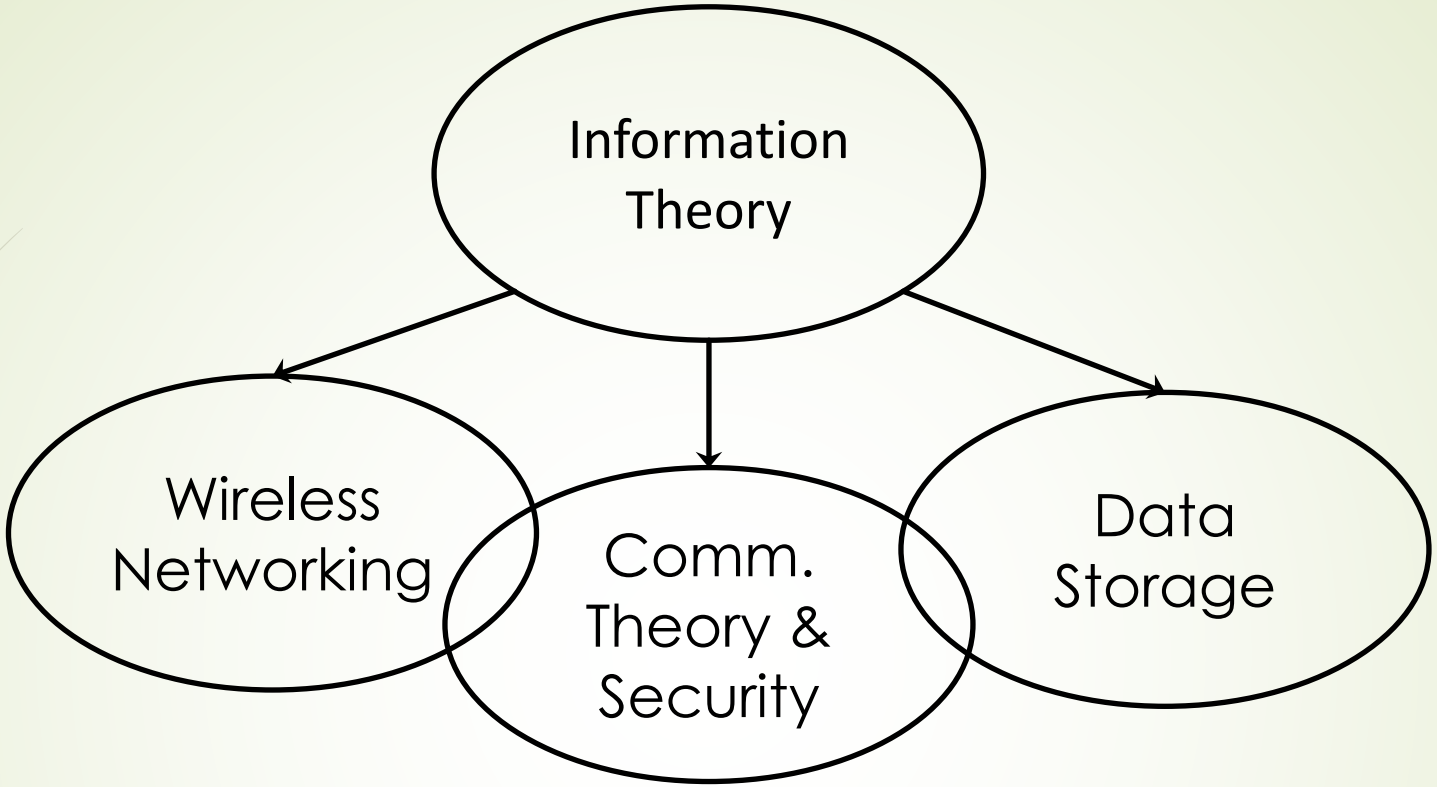
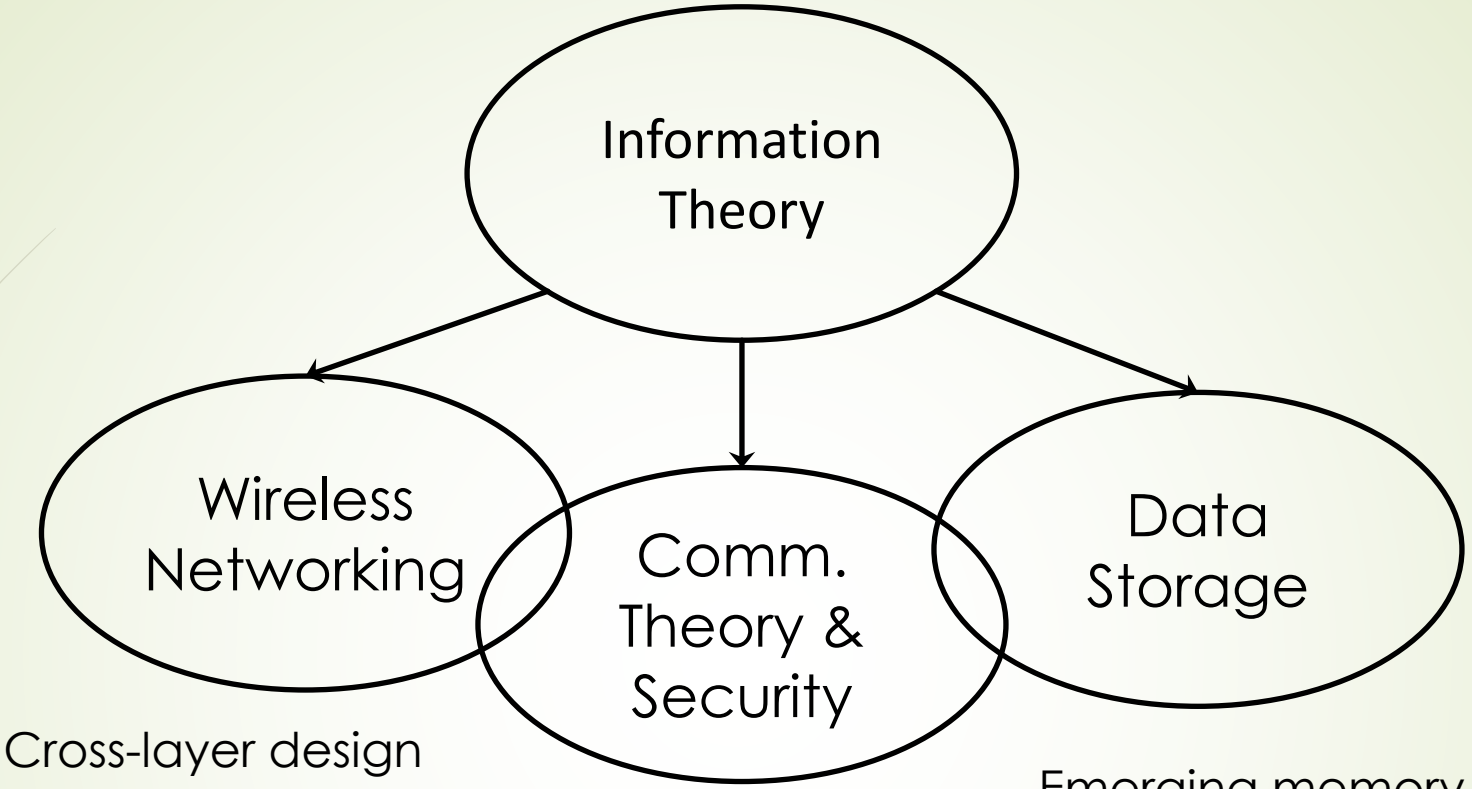
Defending WiFi Networks against Control Channel Attacks

Alireza Vahid, PhD

University of Colorado Denver


Information Theory
Wireless Networking
Comm. Theory & Security
Data Storage



Cross-layer design

Spectrum sharing

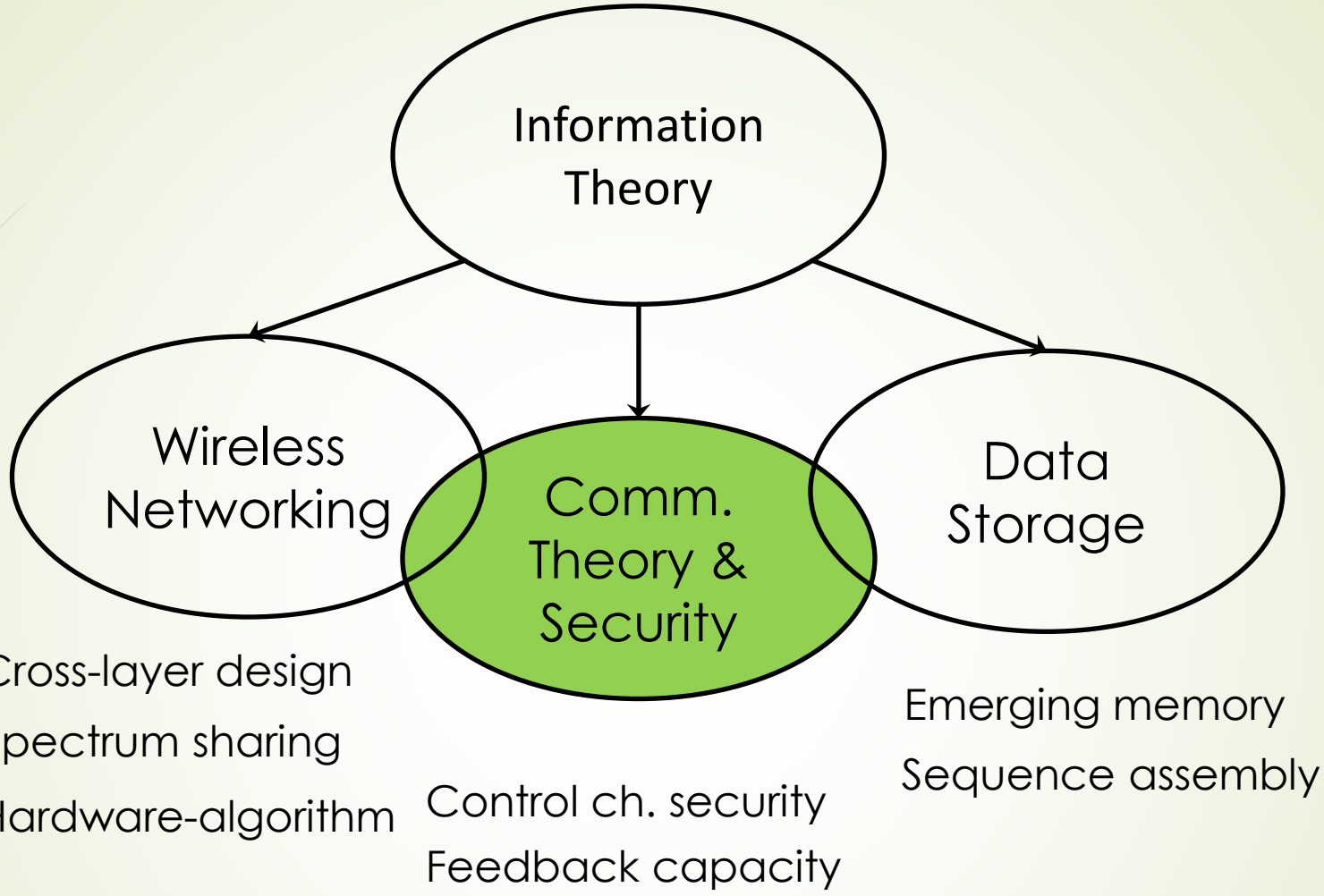
Hardware-algorithm

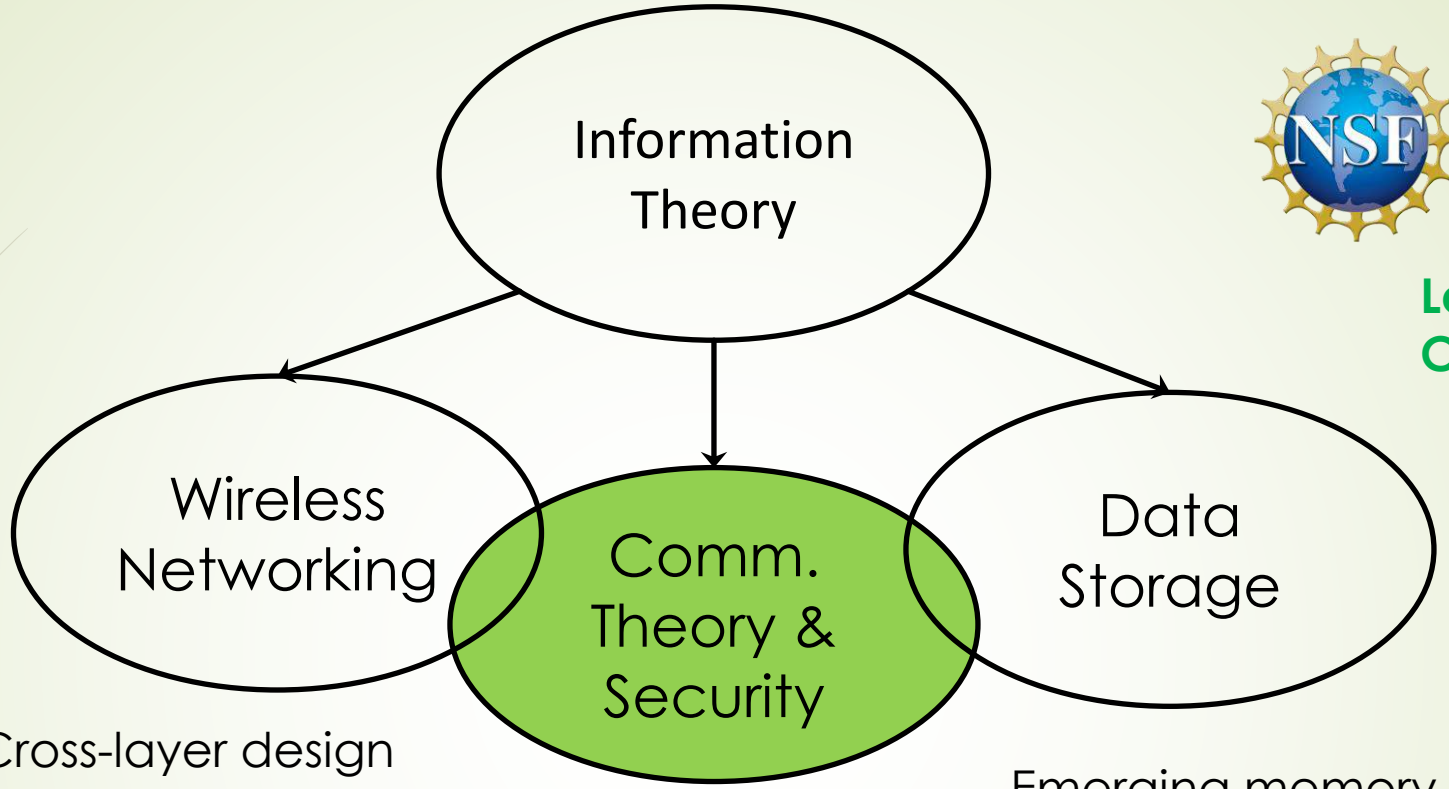
Control ch. security

Feedback capacity

Emerging memory

Sequence assembly


Information Theory
Wireless Networking
Comm. Theory & Security
Data Storage
Cross-layer design
Spectrum sharing
Hardware-algorithm
Control ch. security
Feedback capacity
Emerging memory
Sequence assembly



SWIFT
NRDZ
CNS

Lab Venture Challenge Award!

Cross-layer design
Spectrum sharing
Hardware-algorithm

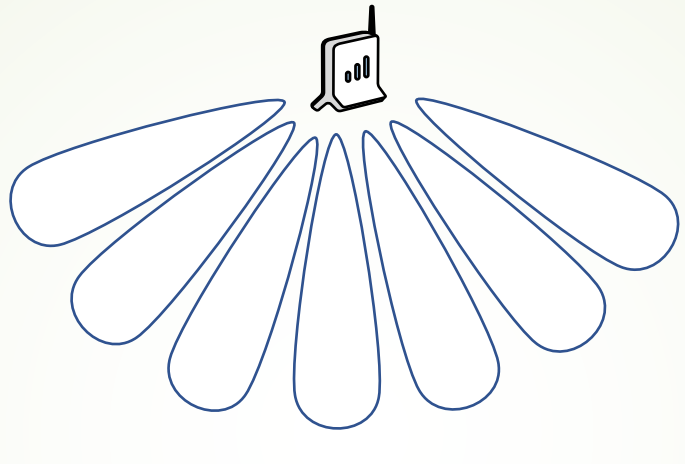
Control ch. security
Feedback capacity

Emerging memory
Sequence assembly

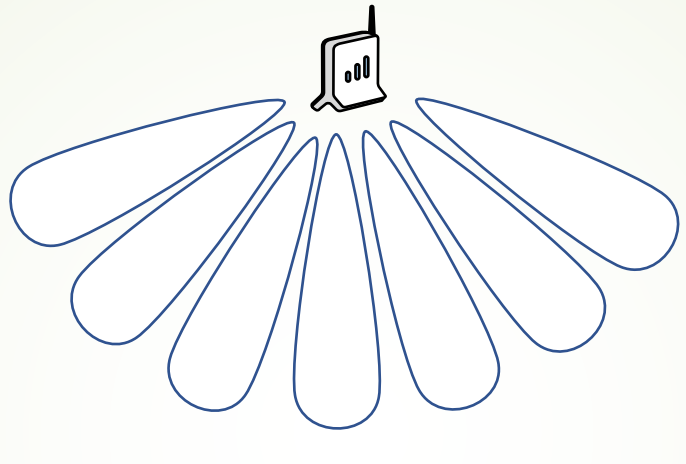
Future Wireless Networks

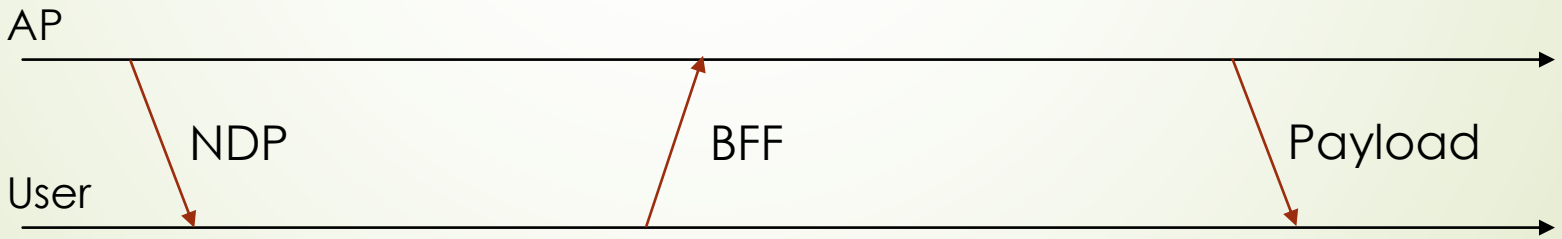
Future Wireless Networks

Control Channel Attack on WiFi-6 (-7)

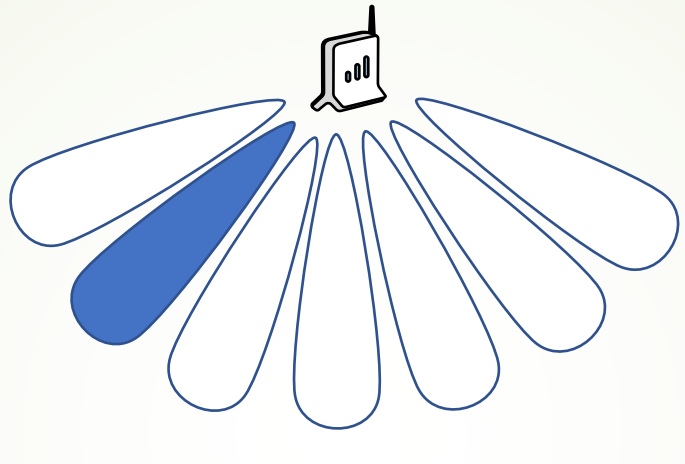


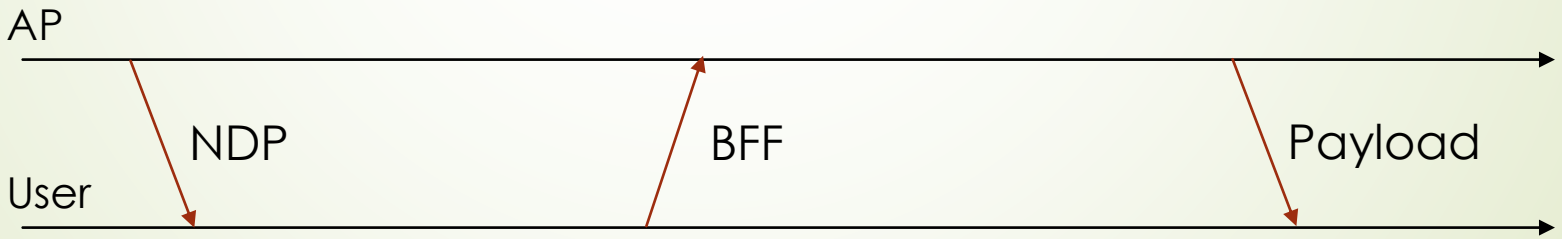
Control Channel Attack on WiFi-6 (-7)



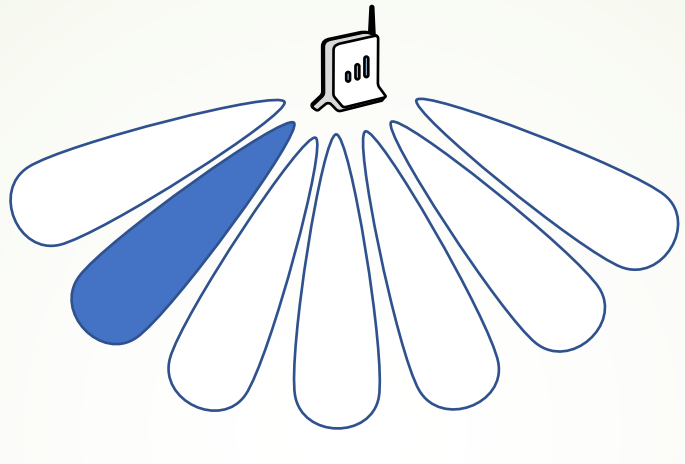


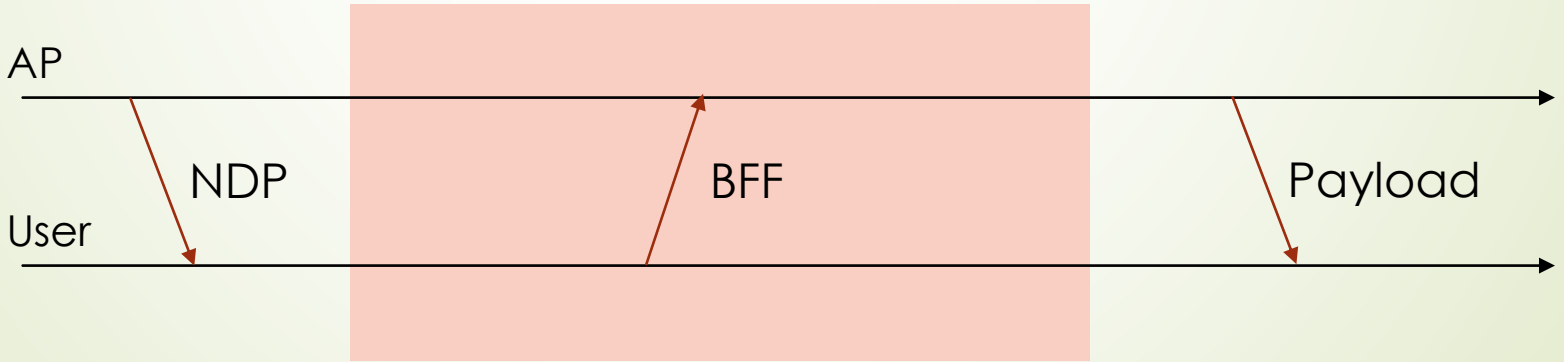
Control Channel Attack on WiFi-6 (-7)



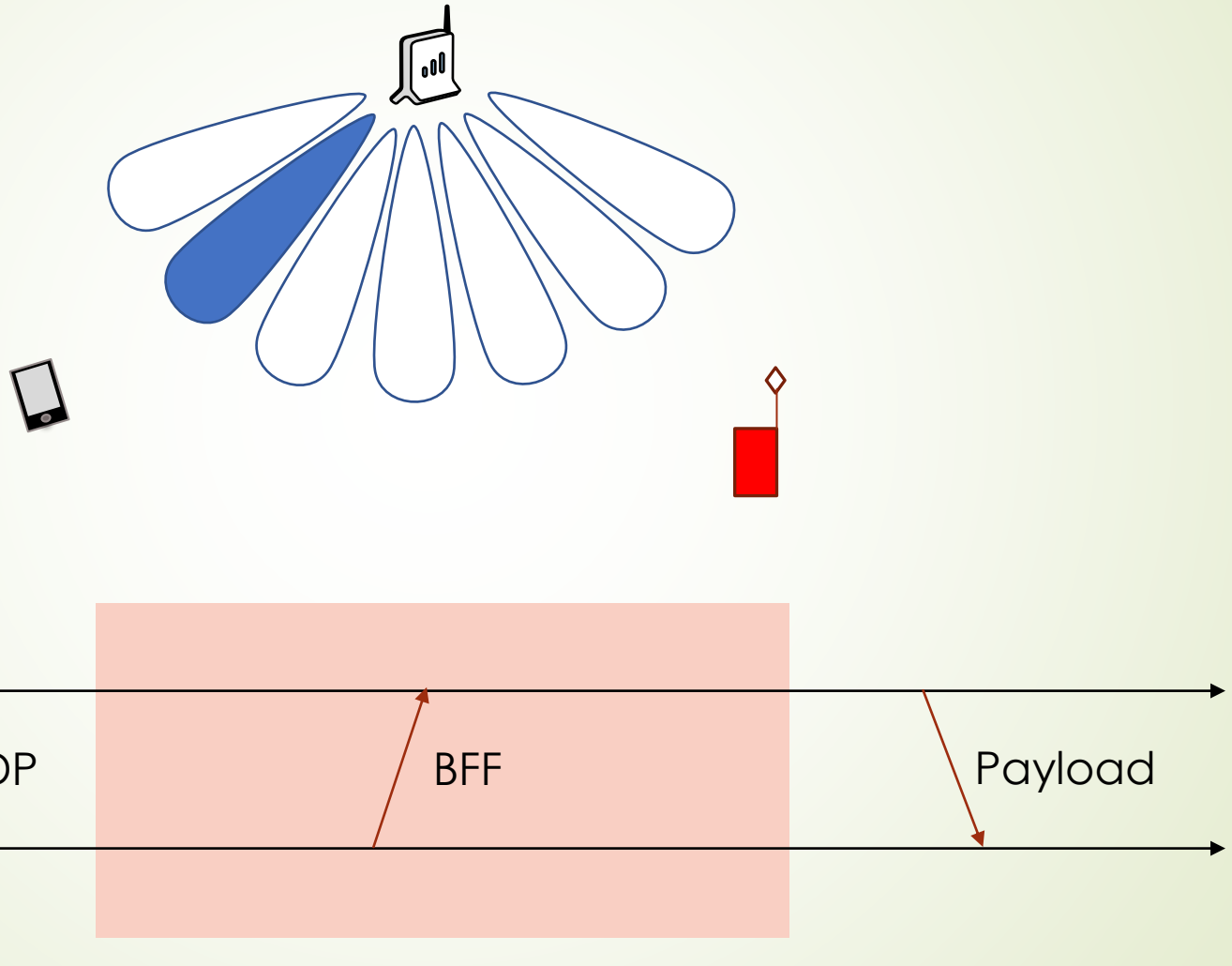


Control Channel Attack on WiFi-6 (-7)

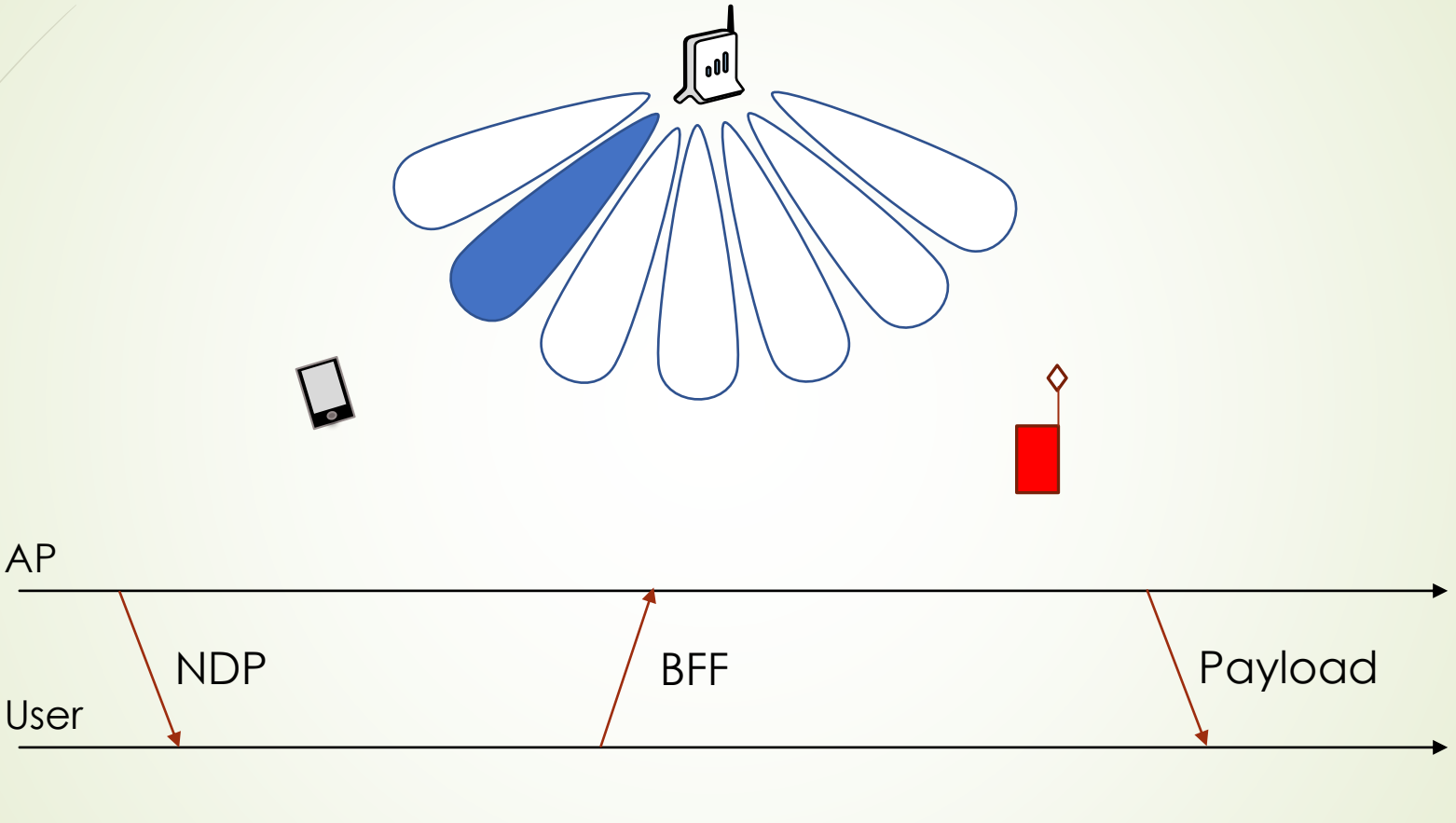




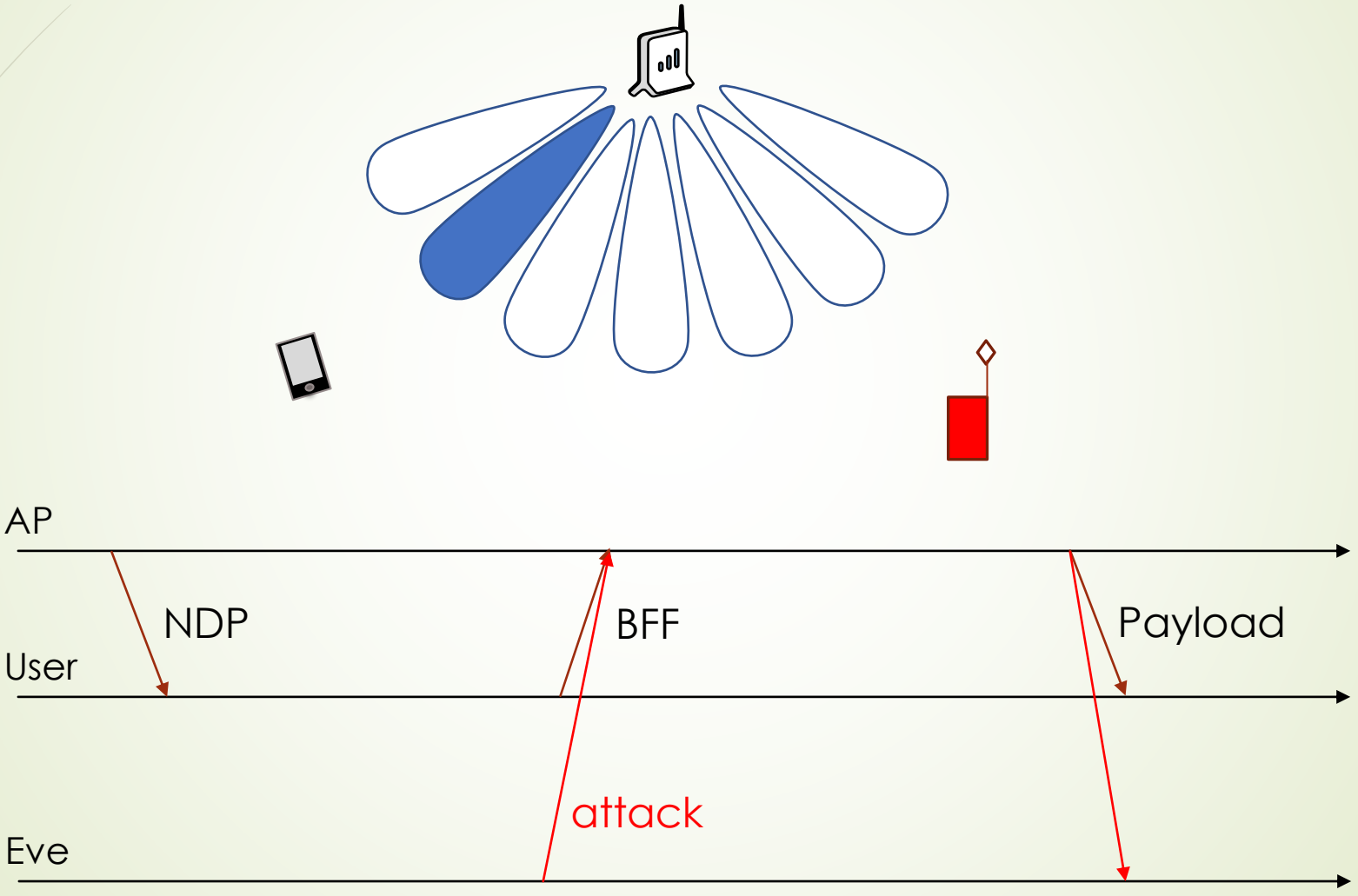
Control Channel Attack on WiFi-6 (-7)



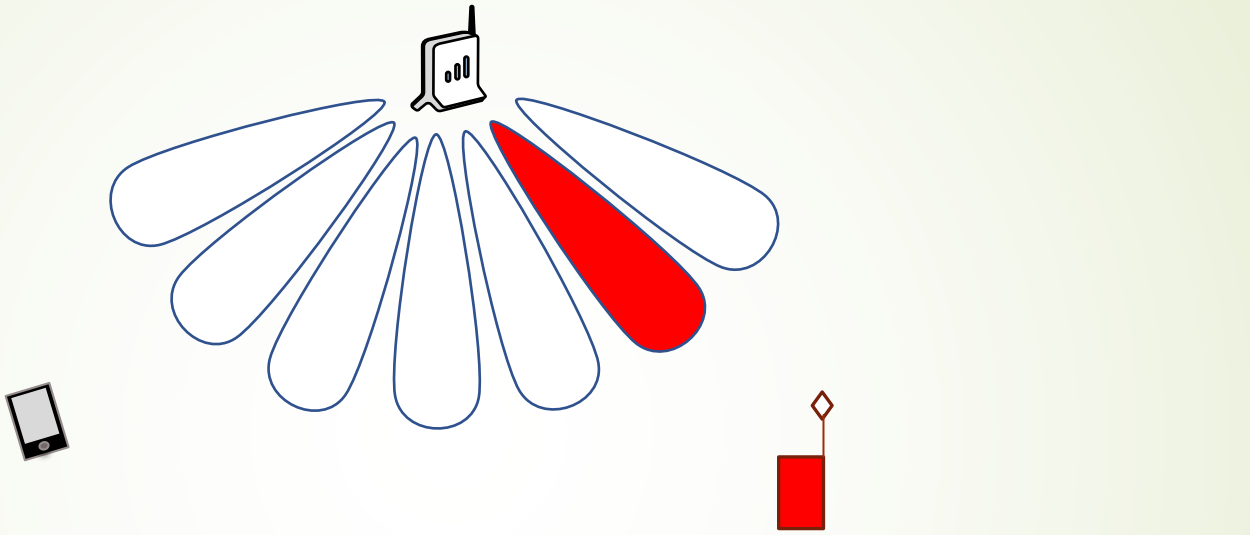
Control Channel Attack on WiFi-6 (-7)

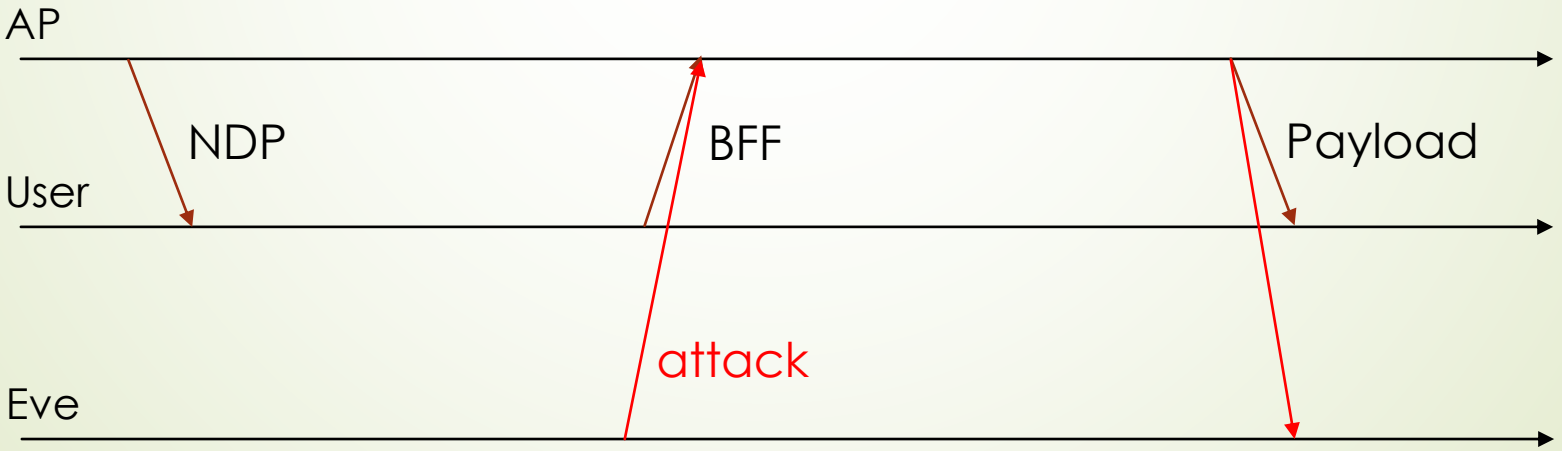


Control Channel Attack on WiFi-6 (-7)

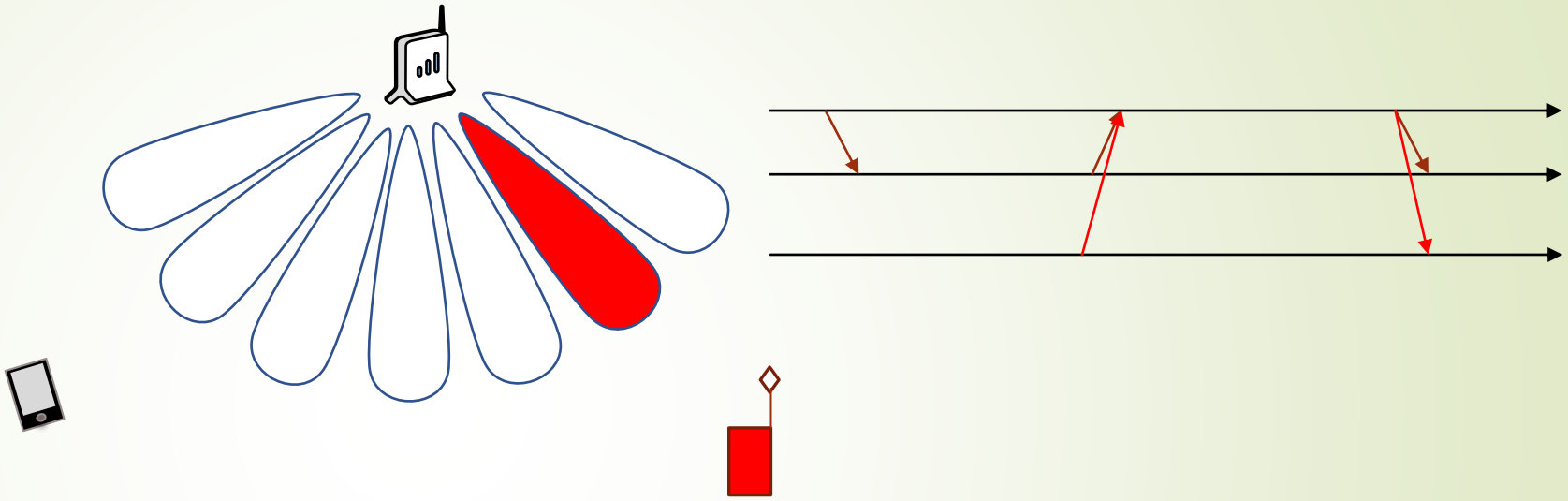


Control Channel Attack on WiFi-6 (-7)

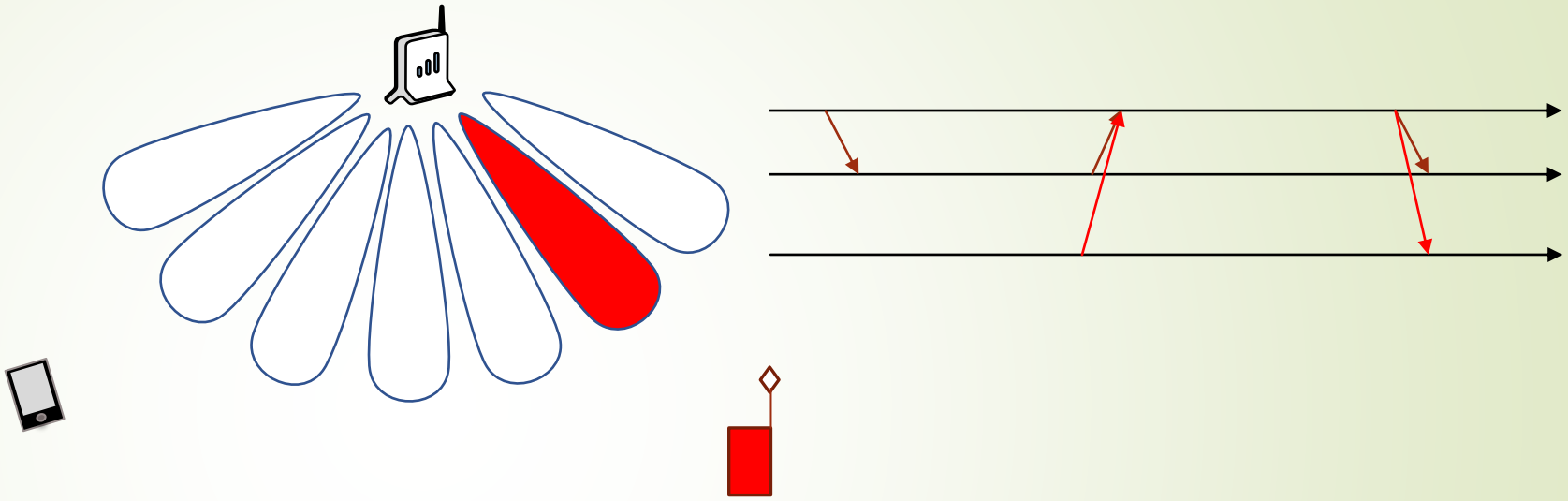




Control Channel Attack on WiFi-6 (-7)

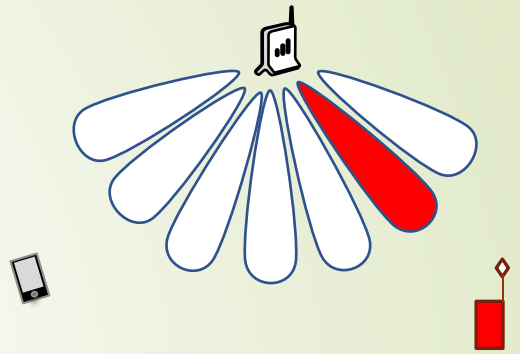


Control Channel Attack on WiFi-6 (-7)

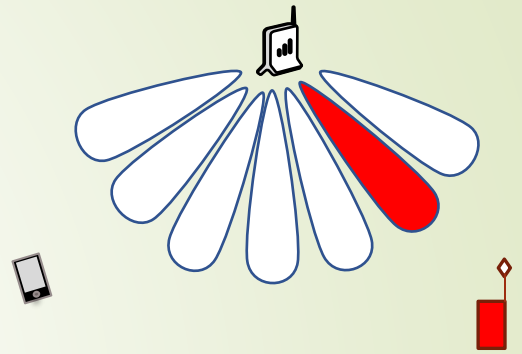


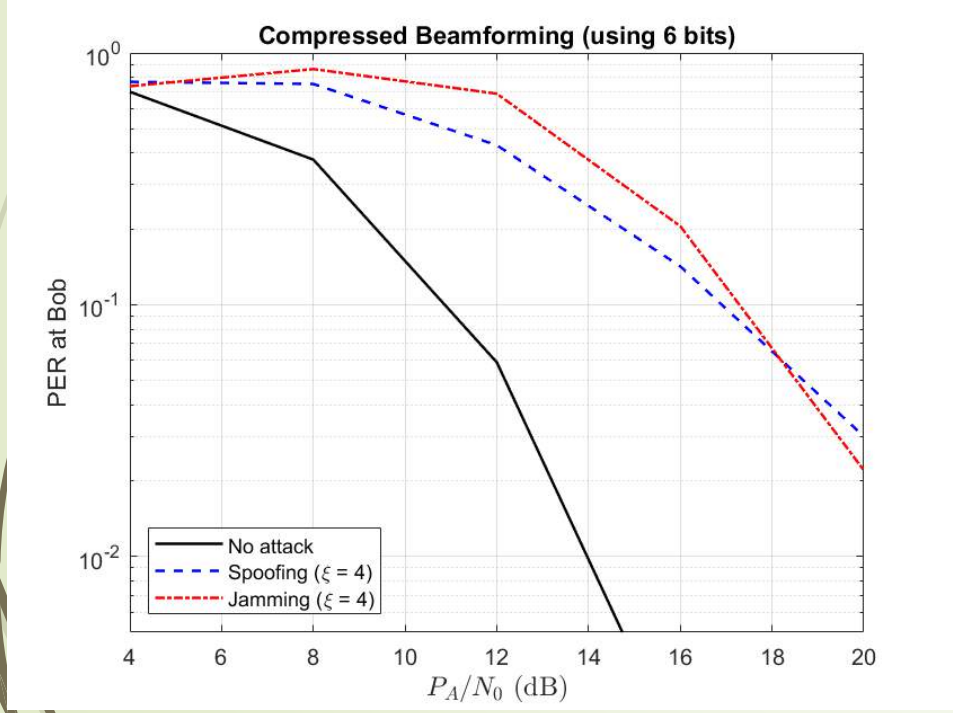
User	Legacy Preamble	RL-SIG	. . . . .	HE-STF	HE-LTF	Data
Eve					HE-LTF	Data

Control Channel Attack on WiFi-6 (-7)

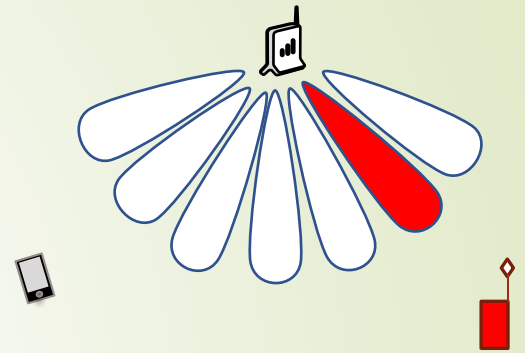


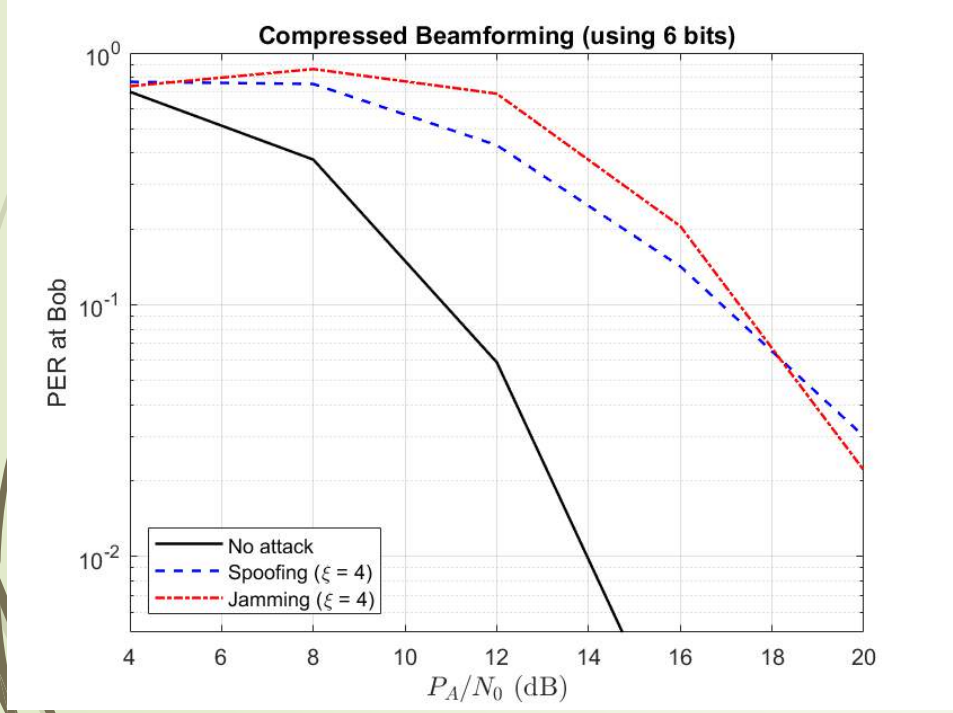
Control Channel Attack on WiFi-6 (-7)

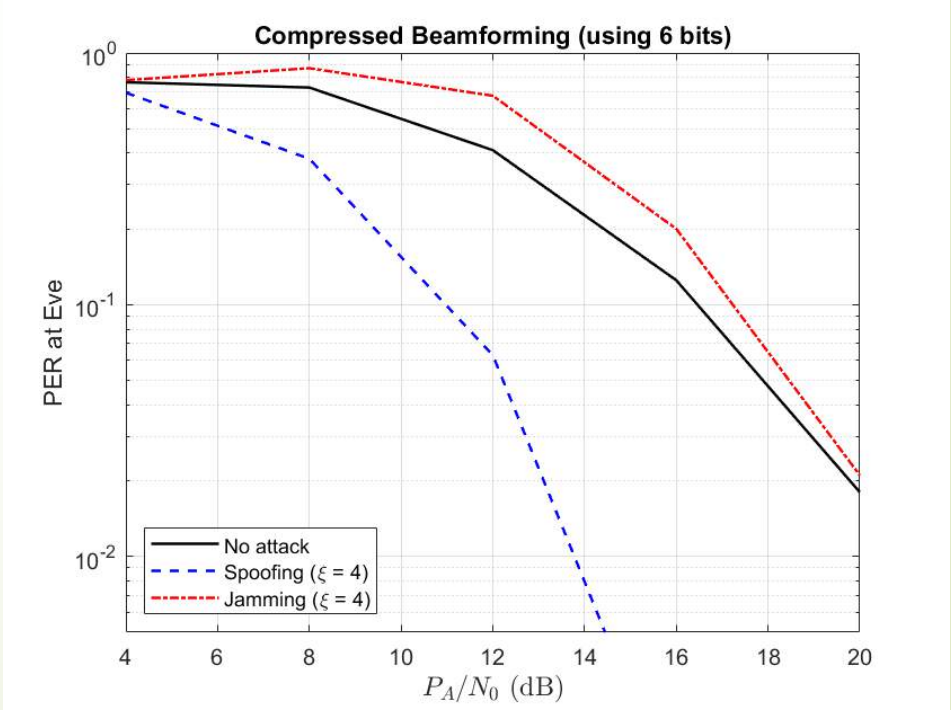




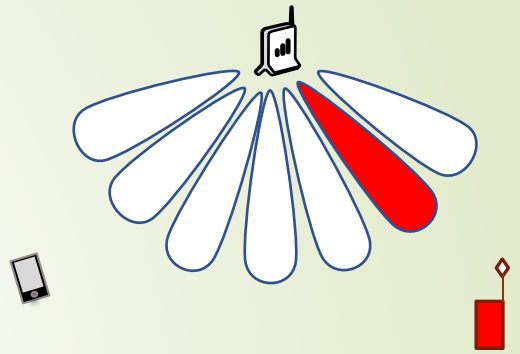
Control Channel Attack on WiFi-6 (-7)



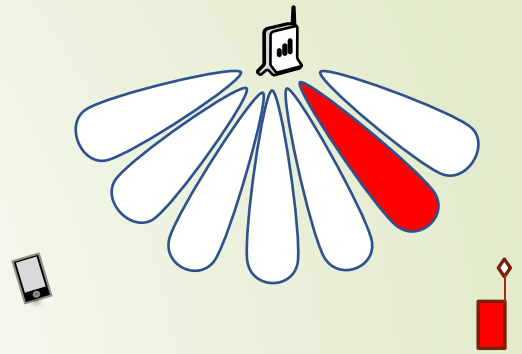




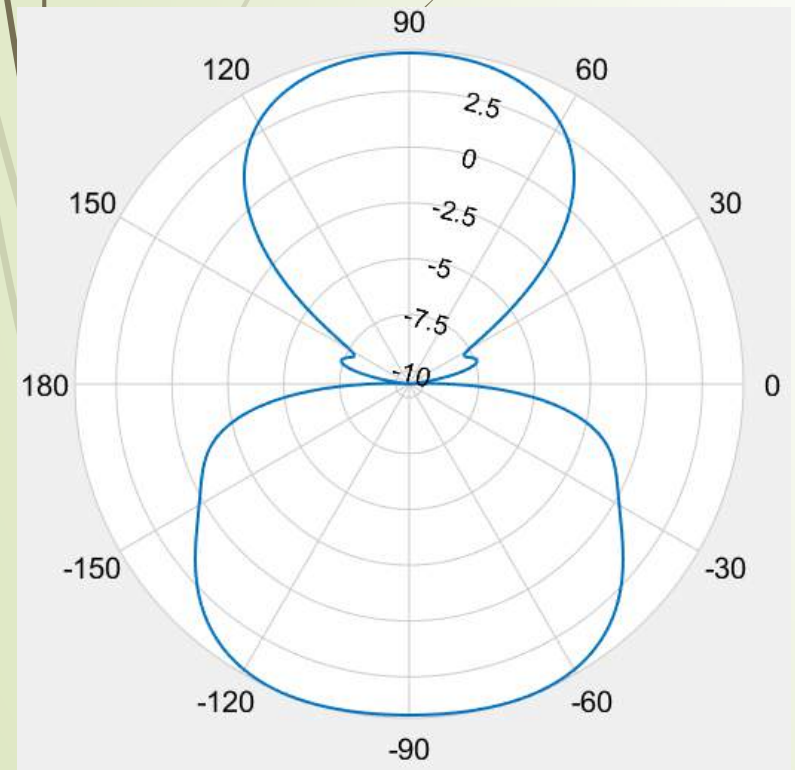
Control Channel Attack on WiFi-6 (-7)



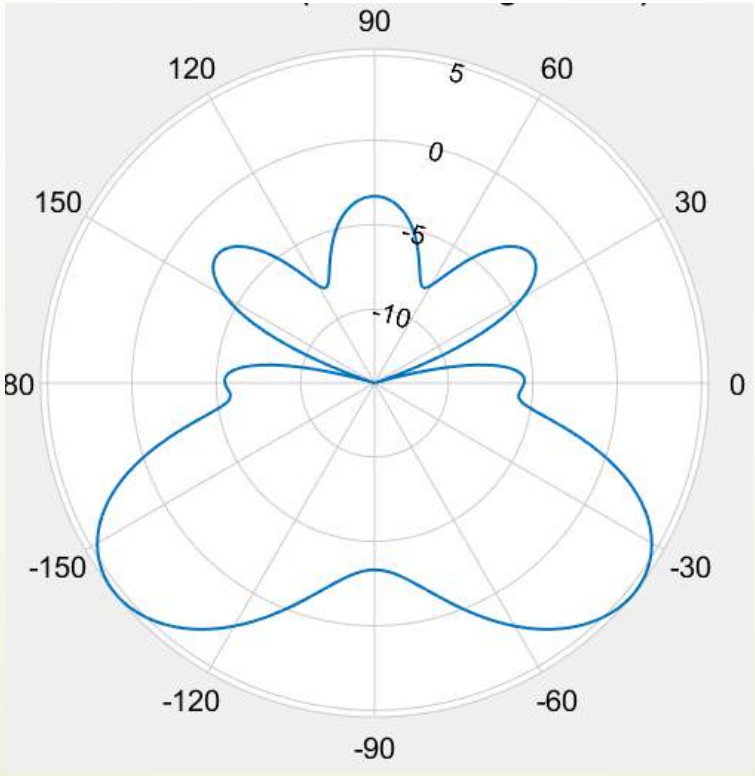
Control Channel Attack on WiFi-6 (-7)



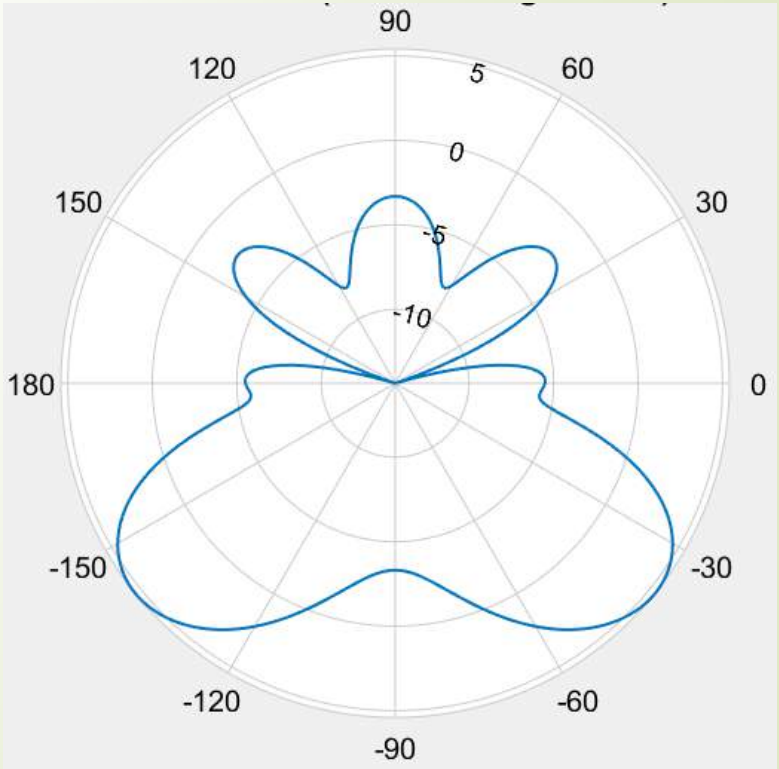
User



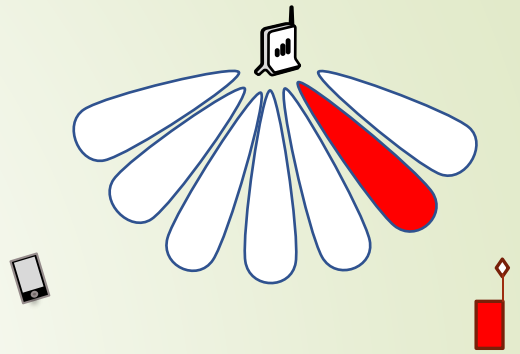
Eve



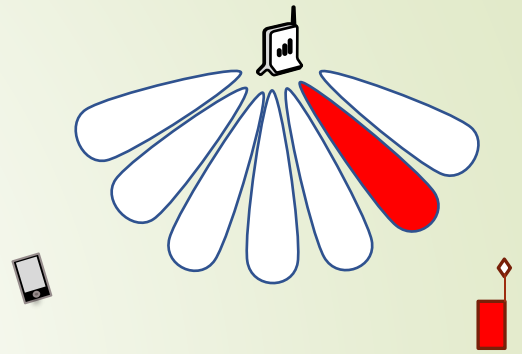
AP



Control Channel Attack on WiFi-6 (-7)

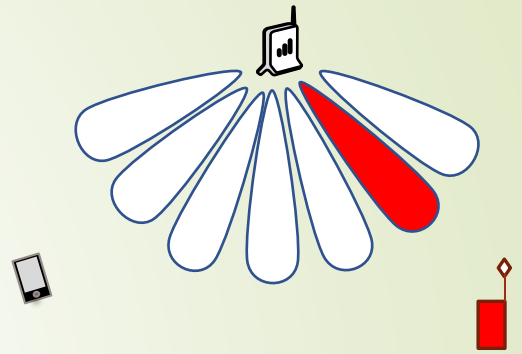


Control Channel Attack on WiFi-6 (-7)



- 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.

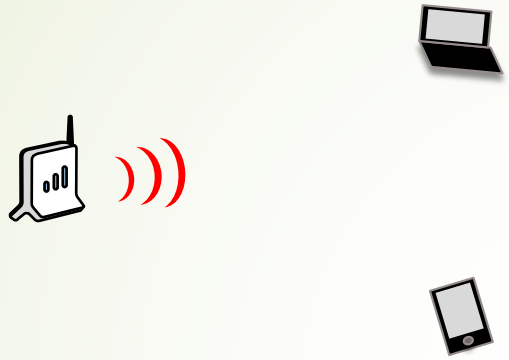
Understanding the fundamentals

- 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

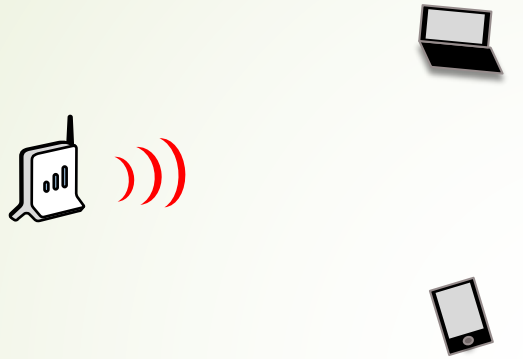
- We look at a fundamental model, the packet broadcast channel.

Denial-of-service attack



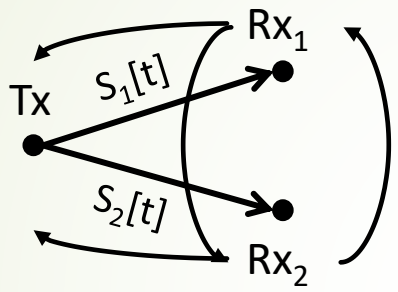
- We look at a fundamental model, the packet broadcast channel.
- Each user informs the transmitter whether the transmitted packet was received successfully or not.

Denial-of-service attack

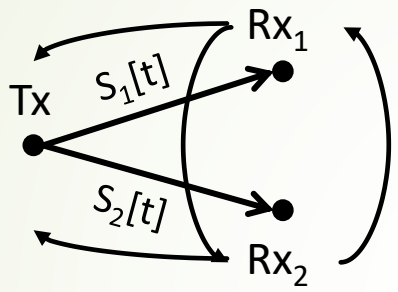


- We look at a fundamental model, the packet broadcast channel.
- Each user informs the transmitter whether the transmitted packet was received successfully or not.
- Why this model?

Channel model and baseline



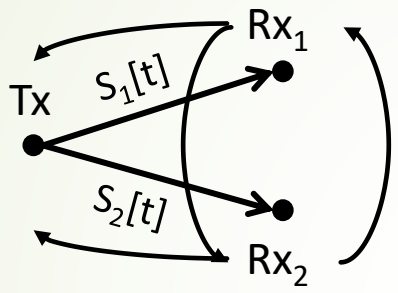
Channel model and baseline



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

S1[t] & S2[t] distributed independently over time

Channel model and baseline

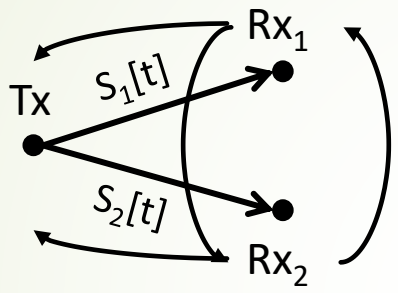


$S_i[t]$ is Bernoulli $(1-\delta_i)$

S1[t] & S2[t] distributed independently over time

Each Rx simply broadcasts its control packet

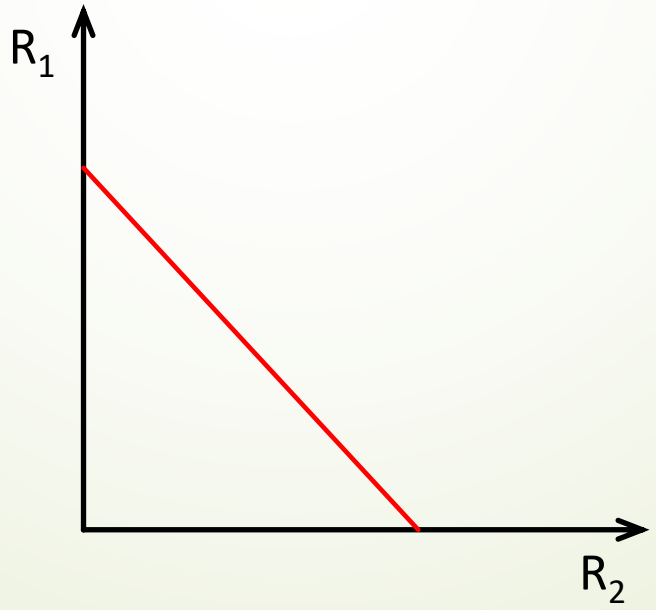
Channel model and baseline



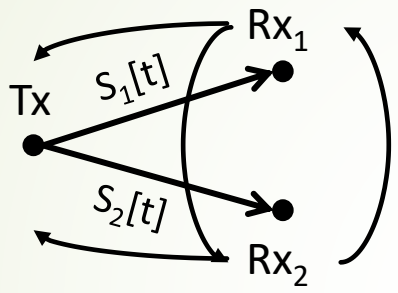
$S_i[t]$ is Bernoulli $(1-\delta_i)$

S1[t] & S2[t] distributed independently over time

Each Rx simply broadcasts its control packet



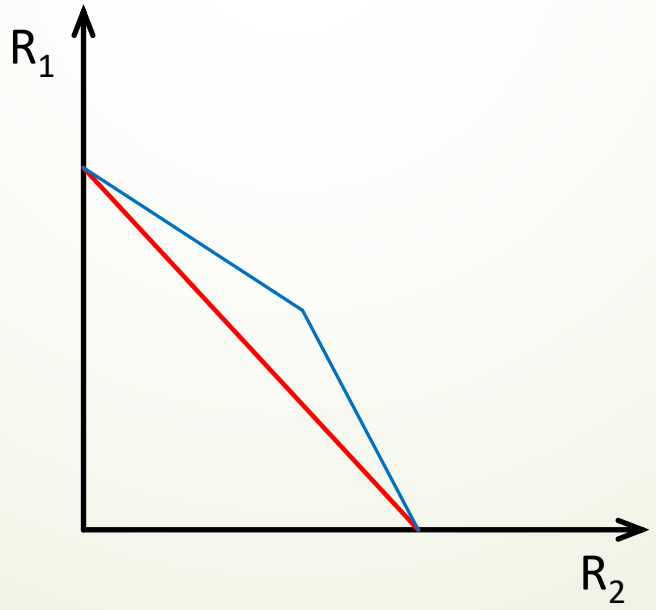
Channel model and baseline



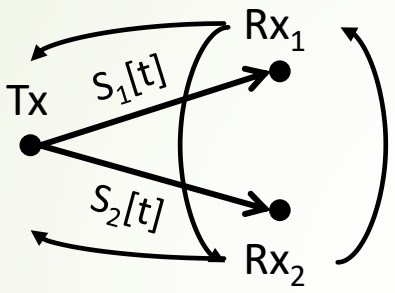
$S_i[t]$ is Bernoulli $(1-\delta_i)$

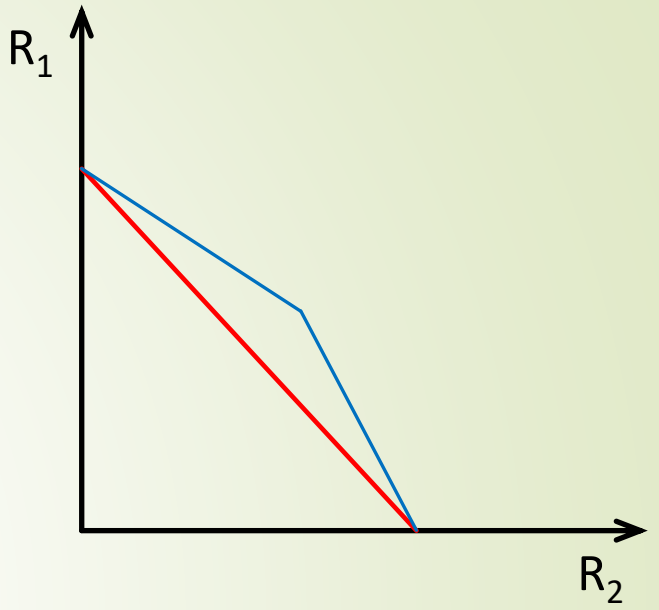
S1[t] & S2[t] distributed independently over time

Each Rx simply broadcasts its control packet

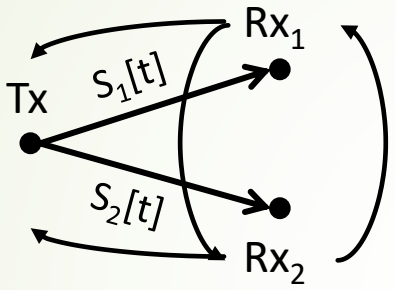


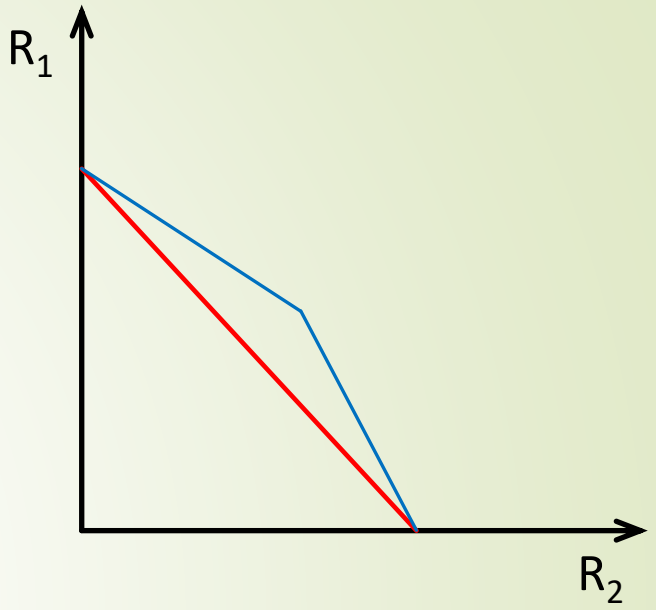
Protocol with no attack



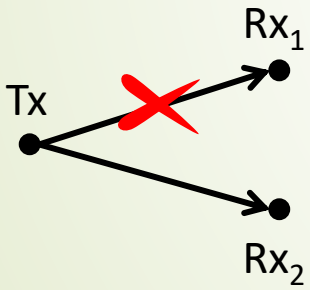


Protocol with no attack



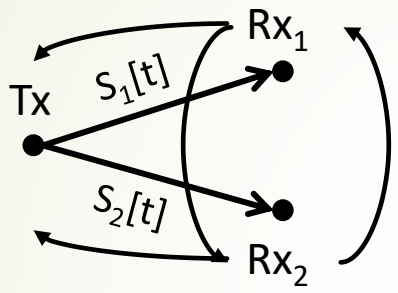


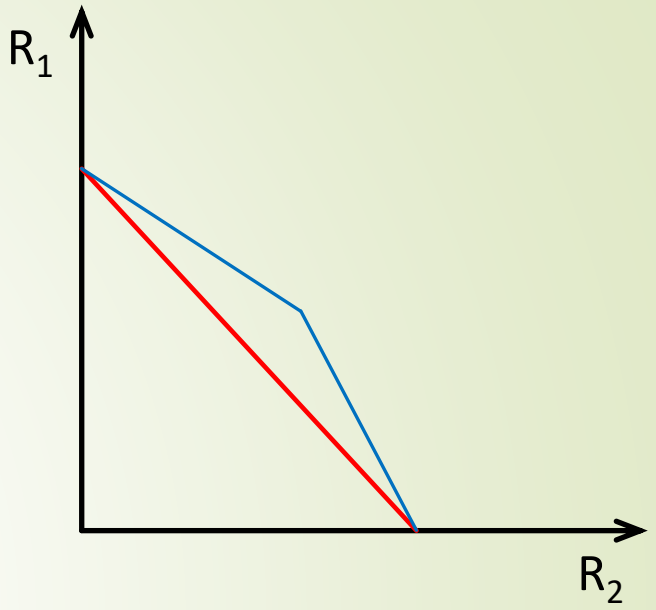
Send user 1's packets



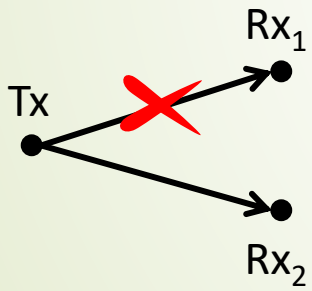
v_1

Protocol with no attack



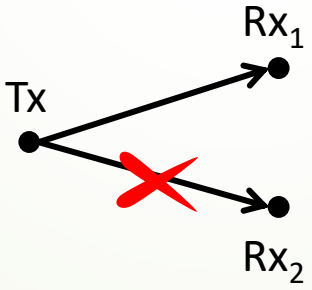


Send user 1's packets



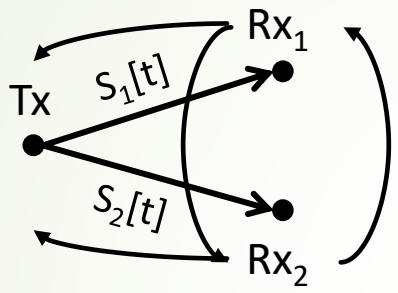
v_1

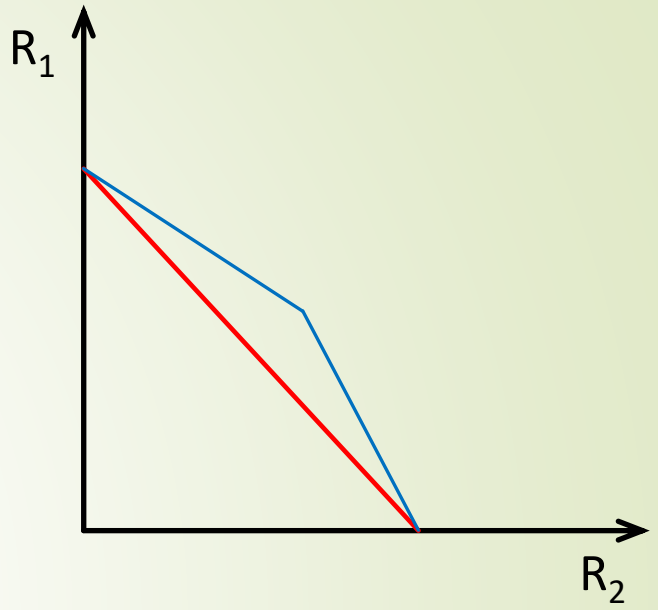
Send user 2's packets



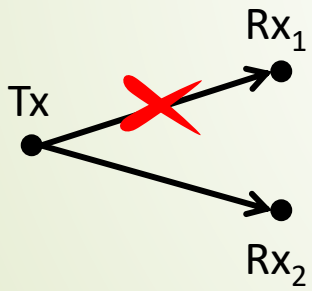
v_2

Protocol with no attack



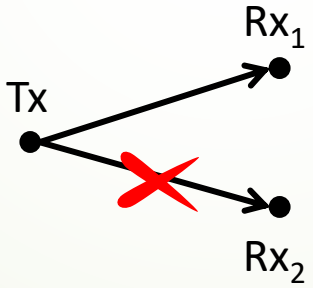


Send user 1's packets



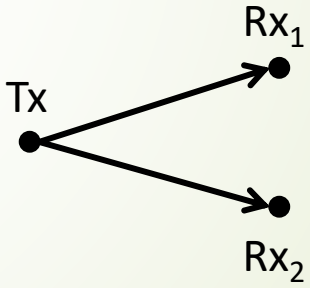
v_1

Send user 2's packets



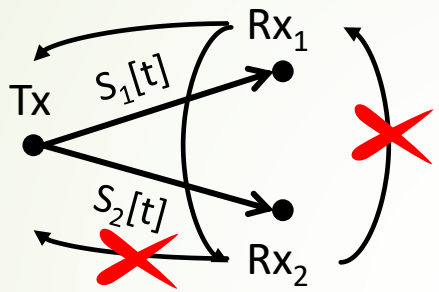
v_2

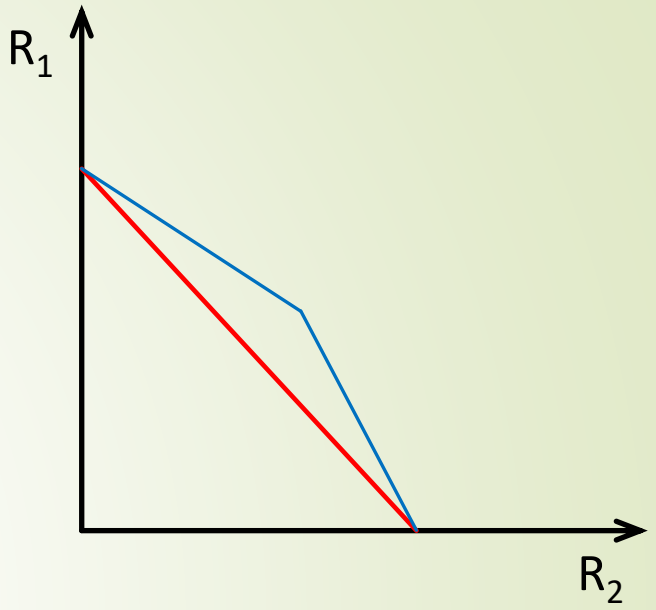
benefit from multicast



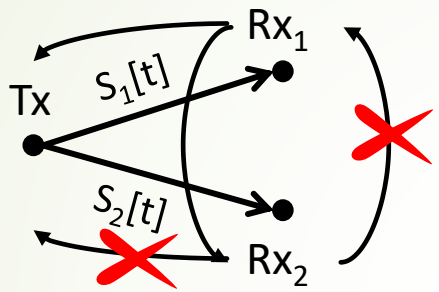
$v_1 + v_2$

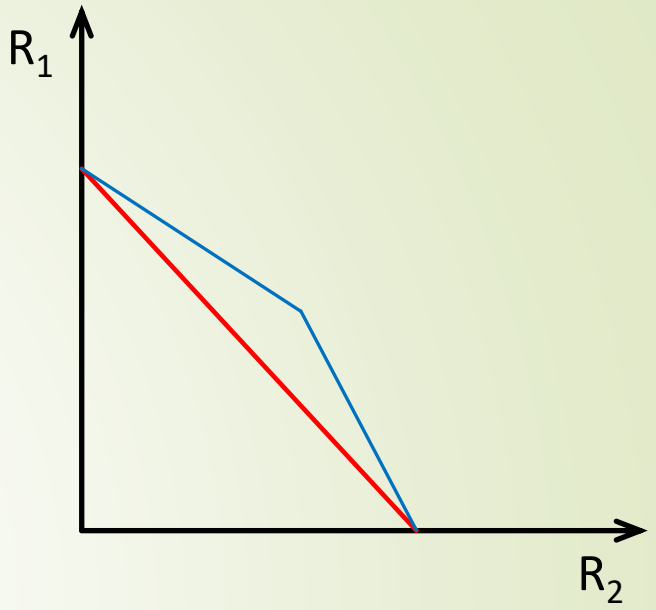
Denial-of-service attack





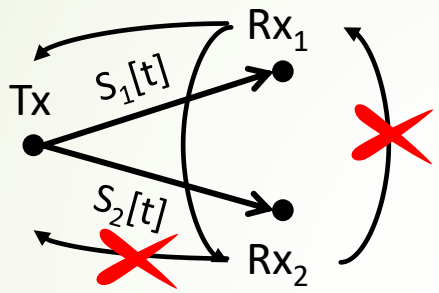
Denial-of-service attack

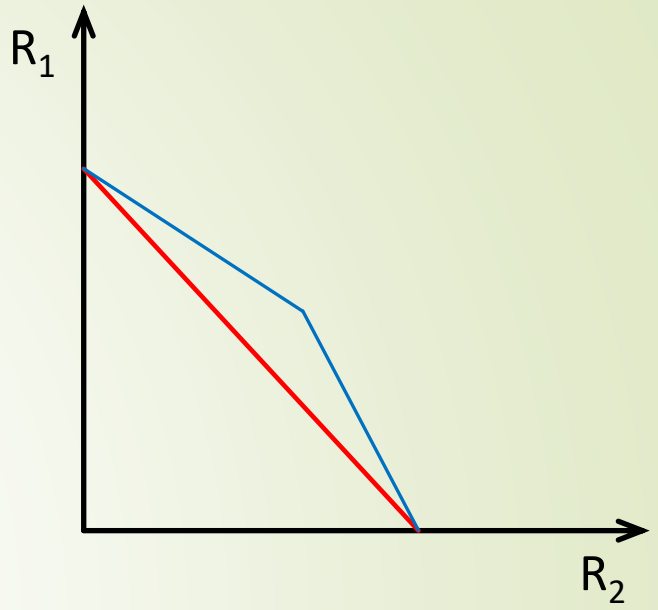




- Is this single-user knowledge still useful?

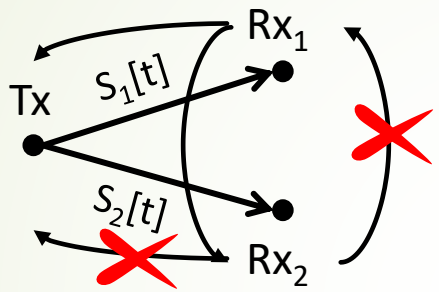
Denial-of-service attack

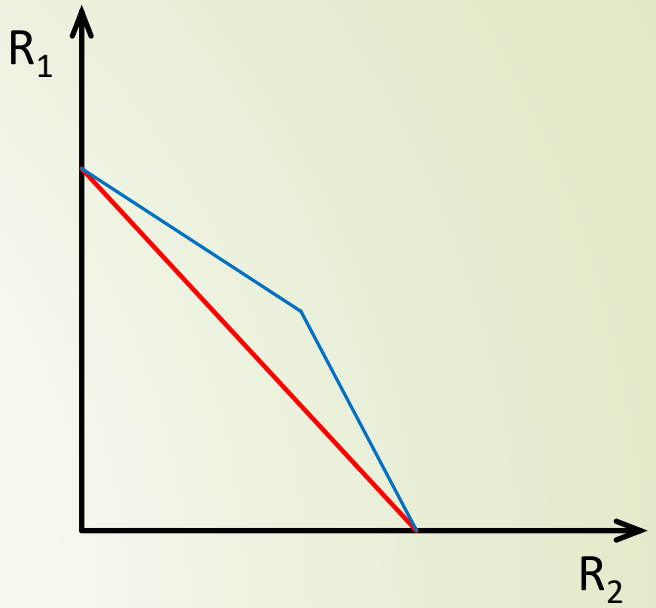




- Is this single-user knowledge still useful?
  - For MISO BC with continuous feedback, the answer is no!

Denial-of-service attack

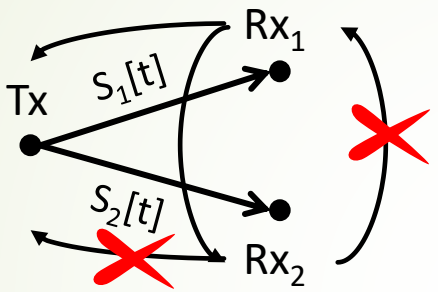




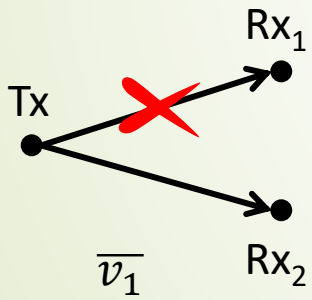
- Is this single-user knowledge still useful?
  - For MISO BC with continuous feedback, the answer is no!
  - We have a much brighter picture in packet networks!

Vahid et. al, "Capacity of broadcast packet erasure channels with single-user delayed CSI," Trans. IT, 2021.

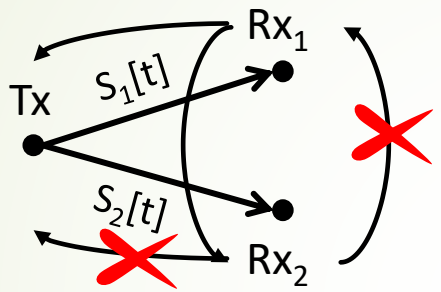
Protocol under strong denial-of-attack



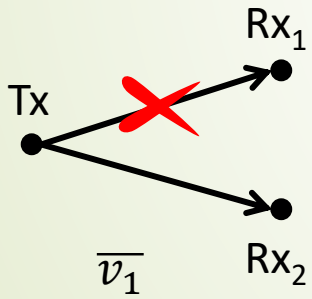
Send user 1's packets



Protocol under strong denial-of-attack

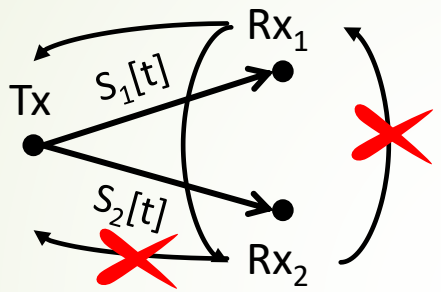


Send user 1's packets

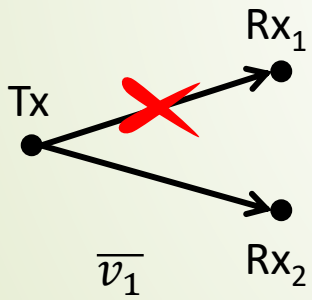


I know what user 1 is missing; and statistically what user 2 gets,

Protocol under strong denial-of-attack

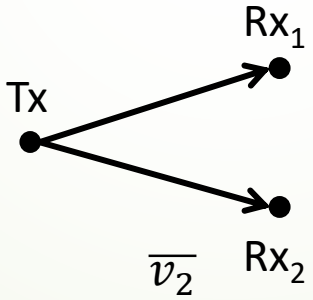


Send user 1's packets

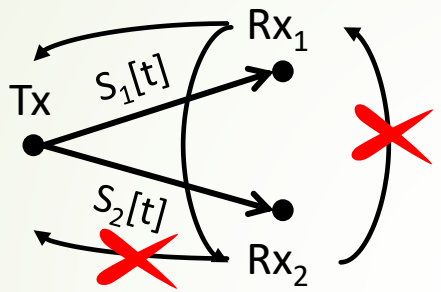


I know what user 1 is missing; and statistically what user 2 gets,

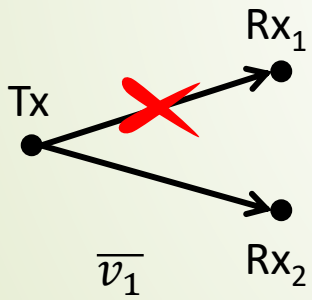
Send user 2's packets



Protocol under strong denial-of-attack

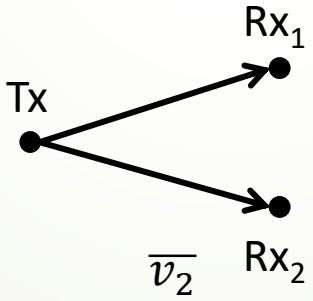


Send user 1's packets



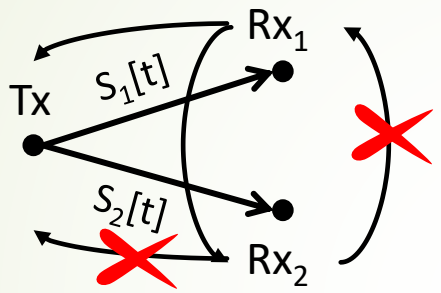
I know what user 1 is missing; and statistically what user 2 gets,

Send user 2's packets

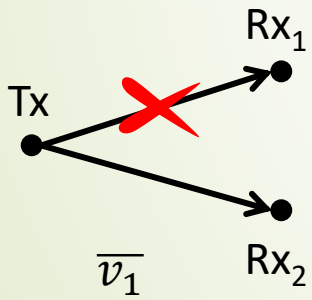


We don't know when user 2 was off! But we know what user 1 receives.

Protocol under strong denial-of-attack

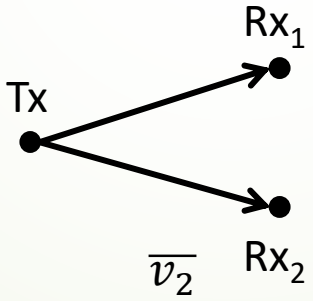


Send user 1's packets



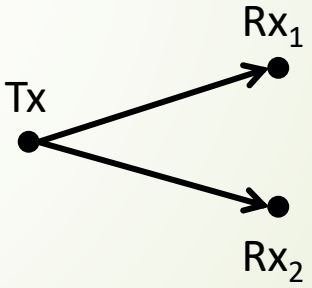
I know what user 1 is missing; and statistically what user 2 gets,

Send user 2's packets

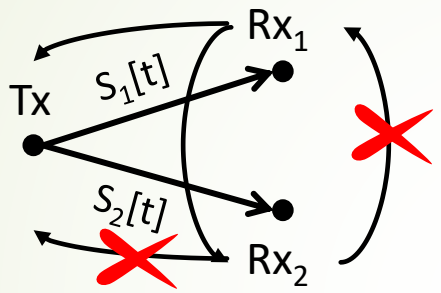


We don't know when user 2 was off! But we know what user 1 receives.

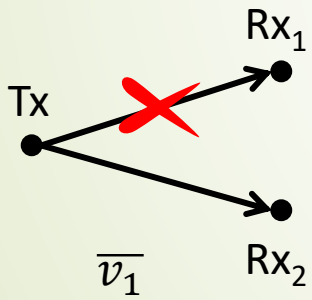
benefit from **feedback**



Protocol under strong denial-of-attack

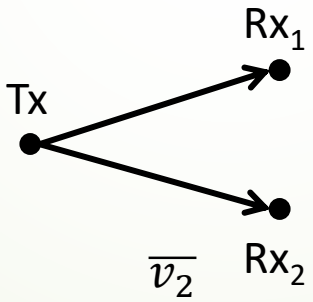


Send user 1's packets



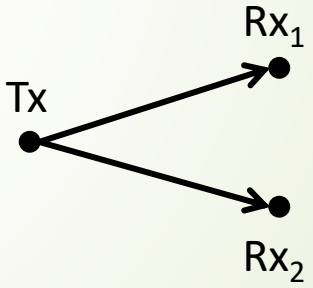
I know what user 1 is missing; and statistically what user 2 gets,

Send user 2's packets



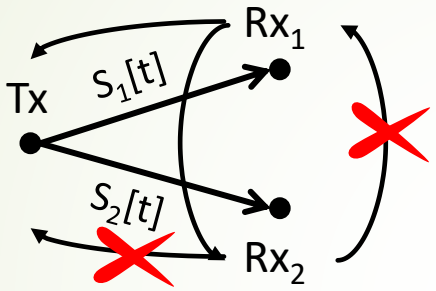
We don't know when user 2 was off! But we know what user 1 receives.

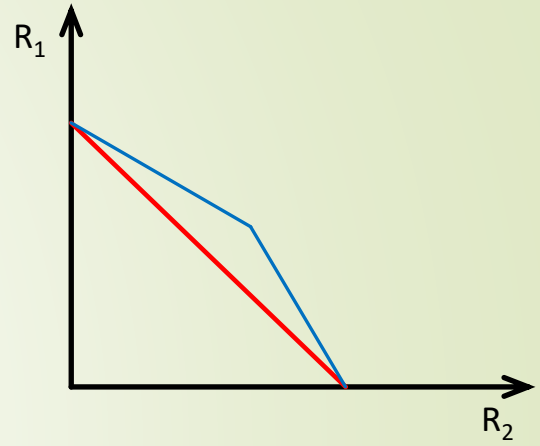
benefit from **feedback**



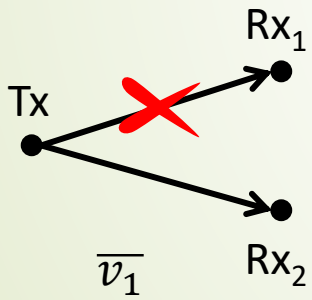
Resend $\overline{v_1}$ until ACK
+
Linearly coded $\overline{v_2}$

Protocol under strong denial-of-attack



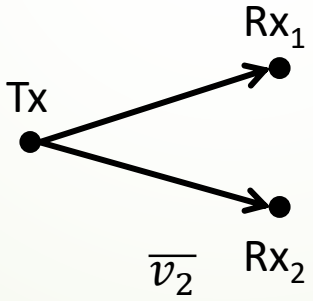


Send user 1's packets



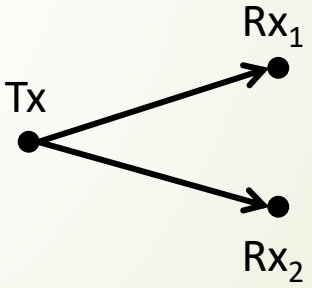
I know what user 1 is missing; and statistically what user 2 gets,

Send user 2's packets



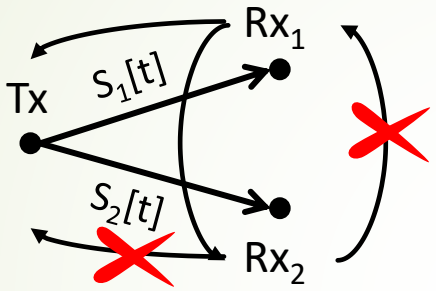
We don't know when user 2 was off! But we know what user 1 receives.

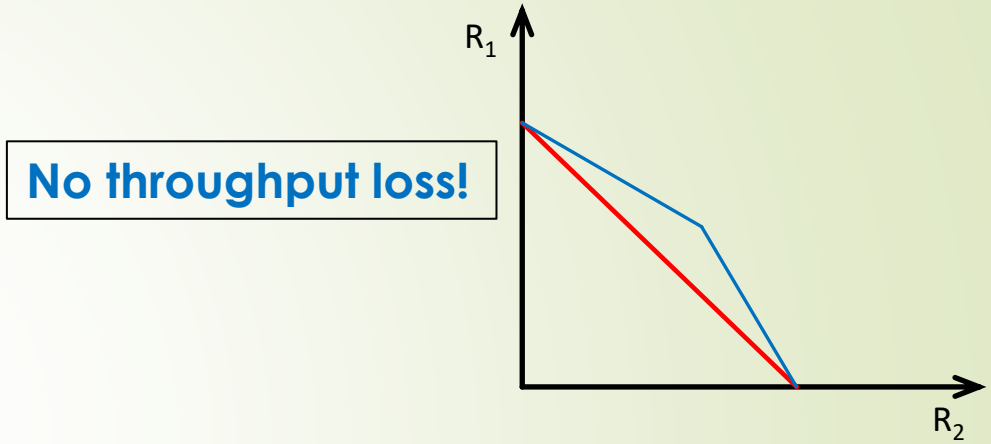
benefit from **feedback**



Resend $\overline{v_1}$ until ACK
+
Linearly coded $\overline{v_2}$

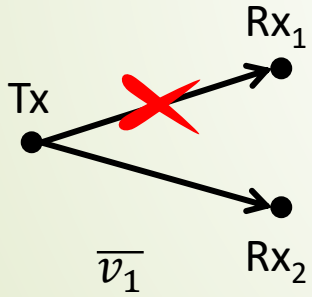
Protocol under strong denial-of-attack





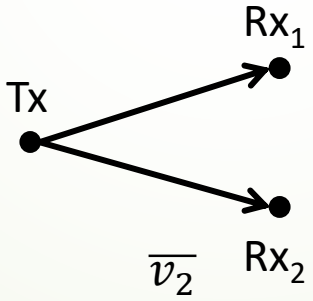
No throughput loss!

Send user 1's packets



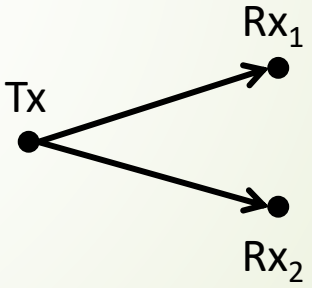
I know what user 1 is missing; and statistically what user 2 gets,

Send user 2's packets



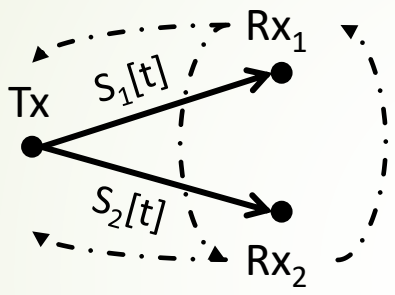
We don't know when user 2 was off! But we know what user 1 receives.

benefit from **feedback**

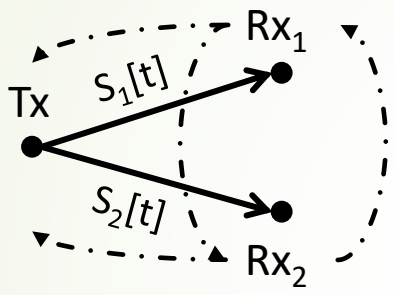


Resend $\overline{v_1}$ until ACK
+
Linearly coded $\overline{v_2}$

General denial-of-attack on control channels



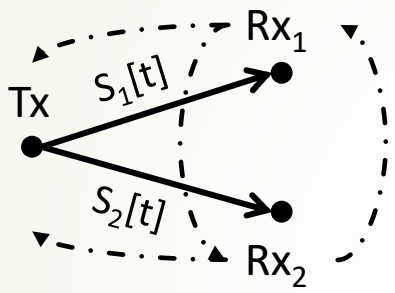
General denial-of-attack on control channels



Each Rx simply broadcasts its control packet.

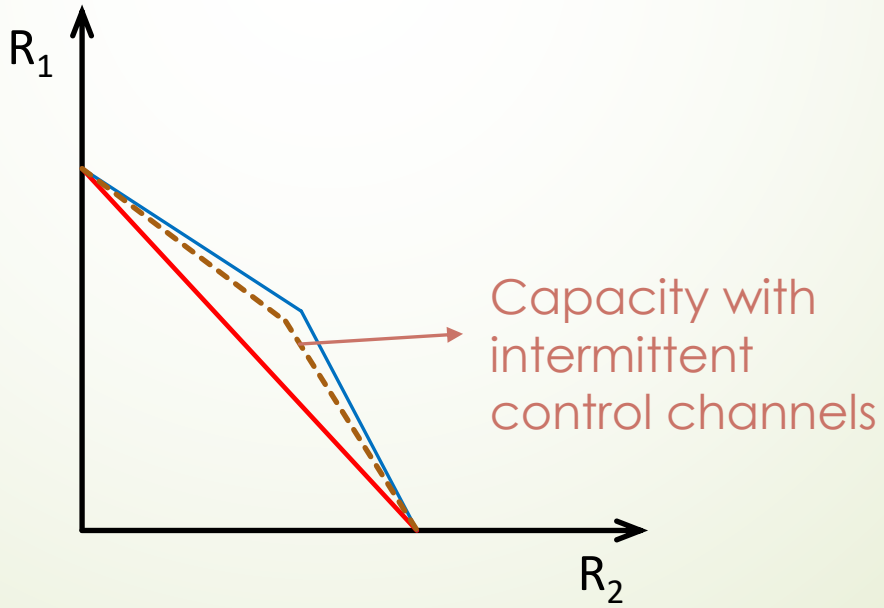
All control channels have some probability of failure.

General denial-of-attack on control channels

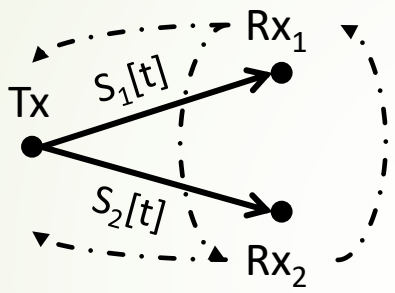


Each Rx simply broadcasts its control packet.

All control channels have some probability of failure.

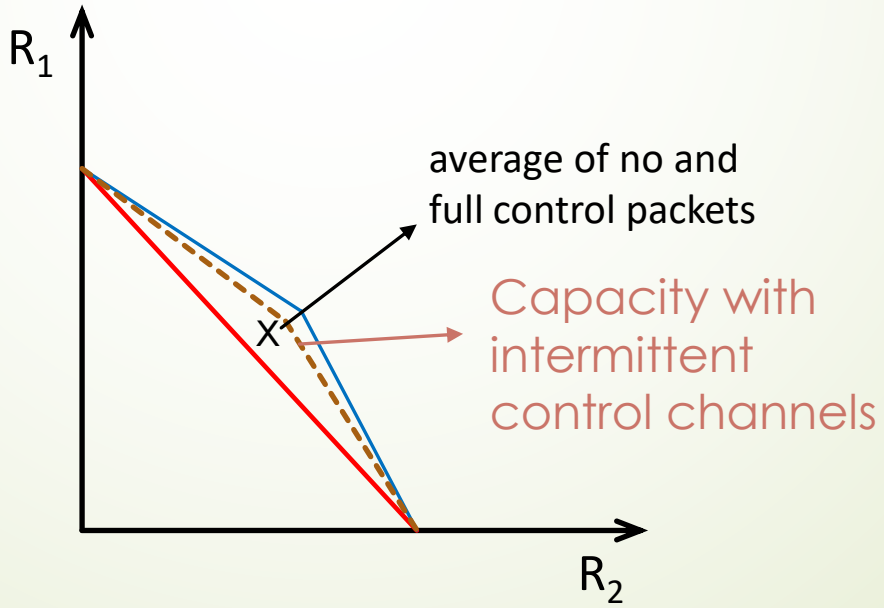


General denial-of-attack on control channels



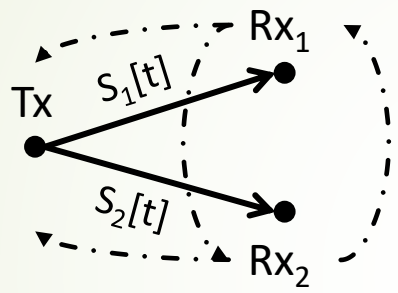
Each Rx simply broadcasts its control packet.

All control channels have some probability of failure.



Vahid et. al, "Erasure broadcast channels with intermittent feedback," Trans. Comm, 2021.

General denial-of-attack on control channels

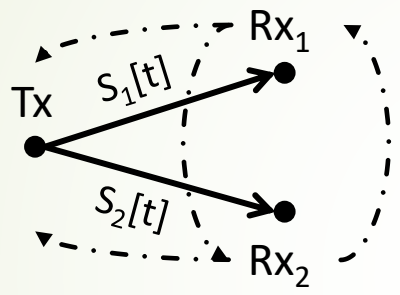


Each Rx simply broadcasts its control packet.

All control channels have some probability of failure.

- Phase 1: Send bits for user 1.

General denial-of-attack on control channels

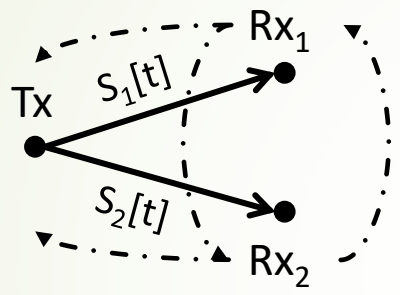


Each Rx simply broadcasts its control packet.

All control channels have some probability of failure.

- 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

General denial-of-attack on control channels

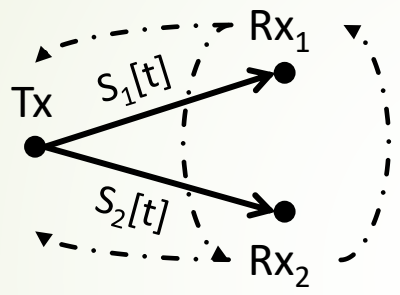


Each Rx simply broadcasts its control packet.

All control channels have some probability of failure.

- 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.

General denial-of-attack on control channels

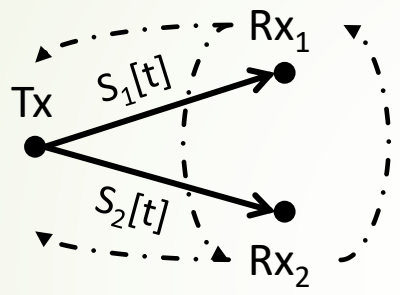


Each Rx simply broadcasts its control packet.

All control channels have some probability of failure.

- 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

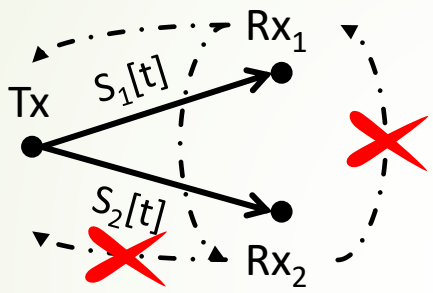


Each Rx simply broadcasts its control packet.

All control channels have some probability of failure.

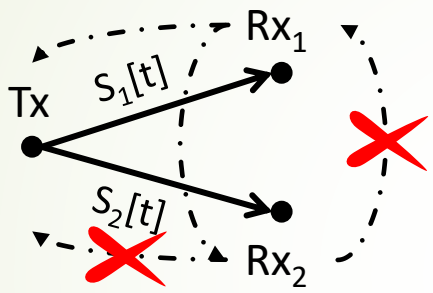
- Phase 1: Send bits for user 1.
  - when there is FB: v_1 are the bits at Rx_2 needed at Rx_1
  - when no FB: $\bar{v}_1$ are statistical equations needed at Rx_1
- Phase 2: Send bits for user 2. Create $\bar{v}_2$ and v_2.
- Phase 3: send the summation of v_1 & v_2.
- Recursion: Use $\bar{v}_1$ & $\bar{v}_2$ as inputs to Phase 1.

Extreme environment

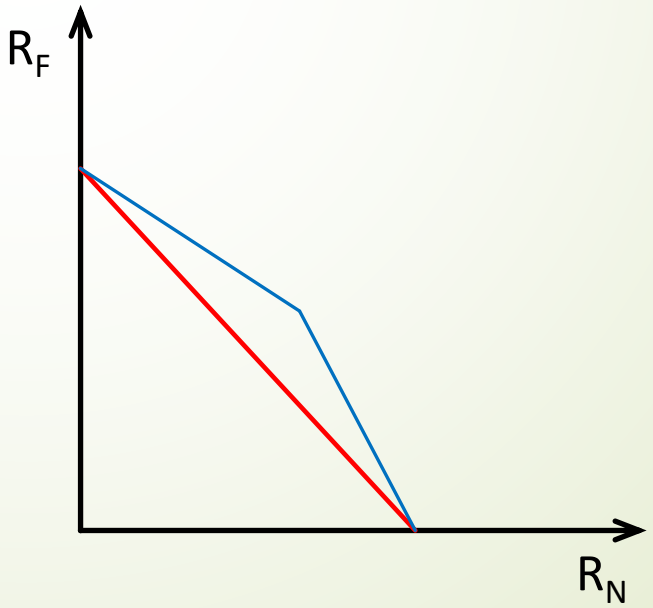


The available control channels have sub-bit capacity!

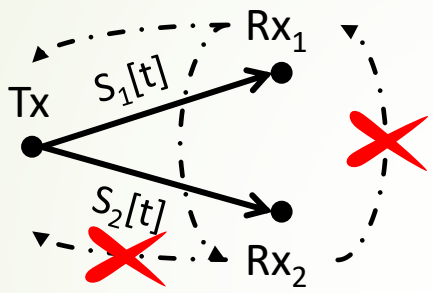
Extreme environment



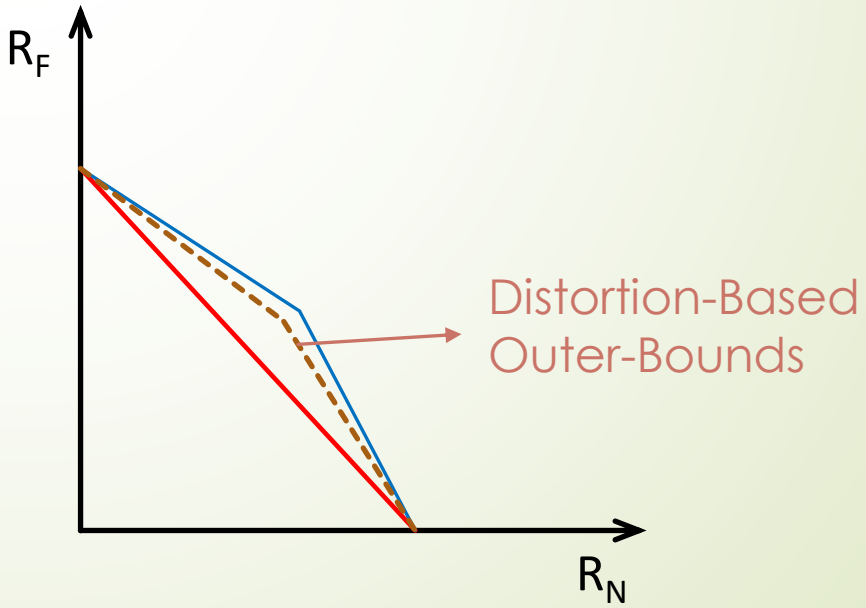
The available control channels have sub-bit capacity!



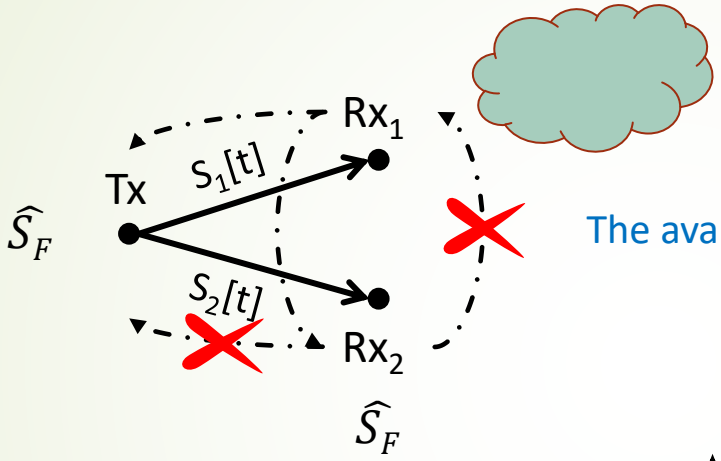
Extreme environment



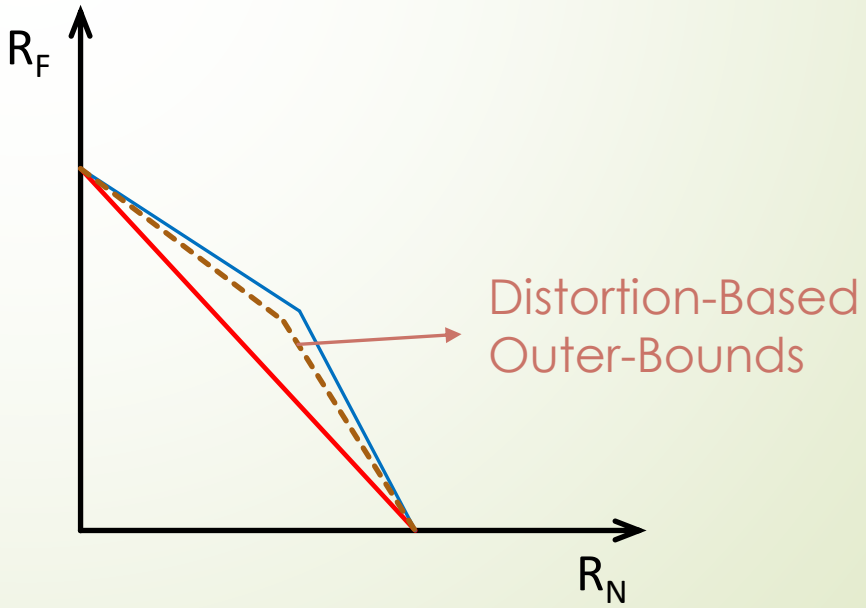
The available control channels have sub-bit capacity!



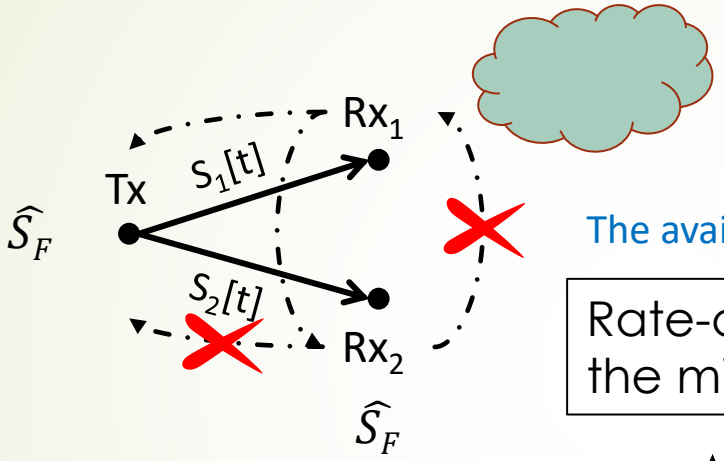
Extreme environment



The available control channels have sub-bit capacity!

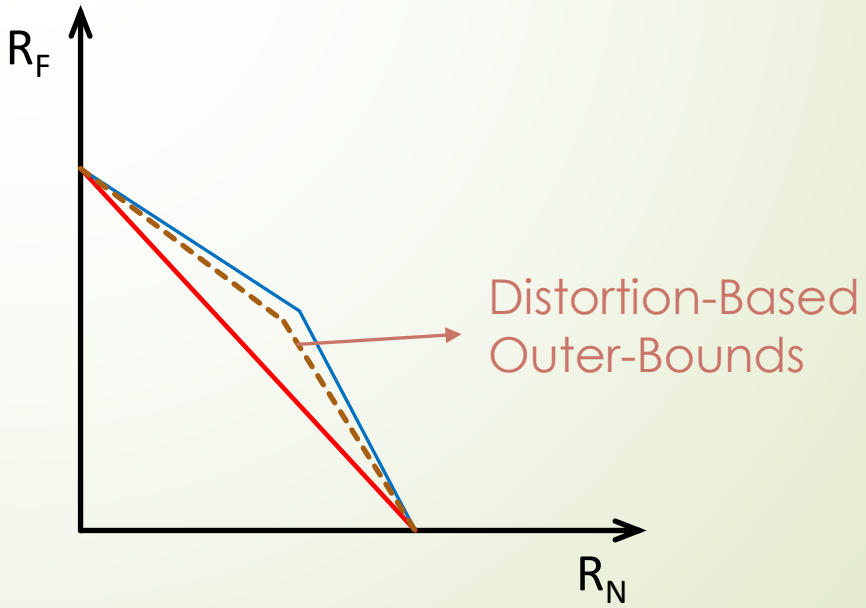


Extreme environment

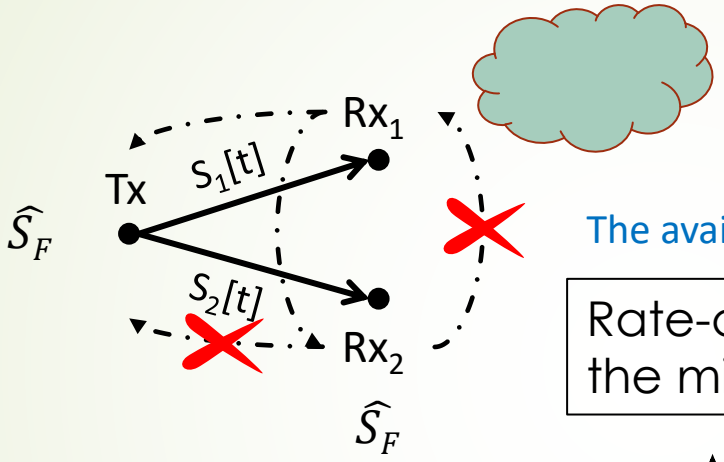


The available control channels have sub-bit capacity!

Rate-distortion theory gives us the minimum attainable distortion.

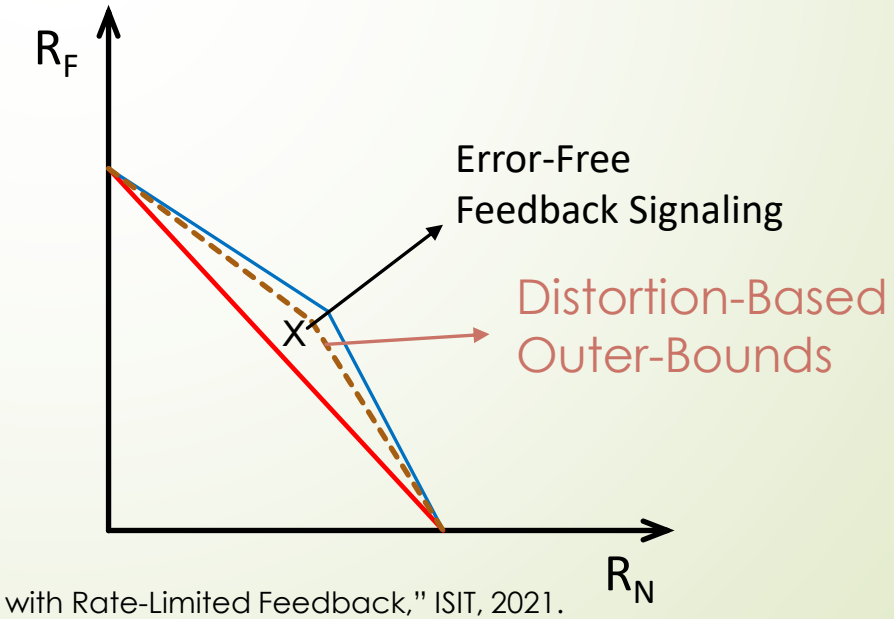


Extreme environment



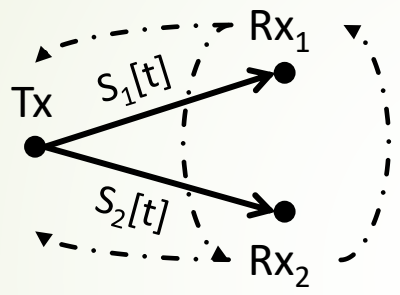
The available control channels have sub-bit capacity!

Rate-distortion theory gives us the minimum attainable distortion.



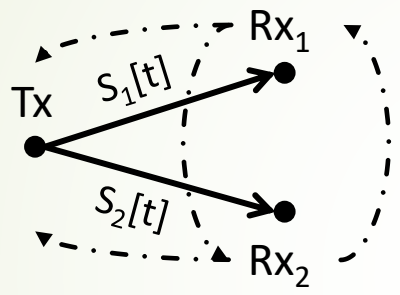
Vahid, "Distortion-Based Outer-Bounds for Channels with Rate-Limited Feedback," ISIT, 2021.

Remaining theoretical questions



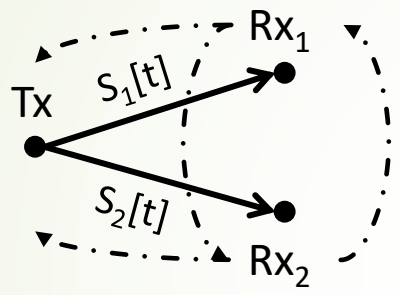
- How do the results scale?

Remaining theoretical questions



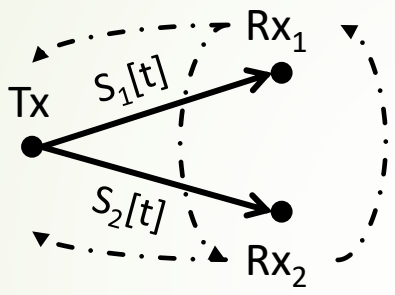
- How do the results scale?
- What is the delay implications of the protocols?

Remaining theoretical questions

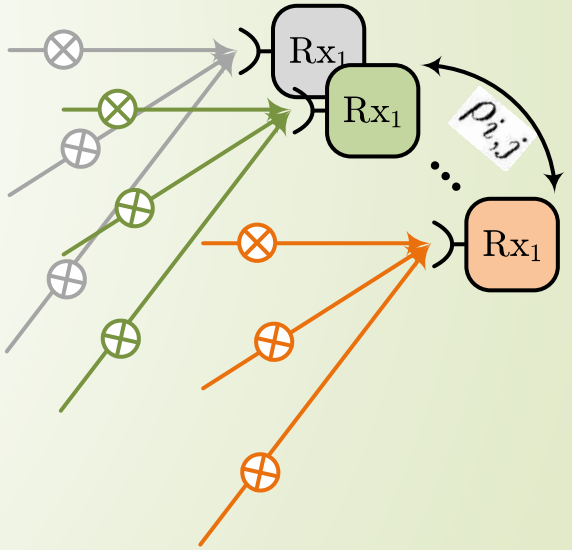


- How do the results scale?
- What is the delay implications of the protocols?
- The extreme sub-bit regime remains open.

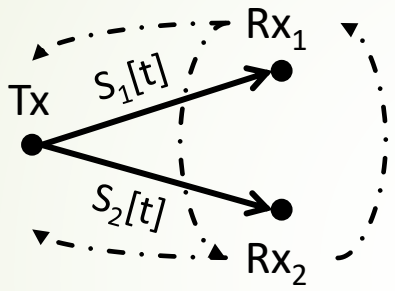
Remaining theoretical questions

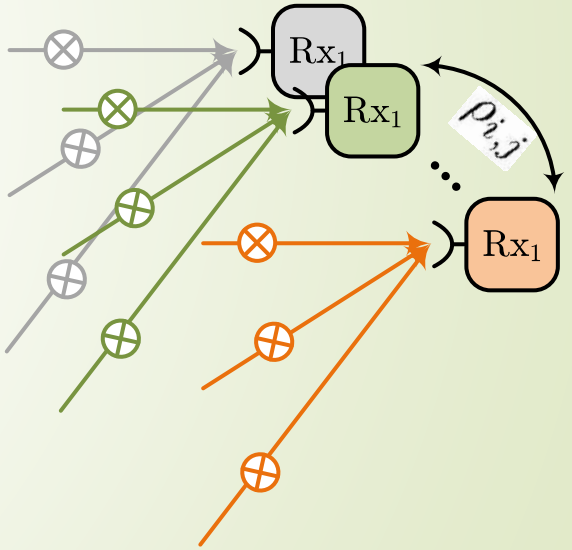


- How do the results scale?
- What is the delay implications of the protocols?
- The extreme sub-bit regime remains open.
- Spectrum sharing



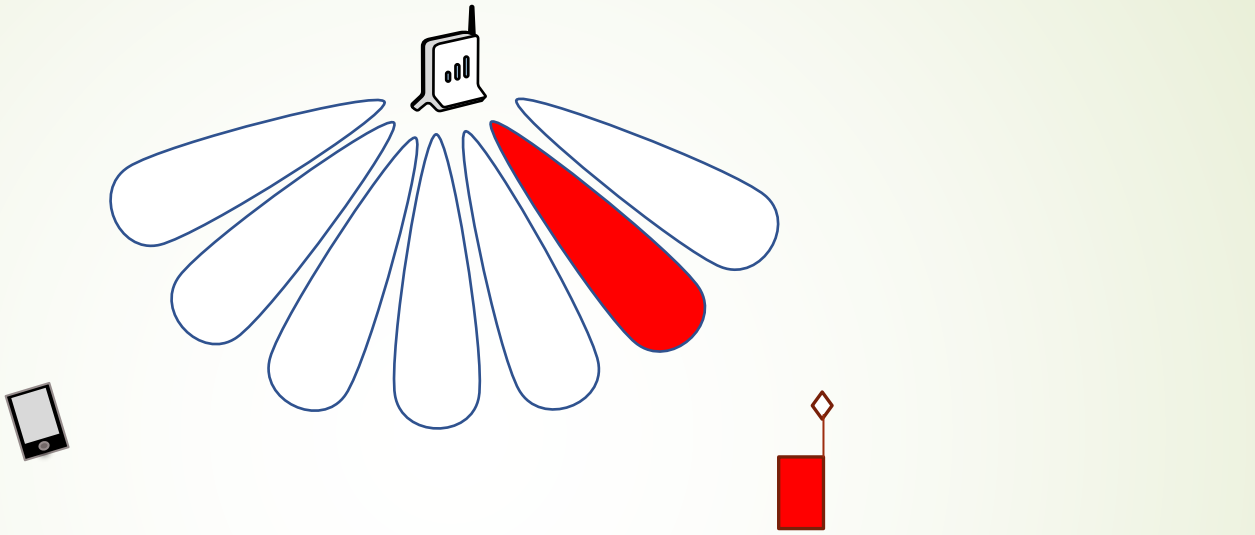
Remaining theoretical questions

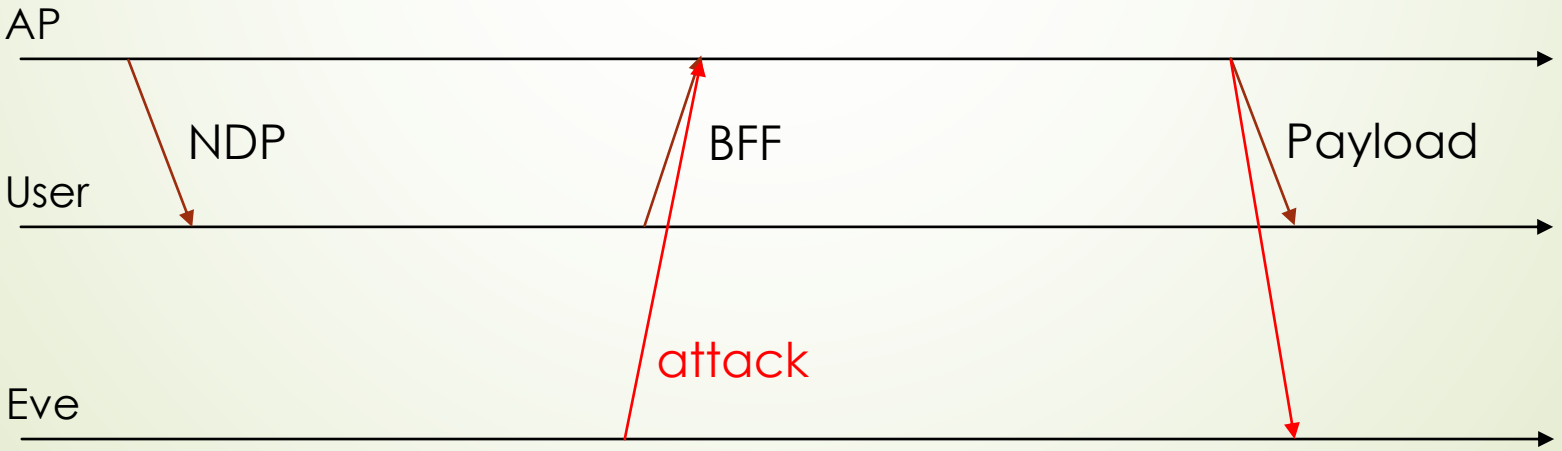




- How do the results scale?
- What is the delay implications of the protocols?
- The extreme sub-bit regime remains open.
- Spectrum sharing
- Can these ideas be incorporated in existing protocols?

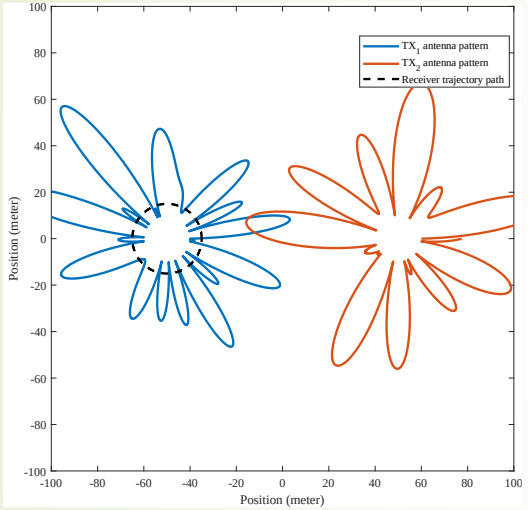
Back to WiFi-6 (-7)



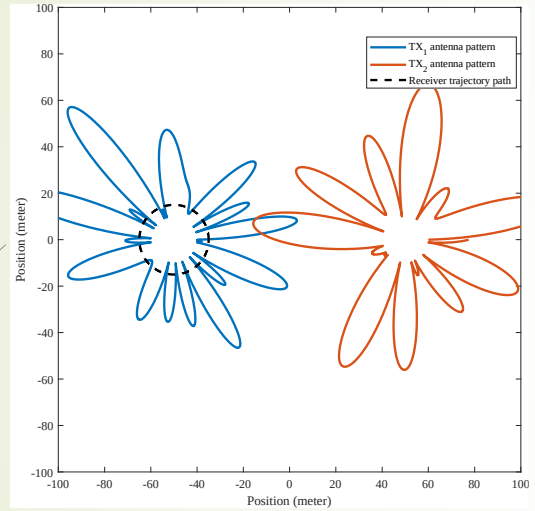


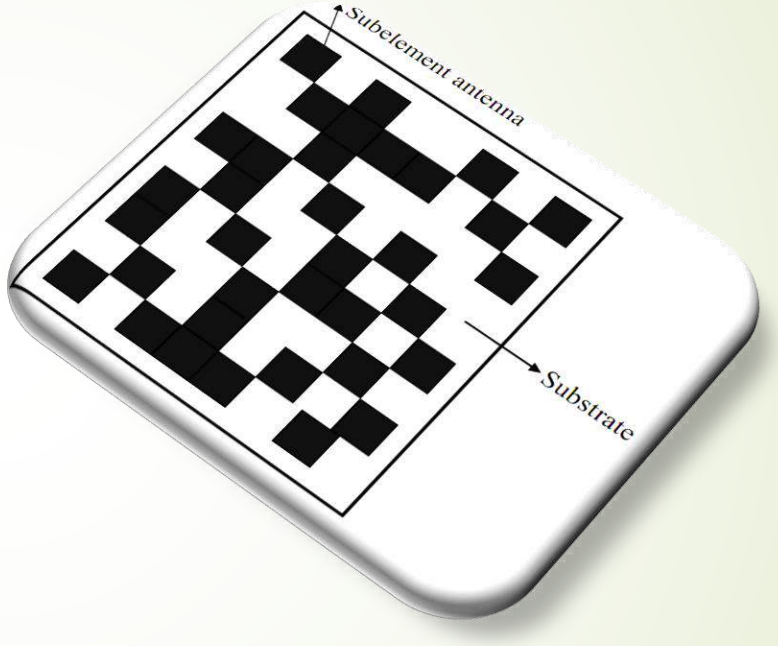
Defending WiFi against Control Ch. Attacks

Defending WiFi against Control Ch. Attacks

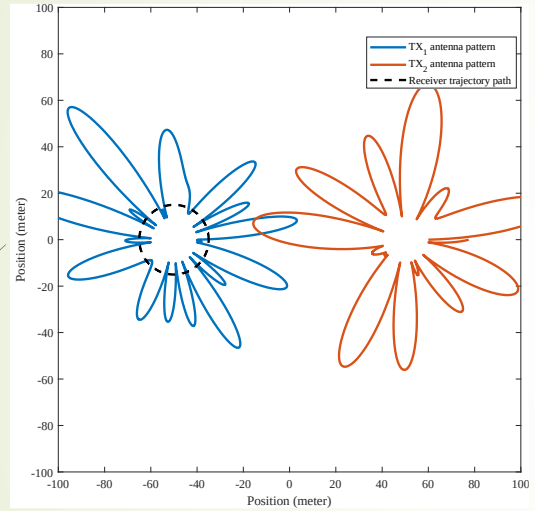


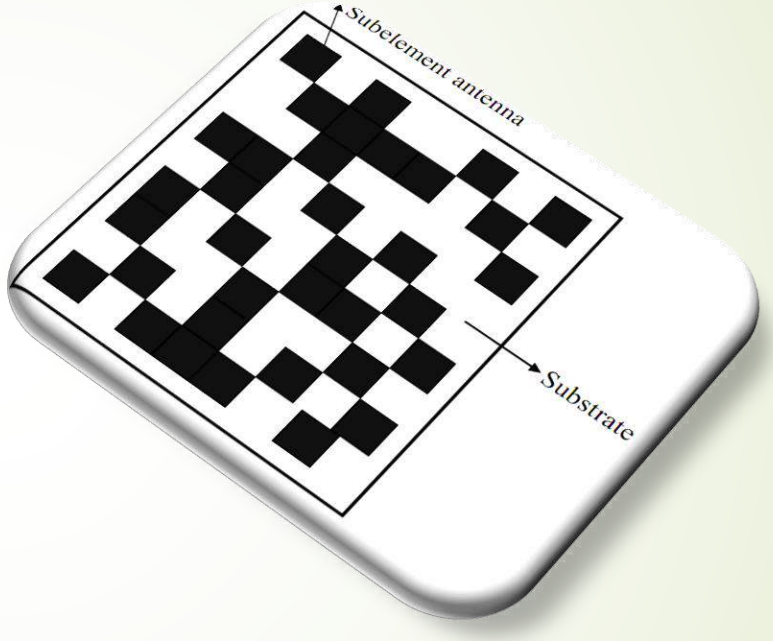
Defending WiFi against Control Ch. Attacks





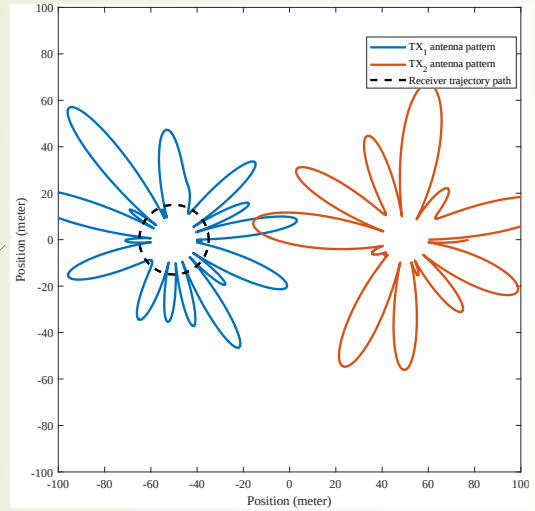
Defending WiFi against Control Ch. Attacks

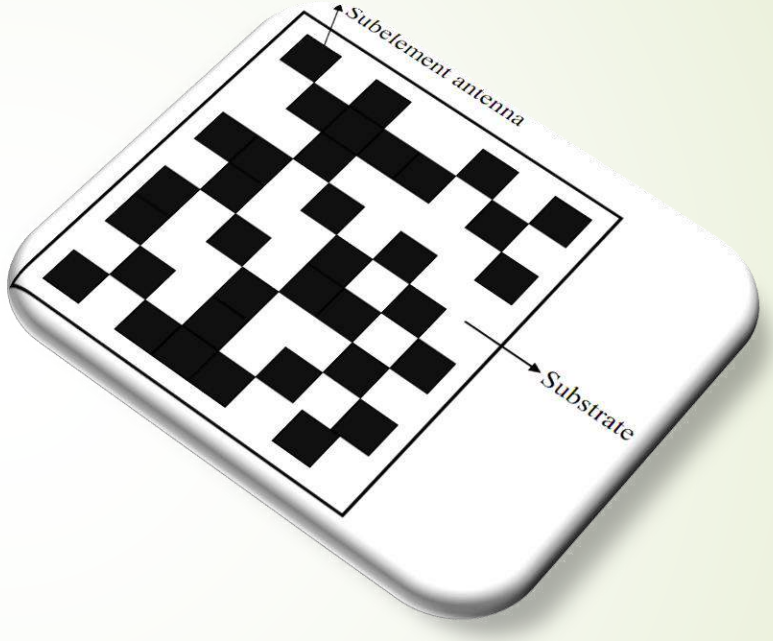




- Desired user will always be at 0° phase, while others see varying phases. (rel. to antenna-selection mod.)

Defending WiFi against Control Ch. Attacks

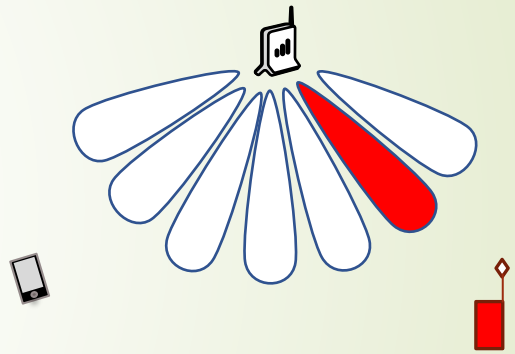




- Desired user will always be at 0° phase, while others see varying phases. (rel. to antenna-selection mod.)
- Embedding information in radiation pattern fluctuations is itself a worthy direction.

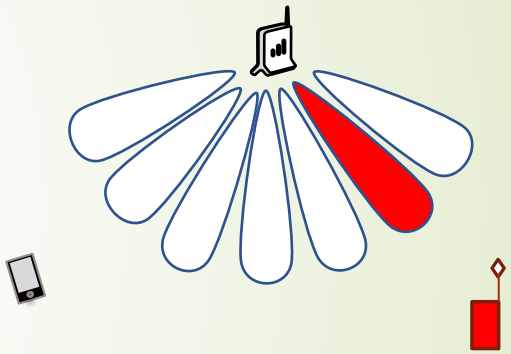
Vahid et al, "Exploiting coherence time variations for opportunistic blind interference alignment," Trans. Comm, 2020.

Defending WiFi against Control Ch. Attacks



Defending WiFi against Control Ch. Attacks

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



Vahid et al, "A Game-Theoretically Optimal Defense Paradigm against Traffic Analysis Attacks Using Multipath Routing and Deception," SACMAT, 2022.

Vahid et al, "Toward practical defense against traffic analysis attacks on encrypted DNS traffic," Computers & Security, 2022.


Higher frequency bands?

Thank you!