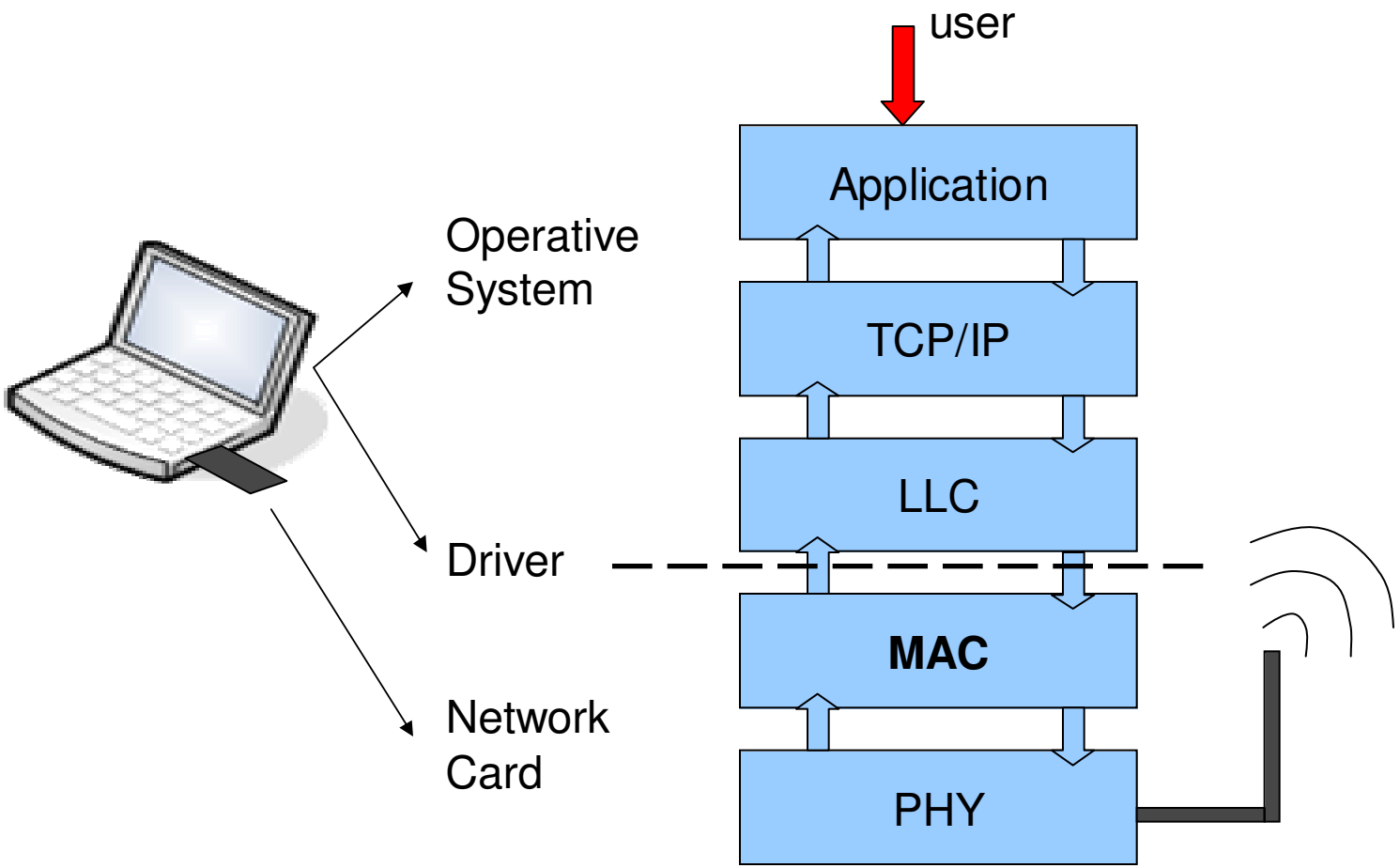
The wild world of WLAN cards

Giuseppe Bianchi, Ilenia Tinnirello

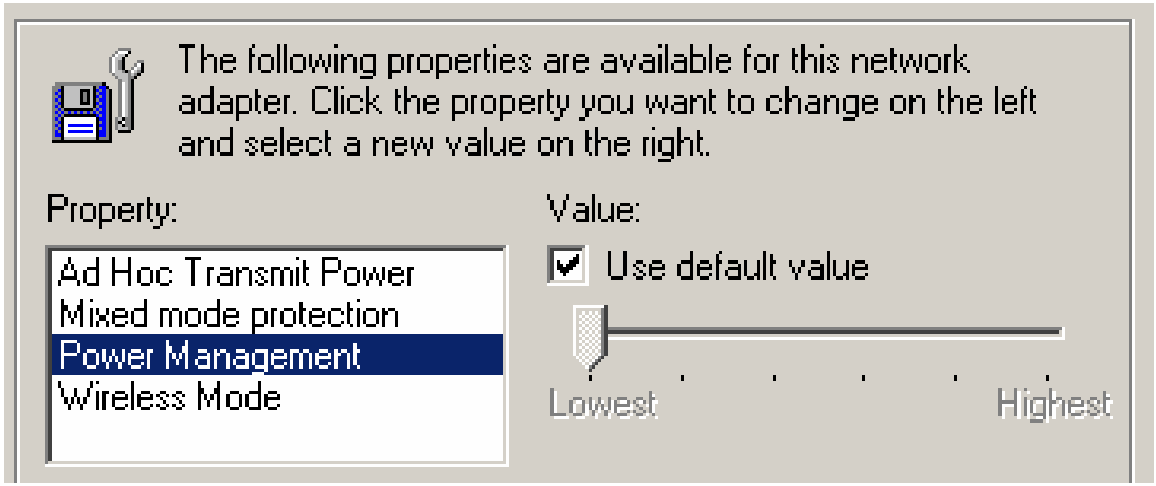
From theory to practice



User perspective: card settings

The user cannot access directly the lower stack layers, but can read/set parameters according to the driver interface, such as transmission channel, RTS threshold, transmission power..

EXAMPLE: Intel-Centrino under WinXP



User perspective: card performance

The user cannot see directly what happens on the radio channel, but it can notice the number of packets successfully received/transmitted (i.e. the throughput) at the application layer (e.g. iperf)

Typical performance measurements (saturating the transmission buffer):

1) Maximum achievable throughput when the station transmits alone
2) Bandwidth repartition with other contending stations

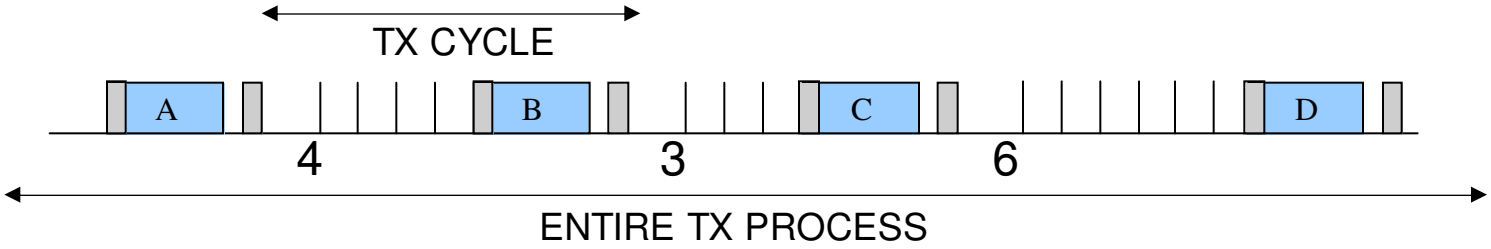
*Both the expected figures can be evaluated analytically as a function of the **packet length** and of the number of **competing stations** [1]*

```
C:\iperf>iperf -c 192.168.0.1 -i 1 -u -t 4 -b 3M
------------------------------------------------------------
Client connecting to 192.168.0.1, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
------------------------------------------------------------
[1916] local 147.46.251.223 port 2790 connected with 192.168.0.1 port 5001
[ ID] Interval       Transfer     Bandwidth
[1916]  0.0- 1.0 sec   368 KBytes  3.01 Mbits/sec
[1916]  1.0- 2.0 sec   366 KBytes  3.00 Mbits/sec
[1916]  2.0- 3.0 sec   366 KBytes  3.00 Mbits/sec
[1916]  3.0- 4.0 sec   366 KBytes  3.00 Mbits/sec
[1916]  0.0- 4.0 sec  1.43 MBytes  2.99 Mbits/sec
```

the ideal case

Max Throughput (1)

- Suppose to have just a single station, with a never empty queue
- Each transmission is originated after a backoff counter expiration (no delay due to the driver which forwards the packets to the network card)
- Since no collision is possible, and no channel error is considered, each backoff is extracted in the range [0, CW_{min}]

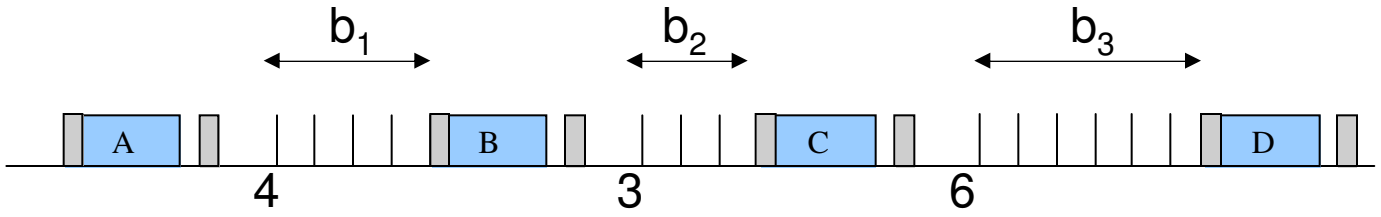


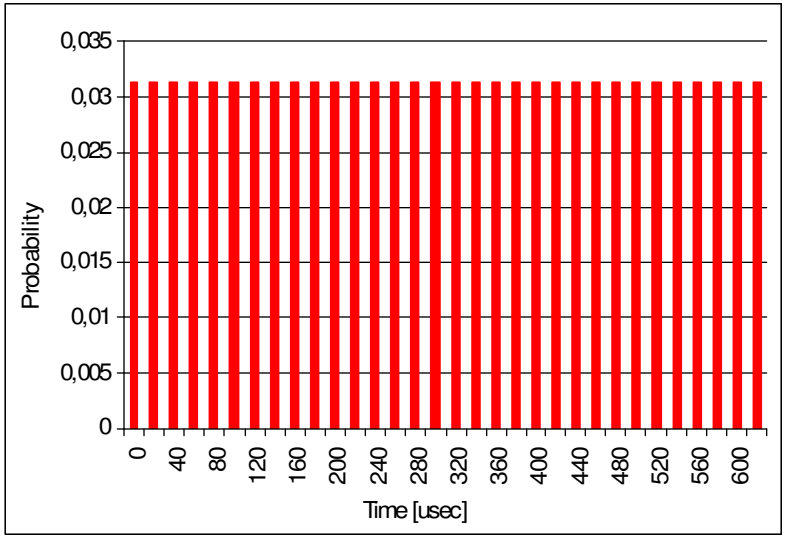
- Different transmission cycles on the channel, composed of:

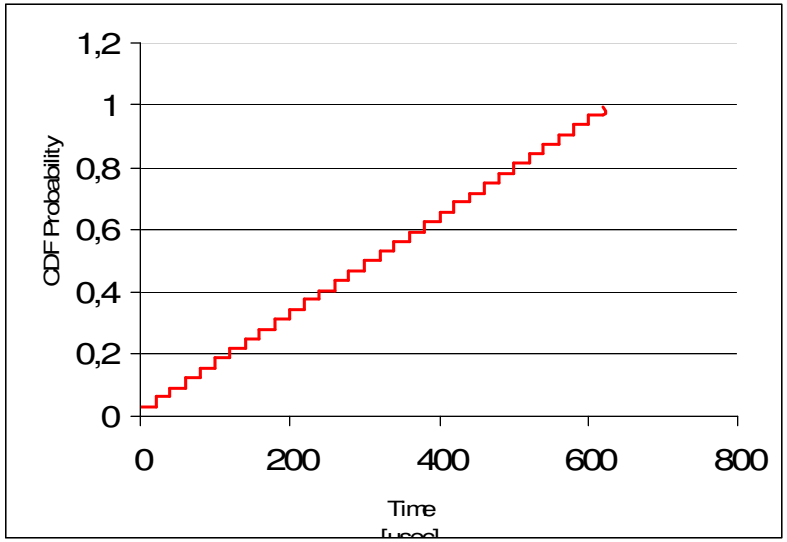
  1) frame transmission time, which depends on the MSDU size, including headers and ACKs;

  2) random delay time, which depends on the backoff extraction.

Inter-Frame Spaces (IFS)

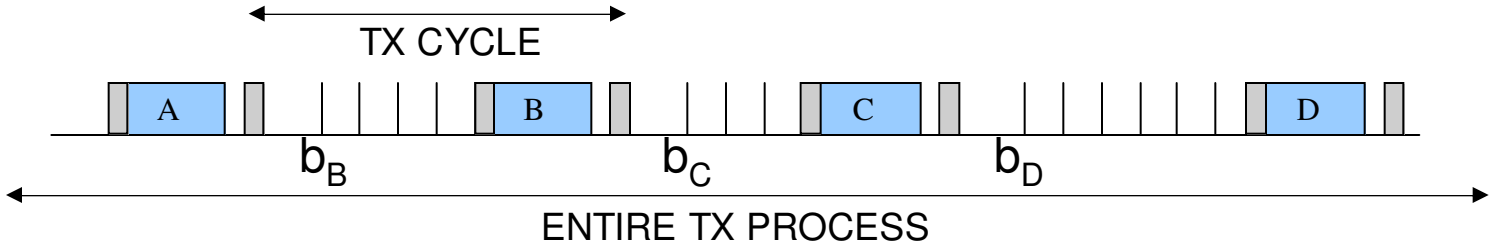






In absence of collisions and frame corruptions, b_i belong to a uniform distribution between [0, CW]T_{slot}, with a step cumulative distribution

Max Throughput (2)



➔ **From the throughput definition:** $$S = \frac{\sum P_i}{\sum \left(T_{FRAME_i} + b_i \right)}$$

➔ **From Renewal Theory:** $$S = \frac{E[P]}{E[T_{FRAME}] + E[b]}$$

➔ **In the case of fixed packet size, given CW_{min}:** $$S = \frac{P}{T_{FRAME} + \frac{CW_{\min}}{2} T_{slot}}$$

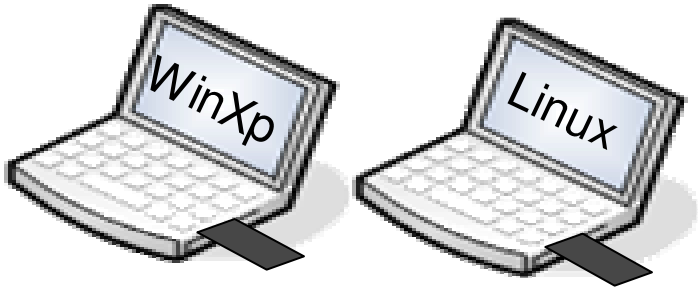
➔ **The result can be extended accounting for the number n of contending stations [1], each of which receives the same ratio S/n of the total throughput**

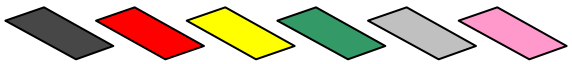
the actual world:
the user perspective

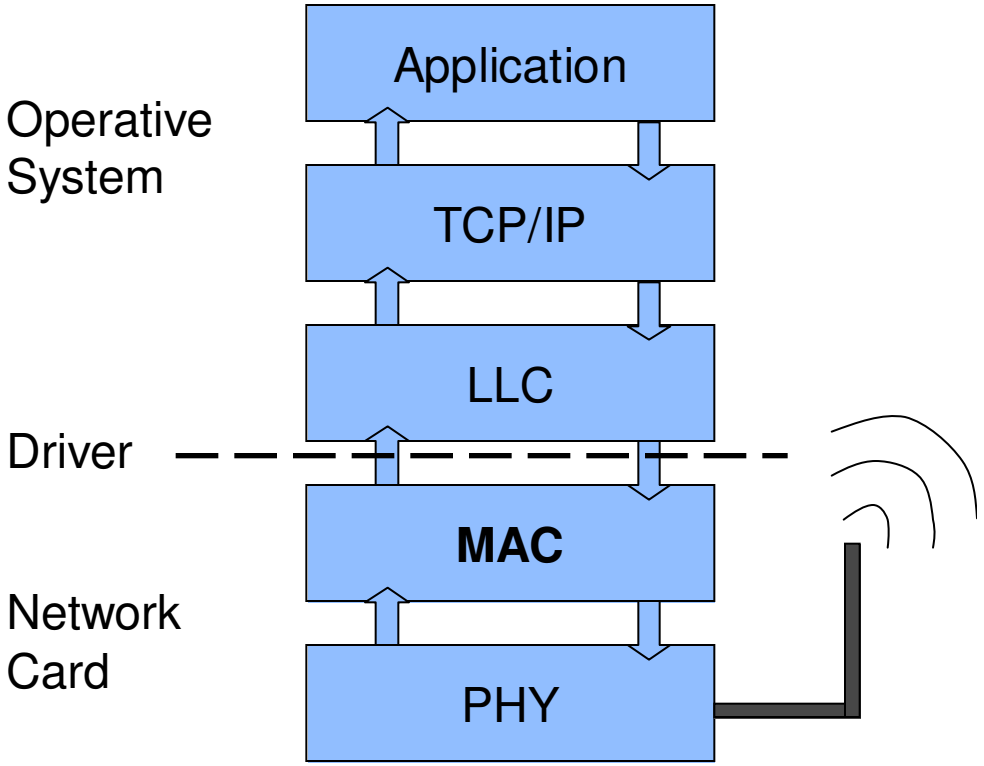
Commercial cards under test

NIC	Chipset	Host Interface
Dlink DWL-650	**Intersil PRISM II**	**PCMCIA**
Dlink DWL-122	**Intersil PRISM II**	**USB 1.0**
Linksys WPC54G	**Broadcom**	**PCMCIA**
INTEL Centrino	**INTEL 2200BG**	**MiniPCI Compliant**
Digicom Palladio	**Realtek RTL8180**	**PCMCIA**
ASUS WL-107g	**Ralink RT2500**	**PCMCIA**

Complete Test Suite

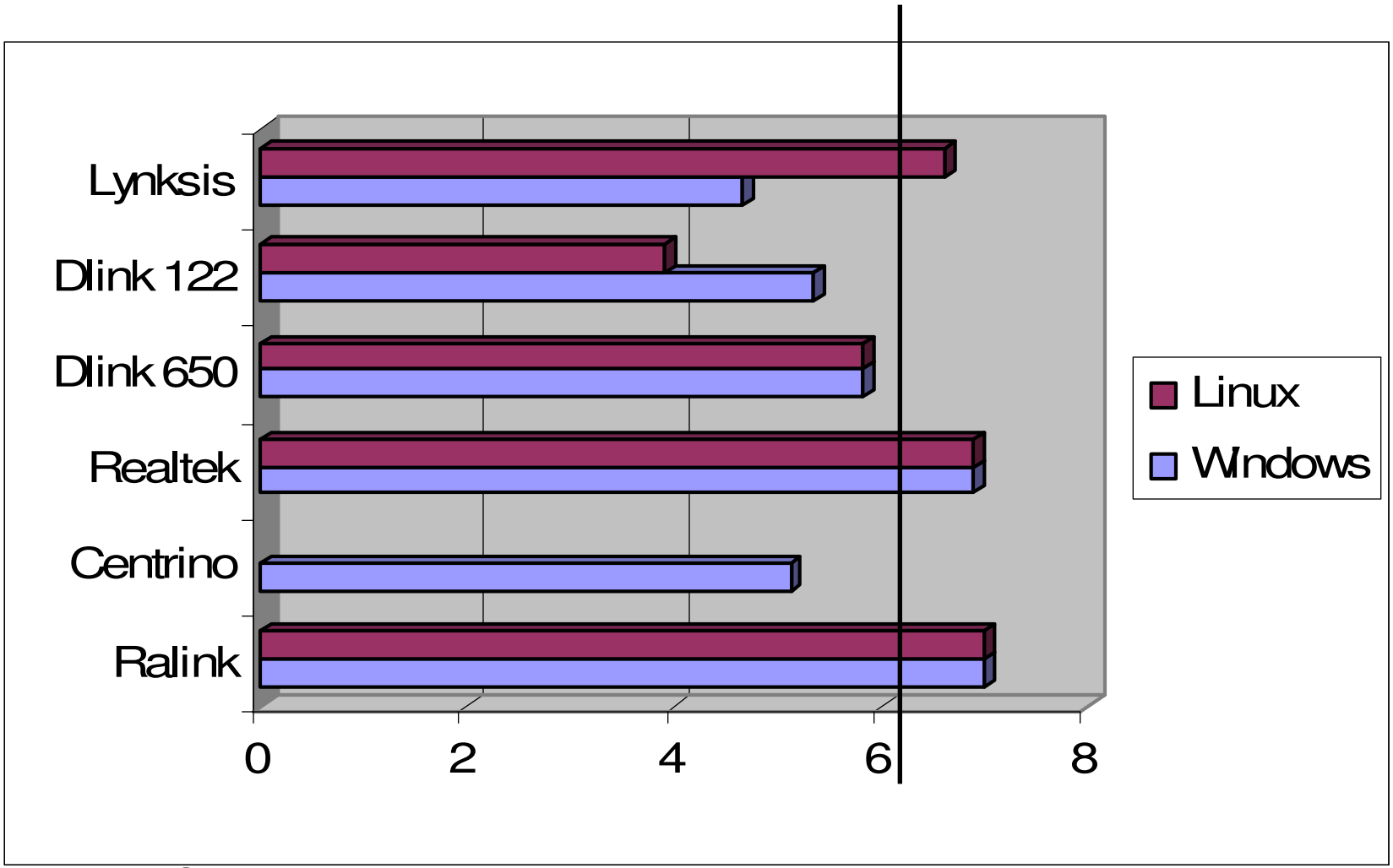






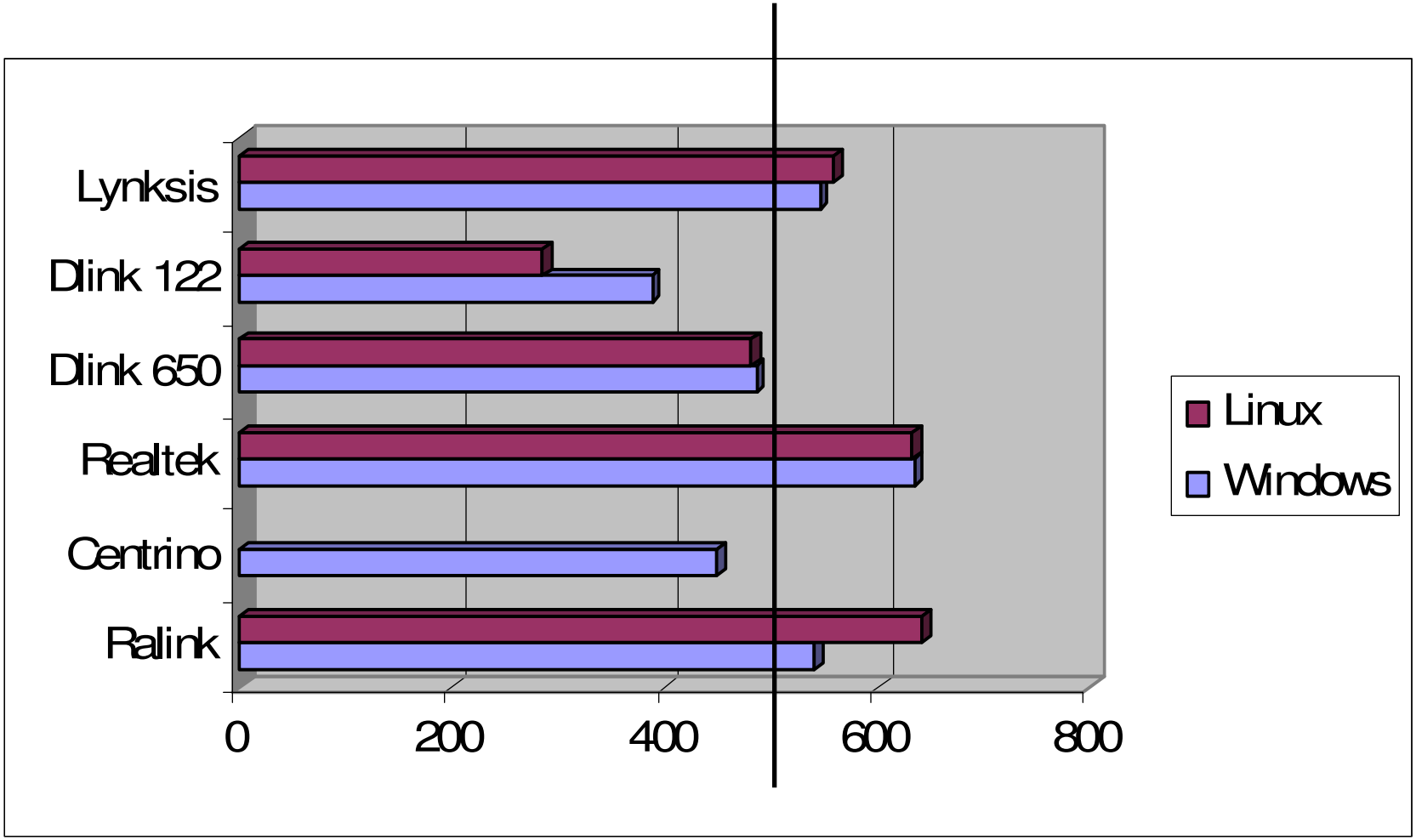
Max Throughput Spread (1)

(Payload =1470 byte, Thr expected = 6.1Mbps)



Max Throughput Spread (2)

(Payload =80 byte, Thr expected = 447 kbps)



What conclusion?

- **Are the differences due to the propagation conditions of each station?**
  - ⇨ We repeated our experiments in different laptop positions, in indoor/outdoor, in a semi-anechoic room.
- **Are the differences due to other external (i.e. not related to the card) factors?**
  - ⇨ We used the same laptop in all the experiments; some results do not depend on the OS; but.. who knows??

With user-side analysis it is not possible to distinguish between:

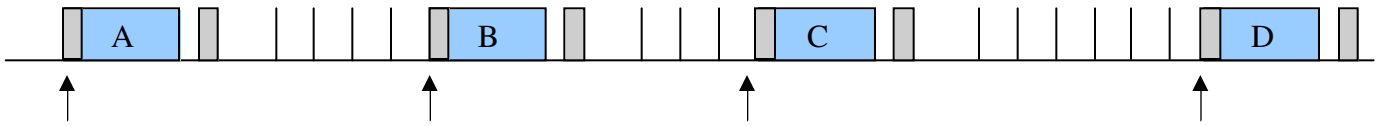
→*not-standard card behavior* (MAC operations)

→*implementation limits* (hardware/firmware, drivers, interfaces).

the actual world:
the radio channel analysis

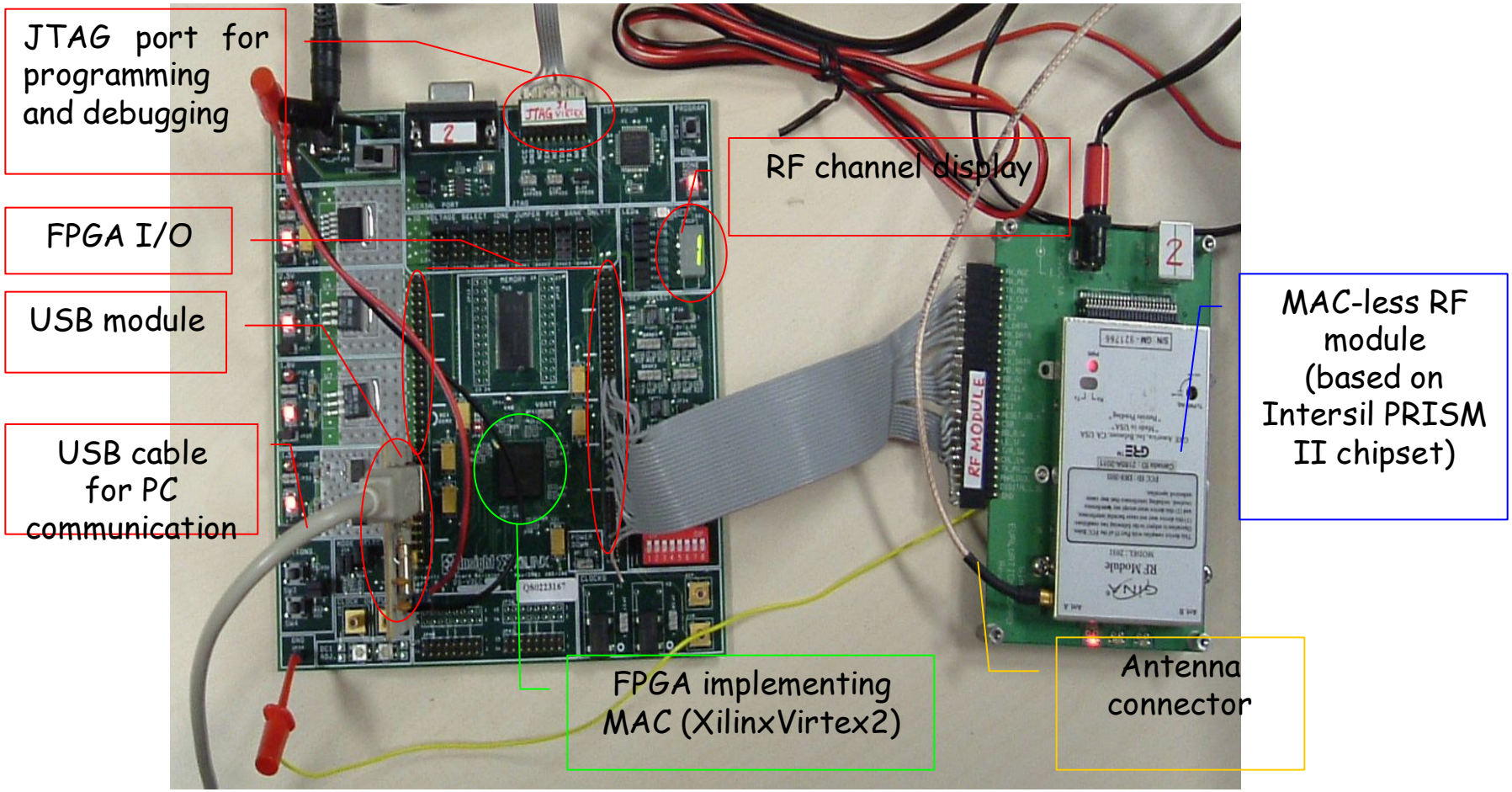
How to look at the channel status?

- **Some drivers allow to read the packet reception times, from which the IFS could be derived..**
  - inaccurate time scale
  - inaccurate estimation of the starting of the reception (the IFS times waste a few tens of usec)

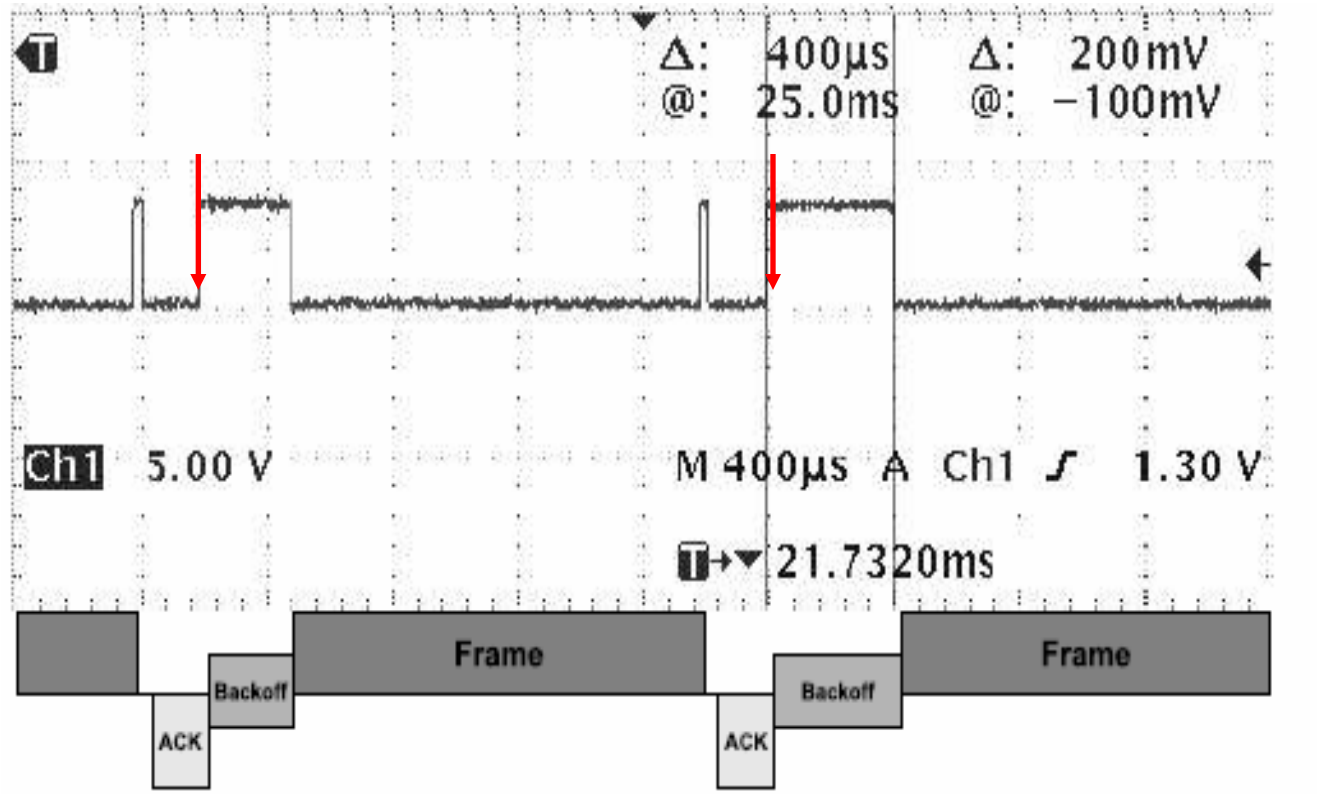


- **We should access the Carrier Sense signal of a monitor card, for recognizing channel activities/inactivities on a digital oscilloscope**
  - **Use of our custom-made card as a channel status reader (but much more!)**

MAC Programmable board: RUNIC



A PHY layer sniffing example

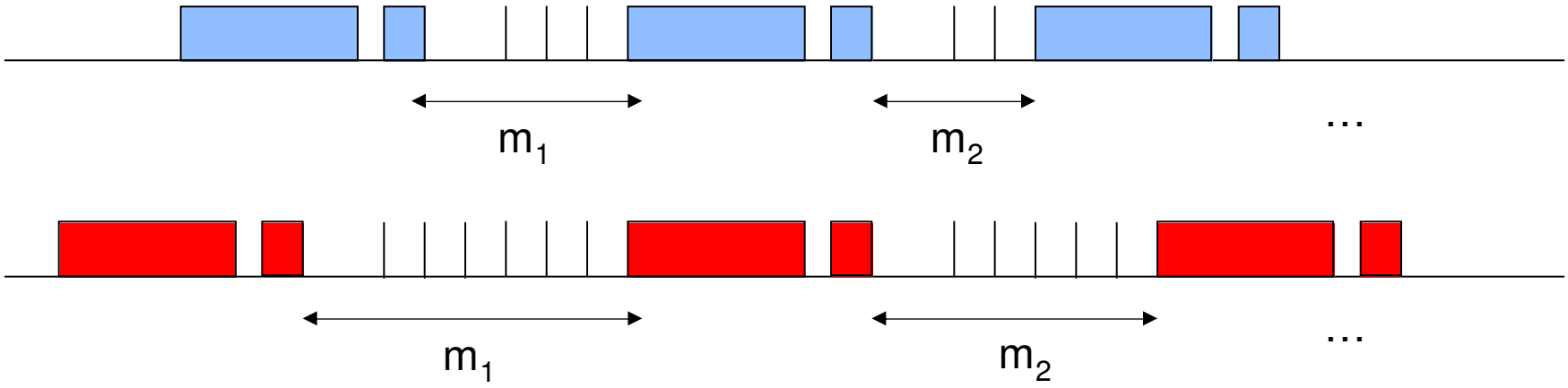


For accuracy purposes, times are read at the busy/idle transition (the idle/busy transition has some random delays)

Channel status analysis

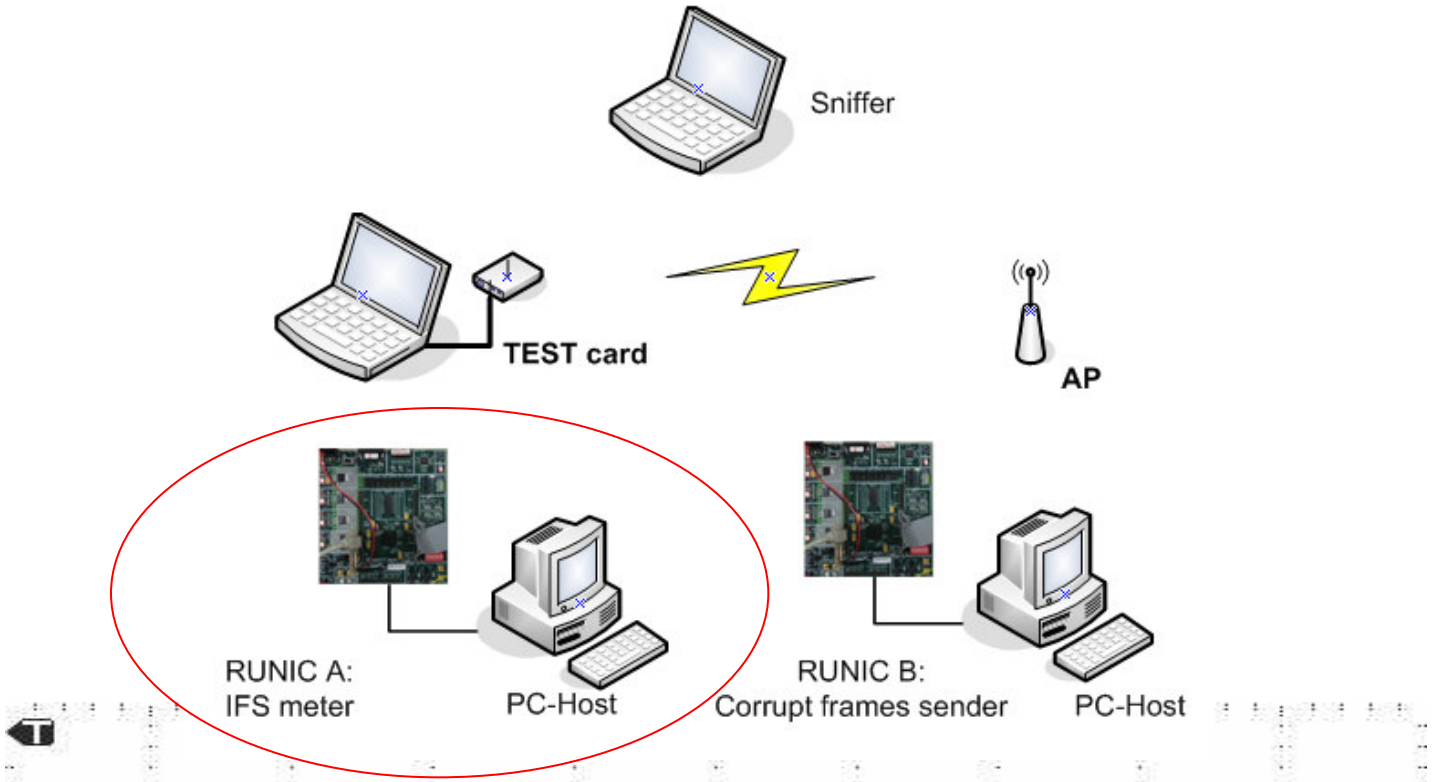
Monitoring of the PHY channel activity when a single test-card transmits continuously

The Inter-Frame-Space statistics allow to indirectly characterize the MAC behavior of the cards



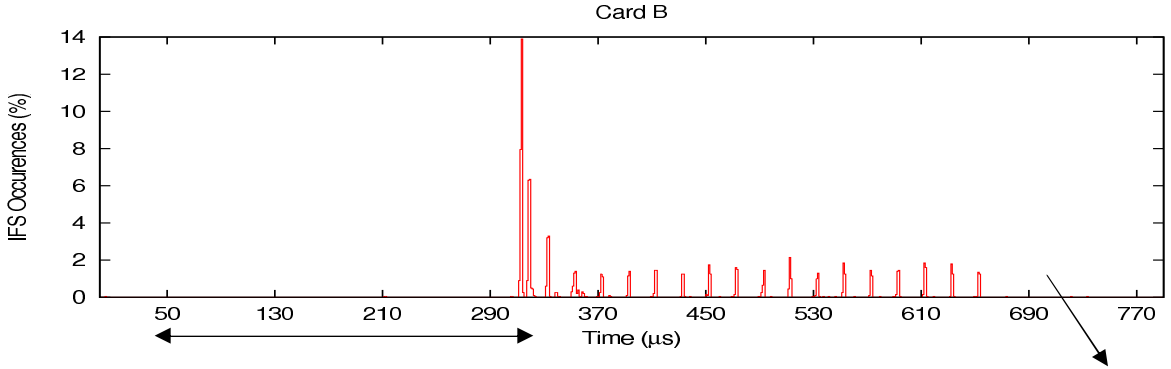
The measures are collected through the carrier-sense signal of our custom-made 802.11 card

Testbed Description



Backoff Analysis

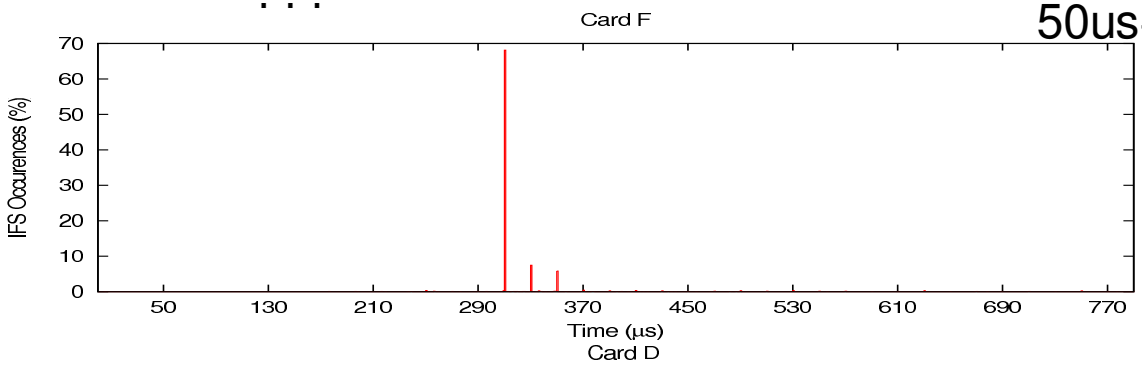
Centrino



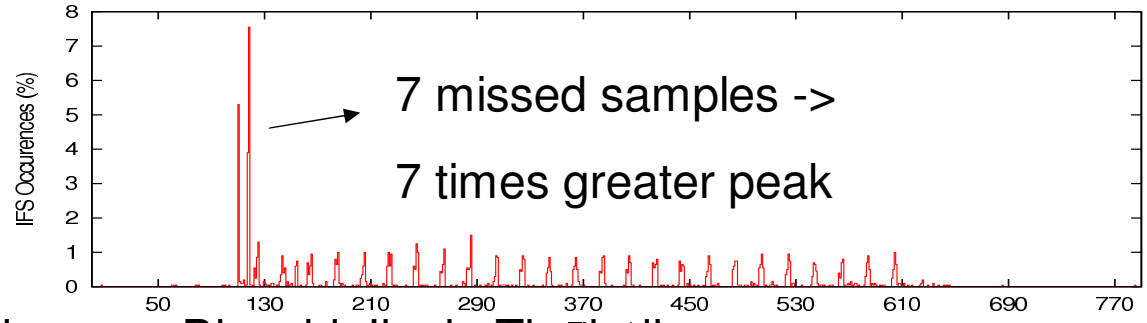
???

50us+20us*31=670us

Cisco



DWL650

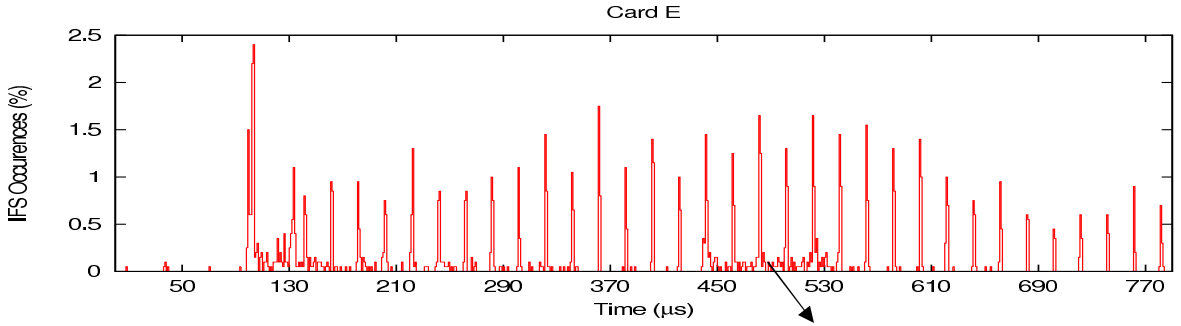


7 missed samples ->

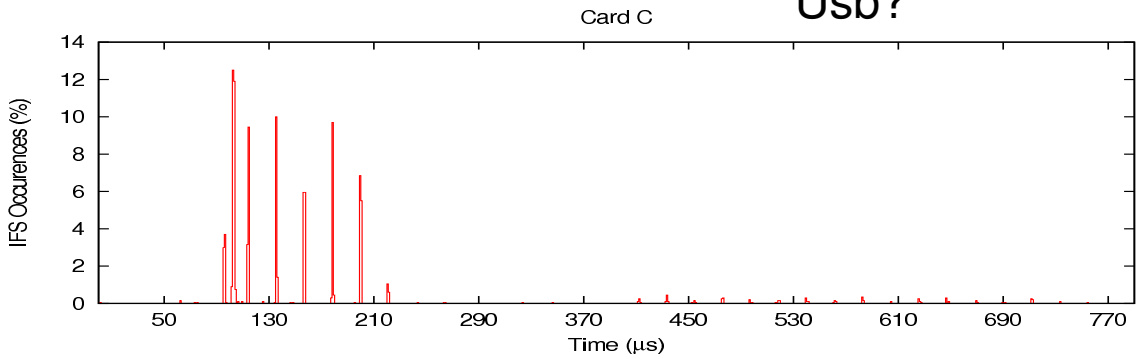
7 times greater peak

Backoff Analysis

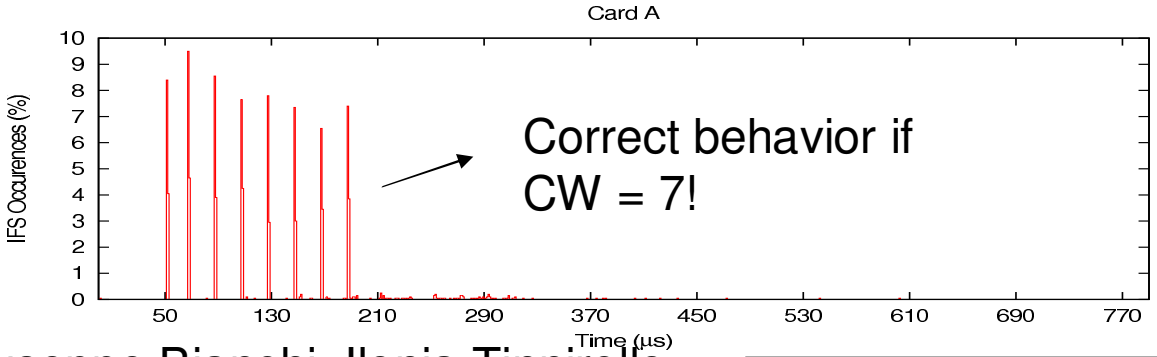
DWL122



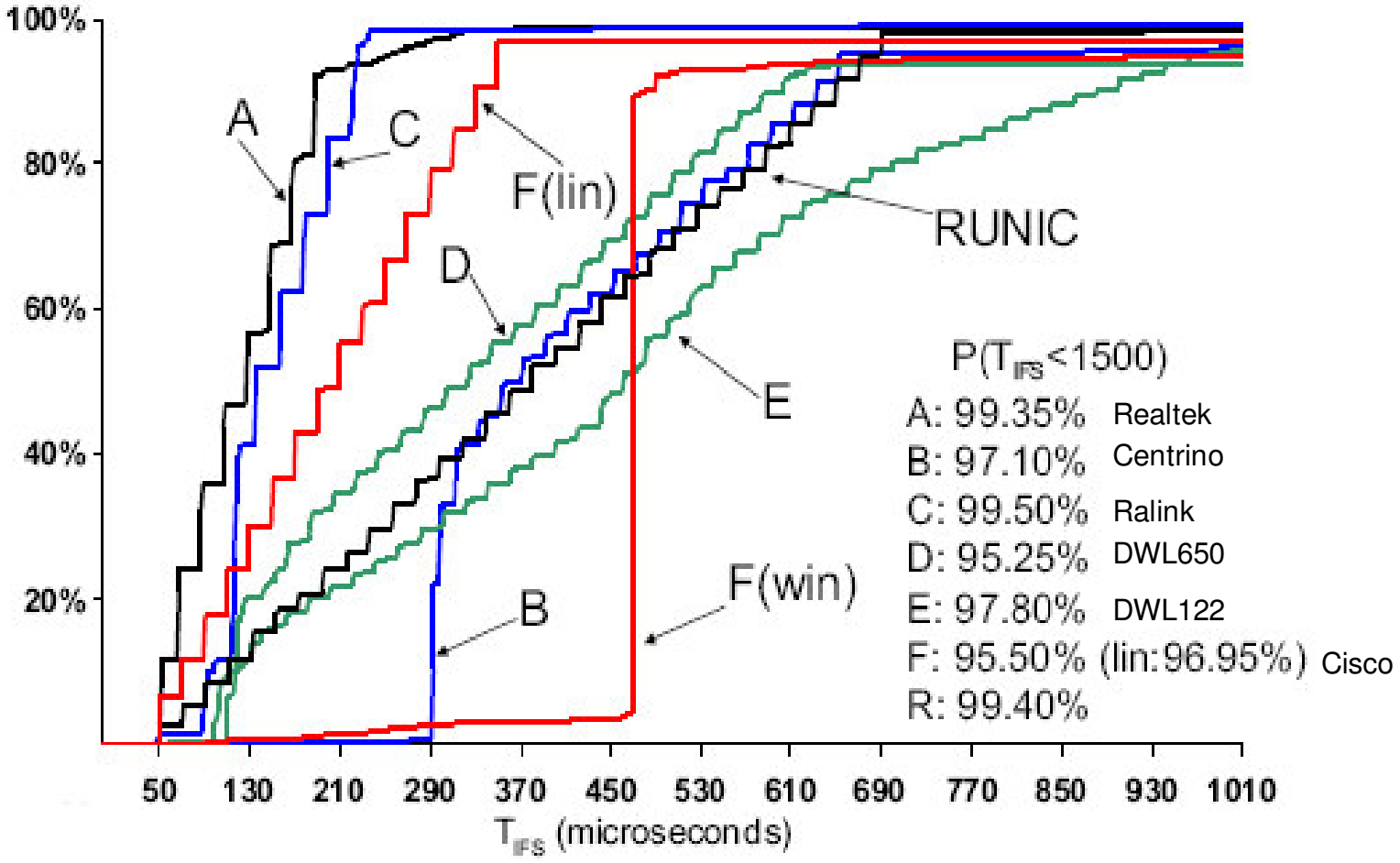
Ralink



Realtek



Backoff Analysis Summary



OS strongly affects the card F performance!

Relaxed Backoff Analysis

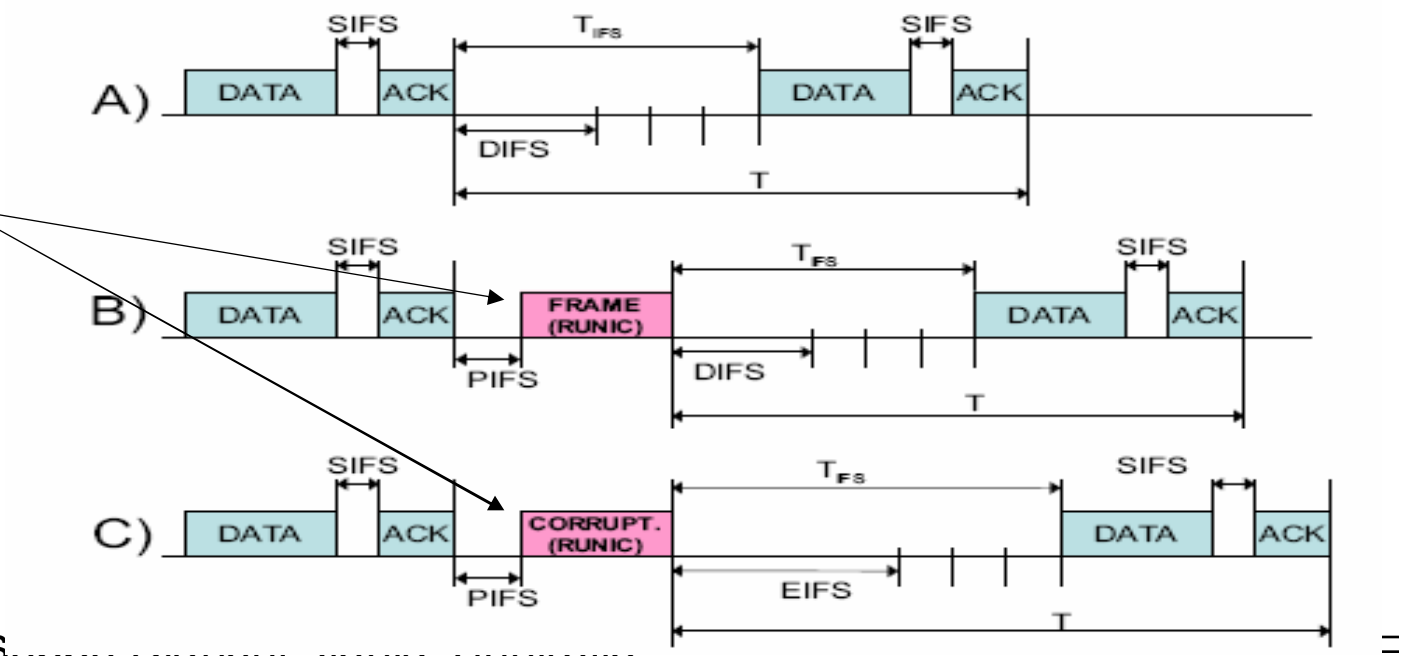
A) *HOL Processing delay*

By delaying artificially the backoff starting of new packets

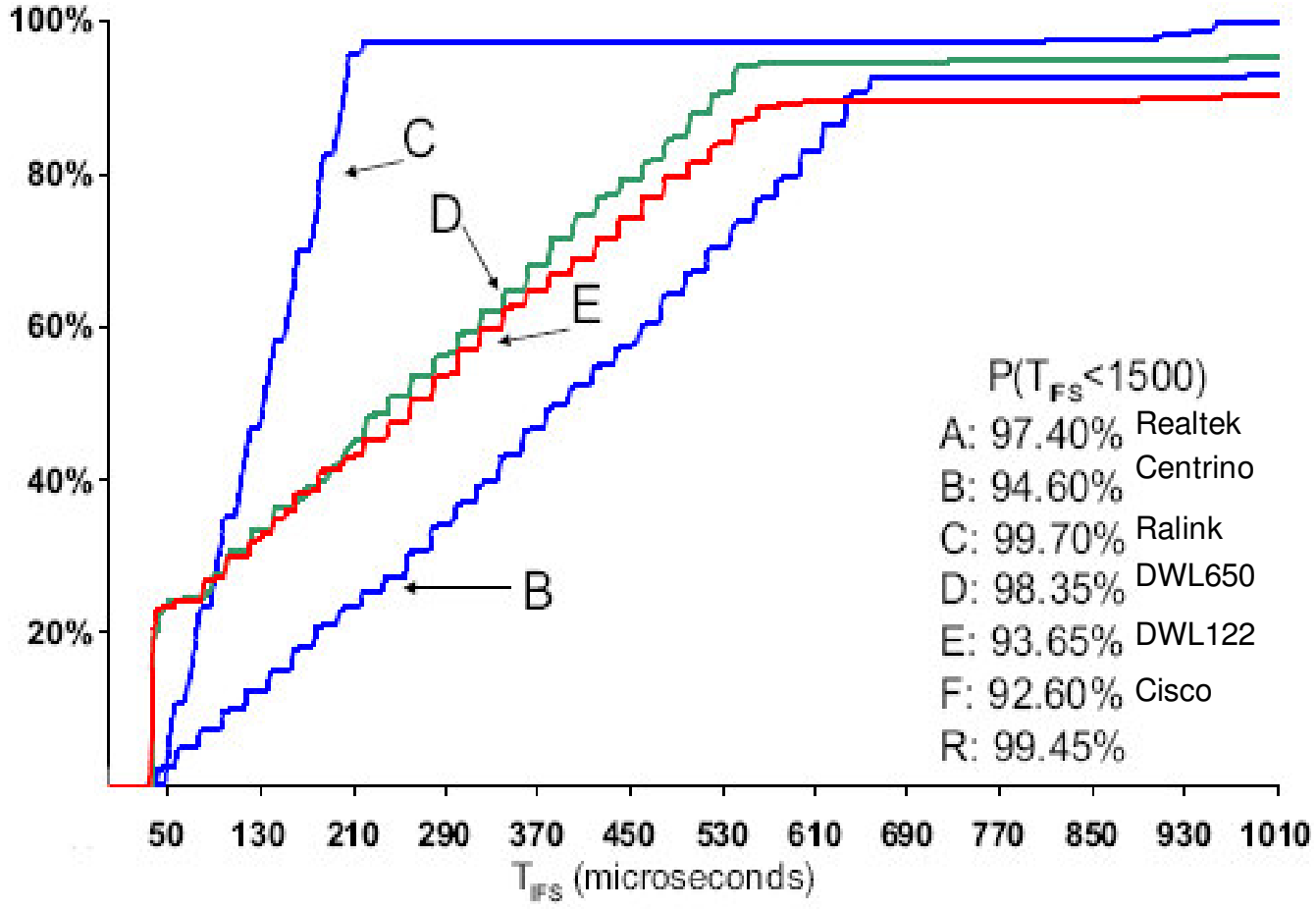
B) EIFS Implementation

By observing inter-frame times which follow the reception of a corrupted frame

Our card as a synchronized channel perturbator



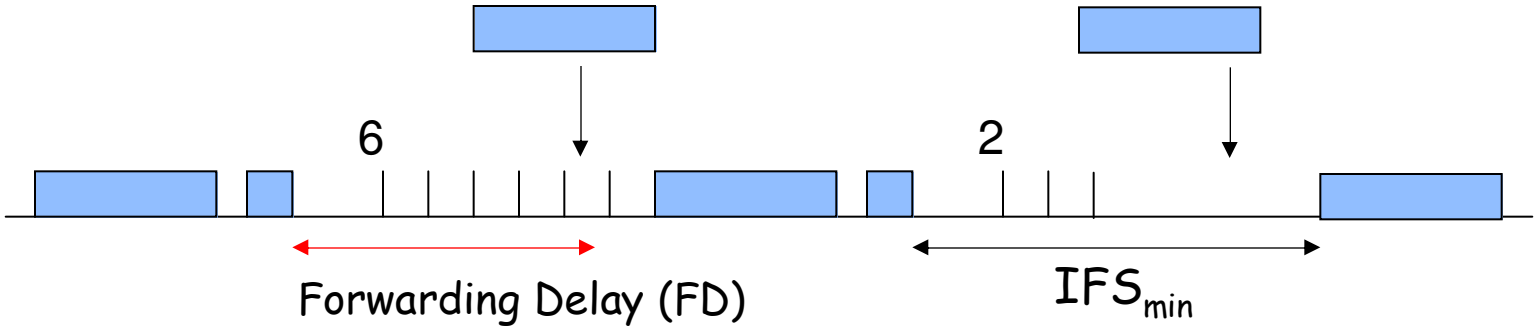
Relaxed Backoff Analysis



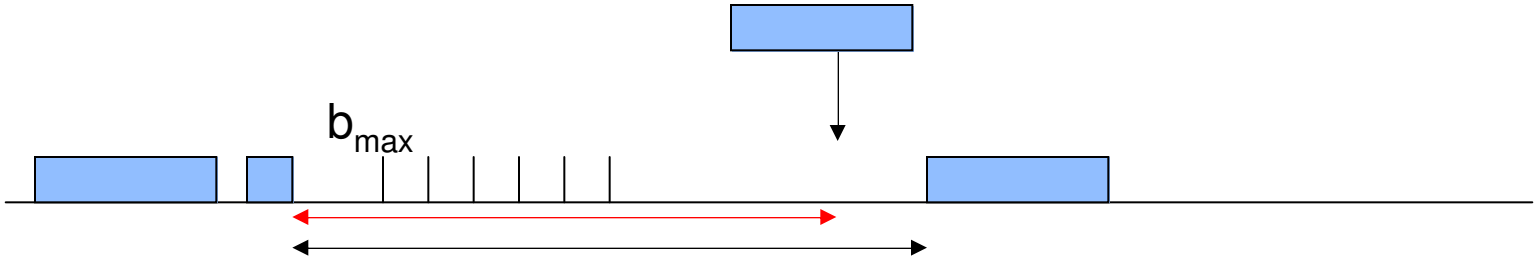
Why some misbehaviors disappear ?

Packet delays and post-backoff

Our hypothesis: whenever the data forwarding to the MAC is managed packet by packet, the stations do not really work in saturation: according to the post-backoff extraction some packets are immediately transmitted



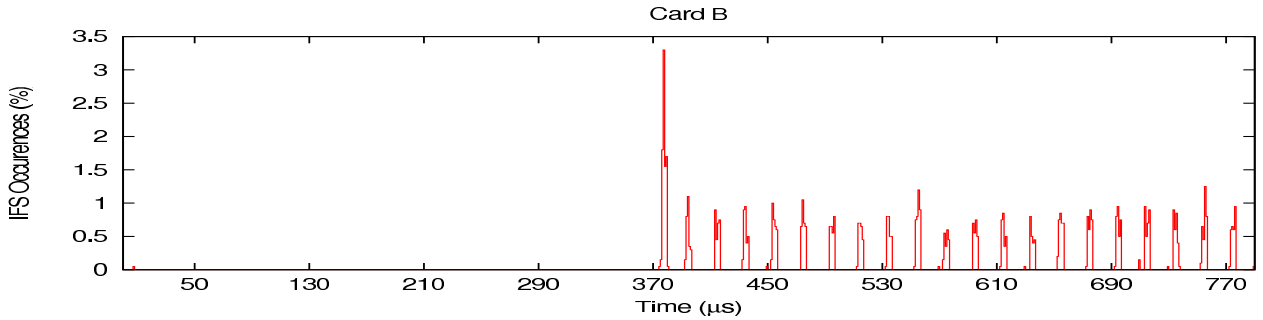
For b=0,1,2,3,4 the IFS is always IFS$_{min}$!



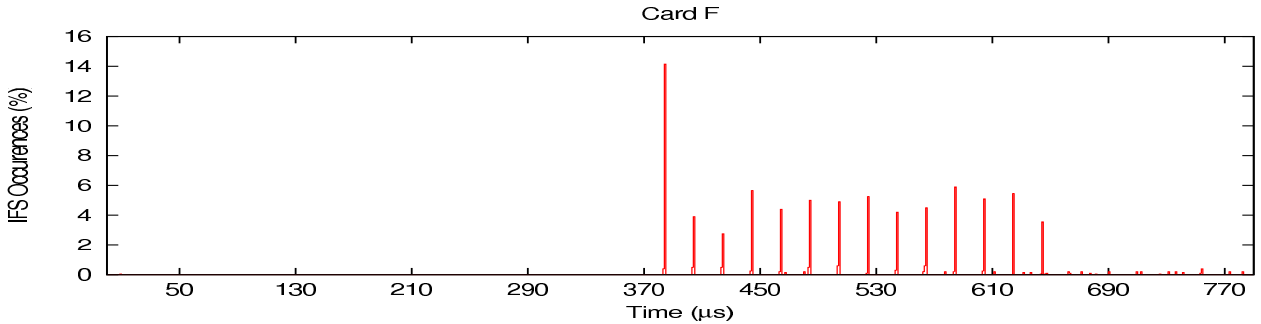
For FD > b$_{max}$, all the IFS are fixed to FD+DIFS

EIFS analysis

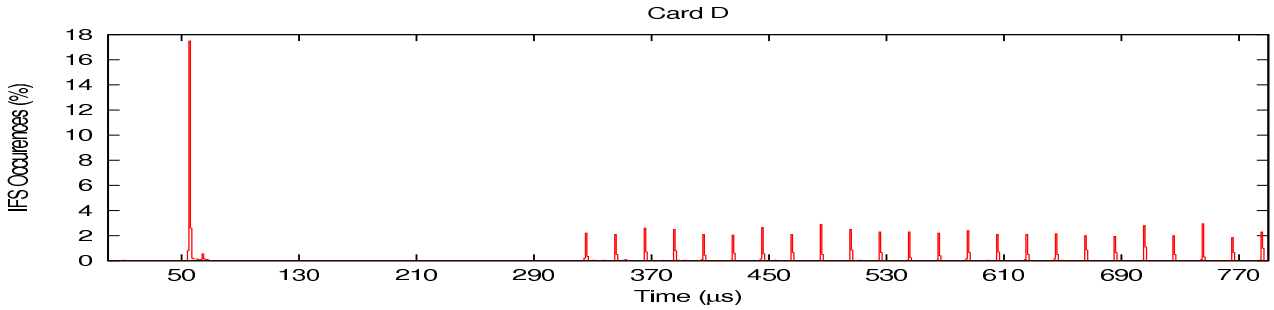
Centrino



Cisco



DWL650

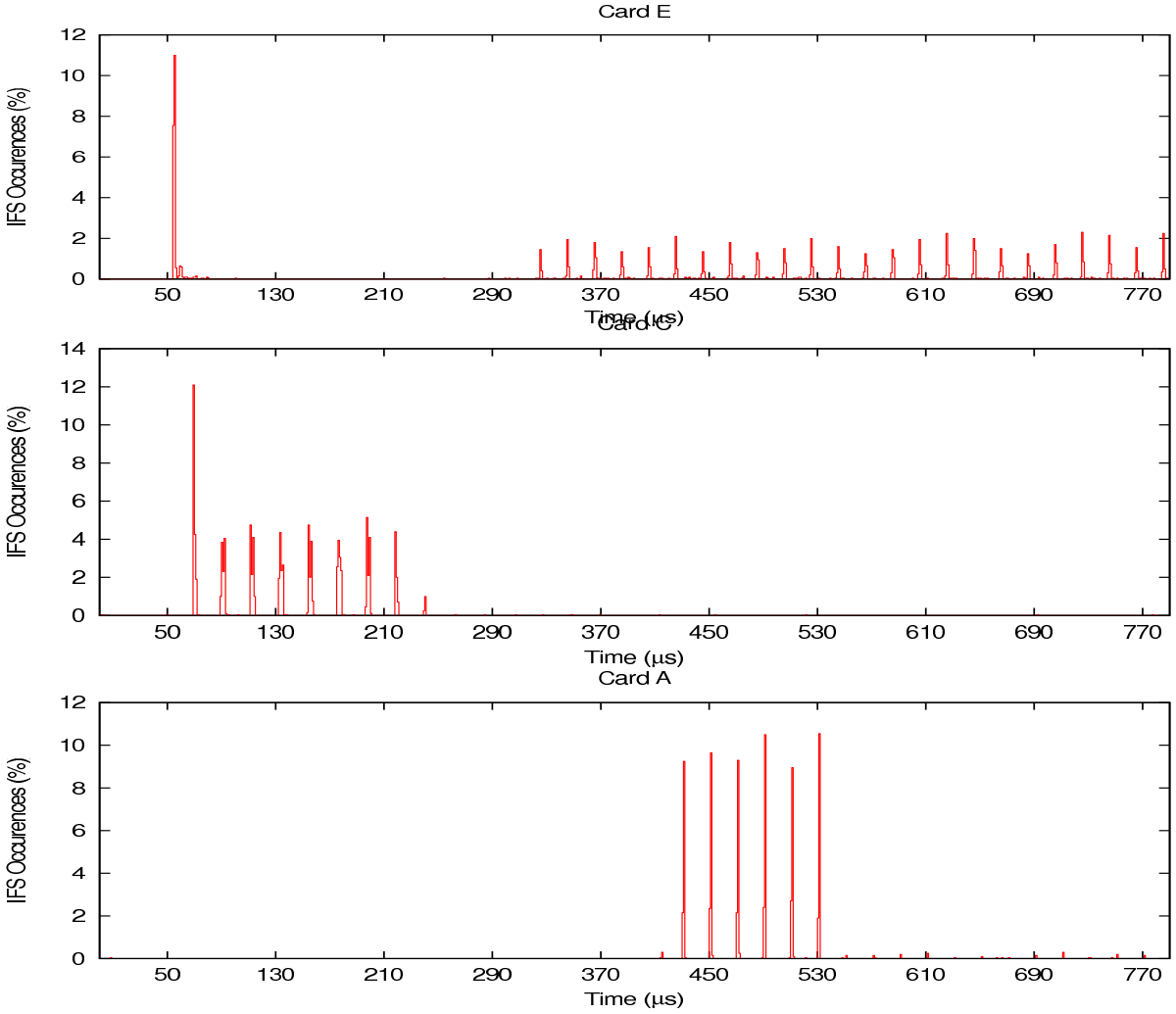


EIFS analysis

DWL122

Ralink

Realtek



Conclusions

- WiFi does not imply standard Fidelity

-Performance unfairness due to different hardware/firmware implementations rather than on measurement conditions

-In such a scenario:

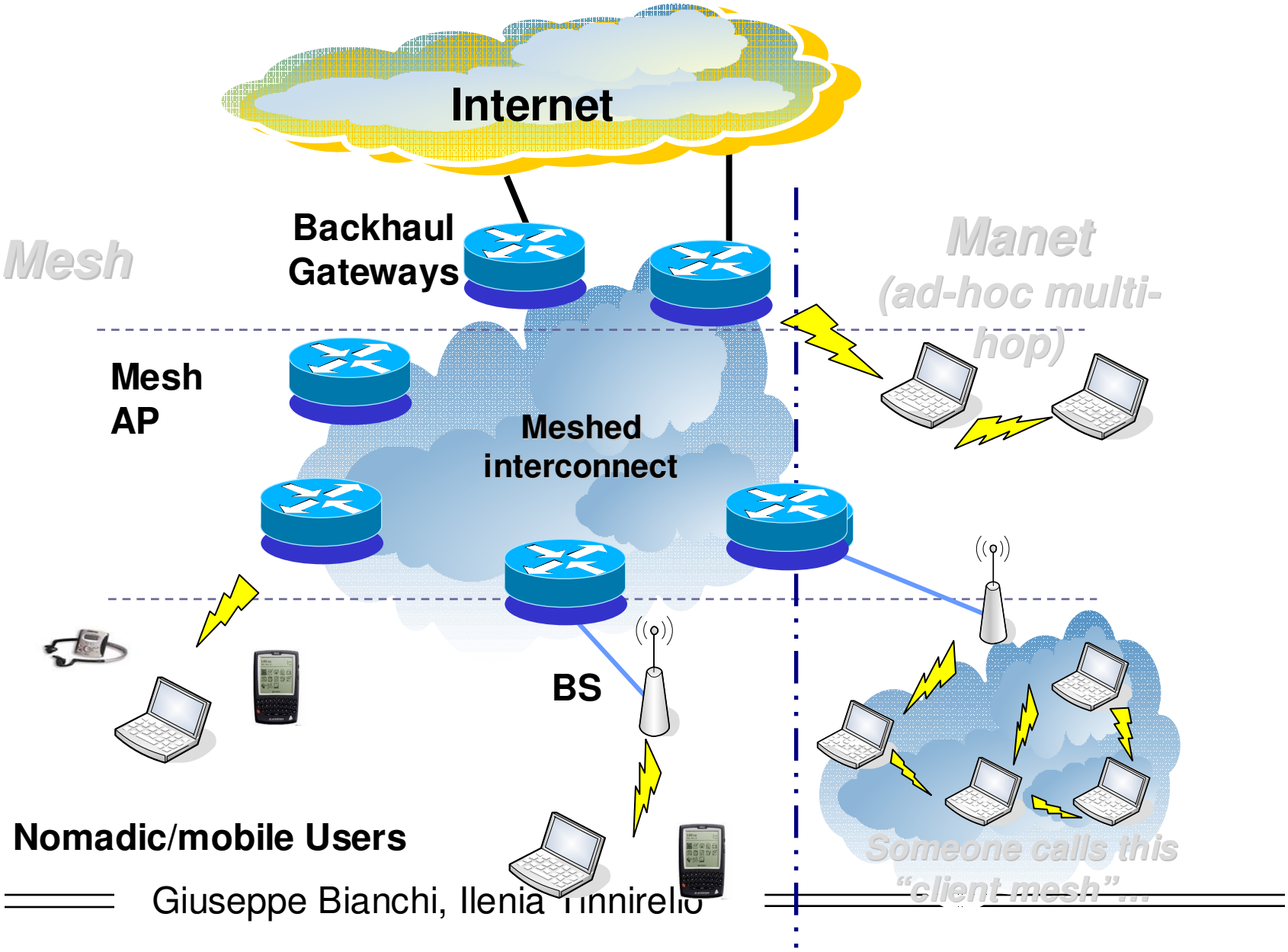
  -how to provide QoS guarantee by means of EDCA??

  -how to define standard-compliancy tests?

Emerging networking scenarios

Giuseppe Bianchi, Ilenia Tinnirello

Emerging Scenario: Wireless Internet?



Birth of Mesh Networks (end of 90')

- **Community-owned Wireless Networks (CWN)**
  - Seattle Wireless; San Francisco Wireless; NYC Wireless
  - … and tons of similar initiatives worldwide

- **CWN motto**
  - NYASPTWYOMB
    - Not Yet Another Service Provider To Whom You Owe Monthly Bill
  - from Seattle Wireless FAQ:
    - **The point of our CWN is to** create a local network infrastructure that replaces the local loop **that is, right now, owned by the telcos and other large corporations. [...]** The network isn't competing with the Internet, it is working in conjunction with the Internet to supplement ways for you to better use connectivity.

CWN deployment

➔ **802.11-based <u>very</u> cheap equipments**

⇨ Antennas, APs, cards

⇨ Often based on own-built antennas

➔ **802.11 for both client access and inter-AP connectivity**

➔ **Open-source routing solutions**

➔ **"How to set-up your own node" – instructions available!**

CWN bias in lessons learned: people involved <u>ARE</u> experts; Management burden (frequency planning, configuration, etc) completely unaccounted by CWN-ers (management and trouble-shooting = …a lot of fun…)

CWN nearer than we think

http://www.ninux.org
http://unituscolo2.servebeer.com

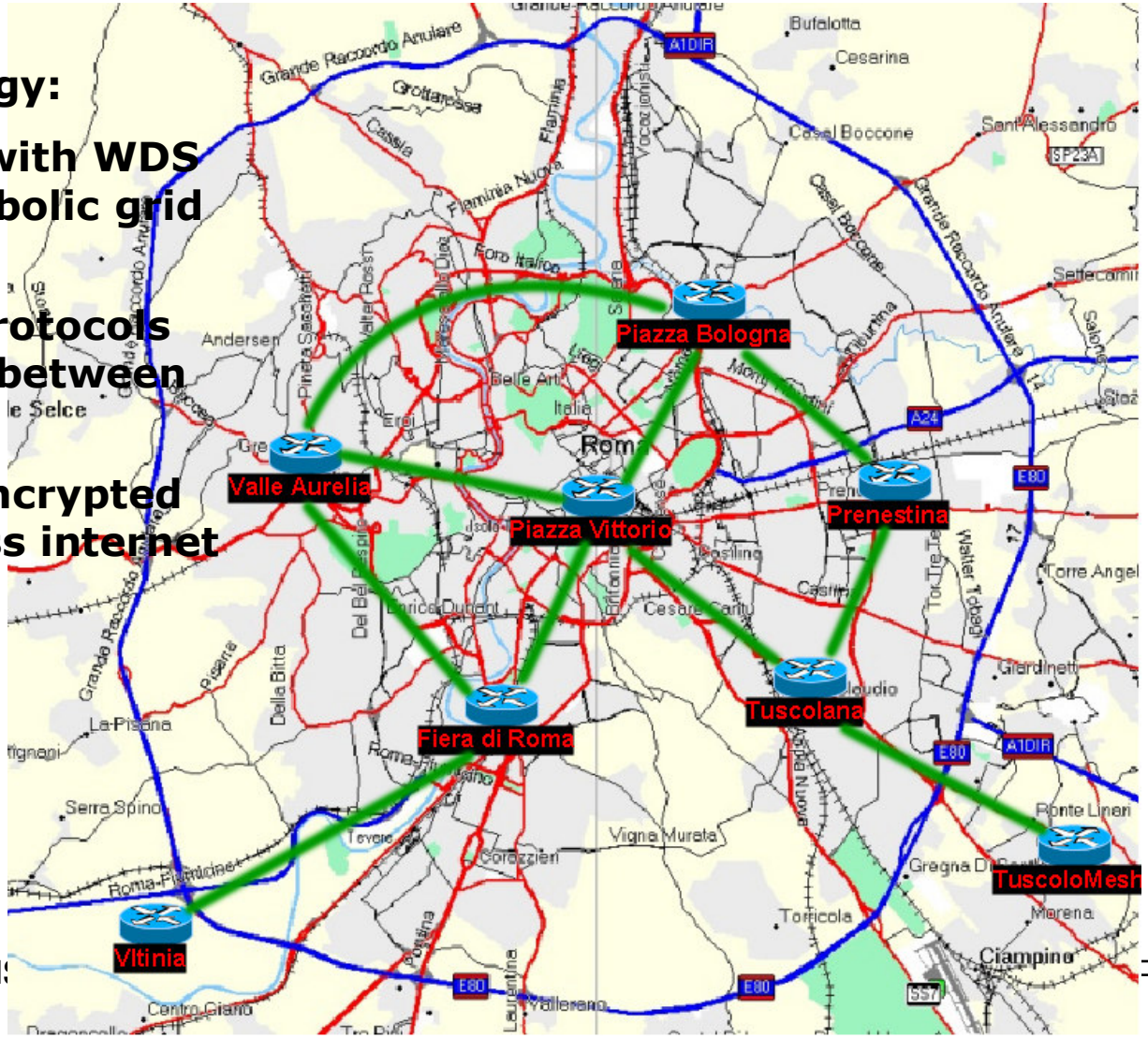
Wireless Community of Rome

Network Topology:

APs connected with WDS links using parabolic grid antennas

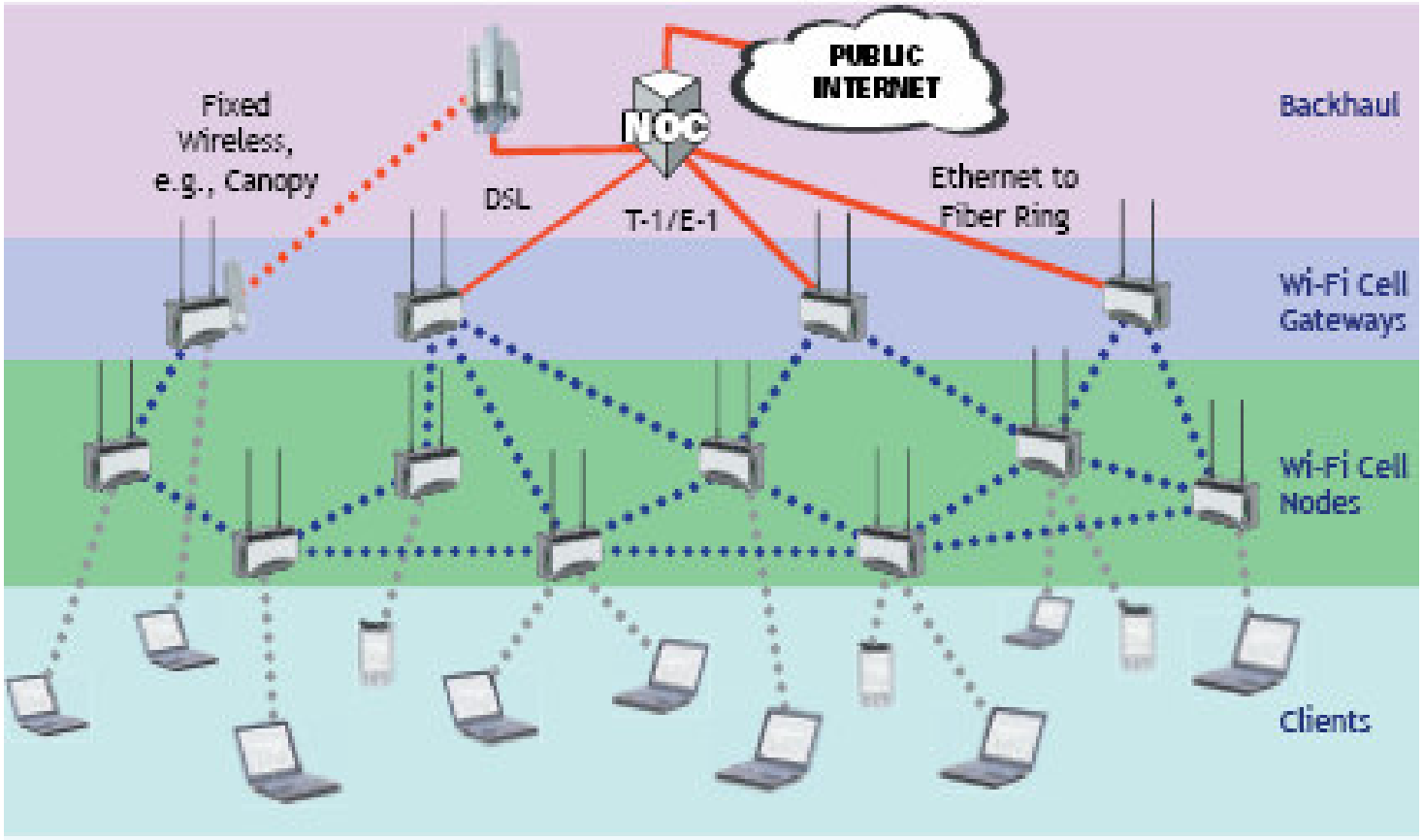
RIP and OSPF protocols exchage routes between APs

Point to point encrypted tunnels to access internet securely



Proprietary mesh: Extended access network

Source: Tropos Networks



Hierarchical structure; wireless backhaul not necessarily 802.11 (e.g. 802.16)

Standardization: 802.11s

➔ **Mesh have been officially recognized as a possible/likely 802.11 extension**

➔ **802.11s PAR (Proposed Authorization Request)**

- ⇨ Draft PAR: September 17, 2003
- ⇨ PAR applications: June 24, 2004
- ⇨ Draft Amendment to STANDARD [FOR] Information Technology-Telecommunications and information exchange between systems-Local and Metropolitan networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: IEEE 802.11 ESS Mesh.

802.11s entering into play

- **QUOTING FROM 802.11S PAR:**
- **802.11s scope:**
  - **To develop an IEEE 802.11 Extended Service Set (ESS) Mesh* with an IEEE 802.11 Wireless Distribution System (WDS)** using the IEEE 802.11 MAC/PHY layers **that supports both broadcast/multicast and unicast delivery over** self-configuring multi-hop topologies**.**
- **802.11s Purpose:**
  - **The IEEE 802.11-1999 (2003 edition) standard provides a four-address frame format for exchanging data packets between APs for the purpose of creating a Wireless Distribution System (WDS), but does not define how to configure or use a WDS. The purpose of the project is to** provide a protocol for auto-configuring paths between APs over self-configuring multi-hop topologies in a WDS **to support both broadcast/multicast and unicast traffic in an ESS Mesh** using the four-address frame format or an extension**.**

Mesh Deployment and Performance

Giuseppe Bianchi, Ilenia Tinnirello

An example of CN: Roofnet

Two approaches to constructing community wireless networks

➔Carefully constructed multi-hop network with nodes in chosen locations + directional antennas for high-quality radio links

➔"Hot-spot"access points to which clients directly connect

- ⇨Do not require much coordination
- ⇨But, not much coverage per wired connection as multi-hop networks

ROOFNET: 37 nodes over 4Km^2

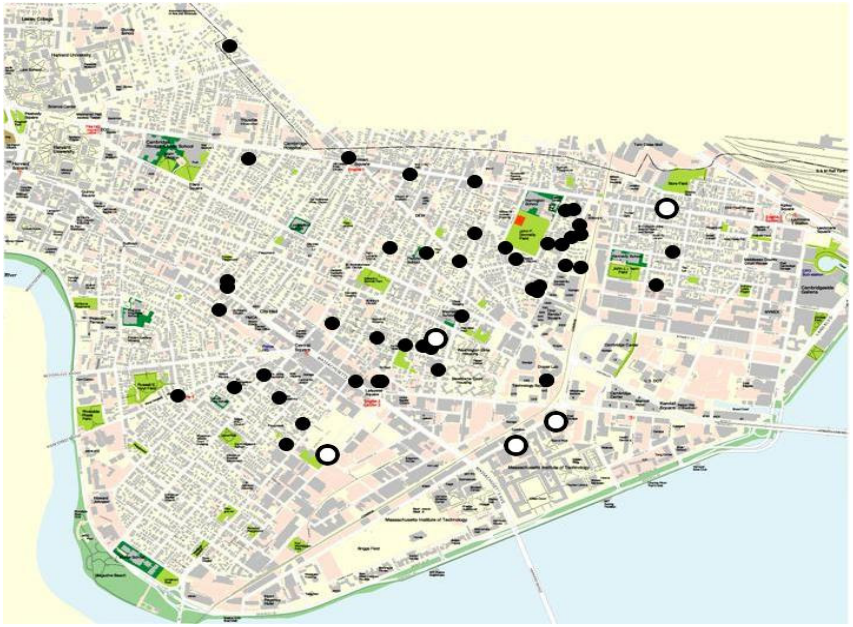
- ⇨Combine the best characteristics of both approaches!
- ⇨Unconstrained node placement (No planning)
- ⇨Omni-directional antennas (No specifically engineered links)
- ⇨Multi-hop routing (Improve coverage/performance)
- ⇨Optimization of routing for throughput in a slowly changing networks (rather than for route repairin a mobile networks)

Roofnet Design

Urban and densely populated area

Mostly 3-or 4-story buildings

Each Roofnet node is hosted by a volunteer user.



Hardware

➔Roofnetnode = PC + 802.11b card + roof-mounted omni-directional antenna

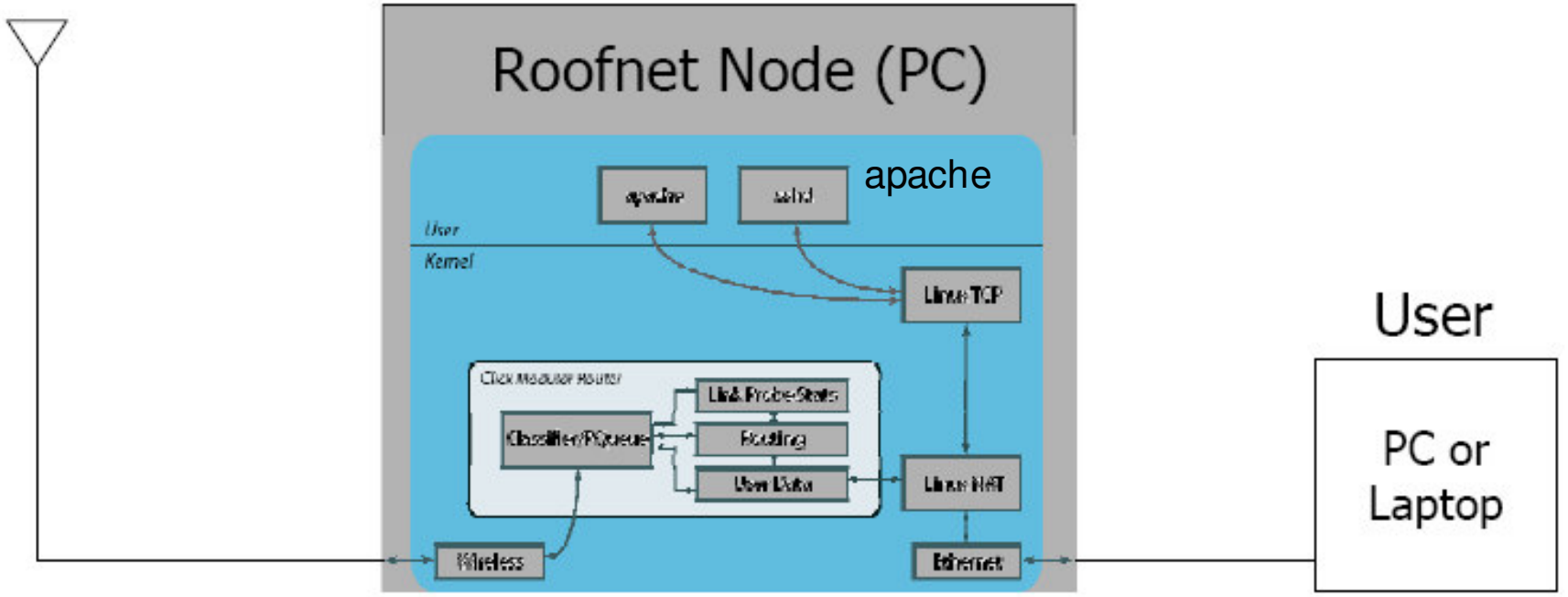
➔The PC's Ethernet port provides Internet service to the user.

➔802.11b wireless card in each node

- ⇨ **Based on the Intersil prism 2.5 chip-set**
- ⇨ **The radios operate with RTS/CTS disabled.**
- ⇨ **All share the same 802.11b channel.**
- ⇨ **Use (Non-standard) pseudo-IBSS mode -> Nodes communicate directly without access points**

Node Software

➔Node software = Linux + Routing S/W + DHCP server



From user's perspective, the node acts like a cable/DSL modem.

Autoconfiguration: Addressing

➔Roofnet carries IP packets inside its own header format and routing protocol.

➔Each Roofnet node has an unique (internal) IP address of the form 10.x.x.x. (meaningful only inside Roofnet)

➔The Roofnet S/W assigns itself addresses automatically, without requiring explicit configuration.

- ⇨Low 24 bits = low 24 bits of Ethernet address
- ⇨High 8 bits = unused class-A IP address block

➔A Roofnet node allocates IP addresses via DHCP to user hosts attached to the node's Ethernet port.

- ⇨From the reserved 192.168.1.x IP address block
- ⇨Uses NAT between Ethernet and Roofnet
- ⇨[192.168.1.x] --(NAT) --> [10.x.x.x]

Autoconfiguration: Gateway and Internet Access

➔Assumption -A small fraction of Roofnet users share their wired Internet access links.

➔Identifying a Roofnetnode as a gateway

- ⇨On start-up, each Roofnet node checks to see if it can reach the Internet through its Ethernet port.
  - → Succeed -advertise itself to Roofnetas an Internet gateway
  - → Fail -acts as a DHCP server and default router for hosts on its Ethernet
- ⇨Each gateway uses NAT between Roofnet and Internet.

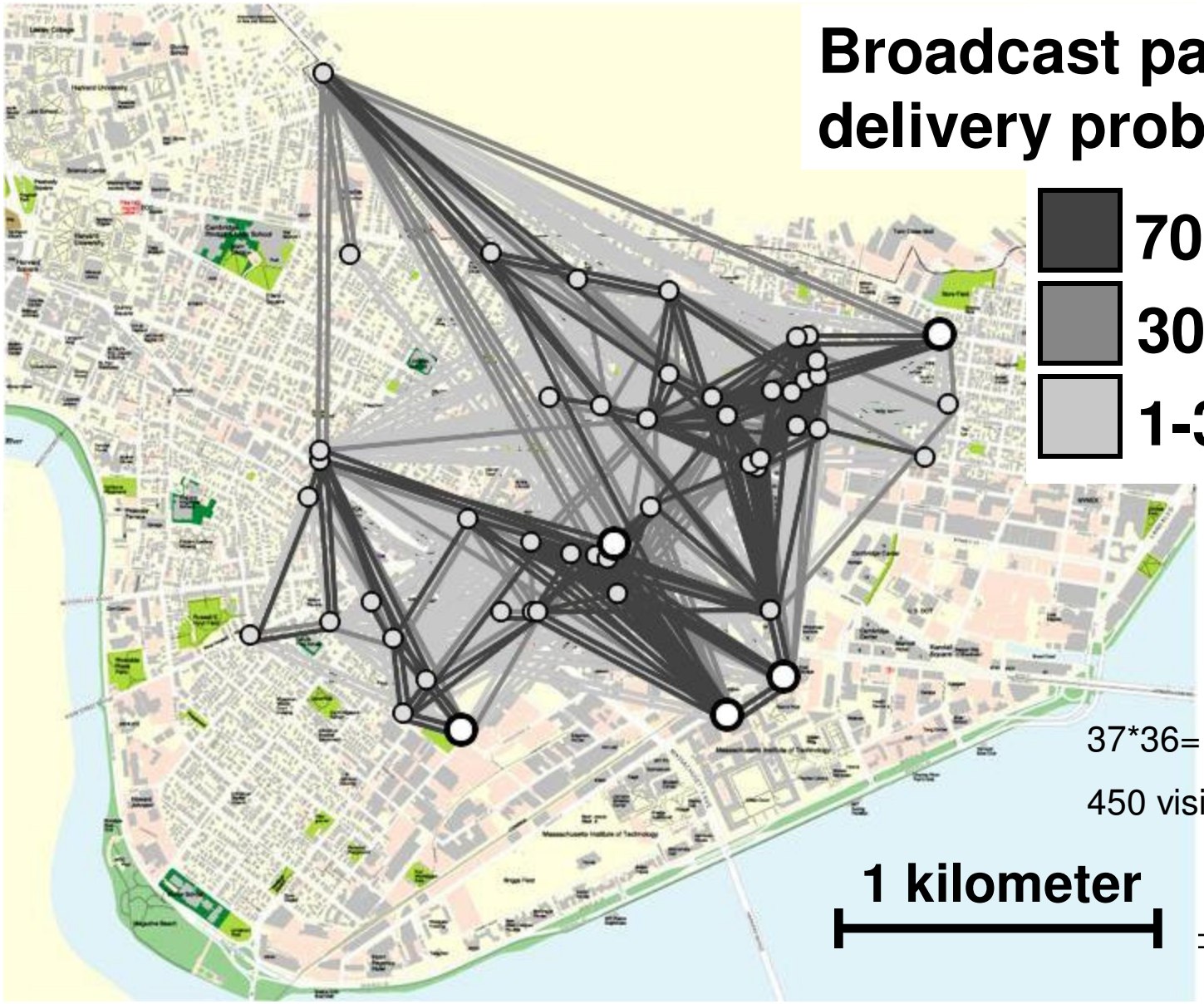
➔When a node sends traffic through Roofnet to the Internet, the node selects the gateway to which it has the best route metric.

➔Roofnet currently has 5 Internet gateways.

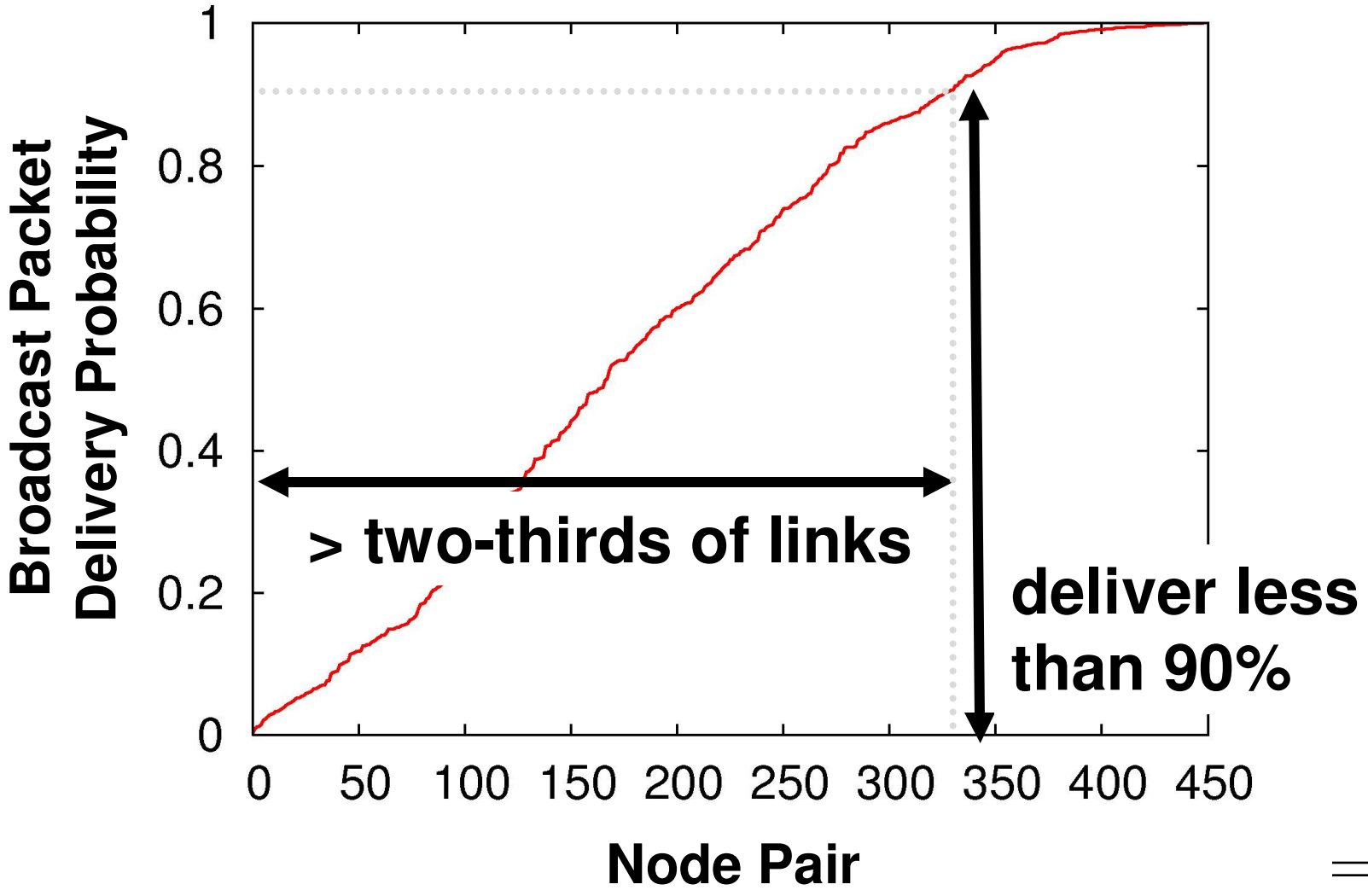
Roofnet Performance

Giuseppe Bianchi, Ilenia Tinnirello

Lossy radio links are common



Delivery probabilities are uniformly distributed



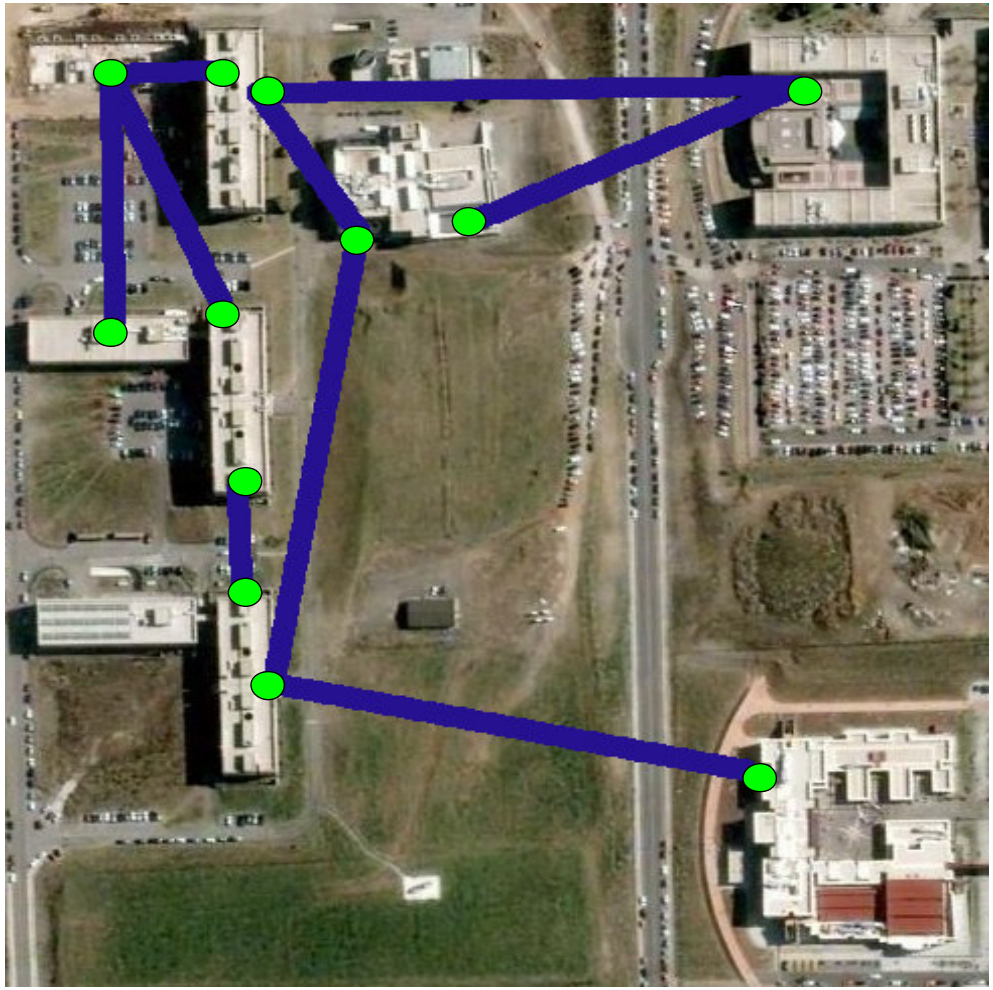
Hypotheses for intermediate delivery rates

1. **Marginal signal-to-noise ratios**
2. **Interference: Long bursts**
3. **Interference: Short bursts (802.11)**
4. ***Multi-path interference***

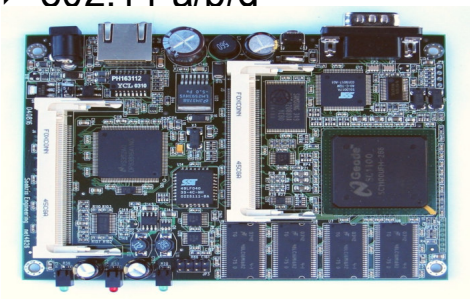
Our Findings

Our Mesh Example

Campus Mesh emulation (Roma TorVergata)

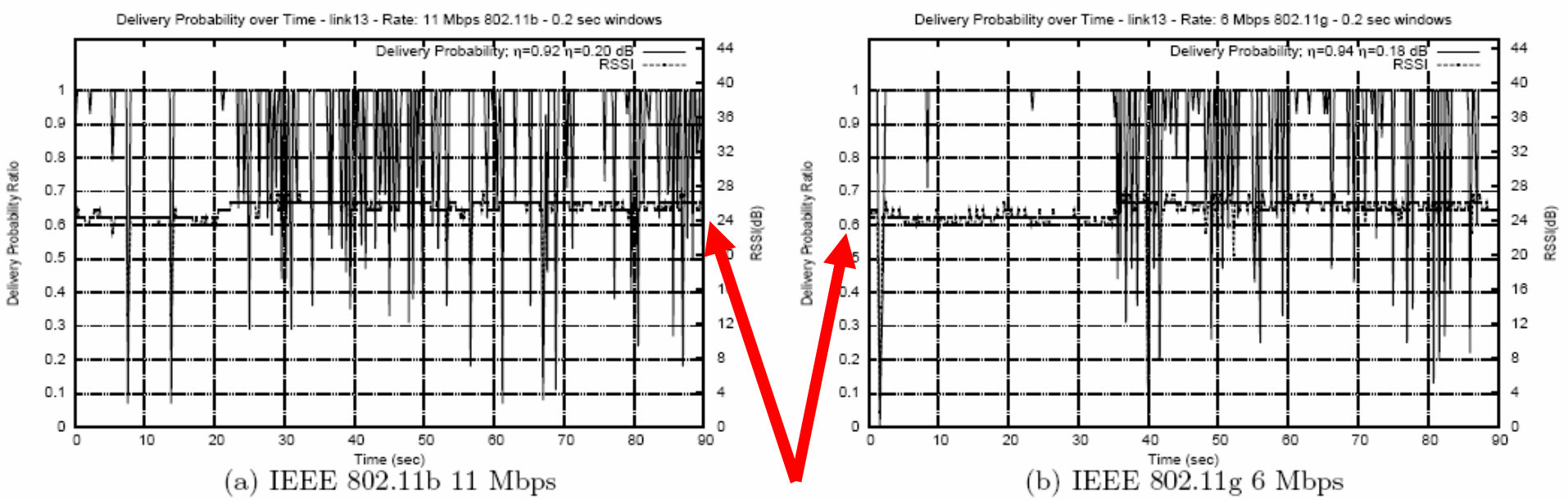


- **9 links**
  - 2x directions
  - Independently tested
- **Phase 1:**
  - PC to PC (manual)
  - 802.11b/g
- **Phase 2:**
  - Soekris (installed)+**Atheros**
  - 802.11 a/b/g



M/B Soekris net4826

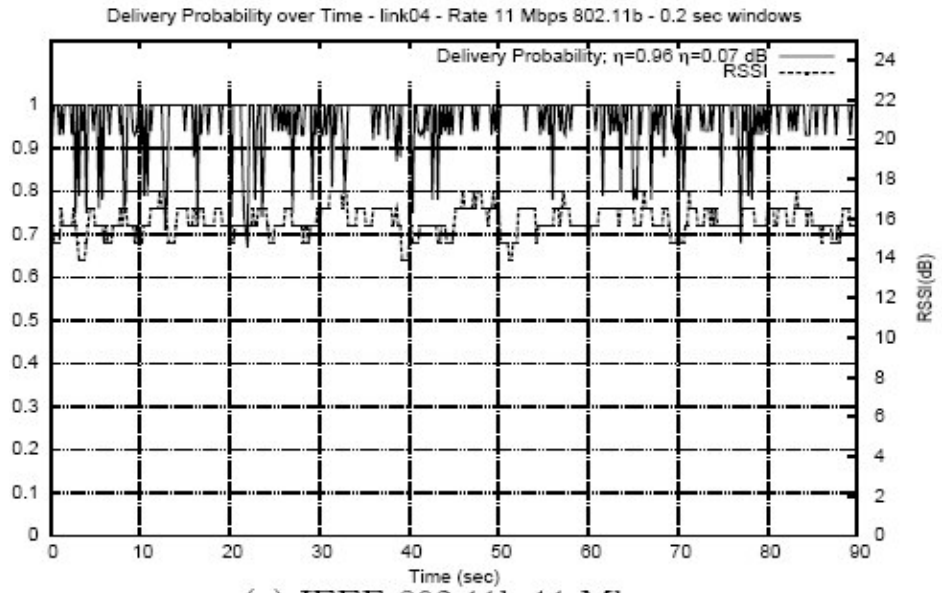
Good link



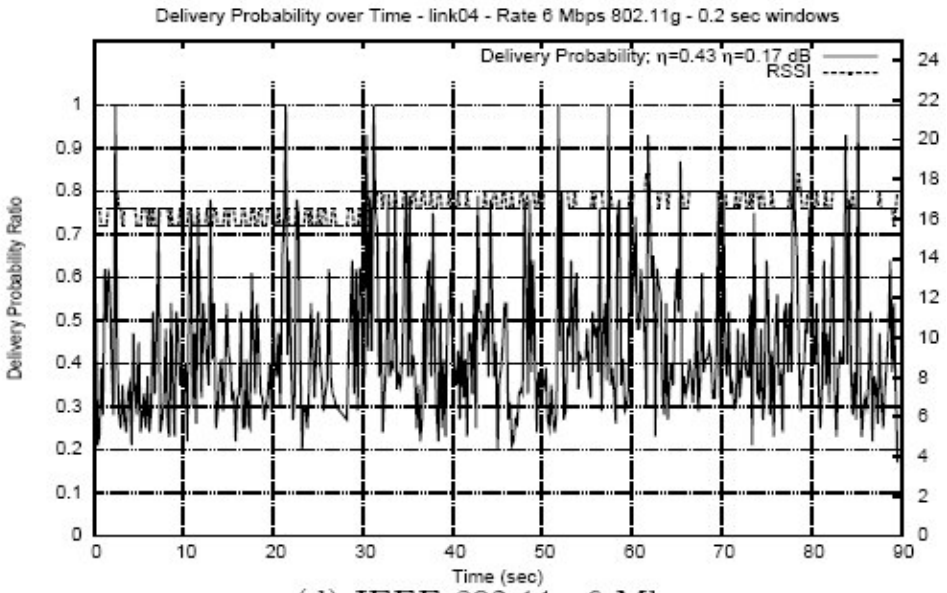
Similar SNR

Similar (high) performance – 92-94% Delivery Probability Ratio
802.11g (lower rate) better than 802.11b (higher rate)

Bad link



(c) IEEE 802.11b 11 Mbps



(d) IEEE 802.11g 6 Mbps

802.11b @ 11 mbps OUTPERFORMS 802.11g @ 6mbps!

Link quality estimation for QoS

➔In emerging multi-cell/mesh network scenarios link quality estimation is becoming very important for route and modulation scheme selection

➔Link quality metrics: usually based on SNR, packet delivery probability, air occupancy times

➔But..

Are measurements available at the *driver level* effective for *link quality* estimation?

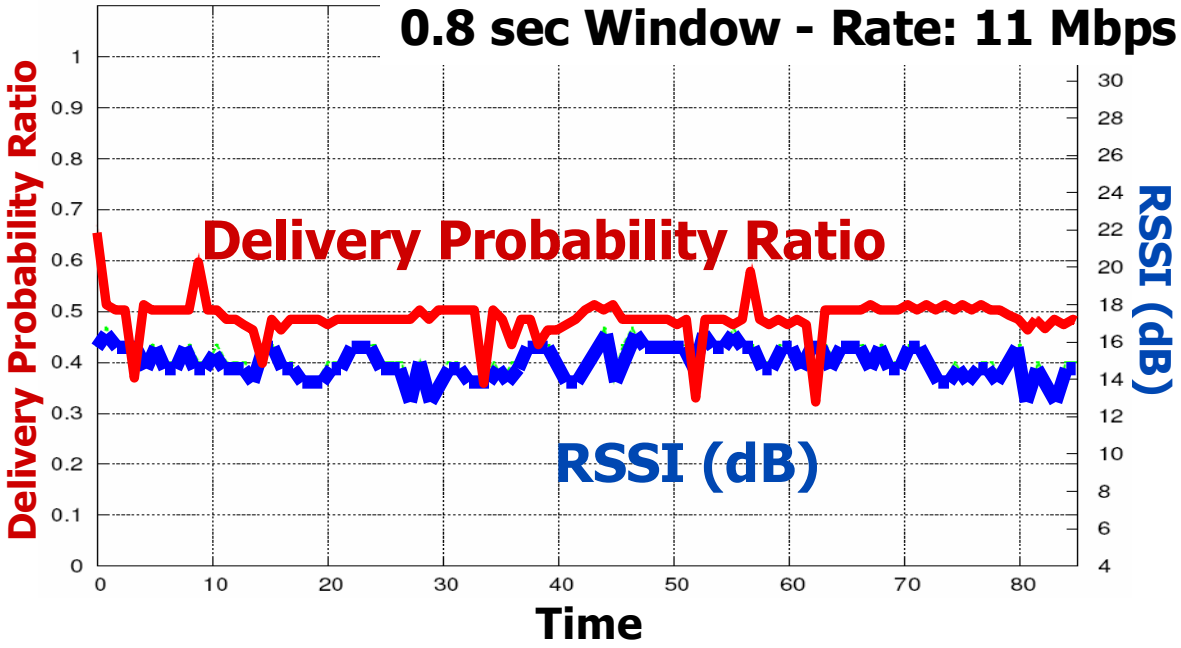
broadcast-based measurements

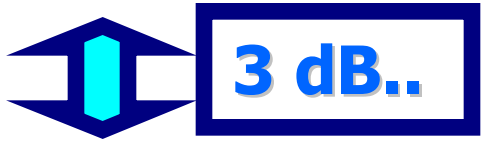
Broadcast-based measurements

- **Widely exploited**
  - link quality probing
  - link cost metric assessment by upper layer routing protocols
  - most Mesh trials and studies rely on broadcast probes

Link testing with broadcast frames

- ➔ **Stable RSSI**
- ➔ **about 50 % of the frames being corrupted**
- ➔ **“intermediate” link quality for most links**
  - ⇨ This is confirmed by several past published works





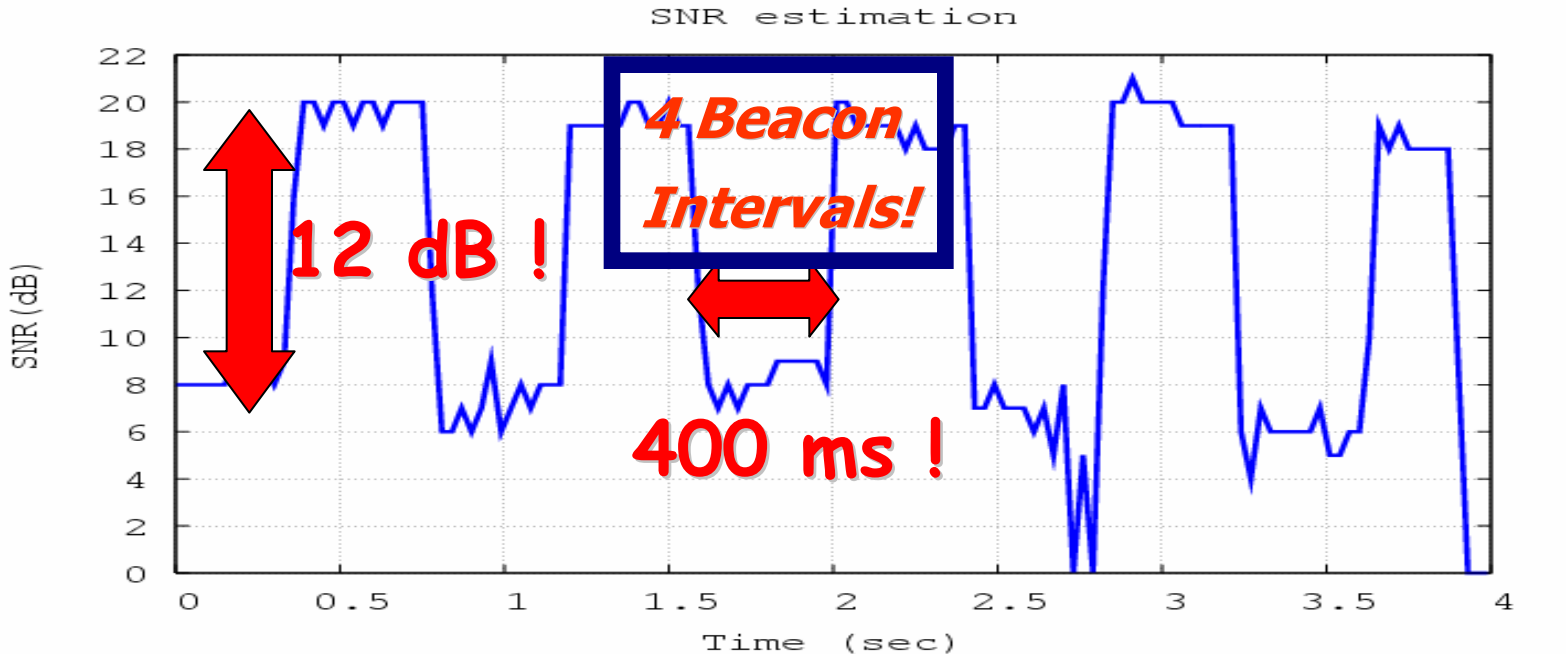
In the absence of further insights, these packet losses might be attributed to bad channel characteristics…

Zooming in

➔ **Window sample changed from** 800 msec **to** 40.96 msec

➔ **Measured RSSI commutates between two 400 ms phases**

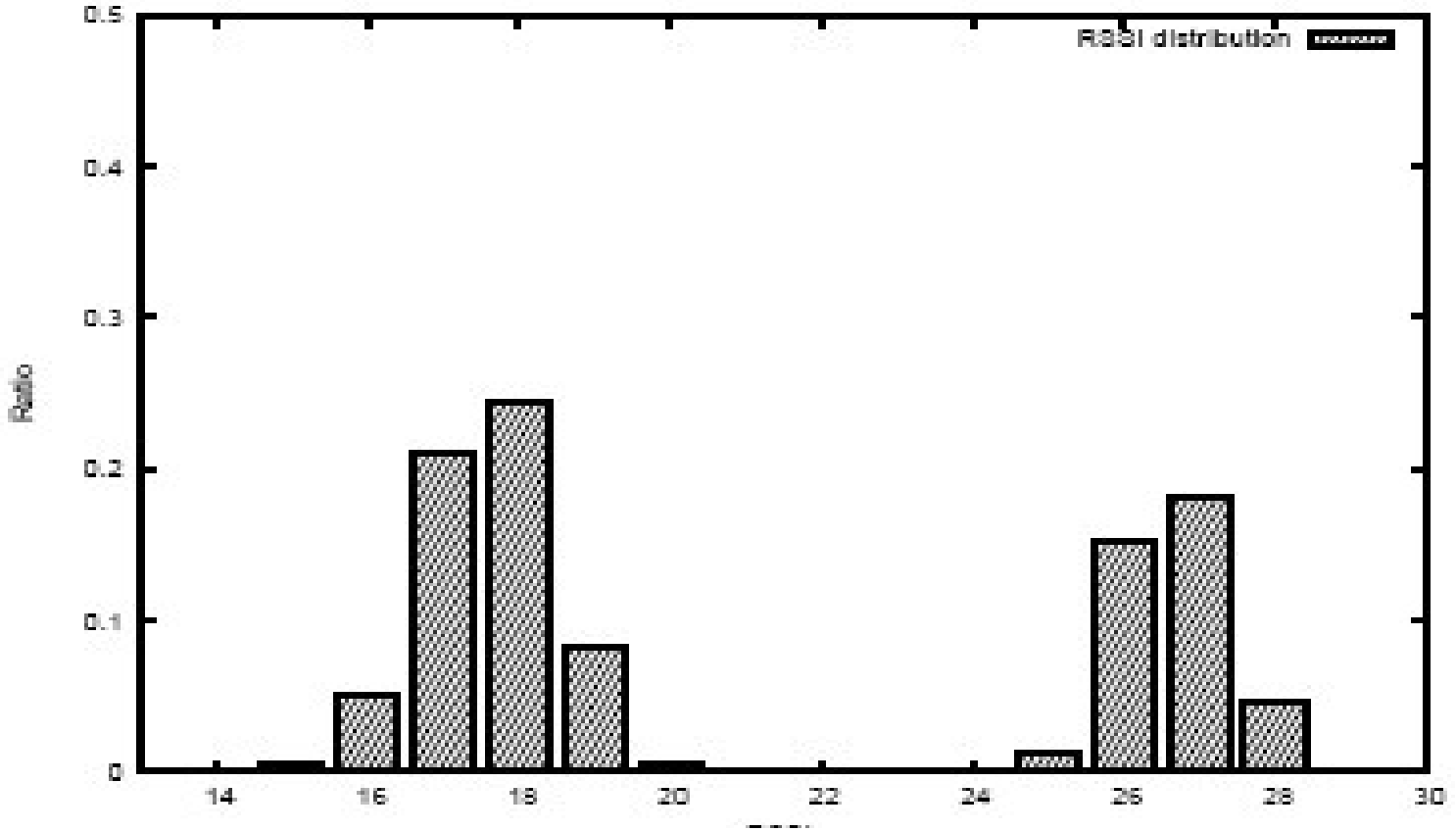
- ⇨ one characterized by a high link quality
- ⇨ the other characterized by a poor link quality and most frames are lost!
- ⇨ 12 dB instead of 3 dB gap!



"intermediate" 50% DPR conditions induced by the RSSI fluctuation

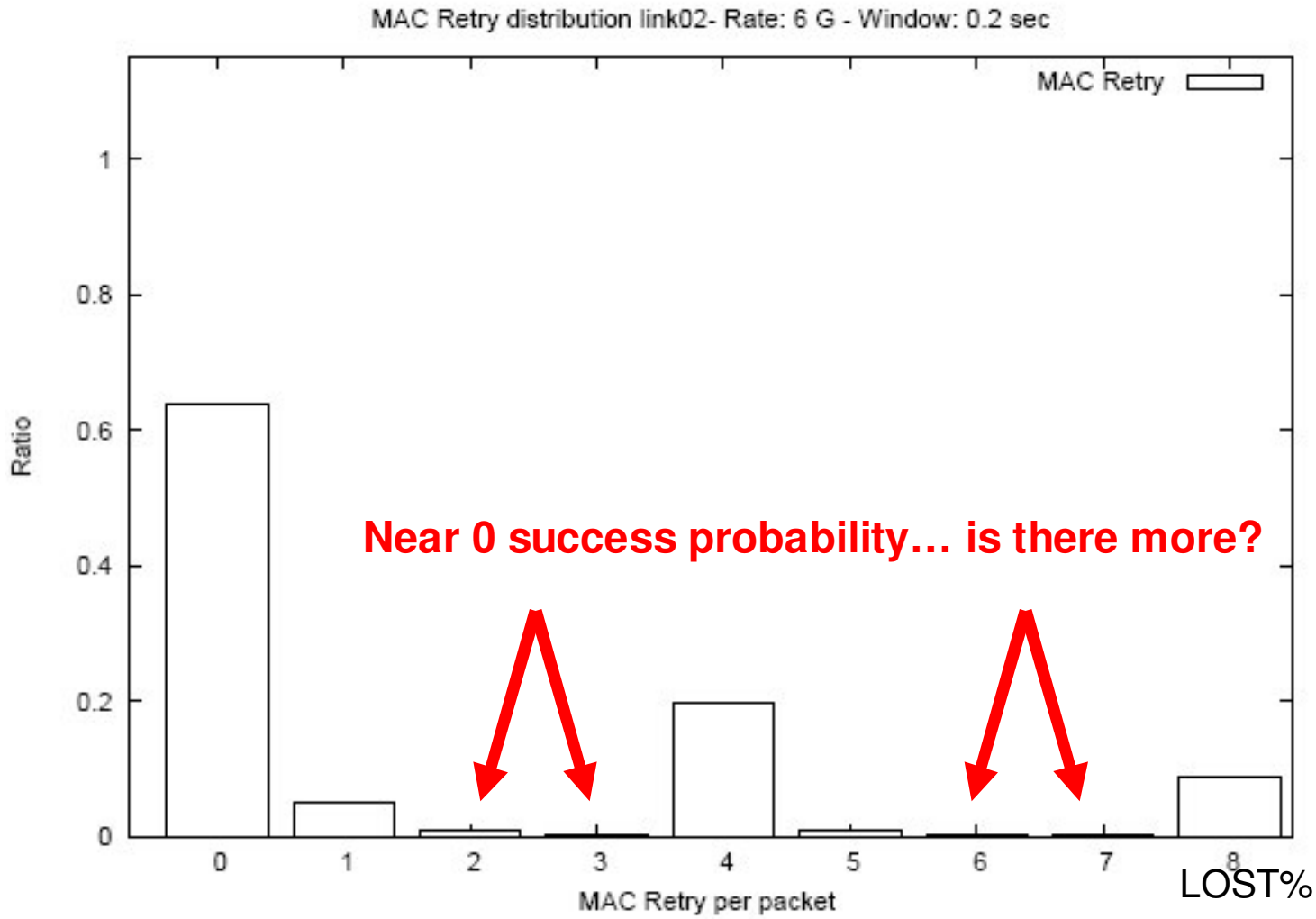
unicast-based measurements

SNR distribution: high/low power levels?



Related retry statistics:

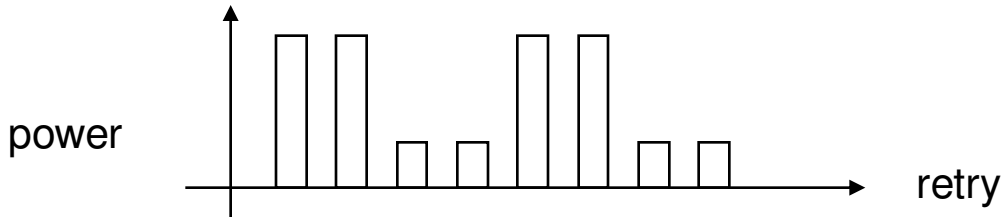
It is more likely to receive a frame with retry 4 than 2?



Atheros unicast RSSI

➔We found that also for unicast data, there is a periodic high/low RSSI sample for frame retransmissions as a function of the retry index

- ⇨ **In bad channel conditions, frames are always lost at the low power level**



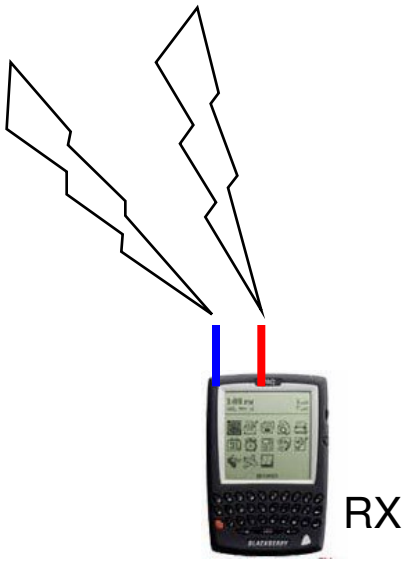
➔For a given channel error probability, due to channel correlation effects, 802.11g has more consecutive frame losses..

➔Consecutive frame losses + periodic low powers , amplify the resulting frame loss probability for 802.11g

Looking for an explanation

- **Proprietary power control for energy saving?**
  - ⇨Which rationale??
- **Antenna diversity!**
  - ⇨Using two antennas, cards can improve their reception performance.. How?
    - →Selecting the highest RSSI signal?
    - →Combining the signals received at both the antennas?
    - →And which antenna should be used for transmissions?

Most common RX Diversity

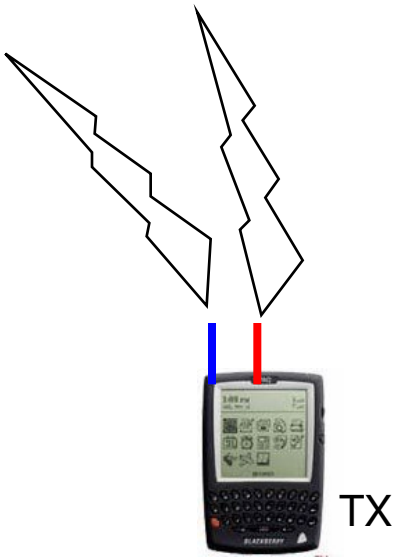


Vendor try to maintain the algorithm as simplest as possible

- Just pick one Antenna..

- When consecutive frames are received with CRC errors, switch to the other one

Most common TX Diversity



- Just pick one Antenna..

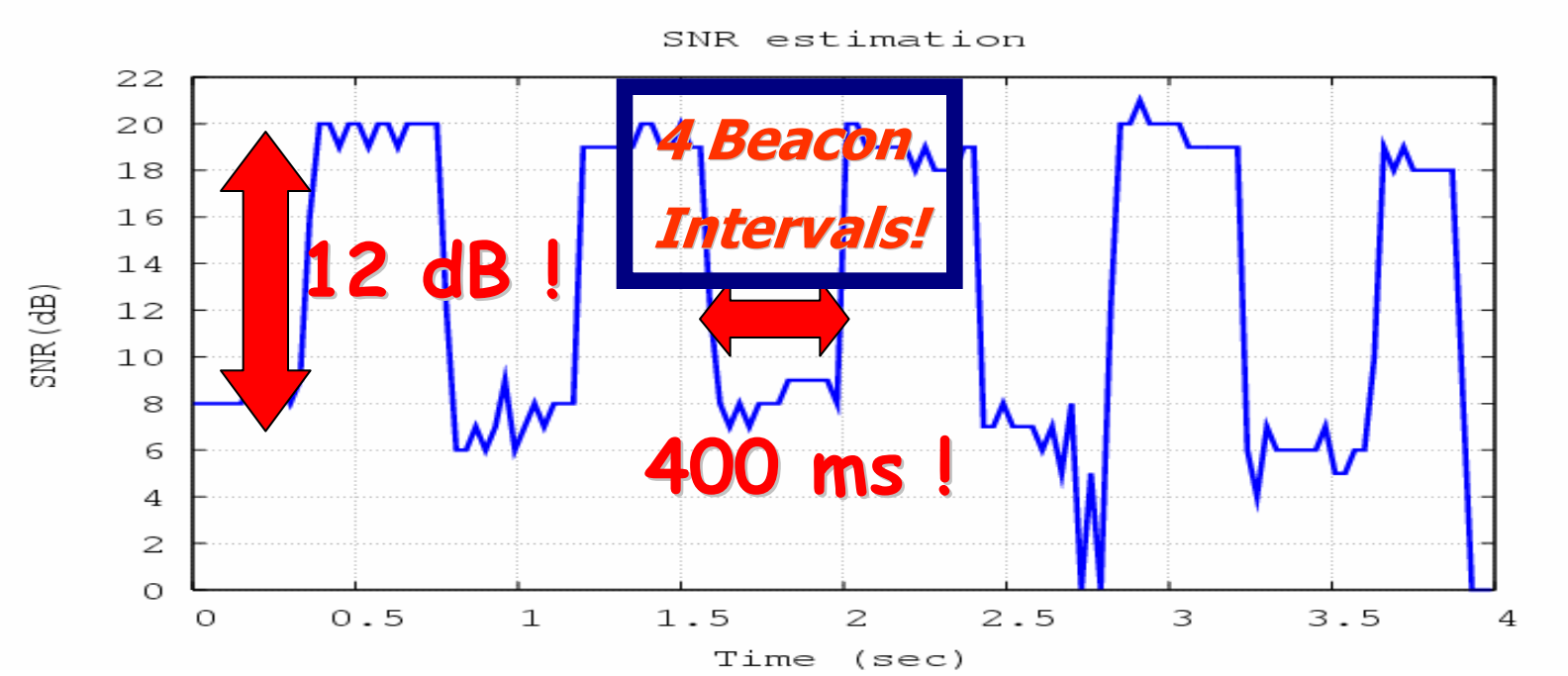
-When consecutive acks are lost, switch to the other one

-For broadcast frame, without feedbacks, just periodic switch

-For acks, use the RX antenna

Effects on outdoor broadcast links

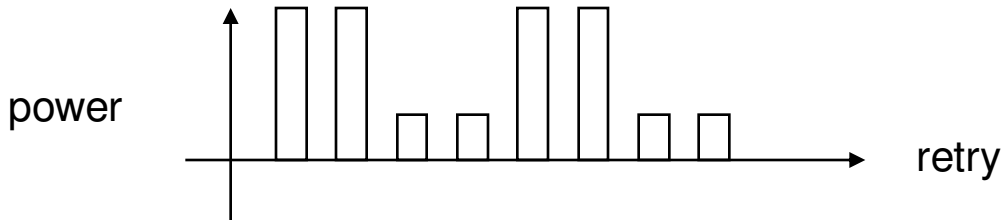
➔ **Due to TX Diversity, if one antenna works better than the other one (often, cards employ only one antenna) , the card works in bad conditions for an half of the time!**



"intermediate" 50% DPR conditions induced by the RSSI fluctuation

Effects on outdoor unicast link

➔Again, due to different antennas performance, radiation power changes as a function of the retransmission index, since periodic antenna switching is triggered!



➔Similarly, RX diversity can originate sudden variations in the ACK RSSI!

Conclusions

VENDOR-DEPENDENT REALITY

- **Vendor-dependence and undocumented vendor solutions**
  - Plainly wrong explaination may occur for experimental phenomena
  - Dangerous trap for QoS actual guarantees
- **New QoS strategies needed**
  - EDCA is not a final solution
  - new interoperability/measurement tests
  - ***distributed control for cheating cards***