Exploiting Programmable Architectures for WiFi/ZigBee Inter-Technology Cooperation

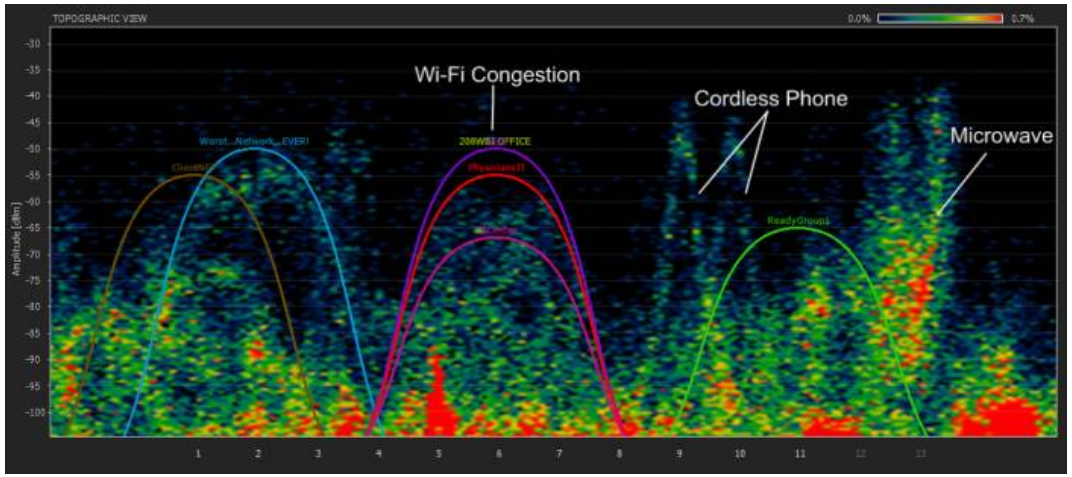
P. De Valck, I. Moerman, D. Croce, **F. Giuliano**, I. Tinnirello, D. Garlisi, E. De Poorter, B. Jooris

UNIVERSITÀ DEGLI STUDI DI PALERMO

Cavalese (TN), Jan 16, 2014

Coordination of multiple technologies

- Typically based on orthogonal channel assignment + other mechanisms to increase robustness to interference
  - Carrier sense, adaptive coding, etc...
- Not always efficient in case of spectrum overloading
  - e.g. ISM bands with WiFi, Bluetooth, ZigBee, phones, microwave



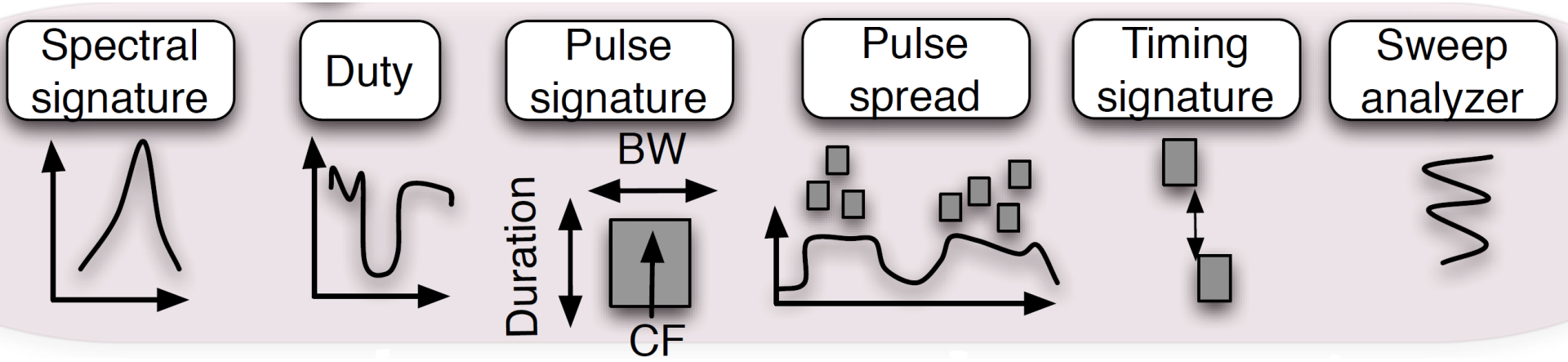
- ***Is it possible to improve coordination by activating an inter-technology communication channel??***

Learning from 'human communications'

- *Non verbal communication* allows to improve the set-up of multiple communication channels
  - to provide a feedback channel to voice channels
  - in noisy environments
- Different forms of non verbal communication
  - Environmental to identify the coexisting channels
  - Para-verbal (volume, tone, rhythm)

Back to wireless networks

- Roadmap to coexistence
  - Adapt to changing radio conditions
  - Inter-technology coordination schemes
- *Identification is the key*
- Typical approach: look at the lowest PHY level
  - Joint analysis of both frequency and time domains



Back to wireless networks

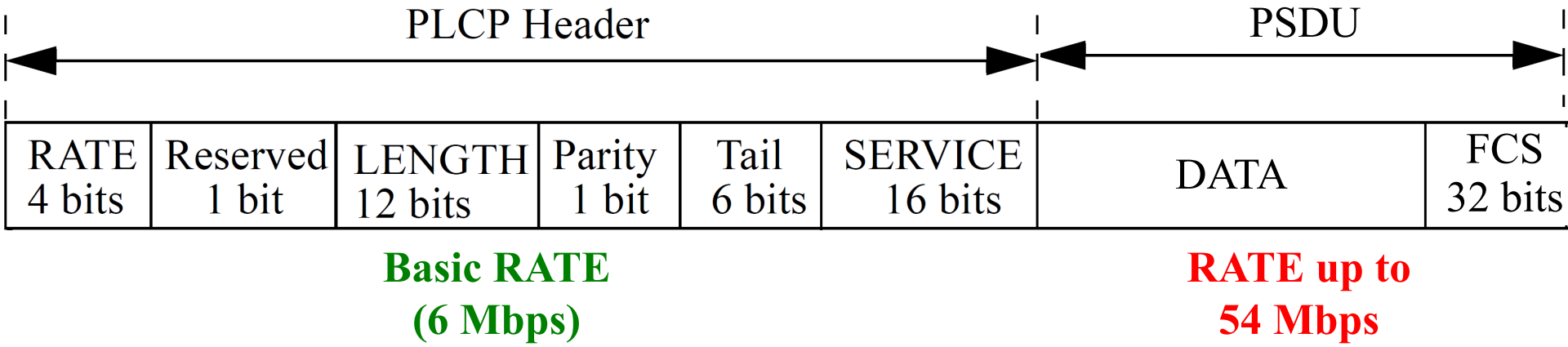
- Roadmap to coexistence
  - Adapt to changing radio conditions
  - Inter-technology coordination schemes
- *Identification is the key*
- Typical approach: look at the lowest PHY level
  - Joint analysis of both frequency and time domains
  - Is there a better/simpler way?
- *What can we learn from Rx errors?*
  - *Can we identify the **type** of interference?*

ErrorSense (TRAC 2014)

- Exploit (WiFi) protocol specific structures
  - PLCP length/rate/parity, MAC version, FCS fields
- Exploit Hardware characteristics
  - How the (WiFi) transceiver reacts to non-(WiFi) signals (timeouts, sensitivity, etc.)
- Keep it simple:
  - No dedicated hardware (*commodity* NICs)
  - No complex PHY layer analysis (in firmware!)
  - No channel scan (no communication disruption)
  - Passive detection only (no overhead)

WiFi reminder

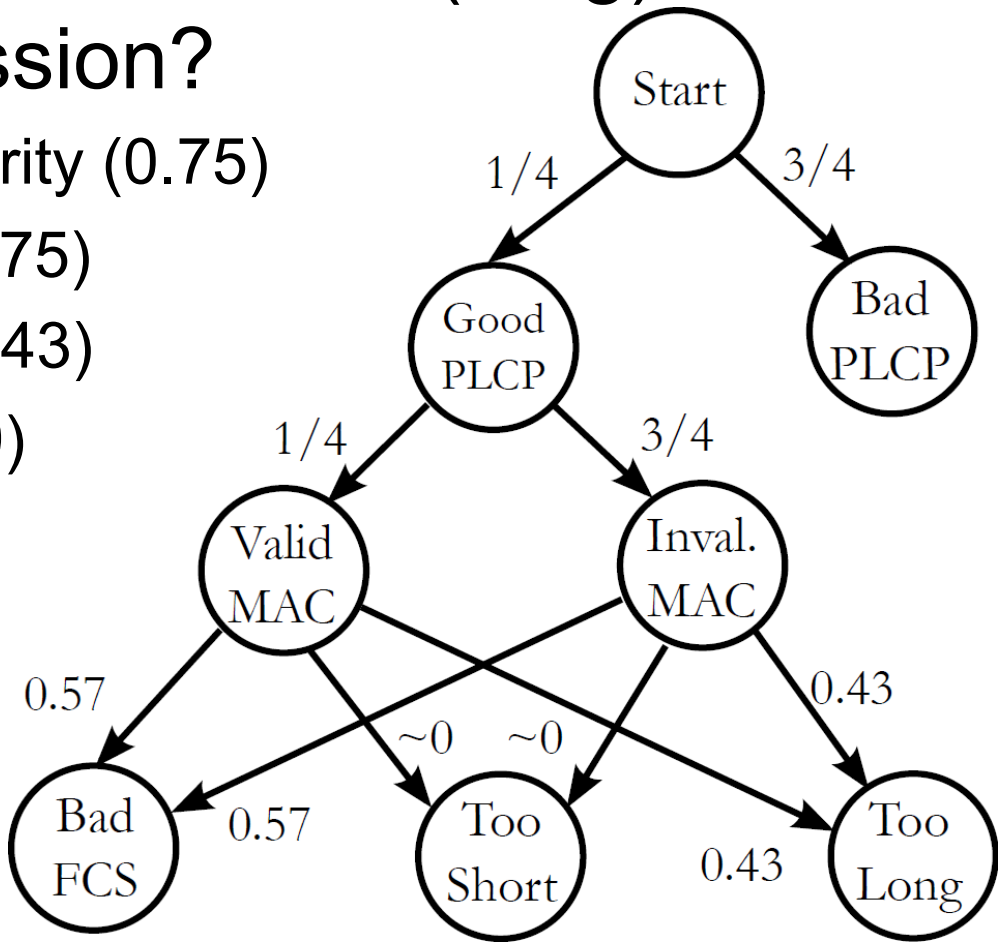
- MAC frames follow a PLCP Header
  - Consider 802.11g:



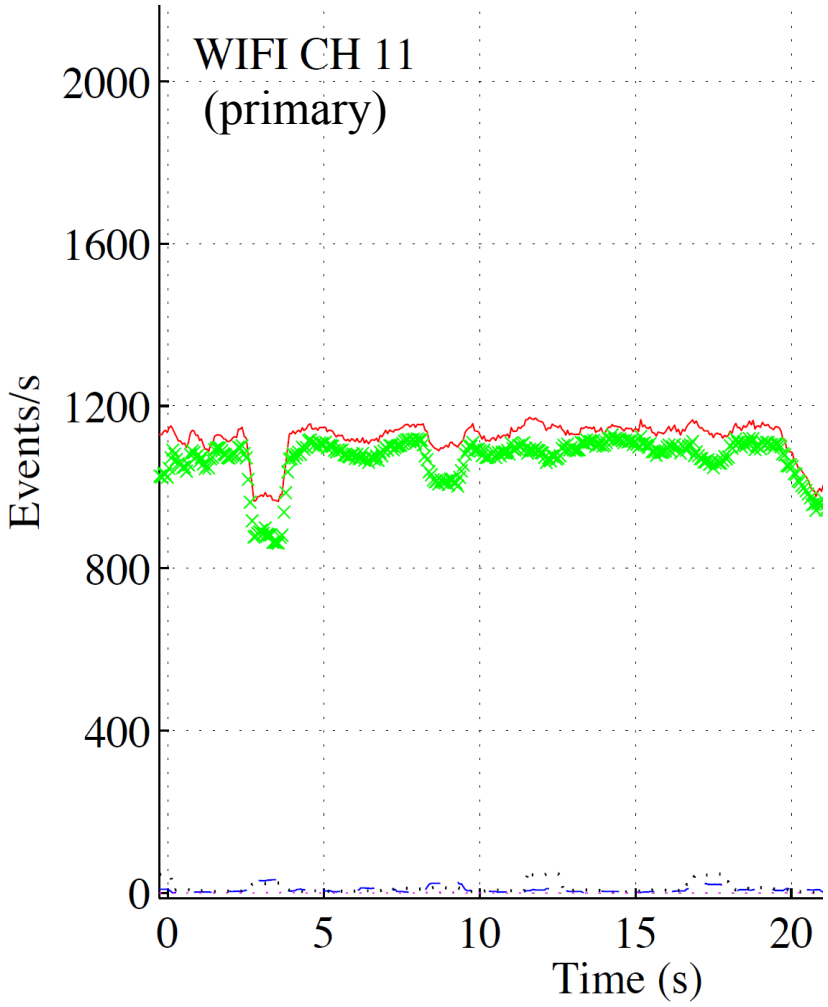
- Some notes on the different fields:
  - Rate: 8 possible values (out of 16!)
  - Length: range 0-4095 (but used range is 14-2346)
  - Parity: only one bit!

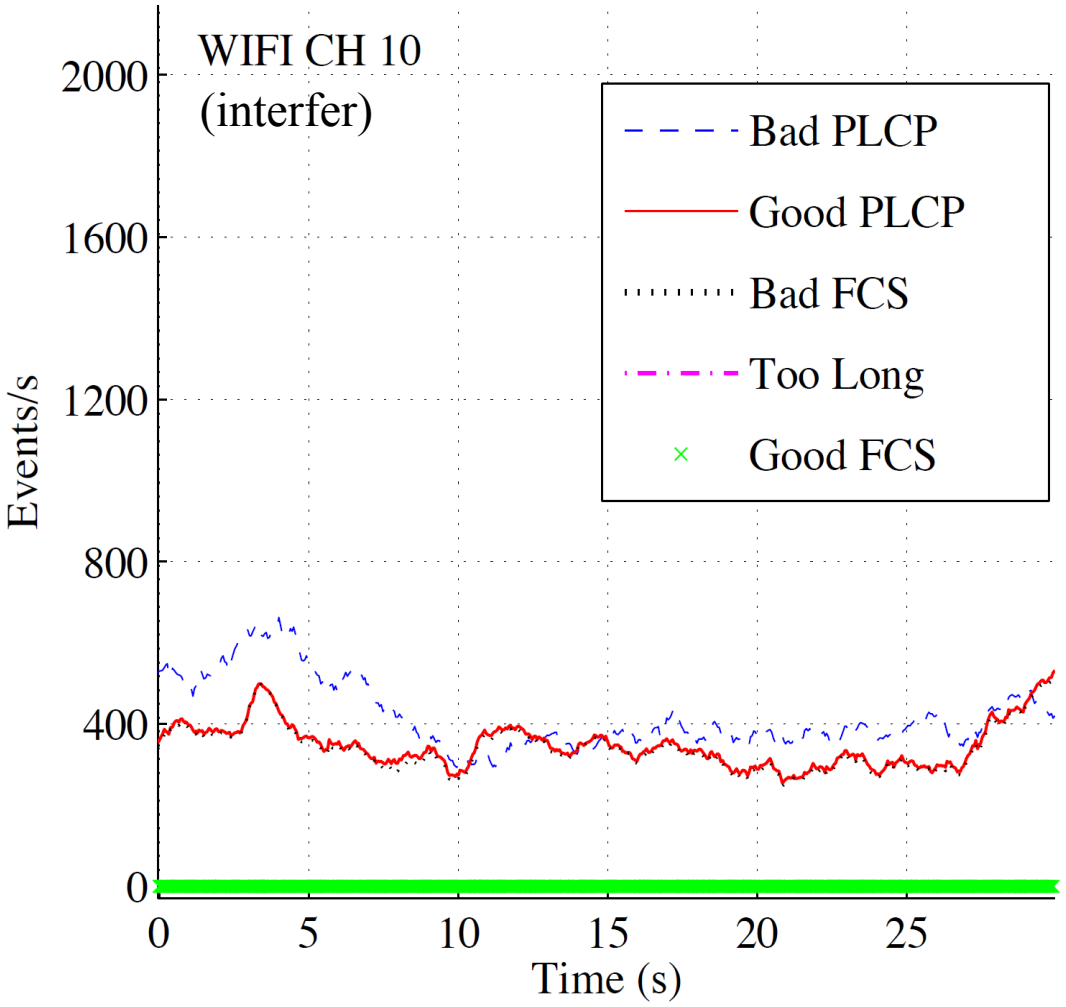
Error events (non-WiFi)

- What goes wrong when WiFi (.11g) receives a non-WiFi transmission?
  - Bad PLCP rate or parity (0.75)
  - Bad MAC version (0.75)
  - Length Too long (~0.43)
  - Length Too short (~0)
  - Bad FCS (~0.57)



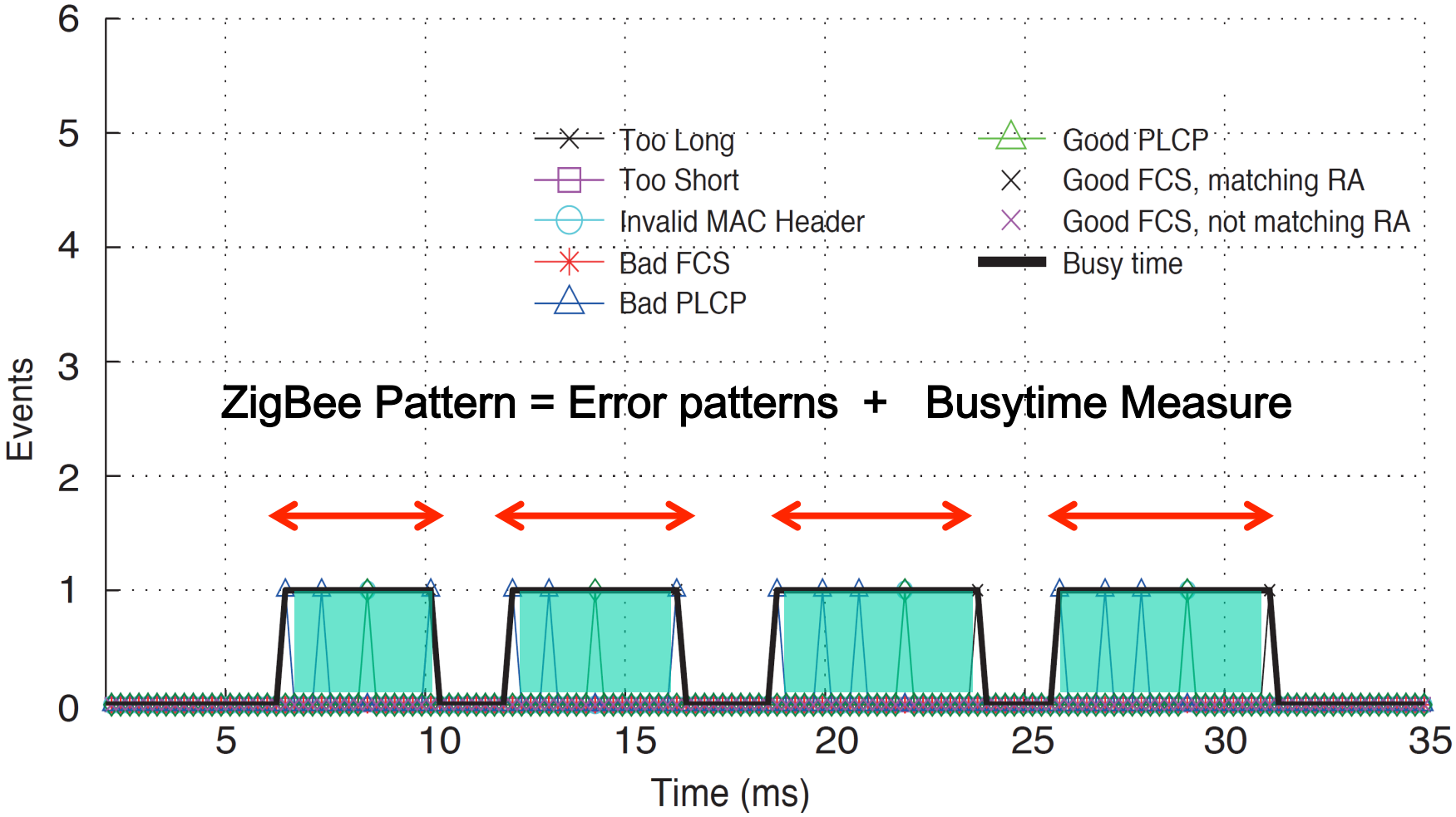
Does it work? (WiFi interference)





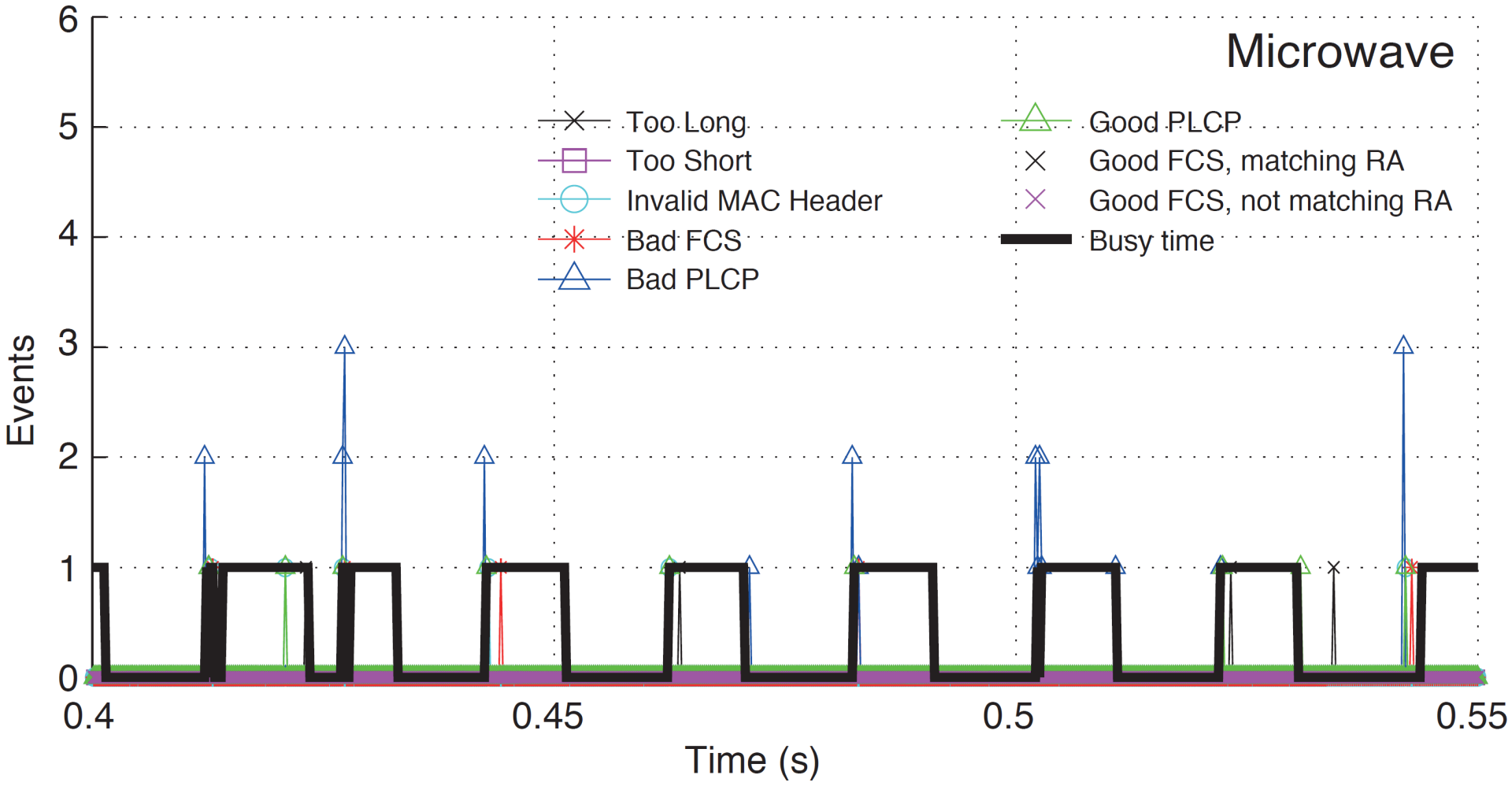
Hardware-specific patterns (I)

- How does the card react to ZigBee frames?



Hardware-specific patterns (II)

- How does the card react to Microwave ovens?



Medium Access Adaptation

- Network Card Requirements:
  - Flexible tuning of MAC parameters on ***runtime***
  - Modification of medium access operation

Key: turn NIC in a Programmable Wireless MAC Architecture

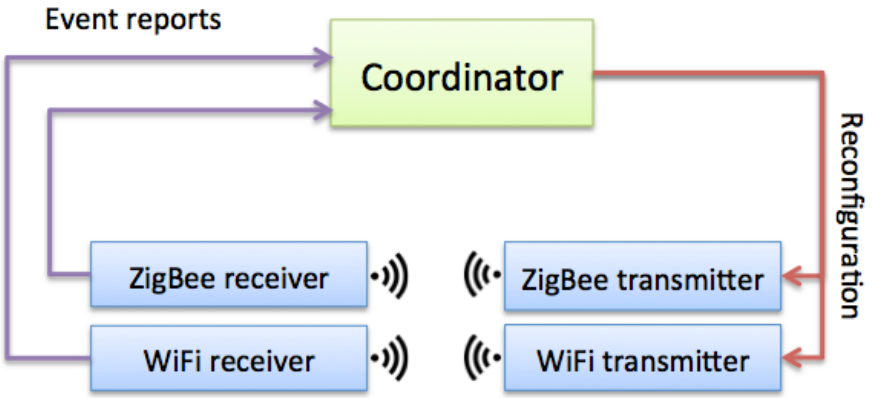
Programmable Wireless Architectures for MAC

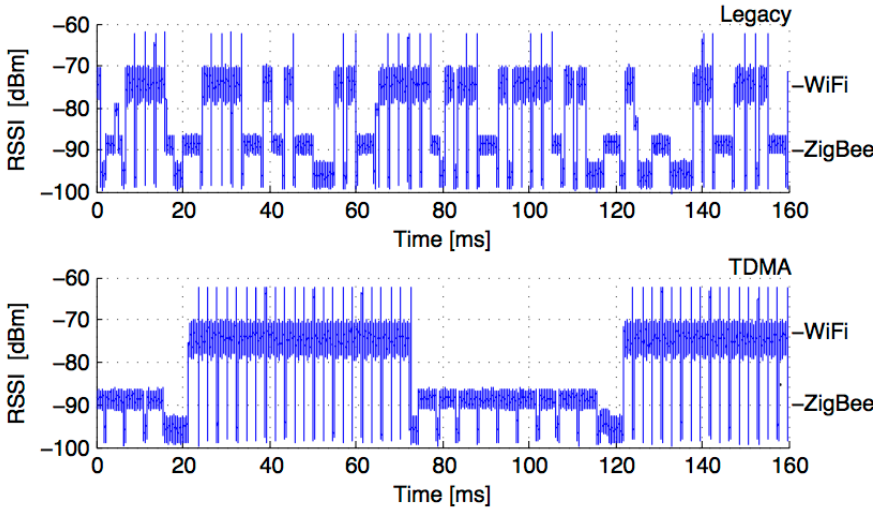
- Abstraction:
  - MAC instructions set → MAC APIs
  - MAC programming logic → MAC Programs
  - Logic Executor → MAC Processor

- *Wireless MAC Processor (802.11)* [IEEE INFOCOM 2012]
  - Reconfigurable MAC in terms of **Finite State Machine**
  - Implemented on 802.11 Commodity Hardware
    - Exploits Error Events detection
- *SnapMAC (802.15.4)* [Journal: Ad Hoc Networks - 2014]
  - separation between the MAC protocol logic and the hardware execution
    - Allows fast TDMA reconfiguration

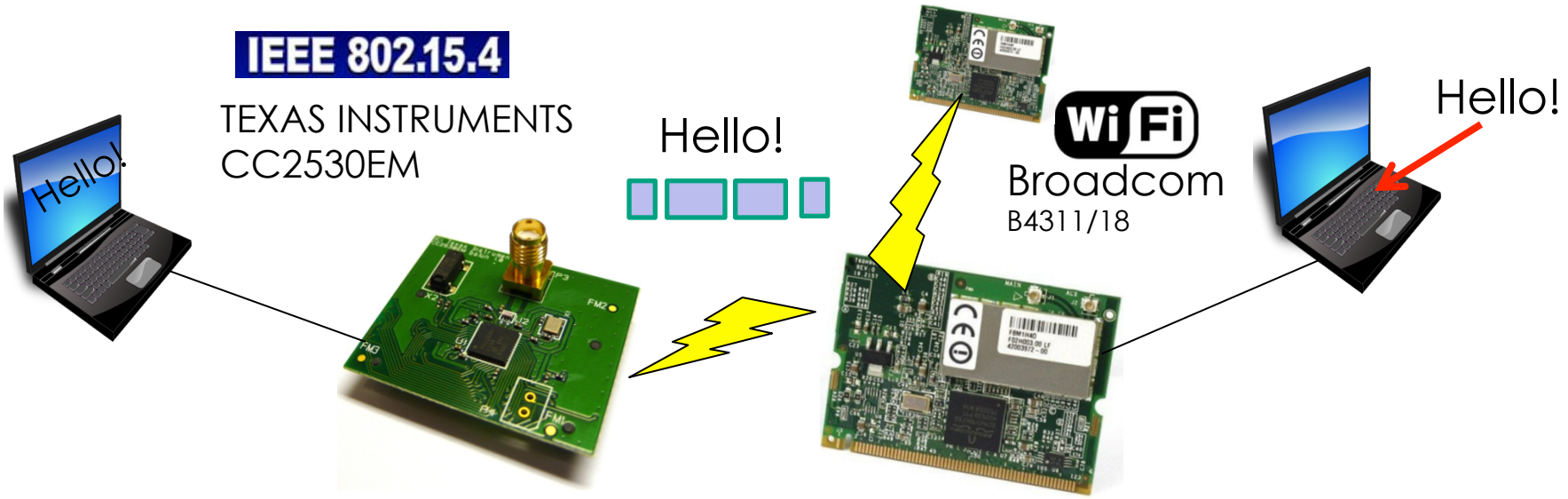
Channel access coordination

- Inter-technology coordination (TDMA-like)
  - Legacy access in each slot





WiFi/ZigBee communications



- *Packet-length communication* with a 802.11 to 802.15.4 link
  - commercial interfaces! Novel receivers could do better..
- Example of **protocol definition** for sending low rate **signaling**
  - Busy time monitoring and statistics for low level analysis
  - Transparent to legacy stations (e.g. frame fragmentation)
- No coordinator/gateway!!!

Conclusions

- Receiver errors can be used to detect the interfering technology
  - Complement classic time/frequency classifiers
    - Improve results, reduce complexity
- Non-conventional channels can be exploited for improving WiFi/ZigBee coexistence
  - Channel sharing with no gateways (cost reduction)
  - Generalizations are possible for programmable/ cognitive networks
- Extend to other technologies or other NICs.

UNIVERSITÀ DEGLI STUDI DI PALERMO

cnit

iMinds

Thanks!!!
Q&A

References

- Croce, D., Gallo, P., Garlisi, D., Giuliano, F., Magione, S., Tinnirello, I.: ***Errorsense: Characterizing wifi error patterns for detecting zigbee interference.*** Wireless Communications and Mobile Computing Conference (IWCMC), 2014 International

- Mil, P.D., Jooris, B., Tytgat, L., Hoebeke, J., Moerman, I., Demeester, P.: ***SnapMAC: A generic mac/phy architecture enabling flexible {MAC} design***. Journal Ad Hoc Networks 17, 37–59 (2014)

- EU FP7 CREW project. http://www.crew-project.eu. Accessed Jan 2014

- Tinnirello, I., Bianchi, G., Gallo, P., Garlisi, D., Giuliano, F., Gringoli, F.: W***ireless MAC processors: Programming mac protocols on commodity hardware***. In: INFOCOM, 2012 Proceedings IEEE, pp. 1269–1277 (2012)

UNIVERSITÀ
DEGLI STUDI
DI PALERMO

cnit

iMinds

Thanks!!!
Q&A

Error events (WiFi)

- Impact of WiFi interference (same technology)

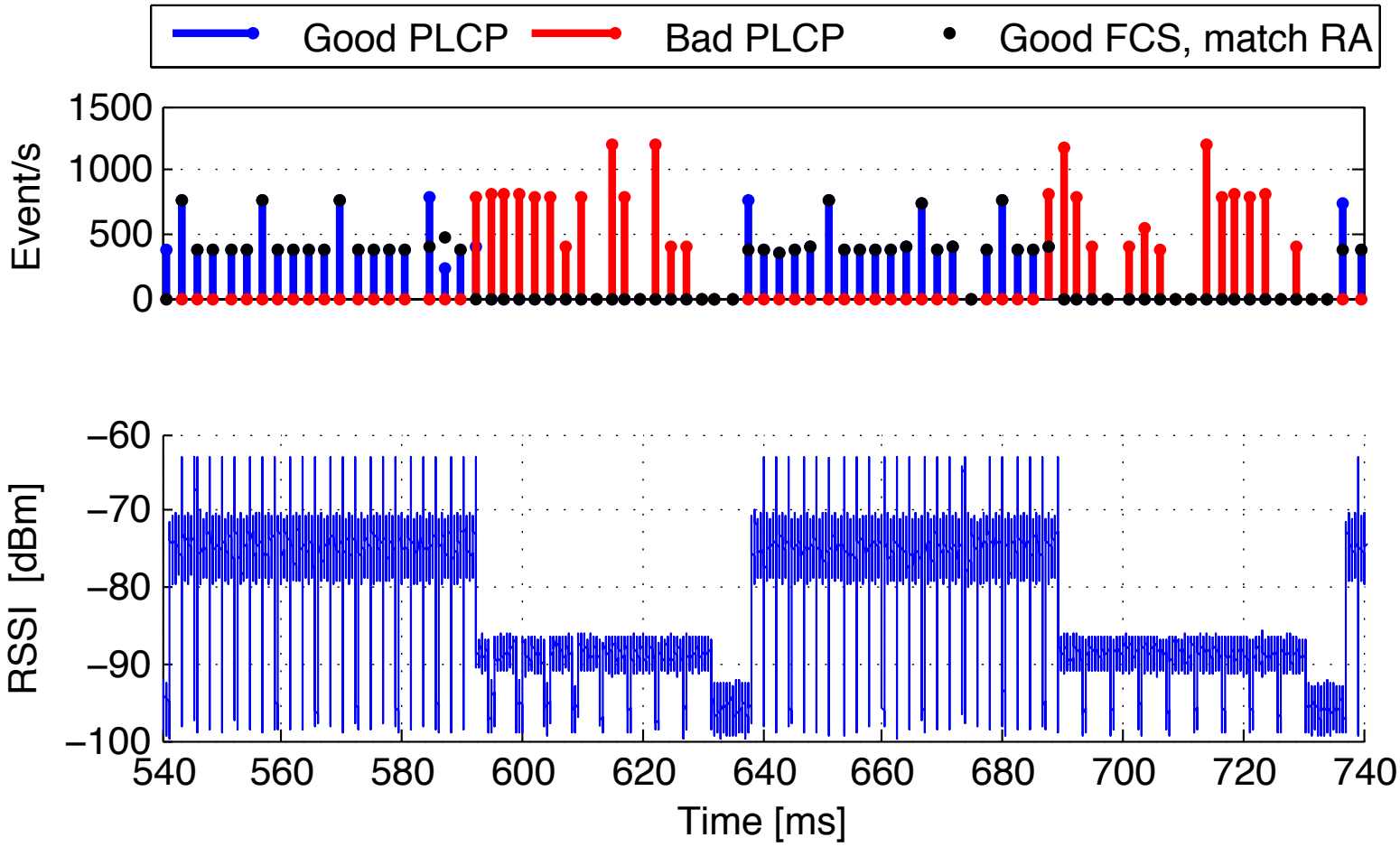
	WiFi ch11		WiFi ch10	
Name	Ev./s	(%)	Ev./s	(%)
Bad PLCP	6.5	(0.5)	455.8	(54.8)
Good PLCP	1110.0	(99.4)	375.8	(45.2)
Invalid MAC	4.0	(0.4)	286.8	(76.3)
Good FCS	1067.1	(96.1)	0	(0.0)
Bad FCS	9.0	(0.8)	368.3	(98.0)
Too Short	0.1	(0.0)	0	(0.0)
Too Long	0.2	(0.0)	0.3	(0.1)

Testbed results

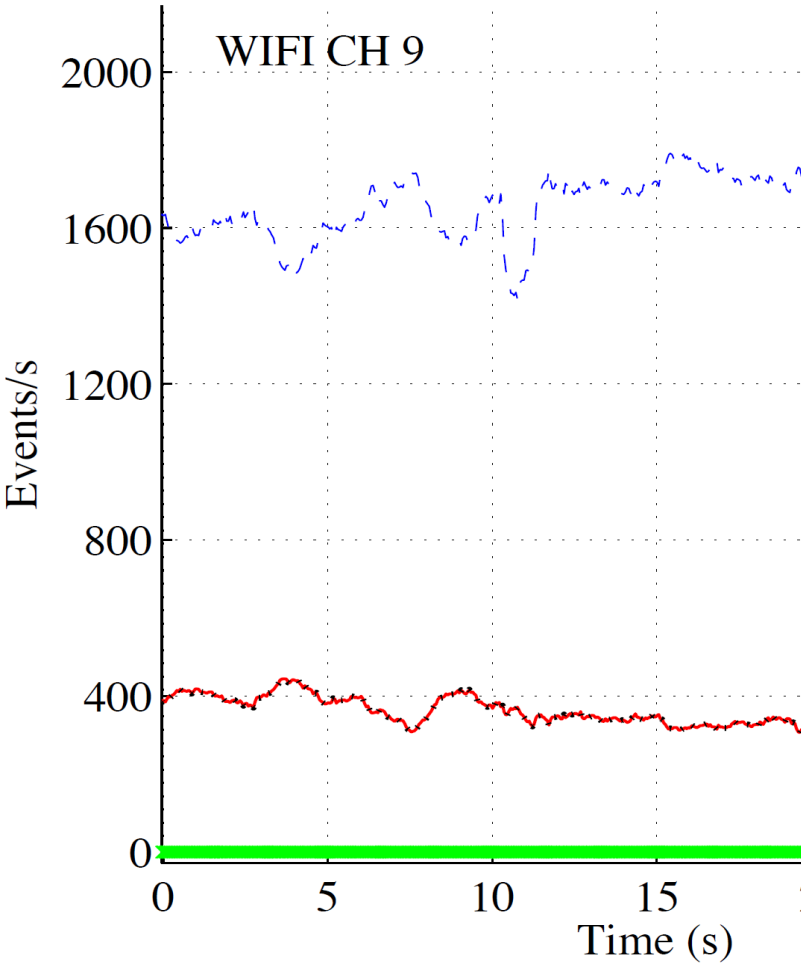
- Implementation in our university lab
  - WiFi card: Broadcom bcm4318, .15.4: MRF24J40
  - Eight possible errors
- Events are detected by monitoring the card
  - No interrupts, must read internal register
  - Polling every 250us
    - Multiple events can occur in the same interval
- Good PLCPs “lock” the receiver
  - Virtual Carrier Sense mechanism

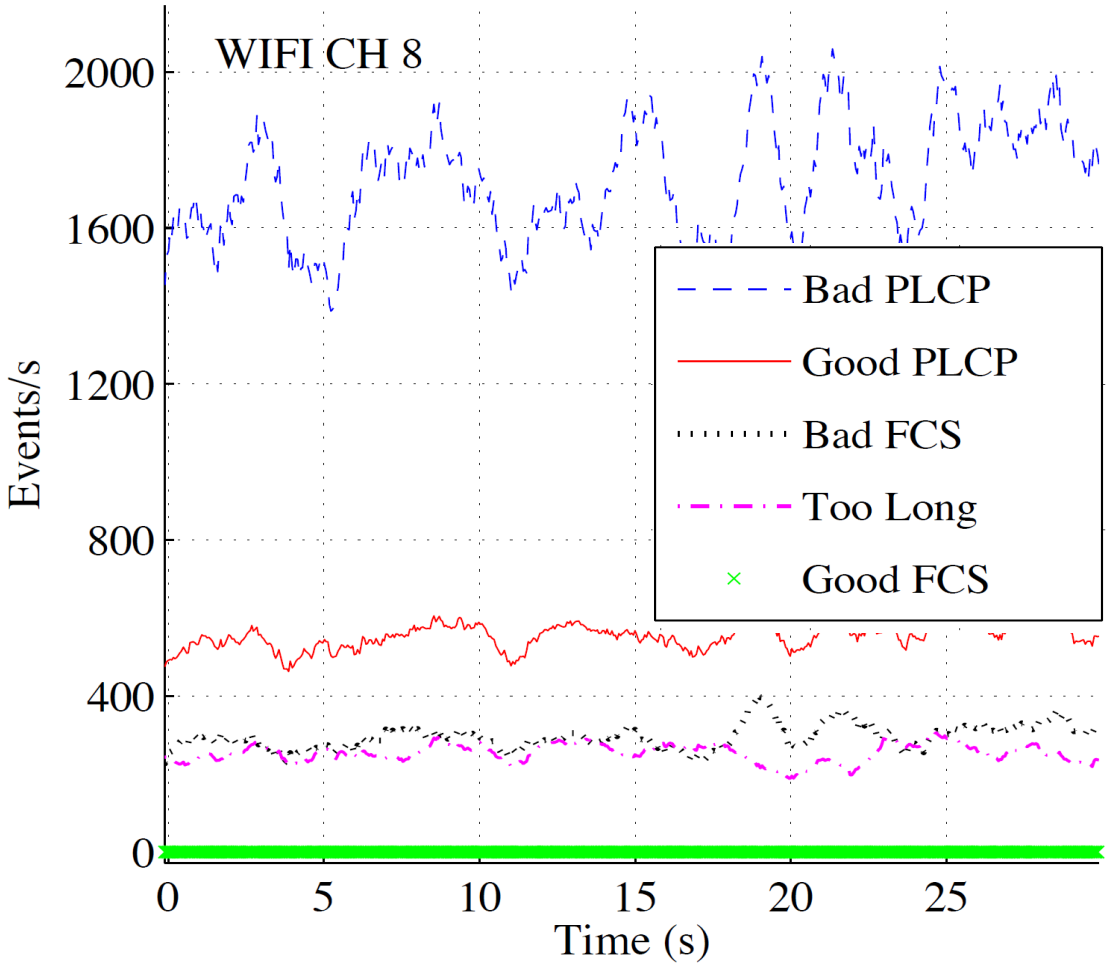
Channel access coordination

- Errors Pattern



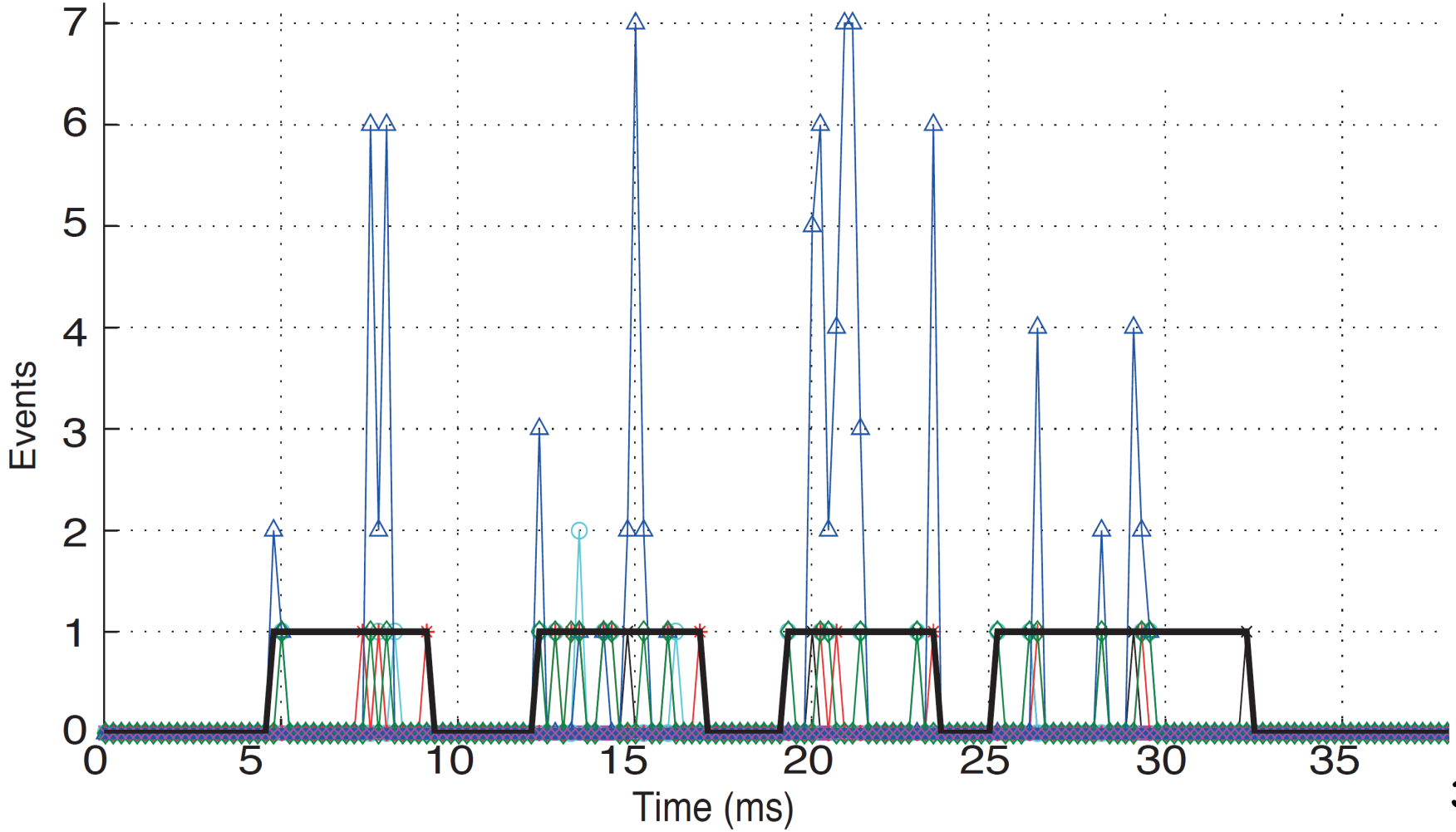
WiFi interference



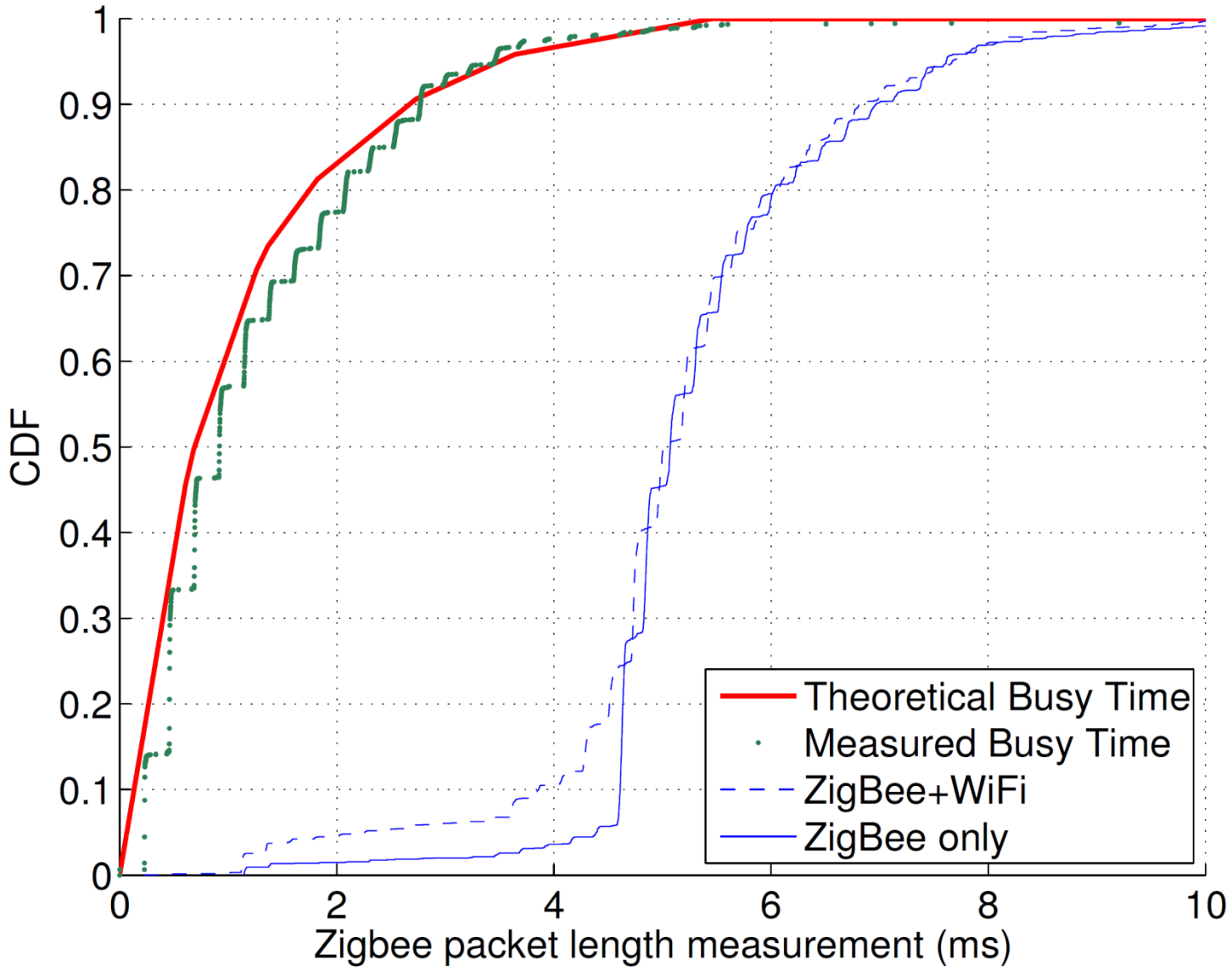


Hardware-specific patterns (II)

- How does the card react to ZigBee frames?

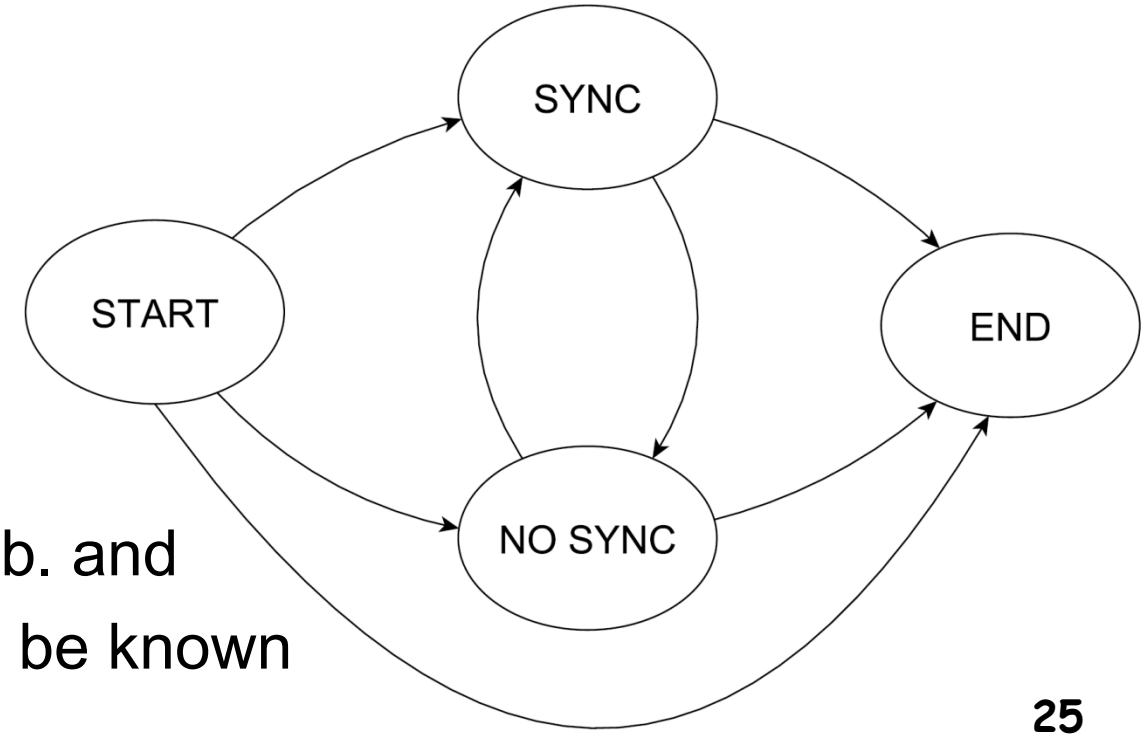


Estimated packet length



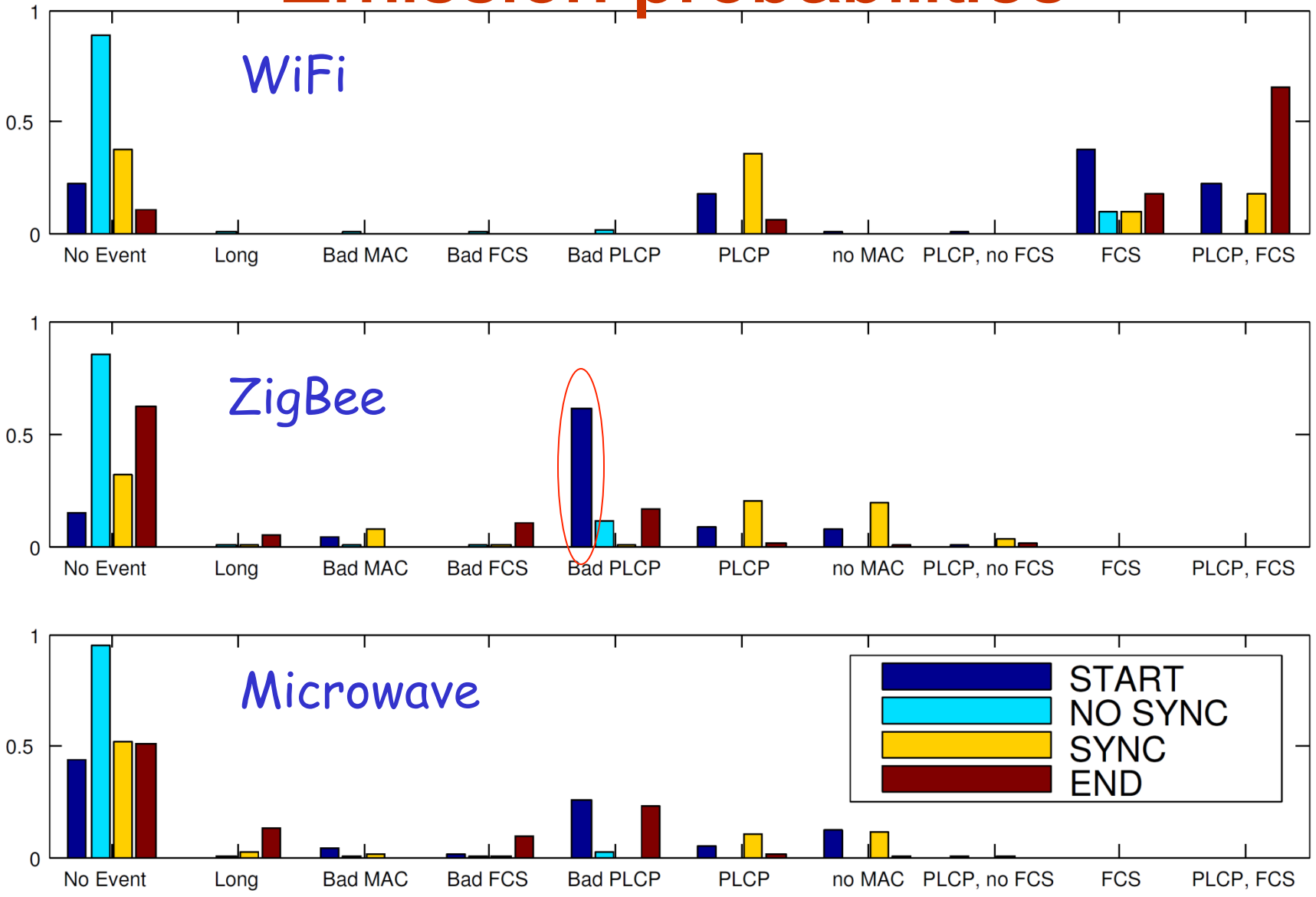
Detecting ZigBee packets

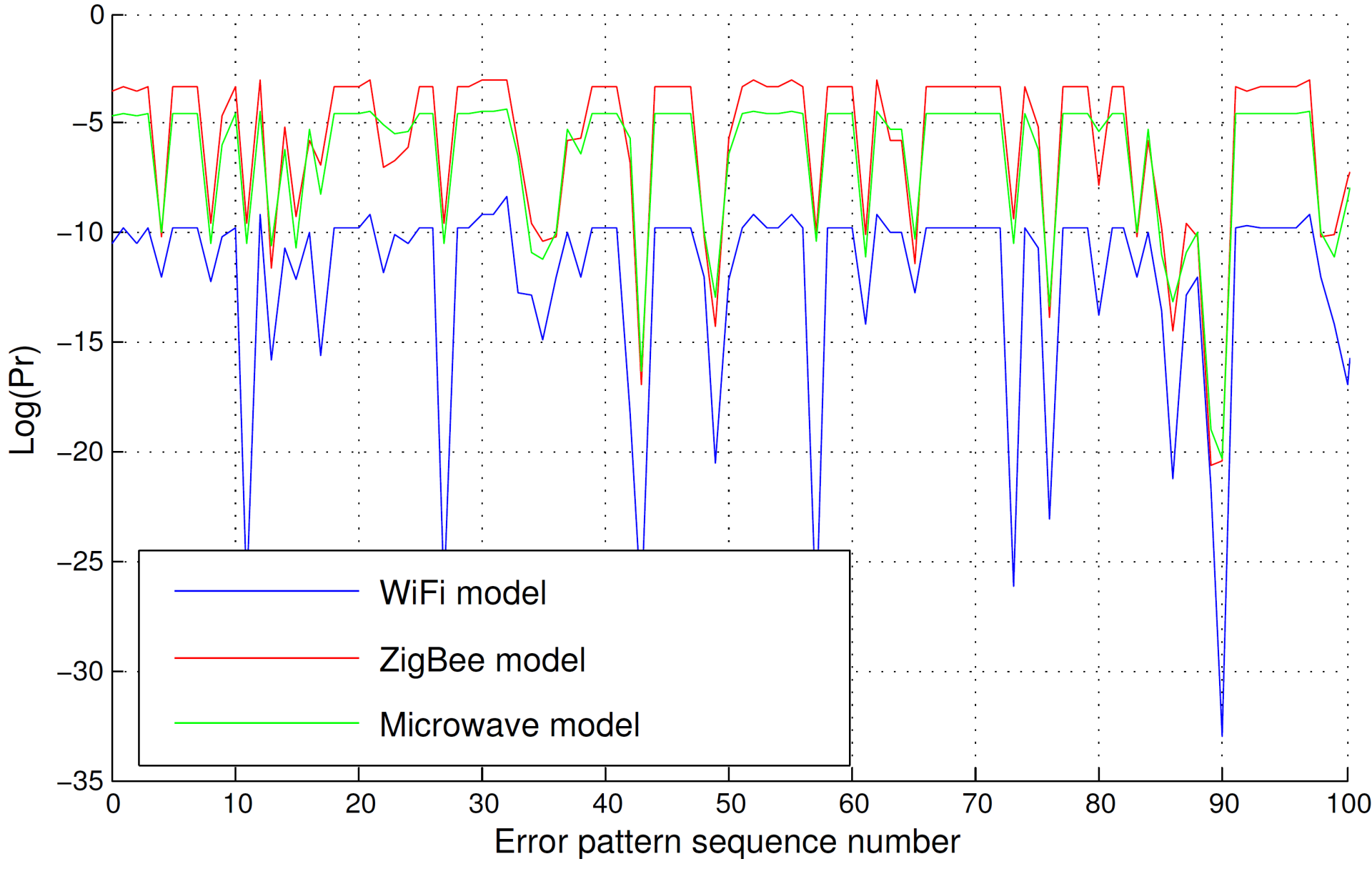
- We use Hidden Markov Models (HMMs) to
  - Track the receiver state given the receiver errors
  - Identify the most likely technology



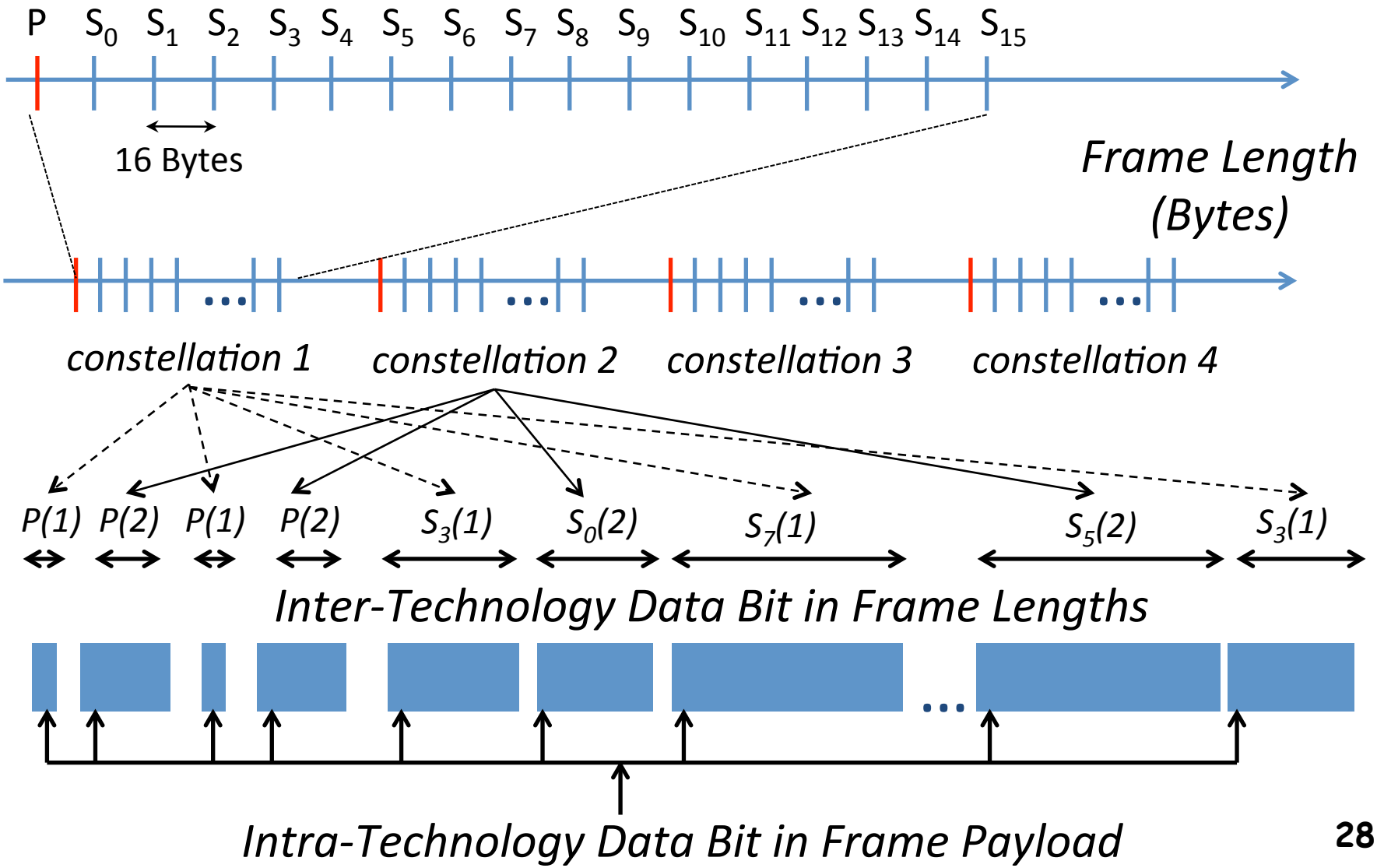
Note: Error (emission) prob. and state transition prob. must be known

Emission probabilities



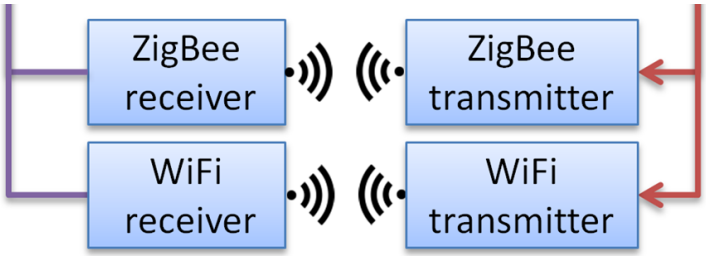

0
−5
−10
−15
−20
−25
−30
−35
Log(Pr)
0
10
20
30
40
50
60
70
80
90
100
Error pattern sequence number
WiFi model
ZigBee model
Microwave model

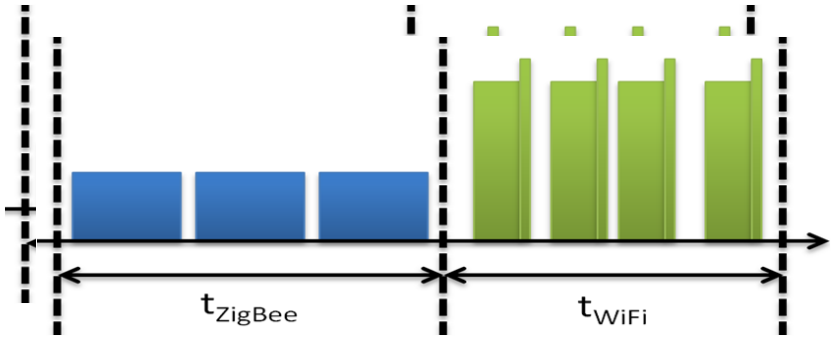
WiFi/ZigBee communication



Remote Use-Case Experiment

- Components at the EU FP7 CREW testbed in Ghent
  - Two alix 802.11 programmable nodes, two SnapMAC enabled 802.15.4 programmable nodes
  - 1 USRP as a channel power sniffer
- TDMA between the two technologies by negotiating the channel allocation time





Error events (non-WiFi)

- What goes wrong when WiFi (.11g) receives a non-WiFi transmission?

BAD PLCP = 1 / 4 (RATE) + 1 / 2(PARITY) = 3 / 4

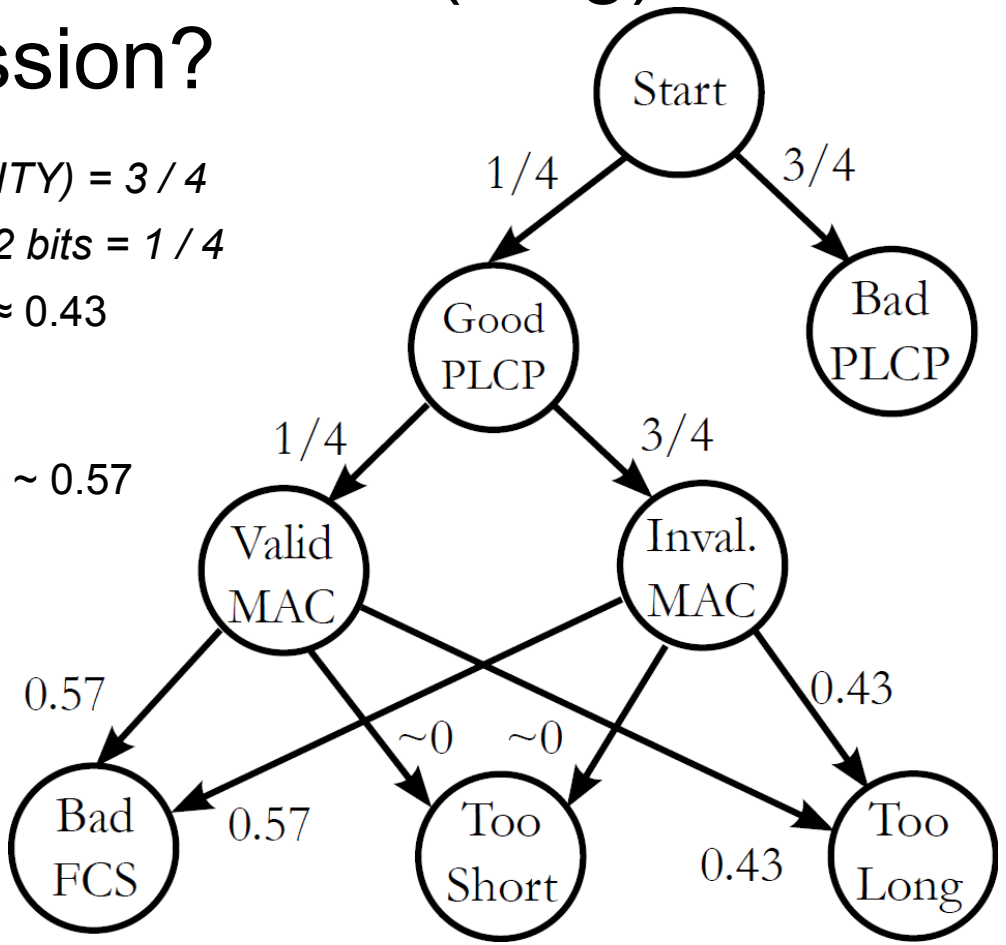
BAD MAC VERSION MAC HEADER, 2 bits = 1 / 4

Too Long probability = 1 − 2346/4096 ≈ 0.43

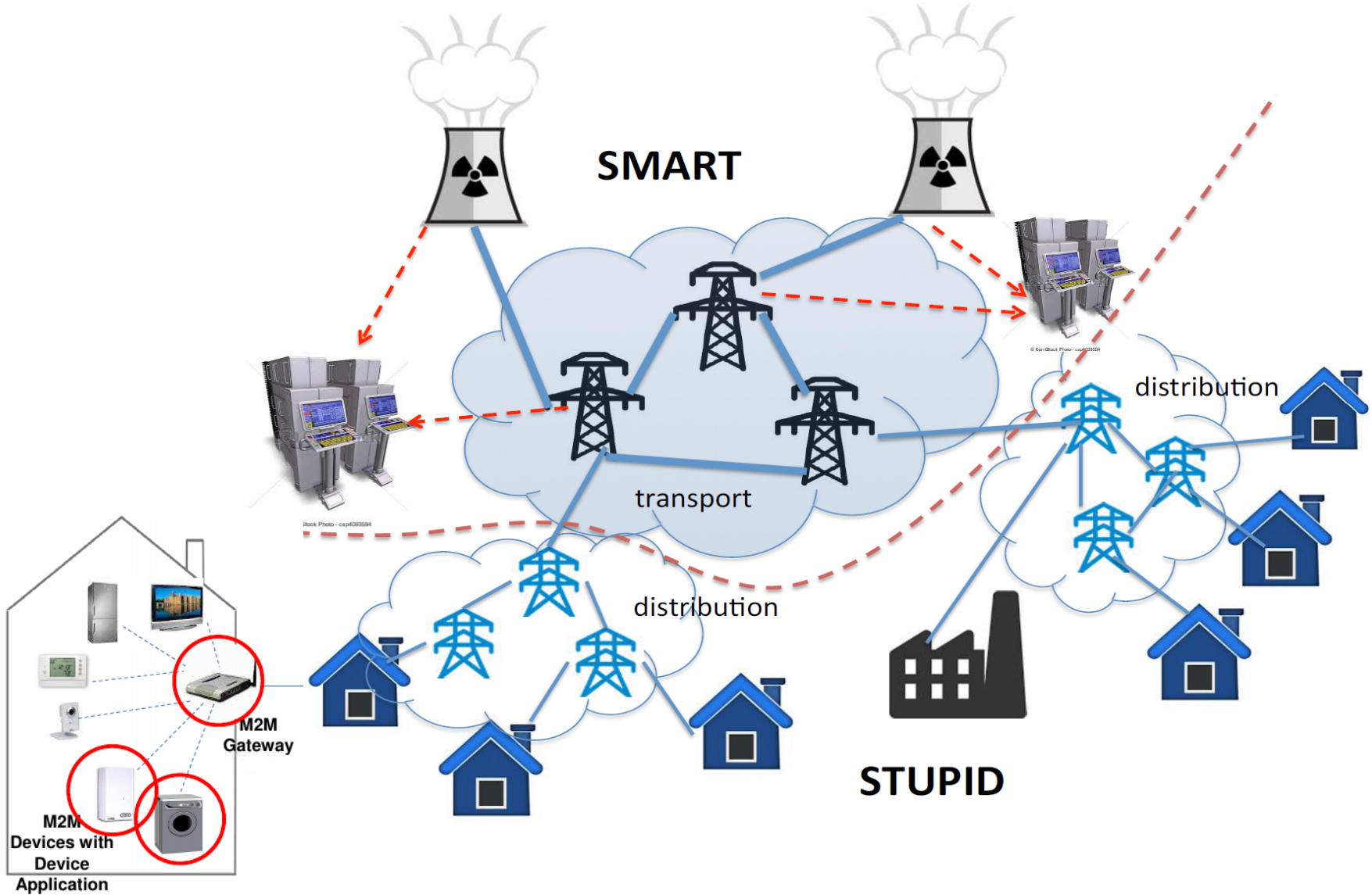
Too Short probability = 14/4096

BAD FCSprobability =

1 – (Too Long OR Too short) ~ 0.57



Traditional Power Grid



Aggregation and privacy in SGs