

gebundenen peripheren Rechner an ein größeres Netzwerk (siehe Abb. 5.64).

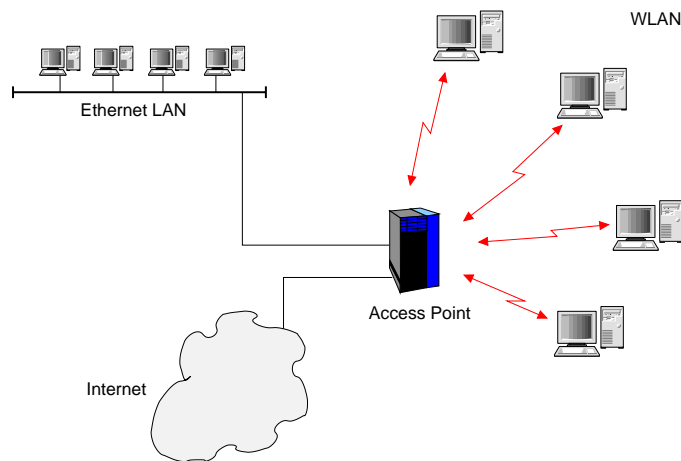


Abb. 5.64. Anbindung eines sternförmigen Funknetzes an weitere Netzwerke

IEEE 802.11 - Wireless Networks. Damit sich WLANs auf breiter Basis durchsetzen konnten, bedurfte es eines Industriestandards wie bei den anderen, bereits behandelten Netzwerkstandards, z.B. Ethernet oder Token Ring. Die für die Standardisierung im LAN-Bereich zuständige Untergruppe IEEE 802 des Institute of Electrical and Electronics Engineers rief daher das zugehörige Kapitel IEEE 802.11 WLAN ins Leben, das einen ersten Standard für drahtlose LANs bereits 1997 verabschiedete. Der ursprüngliche Standard arbeitete im Radiofrequenzbereich (RF) um 2,4 GHz und sah eine Datenübertragungsrate von 1-2 Mbps vor. Die beiden Nachfolgestandards IEEE 802.11a und IEEE 802.11b arbeiten im Bereich von 5,8 GHz bzw. 2,4 GHz und erreichen Übertragungsraten von 5 Mbps bis zu 54 Mbps. 802.11b besitzt eine Übertragungsreichweite von etwa 50 Metern. Zur Redundanzabsicherung und um eventuell auftretende Übertragungsfehler zu vermeiden, wird die in der Praxis erreichbare Datenübertragungsrate auf etwa 70% der theoretisch möglichen festgesetzt. In Tabelle 5.14 sind die einzelnen zu IEEE 802.11 gehörigen Substandards und Untergruppen dargestellt.

In der untersten Protokollschicht des IEEE 802.11 Standards besteht das Problem, daß auf dem für die Datenübertragung zugeteilten Frequenzband oft viele verschiedene Rechner miteinander kommunizieren wollen, wobei sich deren geografischer Standort überschneidet. Wie können also unterschiedliche Kommunikationspartner in einem (oder mehreren überlappenden) Funknetzwerk(en) voneinander unterschieden werden? Zur Lösung dieses Problems wurden in der physikalischen Schicht zwei unterschiedliche Modu-

Tabelle 5.14. IEEE 802.11 und seine Untergruppen

802.11a	54 Mbps im 5 GHz Frequenzband (2002)
802.11b	11 Mbps im 2,4 GHz Frequenzband (1999)
802.11d	zusätzliche Länder
802.11e	Verbesserungen Übertragungsqualität, Sicherheit
802.11f	Inter Access Point-to-Point Protocol
802.11g	20 Mbps im 2.4 GHz Frequenzbereich (in Arbeit)
802.11h	5 GHz Frequenzspektrum und Sendestärkenmanagement
802.11i	Verbesserungen der Sicherheit

lationsverfahren für die Datenübertragung spezifiziert: **Direct Sequence Spread Spectrum (DSSS)** und **Frequency Hopping Spread Spectrum (FHSS)** (siehe Abb. 5.65). Ursprünglich entworfen durch das Militär, definieren beide unterschiedliche Datenübertragungsverfahren, die sich durch hohe Zuverlässigkeit auszeichnen.

FHSS unterteilt dabei das verfügbare Frequenzband in einzelne Kanäle. Es nutzt eine Schmalbandträgerwelle, die permanent ihre Frequenz quasi zufällig nach dem sogenannten **Gaussian Frequency Shift Keying** Verfahren (**GFSK**) wechselt, was eine gewisse Sicherheit gegenüber Abhörversuchen bietet, da ein unberechtigter Dritter nicht in der Lage ist, vorherzusagen, auf welche Frequenz als nächstes gewechselt wird und so das vollständige Signal nicht empfangen kann. Dieses Verfahren ermöglicht es, über FHSS gleichzeitig verschiedene Netzwerke innerhalb desselben physikalischen Raums zu nutzen, wobei die einzelnen Netzwerke unterschiedliche über GFSK festgelegte Frequenzsignaturen nutzen.

DSSS auf der anderen Seite arbeitet vollkommen anders. Es kombiniert den Datenstrom mit einem digitalen Code von höherer Geschwindigkeit, d.h. jedes Datenbit wird auf eine zufällige Bitfolge – den sogenannten **Chipping Code** – abgebildet, die jeweils nur Sender und Empfänger bekannt ist. 1 und 0 werden dabei jeweils durch den Chipping Code und dessen Invertierung repräsentiert und erhalten dadurch eine bestimmte Bitsignatur, über die sie identifiziert werden können. Diese Art der Frequenzmodulation gewährleistet bei entsprechender Synchronisation sogar eine eigene Fehlerkorrektur und ist daher robuster gegenüber zufälligen oder beabsichtigten Störungen.

Die nächsthöher gelegene Protokollschicht des IEEE 802.11 Standards, der Medium Access Layer (MAC), regelt den Vielfachzugriff auf das gemeinsam genutzte Übertragungsmedium. Das im WLAN angewendete Verfahren ist dem bei kabelbasierten Ethernet angewendeten CSMA/CD Algorithmus sehr ähnlich. Wie in dem im Ethernet-Standard IEEE 802.3 festgelegten Zugriffsverfahren verfügen alle Teilnehmer über ein gemeinsames Zugriffsrecht. Um nicht von vorne herein eine Kollision auszulösen, darf bei CSMA/CD ein Rechner nur dann einen Sendevorgang starten, wenn kein Signal auf dem gemeinsam genutzten Übertragungsmedium entdeckt wird. Ebenso überwacht gemäß den IEEE 802.11 Spezifikationen ein Rechner im WLAN den empfan-

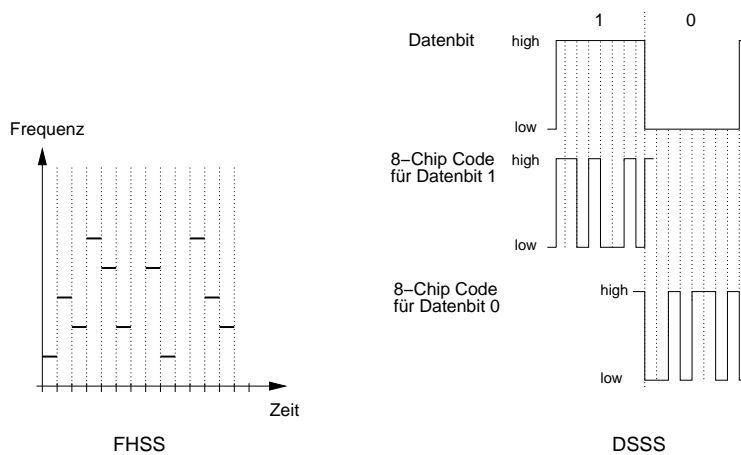


Abb. 5.65. FHSS und DSSS Frequenzmodulationsverfahren für IEEE 802.11 Wireless LAN

genen Energiepegel auf einer zugeteilten Funkfrequenz, um festzustellen, ob ein anderer Rechner gerade eine Datenübertragung durchführt. Wird erkannt, daß ein bestimmter Kanal für eine gewisse Zeitspanne, die als **Distributed Interframe Space** bezeichnet wird, frei ist, darf ein Rechner mit seiner Übertragung starten. Der Empfänger bestätigt den Empfang einer vollständigen Nachricht nach Ablauf einer als **Short Interframe Spacing** bezeichneten Zeitspanne. Wird erkannt, daß der Kanal gerade besetzt ist, wird ein Backoff-Algorithmus angestoßen und der Rechner wartet eine zufällig gewählte Zeitspanne, bevor er den nächsten Senderversuch unternimmt.

Im Gegensatz zum CSMA/CD Algorithmus, der nach einer erkannten Kollision von Datenpaketen entsprechende Maßnahmen einleitet, um den Parallelzugriff verschiedener Teilnehmer zu regeln, wird in IEEE 802.11 ein Kollisionsvermeidungsverfahren angewendet: **Multiple Access with Collision Avoidance (MACA)**. Dieses Verfahren ist kostengünstiger zu implementieren als eine Kollisionserkennung, die die Fähigkeit zum gleichzeitigen Senden und Empfangens voraussetzt. Der Sender veranlaßt dabei im MACA-Verfahren den Empfänger, ein kurzes Datenpaket zu versenden, das alle Teilnehmer in der näheren Umgebung, die einen Konflikt auslösen könnten, dazu bewegt, für die Dauer der Übertragung des nachfolgenden langen Datenpakets keine eigenen Pakete zu versenden.

Angenommen, Rechner A möchte ein Paket an Rechner B senden (siehe Abb.5.66).

- Dann sendet A zunächst ein sehr kurzes, sogenanntes RTS-Datenpaket (Request to Send) (siehe Abb.5.66 (a)), das unter anderem die Länge des eigentlich zu versendenden und in der Regel wesentlich längeren Paketes enthält.

- B antwortet darauf mit einem CTS-Paket (Clear to Send) (siehe Abb.5.66 (b)), das ebenfalls die von A bereits versendete Längeninformation enthält.
- Sobald A das CTS-Paket empfängt, startet A mit dem Versenden des eigentlichen Datenpakets. Jeder Rechner, der das von A gesendete RTS-Paket empfangen hat, muß sich in der Nähe von A befinden und verhält sich nun mindestens solange ruhig, bis das CTS-Paket wieder zurück bei A angekommen ist.
- Jeder Rechner, der das von B übertragene CTS-Paket mitempfängt, befindet sich in der Nachbarschaft von B, und muß für die Zeit der anstehenden Datenübertragung, deren Länge aus dem CTS-Paket entnommen werden kann, das Senden einstellen.
- Ein Rechner C, der sich zwar in Reichweite von A, aber nicht von B befindet und das RTS-Paket zwar empfängt, aber nicht das CTS-Paket, darf während der bevorstehenden Datenübertragung zwischen A und B senden, solange dies nicht mit dem CTS-Paket in Konflikt gerät.
- Anders verhält es sich mit Rechner D, der sich zwar in Reichweite von Rechner B, aber nicht in der von A befindet. D empfängt das CTS-Paket, aber nicht das RTS-Paket. Aus dem Empfang des CTS-Pakets schließt D, daß er sich nahe eines Rechners befindet, der gleich ein Datenpaket empfangen wird, und verhält sich über die im CTS-Paket angegebene Zeitspanne ruhig.
- Trotz dieser Vorsichtsmaßnahmen können Kollisionen auftreten, z.B. wenn B und C zur gleichen Zeit ein RTS-Paket an A versenden. Dieses RTS-Paket geht aufgrund einer Kollision verloren. Stellt ein sendewilliger Rechner fest, daß sein Sendeversuch nicht erfolgreich war, wartet er eine zufällig festgelegte Zeitspanne und beginnt danach erneut seine Übertragung. Dabei wird derselbe Binary Backoff Algorithmus angewendet wie im Falle des CSMA/CD-Algorithmus.
- Zusätzlich sendet der Empfänger nach dem erfolgreichen Empfang des Datenpakets eine Bestätigung (Acknowledgement) zurück an den Sender. Bleibt diese Bestätigung aus, so unternimmt der Sender nach Ablauf einer zufälligen Zeitspanne einen erneuten Sendeversuch.

Da die Definition des IEEE 802.11 Standards noch nicht abgeschlossen ist, fehlen noch festgeschriebene Lösungen für einige wichtige Probleme, wie z.B. ein Standardmechanismus für das sogenannte **Roaming** – dem Übergang vom Sende-/Empfangsbereich eines Access Points (AP) zum nächsten.

Sicherheitsaspekte im WLAN. Funkbasierte lokale Netze können von vornherein nicht ein vergleichbares Niveau an Sicherheit bieten, wie ein kabelgebundenes Netz. Da in WLANs die Luft des freien Raums als Übertragungsmedium genutzt wird, ist hier eine nichtautorisierte Nutzung oder das Abhören des Datenverkehrs wesentlich leichter. Ein sogenannter **Network Sniffer**, der den gesamten Datenverkehr auf einem vorgegebenen Übertragungsmedium mitschneiden und sicherheitsrelevante Informationen her-

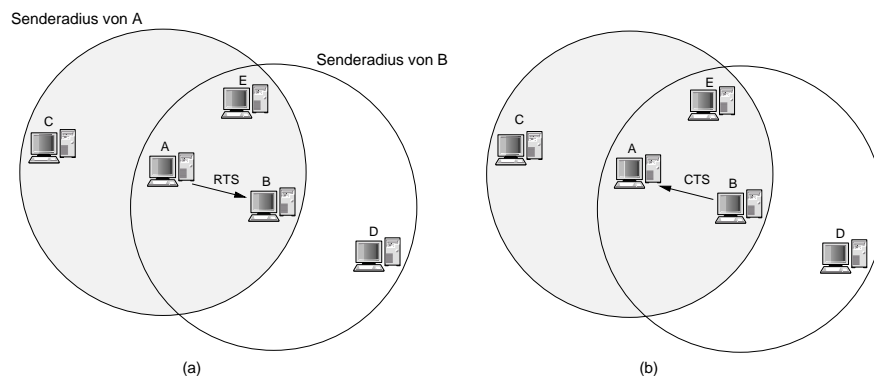


Abb. 5.66. Der MACA Algorithmus zur Kollisionsvermeidung. In (a) sendet A ein RTS-Datenpaket an B und in (b) antwortet B darauf mit einem CTS-Paket

ausfiltern kann, ist ohne Probleme in ein WLAN einzubringen, da kein physikalischer Kontakt zum eigentlichen Netzwerk notwendig ist, wie etwa bei kabelgebundenen Netzwerken.

Auch die Entdeckung eines WLANs fällt einem potentiellen Angreifer in der Regel sehr leicht. Um den am WLAN teilnehmenden Rechnern Zugang zu gewähren, sendet ein Access Point unverschlüsselt sogenannte **Beacon**-Datenpakete aus, um sich bekannt zu machen. Ein mobiler Angreifer muß deshalb nichts weiter tun, als eine Antenne auf sein Autodach zu montieren und während der Fahrt nach Beacon-Datenpaketen zu fahnden. Diese Form des Ausspähens von Funkdatennetzen wird auch als **Parkplatz-Attacke** (Parking Lot Attack) bezeichnet (siehe Abb. 5.67). Eine Firma kann sich zwar über eine Firewall vor unberechtigtem Zugriff aus dem drahtgebundenen Internet schützen, die im Firmennetz befindlichen APs sind jedoch zunächst von dieser Art Schutzmechanismus ausgeschlossen.

Prinzipiell werden die folgenden Arten von Angriffen auf WLANs unterschieden:

- passive Angriffe zur Entschlüsselung des Datenverkehrs durch Methoden der statistischen Analyse,
- aktive Angriffe, um neuen Datenverkehr von nicht autorisierten mobilen Rechnern in das WLAN einzubringen,
- aktive Angriffe zur Entschlüsselung des Datenverkehrs durch Täuschung des AP und
- Wörterbuch-erzeugende Angriffe, die den Datenverkehr über einen längeren Zeitraum aufzeichnen und mit dem Ziel analysieren, eine Echtzeitent-schlüsselung des Datenverkehrs zu erreichen.

Um Angriffen von potentiellen Hackern zu entgehen, die die bereits bekannten Sicherheitslücken der WLAN-Technologie ausnutzen, wurde in IEEE 802.11b das sogenannte **Wired Equivalency Protocol (WEP)** definiert. Ziel die-

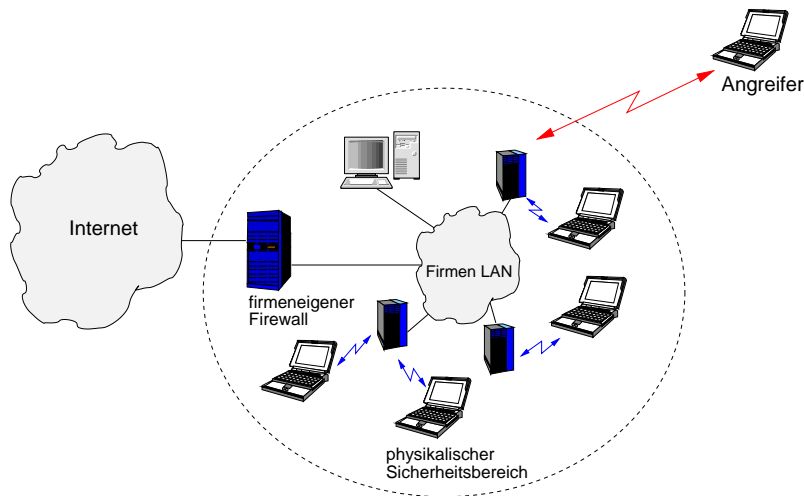


Abb. 5.67. Potentielle Angreifer können in WLANs über die sogenannte *Parking Lot Attack* eindringen

ses Protokolls ist es, die Privatsphäre im WLAN durch Verschlüsselung der übertragenen Datenpakete zu gewährleisten, mit der Nebenfunktion, unautorisierten Zugang zu verhindern. Ein zuverlässiger Schutz von einem Endgerät zum nächsten kann aber auch damit nicht erreicht werden. Das WEP-Protokoll basiert auf einem geheimen, symmetrischen Schlüssel, der zwischen dem AP und anderen teilnehmenden Rechnern vereinbart wird. Mit diesem Schlüssel werden die Datenpakete verschlüsselt, bevor sie versendet werden. Zusätzlich werden die Datenpakete auf Unversehrtheit überprüft, um sicherzustellen, daß sie nicht auf ihrem Weg manipuliert worden sind. Der IEEE 802.11b Standard sieht aber keine Prozedur für das Verteilen der Schlüssel vor. Daher wird in den meisten WLAN-Implementationen so vorgegangen, daß ein einziger Schlüssel manuell festgelegt und dann den teilnehmenden Rechnern vom AP aus übermittelt wird.

Ein weiteres Problem der WEP-Verschlüsselung (siehe Abb. 5.68) liegt im verwendeten Verschlüsselungsalgorithmus, dem **RC4**, einem sogenannten Stream Cypher Algorithmus, selbst begründet. Stream Cypher Algorithmen expandieren einen kurzen, vorgegebenen Schlüssel, den sogenannten **Initialisierungsvektor (IV)**, in einen unendlichen Strom von Pseudozufalls-Schlüsseln. Um den verschlüsselten Text zu erzeugen, der übertragen werden soll, wird dieser Schlüsselstrom mit den eigentlichen Daten, die gesendet werden sollen, bitweise über die Boolesche Operation XOR verknüpft. Der Empfänger kann durch Anwenden derselben Methode die Ursprungsdaten aus den verschlüsselten Daten leicht wiedergewinnen.

<http://www.springer.com/978-3-540-44276-9>

WWW

Kommunikation, Internetworking, Web-Technologien

Meinel, C.; Sack, H.

2004, XLII, 1178 S. In 2 Bänden, nicht einzeln erhältlich.,

Hardcover

ISBN: 978-3-540-44276-9