Wireless networks and Applications

ISEP Nov 2008

Lieven De Strycker
Lieven.DeStrycker@kahosl.be

KaHo Sint-Lieven – 12/11/2008

DraMCo research group

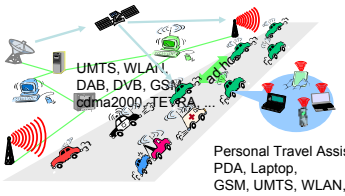
Overview

- The physical layer
- Wireless Personal Area Networks – WPAN
- Wireless Local Area Networks – WLAN

The physical layer

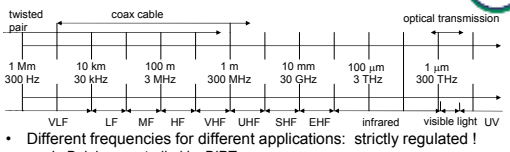
Wireless communication introduction

- Signal is sent by a transmitter to a receiver without the use of wires
- Antennas are used to send and to receive electromagnetic waves
  - Fixed: antennes are at fixed positions
  - Mobile: one of the antennes can move



Personal Travel Assistant,
PDA, Laptop,
GSM, UMTS, WLAN,
Bluetooth, ...

Frequencies



- Different frequencies for different applications: strictly regulated !
  - In Belgium controlled by BIPT
  - In U.S by FCC
  - Worldwide management ITU-T
  - In Portugal ANACOM ??
- Example
  GSM : 890-915 MHz (up), 935-960 MHz(down) (=124 channels) and 1710-1785 MHz (up), 1805-1880 (down) (=374 channels)

Spectrum is scarce (expensive)

Frequencies

- License free frequency bands :
  ISM (Industrial, Science, Medical)
  - 433 MHz : e.g. wireless control (keys, doorbell)
  - 868 MHz : e.g. wireless domotics (-> 915 MHz in US)
  - 2.4 GHz : e.g. WiFi, ZigBee, Bluetooth
  - 5.7 GHz *(U-NII: Unlicensed National Information Infrastructure)*
  - No license required BUT strict rules
- Frequency and wavelength:
  $\lambda = c/f$

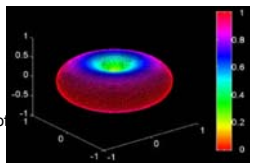
  wavelength λ, speed of light $c \cong 3x10^8$m/s, frequency f

Frequentie	1 MHz	3 MHz	30 MHz	100 MHz	300 MHz	1 GHz	3 GHz
Golflengte	300 m	30 m	10 m	3 m	1 m	30 cm	10 cm

Antennas

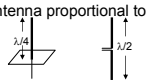
- Goal: radiation and reception of electromagnetic waves, coupling of wires to space for radio transmission
- Isotropic radiator (omnidirectional): equal radiation in all directions (three dimensional) - only a theoretical reference antenna

- Real antennas always have directive effects (vertically and/or horizontally)
- Radiation pattern: measurement of radiation around an antenna

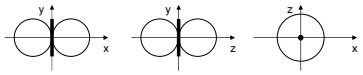


Antennas

- Real antennas are not isotropic radiators, e.g., dipoles with lengths λ/4 on car roofs or λ/2 as Hertzian dipole
  ➔ shape of antenna proportional to wavelength



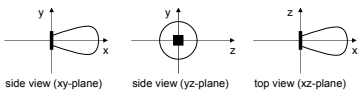
- Example: Radiation pattern of a simple Hertzian dipole



- Gain: maximum power in the direction of the main lobe compared to the power of an isotropic radiator (with the same average power)

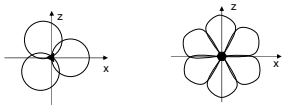
Antennas

- Directed and sectorized antennas e.g. for GSM basestations (more complex structures)



side view (xy-plane) side view (yz-plane) top view (xz-plane)

directed antenna



top view, 3 sector top view, 6 sector

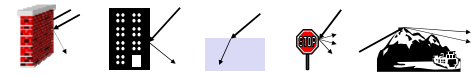
sectorized antenna

Signal propagation

- Propagation in **free space** always like light (straight line)
- **Path loss** : receiving power proportional to 1/d² in vacuum (d = distance between sender and receiver): Line-of-sight **LOS**

$$P_r = P_t \frac{G_t G_r}{(4\pi d / \lambda)^2}$$

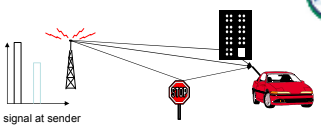
- **Other effects (dependent on the wavelength)**: shadowing, reflection, scattering, diffraction, …
  - ⇒ non-LOS communication possible
  - ⇒ much more loss in real environments : $1/d^n$, mostly n>2
  - ⇒ multipath propagation
- **WLAN/WPANs** in ISM 2.4 GHz and 868/900 MHz frequency bands



shadowing reflection refraction scattering diffraction

Signal propagation: signal strength

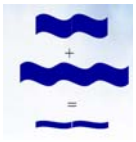
Multipath propagation



signal at sender

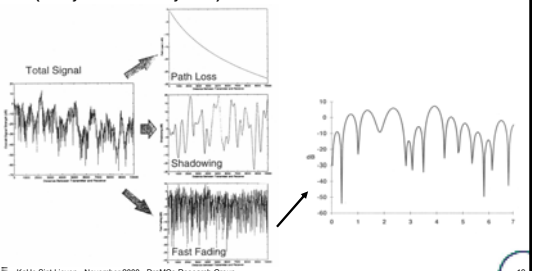
Two signal with difference in path distance of λ

Two signal with difference in path distance of λ/2

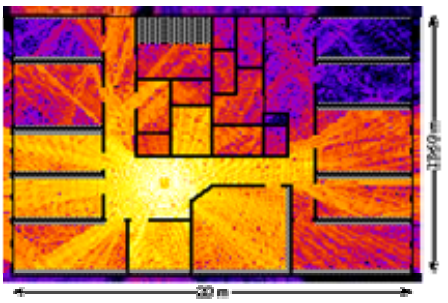


Signal propagation: signal strength

- **Multipath propagation:** phase relation between the signals dependent on place and frequency => large changes in signal strength (constructive and destructive interference)
  - **Impact: at some places signal strength is too small: signal is lost (mainly in small band systems)**

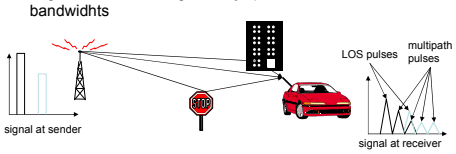


Signal propagation: signal strength



Delay spread

- **Multipath propagation**: **delay spread**
- **InterSymbol Interference (ISI)** => limits the datarate
- **Coherence bandwidth** is widest bandwidth that a transmitted signal can have with negligible ISI (e.g. symbol duration > 10 times rms delay spread)
  - Flat fading
  - Frequency selective fading
- Lager rooms have larger delay spreads and smaller coherence bandwidhts



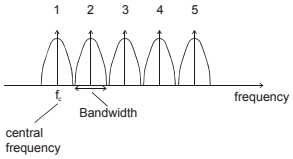
Doppler spread

- **Mobile communications**
  - environment is changing continuously
  - sender and/or receiver are moving
- Channel is continuously changing: **coherence time** is the time over which the changes in the channel characteristics are negligible
  - Slow fading
  - Fast fading
- WPAN and WLAN:
  - Slow faded
  - Flat faded

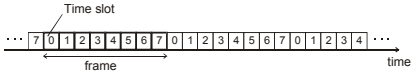
Medium Access Techniques

- All signals through the same medium
- Avoid interference by multiple access techniques
  - FDMA
  - TDMA
  - SDMA
  - CDMA
  - CSMA/CD ??
  - ….

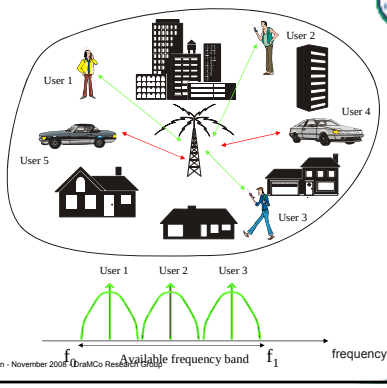
FDMA Frequency Division Multiple Access



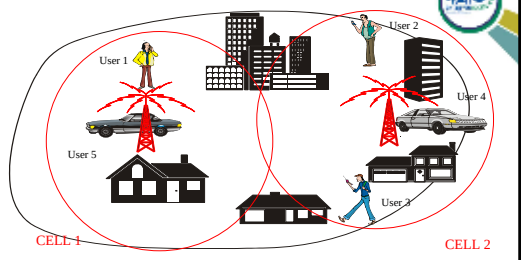
TDMA Time Division Multiple Access

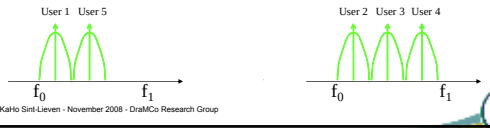


SDMA Space Division Multiple Access: Cellular networks

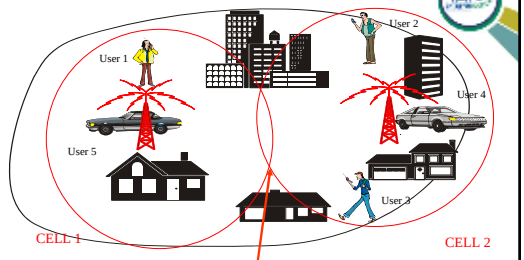


SDMA Space Division Multiple Access : Cellular networks



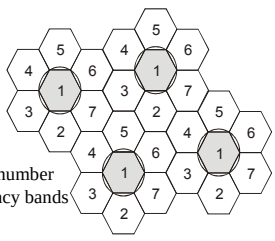


SDMA Space Division Multiple Access : Cellular networks



SDMA Space Division Multiple Access : Cellular networks

- Why ?
  - Limited frequency spectrum
  - Improved power usage



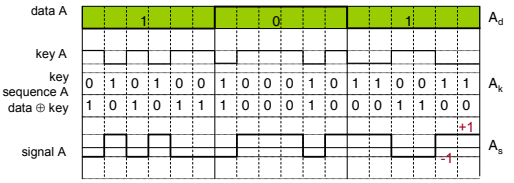
Cells with same number use same frequency bands

Transmission area of cell 1

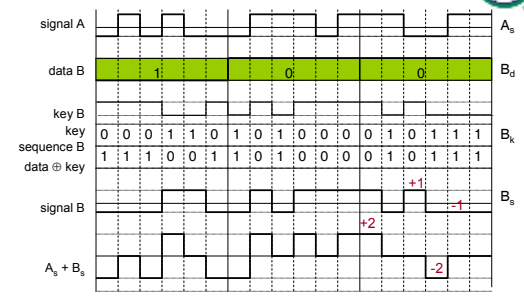
Cell boundaries

CDMA Code Division Multiple Access

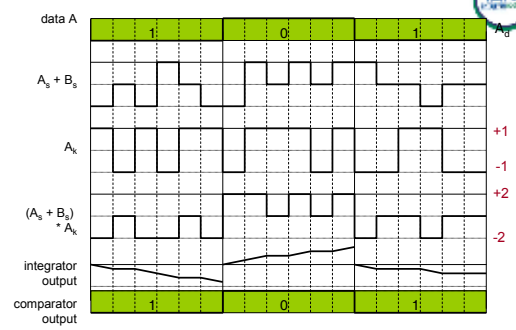
- CDMA (Code Division Multiple Access)
  - all terminals send on the same frequency probably at the same time and can use the whole bandwidth of the transmission channel
  - each sender has a unique random number (the code), the sender XORs the signal with this random number
  - the receiver can "tune" into this signal if it knows the pseudo random number (the code)



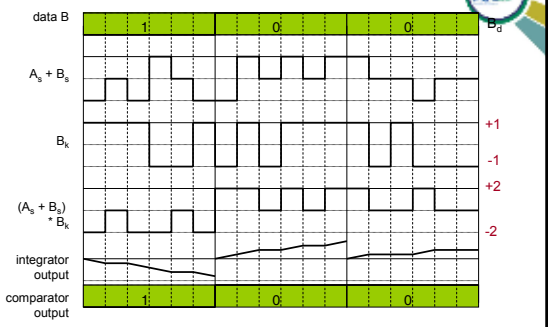
CDMA Code Division Multiple Access



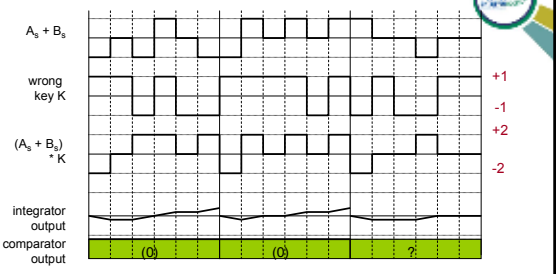
CDMA Code Division Multiple Access



CDMA Code Division Multiple Access



CDMA Code Division Multiple Access

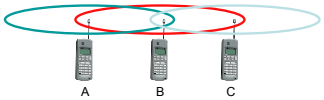


A_s has a larger bandwidth than A_d => Direct Sequence Spread Spectrum (DSSS)

used in WiFi, UMTS (3G)

CSMA/CD

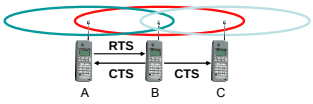
- Carrier Sense Multiple Access/ Collision Detection
- (with random back-off times: Collision Avoidance)
- For CSMA/CD problems that do not exist in wired networks e.g. hidden terminals
  - A sends to B, C cannot receive A
  - C wants to send to B, C senses a “free” medium (CS fails)
  - collision at B, A cannot receive the collision (CD fails)
  - A is “hidden” for C



- Additions to the protocol to avoid this e.g. MACA

MACA

- MACA (Multiple Access with Collision Avoidance) uses short signaling packets for collision avoidance
  - RTS (request to send): a sender request the right to send from a receiver with a short RTS packet before it sends a data packet
  - CTS (clear to send): the receiver grants the right to send as soon as it is ready to receive
- MACA avoids the problem of hidden terminals
  - A and C want to send to B
  - A sends RTS first
  - C waits after receiving CTS from B

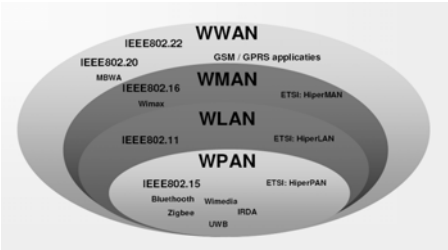


  - Variants of this can be used in WLAN 802.11 (WiFi)

Application domains

- Wireless Telecommunication systems (GSM, UMTS, TETRA,…)
- Broadcast systems (TV, Radio, DAB, DVB)
- Satellite systems (radio and TV broadcast, military, weather, navigation, satellite telephone, backbone for telephone,…)
- Wireless WAN, MAN, LAN, PAN (WiMax, WiFi, Bluetooth, ZigBee,…)

Application domains



Wireless Personal Area Networks - WPAN

Overview

- WPAN ?
- Who's standardizing what ?
- Bluetooth

WPAN ?

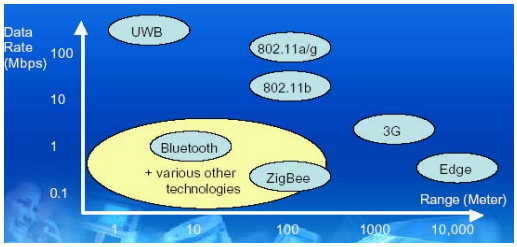
- WPAN : Wireless Personal Area Networks
- short distance wireless networks
- wireless networking of portable and mobile computing devices such as PCs, Personal Digital Assistants (PDAs), peripherals, cell phones, pagers, consumer electronics, sensors, etc; allowing these devices to communicate and interoperate with one another.
- Ranging
  from point-to-point cable replacement
  to meshed networks containing thousands of nodes

  from low bitrate to high bitrate

  from low connection rate to high connection rate
  ....
- various applications with different requirements
- => different standards, with flexibility in standards

Wireless Personal Area Networks - WPAN

Datarates and distances



Wireless Personal Area Networks - WPAN

- Open standards based on IEEE standards
  - High rate : WiMedia
  - Medium rate : Bluetooth
  - Low rate : ZigBee
- But other technologies
  - Z-wave
    - proprietary (Zensys, Denmark): protocol for home control
    - Z-wave Allience : 14/01/2005
    - 868.42 MHz
      BFSK ± 20 kHz
      9600 bits/s
    - Meshed networks (≤232 nodes), routing along different nodes, two-way with acknowledgment
  - Home RF : working group disbanded 2003
  - *Power Line Communications*

Wireless Personal Area Networks - WPAN

Who's standardizing what ?

IEEE 802 LAN/MAN Standards Committee
www.ieee802.org

IEEE 802.15 Working Group for WPAN	IEEE 802.11 WG for WLAN	IEEE 802.16 WG for WMAN
www.ieee802.org/15	www.ieee802.org/11	www.ieee802.org/16
IEEE 802.15.1 Medium rate WPAN **Bluetooth** v1.1 PHY + MAC	WiFi	WiMax
IEEE 802.15.3 High rate WPAN **WiMedia**		
IEEE 802.15.4 Low Rate WPAN **ZigBee** PHY + MAC		

Wireless Personal Area Networks - WPAN

Who's standardizing what ?

Bluetooth

Bluetooth SIG www.bluetooth.org	**Higher layers**
IEEE 802.15.1	**PHY + MAC**

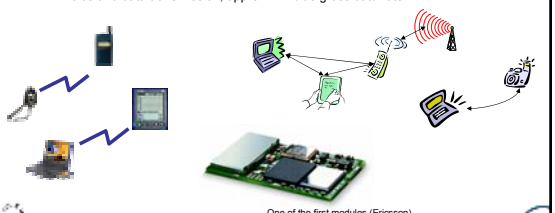
ZigBee

ZigBee Alliance www.zigbee.org	**Higher layers**
IEEE 802.15.4	**PHY + MAC**

WPAN - Bluetooth

Applications

- Idea
  - Universal radio interface for ad-hoc wireless connectivity
  - Interconnecting computer and peripherals, handheld devices, PDAs, **cell phones** – replacement of IrDA
  - Embedded in other devices, goal: 5€/device (2005: 40€/USB bluetooth)
  - Short range (10 m), low power consumption, license-free 2.45 GHz ISM
  - Voice and data transmission, approx. 1 Mbit/s gross data rate



One of the first modules (Ericsson).

WPAN - Bluetooth

- History
  - 1994: Ericsson (Mattison/Haartsen), "MC-link" project
  - Renaming of the project: Bluetooth according to Harald "Blåtand" Gormsen [son of Gorm], King of Denmark in the 10th century
  - 1998: foundation of Bluetooth SIG, www.bluetooth.org (was: Bluetooth.)
  - 1999: erection of a rune stone at Ericsson/Lund ;-)
  - 2001: first consumer products for mass market, spec. version 1.1 released
  - 2005: 5 million chips/week

Bluetooth™

- Special Interest Group
  - Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
  - Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
  - > 2500 members
  - Common specification and certification of products

WPAN - Bluetooth

History and hi-tech…

1999:
Ericsson mobile communications AB reste denna sten till minne av Harald Blåtand, som fick ge sitt namn åt en ny teknologi för trådlös, mobil kommunikation.

WPAN - Bluetooth

…and the real rune stone

Located in Jelling, Denmark, erected by King Harald "Blåtand" in memory of his parents.
The stone has three sides – one side showing a picture of Christ.

Inscription:
"Harald king executes these sepulchral monuments after Gorm, his father and Thyra, his mother. The Harald who won the whole of Denmark and Norway and turned the Danes to Christianity."

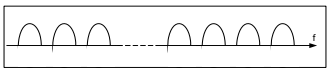
Btw: Blåtand means "of dark complexion" (not having a blue tooth…)

This could be the "original" colors of the stone.
Inscription:
"auk tani karthi kristna" (and made the Danes Christians)

WPAN - Bluetooth

Physical Layer

- Physical layer - Radio
  - 2.4 GHz licence-free ISM band
  - Divided in 79 channels of 1MHz
    - GFSK modulation
    - Symbol rate = 1 Megasymbol/s = **1Mb/s**
  - Timeslots of 625 µs
    - Datapacket is 1, 3 or 5 slots



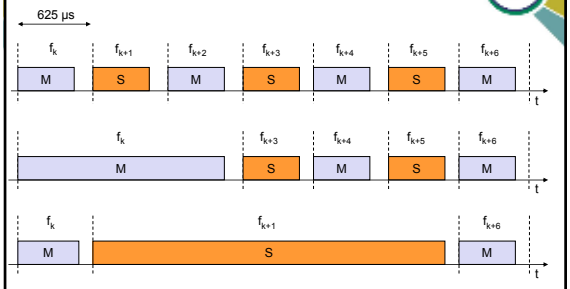
WPAN - Bluetooth

Physical Layer

- Frequency Hopping Spread Spectrum (FSSH)
  - Each packet the radio is tuned to a different channel
  - Pseudo-random generator 2^27 states
  - 1600 hops per second
    - ⇒23.2 hours
  - Goal
    - Avoiding interference with other Bluetooth nets (overlapping piconets are possible)
    - Avoiding interference with other devices in ISM band
    - Fulfilling power regulations in ISM band
    - Security ?
- Three power classes
  - Class 1 = 100 mW (20 dBm)
  - Class 2 = 2.5 mW (4 dBm)
  - Class 3 = 1 mW (0 dBm)
- Half duplex

WPAN - Bluetooth

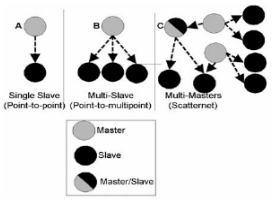
Physical Layer - Frequency selection during data transmission



WPAN - Bluetooth

Baseband Network topologies

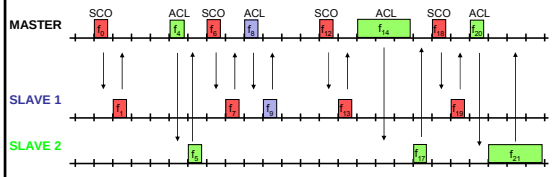
- Master – Slave
  - Each module can act as master or slave
- Piconet
  - One master upto seven slaves
  - TDM
  - Master controls TDM scheme and frequency hopping scheme
- Scatternet
  - Several connected piconets



WPAN - Bluetooth

Baseband link types

- Polling-based TDD packet transmission
  - 625µs slots, master polls slaves
- SCO (Synchronous Connection Oriented) – Voice
  - Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point
- ACL (Asynchronous ConnectionLess) – Data
  - Variable packet size (1,3,5 slots), asymmetric bandwidth, point-to-multipoint



WPAN - Bluetooth

Baseband link types

- Two types of baseband links (physical links)
  - Asynchronous Connectionless ACL
    - high speed, time-insensitive data communication

- Maximum length of one packet is 5 timeslots = Max 2712 databits in payload (DH5 packet)
- Minimum reply length is one slot

⇒Datarate in one direction **723.2 kb/s**, other direction 57.6 kb/s

- Taking into account higher layers -> max bitrate is about **650 kb/s**
- Symmetrical link => **433.9 kb/s (compared to 1Mb/s on air)**

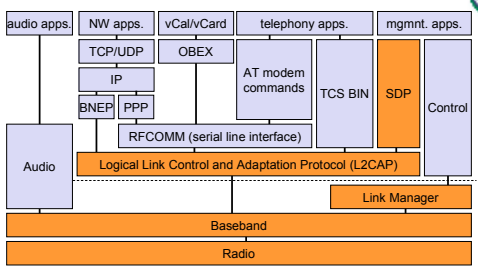
WPAN - Bluetooth

Baseband link types

- Synchronous Connection Oriented SCO
  - Time critical voice and audio
  - 64 kb/s
  - Three full-duplex voice links possible in one piconet
  - Audio quality comparable with GSM

WPAN - Bluetooth

Bluetooth protocol stack



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.

WPAN - Bluetooth

SDP – Service Discovery Protocol

- Inquiry/response protocol for discovering services
  - Searching for and browsing services in radio proximity
  - Adapted to the highly dynamic environment
  - Can be complemented by others like SLP, Jini, Salutation, …
  - Defines discovery only, not the usage of services
  - Caching of discovered services
  - Gradual discovery
- Service record format
  - Information about services provided by attributes
  - Attributes are composed of an 16 bit ID (name) and a value
  - values may be derived from 128 bit Universally Unique Identifiers (UUID)

WPAN - Bluetooth

Additional protocols to support legacy protocols/apps.

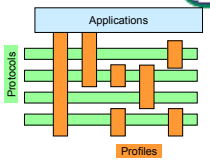
- RFCOMM
  - Emulation of a serial port (supports a large base of legacy applications)
  - Allows multiple ports over a single physical channel
- Telephony Control Protocol Specification (TCS)
  - Call control (setup, release)
  - Group management
- OBEX
  - Exchange of objects, IrDA replacement
- WAP
  - Interacting with applications on cellular phones

WPAN - Bluetooth

Profiles

- Represent default solutions for a certain usage model
  - Vertical slice through the protocol stack
  - Basis for interoperability

- Generic Access Profile
- Service Discovery Application Profile
- Cordless Telephony Profile
- Intercom Profile
- Serial Port Profile
- Headset Profile
- Dial-up Networking Profile
- Fax Profile
- LAN Access Profile
- Generic Object Exchange Profile
- Object Push Profile
- File Transfer Profile
- Synchronization Profile



Additional Profiles
Advanced Audio Distribution
PAN
Audio Video Remote Control
Basic Printing
Basic Imaging
Extended Service Discovery
Generic Audio Video Distribution
Hands Free
Hardcopy Cable Replacement

Wireless Local Area Networks - WLAN

WLAN – 802.11 WiFi

- WiFi : Wireless Fidelity
  - WLAN : Wireless version of LAN
  - Based on IEEE 802.11 a, b and g
  - WiFi guarantees that products work together
  - IEEE describes the physical layer and MAC-layer, all the rest is like wired LAN
  - Different versions of the standard

802.11	2.4 GHz	1 or 2 Mbit/s	**DSSS**,FHSS,Ir	1997	
802.11a	5.0 GHz	6 to 54 Mbit/s	OFDM	1999	WiFi
802.11b	2.4 GHz	5.5 or **11 Mbit/s**	DSSS	1999	WiFi
802.11g	2.4 GHz	**54 Mbit/s**	OFDM	2003	WiFi

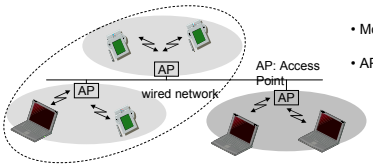
  - 802.11n : draft, standard expected in Nov 2009, OFDM, 2.4GHz/5GHz, 600Mbit/s (max) typ user bitrate 100 Mbit/s

  - Range : 50 – 450 m (depending on bitrate)
  - Power : 0.1 to 0.01 W

WLAN – 802.11 WiFi

Infrastructure vs. ad-hoc networks

Infrastructure network



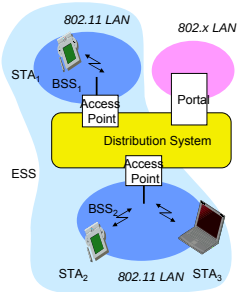
- Most functionality in AP; stations simple
- AP can coordinate medium Access (polling) QoS

Ad-hoc network

More flexibility

WLAN – 802.11 WiFi

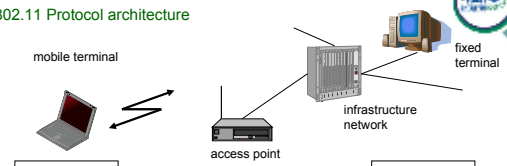
802.11 - Architecture of an infrastructure network



- Station (STA)
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- Basic Service Set (BSS)
  - group of stations using the same radio frequency
- Access Point
  - station integrated into the wireless LAN and the distribution system
- Portal
  - bridge to other (wired) networks
- Distribution System
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

WLAN – 802.11 WiFi

802.11 Protocol architecture



application		application
TCP		TCP
IP		IP
LLC	LLC	LLC
802.11 MAC	802.11 MAC / 802.3 MAC	802.3 MAC
802.11 PHY	802.11 PHY / 802.3 PHY	802.3 PHY

802.3 = Ethernet

WLAN – 802.11 WiFi

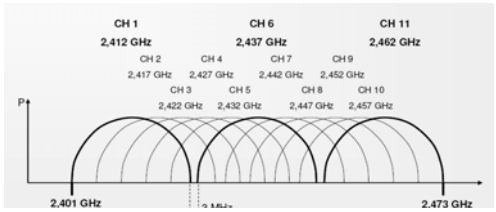
Physical Layer

- 802.11
  - Three PHY:
    - FHSS: frequency hopping spread spectrum (2.4 GHz)
    - DSSS: direct sequence spread spectrum (Barker code) (2.4 GHz)
    - Infra red
  - DSSS most important => 802.11b
  - Bitrates : 1 Mbps , 2 Mbps (optional)
- **802.11b**
  - **DSSS**
  - **2.4 GHz**
  - **Bitrates: 1, 2, 5.5, 11 Mbps (upwards compatible with 802.11 DSSS)**
- 802.11a
  - OFDM
  - 5 GHz
  - Bitrates: upto 54 Mbps
- **802.11g**
  - **OFDM**
  - **2.4 GHz**
  - **Bitrates upto 54 Mbps**
- 802.11n
  - Multiple antennas (MIMO)
  - Bitrates upto 600 Mbps
  - Not available yet ? -> "pre-N"

WLAN – 802.11 WiFi

PHY 802.11b Channel selection (non-overlapping)

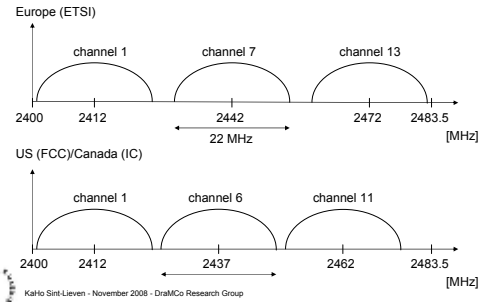
In 2.4 GHz band:
14 channels of 22MHz, central frequency spacing 5MHz => overlapping channels



WLAN – 802.11 WiFi

PHY 802.11b Channel selection (non-overlapping)

- Selection of non-overlapping channels



WLAN – 802.11 WiFi

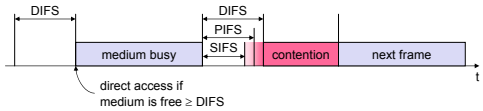
MAC Layer : DFWMAC (Distributed Foundation Wireless MAC)

- Traffic services
  - Asynchronous Data Service (mandatory)
    - exchange of data packets based on "best-effort"
    - support of broadcast and multicast
    - Implemented using DCF (Distributed Coordination Function)
  - Time-Bounded Service (optional)
    - implemented using PCF (Point Coordination Function)
- Access methods
  DFWMAC: Distributed Foundation Wireless MAC
  - DCF: **Distributed** Coordination Function
    - DFWMAC-DCF CSMA/CA (mandatory)
      - collision avoidance via randomized „back-off" mechanism
      - minimum distance between consecutive packets
      - ACK packet for acknowledgements (not for broadcasts)
    - DFWMAC-DCF w/ RTS/CTS (optional)
      - avoids hidden terminal problem
  - PCF: **Point** Coordination Function
    - DFWMAC- PCF (optional)
      - access point polls terminals according to a list

WLAN – 802.11 WiFi

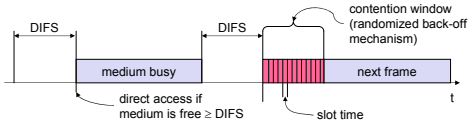
MAC Layer

- Priorities
  - defined through different inter frame spaces
  - no guaranteed, hard priorities
  - SIFS (Short Inter Frame Spacing): (DSSS: 10µs)
    - highest priority, for ACK, CTS, polling response
  - PIFS (PCF IFS) (DSSS : 30µs)
    - medium priority, for time-bounded service using PCF
  - DIFS (DCF, Distributed Coordination Function IFS) (DSSS: 50µs)
    - lowest priority, for asynchronous data service



WLAN – 802.11 WiFi

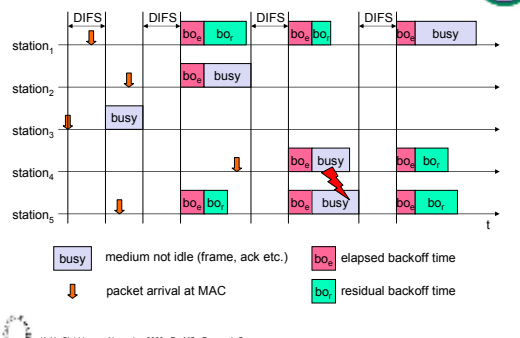
MAC Layer : CSMA/CA basics



- station ready to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

WLAN – 802.11 WiFi

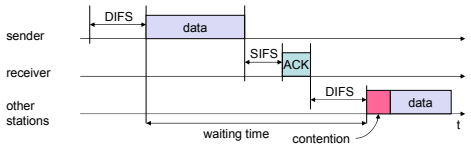
MAC Layer : CSMA/CA basics



WLAN – 802.11 WiFi

MAC Layer : CSMA/CA basics

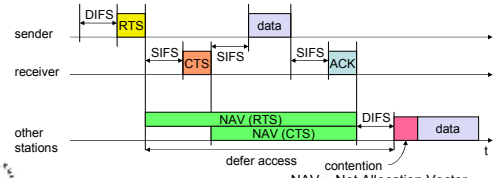
- Sending unicast packets
  - station has to wait for DIFS before sending data
  - receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
  - automatic retransmission of data packets in case of transmission errors



WLAN – 802.11 WiFi

MAC Layer: DFWMAC – DCF with RTS/CTS

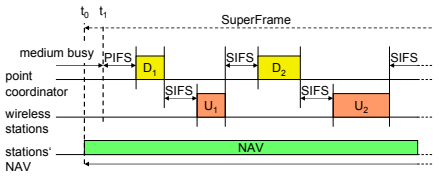
- Sending unicast packets
  - station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs the medium)
  - acknowledgement via CTS (again with reservation parameter) after SIFS by receiver (if ready to receive)
  - sender can now send data at once, acknowledgement via ACK
  - other stations store medium reservations distributed via RTS **and** CTS



NAV = Net Allocation Vector

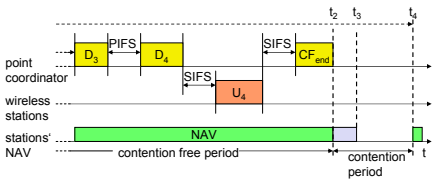
WLAN – 802.11 WiFi

MAC Layer: DFWMAC-PCF I



WLAN – 802.11 WiFi

MAC Layer: DFWMAC-PCF II



WLAN – 802.11 WiFi

WLAN 802.11 MAC Layer: MAC management

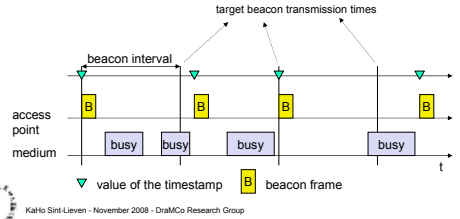
- Synchronization
  - try to find a LAN, try to stay within a LAN
  - synchronisation of internal clocks, generations of beacons
- Power management
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements
- Association/Reassociation
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
  - scanning, i.e. active search for a network
- MIB - Management Information Base
  - managing, read, write (accessible via SNMP)
  - contain all information on current state of AP or station

WLAN – 802.11 WiFi

MAC Management : Synchronization using a Beacon (infrastructure)

Timing Synchronisation Function (TSF) for
- power management
- PCF (superframe prediction)
- FHSS (hopping sequence)

Quasi periodic transmission of beacons (time stamp + other information)
In an infrastructure network : beacons transmitted by AP



WLAN – 802.11 WiFi

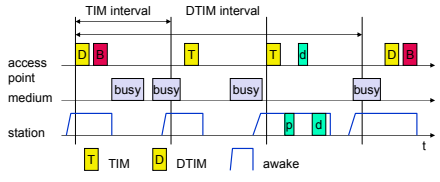
MAC Management : Power management

- Mobile means batteries => power saving is crucial
- Idea: switch the transceiver off if not needed
  - easy for transmitter, but for receiver ?
- States of a station: sleep and awake
- Data can be buffered at sender.
- Timing Synchronization Function (TSF)
  - stations wake up at the same time
  - sender informs the receivers if it has buffered data
  - these receivers stay awake

WLAN – 802.11 WiFi

MAC Management : Power saving with wake-up patterns (infrastructure)

- Infrastructure
  - AP buffers all dataframes for stations using power saving
  - Traffic Indication Map (TIM)
    - list of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)
    - list of broadcast/multicast receivers transmitted by AP



WLAN 802.11 MAC Management : Roaming

- No or bad connection? Then perform:
- Scanning
  - scan the environment, i.e., listen into the medium for beacon signals (passive scanning) or send probes into the medium and wait for an answer (active scanning)
- Reassociation Request
  - station sends a request to one or several AP(s)
- Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request
  - signal the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources

WLAN IEEE 802.11 – other developments

- 802.11c: Bridge Support
  - Definition of MAC procedures to support bridges as extension to 802.1D
- 802.11d: Regulatory Domain Update
  - Support of additional regulations related to channel selection, hopping sequences
- 802.11e: MAC Enhancements – QoS
  - Enhance the current 802.11 MAC to expand support for applications with Quality of Service requirements, and in the capabilities and efficiency of the protocol
  - Definition of a data flow ("connection") with parameters like rate, burst, period…
  - Additional energy saving mechanisms and more efficient retransmission
- 802.11f: Inter-Access Point Protocol
  - Establish an Inter-Access Point Protocol for data exchange via the distribution system
  - Currently unclear to which extend manufacturers will follow this suggestion
- **802.11g: Data Rates 54 Mbit/s, OFDM**
  - **Successful successor of 802.11b, performance loss during mixed operation with 11b**
- **802.11h: Spectrum Managed 802.11a**
  - **Extension for operation of 802.11a in Europe by mechanisms like channel measurement for dynamic channel selection (DFS, Dynamic Frequency Selection) and power control (TPC, Transmit Power Control)**

WLAN IEEE 802.11– other developments

- 802.11i: Enhanced Security Mechanisms
  - Enhance the current 802.11 MAC to provide improvements in security.
  - TKIP enhances the insecure WEP, but remains compatible to older WEP systems
  - AES provides a secure encryption method and is based on new hardware
- 802.11j: Extensions for operations in Japan
  - Changes of 802.11a for operation at 5GHz in Japan using only half the channel width at larger range
- 802.11k: Methods for channel measurements
  - Devices and access points should be able to estimate channel quality in order to be able to choose a better access point of channel
- 802.11m: Updates of the 802.11 standards
- **802.11n: Higher data rates above 100Mbit/s**
  - **Changes of PHY and MAC with the goal of 100Mbit/s at MAC SAP**
  - **MIMO antennas (Multiple Input Multiple Output), up to 600Mbit/s are currently feasible**
  - **However, still a large overhead due to protocol headers and inefficient mechanisms**
- 802.11p: Inter car communications
  - Communication between cars/road side and cars/cars
  - Planned for relative speeds of min. 200km/h and ranges over 1000m
  - Usage of 5.850-5.925GHz band in North America

WLAN IEEE 802.11– other developments

- 802.11r: Faster Handover between BSS
  - Secure, fast handover of a station from one AP to another within an ESS
  - Current mechanisms (even newer standards like 802.11i) plus incompatible devices from different vendors are massive problems for the use of, e.g., VoIP in WLANs
  - Handover should be feasible within 50ms in order to support multimedia applications efficiently
- 802.11s: Mesh Networking
  - Design of a self-configuring Wireless Distribution System (WDS) based on 802.11
  - Support of point-to-point and broadcast communication across several hops
- 802.11t: Performance evaluation of 802.11 networks
  - Standardization of performance measurement schemes
- 802.11u: Interworking with additional external networks
- 802.11v: Network management
  - Extensions of current management functions, channel measurements
  - Definition of a unified interface
- 802.11w: Securing of network control
  - Classical standards like 802.11, but also 802.11i protect only data frames, not the control frames. Thus, this standard should extend 802.11i in a way that, e.g., no control frames can be forged.
- Note: Not all "standards" will end in products, many ideas get stuck at working group level
- Info: www.ieee802.org/11/, 802wirelessworld.com, standards.ieee.org/getieee802/

RF-based indoor positioning

DraMCo research group

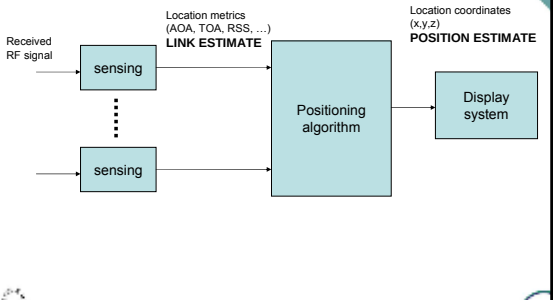
Introduction

- Positioning of objects and persons ***indoor*** based on ***RF-signals***
  (signals from wireless LAN and PAN: WiFi, ZigBee, UWB, RFID, …)

RTLS : Real-time Locating Systems

- Applications
  - Tracking and tracing
    - logistics: just-in-time and in-sequence delivery, supply management, …
    - healtcare institutes: locating (critical/emergency) equipment, patient tracking, ….
  - Location based services (context awareness)

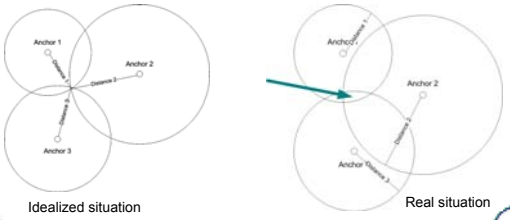
RF based indoor positioning



RF-based indoor positioning

- LINK ESTIMATION
  - Signal strength: RSS *(Received Signal Strength)*
  - Time delay : TOA *(Time Of Arrival)*
  - Direction : AOA *(Angle Of Arrival)*
- POSITION ESTIMATION
  - Most straight forward:

link estimation -> estimate distance between nodes



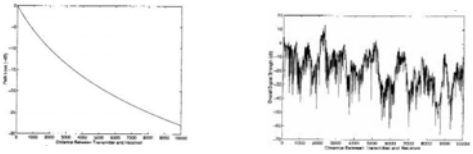
Idealized situation

Real situation

RSS

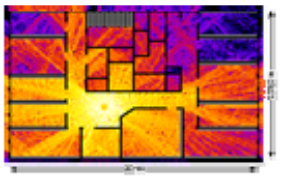
- RSS is most popular metric for WLAN, WPAN localization
  - Most receivers have an RSSI circuit
  - Can be measured during normal datacommunication (without requiring any additional bandwidth or energy)
  - Average power can be measured without any spefic knowledge of the transmitted pulse shape
  - Easy and inexpensive implementation

But notoriously unpredictable !! -> only usefull for rough position estimation



RSS – fingerprinting

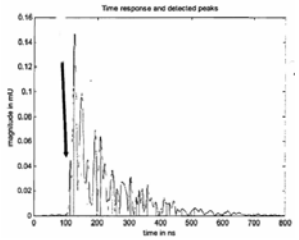
- Alternative solution
  - Pre-measured training points (fingerprinting) and pattern recognition algorithms
    - Popular in WLAN
    - Many variants
    - Ray trancing assistance



  - 2 separate phases:
    - Offline phase (calibration)
      A fingerprint database of the environment is constructed
    - Online phase
      Localization by looking into the database
  - Time-consuming calibration and enviroment is changing

TOA

- Most popular for UWB localization (also used in GPS)
  - Requires adequate bandwidth to isolate the multipath components
- Needs stable and accurate synchronization
- *Possibility* for very precise localization

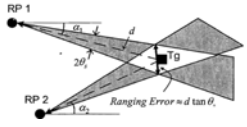


AOA

Angle of Arrival

- In cellular networks : sectored antennas in infrastructure
- MIMO

- Accuracy is proportional to the angle of the antenna
- If direct path is not available : difficult

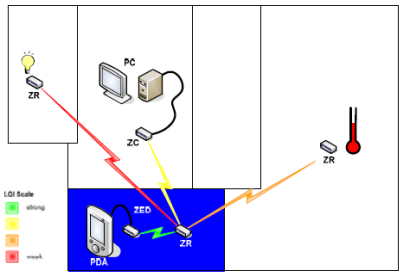


Available technologies

- WIFI based
  - Ekahau
  - CISCO
  - Aeroscout
- ZigBee
- UWB
  - Ubisense

RTLS DOMOTICS APPLICATION with ZIGBEE

- *Developed by DraMCo (KaHo) in cooperation with students*
- PDA enabled with ZigBee, very room has a ZigBee node
- RSS to determine current room of PDA



RTLS DOMOTICS APPLICATION with ZIGBEE

- Screen of PDA changes according to the room
- -> control the parameters of that room from the PDA (light, temperature,...)
- Location dependent service on the PDA

WiFi based technologies

		ekahau	AeroScout	Cisco Systems
Positioning		Full locating	Full locating Chokepoint	Full locating (Chokepoint supported)
Technology		Client based RSSI / Infrastructure based RSSI	TDOA / Infrastructure based RSSI	Infrastructure based RSSI
Infrastructure		Any 802.11 AP / Partner WiFi infrastructure	Dedicated AeroScout HW / Partner WiFi infrastructure	Cisco AP's
Usage		Indoor, walled environments	Open spaces / outdoor / Indoor, walled environments	Indoor, walled environments
Accuracy		With filter: 1m (2-3 sec delay) Without filter: 2m / NVT	3-10m	3-4m
Clients		Ekahau tags can be tracked Other WiFi devices can be tracked when Ekahau is installed (software clients)	AeroScout tags can be tracked Other WiFi devices can be tracked	Every ccx compatible WiFi client can be tracked
Tags	Battery life	- / ++	NVT / ++	NVT
	Extras	Display to send messages Industrial tags with call buttons Tags with integrated temperature sensor Buttons to indicate accident, disaster,...	Tamper proof Telemetry sensors (motion, humidity, pression,...) Buttons to indicate accident, disaster,... Many mounting options WiFi - GPS tag (new!) WiFi - UWB tag (new!) WiFi - Ultrasound tag (new!)	NVT
Support		+++ / ++		-
General		Great site survey tool Great support Relatively easy setup and maintenance Good end user applications Easiest out of the box solution Association is needed	Great end user application Good support Promising player in integration of WiFi, GPS, UWB,... Free choice of database (SQL, Oracle,...) Complicated installation (course needed)	Fewer support Most expensive Simple end user application with few functionality

Thank you for your attention

... looking forward to meet you in Ghent

www.dramco.be