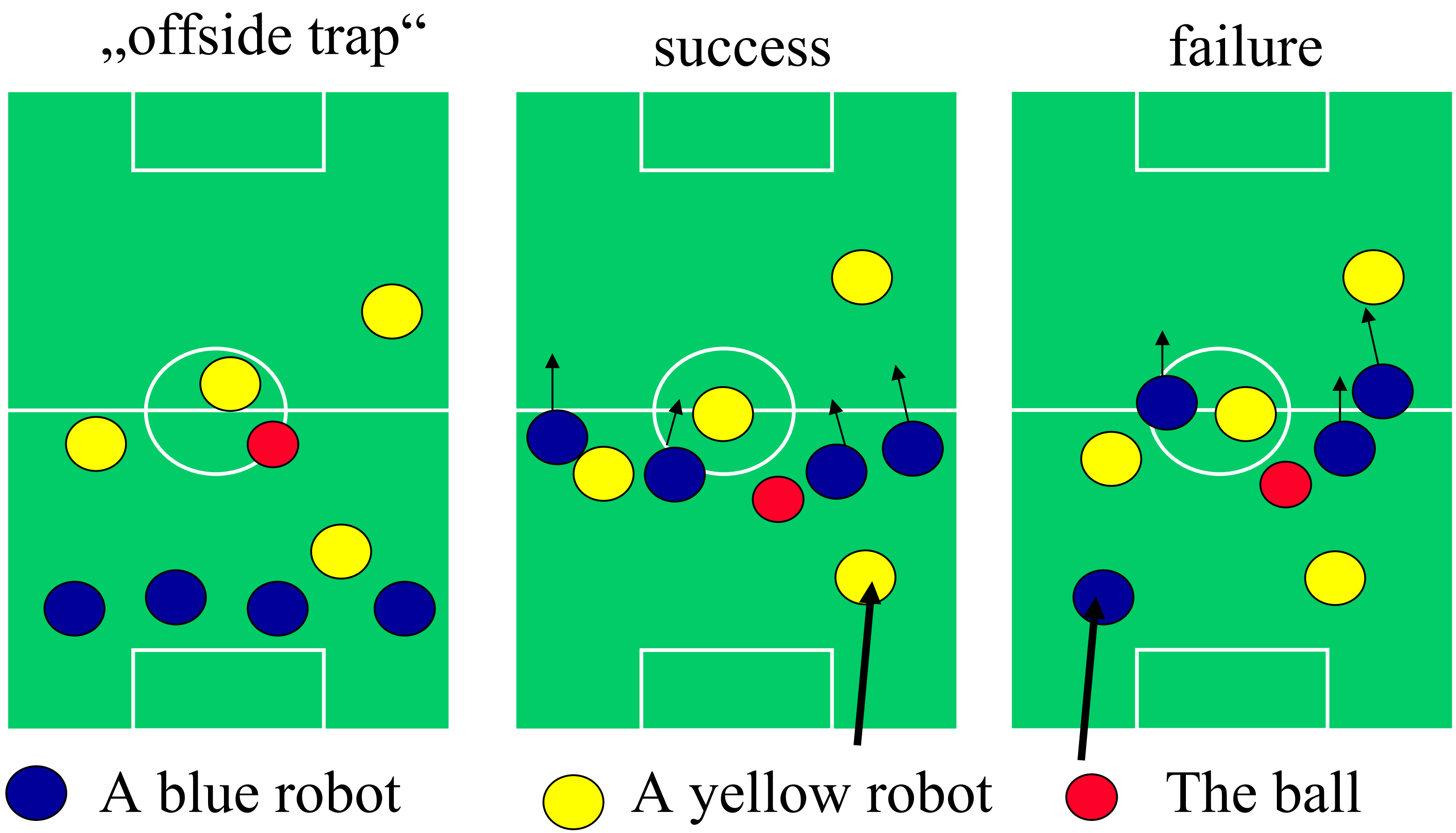
Mobile Robots

Example 5: Cooperating robots

Video

RoboCup (advanced)



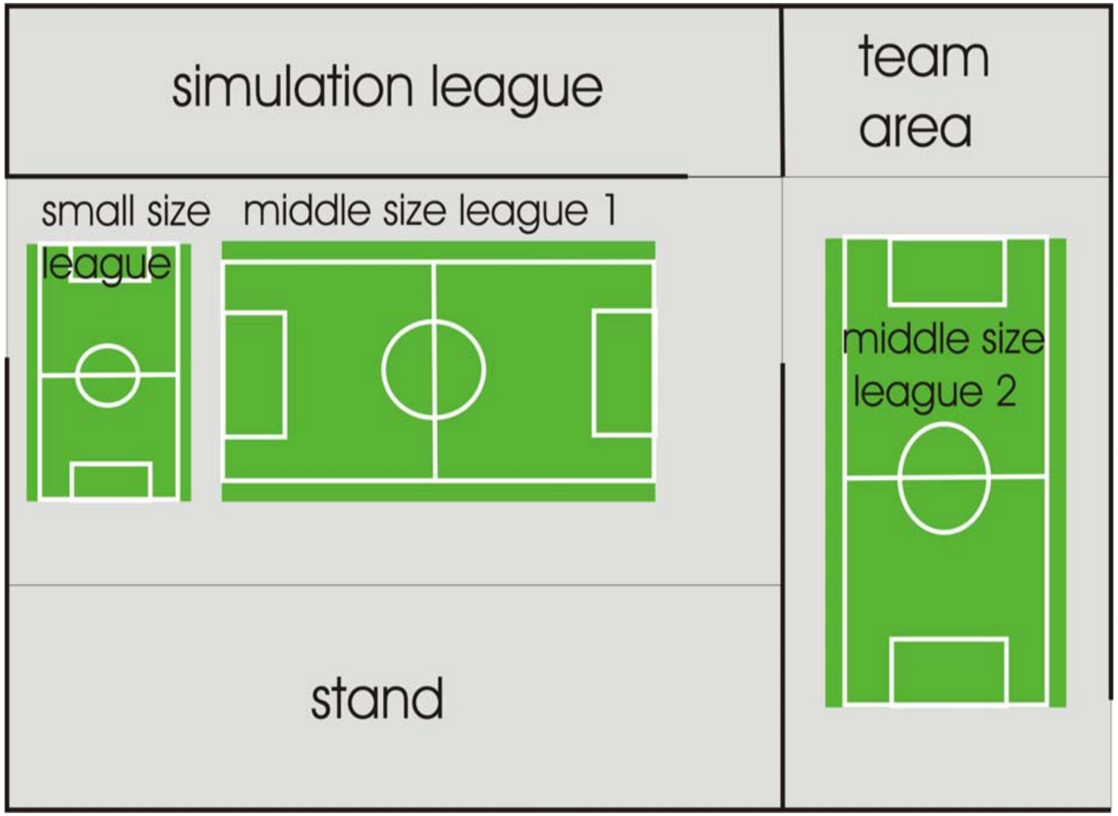
The Problem

- Usage of WLAN for real-time or even safety-critical applications, e.g.
  - Automotive applications
  - Robotics
  - Industrial automation
- General Problem:
  - Is it possible to give QoS (timing and reliability) guarantees for WLAN communication?
- Especially:
  - Is it possible to give any QoS guarantees for WLAN communication in the presence of other interfering wireless communication?

➔ Analysis by measurements under real world conditions (RoboCup)

➔ Derivation of solution concepts

German Open 2002

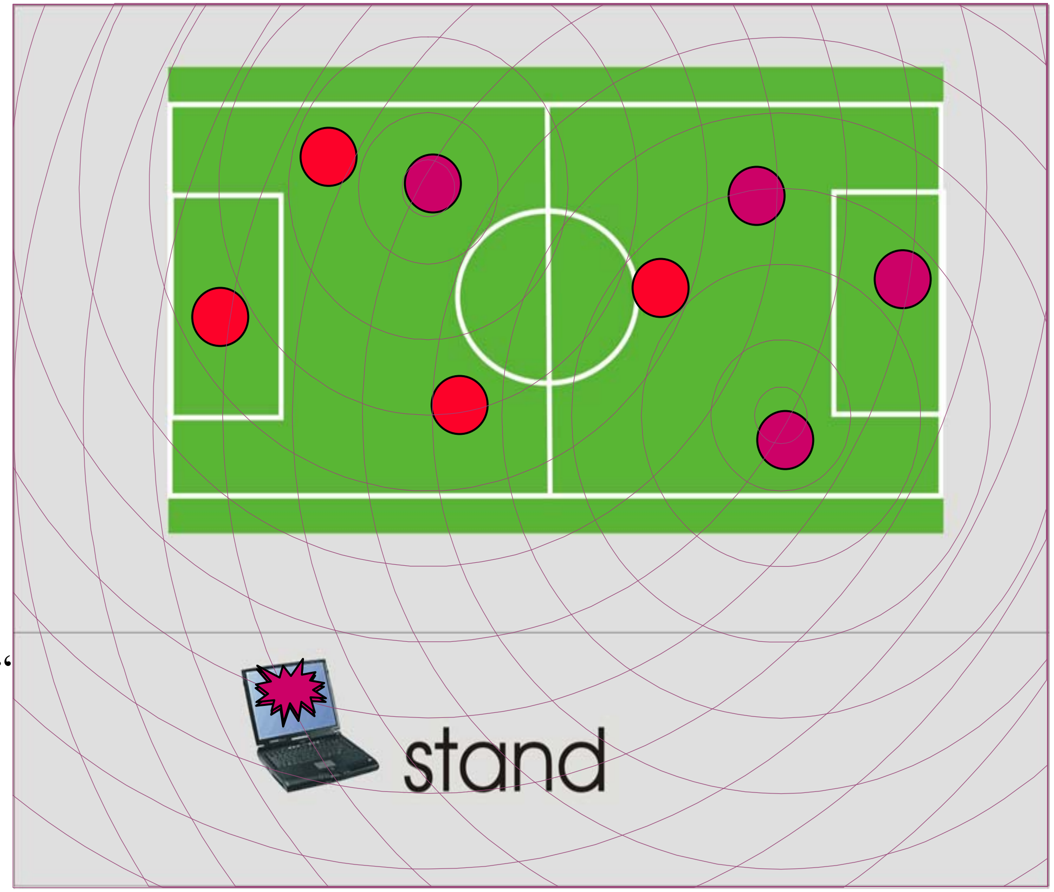


- 12 robot teams
- 2 fields with 2 LANs each; matches are running simultaneously
- Each team uses its own LAN, mostly 802.11 Standard 802.11 FHSS, 802.11 DSSS, proprietary 5GHz LAN
- Teams are faced with severe communication problems during the contests

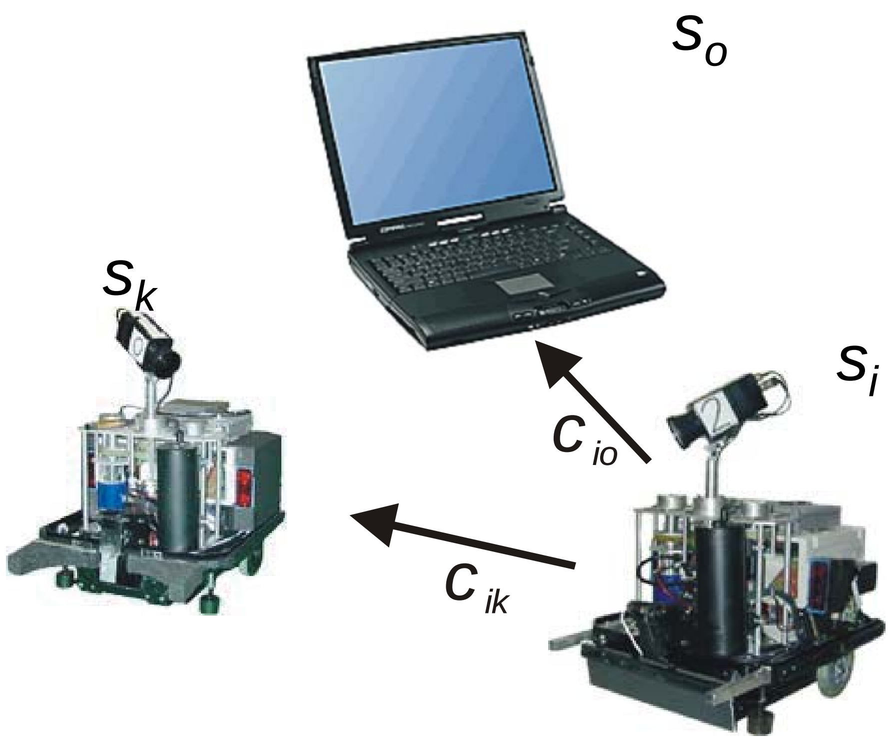
The Measurements

- Observed the LAN of one team during each match
- Captured all MAC-frames (Airopeek)
- 1.740.000 frames during four matches
- Funded by DFG in the program

  „Cooperating Teams of Mobile Robots in Dynamic Environments“

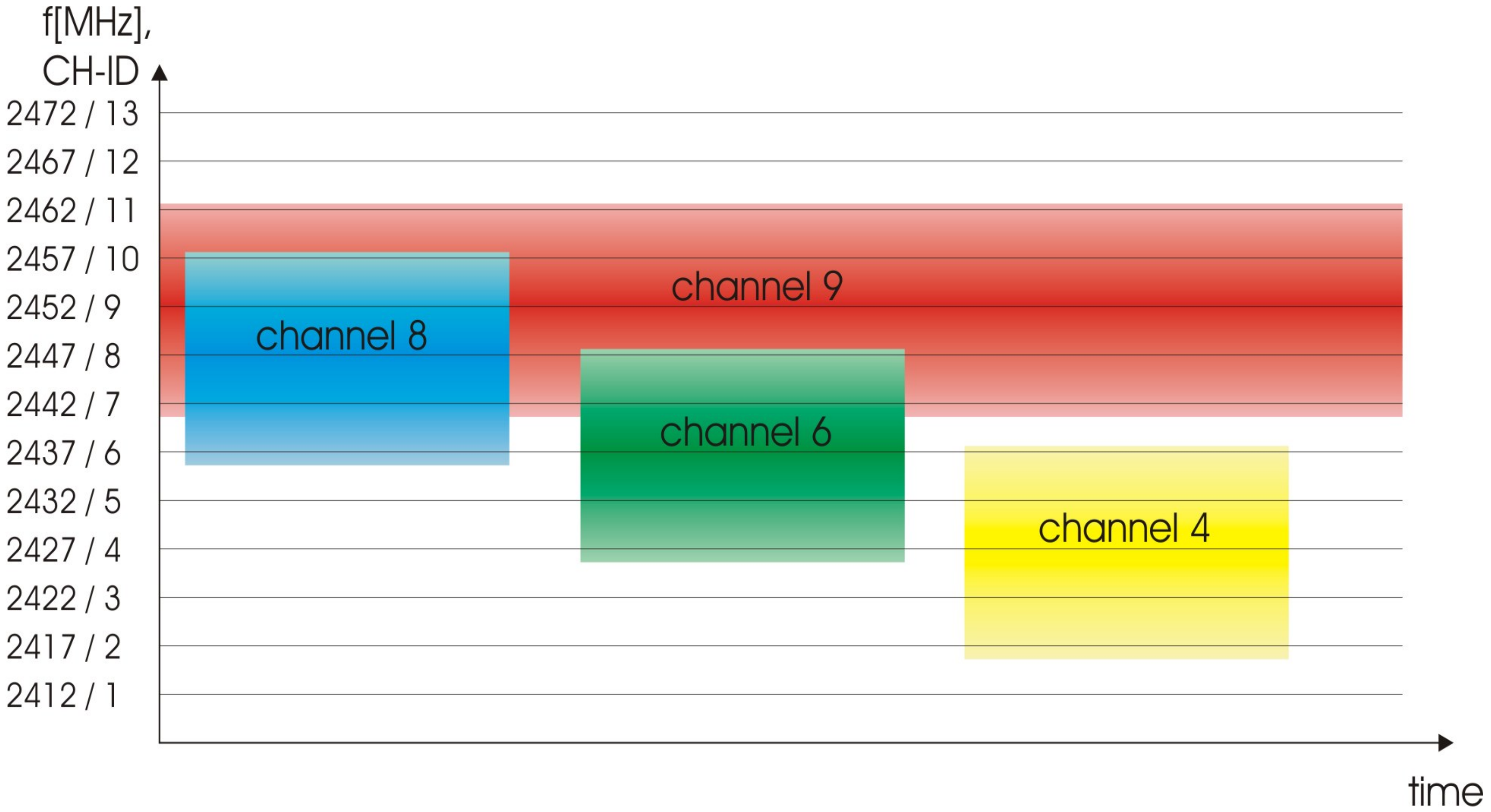


Evaluation

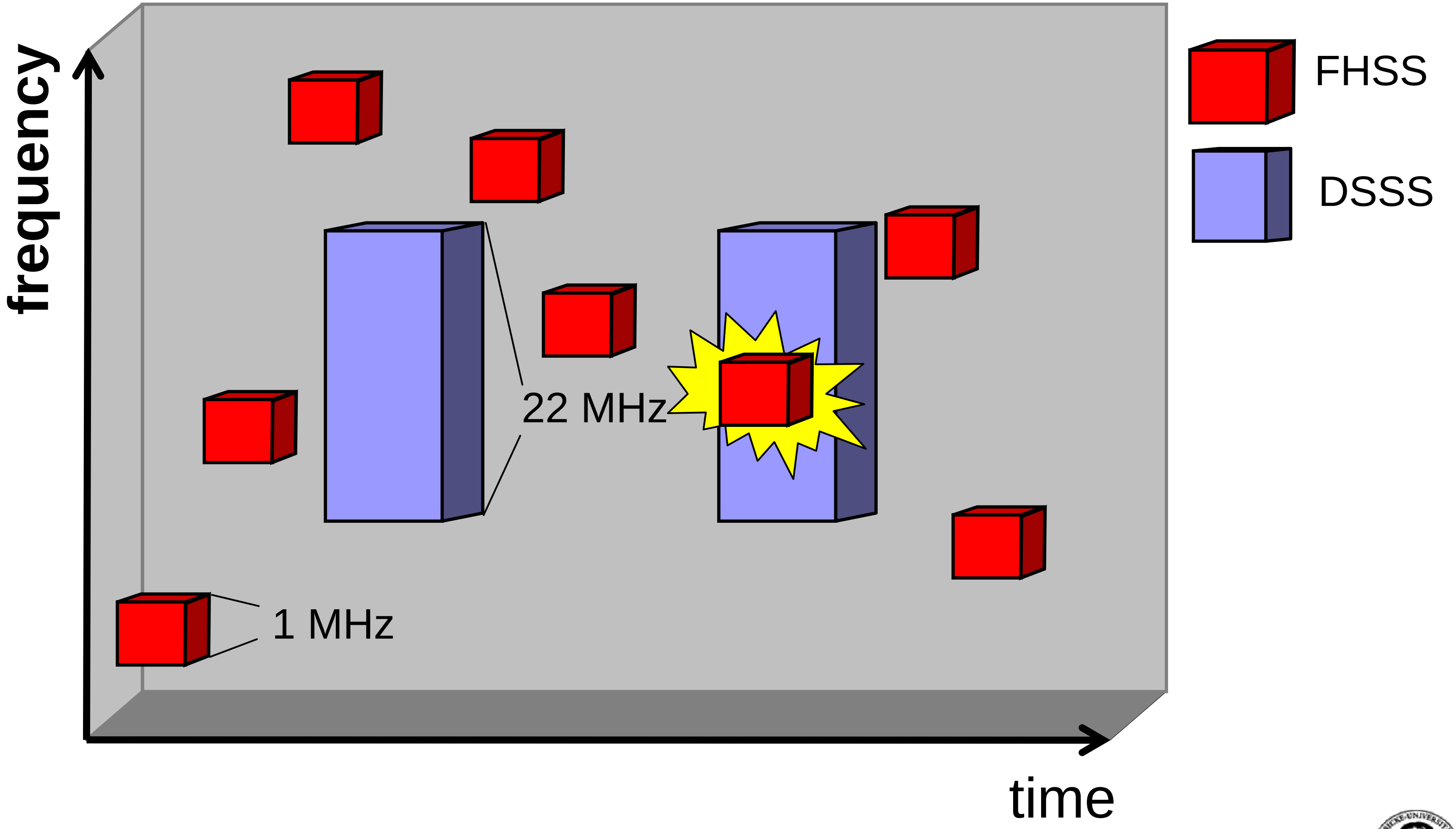


- Reliability measure for interference assessment: loss rate
- Determined as ratio between number of retries and number of point-to-point data frames
- Losses on the observer channel do not impair the results

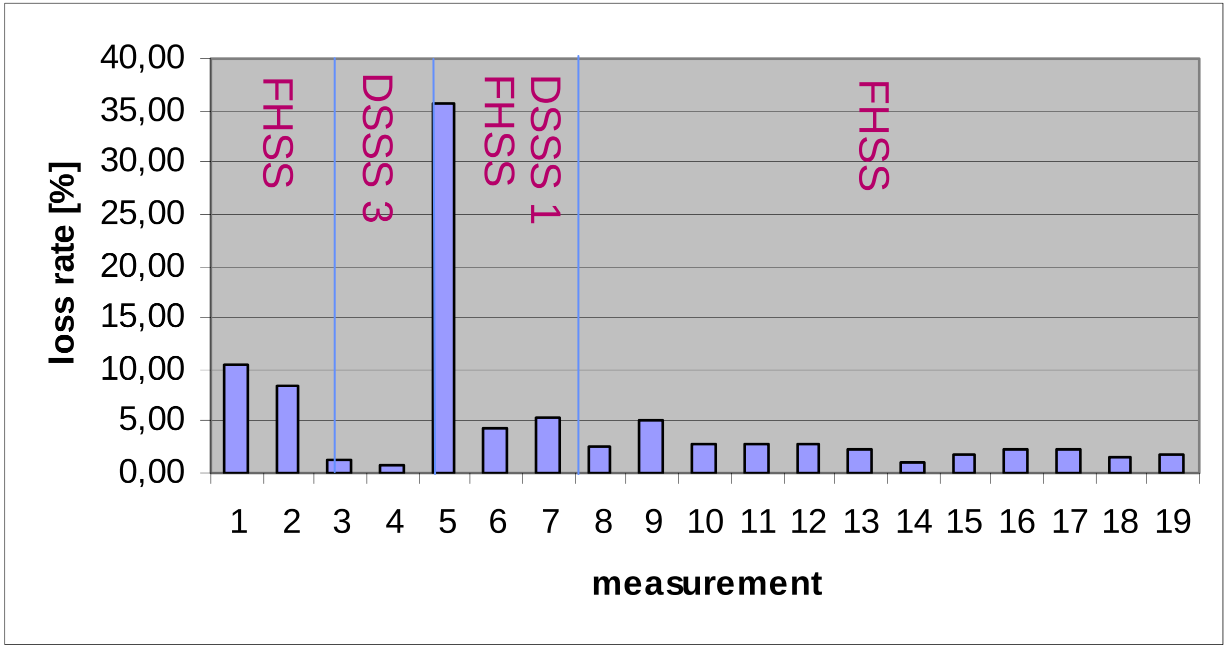
Overlapping DSSS Channels



Interference between FHSS and DSSS



Results

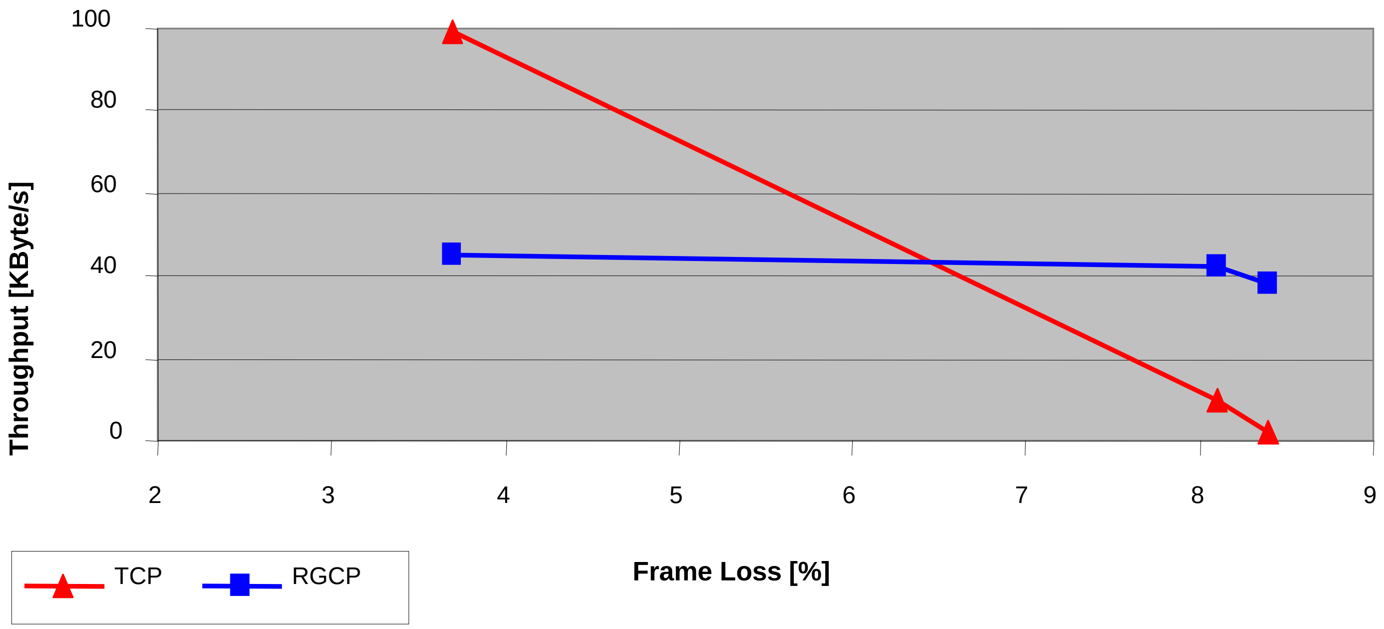


- Loss rates depend on technology and load
- Loss rates are hard to predict and may have extremely high peak values

➔ The use of wireless LANs in a common environment may cause severe problems

Communication Protocols

- Solution must be based on specific properties of the medium (MAC-layer)
  - transport-layer: much longer timeouts and retransmission delays
  - transport-layer: congestion avoidance vs. recovery from message loss
- Solution must support multicasting (cooperative applications)
- Simply adopting TCP is not a solution



Problem Statement

➔How to design a communication protocol that supports

- 1:N communication
- reliable message delivery (total order, atomicity)
- timely message delivery

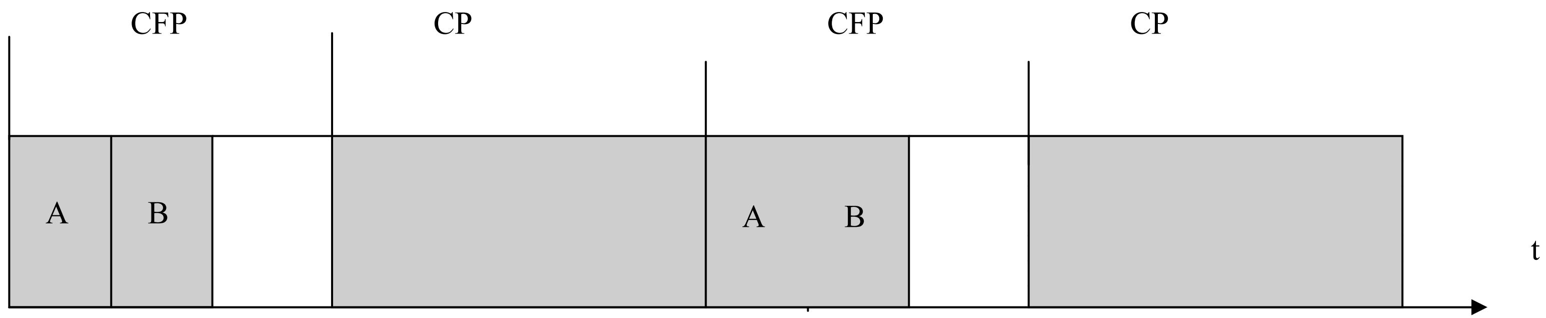
- efficiently on a wireless medium ?

The Approach

- Enhance the IEEE 802.11 standard for wireless LAN
  - the standard is commonly accepted
  - the protocol runs on off-the-shelf hardware components
  - the standard already provides basic support for real-time protocols (specified)

- Wireless medium is a challenge for the design of reliable real-time group communication protocol
  - high degree of message losses
  - limited reach of messages, mobile stations must be considered
  - low bandwidth available -> solution must have low overhead

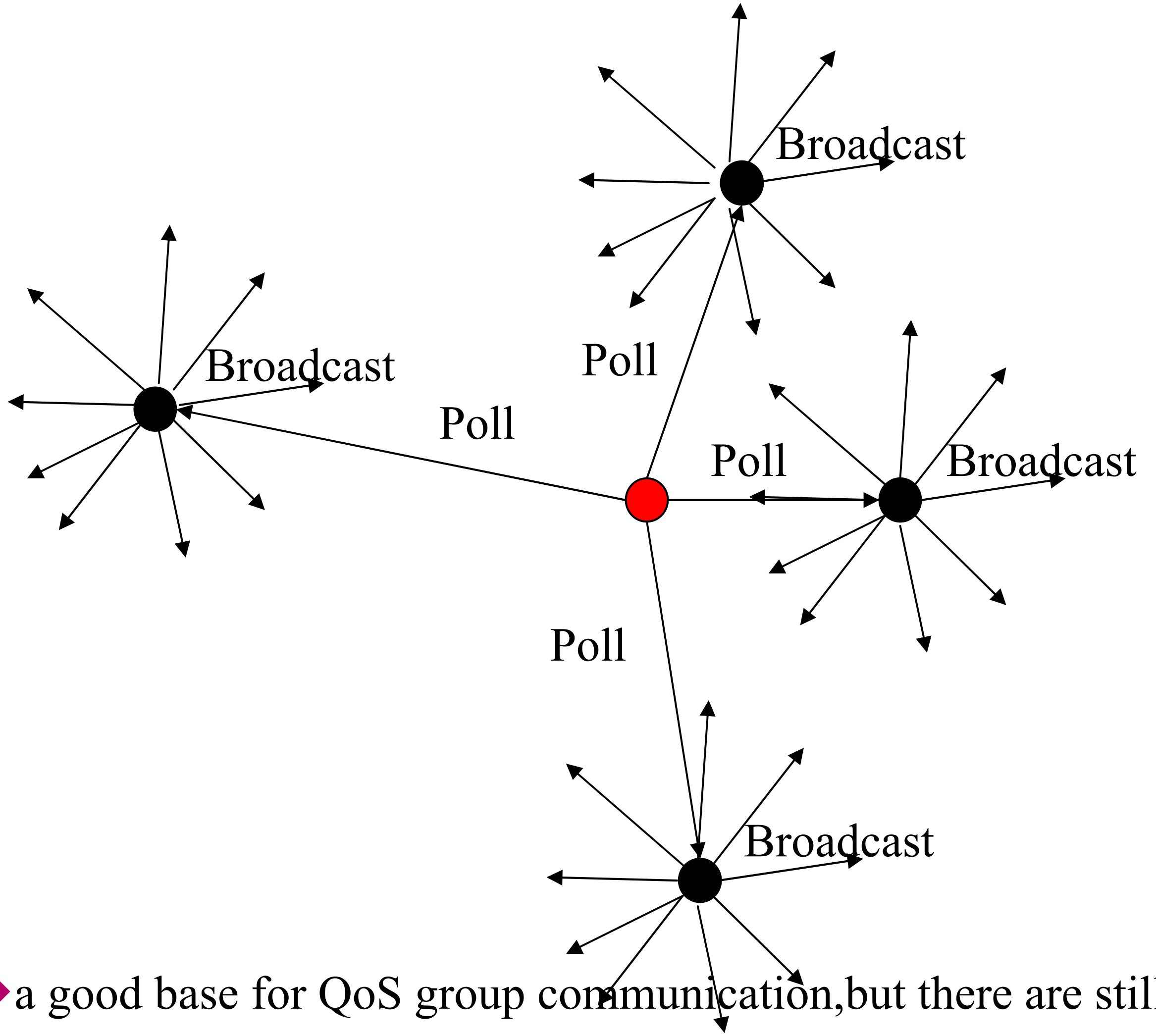
Shared channels over IEEE 802.11 wireless LAN



- Alternating phases of medium access control
- Contention Free Period (CFP) builds basis for QoS communication
- Contention Period (CP) supports efficient best effort communication

IEEE 802.11 contention free access

A central access point grants access to the medium by polling the stations



➔a good base for QoS group communication,but there are still …

Remaining problems

- Messages can be lost, even worse
- Some stations may receive a message, some others may not
- Stations can crash
- Stations can be out of reach
- No timing guarantees are given

➔ Must make specific fault assumptions for giving any kind of guarantees

Fault Assumptions

- Messages are either lost or delivered within a fixed time bound
- Message losses are bounded by an Omission Degree OD
- Stations may fail (silently)
- Stations may leave/enter the reach of other stations
- The access point can be considered to be stable

➔ Reliable real-time communication can be achieved by using redundancy to tolerate faults

Static vs. Dynamic Redundancy

- Static redundancy - Message diffusion
  - principle: every message is transmitted OD+1 times
  - good: simple, no need to detect message losses
  - bad: large overhead

- Dynamic redundancy - Acknowledge/retransmit
  - principle: every message is only retransmitted if a message loss occurs (maximum OD retransmissions)
  - good: small overhead for retransmissions
  - bad: acknowledgements for detecting message loss induce extra overhead

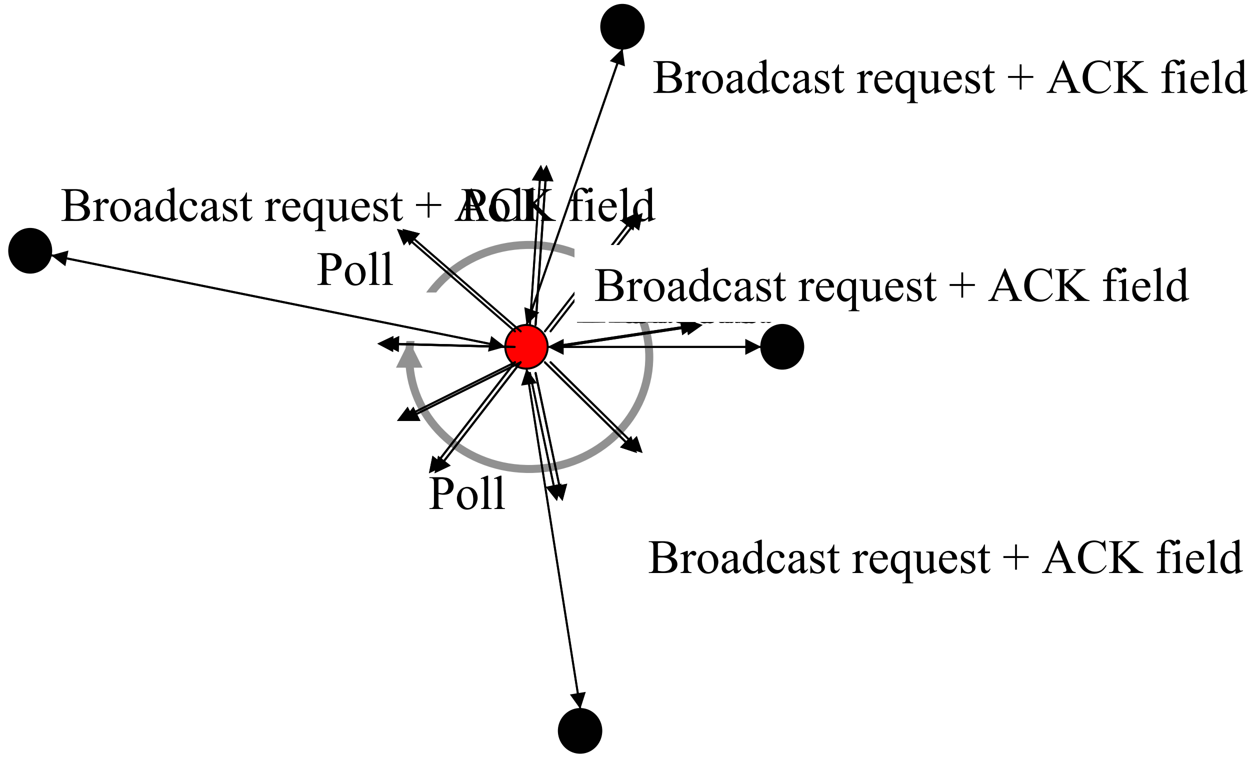
➔ Acknowledgment scheme is crucial

Key ideas of our protocol

- Broadcast messages are routed through the access point
  - Membership problem due to limited reach and mobility solved
  - ordering problem solved
- Efficient acknowledgement scheme
  - communication is organized in rounds of length n
  - one ACK field (n bits) acknowledges all messages of the preceding round
  - ACK field is piggy-backed to the broadcast request message
  - if necessary, the access points retransmits the message of the preceding round (at most OD retransmissions).

➔ no extra acknowledgment messages needed !

Operation of the protocol



Timing Analysis

- Polling/broadcast request messages can be lost
- Broadcast messages can be lost
- At most omission degree OD retransmissions required,
  (OD is dependent on the physical characteristics of the application environment)

➔ worst case delivery time can be computed

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

$(\Delta round := n \times 3\ t_m)$

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

---> worst case delivery time ≈ 680 ms

Example 2: OD = 15

---> worst case delivery time = 1016 ms

Trading Timing Guarantees against Reliability

- 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.
- Approach: Allow the application to limit the number of retransmission and guarantee agreement on consistent delivery

User defined resiliency degree

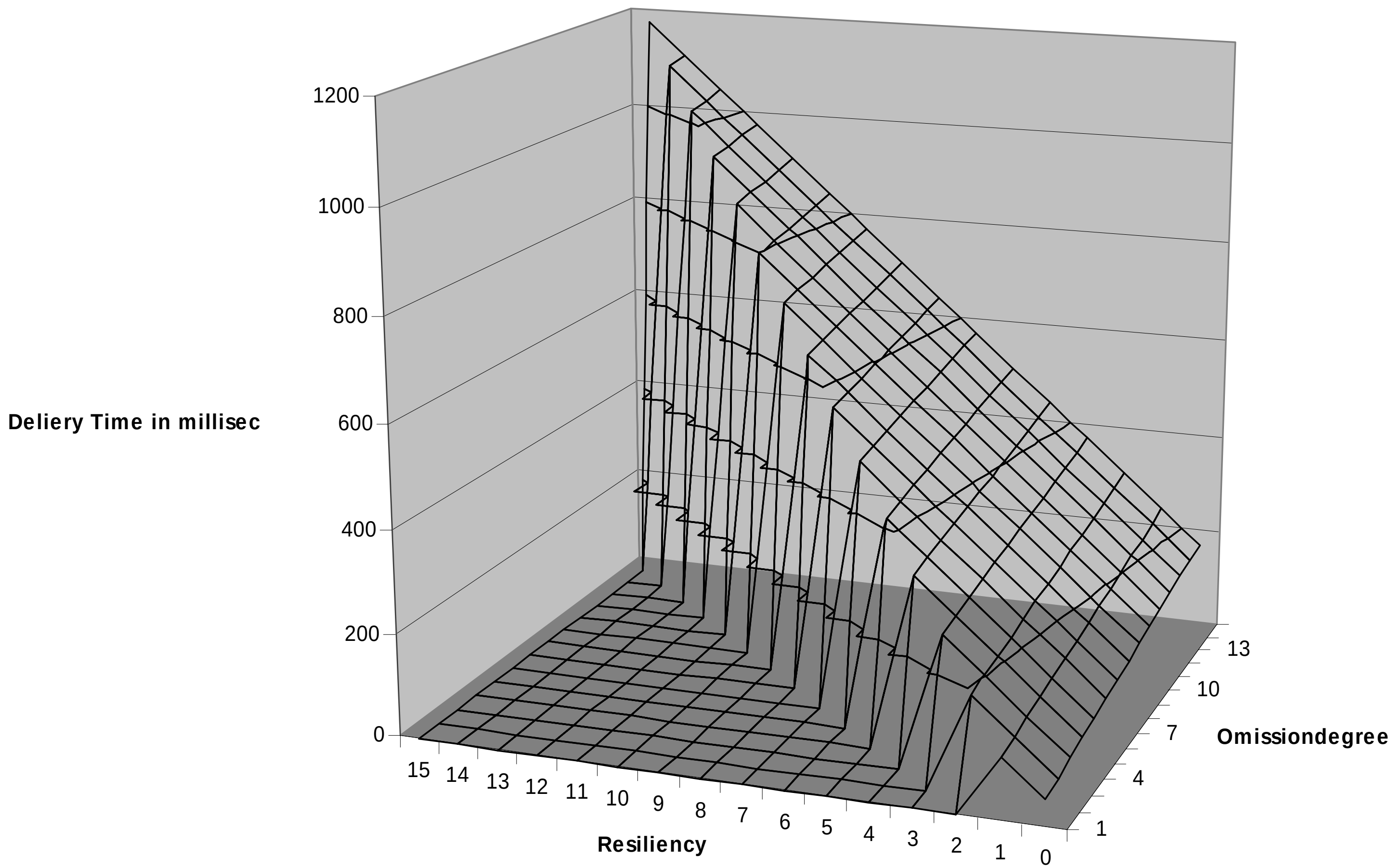
- Limit the number of retransmission by a user defined resiliency degree res(c) (maximum OD)
- If a message is not acknowledged by all stations after res(c) retransmissions, it is rejected.
- The access point puts its decision whether to reject/accept a message in an accept field that is piggy-backed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

Measured Effect of Resiliency Degree

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 = 2%, Office environment

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.

Properties of reliable real-time group communication:

- Integrity (no duplicates, no spontaneous messages)
- Validity (every message is delivered eventually, if no station crashes)
- Agreement (either all or none of the stations receive the message)
- Total Order (all stations receive all messages in the same order)

- Timeliness (there is an upper timing bound on message delivery)

Real-Time (Paradigms) (70)

Taxonomy of Medium Access Control - Protocols: