Eine Option für Firmennetzwerke der Druckereibranche?

eine Projektarbeit von
Jens Heermann, Svend Herder und Alexander Jacob

Vernetzte Produktionssysteme | Fachbereich E | Bergische Universität Wuppertal | 2005

Inhaltsverzeichnis

1. Einleitung

Es gibt ein Menge Gründe, warum Unternehmen über die Nutzung von Wireless-Technologie nachdenken sollten.

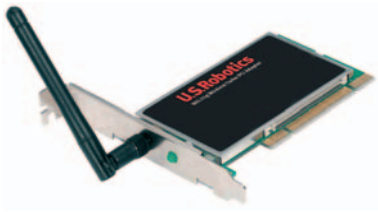
Einer amerikanischen Studie zufolge können bis zu 70 Minuten mehr produktiv genutzter Arbeitszeit, pro Mitarbeiter und pro Tag, durch den Einsatz von kabelloser Technik erzeugt werden. Dies erklärt sich hauptsächlich durch den gestiegenen Komfort und vor allem durch die neu gewonnene Flexibilität. Die Arbeitszeit ist nicht mehr an den Arbeitsplatz oder den Schreibtisch gebunden, sondern kann überall genutzt werden. Allerdings ist dieser Vorteil auch sehr branchenabhängig, der hier genannte sehr hohe Zuwachs kann sicherlich nicht in jedem Betrieb erreicht werden.

Natürlich sind auch die gestiegenen Flexibilität, Mobilität und Komfort durch WLAN-Technologie zu nennen. Die Bildung von Projektgruppen beispielsweise ist dann nicht mehr von der Anzahl der vorhandenen Netzwerkdosen abhängig, sondern kann sehr spontan vorgenommen werden, teilweise sogar ohne Änderungen an der Netzwerkinfrastruktur zu ändern.

Ein weiterer Hauptvorteil von WirelessLAN ist die einfache Installation: Es müssen keine Kabel mehr verlegt werden, was oftmals sehr schwierig umzusetzen, sehr teuer oder auch einfach durch Mietverträge oder Denkmalschutzbestimmungen (z.B. in alten Universitätsgebäuden) verboten ist. Die allgemeinen Kosten für die Netzwerk-Administration sind niedriger, da teilweise bei der Erweiterung eines Netzwerks gar keine administrative Arbeit anfällt und die neuen Recher sich einfach mit dem, in jedem modernen Betriebssytem integrierten Assistenten, in ein vorhandenes Netz einklinken können.

Außerdem ist WirelessLAN eine alternative und kostengünstigere Lösung bei der Vernetzung von weit entfernten Gebäuden. Hier können sowohl die Kosten für Material als auch für den baulichen Aufwand z.B. für die Verlegung kilometerlanger Kabel eingespart werden. Oftmals ist eine eigene direkte Vernetzung nicht mal möglich und es muss auf ein vorhandenen Leitungsnetz z.B. der Telekom zurückgegriffen werden. Das bedeutet, dass eine Standleitung angemietet werden muss, was zusätzlich zu den fixen Mietkosten auch evtl. sogar noch volumenabhängige Transferkosten generiert. Durch direkte Gebäudekopplung mittels WLAN lassen sich diese Kosten einsparen, da außer den Kosten für die Installation und die Geräte keine weiteren Kosten anfallen. Allerdings muss auch in Betracht gezogen werden, dass WLAN-Technologie noch nicht in der Lage ist, die gleichen Bandbreiten und Übertragungsgeschwindigkeiten wie kabelgebundene Netze zu bieten. Deshalb ist die Anwendung auch nicht in allen Bereichen sinnvoll und muss vor einer Entscheidung genau geprüft werden.

2. Komponenten eines kabellosen Netzwerks



Natürlich ist die Anzahl und die Ausstattung der verwendeten Netzwerkkomponenten stark von der Größe und der gewünschten Leistungsfähigkeit abhängig, allerdings sollen im folgenden einmal kurz die wichtigsten und gebräuchlichsten Komponenten vorgestellt werden.

Um überhaupt irgendeine Art von kabellosem Netzwerk aufzubauen, benötigt man an jedem teilnehmenden Client eine Sende- bzw. Empfangseinheit. Diese sogenannten WLAN-Karten sind mit einer kleinen Antenne ausgestattet und übernehmen sowohl das Senden, als auch den Empfang der Daten. Ihre Reichweite ist allerdings auf einige Meter begrenzt. Sie sind entweder für den Einsatz in Desktop-Rechner an der PCI-Schnittstelle erhältlich oder für den mobilen Einsatz in Laptops an der PCMCIA-Schnittstelle erhältlich. Die Hersteller von Hardware-Komponenten gehen aber auch mehr und mehr dazu über, diese Technologie schon onboard, also mit auf dem Mainboard verbaut, oder als Erweiterungskarte mitzuliefern. Vor allem aber bei Laptops ist dies der Fall, da beispielsweise der Chiphersteller Intel sogar schon WLAN-Funktionalität in ihren Centrino- und auch in den kommenden Sonoma-Chipsatz integriert hat. So ist die Anschaffung so einer Funkeinheit oftmals gar nicht mehr nötig, da sie bereits standardmäßig zur Ausstattung gehört.

Sollen aufwändigere Netzwerk-Infrastrukturen realisiert werden, kommt man um den Einsatz von sogenannten Access-Points nicht herum. Diese dienen als Basisstation und der Vermittlung von Datenpaketen zwischen den Clients. Das bedeutet, dass die Clients ihre Daten nun nur noch an den Access-Point senden, der diese dann an den gewünschten Empfänger-Client weiterleitet. Somit fungiert der Access-Point als sogenannter Repeater und vergrößert die Reichweite der einzelnen Clients.

Ist ein größeres Netzwerk geplant, dann wird eventuell der Einsatz von sogenannten Bridges nötig. Diese Geräte verbinden vorhandene, autarke Netzwerke miteinander. So kann man zum Beispiel auch mehrere Firmengebäude miteinander zu einem Gesamtnetzwerk verbinden, aber auch kleinere Netzwerke einzelner Abteilungen lassen sich mit diesen Workgroup-Bridges zusammenfassen.

Eine weitere wichtige Rolle für die Möglichkeiten eines Netzwerks spielen die verwendeten Antennen. Zum Einsatz kommen dabei zum einen die direkt an der WLAN-Karte und dem Router verbauten Antennen, die allerdings nur eine geringe Reichweite haben. Sind die Umgebungsbedingungen z.B. durch Wände oder Maschinen sehr ungünstig, müssen eventuell schon direkt an den Clients Richtantennen angeschlossen werden, die dann direkt auf den Access-Point strahlen. Ohne entsprechende Antennen ist der Aufbau einer Gebäudekopplung gar nicht möglich. Hier kommt die Richtfunktechnik ins Spiel, wobei die Signale gerichtet auf die Empfängerantenne gesendet werden. Dabei ist vor allem wichtig, dass die Antennen eine direkte Sichtverbindung haben. Ist dies nicht der Fall sinkt die Übertragungsleistung.

3 Aufbau-Varianten von WLAN-Netzen

Es werden grundsätzlich drei verschiedene Hauptaufbauvarianten und damit auch Anwendungsbereiche unterschieden:

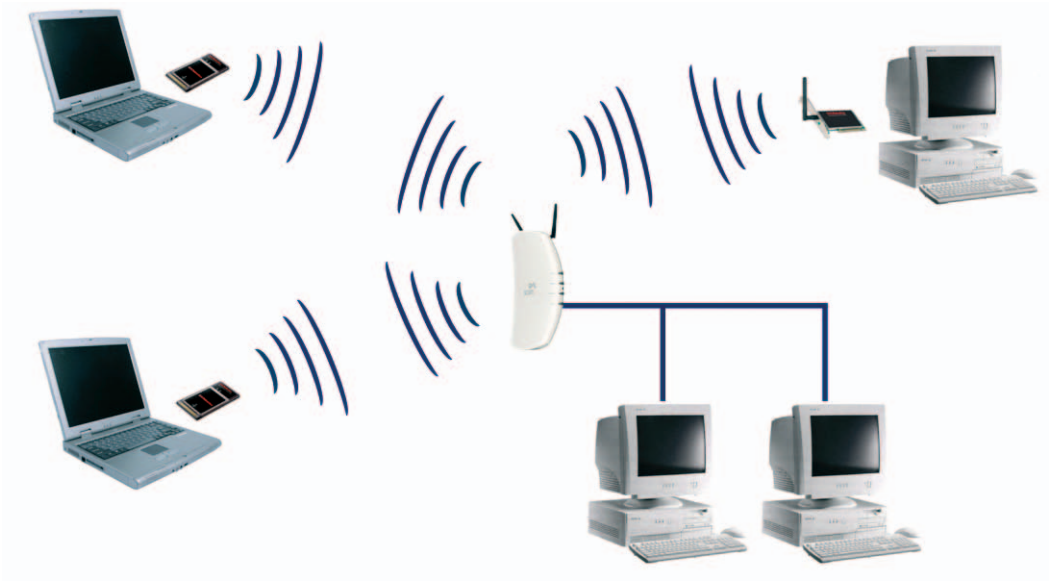
- Independent Basic Service Set (IBSS) oder auch Ad-Hoc-Aufbau
- Extended Service Set (ESS) oder auch Infrastucture-Aufbau
- Gebäudekopplung.

3.1 Independent Basic Service Set (IBSS) / Ad-Hoc

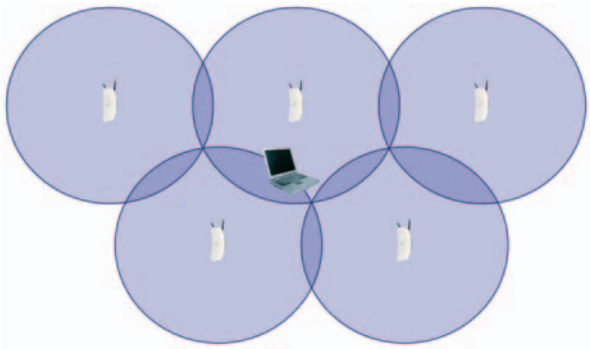
Im Independent Basic Service Set (IBSS) kommunizieren die einzelnen Clients direkt miteinander. In dieser Konfiguration ist es möglich, sich ohne besondere Einstellungen direkt in ein Netzwerk einzuklinken bzw. eines aufzubauen. Deshalb wird dieser Aufbau auch Ad-Hoc-Modus genannt und eignet sich sehr gut dazu eine spontane Vernetzung wie z.B. auf Konferenzen oder ähnlichem herzustellen.

3.2 Extended Service Set (ESS)/Infrastructure

Dieser Netzwerk-Aufbau verfügt über eine festgelegte Kommunikationsinfrastruktur. Alle Clients kommunizieren mit eine Verteilstation, den Access Point. Dieser dient als Repeater und leitet ankommende Datenpakete an die Empfänger-Clients weiter. Dies führt zu einer Erweiterung der Reichweite, da ein Client ja nur noch bis zum Access-Point senden muss und dieser das Signal wieder verstärkt an den innerhalb der Access-Point-Reichweite, aber eventuell außerhalb der eigenen Senderreichweite positionierten Empfänger weiterleiten kann. Dieser Aufbau hat aber den entscheidenden Nachteil, dass der Datendurchsatz sich verringert, da alle Datenpaket durch das Nadelöhr Access-Point geschleust werden müssen.

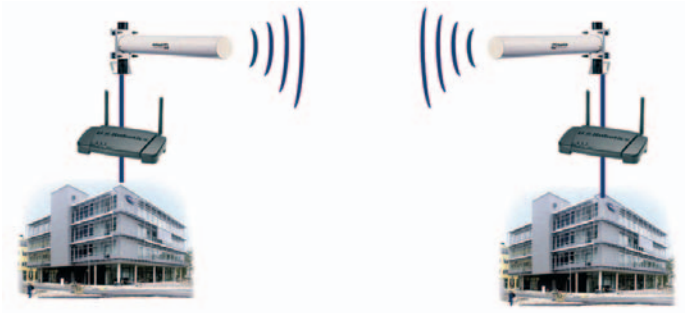


Ein weiteres Feature des Infrasturktur-Modells ist die Möglichkeit des Roaming. Das bedeutet, wenn sich die Funkzellen mehrerer Access-Points überschneiden, kann ein Client ohne Verbindungsunterbrechung zwischen den Funkzellen wechseln. Dies ermöglicht, neben der vollkommenen Mobilität bzw. Flexibilität des Arbeitsortes, auch einen Einsatz zum Beispiel in führerlosen Transportsystemen, die so ferngesteuert und mit Informationen versorgt werden können.



3.3 Gebäudekopplung

Mittels Wireless-Technologie lassen bis zu 7,5 Kilometer weit entfernte Gebäude mit einander koppeln. Hierbei wird allerdings keine Funkzelle aufgebaut, sondern eine direkte Verbindung mittels Richtfunk hergestellt. Dazu benötigt man lediglich in jedem Gebäude eine sogenannte Bridge, um die bisher autarken Netzwerke zu einem zu verbinden und eine Richtfunkantenne. Des weiteren bedingt dieser Aufbau eine direkte Sichtverbindung zwischen den Antennen.



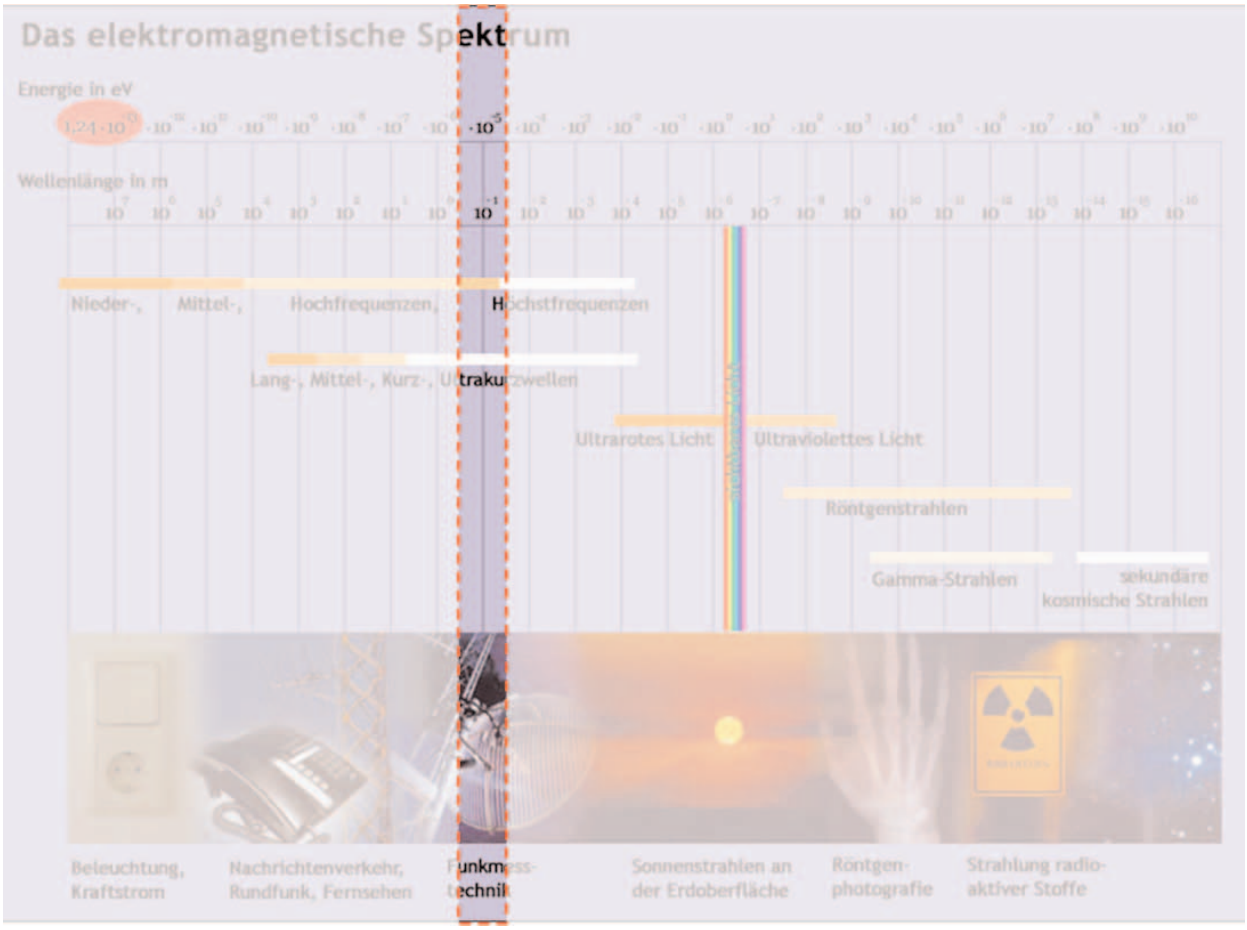
Außerdem wird zwischen einer Punkt-zu-Punkt-Verbindung und einer Punkt-zu-Mehrpunkt-Verbindung unterschieden. In der zweiten Variante strahlt eine zentrale Antenne omnidirektional, also in diverse Richtungen, ab, während die Richtfunkantennen der „Client"-Gebäude direkt auf die Zentralantenne zielen. Ein Einsatzgebiet hierfür wäre beispielsweise, wenn Daten aus einem zentralen Verwaltungsgebäude an mehrere, verteilte Produktionsgebäude gesendet werden sollen.

4. Technische Hintergründe

4.1 Signale

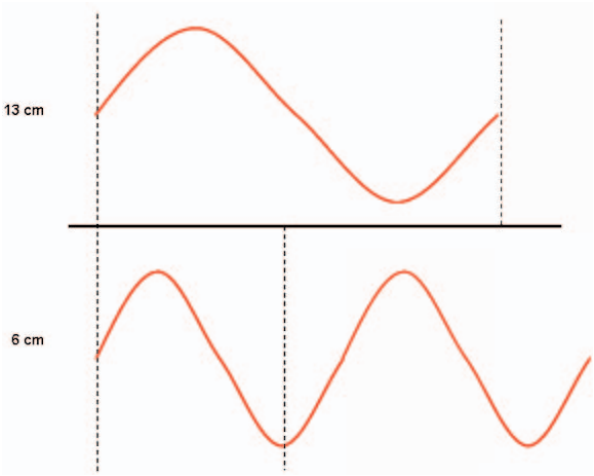
Der größte Unterschied zur konventionellen Ethernet-Technologie ist, dass wir kein physisch greifbares Kabel als Kanal benutzen, sondern unsere Daten quasi durch die Luft übertragen. Der Kanal zwischen Sender und Empfänger wird mittels elektromagnetischer Strahlung aufgebaut.

Der Begriff elektromagnetische Strahlung ist sehr allumfassend und reicht aus, um von Radiowellen über das sichtbare Licht bis hin zur Röntgenstrahlung alles abzudecken.



WLAN bewegt sich in diesem großen Spektrum in zwei Bereichen, dem 2,4 GHz-Bereich und dem 5 GHz-Bereich. Der 2,4 GHz-Bereich hat eine Wellenlänge von rund 13 cm und der 5 GHz-Bereich von 6 cm. Beide Bereiche liegen damit deutlich über dem Wellenlängenbereichen des sichtbaren Lichtes. Dieser, besonders für angehende Bachelors of Print- and Media-Technologies, interessante Bereich befindet sich bei einer Wellenlänge zwischen 720 und 380 nm.

Als Grundlage aus der Physik sei hier kurz angemerkt, dass Wellen, je kurzwelliger sie werden, energiereicher und damit potentiell gefährlicher für den menschlichen Körper werden. Als Beispiel kann hier das energiereiche UV-Licht im Spektrum der Sonne dienen, das bei Menschen Sonnenbrand verursacht.



4.2 Gesundheitsgefährdung durch Strahlung

Dieser Bereich ist für Unternehmen von immenser Bedeutung und sollte in Anbetracht von fortschreitender Entwicklung auf dem Sektor der Funktechnologien aufmerksam beobachtet werden.

Momentan gibt es die verschiedensten Studien über die Gesundheitsrisiken von so genanntem Elektrosmog, der besonders kritisch bei den von nahezu allen verwendeten GSM-Handys betrachtet wird.

Zum momentanen Zeitpunkt kann ein Gesundheitsrisiko durch elektromagnetische Wellen nicht ausgeschlossen werden. Allerdings sollte man bei der Entscheidung Pro-Contra WLAN folgendes berücksichtigen:

Die Sendeleistung eines WLAN - Senders ist in Europa per Gesetz auf 0,1 Watt beschränkt. Ein Standardhandy entwickelt eine Sendeleistung von rund 2 Watt. Diese Leistung ist nicht nur um mehrere Größenordnungen höher, sondern auch umso kritischer im Verhältnis zu sehen, da sie unmittelbar am Kopf entwickelt wird.

Allerdings weisen die GSM Systeme eine dynamische Leistungsanpassung auf, so dass in den meisten Fällen die Sendeleistung der GSM-Stationen deutlich unter diesem Maximalwert liegt.

Wer also seinen Mitarbeitern Handys zur Verfügung stellt und diese für unbedenklich hält, braucht sich bei WLAN keine Sorgen zu machen. Handys und WLAN sind hierbei auch sehr gut miteinander vergleichbar, da sie beide das 2,4 GHz-ISM-Band nutzen.

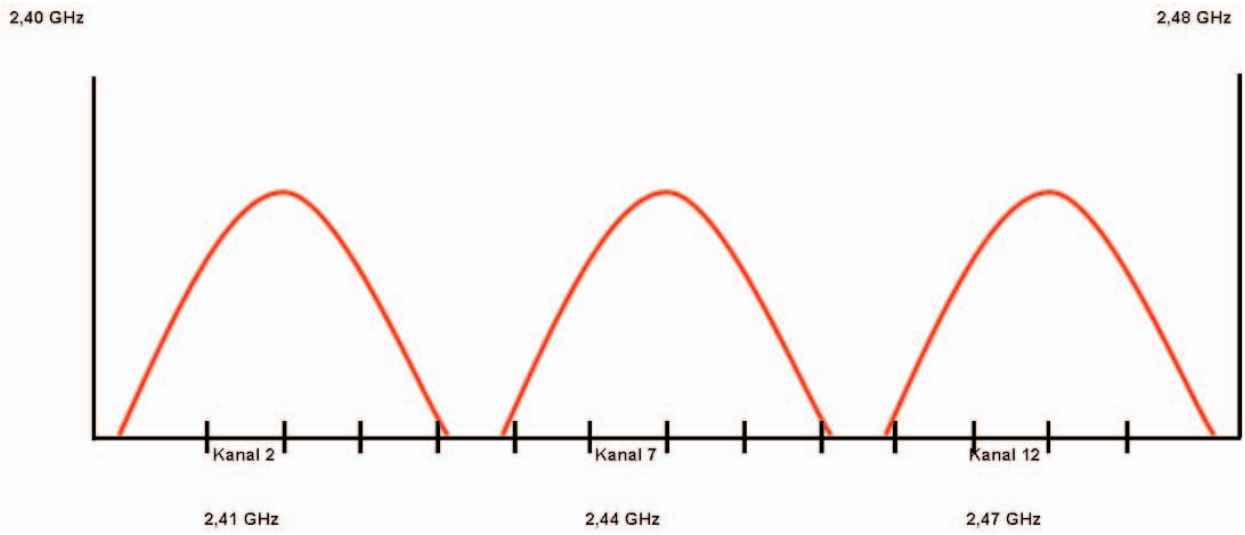
4.3 Reglementierung

ISM steht für Industrial, Scientific und Medical. Dieser Bereich ist von allen nationalen und internationalen Behörden für den Funkverkehr freigegeben. Dadurch, dass die anderen Bereiche strenger Reglementierung unterworfen sind, haben sich sehr viele Technologien in diesem Bereich angesiedelt. Von der Mikrowelle zum Erwärmen von Speisen über die Bluetooth-Technologie, bis hin zu Handynetzen, tummelt sich einiges auf diesem Frequenzband. Und eben auch WLAN. Dadurch, dass dieser Bereich so stark frequentiert ist, war es notwendig und auch wirtschaftlich sinnvoll, die zu Beginn des WLAN aufkommenden proprietären Lösungen einzelner Hersteller durch standardisierte Lösungen zu ersetzen.

4.4 Standardisierung

Das machte sich dann auch die IEEE zur Aufgabe. IEEE steht für Institute of Electrical and Electronics Engineers, Inc.. Diese Organisation ist in etwa vergleichbar mit der europäischen ISO oder der deutschen DIN. Sie definierte 1997 erstmals einen Standard (IEEE 802.11) mit einer Übertragungsrate von damals 1 MBit/s. Dass das nicht das Ende der Entwicklung sein konnte, war von vorneherein klar, dazu war die übertragenen Datenmenge pro Zeit einfach zu gering. Eine Weiterentwicklung war 1999 die Einführung von IEEE 802.11b mit einer (brutto) Übertragungsleistung von 11 MBit/s.

Konsequenter Weise wurde die Technik weiterentwickelt und die Datenübertragungsrate auf heute 54 MBit/s im 2,4 GHz-Bereich gesteigert. Im 2,4 GHz-Frequenzbereich stehen in Deutschland 13 Frequenzkanäle mit einem Frequenzabstand von 5 MHz für die Funkübertragung nach 802.11b zur Verfügung. Bei einer Kanalbandbreite von ca. 22 MHz können jedoch nur maximal 3 Kanäle gleichzeitig überlappungsfrei genutzt werden, beispielsweise die Kanäle 2, 7 und 12. Der Grund für die Abstände zwischen den einzelnen Kanälen ist in der überlagerungs- und damit fehlerfreien Datenübertragung zu suchen.



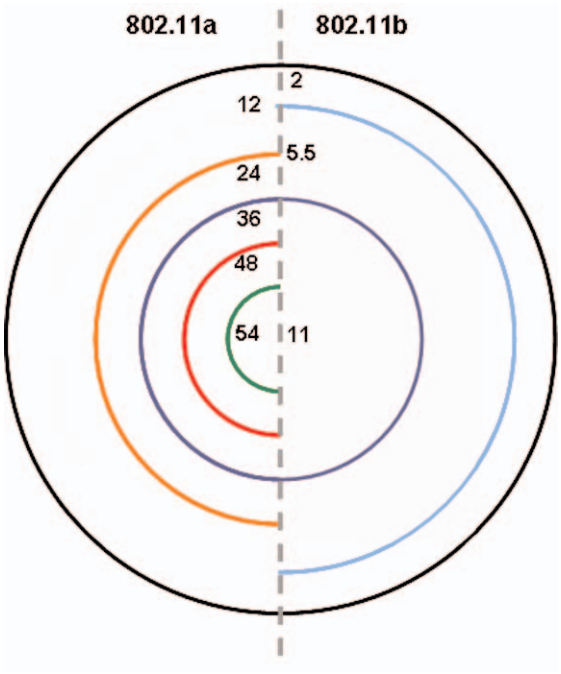
Wie zu sehen ist, stoßen wir im 2,4 GHz-Bereich relativ schnell an unsere Grenzen. Zur Verdeutlichung kann hier angeführt werden, dass in einem Bürogebäude in der Innenstadt maximal drei WLAN-Netze in einem Umkreis von rund 50 Metern betrieben werden können, was in großen Gebäuden eine sehr geringe Kapazität bedeutet.

Also musste eine Alternative zum 2,4 GHz-Bereich gefunden werden. Seit November 2002 ist in Deutschland der zweite Bereich des WLAN freigegeben, der 5 GHz-Bereich. Dieser ist allerdings nach wie vor einer stärkeren Reglementierung unterworfen, da auf diesen Frequenzen internationale Satelliten und der Radar der Bundeswehr arbeiten. Der hierfür entwickelte Standard der IEEE lautet 802.11a.

802.11a und zukünftige 802.11h Systeme nutzen diesen Bereich. Im Frequenzbereich von 5,15 bis 5,35 GHz und von 5,47 bis 5,725 GHz sind in Deutschland insgesamt 19 Kanäle in einem Abstand von 20 MHz unter Auflagen freigegeben worden. Bei einer Kanalbandbreite von 20 MHz werden direkt benachbarte Kanäle hier nicht gestört. Das heißt effektiv mehr nutzbare Kapazität.

Warum nutzen also nicht alle den 5 GHz-Bereich, wenn hier doch deutlich mehr Kapazität zur Verfügung steht?

Damit kommen wir wieder auf eine Grundlage aus der Physik. Zur Erinnerung: hochfrequente, also kurzwellige Wellen sind deutlich energiereicher als Langwellige. Daraus ergibt sich, dass man auch zu ihrer Erzeugung mehr Energie braucht. Das heißt für den 5 GHz-Bereich, dass er viel energieintensiver in der Erzeugung ist, als der 2,4 GHz-Bereich. Die Sendeleistung in WLAN-Netzen ist, wie schon gelesen in Europa auf 0,1 Watt beschränkt. Es wird deutlich, dass ein Funknetzwerk im 5 GHz-Bereich eine Reichweite von 10 bis 15m hat, wohingegen ein Netzwerk im 2,4 GHz-Bereich eine nutzbare Ausdehnung von 30 bis 50m erreichen kann.



In der Grafik, die einen Vergleich zwischen dem IEEE 802.11a und dem b-Standard zieht, ist diese Sendeleistungsbeschränkung nicht ausreichend berücksichtigt dargestellt.

4.5 Dämpfung

So wie Licht durch Hindernisse Schatten wirft und deswegen nicht immer seine maximale Reichweite erreicht, werden auch Funkwellen durch Hindernisse gestört. Dabei ist der 5 GHz-Bereich deutlich anfälliger, da er kurzwelliger ist.

Neben der Entfernung, die ohne Frage das größte Hindernis darstellt, sind besonders feuchte Wände und viele Personen ein großes Hindernis. Beide enthalten Wasser, welches Funkwellen besonders stark behindert. Für das Maschinenumfeld in der Druckerei ist interessant, dass gut leitende Materialien, besonders Metalle ebenfalls den Funkverkehr stören. Sobald irgendeines dieser Hindernisse die jeweilige Wellenlänge überschreitet, sprich dicker als dreizehn bzw. sechs Zentimeter ist, wird das Hindernis zum echten Wellenbrecher.

4.6 Realer Datendurchsatz

Durch die Dämpfung der Signale durch die Umgebungseigenschaften ergibt sich auch, dass die von den Herstellern vollmundig angepriesenen Datendurchsatzraten nicht erreicht werden. Als Faustformel kann hier etwa gelten, dass 50 % der angegebenen Leistung realistisch erreicht werden können. Für ein 11 MBit/s Netz ergibt sich damit ein Datendurchsatz von 5-6 MBit/s und für ein 54 MBit/s Netz ein realistischer Wert von 25-28 MBit/s. Diese Werte sollten allerdings nicht auf die Goldwaage gelegt werden, da diese je nach Umfeld sehr stark schwanken können.

In Perspektive lässt sich im Vergleich zum kabelgebundenen Ethernet jedoch sagen, dass WLAN in näherer Zukunft auf rund 1/10 der im Kabel möglichen Datendurchsatzmenge kommen wird.

5. Sicherheit und Verschlüsselung

Die Sicherheit von Daten und der Schutz vor unbefugtem Zugriff haben in jedem Unternehmen eine hohe Priorität. Vertrauliche Daten über das Unternehmen, die Produktion oder die Mitarbeiter liegen auf Servern und Clients und werden bei einem Ethernet über Kennwörter, vergebene Zugriffsrechte und durch einen Firewall nach außen hin abgesichert. Das gleiche gilt für ein WLAN. Hierbei muss allerdings zusätzlich darauf geachtet werden, dass nicht jeder, der einen Funkempfänger besitzt und in Reichweite des Netzes ist, sich Zugriff verschaffen kann.

Daher werden die Daten, ebenso wie bei einem Ethernet, verschlüsselt.

Die Länge des Schlüssels wird in Bit angegeben. Wenn man daher über eine 128 Bit-Verschlüsselung spricht, sollte man sich immer im Klaren darüber sein, dass es sich dabei um eine Verschlüsselung mit einer Schlüssellänge von 128 Bit handelt.

128 Bit = 2^{128} = 3.4x1038 Zeichen = 340282366920938463463374607431768211 00!

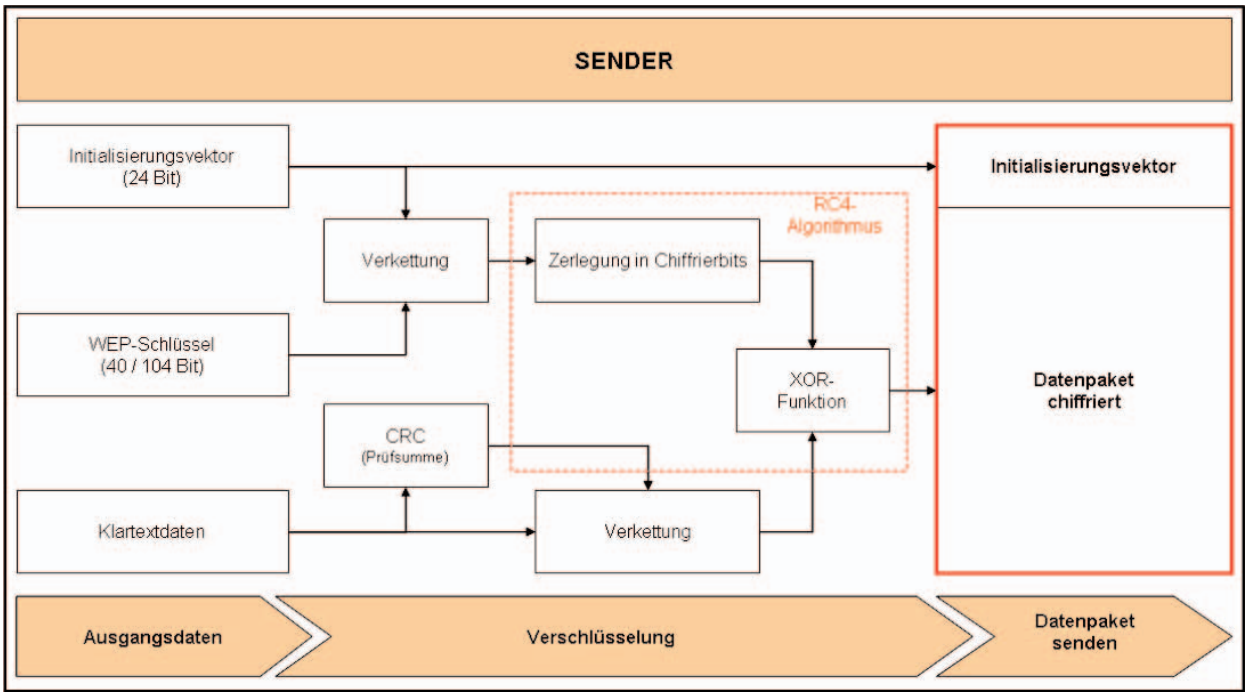
Eine Faustregel besagt, dass, wenn man den Schlüssel um ein Bit verlängert, sich die Stärke des Verschlüsselungsverfahrens gegen Angriffe mittels Ausprobieren verdoppelt.

Das Verschlüsseln mit einer möglichst großen Bit-Zahl erscheint daher mehr als sinnvoll.

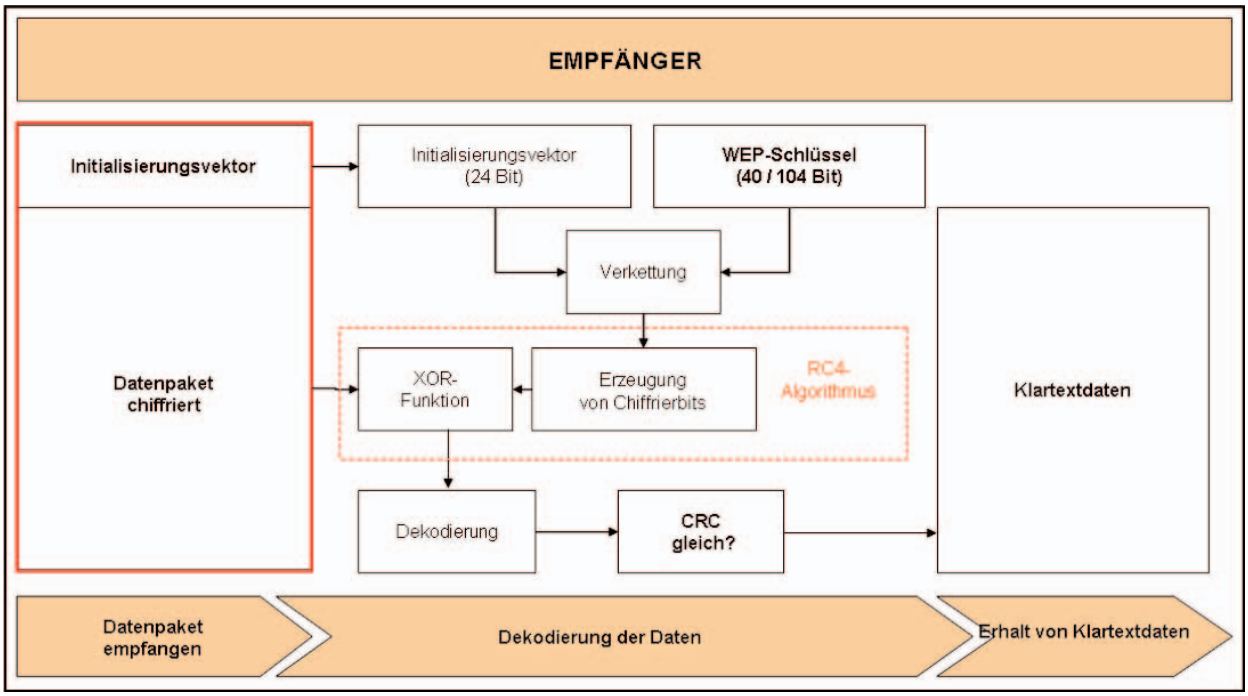
5.1 Wired-Equivalent-Privacy (WEP)

WEP ist die Standardverschlüsselungsvariante für WLANs. Bei den meisten Produkten kann man zwischen WEP 64 und WEP 128 wählen. Die Zahl ergibt sich aus einem frei wählbaren Bereich von 40 bzw. 104 Bit (hier gilt natürlich, je länger der Schlüssel, desto sicherer ist er) und einem Initialisierungsvektor (24 Bit). Der WEP-Algorithmus berechnet über den RC4-Algorithmus (Ron's Cipher 4), der sehr kompakt und schnell ist, aus diesem Startwert einen Strom aus Chiffrierbits. Die zu übertragenden Daten werden anschließend mit der logischen Exklusiv-Oder-Funktion (XOR) und den Chiffrierbits kodiert. Vor die zu sendenden Datenpakete wird der Initialisierungsvektor gesetzt und das Gesamtpaket dann an den Empfänger geschickt.

Da der Initialisierungsvektor mitgeschickt wird und der Empfänger den gleichen WEP-Schlüssel besitzt, ist er in der Lage den gleichen Chiffrierstrom zu erzeugen und durch eine erneute Anwendung der XOR-Funktion die Datenpakete zu dekodieren. Als Prüfsummenalgorithmus für die Übertragung wird ein Cyclic Redundancy Check (CRC) verwendet. CRCs werden vor Beginn der Übertragung und nach Abschluss der Transaktion mathematisch erzeugt und dann verglichen. Durch das Prüfen können vorhersehbare Fehler (z.B. Rauschen) entdeckt werden.

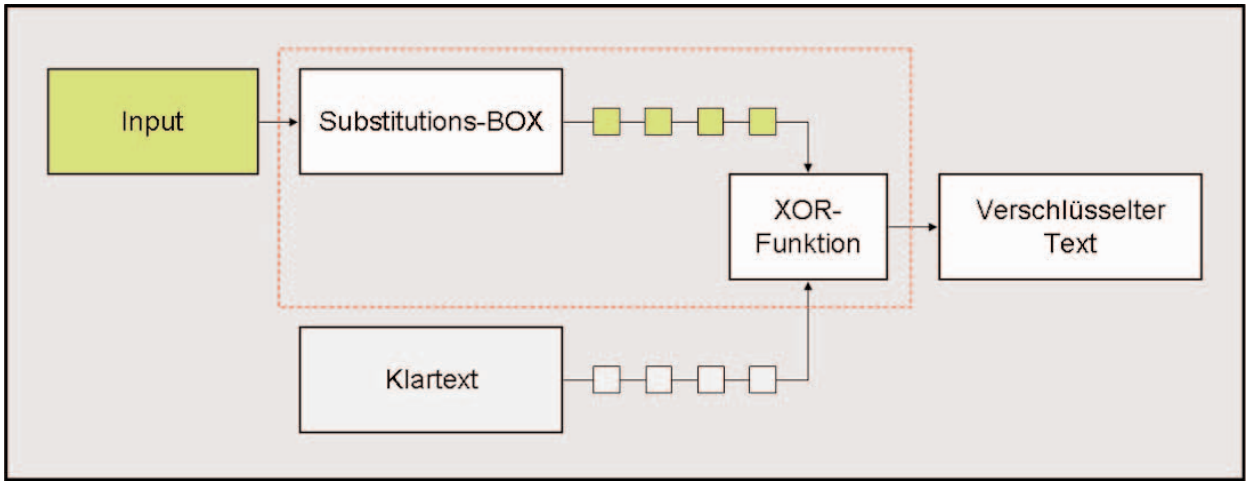


Ein großer Schwachpunkt beim WEP-Verfahren liegt in dem geheimen Schlüssel und dem Initialisierungsvektor. Der Initialisierungsvektor wird im Klartext übertragen, wodurch die Identifizierung von gleichartig kodierten Datenpaketen nicht schwer fällt. Durch Mithören von genügend Daten und entsprechender Software lässt sich sogar der geheime Schlüssel berechnen, da der RC4-Algorithmus durch eine relativ einfache Mathematik bestimmt wird.



5.2 Verschlüsselung von Daten mittels RC4-Algorithmus

Der RC4-Verschlüsselungsalgorithmus dient als Grundlage der Verschlüsselung für die Daten bei der Wireless-Übertragung. Es handelt sich hierbei um einen so genannten Stromchiffrierer, benannt nach Ronald L. Rivest (RC4 ' Ron's Cipher 4). Stromchiffrierer verschlüsseln Bit für Bit und erzeugen mit einem geheimen Schlüssel über eine Substitutionsbox einen Schlüsselstrom. Dieser wird dann mit dem Klartext, auch Bit für Bit, durch die XOR-Funktion (eXclusive-OR bzw. exklusiv-ODER-Verknüpfung) verknüpft.



Eine XOR-Funktion vergleicht das eingehende Bit vom Klartext mit dem aus der Substitutionsbox, das auch zum "Verschlüsseln" benutzt wird. Hierbei können zwei Zustände, 0 und 1, erzeugt werden. Ein Ergebnis ist nur genau dann 1, wenn nur einer der beiden zu verknüpfenden Werte 1 ist; sind beide gleich, ist das Ergebnis 0.

XOR-Verknüpfung zweier Bits:
0 XOR 0 = 0
0 XOR 1 = 1
1 XOR 0 = 1
1 XOR 1 = 0

Wegen der Verschlüsselung auf Bit-Ebene ist der RC4-Algorithmus sehr schnell und findet deshalb auch Anwendung in Echtzeit-Systemen.

5.3 Wi-Fi Protected Access (WPA/WPA2)

Die WPA-Methode ist die Weiterentwicklung von WEP und versucht deren Sicherheitslücken zu schließen. Es wird das "Temporal Key Integrity Protocol" (TKIP) eingesetzt, das für jedes Paket mehrere Schlüssel verwendet. Die erhöhte Sicherheit gegenüber WEP besteht darin, dass der WPA-Schlüssel nur bei der Initialisierung verwendet wird und anschließend ein Session-Key pro Datenpaket zum Einsatz kommt.

Zusätzlich gibt es mehrere Möglichkeiten der Schlüsselverwaltung. Zum einen können die Zugangskennungen auf einem zentralen Server verwaltet werden (Managed Key) oder zum anderen mit einem "Pre-Shared-Key" (WPA-PSK) gearbeitet werden, mit dem sich alle Nutzer eines Netzes mit dem selben Passwort anmelden. Hierbei hängt allerdings die Sicherheit des Systems von der Qualität des Passwortes ab.

Als Erweiterung von WPA (WPA 2) soll die RC4-Verschlüsselung durch den "Advanced Encryption Standard" (AES) ersetzt werden, dessen Verschlüsselungs-Algorithmus nicht nur WLAN, sondern auch den Standard 802.11i noch sicherer machen soll. Im Wesentlichen laufen hierbei die Vorgänge in der Substitutions-Box etwas anders und umfangreicher ab.

5.4 Sicher oder nicht sicher?

Solange die Hinweise, u.a. auch vom Bundesamt für Sicherheit in der Informationstechnik (BSI, http://www.bsi.bund.de), zum Thema Wireless LAN und Verschlüsselung befolgt werden und die Schwachstellen der WEP-Verschlüsselung bekannt sind und ausgeglichen werden, gilt Wireless LAN als sicher.

Zusätzliche Sicherungsmaßnahmen, wie z.B. das Eintragen der MAC-Adressen der am Netzwerk beteiligten User oder das Deaktivieren der Übertragung der Netzwerk-Kennung, sind einzeln abzuwägen und bieten meistens keinen wirklichen Schutz oder eine Barriere für Angreifer.

Eine absolute Sicherheit gibt es leider für keine Netzwerke, die Angriffsfläche ist bei Wireless LAN allerdings als größer einzustufen.

Die höchste Sicherheit bei der Anbindung eines Funk-Clients bietet zurzeit noch ein korrekt eingerichtetes VPN.

6. Kosten

Die Kosten für Hardwarekomponenten bei der Installation einer Netzwerkumgebung bzw. bei einer Umrüstung/Erweiterung bestehender Netzwerke können für viele Unternehmer u.a. einen Schlüssel zur Entscheidung für oder gegen WLAN darstellen.

Grundsätzlich lassen sich die Kosten natürlich nur im Verhältnis zu dem daraus zu ziehenden Nutzen sehen. Eventuelle Mehrkosten für WLAN könnten sich in einer größeren Flexibilität bzw. Einsparung an anderer Stelle auszahlen.

6.1 Ethernet/WLAN

Einen direkten Vergleich zu ziehen ist fast unmöglich. Die Architektur des Office-Bereichs, der Maschinenhalle, Lager, etc. spielt eine wichtige Rolle. Bei der Installation eines herkömmlichen Netzwerkes sind die Kosten für die Verkabelung relativ hoch, allerdings schafft man damit eine solide Basis für ein Netzwerk. Diesen Punkt kann man beim WLAN vollkommen vernachlässigen. Viel wichtiger ist, wie schon bekannt, ein stabiles Signal. Dies lässt sich oftmals nur durch viele Access Points erreichen, wobei hier die Anzahl der Clients, die über einen Access Point senden/empfangen begrenzt ist (geräteabhängig bei durchschnittlich 8) und somit die Kosten mit steigender Teilnehmerzahl im Netzwerk in die Höhe schnellen. Es kann sogar sein, dass jeder Client, ebenso wie jede Maschine oder technische Anlage, die mit Starkstrom betrieben wird, zusätzlich mit einer Richtantenne ausgestattet werden muss, die direkt auf den Access Point strahlt.

Grundlegend kann man bei den Preiskategorien, bei Ethernet- und WLAN-Hardware, zwischen Indoor- und Outdoor-Geräten unterscheiden.

Mit WLAN Outdoor-Komponenten lassen sich zum Beispiel Gebäude verbinden oder Freiflächen vernetzen. Natürlich sind diese Geräte dazu speziell geschützt (z.B. wasserdichte Gehäuse aus Aluminium oder Stahlbeton, die auch säure- und rostfest sind) und dementsprechend teuer. Aber auch Ethernet-Geräte, die im Außenbereich Einsatz finden sind entsprechend geschützt und ebenfalls nicht preiswert.

7. Zukunftsaussichten

Auch beim Thema Wireless-LAN steht die Entwicklung noch nicht am Ende. Ziel ist es nicht nur einen Komfort-Vorteil zu haben, sondern auch die gleiche oder sogar höhere Übertragungsleistung einer kabelgebundenen Verbindung. Auf kurze Distanzen ist das sogar schon gelungen, allerdings gibt man sich damit nicht zufrieden. Deshalb sollen hier kurz die beiden wichtigsten Zukunftstechnologien im Wireless-LAN-Bereich vorgestellt werden.

7.1 Wireless Fidelity (IEEE 802.11n)

Dieser Standard befindet sich aktuell noch in der Phase der Standardierung, d.h. die IEEE berät noch über die zu erwartenden Leistungsmerkmale. Die Verabschiedung des Standards wird Mitte 2005 erwartet, die Markteinführung erster Geräte wird aber erst 2006 oder 2007 stattfinden.

Erwartet werden darf aber eine höherer Datendurchsatz von anfänglich 108 MBit/s, welcher später dann sogar auf bis zu 380 MBit/s gesteigert werden soll. Erreicht werden soll dies durch mehrere parallele Übertragungskanäle, einen höheren Durchsatz in der MAC-Schicht und einen geringeren Overhead, außerdem wird der Wechsel in das 5GHz-Band diskutiert. Des weiteren soll die Verteilung der Bandbreite auf die einzelnen Clients verbessert werden und der Standard abwärtskompatibel zu den älteren Standards bleiben.

Aktuell kommen schon sogenannte Pre-n-Geräte auf den Markt, welche aber nicht dem tatsächlichen Standard entsprechen und deshalb später nicht kompatibel zur kommenden Norm sein werden. Im Unterschied zu den früheren Pre-g-Geräten ist es höchst unwahrscheinlich, dass diese Geräte sich später mittels eines Firmware-Updates zu „echten" n-Standard-Geräten upgraden lassen.

7.2 WIMAX (IEEE 802.16)

Der WIMAX-Standard ist kein direkter Konkurrent des IEEE 802.11n-Standards, da er eher auf den Außeneinsatz ausgelegt ist. Er soll vor allem den flächendeckenden Internetzugang mittels WLAN , z.B. für sogenannte Bürgernetze oder Voice-over-IP (VoIP) ermöglichen. Auch die Gebäudekopplung ist ein mögliches Einsatzgebiet.

Allerdings befindet sich auch dieser Standard noch in der Phase der abschließenden Standardisierung, die Markeinführung ist hier aber schon Anfang 2005 zu erwarten. Leistungsmäßig sollen bis zu 75 MBit/s bei 30 Kilometer Reichweite erreicht werden. Es lässt sich aber jetzt schon sagen, dass real gerade einmal 20 MBit/s bei 600-900 Meter Reichweite, bzw. 4,5 MBit/s bei 15 Kilometern Reichweite erreicht werden können.

Diese Norm ist für den Einsatz in Frequenzbändern über 2,5GHz konzipiert, vorraussichtlich wird diese Technologie im 5GHz-Bereich zum Einsatz kommen. Allerdings wird WIMAX nicht über Features wie garantierte Bandbreiten für die einzelnen Clients oder den vollautomatischen Zellwechsel (Roaming) verfügen, dafür ist die Implementierung in die Intel Centrino-Technologie geplant.

8. Fazit

Abschließend lässt sich sagen, dass die Wireless-LAN-Technologie auf ihrem aktuellen Entwicklungsstand noch keine generelle Alternative zum kabelgebundenen Ethernet ist.

Allerdings können in bestimmten Einsatzgebieten die Vorteile von einer kabellosen Vernetzung, die um einiges geringere Übertragungsleistung kompensieren. Dabei ist die gewonnene Flexibilität sicher der wichtigste Punkt. Aber auch was die Kosten angeht, ist die Nutzung von Wireless-LAN sicherlich eine Überlegung wert. Vor allem die Kostenvorteile bei der Gebäudekopplung sind hier zu nennen. Auch das Thema Sicherheit bedarf beim Einsatz von WLAN einer größerer Aufmerksamkeit, wobei es aber schon durchaus Lösungen gibt, die einen ähnlichen Sicherheitsstandard wie beim kabelgebundenen Netz bieten.

Da beide Technologien ihre spezifischen Vor- und Nachteile haben, lässt sich keine konkrete Empfehlung aussprechen. Statt dessen müssen die genauen Anforderungen und Gegebenheiten im zu vernetzenden Betrieb geprüft werden und dann eine individuelle Netzwerklösung aus Ethernet und WLAN entwickelt werden, die die jeweiligen Vorteile am günstigsten nutzt und das optimale Verhältnis aus Leistung, Kosten und Sicherheit bietet.

9. Quellenverzeichnis

- „Wireless mit Cisco – einfach und schnell - Der Wireless LAN-Leitfaden für Entscheider", Cisco Systems GmbH, 2001
- „Leitfaden Einsatz von WLAN in Unternehmen", Dipl.-Inf. Heiko Kopp, ECCOM - Electronic Commerce Center Mecklenburg-Vorpommern, 2004
- „Studienarbeit S300", Prof. Dr.-Ing. Dr. E.h. Wolfgang Weber, Ruhr-Universität Bochum, 08.01.2003
- „Wireless LAN - Protokolle und Anwendungen", Axel Sikora, Addison-Wesley, 2001
- „WLAN & MoPS", Thomas Böttcher, Rechenzentrum RWTH-Aachen, 2003
- „Sicherheit im Funk-LAN" , Bundesministerium für Sicherheit in der Informationstechnik, Version 1.1, 2003
- ComputerBase.de - Der Wireless LAN Grundlagenreport (http://www.computerbase.de - 25.07.2003)
- Tom's Hardware Guide - Grundlagen: Drahtlose Netzwerke (http://www.tomshardware.de - Teil 1: 10.03.2003, Teil 2: 02.04.2003)
- Wikipedia - Die freie Enzyklopädie (http://de.wikipedia.org/wiki/Hauptseite - 01.02.2005)
- Golem.de - News (http://www.golem.de/0304/25188.html - 01.02.2005)