# WiCop: Engineering WiFi Temporal White-Space for Safe Operations of Wireless Body Area Networks in Medical Applications

Yufei Wang[*], Qixin Wang[*], Zheng Zeng[†], Guanbo Zheng[‡], Rong Zheng[‡]
[*] Dept. of Computing, The Hong Kong Polytechnic Univ.
[†] Dept. of Computer Science, UIUC
[‡] Dept. of Computer Science, Univ. of Houston

Dec. 1, 2011

# Content

Demand

Proposed Framework

Evaluation

Related Work

# Content

Demand

Proposed Framework

Evaluation

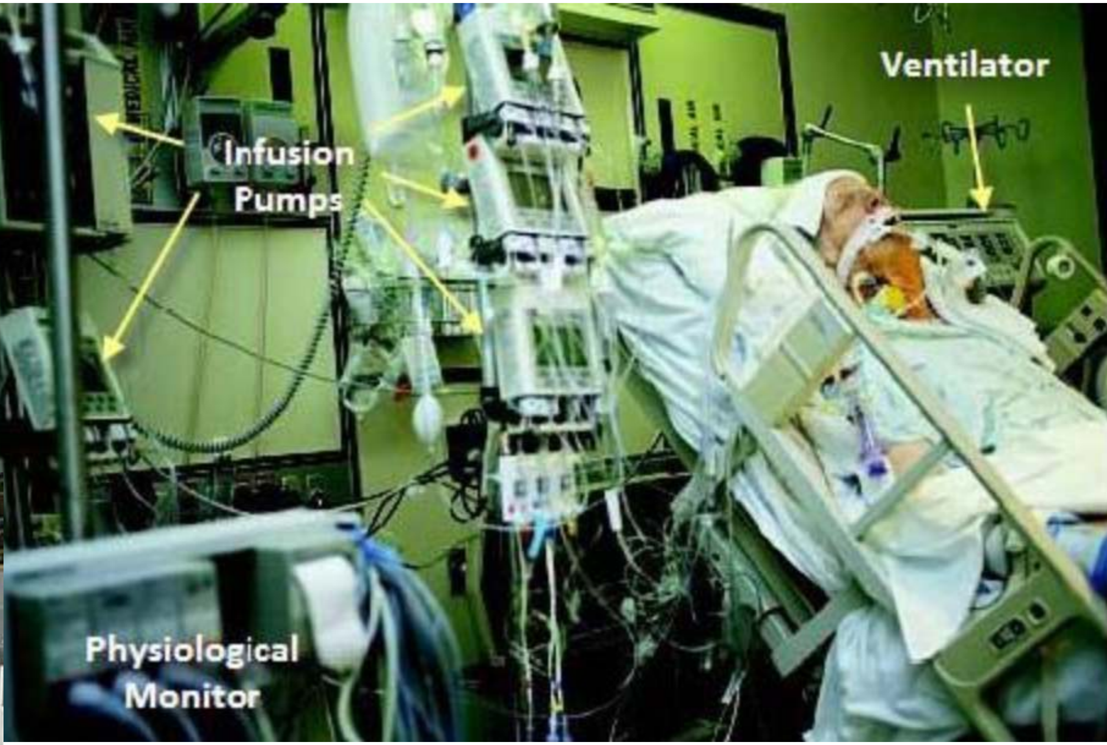
Related Work

# WBAN based medical parameter monitoring overcomes the many drawbacks of wired monitoring.

Tying patient to bed 24x7

Small movement → electrode fall off

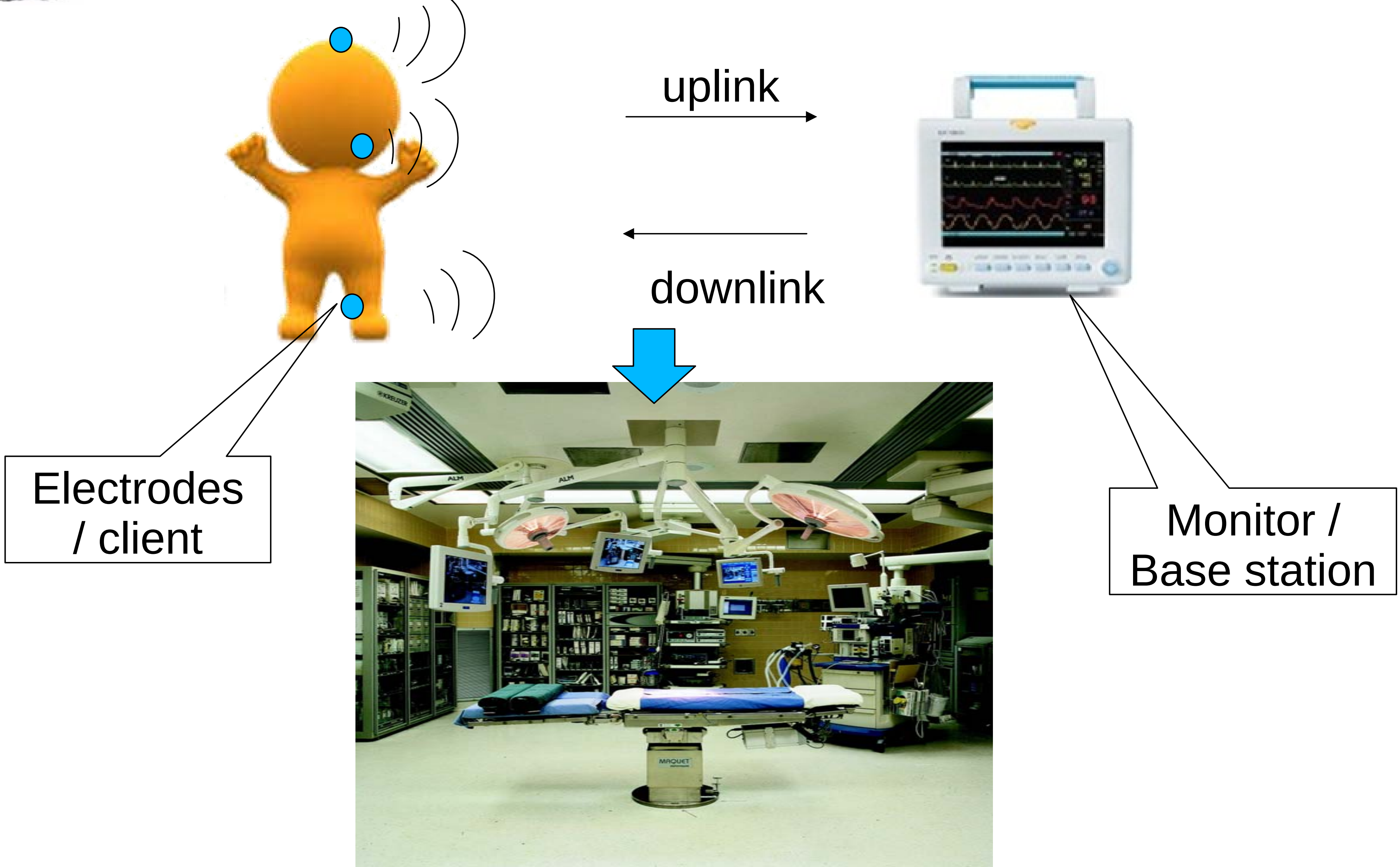
Risk of tripping over wires



Wired Monitoring

(photos from http://www.mdpnp.org )

# Advantages of WBAN based medical parameter monitoring



uplink

downlink

Electrodes / client

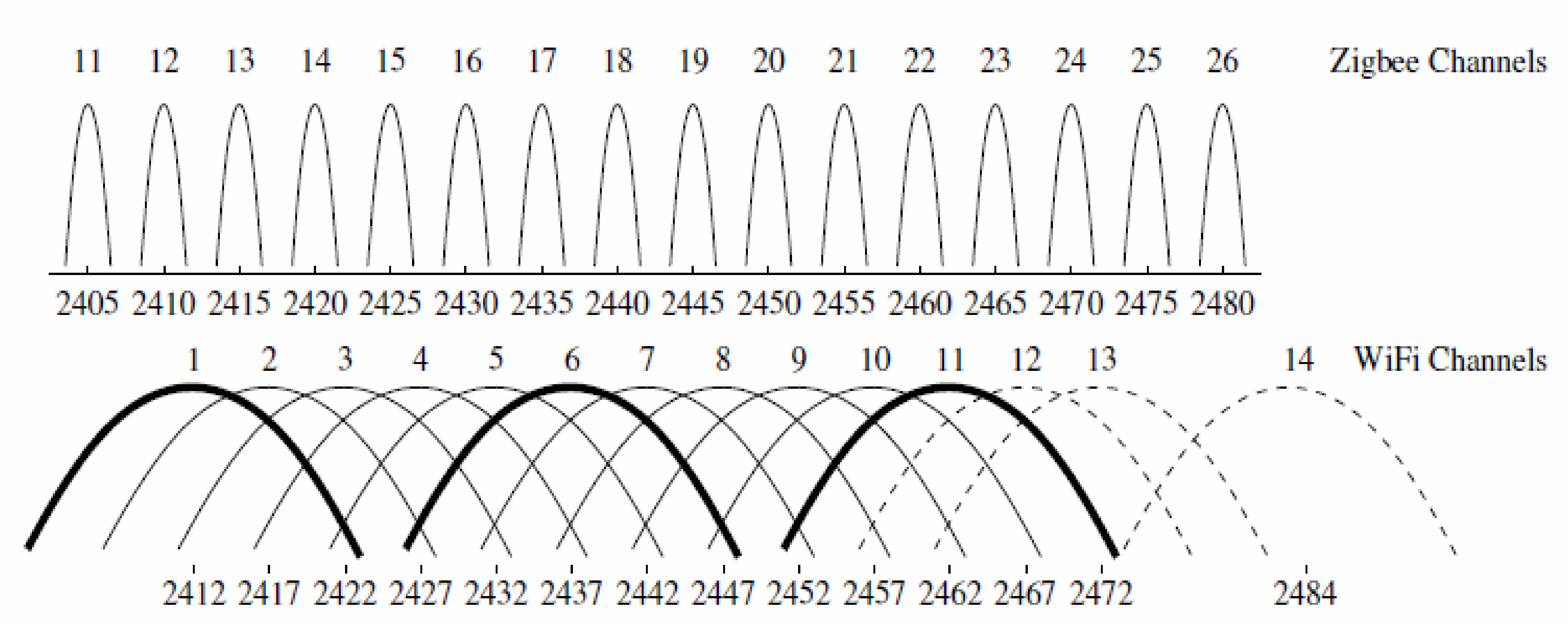
Monitor / Base station

# Medical WBAN Features

- Low duty cycle
  - Typical sampling rate < 300Hz [physionet]
  - Wakeup on demand
- Low data rate ~ 500Kbps [ieee15.6]
- Low transmit power  < 1mW [ieee15.6]
- Disparate Delay requirements
  - Electro-Cardio Graph (ECG): < 500ms [chevrollier05]
  - Body temperature monitoring: several seconds [chipara10]
- Single-Hop centralized WBAN is the preferred architecture

Emerging standard: ZigBee WBAN with centralized polling

# WiFi Co-Channel Interference is a major threat to WBAN [wang11]



Zigbee channels vs. 802.11b WiFi channels [liang10]

# WiFi Co-Channel Interference is a major threat to WBANs

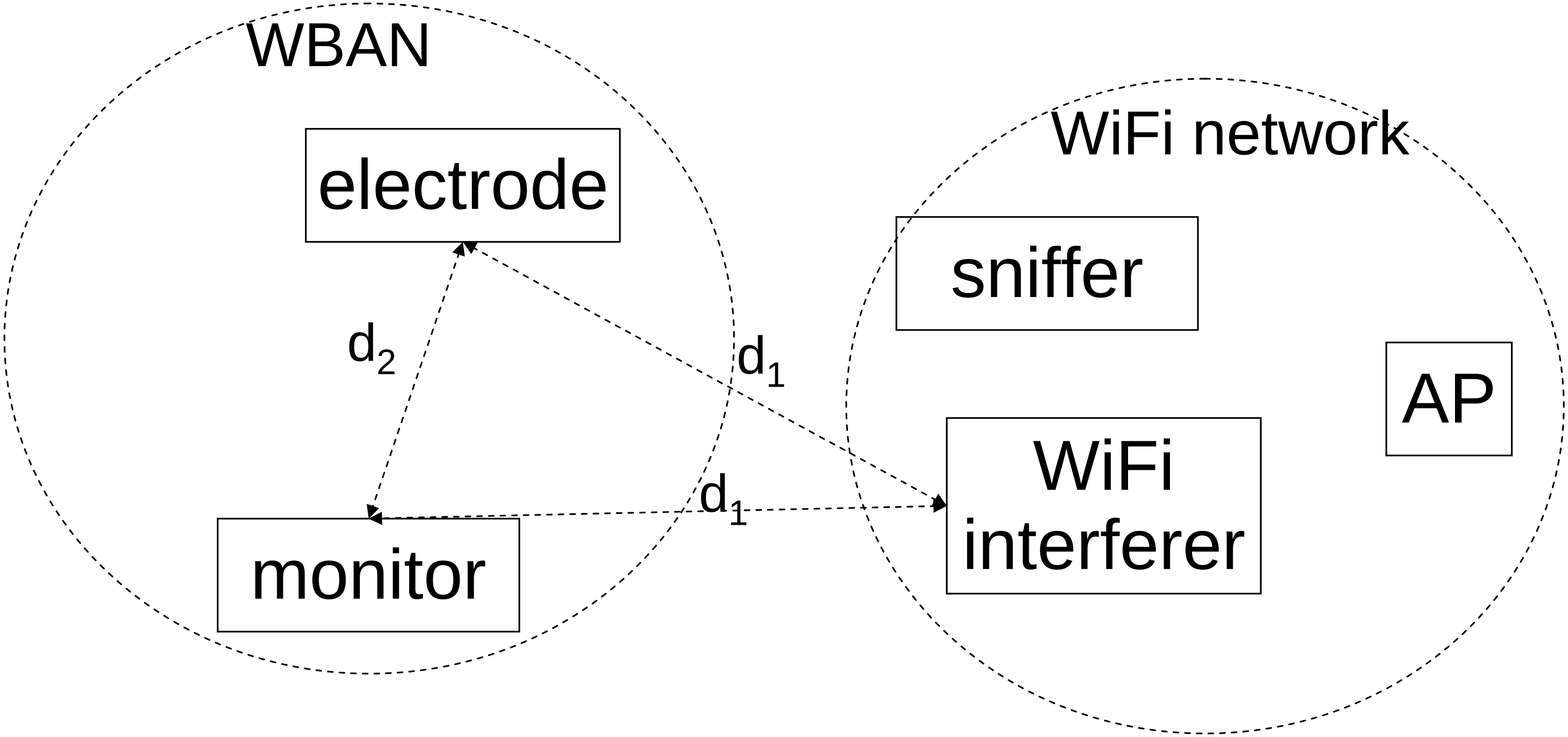
## Power asymmetry [huang10]

- Typical WiFi power $\approx$ 30mW
- Typical Zigbee (Bluetooth, IEEE 802.15.6 etc.) power $\leqslant$ 1mW

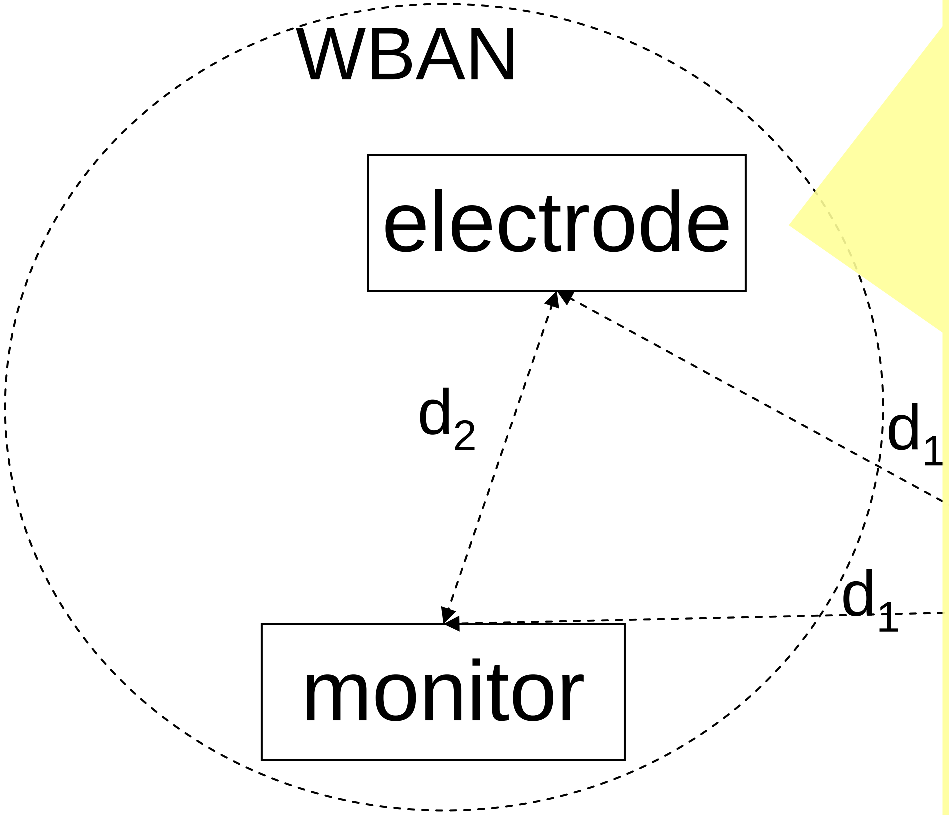
## MAC asymmetry [huang10][gummadi07]

- Many WiFi device use *Carrier Sense* (CS) based *Clear Channel Assessment* (CCA). Such WiFi devices do not back off to Zigbee.
- Many Zigbee uses *Energy Detection* (ED) CCA to assess the channel. Zigbee backs off to WiFi.

# Our experiment confirms the threat of WiFi to WBANs



# Our experiment confirms the threat of WiFi to WBANs

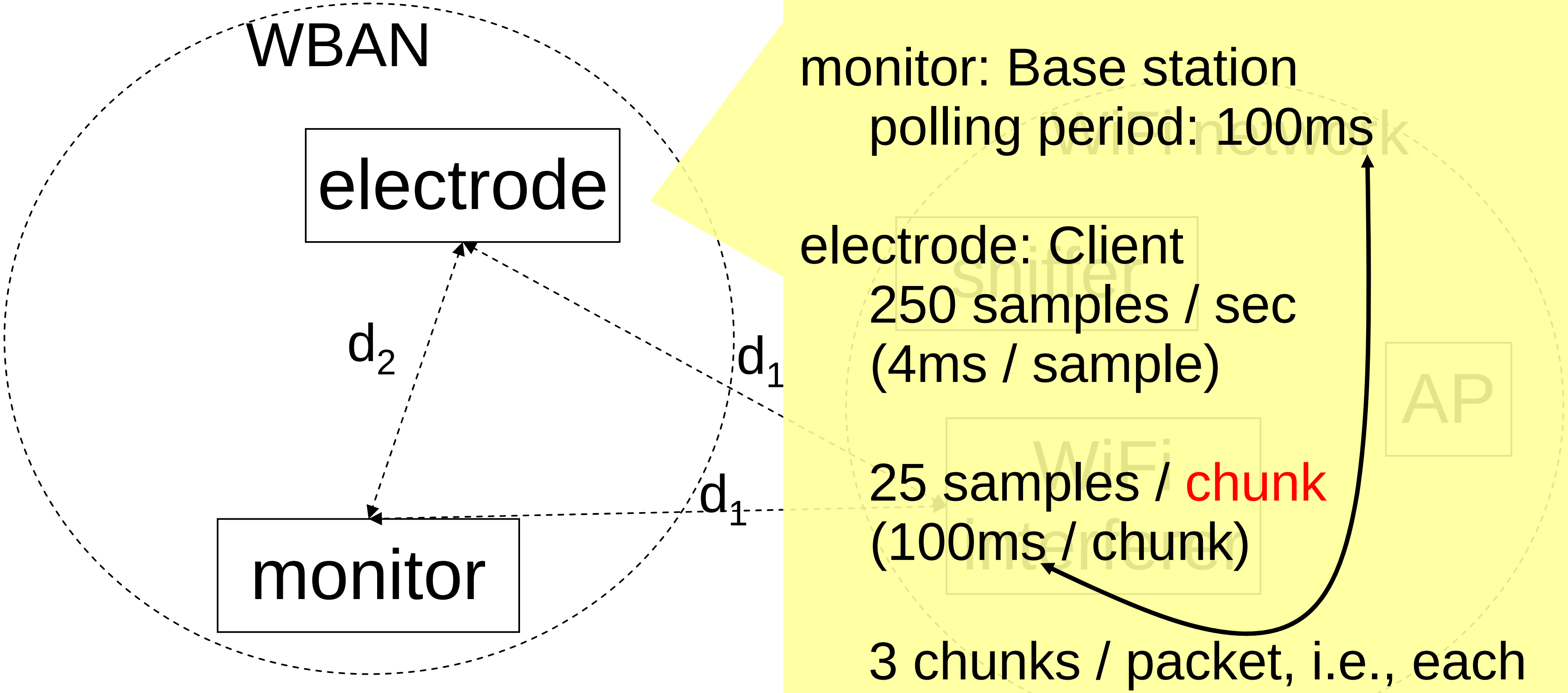


WBAN

monitor: Base station
- polling period: 100ms

electrode: Client
- 250 samples / sec (4ms / sample)
- 25 samples / chunk (100ms / chunk)
- 3 chunks / packet, i.e., each chunk is retransmitted 3 times (costs ≤4ms to send a packet)

# Our experiment confirms the threat of WiFi to WBANs



WBAN

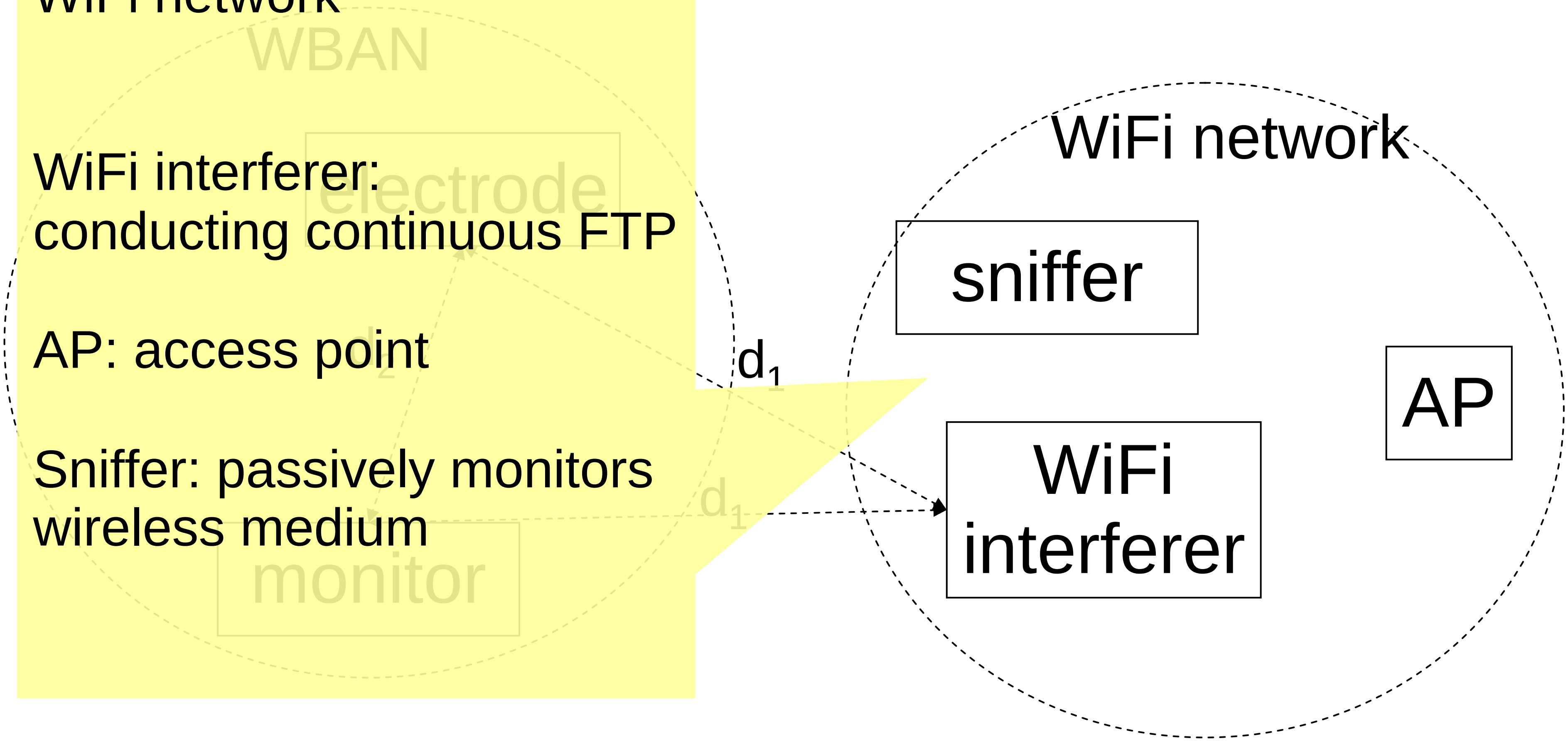
monitor: Base station
polling period: 100ms

electrode: Client
250 samples / sec
(4ms / sample)

25 samples / chunk
(100ms / chunk)

3 chunks / packet, i.e., each chunk is retransmitted 3 times
(costs ≤4ms to send a packet)

# Our experiment confirms the threat of WiFi to WBANs



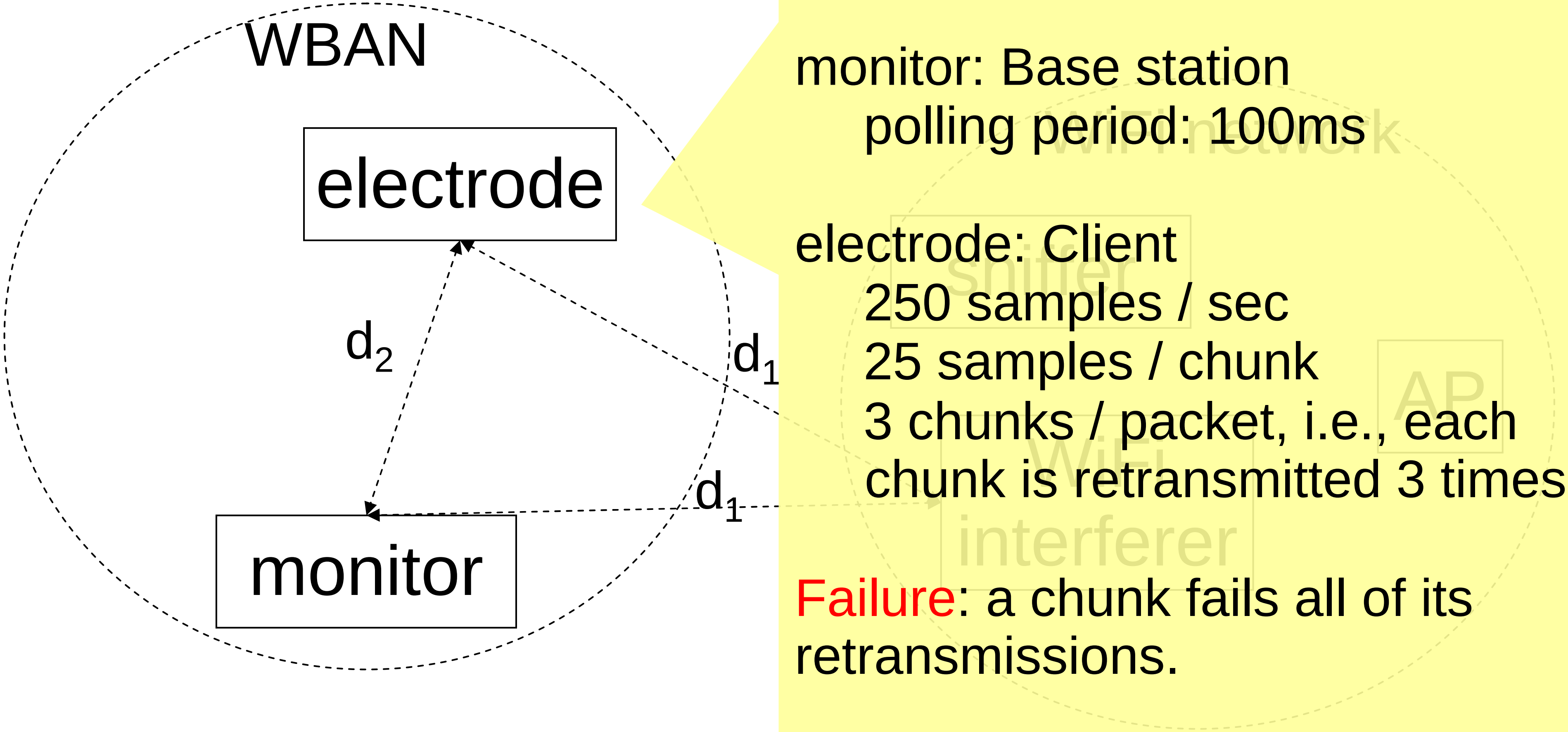
WiFi network

WiFi interferer: conducting continuous FTP

AP: access point

Sniffer: passively monitors wireless medium

# Our experiment confirms the threat of WiFi to WBANs



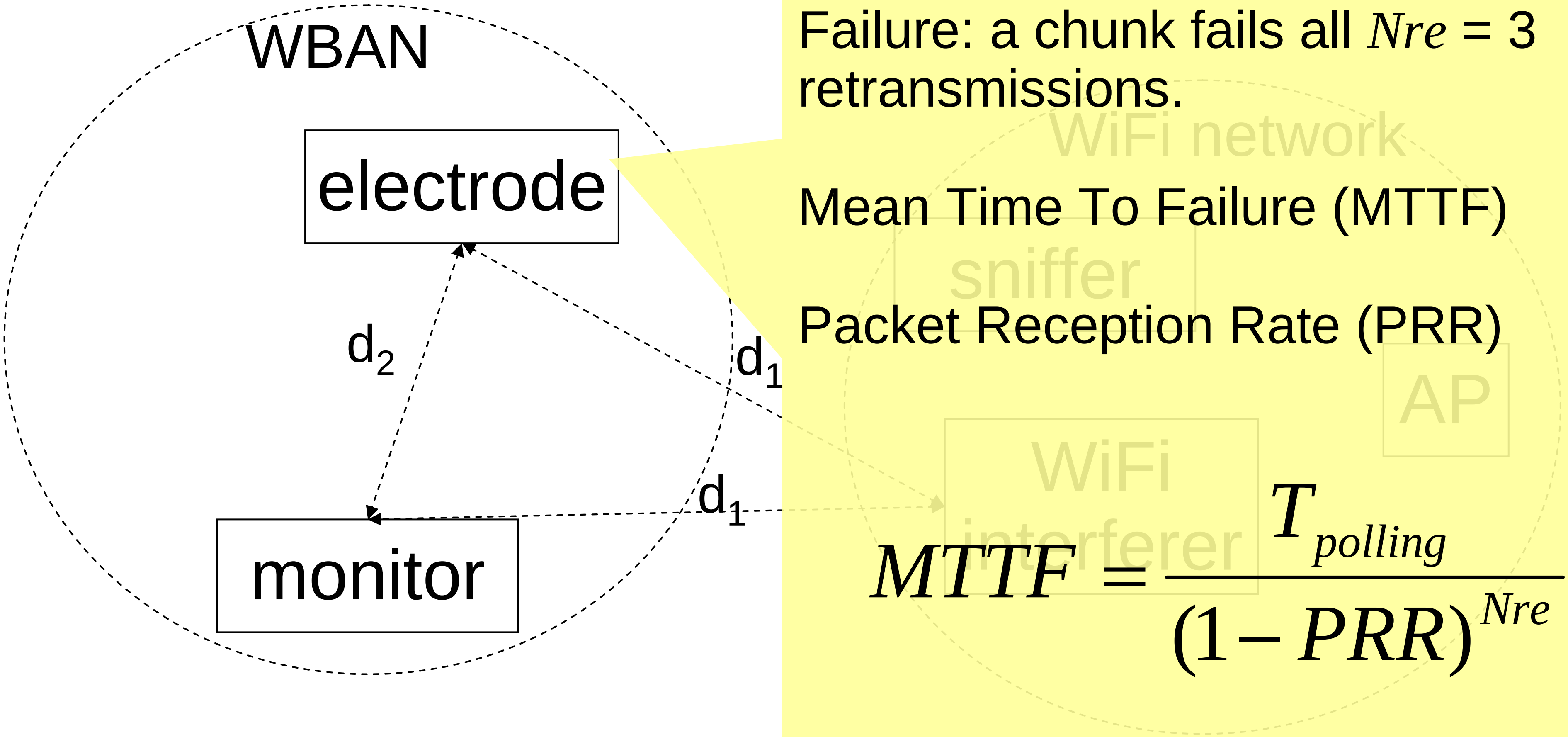
WBAN

monitor: Base station
polling period: 100ms

electrode: Client
250 samples / sec
25 samples / chunk
3 chunks / packet, i.e., each chunk is retransmitted 3 times

Failure: a chunk fails all of its retransmissions.

# Our experiment confirms the threat of WiFi to WBANs



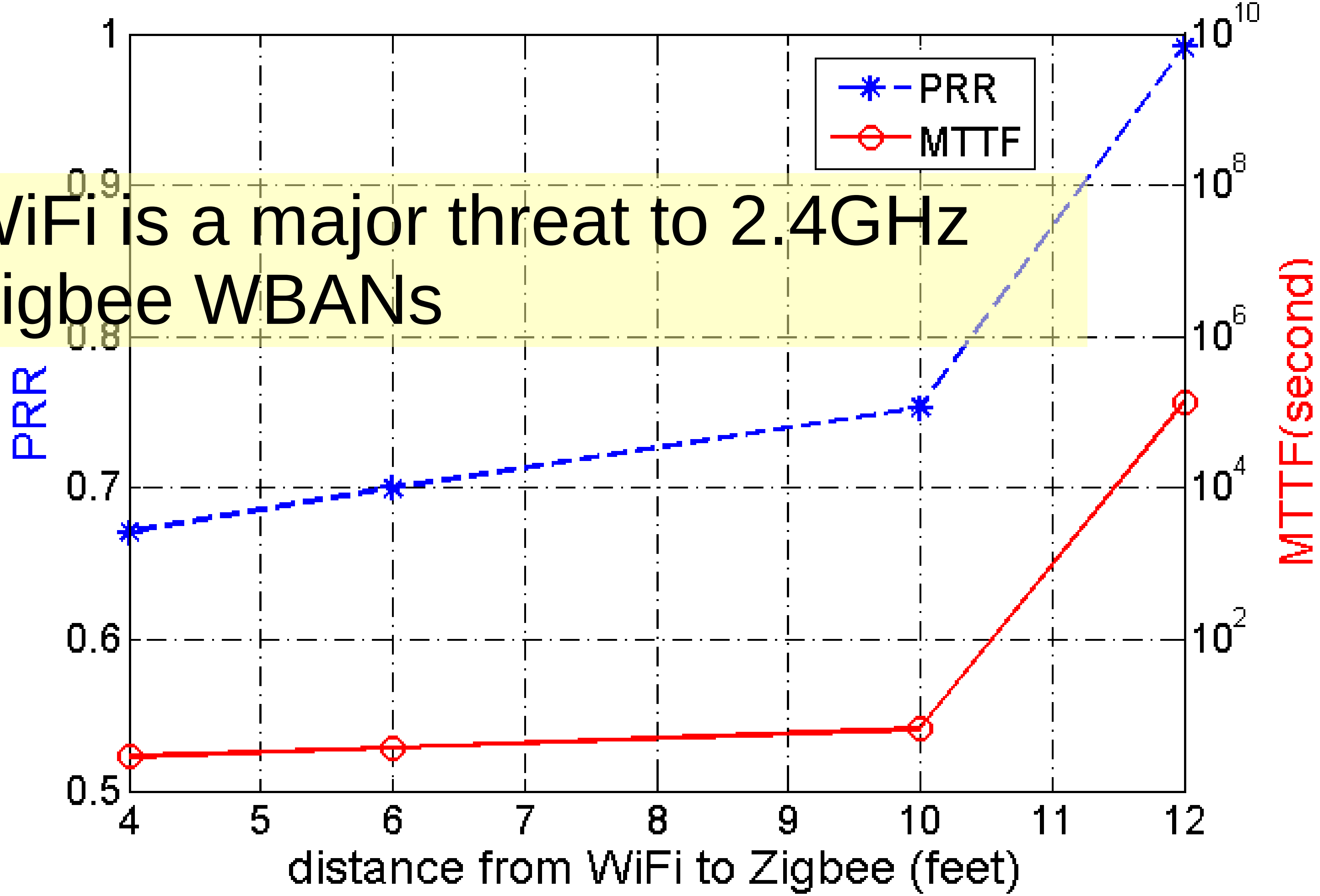
Failure: a chunk fails all $Nre = 3$ retransmissions.

Mean Time To Failure (MTTF)

Packet Reception Rate (PRR)

$$MTTF = \frac{T_{polling}}{(1-PRR)^{Nre}}$$

# Zigbee WBAN performance under WiFi interference



WiFi is a major threat to 2.4GHz Zigbee WBANs

# Content

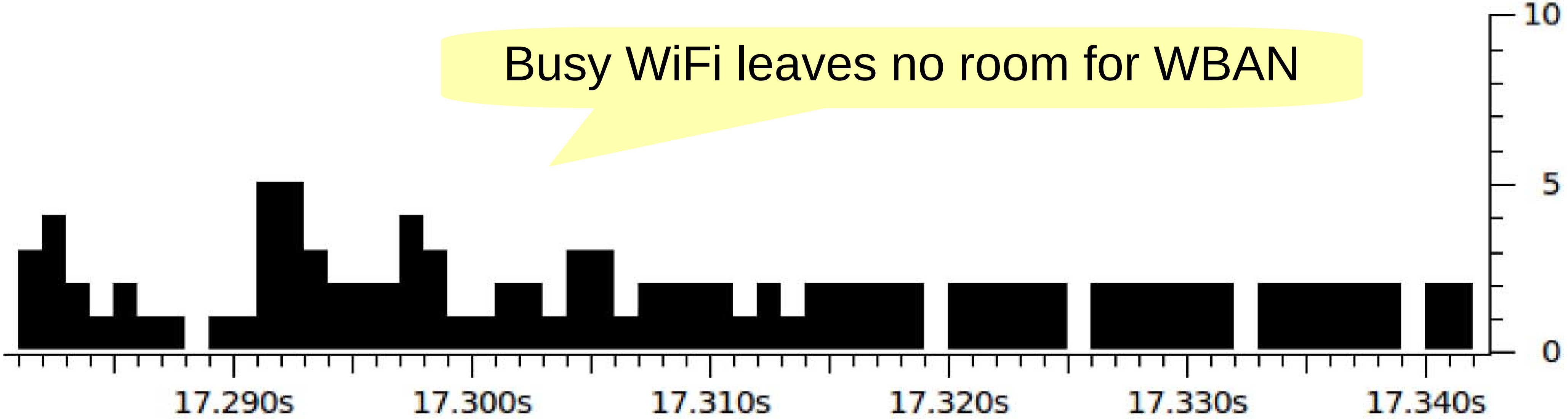
Demand

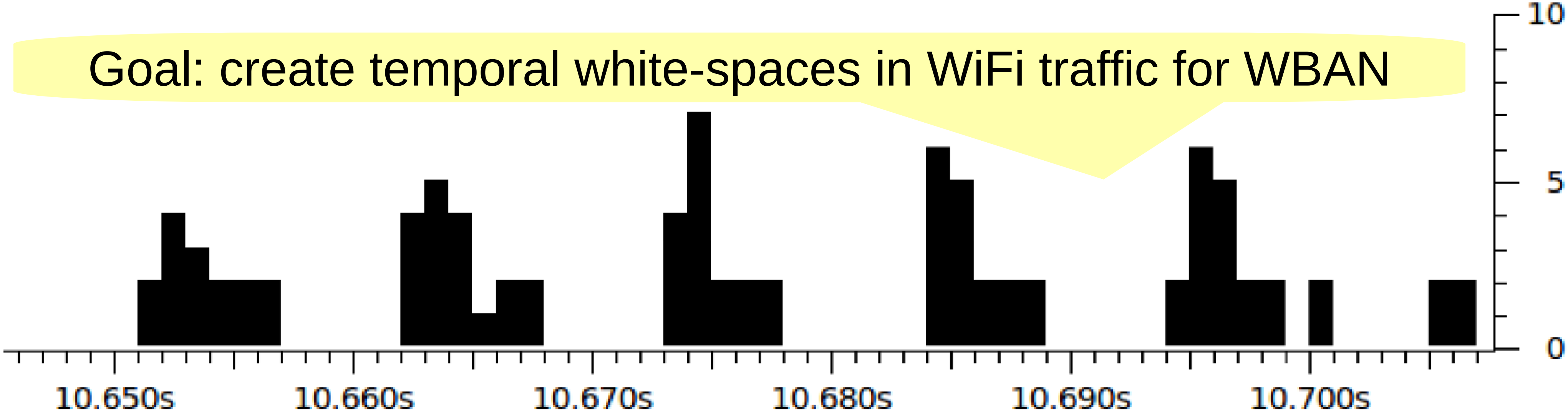
Proposed Framework

Evaluation

Related Work

# “Engineer” temporal white-spaces between WiFi transmissions to allow WBAN transmissions


Busy WiFi leaves no room for WBAN


Goal: create temporal white-spaces in WiFi traffic for WBAN

# Policing: prohibit the transmissions of WiFi interferers in a well-controlled manner

Shield WBAN transmissions in space and time

# Two mechanisms

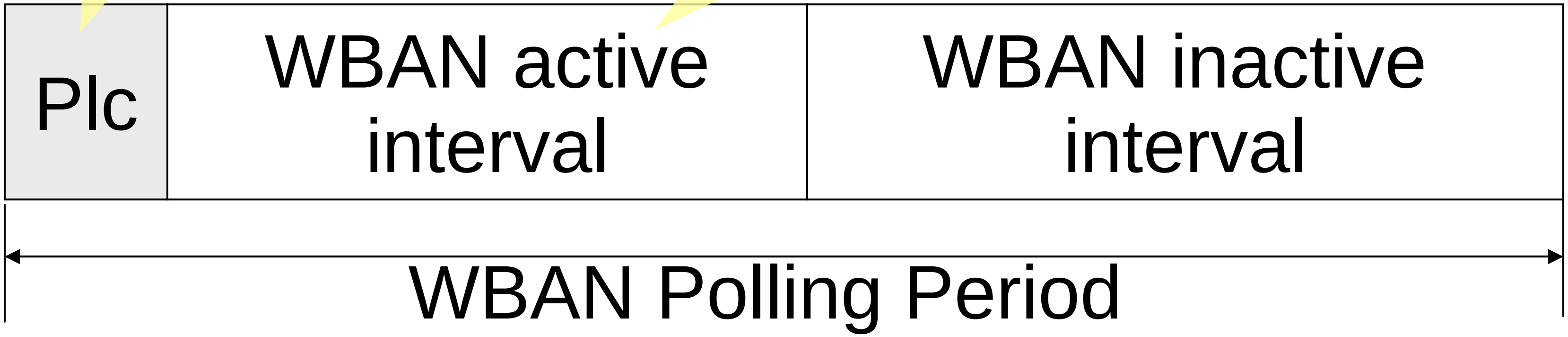
Utilizing the carrier sensing mechanisms in WiFi

- Fake-PHY-Hdr
- DSSS-Nulling

# Fake-PHY-Hdr: temporal scheme

Fake-PHY-Hdr *policing signal* (Plc):
claims a (fake) WiFi packet with duration
= WBAN active interval

Includes:
Downlink beacon
Uplink data



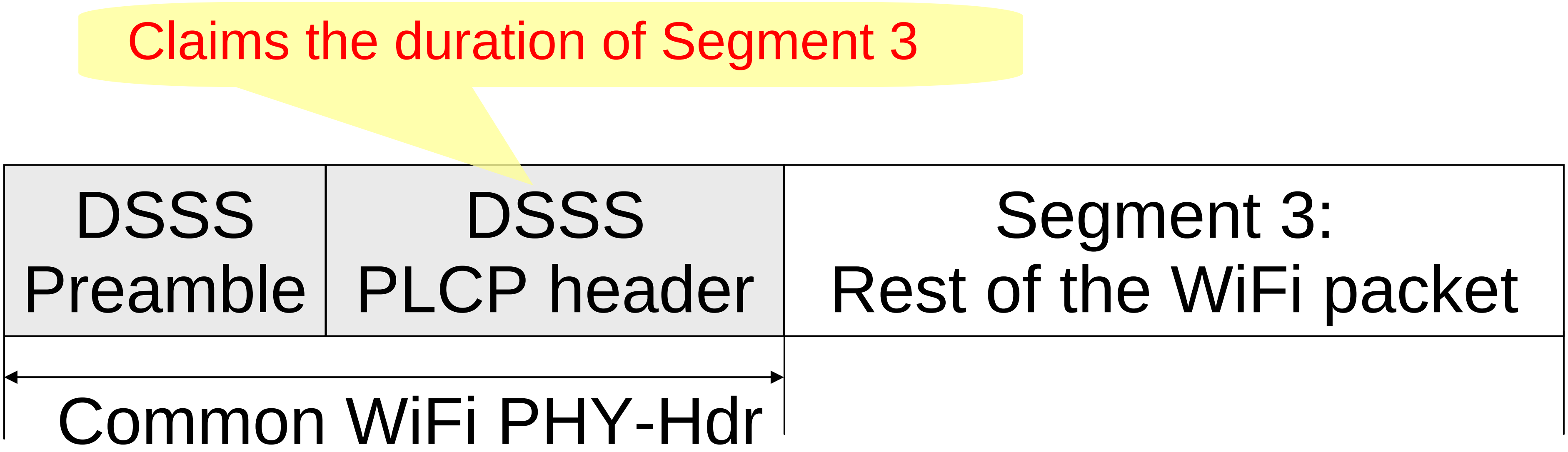
Plc

WBAN active interval

WBAN inactive interval

WBAN Polling Period

# 802.11b/g/n recognize the following PHY-Hdr.



Claims the duration of Segment 3

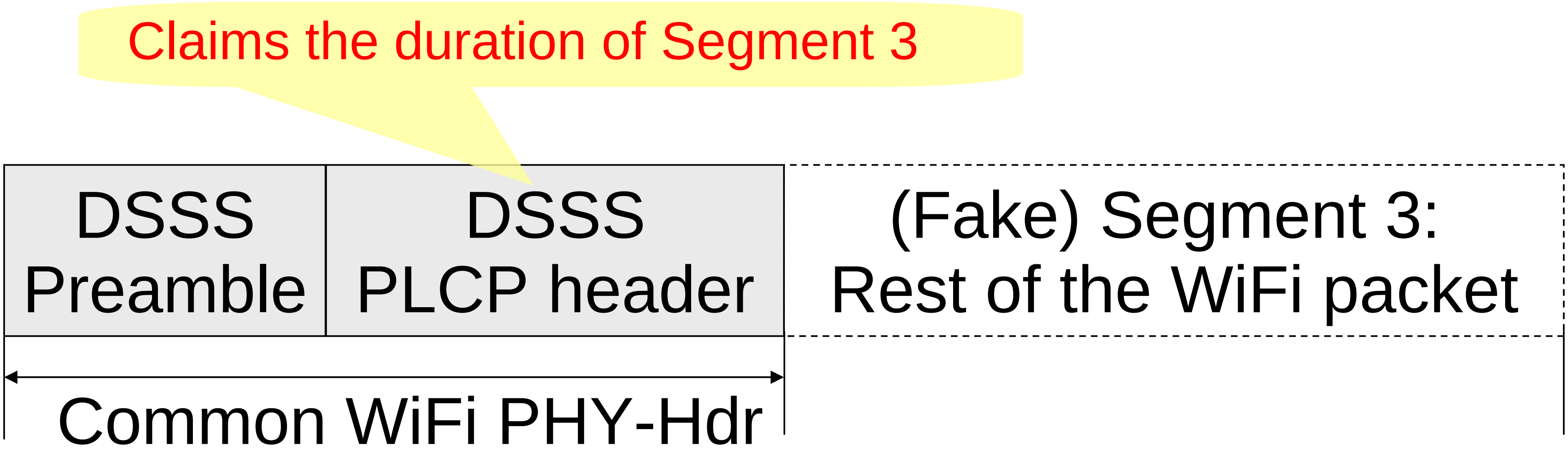
DSSS Preamble

DSSS PLCP header

Segment 3: Rest of the WiFi packet

Common WiFi PHY-Hdr

# WiFi devices will back off for the claimed (fake) Segment 3



Claims the duration of Segment 3

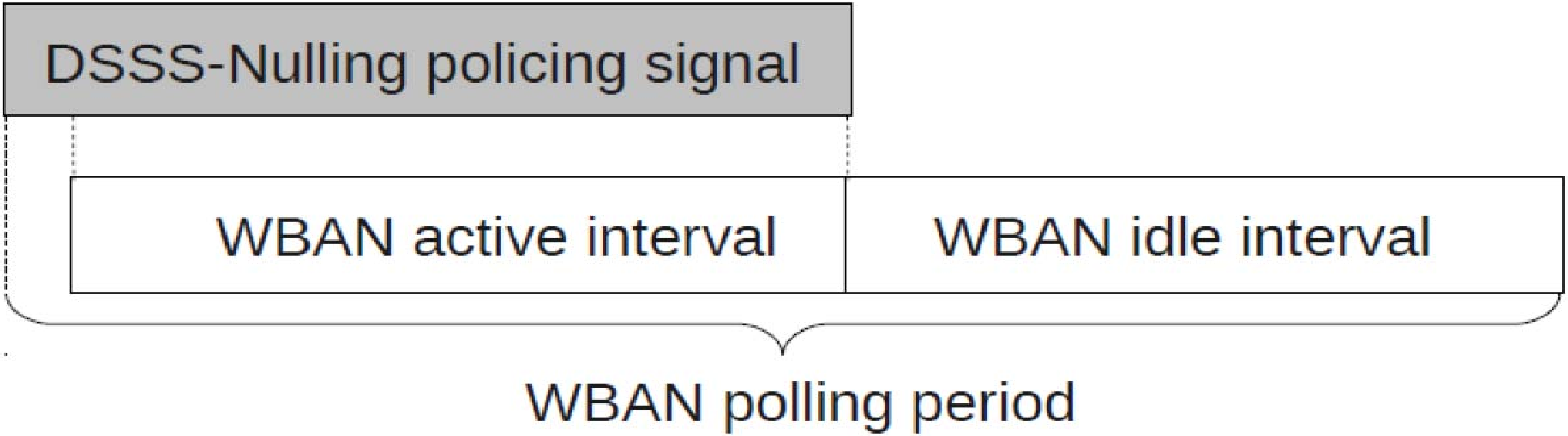
DSSS Preamble

DSSS PLCP header

(Fake) Segment 3: Rest of the WiFi packet

Common WiFi PHY-Hdr

# DSSS-Nulling: repeated DSSS preamble



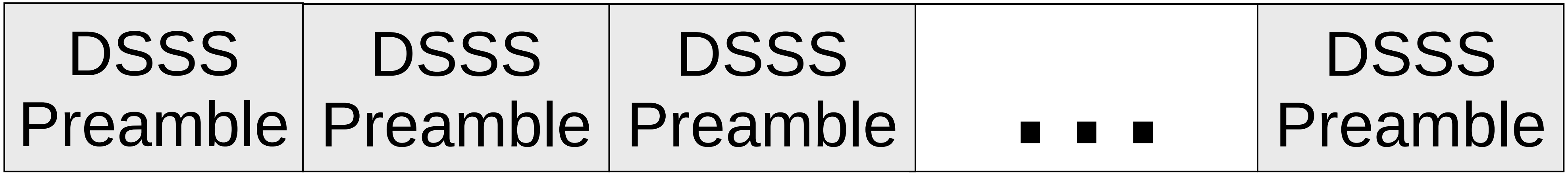
DSSS-Nulling policing signal

WBAN active interval

WBAN idle interval

WBAN polling period

Continuously repeated DSSS Preambles



DSSS Preamble

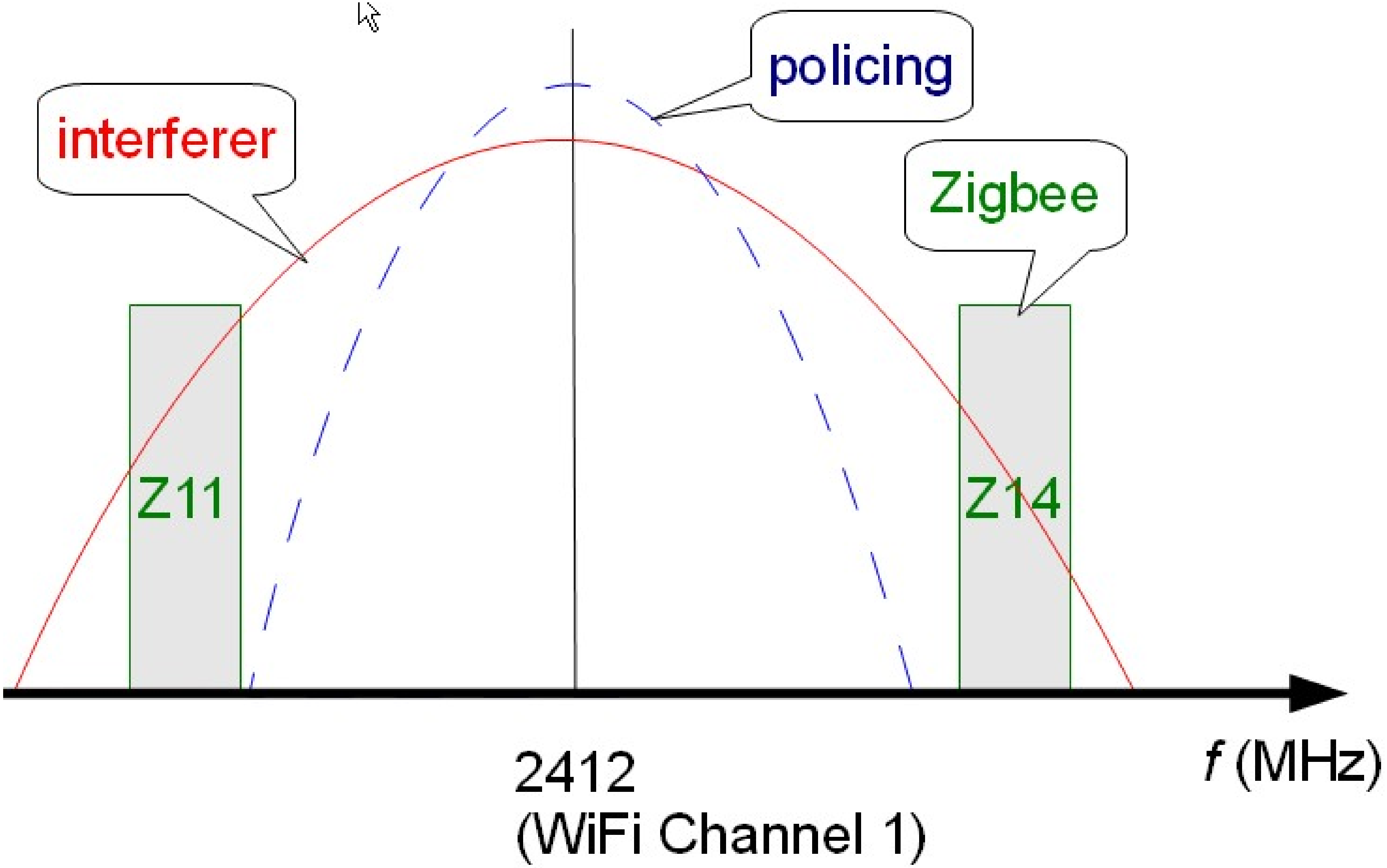
DSSS Preamble

DSSS Preamble

■ ■ ■

DSSS Preamble

# Band-rejection filtered DSSS-Nulling policing signal



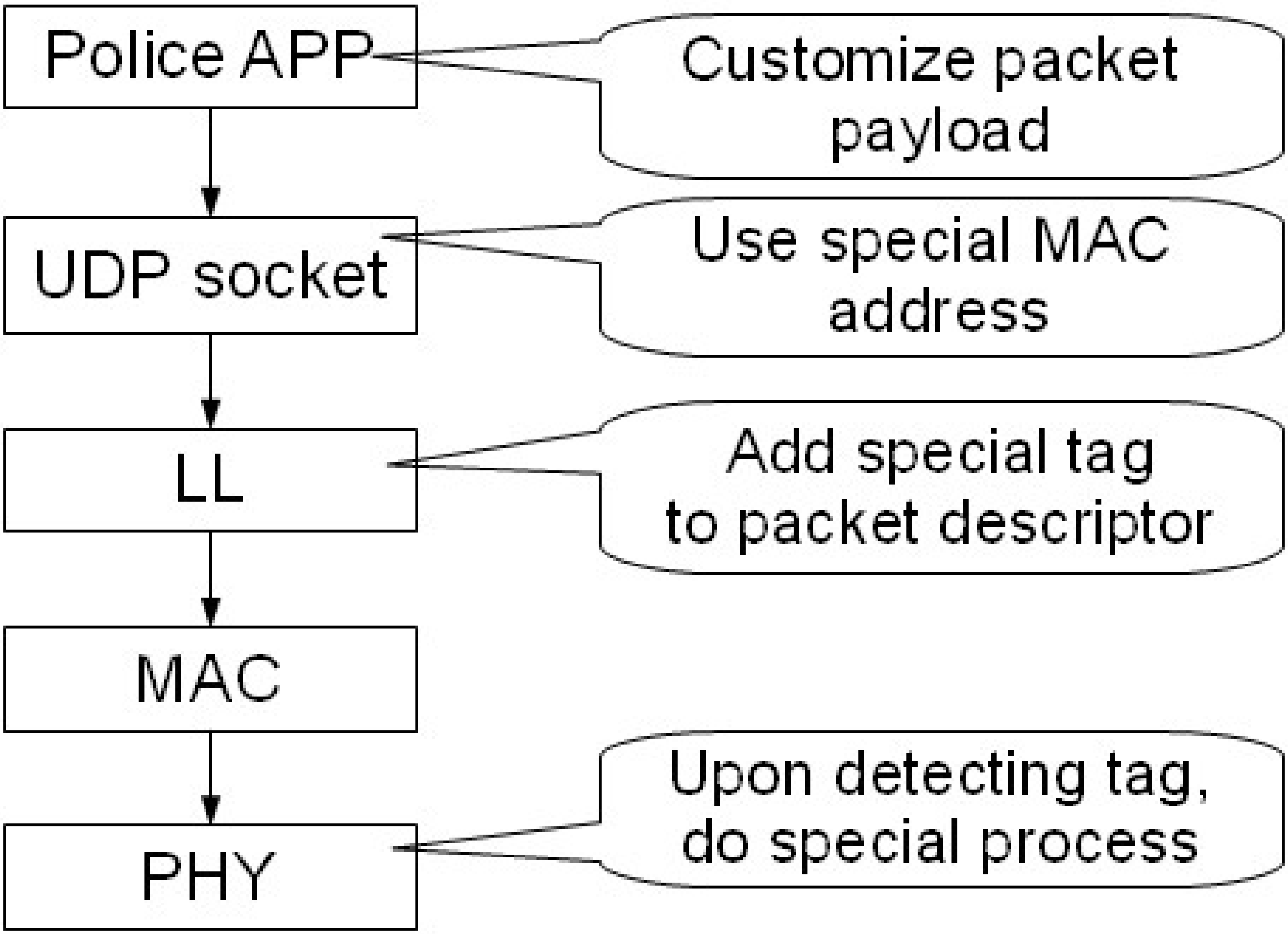
Spectrum illustration of interferer, policing and Zigbee signal

# Implementation details

Hardware platform: Microsoft SORA [tan11]

- A Software Defined Radio platform
- Multi-core based real-time signal processing
- Support PCIe bus
- open source WiFi driver

# Transmission of policing frames



# Content

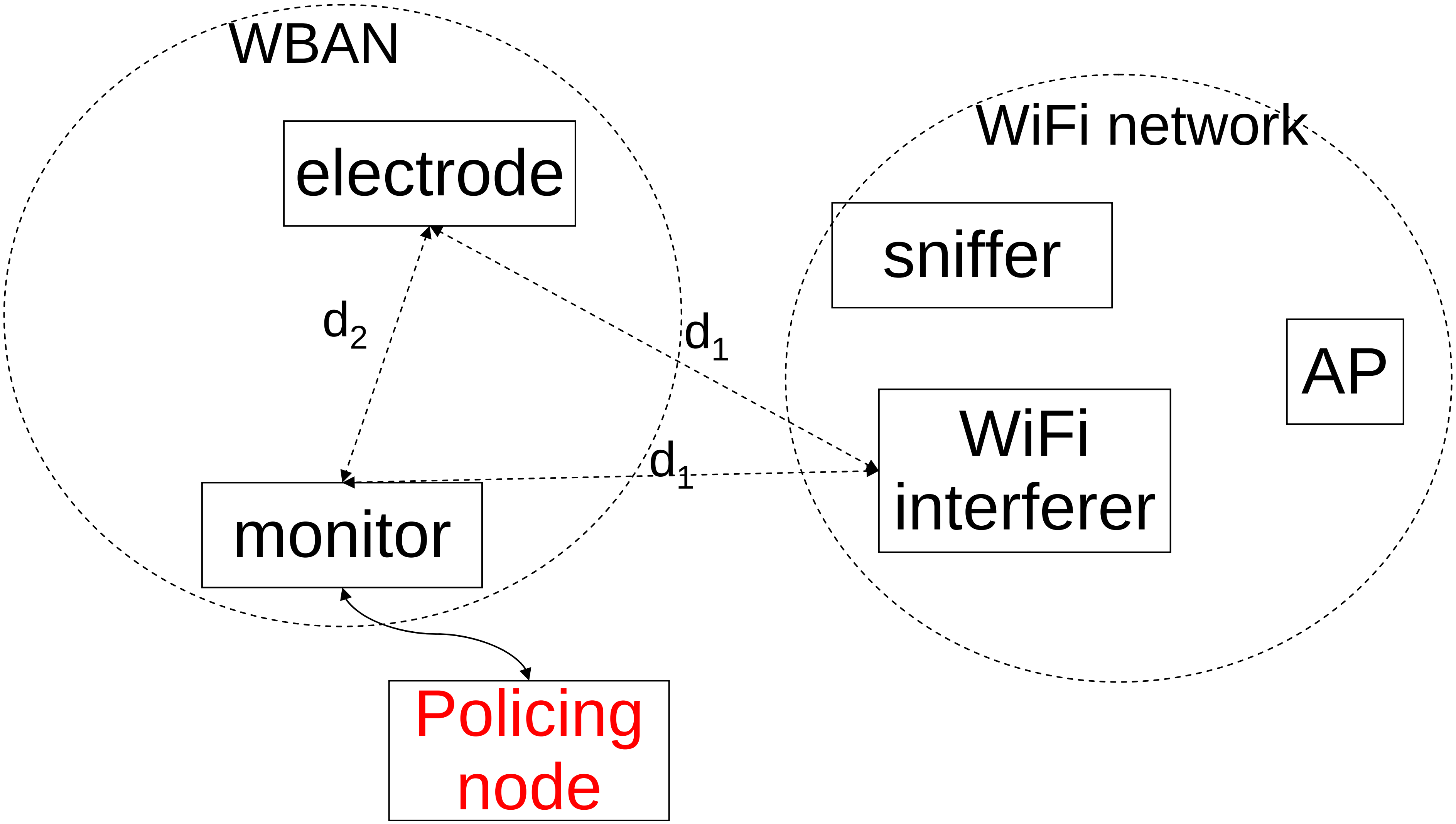
Demand

Proposed Framework

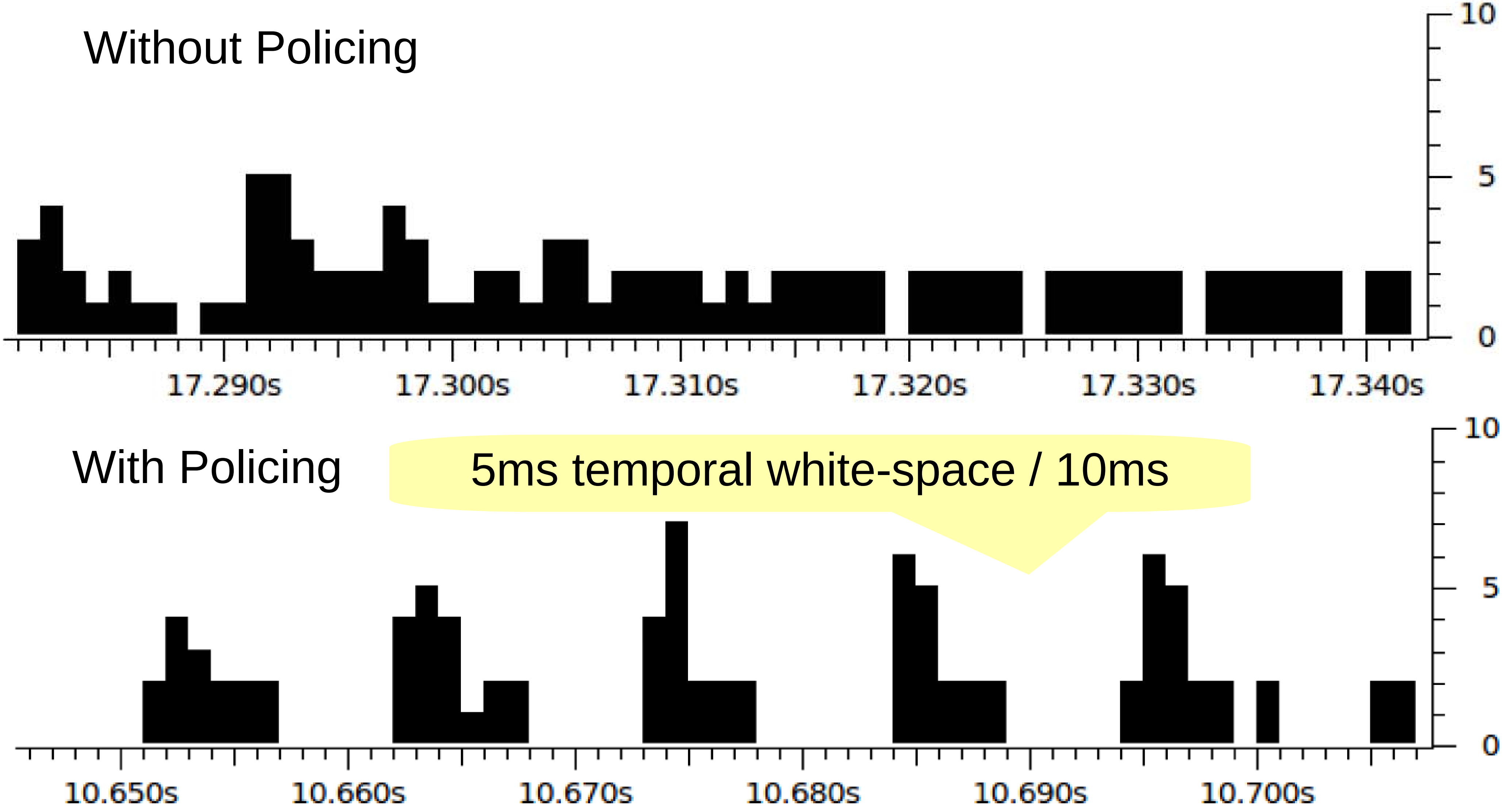
Evaluation

Related Work

The policing node implements the two policing mechanisms



# Temporal whitespaces due to WiCop

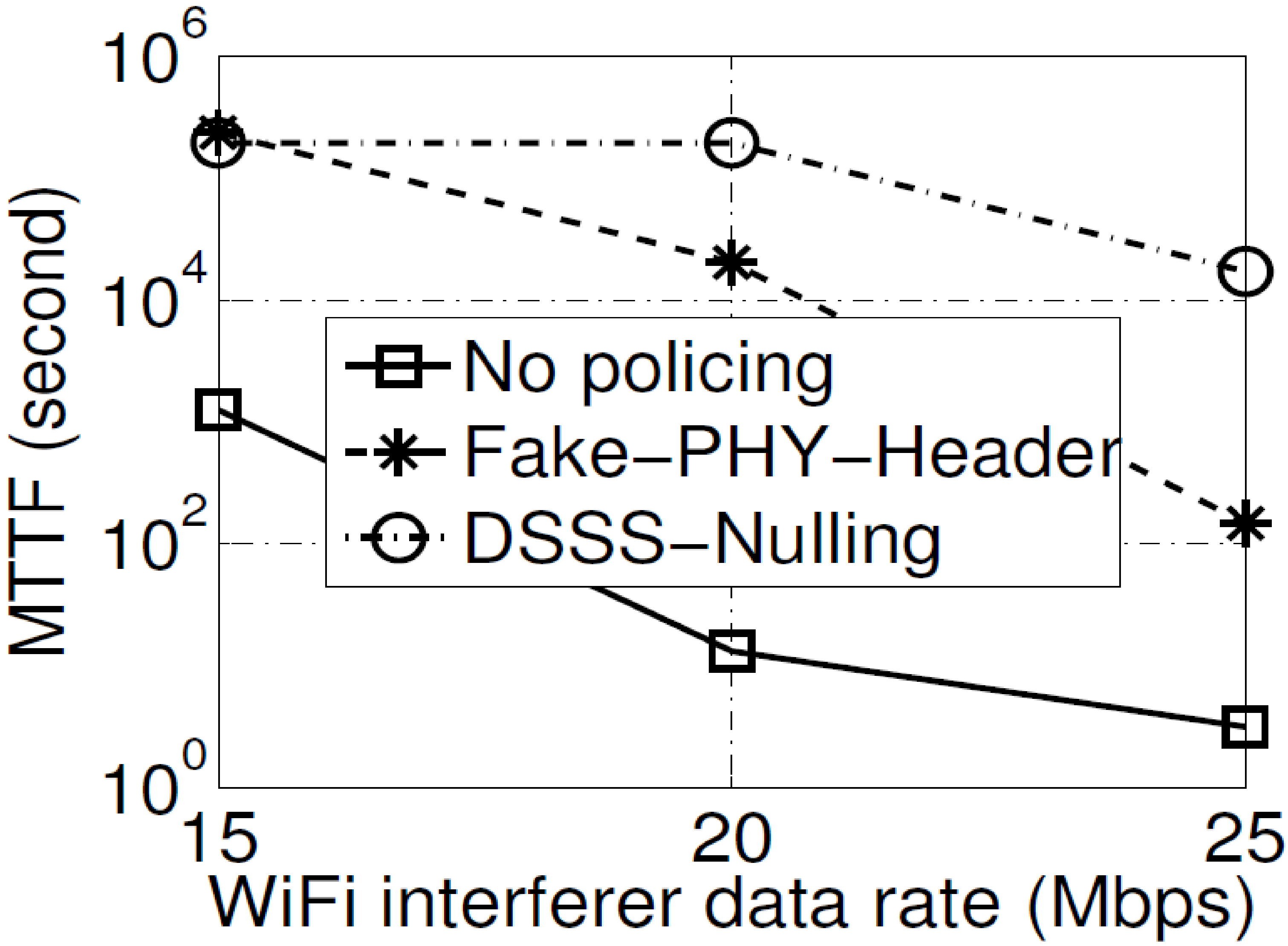


Without Policing

With Policing

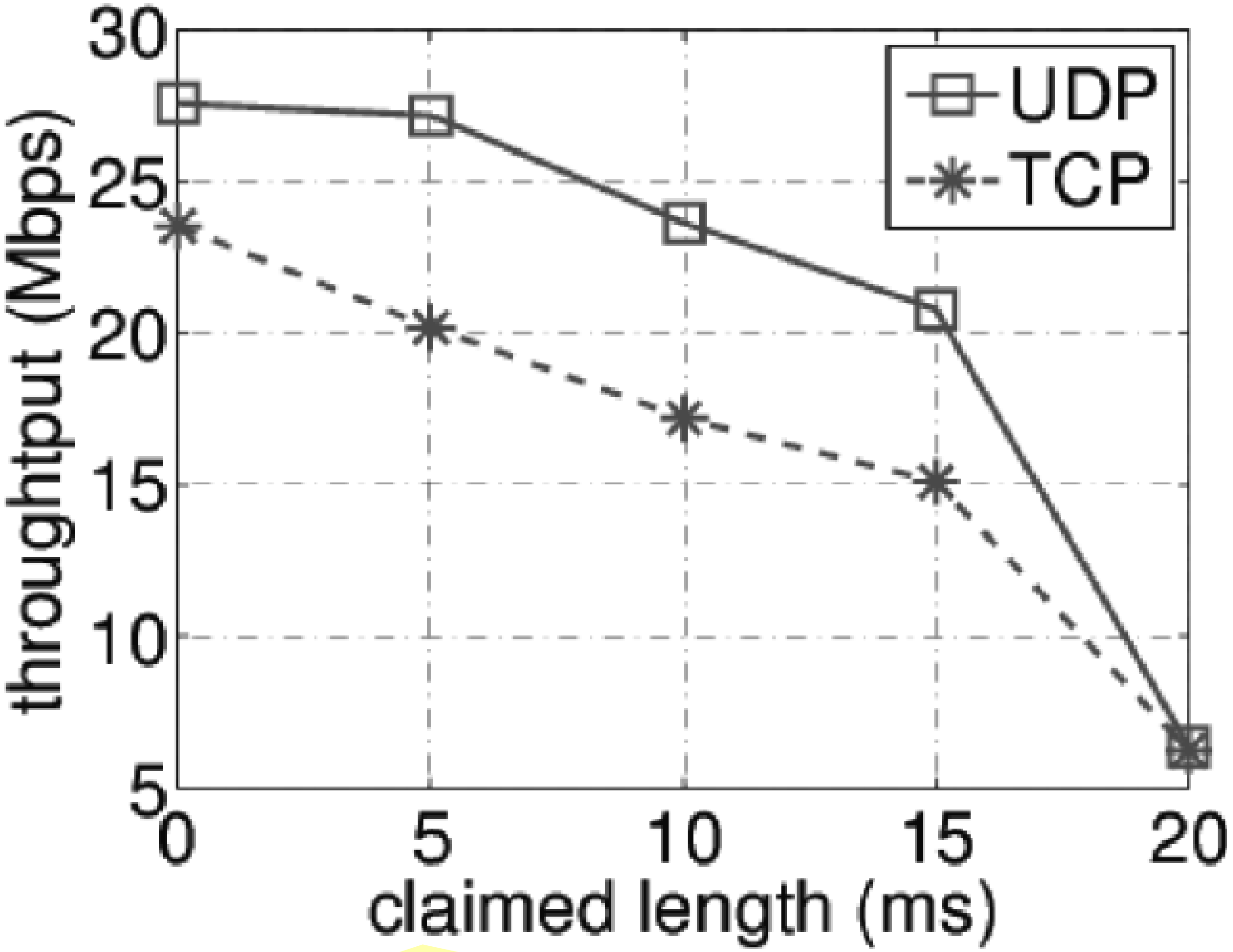
5ms temporal white-space / 10ms

# Mean time to failure



# Moderate Impact on WiFi traffic

WiFi throughput degradation



Use Fake PHY Hdr to claim a white space
WBAN polling period is 25ms

# Content

Demand

Proposed Framework

Evaluation

Related Work

# Methods protecting Zigbee from WiFi

Exploiting (instead of engineering) temporal white-spaces of WiFi traffic [liang10][huang10]

Exploiting (instead of engineering) spectral white-spaces of WiFi traffic [won05][musaloiu-e08]

Use fake RTS to protect Zigbee [hou09]: pros and cons

# WiFi PHY/MAC security

Continuously transmitting WiFi preamble [wullems04].

Fake de-auth packet and fake virtual carrier sense [bellardo94].

DIFS waiting jamming and acknowledge corruption [thuente06]

Partial band jamming [park03] [mishra06] [karhima04]

# Conclusion

WiCop significantly improves WBAN performance

Controlled impact on WiFi

DSSS-Nulling is more effective than Fake-PHY-Hdr in improving MTTF, mainly due to repeated transmissions of DSSS preamble

Fake-PHY-Hdr incurs much less overhead than DSSS-Nulling

# Demo Video

# Thank You!

Questions?

# References

[bellardo94] J. Bellardo et al., “802.11 denial-of-service attacks: real vulnerabilities and practical solutions,” in Proc. of 12th USENIX Security Symposium, v12, 1994.

[chevrollier05] N. Chevrollier et al., On the Use of Wireless Network Technologies in Healthcare Environments. http://citeseerx.ist.psu.edu

[chipara10] O. Chipara et al., “Reliable clinical monitoring using wireless sensor networks: experiences in a step-down hospital unit,” in Proc. of the 8th ACM Conf. on Embedded Networked Sensor Systems, 2010.

[gummadi07] R. Gummadi et al., “Understanding and mitigating the impact of RF interference on 802.11 networks,” in ACM SIGCOMM’07, 2007

[hou09] J. Hou et al., “Minimizing 802.11 interference on ZigBee medical sensors,” in BodyNets’09, 2009.

[huang10] J. Huang et al., “Beyond Co-existence: Exploiting WiFi White Space for ZigBee Performance Assurance,” in ICNP’10, Oct, 2010.

[ieee15.6] IEEE 802.15.6 standard for WBAN.

[karhima04] T. Karhima et al., “IEEE 802.11b/g WLAN tolerance to jamming,” in Military Communications Conference, 2004.

[liang10] C.-J. M. Liang et al., “Surviving Wi-Fi Interference in Low Power ZigBee Networks,” in Proc. of the 8th ACM Conf. on Embedded Networked Sensor Systems, 2010.

[mishra06] A. Mishra et al., “Partially overlapped channels not considered harmful,” in Proc. of the Joint Intl’ Conf. on Measurement and Modeling of Computer Systems, 2006.

# References

[musaloiu-e08] Razvan Musaloiu-E and Andreas Terzis "Minimising the effect of WiFi interference in 802.15.4 wireless sensor networks" International Journal of Sensor Networks, Issue: Volume 3, Number 1 / 2008, Pages: 43 - 54

[park03] J. Park et al., “Effect of partial band jamming on OFDM-based WLAN in 802.11g,” in Proc. of Acoustics, Speech, and Signal Processing, 2003.

[physionet] PhysioNet. http://www.physionet.org

[tan11] K. Tan et al., “SORA: high-performance software radio using general-purpose multicore processors,” in Comm. of the ACM, 54(5), Jan., 2011.

[thuente06] D. J. Thuente et al., “Intelligent jamming in wireless networks with applications to 802.11b and other networks,” in MILCOM’06, 2006.

[wang11] Y. Wang et al., “Evaluating the IEEE 802.15.6 2.4GHz WBAN proposal on medical multi-parameter monitoring under WiFi/Bluetooth interferences,” in Intl’ Journal of E-Health and Medical Communications, 2(3):48-62, Jul.-Sep., 2011.

[won05] Chulho Won; Jong-Hoon Youn; Ali, H.; Sharif, H.; Deogun, J.; , "Adaptive radio channel allocation for supporting coexistence of 802.15.4 and 802.11b," *Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd* , vol.4, no., pp. 2522- 2526, 25-28 Sept., 2005

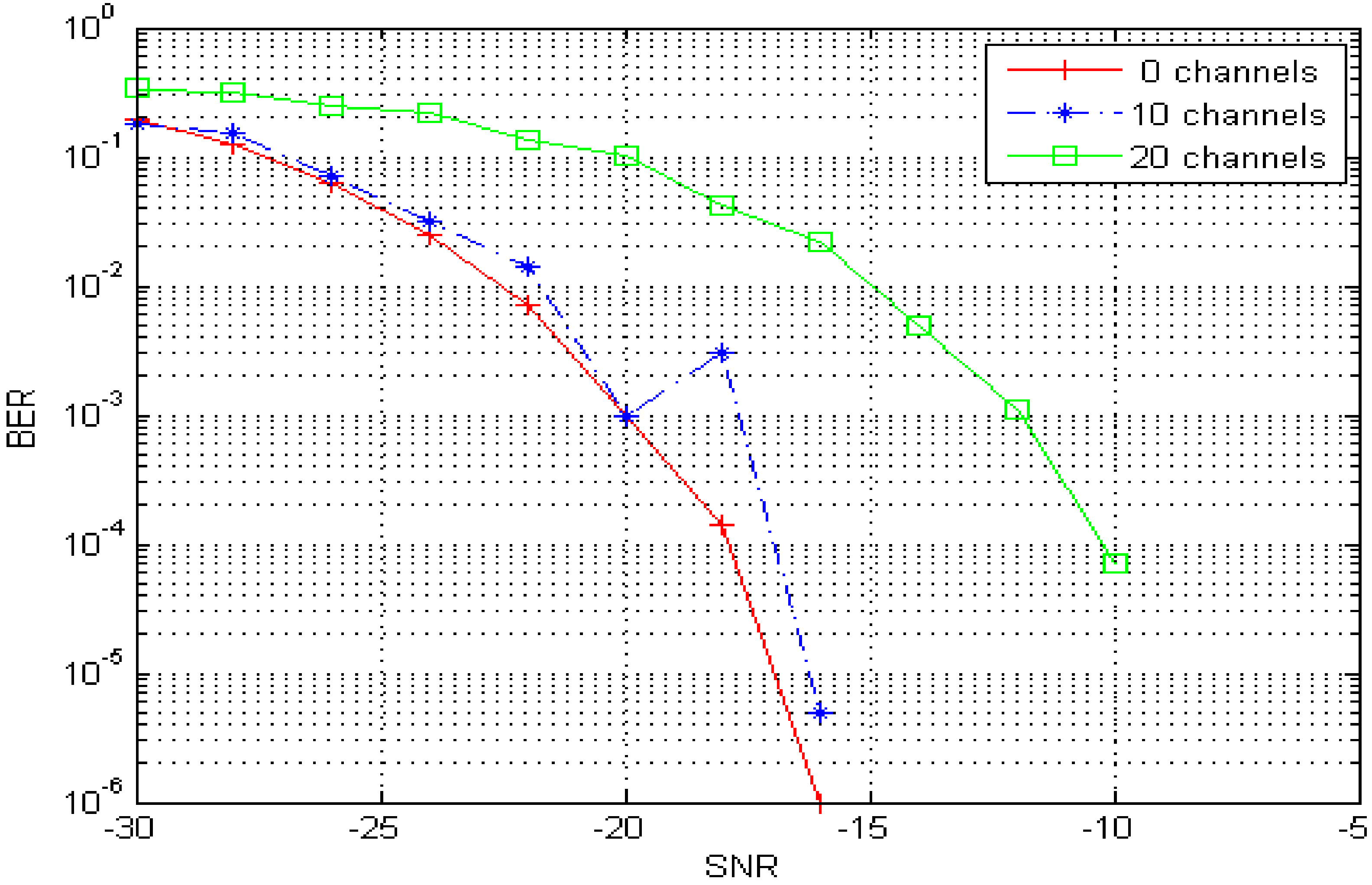
[wullems04] C. Wullems et al., “A trivial denial of service attack on IEEE 802.11 direct sequence spread spectrum wireless LANs,” in Wireless Telecommunications Symposium, 2004.

backup

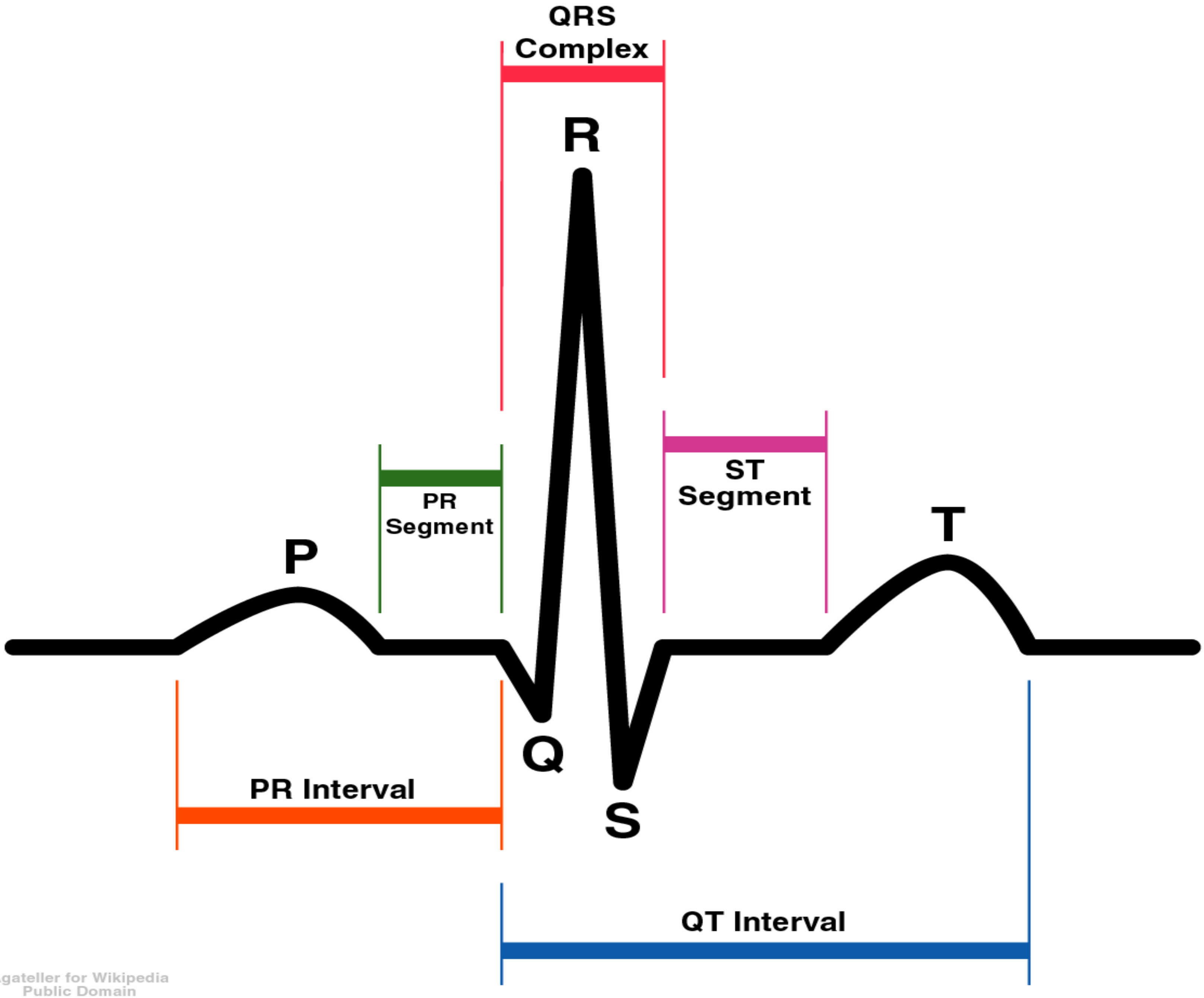
# 2.4GHz wireless scheme candidates to carry out WBAN

| candidates | Merits & demerits |
|---|---|
| WiFi | High data rate & big power |
| Bluetooth | Low power & expensive, persistent connection[Hou09] |
| Zigbee √ | Low cost, low power, long battery life[Hou09] |
| IEEE 802.15.6 2.4GHz Proposal √ | Low cost, low power, long battery life & being developed [15.6NB] |

# "DSSS Nulling" can hold 10 802.15.6 channels

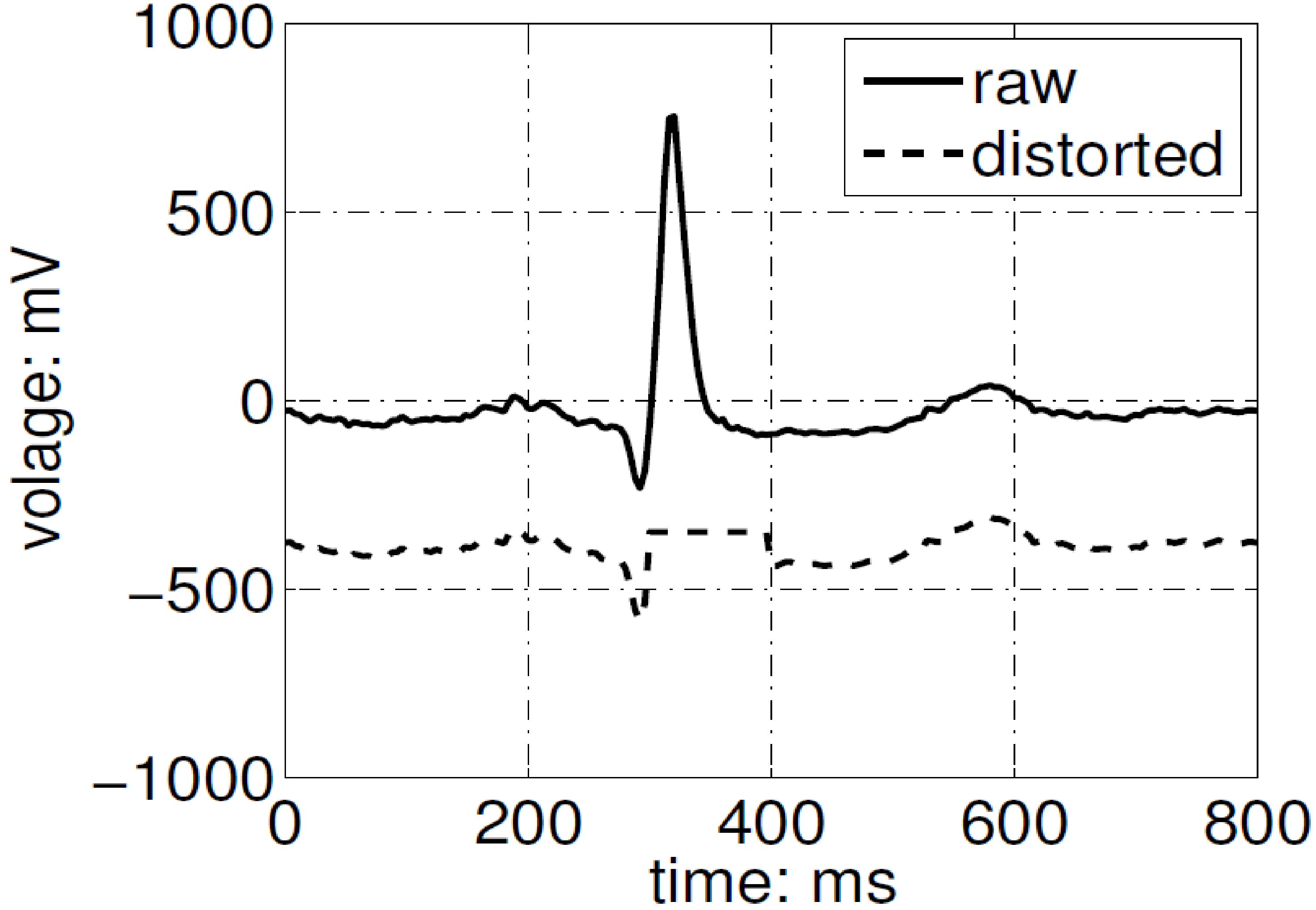


# ECG trace sample [wiki]

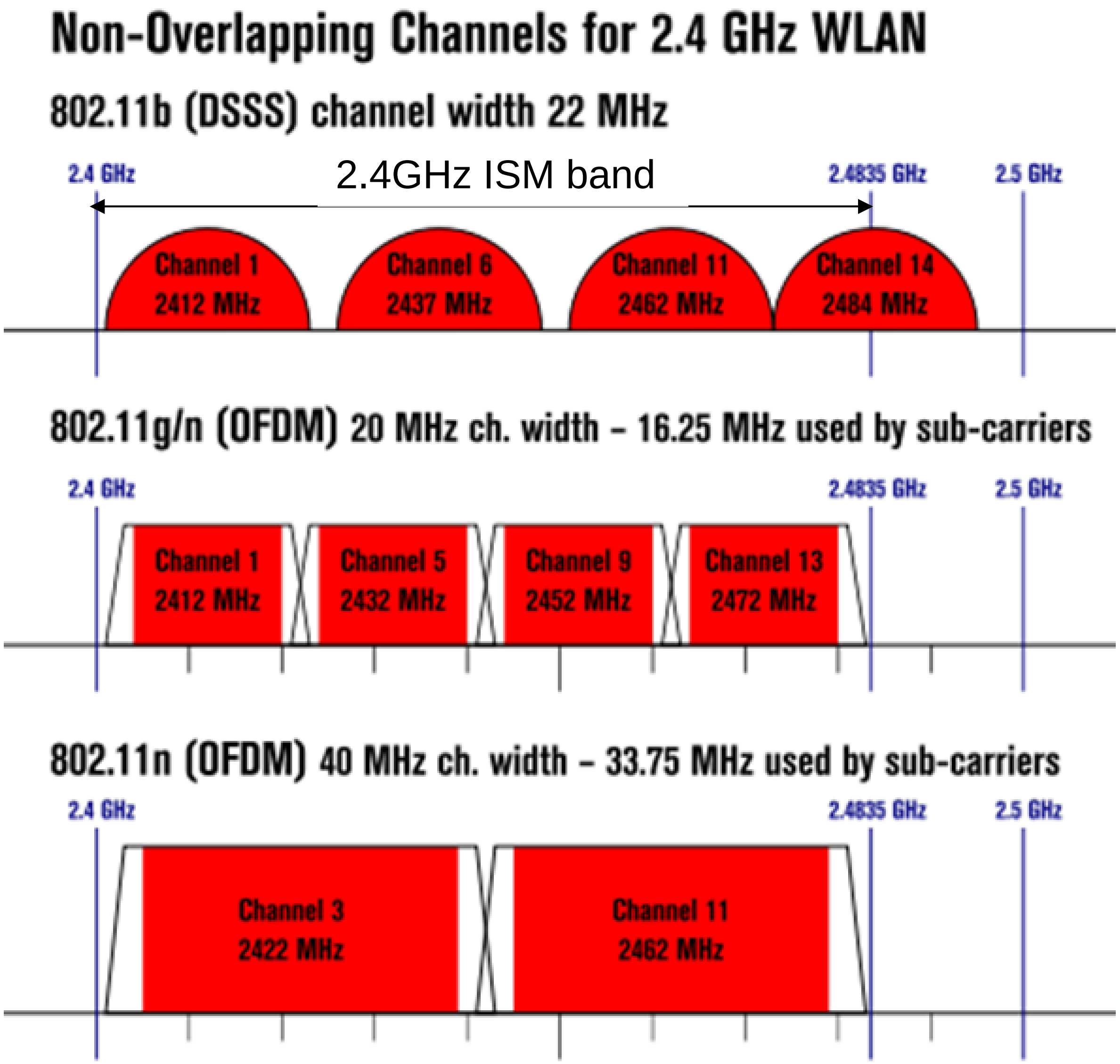


Agateller for Wikipedia
Public Domain

# Raw ECG VS distorted ECG

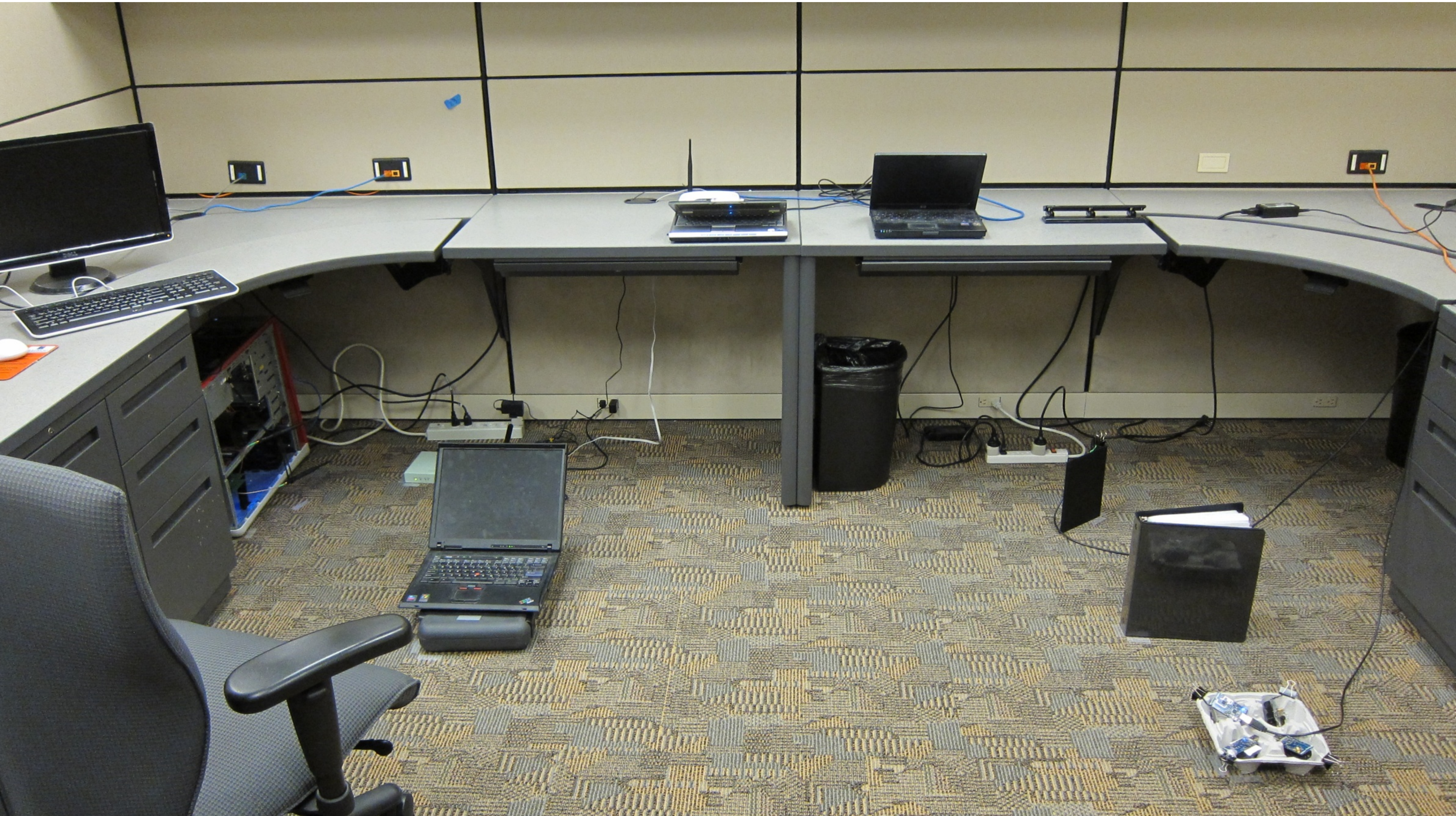


The main threat to WBAN is WiFi jamming [wang11]: two 802.11n WiFi networks can jam the entire 2.4GHz ISM band.

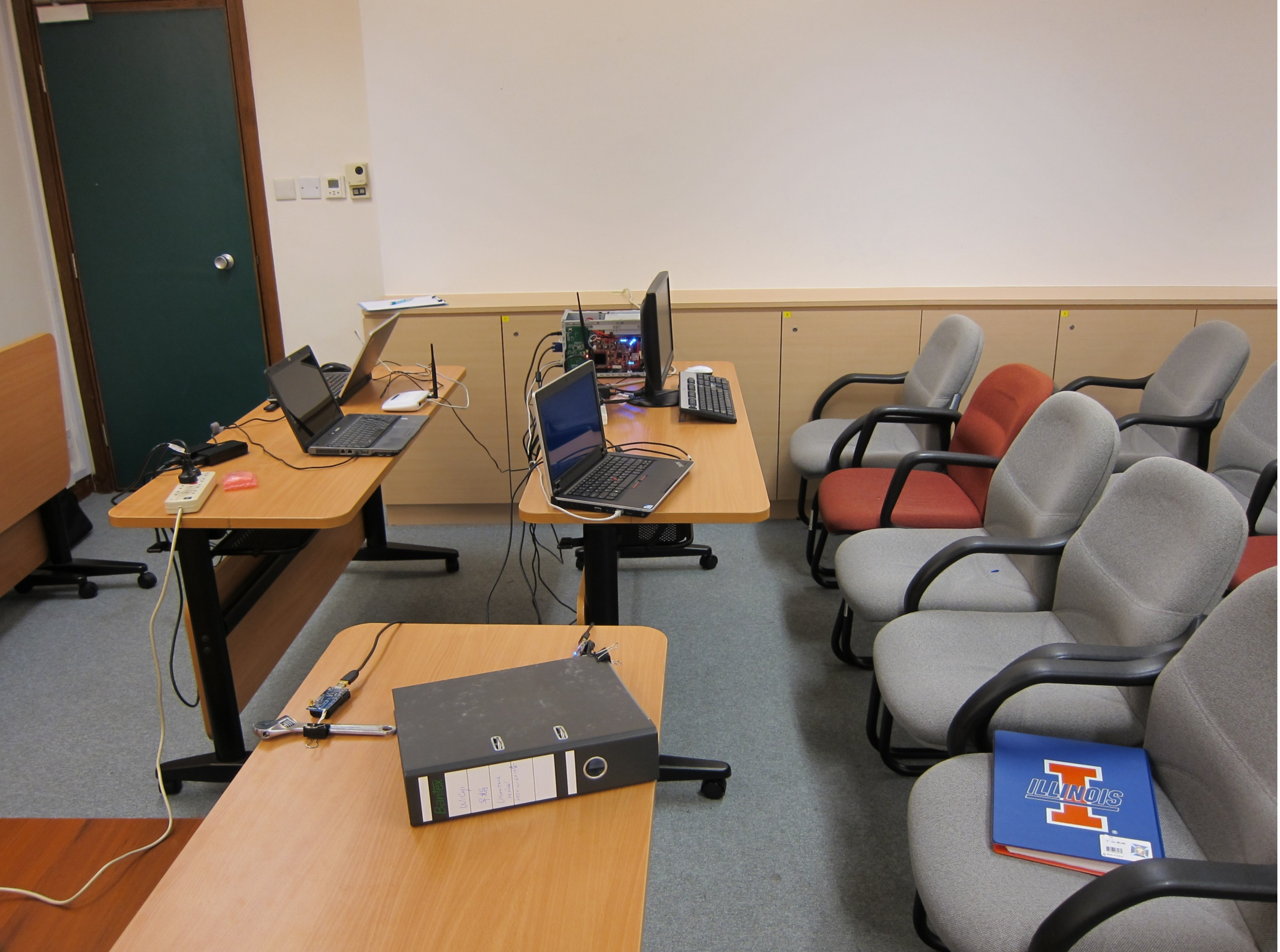


picture quoted from Wiki

# Experiment layout1



# layout



# DSSS-Nulling is better than Fake PHY Hdr

- Fake PHY Hdr just sends a DSSS preamble and DSSS PLCP header
- Upon decoding header error, interferer may use the channel
- DSSS-Nulling keeps transmitting preamble throughout WBAN active interval
- Upon decoding preamble error, interferer may detect successive preamble

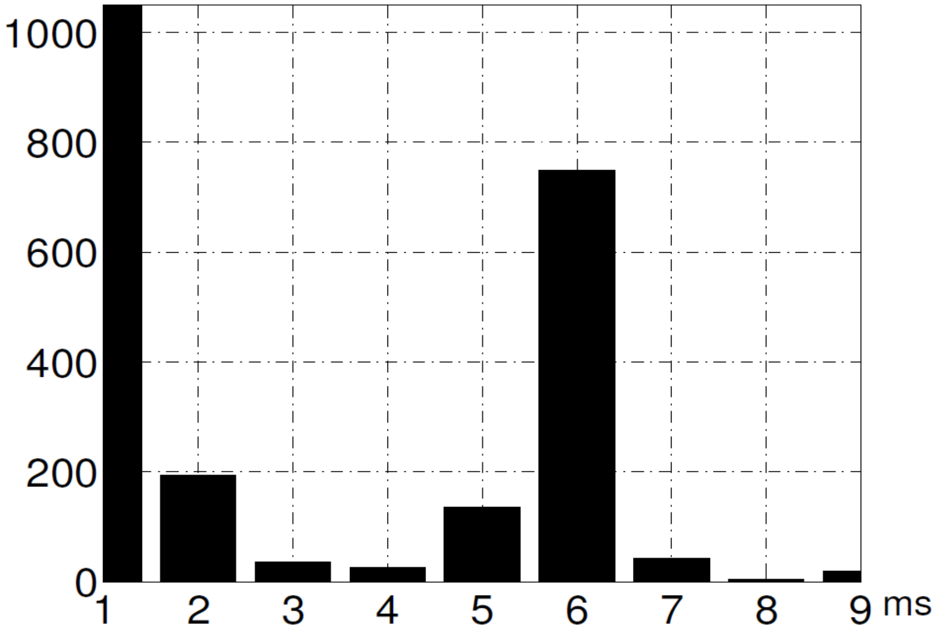
# Clear Channel Assessment (CCA) of WiFi

- decide whether channel is busy
- at least 3 categories:
  - Carrier Sense (CS) only CCA;
    - if detecting WiFi preamble and header
  - Energy Detection (ED) only CCA;
    - If received power exceeds a threshold
  - CS+ED CCA;
    - If detecting WiFi preamble or header, the power of which exceeds a threshold

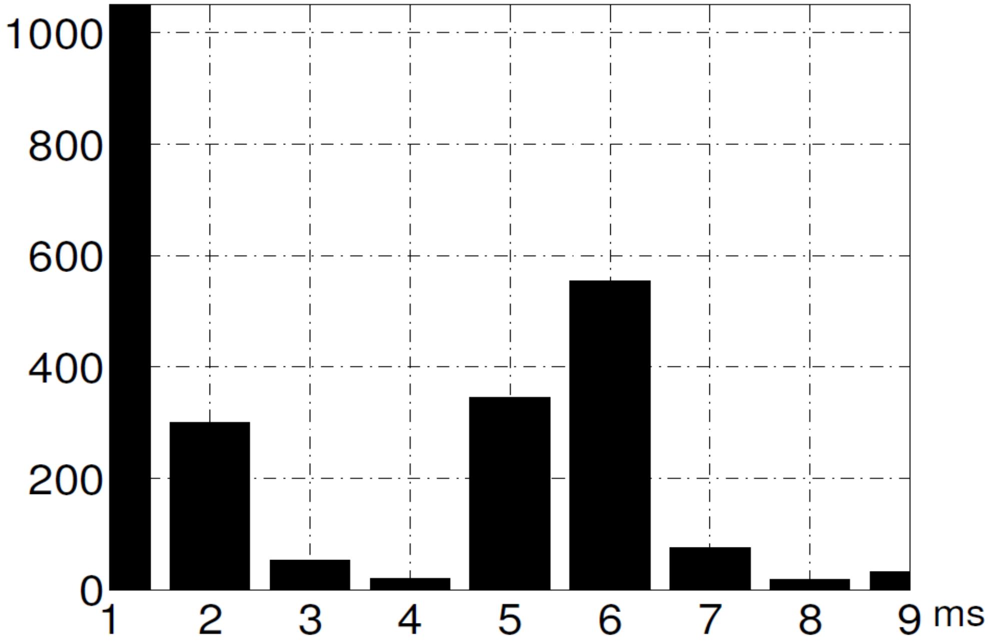
# Comparison between fake PHY Hdr and DSSS-Nulling

| | Fake PHY Hdr | DSSS-Nulling |
|---|---|---|
| Time-frequency efficiency (if policing succeeds) | High | low |
| Policing success probability | Low | high |
| CCA of affected WiFi interferer | CS-only CCA; CS+ED CCA | CS only CCA; ED only CCA; CS+ED CCA |

# White-space histogram



Fake PHY Hdr



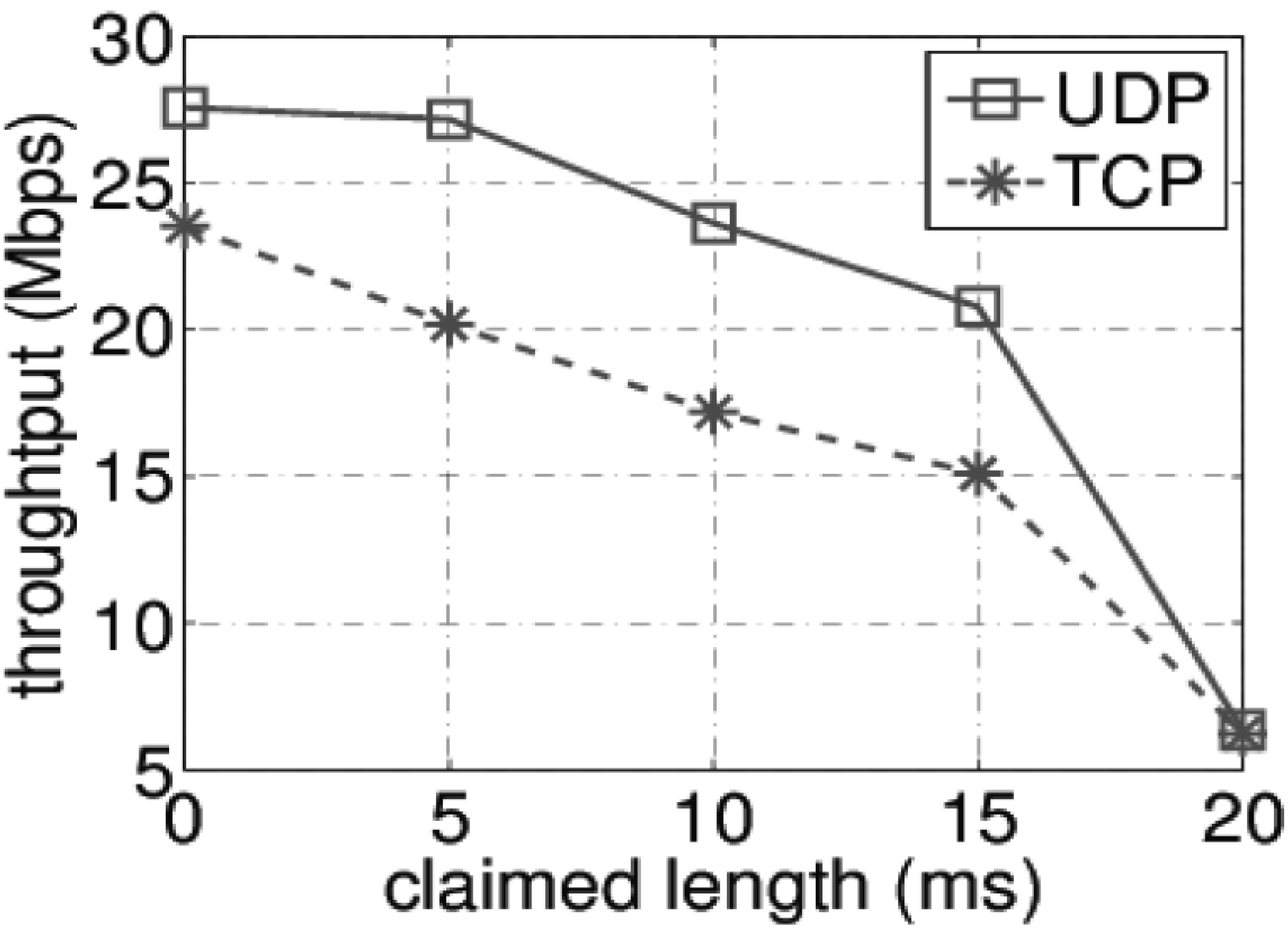
DSSS-Nulling

Send 1000 policing frames, each claiming 5ms white-space

Inter packet interval histogram

Supposed to have 1000 5ms white space

# Negative effect of policing



WiFi is running at the highest rate

Send a fake PHY Hdr policing frame every 25ms,

Claim a white-space equal to 0, 5, 10, 15, 20ms respectively

# Comparison between three policing strategies

| | Fake-PHY-Hdr | Fake-RTS | DSSS-Nulling |
|---|---|---|---|
| Continuous Reservation | + Difficult | +++ Easy | +++ Easy |
| Temporal-Spectral Overhead | +++ Small | ++ Medium | + Big |
| Power Consumption (meaningful in ad hoc scenarios) | +++ Small | ++ Medium | + Large |
| Vendor Independency | + Bad | +++ Good | +++ Good |
| Policing Success Rate (Significance in improving WBAN MTTF) | ++ Medium | + Lowest | +++ Highest |