Technische Universität Darmstadt





TK3: Ubiquitous Computing

Chapter 2: Infrastructure

Part 2: Communication Technology

Lecturer: Dr. Immanuel Schweizer

Copyrighted material – for TUD student use only



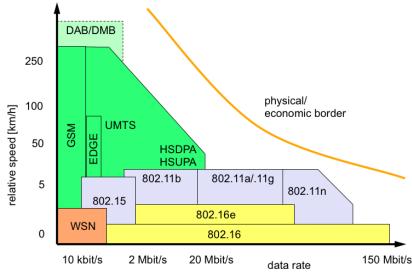
Wireless Classification



- Five major most relevant classes of wireless (non broadcast) networks:
 - Wireless Wide Area Networks
 - GSM, UMTS, LTE
 - Wireless Distribution Networks
 - WiMAX, LTE
 - Wireless Local Area Networks (WLAN)
 - **802.11**
 - Wireless Personal Area Networks (WPAN)
 - Bluetooth, (ZigBee), NFC
 - Wireless Sensor Networks (WSN)
 - ZigBee



- in general: "acronym / classification Babylon reigns!"
- "4G convergence" → maybe this looks different in 5-10 years





Wireless Wide Area Networks



- Development from 2G to 4G (user data rates)
 - GSM (2G): 9.6/14.4 kbit/s
 - GSM+GPRS (2.5G): 53 kbit/s (downlink)
 - GSM+EDGE (2.5G): up to 384 kbit/s
 - UMTS (UTRA FDD/W-CDMA, 3G): up to 384 kbit/s
 - UMTS+HSDPA (3.5G): up to 1.8 Mbit/s first, meanwhile 3.6 and 7.2
 - LTE (3GPP) (marketed as 4G, not according to IMT standards): Peak Upload: 75 Mbit/s Peak Download: 300 Mbit/s
 - LTE Advanced (4G): Peak Upload: 500Mbit/s Peak Download: 1Gbit/s
- Data rates depend very much on
 - Mobility, direction (uplink/downlink), signal strength, cell load, error rate
- Other systems
 - cdmaOne (2G), cdma2000 1X (2.5G), cdma2000 1X EV-DO (3G)
 - Unidirectional (broadcast) systems as an addition: DVB (-T, -H), DMB



Basics: Cellular Networks



For our lecture: a) cell sizes (roughly) categorized according to radius, e.g.:

pico:	r = 50 m	private (home, office)	PicoNet
micro	r = 500 m	inner city (many users)	WLAN, PLMN
macro	r = 10 km	,standard GSM'; city, road	PLMN
hvper	r = 30 km	rural area	PLMN. HALO

overlay r = 200 km high tier antenna coverage HALO, LEO

PLMN: Public Land Mobile Network; LEO: Low Earth Orbit (Satellite)

■ HALO: High Altitude Long Operations; flying/floating platforms

Many categorizations of "cell sizes" exist: LTE "femto cell" is privately operated BTS i.e. "pico" above

b) one example for alternative categorization:
 according to 'outreach':
 Global

Satellite

Pico-CelMicro-Cel Macro-Geldik

BTS

"coverage" (reach):
 in reality, odd shape



Basics: Cellular Networks



Roaming (option in cellular networks, some degree always supported):

- MS may move freely between cells, even (!) switched-off
- MS are "found", identified upon switch-on (cf. incoming calls)

Handover (option in cellular networks):

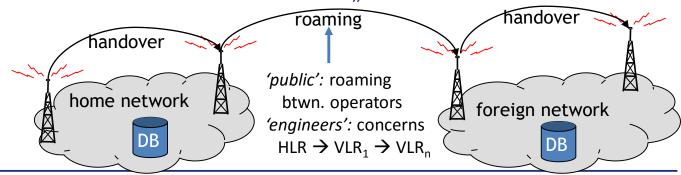
- cross cell boundaries during existing connection (mobile phone: active phone call)
- connection "handed off" to new cell ...
- ... w/o interruption & neticeable effect to user(s) [might be between operators, too]

Home location register HLR:

- each operator (T-Mobile, O2, ...) has at least one HLR
- holds all subscriber data: contract data, current location, ...
- holds pointer to current VLR

Visitor location register VLR

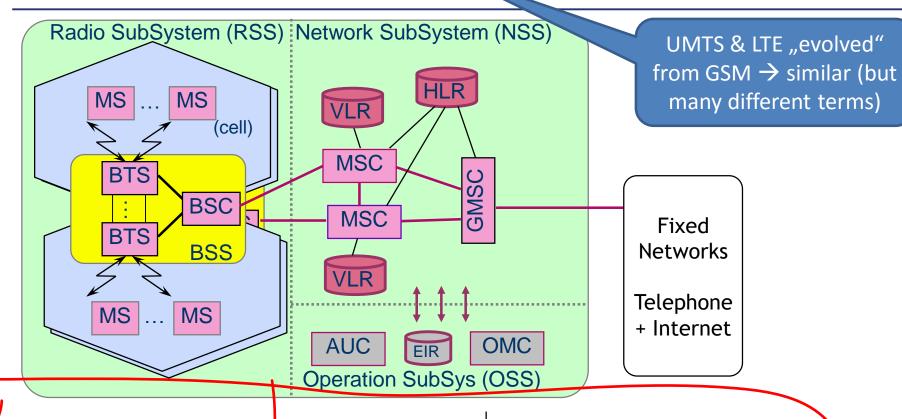
holds all admin. data relevant for the cell in which user "roams"





GSM Architecture





MS: Mobile Station

BTS: Base Transceiver Station

BSC/BSS: Base Station Controller / Subsystem

MSC: Mobile Service Switching Center

GMSC: Gateway MSC

VLR: Visitor Location Register

HLR: Home Location Register

AUC: AUthentication Center

EIR: Equipment Identity Register

OMC: Operation & Maintenance Center



GSM Overview



- Origin: Intl. Telecom. Union ITU \rightarrow Eur. branch CEPT \rightarrow groupe spéciale mobile
- Today: a) European standards rather by ETSI (telecoms + vendors +...)
 - b) name change: Global System for Mobile communication
- Per frequency channel: 200kHz, 256kbps raw symbols + slot guard time
 - \bullet 8 slots \rightarrow phys. channel: pair (freq. channel no. C_n ; timeslot no. t_m), t_m =0..7
 - 32kbps raw symbols per channel; 24,7 kbps raw bits per channel
 - multiframes within (C_n, t_m): 26 (or 51) slots; x-in26/51: logical channels
 - Full rate channel: 24 of 26 slots → 22,8 kbps
 - Half rate channel: 12 of 26 slots → 11,4 kbps
 - Full rate speech: 13kbps voice + 9,8 kbps FEC (forward error correction)
 - Full rate data: 2,4 / 4,6 / 9,6 kbps plus CRC plus FEC (CRC: cyclic redundancy check: checksum)



Data services in GSM





(Circuit Switched Data)

- Data transmission standardized with only 9.6 kbit/s
- Advanced coding allows 14,4 kbit/s
- Not enough for Internet and multimedia applications
- HSCSD (High-Speed Circuit Switched Data)
 - Bundling of several time-slots to get higher AIUR
 (Air Interface User Rate), e.g., 57.6 kbit/s using 4 slots, 14.4 each
 - Advantage was: ready to use, constant quality, simple
 - Disadvantage: channels blocked (no voice transmission; cost!)
- Disadv.: equipment not ready for simultaneous xmit/rcv → ≤4 (2?) slots
 GPRS General Packet Radio Service)
 - Packet switching
 - Using free slots only if data packets ready to send (e.g., 115 kbps using 8 slots temporarily: 8*14.4)
 - Standardization 1998, introduction 2000



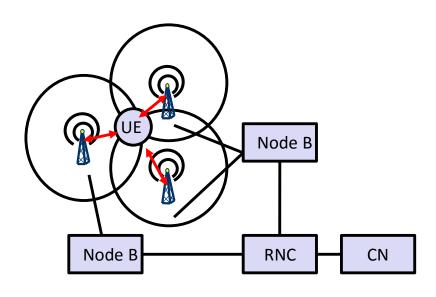
Wireless Wide Area Networks



- UMTS (Universal Mobile Telecommunications System)
 - One out of several 3G standards, but the most successful
 - Builds directly on GSM+GPRS infrastructure

Components

- Node B = BTS
 - Controls several antennas
- RNC: Radio Network Controller
 - Controls several Node Bs
- UE: User Equipment
- CN: Core Network





UMTS vs. GSM



- Introduces CDMA (+)
 - Allows higher data rates
- Soft handover (+)
 - GSM: MS is only connected to a single BS (hard handover)
 - UMTS: MS can be connected to 3 BSes (soft handover)
- More intelligent and dynamic SDMA (+)
 - All cells can use the same frequencies
 - Multipath propagation treated similarly to receiving signal from different senders
- Requires tight power control (-)
 - Signals from different MSes must arrive with roughly same power at BS (requirement of CDMA correlation-based detection)
 - 1500 power control cycles/s
- Cell Breathing (-)
 - Sending with high data rate increases noise for other MSes
 - Other MSes must also increase power -> more noise
 - Devices at the edge reach max. power limit -> cell virtually shrinks



Data services in UMTS



- HSDPA (High Speed Downlink Packet Access)
 - uses 16-QAM instead of QPSK and multicode transmission
 - HS-DSCH (High Speed Downlink Shared Channel)
 - shared by all HSDPA users connected to the NodeB
 - dynamically shared between users
 - supports adaptive coding and modulation
 - 16-QAM and 5 codes -> ~ 3,6 Mbit/s (category 6)
 - 16-QAM and 10 codes -> ~ 7,2 Mbit/s (category 8)
 - more is hardly achievable under real conditions, but defined up to 84,4
 Mbit/s (category 28)
- HSUPA High Speed Uplink Packet Access)
 - uses 16-QAM instead of QPSK and multicode transmission
 - cannot use as many codes as in HSDPA, because more interference on the uplink channel
 - 16-QAM and 2 codes -> ~ 1,4 Mbit/s (category 3)





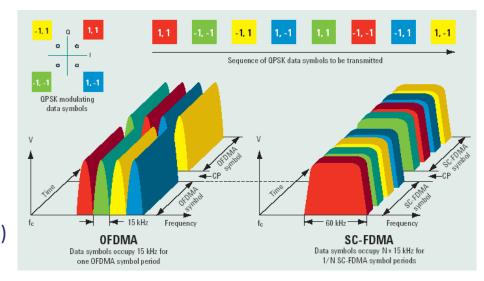
- Long Term Evolution (LTE): 3.9G, frozen with 'release 9' (2010)
 - LTE-Advanced starts with ,release 10' (2011)
 - LTE builds on UMTS → aims to be a Wireless Wide Area Network
 - Many components of the 3G architecture can be reused
 - Uses different radio interface: CDMA → OFDMA & SC-FMDA
- LTE is an all IP network
 - Supports both IPv4 and IPv6
 - No basic provision for voice → use VoIP, or:
 - Several ,evolutionary' substandards: combine 3G-for-voice w/ LTE-for-data
- LTE has lower latency: RoundTrip Time (RTT) ~ 10ms (HSPA: ~ 100ms)
- Includes/supports "almost everything": FDD and TDD and ...:
 - Broadcast (mobile TV) not always implemented
 - Flexible allocation (blocks of subframes for limited time → fast bandwidth variation)
 - Large # of bands (from ~700 to ~3600 MHz), different bandwidths (1.4, 3, N*5MHz)
 - Various speeds (up to 500 km/h), cell sizes: ~100m ... 100 km → rural "last mile"
 - LTE-Advanced (4G): largely asymmetric transmission up-/downlink



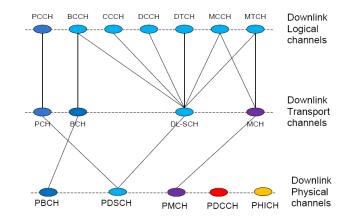


- Downlink: OFDMA (OFDM multiple access)
 - peak downlink speeds using 64QAM [Mbit/s]: 100 (SISO), 172 (2x2 MIMO), 326 (4x4 MIMO)
- Uplink: SC-FDMA (Single carrier FDMA)
 - Reduced peak to average power ratio
 - Peak uplink speeds, in Mbit/s
 50 (QPSK), 57 (16QAM), 86 (64QAM)

(3-4x better spectral efficiency than HSDPA/HSUPA)



- 3-Layer Channel Multiplexing
 - Here, a glimpse at the downlink channels $\rightarrow \rightarrow$
- LTE-Advanced:
 - Coordinated beamforming, multi-carrier (spectrum aggregation), relay support, and more ...



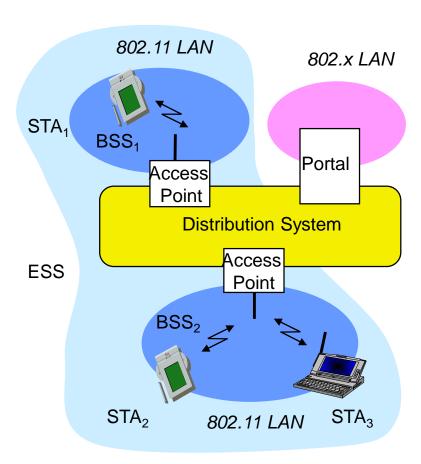


Wireless Local Area Networks (WLAN)



IEEE 802.11 family of WLAN standards

- supports "Infrastructure Networks" and "AdHoc Networks"
- supports "WLAN cells" -> roaming
- operates in unlicensed ISM bands (industry, science, med.)
- Typically only best effort MAC, no service guarantee
- Infrastructure Network Architecture
 - Station (STA)
 - Basic Service Set (BSS)
 - group of stations using same radio freq.
 - Access Point
 - station integrated into WLAN and distribution system
 - Portal
 - bridge to other (wired) networks
 - Distribution System
 - interconnection net; one logical net = ESS: Extended Service Set based on several BSS





802.11: Standards



Standard	802.11a	802.11b	802.11g	802.11n
Year	1999	1999	2003	2009
RF Band (GHz)	5	2,4	2,4	2,4 or 5
Max. raw data rate (Mbps)	54	11	54	600
Modulation	OFDM	DSSS or CCK	DSSS, CCK or OFDM	DSSS, CCK or OFDM
# of spatial streams	1	1	1	1-4

802.11 ac: 2012+, 5GHz (2.4 for 11n compat.), >1Gbps, up to 8 spatial streams

- Modulations (FH was used in 'legacy' 802.11-1997, even Infrared was defined):
 - DSSS (Direct Sequence Spread Spectrum)
 - CCK (Complementary Code Keying) DSSS variant, see later
 - OFDM (Orthogonal Frequency Division Multiplex)



802.11 - MAC Layer



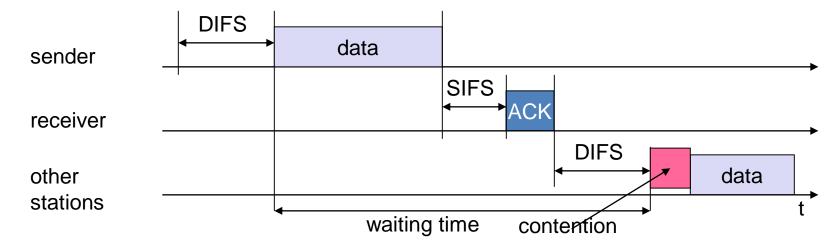
- Traffic services
 - (Asynchronous Data Service (mandatory)
 - exchange of data packets based on "best-effort"
 - support of broadcast and multicast
 - Time-Bounded Service (optional)
 - implemented using PCF (Point Coordination Function)
- Access methods: DFWMAC = Distributed Foundation Wireless MAC (distributed "D" or polling based "P" access ctrl. functions DCF/PCF)
 - DFWMAC-DC 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
 - DFWMAC-(PCF (pptional)
 - access point polls terminals according to a list







- Remember: CSMA/CA
 - DIFS = Data Inter-Frame Spacing, SIFS = Signal Inter-Frame Spacing
- Here: acknowledging 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



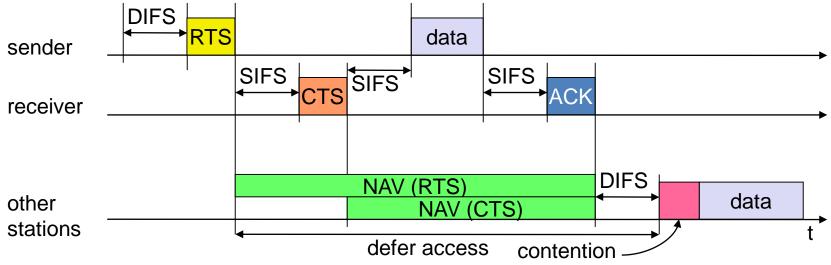


802.11 - DFWMAC w/ RTS/CTS



Sending unicast packets

- Station can send RTS with reservation parameter after waiting for DIFS (reservation determines amount of time the data packet needs medium)
- Acknowledgement via CTS 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
- Optional fragmentation (data fragmented → reduced error probability)



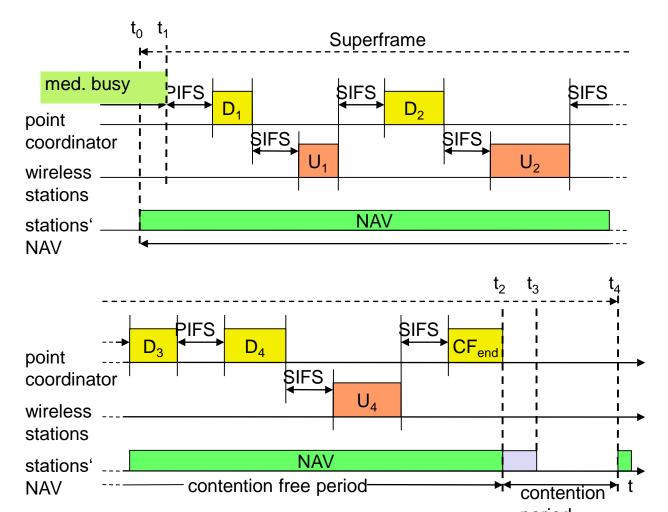
NAV: Net allocation vector (min. forbidden time for other stations)



802.11 - DFWMAC w/ PCF



point coordinator determines access (down/up link); polling & contention phases may alter



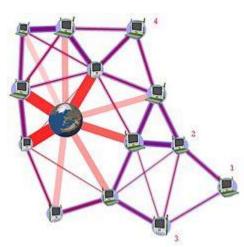


802.11s



- Adding Mesh Networking
 - No access point needed; Multihop wireless network enabled

- Addition on top of 802.11
 - Peer Link Management protocol for neighbor discovery
 - Nodes transmit beacons
 - Link formed upon receiving neighbor beacons
 - Hybrid Wireless Mesh Protocol (HWMP);
 - uses MAC addresses for "routing" thus called path selection
 - Proactive protocol; Modification of AODV





802.11s



- 3 types of nodes; each can forward frames
 - Mesh Point (MP)
 - Supports Peer Link Management and HWMP
 - Mesh Access Point (MAP)
 - A normal Access Point augmented with mesh functionality
 - Mesh Portal (MPP)
 - A MP with Internet access acting as Gateway
- Applications
 - One Laptop per Child using pre-802.11s
 - Part of the Linux kernel (>=2.6.26)
 - What about smartphones? Good idea, but not yet implemented!



Wireless Personal Area Networks



Bluetooth: Goals

- Provide small, inexpensive, power-conscious radio system
- Personal short-range (~10m) networks
- "Cable replacement" not really intended as WLAN technology
- Embedded in many devices: mobile phones, laptops, PDAs, cameras
- 1.The cordless desktop (headset, loudspeaker... → audio!)
- 2.Object Exchange (OBEX) Push (send images from phone to PC)
- 3. Tethering (Internet access from PC via GSM phone)



Profiles: define functionality for connection of "logically matching" devices (e.g., headset profile, handsfree profile, ...)

- Origin of technology:
 - Five founders: Nokia, Ericsson, Intel, IBM, Toshiba) → 1000+!!
 - Idea: advance "wireless car key" chip ("1\$-world") to appliances
- Origin of name:
 - Danish king Bluetooth (940-981), unified (!) Danemark & Norway



Bluetooth: Basics



Bluetooth Versions:

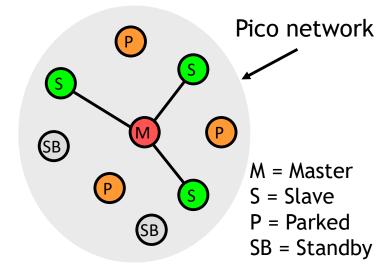
- 1.1, 1.2: speed, HW functionality → better communication, audio, ...
- 2.0: Enhanced Data Rate (EDR): up to 2.1 Mbps, more profiles
- 3.0: Ultra WideBand (UWB)
- 4.0: Bluetooth low energy (BLE)

Piconet:

- Each piconet has one master and ≤ 7 slaves
- Master controls medium access (strict polling scheme)
- Master determines hopping sequence
 - Different networks use different hopping sequences (low probability of collision)
- Master role can be switched (optional)
- Several low-power modes
- Security model requires pairing
 - almost always: manual, requires user interaction

Scatternet:

- multiple piconets can form a scatternet
- node is slave in one piconet and master in another





Bluetooth Baseband



"Radio" Layer:

- Frequency: 2.4 2.4835 GHz (most of Europe, USA)
- 79 (.fr, .jp, .es: 23) channels ("hop carriers")

CDMA-FH:

- CDMA-FH: 1.600 hops/s -> slot is 625μs, 1 Mbps
- Frequency usually hops after each slot
- TDD: all even-numbered slots are reserved for the master
- Multi-slot packets: occupy 3 or 5 slots, frequency not changed

Connection types / Packet types

- SCO (synchronous connection-oriented) link, telephony: "reserve each n-th slot"
 - HV1/2/3: HiFi voice, all 1-slot, reserves every 2nd/ 4th /6th slot, use FEC1/3, 2/3, and none
- ACL (asynchronous connectionless) links for everything else
 - DM1/3/5: data medium, 3 & 5 are multislot, 2/3 FEC
 - DH1/3/5: data high, 3 & 5 are multislot, no FEC

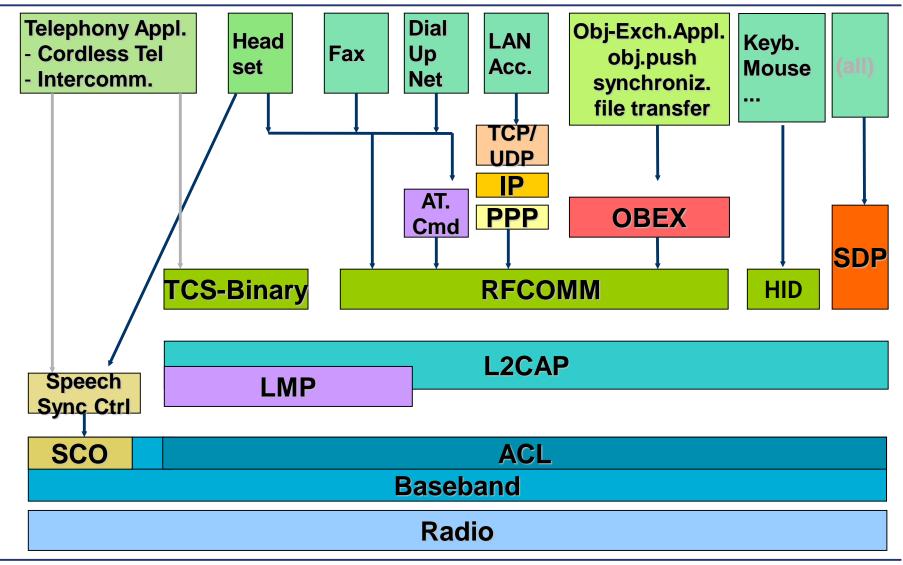
Error correction schemes: none, "1/3" or "2/3"

- 1/3: each bit individually repeated 3 times
- 2/3: groups of ten bits are expanded to 15 bits (5 parity bits)



Bluetooth Protocol Stack







Bluetooth Protocol Stack



Bluetooth Protocol Stack

- Link Manager Protocol LMP responsible for SCO/ACL link mgmt.
- L2CAP: logical link control & adaptation protocol: general API
- TCS-bin (telephony control protocol specification binary) common management for telephony applications
- RFCOMM emulates serial link "cable" (up to 60 logical links)
- AT command emulation for modem compatibility
- SDP (service discovery protocol) in later chapter
- OBEX (object exchange) is compatible w/ IrDA: send biz card, photo
- HID (human interface device) is compatible w/ USB

Bluetooth Profiles

- A profile specifies all details needed to use, connect, control, ... a device
 - parts of the Bluetooth stack used
 - options, parameters, SDP record
- >30 profiles are defined
- Example: Headset Profile specifies
 - audio is transported via SCO, audio encoding, ...
 - device is controlled via a RFCOMM connection using AT commands
 - AT command set



Wireless Sensor Networks



- Key characteristics
 - Network is embedded in the environment
 - Nodes measure and influence the environment
 - Nodes process information and communicate it wirelessly
 - Network is self-organizing and energy efficient
 - Potentially high number of nodes at very low cost per node
- Differences to WLAN, WPAN, classical ad-hoc networks
 - WSN is much more application specific, application driven
 - Device power in WSNs is rather limited, lower data rates, embedded
 - WSNs can be large scale with thousands of nodes
 - WSNs are data centric, individual node may be dispensable
 - Much lower cost per node



Wireless Sensor Networks



- Machine and vehicle monitoring
 - Sensor nodes in moveable parts
 - Monitoring of temperatures, fluid levels, ...
 - Calculation of maintenance intervals
- Smart Cities
 - Intelligent buildings, building monitoring
 - Intrusion detection, mechanical stress detection
 - Smart heating, ventilating, air conditioning
- Health & medicine
 - Long-term monitoring of patients with minimal restrictions
 - Assisted Living
- Environmental monitoring, person tracking
 - Monitoring of wildlife and national parks
 - Cheap and (almost) invisible person monitoring
 - Monitoring demilitarized zones, ...
- Logistics
 - Dataloggers: Temperature, Humidity, Acceleration/Shock
- ... and many more









ZigBee





- Bluetooth Desktop / Personal Area Net: few, "valued" devices
- ZigBee scales up to sensor networks ("smart dust") in terms of power, #of nodes, management …

Market Name Standard	GPRS/UMTS (TDMA/CDMA)	Wi-Fi™ 802.11b	Bluetooth™ 802.15.1	ZigBee™ 802.15.4
Application Focus	LongDist. Voice/Data	Web, Email, Video	Cable Replacement	Monitoring & Cntrl
System Resources	16MB+	1MB+	250KB+	4KB - 32KB
Battery Life (days)	1-7	.5 - 5	1 - 7	100 - 1,000+
Network Size	(1)	(32)	7	255 / 65,000
Bandwidth (kb/s)	14 - 2000	11,000+	720	20 - 250
Transmission Range (m)	1,000+	1 - 100	1 - 10+	1 - 100+
Success Metrics	Reach, Quality	Speed, Flexibility	Cost, Convenience	Reliab., Power, Cost



ZigBee Node Types, Protocol Stack

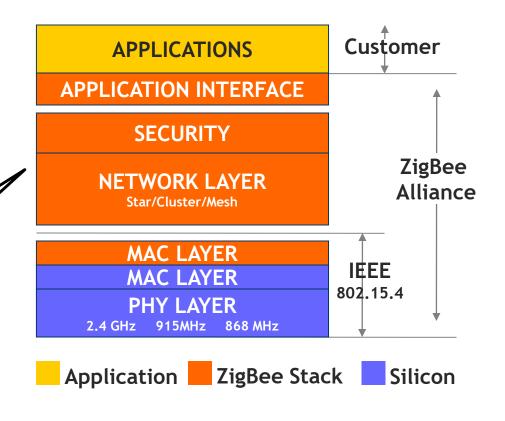


- a) FFN vs. RFN: Full Function Nodes—Reduced Function Nodes
- b) Coordinator vs. Router vs. EndNode

Only EndNode may (!) be RFN

- Microcontroller utilized
- FFN protocol stack <32 k
- RFN protocol stack ~4k
- Coordinators: extra RAM (DBs f. nodes/transactions/pairing)
- PHY: OQPSK (2.4GHz); CDMA
- MAC: CSMA/CA

ZigBee Net can be replaced w/ IEEE802 MAC + IP







Key thesis

- One size does not fit all!
- Many different wireless systems already exist and there will be more in the future
- You can't beat physics ... thus different systems are needed
 - Different ranges, data rates, robustness, power consumption ...
- Performance fluctuations, interrupts, lack of resources etc. have to be taken into account by applications
- Convergence will come, but ...
 - Applications will have to run on many different networks, thus adaptivity is important
 - Convergence on the network layer, but still many open issues
 - Security, reliability, maintenance, charging models, quality-of-service...



Summary: WWAN



- Wireless Wide Area Networks
 - Mobile voice comm. has become a "ubiquitous demand" anyway
 - Mobile data services / mobile Internet use growing
- GSM (2G)
 - Wide area cellular network
 - Circuit-switched, designed for voice comm. only
- EDGE (2.5G)
 - adds packet-switching extension for free slots
- UMTS (3G)
 - CDMA s. FDMA+TDMA: better spectrum utilization and robustness
 - fo guard bands / guard times necessary
 - frequencies can be reused in adjacent cells
 - channel assignment much more flexible:
 silence (speech) -> no data to send -> less noise for other comm.
 - preading -> more robust against narrowband interference
- HSDPA // HSUPA (3.5G)
 - QFDM in tead of CDMA
 - better spectrum utilization, higher data rates
 - less interference between cells (even SFNs for downlink)
- LTE ("3.99G")
 - less latency, packet switching only, All-IP networks



Summary: WLAN



- Today: 802.11 family is the ubiquitous standard
 - competitors have disappeared, e.g., HiperLAN
- Substandards
 - 802.11b: 2.4 GHz, DSSS (2 Mbit/s), CCK (11 Mbit/s)
 - 802.11a: 5 GHz, OFDM (54 Mbit/s)
 - 802.11g: 2.4 GHz, OFDM (54 Mbit/s)
 - 802.11n: 2.4/5 GHz, OFDM (150...600 Mbit/s)
- Wireless Distribution Networks
 - 802.16 / WiMAX
 - Directed connections, enable DSL connectivity for rural areas
 - Terminal mobility requires 802.16e
 - Directly competed with HSDPA/HSUPA and LTE
 - WiMAX is an "extended LAN technology" does not have the infrastructure components of WWANs
 - WiMAX does not integrate in existing GSM/UMTS infrastructure
 - In the US Sprint has started with WiMAX is now switching to LTE!



Summary: WPAN, etc.



- Which one is best for my Ubicomp application? A discussion of: Bluetooth, ZigBee & WLAN
- Bluetooth
 - "designed to connect a headset wirelessly to a cellphone"
 - most other things turn out to be a hack (see HIDs below)
 - Pros:
 - easy to implement, because of simple modulation and MAC
 - relatively low power
 - Cons:
 - not much more than "cable replacement"
 - pairing procedure unsuitable for WSNs or ad-hoc networks
 - strict master/slave polling scheme
 - nonsense for HID devices
 - sensors could not push data to the master
 - high latency
 - IP data connections are "circuit switched"
 - IP traffic tunneled using PPP through an RFCOMM link
 - broadcast functionality of wireless network lost
 - only 7 slaves



Summary: WPAN, etc.



ZigBee

- designed for sensor networks, where typically
 - many nodes are interconnected
 - nodes sleep most of the time
 - nodes occasionally send small amounts of data

■ Pros:

- very low power
- software stack kept simple (smaller than Bluetooth)
- flexible radio layer: 10m 1.5km range
- flexible MAC: non-beacon networks, beacon-enabled networks
- supports large networks
- supports different network topologies (star, mesh, hybrid)

Cons:

low data rate



Summary: WPAN, etc.



WLAN

- complex radio, signal processing, and software stack
- requires high power
 - general rule: energy needed to decode a signal is proportional to data rate

Convergence? (WPAN,WLAN,WSN)

- possible solution: use two radios
 - MAC radio: simple modulation, low bandwidth, low power
 - data radio: modulation selectable based on demand
- research prototypes exist, but currently there is no real business case
- related: Cognitive Radio: "fully reconfigurable radio that automatically changes its communication variables in response to network and user demands"

Cognitive Radio - Goals

- Spectrum Sensing: detecting unused spectrum
- Spectrum Management: select spectrum that best meets user reqs.
- Spectrum Mobility: adapt to changes
- Spectrum Sharing: similar to MAC

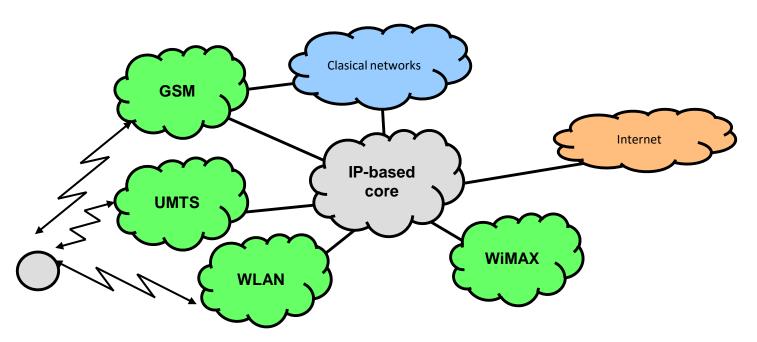


Convergence – the 4th Generation



Trends

- Key idea: Always Best Connected (ABC)
- Many different wireless & mobile systems will co-exist due to physics, applications, limitations, key properties
- Big mobile operators will also operate WLAN, etc.





Inlet: Enabling Technologies



