Auszug aus dem Buch:

Netzwerkfehler – finden und beheben

Das Profibuch

Mathias Hein, Bernd Maciejewski

Franzis' Verlag GmbH
EAN: 9783772366963 (ISBN: 3-7723-6696-1)
454 Seiten, hardcover, 18 x 25cm, 2003, inkl. CD-ROM

Kapitel 3.6 Fehlersuche in WLANs

von Martin Heine

Nachdem sich zur ortsfesten Anbindung von PCs oder anderer Computer sich die lokalen Netze (LAN), festgeschrieben in der IEEE 802.3 in den vergangenen Jahren sehr bewährt haben, gewinnt der Trend „Wireless“ - die drahtlose Variante IEEE 802.11 oder auch Wireless LAN genann bei der Vernetzung von Computern zunehmend an Popularität.. Damit wird aus dem klassischen Ethernet endlich ein „echtes“ Äther-Netz“ - ist doch der Begriff Ethernet eigentlich schon abgeleitet aus dem Begriff Äther. Erst entstanden mehrere, zum Teil konkurrierende, Verfahren, Übetragung via Infrarot, das Frequency Hopping Spread Spectrum (FHSS) mit 1 und 2 MBit/s und das Direct-Sequence-Spread-Spectrum-Verfahren (DSSS) mit ebenfalls 1 und 2 MBit/s beide Funkübertragungstechniken im lizenzfreien 2,4-GHz-Bereich, das so genannte ISM-Band (Industrial, Scientific, Medical) bis im Jahr 1999 die 802.11 Arbeitsgruppe innerhalb des Institute of Electrical and Electronic Engeneers (IEEE) zum Thema Wireless LANs (WLAN) ihre Arbeit aufnahm. Die WLAN-Gruppe konzentriert sich auf die Themenschwerpunkte der physikalischen Layer (PHY) und den MAC Layer. In der PHY-Gruppe wurden die Definitionen für die physikalische Schicht (z.B. Modulationsarten) von Wireless LANs festgelegt. Die MAC-Gruppe versucht einen Standard für den Media Access Layer festzuschreiben. 1999 traten zwei neue Spezifikationen auf den Plan. Die erste, IEEE 802.11b, war eine Erweiterung des ursprünglichen Standards. Sie basiert auf dem DSSS-Verfahren, verwendet aber ein effizienteres Kodierungsverfahren namens Complimentary Code Keying (CCK). Die Bruttodatenrate betrug 11 MBit/s. Die zweite Norm war der 802.11a Standard, der das 5,2-GHz-Band nutzt und eine Übertragungsgeschwindigkeit von 54 MBit/s vorsieht. Im Gegensatz zu 802.11b arbeitet 802.11a mit mehreren Trägerfrequenzen und der Modulationstechnik Orthogonal Frequency Division Multiplexing (OFDM). Bereits im März 2000 formierte sich innerhalb der Arbeitsgruppe IEEE 802.11 eine Study Group. Sie prüfte, ob es technisch machbar ist, den 802.11b-Standard zu erweitern, um Datenraten von mehr als 20 MBit/s zu erzielen. Im Juli desselben Jahres erhält die

Gruppe offiziell den Status einer Task Group und beginnt mit den Arbeiten an der Norm IEEE 802.11g. Das Ziel: eine Übertragungsrate von 54 MBit/s in WLANs, die im 2,4-GHz-Band arbeiten. Bereits im Mai 2001 liegen vpn Texas Instruments und von Intersil zwei Entwürfe zur 802.11g-Norm vor. Der TI-Vorschlag sieht eine Bandbreite von 22 MBit/s vor und basiert auf dem PBCC-22-Kodierungsschema, der Vorschlag von Intersil mit einer Übertragungsrate von 54 MBit/s basiert auf Grundlage der CCK-OFMD-Kodierung. Im November 2001 wurde der Intersil-Ansatz im Normentwurf als Standardverfahren fixiert, während Texas Instruments' Technik als Option zur Verfügung stehen soll. Die Arbeitsgruppe 802.11h formiert sich, um eine Version des WLAN-Standards IEEE 802.11a zu erarbeiten, die sich mit den Vorgaben des European Telecommunications Standards Institute (ETSI) und dem Hiperlan-2-Projekt verträgt.

In Japan sind drei unterschiedliche Systeme für "Multimedia Mobile Access Communication", MMAC, festgelegt, HiSWAN, eine 802.11a-ähnliches Ethernet und der Wireless Home Link (Firewire) nach IEEE 1394 freigehalten für "Industry, Science, Medical",

WLAN ist von einer eigenen "Wireless Ethernet Compatibility Alliance", WECA, unter IEEE 802.11b definiert und nennt sich Wi-Fi, "Wireless Fidelity", vulgo Wire-Fire. In Europa hat 802.11b insgesamt 13 Kanäle – wobei in einer zellularen flächendeckenden Topologie jeweils nur etwa vier gegenseitig störungsfrei zur Verfügung stehen. In Europa beträgt die höchstzulässige Antennenleistung 100 mW – für alle Kanäle eines Senders zusammen! Die Übertragung wird notfalls adaptiv auf 5,5, 2 oder 1 MBit/s herunter geregelt, wobei im Idealfall mit Richtfunkantennen Entfernungen weniger Kilometer überbrückt werden können.

Bei der Entwicklung, Produktion und Einsatz von WLAN Komponenten, Hotspots oder der Planung komplexer drahtlose Netze ist ein ausgiebiger Test aller Komponenten unerlässlich - ist das Risiko eines Ausfalls und die daraus entstehende wirtschaftlichen Verluste aus Gründen ungenügender Analyse aller Systemfunktionen viel zu hoch. Analyse, Test und Fehlersuche in Bezug auf Wireless LAN umfasst ein großes Spektrum. Angefangen auf der Chip Ebene über Netzwerkkomponenten und Netzwerkhardware, bis hin zur Netzwerkadministration, Hotspot Billing und Zellen Roaming stellen sich viele Fragen; wie effektiv wird zum Beispiel der Einfluss einer Interferenz im 2,4GHz Bereich minimiert? Was für eine Art „hand-off delay" wird erwartet wenn ein User von einer WLAN Zelle in die andere wechselt, oder sogar von WLAN ins UMTS oder GPRS Netz. Wie stark beeinflusst die Implementierung von sicherheitsrelevanten Mechanismen im MAC- und auch in höheren Layern die Netzwerkleistungsfähigkeit? Wie gut kann ein Access Point die Leistung regulieren? All diese Faktoren, ganz zu schweigen von Fragen über end-to-end Performance, Latenz-Zeit und Packet Verlust können durch geeignete Tests und Analysen erst richtig transparent gemacht werden. Da der größte Unterschied zwischen LAN und WLAN im Übertragungsmedium liegt, und auch

dadurch, dass viele Übertragungskanäle gleichzeitig in einem Raum präsent sein können, ist die Arbeitsweise im Layer 1 des OSI Schichtenmodells wohl die Interessanteste.

Fehler- und Performance Analyse in der physikalische Ebene von WLANs

Angefangen auf der Bit-Übertragungsschicht (Schicht 1) der WLANs ergeben sich naturgemäß die größten Unterschiede zur Draht-gebundenen Kommunikation. Bei der Spezifikation des physischen Protokolls sind die Eigenschaften der Übertragung über die Luftschnittstelle zu berücksichtigen. Das gilt besonders für die möglichen Störungen, für die im Wesentlichen drei Ursachen in Frage kommen:

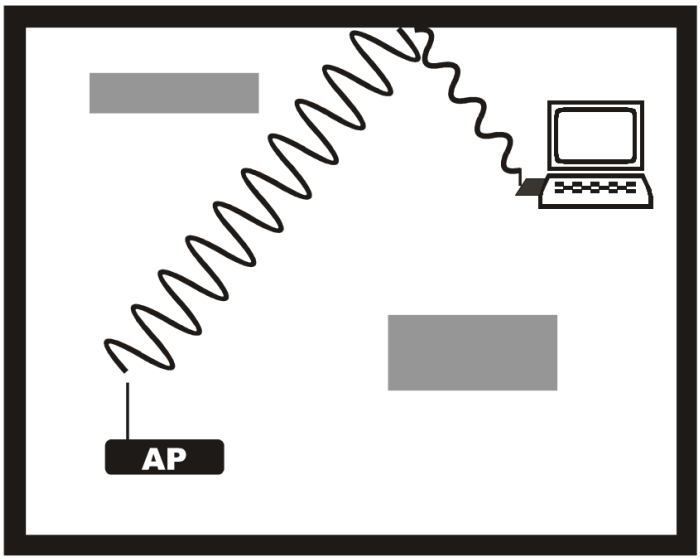
- Rauschen und Interferenzen im Übertragungskanal.
- Signale anderer Stationen, die nach dem 802.11-Standard arbeiten. Selbst wenn deren Signalpegel für einen Datenaustausch nicht mehr ausreicht, können sie unter Umständen die Übertragungsverfahren noch beeinflussen.
- Signale anderer Stationen, die nicht dem 802.11-Standard entsprechen, aber den gleichen Frequenzbereich nutzen. Dazu gehören auch Interferenzen von Mikrowellenherden.

Es macht also Sinn, die Fehler bei mangelnder WLAN Versorgung nicht gleich in den Protokollen zu suchen, sondern - analog zum Kabel-basierenden LAN der Test des Kabels - erstmal zu untersuchen ob eine Funkverbindung überhaupt möglich ist. Stahlbeton-Mauern zum Beispiel sind schon fast ein undurchdringbares Hindernis für 2.4 oder 5 GHz.
Ist eine problemlose WLAN Verbindung mit der verwendeten Hardware in nächster Nähe möglich, jedoch nicht am gewollten, liegt es in aller Regel an den oben genannten Ursachen.

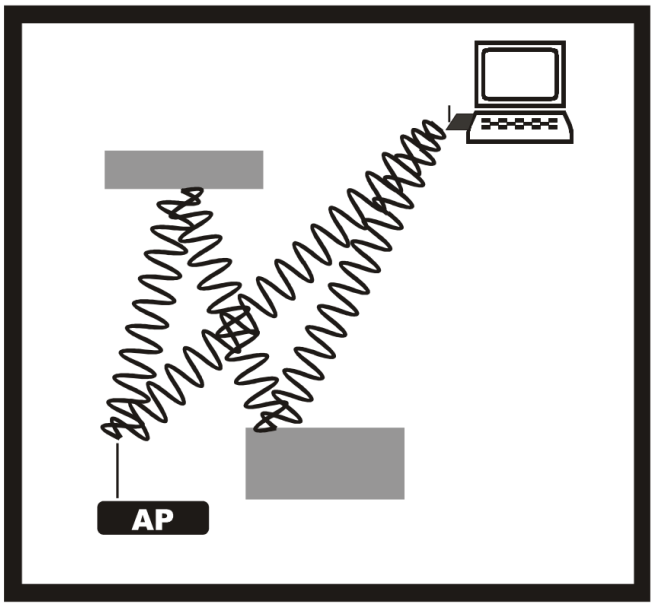
Real Live RF Propagation

IEEE 802.11b bzw. IEEE 802.11a sind zwar mit einer potenziellen Datenübetragungsrate von 11Mbps bzw. 54Mbps angegeben, doch die wirkliche Übertragungsrate ist nicht nur abhängig von der „Empfangsstärke“ wie im Jargon oft bezeichnet, sondern vielmehr abhängig vom Aufbau der physikalische Schnittstelle. HF-Reflektionen, (Multipath Effekte) die Interferenzen erzeugen, Kanalverlust oder Signalverzögerungen erzeugen bereiten die größten Probleme in der WLAN Hardware Entwicklung. Die Simulation bzw. Messung solcher Multipath Probleme - Reflektionen des eigenen Signals von Wänden, Boden oder sonstigen Hindernissen aus Gründen der Signallaufzeit, die im ungünstigsten Fall um 180 Grad phasenverschoben sind und für Signalauslöschung sorgen, ist wesentlich schwieriger als die Messtechnik von Reflektionen in Twisted Pair Kabeln in verdrahteten Netzen. Eine Funkverbindung im 2,4GHz oder 5GHz Bereich, die auf freiem Feld über eine Distanz von mehreren Kilometern problemlos aufgebaut

werden kann, funktioniert im Innenbereich oft nur über wenige Meter. Ausbreitung von Funkwellen verhalten sich in Räumen vollkommen anders als auf freiem Feld. 2,4 GHz wird auch in Mikrowellenherden verwendet, da Wasser in Lebensmittel genau diese Frequenz am besten absorbiert und es sich dadurch erhitzt. Dementsprechend wird also 2,4GHz von WLANs auch schon von umherlaufenden Menschen beeinflusst. Je nach Hindernis wie zum Beispiel Möbelstücke oder Wände dämpfen bis zu 20dB. Auf welchen Weg nun also die Funkwellen in einem Raum wirklich vom Sender zum Empfänger gelangen lässt sich schwer feststellen. Grundsätzlich gibt es zwei Arten von Multipath Effekten:



Verminderte Signalstärke indem es über eine Reflektierende Wand vom Sender zum Empfänger gelangt



- Verminderte Signalstärke durch Interferenz, die Summe mehrerer Signale die sich nach Reflektionen an bestimmten Punkten auslöschen.

Die Spread-Spektrum Technologie von WLAN wirkt diesen Multipath Effekten etwas entgegen. Zusätzlich verwenden viele Hersteller zwei Antennen an ihrem Access Point anstatt nur eine. Damit kann erreicht werden, dass immer eine der beiden Antennen nicht in so einem Auslöschpunkt sitzt und damit die Zellabdeckung wesentlich verbessert werden kann. Die erste WLAN Chip Generation, PRISM I war nur mit einem einfachen IF Design ausgestattet und erst etwas später als der HFA3860 Basisband Prozessor auf dem Markt kam wurde unter der Marktbezeichnung „High Rate“ eine Standard JTC Multipath entgegenwirkende „Delay Spread Performance“ realisiert. Die ersten Chips der zweiten Generation, der PRISM II Chipsatz hatten einen RAKE Receiver, der speziell Multipath Effekte sowie viele andere Interferenz bedingte Störungen durch entsprechende Phasendetektion und Regelungen bekämpfte. Noch mehr Verbesserungen wurden mit dem PRISM II Chip HFA3863 erzielt. Ein sogenannter DFE (Decision Feedback Equalizer) verbessert die Delay Spread Performance um das Doppelte.
Eine weitere Fehlerquelle ist die sogenannte ISI (Intersymbol Interferenz). ISI bedeutet eine Überlappung der einzelnen Datenpulse, verursacht durch Multipath Signalverzögerungen. Die einzelnen Datenbits können vom Empfänger nicht mehr auseinandergehalten werden und es kommt zum Fehler. Auch deshalb ist es zur Vermeidung von ISI Effekten wichtig, Multipath Effekte so gering wie möglich zu halten.
Unter dem Begriff „Hidden Station“-Problem ist eine Problematik beschrieben, die im freien Raum auftritt, bei dem jeder Teilnehmer in einem Funknetzwerk ein nahezu kreisförmiges Feld beschreibt, in dem seine Aussendungen empfangen werden können (außer bei der Verwendung von Richtantennen, aber die sind für *Inhouse*- Anwendungen, um die es hier geht, uninteressant).
Angenommen, zwei mobile Clients, möchten beide Daten an einen Access Point schicken Prinzipiell hört jedes Gerät in einem Funknetzwerk erst nach, ob der Funkkanal frei ist, bevor es seine Aussendung beginnt. Hier können die zwei Clients aber nicht hören und beginnen unter Umständen gleichzeitig damit, ihre Daten an den Access Point zu schicken. Aus Sicht des Access Points kommt es zu einer Datenkolission, die Daten müssen neu gesendet werden. Um diese Problematik zu vermeiden, definiert IEEE 802.11 ein Protokoll, nach dem jeder mobile Client beim Access Point zunächst ankündigen muß, daß er Daten senden möchte. Bekommt er die Bestätigung für seine Anfrage, darf er die Aussendung beginnen. Anschließend schickt der Access Point eine weitere Bestätigung, um dem mobilen Client mitzuteilen, daß die Daten fehlerfrei empfangen werden konnten. Das Protokoll wird *RTS-CTS-Protokoll* genannt, wobei *RTS* für *Ready To Send* und *CTS* für *Clear To Send* steht.

WLAN Richtfunkstrecken

Oft sollen zwei nahegelegene Bürogebäude Netzwerktechnisch miteinander verbunden werden. Ist die Entfernung nicht größer als zwei bis drei Kilometer kann durch Einsatz von Richtfunkantennen eine WLAN Richtfunkverbindung eingerichtet werden. Entgegengesetzt zu Kurzwellenfunkverbindungen sind bei Wellenlängen im WLAN-Bereich nur Verbindungen mit direkter Sicht möglich. Das heißt bei Strecken von mehr als 100 Metern reicht ein einziger Baum aus, um eine Funkverbindung zu unterbrechen.

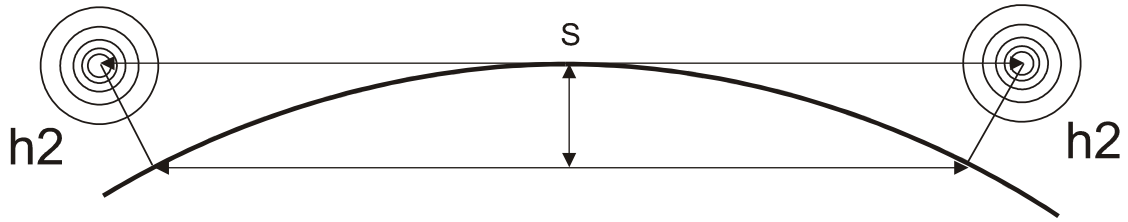


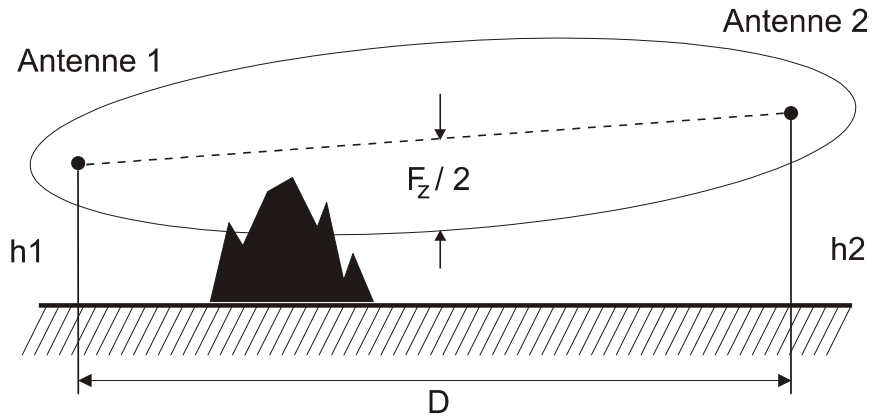
Abbildung Sichtbehinderung durch Erdkrümmung

Schon die Erdkrümmung sorgt bei einigen Kilometern Entfernung dafür, dass eine Sicht zwischen zwei Antennen nicht mehr vorhanden ist. Darum gilt stets, je höher die Antennen, desto besser. Nach einer Faustformel ist die Überhöhung auf der Mitte der Strecke.

$$ht = \frac{d^2}{68}$$

Höhe in m, d in km.

Gelegentlich kann es jedoch vorkommen, dass trotz direkter Sichtverbindung eine Funkverbindung nicht möglich ist.



$$\frac{F_z}{2} = 0.5\sqrt{\lambda\ D}$$

Abbildung: Fresnel Bereich einer WLAN Richtfunkstrecke

Für eine ungestörte Übertragung muss nicht nur direkte Sichtverbindung herrschen, sondern ein ganz bestimmter Raum zwischen Sender und Empfänger frei von Hindernissen aller Art sein. Dieser Raum wird nach dem französischen Ingenieur Augustine Jean Fresnel die Fresnel'sche Zone benannt. Ist dies nicht gegeben, können sich Interferenzen zwischen den direkten Wellen und den, von einem Hindernis reflektierten, Wellen ergeben. Hersteller von Richtfunk Hardware geben hierbei einen Grenzwert an, bei dem sie eine Verbindung sicherstellen. Mit Hilfe der Fresnel-Zonen läßt sich der Einfluss von Hindernissen im Ausbreitungsweg quantitativ angeben. Sollen z.B. mindestens 60% der Fresnelzone frei bleiben, und eine Bridge-Verbindung von 2km Entfernung aufgebaut werden, muss sichergestellt sein, dass in der Mitte der Verbindung, also nach 1km mindestens 6m zum nächsten Hindernis frei bleiben muss. Gegebenenfalls muss der Antennenmast umplatziert oder erhöht werden. Ein weiterer Störfaktor bei der Übertragung von Funkwellen können Gebäude oder Berge sein, die sich hinter den Antennen befinden; diese können als Reflexionsherd Unterbrechungen verursachen. Durch Laufzeitunterschiede zwischen dem direkten und dem, über den Reflexionspunkt erzeugten Funkstrahl ergeben sich Phasenverschiebungen, die eine Auslöschung zur Folge haben können.

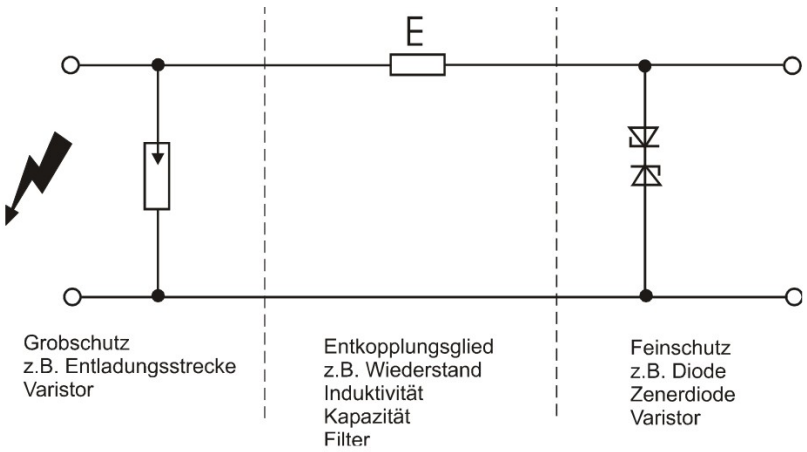
Blitzschutz von Richtfunk Antennensystemen

Die Häufigste Ursache für Ausfälle von WLAN Richtfunkverbindungen sind Statische Ladungen in der Atmosphäre und Gewitter Blitzentladungen. Für den Schutz von Antennen auf dem Dach oder auf Masten gegen Blitzentladungen und statische atmosphärische Entladungen gibt es eine einschlägige Normenreihe und wird unter VDE 0185 [1] bis [3] behandelt. Das Antennensystem (so die Definition dieser Normenreihe) muss einem Blitz-Stoßstrom von100kA (Stirnzeit T1 = 10 ms, Rücken Halbwertzeit T2 = 350 ms) entsprechend der Schutzklasse III, diein der Normenreihe VDE 0185 [4] bzw. [5] definiert ist, standhalten. Das Antennen-System muss in den Potenzialausgleich des Gebäudes einbezogen werden.

Überspannungsschutz

Zur Vermeidung einer Beschädigung der APs, Rechner und Netzwerke durch Blitzschlag oder statische Entladungen können Überspannungs-Schutz Komponenten eingesetzt werden. Die Einkopplung von Überspannungen kann galvanisch, induktiv oder kapazitiv erfolgen. Diese Einkopplungen können duch geeignete Sperren abgeblockt - oder abgeleitet werden. Diese beiden Methoden werden oft kombiniert.

Abbildung:



Überspannungsschutzmassnahmen

Zum Einsatz kommen hierbei Bauelemente wie Trennfunkstrecken, Überspannungsableiter und Varistoren als Feinschutz.

Trennfunkstrecken sind gekapselte Luftfunkenstrecken. Ist eine Überspannung am Eingang (z.B. Blitzschlag in die Antenne) stellen sie bei Überschreitung einer bestimmten „Zündspannung“ einen Kurzschluss dar. Das Zünd- und Löschverhalten dieser Bauelemente wird massgeblich bestimmt durch Elektrodenform und Abstand der Elektroden. Überspannungsableiter sind mit einem Edelgas (Argon oder Neon) gefüllte Keramik oder Glasröhrchen mit zwei Elektroden. Bei Überspannung ergibt sich ein ionisierter Kanal der die Überspannung ableitet. Ein Varistor ist ein Spannungsabhängiger Widerstand mit einer stark ausgeprägten Spannungs/Strom Kennlinie. Bei Überschreitung der Knickspannung (Die Spannung, bei der die Stromkennlinie rapide ansteigt) bricht der Widerstand in kurzer Zeit vom Megaohm bereich auf kleiner 1 Ohm zusammen. Varistoren werden auch häufig zum Schutz vieler Geräte parallel zum Netzspannungseingang eingebaut.

Speziell zum Schutz von WLAN Accesspoints gibt es eine ganze Reihe von Herstellern, die diese Blitzschutzkomponenten speziell für WLAN Frequenzbereiche anbieten.

Abbildung: Blitz- und Überspannungsschutz (Quelle: Lancom)

Mess- Technik und Geräte

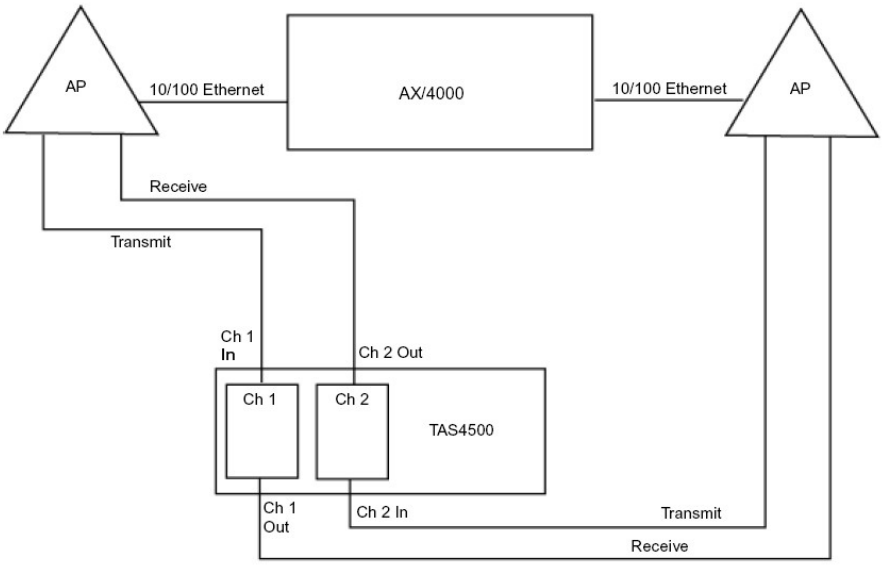
Störungen durch ISI-, Multipath, Rayleigh- und Rician Fading (wie nachfolgend näher beschrieben) wirken sich in meistens durch Paket Verluste aus. Fehlende Bits werden detektiert und das entsprechende Packet dann nicht akzeptiert. Fehlen mehrere Pakete kann die Datenverbindung komplett unterbrochen werden. Die Suche nach der Ursache ist oft wie die Suche nach der Stecknadel im Heuhaufen. Liegt es an einem Multipath-, Fressnell oder ISI Effekt? Unterschiedliche Messgeräte speziell für die Analyse und Fehlersuche auf der physikalischen Ebene aber auch zur Analyse von Packet Loss und Protokollen von Wireless LANs werden mittlerweile von einigen Herstellern angeboten.
Die Firma Spirent Communications bietet für die Messung von Hardwarekomponennten wie Access Points (APs) und Network Interface Clients (NICs) auf dem Layer 1 für 802.11b einen Hochfrequenz Channel Emulator an, mit der Bezeichnung FLEX4500. Der Emulator arbeitet im Frequenzbereich 25 bis 3000 MHz und ist mit der FLEX5 6 GHz Option auch für 802.11a anwendbar. Er ist als Zweikanal Emulator 12-Path aufgebaut und unterstützt beide Kanalmodi wie JTC‘94 sowie Exponentially Decaing (Naftali). Auch frei definierbare Kanalmodelle werden durch einer sehr leistungsfähigen Technologie genannt DEE (Dynamic Environment Emulation) unterstützt.

Rayleigh- und Rician Fading

Der englische Physiker Lord Rayleigh konnte 1871 nachweisen, daß das Sonnenlicht an den Luftmolekülen in alle Richtungen gestreut wird. Weiterhin zeigte er, daß die kurzwelligen Lichtstrahlen (also Violett und Blau mit Wellenlängen L=0,38 bis 0,45 µm) an diesen kleinen Partikeln stärker gestreut werden als das langwellige Licht (Orange und Rot, L=0,65 bis 0,75 µm). Von Ihm stammt auch der Begriff Rayleigh Fading oder Rayleighdichte ab, der sich bei Multipath Effekten in drahtlosen, höherfrequenten Übertragungstechniken, bei denen kein einzelner Pfad dominiert, etabliert hat. Gibt es zwischen Sender und Empfänger eine direkte Sichtverbindung (LOS - Line Of Sight) so dominiert energiemäßig der direkte Pfad und damit sind nicht mehr alle Annahmen für das Rayleighmodell erfüllt. Allerdings lässt sich das Rayleighmodell um den direkten Pfad erweitern und man erhält die so genannte Ricedichte.

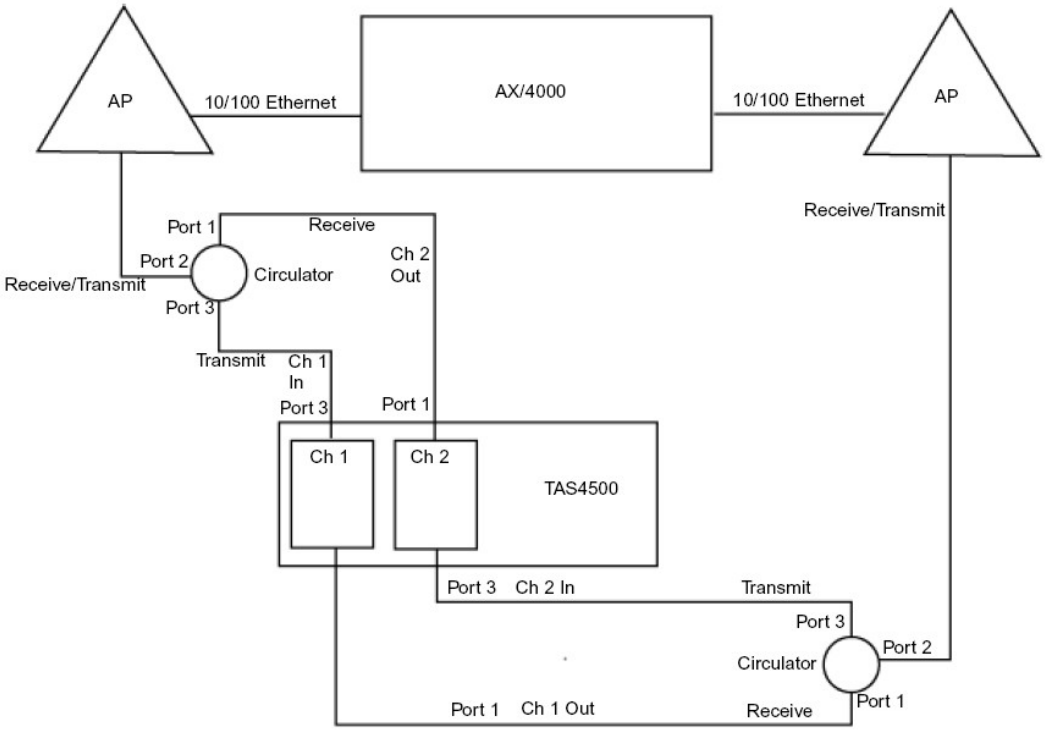
Simulation von Rayleigh Fading zur Messung des Verhaltens von WLAN APs und NICs

Ein typischer Versuchsaufbau zum Test von APs bzw. NICs auf OSI Ebene 1 wie sie sich bei Rayleight Fading Multipath Effekten verhalten, ist nachfolgend dargestellt:



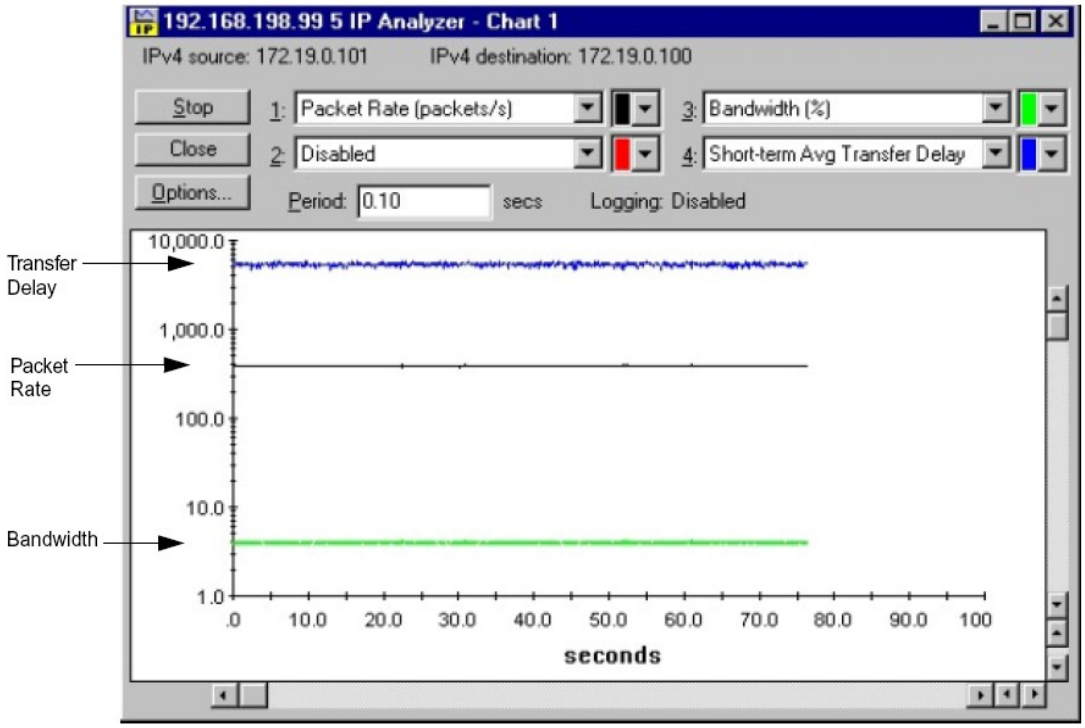
Versuchsaufbau zum Test von WLAN Layer 1

Hierbei wird ein Spirent Communications Adtech AX/4000 Broadband Emulator benutzt, um die notwendigen Traffic zu erzeugen, sowie das Ergebnis des Versuchs zu analysieren. Die Antennenausgänge der APs werden ohne Antennen mit Koaxleitungen direkt mit den Emulator verbunden. Der oben gezeigte Aufbau eignet sich allerdings nur für APs mit zwei Antennen, eine für Empfang und die andere zum Senden. Viele APs allerdings nur mit einer Antenne arbeiten, müssen noch zusätzlich noch Circulatoren eingebaut werden, die die Sende- und Empfangssignale mischen.



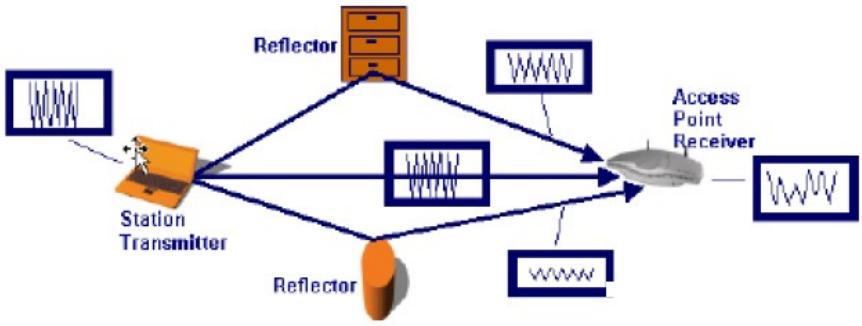
Versuchsaufbau zum Test von WLAN Layer 1 für Single Antennen APs

Als erstes wird untersucht wie sich die APs verhalten ohne dass irgendwelche Störungen simuliert werden. Wird z.B. der AX/400 auf 4Mbps Traffic eingestellt zeugt sich folgendes Messergebnis:



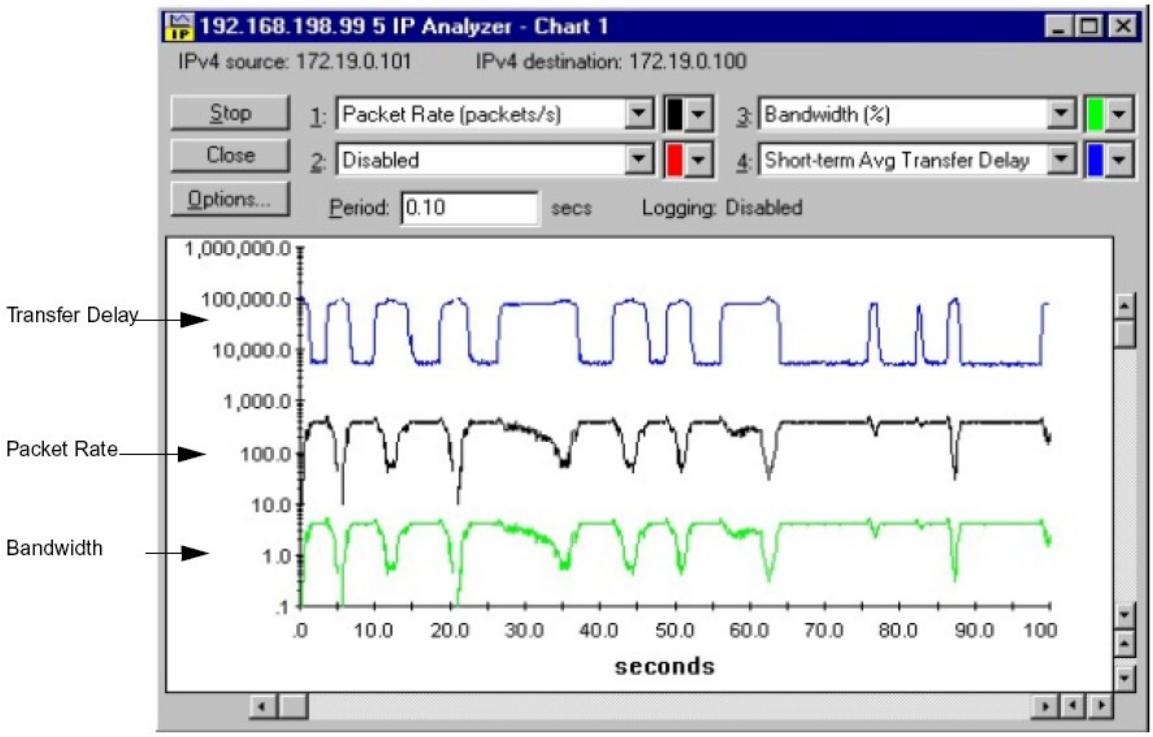
Screenshot AX/4000 AP-Test Layer 1 ohne Störeinflüsse

Zur Untersuchung des Einflusses von Störgrössen auf die Leistungsfähigkeit der APs werden nun Gegebenheiten wie sie in einem Büro vorkommen simuliert.



Situation in einem Raum

Der AX/4000 verfügt über die verschiedensten Einflussgrößen Simulationen. Bei dieser Simulation wird die Funktion „Rayleigh“ verwendet. Durch verschiedene Einstellungen an Fading Velocity und der Auswahl eines „Power Spektrum Shapes“ und einer „Distribution“ von typischen 6 dB ergibt sich ein erstaunliches Ergebnis wie in der Praxis die tatsächliche Leistungsfähigkeit eines WLANs aussehen kann:



Screenshot AX/4000 AP-Test Layer 1 mit Impairment Störeinflüsse

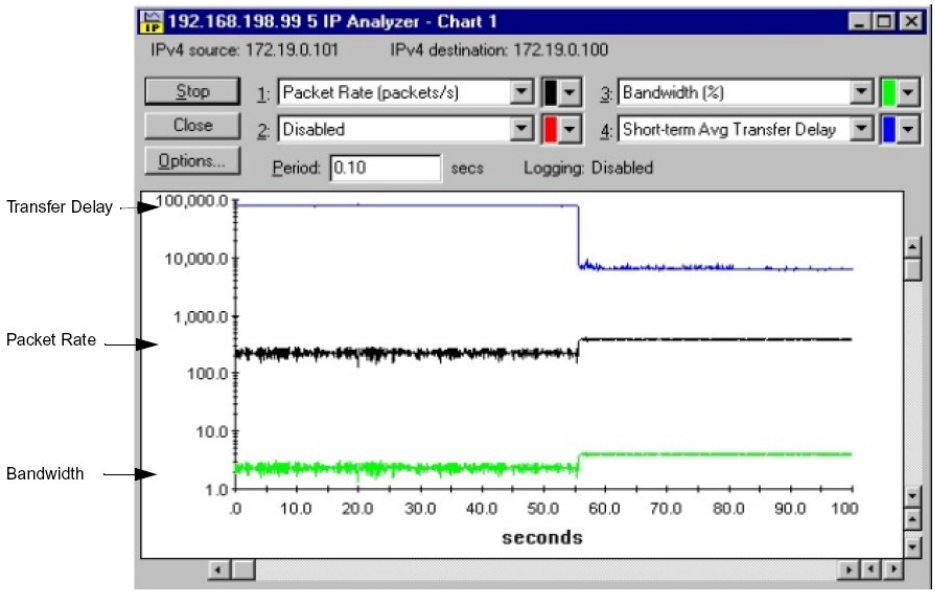
Es zeigt sich deutlich eine Relation zwischen Packet Rate und Transfer Delay. Wenn die Packet Rate sinkt wird das Transfer Delay größer. Der Grund hierfür ist, dass der Sender jedes nicht korrekt empfangene Datenpaket erneut versendet. Da nun wesentlich mehr übertragen wird, also die Pakete mehrmals verschickt, benötigt der AP mehr Zeit und die Latenzzeit erhöht sich folglich. Paketrate und Bandbreite sind dabei in unmittelbarer Relation zueinander.

Rician Fading

Rician Fading tritt auf, wenn ein starkes Signal das auf direktem Wege vom Sender zum Empfänger gelangt mit nahezu gleicher Signalverzögerung am Empfänger eintrifft wie die von nahe gelegenen Hindernissen reflektierten Multipath Signale. Durch zwei zusätzlich einstellbare Variablen am AX/4000, dem Winkel des eintreffenden LOS Signals (LOS = Line Of Sight, das direkt ankommende Signal) und einem Faktor K, der die Relation zwischen der LOS Signalstärke und der Summe aller Reflektierten Signalen angibt.

Delay Spread

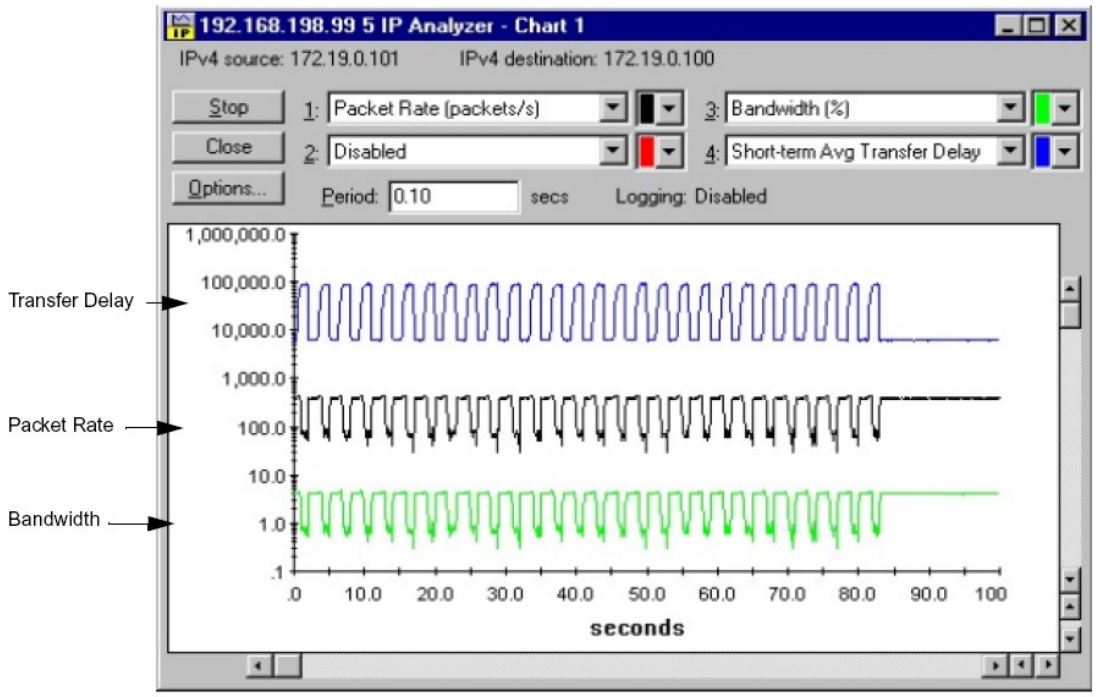
Unter Delay Spread versteht man wenn es durch das zeit-unterschiedliche Eintreffen von gleichen „SYMBOLS“, (Datenpulse), über verschiedene Wege zur Inter-Symbol Interferenz (ISI) kommt. Das Mess-System verfügt über eine Funktion, mit der solche Erscheinungen simuliert werden - und die Reaktion von AP und NIC gemessen werden kann.



Im Gegensatz zu Fading Erscheinungen entsteht durch Delay Spread ein eher gleichbleibender, linearer Einfluss. Die Latenzzeiten werden etwas höher, wobei aber Paketrate und Bandbreite sich kaum verändern.

Phase Shift

Da zur Übertragung der einzelnen Bits bei WLAN mit unterschiedlichen Kodierungsverfahren immer die Phase moduliert ist, reagieren APs und NICs empfindlich gegen relative Phasenfehler, die in ungünstigen Fällen ebenfalls durch Multipath Effekte vorkommen können. Die Reaktion von WLAN Komponenten auf solcher Phasen-verschiebe-Fehler, bzw. wie gut ein Sender oer Empfänger diese Fehler ausgleichen kann, kann ebenfalls mit gleichem Messaufbau untersucht werden, indem die relative Phase in 0.1 Schritten von Null bis 360 Grad „duchgedreht“ wird.

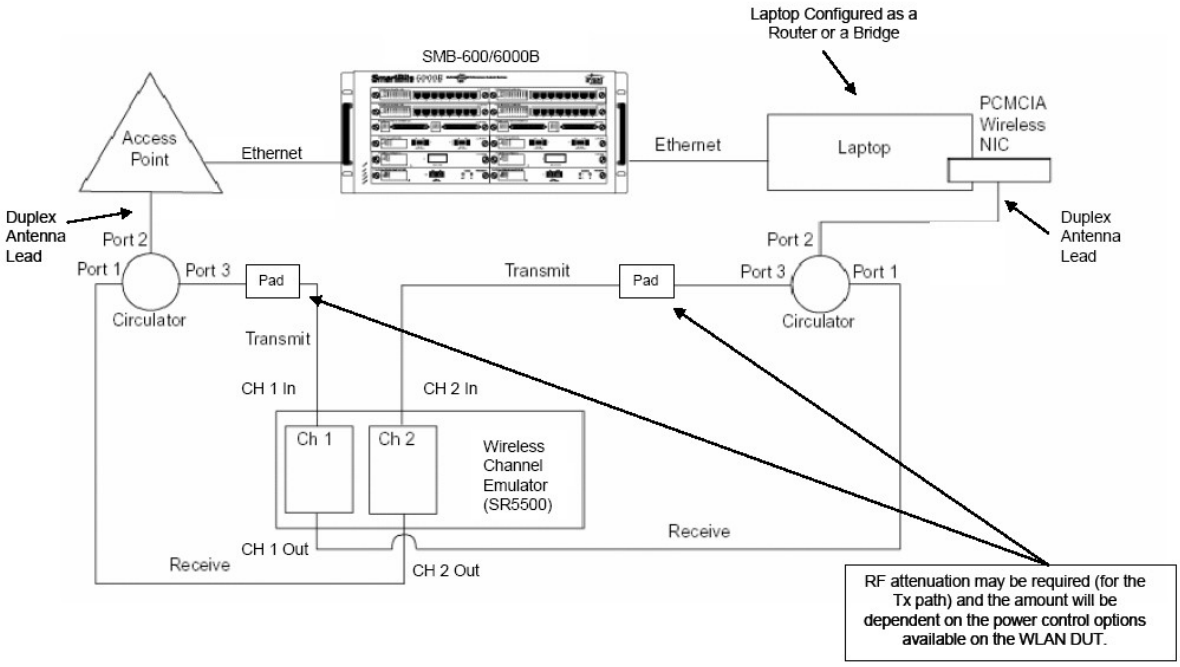


Reaktion von APs auf relative Phasenverschiebung

Ähnlich wie bei Impairment Störeinflüsse oszilliert Transfer Delay, Packet Rate und Bandwith. Die Phasenverschiebung erzeugt Symbol Fehler. Da der Empfänger selber nicht registriert, ob ein Datenpaket korrekt oder falsch ist, wird bei Erkennung von Fehlern auf höheren Layern immer das ganze Packet neu gesendet. Daher erhöht sich die Latenzzeit und entsprechend die Packetrate.

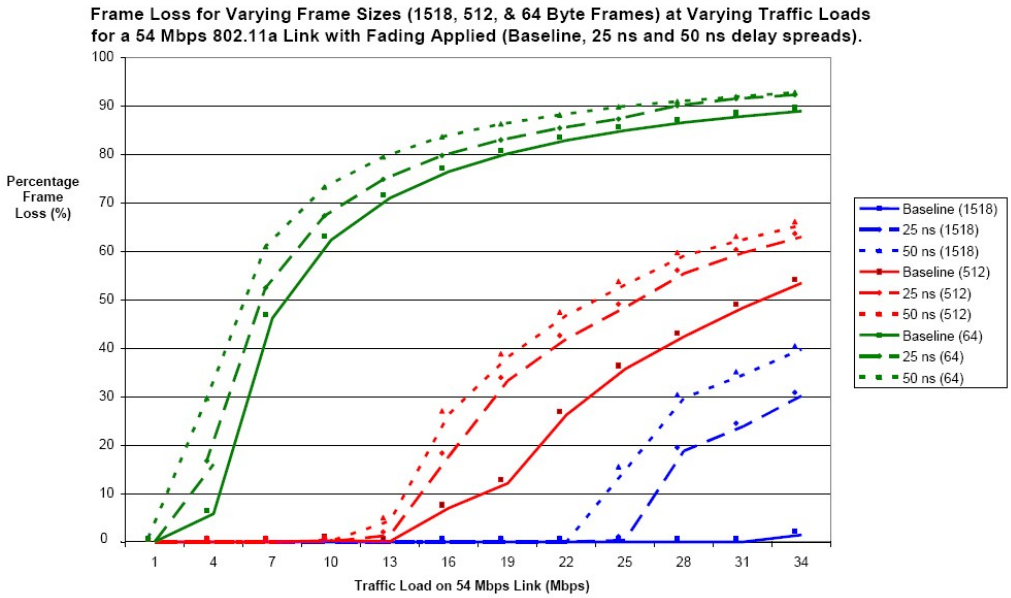
Zusammenhänge zwischen Framegrösse, Frameloss, Traffic und Delay Spread, sind ein typisches alltägliches Szenario in WLANs. Unter Verwendung des SR5500 Wireless Channel

Emulators von Spirent und SMB600/600B Ethernet Generator / Analyzer kann mit folgendem Messaufbau eine sehr gute Veranschaulichung dieser Zusammenhänge gezeigt werden.



Aufbau zur Messung von Framelost in Abhängigkeit von Framegröße, Traffic und Delay Spread

Wie im ersten Aufbau werden Circulatoren für den AP und NIC verwendet, da Sende- und Empfang über die gleiche Antennenbuchse gehen. Ein Laptop betreibt die NIC und arbeitet als Router bzw. Bridge. Die Frame-Loss Tests werden mit drei verschiedenen Frame Größen (1518, 512, and 64 Bytes) unter drei unterschiedlichen Umgebungs Szenarios, die sich jeweils in unterschiedlichen Delay Spread Zeiten unterscheiden (baseline, a 25 ns rms delay spread, und 50 ns rms delay spread). Zusätzlich wird noch die Rraffic Load Rate des 54 Mbps Links in 3 Mbps Schritten von 1 Mbps bis34 Mbps erhöht. Das Resultat:



Wie zu erwarten erhöht sich der Frame Verlust wenn der Datenverkehr zunimmt. Auch bei kleineren Frame Grössen ist der Datenverlust größer bei ansteigendem Traffic. Wie ebenfalls fast vorherzusehen steigt die Fehlerrate auch bei größeren Delay Spreads.

Ausser Spirent haben natürlich auch andere Hersteller Messgeräte auf dem Markt, mit denen sich Fehlern in WLANs aufspüren lassen. Oft handelt es sich dabei um schon seit geraumer Zeit im Markt etablierte Geräte aus der Hochfrequenz Ecke, meist spezialisiert auf Layer 1, Netzwerkanalyse (Analyse von sicherheitsrelevanten Protokollebenen) und Mobilfunk Branche, die mit Optionen, Zusätzen oder Umbauten nun zu WLAN Messegräten mutieren. Viele dieser Anylizer sind hauptsächlich als Software Applikationen auf einem PDAs realisiert, die zusammen mit bestimmten WLAN Compact Flash Karten sehr portable Lösungen zur Fehlersuche vor Ort sind. Um einen kleinen Überblick über das Angebot auf dem Markt zu bekommen sind nachfolgend einige dieser Geräte vorgestellt.

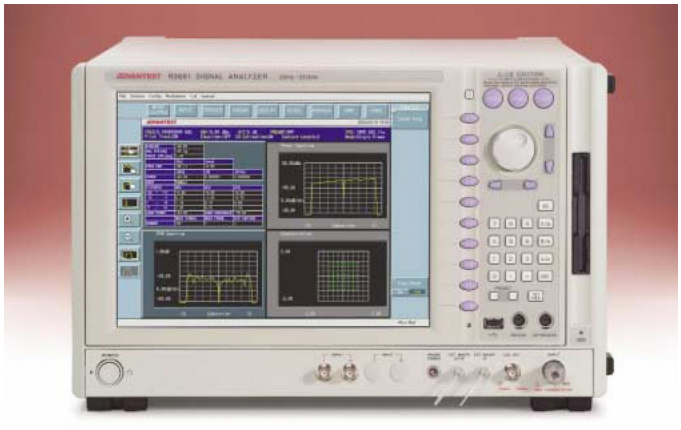
Die Simulation von Funkübertragungsstrecken basiert, wie beispielsweise bei dem Prop Sim C2 oder Prop Sim C8 der Firma Elektrobit, auf einer ausgeklügelten FIR-Filterarchitektur (Finite Impulse Response) mit zeitlich schnell veränderlichen Koeffizienten. Dies erlaubt eine realistische Nachbildung von schnell variierendem Mehrwegempfang, wie er in der Praxis häufig auftritt. Neben verschiedenen Modellen für die unterschiedlichsten Funkübertragungsstrecken – beispielsweise gebäudeintern,städtisch, ländlich – lassensich in solchen Geräten im Idealfall auch Daten von zuvor ausgemessenen Übertragungsstrecken beliebig oft reproduzieren.

Der Funkkanalsimulator Prop Sim C2 von Elektrobit arbeitet mit vorgefertigten und selbst definierten Kanalmodellen oder verarbeitet die mit dem Prop Sound vor Ort gemessenen Daten für die Simulation

Mit einer Softwareoption komplettiert Agilent seine Analyse-Tools für Tests an Wireless-LAN-Komponenten für den Vektor-Signalanalysator VSA 89600 ist, so der Hersteller, ist die Analyse komplexer Signale bei allen vorhandenen und vorgeschlagenen WLAN-Standards – 802.11a,802.11b und 802.11g – möglich. Die 802.11g-Software beherrscht, wie die beiden bekannten Tools, unter anderem die Demodulation von WLAN-Bursts, die automatische Bestimmung aller im Signal vorhandenen Modulations-Formate sowie die Fähigkeit, die Modulations-Qualität zu überprüfen. An für den 802.11g-Standard spezifischen Merkmalen, nennt Agilent das automatische Erkennen, Demodulieren und Despreading der vier 802.11b-Signalformate (1, 2, 5,5 und 11 MHz) sowie das Erkennen und Decodieren der optionalen 802.11b- und 802.11g-PBCC-Formate. Die Software erkennt außerdem das optionale CCKOFDM-Format und ermöglicht ein automatisches Demodulieren, Despreading und Descrambling der Präambel, um die voraussichtliche Burst-Länge und den Modulationstyp bestimmen zu können. Darüber hinaus gibt es auch für den Vektor-Signalgenerator E4438C ESG eine Software, das 802.11g-WLAN-Studio. Sie erlaubt das Erzeugen von Testsignalen für die Prüfung von 802.11g-Bauteilen sowie -Empfängern. Auch diese Software ergänzt die vorhandenen Tools für die Standards 802.11a und 802.11b. (MK)

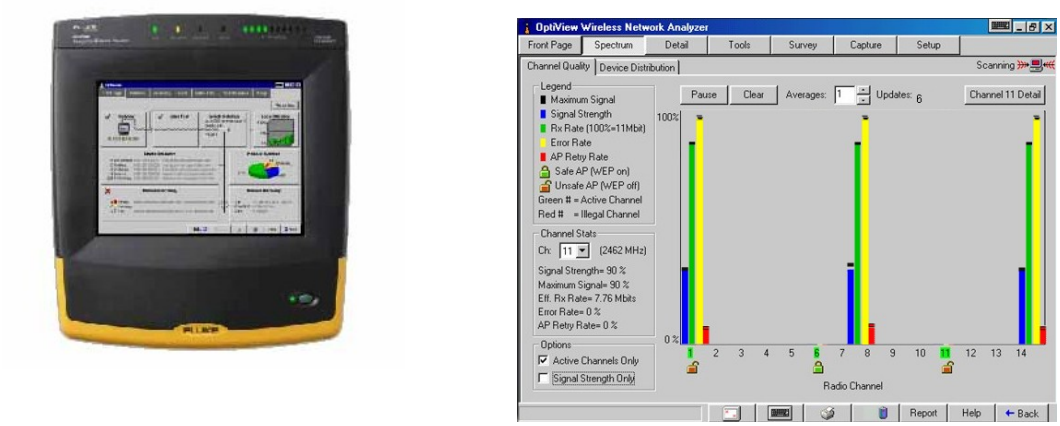
Der ADVANTEST R3681 ist ein Kombigerät aus Spektrum Analyzer, Signalgenerator, und Arbitrary Waveform Generator. Mit der OFDM (Orthogonal Frequency Division Multiplexing) Modulationsanalyse Option für 802.11, HiperLAN/2 und HisWAN können mit diesem Gerät WLAN Tests im Bereich RF Input, I/Q Baseband Input und alle weiteren WLAN spezifischen Signale und Modulationen, sehr genau gemessen und untersucht werden. Mit einer mittleren Display Noise Level von -158dBm, Third Order Intermodulation Distortion von 26dBm und Signal Purity von 122 dBc/Hz (@ 800MHz und 10kHz Offset) gehört der R2681 zu den wohl

genauesten, aber auch teuersten Instrumenten zur Fehleranalyse in der Layer 1 Ebene und findet seinen Platz wohl am ehesten bei der Chip Entwicklung der nächsten Generationen.



ADVANTEST R3681

Mit Optivew Wireless, als Erweiterung des bestehenden „OptiView Integrated Network Analyzer“ offeriert Fluke ein sehr leistungsfähiges Gerät zur WLAN Fehlersuche. Für den Einstieg in die Analyse findet OptiView einmal die pro Kanal gefundenen Access-Points (»Access-Point-View«), oder der Administrator informiert sich für alle Funkkanäle über die WLAN-Parameter wie genutzte Bandbreite oder Anzahl der Geräte (»Spectrum-View«). Die »Wireless-Site-Survey-View« speichert ein Gesamtbild über das WLAN ab. Dazu gehören auch die Performance-Metriken der Access-Points. Über die View erkennt der Administrator Veränderungen bei der Bandbreite, Signalstärke oder den Fehlerraten bei späteren Messungen. Zudem kann er Wireless-Geräte als bekannt kennzeichnen. So fallen unwünschte Access-Points bei späteren Messungen sofort auf.
In der »Conservation-View« zeigt der Analyzer die Kommunikation zwischen einem Access-Point und WLAN-Client an. Dies hilft spezielle Verbindungsprobleme zwischen den Beiden zu analysieren. Mit Hilfe der Access-Point-View sieht der Administrator alle Parameter bezüglich eines Access-Points wie Konfigurations- und Sicherheitseinstellungen, Durchsatz oder Anzahl der Clients. Zusätzlich hilft diese Ansicht bei der Lokalisierung unerwünschter Access-Points. Die Spectrum-View dient zur Überprüfung von Konfigurationen oder der gleichmäßigen Auslastung der Funkkanäle. Weiter bringt der Analyzer ein Tool für die Erfassung und Decodierung der WLAN-Pakete mit. Mittels FTP-Transfer ermittelt das Gerät den tatsächlichen Durchsatz. Ein MIB-Browser (Management-Information-Base) zeigt die MIBs der Access-Points an.



Optivew mit Wireless Option.

Zusätzlich zur Wireless-Option für OptiView hat Fluke Networks mit dem WaveRunner einen handlichen unter Linux laufenden PDA vorgestellt. Mit Farbdisplay und Pen-Bedienung ermöglicht er dem Benutzer den unkomplizierten Zugang zu einer Reihe von Test-Hilfsmitteln – von der Feststellung drahtloser Zugangspunkte und Clients über das Scannen von Funk-Kanälen und der Auswertung der Funksignalstärke bis hin zu Analyse des drahtlosen Datenverkehrs. Daneben bietet WaveRunner eine Vielzahl client-basierter Tools zur Fehlersuche (z.B. Link, Ping und Durchsatz). Mit dieser Lösung stehen die Troubleshooting-Funktionen von OneTouch, NetTool und LinkRunner als Fehlersuch-Werkzeuge im Netzwerkbereich nunmehr auch für Funk-Netzwerke zur Verfügung. Dazu Michael Simon: “Wireless-LANs erfordern vom IT-Manager eine flexible Vorgehensweise, denn er muss die elektromagnetischen Wellen in der Umgebung seines Firmen-Netzwerks fortlaufend überwachen. Hieraus resultiert der Bedarf an Geräten, die den Benutzer nicht mehr zwingen, vom Schreibtisch aus Werte auf der Bedienoberfläche einer Software zu überprüfen. Mit WaveRunner kann der Anwender die Fehlersuche buchstäblich in die Hand nehmen und muss nicht mehr einen Laptop zwischen Konferenzräumen und Kabelschränken hin und her schleppen.”

Fluke Waverunner

Waverunner z.B. kann folgende Informationen
bieten:

- Wo befindet sich der AP?
- Wer greift auf den AP zu?
- Wo sind die Aps zu positionieren?
- Wie sind die Kanäle zuzuweisen?
- Können die Clients zu den APs Verbindung aufnehmen?
- Ist eine ausreichende Abdeckung gewährleistet?
- Erkennen die Clients den AP?
- Wurde WEP ordnungsgemäß implementiert?
- Erkennt der Client Key-Geräte (Server, Router....)?
- Funktioniert die WLAN-Karte überhaupt?

Acternas AirMagnet bietet mit der Analysesoftware für Handhelds oder Laptops die mobilen Lösungen für 802.1x WLANs zum installieren, administrieren oder sichern.

Airmagnet von Acterna

Die Kernfähigkeiten des Airmagnet umfassen Standorterhebung, Verbindungstroubleshooting sowie Sicherheits- und Performance-Management. Airmagnet unterstützt ferner PC-Cards von Symbol Technologies und Proxim sowie eine Compactflash-Karte von Proxim Airmagnet scannt passiv alle 14 Kanäle im 2,4-GHz-Band, analysiert den Verkehr und wendet sein Airwise-Experten-Analysesystem an, das Alarme und Alerts für 31 Sicherheitsbedingungen, 24 Performance-Bedingungen und 13 sonstige Diagnosepunkte beinhaltet. Das System entdeckt ungeschützte APs, Kanalrauschen (z.B. durch Mikrowellenherde oder schnurlose Telefone verursacht), mehrfache APs auf demselben Kanal, Ad-hoc-Verkehr und bietet detaillierte Echtzeitmessungen von Funksignalen. Einfache Verbindungsprobleme (nicht übereinstimmende SSIDs) lassen sich mit Airmagnet ebenso diagnostizieren wie komplexe Cisco-802.1x/LEAP-Authentifizierungsprobleme Werkzeuge für eine rudimentäre Paketanalyse mit Filterfähigkeiten sind ebenfalls vorhanden. Auch eine Reihe nützlicher Werkzeuge für die Durchführung von Standorterhebungen, Durchsatzmessungen, Ping- und Trace-Route-Tests sind integriert. Die kraftvollste Komponente von Airmagnet ist dessen Airwise-Experten-Engine, die Sicherheits- und Performanceanalysen bietet. Die Sicherheitsalarme sind umfassend — der letzten Version wurden 15 Alarme hinzugefügt, darunter welche für die Verknüpfung und Authentifikation, für Denial-of-Service-, RF-Jamming- und Dictionary-Attacken und EAP-Rekeying-Probleme. Zu den Basisalarmen gehören Alarme, die nicht autorisierte und falsch konfigurierte APs sowie APs

mit ausgeschaltetem WEP entdecken sowie Alarme für Sicherheitsanalysen bei Problemen mit der 802.1x-Authentifizierung oder L2TP-, PPTP-, SSH- und IPSec-VPN-Tunneln. Die Performanceanalysen von Airwise generieren Alerts oder Alarme, wenn sie hohe Fehler- oder Wiederholungsraten, verfehlte Beacons, exzessiven Multicast- und Broadcastverkehrs, Kanäle mit hohem Noiselevel und überladene APs entdecken. Hier einige Funktionen im Überblick:

- Wireless RF-Status: Erfassen und dokumentieren von Überlast, Bandbreite, Broadcasting
- Aktives und passives Erfassen von SSIDs, identifizieren und loggen von Access Points (APs) und Stationen
- Nutzen von Expertenwissen im Messtool für Fehlererkennung und -behebung
- AirWise Validieren von 802.1x/LEAP/TKIP/MIC
- Überwachen und automatische Alarmierung bei 30 Performance- und Sicherheitsparametern
- Aufzeichnen und Dekodieren von Protokollen mit der Option der Speicherung im Sniffer-Format zur detaillierten Offline-Analyse, z.B. mit LinkView von Acterna
- Aufspüren von Sicherheitslücken, z.B. WEP disabled, Encryption-Schwächen oder “Flooding of association tables”
- Aktives Performance-Management

Nicht nur zum Auffinden von Hotspots sondern vorallem auch auch für die Layer 1 HF Fehleranalyse von WLAN Komponenten wie unter anderem auch die Erkennung und Analyse von Multipath Effekten wurde von Berkeley Varitronics Systems (BVS) ein Gerät namens Yellowjacket entwickelt. Für Administratoren, die kalibrierte Spektrumanalysen benötigen, ist Yellowjacket die erste Wahl. Das Produkt besteht aus einem Compaq-iPaq und einem Stück Hardware, das auf den PDA geschoben wird.

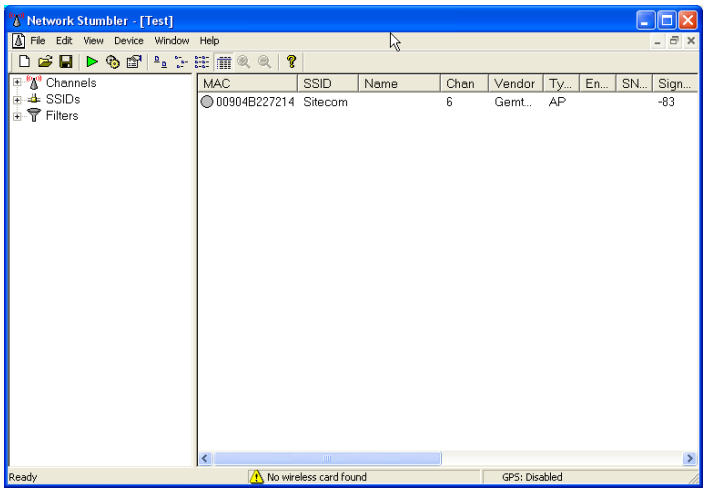
Berkeley Varitronics Systems (BVS) Yellowjacket

Einige Merkmale von BVS Yellowjacket:

- 5 GHz coverage for (OFDM) alle network channels im IEEE 802.11a standard
- Spectrum Analyzer sweep mit PEAK SEARCH und 3 speziellen wavform signal traces
- Receive, Filter und complex DSSS studies processing, alles in Pocket PC® Umgebung.
- RSSI; narrow band & total channel power.

WarDriving

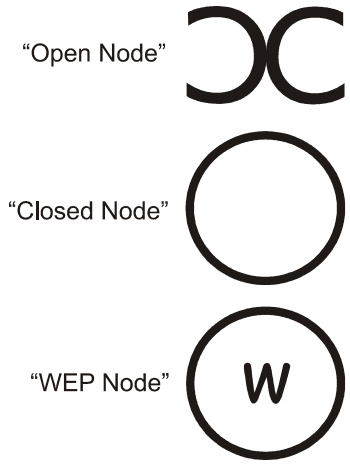
Eine ganz andere Art der „Fehlersuche in WLANs“ ist die Suche nach den Fehlern von Netzwerkadministratoren, vorallem denen in interessanten Firmen oder Hotspots, die den Fehler machen, ihre WLAN Netzwerke nicht genug gegen Eindringlinge abzusichern. Damit gemeint ist WarDriving, eine seit geraumer Zeit etwas zweifelhafte neue Freizeitbeschäftigung immer größerer Beliebtheit. „War“ steht für „Wireless Access Revolution“.
Beim WarDriving werden Funknetze mit Hilfe von frei erhältlichen Tools aufgespürt. Dann wird versucht in das Funknetz einzudringen, sofern es überhaupt gesichert ist. Da die Ausrüstung für das „WarDriving“ sehr günstig ist und das Eindringen in die Netze keine größeren Schwierigkeiten bereitet, hat sich bei den Hackern ein Art Subkultur entwickelt. Der Hacker installiert, z.B. auf seinem Notebook, ein frei erhältliche Tools wie Netstumbler und WEPCrack. Netstumbler ist in der Lage Access Points ausfindig zu machen wobei mit WEPCrack ein gefundenes, verschlüsseltes Netz dann gehackt werden kann. Eine handelsübliche WLAN-Karte genügt, um die Verbindung mit dem fremden WLAN herzustellen. Der Hacker setzt sich nun in sein Auto und fährt mit eingeschaltetem Notebook die Gegend ab. Sobald ein Funknetz in Reichweite ist schlägt der Netstumbler Alarm und zeigt automatisch alle Access Points im Empfangsbereich an sowie deren SSID, die MAC-Adresse und die Verschlüsselungsart (z.B. WEP). Mit einer GPS Schnittstelle und visuelle Landkarten im Internet, können Standorte von Funknetzen „gemapped“ werden.



Screenshot eines Entdeckten APs mit Netstumbler

WarChalking

Unter Warchalking versteht man die öffentliche Kennzeichnung offener Funknetzwerke wie etwa durch Kreidezeichen an Hauswänden und auf Bürgersteigen. Hat ein Hacker einen AP gefunden, der sich Knacken lässt, oder sogar offen ist, möchte er dies oft gerne der Nachwelt mitteilen, sodass andere ebenfalls davon profitieren können. Mit Kreide z.B. werden dann in der Nähe dieses drahtlosen Netzzugangs unauffällig Zeichen angebracht.



„Open Node“

Hier befindet sich ein offenes Funknetz, welches direkt Zugang ins Internet liefert.

„Closed Node“

Hier befindet sich ein geschlossenes Funknetz, wo es entweder gar keinen oder zumindest keinen öffentlichen Internetzugang gibt.

„WEP Node“

Hier werden die Daten mit WEP verschlüsselt übertragen. Für die Analyse von Verschlüsselungsmethoden, VPNs (Virtual Private Tunneling), zur Aufdeckung von Sicherheitslücken in WLANs usw. auf der Protokoll Ebene gibt es eine ganze Reihe unterschiedlicher Software, die meiste kommt aus der Open Source Gemeinde.

Airopeek

Dieses kommerzielle Tool kommt vom amerikanischen Analyzerprofi WildPackets. Die aktuelle Version von Airopek NX stellt einen professionellen Protokollanalyzer für drahtlose Netze nach zur Verfügung. Mit einen Preis von 4000 Euro ist er aber sicherlich nicht für jeden WarDriver auf legale Weise erschwinglich. Airopeek ist in erster Linie kein WLAN-Sniffer im eigentlichen Sinne, sondern soll den WLAN-Administrator bei der Suche nach Sicherheitslücken in Netzwerk

unterstützen. Seine Hauptaufgabe ist es detaillierte Information über das Geschehen im Funknetzwerk zu liefern. Der Analyzer unterstützt die meisten gängigen WLAN-Karten und kann fast alle Protokolle analysieren. Des weiteren ist er auch dazu geeignet um sogenannte "wilde" APs aufspüren.

Observer ist ein Analyzer von Network Instruments. Der normale Ethernet Analyzer wurde um ein 802.11 Funktion erweitert. Der Preis für diesen Analyzer ist ebenfalls sehr hoch angesetzt.

Wireless Sniffer

Dieser Protokoll-Aanalyzer ist der drahtlose Nachfolger der erfolgreichen Sniffer-Familie von Analyse- und Managementschwergewicht Network Associates. Er bietet in etwa die gleichen Funktionen wie der Airopeek und der Observer. Sein Preis liegt jedoch mehr als das Doppelte über dem des Airopeeks.

Netstumbler

Diese Freeware ist das am meisten genutzte Tool zum Aufspüren von WLANs. Zusätzlich liefert Netstumbler auch Informationen über die eingesetzten Client-Adaptern und Access Points. Nutzt man ebenfalls einen GPS-Receiver (Global Positioning System), kann man sehr schnell eine Karte mit Empfangsbereichen des gefundenen WLANs erstellt werden. Die Informationen von Hersteller-Daten der Access Points und deren WEP-Implementierungen können für weitere Attacken genutzt werden.

ApSniff

Dient ebenso wie der Netstumbler zum Auffinden von Access Points.

AP Scanner

Tools welche auf einem Mac arbeiten, sind eher selten. Eines der bekannteren Tools ist der AP Scanner. Mit ihm ist man in der Lage alle in der näheren Umgebung befindlichen Funknetze auszumachen. Zudem werden einige wenige Informationen dargestellt. Der AP Scanner gehört nicht zu den Tools, welche dem Netzwerkadministrator Kopfschmerzen bereiten.

AiroSniff

Bei AiroSniff handelt es sich um ein vergleichsweise rudimentäres Tool für FreeBSD, das Informationen aus dem Interface einer Cisco Aironet PC-Card ausliest. Es bietet einem die Möglichkeit alle in der näheren Umgebung befindlichen Funknetze auszumachen. Damit sind aber schon alle Möglichkeiten des Tools ausgeschöpft.

Airsnort

Das von den WarDrivern am meisten geliebte und von den WLAN-Administratoren am meist gehasste Tool ist Airsnort. Hauptfunktion dieses Tools ist die Ermittlung von WEP-Keys in relativ kurzer Zeit. Dazu schreibt das Tool zunächst die empfangenen Datenpakete mit und versucht dann mit dem gleichen Verfahren, wie es WEPcrack nutzt, den WEP-Key zu dekodieren. Verbunden mit einen schnellen Rechner lassen sich die meisten WLANs sehr schnell entschlüsseln. Der einzige Nachteil von Airsnort ist, dass es APs nicht aufspüren kann. Dafür gibt es jedoch genügend andere Tools, welche dazu in der Lage sind.

AirTraf

Dieses Tool bietet eine Menge verschiedener Möglichkeiten. AirTraf kann Packete mitsniffen und auch dekodieren. Des weiteren kann die Software natürlich auch AP aufspüren und entsprechende Daten liefert. Des weiteren bietet AirTraf die Möglichkeit alle empfangenen Daten in einer Datenbankform abzuspeichern, dadurch können verschiedene Tools auf die gleichen Daten zugreifen. AirTraf ist noch in Entwicklung, es gibt allerdings auch stabiles Releases.

Fake AP

Black Alchemy's Fake AP

Black Alchemy's Fake AP generates thousands of counterfeit 802.11b access points. Hide in plain sight amongst Fake AP's cacophony of beacon frames. As part of a honeypot or as an instrument of your site security plan, Fake AP confuses Wardrivers, NetStumblers, Script Kiddies, and other undesirables.

Freestumble

Hierbei handelt es sich um ein Derivat von NetStumbler. Im Gegensatz zum Original soll dieses Hilfsprogramm wesentlich mehr Karten unterstützen, sowie unter Linux laufen. Zurzeit arbeitet der Entwickler am Freestumble nicht weiter. Eine funktionsfähige Version wird zwar von vielen WarDrivern erwartet, ob es aber je eine geben wird, ist noch nicht abzusehen.

Kismet

Das Freeware-Projekt Kismet entwickelte einen WLAN-Sniffer für die Linux-Kommandozeile an. Das Tool kann WLANs aufspüren und liefert zusätzliche Informationen über Status der Verschlüsselung oder vorhandene DHCP-Dienste. Kismet besitzt aufgrund seiner Flexibilität gegenüber den anderen Tools einen recht großen Vorteil. Es unterstützt alle Client-Karten, die unter Linux laufen.

Hier noch einige weitere Tools zur Aufspürung sicherheitsrelevanter Fehler:

Odyssey WLAN Security Software
PocketWarrior
PocketWarrior
PrismStumbler
THC-WarDrive
SSID Sniff
WarLinux
Wavemon
WaveStumbler
Wellenreiter
WEPcrack

Die Fehlersuche in WLANs ist ein sehr weitreichendes Thema. Sie beginnt im Labor bei der Entwicklung der Chips und Sendetechniken und endet quasi auf der Strasse auf der Suche nach Sicherheitslücken im Firmennetzwerk. Die Gründe eines nicht korrekt funktionierenden WLANs können an einer falsch eingerichteten Netzwerkeinstellung liegen, aber auch ganz trivial an einem lecken Mikrowellenherd. An welcher Stelle mit der Fehlersuche nun letztendlich begonnen wird kann wie bei den meisten Netzwerkproblemen wohl hauptsächlich nur durch Erfahrungswerte und Gefühl entschieden werden. Ein „Allround Gerät“ welches aus allen Fehlermöglichkeiten in sämtlichen OSI Schichten im Klartext sagt, wo der Haken ist, gibt es nicht und wird es wohl nie geben. Bei LAN Netzwerken kann immerhin als erste Untersuchung

geschaut werden, ob den überhaupt das Kabel angeschlossen ist, und die LEDs blinken. Bei WLAN ist das schon nicht mehr möglich. Es macht aber auf der anderen Seite bestimmt auch keinen Sinn (ganz zu schweigen von den Kosten), bei einer nichtfunktionierenden Verbindung gleich mit „Kanonen auf Spatzen schiessen“ und dem fast 70.000 teuren ADVANTEST R3681 dem Fehler auf die Pelle zu rücken, denn unter Umständen funktionierts schon wieder, wenn das Laptop um ein paar Zentimeter verschoben wird.

Martin Heine M.Sc.

studierte Elektrotechnik in Kempten im Allgäu und wechselte dann zur Hochschule Reutlingen, Fachrichtung Elektronik/Halbleitertechnik wo er erst seinen Abschluss als Dipl.-Ing.(FH). absolvierte. Als freier Mitarbeiter in der Elektronik-Hardware und Firmware Entwicklung arbeitete er an zahlreichen internationalen Forschungsprojekten an der Universität Stuttgart und der Deutschen Forschungsgesellschaft für Luft und Raumfahrt (DLR). Während seines USA Aufenthalts entwickelte er unter anderen für Laird Technologies und Hirschmann Multifunktions-Antennen und Mobilfunk / GPS Telematik Systeme für die Automobilbranche und erhielt fünf U.S. Patente. Nach anschließender mehrjähriger Mitarbeit beim ZDF (Zweites Deutsches Fernsehen), und einem Aufbaustudium als "Computer Based Engineering Master of Science" war er zwei Jahre bei Rohde & Schwarz im Bereich Software Definde Radio tätig. Als freier Berater, Entwickler und Fachjournalist im IT-Bereich, spezialisiert auf Embedded Systems, Power Management, Magnet-gelagerte Hochgeschwindigkeits-Antriebe, Biosignalverarbeitung, Medizintechnik arbeitet er an zahlreichen Projekten für die Textil-, Medizin-, Verteidigungs-, und Luft & Raumfahrt Branche. Eines seiner Projekte wurde mit dem deutschen Innovationspreis "Otto von Guericke" der AiF ausgezeichnet. Als Autor wirkte Martin Heine an mehreren Grundlagenbüchern mit, unter anderen „Wireless LAN“ und „Ethernet“ der Professional Series vom Franzis Verlag, und veröffentlichte viele Fachartikel in diversen Fachzeitschriften wie Network Computing, IT-Sicherheit, Funkschau und weitere.