Albert-Ludwigs-Universität Freiburg
Institut für Informatik
Lehrstuhl für Rechnernetze und Telematik

WS 2007/2008

Seminararbeit

WLAN
Der 802.11 Standard

Daniel Guagnin

8. Januar 2008

Betreut durch Prof. Christian Schindelhauer

Abstract

Eine kurze Übersicht wofür Wireless LAN eingesetzt wird, beziehungsweise aus welchen Bedürfnissen es enstand. Im Anschluss daran werden wesentliche Punkte der Media Access Control Schicht des 802.11 Protokolls erläutert.

Inhaltsverzeichnis

1 Einleitung

Im ersten Abschnitt wird der Frage nachgegangen, aus welchen Bedürfnissen WLAN entstand, beziehungsweise welche Verwendungsmöglichkeiten es bietet, und welche Anforderungen sich daraus an das 802.11 Protokoll ergeben. Dabei wird auch eine kleine Übersicht alternativer drahtloser Datenübetragungsprotokolle geboten. Im folgenden Abschnitt wird schließlich auch auf wesentliche Merkmale des 802.11-Protokolls eingegangen und die Funktionsweise grundlegend erläutert. Im abschließenden Abschnitt wird ein kleiner Ausblick über mögliche Problemstellungen oder Chancen drahtloser Datenübertragungstechniken gegeben.

2 Motivation

Zur Motivation der Thematik werden verschiendene Verwendungsmöglichkeiten von WLAN angesprochen und daraus resultierende Ansprüche formuliert, sowie eine Übersicht über verschiedene drahtlose Technologien dargestellt. Anschließend wird ein kleiner Abriß der Entstehungsgeschichte des Wireless LAN gezeichnet.

2.1 Verwendungsmöglichkeiten

Wenngleich die frühen WLAN-Produkte als Substitute für LAN angepriesen wurden, konnte WLAN bisher Wired LAN noch nicht vollständig ersetzen. Gründe hierfür liegen hauptsächlich in der Durchsatzrate und der Sicherheit, die sich erst in den letzten Jahren an den LAN Standard annähern. Ein weiterer Grund könnte die Tatsache sein, dass als WLAN auf den Markt kam, die nötige Kabel-Infrastruktur in vielen Computer-Netzwerkumgebungen schon installiert war, und somit die Kostenersparnis der Kabel nicht gegeben war, außerdem standen diesen Kosten sehr hohe Preise der WLAN-Produkte gegenüber. Somit etablierte sich WLAN hauptsächlich als Erweiterung der Wired LANs. Das heißt, dass an ein bestehendes LAN Access-Points angeschlossen werden, um das bestehende Netzwerk zu erweitern (LAN-Extension genannt). Die Konstellation verschiedener WLAN-Zellen (Basic Sets), die via eines Backbone verbunden sind wird in der Literatur Extended Set Service genannt.[4]

Diese Erweiterung des Netzwerkes ermöglicht den Nomadischen und Mobilen Zugang. Nomadisch steht hier für die stationäre Nutzung von verschiedenen, wechselnden Orten aus, mobiler Zugang hingegen bedeutet die Netzanbindung während sich der mobile Client selbst bewegt (Beispielsweise ein WLAN-Telefonat, während sich der Benutzer durch

eine große Lagerhalle bewegt). Besondere Anforderungen stellen sich dabei beim Durchlaufen verschiedener WLAN-Zellen, da hier die Anmeldung am neuen Access Point gemanaged werden muss, während gerade bei Sprachapplikationen die Durchsatzrate nicht abbrechen darf.

Eine weitere Verwendungsmöglichkeit drahtloser Datenkommunikation ist die Verbindung zweier Netzwerke, die in verschiedenen, nicht all zu weit voneinander entfernten, Gebäuden liegen. In Anbetracht der Kosten die das Aufreißen der Strasse verursachen würde, ist eine Verbindung über eine drahtlose Bridge hier naheliegend.

Als letzte Möglichkeit, die hier Erwähnung finden soll, sei das Ad Hoc Netzwerk genannt, das sich vor allem zum spontanen Datenaustausch zwischen mobilen Stationen anbietet. Hierbei wird keine Access-Point-Infrastruktur benötigt.

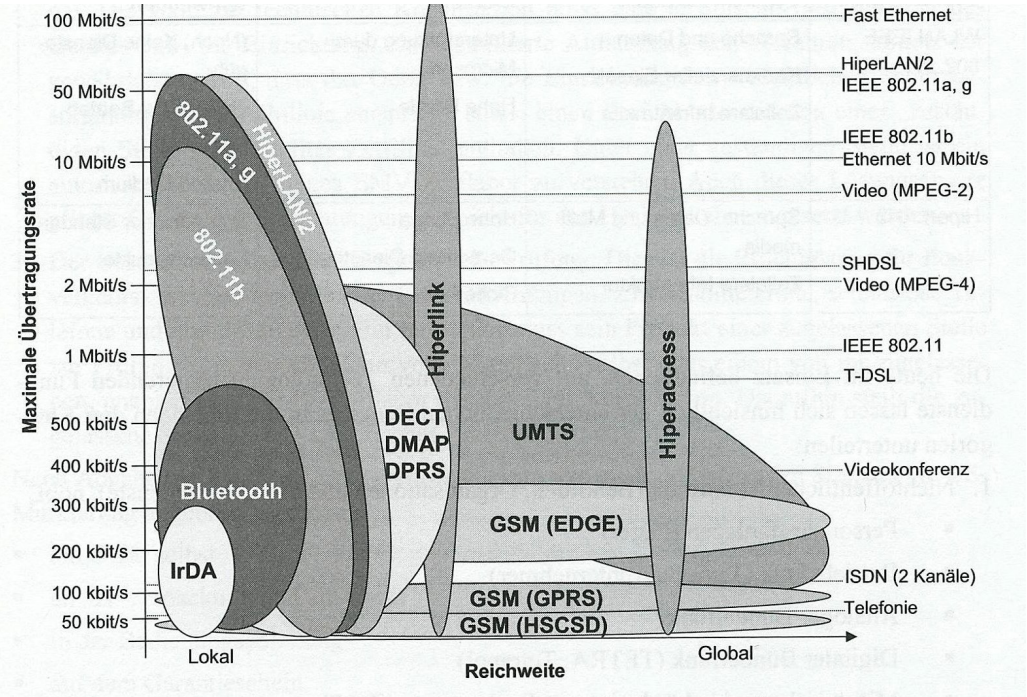
2.2 Anforderungen

Zu den wichtigsten Anforderungen eines Netzwerkes gehört an erster Stelle die Sicherheit der übermittelten Daten. Oftmals beruht ein großer Teil des Kapitalstocks von Unternehmen auf internem Wissen, das selbstverständlich intern bleiben sollte. Die drahtlose Verbindungsmöglichkeit muss daher ungewollte Teilnehmer ausschließen, die ohne das verkabelte Gebäude betreten zu müssen und an der Firewall vorbei prinzipiell die Möglichkeit des Einstiegs ins interne Netzwerk haben. Angelehnt an die Sicherheit des Wired LAN wurde der anfänglich im IEEE[1] 802.11 implementierte Sicherheitsstandard WEP genannt, was für "Wired Equivalent Privacy" steht. Diesem Anspruch wurde die Implementation jedoch nicht gerecht, weshalb das WPA-Verschlüsselungsverfahren folgte.[2]

Weitere Kriterien sind bei steigenden Datenvolumina natürlich Durchsatzrate und Verbindungstreue. Diese beiden Punkte verschlechtern sich vehement bei einer großen Anzahl von Clients, wie es auf Tagungen mit vielen Teilnehmern leicht der Fall sein kann. Eine weitere Schwierigkeit ist der oben genannte Wechsel von Access-Point-Zellen, was ein grundlegender Faktor für die Mobilität der mobilen Clients ist. Ebenfalls sollte bei der Implementation von Wireless LAN Standards ein Augenmerk auf den Stromverbrauch gelegt werden, da die mobilen Clients in der Regel mit Akku betrieben werden und Strom somit eine knappe Ressource ist.

[1] Institute of Electrical and Electronics Engineers
[2] Näheres zu WEP und WPA ist in [3] Kapitel 8 zu finden.

2.3 Techniken



In dieser Abbildung sind verschiedene drahtlose Kommunkationstechniken dargestellt. Hier kann man leicht die Reichweite und Durchsatzraten ablesen. Quelle: [3] S.22

2.4 Geschichte

Als erster Meilenstein in der drahtlosen Netzwerkgeschichte sollte wohl das ALOHA-Netzwerk gelten, dass verschiedene Computer über Inselgrenzen hinweg verband. Dieses Funkprotokoll, das ein Vorläufer des Ethernet war, wurde schon in den 60er Jahren entwickelt. Ab Mitte der Achziger Jahre folgten dann weitere Wireless-LAN Produkte, die auf verschiedene Technologien wie auch Infrarot und DECT setzten. Davon seien hier einige herausgegriffen (nach [3]:S.39):

- 1986 kamen die ersten proprietären WLANs auf den Markt. Sie benutzten den Frequenzbereich von 900MHz und kamen auf Bitraten von 840kbit/s.

- 1990 kamen Wavelan von NCR, das auf Datenraten von 2Mbit/s auf der 2,4Ghz-Frequenz kam, und 1991 Altair von Motorola, das auf der 18Ghz-Frequenz 10Mbit/s bereitstellte, heraus
- 1991 entwickelte Olivetti ein WLAN auf Basis des DECT, was heute hauptsächlich für schnurlose Telefonie verwendet wird, und erreichte damit Bitraten von 1,1Mbit/s
- ebenfalls 1991 stellte AndroDat ein auf Infrarot basiertes WLAN vor, dass allerdings nur auf 19,2kbit/s kam

1992 begann schliesslich dass IEEE mit der Entwicklung des 802.11 Protokolls. Dabei hatte das IEEE zum Ziel die in Abschnitt 2.2 genannten Bedürfnisse an Wireless LAN zu erfüllen. Während der Markt mobiler Netzwerkgeräte damals sprunghaft anstieg, war ein weiterer begünstigender Faktor der Entwicklung des Standards die vorangegangene Entwicklung der Hardware, also verschiedener Funk-Übertragungstechniken. Das IEEE spezialisierte sich bei Entwicklung auf die Ausnutzung der lizenzfreien ISM-Frequenzen[3]. ([3]:S.40) Die Lizenzfreiheit begünstigte auch anschließend die schnelle Verbreitung des Standards.

3 Der 802.11 Standard

3.1 Allgemeines

Zuerst werden die Ziele des IEEE bei der Entwicklung des 802.11 Standards erläutert, im Anschluß an weitere Bemerkungen zur Entwicklung und Problemstellung des Wireless LAN wird die Funktionsweise der Media Access Control Schicht dargelegt.

Neben den in Abschnitt 2.2 genannten Aspekten spielt die Kompatibilität zum Ethernet Standard 802 eine wichtige Rolle. Zur effizienten Gestaltung werden Pakete außerdem in der MAC-Schicht geprüft und neu angefordert, damit nicht die darüber liegenden Protokolle diese neu anfordern müssen.

> IEEE 802.11 is required to appear to higher layers [logical link control (LLC)] as a current style IEEE 802 LAN. This requires that the IEEE 802.11 network handle station mobility within the MAC sublayer. To meet reliability assumptions (that LLC makes about lower layers), it is necessary for IEEE 802.11 to incorporate functionality that is untraditional for MAC sublayers. ([2]:S.10)

[3] ISM steht für Industrial, Medical, Science; also Industrie, Medizin und Wisschenschaft

An dieser Stelle seien noch zwei Institutionen genannt, die sich etabliert haben zur Unterstützung und Verbesserung des Standards. Zum einen bemühte sich die Wi-Fi Alliance um Kompatibilität der Geräte verschiedender Hersteller indem sie ein Gütesiegel entwickelte. Wi-Fi ist dabei abgeleitet von Hi-Fi, also High Fidelity (hohe Wiedergabetreue). Sie enstand aus der Vorgängerorganisation WECA, das steht für "Wireless Ethernet Compatibility Alliance".[4] Zum anderen gibt es die WLANA (Wireless LAN Associaton), die als unabhängige Informationsquelle dient und sich die Förderung von WLAN-Anwendungen zur Aufgabe gemacht hat[5] Hier kann man sich beipielsweise auch die IEEE-Standard-Papers herunterladen.

Erwähnt seien hier noch die maßgeblichen Komponenten, die an einem WLAN beteiligt sind. Abgesehen von in Abschnitt 2.1 genanntem Backbone-System das gegebenenfalls meherere Access Points zu einem erweiterten Set verbindet ist für jede einzelne WLAN-Zelle ein Access Point notwendig, der die verschiedenen mobilen Clients verwaltet und miteinander verbindet. An diesem meldet sich jeder Client an und wird somit Teil des Netzwerkes. Somit entsteht eine Zellen-Struktur, die nach Bedarf erweitert werden kann. Im Ad Hoc Modus, in dem mobile Clients eine direkte Verbindung untereinander aufbauen ist kein Access Point und somit keine weitere Infrastruktur notwendig.

3.1.1 Entwicklung

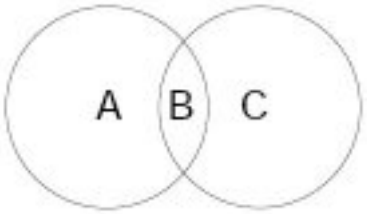
Zur Übersicht werden nun ein paar wesentliche Schritte in der Entwicklung des 802.11 Standards aufgezählt. 1997 wurde die erste Version des 802.11 Standards veröffentlicht. Auf dem 2,4 Ghz-Band konnte eine Datenrate von bis zu 1-2 Mbit/s erreicht werden. Diese Version wurde mit dem Frequenzsprungverfahren (FHSS) verwirklicht. Ab 1999 erreichte der 802.11b auf der selben Bandbreite 11 Mbit/s, hier kam das Direktsequenzverfahren (DSSS) zum Einsatz. Dieser Standard war in Europa aufgrund starker Beschränkungen des 5 Ghz-Bandes lange der maßgebliche Standard während andernorts schon der 802.11a Standard im 5 GHz-Band 54 Mbit/s Datenrate bereitstellen konnte. Jedoch wurde dies mit dem g-Standard auch im 2,4 Ghz-Band nachgeholt. Ein weiterer wichtiger Schritt war die Entwicklung der WPA-Verschlüsselung, die von der 802.11i Gruppe entwickelt wurde. Deren Ziel ist die Verbesserung von Sicherheit und Authentifizierung, die WPA-Verschlüsselung wurde jedoch vor Abschluß der Arbeiten an 802.11i schon vorgereicht, um der dringlichen Nachbesserung der WEP Verschlüsselung nachzukommen ([3]:S.30)

[4] http://www.wi-fi.org/
[5] http://www.wlana.org/

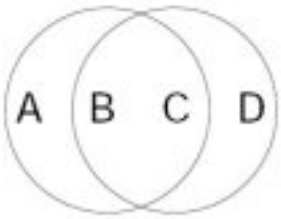
3.1.2 Besonderheiten von WLAN

Zwei Besonderheiten eines WLAN im Gegensatz zu Wired LAN sind das Hidden Station und das Exposed Station Problem, die im Ethernet verwendete Collision Detection erschweren.

Hidden Station: Da die verschiedenen Clients eines Access Points sich nicht zwangsläufig gegenseitig erreichen können, d.h.nicht immer gegenseitig in Reichweite sind, werden potentielle Kollisionen zunächst nicht immer erkannt. Beispielsweise wenn A an B Daten senden will, B jedoch von C Daten empfängt, nimmt nach der Collision Detection-Methode A dies nicht wahr und sendet, was eine Kollision verursacht.



Exposed Station: Hier ist das Problem gewissermaßen umgedreht. Der Sender registriert Störungen und wartet eine fremde Datenübertragung ab, jedoch betreffen diese Störungen nicht den Empfänger, das heißt, dass der Sender getrost senden könnte. Beispielsweise sendet B an A Daten. B ist in Reichweite von C, daher registriert C dies als Störungen und wartet. Jedoch liegt D, der Empfänger von C außerhalb der Reichweite von B und könnte daher ungestört empfangen. [6]



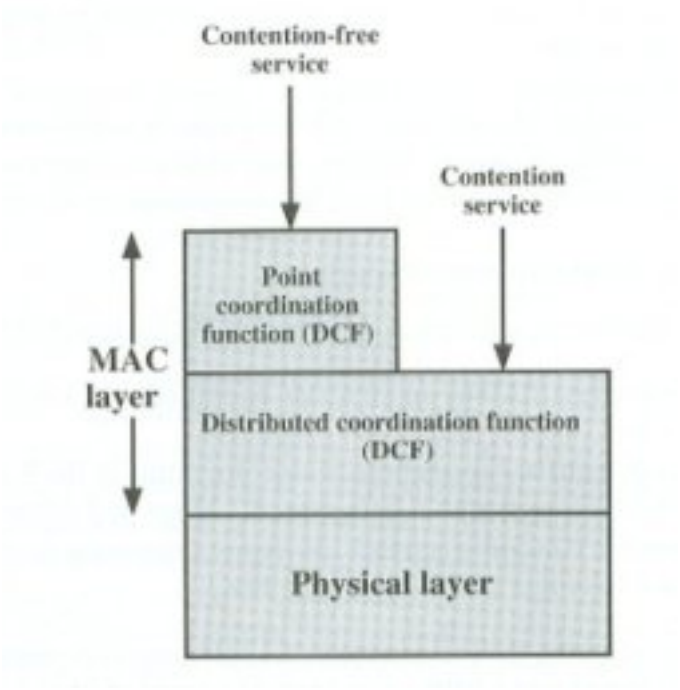
Grafiken: [6]

Des Weiteren setzt Collision Detection Full-Duplex-Betrieb voraus, was bei der verwendeten Funktechnologie jedoch wesentlich teuerer wäre, weshalb lediglich Half-Duplex implementiert ist. Aufgrund der hohen Fehlerrate bei Funk-Übertragung sollte jedoch in der MAC-Schicht zusätzliche Fehlerkorrektur umgesetzt werden, damit die darüber liegenden Protokolle weniger Anfragen stellen müssen und somit die Effizienz gesteigert wird. Daher wird im 802.11-Protokoll im Carrier Sense Multiple Access- Verfahren (CS-

MA) statt der genannten Collision Detection die unten erläuterte Collision Avoidance verwendet (CSMA/CA) ([3]:S.44)

3.2 Die Media Access Control Schicht

In der Media Access Control-Schicht (MAC) werden zur Koordination der Sende und Empfangsverwaltung zwei unterschiedliche Zugriffsverfahren verwendet, die im folgenden erläutert werden. Einerseits die so genannte Distributed Coordination Function (DCF) mit CSMA/CA. Dort herrscht Wettbewerb unter den Teilnehmern, im Gegensatz zu Point Coordinarion Function (PCF); dort wird die Zugriffskontrolle allein durch den Access Point koordiniert (der in diesem Zusammenhang daher auch "Point Coordinator" genannt wird). DCF bildet dabei die untere Schicht, während PCF darüber liegt und auch gewisse Features von PCF ausnutzt. DCF wird auch bei Ad Hoc-Netzwerken verwendet. Bei zeitkritischen Daten ist PCF effizienter, da der Koordinator den kritischen Daten eine höhere Priorität einräumen kann. ([4]:S.503f)



Quelle: [4] S.504

3.2.1 Distributed Coordination

Bei DCF kommt also ein Carrier Sense Multiple Access (CSMA)-Verfahren zum Einsatz. Dass heisst, vor dem Senden der Daten wird der Zustand des Empfängers abgefragt, erst wenn das Medium als frei erkannt wird, werden die Datenpakete gesendet, andernfalls wird abgewartet bis der Empfänger frei wird. Wie oben erwähnt funktioniert die bei Ethernet verwendete Collision Detection bei WLAN nicht, da Duplex-Betrieb erforderlich wäre und darüber hinaus nicht alle Stationen sich gegenseitig erreichen können. Daher kommt hier ein besonderes Collision Avoidance Verfahren zum Einsatz, um die Anzahl der Kollisionen zu verringern. ([3]:S.43f)

Hierbei wird das Kollisionsproblem durch eine zusätzliche Verzögerung des Sendens um einen kurzen Zeitraum, Interframe Space (IFS) genannt, gelöst. Dieser Zeitraum wird abhängig von einer Zufallsvariablen variiert um zu verhindern, dass nach einer Übertragung alle Sender auf einmal anfragen. Somit wird die Kollisionswahrscheinlichkeit verringert. Wenn die adressierte Station also nach der vorangegangenen Übertragung frei ist, wird noch diese IFS-Zeitspanne abgewartet ob die Station frei bleibt. Ist das nicht der Fall wird wiederholt angefragt. Bei DCF wird dieser Zeitraum DIFS genannt: Distributed IFS. Bleibt nach Ende der nächsten Übertragung die Leitung wieder nicht lange genug frei, wird der Zufallszahlenraum, aus dem die Zufallsvariable gewonnen wird, erhöht.

Zusätzlich wird vom Empfänger nach der erfolgreichen Übertragung ein "positive Acknowledge"-Paket (ACK) gesendet. Erhält der Sender das ACK-Signal nicht, sendet er die Daten erneut. Jedoch wird bei Erreichen einer festgelegten Zahl von wiederholtem Senden die Anfrage abgebrochen und ein höheres Protokoll muss die Daten erneut anfordern. Nach der Bestätigung gibt es einen Wettbewerb zwischen den sendewilligen Stationen, der Sender mit der kürzesten IFS kommt als nächstes zum Zug. [3]

Außerdem wird zur zusätzlichen Effizienzsteigerung das sogenannte "Virtual Carrier Sense"-Verfahren verwendet. Wenn der Empfänger frei ist wird vor dem Senden der eigentlichen Datenpakete ein "Request to send"-Signal (RTS) gesendet, das alle erreichbaren Stationen empfangen. Dieses Signal enthält auch die Sendedauer. Der Empfänger antwortet mit einem "Clear to send"-Signal (CTS), dass wiederum alle potentiellen Sender in Reichweite empfangen und somit wissen, dass dieser Empfänger nicht frei ist. [3]

3.2.2 Point Coordination

Hier wird der Datenzugriffe wettbewerbsfrei durch den Access Point koordiniert. Dieser hat immer einen kürzeren IFS, Point Coordination IFS genannt (PIFS), und dadurch

eine höhere Priorität. Somit lässt sich gerade bei zeitkritischen Diensten wie Sprache und Video eine schnellere Übertragung realisieren.

3.2.3 Fragmentierung

Um die Fehler der Übertragung zu reduzieren, und dabei Kompatibilität zu Ethernet zu behalten, werden die größeren Ethernet Pakete (bis zu 1.522Bytes) in kürzere Rahmen eingeteilt. Denn bei der höheren Bitfehlerrate steigt die Wahrscheinlichkeit, dass ein Daten-Frame gestört wird und verworfen werden muss. Bei einem kleineren zerstörtem Frame ist jedoch der Overhead des erneuten Sendens kleiner, und somit die Übertragung insgesamt schneller.

4 Ausblick

Im letzten Abschnitt soll ein kleiner Ausblick über weitere drahtlose Funktechnologien gegeben werden, die unter Umständen eine Rolle in der Zukunft spielen könnten.

Eine Technologie die hier Erwähnung finden soll ist WIMAX. Es handelt sich dabei um ein Breitband-Angebot über Funk, das sich besonders in Gegenden mit wenigen Teilnehmern eignet. Bisher wird dies nur an wenigen Punkten eingesetzt, es zeigt jedoch das Potential von Funkübertragung, denn WIMAX, das auf dem IEEE 802.16 Standard basiert, bietet über 50km eine maximale Datenrate von 70Mbit/s. ([3]:S.43)

HIPERLAN2 findet bisher hier in Deutschland kaum Anwendung, vermutlich weil es auf dem 5,2 Ghz-Band arbeitet. Es werden Datenraten bis zu 54Mbit/s unterstützt. Das Protokoll ist kompatibel mit IP, Ehternet, IP, PPP, ATM und IEEE 1394 und unterstützt sowohl Infrastruktur-basierte als auch Adhoc-Netzwerke.([3]:S.31)

Der IEEE 802.11n in der 802.11-Familie bleibt zu erwarten. Nach aktuellen Planungen soll das erste Release in der zweiten Hälfte von 2008 stattfinden. Das Protokoll zeichnet sich aus durch einen erhöhten Durchsatz von effektiven 100-200Mbit. Also auch bei mehreren Anwendern kann der Standard mit den 100Mbit von Fast Ethernet mithalten. Damit wird also auch bei einer hohen Anzahl von Clients eine gute Bandbreite möglich sein. Außerdem soll die Reichweite des 802.11n größer sein als die Vorgänger in der 802.11-Familie. Ebenfalls wird eine gleichmäßigere, zuverlässigere Abdeckung möglich, wodurch auch weniger Access Points benötigt werden. Beim Senden werden mehrere Antennen gleichzeitig verwendet, zum Einsatz kommen Spatial Division Multiplexing (SDM) und Multiple Input, Multiple Output (MIMO). Das Problem könnte sein, dass alte Clients im Netz die Leistungsfähigkeit des gesamten Netzwerkbereichs verringern. Bevorzugt wird

beim n-Standard das 5 Ghz-Band, dabei wird bei den Vorbereitungen den Europäischen Richtlinien Rechnung getragen. [1]

Vielversprechend könnte auch die weitere Entwicklung des Roaming sein. Dies soll ermöglichen mit einem Mobilen Client verschiendene WLANs zu benutzen, indem der Client sich bei den Access Points anmeldet (ähnlich wie bei GSM), damit die verschiedenen Netz-Betreiber untereinander abrechnen können. Das Problem stellt bislang noch der Handover dar. Beim Wechsel von WLAN-Zellen, muss sich das Gerät beim anderen Access Point anmelden. Hierbeit ensteht ein Datenraten-Engpaß der gerade bei Zeitkritischen Diensten wie Paketvermittelter Sprache vermieden werden muss. Die Verbesserung dieses Handovers ist auch Bestandteil des Aufgabenkatalogs des 802.11r-Teams. [5]

Literatur

[1] Roger Hockaday. Mehr als nur verbessertes wi-fi. *LANline*, November 2007.

[2] IEEE. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. IEEE, 1999.

[3] Gerhard Kafka. *WLAN. Technik, Standards, Planung und Sicherheit fuer Wireless LAN*. Hanser, 2005.

[4] William Stallings. *Data and computer communications*. Prentice-Hall, Inc., 2000.

[5] Michael Knuth Stefan Witte. Roaming und billing für hotspots. *LANline*, Spezial I/2004(Konradin):84–88, 2004.

[6] Philipp Stephan. Wireless LAN 802.11. Seminararbeit, 2003.