



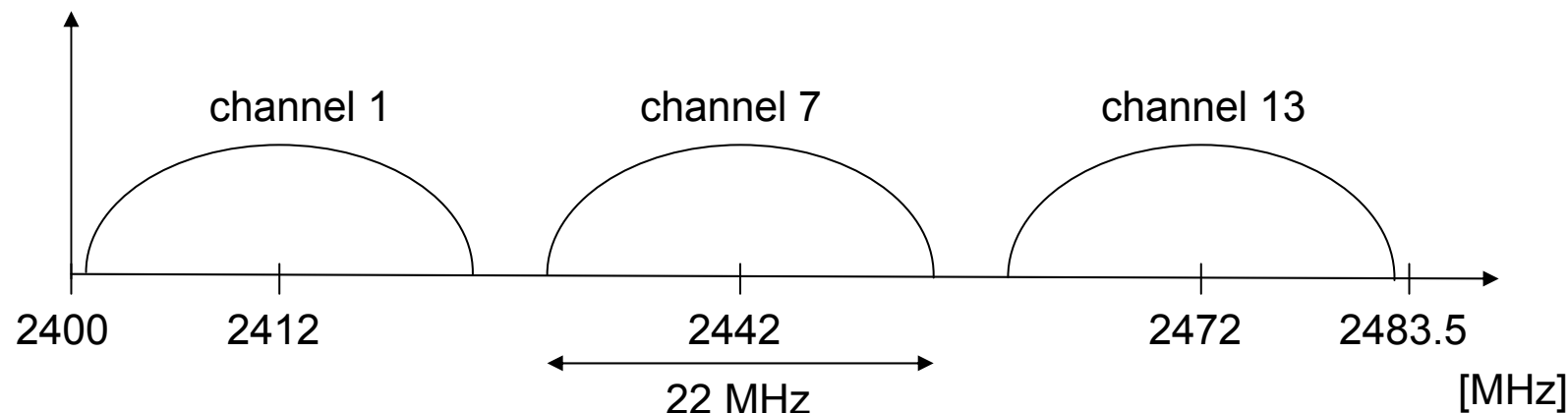
Variations of the IEEE 802.11 (WLAN) Standard (1)



802.11 b

- ❑ Modifications in the transmission (physical layer) allowing data rates up to ca. 11 Mbit/s by implementing DSSS more efficiently
- ❑ within license-free 2.4 GHz ISM-band
- ❑ 13 channels (N. America 11, Japan 14), each channel has a bandwidth of 22MHz

Europe (ETSI)



- ❑ Mac-layer remains the same

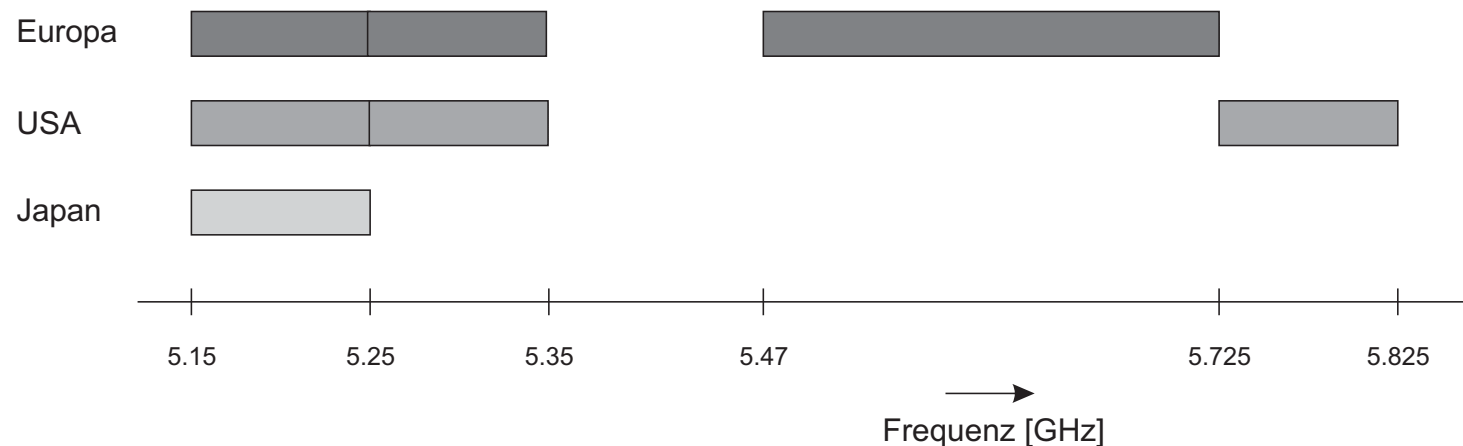


Variations of the IEEE 802.11 (WLAN) Standard (2)



802.11 a

- ❑ Modifications in the transmission (physical layer) allowing data rates up to ca. 54 Mbit/s
- ❑ within 5 GHz ISM-band
- ❑ OFDM (Orthogonal Frequency Division Multiplexing) used
- ❑ altogether 455 MHz available (USA 300, Japan 100)



- ❑ less transmission range (e.g. 54 Mbit/s up to 5 m, 24 up to 30m, 12 up to 60 m)
- ❑ some products
- ❑ Mac-layer remains the same



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 priority classes
- ❑ 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, e.g. standardizing roaming also between access points of different manufacturers
- ❑ Currently unclear to which extent manufacturers will follow this suggestion

802.11g: Data Rates > 20 Mbit/s at 2.4 GHz; if 54 Mbit/s ---> OFDM

- ❑ Successful successor of 802.11b, performance loss during mixed operation with 11b but possible

802.11i: Enhanced Security Mechanisms

- ❑ Enhance the current 802.11 MAC to provide improvements in security following the standard 802.1x for LANs
- ❑ TKIP enhances the insecure WEP, but remains compatible to older WEP systems
- ❑ AES provides a secure encryption method and is based on new hardware



Summary (1)



- ❑ For WLANs (corresponding to the IEEE 802.11 standard) exist different physical layers all having a uniform interface to the MAC layer.
- ❑ The 802.11 standard (1997) defines two physical layers in the license-free 2,4 GHz ISM - band (FHSS and DSSS) and one physical layer in the infrared frequency range supporting data rates of 1 and 2 Mbit/s each.
- ❑ Almost all commercial products use FHSS or DSSS technology, in the beginning mostly FHSS.
- ❑ Nowadays DSSS is mostly used because it can also support data rates of 5,5 and 11 Mbit/s. Those extensions have been defined 1999 in the 802.11b standard.
- ❑ Also since 1999, the 802.11a standard defines an additional physical layer in the licensed 5 GHz band. It uses the OFDM technology providing data rates up to 54 Mbit/s. It has strong similarities to the European standard HIPERLAN/2 using the same technology.
- ❑ Higher data rates in general imply less transmission range. E.g., FHSS und DSSS systems with 2 Mbit/s offer a range of about 100m, with OFDM technology providing 24 Mbit/s it is only about 30m, providing 54 Mbit/s only 5 m.



Summary (2)



- ❑ Ad-hoc networks consist of cells with limited range in which stations can communicate wireless.
- ❑ Infrastructure networks connect many individual cells via a wired (backbone) network called Distribution System. The connection point for each cell to the DS is the Access Point. This allows the stations of the cells to access also external networks like the Internet. However, the necessary protocols so far are not part of the 802.11 standard specification, but is vendor-dependent (802.11f is an ongoing attempt to change this).
- ❑ In infrastructure networks APs support the *roaming* of mobile stations, meaning that stations can freely move from one cell to the other without leaving connection to the external network at any time. Scanning allows stations to find adequate new APs to submit registration requests.
- ❑ The standard procedure to control shared access on the MAC-layer (CSMA/CA) is adopted from its wired pendant, the Ethernet (CSMA/CD). Because the radio medium does not allow to detect collisions reliably, collisions should be avoided by introducing random back-off (waiting) times.
- ❑ Additionally exchanging short control messages (Request-to-Send/Clear-to-Send) enhances considerably the probability of collision-free medium access because it introduces an implicit medium reservation scheme and it solves the *hidden station* problem.
- ❑ The optional PCF approach may support time- critical (real-time) applications, because collision-free access can be guaranteed due to a centralized (master/slave) control of the medium access.
- ❑ Synchronization of station-internal clocks and power management allowing stations to enter a „sleep“ mode contributes to save energy without risking message losses.



Wireless LANs (2)



Major disadvantages:

Less to no Quality of Service (QoS) regarding the most important parameters

- ❑ Bandwidth
 - much lower in general (1-10 Mbit/sec vs 100 - 1000Mbit/sec) (**performance aspect**)
 - difficult to predict (**real-time aspect**)
- ❑ Transmission errors
 - tremendously higher loss rates (on average 10^{-4} versus 10^{-12}) (**reliability aspect**)
- ❑ Latencies
 - much higher (**performance aspect**)
 - less predictable (**real-time aspect**)

Question:

Problems solved by using the WLAN Standard?



What about Real-Time?



In order to guarantee real-time behavior of the communication subsystem, the system should have pretty good knowledge about the following parameters:

- **available bandwidth b :**
of bytes that can be transmitted from sender to receiver within unit time (e.g. a second)
- **transmission reliability r :**
probability, that a frame sent will arrive correctly at the receiver
- **latency l :**
time left from a message ready to be sent until successful arrival (obviously dependent from b and r but not to be determined deterministically (r denotes a probabilistic value))

Considering PCF:

Determining b : **ok**, in contrast to DCF

Determining r : **??**, certainly much lower than in the wired case

Determining l : **??**, predicting the # of retransmissions for each individual case is the big problem



Reliability



Remaining problems to be solved:

Messages can be lost (on average 10^{-4} versus 10^{-12} in LANs), even worse:

- Some stations may receive a message, some others may not (in case of broadcasts)
- Stations can crash
- Stations can be out of reach

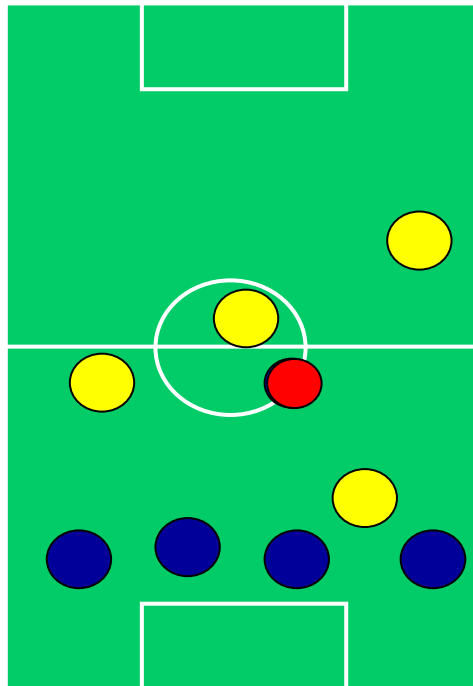
Even more:

Is message loss due to interference to other ongoing wireless communication an important factor to be considered when using WLAN, making things worse?

If, e.g.

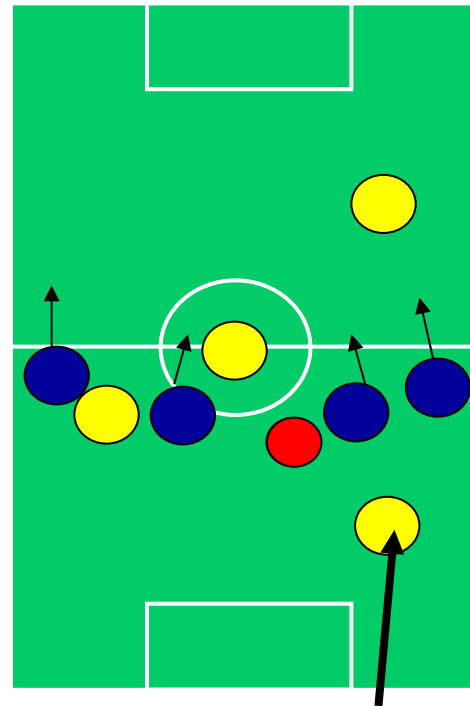
- other WLANs are sending on neighbored channels
 - terminals like laptops and mobile phones communicate via Bluetooth in reach of the WLAN stations
- Analysis by measurements under real world conditions (RoboCup)

„offside trap“



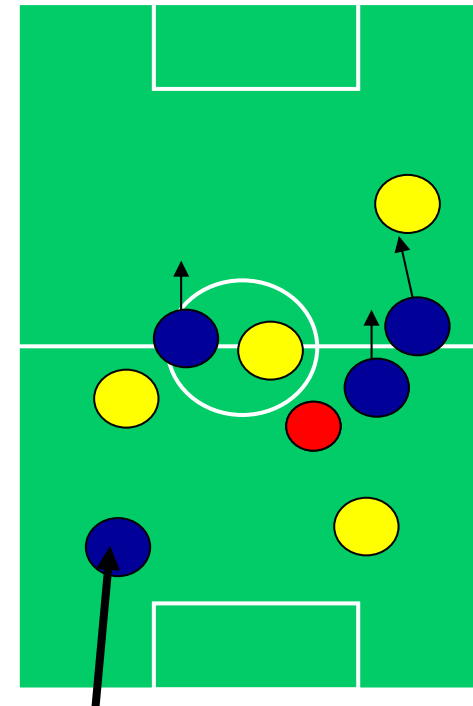
● A blue robot

success

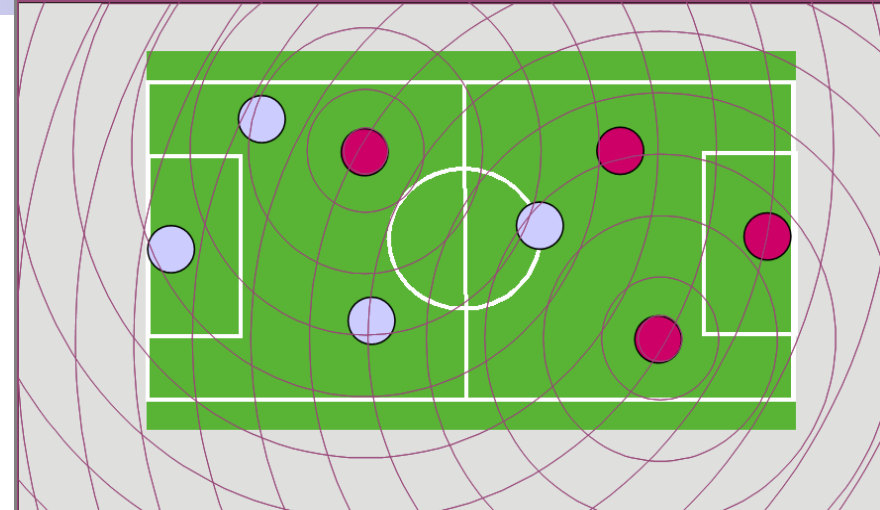





● A yellow robot

failure



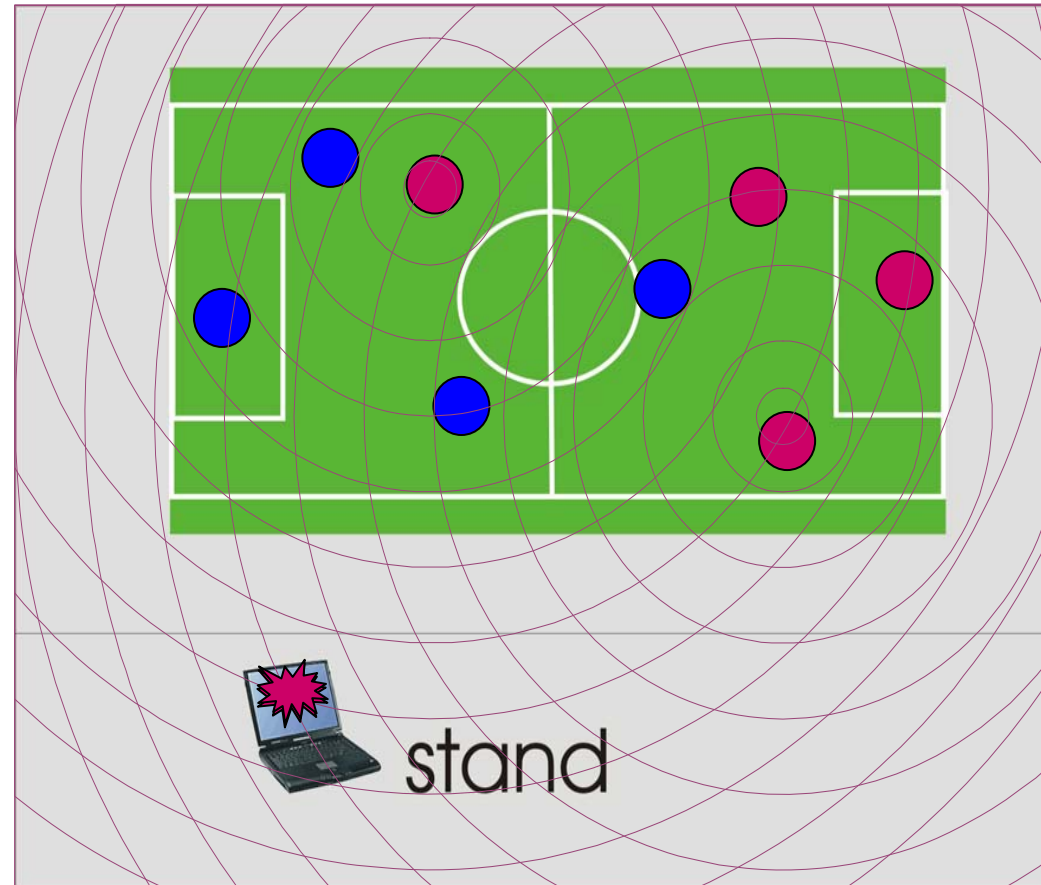
● The ball

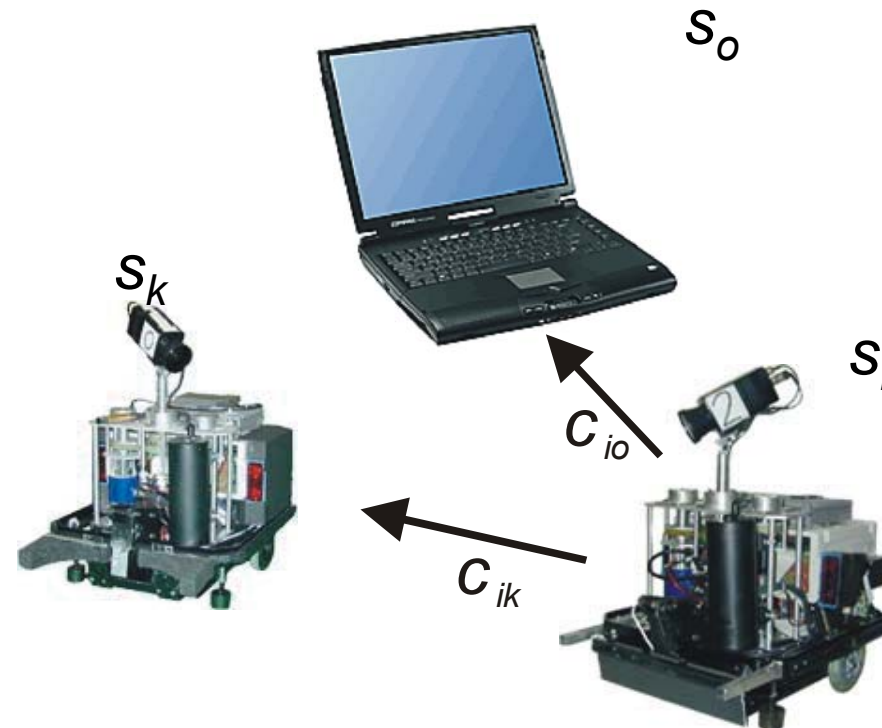


simulation league		team area
small size league	middle size league 1	middle size league 2
		
stand		

- ❑ 12 robot teams
- ❑ 2 fields with 2 LANs each; matches are running simultaneously
- ❑ Each team uses its own LAN, mostly 802.11 Standard 802.11 FHSS, 802.11 DSSS, proprietary 5GHz LAN
- ❑ Teams are faced with severe communication problems during the contests

- ❑ Observed the WLAN of one team during each match
- ❑ Captured all MAC-frames (Airopeek)
- ❑ 1.740.000 frames during four matches
- ❑ Funded by DFG in its Priority Program „Cooperating Teams of Mobile Robots in Dynamic Environments“

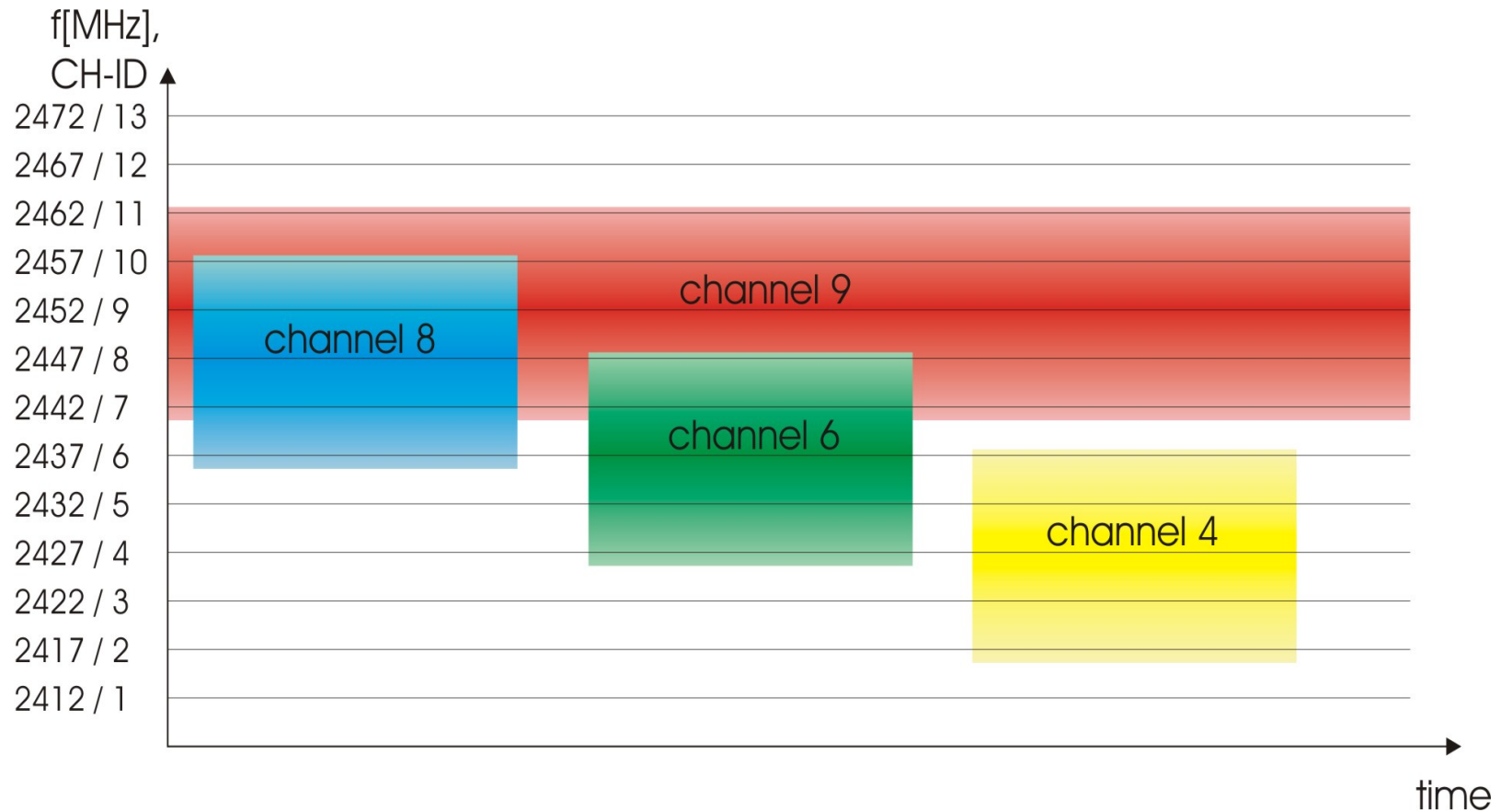




- ❑ Reliability measure for interference assessment: loss rate
- ❑ Determined as ratio between number of retries and number of point-to-point data frames
- ❑ Losses on the observer channel do not impair the results

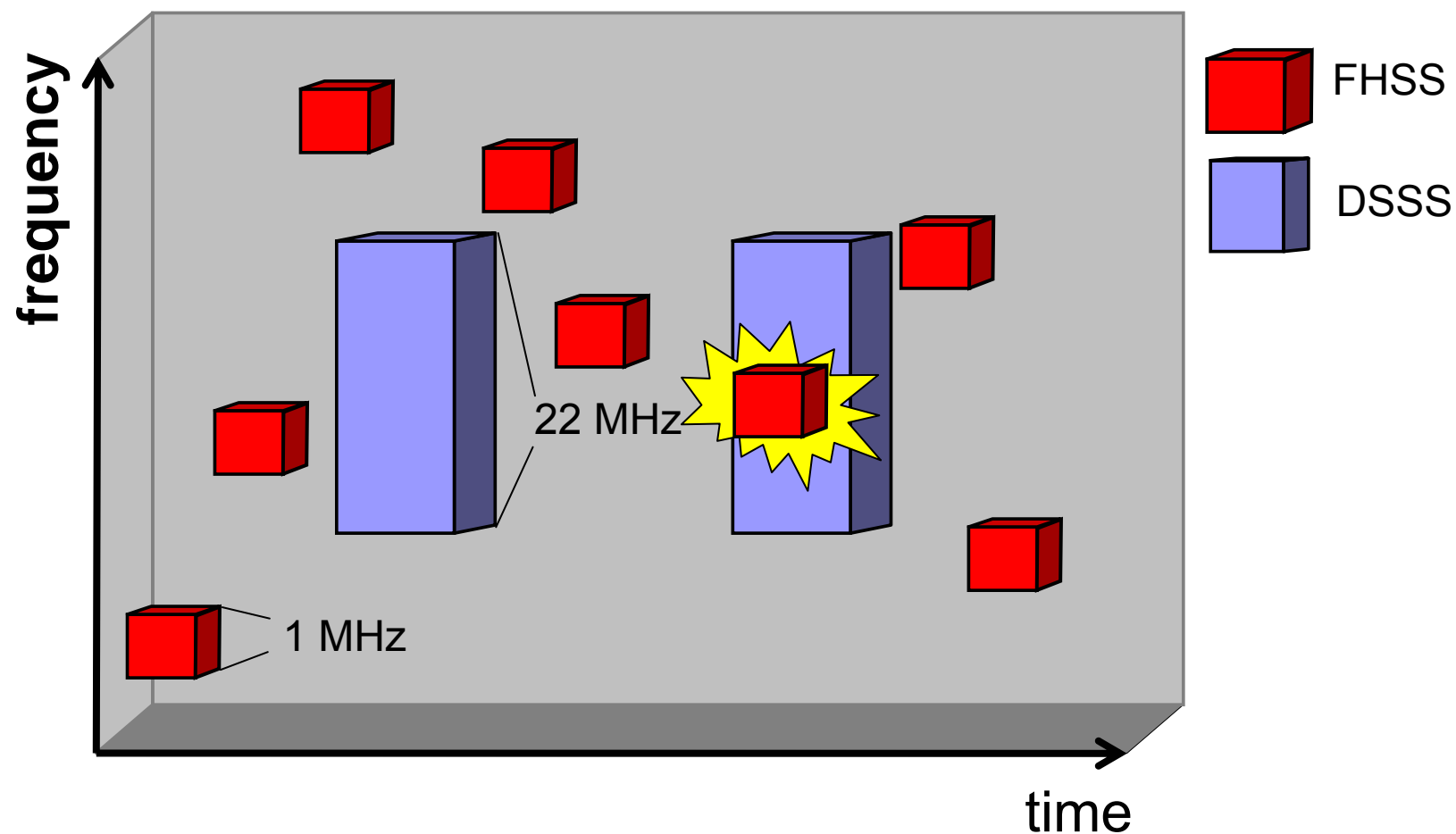


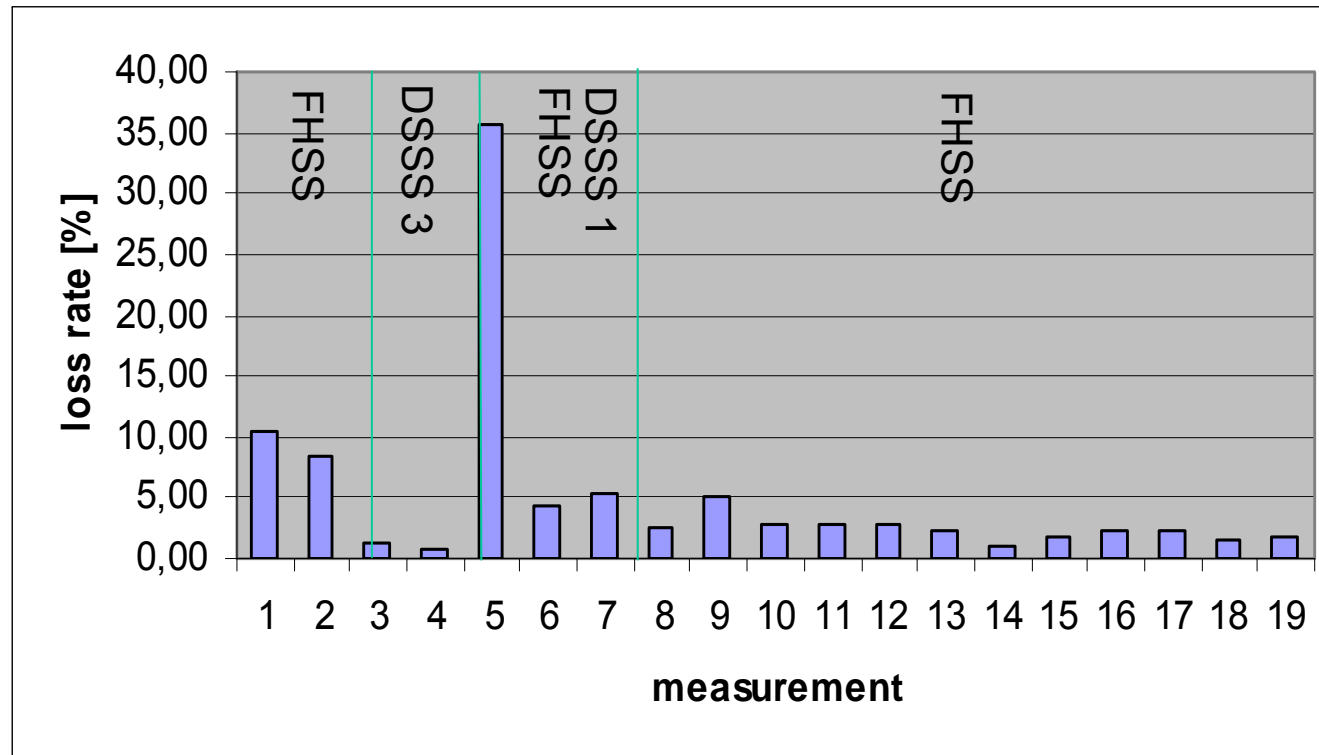
Overlapping DSSS Channels





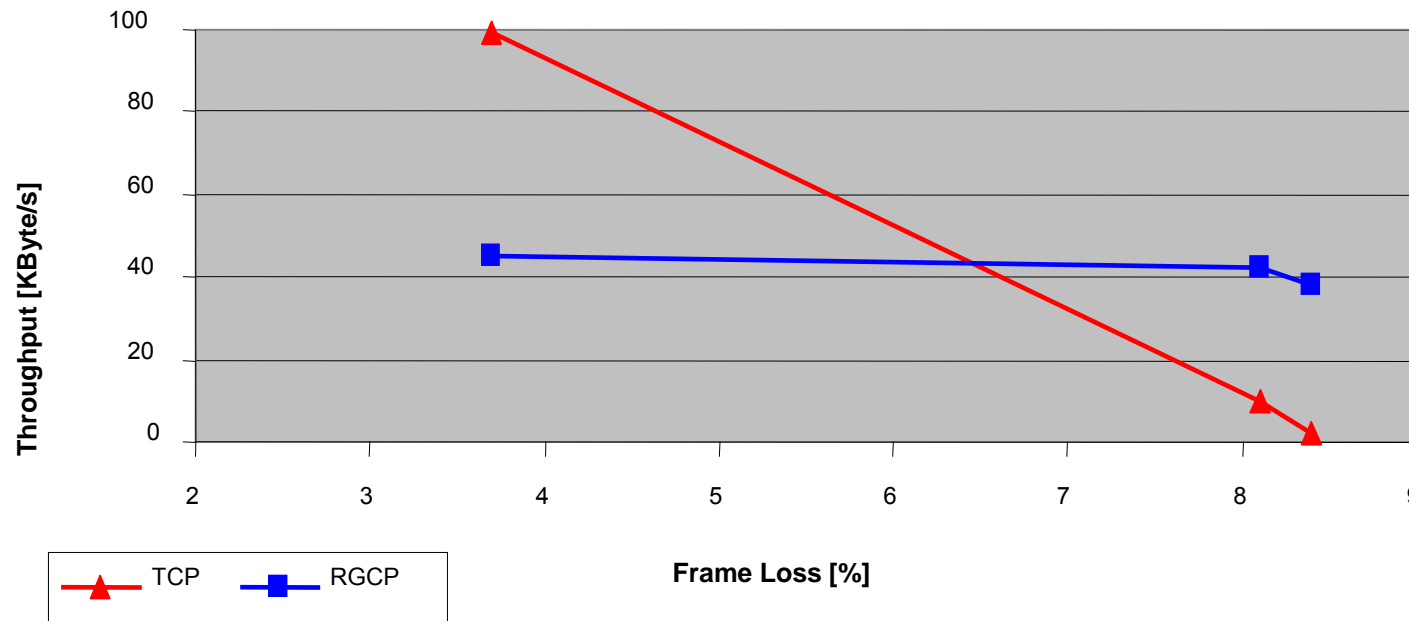
Interference between FHSS and DSSS





- ❑ Loss rates are much higher in the presence of other wireless networks
- ❑ Loss rates depend on technology and load
- ➔ Loss rates are hard to predict and may have extremely high peak values
- ➔ The use of WLANs in a public environment may cause severe problems

- ❑ Solution should be based on PCF of the MAC-layer
 - ❑ transport-layer: much longer timeouts and retransmission delays
 - ❑ transport-layer: congestion avoidance vs. recovery from message loss
- ❖ **Simply adopting TCP is not a solution**
- ❑ Solution must support multicasting (air is a broadcast medium!)





- ❑ Messages are either lost or delivered within a fixed time bound (synchronous system)
 - ❑ Stations may fail (silently)
 - ❑ Message losses are bounded by an Omission Degree OD
 - ❑ Stations may leave/enter the reach of other stations
 - ❑ The access point can be considered to be stable
- ➔ Reliability can be achieved by using redundancy to tolerate these faults



How to implement redundancy?



Static vs. Dynamic Redundancy

- ❑ Static redundancy - Message diffusion
 - ❑ principle: every message is transmitted $OD+1$ times
 - ❑ good: simple, no need to detect message losses, no timing redundancy (overhead)
 - ❑ bad: large overhead in bandwidth
- ❑ Dynamic redundancy ---> Acknowledge/retransmit also for broadcasts
 - ❑ principle: every message is only retransmitted if a message loss occurs (maximum OD retransmissions)
 - ❑ good: small overhead for retransmissions compared to message diffusion
 - ❑ bad: acknowledgements for detecting message loss induce extra overhead also in time

➔ Acknowledgment scheme is crucial



A Solution Approach



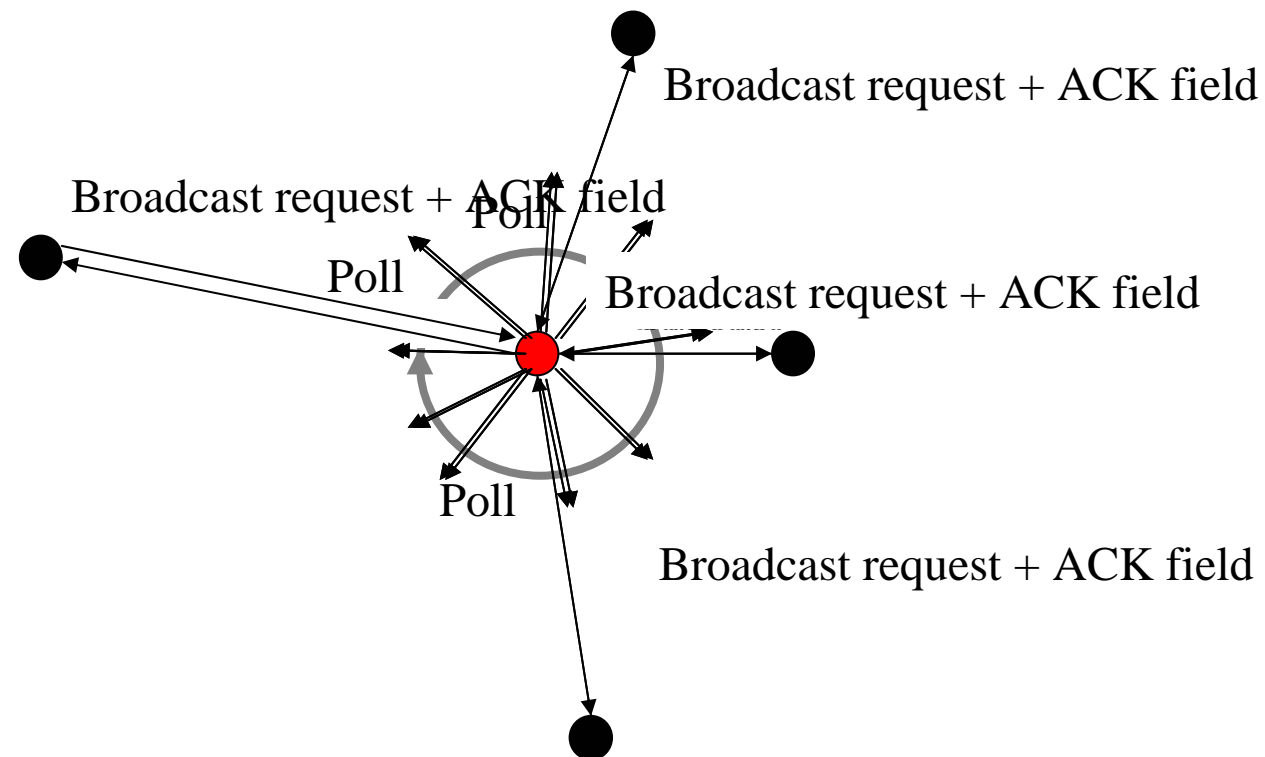
Key ideas of the protocol:

- ❑ Broadcast messages are routed through a coordinator, e.g. the access point
 - ❑ limited reach and mobility problem solved (membership)
 - ❑ ordering problem solved (establishing a central sequencer)
- ❑ Efficient acknowledgement scheme
 - ❑ communication is organized in rounds of length n ($n = \#$ of group members)
 - ❑ one ACK field (n bits) to acknowledge the messages of the preceding round
 - ❑ ACK field is piggy-backed to the broadcast request message



- ❑ if all stations acknowledge the message sent by a station in the preceding round, the next message of that station can be transmitted
- ❑ otherwise, its old message is retransmitted

→ no extra acknowledgment messages needed !





Timing Analysis



- ❑ 2 messages carrying payload (broadcast request and broadcast message) can be lost in the course of executing one broadcast
- ❑ A *round* constitutes the sending of one broadcast per station
- ❑ At most omission degree OD retransmissions allowed
(OD is dependent on the physical characteristics of the application environment or the standard (WLAN specification only allows 7 retransmissions))

➔ worst case *delivery time* Δbc_{max} (time until message committed, .e. propagated to the next layer (IP) of receiver station) can be computed:

$$\Delta bc_{max} \approx 2 \times OD \times \Delta round$$

($\Delta round := n \times 3 t_m$) (*polling itself is added to the two payload messages*)

Example 1: OD = 10, n = 4 stations, t_m = delay for a single message = 2,8 ms

---> worst case delivery time \approx 680 ms

Example 2: OD = 15

---> worst case delivery time = 1016 ms



- ❑ Problem: How to achieve better timing guarantees ?
- ❑ Observation: applications may afford to loose a (late) messages, if it is guaranteed that all stations reject the message in this case, and thus, remain in a consistent state
- ❑ Approach: Allow the application to limit the number of retransmission and guarantee agreement on consistent delivery
(atomicity of broadcast, all-or-nothing property)



- ❑ Limit the number of retransmission by a user defined resiliency degree $\text{res}(c)$ (maximum OD)
- ❑ If a message is not acknowledged by all stations after $\text{res}(c)$ retransmissions, it is rejected.
- ❑ The access point puts its decision whether to reject/accept a message in an accept field that is piggy-backed with every broadcast message.

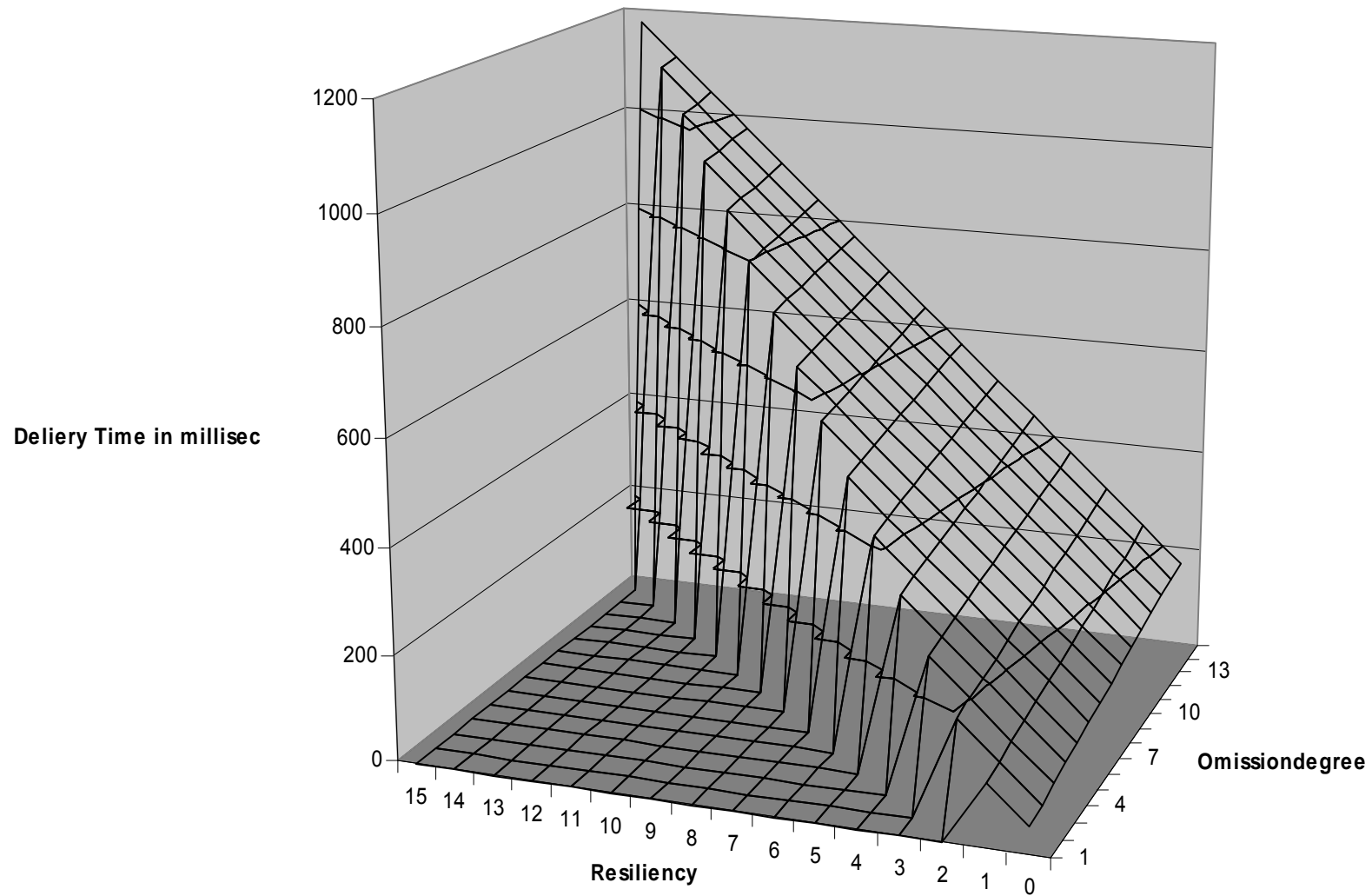
Resiliency degree	Messages lost per sec.	Timing guarantee = worst case time in ms	Measured Throughput (msg/sec)
0	4,0	168	100
1	2,1	235	99
2	0,5	302	97
3	0,04	369	98
4	0	436	98
15	0	1176	100

Parameters:

OD = 15, Message length = 100 Bytes, 4 Stations, Mobility simulation (out of reach (moving, obstacles like walls etc) => 2% message losses induced by means of fault injection (to counteract the almost perfect office environment where measurements were done)



Timing guarantee

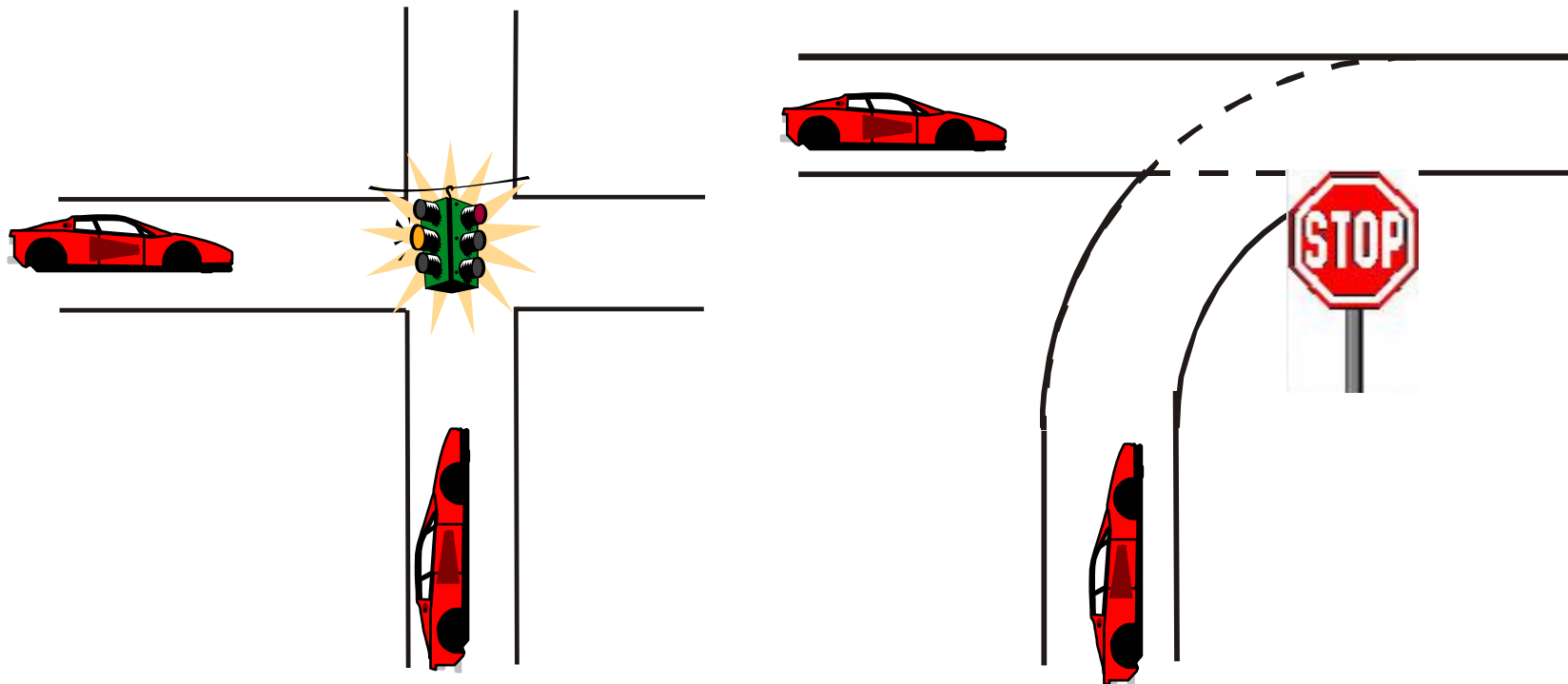




Summary of the key ideas



- ❑ The access point acts as central router.
- ❑ Dynamic redundancy is applied for reliable and timely message delivery.
- ❑ Acknowledgements for the messages of the preceding round are piggy-backed to the broadcast request message.
- ❑ Retransmissions can be limited. A consistent decision is achieved by piggy-backing accept/reject information to broadcast messages.
- ❑ Introducing the resiliency factor to balance the trade-off between reliability (adding redundancy) and real-time (less time redundancy (i.e. retransmissions))



- ❑ vehicles are forced to stop, even if resource is free
- ❑ low throughput
- ⇒ apply **resource scheduling** instead

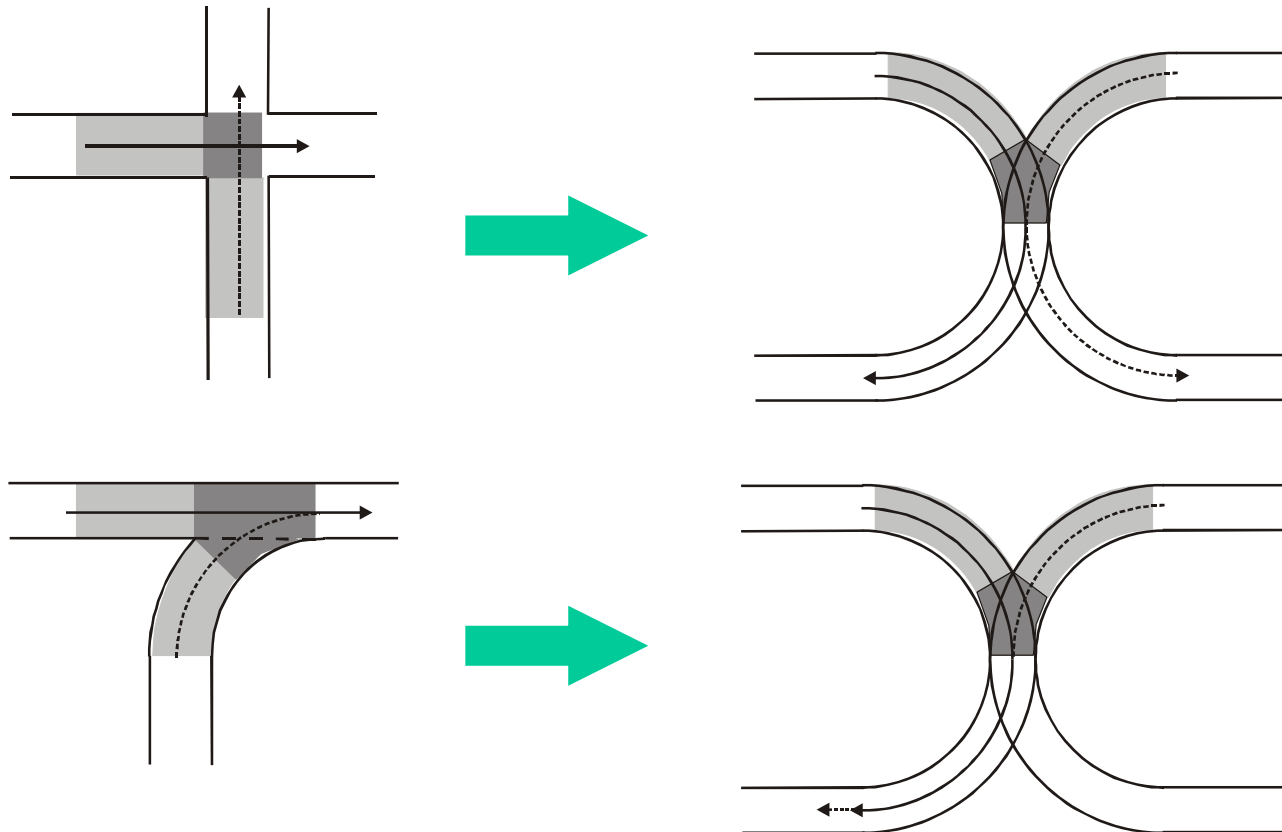


Design an architecture that allows the

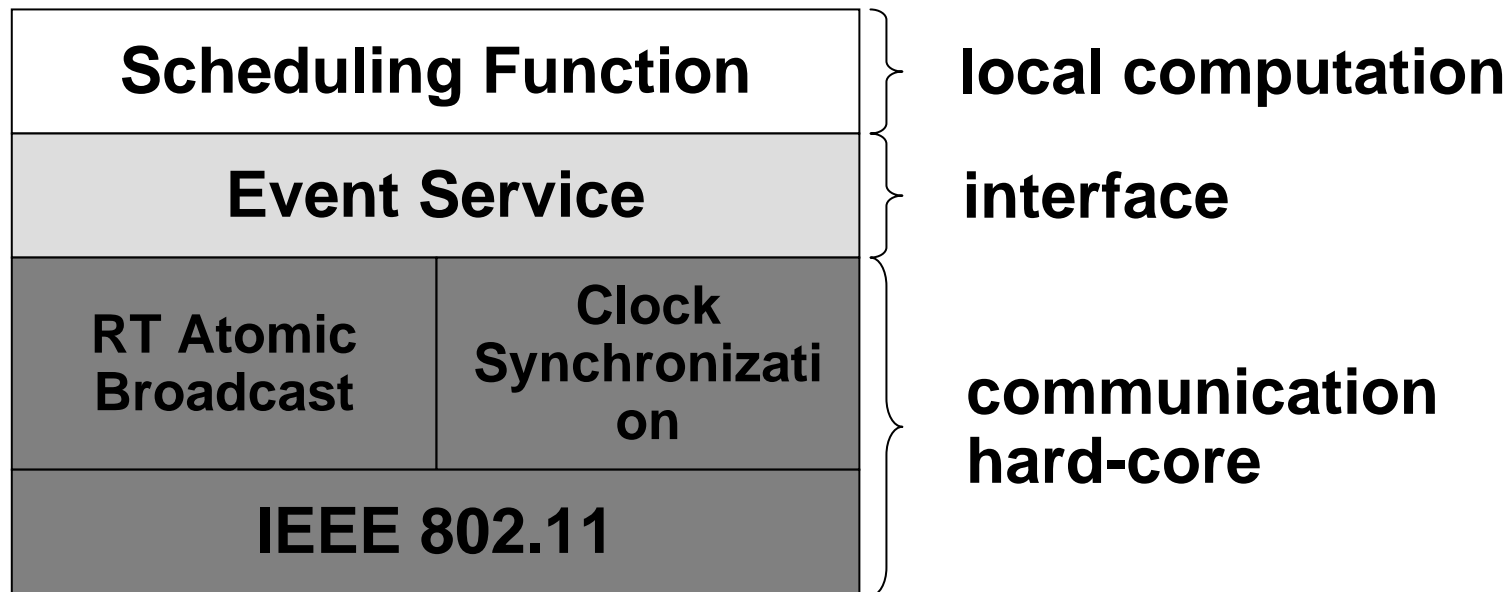
distributed scheduling of shared resources

reliably and in real-time

for a highly dynamic group of mobile systems.



- **Schedule the hot spot among all mobile systems that are within the approaching zone**



FIFO:

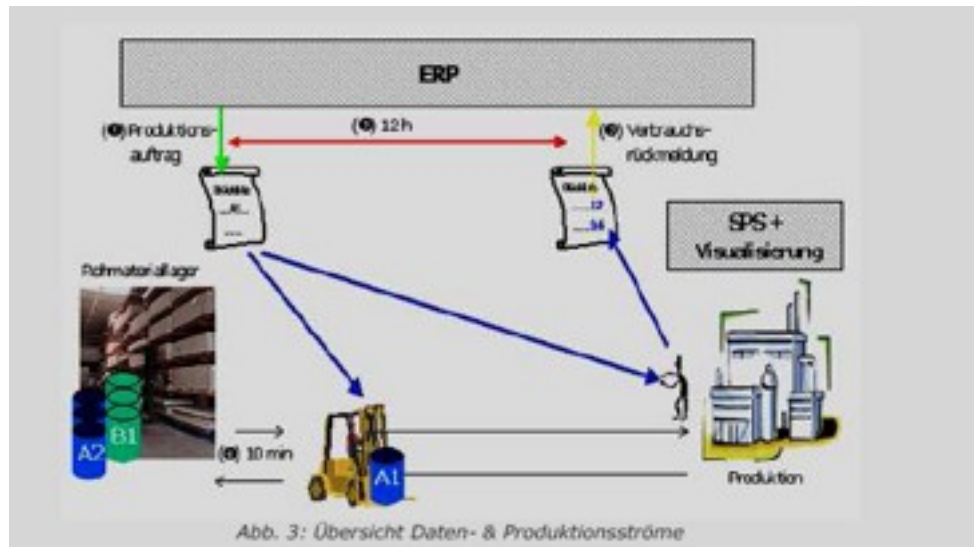
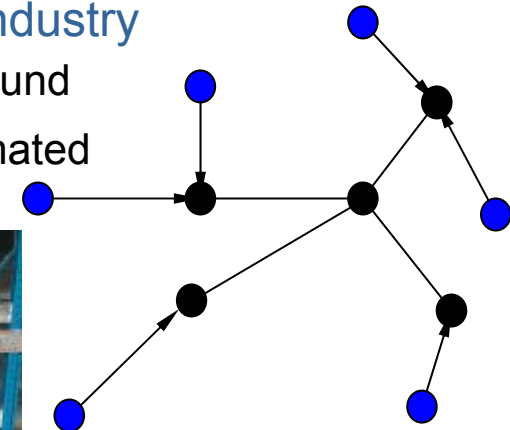
- ❑ Based on arrival times
- ❑ Static priorities

PET (Predicted Enter Times):

- ❑ Position and velocity based
- ❑ Dynamic priorities
- ❑ Steps to be executed:
 1. Step: Compute for each system s_i the predicted enter time $s_i.t_{pe}$
 2. Step: Order the systems by ascending $s_i.t_{pe}$
 3. Step: Determine for each system s_i the scheduled enter time $s_i.t_{se}$

Application scenario: mobile transport systems in automation industry

- Baggage transport systems (Destination Coded Vehicles), railbound
- AGV's (Automatically Guided Vehicles), track oriented, in automated manufacturing
- Warehouse container system, railbound
- warehouse (inventory) logistics





Remote control applications have real-time requirements



Real-time requirements

- ❑ Latency: control data (operator -> client)
- ❑ Throughput: video feedback (client -> operator)

Zur Anzeige wird der QuickTime™
Dekompressor „h264“
benötigt.



Wired Infrastructures are reliable but not flexible



Network infrastructure today

- ❑ Wired backbone
- ❑ Wireless only in the last step (single cell)
- ❑ Advantage: reliability of the backbone
- ❑ Disadvantages: limited flexibility and high cabling cost

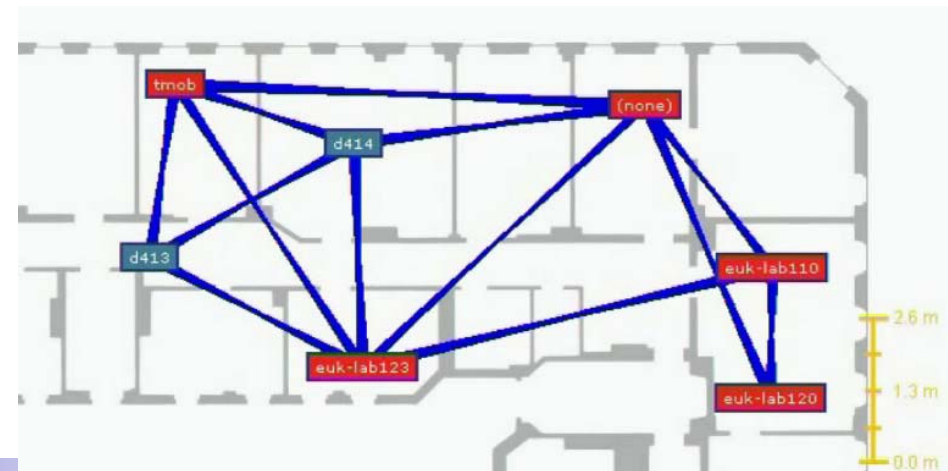
First step: WDS (Wireless Distribution System)

- ❑ Replace the wires by static wireless connections
- ❑ Client communicates only with single AP
- ❑ Nothing changes for the mobile client (robot)
- ❑ Disadvantages:
 - No automatic re-routing is possible within the network infrastructure
 - No alternative paths from client to infrastructure



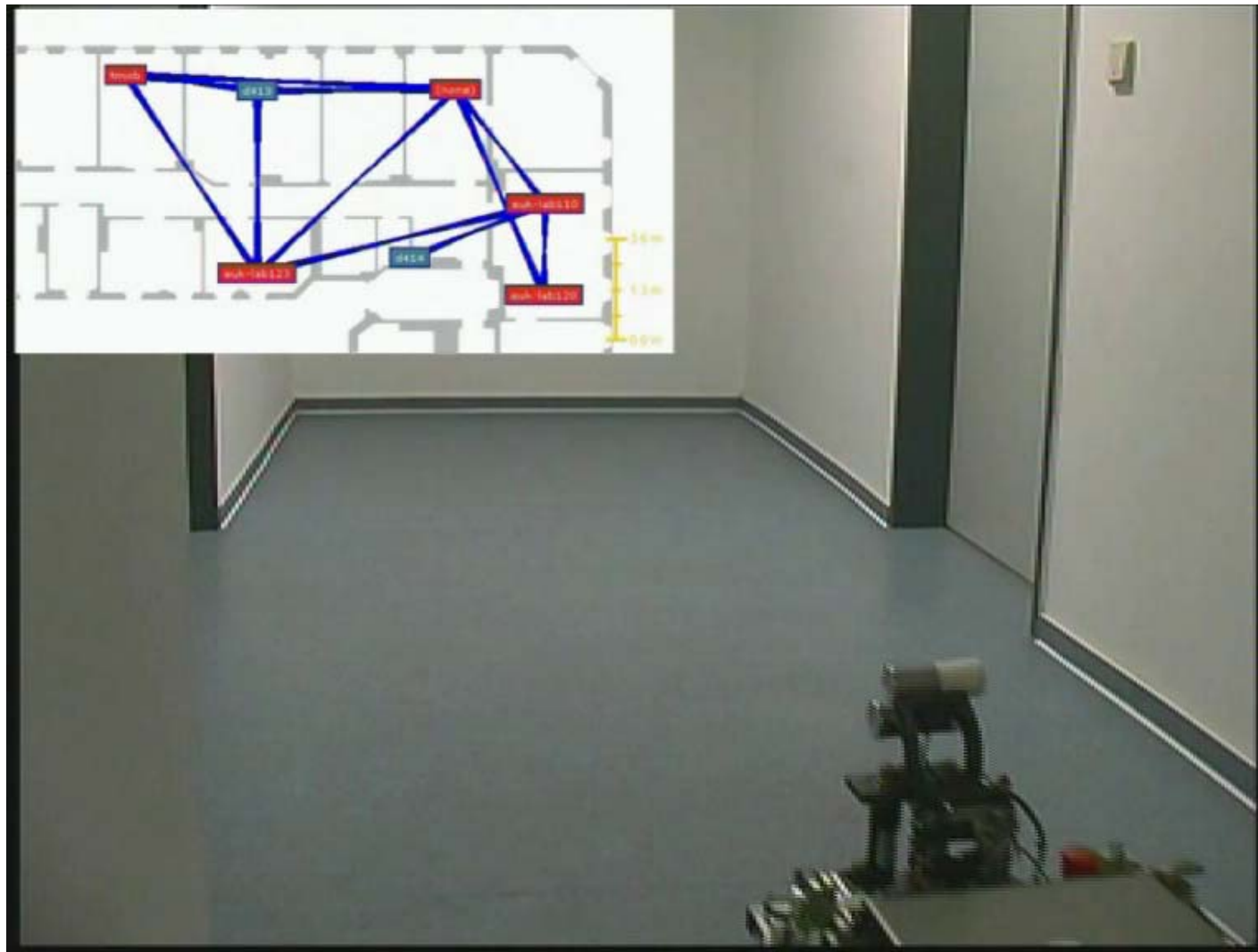
Second step: Mesh Networks

- ❑ Ad-hoc communication
- ❑ Mobile clients
- ❑ Static wireless infrastructure nodes (mesh nodes)
- ❑ Automatic topology configuration
- ❑ Client communicates with multiple mesh nodes
- ❑ Advantages: flexibility, fault tolerance, real-time





Example: seamless roaming in mesh networks





How to guarantee real-time requirements?



Price: we have to do routing

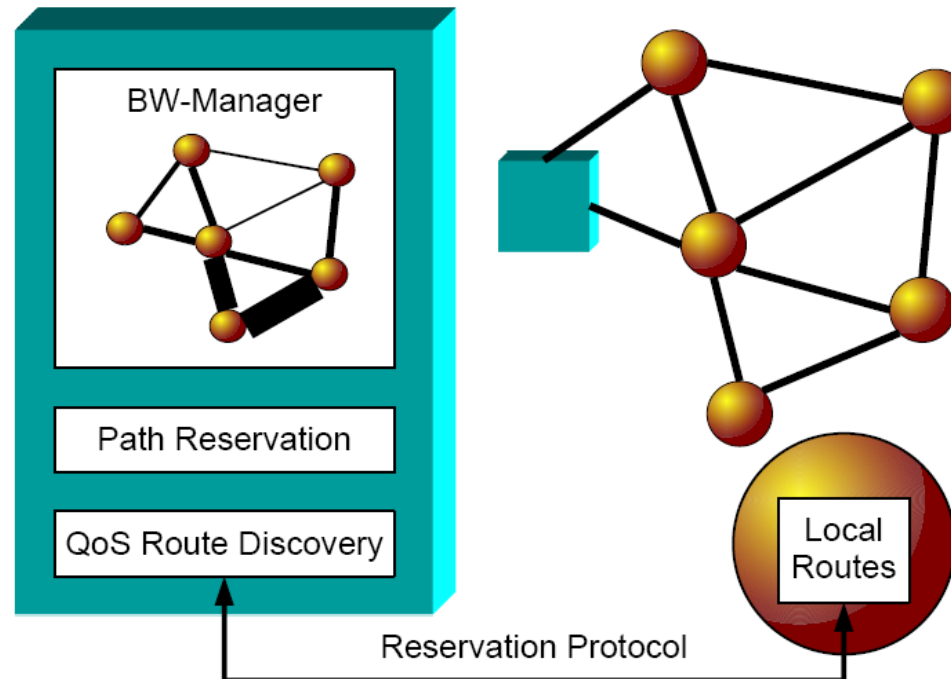
- ❑ Multi-hop end-to-end communication

Traditional routing does not guarantee real-time requirements

We need routing with guaranteed throughput to guarantee the real-time requirements:

- ❑ Throughput: amount of data per time [bits/sec] guaranteed to the application
- ❑ Latency: time [sec] to deliver a packet
- ❑ Bandwidth: data rate provided by the physical medium

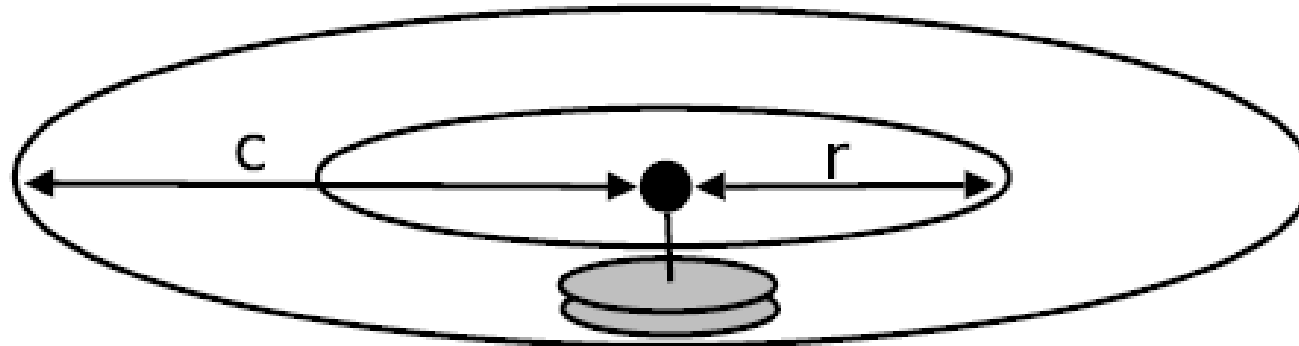
How to embed throughput guarantees in the routing?



Central instance for bandwidth reservation

But what is the available bandwidth?

The problem is more difficult to answer in CSMA wireless networks



Communication area ($d < r$)

Medium sharing area ($d < c$)

- ❑ Bandwidth is shared among all nodes in this area
- ❑ But: no communication for ($r < d < c$)!

=> How to coordinate with nodes in ($r < d < c$) when no communication is possible?



The existing approaches are either unreliable or inefficient



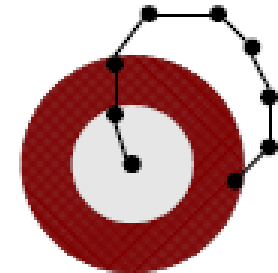
Existing approaches make assumptions for the available bandwidth based on the network topology:

Optimistic

- ❑ Assumptions about the medium sharing area
- ❑ For instance: only 2-hop neighbours share the medium
- ❑ Not reliable: see contra-example ->

Pessimistic

- ❑ All nodes share the medium
- ❑ Conservative
- ❑ Low bandwidth utilization



=> Measurement-based approach is required



Calibration: measuring the medium sharing



No assumptions from the network topology

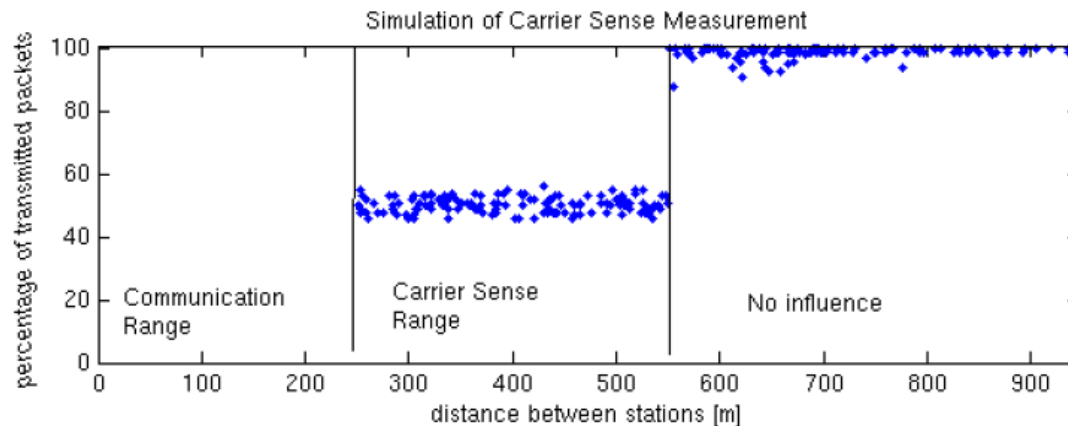
Pair wise medium probes

Every two stations (pair)

- Try to achieve 100% medium utilization by sending packets continuously
- All other stations observe and report
- Util. / station < 100% => Shared medium

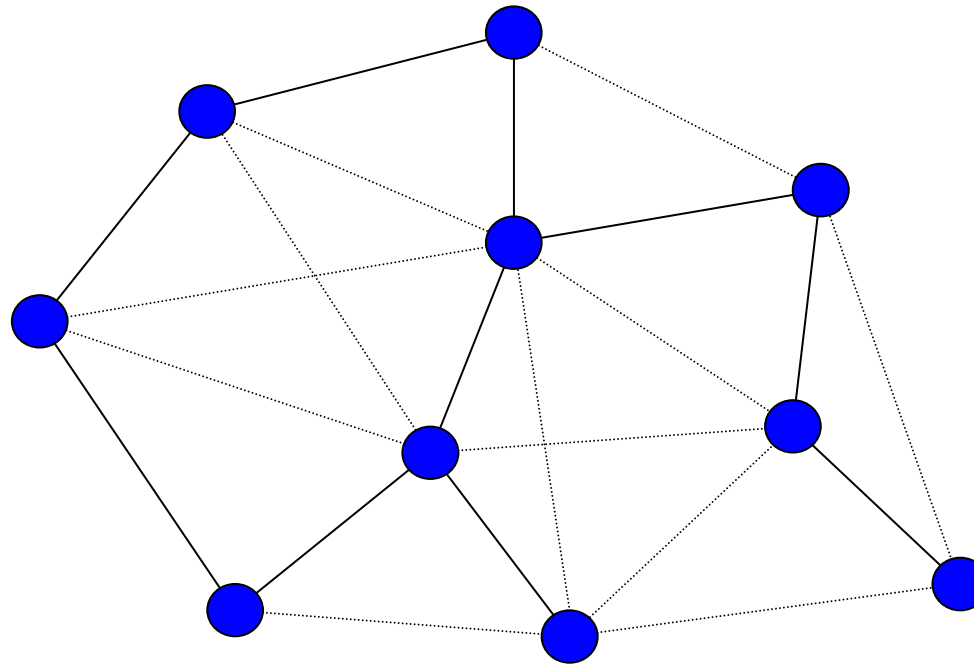
Rule: 50%: “medium sharing”, 100%: “no medium sharing”

Price: effort in the deployment phase





MANET (Multihop (Mobile) Ad hoc NETwork)



Examples for application areas needing QoS including soft RT requirements:

- ☐ Search and Rescue
- ☐ Sensor networks
- ☐ VOIP

Mobility Support (Network Layer)



Routing in the Internet works

- ❑ based on IP destination address (e.g. 129.13.42.99) ---> network prefix (in this case 129.13.42) determines physical subnet
- ➔ change of physical subnet implies change of IP address

Changing the IP-address?

- ❑ adjust the host IP address depending on the current location (e.g. using DHCP)
 - ➔ only useful to act as client of services (e.g. accessing WWW)
 - ➔ almost impossible to find a mobile system
 - ➔ no complete integration
- ❑ use dynamic DNS to update actual IP address
 - ➔ DNS updates take too long time (up to one day)
 - ➔ TCP connections break, security problems etc



Requirements to Mobile IP



Transparency

- ❑ to protocols of higher layers (e.g. TCP) and applications (in principle)
→ mobile end-systems keep their IP address

Compatibility

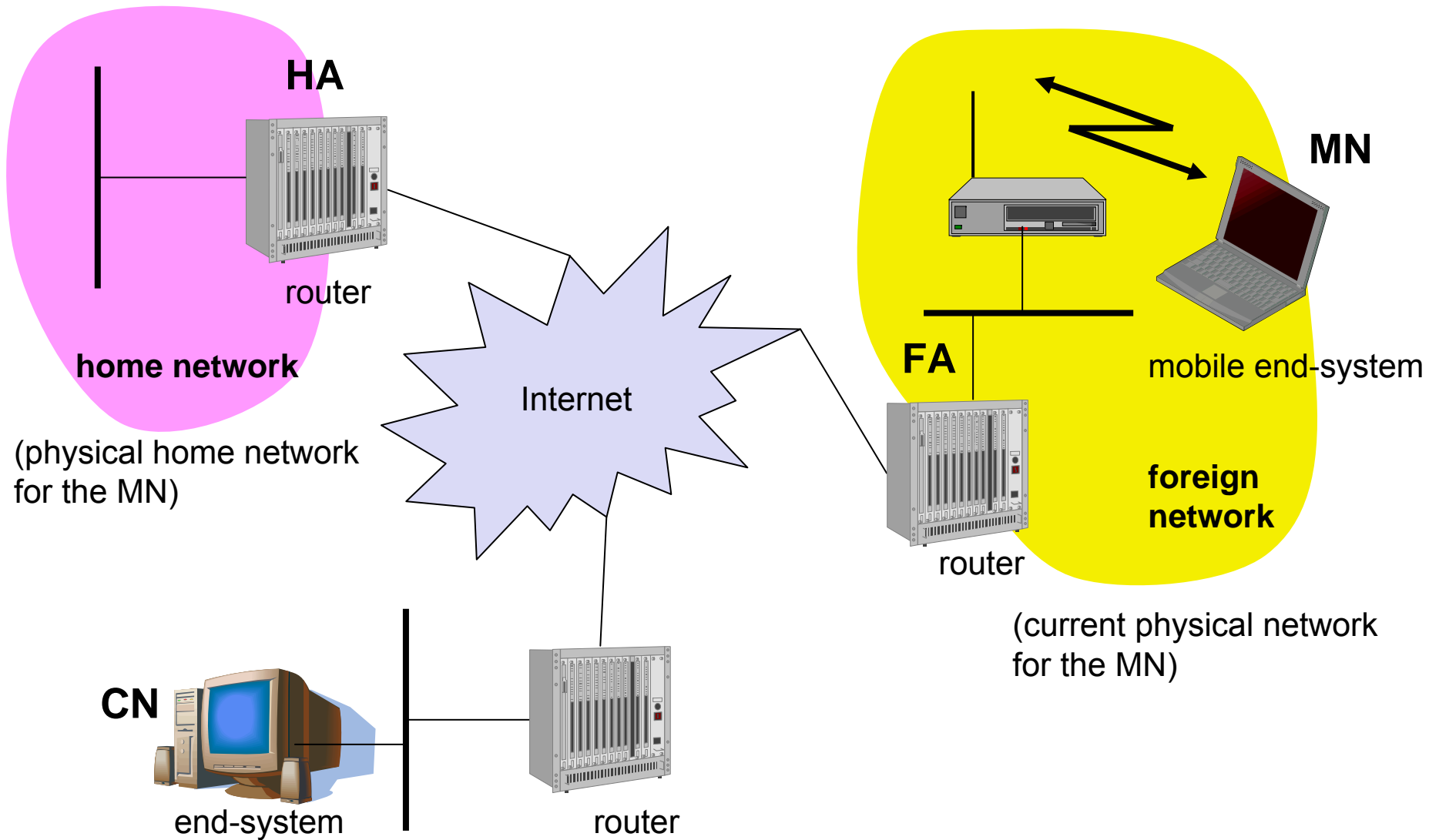
- ❑ to protocols of higher layers (e.g. TCP) and applications (e.g. WWW browser)
- ❑ changes to routers should be not required
- ❑ support of the same layer 2 protocols as IP
- ❑ access to existing Internet services should be not affected

Security

- ❑ authentication of all messages used to manage mobility (e.g. registration)

Efficiency and scalability

- ❑ only few additional messages necessary to manage mobility (connection typically via a low bandwidth radio link)





Mobile Node (MN)

- ❑ system (node) that can change the point of connection to the network without changing its IP address

Correspondent Node (CN)

- ❑ communication partner

Home Agent (HA)

- ❑ system in the home network of the MN, typically a router
- ❑ registers the location of the MN, tunnels IP datagrams to the COA representing the end-point of the tunnel

Foreign Agent (FA)

- ❑ system in the current foreign network of the MN, typically a router
- ❑ forwards the tunneled datagrams to the MN, typically also the default router for the MN

Care-of Address (COA)

- ❑ address of the current tunnel end-point for the MN (at FA or MN)
- ❑ actual location of the MN from an IP point of view

Introduction

Challenges

Approach

Architecture

Comm. Services

Conclusion



- autover®: an airport baggage handling system
 - autonomous rail-bound vehicles transport baggage in airports
 - flexibility and throughput

- Multishuttle: a warehouse system
 - autonomous rail-bound vehicles transport containers inside and outside the warehouse
 - cost and scalability

- Fast motion and effective coordination are the key to high throughput and low cost
- ✂ Reliable and timely wireless communication required
- ✂ Separate application and communication concerns





Kurzfristiger, eingeschränkt planbarer Aufbau in unbekannten Umgebungen

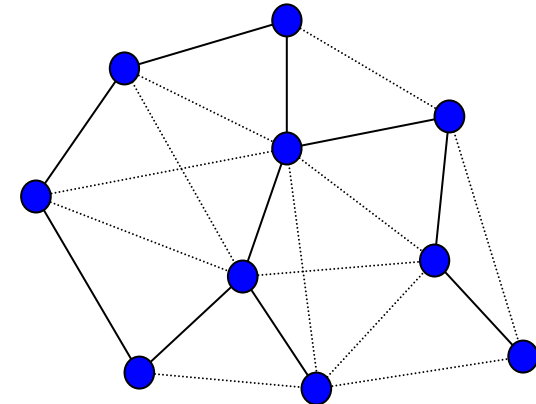
Keine ortsfesten Zellen / Knoten

Topologie bildet und ändert sich dynamisch

→ Netzwerk muss sich selbst organisieren und adaptieren

Überlagerung der Zellen nicht planbar

→ Basisdienste inhärent nicht vorhanden und müssen noch bereitgestellt werden



■ Anwendungsfall: Search and Rescue, Sensornetzwerke, VOIP

- Erforderlich: Echtzeit, Zuverlässigkeit und Sicherheit



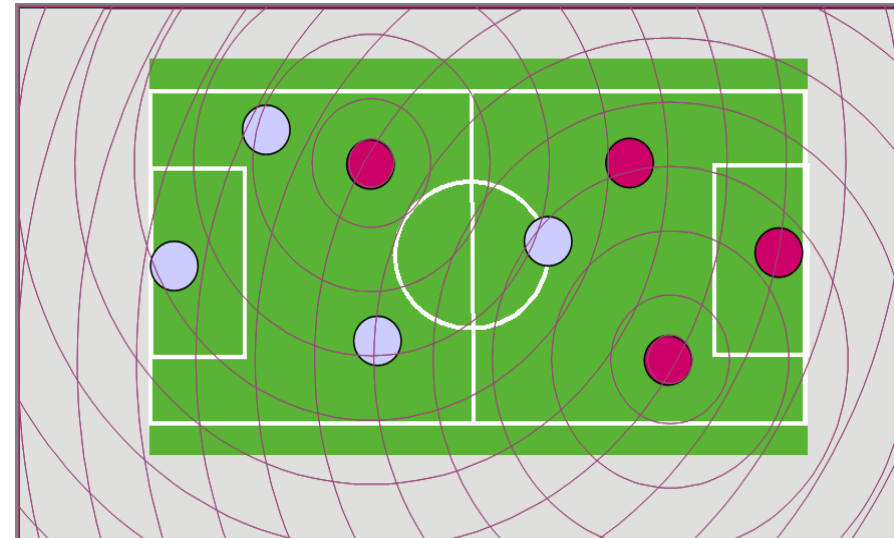
50 Edgar Nett



Mobile Computer Communication



SS'10



Direkte Erreichbarkeit, Zugriff auf ein gemeinsames Medium

→ Basisdienste inhärent vorhanden

QoS - Echtzeit, Zuverlässigkeit (und Sicherheit) - sind zu gewährleisten

Erfüllt durch:

- ❑ Geeignete Kommunikationsprotokolle

Alternative:

- ❑ Informationsgewinnung auf anderen Wegen (Vision,...)

→ Was ist mit großflächigen Anwendungen, die mehrzellige Netze erfordern?

- 2 prinzipielle Alternativen unterscheidbar

Distinguishing aspects of wireless LAN networks:

no exact range limits for receiving messages

no protection against unfriendly environment

dynamic topologies

not completely connected

But

High potential for many industrial applications



World Championship in Melbourne: Final



