen bereits einige kommerzielle Anbieter **Funknetzwerke in Innenstadtbereichen** - auf in der Hoffnung auf **zahlungskräftige Kundschaft**.

Die **Geschäftsmodelle der Anbieter**, die Funknetzwerke an solchen "HotSpots" oder "PublicSpots" bereit stellen, sind vielfältig: Mal wird die **verbrauchte Online-Zeit** abgerechnet, mal werden **Zeitkontingente** ähnlich der aus dem Handy-Umfeld bekannten Prepaid-Card angeboten. Wieder andere Anbieter setzen auf **Provisionsumsätze** aus Informationsangeboten, die sie Benutzern



Wireless LAN – Funknetzwerke

Anwendungsbereiche, Geschäftsmodelle, Funktionsweise und Sicherheitsaspekte

zwangsweise präsentieren, wenn diese über das Funknetz im WorldWideWeb surfen. Hier sind längst **nicht alle Möglichkeiten ausgeschöpft**.

IEEE 802.11b - was bedeutet das?

Die bisherige Entwicklung hat eine **erhebliche Anzahl** zum Teil konkurrierender **Standards** im Bereich der Funknetztechnologie hervorgebracht: GSM, GPRS, HSCSD, UMTS, imode, Bluetooth, DIRC, DECT, DAB und UWB - um nur die Wichtigsten zu nennen.

Auf dem **IEEE 802.11b Standard** (oft auch "Wireless Lan", "WLAN" oder auch "WiFi - Wireless Fidelity" genannt) basierende Funknetzwerke sind durch **folgende Merkmale** gekennzeichnet:

- Sie arbeiten im **2,4 GHz Band**.
- Sie verwenden **eines von zwei Übertragungsverfahren**: Frequency Hopping Spread Spectrum (FHSS) oder Direct Sequence Spread Spectrum (DSSS).
- Sie unterstützen Übertragungsgeschwindigkeiten von **1, 2, 5 und 11 MBit/s**.
- Sie unterstützen **Multi-Channel-Roaming**, das bei gleichzeitiger Nutzung mehrerer Zellen höhere Übertragungsgeschwindigkeiten ermöglicht.
- Sie bieten eine **Verschlüsselung** (Wireless Equivalent Privacy - WEP) mit verschiedenen Schlüssellängen, die sich allerdings inzwischen als unsicher erwiesen hat.

Bestandteile von Funknetzwerken

Für den Aufbau von Funknetzwerken sind **nur wenige Komponenten** erforderlich, die alle **mobil** sind und daher bei Umzügen oder Erweiterungen eine sehr **hohe Investitionssicherheit bieten**.

Wie jedes Funknetzwerk ist auch ein IEEE 802.11b basiertes Netz aus einzelnen Zellen aufgebaut. Jede Zelle wird von einem sogenannten **"Access Point"** gebildet, welcher sendet und empfängt. Access Points sind in den unterschiedlichsten Formen erhältlich. Der „Airport“ der Firma Apple, die als Pioniere Wireless LAN am Massenmarkt hoffähig machte, besticht durch sein futuristisches Design. Access Points anderer Hersteller bieten in der Regel weniger optischen Reiz und verraten ihre Funktion durch eine deutlich sichtbare Antenne.



Wireless LAN – Funknetzwerke

Anwendungsbereiche, Geschäftsmodelle, Funktionsweise und Sicherheitsaspekte

Das Gegenstück zum Access Point bilden die entsprechenden **Erweiterungen für PCs und Notebooks**. In der Regel handelt es sich hierbei um PCMCIA- bzw. PC-Karten. Für den Einsatz in Desktop-PCs werden diese über dafür vorgesehene Adapter in den PC eingebaut. Die Karten der meisten Hersteller erlauben es auch, direkt von PC-Karte zu PC-Karte zu funken und so ohne den Umweg über einen Access Point Daten zu übertragen. Diese Betriebsart wird meist als **"Ad-Hoc Modus"** bezeichnet. In Notebooks der neuesten Generation sind Funknetzwerkkarten oft bereits werkseitig eingebaut.

Neben der reinen Netzwerk-Hardware benötigt ein Funknetzwerk natürlich auch **Softwarekomponenten**. So sind für den Betrieb beispielsweise Dienste aufzubauen und zu konfigurieren, die Benutzer authentisieren, diese mit IP-Adressen versorgen und nach Benutzung des Netzwerkes ggf. eine **Rechnungsstellung** erlauben. Zum Teil ist solche Software bereits Bestandteil des Angebots verschiedener Hersteller - zum Teil können aber auch **Eigenentwicklungen** - besonders im Bereich der Abrechnung - notwendig werden.

Drahtlos = grenzenlos?

Um die **Sende- bzw. Empfangsreichweite** von Access Points und PC-Karten zu verbessern, kann bei manchen Fabrikaten die mitgelieferte Antenne gegen eine Bessere ausgetauscht werden. Damit ist es zum Beispiel möglich, **Entfernungen von mehreren Kilometern** zwischen zwei Access Points zu überbrücken – Sichtkontakt zwischen beiden Punkten vorausgesetzt.

Generell richtet sich die jedem Benutzer zur Verfügung stehende **Übertragungsgeschwindigkeit** nach der **Access Point "Dichte"** in seiner Umgebung. Die Access Point "Dichte" ist wiederum abhängig von der **Sendeleistung** der einzelnen Access Points und dem von ihnen abzudeckenden Gebiet. Beim Aufbau eines Funknetzwerks ist also die **"richtige" Platzierung** von Access Points eine der wichtigsten und schwierigsten Aufgaben. Dabei sind in der Regel **bauliche Gegebenheiten** (Stahlbeton, Holz, Wasser) zu berücksichtigen, die die Sendeleistung der einzelnen Access Points beeinträchtigen können.



Wireless LAN – Funknetzwerke

Anwendungsbereiche, Geschäftsmodelle, Funktionsweise und Sicherheitsaspekte

Mehr Freiheit – mit Sicherheit?

Der durch die Verfügbarkeit erschwinglicher Hardware verstärkte Einsatz von Funknetzwerken in verschiedensten Bereichen hat schnell die **Schwächen dieser Technologie** ans Licht gebracht. Erst kürzlich hat die **Demontage der WEP-Verschlüsselung** gezeigt, dass am grünen Tisch entworfene "Standards" diesen Namen nur nach ausgiebiger Praxiserprobung verdienen. Die Verschlüsselungstechnologie war ins Blickfeld von **Kryptographie-Experten** in aller Welt gerückt, die sie einer gründlichen Prüfung unterzogen - was bis dahin auf Grund der Struktur der Standardisierungsgremien unterblieben war.

Als Ergebnis dieser Prüfung sind nun **Werkzeuge verfügbar**, die das Entschlüsseln von über Funk übertragenem Netzwerkverkehr auf Basis statistischer Analyse ermöglichen. Bei heute gängigen Prozessortaktzahlen kann das **extrem schnell** gehen. Die **WEP-Verschlüsselung** von Funknetzen ist also **grundsätzlich als unsicher** anzusehen. Sie kann weder Authentizität noch Integrität und Vertraulichkeit von Daten gewährleisten.

Unternehmen und Benutzer, die sensitive Daten über Funknetzwerke transportieren wollen, müssen folglich **selbst für Verschlüsselung sorgen**. Das gilt auch für Anmeldeinformationen am Netzwerk, sofern nicht auf Authentisierungsdienste wie z. B. Kerberos zurückgegriffen wird. Auf **Anwendungsebene** können Daten unter **Verwendung von SSL/TLS** (z.B. https, IMAP-over-SSL) verschlüsselt werden. Verschlüsselung auf **Netzwerkebene** wird durch die **Verwendung eines VPN-Protokolls** wie z. B. IPSec erreicht. In Unternehmen sollte das Funknetz also außerhalb der Firewall liegen und den Zugriff auf Unternehmensressourcen nur authentisiert und verschlüsselt erlauben.

Die für die erforderliche Verschlüsselung anfallenden **Kosten** sind **nicht zu vernachlässigen**. Funktionierende frei verfügbare IPSec basierte Lösungen sind nämlich für diesen Anwendungsfall noch Mangelware. In der Regel wird also für jeden Arbeitsplatz, der mobil via Funk-LAN auf das Unternehmensnetzwerk zugreifen soll, eine Lizenz für einen IPSec-Client fällig.

Wireless LAN – Funknetzwerke

Anwendungsbereiche, Geschäftsmodelle, Funktionsweise und Sicherheitsaspekte

Fazit

Viele generelle Tendenzen weisen darauf hin, dass die verkabelte Kommunikation in absehbarer Zeit in Argumentationsnöte kommen wird. Funknetze bieten auf Grund ihrer **Mobilität** völlig **neue Nutzungsmöglichkeiten** und erschließen eine **neue Qualität** im Einsatz von Rechnern. Durch **sinkende Preise** bei gleichzeitiger **Ausweitung der Bandbreiten** haben sich Wireless LANs in der Zwischenzeit als **einfache und kostengünstige Alternativlösung** etabliert. Die **zukünftige Kommunikation** im teilnehmer-nahen Bereich wird, wo immer dies vorteilhaft ist, **drahtlos** sein.

Sie haben weitere Fragen zu Geschäftsmodellen, Aufbau und Sicherheit von Funknetzwerken? Unsere Berater stehen Ihnen gern zur Verfügung.

Ihre e-trend Team



e - t r e n d

Impressum

e-trends im Abo
Ausgabe 8
Oktober 2001
ISSN 1618-5854

Verantwortlich
Hauke Peyn (Geschäftsführer)
Volker Liedtke (Geschäftsführer)

e-trend
Media Consulting GmbH
Herforder Str. 74
33602 Bielefeld
fon +49(521) 96751-0
fax +49(521) 96751-99

<http://www.e-trend.de>
e-Mail: newsletter@e-trend.de

Newsletter-Abo unter
<http://www.e-trend.de/newsletter>

Alle Angaben ohne Gewähr
© Copyright e-trend 2001