Towards an Open Source IEEE 802.11p Stack

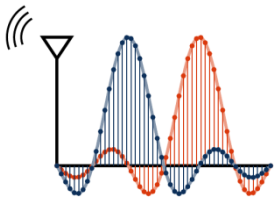
Bastian Bloessl <bloessl@ccs-labs.org>

Computer and Communication Systems Group, University of Innsbruck, Austria

February 2014 · FOSDEM · SDR Dev Room · Brussels, Belgium

Outline

- Introduction



WiME

Wireless **M**easurement and **E**xperimentation

  - IEEE 802.11p Transceiver

    - Applications

Improved SDR Platforms

Hardware

- {B,N}210
- HackRF
- BladeRF

GNU Radio

- VOLK
- Async. Messages
- OFDM Reference Design

Standards

- DVB-T
- LTE
- WiFi

SDR in EE and CS

Electrical Engineering

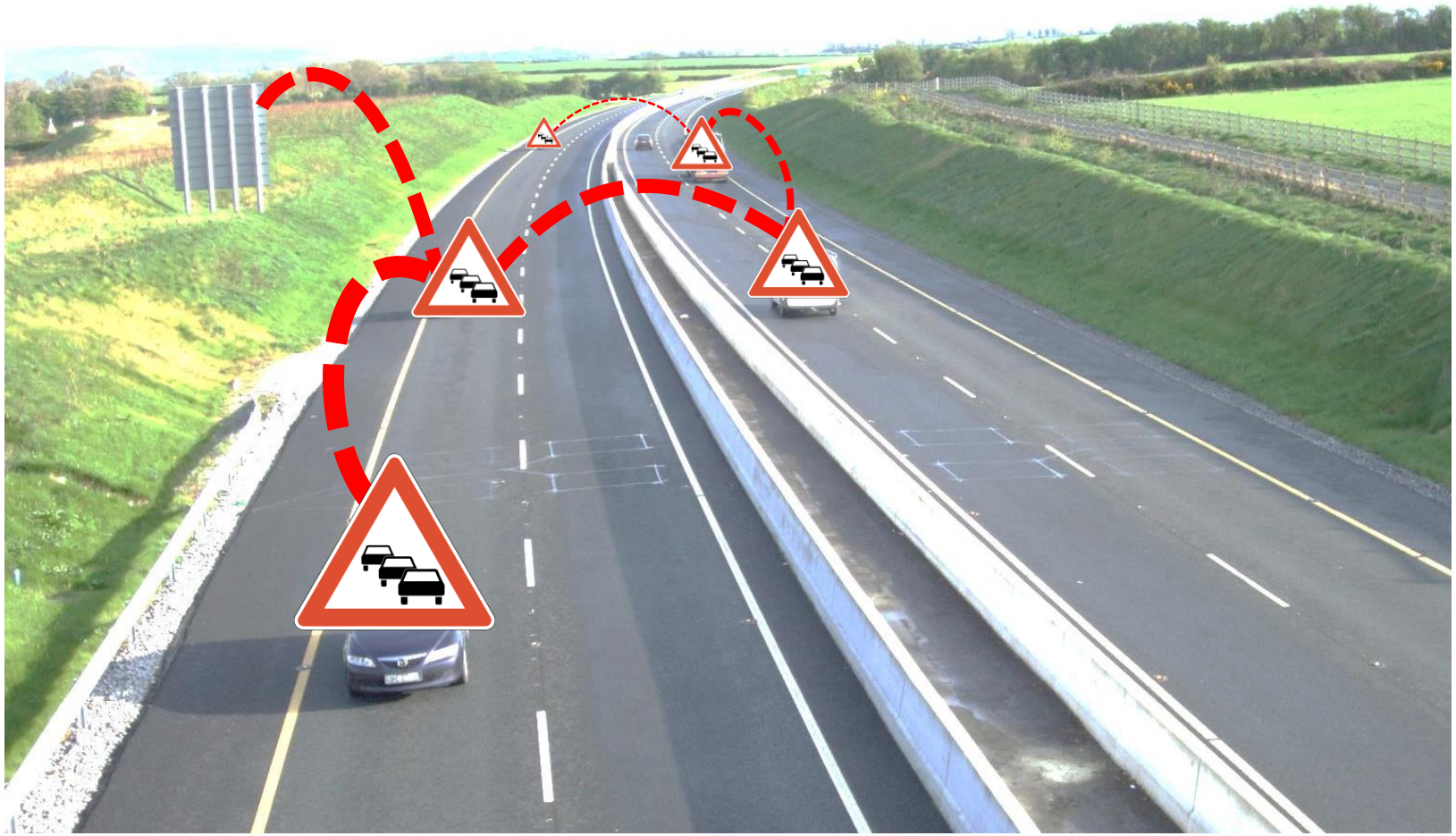
- Signal processing
- Receiver design
- Signal propagation

Computer Science

- Network protocols
- Network simulation
- Security / Privacy

Example: **Vehicular Networks**

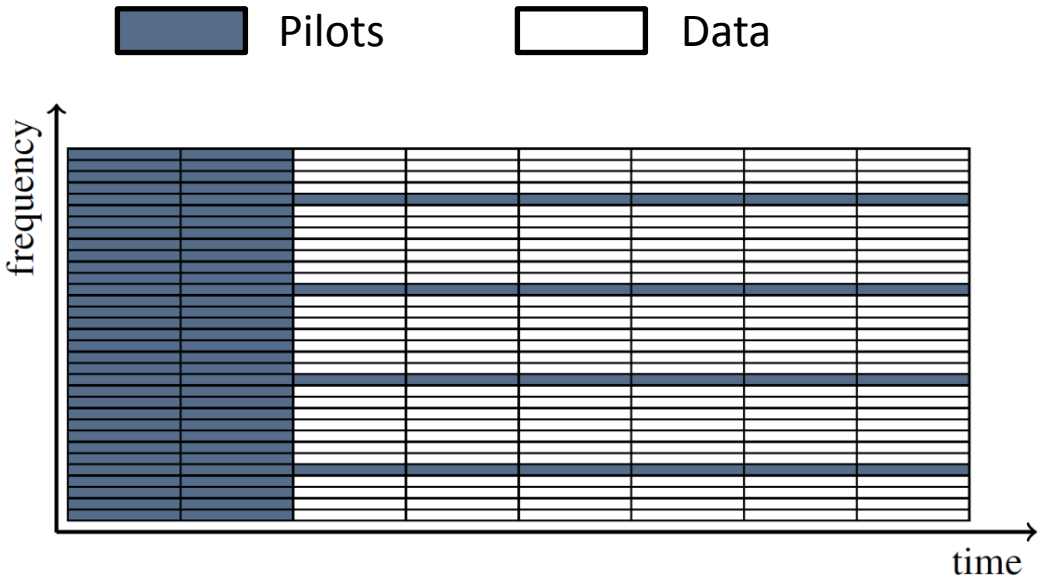
Vision: Vehicular Ad Hoc Networks



IEEE 802.11p Standard

- Standardized in 2011
- Dedicated spectrum

- Adaption of WiFi
  - OFDM
  - 64 subcarriers
  - 10 MHz bandwidth
- Problem:
  - Designed for indoor environments



Current Experimental Platforms

- Prototypes
  - Cohda MK2
- Adapted WiFi cards
  - Unex DCMA-86P2
  - Atheros

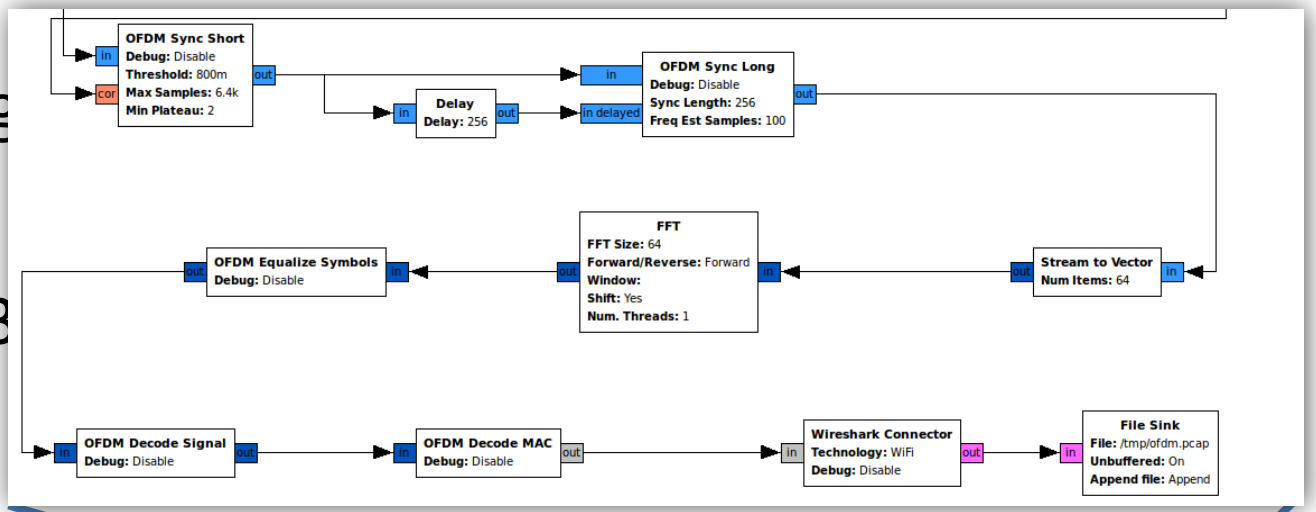
Limited Information / Blackbox

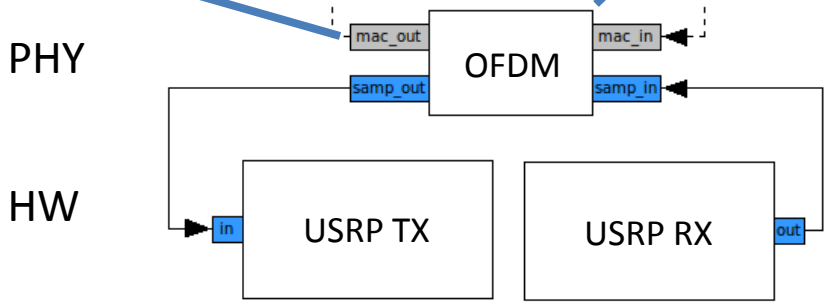
IEEE 802.11p Transceiver

Bastian Bloessl, Michele Segata, Christoph Sommer and Falko Dressler, "**Towards an Open Source IEEE 802.11p Stack: A Full SDR-based Transceiver in GNURadio**," Proceedings of 5th IEEE Vehicular Networking Conference (VNC 2013), Boston, MA, December 2013, pp. 143-149.

Transceiver Design

- Layered Desig
- Hierarchical B
- Extendable
  - Wireshark
  - Linux TCP/IP
- No changes to FPGA

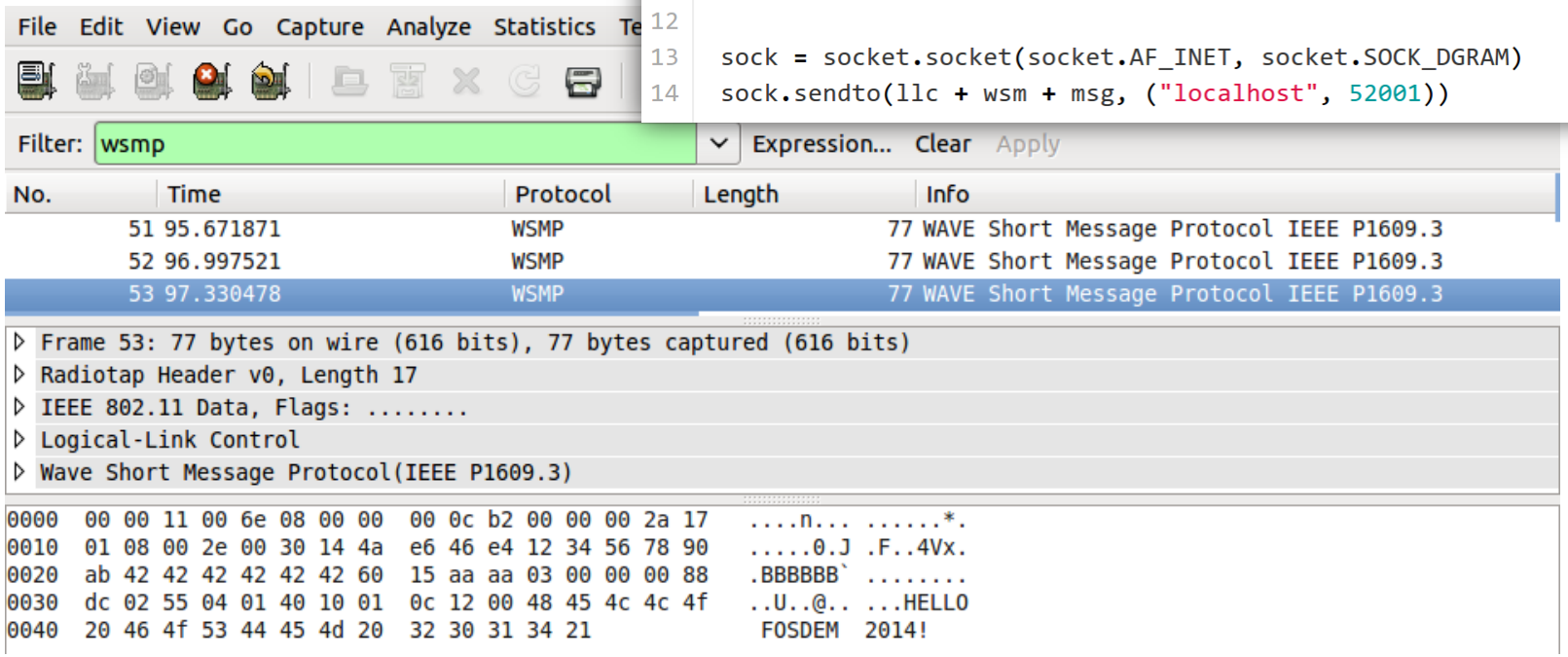




Application Interface

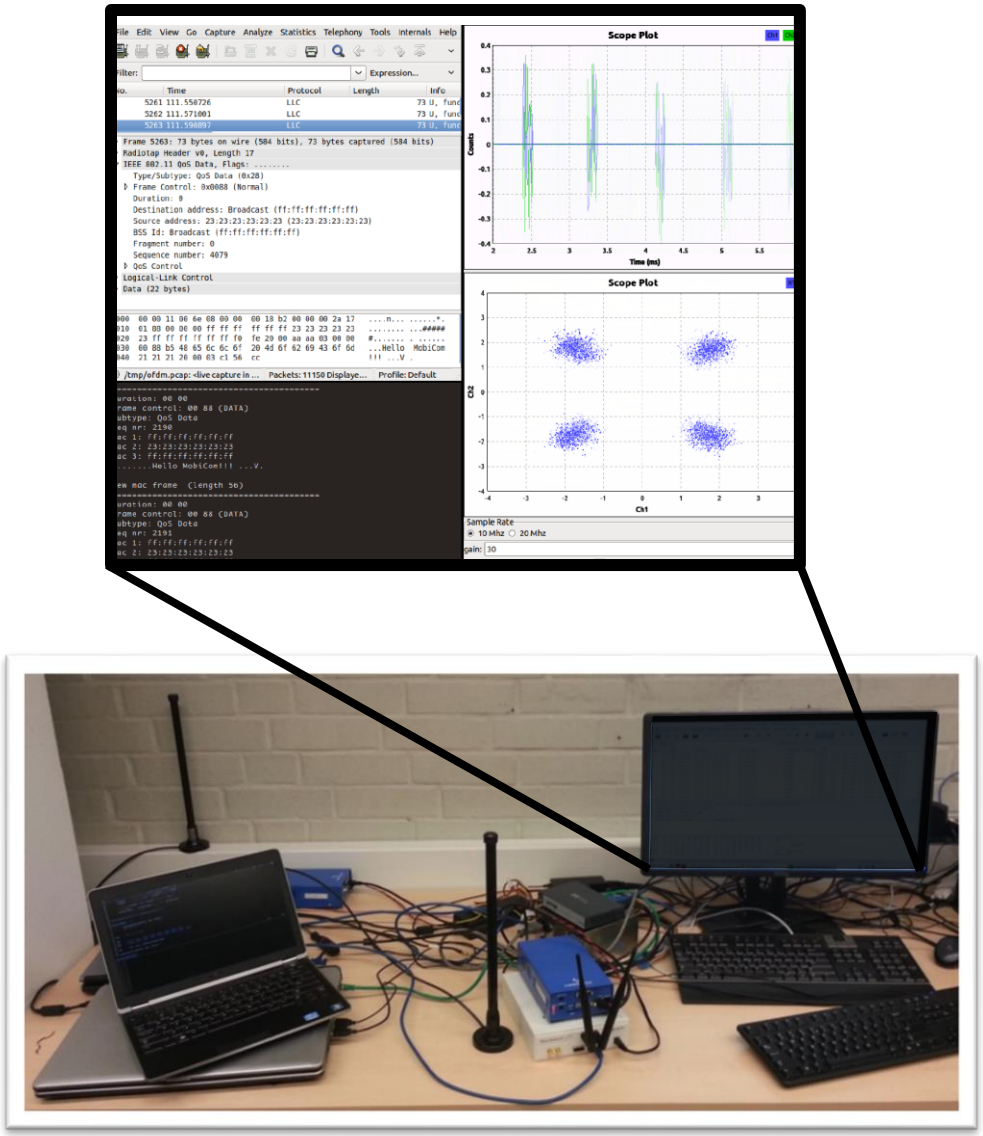
- Connect to SDR via TCP/UDP sockets

```python
#!/usr/bin/env python

import socket, struct

msg = "HELLO FOSDEM 2014!"

llc = struct.pack("8B", 0xaa, 0xaa, 0x03, 0x00, 0x00,
                        0x00, 0x88, 0xdc)

wsm = struct.pack("8BH", 0x02, 0x55, 0x04, 0x01, 0x40,
                         0x10, 0x01, 0x0c, len(msg))

sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
sock.sendto(llc + wsm + msg, ("localhost", 52001))
```

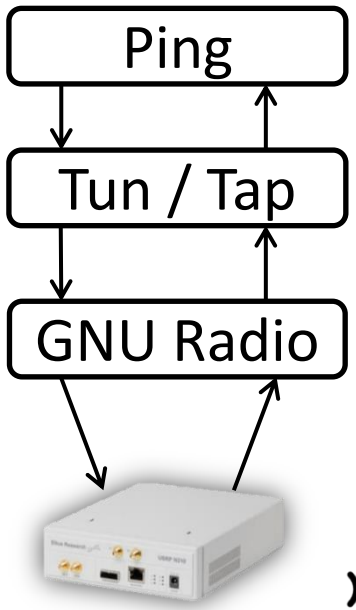


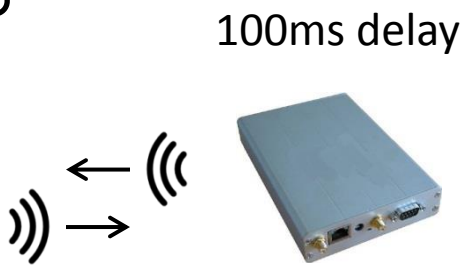
Interoperability

- IEEE 802.11a/g
  - MacBook Pro
  - Intel Ultimate N6300
  - Air Live X.USB
- IEEE 802.11p
  - Cohda Wireless MK2
  - Unex DCMA-86P2 Atheros-based



Limitations of GPP-based Platform



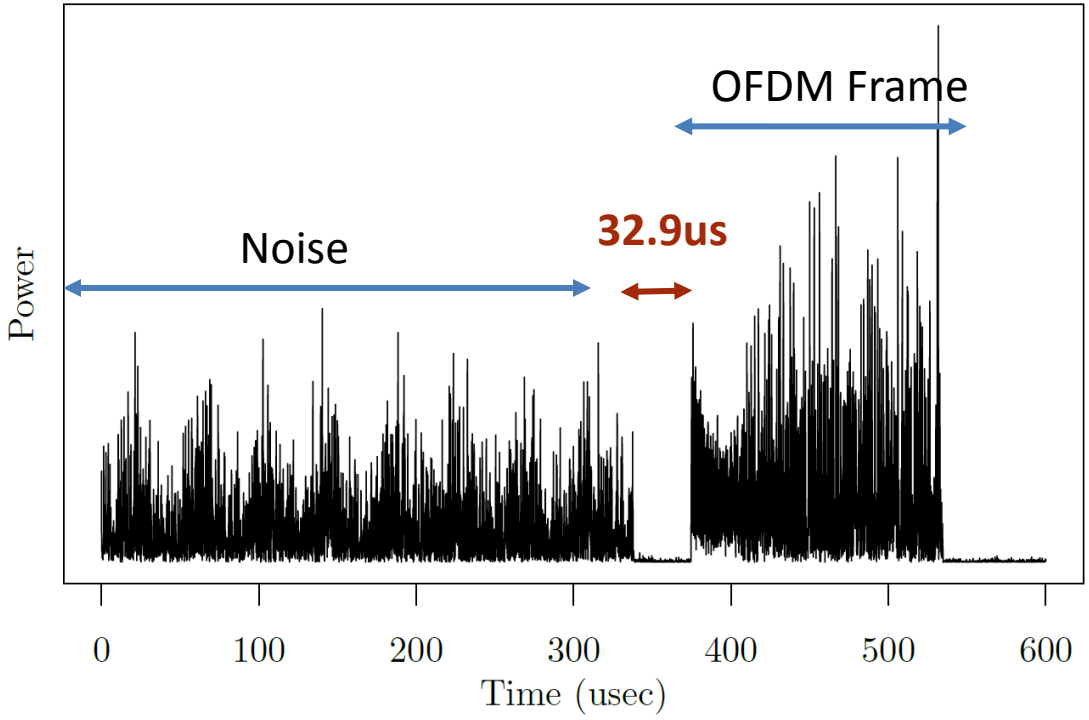



```
64 bytes from 192.168.123.2: icmp_req=504 ttl=64 time=110 ms
64 bytes from 192.168.123.2: icmp_req=505 ttl=64 time=108 ms
64 bytes from 192.168.123.2: icmp_req=506 ttl=64 time=127 ms
64 bytes from 192.168.123.2: icmp_req=509 ttl=64 time=106 ms
64 bytes from 192.168.123.2: icmp_req=510 ttl=64 time=105 ms
64 bytes from 192.168.123.2: icmp_req=512 ttl=64 time=116 ms
64 bytes from 192.168.123.2: icmp_req=514 ttl=64 time=106 ms
```

- RTS / CTS
- Acknowledgments
- Duration Field

Carrier Sensing and Channel Access

- CSMA on PC has too high delay
- CSMA on FPGA is feasible



A. Puschmann, P. Di Francesco, M. A. Kalil, L. A. DaSilva, and A. Mitschele-Thiel, "**Enhancing the Performance of Random Access MAC Protocols for Low-cost SDRs**," in 8th International Workshop on Wireless Network Testbeds Experimental Evaluation and Characterization (WiNTECH 2013). Miami, FL: ACM, September 2013.

Applications

Fuzzing

- Form of penetration testing
- Send random, cluttered, non-standard frames
- See what happens to the device / driver / firmware

„ If fuzzing doesn‘t solve your problem, you‘re not doing enough of it “

Privacy and Fingerprinting

- EE
  - Channel features
  - Characteristics of analog HW

- CS
  - Traffic patterns (when, where, packet size, …)
  - MAC address / temporary identity

- SDR
  - Implementation details of chip / firmware / driver

Enabling Realistic Simulations

Measurement results

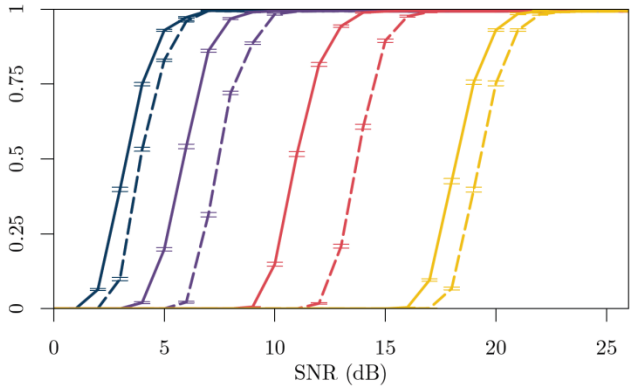
- Coherence bandwidth
- Coherence time
- Channel taps

Network simulation

- Frame Error Curves
- OFDM interference

channel models

+ gr-ieee802-11 =



…in Conclusion

Conclusion

- SDR-based IEEE 802.11p OFDM transceiver
- Modular and extensible
- Many applications
- Open Source
  - http://www.ccs-labs.org/projects/wime/

Other Projects

- gr-rds
  - Radio Data Service
  - FM Radio

- gr-ieee802-15-4
  - ZigBee
  - 2.4GHz O-QPSK PHY