Wireless Local Area Network nach IEEE 802.11

Ulrich Bareth
Matthias Röckl

Hauptseminar “Dienste & Infrastrukturen mobiler Systeme”
Wintersemester 03/04

Gliederung

- Vor- und Nachteile drahtloser Datenübertragung
- Anwendungsgebiete
- Netztopologien
- Protokollaufbau
- Übersicht zum Standard
- Wi-Fi (Wireless Fidelity)
- Ausblick

Vorteile drahtloser Datenübertragung

- Vorteile von Funknetzen:
  - **Mobilität** und **Flexibilität** (spontane Meetings, keine Kabel mitzunehmen)
  - **Verkabelung** manchmal nicht möglich oder unrentabel (Denkmalschutz, Brandschutzwände, Stolperfallen)
  - **Vollständige Vermaschung** (jeder mit jedem)
  - **Kosten** (keine Infrastruktur nötig, ein AP kann viele Teilnehmer versorgen)
  - Gute **Skalierbarkeit** (ein AP versorgt viele STAs ohne Zusatzaufwand)
  - **Lizenzfrei** (im Gegensatz zu UMTS)

Nachteile drahtloser Datenübertragung

- Nachteile von Funknetzen:
  - **Interferenzen** können Übertragung stören (Mikrowellen, Radar)
  - Gemeinsam genutztes **Medium Luft** (Bandbreite, nicht beliebig viele Netze in einem Bereich)
  - nationale **Restriktionen** (Sendeleistung, Frequenzbandnutzung)
  - **Sicherheit** (Schwachstellen in WEP)
  - **teure** Endgeräte (ab 50)
  - Hohe **Leistungsaufnahme** (Energieknappheit bei mobilen Geräten)
  - **Gesundheitsaspekte** (Wirkung von Funkwellen auf den Organismus)
  - **Kompatibilität** (Proprietäre Lösungen der Hersteller)

Anwendungsgebiete

- WLANs haben bereits jetzt ein breites Anwendungsspektrum:

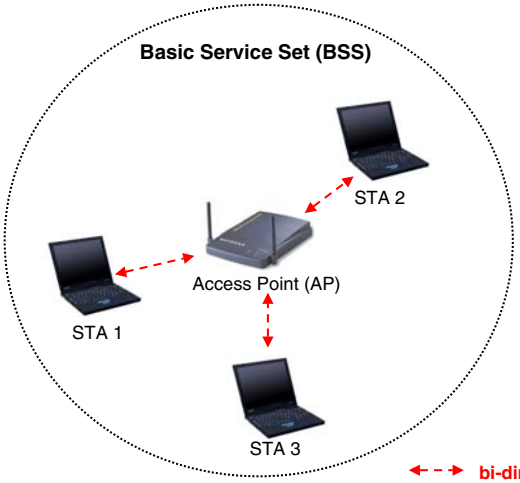
- Firmennetzwerke
- Hotspots (Uni, Englischer Garten, Kaffeehäuser(Puck), McDonalds)
- Messen
- SOHO (Small Office, Home Office)
- Vernetzung von strukturschwachen Regionen
- Last mile (z.B. zwischen 2 Bürogebäuden)

Geschichte

- 1963: Entstehung von IEEE (Institute of Electrical and Electronics Engineers)
- 1987: eigene Untergruppe 802.4L des Token Bus Standard (802.4) forscht auf dem Gebiet drahtloser Netze
- 1990: Normierungsauftrag für 802.4L erteilt => ab jetzt 802.11
- weltweite regulatorische und technologische Unterschiede verzögern die Entwicklung erheblich, so dass eine Fristverlängerung genehmigt werden muss
- 1997: 802.11 Standard wird verabschiedet
- 2000: Higher Data Rate Extensions => bis 11MBit/s bzw. 54 Mbit/s
- 2003: 802.11g => 54 Mbit/s und abwärtskompatibel zu 802.11b

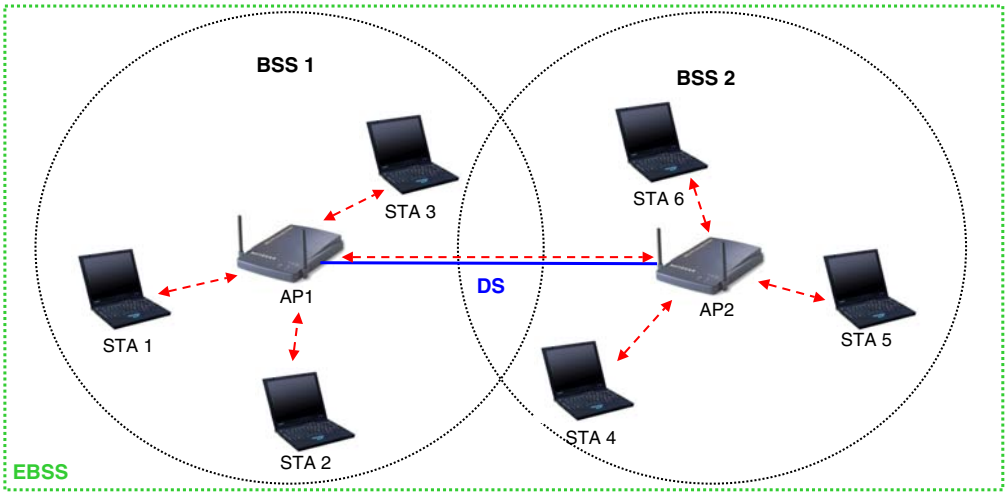
Infrastrukturmodus

- Im **Infrastrukturmodus** verbindet ein Access Point(AP) mehrere Stations(STAs):



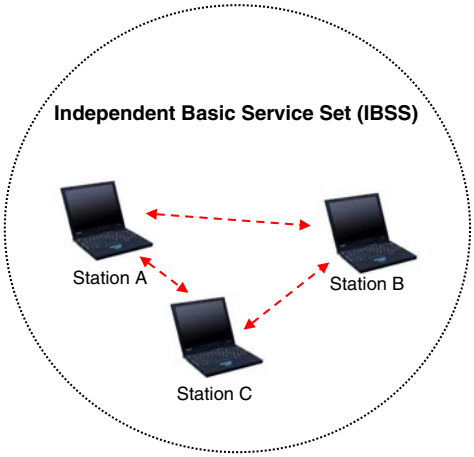
Infrastrukturmodus (EBSS)

- Wenn mehrere APs durch ein **DS(Distribution System)** verbunden werden spricht man von einem **EBSS(Extended Basic Service Set)**



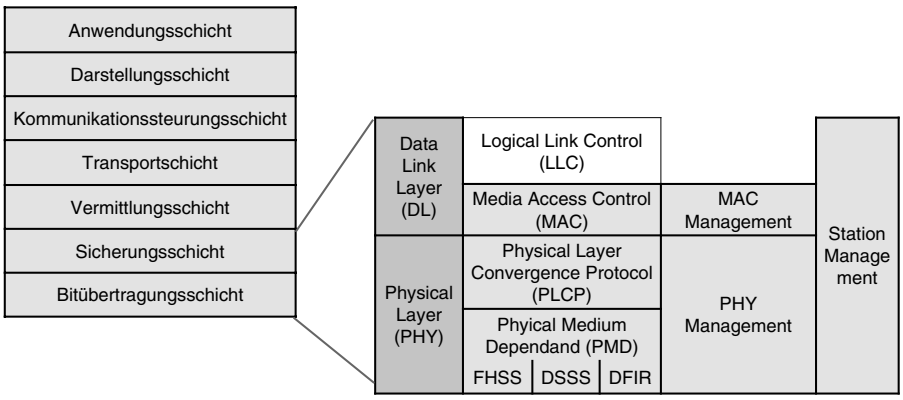
Ad-Hoc Modus

- Im **Ad-Hoc-Modus** kommunizieren die Teilnehmer direkt miteinander



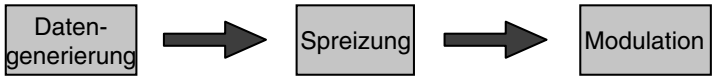
Schichtenmodell

- IEEE 802.11 Standard spezifiziert die Bitübertragungsschicht (PHY) und die Mediumzugriffsschicht (MAC) des ISO OSI-Schichtenmodells



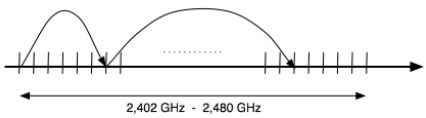
PHY-Schicht

- PLCP-Schicht: einheitliche Schnittstelle für MAC-Schicht unabhängig der zugrundeliegenden PMD-Schicht
- PMD-Schicht: drei Bitübertragungsverfahren, die sich unterscheiden durch:
- Frequenzband: Frequenz der Trägerwelle, Sendeleistung
- Spreizverfahren: Spreizung von schmalbandigen Signalen auf größeren Frequenzbereich
  - Reduzierung der Störanfälligkeit
  - "Verschlüsselung"
- Modulation: Bewusste Veränderung der Trägerwelle zur Datenübertragung



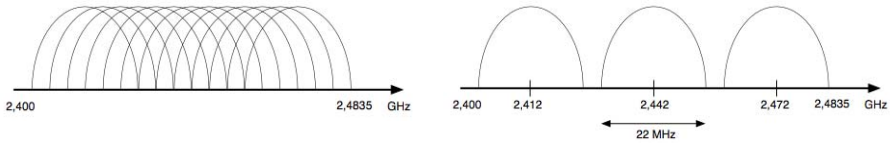
PHY-Schicht: Frequency Hopping Spread Spectrum

- Funkübertragung im lizenzfreien 2,4 GHz ISM-Band
- Sendeleistung: 100 mW EIRP (D), 1 W EIRP (USA)
- Spreizung:
- Pseudozufällige Sprungfolge über 79 disjunkte Kanäle mit einer Bandbreite von 1 MHz
- mind. 2,5 Frequenzsprünge pro Sekunde mit einem Mindestabstand von 6 MHz
- Data Whitening:
- Scrambling (Polynom: $G(x) = x^7 + x^4 + 1$): Entfernen von Gleichstromanteilen
- 32/33-Kodierung: Einfügen eines Stuff-Symbols zur besseren Synchronisation
- Modulation:
- 2-Level Gaussian Frequency Shift Keying (2GFSK): Übertragungsrate von 1 Mbps
- 4-Level Gaussian Frequency Shift Keying (4GFSK): Übertragungsrate von 2 Mbps



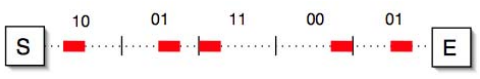
PHY-Schicht: Direct Sequence Spread Sprectrum

- Funkübertragung im lizenzfreien 2,4 GHz ISM-Band
- Sendeleistung: 100 mW EIRP (D), 1 W EIRP (USA)
- 13 überlappende Kanäle mit einer Bandbreite von 22 MHz (D)
- Mindestabstand von 30 MHz bei überlappenden oder adjazenten BSS (D)
- Spreizung: 11 Chip Barker Code +1 -1 +1 +1 -1 +1 +1 +1 -1 -1 -1
- Data Whitening:
- Scrambling (Polynom: $G(x) = x^7 + x^4 + 1$): Entfernen von Gleichstromanteilen
- Modulation:
- Differential Binary Phase Shift Keying (DBPSK): Übertragungsrate von 1 MBit/s
- Differential Quadrature Phase Shift Keying (DQPSK): Übertragungsrate von 2 MBit/s



PHY-Schicht: Diffused Infrared

- Übertragung mit infrarotem Licht mit einer Wellenlänge von 850 nm - 900 nm und einer Impulslänge von 250 ns
- Nur innerhalb geschlossener Räume einsetzbar mit einer Reichweite bis 20 Meter
- Günstige Hardware
- keine Vorgaben durch Regulierungsbehörde
- Modulation:
- 16-Puls-Phasen-Modulation (16PPM): Übertragungsrate von 1 MBit/s
- 4-Puls-Phasen-Modulation (4PPM): Übertragungsrate von 2 MBit/s
- wird in der Praxis nicht eingesetzt



PHY-Schicht bei IEEE 802.11a/b

- IEEE 802.11b
- Übertragungsraten von 1; 2; 5,5 und 11 MBit/s
- High Rate DSSS im 2,4 GHz ISM-Band
- Ähnlich zu DSSS, jdeoch wird statt mit 11-Chip Barker Codes mit 8-Bit Complementary Codes (CCs) gespreizt
- Dabei wählen die ersten 2 bzw. 6 Bits einen aus 4 bzw. 64 CCs aus
- Modulation: 2 Bits werden mit einem CC gespreizt und mit DQPSK auf die Trägerfrequenz aufmoduliert
- IEEE 802.11a
- Übertragungsraten von 6; 9; 12; 18; 24; 36; 48 oder 54 MBit/s
- Orthogonal Frequency Division Multiplex (OFDM) im 5 GHz ISM-Band
- Parallele Nutzung von bis zu 52 disjunkten Subträgerfrequenzen
- Modulation: DBPSK, DQPSK, 16-QAM, 64-QAM

PLCP-Rahmen

FHSS

Synchroni-zation	Start Frame Delimiter	Packet Length Width	Packet Signaling Field	Frame Check Sequence	Whitened SDU
80	16	12	4	16	<=4095 Byte
Preamble		Header			Daten

DSSS

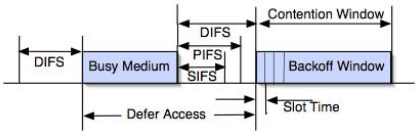
Synchroni-zation	Start Frame Delimiter	Signal	Service	Length	Frame Check Sequence	Whitened SDU
128	16	8	8	16	16	<=4095 Byte
Preamble		Header				Daten

DFIR

Synchroni-zation	Start Frame Delimiter	Data Rate	DC Level Adjustment	Length	Frame Check Sequence	Whitened SDU
57-73	4	3	32	16	16	<=2500 Byte
Preamble		Header				Daten

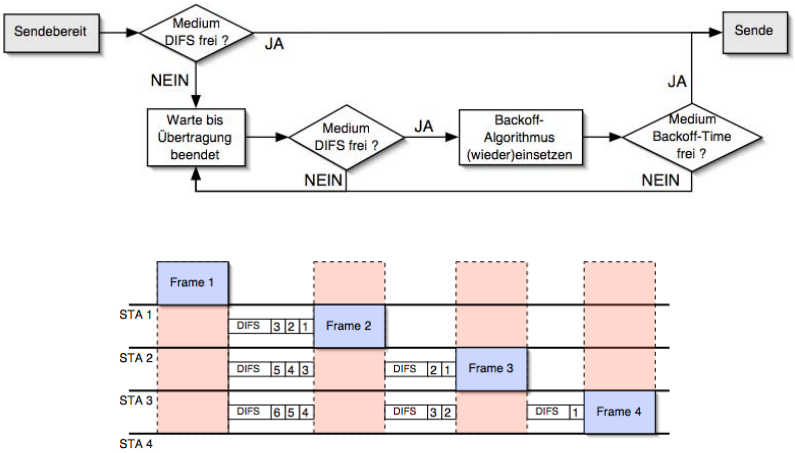
MAC-Schicht: Distributed Coordination Function

- Zugriffsteuerung auf das Medium mittels Carrier Sense Multiple Access mit Collision Avoidance (CSMA/CA)
- dezentrale Zugriffssteuerung durch prioritätsbasiertes Wettbewerbsverfahren
- Mediumzugriff erst nach konstanter + zufälliger Wartezeit (Backoff-Algorithmus)
- konstante Wartezeiten:
  - DCF Interframe Space (DIFS) >
  - PCF Interframe Space (PIFS) >
  - Short Interframe Space (SIFS)



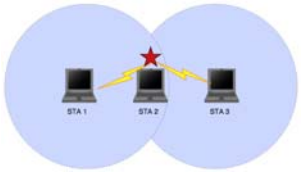
- zufällige Wartezeiten:
  - Bestimmung durch Pseudozufallsfunktion
  - Tradeoff zwischen langen Wartezeiten und vielen Kollisionen wird durch ein dynamisches Verfahren zur Bestimmung des Contention Windows erreicht
- Erkennung von Fehlübertragungen durch Quittungsverfahren

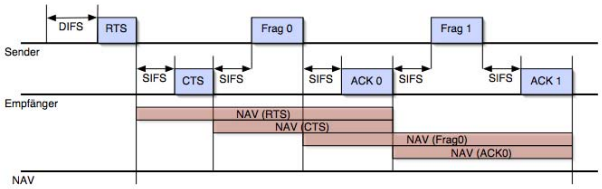
MAC-Schicht: einfaches CSMA/CA



MAC-Schicht: CSMA/CA mit RTS/CTS

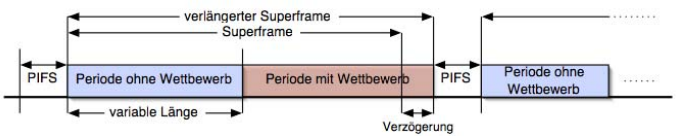
- Virtuelle Reservierung des Mediums mittels CSMA/CA mit Request-To-Send (RTS) und Clear-To-Send (CTS) als Lösung für Hidden-Terminal-Problem
- Sender sendet nach Wettbewerb RTS-Nachricht mit Dauer der anstehenden Übertragung - Empfänger antwortet mit CTS-Nachricht, die ebenfalls die Dauer der Übertragung enthält
- Alle Stationen im Empfangsbereich von Sender und Empfänger haben dadurch Kenntnis über die bevorstehende Übertragung





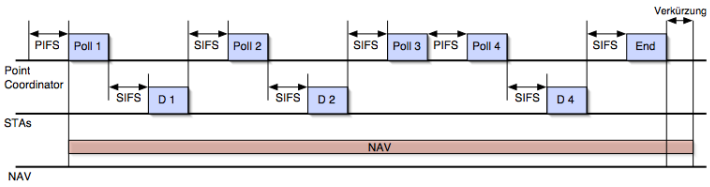
MAC-Schicht: Point Coordination Function I

- Zentrale Steuerung des Mediumzugriffs durch einen Point Coordinator (meist AP)
- Polling: Point Coordinator teilt jeder Station im Round Robin Verfahren das Medium zu
- Zugriffszeit wird in Superframes aufgeteilt:
- Periode ohne Wettbewerb: Zugriffssteuerung mittels PCF
- Periode mit Wettbewerb: Zugriffssteuerung mittels DCF
- PCF hat höhere Priorität als DCF (PIFS<DIFS)
- Point Coordinator kann bei Bedarf die Periode mit Wettbewerb überspringen



MAC-Schicht: Point Coordination Function II

- Point Coordinator sendet STA eine Poll-Nachricht (evtl. inklusive Daten und Quittung für vorhergehende Nachricht)
- STA kann daraufhin nach einer Wartezeit von SIFS einen Rahmen senden
- Sendet eine STA keinen Rahmen, sendet der Point Coordinator nach einer Wartezeit von PIFS automatisch der nächsten Station eine Poll-Nachricht
- Zeitdauer der Periode ohne Wettbewerb wird angezeigt durch:
- Setzen des NAV-Wertes
- Nachricht zu Beginn und Ende der wettbewerbsfreien Periode

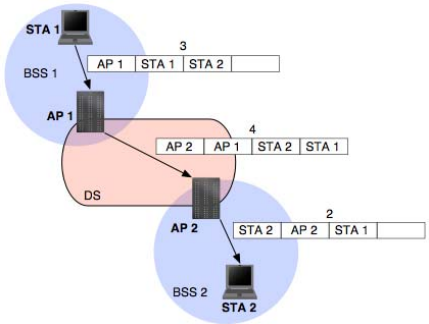


MAC-Rahmen

	Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS
Byte	2	2	6	6	6	2	6	0-2312	4
	Header							Body	

	Prot. Vers	Type	Sub-type	To DS	From DS	More Frag	Retry	Pwr Man	More Dat	WEP	Order
Bit	2	2	4	1	1	1	1	1	1	1	1

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	phys. Empfäng.	phys. Sender	BSSID	-
0	1	phys. Empfäng.	BSSID	log. Sender	-
1	0	BSSID	phys. Sender	log. Empfäng.	-
0	0	phys. Empfäng.	phys. Sender	log. Empfäng.	log. Sender

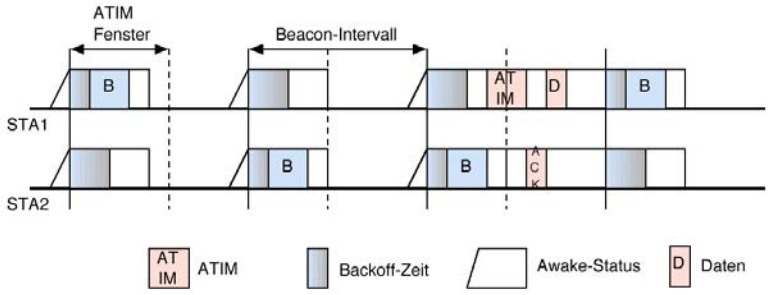


MAC Management Sublayer

- Im MAC Management Sublayer werden Mechanismen bereitgestellt, die für den Betrieb eines WLAN wichtig sind.
  - Im Infrastrukturmodus werden diese Funktionen hauptsächlich vom AP verwaltet und koordiniert.
  - Im Ad-Hoc-Modus sind die STAs selbst für die Bereitstellung der Funktionen verantwortlich, da es keine zentrale Einheit gibt.
- Zu den wichtigsten dieser Funktionen gehören:
  - Synchronisation (Timing Synchronization Function)
  - Roaming (transparenter Wechsel zwischen Funkzellen eines ESS)
  - Stromsparmechanismen (Power Management)
  - Sicherheit (Verschlüsselung und Authentisierung)

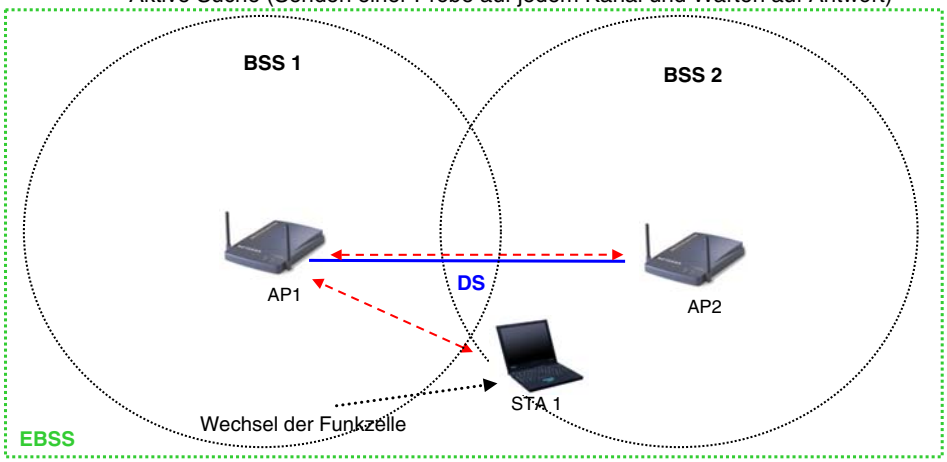
Synchronisation (TSF)

- Synchronisation ist wichtig(Sprungfolgen im FHSS, Energiesparmechanismus, PCF)
- Beacon-Frame mit Zeitstempel(Sendezeitpunkt) wird quasi-periodisch gesendet (in jedem Beacon-Intervall(ca. 50 ms) einmal)
- Sendezeitpunkt kann sich verspäten (falls Medium bereits belegt ist)
- Empfangende STAs justieren ihre internen Uhren nach dem erhaltenen Zeitstempel
- “verlorene” Beacons werden nicht wiederholt



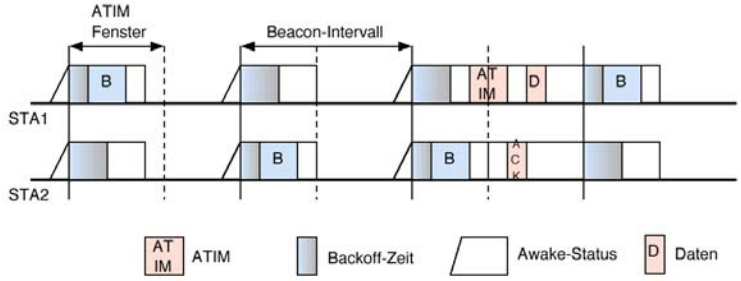
Roaming

- Wechsel von einer Funkzelle in die nächste, möglichst ohne die Verbindung zu verlieren
  - Passive Suche (Empfang von Beacon-Frames)
  - Aktive Suche (Senden einer Probe auf jedem Kanal und Warten auf Antwort)



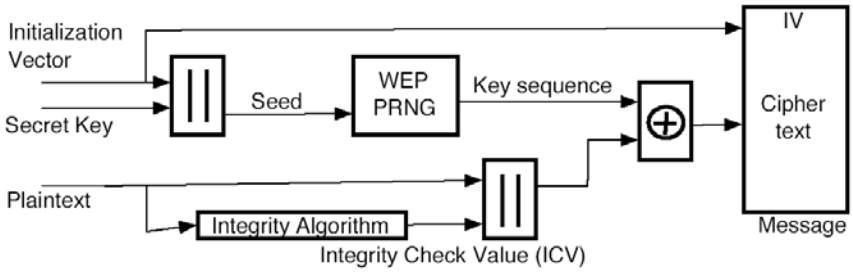
Power Management

- Akku von mobilen Geräten mit WLAN sollte möglichst lange halten
- Daten werden meist in Bursts übertragen => STAs oft idle(ungenutzt) => Sende- und Empfangselektronik kann abschaltet werden (Doze-Status)
- Jede STA geht zu Beginn jedes Beacon-Intervalls vom Doze- in den Awake-Status, um in der TIM(Traffic Indication Map) nachzusehen, ob Nachrichten für sie zwischengespeichert wurden
  - Falls ja: Daten werden übertragen; danach wieder Doze-Status
  - Falls Nein: sofort wieder Doze-Status
- TIM wird im Infrastrukturmodus im AP verwaltet, ansonsten in jeder STA



Sicherheit

- Sicherheit wird bei IEEE 802.11 mit “hauseigenem” WEP(Wired Equivalent Privacy) Standard realisiert:
- IV(Initialisierungsvektor mit 24 Bit Länge) wird mit dem Shared Secret Key (40 Bit oder 104 Bit) mittels RC4 zu Key Sequence verarbeitet
- An Plaintext wird ein ICV(Integrity Check Value) angehängt (CRC-32)
- XOR-Verknüpfung von Key Sequence und Plaintext gefolgt von ICV
- Der so verschlüsselte Text wird zusammen mit dem unverschlüsselten IV übertragen



Übersicht zu den 802.11 Standards(1)

- IEEE 802.11 – ”1997”
  - Erster verabschiedeter Standard für drahtlose Netze
  - Spezifiziert PHY und MAC Schichten des ISO-OSI-Referenzmodells
  - Frequenzband: 2,4-2,48 GHz im lizenzfreien ISM-Band (Industrial Scientific Medical)
  - Übertragungsraten bis 2 Mbit/s
- IEEE 802.11a – “High data rate extension in the 5 GHz band”
  - Erschliessung des 5 GHz Bereichs
  - Übertragungsraten bis 54 Mbit/s
  - OFDM
- IEEE 802.11b – “Higher data rate extension in the 2,45 GHz band”
  - 2,4 GHz
  - Übertragungsraten bis 11 Mbit/s
  - CKK

Übersicht zu den 802.11 Standards(2)

- IEEE 802.11c – ”Supplement to Bridge Standard”
  - Verbindung zu Subnetzen protokollmäßig auf OSI-Schicht 2
- IEEE 802.11d – “Update of regulatory domains”
  - Untersuchung von Regulierungsvorgaben in Nordamerika(einzelne Staaten autark in der Frequenzvergabe) und Europa
- IEEE 802.11e – “MAC Enhancements for Quality of Service”
  - Verbesserung der QoS-Funktionalität
  - HCF(Hybrid Coordination Function) im Infrastrukturmodus
  - EDCF(Enhanced Distributed Coordination Funktion) im Ad-Hoc-Modus
- IEEE 802.11f – “IAPP Inter Access Point Protocol”
  - Kompatibilität unterschiedlicher APs durch ein einheitliches Protocol

Übersicht zu den 802.11 Standards(3)

- IEEE 802.11g – ”Higher Rate Extension to 802.11b”
  - OFDM jetzt auch für 2,4 GHz
  - Bis 54 Mbit/s
  - Abwärtskompatibilität zu 802.11b
- IEEE 802.11h – “SMa Spectrum Managed 802.11a”
  - Ergänzungstandard zur Regulierung der Signalstärke und für Dynamische Frequenzwahl
  - TPC(Transmission Power Control) reduziert Sendestärke auf ein Minimum
  - DFS(Dynamic Frequency Selection) wechselt Frequenz falls Medium bereits anderweitig belegt ist
- IEEE 802.11i – “MAC Enhancements for Security”
  - Sicherheitslücken im WEP-Standard sollen geschlossen werden
- IEEE 802.11j – “4.9 GHz – 5 GHz Operation in Japan”
  - Verhandlungen zu 5 GHZ Band in Japan

Übersicht zu den 802.11 Standards(4)

- IEEE 802.11k – ”Radio Resource Measurement of Wireless LANs”
  - Optimierung der Auslastung von WLANs mit Hilfe von Messungen
  - Momentan entscheidet nur die Empfangsstärke über die Wahl des APs
- IEEE 802.11m – “Maintenance PAR”
  - Verwaltung von Korrekturen im 802.11 – 1997 Standard
  - Vielleicht entsteht daraus 802.11 – 2004 ??
- IEEE 802.11n – “High Troughput”
  - Neue Task-Group für höhere Übertragungsraten bis zu 320 Mbit/s
  - Noch kein PAR erteilt

Die Zukunft von IEEE 802.11

- Momentane Schwächen müssen behoben werden (QoS, Sicherheit)
- WLAN Konkurrenz zu UMTS 3G?