Projektarbeit

VoIP und IPsec über ein Wireless LAN

Dokumentation
Mario Gersbach und Marcel Kunz

Thema der Arbeit	VoIP und IPsec über ein Wireless LAN
Studenten	Mario Gersbach Marcel Kunz
Kontaktadressen	i7gersba@zhwin.ch i7kunz@zhwin.ch
Dozent	Dr. Andreas Steffen
Auftraggeber	Siemens Schweiz AG
Ausgabe der Arbeit	23. Mai 2000
Abgabe der Arbeit	21. Juli 2000

Inhalt

1 Vorwort

Der anhaltende Boom in Richtung kabellose Kommunikation macht das Wireless LAN mit seinem Standard 802.11 zu einem aktuellen Thema. Die einfache Installation und der extrem einfache Betrieb des I-Gate machen das Produkt sympathisch und marktgerecht für den Geschäfts- sowie auch für den privaten Betrieb.

Die Aufgabe dieser Projektarbeit wurde uns von der Firma Siemens Schweiz AG gestellt. Die für uns sehr interessante Aufgabe beinhaltet eine Einarbeitung ins Thema, die wir natürlich nur spärlich dokumentieren können, da sie mehrheitlich aus Dokumentationen und Homepages lesen besteht, das Messen von verschiedensten Situationen und der Präsentation im Technikum Winterthur, welche uns noch bevorsteht.

Da wir von Anfang an sehr engagiert zur Sache gingen und Herr Steffen die Arbeit im Vorfeld sehr gut vorbereitet hatte, konnten wir diese Projektarbeit ohne Zeitdruck fertigstellen.

Von der ZHW wurde uns ein für unser Projekt ausgerüsteter Arbeitsplatz und sehr gute Betreuung mit wöchentlichen Sitzungen zur Verfügung gestellt, wofür wir vor allem Herrn Dr. Andreas Steffen danken möchten.

Winterthur, 21. Juli 2000

Mario Gersbach Marcel Kunz

2 Aufgabenstellung

Sinkende Preise machen die auf dem IEEE 802.11 Standard basierenden Wireless LANs immer attraktiver. Allerdings ist sich der Benutzer an den Datendurchsatz und die Verzögerungszeiten eines IEEE 802.3 Ethernet basierten LANs mit Bitraten von 10-100 Mbps gewöhnt und stellt automatisch entsprechende Vergleiche an.

Diese Projektarbeit soll abklären, mit welchem aktuellen Durchsatz und welchen Verzögerungszeiten beim praktischen Betrieb eines 2 Mbps WLANs gerechnet werden muss. Dabei soll die spezielle Situation berücksichtigt werden, dass sich oft nicht alle WLAN-Teilnehmer gleichzeitig hören können (Hidden Terminal Problem). Weiter soll der eventuell störende Einfluss eines im 2.5 GHz ISM-Band betriebenen Mikrowellenofens abgeklärt werden.

Voice over IP Anwendungen sind im Kommen. Es soll untersucht werden, ob die wesentlich grösseren Packetverzögerungsschwankungen eines WLANs einen nennenswerten Einfluss auf die Qualität einer drahtlosen VoIP Verbindung haben.

Drahtlose LANs können leicht abgehört werden und gelten deshalb als nicht sicher. Die optionale Verschlüsselung mit einem 40 bit RC4 Stream Cipher trägt auch nicht viel zur Vertrauensbildung bei. Es soll untersucht werden, ob eine IPsec Verbindung bei drahtloser Übertragung irgendwelche Probleme mit sich bringt.

Vollständige Aufgabenstellung siehe Kapitel 10.5

3 IEEE 802.11

Diese Norm, die im Juni 1997 verabschiedet wurde, spezifiziert drei verschiedene kabellose Medien:
- Direct Sequence Spread Spectrum (DSSS)
- Frequency Hopping Spread Spectrum (FHSS)
- Infrarot

Definiert werden in der 802.11 folgende Spezifikationen:
- Media Access Control (MAC), die speziell auf Wireless LAN Anforderungen angepasst wurde
- Physical Layer (Phy) für DSSS
- Physical Layer (Phy) für FHSS
- Physical Layer (Phy) für Infrarot

Merkmale des Physical Layers bei DSSS:
- 2 Mbit/s Datenübertragungsgeschwindigkeit mit automatischer Verringerung auf 1 Mbit/s bei schlechten Ausbreitungsbedingungen
- 2,4 GHz Band
- Vorgegebener Spreizcode

Bei der IEEE 802.11 wurde auf besondere Robustheit der Datenübertragung geachtet. Nachfolgend einige besondere Merkmale in Stichworten:
- CSMA/CA mit MAC Schicht ACKnowledge (für geringeren Datenverlust)
- RTS/CTS (Ready to send/ Clear to send)
- Automatische Einstellung der Datenrate (bei schlechten Übertragungsbedingungen wird automatisch von 2 Mbps auf 1 Mbps umgeschaltet)
- Aufteilung der Information in einzelne Informationsblöcke (ergibt eine höhere Performance bei Störungen)
- Multi Channel Roaming (erhöht die Mobilität und die Performance, bis zu einer Datenrate von 6 Mbps)
- Power Management (zur Schonung der Batterie)

- Verschlüsselung (Wired Equivalent Privacy, WEP) basierend auf dem RC4-Algorithmus

Bemerkung zur IEEE 802.11: Durch die Norm ergibt sich der grosse Vorteil für den Anwender, dass Geräte verschiedener Hersteller in einem kabellosen Netzwerk verwendet werden können. Ein Mischen von Geräten mit FHSS und DSSS ist jedoch nicht möglich (bedingt durch die verschiedenen Modulationsarten).

Leider wurde auch der Informationsaustausch zwischen den Access Points von der IEEE 802.11 nicht geregelt. Dadurch ist das Roaming zwischen Access Points verschiedener Hersteller nicht möglich.

Zur Zeit arbeitet man an zwei Erweiterungen des Standards 802.11. Die 802.11a und die 802.11b.

- 802.11a: Eine Datenrate von bis zu 54 Mbit/s im 5 GHz-Bereich (Der Bereich ist in Europa für HIPERLAN spezifiziert).
- 802.11b: Erhöhung der Datenrate bei FHSS auf 3 Mbit/s und DSSS auf 11 Mbit/s im 2,4 GHz-Band.

(URL1)

4 Direct Sequence (DSSS)

Bei der Direct Sequence Technik arbeiten Sender und Empfänger in einem festgelegten Frequenzbereich. Dabei erfolgt die Bandspreizung bereits auf Signalebene. Dazu verschlüsselt der Sender jedes Datenbit in einer Pseudozufallsfolge aus mindestens 10 Zuständen, den sogenannten ‚Chips', welche dann in dem festgelegten Frequenzband gesendet werden. Für unauthorisierte Zuhörer verschwindet das Signal dadurch im Hintergrundrauschen. Der Empfänger, welcher die Verschlüsselungssequenz kennen muss, kann aus dem scheinbaren Rauschen die ursprüngliche Bitfolge restaurieren. Auch hier sind mehrere Kanäle im selben Band möglich, da eine Pseudozufallsfolge immer nur von einem Sender-Empfänger-Paar benutzt wird.

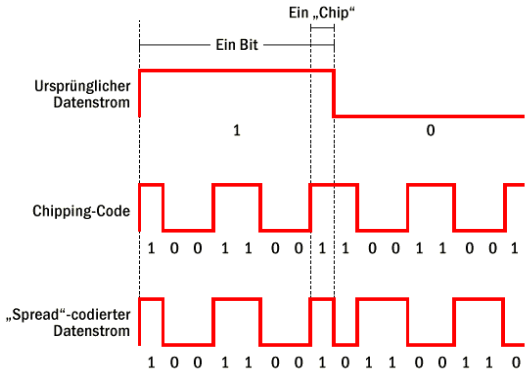

Bild 4.1: Das DSSS-Verfahren vermischt die Nutzinformation mit Fülldaten, dem sogenannten Chipping Code

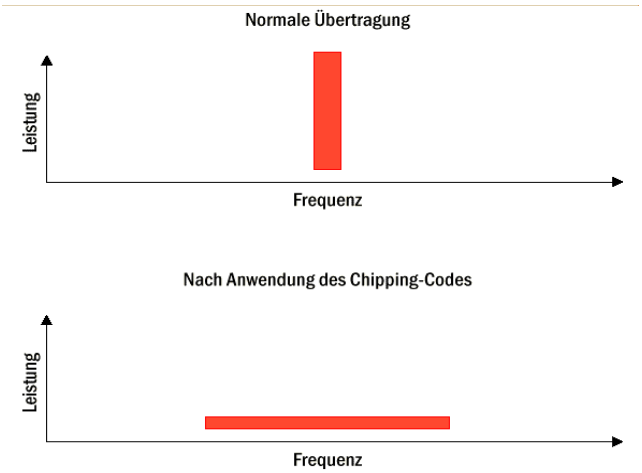

Bild 4.2: DSSS verbreitert den Frequenzbereich der Datenübertragung

Die DSSS-Technik ist im Gegensatz zum Frequency Hopping unempfindlicher gegen Interferenzen (Delay Spread). Da bei drahtlosen Übertragungen das Signal nicht nur geradlinig vom Sender zum Empfänger geht, sondern auch über mehrfache Reflexionen an Wänden oder Gegenständen zum Ziel gelangt, erreichen den Empfänger mehrere zeitlich versetzte, abgeschwächte oder verzerrte Signale. Dabei können sich die Signale addieren oder auch gegenseitig auslöschen. Der Empfänger muss daraus trotzdem den übertragenen Wert erkennen können. Beim DSSS steht dafür ein breiteres `Frequenz-Fenster' zur Verfügung, so dass hier der Einfluss der Störungen kleiner ist. Ausserdem ist ein Recovering von beschädigten Daten möglich, so dass ein erneuter Transfer unnötig ist.

(URL3)

5 Das hidden-terminal-Problem

5.1 Das Problem

Bei drahtgebundenen LANs gilt eine wichtige Voraussetzung: Jede Station empfängt alles, was eine beliebige andere Station sendet, die am gleichen Kabel angeschlossen ist. Diese Annahme gilt bei WLANs nicht. Das sogenannte hidden-terminal-Problem ist in Abbildung 5.1 dargestellt.

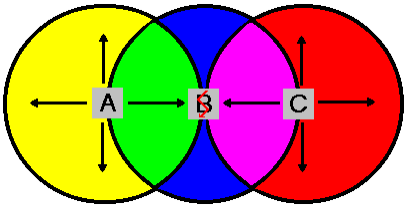

Bild 5.1: hidden-terminal Konstellation

Obwohl gerade von Station A eine Übertragung nach Station B erfolgt, erkennt Station C einen freien Kanal und kann selbst z.B. zu Station B senden. Daher kommt es bei Station B zu einer Kollision. Ein herkömmlicher Carrier-Sense-Mechanismus ist also bei WLANs unzureichend.

5.2 Normale Kollisionsdetektion: Distributed Coordination Function (DCF)

Die Distributed Coordination Function (DCF) ist die grundlegende Zugriffsmethode des MAC nach IEEE 802.11. Sie ist auch unter dem Namen Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) bekannt. Ein CSMA/CD-Verfahren wie beim Ethernet ist aus physikalischen Gründen nicht realisierbar, da eine Station zu jedem Zeitpunkt nur entweder senden oder empfangen kann.
Bei Verwendung des CSMA/CA-Verfahrens hört eine sendewillige Station das WM ab. Ist es belegt, muss auf die Beendigung der laufenden Datenübertragung gewartet werden. Das exposed-terminal-Problem wird also im IEEE 802.11 Standard nicht gelöst.
Der Zeitpunkt der höchsten Wahrscheinlichkeit für eine Kollision liegt nach dem Ende der Übertragung eines Frames. Denn es haben möglicherweise mehrere Stationen auf ein frei werdendes Medium gewartet und beginnen nun unmittelbar mit der Datenübertragung. Da Kollisionen nicht sofort erkannt werden können, reduzieren sie den Datendurchsatz bei WLANs stärker als zum Beispiel beim Ethernet, wo die Übertragung bei Erkennung einer Kollision sofort unterbrochen wird. Aus diesem Grund wird nach Erkennung des freien Mediums neben einem fest vorgeschriebenen Distributed Coordination Function Inter Frame Space noch eine zufällige Zeit gewartet, die sogenannte Backoff Time. Die Backoff Time ist ein Vielfaches der sogenannten Slot Time. Die Slot Time ist für die verschiedenen Physical Layer unterschiedlich und beträgt zum Beispiel beim FHSS-Verfahren 50µs. Stellt die Station während ihrer Backoff Time erneute Aktivität auf dem Medium fest, so wird der Backoff Timer angehalten und behält seinen aktuellen Wert bei. Wenn das Medium wieder für die Zeit eines DIFS frei wird, erhält die Station eine erhöhte Priorität, da sie nur noch ihre reduzierte Backoff Zeit warten muss.

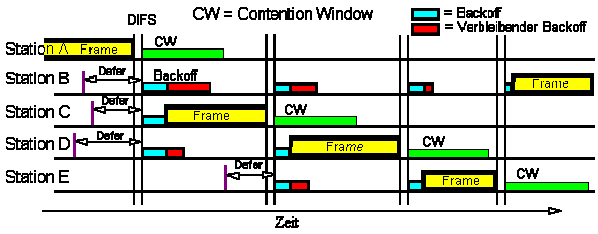

Bild 5.2: Backoff-Verfahren

Natürlich kann es vorkommen, dass sich zwei Stationen für die gleiche Wartezeit entscheiden, was zu einer Kollision führt. Das Verfahren kann also Kollisionen nicht gänzlich vermeiden, sondern nur deren Wahrscheinlichkeit verringern. Es trägt also seinen Namen (Collision Avoidance) eigentlich zu unrecht. Bei wiederholten Versuchen, einen Frame zu übertragen, steigt die Backoff Time exponentiell an:

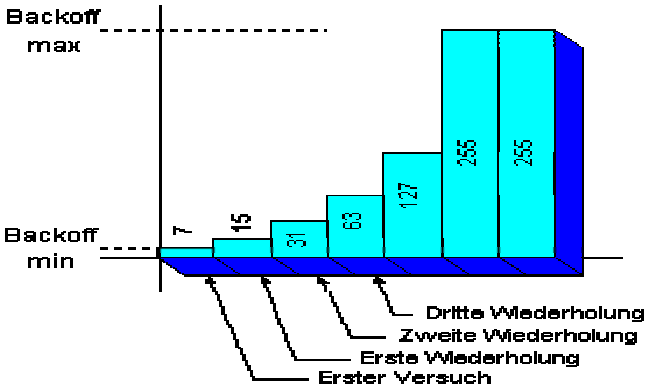

Bild 5.3: Backoff-Einfluss

Nach erfolgreichem Empfang eines Daten-Frames wird mit höchster Priorität ein positives Acknowledgement (ACK) versandt.
Nach erfolgreicher Übertragung eines Frames muss eine Station aus Fairness die Zeit des sogenannten Contention Windows (CW) abwarten, bevor sie erneut übertragen darf. Die Grösse des CW ist vom verwendeten Physical Layer abhängig, der Minimalwert liegt bei Verwendung von FHSS bei dem 15fachen der Slot Time (also bei 750µs). Das CW wird wie der Backoff bei erkannten Übertragungsfehlern in Zweierpotzenzschritten vergrössert. Der Maximalwert bei FHSS liegt bei dem 1023fachen der Slot Time, also bei etwa 51ms. In dem Fall, dass nur diese eine Station senden will, bedeutet das Abwarten des CW natürlich einen nicht zu vernachlässigenden Effizienz-Verlust.

5.3 Die Lösung: Virtueller Carrier Sense (RTS/CTS)

Bei den bisherigen Betrachtungen wurde das hidden-terminal-Problem ausser Acht gelassen. Es besteht daher die Möglichkeit durch Verwendung von Ready To Send (RTS) beziehungsweise Clear To Send (CTS) Frames einen virtuellen Carrier Sense aufzubauen. Wenn Station A ein Daten-Frame zu Station B schicken möchte, fragt sie zunächst durch Versenden eines kurzen RTS-Frames bei B nach. Im RTS-Frame wird die erwartete Länge der Übertragung mitgeteilt. Durch dieses Frame sind alle Stationen über die eventuell bevorstehende Übertragung informiert und setzen ihren virtuellen Carrier Sense für die angegebene Zeit auf besetzt. Antwortet nun Station B mit einem CTS-Frame, der ebenfalls die erwartete Übertragungsdauer enthält, so wissen auch alle Stationen im Sendebereich von Station B über die bevorstehende Übertragung Bescheid, insbesondere auch die Station C, die den RTS-Frame von Station A nicht empfangen hat.
CTS-Frames werden mit der höchsten Priorität versandt. Dadurch wird verhindert, dass während des RTS/CTS-Handshakes und der zugehörigen Datenübertragung inklusive ACK eine weitere Station das Senderecht erhält.

Durch die Verwendung des RTS/CTS-Handshakes werden jedoch Kollisionen auch nicht ganz vermieden, jedoch werden höchstens die RTS/CTS-Frames gestört und nicht die längeren Daten-Frames. Dieser Mechanismus ist also nur ab einer gewissen Mindestgrösse von Daten-Frames sinnvoll, da er zusätzlichen Overhead bedeutet. Die Grenze, ab der mit RTS/CTS-Handshake gearbeitet werden soll, ist nicht im Standard festgelegt. Es kann also immer, teilweise, oder gar nicht eingesetzt werden. Ein typischer Grenzwert liegt bei einer MPDU-Grösse von 120 Byte.

(URL9)

6 IPsec: PGPnet

Um das I-Gate unter Verwendung von IPsec zu prüfen, haben wir PGPnet installiert. Das Ziel ist eine verschlüsselte (1024Bit) End-zu-End Verbindung mit dem Shared Key-Verfahren. Dabei haben wir folgend Features von PGP Version 6.5.1 verwendet:

IKE (Internet Key Exchange)

- Authentication (Authentifizierung mittels): RSA oder DSS Signatur oder eines Shared Key (gemeinsamer Key)
- Hash: SHA-1 oder MD5 Cipher, Verschlüsselung mit CAST oder Triple-DES
- DH (Diffie-Hellmann Keylänge): 1024 oder 1536-bit

IPSEC

- AH (Authentication Header): IPSec-Unterprotokoll, dass nur die Authentifizierung verschiedener Teile eines IP Headers über SHA-1 oder MD5 Hashes regelt
- ESP (Encapsulating Security Payload): IPSec-Unterprotokoll, dass die Verschlüsselung per CAST oder Triple-DES Algorithmus und die Authentifizierung per SHA-1 oder MD5 Hash regelt
- IPPCP (IP Payload Compression Protocol): Datenkompresssion per LZS oder Deflate
- Perfect Forward Secrecy: Keylänge des Diffie-Hellmann Keys für alle definierten IPSec Anträge

Die detaillierten Einstellungen sind in folgenden Screen ersichtlich:

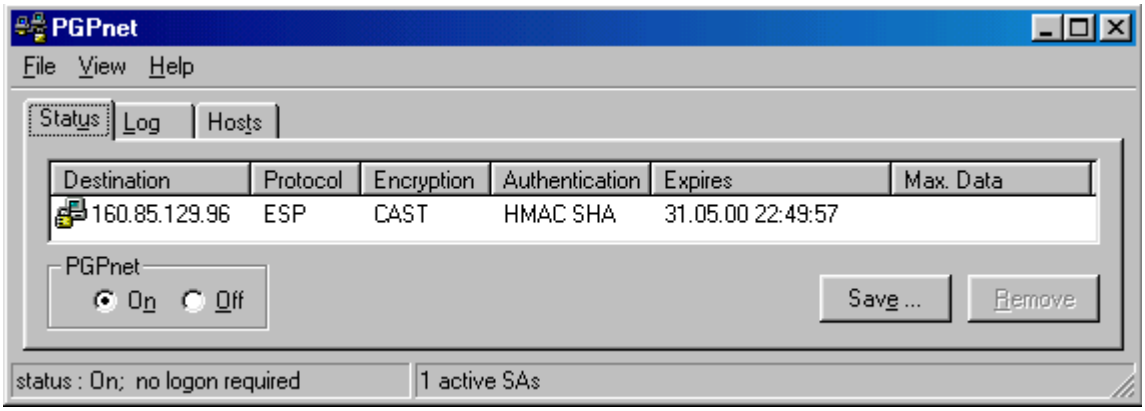

Bild 6.1: PGPnet Status

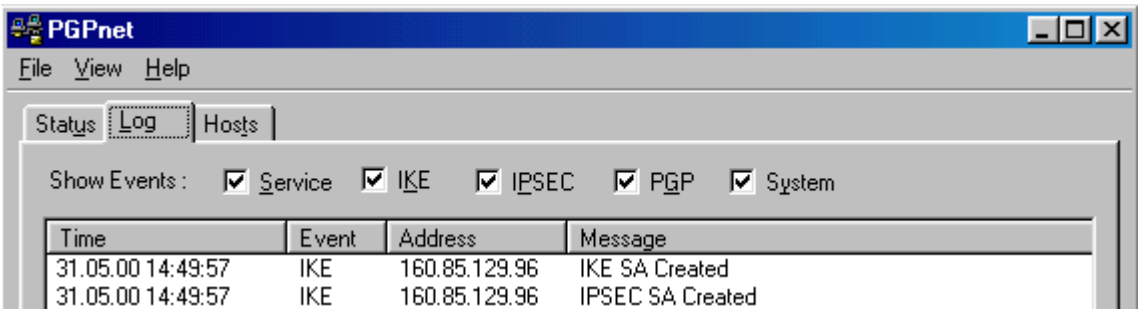

Bild 6.2: PGPnet Log

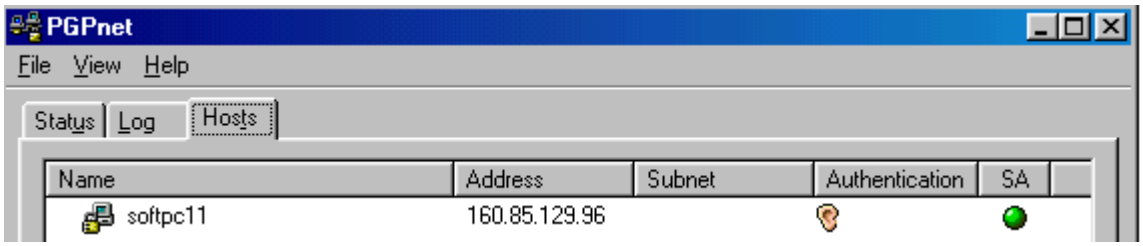

Bild 6.3: PGPnet Hosts

(URL4)

7 Testfälle

Hier aufgeführte Messwerte beruhen auf einem Mittel von 2..5 Messungen. Dabei wird eine Datei vom 10‘000‘000 Byte (9.5 MByte) transferiert. Das Netz funktioniert im Infrastructure Mode, so bestimmt der Basisport die Parameter. Die Detailierten Messresultate sind in den Kapitel 10.2.3 und 10.2.4 notiert.

7.1 Ohne Hidden Terminals

7.1.1 Normaler FTP, variable Paketlänge

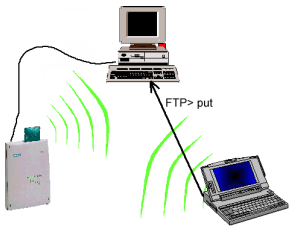

Bild 7.1: Versuchsaufbau

Nr	Messungs-Nummer
CPU	CPU-Auslastung
KNr	Kanalnummer
L	Paketlänge in Bytes
T	Zeit in Sekunden

Bild 7.2: Legende zu 7.3

Bedingungen: ungestört, FTP ASCII Modus

Nr	CPU	KNr	L [Bytes]	t [s]	Rate	Rate
1	<20%	11	1550 Bytes	58s	172 KByte/s	1.35 MBit/s
2	<20%	11	1000 Bytes	58s	172 KByte/s	1.35 MBit/s

Bild 7.3: Normaler FTP, variable Paketlänge

Fazit: Die Übertragungsrate erreicht im besten Fall 1.35 MBit/s.

7.1.2 Verschlüsselter FTP

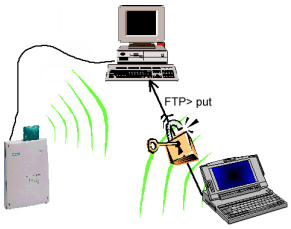

Bild 7.4: Versuchsaufbau

Nr	Messungs-Nummer
CPU	CPU-Auslastung
Cipher	Cipher
Hash	Hash
DH	Diffie-Hellman
KNr	Kanalnummer
L	Paketlänge in Bytes
t	Zeit in Sekunden

Bild 7.5: Legende zu 7.6

Bedingungen: ungestört, FTP ASCII Modus, PGPnet mit einem Shared Key

Nr	CPU	Hash	Cipher	DH	L	KNr	t	Rate	Rate
3	<20%	MD5	CAST	1024 Bits	1550 Bytes	11	66s	152KBytes/s	1.18MBit/s
4	<20%	MD5	CAST	1024 Bits	1000 Bytes	11	68s	147KBytes/s	1.18MBit/s
5	<20%	MD5	TripleDES	1024 Bits	1550 Bytes	11	67s	149KBytes/s	1.17MBit/s
6	<20%	MD5	TripleDES	1024 Bits	1000 Bytes	11	66s	152KBytes/s	1.18MBit/s

Bild 7.6: Verschlüsselter FTP

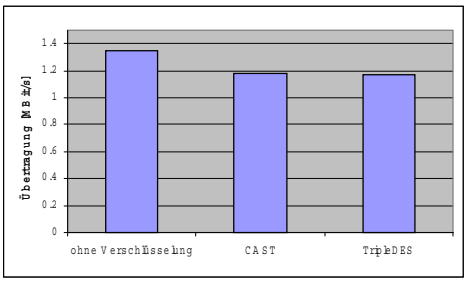

Bild 7.7: Vergleich der Übertragung mit und ohne Verschlüsselung mit einer Paketlänge von 1550 Bytes.

Fazit: In Verbindung mit IPsec sind nie Probleme aufgetreten, jedoch verringert sich die Nutzbandbreite um 13 %. Der folgende Header trägt einen kleinen Teil zu diesem Verlust bei.

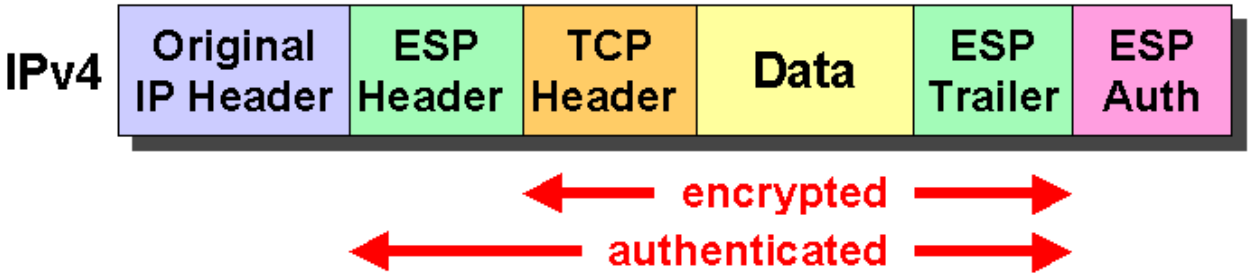

Bild 7.8: Verschlüsseltes IP-Paket

7.1.3 Paralleler FTP

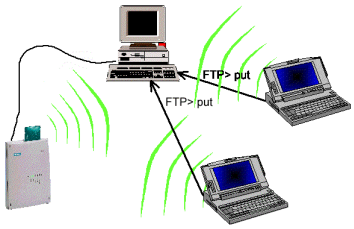

Bild 7.9: Versuchsaufbau

Nr	Messungs-Nummer
CPU	CPU-Auslastung
KNr	Kanalnummer
L	Paketlänge in Bytes
t	Zeit in Sekunden

Bild 7.10: Legende zu 7.11

Bedingungen: Beide Laptops beginnen den Transfer miteinander.

Nr	L [Bytes]	KNr	t [s]	Rate	Rate
7	1550 Bytes	11	115s	174 KByte/s	1.35 MBit/s

Bild 7.11: Paralleler FTP

Fazit: Es wird die doppelte Datenmenge in der doppelten Zeit übertragen, was zur gleichen Datenrate führt. Das heisst die Kollisionserkennungs-Verfahren verrichtet ihren Dienst optimal. Einzig bleibt die Frage, warum der eine Laptop immer schneller ist als der andere.

7.1.4 Mikrowelle in unmittelbarer Nähe vom Basisport mit variabler Paketlänge

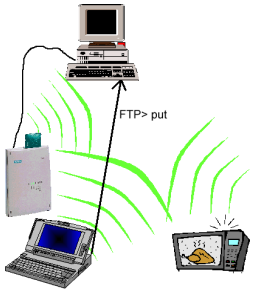

Bild 7.12: Versuchsaufbau

Nr	Messungs-Nummer
CPU	CPU-Auslastung
KNr	Kanalnummer
L	Paketlänge in Bytes
t	Zeit in Sekunden

Bild 7.13: Legende zu 7.14 und 7.16

Bedingungen: Mikrowelle steht unmittelbar vor dem Basisport und heizt mit 800 Watt einen Liter Wasser auf

Nr	L [Bytes]	KNr	t [s]	Rate	Rate
8	1550 Bytes	11	161s	62 Kbyte/s	0.48 MBit/s
9	1000 Bytes	11	162s	61 Kbyte/s	0.48 MBit/s
9/600	600 Bytes	11	201s	50 Kbyte/s	0.39 MBit/s
10	1550 Bytes	7	492s	20 Kbyte/s	0.16 MBit/s
11	1550 Bytes	3	133s	75 Kbyte/s	0.59 MBit/s
12	1550 Bytes	13	71s	142 KByte/s	1.11 MBit/s

Bild 7.14: Mikrowelle in unmittelbarer Nähe vom Basisport mit variabler Paketlänge

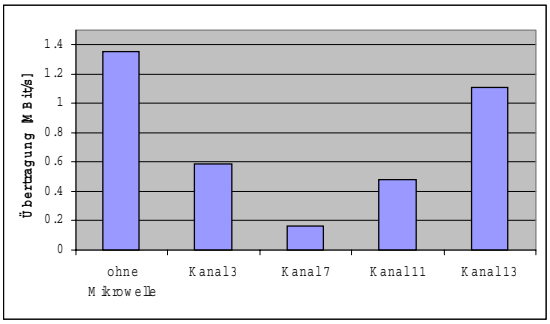

Bild 7.15: Kanalvergleich

Bedingungen: Beide Laptops beginnen den Transfer miteinander, während die Mikrowelle mit voller Leistung stört.

Nr	L [Bytes]	KNr	t [s]	Rate	Rate
13	1550 Bytes	11	268s	75 Kbyte/s	0.58 MBit/s

Bild 7.16: volle Leistung

Fazit: In diesen Messungen überlappen sich die Spektren der Mikrowelle und des I-Gate zum Teil vollständig. Die Erwartungen, dass mit kürzerer Paketlänge mehr Durchsatz erreicht werden kann, hat sich nicht bestätigt.

7.1.4.1 Illustrationen

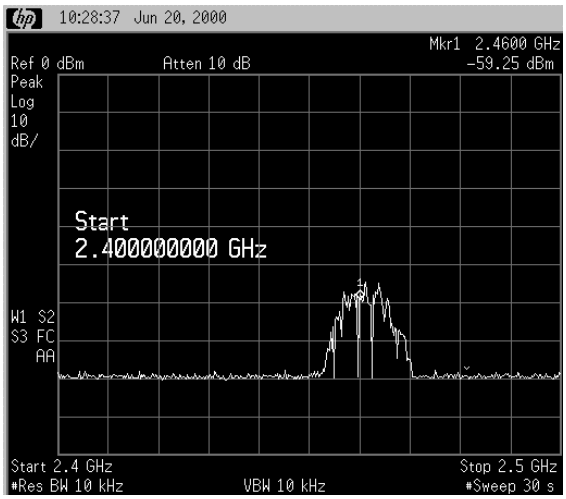

Bild 7.16: Spektrums während des Senden auf Kanal 11 ohne Mikrowellenofen

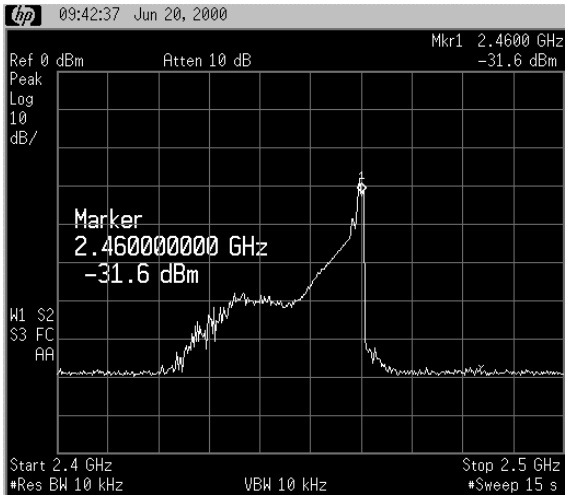

Bild 7.17: Bild des Störspektrums des Mikrowellenofens (Das Spektrum variiert sehr stark)

(URL7), (URL6)

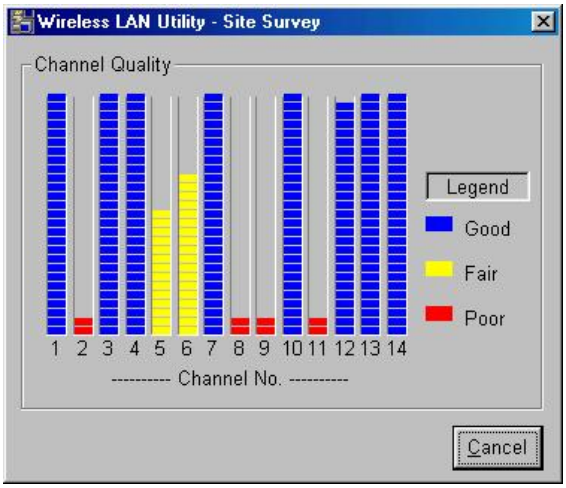

Bild 7.18: Das Siemens I-Gate Utility zeigt hier die Qualität der einzelnen Kanäle auf (Basisport steht unmittelbar neben der Mikrowelle).

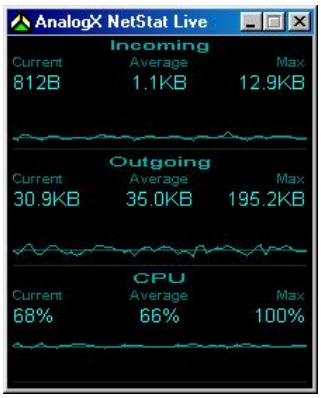

Bild 7.19: Mit diesem Tool können wir den Verlauf der Datenrate über eine Minute hinweg beobachten:

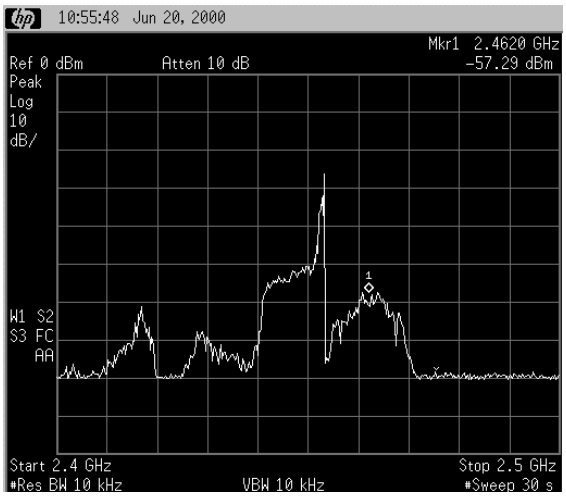

Bild 7.20: Spektrums während des Senden mit Kanal 11 und Mikrowellenofen

7.1.5 Mikrowelle im selben Raum: 6m Abstand

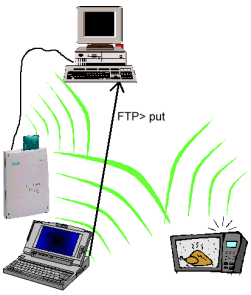

Bild 7.21: Versuchsaufbau

Nr	Messungs-Nummer
CPU	CPU-Auslastung
KNr	Kanalnummer
L	Paketlänge in Bytes
t	Zeit in Sekunden

Bild 7.22: Legende zu 7.23

Bedingungen: Mikrowelle steht im selben Raum ~6m von der Basisstation entfernt und heizt mit 800 Watt einen Liter Wasser auf.

Nr	L [Bytes]	KNr	t [s]	Rate	Rate
14	1550 Bytes	1	58s	171 KByte/s	1.31 MBit/s
15	1550 Bytes	2	58	172 KByte/s	1.31 MBit/s
16	1550 Bytes	3	58	172 KByte/s	1.31 MBit/s
17	1550 Bytes	4	58	172 KByte/s	1.31 MBit/s
18	1550 Bytes	5	58s	172 KByte/s	1.31 MBit/s
19	1550 Bytes	6	61s	164 KByte/s	1.25 MBit/s
20	1550 Bytes	7	75s	133 KByte/s	1.01 MBit/s
21	1550 Bytes	8	78s	128 KByte/s	0.98 MBit/s

22	1550 Bytes	9	68s	148 KByte/s	1.13 MBit/s
23	1550 Bytes	10	60s	166 KByte/s	1.27 MBit/s
24	1550 Bytes	11	59s	171 KByte/s	1.30 MBit/s
25	1550 Bytes	12	58s	171 KByte/s	1.31 MBit/s
26	1550 Bytes	13	58s	171 KByte/s	1.31 MBit/s

Bild 7.23: Mikrowelle im selben Raum: 6m Abstand

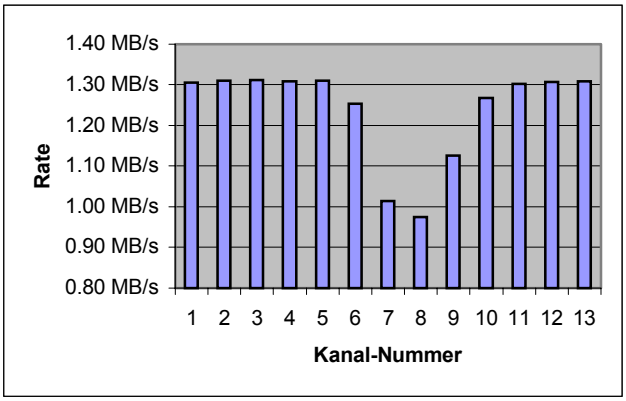

Bild 7.24: Kanalvergleich

Fazit: siehe Fazit 7.1.6

7.1.6 Mikrowelle im selben Raum: 3m Abstand

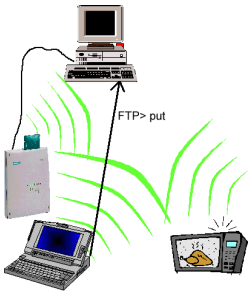

Bild 7.25: Versuchsaufbau

Nr	Messungs-Nummer
CPU	CPU-Auslastung
KNr	Kanalnummer
L	Paketlänge in Bytes
t	Zeit in Sekunden

Bild 7.25: Legende zu 7.26

Bedingungen: Mikrowelle steht im selben Raum ~3m von der Basisstation entfernt und heizt mit 800 Watt einen Liter Wasser

Nr	L [Bytes]	KNr	t [s]	Rate	Rate
27	1550 Bytes	1	58s	172 KByte/s	1.31 MBit/s
28	1550 Bytes	2	58s	171 KByte/s	1.31 MBit/s
29	1550 Bytes	3	58s	171 KByte/s	1.31 MBit/s
30	1550 Bytes	4	58s	172 KByte/s	1.31 MBit/s
31	1550 Bytes	5	58s	171 KByte/s	1.31 MBit/s
32	1550 Bytes	6	63s	159 KByte/s	1.21 MBit/s
33	1550 Bytes	7	73s	137 KByte/s	1.05 MBit/s
34	1550 Bytes	8	71s	141 KByte/s	1.07 MBit/s
35	1550 Bytes	9	69s	145 KByte/s	1.11 MBit/s
36	1550 Bytes	10	63s	159 KByte/s	1.21 MBit/s
37	1550 Bytes	11	58s	171 KByte/s	1.31 MBit/s
38	1550 Bytes	12	59s	171 KByte/s	1.30 MBit/s
39	1550 Bytes	13	58s	171 KByte/s	1.31 MBit/s

Bild 7.26: Mikrowelle im selben Raum: 3m Abstand

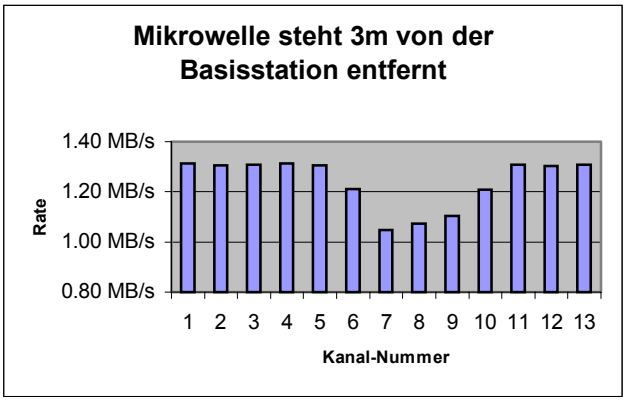

Bild 7.27: Kanalvergleich

Fazit: Diese Konstellation kommt einer realistischen Büroumgebung nahe. Da der Mikrowellenofen nicht die ganze Zeit eingeschaltet ist, ergeben sich keine ernsthaften Probleme. TCP-Retransmits konnten wir nie beobachten. Nach Möglichkeit sollten natürlich trotzdem nicht die Kanäle 6,7,8,9,10 in der Nähe eines Mikrowellenofens benützt werden.

7.1.7 Normaler FTP in grössere Distanz

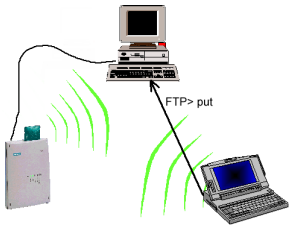

Bild 7.28: Versuchsaufbau

Nr	Messungs-Nummer
s	Abstand Basisport-Mobilestation
SS	Signalstärke
CPU	CPU-Auslastung
KNr	Kanalnummer
L	Paketlänge in Bytes
t	Zeit in Sekunden

Bild 7.29: Legende zu 7.30

Bedingungen: Wir senden wie gehabt 10‘000‘000 Bytes und entfernen uns immer weiter vom der Basisport. Der Basisport befindet sich im Zimmer E507 und die Mobilstation steht im entsprechenden Abstand im Gang.

Nr	S	Wände	Etagen	SS	L [Bytes]	KNr	t [s]	Rate	Rate
40	10m	min. 1	0	84..100%	1550 Bytes	10	58s	172 KByte/s	1.35 MBit/s
41	20m	min. 1	0	78%	1550 Bytes	10	58s	172 KByte/s	1.35 MBit/s
42	40m	min. 1	0	68%	1550 Bytes	10	58s	172 KByte/s	1.35 MBit/s
43	20m	min. 1	1	57..60%	1550 Bytes	10	85s	117 KByte/s	0.92 MBit/s
44	>20m	min. 1	1	52..57%	1550 Bytes	10	92s	108 KByte/s	0.85 MBit/s

Bild 7.30: Normaler FTP in grössere Distanz

Fazit: Die maximale mögliche Distanz zwischen Mobil- und Basisstation ist in unserem Fall ca. 40m. Diese Distanz ist aber extrem von der Umgebung abhängig. Das ideale Einsatzgebiet für das I-Gate ist in einem Grossraumbüro oder in benachbarten Räumen.

7.1.8 Ad-hoc vs. Infrastructure Mode

Bedingungen: ungestört, Windows copy

Nr	Mode	t [s]
45	Standard (Ad-hoc)	64s
46	Infrastructure	134s

Bild 7.30a: Ad-hoc vs. Infrastructure Mode

Fazit: Da im Infrastructure Mode jedes Paket einmal von der Mobilstation und einmal von der Basisport gesendet wird, brauchen wir doppelt so lange um das Paket zu übermitteln.

7.2 Hidden Terminals

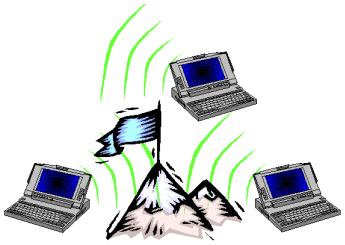

Bild 7.31: Versuchsaufbau

Im Infrastruktur-Modus mit einem Basisport und zwei Mobilstationen ist es nicht möglich mit dem Hidden-Terminal Problem zu experimentieren, da der Basisport als Bridge fungiert: „Im Gegensatz zum Ad-hoc-Modus wird die Funkzelle jedoch immer von der Basis-Station aufgespannt, und jede Station muss sich bei der Basis-Station anmelden, bevor sie Daten in der Funkzelle austauschen darf. Der Basis-Station kommt dabei üblicherweise auch die Funktion einer ‚Relaisstation' für Daten zu."
(Dok1)

7.3 VoIP

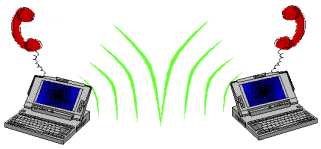

Bild 7.32: Versuchsaufbau

Um das Funktionieren von VoIP auf dem WLAN zu testen haben wir folgende Konstellationen ausprobiert:

7.3.1 Messmethode

Eine Person 1 zählt im Sekundentakt und Person 2 hält ihr Mikrofon an den Kopfhörer. So konnte die Person 1 sozusagen ihr eigenes Echo hören. Das entspricht nun der doppelten Verzögerung die jeweils eine Person empfindet.

7.3.2 Ad-hoc-Modus

In dieser Konstellationen sprechen wir mit NetMeeting Version 3.0 über die 2 Laptops im Ad-hoc-Modus miteinander.

7.3.2.1 Laptops nebeneinander

Die Sprechqualität ist wie erwartet sehr gut. Die Verzögerung ist ungefähr ¼ Sekunden.

7.3.2.2 Laptops in 20 m Entfernung

Der eine Laptop entfernt sich ca. 20m aus dem Raum. Ein Gespräch ist nur noch bedingt möglich. Es entstehen Unterbrüche von ¼...1 Sekunde.

7.3.3 VoIP während FTP

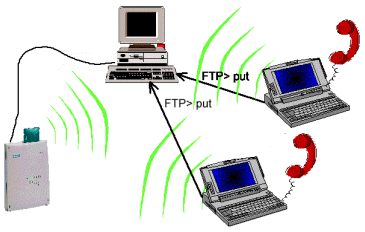

Bild 7.33: Versuchsaufbau

Mit nur einem FTP neben dem Gespräch merkt man keine Verschlechterung. Starten wir jedoch auf beiden Laptops einen FTP so entstehen kurze Unterbrüche. Eine Verständigung ist immer noch möglich.

7.4 Besprechung der Messungen

7.4.1 maximalen Nutzrate

Bei der Betrachtung der eher bescheidenen maximalen Nutzrate ist folgende Liste von Bremseinflüssen zu beachten:

- Kollisionsdetektion DCF bzw. CSMA/CD, ACK, Backoff (Contention Window)...
- RTS/CTS Verkehr
- PLCP, Mac Sublayer:

SYNC 128 bit preample	SFD 16 bits	SIGNAL 8 bits	SERVICE 8bits	LENGTH 16 bits	CRC 16 bits	
PLCP Preample	PLCP Header					Payload MPDU
PPDU						

- 802.11 Mac Frame:

Octets	2	2	6	6	6	2	6	0-2312	4
Frame Control	Duration ID	Address 1	Address 2	Address 3	Se-quence Control	Address 4	Frame Body	CRC	

- Status und Anweisungen des Basisports

Sicher spielen auch noch andere Faktoren eine Rolle.

7.4.2 Mikrowellenofen

Der Mikrowellenofen kann selbst in nächster Nähe die Verbindung nicht vollständig überdecken, was dem DSSS-Protokoll zu verdanken ist. Zu beachten ist dabei, dass kommerzielle Mikrowellenöfen nur während einer Halbwelle senden (siehe 10.3.2) .Mit der Annahme das ein typisches IP-Paket ungefähr 4 ms dauert, passen ungefähr 4 IP-Pakete in diesen Unterbruch des Störsenders.

7.4.3 VoIP

Betrachtet man reine Sprachübertragung, so wird hier eine maximale Umlaufverzögerung von ca. 100 bis 200 Millisekunden als gut, eine Verzögerung von mehr als 800 Millisekunden als nicht tolerierbar

eingestuft. Wir haben unsere Verzögerungen auf 250 bis 1000 Millisekunden eingeschätzt, was mittel gut bis miserabel entspricht.

7.4.4 Paketgrösse

Die Angabe der Paketgrösse resp. Packet Size in der Konfiguration des Basisports wurde von uns während des Messen immer als effektive Paketgrösse verstanden. An der Demonstration unseres Projektes wurden wir dann jedoch aufgeklärt, dass es sich bei dieser Grösse um ein RTS/CTS-Umschaltgrösse handelt. D. h. bei Paketen, die grösser als diese RTS/CTS-Umschaltgrösse sind, wird der Ready to Send/Clear to Send-Handshake angewendet. Da die Fragmentierung durch den Windows TCP/IP-Treiber (bzw PGP-Treiber) geschieht, haben wir leider keine Kontrolle über die IP-Paketgrösse.

7.4.5 Infrastructure Mode

An der Demonstration unseres Projektes wurde unsere Vermutung, dass das Basisport im Infrastructure-Mode alle Pakete weiterleitet und somit immer als Relais funktioniert bestätigt. Schön illustriert das der Testfall 7.1.8

8 Konfiguration über Telnet

Die Konfiguration der Basisstation erfolgt über Telnet, Terminal-Programme sowie über SNMP.

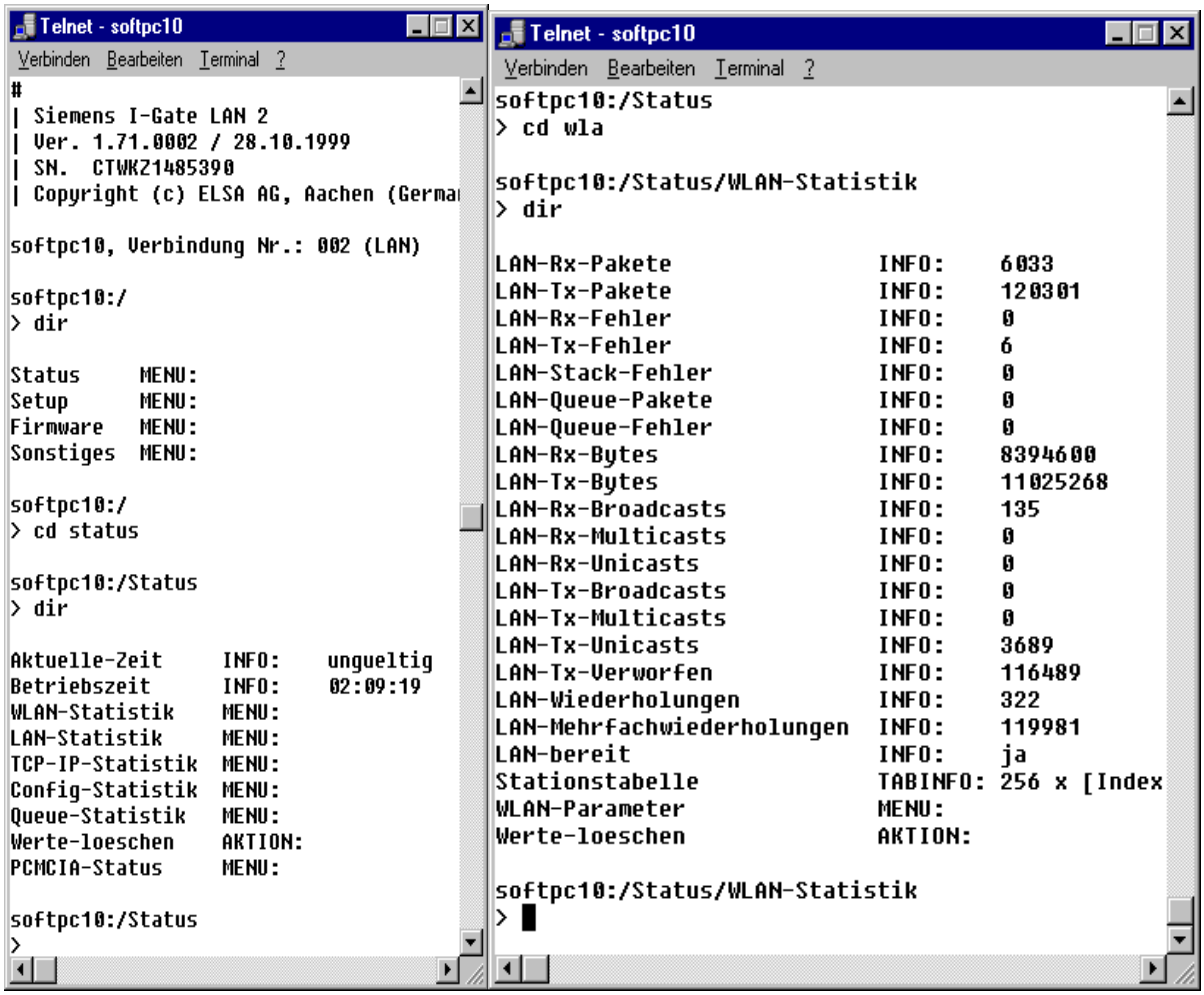

Bild 8.1: Telnet Beispiele

9 Quellenverzeichnis

Zur Einarbeitung in die Thematik haben wir uns verschiedener Medien bedient.

9.1 Dokumentationen

- *DOK1:* I-GATE_LAN_2_9911_03.pdf (1.8MB)
  (Technische Grundlagen, Beschreibung der Menupunkte, Protokolle) Ver.0:20.04.98/Ver. 31:15.10.99
  kann gefunden werden auf: http://www.siemens.ch/icw/produkte/prod_igate_support.htm

9.2 Internet

- *URL1:* Dipl.-Ing. Rolf-Günter Hauk & Wireless LAN: IEEE 802.11
  http://www.hauk.vogelsberg-online.de/vorschri.htm
- *URL2:* IS95 -- ein Direct Sequence Spread Spectrum CDMA-System
  http://www.nesi.e-technik.tu-darmstadt.de/uli/L/node45.html
- *URL3:* Wireless LAN : Rudi,MMT, Fraunhofer IGD, Rostock
  http://www.egd.igd.fhg.de/fhg_igd/abteilungen/a3/PROJECTS/Wlan/wireless_d.html#DSSS
- *URL4: PGPnet oder "Die Konfiguration und Anwendung des VPN PGPnet"*
  http://www.cce-bbs.net/pgp/pgp13.html
- *URL5:* Hidden terminal problem:
  http://gaia.cs.umass.edu/kurose/ethernet/80211.htm
- *URL6:* Spectrum produced by Magnetron
  http://www.ee.sun.ac.za/ehg/imeier/supply_spectra.html
- *URL7:* The Magnetron Tube
  http://www.gallawa.com/Microtech/magnetron.html
- *URL8:* Drahtlose Hochleistungskommunikation
  http://www-student.informatik.uni-bonn.de:8001/~karl/wlan/index.html
- *URL9:* Probleme bei drahtlosen LANs:
  http://www-student.informatik.uni-bonn.de:8001/~karl/wlan/probleme.html

10 Anhang

10.1 Glossar

- **CSMA/CD(carrier sense multiple access with collision detection)**
  Zugangsverfahren mit Leitungsabfrage und Kollisionserkennung (Listen WhileTalking) nach einer Random-Access-Methode, das bei Lokalen Netzen (LAN) in Bustopologie mehreren Netzwerk-stationen den Zugriff auf das Übertragungsmedium regelt.
- **PLCP(Physical Layer Convergence Protocol)**
- **PHY (Physical Layer)**
  Text.
- **MAC (Medium Access Control)**
  Text
- **CAST(Carlisle Adams Stafford Tavares)**
  CAST ist ein freier, schnell arbeitender Algorithmus mit einer Keygrösse von 128-bit, der noch nicht so lang und gut untersucht ist wie IDEA
- **TripleDES(data encryption standard)**
  Beim TripleDES - Algorithmus handelt es sich um eine sogenannte Produktverschlüsselung, bei der als elementare Verschlüsselungen und Transpositionen verwendet werden.
- **MD5 und SHA-1-Algorithmus**
  MD5 und SHA-1 sind in Authentifikatioinsprotokollen verwendete Algorithmen , die auf einer Einwegübertragung mittels Hash-Funktionen und eines Schlüssels basiert.
- **MPDU(MAC protocol data unit)**
- **WM(wireless medium)**
  Damit ist die Luft gemeint.
- **EI(ETSI)**
  European Telecommunications Standard Industrie Europäisches Gremium das u.a. den DECT-Standard festgeschrieben hat.

10.2 Detaillierte Messwerte und Geräteinformationen

10.2.1 Kanäle und Frequenzen

Kanal.Nr	Mittelfrequenz[MHz]	EI(ETSI) -Zulassung
1	2412	Ja
2	2417	Ja
3	2422	Ja
4	2427	Ja
5	2432	Ja
6	2437	Ja
7	2442	Ja
8	2447	Ja
9	2452	Ja
10	2457	Ja
11	2462	Ja
12	2467	Ja
13	2472	Ja
14	2484	Nein

Bild 10.1: Kanäle und Frequenzen nach IEEE 802.11

10.2.2 Kanalbreite

Da das DSSS-Signal eine Breite von 22 MHz hat, sind im selben Umfeld nur 3 Kanäle gleichzeitig nutzbar. Im I-Gate Benutzerhandbuch. werden darum die Kanäle 3, 8 und 13 empfolen.

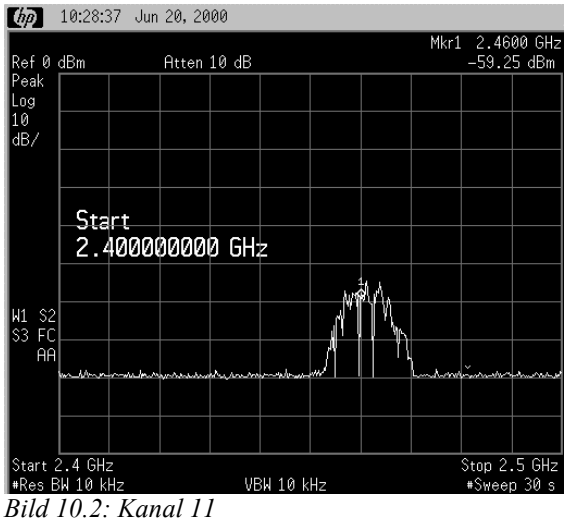

Bild 10.2: Kanal 11

10.2.3 Detaillierte Messwerte Serie 1

Messung	Zeit in s	Übertragungs- rate in kByte/s	Paketlänge	CPU Auslastung in %	Ipsec
1	58.05	172.24	1550	<10	Nein
1	57.89	172.74	1550	<10	Nein
1	57.88	172.79	1550	<10	Nein
2	58.06	172.24	1000	<10	Nein
2	58.6	170.65	1000	<10	Nein
2	58.77	170.13	1000	<10	Nein
3	66.18	151.10	1550	~20	CAST
3	65.96	151.61	1550	~22	CAST
3	66.41	150.58	1550	~20	CAST
4	68.82	145.31	1000	~10	CAST
4	67.67	147.78	1000	~27	CAST
4	67.17	148.88	1000	~30	CAST
5	66.84	149.61	1550	~25	3DES
5	67.45	148.26	1550	~24	3DES
5	66.95	149.37	1550	~24	3DES
6	66.46	150.47	1000	~24	3DES
6	66.19	151.08	1000	~24	3DES
6	67.01	149.23	1000	~25	3DES
7 Laptop 1	98.48		1550		Nein
7 Laptop 2	115.45		1550		Nein
7 Laptop 1	100.51		1550		Nein
7 Laptop 2	115.40		1550		Nein
7 Laptop 1	98.32		1550		Nein
7 Laptop 2	115.01		1550		Nein
8	167.5	59.69	1550	~63	Nein
8	172.42	58.34	1550	~67	Nein
8	145.27	68.84	1550	~68	Nein
9	144.07	69.41	1000	~67	Nein
9	226.18	44.21	1000	~70	Nein
9	143.52	69.68	1000	~67	Nein
9	138.80	72.05	1000	~65	Nein
9/600	201.24	49.69	600	~67	Nein

10	559.91	17.86	1550	~72	Nein
10	426.44	23.45	1550	~71	Nein
11	117.93	84.80	1550	~44	Nein
11	156.53	63.89	1550	~38	Nein
11	125.12	79.92	1550	~29	Nein
12	75.73	132.40	1550	~33	Nein
12	67.55	148.04	1550	~35	Nein
12	70.91	141.02	1550	~38	Nein
13 Laptop 1	222.67		1550	~47	Nein
13 Laptop 2	281.27		1550	~67	Nein
13 Laptop 1	226.08		1550	~38	Nein
13 Laptop 2	269.24		1550	~45	Nein
13 Laptop 1	212.94		1550	~32	Nein
13 Laptop 2	254.52		1550	~47	Nein

Bild 10.4: Serie 1

10.2.4 Detaillierte Messwerte Serie 2

Messung	Kanal	Zeit 1	Rate 1	Zeit 2	Rate 2	Zeit 3	Rate 3	Zeit Durchschnitt	Rate Durchschnitt
14	1	58.43 s	171.14 KB/s	58.55 s	170.79 KB/s	58.33 s	171.44 KB/s	58.44 s	171.13 KB/s
15	2	58.28 s	171.59 KB/s	58.22 s	171.76 KB/s	58.17 s	171.91 KB/s	58.22 s	171.75 KB/s
16	3	58.22 s	171.76 KB/s	58.17 s	171.91 KB/s	58.12 s	172.06 KB/s	58.17 s	171.91 KB/s
17	4	58.45 s	171.09 KB/s	57.95 s	172.56 KB/s	58.50 s	170.94 KB/s	58.30 s	171.53 KB/s
18	5	58.17 s	171.91 KB/s	58.31 s	171.50 KB/s	58.17 s	171.91 KB/s	58.22 s	171.77 KB/s
19	6	60.63 s	164.93 KB/s	59.71 s	167.48 KB/s	62.18 s	160.82 KB/s	60.84 s	164.37 KB/s
20	7	74.76 s	133.76 KB/s	80.74 s	123.85 KB/s	70.31 s	142.23 KB/s	75.27 s	132.86 KB/s
21	8	70.63 s	141.58 KB/s	84.20 s	118.76 KB/s	79.89 s	125.17 KB/s	78.24 s	127.81 KB/s
22	9	66.90 s	149.48 KB/s	69.70 s	143.47 KB/s	66.79 s	149.72 KB/s	67.80 s	147.50 KB/s
23	10	59.92 s	166.89 KB/s	61.24 s	163.29 KB/s	59.43 s	168.27 KB/s	60.20 s	166.12 KB/s
24	11	58.17 s	171.91 KB/s	58.22 s	171.76 KB/s	59.42 s	168.29 KB/s	58.60 s	170.64 KB/s
25	12	58.61 s	170.62 KB/s	58.16 s	171.94 KB/s	58.27 s	171.61 KB/s	58.35 s	171.39 KB/s
26	13	58.39 s	171.26 KB/s	58.49 s	170.97 KB/s	58.11 s	172.09 KB/s	58.33 s	171.44 KB/s
27	1	58.12 s	172.06 KB/s					58.12 s	172.06 KB/s
28	2	58.39 s	171.26 KB/s					58.39 s	171.26 KB/s
29	3	58.33 s	171.44 KB/s					58.33 s	171.44 KB/s
30	4	58.06 s	172.24 KB/s					58.06 s	172.24 KB/s
31	5	58.27 s	171.61 KB/s	58.55 s				58.41 s	171.20 KB/s
32	6	61.96 s	161.39 KB/s	63.82 s	156.69 KB/s	63.11 s	158.45 KB/s	62.96 s	158.82 KB/s
33	7	72.28 s	138.35 KB/s	71.24 s	140.37 KB/s	74.70 s	133.87 KB/s	72.74 s	137.48 KB/s
34	8	71.29 s	140.27 KB/s	70.30 s	142.25 KB/s	71.62 s	139.63 KB/s	71.07 s	140.71 KB/s
35	9	66.57 s	150.22 KB/s	65.80 s	151.98 KB/s	74.76 s	133.76 KB/s	69.04 s	144.84 KB/s
36	10	64.15 s	155.88 KB/s	62.34 s	160.41 KB/s	62.72 s	159.44 KB/s	63.07 s	158.55 KB/s
37	11	58.27 s	171.61 KB/s	58.39 s	171.26 KB/s			58.33 s	171.44 KB/s
38	12	58.61 s	170.62 KB/s					58.61 s	170.62 KB/s
39	13	58.33 s	171.44 KB/s					58.33 s	171.44 KB/s
40	10	57.94		58.39		58.49			
41	10	58.44		58.71					
42	10	58.77		57.95					
43	10	114.63		73.66		68.6			

44	10	103.86		100.12		74.48			

Bild 10.5: Serie 2

10.2.5 Geräteinformationen

Laptops:	MAXDATA Vision 340C Celeron 566MHz, 12,1", WIN-98
ServerPC:	Pentium3-550, 128MB Ram, Windows NT mit Option Pack
BasisPort:	Siemens I-Gate Serie-Nr.: CTWKZ14853090, Firmware 1.71.0.0002, Hardware-Release A
Funk-Netzwerkkarte:	Siemens I-Gate 10-992100165 (alle Einzelmessungen), Firmware 2.0.6, Windowstreiber 4.10.2222(3.3.2000) Siemens I-Gate V4411-Z3-X11, Firmware 2.0.6, Windowstreiber 4.10.2222(3.3.2000)
Mikrowellenofen:	Novamatic MW1800, Ausgangsleistung 800 Watt

10.3 Email mit Ingolf Meier

Electro-Heating Laboratory
Department of Electrical and Electronic Engineering
University of Stellenbosch
Stellenbosch 7600
South Africa
IMeier@ing.sun.ac.za

10.3.1 Unsere Anfrage

Sehr geehrter Herr Meier
Bei meiner Frage geht es mehr um die Einflüsse in der Luft. Wir sind an einem Wireless LAN am messen und benutzen da einen Mikrowellenofen als Störquelle. Da haben wir gemerkt, auch wenn das Mikrowellengerät das Spekrum unseres Wireless LAN völlig zudekt, dass die TCP-Packete trotzdem ankommen, einfach viel langsamer. **Wir haben dann vermutet, dass der Mikrowellenofen nur während einer Halbwelle sendet und während der 2. gar nicht stört.**
Wir wollten da Sie als Experte fragen, ob wir da mit unseren Vermutungen richtig sind,oder ob das ein anderer Effekt sein muss.
Mit freundlichen Grüssen aus der Schweiz Mario Gersbach

10.3.2 Antwort

Hallo Mario!
Ihre Vermutung ist richtig.Gut das Sie wireless LAN erwaehnen. Ich mache mal die wilde Vermutung das
Spread Spectrum oder aehnlich benutzt werden. Dann naehmlich gibt es noch einen 'Zwischenraum' in dem Sie uebertragen koennen.
Angehaeftet habe ich ein GIF Bild in dem daegestellt sind:

- Gruen: **Spannung von einer Detector Diode in Mikrowellenfeld. Diese Liene hat eine Relation zur Ausgesendeten Leistung des Magnetrons.**
- Blau: Anodenstrom
- Rot: Cathodenspannung

Die Netsfrequenz in Sued-Afrika ist 50Hz, was man auch dem Graphen entnehmen kann. Von diesem Graphen koennen Sie sehen wann das Magnetron sendet, naemlich nur wenn knapp ueber -4000V unterschritten werden. Das heisst das fuer etwas mehr als 1/50 Sekunden die Roehre aus ist. Genau wovon Sie sprachen. In dem Bereich in dem sie an ist tritt Frequenzmodulation durch die Strohmstaerke auf. Das heisst

das nicht das gesammte Band immer gleichzeitig gestoehrt ist! Nur immer eine Frequenz zur Zeit!! (Kann man nicht auf dem Spektrumanalysator sehen, aber wenn Sie das Signal heruntermixen und es auf einem schnellen Oscilloscope betrachten werden Sie es sehen.) Auch werden Sie von der gruenen Linie im Graphen sehen das die Ausgangsleistung sehr unterschiedlich ist ... Spitzenleistung bei ungefaehr 5kW in einem 800W Ofen ... ist ja nur ein Mittelwert von 800W!!!!
Also es liegt ein Kombinierter Effekt vor vermute ich.Als breitbandige Stoehrquelle ist das Mikrowellenmagnetron also nicht so eine gute Idee vermute ich mal. Es wird zwar die am haeufigsten auftretende sein, aber eventuell ist eine 'White Noise Source' das etwas besser, oder was auch gut geht ein VCO der mit einem Random Signal schnell moduliert wird (ging ganz gut bei 900MHz um Handies zu stoehren), ist aber eigentlich FM modulation.
Ich hoffe die Antwort hilft, sonst einfach nachfragen.
Viele Gruesse, Ingolf

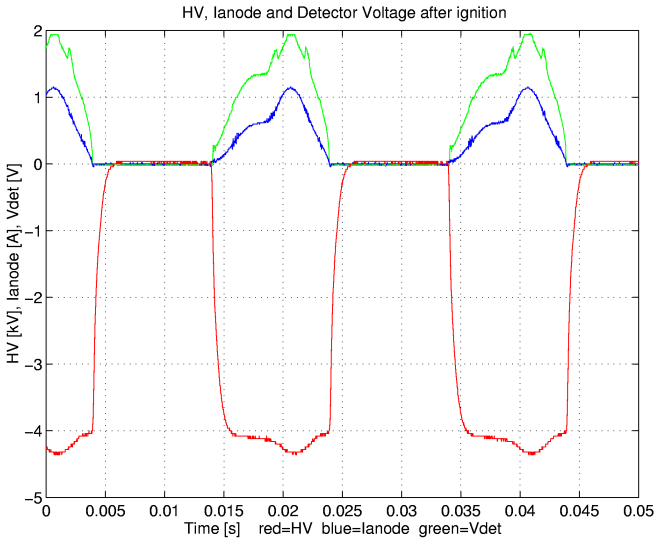

Bild 10.6: Attachment

10.4 Zeiterfassung

10.4.1 M. Gersbach

Datum	Aktion	investierte Zeit
23. Mai 2000	PA entgegen nehmen, Arbeitsplatz installation, einarbeiten in I-Gate	5 h
24. Mai 2000	Notebook installieren, IEEE 802.11 bis Kapitel 5 gelesen	4 h
25. Mai 2000	I-Gate inatallieren:at hoc	4 h
26. Mai 2000	Netmeeting funktioniert, Anbindung ans Schulnetz fehlgeschlagen	5 h
29. Mai 2000	Anbindung ans Schulnetz funktioniert	6 h
30. Mai 2000	PGP verschlüsselt, Telnetgehversuche, Rollcage	4 h
31. Mai 2000	PGP Doku	2 h
2. Mai 2000	Telnet, PGP Doku	3 h
6. Juni 2000	PGP zum Zweiten	3 h
8. Juni 2000	Besprechung der Messungen, Doku	4 h
16. Juni 2000	Doku, Messungen	3 h

19. Juni 2000	Messungen CAST	3	h
20. Juni 2000	Messungen Microwelle Doku	7	h
22. Juni 2000	Besprechung der Messungen, Doku	3	h
23. Juni 2000	Nachbarkanäle 6 m	3	h
26. Juni 2000	Nachbarkanäle 6 m, Doku, Bildli	5	h
27. Juni 2000	hidden terminal	6	h
7. Juli 2000	Kommentar zu Messungen	3	h
10. Juli 2000	Doku, ad-hoc Messungen	5	h
11. Juli 2000	Vorwort,Doku fertig	3	h
12. Juli 2000	Präsentation vorbereiten	3	h
14. Juli 2000	Präsentation	4	h

Bild 10.7: Zeiterfassung

10.4.2 M. Kunz

Datum	Aktion	Zeit
23. Mai 2000	Ausgabe der PA, Inbetriebnahme der Notbooks, Einlesen in die Materie	6 1/2 h
25. Mai 2000	1. Aufsetzen des Netzwerks	4 h
26. Mai 2000	NetMeeting in Betrieb nehmen, Besprechung mit Steffen	4 1/2 h
29. Mai 2000	Anbindung ans Schulnetz funktioniert	6 h
30. Mai 2000	Besprechung mit Steffen, PGP Inbetriebnahme	4 h
2. Juni 2000	I-Gate-Treiber und Firmware ubdaten --> die Netzwerkverbindung läuft viel besser	3 h
5. Juni 2000	Telnet ausprobieren, studieren	3 1/2 h
6. Juni 2000	Doku	5 h
8. Juni 2000	Besprechung der Messungen, Doku	4 h
16. Juni 2000	Doku, Messungen	3 h
19. Juni 2000	Messungen CAST	3 h
20. Juni 2000	Messungen Mikrowelle, Doku	7 h
22. Juni 2000	Besprechung der Messungen, Doku	3 h
23. Juni 2000	Mikrowellenmessung: Nachbarkanäle 6 m	3 h
26. Juni 2000	Mikrowellenmessung: Nachbarkanäle 6 m, Doku, Bilder	5 h
27. Juni 2000	hidden terminal	6 h
4. Juli 2000	Besprechnung mit Steffen, Doku	3 h
10. Juli 2000	Doku korrigieren, Bilder	6 h
11. Juli 2000	Besprechung mit Steffen, Präsentation vorbereiten	6 h
13. Juli 2000	Präsentation vorbereiten	3 h
14. Juli 2000	Präsentation	4 h
18. Juli 2000	Dokumentation fertigstellen	6 h

Bild 10.8: Zeiterfassung

10.5 Vollständige Aufgabenstellung: VoIP und IPsec über ein Wireless LAN

Studierende:

- Mario Gersbach, IT3b
- Marcel Kunz, IT3b

Termine:

- Ausgabe: Dienstag, 23.05.2000 10:00 - 11:00 im E509
- Abgabe: Freitag, 21.07.2000

Beschreibung:

Sinkende Preise machen die auf dem IEEE 802.11 Standard basierenden Wireless LANs immer attraktiver. Allerdings ist sich der Benutzer an den Datendurchsatz und die Verzögerungszeiten eines IEEE 802.3 Ethernet basierten LANs mit Bitraten von 10-100 Mbps gewöhnt und stellt automatisch entsprechende Vergleiche an.

Diese Projektarbeit soll abklären, mit welchem aktuellen Durchsatz und welchen Verzögerungszeiten beim praktischen Betrieb eines 2 Mbps WLANs gerechnet werden muss. Dabei soll die spezielle Situation berücksichtigt werden, dass sich oft nicht alle WLAN-Teilnehmer gleichzeitig hören können (Hidden Terminal Problem). Weiter soll der eventuell störende Einfluss eines im 2.5 GHz ISM-Band betriebenen Mikrowellenofens abgeklärt werden.

Voice over IP Anwendungen sind im Kommen. Es soll untersucht werden, ob die wesentlich grösseren Packetverzögerungsschwankungen eines WLANs einen nennenswerten Einfluss auf die Qualität einer drahtlosen VoIP Verbindung haben.

Drahtlose LANs können leicht abgehört werden und gelten deshalb als nicht sicher. Die optionale Verschlüsselung mit einem 40 bit RC4 Stream Cipher trägt auch nicht viel zur Vertrauensbildung bei. Es soll untersucht werden, ob eine IPsec Verbindung bei drahtloser Übertragung irgendwelche Probleme mit sich bringt.

Aufgaben:

- Funktionsweise eines IEEE 802.11 Wireless LANs studieren
- Siemens I-Gate installieren, SW Upgrade auf Version 1.1 vornehmen
- Microsoft Netmeeting 3.01 und PGPnet 6.5.3 installieren
- Situation 1 (keine Hidden-Terminals)
    - I-Gate LAN Basisport mit Ethernet Verbindung zu einem Server
    - Notebook PCs A und B im Infrastructure Mode, sehen sich gegenseitig.
- Situation 2 (Hidden Terminals)
    - I-Gate LAN Basisport mit Ethernet Verbindung zu einem Server
    - Notebook PCs A und B im Infrastructure Mode, sehen sich gegenseitig nicht
- Experimente zum Hidden-Terminal Problem
    - Referenzmessung für Datendurchsatz Server->PC in Situation 1:
        - Paralleles Filecopy Server-> PC A und Server -> PC B, Zeit stoppen
        - I-Gate Packetlänge 1000, 1550 und 2000 Bytes (Einstellung an MP und AP)
    - Datendurchsatz in Situation 2 messen
        - Paralleles Filecopy Server -> PC A und Server -> PC B, Zeit stoppen
        - I-Gate Packetlänge 1000, 1550 und 2000 Bytes (Einstellung an MP und AP)
- Experimente mit Mikrowellenofen
    - Gleiche Tests wie zum Hidden-Terminal Problem, aber ein Mikrowellenofen in der Nähe des LAN Basisports (AP) oder eines Notebook PCs (MP).

- Experimente mit PGPnet
  - Gesicherte Verbindungen zwischen den PCs und zwischen Server und PCs
  - Eventuell auftretende Probleme erfassen und beschreiben.
- Experimente mit Voice over IP
  - VoIP Verbindungen zwischen den PCs und zwischen Server und PCs herstellen
  - NetMeeting Dreierkonferenz mit beiden Notebook PCs und Server
  - Mittels Datentransfer I-Gate Kapazität sättigen, Einfluss auf VoIP feststellen.
- Vollständige Dokumentation aller Experimente (Messaufbau, Messresultate)
- Eigene Schlussfolgerungen und Empfehlungen

Infrastruktur / Tools:

- Raum: **E507**
- Rechner: 2 Notebook PCs mit Windows 98, 2 PCs mit Windows NT 4.0
- SW: I-Gate SW, Microsoft NetMeeting 3.01, PGPNet 6.5.3 VPN Client
- WLAN: I-Gate 2 Mbps LAN Bridge, I-Gate 2 Mbps PCMCIA Cards
- Störer: 800 W Mikrowellenofen
- Messgeräte: HP Spectrumanalyzer, Wandel & Goltermann LANalyzer

Literatur / Links:

- Siemens I-Gate Site
  http://www.siemens.ch/i-gate/
- Siemens I-Gate SW Release V1.1
  http://www.siemens.ch/icw/igate/support/support.htm#sw_release
- IEEE 802.11 Wireless LAN Tutorial
  ftp://stdsbbs.ieee.org/pub/802_main/802.11/tutorial/index.html
- IEEE 802.11 Wireless LAN Standard, Draft 9.0, 18. Nov. 1998
  Wireless LAN Medium Access Control and Physical Layer Specifications
- Microsoft NetMeeting 3.01
  http://www.microsoft.com/windows/netmeeting/
- PGPnet 6.5.3 US Freeware Version
  http://www.pgpi.com