

Freie WLAN-Netze

Robert Karabensch

Sebastian Scheibe

Björn Bühring

Information Rules WS 2004/05

TU-Berlin

Inhalt:

1 Einleitung

2.1 Commons

2.2 Anti-Commons

2.3 Idee des Internet

2.4 Idee der freien WLAN-Netze

2.5 Commons/Anti-Commons Diskussion bzgl. Internet/Freie WLAN-Netze

3.1 Geschichte des WLAN

3.2 Pico-Peering Vertrag

3.3 Aktuelle Fassung der PPA

4.1 Einsatzgebiete

4.2 Betriebsmodi

4.3 Sicherheitsaspekte

4.4 Ein kurzes Fazit

5 Rasant ansteigende Zahl von freien Netzen kontra kommerzielles Interesse der Provider

1 Einleitung

In dieser Ausarbeitung haben wir uns mit den Freien WLAN-Netzen beschäftigt, wobei wir einen besonderen Augenmerk auf die Frage gelegt haben : „Freie WLAN-Netze – das bessere Internet?“. Mit dieser Ausarbeitung soll jedoch keine Antwort auf die Frage gegeben werden, sondern nur einige Aspekte dieser Netzidee näher betrachtet werden. Zuerst werden die Idee, danach die geschichtliche Entwicklung und zum Schluss die technischen Aspekte beleuchtet, um einen kleinen Überblick über dieses Thema zu verschaffen.

2.1 Commons

Commons bezeichnen eine Ressource, die von mehreren Menschen gleichzeitig genutzt wird, wobei keiner Besitzansprüche hat. Weiter hat auch keiner das Recht den anderen von der Nutzung auszuschließen. Im deutschen ist das Wort der Allmende eher gebräuchlich, beschreibt aber das selbe.

Im frühen Mittelalter gab es in fast jeden Dorf einen Platz oder eine Wiese, die von jedem Dorfbewohner benutzt werden durfte. Jedoch sind Commons heutzutage kaum noch im ursprünglichen Sinne (Acker, Stadtplatz) vorhanden, jedoch wurde die Diskussion über die Commons, auf die ich noch eingehen werde, auf andere Gebiete ausgeweitet, wie z.B. das Internet. Bei der Diskussion über die Commons geht es vornehmlich darum, ob es sinnvoll ist eine Ressource nach dem Prinzip der Commons zu nutzen, dies bedeutet, dass jeder das Common frei nutzen darf, ohne jegliche Einschränkung in Dauer und Umfang.

Im Jahre 1968 verfasste Garrett Hardin den Artikel „Tragedy of the Commons“, der jahrzehntelang die Diskussion über die Commons beherrschte. Seiner Meinung nach sei jede Commons dem Untergang geweiht. Dies wird damit begründet, dass z.B. auf einem Acker, der als Common genutzt wird, mit der Zeit zu viele Tiere weiden werden, mit der Begründung: „It is to be expected that each herdsman will try to keep as many cattle as possible on the commons.“ [Hardin,1968]. Hieraus ergibt sich die totale Abnutzung der Ressource auf Dauer, da es eine grundlegende Eigenschaft des Menschen sei, daß er versuchen würde seinen eigenen Nutzen ohne Rücksicht auf die anderen zu maximieren.

Erst im Jahre 1999 verfasste Prof. Elinor Ostrom eine These dagegen. In ihrem Text „Coping with Tragedies of the Commons“ belegt sie die Aussage, dass es durchaus Commons geben kann, deren Ressource auf Dauer nicht abgenutzt wird. Hierbei ist eine wichtiges Argument, dass sie in Laborversuchen gezeigt hat, dass der Mensch nicht automatisch darauf aus ist, seinen eigenen Erfolg immer zu maximieren, sondern dass der Mensch unter gewissen Umständen (geeignete

Kommunikationswege) bereit ist, seine Handlung zu koordinieren, so dass die Ressource effizient genutzt werden kann. Weiter sind die Eigenschaften der Nutzer, sowie die der Ressource (abnutzbarkeit) wichtig, um darüber zu entscheiden, ob eine Ressource als Common genutzt werden kann oder nicht.

Zusammenfassend lässt sich also sagen, dass es bei der Diskussion um ein Commons es besonders auf die Beschaffenheit der Ressource, aber auch der Nutzer ankommt.

2.2 Anti-Commons

Eine weitere Diskussion, die erst in den letzten Jahren aufgekommen ist, ist die Diskussion über Anti-Commons¹. Wie der Name schon sagt sind Anti-Commons das genaue Gegenteil von Commons, da die Ressource hier auch von einer großen Anzahl von Menschen genutzt wird, jedoch hat jeder einzelne das Recht den anderen an der Nutzung zu hindern, daraus folgt: „In an anticommons, by my definition, multiple owners are each endowed with the right to exclude others from a scarce resource, and no one has an effective privilege of use.“ [Heller,1997]. Also wird bei den Anti-Commons die Ressource nicht abgenutzt, sondern ineffizient genutzt.

Bei der späteren Betrachtung des Internet und der Freien WLAN-Netze bezüglich der Anti-Commons, wollen wir nicht die genaue Definition von Heller anwenden, sondern werden uns auf die etwas weiter gefasste Definition beziehen, wie sie auch in dem Artikel von Kamppari verwendet wird: „...if we replace the total exclusion by additional costs accrued by taking e.g. the site terms of use into account we may well describe the outcome with the same mathematical and graphical models.“, da auf Internetseiten eigentlich nicht mehrere Leute das Recht haben jemanden zu behindern, sondern es fallen eher zusätzliche Kosten aufgrund von Registrierungen und so weiter an. Wodurch sich wie später betrachtet auch eine Ineffiziente Nutzung ergeben kann.

2.3 Idee des Internet

Eine der grundlegendsten Ideen des Internets hat 1962 J.C.R. Licklider des MIT verfasst: „... a globally interconnected set of computers through which everyone could quickly access data and programs from any site“ [Leiner, 2003]. Dies betrachtet aber nur einen Teil der anfänglichen Idee hinter dem Internet.

Ein sehr viel wichtigerer Aspekt war der Community-Gedanke, hierbei geht es vorwiegend darum,

¹ Der Begriff wurde von Michael A. Heller 1997 in seinem Artikel „The Tragedy of the Anti-Commons: Property in the Transition from Marx to Markets“ in Anlehnung an die Commons Diskussion eingeführt.

dass eine große Gemeinschaft in der Lage ist frei Informationen auszutauschen. Für diesen Aspekt waren natürlich die an der Entwicklung beteiligten Universitäten ausschlaggebend, da es der akademischen Tradition folgt: „... of open publication of ideas and results“[Leiner, 2003].

In den Jahren von 1960 bis Ende der 1970er gab es schon eine Menge kleiner Forschungsnetze, welche als closed communities benannt werden können, da sie nur für eine begrenzte Anzahl von Nutzern zugänglich waren. Diese Netze dienten genau dem vorher angesprochenen schnellen Austausch von Informationen. Daher war mit ein grundlegender Gedanke bei der Entwicklung des Internet, dass hiermit viele kleine Netze zu einem großen verbunden werden sollten. Um diese Möglichkeit sicher zu stellen wurde die Idee des Open Architecture Networking entwickelt, diese besagt, dass keiner in der Wahl der Netzwerkarchitektur seines Netzes eingeschränkt sein soll, nur weil er sich dem Internet oder einem anderen Netz anschließen möchte. Daraus folgt auch, daß das heutige Internet eigentlich eine riesige Ansammlung kleiner Netze, wie Privat- oder Firmennetze ist. Um die Entwicklung des Internets zu beschleunigen und jedem die Möglichkeit zu geben, sich mit dem Internet zu verbinden, sollten alle Dokumente über die Protokolle frei zugänglich sein. Dies war auch sehr wichtig, damit die Benutzer nicht an ein Netzwerkprodukt gebunden sind, da durch die freie Verfügbarkeit der Protokolle, diese in jegliche Software mit eingebunden werden kann. Um eine große Akzeptanz herzustellen, und zur Minimierung der Entwicklungskosten wurden die Protokolle von einer großen Community gemeinsam entwickelt.

Die Bedeutung des Informationsaustauschs sieht man vor allem in der rasanten Entwicklung von Kommunikationswerkzeugen, wie der E-Mail und RFCs. Durch die E-Mails war eine schnellere Kommunikation als auf dem Postweg möglich. Die RFC (Request For Comment) dienen besonders dazu, um für neue Ideen Kommentare zu bekommen, um seine Idee weiterzuentwickeln. Hier zeigt sich auch wieder der Community-Gedanke, dass man als Gemeinschaft die Entwicklung schneller und besser vorantreiben kann.

2.4 Idee der Freien WLAN-Netze

Bei den Freien WLAN-Netzen wird die Grundidee des Internet mit aufgenommen, und noch weiter verfeinert und vor allem in einem Dokument / Abkommen verfestigt. Um die Idee der Freiheit in den Netzen zu veranschaulichen wird hier das „Kommunikationsmodell Netzfreiheit“² benutzt:

- Physisch/materielle Netzfreiheit
- Zugangsfreiheit
- Kommunikationsfreiheit

² Das „Kommunikationsmodell Netzfreiheit“ ist aus dem Buch Freie Netze von Armin Medosch entnommen [Medosch,2003]

-Medienfreiheit

Auf der Ebene der physisch/materiellen Netzfreiheit, geht es um die bei der Idee des Internets angesprochene Möglichkeit für jeden ein eigenes individuelles Netz aufzubauen. Trotzdem soll natürlich die Möglichkeit bestehen sich mit den Freien Netzen zu verbinden. Bei dieser Schicht soll bei den Freien WLAN-Netzen noch der kostengünstige oder fast kostenlose Netzzugang zählen, der zur Grundidee der Netze gehört.

Die Zugangsfreiheit besagt, dass es allen Nutzern ermöglicht werden soll die freien Netze zu nutzen, solange sie keine finanziellen Interessen verfolgen.

Bei der Kommunikationsfreiheit geht es um die Möglichkeit, dass jeder mit jedem kommunizieren kann und hierbei auch frei bei der Wahl seiner Medien ist (Medienfreiheit).

Wichtigster Unterschied zum Internet ist, dass von vornherein keine kommerziellen Interessen zugelassen sind.

Ein weiterer Bestandteil ist das Ressource-Sharing, da jeder einen Teil seiner Ressource für die gesamte Community freigibt, da über das eigene Netz nach der Mesh-Netzwerkarchitektur die Daten anderen Teilnehmer transportiert werden.

2.5 Commons/Anti-Commons Diskussion bzgl. Internet und Freie WLAN-Netze

Bei der Diskussion über die Entwicklung des Internet und der Freien WLAN-Netze ist die Betrachtung der Commons-Diskussion sehr wichtig, da man beide Netze in gewissen Maßen als Commons auffassen kann.

Die Ressource, über die bei den Netzen diskutiert wird, sind die Informationen in Form von Daten und die Bandbreite.

Wenn man die Information als Ressource betrachtet, so kommt man zu dem Ergebnis, dass diese Ressource nicht abnutzbar ist, da Daten bzw. Informationen in den Netzen nur kopiert werden und daher nicht abgenutzt werden können. Folglich kann man die Theorie von Elinor Ostrom anwenden, dass je nach Beschaffenheit der Ressource, z.B. nicht abnutzbar, ein Common grundsätzlich möglich ist. Bei der Bandbreite sieht es ähnlich aus, diese ist auch nicht abnutzbar, jedoch kann es zu Engpässen kommen. Obwohl dies beim Internet eher zu vernachlässigen ist, da die Datenleitungen heute so stark ausgebaut sind, dass es nur selten zu solchen Engpässen kommt. Die Bandbreite spielt aber schon eher bei den Freien WLAN-Netzen eine Rolle, da es hier auf Grund der Mesh-Topographie schnell zu sogenannten „Flaschenhälsen“, also Engpässen, kommen kann.

Beide Netze werden noch unter dem Aspekt der Anti-Commons betrachtet, hierbei kann man sagen, dass das Internet sich stark in diese Richtung entwickelt. Da immer mehr staatliche Institutionen

und Unternehmen versuchen hierauf Einfluss zu nehmen, so dass es zu immer stärkeren Restriktionen kommt. Weiter nimmt auch die Anzahl der kosten- und registrierungspflichtigen Seiten zu. Wie schon vorher erwähnt erhöht dies die persönlichen Kosten jedes einzelnen, wodurch die Anzahl der User stetig abnimmt. Hieraus kann man folgern, dass die Ressource Bandbreite und Information ineffizient genutzt werden, da sich die User es immer mehr überlegen werden bestimmte Informationen abzurufen, da der Aufwand hierfür zunimmt. Dieses Problem wird bei den Freien Netzen versucht zu verhindern, indem die kostenfreie Nutzung ein Grundbestandteil der Freien Netze ist, und daher auch in dem noch später erläuterten Pico-Peering-Agreement erwähnt wird.

3.1 Geschichte des Wlan

Die Geschichte des Datenfunks begann schon am Anfang des zwanzigsten Jahrhunderts in der Seefahrt, wo man mit Hilfe des Morsecodes drahtlose Zeitungen für die Passagiere auf den Schiffen erstellte. Diese wurden mittels Funkübertragungen von den jeweiligen Küstenstationen auf die Schiffe gesendet. Die Reichweite der damaligen Übertragungen war noch sehr begrenzt und konnte sich durch die jeweiligen Wetterverhältnisse verbessern oder verschlechtern.

Das eigentliche Wlan so wie wir es heute kennen, wurde aber erst viel später entwickelt, seinen Anfang nahm es in den 70er Jahren. Damals wurde unter der Leitung von NORMAN ABRAMSON die Funktechnologie und das Netzwerk zum ersten Mal zusammen eingesetzt. Man verband auf diese Weise die sieben verschiedenen Forschungskomplexe der Universität von Hawaii, die auf vier verschiedenen Inseln verteilt waren. Durch eine sternförmige Verbindung wurden die vier Inseln mit dem Zentralrechner in Oahu verbunden. Die Forschungskomplexe hatten nur die Möglichkeit über diesen Zentralcomputer mit den anderen Außenstellen Kontakt aufzunehmen.

Zur gleichen Zeit schrieb ein junger Student mit dem Namen BOB METCALFE an seiner Doktorarbeit. Er interessierte sich sehr für die Forschungsarbeiten von ABRAMSON und nachdem er seinen Abschluss hatte, verbrachte er noch ein Jahr an der Universität von Hawaii. Nach diesem einen Jahr wechselte er zum Xerox PARC, wo die dortigen Wissenschaftler schon an einer Forschung arbeiteten, welche später als PC (Personal Computer) bekannt werden sollte. Damals waren die dortigen PC's noch nicht untereinander vernetzt. BOB METCALFE begann zusammen mit seinem Kollegen DAVID BOGGS, aufbauend auf den Arbeiten von ABRAMSON, an einer Vernetzung zu forschen, die später als LAN (Local Area Network) bekannt werden sollte.

Die Netzwerktechnologie, welche auch unter dem Namen Ethernet bekannt wurde, ist 1976 erstmals implementiert worden.

1978 wurde der erste Ethernetstandard mit Übertragungsraten von 10 Mbps entwickelt.

Die IEEE begann 1980 mit der Entwicklung eines herstellerunabhängigen Standards für LAN, der wenig später den ersten Standard 802.3 hervorbrachte.

1968 wurde von den Forschern ein Prototyp zur paketvermittelnden Kommunikation vorgestellt, welche von der ARPA (Advanced Research Projects Agency) finanziell gefördert wurde.

Die ARPA hatte sich zum Ziel gesetzt, eine Netzwerktechnologie zu entwickeln, die es im Kampfeinsatz jederzeit ermöglichen sollte, dass die Fahrzeuge in Kontakt mit der Basisstation standen. So sollten immer die aktuellsten Informationen aus dem jeweiligen Krisengebiet schnell an die Kommandozentralen weitergeleitet werden, damit man auf eine etwaige Bedrohung schnell reagieren konnte. Durch eine Technikdemonstration, bei der ein Wissenschaftler von einem LKW aus, ausgestattet mit einem Laptop, versuchte einen Computer in London zu benutzen, erkannte man, dass die verwendeten Protokolle noch nicht ausgereift genug waren, um verschiedene Netze über bestimmte Entfernungen miteinander zu verbinden. Die ARPA begann daraufhin ihre Forschungen in dem Bereich der Protokolle zu intensivieren. So kam es zur Geburtsstunde des TCP / IP-Protokolls. Dieses Protokoll wurde entwickelt, um verschiedene Netze untereinander zu verbinden und um den Datenaustausch zu ermöglichen.

Verschiedene Firmen sowie die Universität von Berkeley wurden von der ARPA damit beauftragt, das Protokoll in Unix zu integrieren. Das wiederum hatte zur Folge, dass sich zum einen Unix weiter durchsetzen konnte, aber auch das verwendete Protokoll fand schnelle Verbreitung. Immer häufiger sprach man vom so genannten Internetworks und 1983 setzte sich das TCP / IP-Protokoll endgültig als Standard durch.

1985 kam es dazu, dass die FCC (Federal Communications Commission) das ISM (Industrial Scientific and Medical)-Band freigab und die Industrie daraufhin mit der Entwicklung von Funktechnologien begann. 1997 wurde der erste Funk-Standard der 802.11 verabschiedet.

3.2 Pico-Peering-Vertrag

Der Begriff Pico-Peering ist eine Schöpfung von JULIAN PRIEST. Das Wort „Pico“ verweist allgemein auf die Kleinheit der Netze. Peering steht für das Abkommen, das die einzelnen Provider untereinander über den Austausch der Daten schließen. Pico-Peering zeigt davon, wie die Abkommen der Provider (Peering) auf sozialer, juristischer und technischer Ebene umgesetzt werden sollen.

Im Oktober 2002 fand der BerLon-Workshop in den bootlabs in Berlin statt. Hier trafen sich die Netzbegeisterten zum gemeinsamen Debattieren und Ideenaustausch. Am Rande des Workshops fand sich eine kleine Gruppe um JULIAN PRIEST, SAUL ALBERT, ADAM BURNS, JAMES STEVENS, PIT SCHULTZ, FLORIAN CRAMER, THOMAS KAULMANN, JÜRGEN NEUMANN, SEBASTIAN BÜTTRICH, DAVID

CUERTELLES SOWIE ARMIN MEDOSCH zusammen, welche mit den Beratungen zum Pico-Peering in einem separaten Raum am Rande des Workshops begannen. Die meisten der Anwesenden hatten genaue Vorstellungen von freien Netzen. Man kam zu der Auffassung, dass dies für die immer größer werdende Vernetzung nicht mehr ausreichte. Es mußten gewisse Regeln aufgestellt werden. Ein großes Problem, was dabei bewältigt werden musste, war, dass die meisten Netzwerker Individualisten waren und sich nicht gern Vorschriften machen ließen. Viele sahen in dem Wort „Agreement“ schon eine Welt voller Einschränkungen durch Gesetze. Man wusste zur damaligen Zeit auch noch nicht genau, auf welcher Ebene die PPA wirksam werden sollte.

Im Laufe des ersten Tages einigte man sich darauf, dass es drei Fassungen der PPA geben sollte. Eine Fassung für den Juristen, eine maschinenlesbare und eine Fassung für den Normalbürger. Des Weiteren überlegten sich die Teilnehmer, welche Lizenz sie am besten für die PPA heranziehen konnten und man kam zu dem Entschluss, dass die GNU Documentation Licence und die Debian Licence am besten als Vorbilder für die PPA geeignet wären. Denn diese Lizenzen bezogen sich nicht nur auf die Software, sondern auch auf die Dokumentation zur Software. Eine solche Lizenz war wichtig, da in den Netzen freie Software eingesetzt und weiterentwickelt werden sollte, was natürlich eine freie Netzstruktur voraussetzt.

ADAM BURNS, der schon ein Grundsatzpapier zu Hause entwickelt hatte, schlug vor, dass die Teilnehmer sich zur Offenheit verpflichten. „Alles was nicht explizit verboten ist, sollte erlaubt sein.“(Quelle: Armin Medosch)

Da die Dienste kostenlos angeboten werden, sollten, war die Qualität mit der von kommerziellen Netzen nicht vergleichbar. Es ging bei dem Abkommen um den freien Datentransit. Die Vorstellung bestand darin, dass die freien Netze die Ränder der kommerziellen Netze konsumieren.

Am zweiten Tag des Workshops traf man sich nochmals, um ein Protokoll anzufertigen, welches danach sofort in der Wiki veröffentlicht wurde.

Schnell wurde jedoch klar, dass man noch ein gutes Stück von einer brauchbaren Fassung entfernt war. Anfang März traf sich der harte Kern der Gemeinschaft nochmals in Kopenhagen. Hier wurde unter einem gewissen Zeitdruck die erste Fassung der PPA und aufbauend auf den Ergebnissen aus Berlin, fertiggestellt.

3.3 Aktuelle Fassung der PPA

1. Freier Transit

- Der Eigentümer bestätigt, freien Transit über seine freie Netzwerkinfrastruktur anzubieten

- Der Eigentümer bestätigt, die Daten, die seine freie Netzwerkinfrastruktur passieren, weder störend zu beeinträchtigen noch zu verändern.

2. Offene Kommunikation

- Der Eigentümer erklärt, alle Informationen zu veröffentlichen, die für die Verbindung mit seiner Netzwerkinfrastruktur notwendig sind.
- Diese Information soll (muss?) unter einer freien Lizenz (free licence) veröffentlicht werden.
- Der Eigentümer erklärt, erreichbar zu sein und wird dazu wenigstens eine E-Mail-Adresse bekanntgeben.

3. Keine Garantie (Haftungsausschluss)

- Es wird keinerlei garantierter Dienst (Betrieb, Service) vereinbart. (Es gibt keine Garantie für die Verfügbarkeit / Qualität des Dienstes.)
- Der Dienst (Betrieb, Service) wird ohne Gewähr bereitgestellt, ohne Garantie oder Verpflichtung jedweder Art.
- Der Dienst (Betrieb, Service) kann jeder Zeit ohne weitere Erklärung beschränkt oder eingestellt werden.

4. Nutzungsbestimmungen

- Der Eigentümer ist berechtigt, eine akzeptierbare Benutzungsrichtlinie (use policy) zu formulieren.
- Diese kann Informationen über zusätzlich (neben den grundsätzlich) angebotene Dienste enthalten.
- Dem Eigentümer steht es frei, die Richtlinie selber zu formulieren, so lange diese nicht den Punkten 1 bis 3 dieser Vereinbarung widersprechen (siehe Punkt 5).

5. Lokale (individuelle) Zusätze

- Hier können vom Eigentümer selbst Ergänzungen zur Vertragsvereinbarung vorgenommen werden.

Begriffserklärungen

- Eigentümer: Der Eigentümer verfügt über das Recht, seine Netzwerkinfrastruktur zu betreiben und einen Teil ihrer Funktionalität für das freie Netzwerk (FreeNetwork) bereitzustellen (zu stiften, zu spenden).
- Transit: Transit ist der Austausch von Daten in ein Netzwerk hinein, heraus oder durch ein Netzwerk hindurch.
- Freier Transit: Freier Transit bedeutet, dass der Eigentümer weder Gebühren für den Transit von Daten erhebt, noch die Daten verändert.

- Freies Netzwerk: Das Freie Netzwerk ist die Summe der miteinander verbundenen Hard- und Software, dessen Anteil für den freien Transit vom Eigentümer dieser Ressourcen zu Verfügung gestellt wird.
- Der Dienst: Der Dienst (Betrieb, Service) besteht aus freiem Transit und zusätzlichen Diensten.
- Zusätzliche Dienste: Im Sinne des PPA ist ein Zusätzlicher Dienst alles was über freien Transit hinaus geht. Zum Beispiel die Bereitstellung eines DHCP-Servers, WEB-Servers oder Mail-Server

Quelle:<http://www.picopeer.net/PPA-de.html>

4.1. Einsatzgebiete

Nun kann man sich mit Recht die Frage stellen: Warum überhaupt WLAN?

Vor allem angesichts der Vielfalt bereits existierender, gut ausgebauter Netze und der mit der WLAN-Technik verbundenen Vielzahl von Problemen wie Datenschutz und Datenmanipulation, Virenbedrohung und der Netzwerksicherheit im Allgemeinen.

Mit einem Blick auf aktuelle Anwendungsgebiete, in denen bereits heute kein anderes System mehr denkbar ist lässt sich die Frage allerdings sehr schnell beantworten.

Die ersten Kabel-unabhängigen Netzwerklösungen kamen vorrangig in der Industrie zum Einsatz. Bereits seit vielen Jahren sind Firmen-interne, funkbasierte Intranetze in Unternehmen und Produktionsstätten weit verbreitet.

Die Vorteile liegen ja auch auf der Hand: ein gleichzeitig schnelles - da räumlich sehr begrenztes - und sicheres - da nach außen abgeschottetes (von den wenigen AccessPoints in andere Netze mal abgesehen) - Netzwerk, auf das jeder Mitarbeiter Zugriff hat, sofern gerade ein PC, Notebook oder Terminal verfügbar ist.

Mit dem Einsatz der Datenübertragung per Funkverbindung erreichen diese Netzwerke nun eine noch höhere Effizienz und Flexibilität als mit herkömmlichen Datenleitungen. Die fest verankerten, stationären Terminals können je nach Erfordernis durch mit entsprechenden Funkkarten versehene Laptops, PDA's und ähnliche Geräte ersetzt werden oder werden selbst zum WLAN-Knoten umgerüstet.

Neben Anwendungsbereichen in der Verwaltung von Lagerbeständen, und der ständigen Pflege von Produktions- und Fertigungsdaten während des gesamten Produktionsprozesses treten Büroanwendungen immer mehr in den Vordergrund. Sei es im Gesundheitsbereich der ständige und ortsunabhängige Zugriff auf Kranken- und Pflegedaten in Krankenhäusern und Praxen oder im normalen Büroalltag die Teilnahme mit Notebook und Netzwerkzugriff auch an spontan einberufenen (Video-)Konferenzen und Meetings.

Die Mobilität oder genauer die Möglichkeit des ortsunabhängigen Datenzugriffs (mobile Access), die Flexibilität des kompletten Arbeitsplatzes innerhalb eines Unternehmens und der Austausch von stetig größer werdenden Datenmengen spielen eine immer wichtigere Rolle im täglichen (Berufs-) Leben.

Des Weiteren gibt es Bereiche, in denen der Aufbau von Kabel-Netzwerken durch bestehende gesetzliche Restriktionen stark eingeschränkt wird (z.B. Denkmalschutz) oder allein durch die baulichen Gegebenheiten sehr schwierig und kostenintensiv oder gar unmöglich ist.

Man denke nur an die unzähligen Kilometer Kabel, die in Bürogebäuden überall auf der Welt verlegt wurden nur um jeden Arbeitsplatzrechner oder jedes Terminal mit einem oder mehreren meist zentralen Drucker zu verbinden. Die ersten marktfähigen Lösungen – Wireless-Printserver – werden bereits mit Erfolg und vergleichsweise geringen Kosten eingesetzt.

Eine bedienerfreundliche Benutzung und der geringe Aufwand für den Zugriff auf bestehende Netzwerke wie dem Internet machte die WLAN-Technik schnell auch dem „Heim“-Anwender zugänglich.

So sind WLAN-Netze auf Bahnhöfen und Flughäfen (neuerdings auch in Zügen und Flugzeugen selbst), Universitäten und Hotels, auf Messen und anderen Großveranstaltungen schon fast nicht mehr wegzudenken. Ein Laptop mit Funknetzwerkkarte reicht aus und die vier Stunden bis der Anschlusszug abfährt vergehen wie im Flug.

4.2. Betriebsmodi

Es gibt zwei grundlegende Betriebsmodi ein WLAN-Netzwerk zu betreiben.

Beim **Ad-Hoc** oder auch **Peer-to-Peer-Modus** kommunizieren verschiedene, gleichwertige Clients (PC, Laptop, Palm, etc.) mittels geeigneter Software miteinander. Jeder einzelne Knoten eines so errichteten, nach außen abgekapselten Netzes ist gleichzeitig Sender und Empfänger beliebiger

Daten und Router für die Informationsvermittlung zweier nicht direkt benachbarter Clients.

Dieses sich selbst organisierende Netzwerk bietet zum einen den Vorteil des geringst möglichen administrativen Aufwands (es gibt de facto keinen Netzwerkadministratoren) und zum anderen eine ausgewogene Lastverteilung, da kein zentraler Punkt zur Verwaltung und Datenübertragung und –vermittlung benötigt wird. Der berühmte Bottleneck-Effekt wird bei diesen auch Mesh-Netzwerken oder MANet (Mobile Ad-Hoc-Network) genannten Netzwerken also von Anfang an verhindert.

Im Gegensatz zum Ad-Hoc- gibt es beim **Infrastruktur-Modus** einen (oder mehrere) ausgezeichnete Netzwerkknoten. Diese als Access Points bezeichneten Knotenpunkte organisieren die Kommunikation aller Clients, die sich mit Ihrer MAC-Adresse bei dem jeweiligen Access Point angemeldet haben. Sie sind also sowohl Router innerhalb des WLAN-Netzes als auch Einstiegspunkt (Hotspot) in andere (Kabel-)Netze, wie z.B. dem Internet.

Die Gefahr des schon erwähnten Effektes, bei dem die verfügbare Bandbreite ab einem bestimmten Datenaufkommen zum Flaschenhals wird kann hier allerdings mit dem Einfügen weiterer Access Points entschärft werden.

Bei beiden Modi besteht allerdings wie auch bei allen anderen Netzwerktopologien das Problem, dass bei steigender Anzahl der Knoten die Komplexität des Netzwerkes und damit das Datenvolumen zur Kommunikation stark ansteigt. So gibt es in jedem Netzwerk Knotenpunkte die weniger ausgelastet sind und solche, die eher dazu neigen, einen Engpass für die Kommunikation innerhalb des Netzes darzustellen.

4.3 Sicherheitsaspekte

Das offensichtlich größte Problem von WLAN-Netzwerken ist jedoch die Tatsache, dass die Informationen von (meist Rundstrahl-)Antennen allseitig, also in jede beliebige Richtung ausgesandt und empfangen werden und damit die Sicherheit solcher Netze.

Als WarDriving (Wireless Access Revolution) wird das Aufspüren, als WarChalking oder NetStumbling sogar das Katalogisieren von mehr oder (offensichtlich) weniger sicheren Funknetzwerken bezeichnet.

Ein WLAN-fähiger Laptop reicht meist aus um auf ‚Jagt‘ nach ungeschützten Netzen zu gehen.

Allein das Mitlesen von Daten, die Datenspionage kann aus Datenschutz-rechtlicher Sicht verheerende Folgen für den Netzbetreiber haben, wenn es sich z.B. um sensible Patientenakten in Krankenhäusern oder ganz allgemein um personengebundene, vertrauliche Daten in Ämtern,

Rechtsanwaltskanzleien, Banken oder Arztpraxen handelt.

Werden die Daten darüber hinaus verändert - Datensabotage - oder sich jemand über ein betriebliches Netz ins Internet einwählt und von dort aus Angriffe auf dritte vornimmt, kann das das Ende eines ganzen Unternehmens bedeuten.

Eine Vielzahl von Verschlüsselungsalgorithmen wie z.B. WEP, WPA, WPA2 und weitere, wurden speziell für die Übermittlung von Informationen über das Medium Luft entwickelt, bieten allerdings nur begrenzten Schutz vor unerlaubtem Zugriff auf das Netzwerk und damit auf die Informationen. Die Kombination mit weiteren Sicherheitsvorkehrungen wie der Verwendung von Firewalls, eines VPN-Servers (Aufbau sog. VPN-Tunnel) und Sicherheitszertifikaten wie sie im Internet weit verbreitet sind ist dringend zu empfehlen.

Ein MAC-Adress-Filter bestimmt, welche Clients dem Netz beitreten dürfen; ungebetenen Gästen wird damit (zumindest vorerst) die Tür verschlossen.

Vorwiegend in industriellen Funknetzen hat sich darüber hinaus ein zeitgesteuerter Netzwerkzugriff bewährt – nach Arbeitsende oder z.B. nachts muss nicht unbedingt von jedem Terminal auf dem gesamten Betriebsgelände auf das Netz zugegriffen werden können.

Nicht als letzter Punkt sei an dieser Stelle auf die Verwendung von Richtfunkantennen hingewiesen. Sie haben gegenüber Rundstrahlantennen, die je nach den räumlichen Gegebenheiten 30 bis 100 Meter Reichweite (in jede beliebige Richtung) erreichen, einen deutlich geringeren Abstrahlwinkel und können so nicht nur Fremdnutzern die Empfangleistung entziehen, sondern zusätzlich die Funkreichweite auf mehrere Kilometer Länge erhöhen.

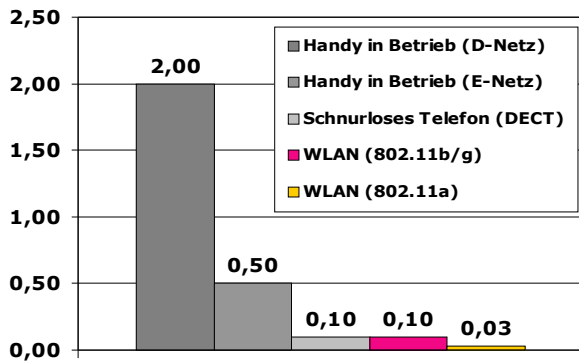
4.4 Ein Kurzes Fazit

Obwohl die zusätzliche Strahlungsbelastung und vor allem die Sicherheit die meist diskutierten und schwerwiegendsten Nachteile von Funk-basierten Netzwerken sind, überwiegt allein schon der potenzielle Nutzen bzw. die Fülle der Möglichkeiten:

Zahl- und kostenlose, da nach dem PPA Lizenzfreie Dienste wie z.B. VoiceOverIP, Bildtelefonie, Audio- und Videostreaming, Communityradio und WebTV (betreiben und hören) sind denkbar und werden schon heute genutzt.

Weitere Vorteile von WLAN-Netzen sind die einfache, schnelle und kostengünstige Installation, die geringen Administrationskosten, die Lizenz- und Kommerzfreiheit und die im Vergleich zu anderen

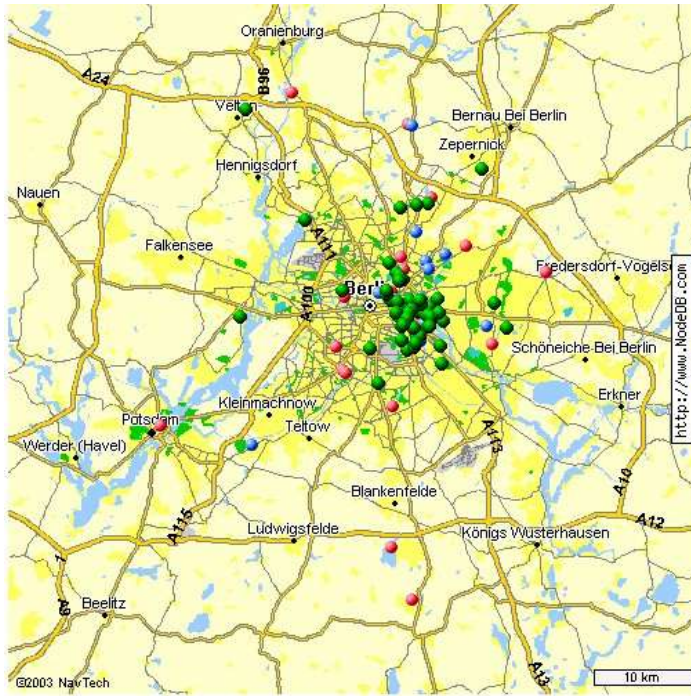
Drahtlosen Kommunikationssystemen (Mobiltelefon) geringe gesundheitliche Belastung:



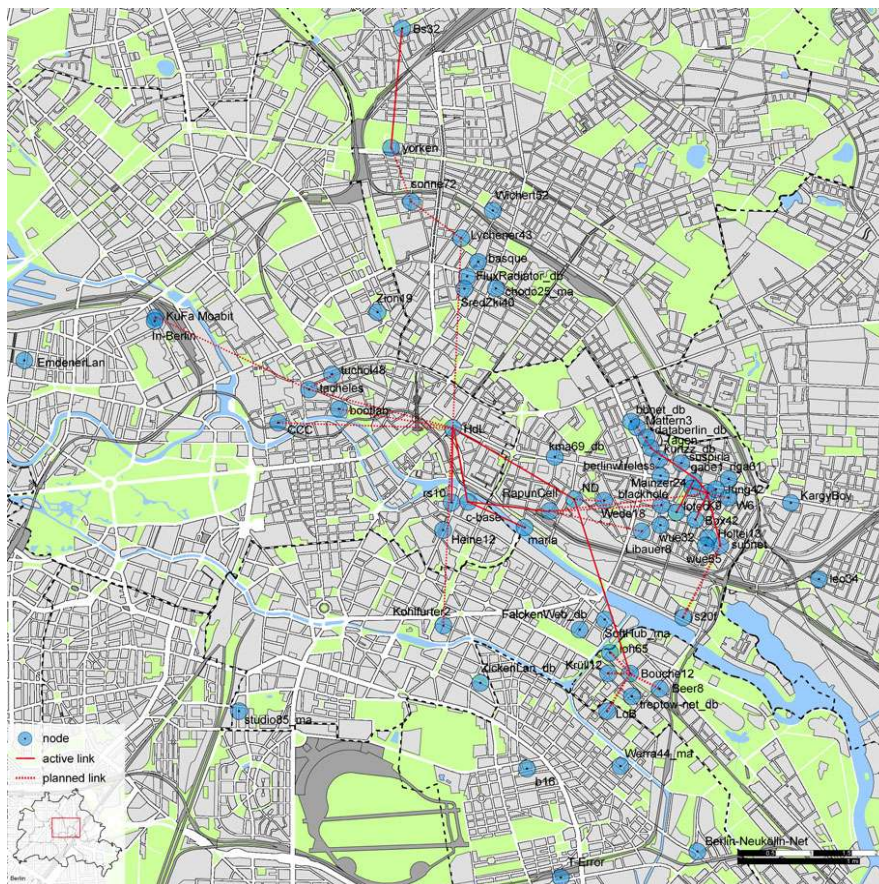
Quelle: Freie Funkbasierte Netzwerke. Internet: <http://www.freifunk.net>

5 Rasant ansteigende Zahl von freien Netzen kontra kommerzielles Interesse der Provider

Das immer größer werdende Netz mit seinen inzwischen Tausenden von Usern ist auch den großen Providern nicht verborgen geblieben. In den USA, speziell im Bundesstaat Pennsylvania, sollte mit Hilfe von öffentlichen Geldern eine ganze Stadt (Philadelphia) mit eigenem Wlan versorgt werden. Dieses Projekt sollte mit 10-12 Mio US Dollar unterstützt werden. Der Provider Verizon Communication sah darin aber eine Gefahr für das eigene Geschäft, da man annahm, dass ein so gefördertes Projekt dem Endverbraucher billiger käme, als das eigene Angebot eine Gefahr für das eigene Geschäft. Durch das neu verabschiedete Telekommunikationsgesetz in Pennsylvania ist es den örtlichen Kommunen und Städten untersagt, den Bürgern eigene Breitbandnetze anzubieten, ohne den großen lokalen Telefongesellschaften, entsprechende Angebote unterbreitet zu haben. Sollten sich diese innerhalb von 14 Monaten dazu entscheiden, selbst ein Netz aufzubauen, müssen sie ihre Pläne verwerfen. Dies stellt einen Rückschlag für die freien Netze dar, zeigt aber gleichzeitig auch, wie konkurrenzfähig sie geworden sind.



Entwicklung der freien Wlan Netze in Berlin und Umgebung



Entwicklung der freien Wlan Netze in Berlin

Literaturverzeichnis

Hardin, Garrett (1968), „Tragedy of the Commons“, in: Science, Nr. 162; S.1243-1248.

Heller, Michael A. (1997), „The Tragedy of the Anti-Commons: Property in the Transition from Marx to Markets“, William Davidson Institute Working Papers Series40, William Davidson Institute at the University of Michigan Business School,
<http://ideas.repec.org/p/wdi/papers/1997-40.html> (besucht: 14.12.2004)

Kamppari, Sauli (2004), „Tragedy of digital anti-commons“,
http://www.netlab.hut.fi/opetus/s38042/s04/Presentations/06102004_Kamppari/Kamppari_paper.pdf (besucht: 14.12.2004)

Leiner, M. Barry (2003), „A brief History of the Internet“,
<http://www.isoc.org/internet/history/brief.shtml> (besucht: 14.12.2004).

Medosch, Armin (2003), „Freie Netze“, Heinz-Heise-Verlag, Hannover.

Ostrom, Elinor (1999), „Coping with Tragedies of the Commons“, in: The Annual Review of Political Science 2; S.493–535.

<http://wiki.uni-konstanz.de/wiki/bin/view/Wireless/WirelessLAN>

<http://www.wlan-seite.de/>

<http://wlanfhain.databang.org/>

<http://www.freifunk.net>

<http://www.informationsarchiv.de>

<http://www.wikipedia.com>

<http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/53861&words=Verizon>

<http://www.freifunk.net/>

<http://www.nodedb.com>

<http://www.picopeer.net/PPA-de.html>