Understanding and Mitigating the Impact of RF Interference on 802.11 Networks

Ramakrishna Gummadi UCS
David Wetherall Intel Research
Ben Greenstein University of Washington
Srinivasan Seshan CMU

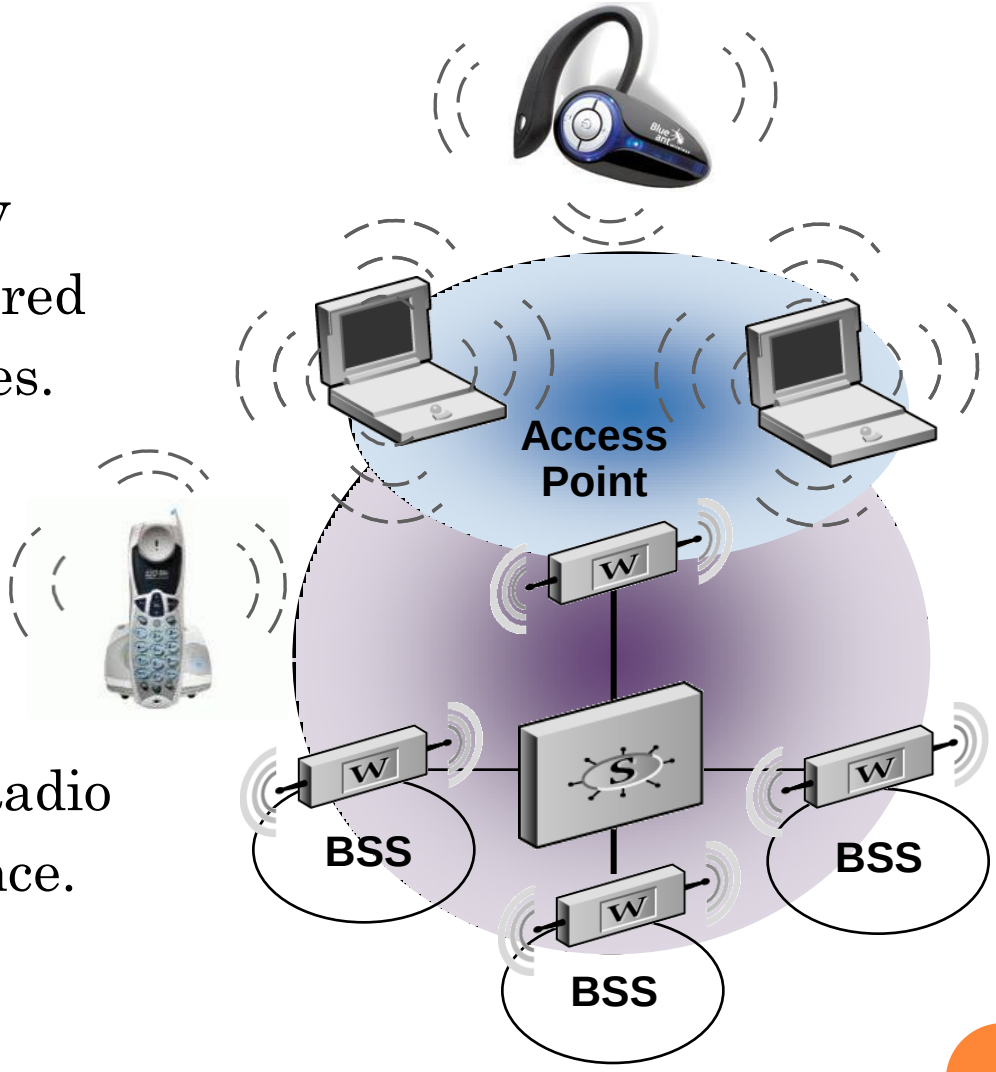
Presented by;
Andrew Keating
Murad Kaplan

OUTLINE

- Introduction
- 802.11 Background
- Experimental Setup
- Causes and Effects of Interference
- Modeling Interference Effects
- Rapid Channel Hopping
- Conclusion

Introduction

- Wireless Technology
  - An alternative to wired networks in enterprises.
  - Enable mobility.
  - Provide city-wide internet access.
- Problem:
  - Vulnerable to RF (Radio Frequency) interference.



Introduction (cont'd)

- Problem (who to consider)
  - *Selfish interferers e.g.* Zigbee nodes and cordless phones.

  - *Malicious interferers e.g.* Wireless jammers.

Introduction (cont'd)

Motivations:

- Explore the impact of interference on 802.11 links and to develop techniques that make 802.11 more resistant to interference.
- Experimental results confirm anecdotal evidence that a range of selfish and malicious interferers (802.11 waveforms, Zigbee, a wireless camera jammer, a cordless phone) cause 802.11 performance to degrade much more significantly than expected from simple SINR considerations

Introduction (cont'd)

Contributions:

- Quantifying the extent and magnitude of 802.11's vulnerability to interference.
- Extending the SINR model to capture the limitations.
- Implementing and evaluating a rapid channel hopping scheme that can withstand even multiple strong interferers in a realistic setting.

OUTLINE

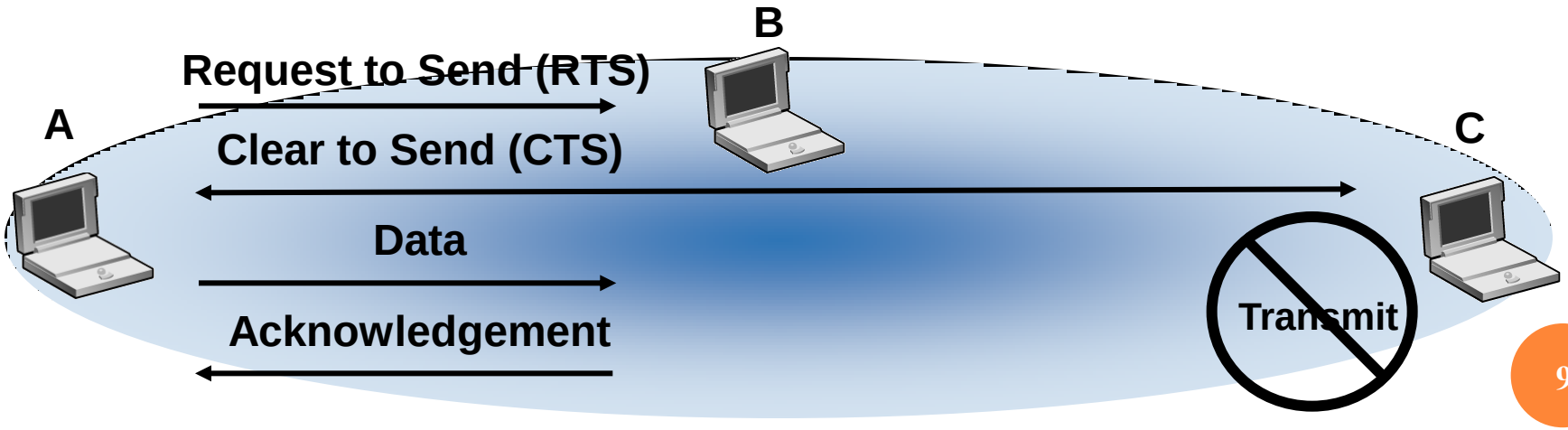
- Introduction
- 802.11 Background
- Experimental Setup
- Causes and Effects of Interference
- Modeling Interference Effects
- Rapid Channel Hopping
- Conclusion

802.11 Background (cont'd)

- RTS/CTS
- Management Packets
- PLCP
- Overlapping Channels

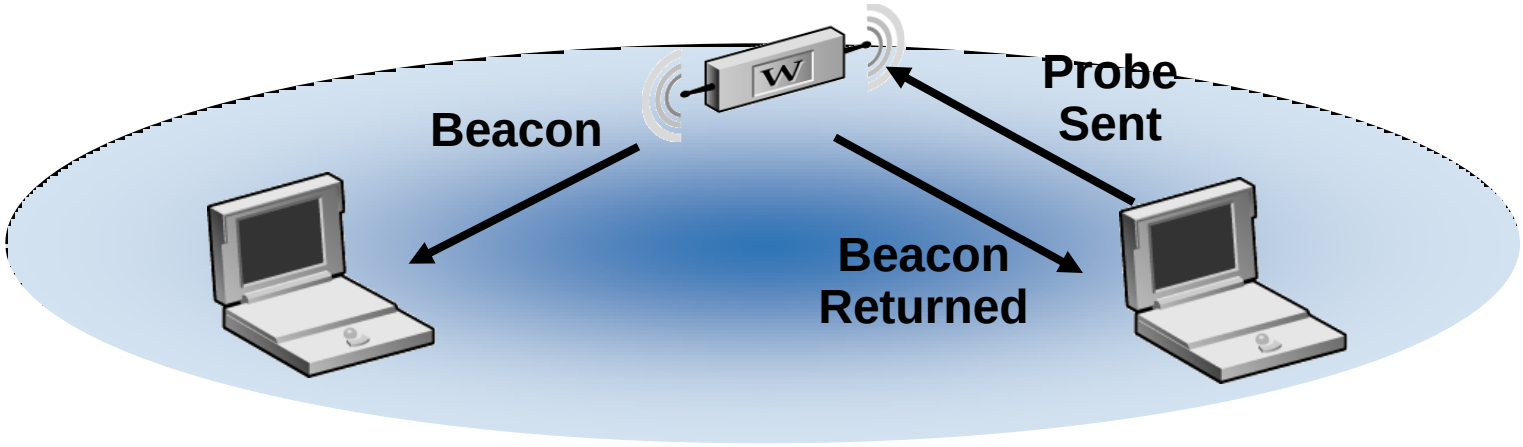
802.11 Background (cont'd) RTS/CTS

- Used to provide CSMA/CA control.
- Avoids bandwidth loss due to collisions.
- Short control messages (frames) sent to start or stop transmission.
- Configurable option – RTS Threshold.



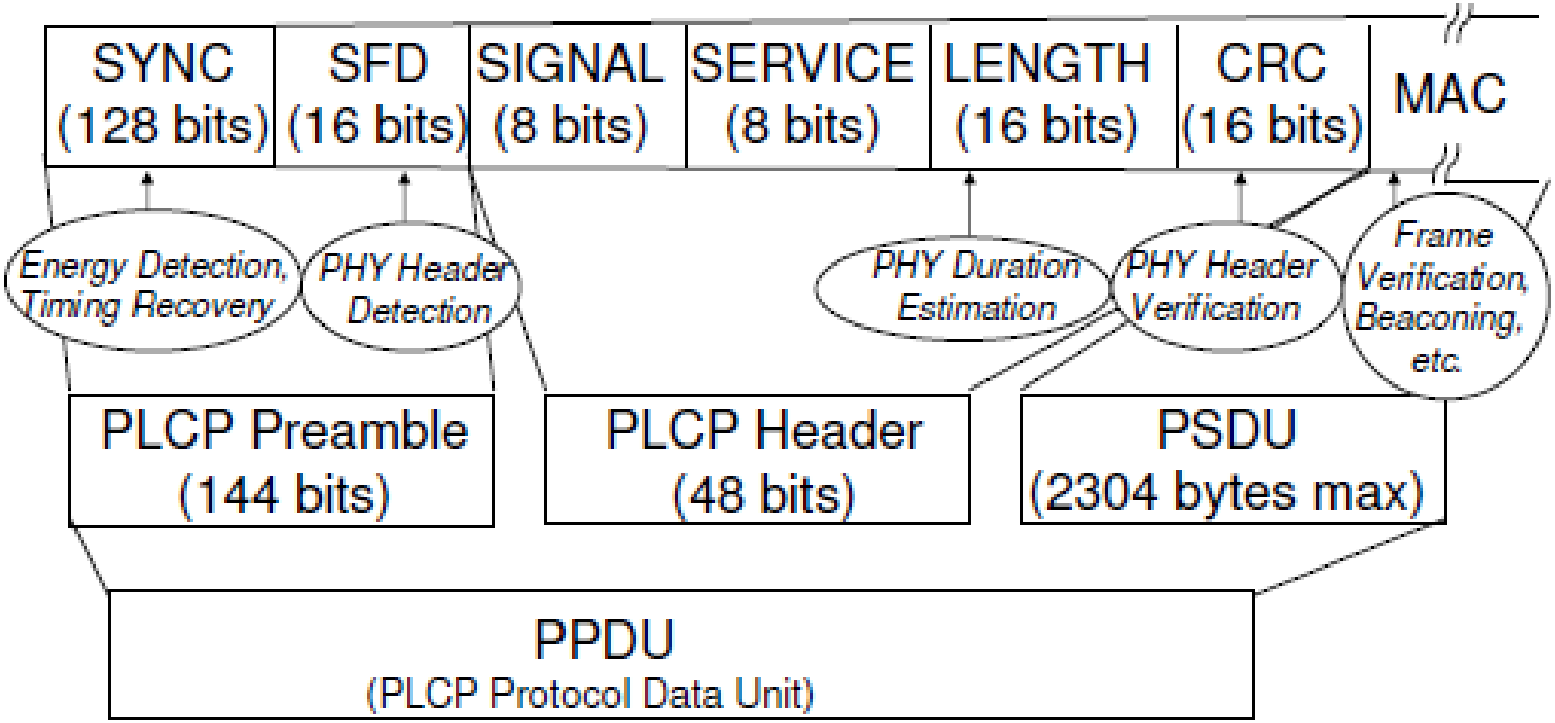
802.11 Background (cont'd) Management Packets

- Scanning
- Station (user) Authentication and Association
- Beacon Management
- Power Management Mode



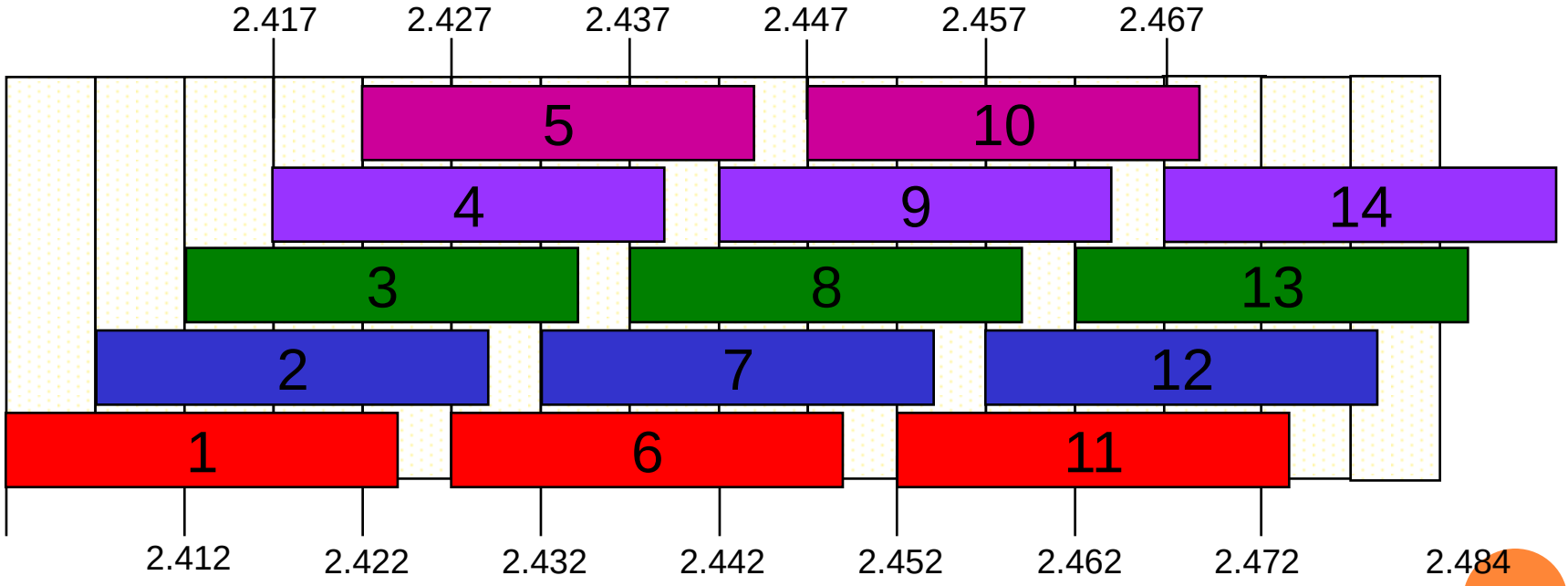
PLCP - Physical Layer Convergence Protocol

Physical Layer Convergence Protocol



802.11 Background (cont'd) Overlapping Channels

- 802.11b/g transmission occurs on one of 11 overlapping channels in the 2.4GHz North American ISM band.



802.11 Background (cont'd)
802.11b/g

- Operates in the 2.4 GHz ISM band
  - 14 total channels
  - Only 1-3 channels usable at any time
- 802.11b supports data rates up to 11 Mbps
  - Uses DSSS
- 802.11g supports data rates up to 54 Mbps
  - Similar data rates as 802.11a
  - Backward compatible with 802.11b
- Coverage up to 100 meters (328 feet)
- Most commonly implemented standard, "Wi-Fi"
- Crowded frequency band

OUTLINE

- Introduction
- 802.11 Background
- Experimental Setup
- Causes and Effects of Interference
- Modeling Interference Effects
- Rapid Channel Hopping
- Conclusion

Experimental Setup (cont'd)

- Client and AP
- Interferers
- Tests and Metrics

Experimental Setup (cont'd)

- Client and AP
  - Client:

    A Linux laptop equipped with 802.11 NICs from Intersil (802.11b)

  - AP:

    A Linux laptop with either an Intersil PRISM 2.5 in 802.11b mode (using the *HostAP driver) or an Atheros AR5006X*

Experimental Setup (cont'd)

- Interferers
  - Two malicious (Linux desktop with PRISMPCI NIC and camera jammer).
  - Two selfish devices (a Zigbee sensor node and a Panasonic cordless phone).

Experimental Setup (cont'd)

- Interferers and their characteristics.

Interferer	Power(dBm)	BW(MHz)	Range(m)
PRISM 2.5	$[-20, 20]$	22	~30
2.4GHz jammer	30	1, FH	~20
CC2420 (Zigbee)	$[-24, 0]$	5	~6
Cordless phone	20	0.003, FH	~2

Experimental Setup (cont'd)
Tests and Metrics

- Each test consists of the client doing a one-way UDP or a TCP transfer of several megabytes between itself and a wired source or sink *E through the AP*.
- Measure overall performance in terms of throughput and latency.
- Measure kernel-level end-to-end packet transmissions and receptions at one-second intervals.
- Collect many low-level 802.11 statistics at the AP and the client (number of PLCP reception errors, PHY CRC errors, MAC CRC errors, etc)

OUTLINE

- Introduction
- 802.11 Background
- Experimental Setup
- Causes and Effects of Interference
- Modeling Interference Effects
- Rapid Channel Hopping
- Conclusion

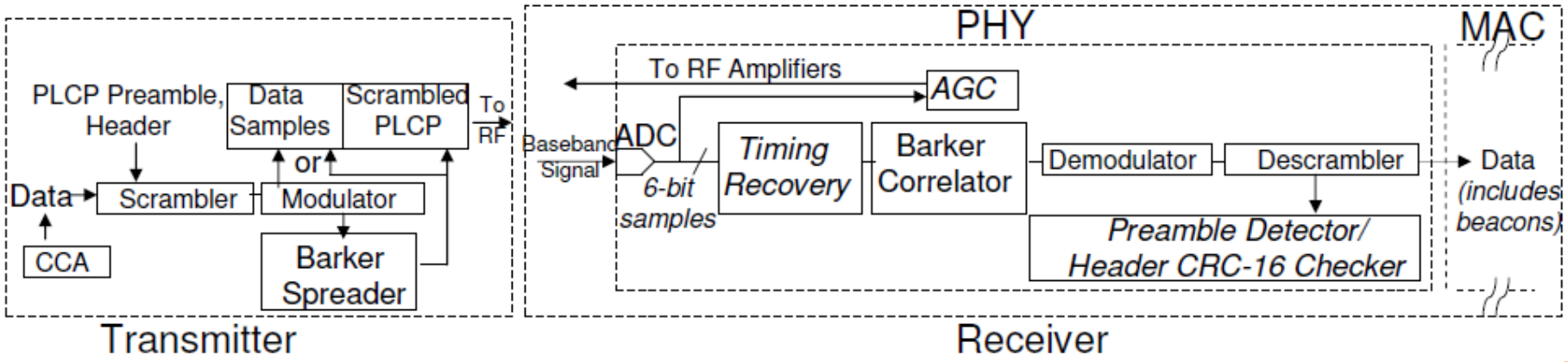
Causes and Effects of Interference

- **Timing Recovery Interference.**
- **Dynamic Range Limitation.**
- **Header Processing Interference.**
- **Impact of Interference on 802.11g/n.**
- **Impact of Frequency Separation.**

- *Test with NICs from different vendors (PRISM, Atheros and Intel depending on the test) to check that these effects are not implementation artifacts.*
- *Test with 802.11g and 802.11n to check that that these effects are not 802.11b PHY artifacts*

Causes and Effects of Interference (cont'd)

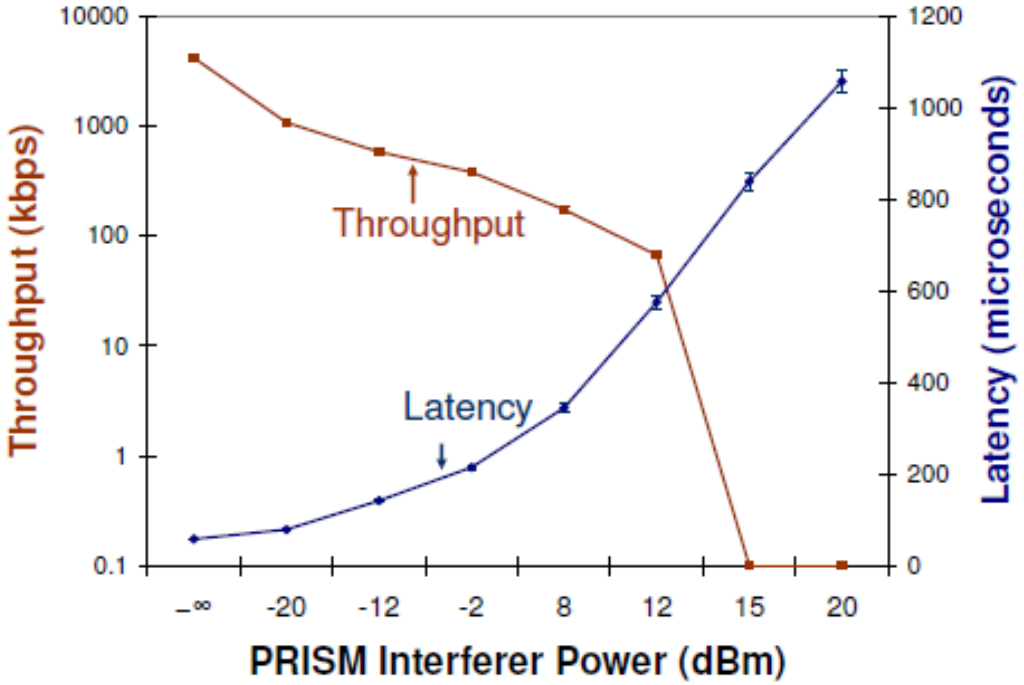
Timing Recovery Interference



- Sender clock extraction is done in the Timing Recovery module.
- If this module fails to lock onto the sender's clock, the receiver will sense energy, but not recognize it as valid modulated *SYNC bits*.
- Since the interferer's clock and the transmitter's clock are unsynchronized, the Timing Recovery module at the receiver cannot lock onto the transmitter's clock.
- The receiver therefore only records energy detection events, but does not detect any packet transmissions.
- Thus, packets sent by the transmitter are lost at the receiver.

Causes and Effects of Interference (cont'd)

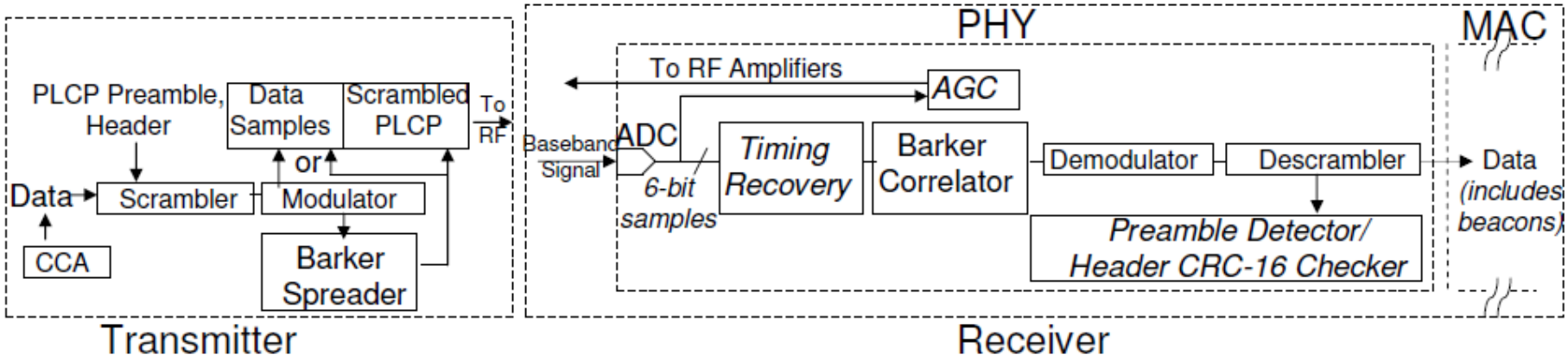
Timing Recovery Interference



Throughput and latency vs. interferer power caused by interference affecting timing recovery.

Causes and Effects of Interference (cont'd)

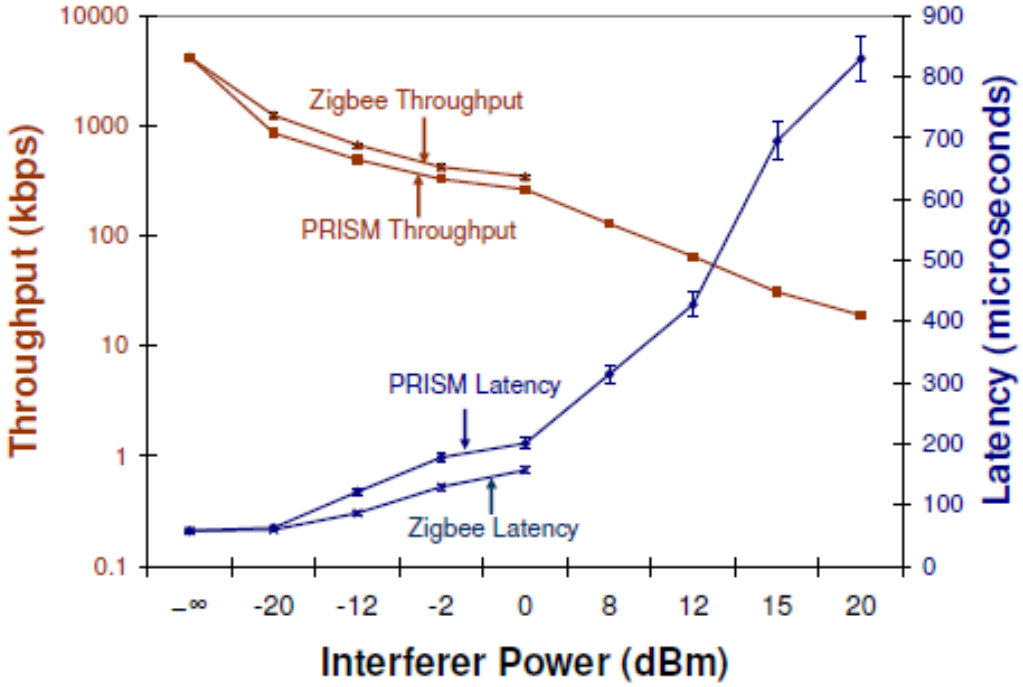
Dynamic Range Limitation.



- Receivers need to decode packets over a very large range of signal strengths (−10dBm to −70dBm).
- ADC can make the best use of the fixed-width bits that are available to represent the digital samples of the signal.
- AGC samples these voltage levels during the PLCP preamble processing, and controls the gain of the RF and the IF amplifiers so that the signal samples can occupy the entire ADC range.

Causes and Effects of Interference (cont'd)

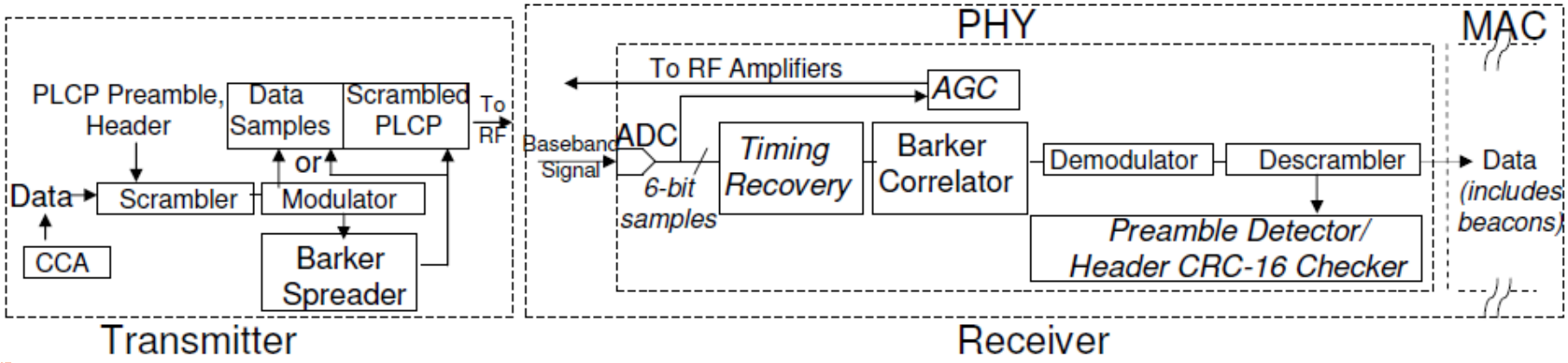
Dynamic Range Limitation.



Throughput and latency vs. interferer power caused by interference affecting dynamic range selection.

Causes and Effects of Interference (cont'd)

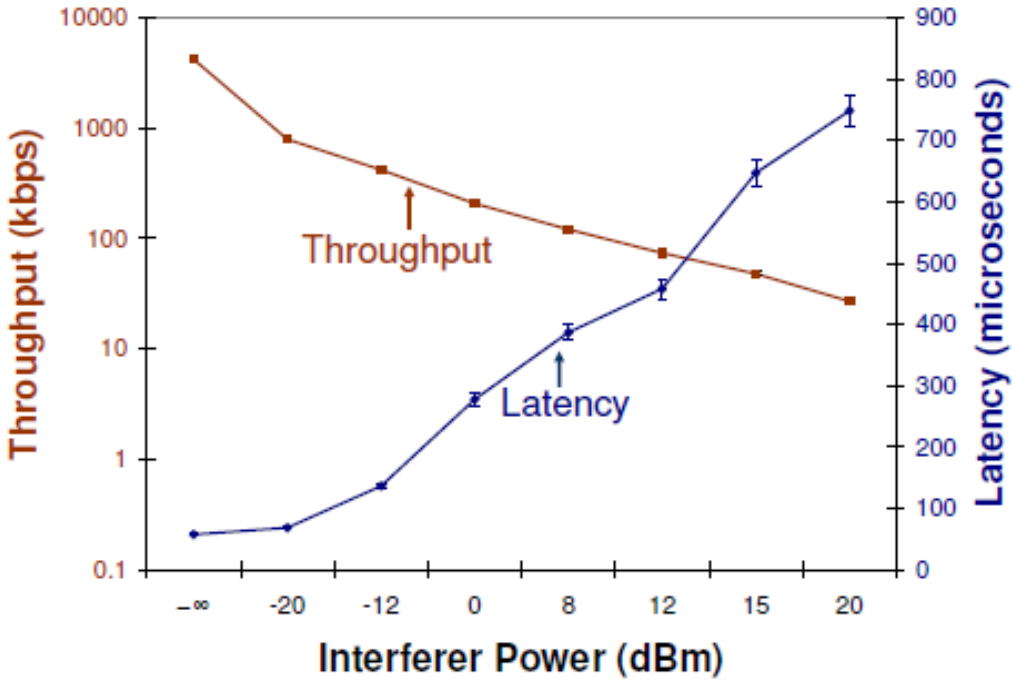
Header Processing Interference.



- *Start Frame Delimiter (SFD),* this field signals to the receiver that the PLCP header is about to be sent.
- Receivers are ready for the SFD pattern before it arrives.
- If the receiver's Preamble Detector module sees the SFD pattern from the interferer before it sees it from the transmitter, it starts processing the header before the actual header from the transmitter arrives at the receiver.

Causes and Effects of Interference (cont'd)

Header Processing Interference.



Throughput and latency vs. interferer power caused by interference affecting header processing.

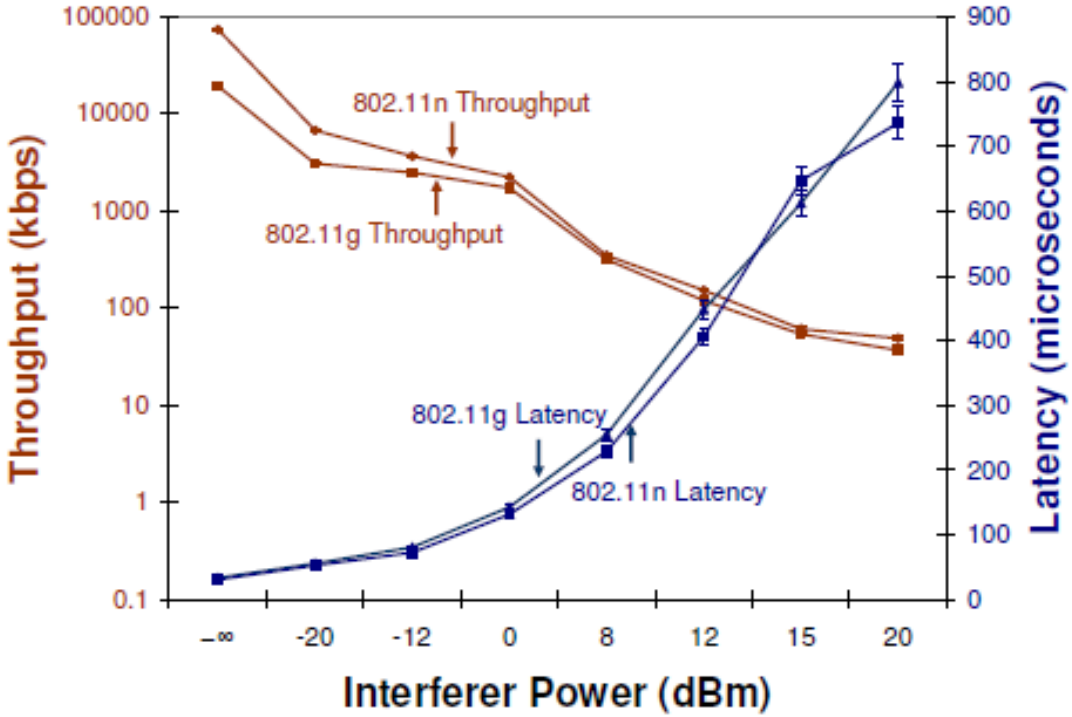
Causes and Effects of Interference (cont'd)

Impact of Interference on 802.11g/n.

- 802.11g/n are different enough from 802.11b to question whether interference can decrease their link throughputs drastically as well.
- 802.11g does not use the Barker Correlator module, and the Demodulator module is quite different because it uses OFDM.
- 802.11n standard applies spatial coding techniques, which use multiple transmitter and receiver antennas. OFDM.

Causes and Effects of Interference (cont'd)

Impact of Interference on 802.11g/n.



Throughput and latency vs. interferer power for 802.11g/n.

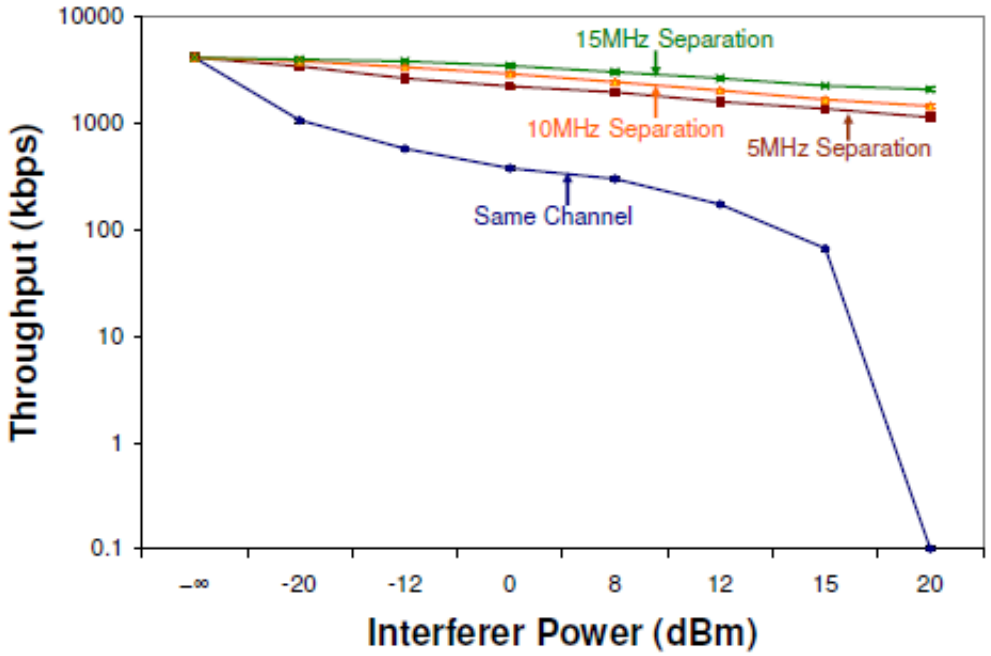
Causes and Effects of Interference (cont'd)

Impact of Frequency Separation.

- The authors expected the interference to be mitigated for two main reasons:
  - The sensitivity of the RF amplifiers at the receiver falls off with frequency separation.
  - The RF filters in the receiver remove interference power on frequencies that do not overlap the receiver's frequencies.
  - The tolerance to interference suggests that channel hopping may be an effective remedy in mitigating interference.

Causes and Effects of Interference (cont'd)

Impact of Frequency Separation.



Throughput and latency vs. interferer power with frequency separation.

OUTLINE

- Introduction
- 802.11 Background
- Experimental Setup
- Causes and Effects of Interference
- Modeling Interference Effects
- Rapid Channel Hopping
- Conclusion

Modeling Interference Effects

- SINR is Signal to Interference plus Noise Ratio
  - Used by ns-2 and other network simulators
  - Does not account for NIC weaknesses
- Authors introduce SINR plus…
  - Dynamic range selection limitation due to AGC
  - Receiver sensitivity non-linearity
  - Remember – these two limitations cause weak/narrow-band interferers to be very effective

Modeling Interference Effects (Cont'd)
Signal to Interference Plus Noise Ratio

$$SINR(x,t) = \frac{S(x,t)}{I(x,t) + N_{\text{env}}}$$

- Packet *x*, Time *t*
- *S(x,t)*: Signal power
- *I(x,t)*: Interference
- *N*env: Noise
  - This value is complex, but mainly represents the channel and antenna noise

Modeling Interference Effects (Cont'd) Interference Model

- Interference *I(.)* is sum of all undesirable signals *S(y, t)* (both external interferers and self-interference due to multipath) that arrive at the receiver at time *t:*

$$I(x,t) = \sum_{y \neq x} S(y,t)$$

- However, line-of-sight setup eliminates multipath, so we can consider *I(.)* to represent instantaneous interferer power

Modeling Interference Effects (cont'd) Non-linearity in Receiver Sensitivity

- Attenuation away from center frequency
  - Non-linear, thus we need to integrate interference power with receiver sensitivity over the entire frequency range [*f1,f2*]
  - *R(f)* is receiver sensitivity at frequency *f*

$$I(x,t) = \sum_{y \neq x} \int_{f1}^{f2} R(f) S(y,t) df$$

Channel	Lower Freq	Center Freq	High Freq
1	2.401	2.412	2.423
2	2.404	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438

Modeling Interference Effects (Cont'd) Accounting for Processing Gain

- To decode an 802.11b signal correctly, an SINR of at least 10dB is required
- Barker coding provides an additional 10.4dB processing gain
- Therefore, a signal can theoretically be -0.4dB weaker than an interferer and still be received

Modeling Interference Effects (cont'd)
AGC Behavior

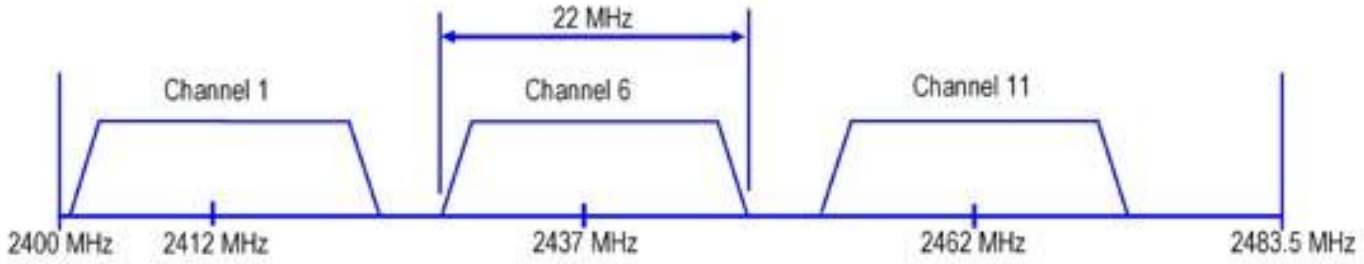
- Automatic Gain Control can degrade SINR by as much as 30dB
- Smax: NIC-dependent signal strength threshold

$$SINR(x,t) = \begin{cases} SINR(x,t) - 30\text{dB}, & \text{if } S(x,t) > S_{\max} \\ SINR(x,t), & \text{if } S(x,t) \leq S_{\max} \end{cases}$$

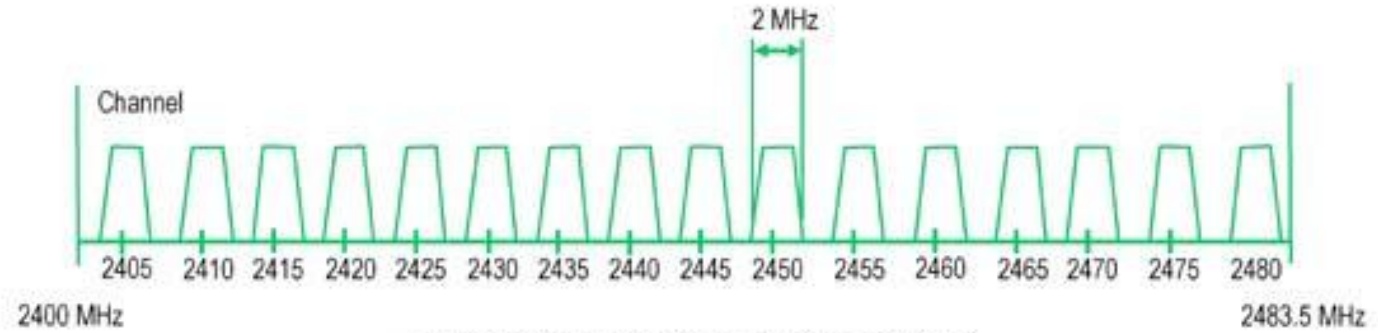
- Recall the -0.4dB SINR margin with Barker coding
- Thus **signal cannot be demodulated unless it is 29.6dB greater than the interferer**

Applying the Model 802.11 and Zigbee Offset

- By design, the center frequencies of Zigbee and 802.11 are always offset by at least 2 MHz



a) IEEE 802.11b North American channel selection (non-overlapping)



b) IEEE 802.15.4 channel selection (2400 MHz PHY)

Source: IEEE 802.15.4 specification

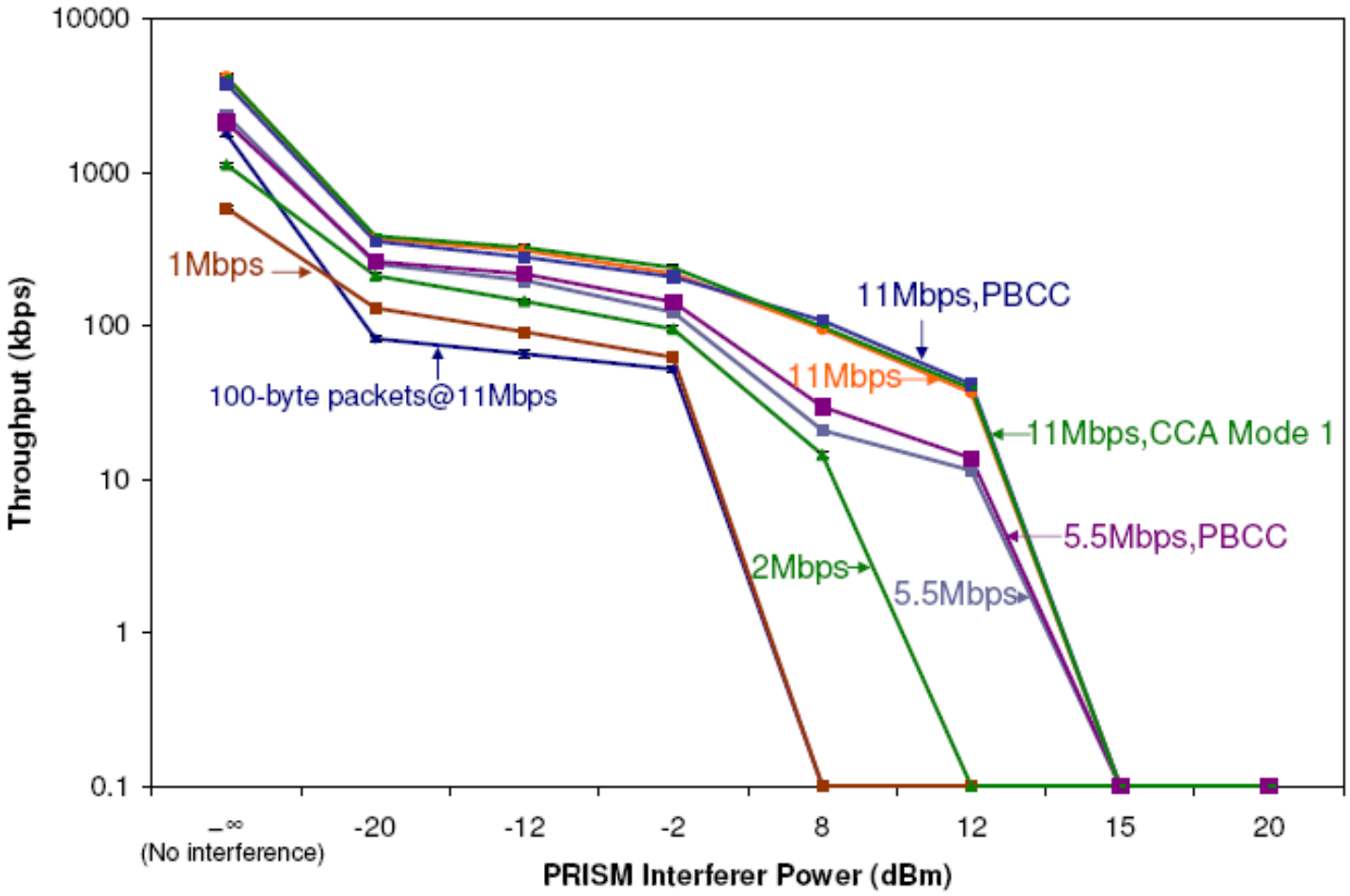
Applying the Model (cont'd) Narrow-band Zigbee

- Signal Power: -18dBm
- Zigbee Interference Power: -35dBm
- At 2MHz, receiver sensitivity is 10dB below center frequency (PRISM Datasheet)
- SINR = (-18) – (-35) + 10 = 27dBm
- This is below the required SINR of 29.6dB, and as a result the Zigbee narrow-band interferer can cause heavy losses

Applying the Model (Cont'd) Ineffective 802.11 Modifications

- Authors don't "show their work" – space constraints?
- Changing CCA Thresholds and Modes
  - Only changes transmitter behavior, while losses are also observed at the receiver
- Adding Forward Error Correction
  - Adds 4dB coding gain for BPSK/QPSK modulations – not enough
- Changing packet sizes
  - 1500b to 100b drops SINR requirement by 4dB, but not enough to counteract interferers
- Changing rates and modulations
  - Avoiding Barker modulations not good enough

Ineffective 802.11 Modifications



OUTLINE

- Introduction
- 802.11 Background
- Experimental Setup
- Causes and Effects of Interference
- Modeling Interference Effects
- Rapid Channel Hopping
- Conclusion

Rapid Channel Hopping

- Recall that separating the frequency of the receiver and interferer by > 5MHz is effective
  - Unless the attack jams all channels at once
- Typically channel changes in 802.11 NICs only occur in response to failures, and at a slow rate
- Main goals – efficiency and power to withstand even malicious interferers
- Feasible – most NICs support changing channel in software quickly

Rapid Channel Hopping (cont'd) Design Choices

- Channel switching latency (PRISM: 250us, Intel 500 us) in hardware
- 10ms dwell time (2.5% channel switching overhead on PRISM, 5% on Intel)
- Channel hopping sequence is MD5-hashed to ensure resistance to attackers
- Upon detecting link degradation, the AP begins channel hopping
- Clients are disconnected, find the AP, receive MD5 seed and begin hopping themselves

Rapid Channel Hopping (cont'd) Adversary Design

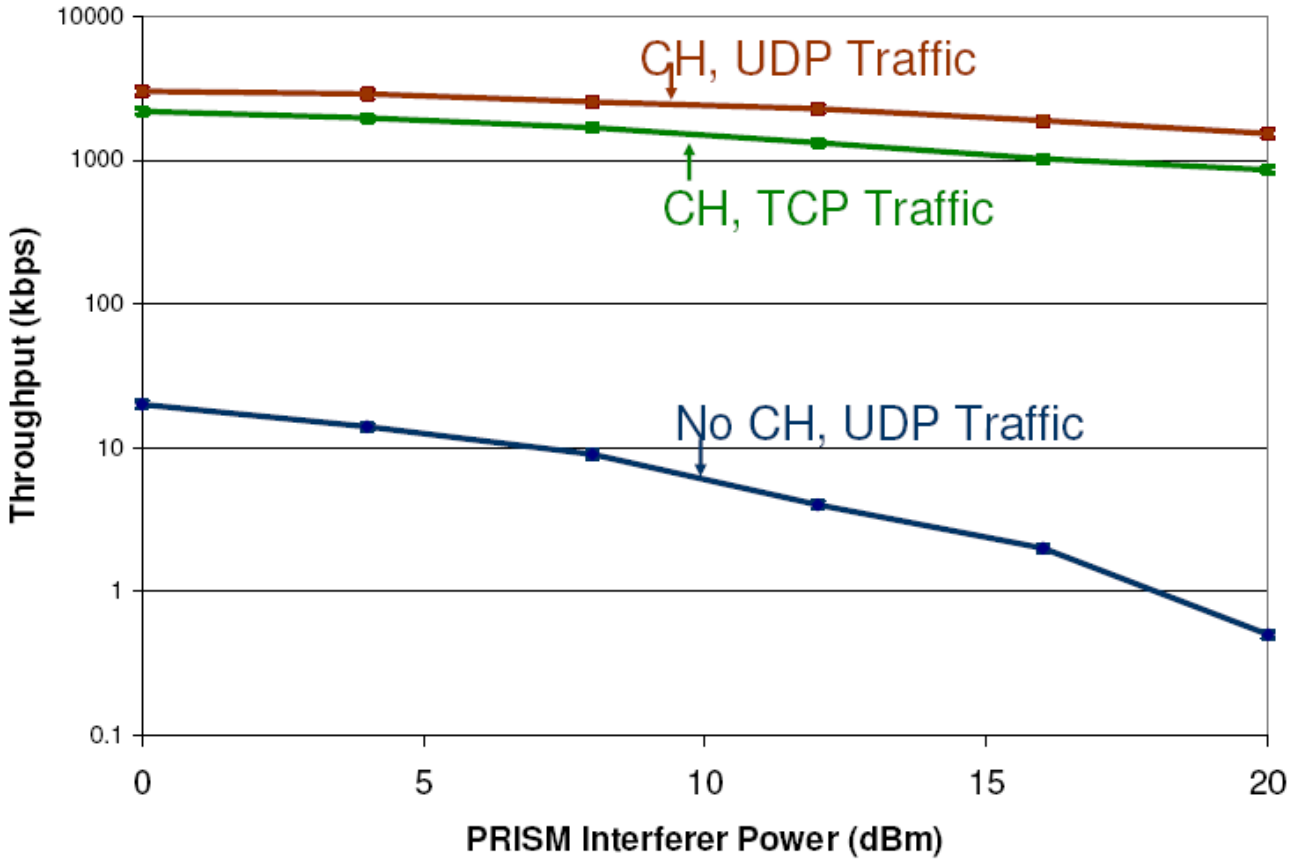
- Recall that if three successive beacons are lost, clients are disconnected for all practical purposes
- Attack methodology - randomly pick a channel, disrupt for a short period, repeat
  - 1/11 probability of successful jam (11 channels), only 0.1% success rate if assuming 100ms between beacon transmissions
- Better strategy – listen on random channels and disrupt when the active channel is found

Rapid Channel Hopping (cont'd) Evaluation

- One AP and three clients (C1-C3) and three PRISM interferers (P1-P3) – 802.11b
- One of each: cordless phone, Zigbee sensor mote, wireless camera jammer
- CH degrades throughput from 4.4 to 3.6 Mbit/s
  - Unidirectional 1500-byte packet UDP, no interference
  - Attributed to loss before, during and after switching channels

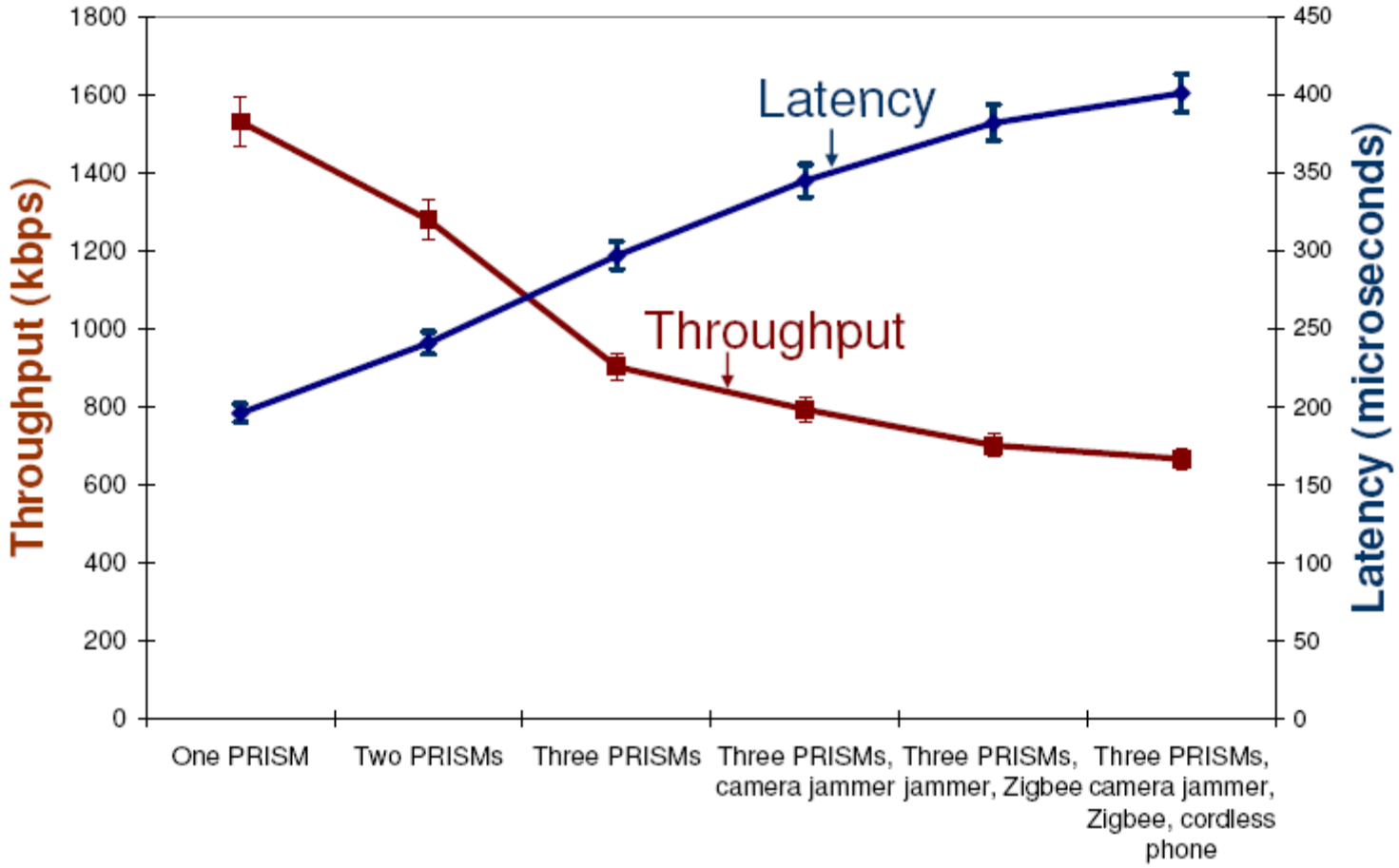
Single PRISM Interferer Throughput

- Authors don't specify which attack method used (random channel or active channel)



Multiple Interferers

- Three PRISM interferers coordinate interference schedules so they don't overlap



Related Work

- RF Interference/Jamming
- 802.11 Denial of Service
- Channel Hopping
- Not an overwhelming amount of original work is actually presented in this paper

OUTLINE

- Introduction
- 802.11 Background
- Experimental Setup
- Causes and Effects of Interference
- Modeling Interference Effects
- Rapid Channel Hopping
- Conclusion

Conclusions

- Even weak and narrow-band RF interference can significantly disrupt an 802.11 network
- Changing 802.11 parameters is ineffective in counteracting this
- Rapid channel hopping greatly improves interference tolerance
- Findings are hardware-specific, and only concrete for the NICs investigated
- Channel hopping is ineffective against attacks which target all channels