

WLANs – Ethernet mal anders

Vorversion des Artikels Netzwerkzugang ohne Kabel
der NetworkWorld 1/2 Januar 2000, Seiten 22-24

Jean-Pierre Ebert und Berthold Rathke

Fachgebiet Telekommunikationsnetze

Technische Universität Berlin

Email: {ebert,rathke}@ee.tu-berlin.de

URL: <http://www-tnk.ee.tu-berlin.de/~{ebert,rathke}>

29. Januar 2000

Zusammenfassung

Funk LANs (WLAN) erfreuen sich immer größerer Beliebtheit, wie neueste Verkaufszahlen zeigen. Leistungsfähigkeit, Stabilität und Preis von WLANs sind mittlerweile in Bereichen, die Netzwerklösungen auf WLAN-basis für ein breiteres Anwenderspektrum interessant machen. Trotz dieser Fortschritte gibt es Knackpunkte, die vor dem Kauf und der Installation bedacht werden sollten. Der Artikel geht auf die wichtigsten Punkte ein.

WLAN Überblick

Der immer breitere Einsatz von Funk LANs (WLANs)

ist nicht nur sinkenden Preisen, verbesserter Leistungsfähigkeit, einem mittlerweile existierendem Standard und einem besseren Marketing geschuldet. Auch die Tatsachen, daß frühe Installationen den Nutzen dieser Technologie demonstriert haben und sich durch WLANs vertikale Netzwerkszenarios realisieren lassen, die Serviceverbesserungen und Kostenersparnisse mit sich bringen, haben dazu beigetragen. Noch interessanter werden WLANs durch jetzt verfügbare Hochgeschwindigkeitslösungen. Diese erlauben nunmehr mit bis zu 11Mbit/s Daten zu übertragen.

WLANs werden derzeit

in zwei Gremien standardisiert: ETSI (European Telecommunications Standards Institut) und IEEE (Institut of Electrical and Electronic Engineers). Die ETSI spezifiziert WLANs unter dem Synonym HIPERLAN (High Performance LAN) während das IEEE die schlichte Nummer 802.11 verwendet. Der IEEE 802.11 Standard wurde 1997 verabschiedet und unzählige Produkte sind hierfür verfügbar. Der HIPERLAN Typ 1 Standard wurde 1998 verabschiedet. Trotz der beeindruckenden Leistungsdaten ist hierfür nicht ein Produkt in Sicht. Einer der Gründe dürfte der in relativ kurzer Zeit zu erwartende Nachfolger

HIPERLAN Typ 2 sein. Dieser soll nicht nur Datenraten bis zu 54Mbit/s erlauben sondern auch eine Dienst differenzierung unterstützen. Das ist besonders dann interessant, wenn neben Daten auch Sprache oder Bilder übertragen werden sollen. Beim IEEE 802.11 sind ebenfalls zwei Standardisierungsaktivitäten angesiedelt, die sich mit Hochgeschwindigkeitsversionen von WLANs beschäftigen: IEEE 802.11a und IEEE802.11b. Letztere hat sich kürzlich auf die Endversion des Standards geeinigt, der Datenraten von bis zu 11Mbit/s unterstützt und dabei voll kompatibel zur Urversion ist, welche eine Datenrate von bis zu 2 Mbit/s erlaubt. IEEE 802.11a-basierte Systeme sollen wie auch HIPERLAN Typ 2 System eine Datenrate von bis zu 54 Mbit/s unterstützen. Interessanterweise gleichen sich beide Standards bis auf einige Details was Modulation, Kodierung und Systemparameter angeht. Signifikant unterschiedlich ist jedoch das sogenannte Medium Access Control - Verfahren, daß den Zugriff verschiedener Endgeräte auf die gemeinsam benutzte Funkressource regelt. Während das IEEE auf das bewährte CSMA/CA-

Verfahren (Carrier Sense Multiple Access / Collision Avoidance) setzt, geht HIPERLAN neue und aufwendigere Wege, um Echt-Zeit-Dienste zu ermöglichen. Mit einer Verabschiedung beider Standards ist im nächsten Jahr zu rechnen. Erste Produkte sind innerhalb der nächsten 1-2 Jahre zu erwarten. Welches der Systeme sich einmal durchsetzen wird, kann im Moment niemand sagen. Der Einsatz von WLANs birgt viele neue Möglichkeiten. Aber auch einige Knackpunkte sind zu beachten, die nachfolgend anhand des derzeit populären IEEE 802.11 Systems beschrieben sind.

1 Konkurrenz

Neben klassischen WLANs werden heute und in Zukunft auch andere Datenfunksysteme betrieben. Zuerst wäre hier Bluetooth und HomeRF zu nennen aber auch IRDA und DECT-basierte Lösungen zählen dazu. Ein potentiell Problem dabei sind die Frequenzbereiche (2.4/5.1 GHz), in denen solche Systeme hauptsächlich betrieben werden. Würden beispielsweise IEEE 802.11b und Bluetooth Systeme am gleichen Ort und zur selben Zeit betrieben, so ist mit

erheblichen Leistungsbeeinträchtigungen während des Betriebs zu rechnen. In diesem Fall kann das bis zum zeitweiligen Totalausfall des IEEE 802.11 Systems führen, während das Bluetooth System relativ unbeeinträchtigt weiter arbeitet. Eine Lösung für derartige Probleme ist noch nicht in Sicht. Hinzukommen noch Störungen von artfremden Systemen, wie beispielsweise Mikrowellen. Aber auch gleichartige Systeme, die beispielsweise in der Nachbarfirma installiert wurden und schon einen Teil der Funkressourcen belegen können zum Problem werden. Es obliegt also dem Anwender, derartige Störquellen im Netzwerkkonzept zu beachten oder zu eliminieren.

2 Komponenten

Um ein drahtloses Netzwerk aufzubauen, müssen einzelne Basiskomponenten des WLANs miteinander verbunden werden. Je nach Art und Typ der Basiskomponenten ergeben sich unterschiedliche Netzwerkkonfigurationen (siehe Bilder Grundkonfigurationen).

Um ein einfaches WLAN in Betrieb zu nehmen, werden Einschubkarten (Network Inter-

face Cards - NIC) für die Endsysteme benötigt. Ihre Ausführung wird von den jeweils verwendeten Endsystemen bestimmt. Laptops benötigen PCMCIA-NICs. Sie werden einfach in den PCMCIA-Einsteckplatz des Laptops hineingeschoben. Übliche Desktop PC Systeme benötigen Einschubkarten, die an den jeweiligen Systembus des PCs (z.B. ISA oder PCI) angepaßt sind. Es ist ein Trend zu erkennen, daß die Einschubkarten für Desktop PC Systeme einfach als PCMCIA-Karte mit einer entsprechenden Anpassung an den Systembus (PCMCIA-Laufwerke) realisiert werden. Diese Variante ist mit Blick auf die Kosten nicht nur attraktiv für die Hersteller sondern auch für den Benutzer, da er beispielsweise die PCMCIA-WLAN-Karte nur aus dem PCMCIA-Laufwerk ziehen muß, um sie wahlweise in einem Laptop zu verwenden.

Im Preis der Einschubkarten ist in der Regel die zweite Basiskomponente der WLANs - die Antenne - enthalten. Die mitgelieferte Antenne zeichnet sich zumeist durch eine omnidirektionale Abstrahlung der Funkwellen aus. Dies ist für die meisten Anwendungen ausreichend. Für spezielle Anwendungen ist

diese Art von Antennen ungünstig. Sollen beispielsweise zwei weiter auseinanderliegende Gebäude miteinander verbunden werden, kann unter Umständen die Leistung einer omnidirektionalen Antenne nicht ausreichen. Abhilfe schaffen sogenannte Richtantennen, die zumeist als Patch- oder Yagi-Antenne ausgelegt sind (siehe Bild Antennentypen). Sie erzeugen einen mehr oder weniger stark gebündelten Funkstrahl. Somit lassen sich Entfernungen von bis zu mehreren Kilometern überbrücken. Durch die starke Bündelung müssen Yagi-Antennen exakt ausgerichtet werden. Kleine Abweichungen führen zu großem Verlust an Bandbreite. Die Patch-Antenne ist dagegen einfacher zu handhaben, wenngleich auch die Reichweite darunter leidet. Sie wird mittels eines Klebestreifens an Decken oder Wänden fixiert. Ihre Bauform ist eher "platt". Dadurch ergibt sich eine Richtcharakteristik, die der einer Halbkugel ähnelt. Beim Kauf einer Zusatzantenne, sollte man jedoch darauf achten, daß sie mechanisch an die Einschubkarte angeschlossen werden kann. Dies ist nicht immer gewährleistet und bedeutet Zusatzkosten für den Erwerb einer ent-

sprechenden Einschubkarte.

Mit mehreren solcher Systeme, jeweils aus einem NIC und einer Antenne bestehend, kann man ein sogenanntes Ad-hoc WLAN aufbauen. Solche von der Art her "spontanen" Netze ergeben sich, wenn mehrere Endgeräte ohne weitere organisatorische Zwänge miteinander kommunizieren (Besprechungen, Konferenzen, etc.). Adhoc-Netze haben jedoch keinen Zugang zu anderen Netzwerken (Firmennetze, Fernsprechnetze, GSM usw.). In diesem Fall wird eine weitere Komponente - eine Basisstation - benötigt. Sie regelt den Zugang zu anderen Netzwerken. Am Markt erhältliche Basisstationen, bieten meistens einen Zugang zum Ethernet. Neuere Produkte, die speziell auch für den häuslichen Bereich entwickelt wurden, enthalten bereits Modems zum Anschluß an das Fernsprechnetzwirk. Zukünftig werden auch Übergänge zu ADSL Netzwerken mit höheren Bandbreiten verfügbar sein. Nebenbei entfällt auch zu Hause der Kabelsalat für den Anschluß von weiteren PC Komponenten wie Drucker und Fax. Diese Art von Netzwerk wird als "Single Cell"- Konfiguration bezeichnet. Werden mehrere

der Basisstationen gleichzeitig betrieben und über ein drahtgebundenes Netz miteinander verbunden, spricht man von Multi-Cell-Konfiguration. In Firmennetzen, hat die Basisstationen jedoch noch weitere Funktionen zu erfüllen. In der Regel sind heute drahtgebundene Netzwerke installiert, die Datenraten größer als 100 Mbit/s transportieren können. Da WLANs eine vergleichsweise niedrige Bandbreite haben, müssen die Funkzellen gegen unnötigen Datenverkehr geschützt werden. Basisstationen enthalten zu diesem Zweck Filterfunktionen. Mit ihnen wird der Datenverkehr gesperrt, der nicht für die mobilen Endsysteme bestimmt ist.

3 Leistungsdaten

Die Datenraten, die in den Spezifikationen der Hersteller angegeben werden, sind eindrucksvoll – 1, 2, 8, 11 Mbit/s und in Zukunft auch 54 Mbit/s. Das vor allem vor dem Hintergrund der bisherigen Möglichkeiten von wenigen Kbit/s (z.B. GSM), die selbst das Absenden einer simplen Textmail zum minutenlangen Wartespiel werden lassen. Aber was steckt wirklich hinter den Zahlen? Die angegebe-

nen Datenraten sind Bruttodatenraten. Sie geben an, mit welcher Geschwindigkeit ein Bitstrom auf den Funkkanal gesendet wird. Verschiedene Ursachen sorgen dafür, das die Applikation/Benutzer nur einen Teil der Bruttodatenrate wirklich nutzen kann. Messungen in unserem Hause mit einem 11 Mbit/s WLAN von Aironet haben gezeigt, daß im besten Falle mit einer Übertragungsrate von ca. 4.5 Mbit/s zu rechnen ist. Nicht besser sieht es bei den Konkurrenten aus. Die Ursache hierfür ist zum einen in der Fehleranfälligkeit des Kanals und zum anderen im Protokolloverhead zu suchen. Zum Protokolloverhead gehören notwendige Paketheader, Trailer, Steuernachrichten und sogenannte Guardtimes. Die Fehleranfälligkeit läßt sich grundsätzlich durch eine günstigere Positionierung des Sender/Empfänger-Paars verringern. Zusätzlich hat man die Möglichkeit mit einer geringeren Datenrate zu senden. Einige Hersteller unterstützen mit einer Automatik die Wahl der richtigen Datenrate. Wird der Funkkanal schlecht, wird auf eine niedrigere Datenrate umgeschaltet und umgekehrt. Wenn man jedoch aus verschiedenen Gründen nur mit einer bestimmten

Datenrate senden und trotzdem nur geringere Einbußen hinnehmen möchte, kann man sich mit einem kleinen Trick behelfen. Die meisten WLAN-Systeme haben einen Konfigurationsparameter, der die maximale Größe eines Datenpaketes festlegt. Im Idealfall – also optimale Übertragungsbedingungen – sollte hier der Maximalwert eingetragen sein. Weichen die Kanalbedingungen nach unten hin ab, z.B. viele Übertragungsfehler, dann sollte dieser Wert kleiner gewählt werden. Alle Datenpakete die länger als dieser Wert sind, werden zerhackt, übertragen und beim Empfänger wieder zusammengesetzt. Die Methode ist deshalb erfolgreich, weil es für kleinere Pakete unwahrscheinlicher als für große Pakete ist, von einem Bitfehler getroffen zu werden. Zur Reduktion des Protokolloverheads kann man nur wenig beitragen. Zwei vom Anwender zu beachtende Punkte spielen hier eine Rolle. Erstens sollten sich nie zuviele WLAN-Terminals gleichzeitig in einer Funkzelle befinden und hohe Übertragungsanforderungen haben. Zweitens sollten die zu übertragenden Datenpakete so groß wie möglich bleiben, d.h. sie sollten nur dann zerhackt werden, wenn sie zu

groß für die entsprechend schlechten Funkkanalbedingungen sind. Messungen haben gezeigt, das sich der Durchsatz von 4.4 Mbit/s bei einer Bruttodatenrate von 11 Mbit/s um eine Größenordnung reduziert, wenn statt 1500 Byte Pakete 256 Byte Pakete gesendet werden. Wenn man sich heutigen Internetverkehr anschaut, bei dem bis zu 70 % der transportierten Datenpakete kleiner sind als 500 Byte, kann man leicht erahnen, das selbst Nettodatenraten von 4.4 Mbit/s illusorisch sind.

4 Sicherheit

Funkübertragung wird als generell anfällig gegen Lauschangriffe betrachtet. Nicht so bei WLANs. Erstens macht es zumeist das Übertragungsverfahren sehr kompliziert das entsprechende Funksignal zu filtern. Zweitens sorgen verschiedene Verschlüsselungsroutinen wie Scrampling oder WEP (Wired Equivalent Privacy) für die nötige Sicherheit. Letzteres basiert auf dem RC-4 Verschlüsselungsalgorithmus der Fa. RSA, Inc. Problematisch ist jedoch, das viele WLAN-Hersteller zusätzliche proprietäre Verschlüsselungsroutinen anbieten, die

untereinander nicht kompatibel sind, so daß der gemeinsame sichere Betrieb von WLANs-Systemen verschiedener Hersteller nur dann möglich wäre, wenn alle Systeme die Verschlüsselung entweder abschalten oder den im Standard spezifizierten Verschlüsselungsalgorithmus verwenden.

5 Netzplanung

Die Netzplanung bedarf in WLAN-Netzen noch größerer Sorgfalt als in kabelgebundenen Netzen. Grund hierfür ist wiederum der Funkkanal, der fehleranfällig ist und nur eine beschränkte Kapazität besitzt. Während man beispielsweise bei zusätzlichen Bandbreitenbedarf in kabelgebundenen Lösungen einfach beliebig viele zusätzliche Kabel legen kann oder auf eine schnellere Übertragungstechnologie ausweicht, hat man bei WLANs nur beschränkte Möglichkeiten mehr Netzkapazität zu schaffen. Eine Möglichkeit wäre, mehrere Funkzellen zu überlagern, wobei das insbesondere bei hohen Übertragungsraten aufgrund der gegenseitigen Störeinflüsse nur begrenzt möglich ist. Läßt man Übertragungsraten von bis zu 11 Mbit/s

zu, so kann man lediglich 3 WLAN-Funkzellen überlagern ohne Leistungseinbußen hinnehmen zu müssen. Eine weitere wichtige Rolle bei der Netzplanung spielt die Platzierung von Endgeräten und Basisstationen. Besonderen Einfluß haben hier bauliche Aspekte, wie die Architektur und verwendete Materialien. Wenn ein WLAN in einer relativ offenen Umgebung (z.B. einem Großraumbüro oder Industriehalle) installiert wird, benötigt man voraussichtlich weniger Basisstationen als in einem Bürogebäude mit vielen kleinen Büros. Ein gewisser Spielraum ist durch die mögliche Variation der Datenrate gegeben. Bei niedrigen Datenraten lassen sich größere Entfernungen überbrücken, während bei hohen Datenraten die Konnektivität auf wenige Meter beschränkt sein kann. Ist an gewissen Orten eine geringere Datenrate akzeptabel, wird auch die Anzahl der notwendigen Basisstationen geringer ausfallen. Für die Planung von WLANs gibt es prinzipiell zwei Möglichkeiten. Die erste Möglichkeit erfordert einen genauen Bauplan des zu vernetzenden Areals. Danach kann man anhand von Funksignal-Dämpfungstabellen für bestimmte Materialien und Umgebungen

eine Abschätzung treffen, an welchen Stellen eine Basis- oder Relaystation platziert werden muß. Leider bieten nur einige wenige Hersteller solche Schätzhilfen an. Hinzu kommt, daß die Schätzung im Einzelfall falsch sein kann. Der zweite Ansatz ist in dieser Hinsicht akurater, wengleich auch teurer. Hierfür wird eine Basisstation und eine WLAN-Einschubkarte für einen PC oder Laptop benötigt. Nach der Plazierung und Installation der Basisstation wird von möglichst vielen Punkten im Gebäude oder der entsprechenden Umgebung mittels des PC/Laptops die Qualität des Links bestimmt. Hierfür wird von den meisten Herstellern eine produktspezifische Software bereitgestellt. Diese gibt Auskunft über Empfangsfeldstärken, Signalqualität, Rauschlevel, Verlustraten, etc. Anhand dieser Messungen kann entschieden werden, ob die Basisstation an einem anderen Ort platziert werden muß oder ob zusätzliche Basisstationen notwendig sind. Als dritte Option kommt die Auswahl eines entsprechenden Antennensystems in Frage.

6 Roaming

Bucht sich eine Mobilstation aufgrund sich verschlechternder Sende- und Empfangsbedingungen in einer anderen Funkzelle ein, spricht man von Roaming. Das Problem hierbei ist, daß dieser Umbuchungsvorgang zu einer längeren Unterbrechung einer bestehenden Netzwerkverbindung führen kann, da diese Verbindung von einer Basisstation an die neue Basisstation überreicht werden muß. In allen neueren WLAN-Produkten wurden hierfür sehr gute Lösungen integriert, die minimale Unterbrechungszeiten garantieren und sich je nach Produkt und Anwendungsfall über Parameter anpassen lassen. Das geht im Einzelfall sogar soweit, daß bei Überlast Mobilstationen in eine neue Funkzelle mit weniger Belastung umgebucht werden. Für den absehbaren Fall, daß WLAN-Netzwerkinterfaces verschiedenster Hersteller einmal miteinander kommunizieren können, ergibt sich jedoch ein neues Problem. Die verwendeten Roaming-Protokolle sind proprietär, so daß ein reibungsloses übergeben von Netzwerkverbindungen zwischen Basisstationen verschiedener Hersteller nicht möglich ist. Dieses Problem sollte mit

einem einheitliche Protokoll, das Inter-Access Point Protocol (IAPP) genannt wird, behoben werden. Leider beabsichtigen bisher nur weniger Hersteller den Einsatz dieses Protokolls.

7 Kompatibilität

Die Kompatibilität von WLANs kann aus 2 verschiedenen Richtungen betrachtet werden: Produktkompatibilität und Versionskompatibilität.

Unter Produktkompatibilität wird der gleichzeitige korrekte Betrieb von WLAN-Komponenten verschiedener Hersteller verstanden. Wer glaubt, wie bei Ethernet-Netzwerkinterfacekarten aus der Breite des Angebots frei auswählen zu können, wird sich arg enttäuscht sehen. Die WLAN-Produkte verschiedener Hersteller sind nur teilweise kompatibel, und das auch nur eingeschränkt. Genau dieser Punkt führte bisher zu einer gewissen Zurückhaltung bei potentiellen Käufern. Dieser Problematik haben sich hauptsächlich drei Organisationen – University of New Hampshire (USA) Interoperability Lab, Wireless LAN Alliance (WLANA) und Wireless Ethernet Compatibility Alliance

(WECA) – verschrieben. Alle namhaften WLAN-Hersteller sind in diesen Organisationen vertreten. Dort werden die offene Punkte im IEEE 802.11 Standard geschlossen und Kataloge für Minimalanforderungen erstellt, um die Kompatibilität der verschiedenen Produkte zu erreichen. Außerdem fungieren diese Organisationen als Zertifizierungsinstanzen. Unter Versionskompatibilität wird das korrekte Zusammenspiel verschiedener Generationen oder Typen von WLANs eines Herstellers verstanden. Hier sind nur kleinere Inkompatibilitäten zu verzeichnen, da schon der IEEE 802.11 Standard Mechanismen zur Rückwärtskompatibilität spezifiziert. Hersteller, die bisher nicht standardkonforme WLAN-Lösungen angeboten haben und jetzt jedoch zusätzlich standardkonforme Produkte verkaufen, bieten zumeist eine akzeptable Migrationslösung an.

8 Betriebssysteme

Eine weitere wichtige Frage für den Aufbau eines WLANs ist die Kompatibilität mit Betriebssystemen. Die Hersteller von WLANs bieten für nahezu alle gängi-

gen Betriebssysteme, wie Microsoft Windows oder Apple's MacOS Produkte an. Auch für das immer populärer werdende Unix-Derivat Linux, daß mittlerweile auch professionell genutzt wird, gibt es Betriebssystemunterstützungen. Für alle namhaften Produkte wurden Treiber entwickelt. Mehrere Probleme stellen sich hier. Die meisten Treiber wurden, wie bei Linux-Software üblich, nichtkommerziell und in der Freizeit von begeistertern Programmierern geschrieben. Da die WLAN-Hersteller zumeist zurückhaltend auf die Freigabe notwendiger Spezifikationen reagieren, kann es vorkommen, daß nicht alle möglichen Features der WLAN-Karten genutzt werden können. Ebenso hundert es bei der Portierung der Konfigurations- und Management-Software. Da jedoch Linux nicht mehr aus dem Betriebssystemmarkt wegzudenken ist und wahrscheinlich in Zukunft einen noch größeren Teil des Marktes besetzen wird, sollten diese Probleme bald vom Tisch sein.

Bits in der Luft

WLANs übertragen wie drahtgebundene System Ih-

re Daten in Bits und Bytes. Da jeder Übertragungskanal seine Spezifika besitzt, müssen die zu übertragenen Bits vorher umgewandelt (moduliert) werden. Die Anforderungen an ein solches Modulationsverfahren werden durch das Einsatzgebiet und technische Randbestimmungen wie beispielsweise bereitgestelltes Frequenzband bestimmt. Besonders wichtig ist, dass Modulationsverfahren für WLAN robust gegen Störeffekte wie Mehrwegeausbreitung des Funksignals sind. Mehrwegeausbreitung ist vor allem dann gegeben, wenn man ein WLAN in Gebäuden betreibt, da hier das Funksignal von Wänden, Decken, Fenstern und Fußböden gleichzeitig reflektiert werden kann. Aufgrund der unterschiedlichen Signalwege kommt das gleiche Signal mehrmals und gegebenenfalls zeitversetzt am Empfänger an, was zur Auslöschung des Funksignals führen kann. Weiterhin sollte ein Modulationsverfahren robust gegen Stör- und Lauschangriffe sein, da dies insbesondere wichtig für den kommerziellen Einsatz ist. Zu den durch die technischen Randbedingungen gesetzten Forderungen gehören die effiziente Ausnutzung des verfügbaren Frequenz-

spektrums sowie die preiswerte Implementierbarkeit, die letztendlich Auswirkung auf den Verkaufspreis von WLANs hat.

Fast alle heute verfügbaren WLANs benutzen ein Spreizspektrum-Verfahren, obwohl der IEEE802.11-Standard auch explizit ein Infrarot-Übertragungsverfahren spezifiziert. Das Spreizspektrumverfahren wurde in den 40er Jahren durch die amerikanischen Militärs entwickelt, um eine abhör- und stör-sichere sowie robuste Übertragung von sensiblen Daten zu gewährleisten. Beim Spreizspektrum-Verfahren (Spread Spectrum) wird ein schmalbandiges Funk-signal mit relativ hoher Leistung auf ein breiteres Frequenzspektrum verteilt (siehe Bild Direct Sequenz Spread Spectrum Prinzip I). Das resultierende Signal unterscheidet sich letztendlich nicht mehr von dem des natürlichen Weißen Rauschens. Somit ist es beispielsweise für einen Abhörer äußerst schwierig das Funksignal zu detektieren oder auch zu stören. Für die Spreizung des Signals gibt es wiederum zwei Verfahren, welche im Fachgebrauch als Frequency Hopping und Direct Sequence Spread Spectrum (FH/DSSS) be-

zeichnet werden. Bei erstgenanntem Verfahren wird nach einer jeweils sehr kurzen Übertragungszeit die Übertragungsfrequenz gewechselt (siehe Bild Frequenz Hopping Spread Spectrum Prinzip). Beim DSSS-Verfahren wird das Signal mit einer bestimmten Bitfolge die eine Frequenz von 11Mbits/s hat multipliziert (siehe Bild Direct Sequenz Spread Spectrum Prinzip II). Ein Empfänger kann nur dann das entsprechende Signal empfangen, wenn er synchronisiert ist und entweder die Abfolge der Sprungfrequenzen kennt bzw. die Bitfolge, mit der das Signal multipliziert wurde. Um unterschiedliche Bitraten zu erzielen werden spezielle Modulationsverfahren eingesetzt, die den jeweiligen Spreizspektrum-Verfahren vorgeschaltet sind. Als Daumenregel gilt, dass je höherwertig das Modulationsverfahren und letztendlich die Datenrate, desto höher ist die Fehleranfälligkeit der Übertragung. Das ist auch der Grund dafür, warum beispielsweise beim DSSS-WLANs die überbrückbaren Entfernungen mit der Bitrate sinken. Moderne WLAN-Systeme haben deshalb ein sogenanntes Automatic-Rate-Select implementiert, welches au-

tomatisch die richtige Modulation für die entsprechenden Umgebungsbedingungen einstellt. Die sich anschließende Frage, welches Übertragungsverfahren (FH/DS) nun das bessere ist kann nicht pauschal beantwortet und hängt vom jeweiligen Einsatzzweck ab. Informationen hierzu sind beispielweise in sogenannten White Papers auf den WWW-Seiten von Funk-Chip-Herstellern wie Intersil oder direkt den WLAN-Produzenten erhältlich.

Zukünftige WLANs mit noch höheren Übertragungsraten von bis zu 54 Mbit/s setzen auf eine neue Übertragungstechnologie und ein neues Frequenzband im 5GHz-Bereich. Das Übertragungsverfahren hierfür relativ aufwendige und wird Orthogonal Frequency Division Multiplexing (OFDM) genannt. Leider halten sich Chip-Hersteller und WLAN-Produktentwickler sehr bedeckt, so dass nichts über die realen Eigenschaften und Leistungsmerkmale solcher System bekannt ist.

Zusammenfassung

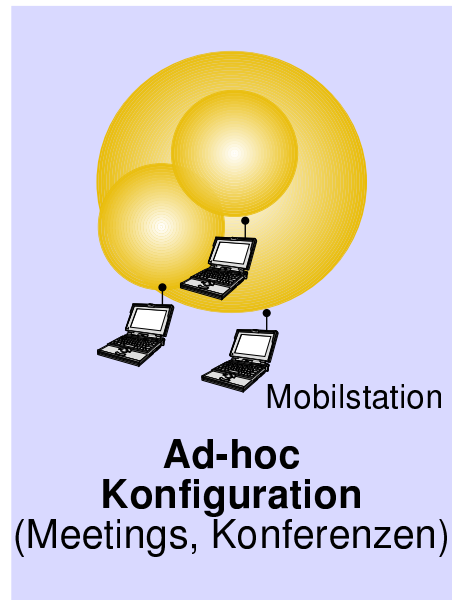
WLANs sind nicht nur eine ernstzunehmende Alternative zu drahtgebundenen LANs sondern bie-

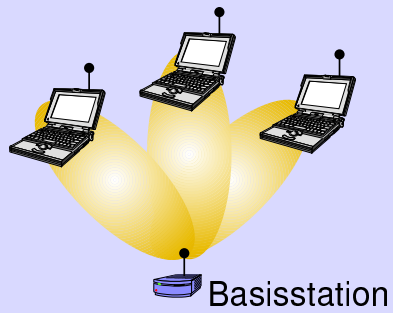
ten darüber hinaus weitere Dienste und Möglichkeiten an. Für einen erfolgreichen Aufbau und Betrieb eines solchen Funknetzes sind jedoch sorgfältige Vorüberlegungen und Tests notwendig.

Abbildungen

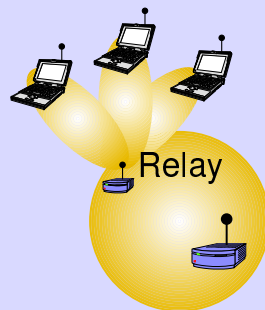
Bilder lassen sich beliebig skalieren, da in eps-Format. Original Macromedia-Freehand-Dateien für Macintosh sind mitgeliefert. Bilder sind in Farbe.

Gundkonfigurationen

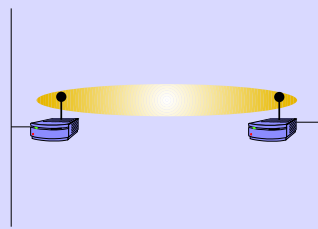




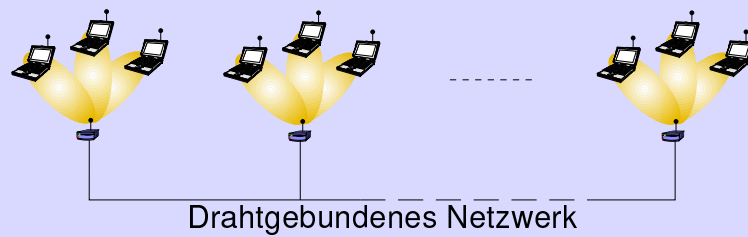
**Single Cell
Konfiguration**
(Bürräume, Home)



**Relay
Konfiguration**
(Umgebung mit
schlechtem Empfang)






**“Punkt-zu-Punkt”
Konfiguration**
(Gebäudeverbindung)



Verkabelte Konfiguration
(Gebäude)

Antennentypen

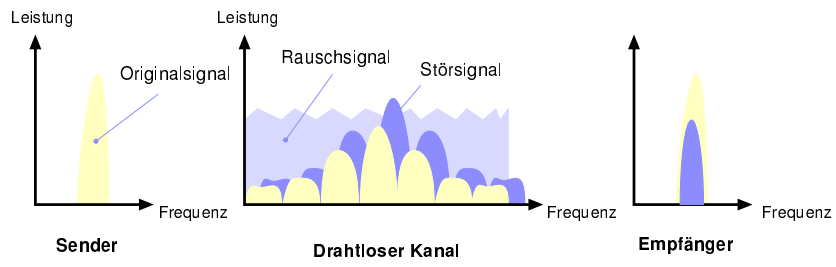
Antennentyp	Charkteristik	Reichweite
Ominidirektional		Mehrere Büroräume
Patch		Mehrere Büroräume
Yagi		Mehrere Kilometer

Sprachunterstützung der WLAN-Technologien

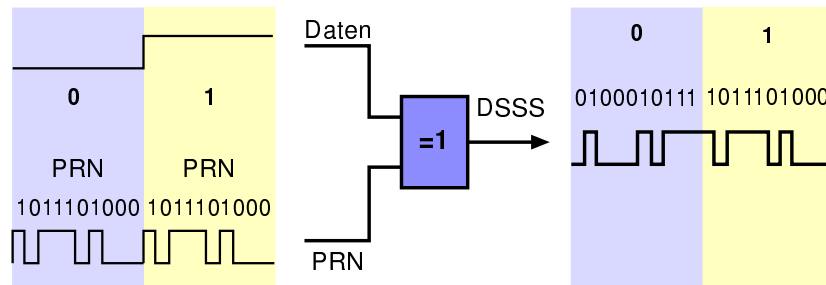
Technology	max. Datenrate in Mbit/s	Sprache
HIPERLAN I*	20	nein
HIPERLAN II*	54	nein
IEEE 802.11	2	ja**
IEEE 802.11a*	54	ja
IEEE 802.11b	11	ja**
Bluetooth*	2	ja
HomeRF*	2	ja
DECT (LAN)	0,192	ja
IrDA	4	nein

* zur Zeit keine Produkte verfügbar ** nicht implementiert

Modulation

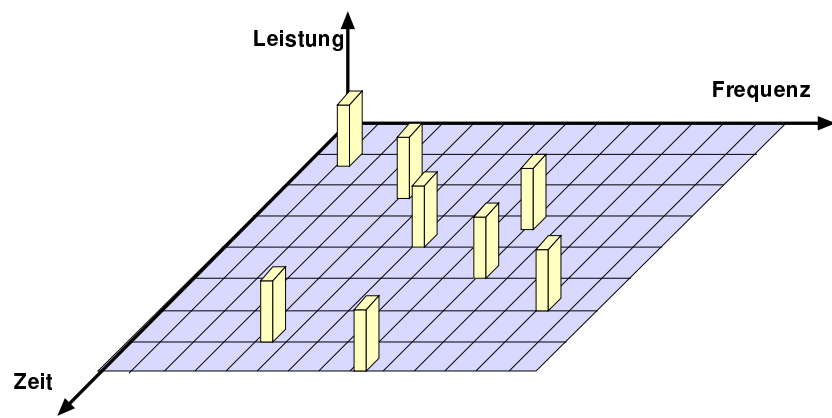


Direct Sequence Spread Spectrum (DSSS) Prinzip



PRN: Pseudo Random Numerical

Direct Sequence Spread Spectrum (DSSS) Prinzip



Frequency Hopping Spread Spectrum (FHSS) Prinzip