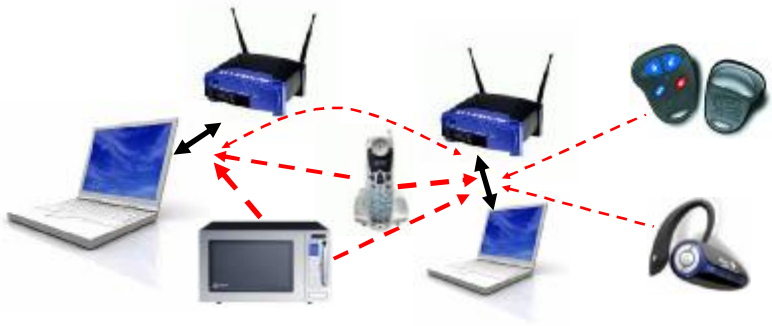
Understanding and Mitigating the Impact of RF Interference on 802.11 Networks

Ramki Gummadi (MIT), David Wetherall (UW)
Ben Greenstein (IRS), Srinivasan Seshan (CMU)

1

Growing interference in unlicensed bands

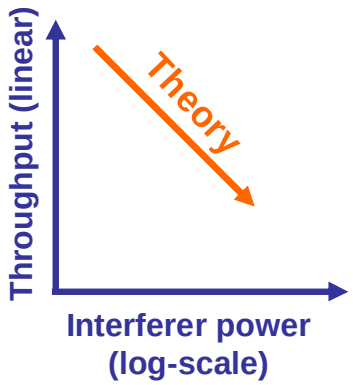
- Anecdotal evidence of problems, but how severe?
- Characterize how 802.11 operates under interference in practice



2

What do we expect?

- Throughput to decrease linearly with interference
- There to be lots of options for 802.11 devices to tolerate interference
  - Bit-rate adaptation
  - Power control
  - FEC
  - Packet size variation
  - Spread-spectrum processing
  - Transmission and reception diversity



3

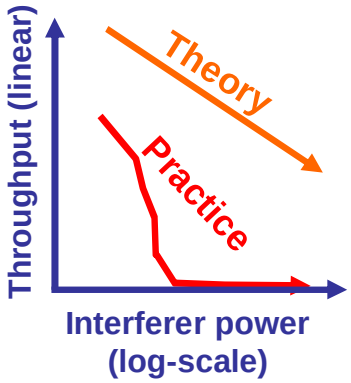
Key questions for this talk

- How damaging can a low-power and/or narrow-band interferer be?
- How can today's hardware tolerate interference well?
  - What 802.11 options work well, and why?

4

What we see

- Effects of interference more severe in practice
- Caused by hardware limitations of commodity cards, which theory doesn't model



5

Talk organization

- Characterizing the impact of interference
- Tolerating interference today

6

Experimental setup

Access Point

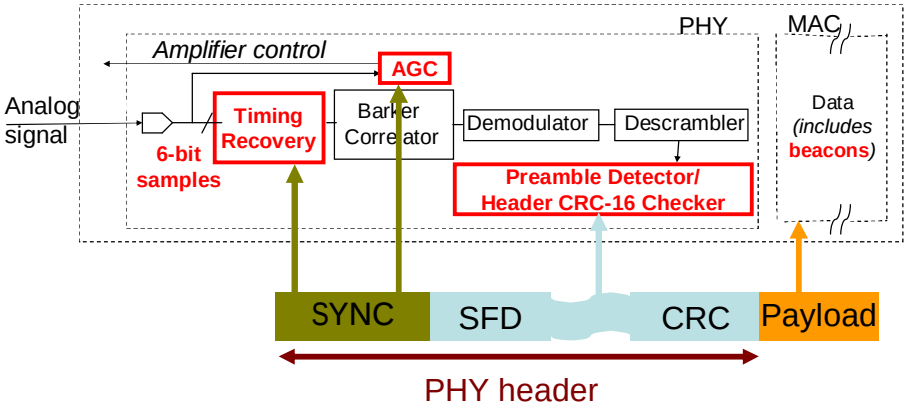
UDP flow

802.11 interferer

802.11 Client

7

802.11 receiver path



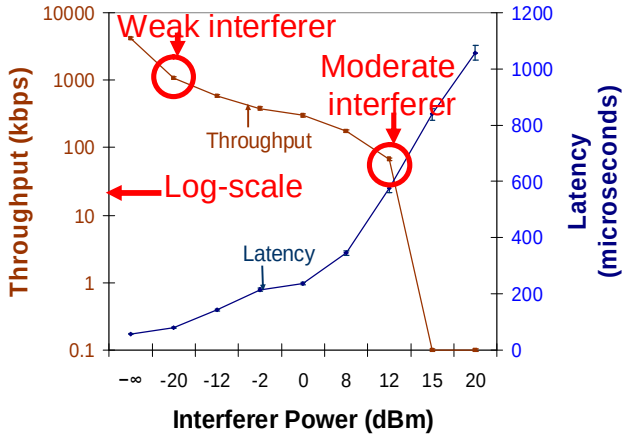
Extend SINR model (in paper) to capture these vulnerabilities

Interested in worst-case natural or adversarial interference

8

Timing recovery interference

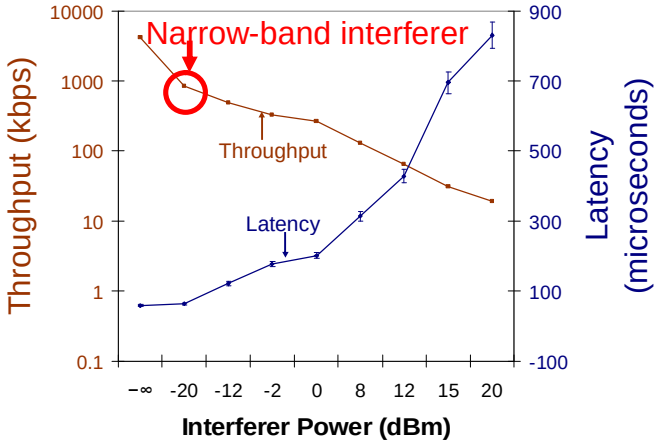
- Interferer sends continuous SYNC pattern
  - Interferes with packet acquisition (PHY reception errors)



9

Dynamic range selection

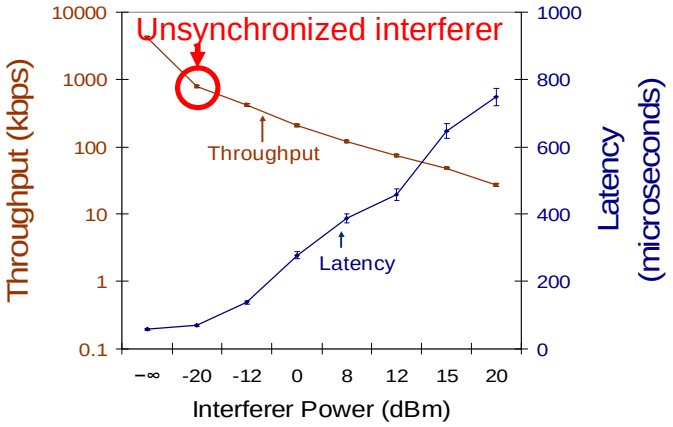
- Interferer sends on-off random patterns (5ms/1ms)
  - AGC selects a low-gain amplifier that has high processing noise (packet CRC errors)



10

Header processing interference

- Interferer sends continuous 16-bit Start Frame Delimiters
- Affects PHY header processing (header CRC errors)



11

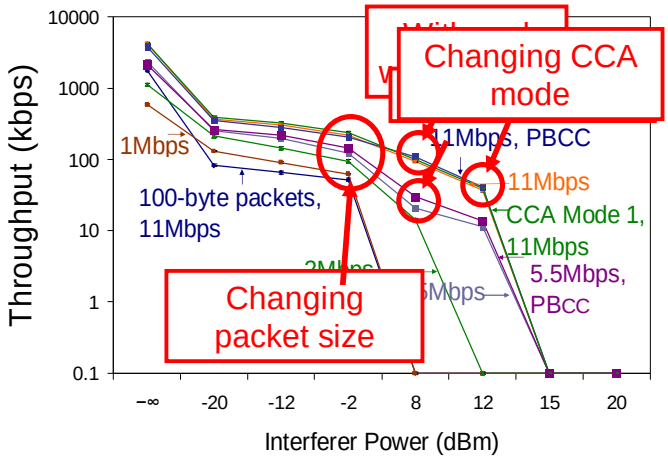
Interference mitigation options

- Lower the bit rate
- Decrease the packet size
- Choose a different modulation scheme
- Leverage multipath (802.11n)
- Move to a clear channel

12

Impact of 802.11 parameters

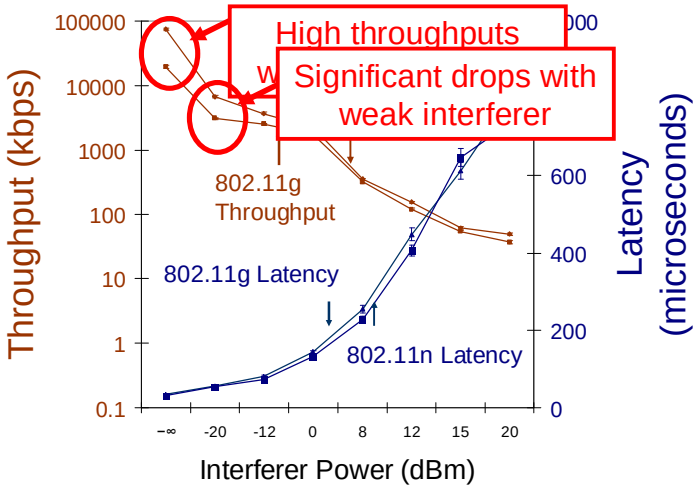
- Rate adaptation, packet sizes, FEC, and varying CCA parameters do not help



13

Impact of 802.11g/n

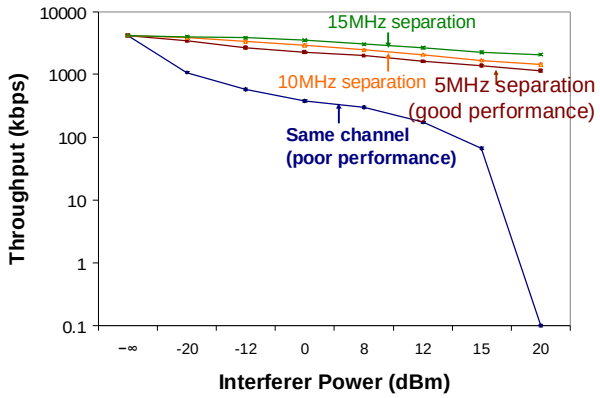
- No significant performance improvement



14

Impact of frequency separation

- But, even small frequency separation (i.e., adjacent 802.11 channel) helps
  - Channel hopping to mitigate interference?



15

Talk organization

- Characterizing the impact of interference
- Tolerating interference today

16

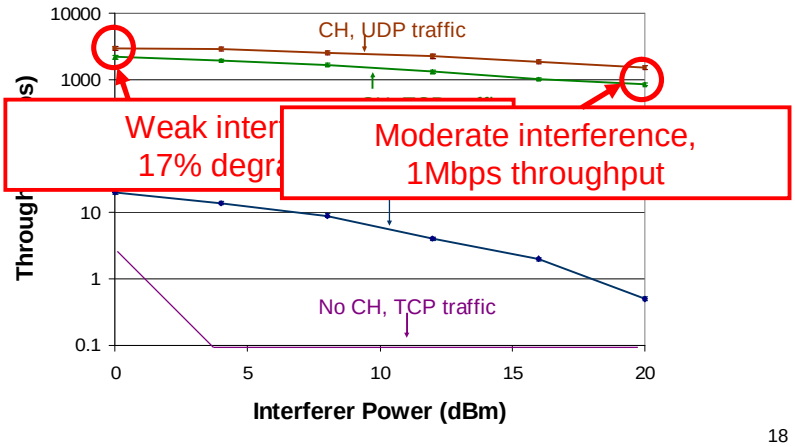
Rapid channel hopping

- Use existing hardware
  - Design dictated by radio PHY and MAC properties (synchronization, scanning, and switching latencies)
- Design must accommodate adversarial and natural interference **à** channel hopping
  - Test with an oracle-based adversary
- Design overview
  - Packet loss during switching + adversary's search speed **à** 10ms dwell period
  - Next hop is determined using a secure hash chain
  - Triggered only when heavy packet loss is detected

17

Evaluation of channel hopping

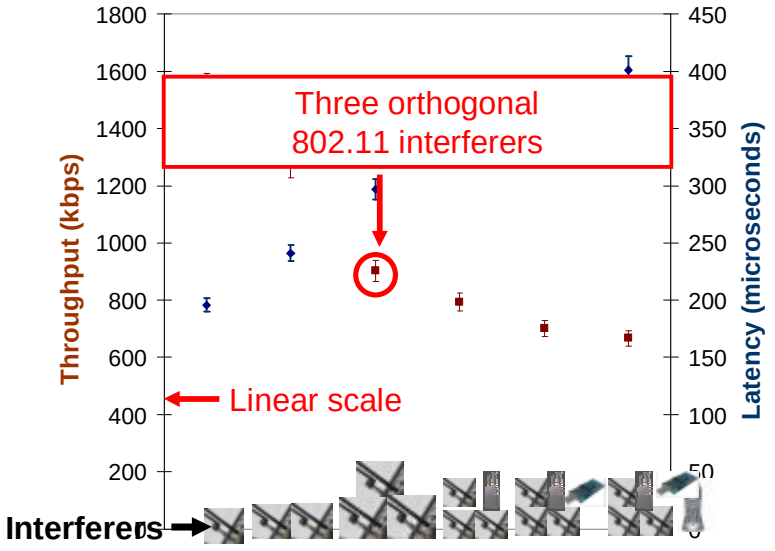
- Good TCP & UDP performance, low loss rate



18

Evaluation of channel hopping

- Acceptable throughput even with multiple interferers



19

Conclusions

- Lot of previous work on RF interference
  - We show 802.11 NICs have additional PHY and MAC fragilities
- Interference causes substantial degradation in commodity NICs
  - Even weak and narrow-band interferers are surprisingly effective
- Changing 802.11 parameters does not mitigate interference, but rapid channel hopping can

20

Thanks!
Questions?

ramki@csail.mit.edu

21