EEC173B/ECS152C, Winter 2006

Wireless Personal Area Networks (PAN)

- *Bluetooth and Wireless PAN (802.15)*
- *IEEE 802.15.4 and Zigbee*
- *RFIDs*

Acknowledgment: Selected slides from Prof. Schiller

What is a PAN?

WAN 

LAN

MAN 

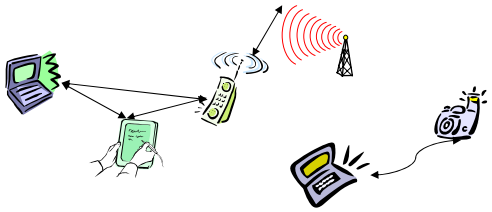

PAN

Acknowledgment: Selected slides from Prof. Schiller

Bluetooth

- Short range (10 m), low power consumption, 2.45 GHz ISM
- Voice and data transmission, approx. 1 Mbit/s gross data rate
- Universal radio interface for ad-hoc wireless connectivity
- Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
- Embedded in other devices

One of the first modules (Ericsson).



3

Bluetooth: History

- 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
  - 1999: erection of a rune stone at Ericsson/Lund ;-)
  - 2001: first consumer products for mass market, spec. version 1.1 released
- 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

Bluetooth™

4

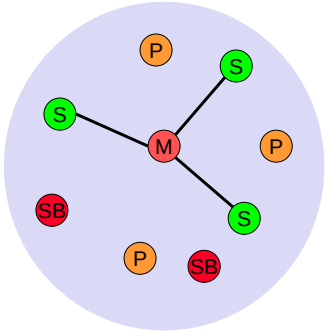
Bluetooth Characteristics

- 2.4 GHz ISM band, 79 RF channels, 1 MHz carrier spacing
  - Channel 0: 2402 MHz … channel 78: 2480 MHz
  - G-FSK modulation, 1-100 mW transmit power
- FHSS and TDD
  - Frequency hopping with 1600 hops/s
  - Hopping in a pseudo random fashion, determined by a master
  - Time division duplex for send/receive separation
- Voice link – SCO (Synchronous Connection Oriented)
  - FEC (forward error correction), no retransmission, 64 kbit/s duplex, point-to-point, circuit switched
- Data link – ACL (Asynchronous ConnectionLess)
  - Asynchronous, fast acknowledge, point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched
- Topology
  - Overlapping piconets (stars) forming a scatternet

5

Piconet

- Collection of devices connected in an ad hoc fashion
- Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)
- One unit acts as master and the others as slaves for the lifetime of the piconet
- Master determines hopping pattern, slaves have to synchronize
- Each piconet has a unique hopping pattern (called FH channel)
- Participation in a piconet = synchronization to hopping sequence
- Multiple devices use TDMA for channel access
- Parked devices remain synchronized, but do not transmit data.

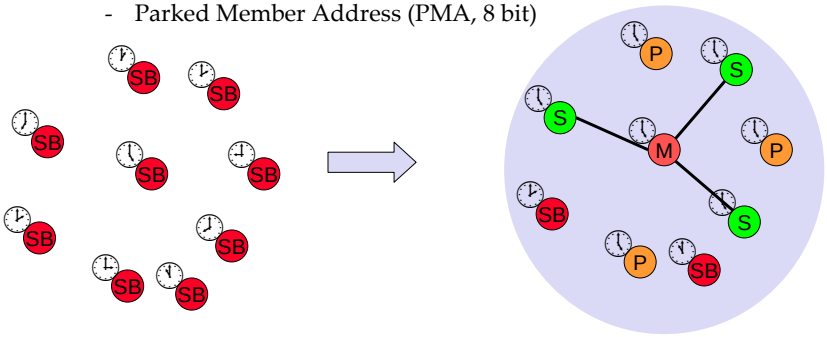


M=Master P=Parked
S=Slave SB=Standby

6

Forming a piconet

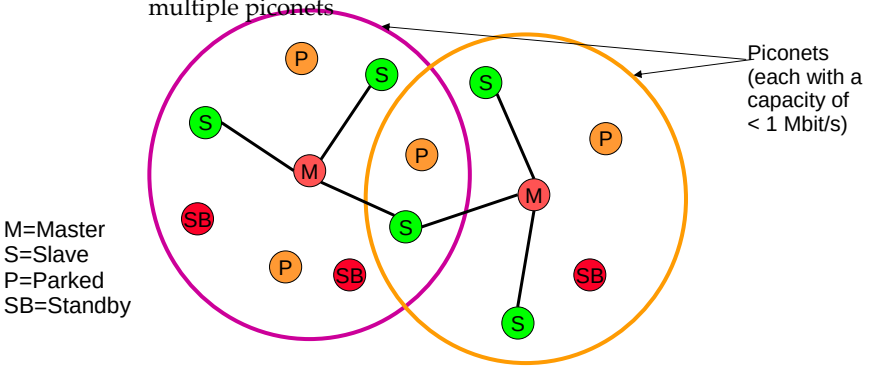
- Master gives slaves its clock and device ID
  - Hopping pattern: determined by device ID (48 bit, unique worldwide)
- Tens of piconets can coexist in the same coverage range
  - Each link is encoded and protected against eavesdropping
- Addressing
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)



7

Scatternet

- Linking of multiple co-located piconets through the sharing of common master or slave devices
  - Devices can be slave in one piconet and master of another
- Communication between piconets
  - Devices jumping back and forth between the piconets
  - A slave can adjust its frequency hopping to participate in multiple piconets



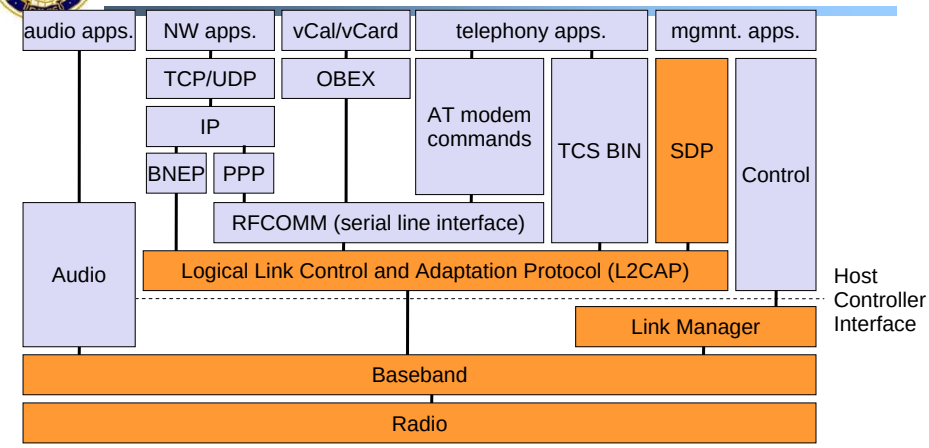
8

Core Protocols

- Radio
  - Specifies air interface, frequency, use of frequency hopping, modulation scheme and transmission power
- Baseband
  - Concerned with connection establishment within a piconet, addressing, packet format, timing and power control
- Link manager protocol (LMP)
  - Responsible for link setup between Bluetooth devices and ongoing link management
- Logical link control and adaptation protocol (L2CAP)
  - Adapts upper-layer protocols to the baseband layer
- Service Discovery Protocol (SDP)
  - Device information, services and their characteristics can be queried to establish a connection

9

Bluetooth protocol stack



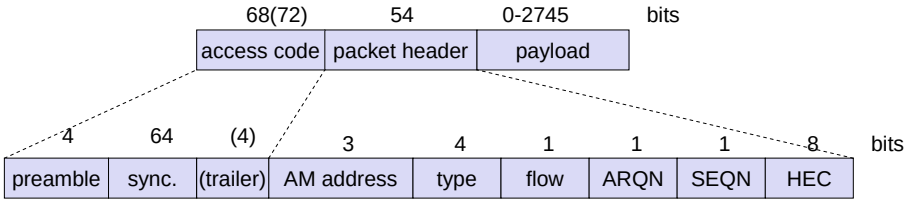
AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.

10

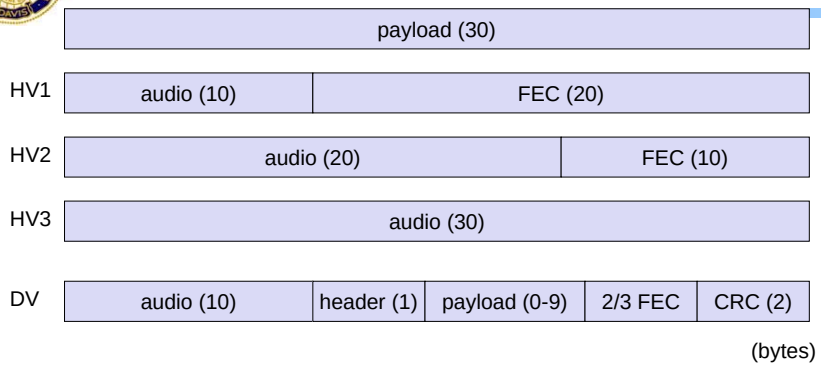
Ref #1: Bluetooth Baseband

- Piconet/channel definition
- Low-level packet definition
  - Access code
    - Channel, device access, e.g., derived from master
  - Packet header
    - 1/3-FEC, active member address (broadcast + 7 slaves), link type, alternating bit ARQ/SEQ, checksum



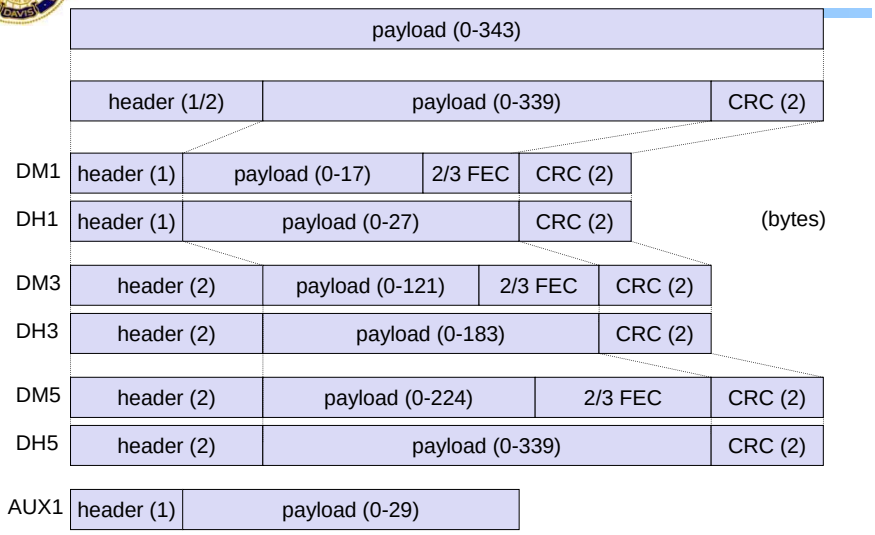
11

Ref #2: SCO payload types



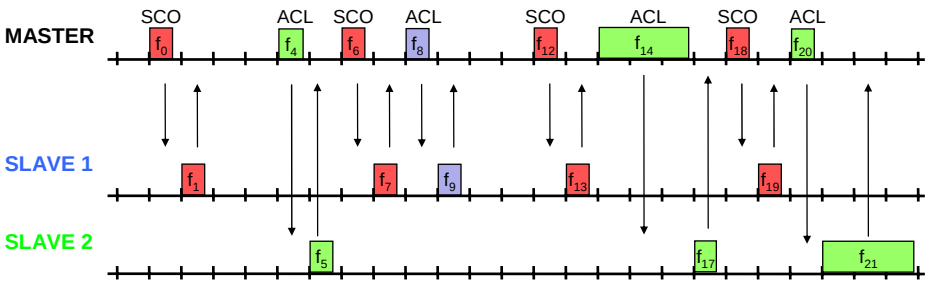
12

Ref #3: ACL Payload types



13

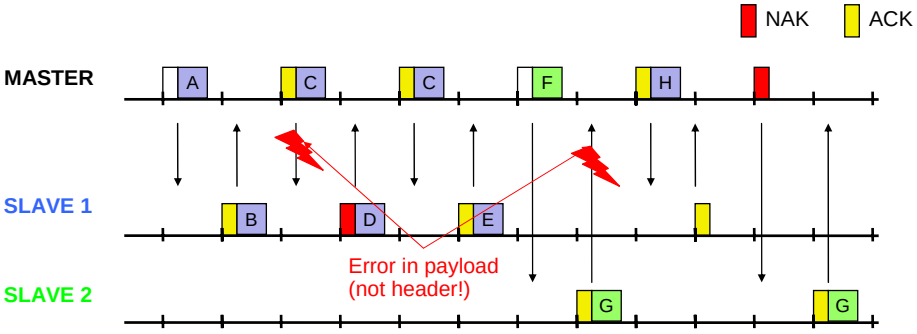
Illustration: Baseband Link Types



14

Robustness

- Slow frequency hopping with hopping patterns determined by a master
  - Protection from interference on certain frequencies
  - Separation from other piconets (FH-CDMA)
- Retransmission: ACL only, very fast
- Forward Error Correction: SCO and ACL



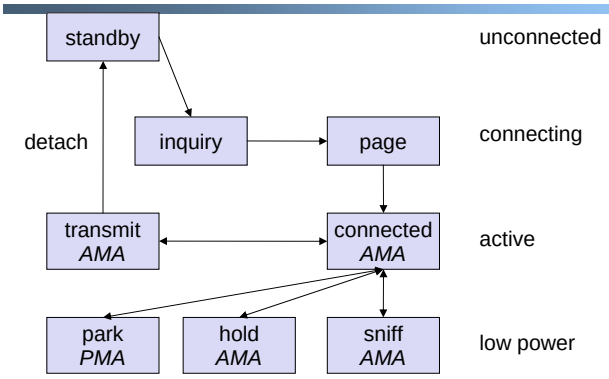
15

L2CAP - Logical Link Control and Adaptation Protocol

- Simple data link protocol on top of baseband
- Connection oriented, connectionless, and signaling channels
- Protocol multiplexing
  - RFCOMM, SDP, telephony control
- Segmentation & reassembly
  - Up to 64kbyte user data, 16 bit CRC used from baseband
- QoS flow specification per channel
  - Follows RFC 1363, specifies delay, jitter, bursts, bandwidth
- Group abstraction
  - Create/close group, add/remove member

16

Baseband States of A Bluetooth Device



Standby: do nothing
Inquire: search for other devices
Page: connect to a specific device
Connected: participate in a piconet

Park: release AMA, get PMA
Sniff: listen periodically, not each slot
Hold: stop ACL, SCO still possible, possibly participate in another piconet

Device Inquiry

- At a longer period (60-120s) devices do Inquiry
  - During inquiry, send probes out on each frequency
- Devices do Inquiry scan every 1.28s for 11ms
  - Inquiry scan will detect an inquiry probe
  - If an inquiry is detected, and inquiry response is sent
- The minimum time to get inquiry responses is 4s!
- *Devices can discover or be discovered – not both!*

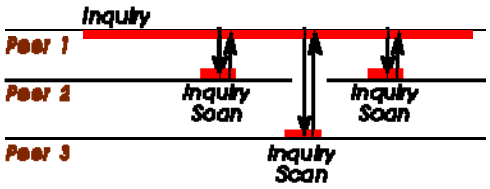


Photo thanks to: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Papers/BT.Demand.html

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)

19

Additional Protocols

- RFCOMM – Cable Replacement Protocols
  - Emulation of a serial port (supports a large base of legacy applications) to make replacement of cable techniques transparent
  - Allows multiple ports over a single physical channel
- Telephony Control Protocol Specification (TCS)
  - Call control (setup, release) signaling for the establishment of speech and data calls between Bluetooth devices
  - Defines mobility/group management procedures
- Adopted Protocls
  - PPP: point-to-point protocol (IP)
  - TCP/UDP/IP
  - OBEX: Exchange of objects, IrDA replacement
  - WAE/WAP: Wireless application environment and wireless application protocols are incorporated
    - Interacting with applications on cellular phones

20

Bluetooth/WPAN Summary

- Data rate
  - Synchronous, connection-oriented: 64 kbit/s
  - Asynchronous, connectionless
    - 433.9 kbit/s symmetric
    - 723.2 / 57.6 kbit/s asymmetric
- Transmission range
  - POS (Personal Operating Space) up to 10 m
  - With special transceivers up to 100 m
- Frequency
  - Free 2.4 GHz ISM-band
- Security
  - Challenge/response (SAFER+), hopping sequence
- Cost
  - 50€ adapter, drop to 5€ if integrated
- Availability
  - Integrated into some products, several vendors

Bluetooth/WPAN Summary

- Connection set-up time
  - Depends on power-mode
  - Max. 2.56s, avg. 0.64s
- Quality of Service
  - Guarantees, ARQ/FEC
- Manageability
  - Public/private keys needed, key management not specified, simple system integration
- Advantages
  - Already integrated into several products, available worldwide, free ISM-band, several vendors, simple system, simple ad-hoc networking, peer to peer, scatternets
- Disadvantages
  - Interference on ISM-band
  - Limited range
  - Max. 8 devices/network&master
  - High set-up latency

IEEE 802.15 – Future Developments

- 802.15.2: Co-existance
  - Coexistence of Wireless Personal Area Networks (802.15) and Wireless Local Area Networks (802.11), quantify the mutual interference
- 802.15.3: High-Rate
  - Standard for high-rate (20Mbit/s or greater) WPANs, while still low-power/low-cost
  - Data Rates: 11, 22, 33, 44, 55 Mbit/s
  - Quality of Service isochronous protocol
  - Ad hoc peer-to-peer networking
  - Security
  - Low power consumption
  - Low cost
  - Designed to meet the demanding requirements of portable consumer imaging and multimedia applications

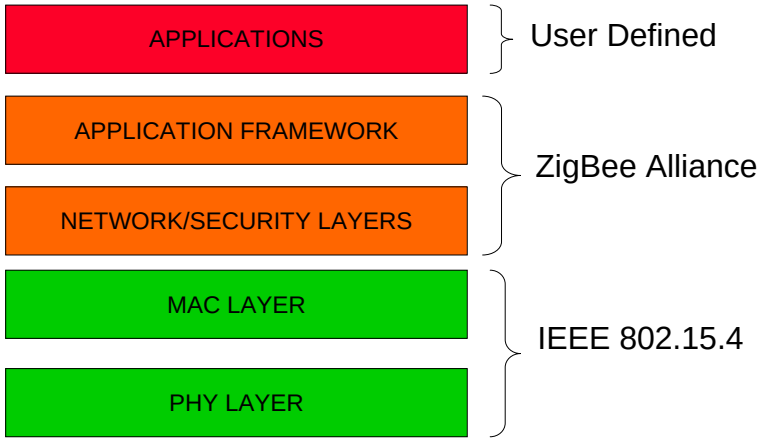
23

IEEE 802.15.4

- 802.15.4: Low-Rate, Very Low-Power
  - Low data rate solution with multi-month to multi-year battery life and very low complexity
  - Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation
- Foundation of the ZigBee initiative

24

ZigBee + 802.15.4 Protocol Stack



25

IEEE 802.15.4 Characteristics

- Data rate: 868 MHz: 20 kbps, 915 MHz: 40 kbps, 2.4 GHz: 250 kbps
- Range = 10-20 m
- Latency ~15ms
- Channels: 868/915 MHz, and 2.4 GHz
- Addressing: short 16-bit or 64-bit IEEE
- Channel access: CSMA-CA and slotted CSMA-CA

26

Applications

- Industrial control and monitoring
- Public safety
- Sensing and location determination at disaster sites
- Automotive sensing
- Smart badges and tags
- Home automation and networking
  - Computing devices and peripherals (latency critical devices)
  - Entertainment system
  - Heating, cooling, lighting, security
  - Controls of doors, windows, devices
  - Health monitoring

27

MAC & PHY

- Maximum size of MAC frame = 127 bytes
- Frame types:
  - Beacon frame
  - Data frame
  - Acknowledgment frame
  - MAC command frame
- Use of superframes to provision contention-free access
- Both PHYs are based on DSSS methods

28

MAC Features

- In a beacon-enabled network with superframes, slotted CSMA-CA is used
- In networks without beacons, standard CSMA-CA is used
- A successful reception is always ack'ed
- Provides three levels of security
  - No security
  - Access control lists
  - Symmetric key security

29

ZigBee

- The ZigBee Alliance is an association of more than 100 companies working together to enable reliable, cost-effective, low-power, wirelessly networked, monitoring and control products based on an open global standard.
- ZigBee defines the network, security and application framework profile layers for an IEEE 802.15.4-based system
- Security:
  - Access control lists, packet freshness timers, 128-bit encryption

30

ZigBee Network Layer

- Starting a network
- Joining and leaving a network
- Configuring a new device
- Addressing
- Synchronization
- Security
- Routing
  - Hierarchical routing with table-driven optimizations

31

ZigBee Network Coordinator & Node

- Network Coordinator
  - Sets up a network
  - Transmits network beacons
  - Manages network nodes
  - Stores network node information
  - Routes messages between paired nodes
  - Typically operates in the receive state
- Network Node
  - Designed for battery powered or high energy savings
  - Searches for available networks
  - Transfers data from its application as necessary
  - Determines whether data is pending
  - Requests data from the network coordinator
  - Can sleep for extended periods

32

ZigBee Traffic Types and Applications

- Traffic Types:
  - Periodic Data
    - Application defined – beaconing systems
  - Intermittent Data
    - Application or external stimulus based
  - Repetitive Low Latency Data
    - Time slot allocation, guaranteed low latency
- Application Characteristics:
  - Low duty cycle sensor networks (<1%)
  - Quickly attach, detach, and go to sleep
  - Low power consumption
  - Smaller packet size – higher effective throughput values
- Topology
  - Star
    - PAN coordinator at the center
  - Peer-to-peer
  - Cluster tree

33

Ok, ZigBee is small and low-power...

- But we want lower-power, and even smaller!

34

RFID (Radio Frequency Identification)

- Data rate
  - Transmission of ID only (e.g., 48 bit, 64kbit, 1 Mbit)
  - 9.6 – 115 kbit/s
- Transmission range
  - Passive: up to 3 m
  - Active: up to 30-100 m
  - Simultaneous detection of up to, e.g., 256 tags, scanning of, e.g., 40 tags/s
- Frequency
  - 125 kHz, 13.56 MHz, 433 MHz, 2.4 GHz, 5.8 GHz and many others
- Security
  - Application dependent, typ. no crypt. on RFID device
- Cost
  - Very cheap tags, down to 1€ (passive)
- Availability
  - Many products, many vendors

35

RFID (Cont'd)

- Connection set-up time
  - Depends on product/medium access scheme (typ. 2 ms per device)
- Quality of Service
  - none
- Manageability
  - Very simple, same as serial interface
- Special Advantages
  - Extremely low cost, large experience, high volume available, no power for passive RFIDs needed, large variety of products, relative speeds up to 300 km/h, broad temp. range
- Disadvantages
  - No QoS, simple denial of service, crowded ISM bands, typ. one-way (activation/ transmission of ID)

36

RFID (Cont'd)

- Function
  - Standard: In response to a radio interrogation signal from a reader (base station) the RFID tags transmit their ID
  - Enhanced: additionally data can be sent to the tags, different media access schemes (collision avoidance)
- Features
  - No line-of sight required (compared to, e.g., laser scanners)
  - RFID tags withstand difficult environmental conditions (sunlight, cold, frost, dirt etc.)
  - Products available with read/write memory, smart-card capabilities
- Categories
  - Passive RFID: operating power comes from the reader over the air which is feasible up to distances of 3 m, low price (1€)
  - Active RFID: battery powered, distances up to 100 m

37

RFID: Applications

- Applications
  - Total asset visibility: tracking of goods during manufacturing, localization of pallets, goods etc.
  - Loyalty cards: customers use RFID tags for payment at, e.g., gas stations, collection of buying patterns
  - Automated toll collection: RFIDs mounted in windshields allow commuters to drive through toll plazas without stopping
  - Others: access control, animal identification, tracking of hazardous material, inventory control, warehouse management, ...
- Local Positioning Systems
  - GPS useless indoors or underground, problematic in cities with high buildings
  - RFID tags transmit signals, receivers estimate the tag location by measuring the signal's time of flight

38

RFID: Challenges

- Security
  - Denial-of-Service attacks are always possible
    - Interference of the wireless transmission, shielding of transceivers
  - IDs via manufacturing or one time programming
  - Key exchange via, e.g., RSA possible, encryption via, e.g., AES
- Future Trends
  - RTLS: Real-Time Locating System – big efforts to make total asset visibility come true
  - Integration of RFID technology into the manufacturing, distribution and logistics chain
  - Creation of „electronic manifests“ at item or package level (embedded inexpensive passive RFID tags)
  - 3D tracking of children, patients

39

RFID – Example Products

- Intermec RFID UHF OEM Reader
  - Read range up to 7m
  - Anticollision algorithm allows for scanning of 40 tags per second regardless of the number of tags within the reading zone
  - US: unlicensed 915 MHz, Frequency Hopping
  - Read: 8 byte < 32 ms
  - Write: 1 byte < 100ms

- Wireless Mountain Spider
  - Proprietary sparse code anti-collision algorithm
  - Detection range 15 m indoor, 100 m line-of-sight
  - > 1 billion distinct codes
  - Read rate > 75 tags/s
  - Operates at 308 MHz

40

PAN Discussion Points

- General trend: low power, low profile
  - RFID: no power!
- Ubiquitous networking
- Security/privacy concerns?
- Neat research ideas?

41