An Experimental Approach to WLAN Research - A Short Tutorial

Christian Hoene

Sep 13th, 2002

TU-Berlin

Introduction

- No analysis without simulation or experiments
- No simulation without analysis or experiments
- No experiments without simulation or analysis.

- Can your WLAN PHY/MAC/Link enhancements be implemented and experimentally proven?

Indented Goals

- Researcher
  - Knowing what can be done
- Students
  - Knowing how to conduct WLAN experiment
  - Chipsets and WLAN cards
  - Measurement Tools
  - Programming

Contents

- Challenges of WLAN programming
- Overview on WLAN industry
- Intersil Prism2 IEEE 802.11b Chipset
- Measurement Tools
- Some examples from our labs

Challenges

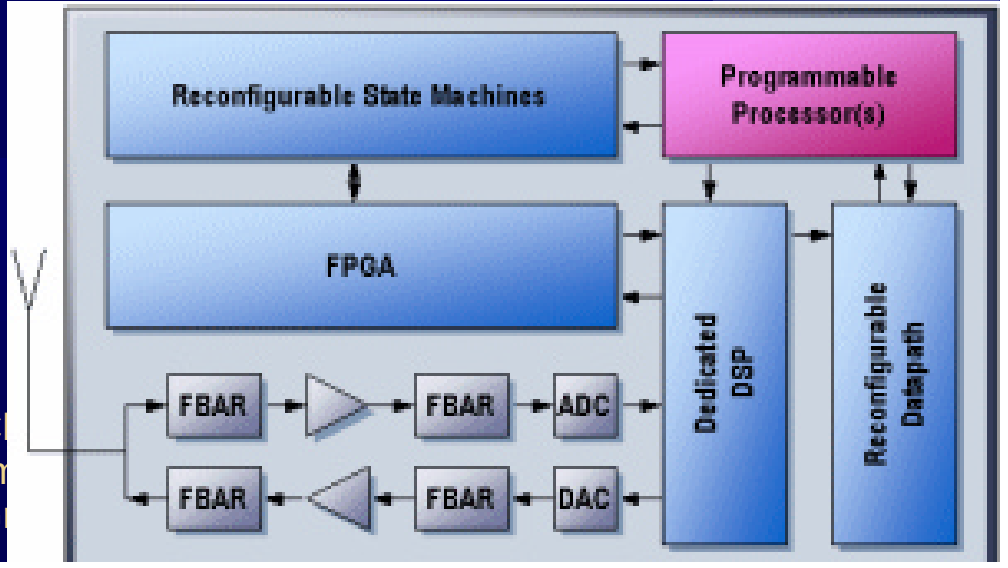
- Why it is not that simple to implement layer 1 or 2 protocols and algorithms?
- Why is it more challenging than other protocol implementations?

1. Technology constraints
2. Regulation concerns.
3. Industry fears

Technology Constraints

- Link- and MAC protocol: Hard real-time requirements
- Physical layer: High computational complexity (modulation)
- Cost and energy efficiency is required.

- Software Defined Radio is highly programmable, but not efficient.
- Most radio modems combine
  ASIC, FPGA, DSP and CPU, but have limit programmability
- One example: Berkeley Pico Nodes



Regulation Issues

- A Software Defined Radio is by definition of FCC:
- "Software defined radio. A radio that includes a transmitter in which the operating parameters of the transmitter, including the ***frequency range***, ***modulation type*** and maximum radiated or conducted ***output power*** can be altered by making a change in software without making any hardware changes.“
- Software defined radios must not be controllable by generally available software.
- No open source SDR or device drivers?

Industry Fears

To program commercial a radio modem you need its documentation and/or source code.

“On top of Atheros' issues regarding protection of its intellectual property (where are a small company that has invested a significant amount of resource in its code base and hopes to reclaim some small portion of those costs through licensing)”

“Atheros and its customers (and, more importantly, potentially the entire wireless LAN community) could be subject to significant restrictions from the radio authorities, which could damage the whole industry.

Adam Tachner, Intellectual Property Counsel, Atheros

(do not expect much help)

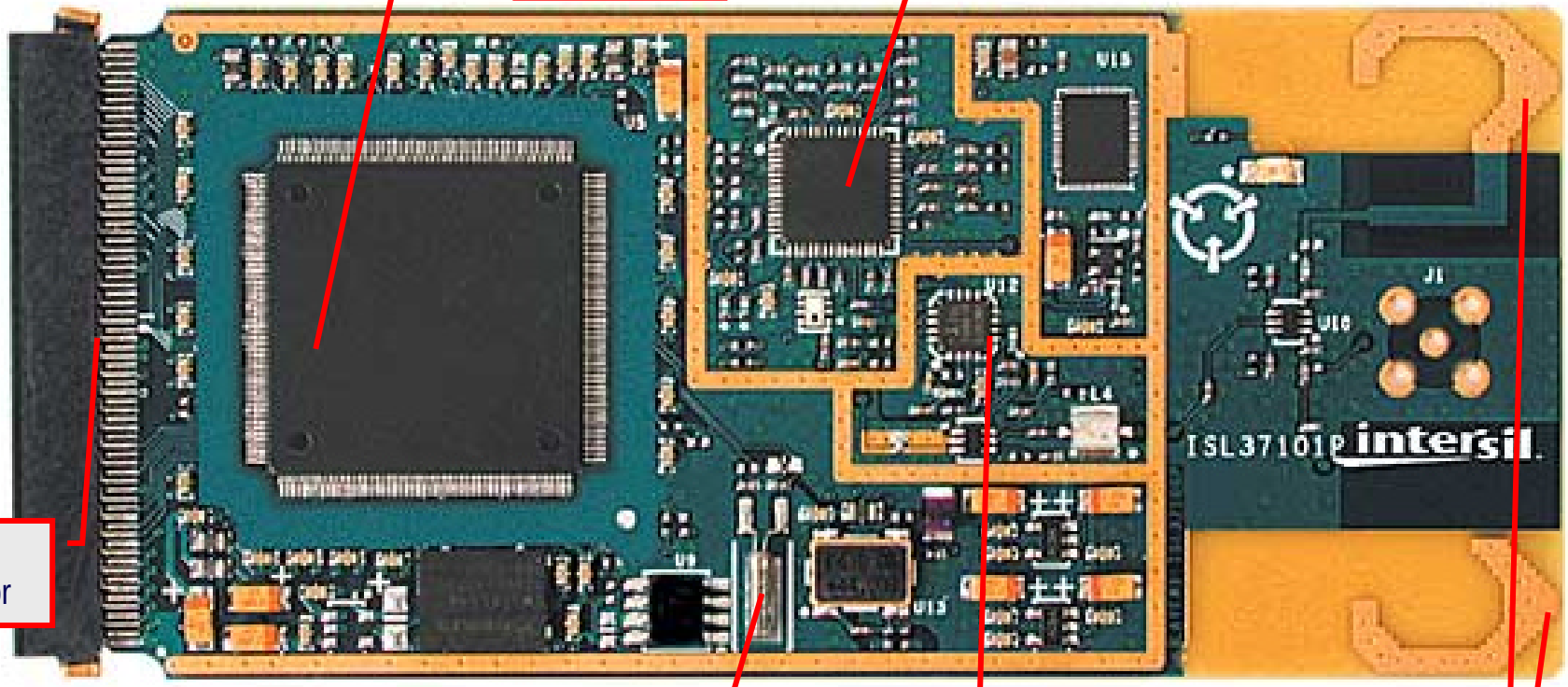
WLAN Industry Overview

- Semiconductor manufactures
  - Intersil, RF Solution, Atheros, TI
- Radio modem manufactures/OEM
  - Lucent, D-Link, Zoom, Ericsson, Siemens, Nokia, Intel,…
- Solutions
  - IEEE 802.11b: base all on chips from Intersil (PRISM)
  - Aironet PC4500/PC4800 based Prism 1 chipset
  - WaveLAN: Prism 2 chipset with special firmware
  - Prism 2 Reference Design: most common …
    - Latest chipsets 2.5 and 3 are compatible
  - Atheros AR5001X: Intel, Acer, Sony, …
    - IEEE 802.11a, 5 GHz
  - Tality IP
    - SDR Solution based in FPGAs
- Other emerging chipsets from ComSilica, Envarta, Spirea, Synad, RF Solution, …

Intersil IEEE 802.11b Radio Modems

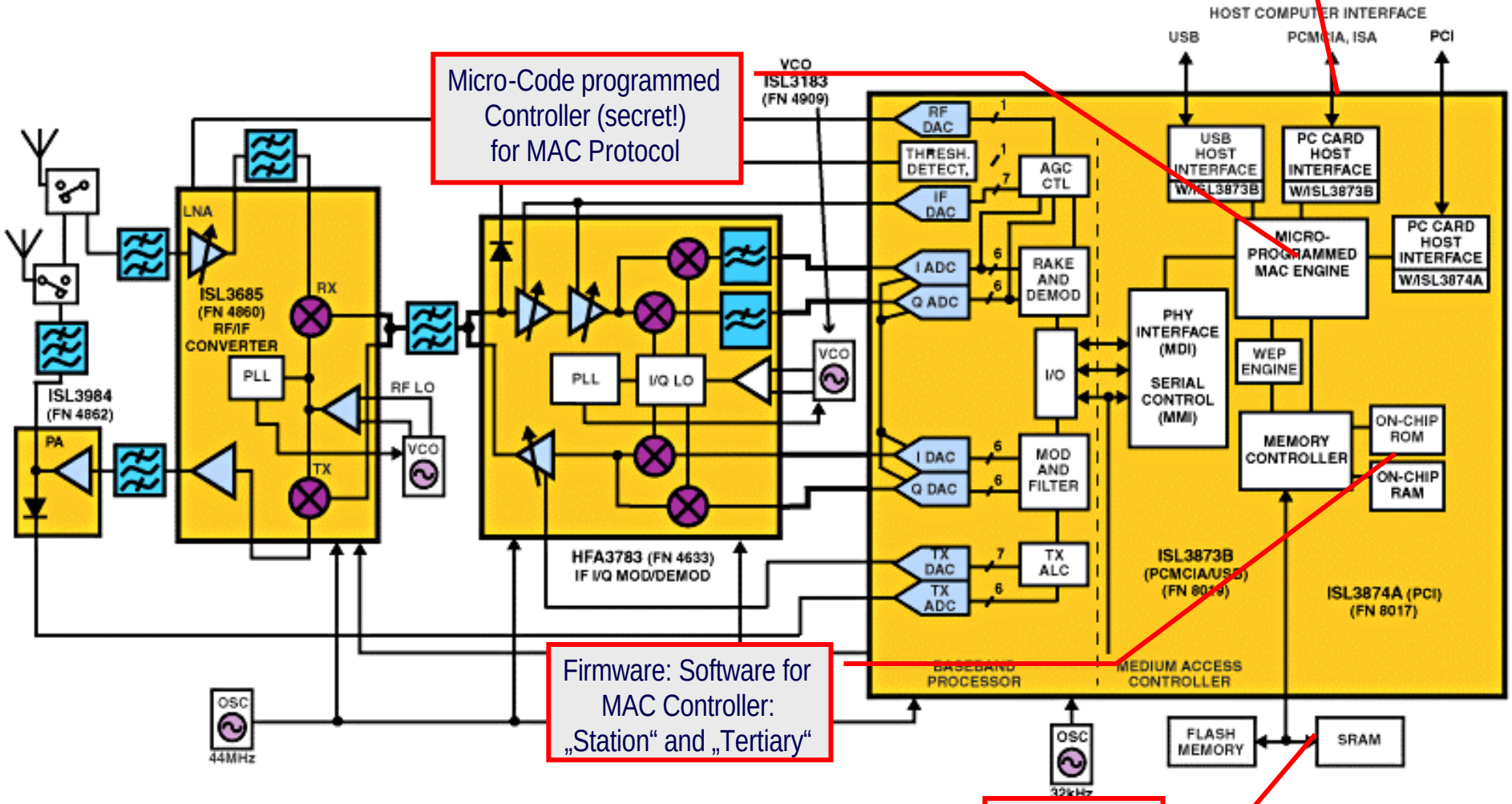
- Based on Prism 1,2,2.5, and 3 chipsets.
- widely used, cheap
- Many features
- Documentation is available under NDA
- Multiple open source device drivers:
  - Host AP (http://hostap.epitest.fi/)
  - Linux-WLAN (http://www.linux-wlan.com/linux-wlan/)

Prism2: PC-Card



Prism2: Block Picture

Documented Interfaces: USB, ISA (PCMCIA), PCI (Card Bus)



How much can I program?

- Limits:
  - Hardware is not programmable
  - No documentation about firmware
  - Thus MAC and modulation is not programmable
- Scope of Programmability
  1. Programming device driver (layer 2)
  2. Configuring radio modem: Modulation, RTS/CTS, fragmentation, retransmission, frequency, TX-Power, operating mode, association, authentication, MAC mode (PCF/DCF), power saving

What can be measured?

- Packets:
  - all IEEE 802.11 packets on the air (DATA, ACK, RTS, CTS, beacons)
  - even without CRC check
  - MAC addresses, signal strength, modulation on a per packet basis
  - Arrival time (resolution 1µs)
- Mobility
  - Handovers
  - Channel scans (other base stations)
- Authentification and Registering

HostAP Driver: Installation

- Get it from http://hostap.epitest.fi/
  - Thanks to Jouni Malinen
  - (other drivers: wavelan, linux-wlan)
- Read the manuals and README files
- Installation (as root)
  - # cd /usr/src/
  - # tar xfv Prism2-2002-05-19.tgz
  - # cd Prism2-2002-05-19
  - # make pccard install_pccard
  - # vi /etc/pcmcia/hostap_cs.conf
    Change line “module hostap_cs” to support the local WLAN network
- restart

Wireless Tools: Installation

- Get Wireless Tools from
  http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html
- Read the manuals and README files
- Installation (as root)

```
# cd /usr/src/
# tar xfv wireless_tools.24.tar.gz
# cd wireless_tools.24
# make all install
# Iwconfig
```

Measurement Tools

- Tcpdump (libpcap) (http://www.tcpdump.org/)
  L5-3 Protocols, including IEEE 802.11/PRISM headers
- Ethereal (http://www.ethereal.com/)
  (L5-3 Protocols, IEEE 802.11/PRISM headers)
- Snuffle (http://www-tkn.ee.tu-berlin.de/research/easysnuffle/)
  Internal protocol states, performance, radio modem signal strength and speed
- Device driver's log and proc files
  for error messages and debugging

Atheros Chipsets

- Documentation is available
- Programmability is similar to Intersil
- But no Linux Device Driver yet
  but Reyk Floeter is working on it.
- Programming back-off and power is possible
- No support from Atheros

Tality IP solutions

- Tality sells IEEE 802.11 solutions as Intellectual Property (as source code)
- Including IEEE 802.11a/b MAC, e, I, g, …
- Also available:
  FPGA development board
- Highly programmable,
  but quite expensive

Examples

Experiments conducted at Telecommunication Networks Group, TU-Berlin

- Power Measurements

  J.-P. Ebert, B. Burns, and A. Wolisz, "A Trace-based Approach for determining the Energy Consumption of a WLAN Network Interface", In Proc. of European Wireless 2002, pp. 230-236, Florence, Italy, February 2002.

- SPB Booster to improve Voice over WLAN

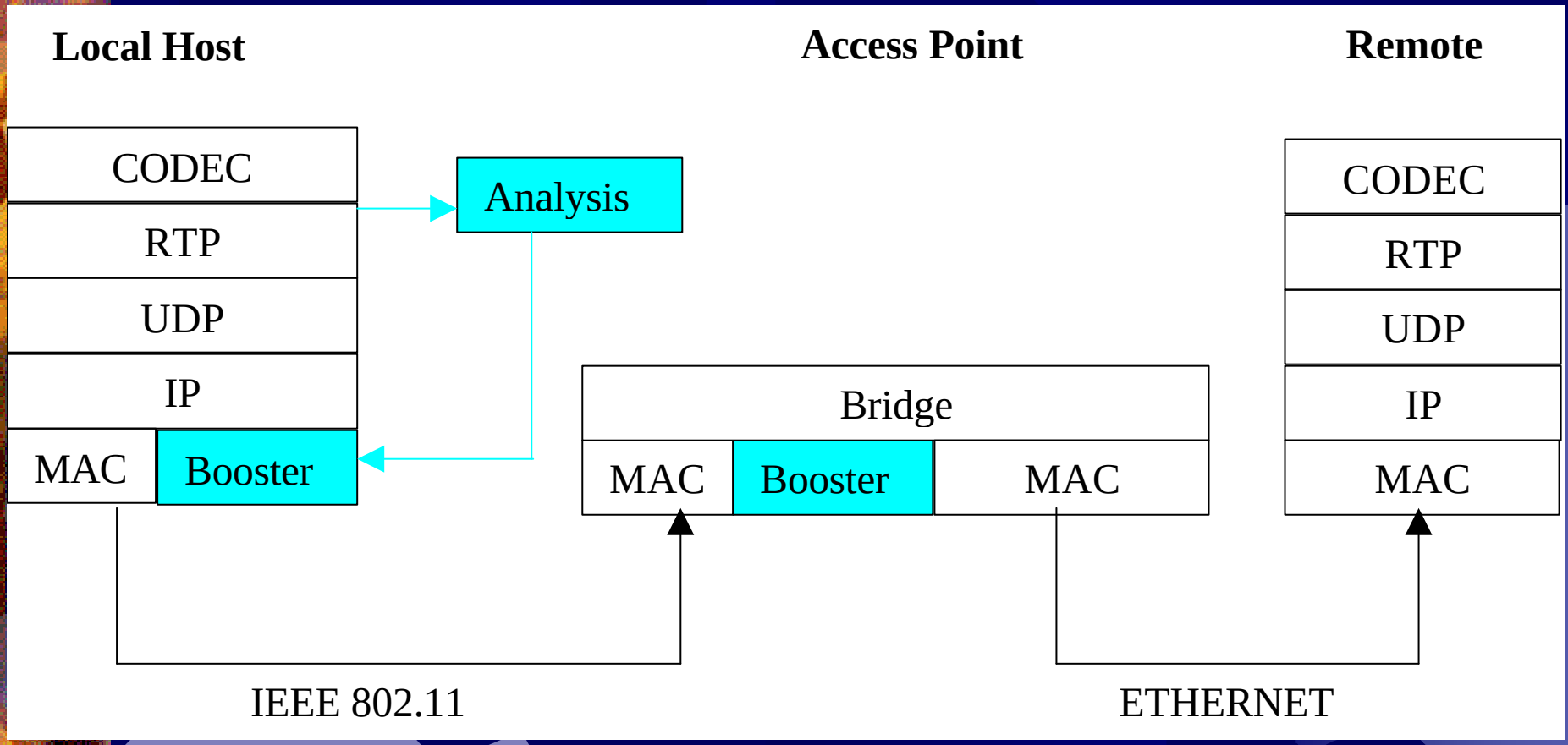
  H. Sanneck, W. Mohr, N. T. L. Le, C. Hoene, and A. Wolisz, "Quality of Service Support for Voice Over IP over Wireless", In S. Dixit, editor, Wireless IP, chapter 10, Artech House, Norwood, MA, USA, October 2002, accepted for publication.

- Measurement of Packet Loss during Slow Movement

Speech Property Based (SPB) Booster for VoIP on IEEE802.11b

- Improves the perceptual quality
- Use speech properties to
- adapts link layer protocol on a per packet basis
- Based on observation from Sanneck:
  - Segment losses at unvoiced/voice transitions are most important
  - Because frame based codecs (e.g. G.729) conceal
    of lost segment worse

SPB Booster: Architecture



SPB Booster: Design and Implementation

Design:

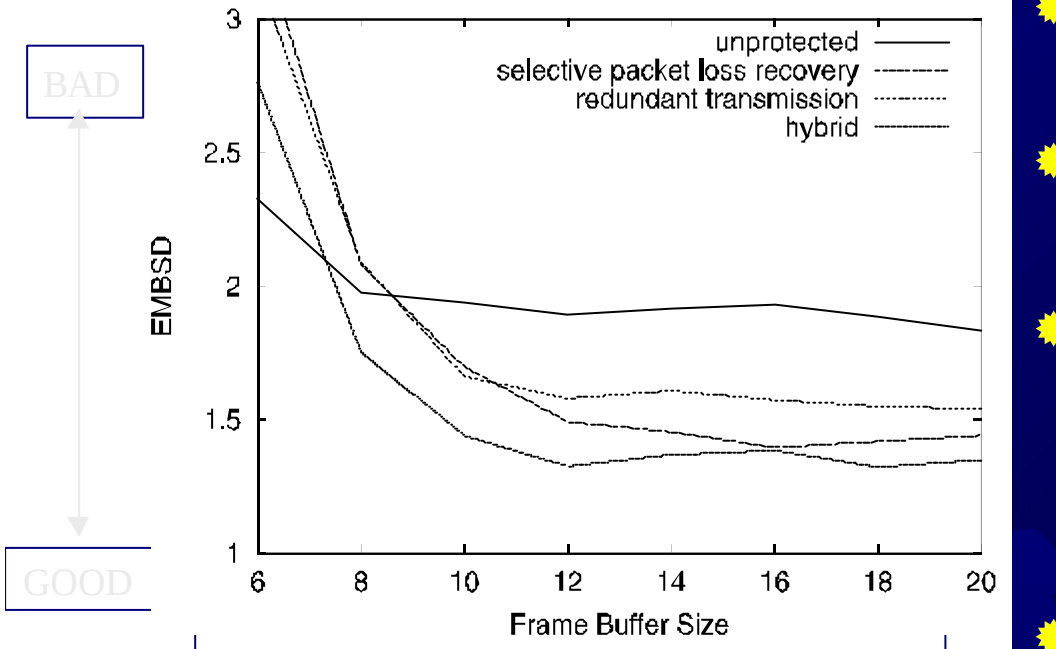
- Protecting of important Packets with three algorithms

1. Selective Packet Loss Recovery
2. Redundant Transmission
3. Hybrid mechanism

Measurements:

- Conducted experimental measurements
- Using commercial WLAN and a modified device driver.

SPB Booster: Results



Measurement Results : EMBSD / Buffer Size for all the analyzed cases

- Improvement of Voice Quality at high error rates
- A better losses distribution
- Improvement of the QoS at the link layers are possible!
- Simulations have confirmed the results

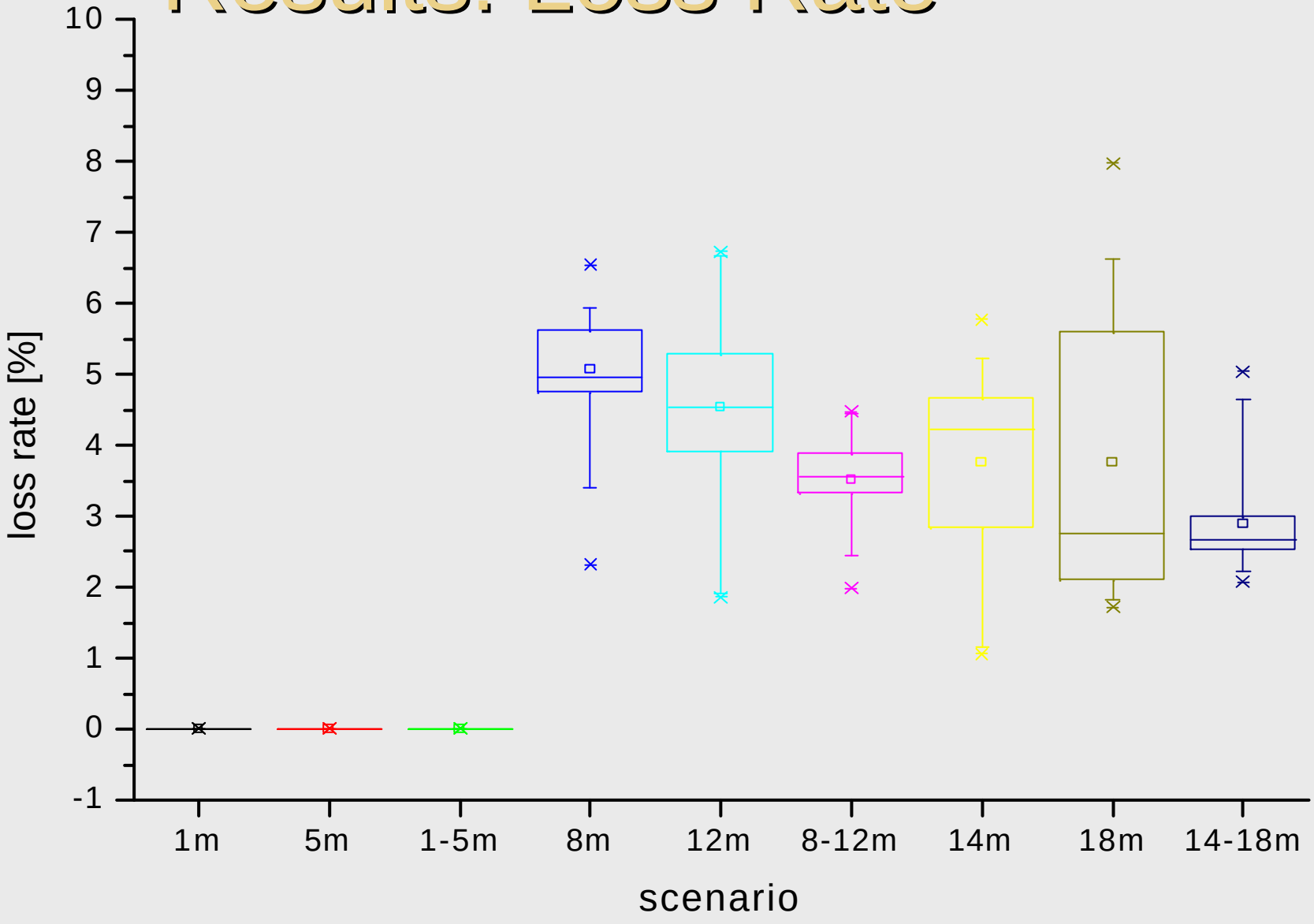
VoIP Packet Loss Measurements

Using WLAN for VoIP

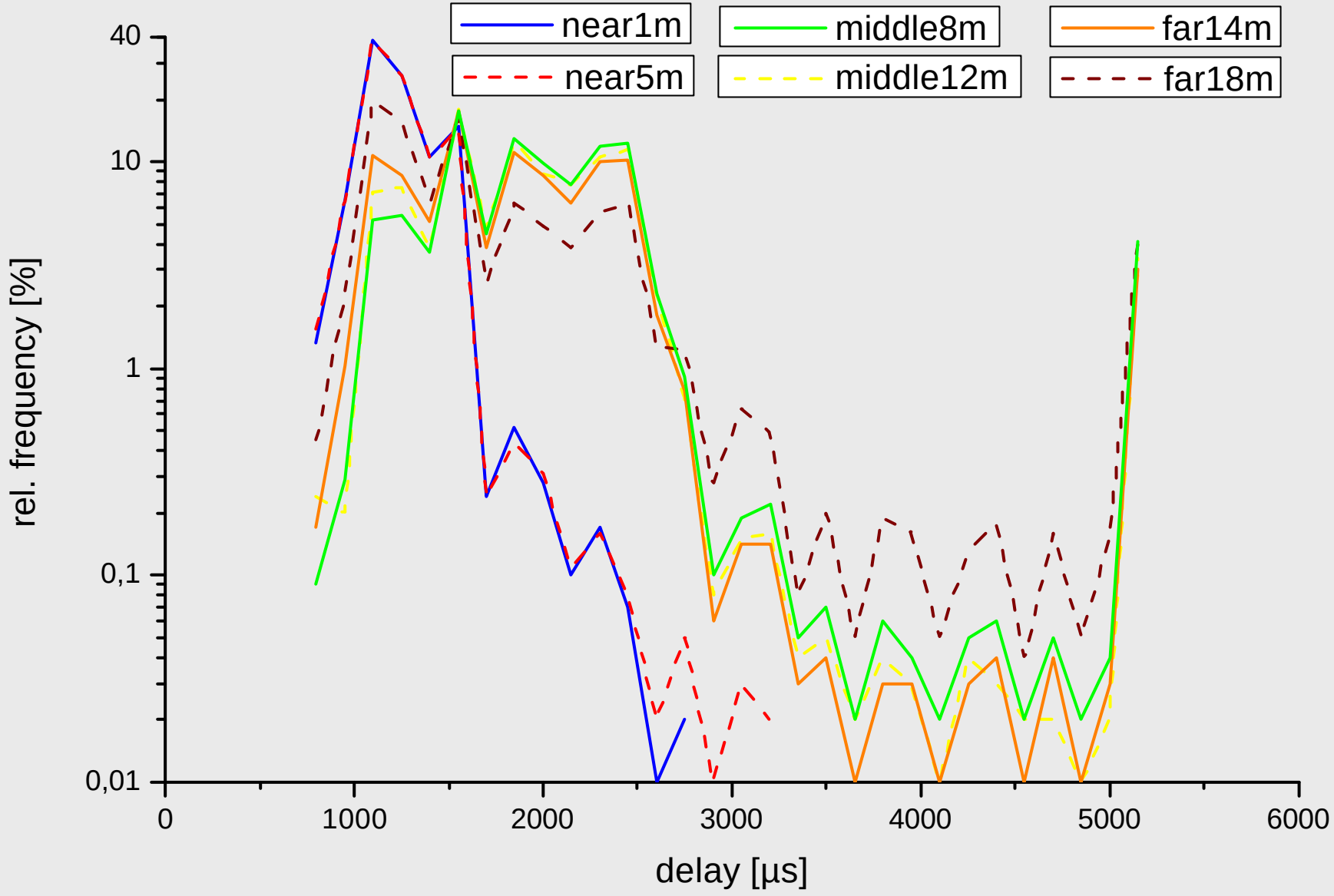
- Does human movement decrease the link quality?
- Measured metrics: delay and loss rate at network layer
- One base station and one client
  using Prism2 IEEE 802.11b with default configuration
- No background traffic
- Simulated movement of client

Experimental Movement Simulator

Results: Loss Rate



Results: Delay Histogram



Results: Explanation

- Delay increased with distance because of adaptive modulation and higher number of retransmission attemps.
- Some high delays (up to 150ms) are due to management frames and interrupt latencies.
- If the mobile moves, the channel quality changes faster
- Therefore, the probality is higher that the channel quality has improved within the maximal number of retries
- A analytical paper confirms our results.

Summary

- WLAN programming is possible!
- Implementation possibility depend on limitations radio modem technology
- Measurement are hard to be reproducible
- Demos and pilots can be implemented

- Thank you