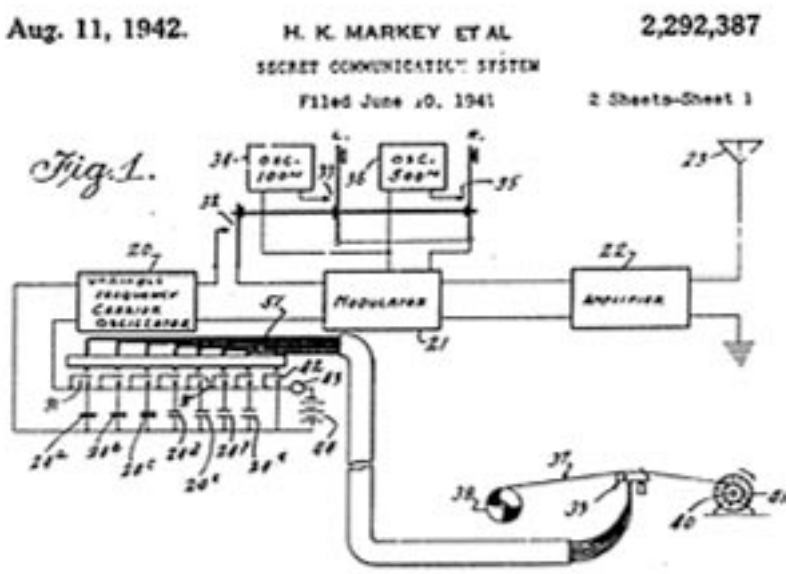
Funknetz an der Universität Konstanz

Version 1.0

Stephan Pietzko
stephan.pietzko@uni-konstanz.de

Kurzeinführung – Buzzwords

- Funknetz, Wireless LAN, Wireless Network, WLAN, WaveLAN, 802.11b sind alles Synonyme
- 802.11b hat nichts mit DECT, Bluetooth, HomeRF, WAP, UMTS, iMode, GPS, 433 MHz zu tun
- ISM 2,4 GHz Band (2400 - 2483,5MHz)
- IEEE 802.11 (1997) Modulationen FHSS (Frequency Hopping Spread Spectrum), DSSS (Direct Sequence Spread Spectrum) und IR (Infrarot); 1 und 2 Mbps
- Max. Sendeleistung 100 mW ERIP (Effective Isotropically Radiated Power)
- Das WirelessLAN deckt die ersten eineinhalb Layer im OSI-Model ab und erscheint dem Betriebssystem wie ein normaler Netzwerkanschluss. 802.11 an sich arbeitet mit CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)



Kurzeinführung – 802.11b

- Man braucht einen Laptop mit PCMCIA-Funkkarte und ein Stück Software

- Zwei Modi: “Ad hoc mode” (IBSS) – zwei Laptops direkt und “Infrastructur mode” (BSS und ESS) – mehrere Laptops und ein Access Point (AP)

FHSS und IR sind mit der Erweiterung auf 802.11b hinfällig geworden

- Heute nur IEEE 802.11b (1999) DSSS (Direct Sequence Spread Spectrum); 1, 2, 5.5, 11 Mbps

- Das Band ist in Europa in 13 Kanäle aufgeteilt, mit denen man Aufgrund des Spreizbandes auf
3 nichtüberlappenden Frequenzen senden kann.

- Reichweiten auf der grünen Wiese ca. 300m, im Büro ca. 80m und bei viel Stahlbeton auch deutlich weniger. Mit besonderen Antennen und Sichtverbindung sind auch mal 20km möglich.

- Die Ausbreitung läuft oft mehr über Reflexion als über Durchdringung. Sie entspricht in etwa einer Mischung aus optischer und akustischer Ausbreitung.

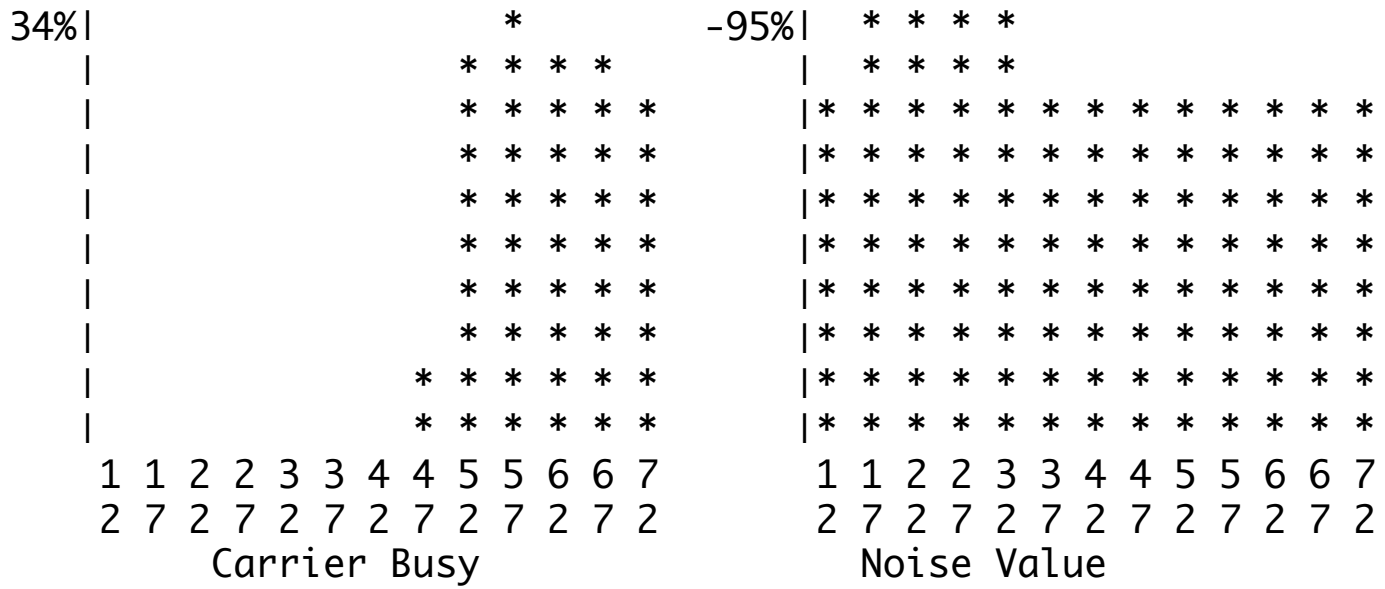
- zwei Fraktionen: Intersil (Cisco, Proxim, 3Com ...) und Lucent (Apple, Hewlett Packard, IBM ...)

Kurzeinführung – Geschichte

- Die Schauspielerin Hedy Lamarr und der Musiker George Antheil erfanden Frequency Hopping und erhielten dafür 1942 ein Patent in den USA.

- Aloha-Net 1969 war die Hawaiianische Variante des Arpanet/Ethernet und nimmt viele moderen Ansätze vorweg

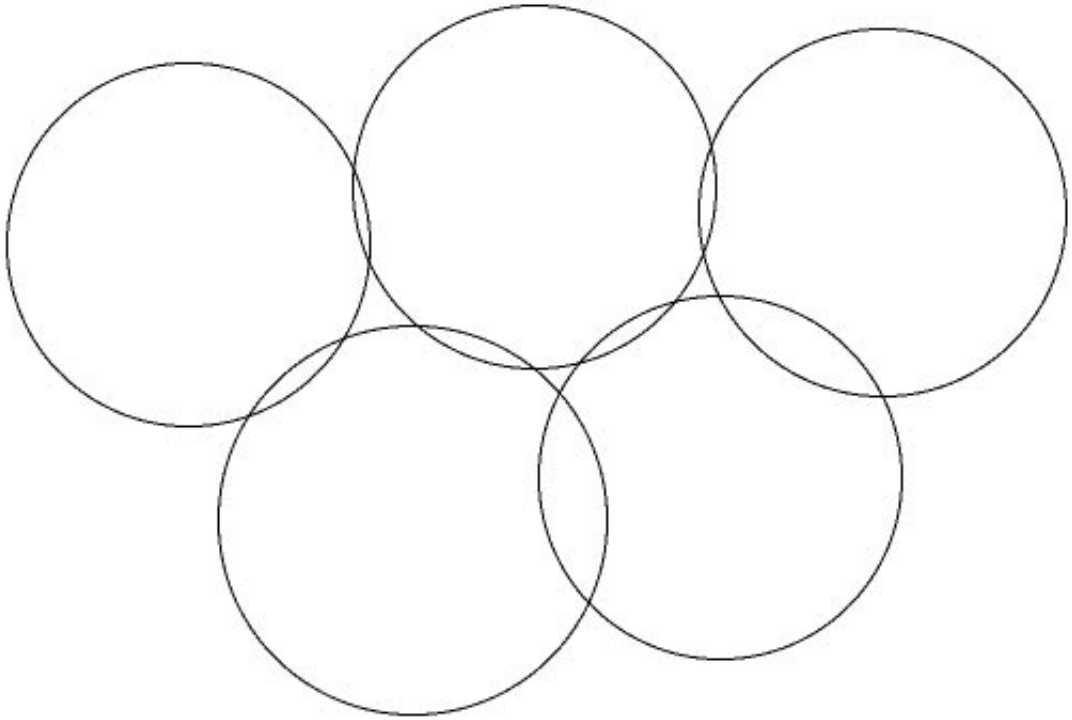
Standardfehler I – Kanalabstand



Access Point sendet auf 2,472MHz (Kanal 13) ...
das heisst, dass selbst 3 Frequenzen parallel eng werden.

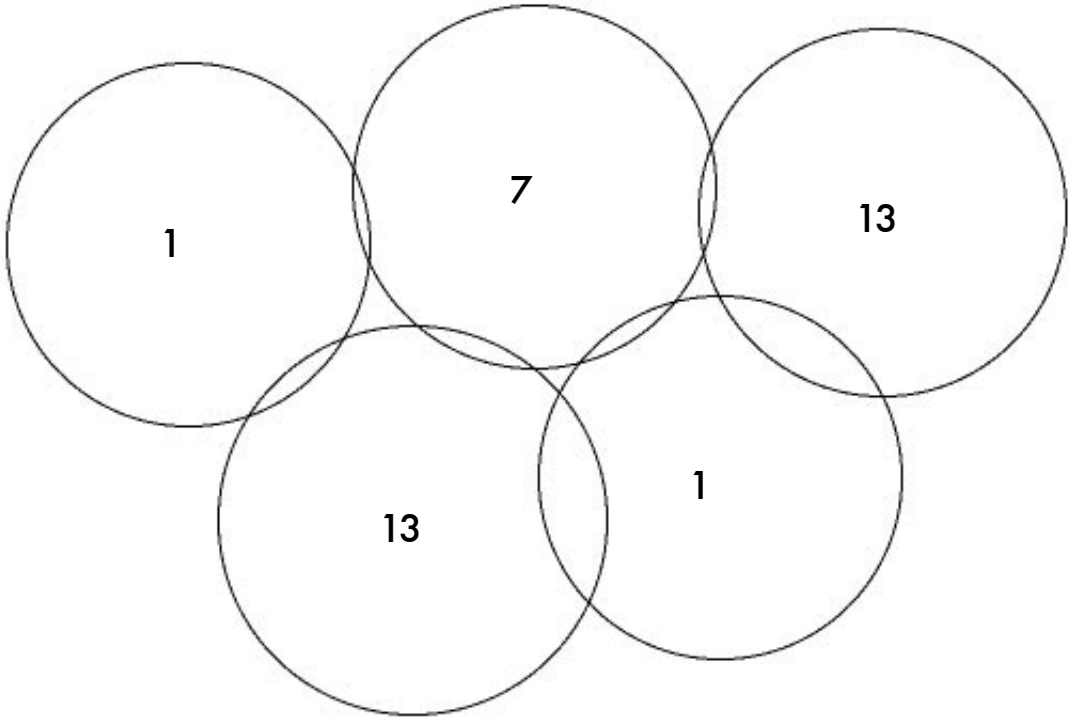
Standardfehler II – räumlicher Abstand

- Man will einen Bereich mit Wireless LAN versorgen und nimmt dazu einige Access Points



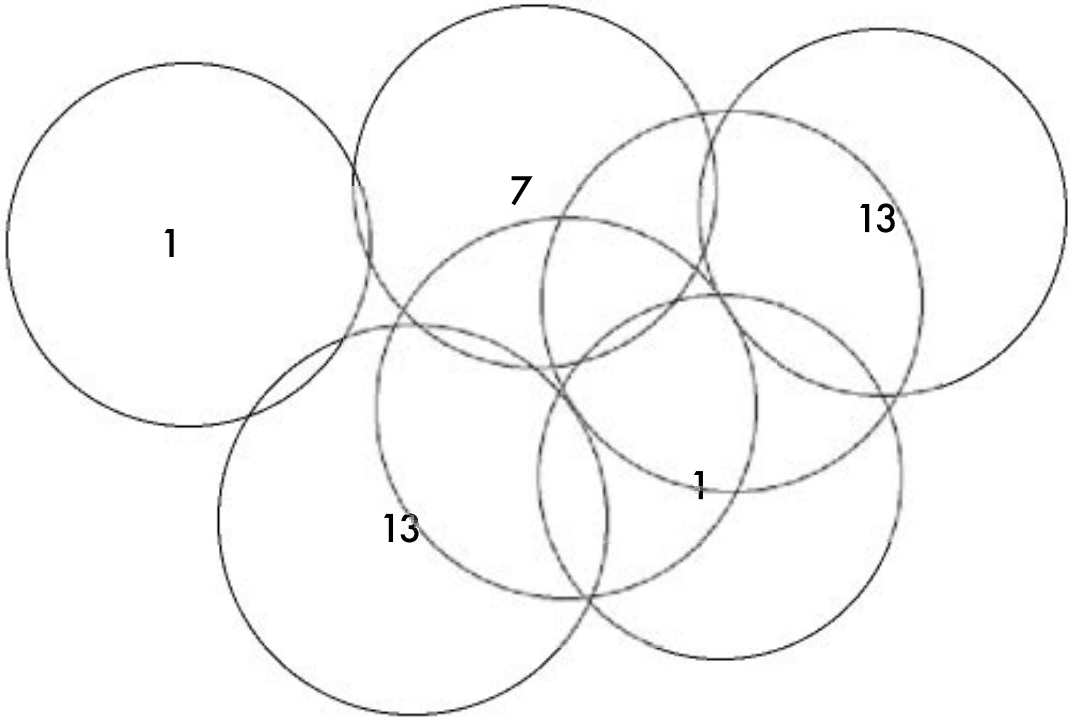
Standardfehler II – räumlicher Abstand

- Man will einen Bereich mit Wireless LAN versorgen und nimmt dazu einige Access Points



Standardfehler II – räumlicher Abstand

- Man will einen Bereich mit Wireless LAN versorgen und nimmt dazu einige Access Points

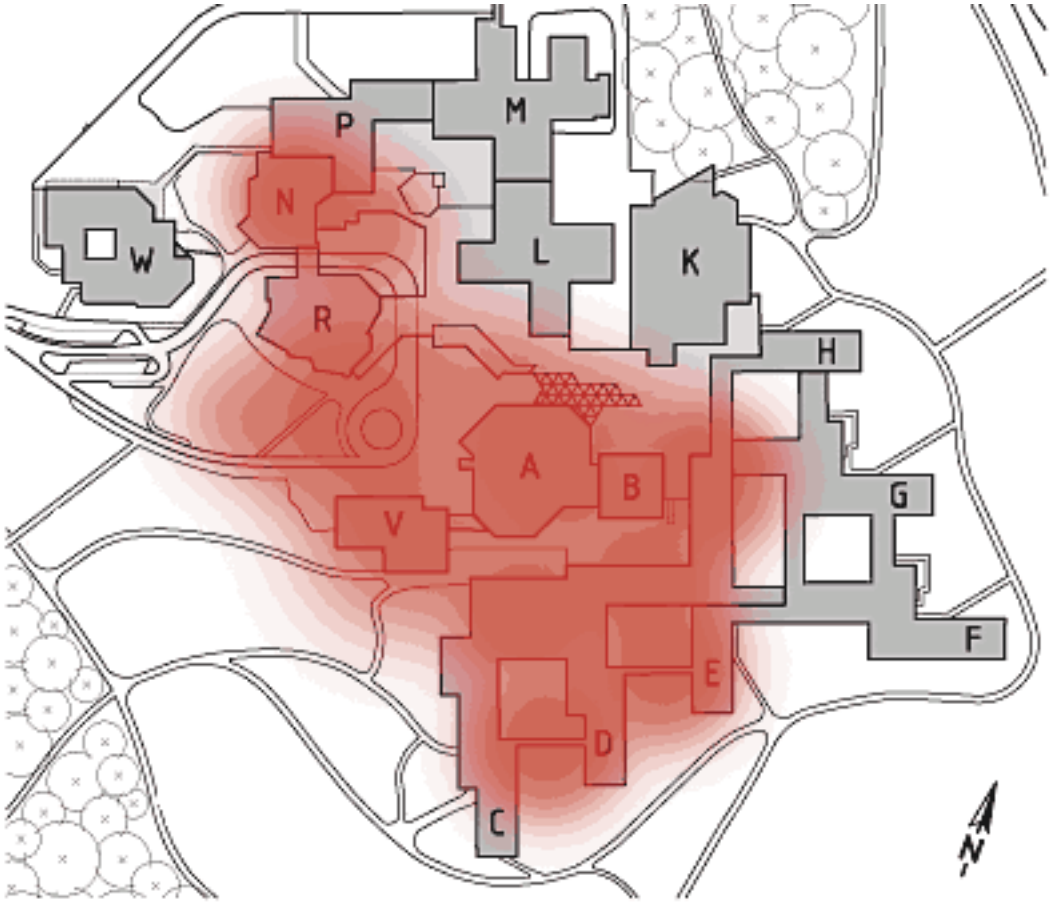


- In der Realität sieht das meist schlimmer aus, da die Zellen zerklüftet und oft viel enger sind. Allerdings fällt das erst unter Last auf.

Universität Konstanz

Universität Konstanz

Universität Konstanz – Strategien



- Versorgung der offenen Bereich ohne klassische Kupferverkabelung, kein Ersatz für die normale Verkabelung
- komplette Versorgung der Bibliothek
- möglichst keine gegenseitigen Störungen
- Funkzellen werden Sicherheitstechnisch als "Außen" betrachtet
- Integriertes Konzept für die Authentifizierung und das LAN-Management; Durchgriff auf die zentrale Benutzerdatenbank
- Keine Hardware und kein Betriebssystem soll ausgeschlossen werden; Einsatz von offenen Standards. Wir versuchen zumindest Windows, Mac OS, Linux und BSD zu unterstützen.
- Die Benutzer dürfen frei surfen, solange wir wissen an wen wir uns bei Problemen wenden müssen.

Universität Konstanz – Erfahrungen

- Die Uni hat Funk seit Ende 2000

- Funkhoheit ist zentral verwaltet, d.h. keiner darf mit Access Points drauflos-funken

- Generell muss man ein grösseres Funknetz planen bzw. vor Ort messen.

- Das Funknetz ist ein eigenes abgeschlossenes Netzwerk, aus dem man nur nach Authentifizierung via IPSec oder (PPTP) rauskommt.

- Die Versorgung der weniger begüterten Studenten mit Laptops ist kaum lösbar! (Mit Geld Laptops verschenken, auf günstigere Preise warten oder mit den Herstellern gute Preise aushandeln)

Universität Konstanz – Bibliothek

- Konstanzer Uni Bibliothek: größte Freihandbibliothek Deutschlands, rund um die Uhr geöffnet, von Anfang an EDV-gestützt und seit Ende 2000 mit Funknetz

- Die Bibliothek ist ein verschlungener Ring quer durch die ganze Uni.

- Viel Stahlbeton und Glas (incl. Drahtglas)

- Die Bibliothek wird mit 5 Access Points komplett versorgt.

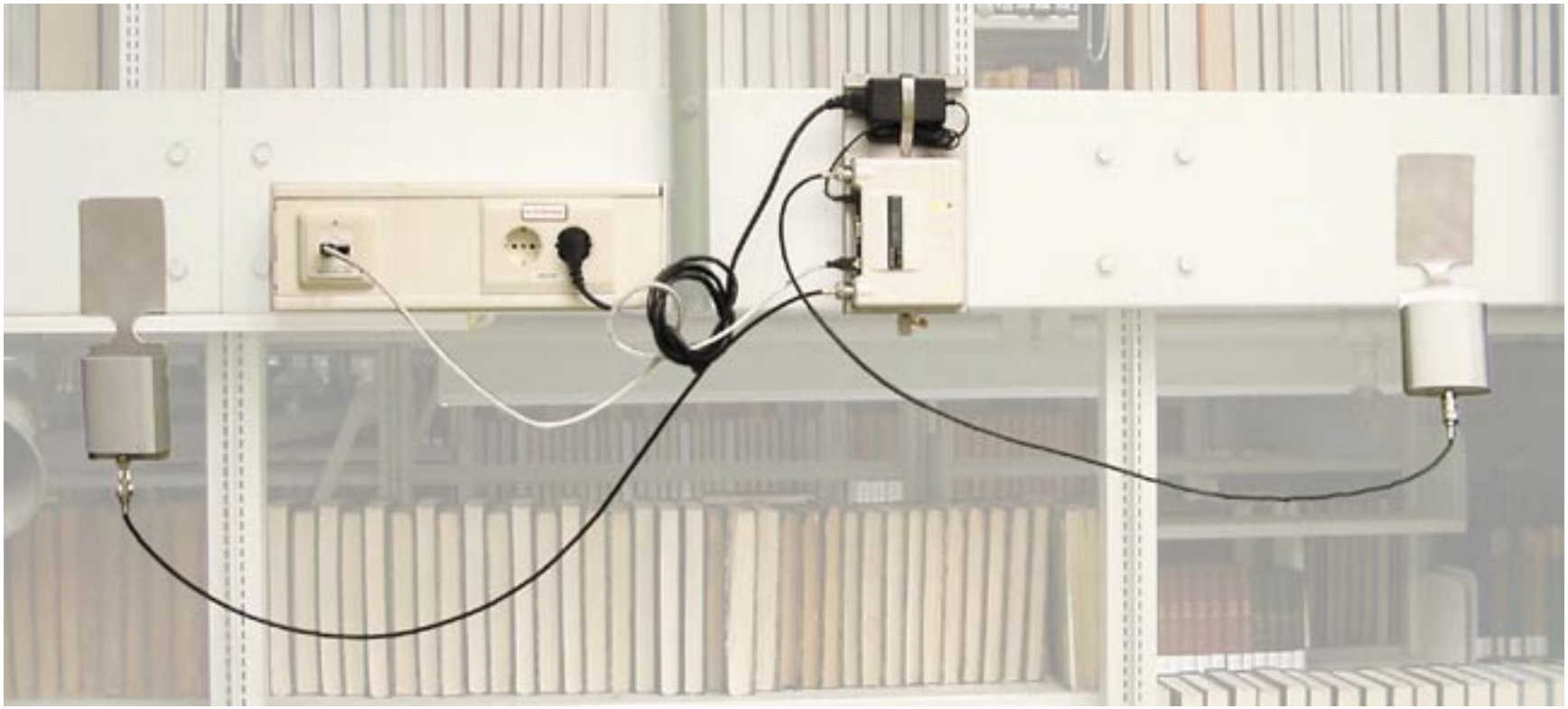
- Der Funkversorgung in der Bibliothek ist mit Abstand am beliebtesten.

Universität Konstanz – Bibliothek

Universität Konstanz – Bibliothek

Universität Konstanz – Bibliothek

- Cisco Access Points; externe Antennen, leistungsfähige CPU und reduzierbare Sendeleistung



Universität Konstanz – Bibliothek

• Die externe Antennen haben sich als Joker erwiesen, da die Funkwellen oft sonderbare Wege gehen und man sie mit Antennen noch am besten beeinflussen kann.

• Die reduzierbare Sendeleistung ist bei gerichteteren Antennen notwendig (100 mW ERIP). Wir haben die RegTP in nur wenigen hundert Meter Entfernung. Der Standort Konstanz kontrolliert auf einigen Bändern den Funkverkehr – weltweit!

Universität Konstanz – Limnologie

- Viele Möglich-keiten ha-ben sich erst im Laufe der Einführung ergeben und werden auch laufend neu entdeckt.

Wireless LAN – Zukunft?

2,4 GHz

IEEE 802.11b (2,4 GHz, 11 Mbps, 3 paralle Frequenzen)

IEEE 802.11g (noch nicht verabschiedet, 2,4 GHz, 22 Mbps, 8! parallele Frequenzen, OFDM)

5 GHz Europa, USA, Japan vergeben dieses Band unterschiedlich

HiperLAN/2 (5 GHz, 54 Mbps, 19 paralle Frequenzen, QoS, DFS, TPC, OFDM). Dieses Band ist in Europa von der ETSI für HiperLAN/2 reserviert.

IEEE 802.11a (5 GHz, 54 Mbps, OFDM, 11b einfach aufgebla sen); Viel Marketing

IEEE 802.11a + 802.11h (DFS, TPC) + 802.11j (Rücksicht auf andere); soll mit der Marktmacht auch in Europa durchge drückt werden.

- 5 GHz braucht andere Funkzellen, Ausbreitung noch "op tischer", weniger Störer, in Europa breiteres Band, vermutlich deutlich teurer.

Man kann noch eine ganze Weile auf 802.11b setzen.


HiperLAN/2

(Un-) Sicherheit im WirelessLAN

- versteckte SSID ist keine Sicherheit!

- Zugriff auf bestimmte MAC-Adressen bei größeren Installationen aufwändig und ist auch umgehbar. Zudem ist die MAC-Adresse nicht ungedingt an Personen gebunden.

- WEP – egal ob 40 oder 104 Bit – ist nicht sicher, da die Implementation schwach ist und einen RC4 Stromchiffrierer benutzt, so dass

    Ciphertext1 XOR Ciphertext2 = Klartext1 XOR Klartext2

"Das ganze Design des WEP Protokolls erinnert an einen Studienanfänger, welcher aus religiösen Gründen nur jede zweite Vorlesung der Kryptographie-Einführung besucht hat." (Rüdiger Weiss; Datenschleuder #75)

- "Wardriving" zeigt, dass fast alle Firmen, Krankenhäuser, Behörden offen sind.

Alternativen

VPN als Alternative

- PPTP

"Do not use PPTP" (PPTP FAQ)

- IPSec (komplex, sicher, wenig Platformübergreifend)

Portbasierte Authentifizierung

- Lucent (802.1x)
- Cisco, Apple (LEAP, EAP)

komplex, noch proprietär, nicht Platformübergreifend, WAP-Phänomen

Die meisten Unis tendieren zu einer Authentifizierung auf IPSec-Basis.

Stephan Pietzko
<stephan.pietzko@uni-konstanz.de>