Defending WiFi Networks against Control Channel Attacks

Alireza Vahid, PhD
University of Colorado Denver
Information Theory

Wireless Networking
- Cross-layer design
- Spectrum sharing
- Hardware-algorithm

Comm. Theory & Security
- Control ch. security
- Feedback capacity

Data Storage
- Emerging memory
- Sequence assembly
Future Wireless Networks
Future Wireless Networks
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)

AP

User

Eve

NDP

BFF

Payload

attack
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)
Control Channel Attack on WiFi-6 (-7)

- If the attack is successful, the following control packets (e.g., ACK/NACK) will be likely corrupted.
Control Channel Attack on WiFi-6 (-7)

- If the attack is successful, the following control packets (e.g., ACK/NACK) will be likely corrupted.

- Plan:
  - Quantify the impact
  - Detect
  - Defend
Understanding the fundamentals

- We want to quantify the impact and devise the protocols accordingly.
Understanding the fundamentals

- We want to quantify the impact and devise the protocols accordingly.
- We focus on small ACK/NACK control packets in a broadcast setting.
Denial-of-service attack

- We look at a fundamental model, the packet broadcast channel.
Denial-of-service attack

- We look at a fundamental model, the packet broadcast channel.

- Each user informs the transmitter whether the transmitted packet was received successfully or not.
Denial-of-service attack

- We look at a fundamental model, the packet broadcast channel.
- Each user informs the transmitter whether the transmitted packet was received successfully or not.
- Why this model?
Channel model and baseline
Channel model and baseline

\[ S_i[t] \text{ is Bernoulli } (1-\delta_i) \]

\[ S1[t] \text{ & } S2[t] \text{ distributed independently over time} \]
Channel model and baseline

$S_i[t]$ is Bernoulli $(1-\delta_i)$

$S_1[t]$ & $S_2[t]$ distributed independently over time

Each Rx simply broadcasts its control packet
Channel model and baseline

$S_i[t]$ is Bernoulli $(1-\delta_i)$

$S_1[t]$ & $S_2[t]$ distributed independently over time

Each Rx simply broadcasts its control packet
Channel model and baseline

$S_i[t]$ is Bernoulli $(1 - \delta_i)$

$S_1[t]$ & $S_2[t]$ distributed independently over time

Each Rx simply broadcasts its control packet
Protocol with no attack

\[ \text{Rx}_1, \text{Rx}_2 \]

\[ \mathcal{S}_1[t], \mathcal{S}_2[t] \]

\[ \text{Tx} \]
Protocol with no attack

Send user 1’s packets
Protocol with no attack

Send user 1’s packets
Send user 2’s packets
Protocol with no attack

Send user 1’s packets

Send user 2’s packets

benefit from multicast

$v_1$

$v_2$

$v_1 + v_2$
Denial-of-service attack

Diagram showing interaction between Tx, Rx₁, and Rx₂ with symbols S₁[t] and S₂[t].
Denial-of-service attack

- Is this single-user knowledge still useful?
Denial-of-service attack

- Is this single-user knowledge still useful?
- For MISO BC with continuous feedback, the answer is no!
Denial-of-service attack

- Is this single-user knowledge still useful?
  - For MISO BC with continuous feedback, the answer is no!
  - We have a much brighter picture in packet networks!

Protocol under strong denial-of-attack

Send user 1’s packets
Protocol under strong denial-of-attack

I know what user 1 is missing; and statistically what user 2 gets,
Protocol under strong denial-of-attack

I know what user 1 is missing; and statistically what user 2 gets,
Protocol under strong denial-of-attack

Send user 1’s packets

Send user 2’s packets

I know what user 1 is missing; and statistically what user 2 gets,

We don’t know when user 2 was off! But we know what user 1 receives.
Protocol under strong denial-of-attack

Send user 1’s packets

- I know what user 1 is missing; and statistically what user 2 gets,

Send user 2’s packets

- We don’t know when user 2 was off! But we know what user 1 receives.

benefit from feedback
Protocol under strong denial-of-attack

Send user 1’s packets

I know what user 1 is missing; and statistically what user 2 gets,

Send user 2’s packets

We don’t know when user 2 was off! But we know what user 1 receives.

Benefit from feedback

Resend $\overline{v}_1$ until ACK + Linearly coded $\overline{v}_2$
Protocol under strong denial-of-attack

Send user 1’s packets

I know what user 1 is missing; and statistically what user 2 gets,

Send user 2’s packets

We don’t know when user 2 was off! But we know what user 1 receives.

benefit from feedback

Resend $v_1$ until ACK + Linearly coded $v_2$
Protocol under strong denial-of-attack

Send user 1’s packets

I know what user 1 is missing; and statistically what user 2 gets,

Send user 2’s packets

We don’t know when user 2 was off! But we know what user 1 receives.

Resend $\overline{v}_1$ until ACK + Linearly coded $\overline{v}_2$

No throughput loss!
General denial-of-attack on control channels
General denial-of-attack on control channels

Each Rx simply broadcasts its control packet.

All control channels have some probability of failure.
General denial-of-attack on control channels

Each Rx simply broadcasts its control packet.

All control channels have some probability of failure.

Capacity with intermittent control channels
General denial-of-attack on control channels

Each Rx simply broadcasts its control packet.

All control channels have some probability of failure.

General denial-of-attack on control channels

- Phase 1: Send bits for user 1.

Each Rx simply broadcasts its control packet.

All control channels have some probability of failure.
General denial-of-attack on control channels

Phase 1: Send bits for user 1.
- when there is FB: $v_1$ are the bits at Rx$_2$ needed at Rx$_1$
- when no FB: $\bar{v}_1$ are statistical equations needed at Rx$_1$

Each Rx simply broadcasts its control packet.

All control channels have some probability of failure.
General denial-of-attack on control channels

- Phase 1: Send bits for user 1.
  - when there is FB: $v_1$ are the bits at Rx$_2$ needed at Rx$_1$
  - when no FB: $\bar{v}_1$ are statistical equations needed at Rx$_1$
- Phase 2: Send bits for user 2. Create $\bar{v}_2$ and $v_2$.

Each Rx simply broadcasts its control packet.

All control channels have some probability of failure.
General denial-of-attack on control channels

- Phase 1: Send bits for user 1.
  - when there is FB: $v_1$ are the bits at Rx$_2$ needed at Rx$_1$
  - when no FB: $\bar{v}_1$ are statistical equations needed at Rx$_1$
- Phase 2: Send bits for user 2. Create $\bar{v}_2$ and $v_2$.
- Phase 3: send the summation of $v_1$ & $v_2$.
General denial-of-attack on control channels

- Phase 1: Send bits for user 1.
  - when there is FB: $v_1$ are the bits at Rx$_2$ needed at Rx$_1$
  - when no FB: $\bar{v}_1$ are statistical equations needed at Rx$_1$
- Phase 2: Send bits for user 2. Create $\bar{v}_2$ and $v_2$.
- Phase 3: send the summation of $v_1$ & $v_2$.
- Recursion: Use $\bar{v}_1$ & $\bar{v}_2$ as inputs to Phase 1.

Each Rx simply broadcasts its control packet.
All control channels have some probability of failure.
The available control channels have sub-bit capacity!
Extreme environment

The available control channels have sub-bit capacity!
Extreme environment

The available control channels have sub-bit capacity!

Distortion-Based Outer-Bounds
The available control channels have sub-bit capacity!
Extreme environment

The available control channels have sub-bit capacity!

Rate-distortion theory gives us the minimum attainable distortion.

Distortion-Based Outer-Bounds
The available control channels have sub-bit capacity!

Rate-distortion theory gives us the minimum attainable distortion.

Remaining theoretical questions

- How do the results scale?
How do the results scale?

What is the delay implications of the protocols?
Remaining theoretical questions

- How do the results scale?
- What is the delay implications of the protocols?
- The extreme sub-bit regime remains open.
Remaining theoretical questions

- How do the results scale?
- What is the delay implications of the protocols?
- The extreme sub-bit regime remains open.
- Spectrum sharing
Remaining theoretical questions

- How do the results scale?
- What is the delay implications of the protocols?
- The extreme sub-bit regime remains open.
- Spectrum sharing
- Can these ideas be incorporated in existing protocols?
Back to WiFi-6 (-7)
Defending WiFi against Control Ch. Attacks
Defending WiFi against Control Ch. Attacks
Defending WiFi against Control Ch. Attacks
Defending WiFi against Control Ch. Attacks

- Desired user will always be at 0° phase, while others see varying phases. (rel. to antenna-selection mod.)
Defending WiFi against Control Ch. Attacks

- Desired user will always be at 0° phase, while others see varying phases. (rel. to antenna-selection mod.)
- Embedding information in radiation pattern fluctuations is itself a worthy direction.

Defending WiFi against Control Ch. Attacks
Defending WiFi against Control Ch. Attacks

- Radiation pattern fluctuations.
- WiFi localization (e.g., time of flight).
- Channel signatures.


Higher frequency bands?
Thank you!

Higher frequency bands?