Orthogonality-Sabotaging Attacks against OFDMA-based Wireless Networks

Shangqing Zhao, Zhuo Lu, Zhengping Luo, Yao Liu

University of South Florida

USF
UNIVERSITY OF
SOUTH FLORIDA

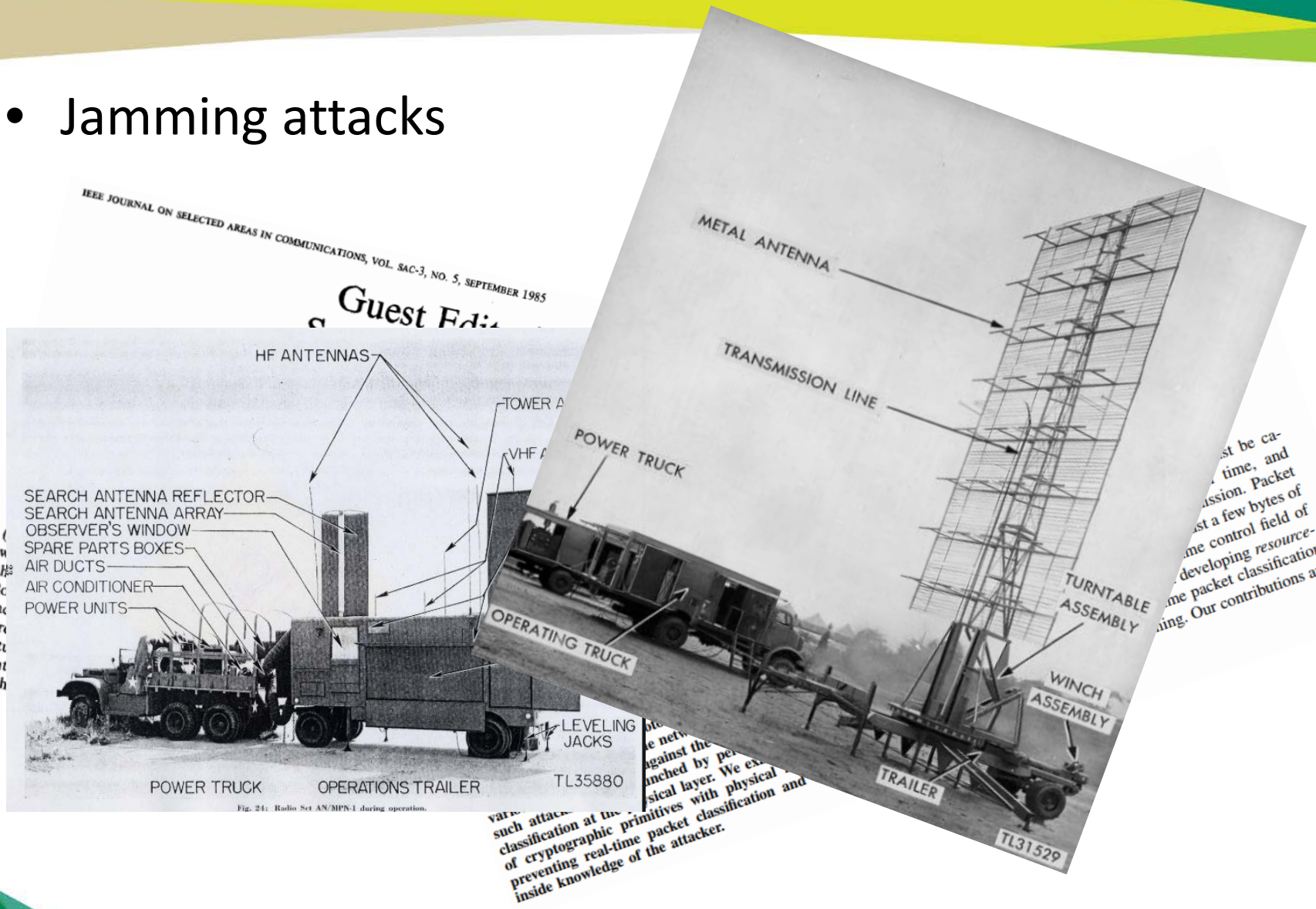
USF UNIVERSITY OF SOUTH FLORIDA

OUTLINE

- Background
- Attack Strategy and Evaluation
  - Motivation of orthogonality sabotaging
  - Experimental Evaluation
- Identification and Detection
- Conclusion

JAMMING ATTACKS

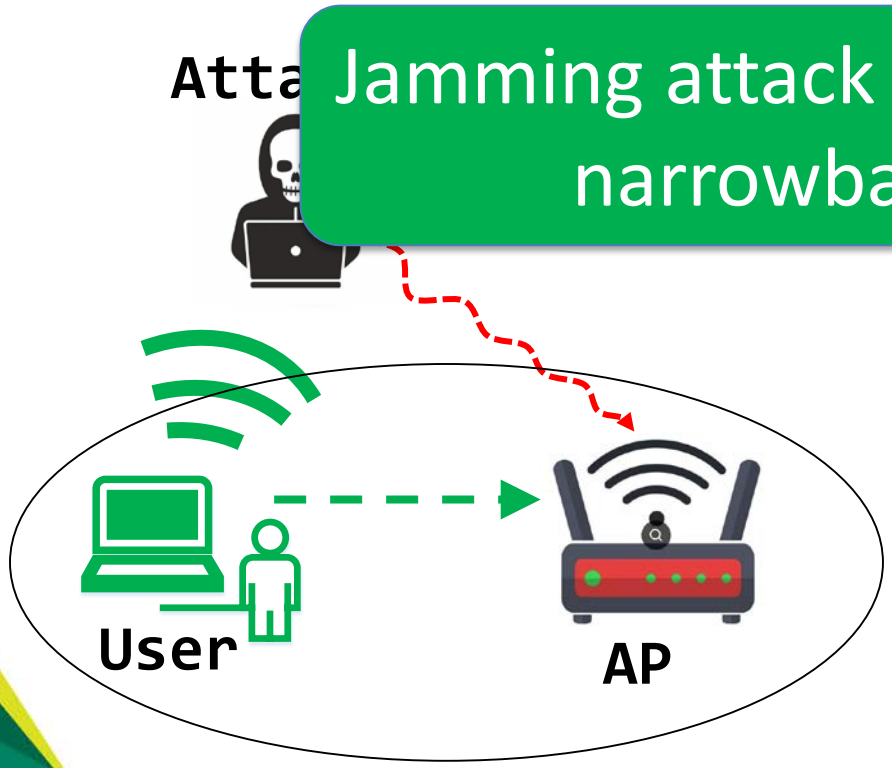
- Jamming attacks



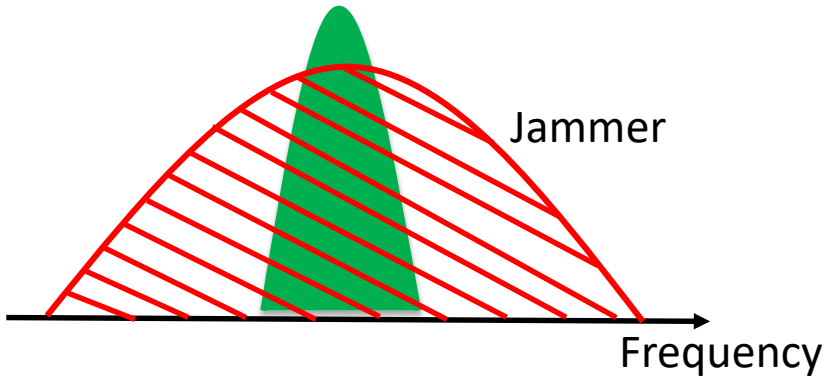
JAMMING ATTACKS

- Jamming attacks

  --- broadcast nature of wireless signals



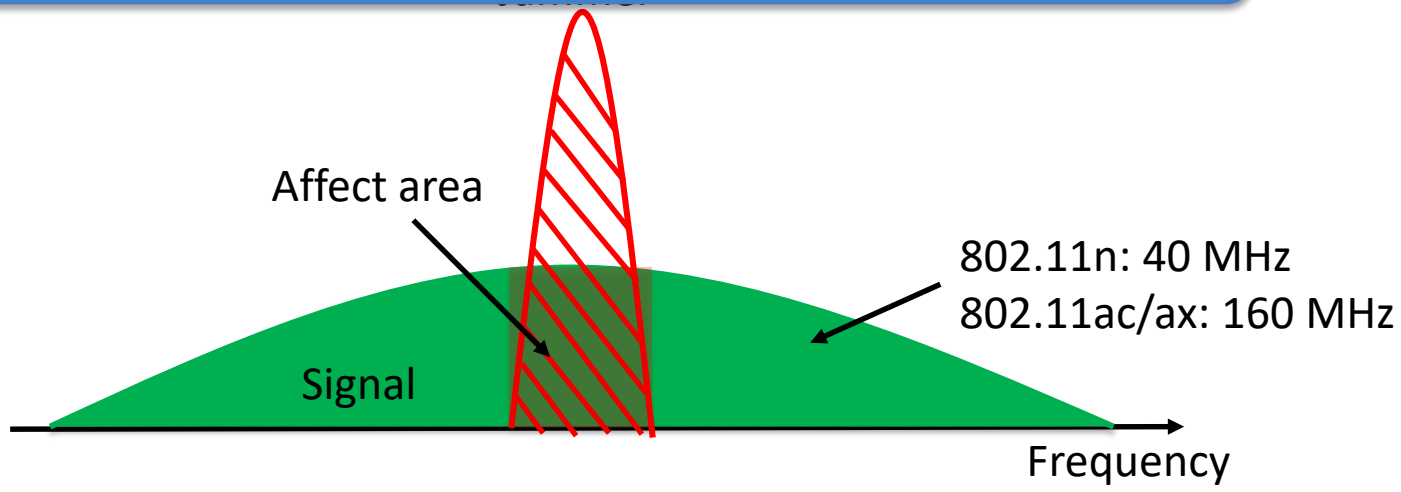
Jamming attack works well against narrowband systems



JAMMING ATTACKS

- Traditional: jammer cannot disrupt signals beyond its covered bandwidth

Narrow-band jamming is usually not effective for broadband systems



JAMMING ATTACKS

- Traditional: jammer cannot disrupt signals beyond its covered bandwidth

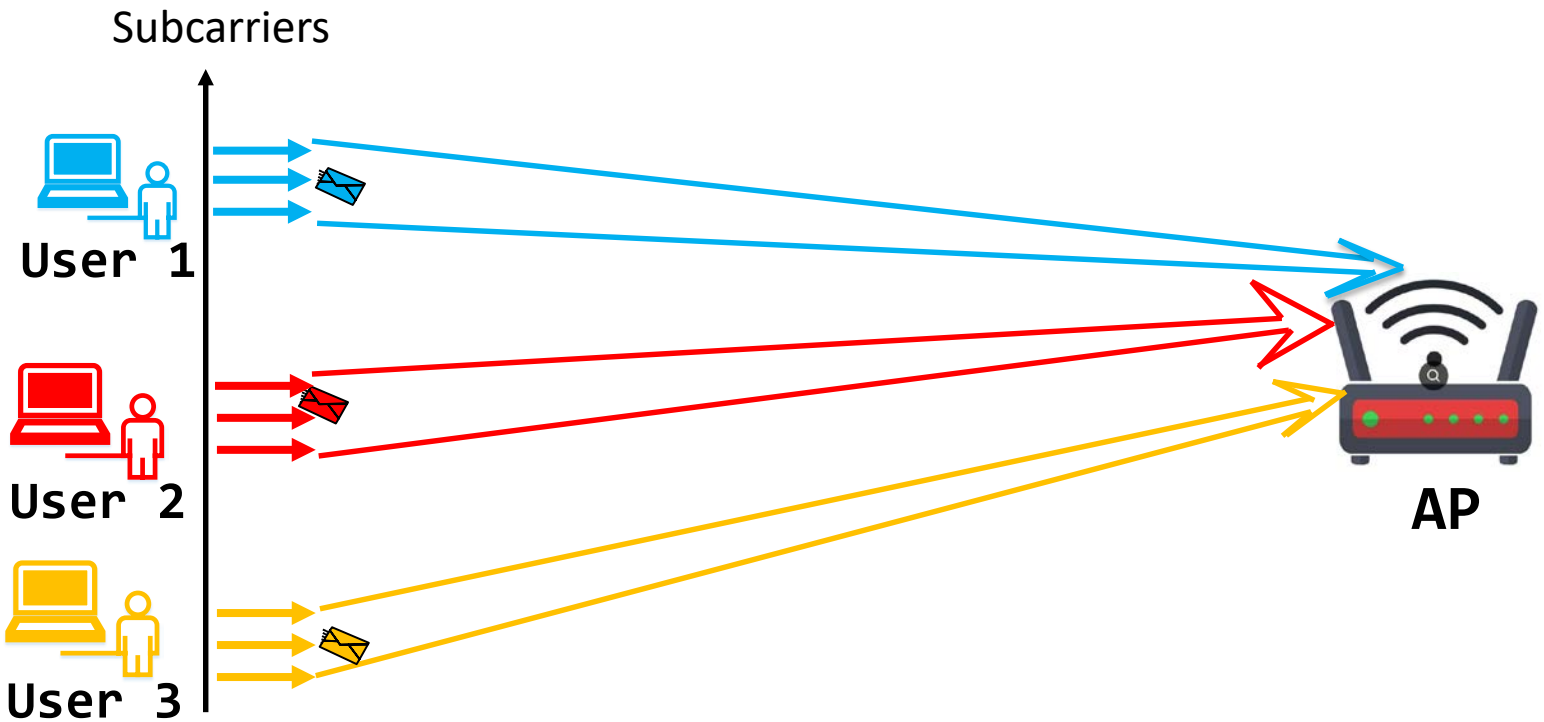
NOT always hold in *OFDM(A)* systems !!

OFDMA

- OFDMA

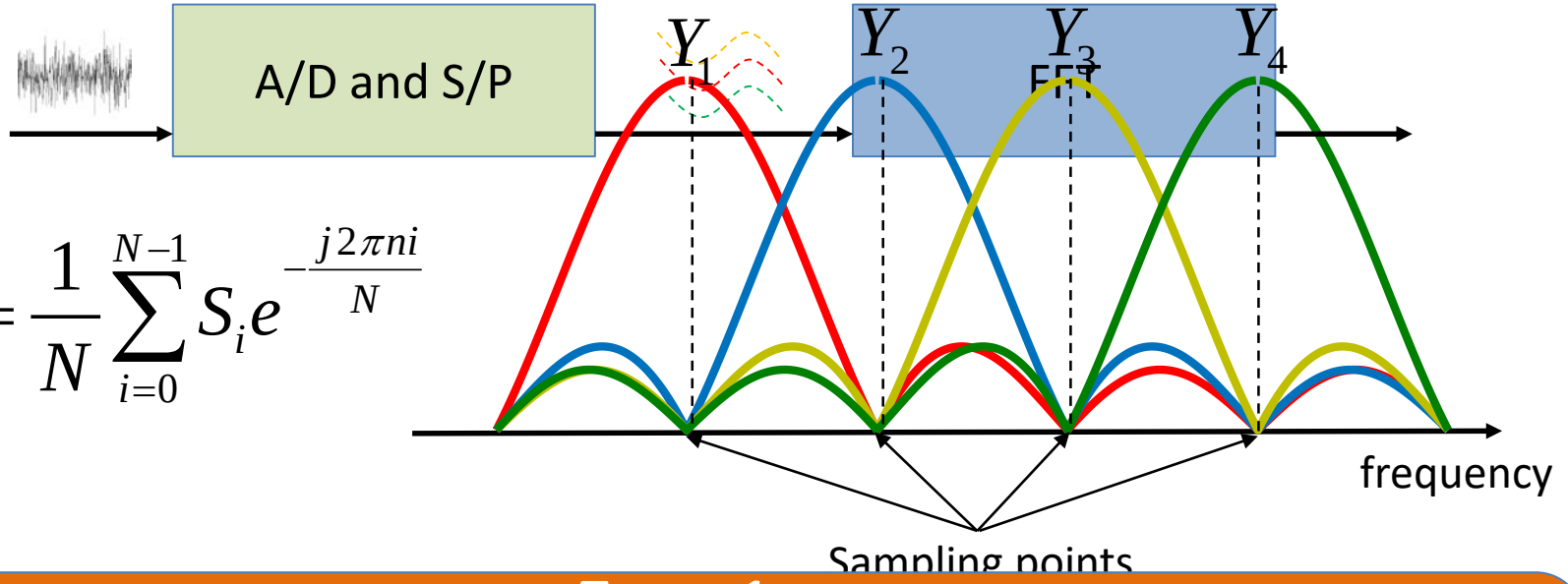
  --- spectrum is split into multiple orthogonal subcarriers

  --- assigns a part of subcarriers to each user



OFDMA

- OFDMA Receiver (at the AP)



$$Y_n = \frac{1}{N}\sum_{i=0}^{N-1} S_i e^{-\frac{j2\pi ni}{N}}$$

Fact 1:

Frequency-domain signals are on all subcarriers are orthogonal to each other

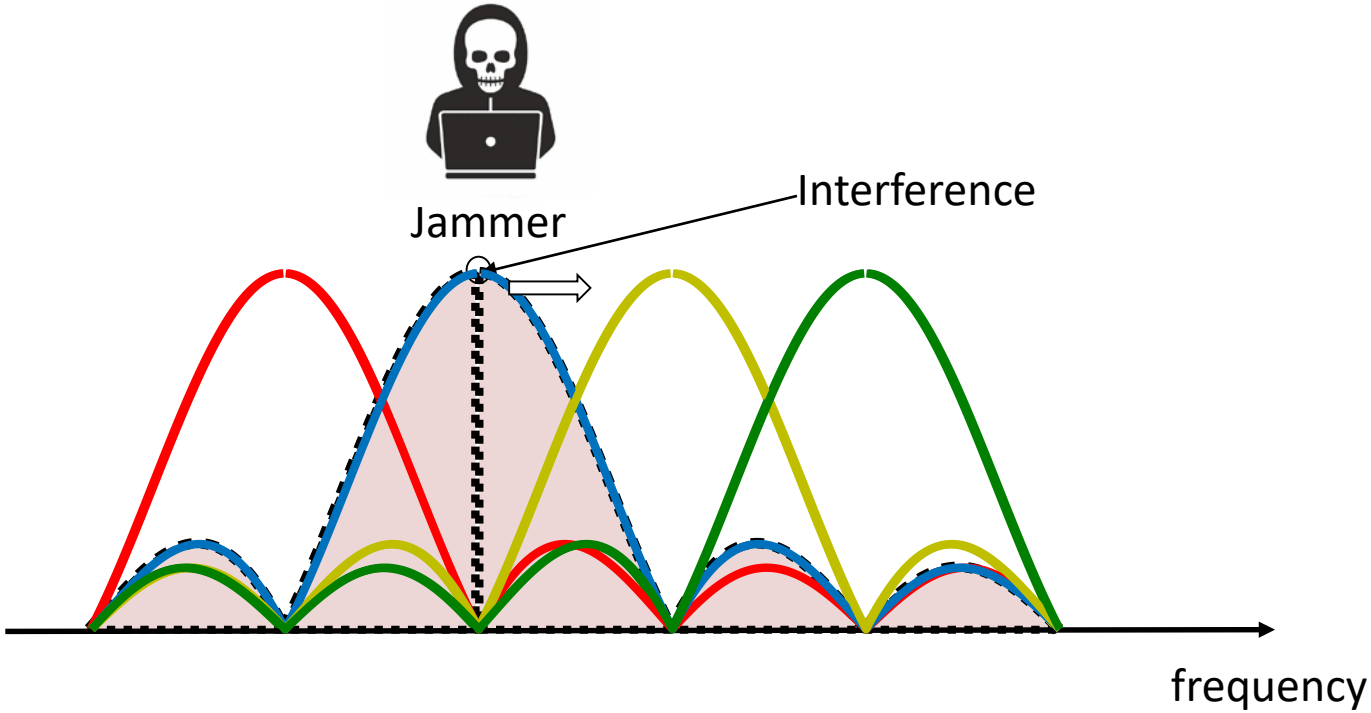
ATTACK

Orthogonality-Sabotaging Attacks

- Key idea:
  - Use a narrowband jamming signal to disrupt the broadband OFDMA based system
- Methodology:
  - Intentionally transmits a jamming signal with unaligned central frequency to other subcarriers, to break the orthogonality.
- Two goals:
  - Understand its impact
  - Detect and localize the attack

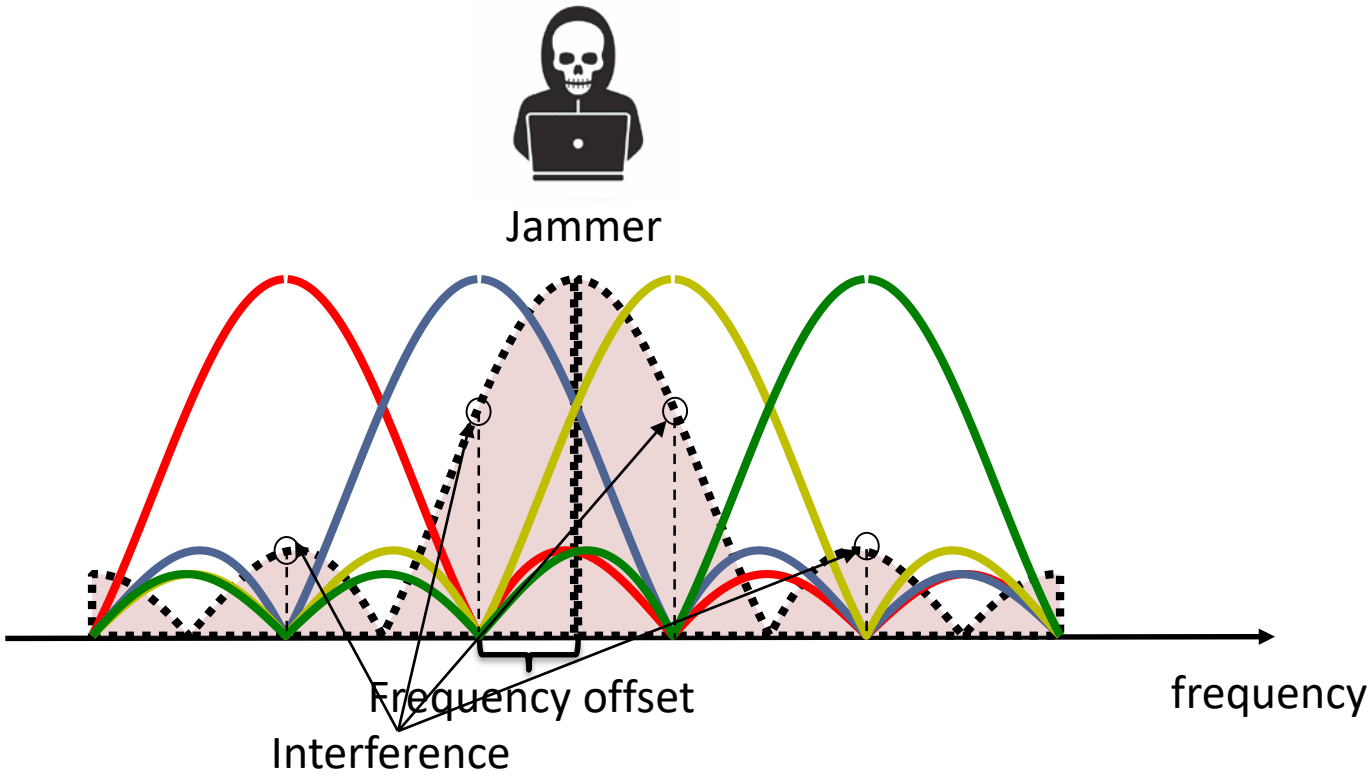
ATTACK

- Attack with *no frequency offset*



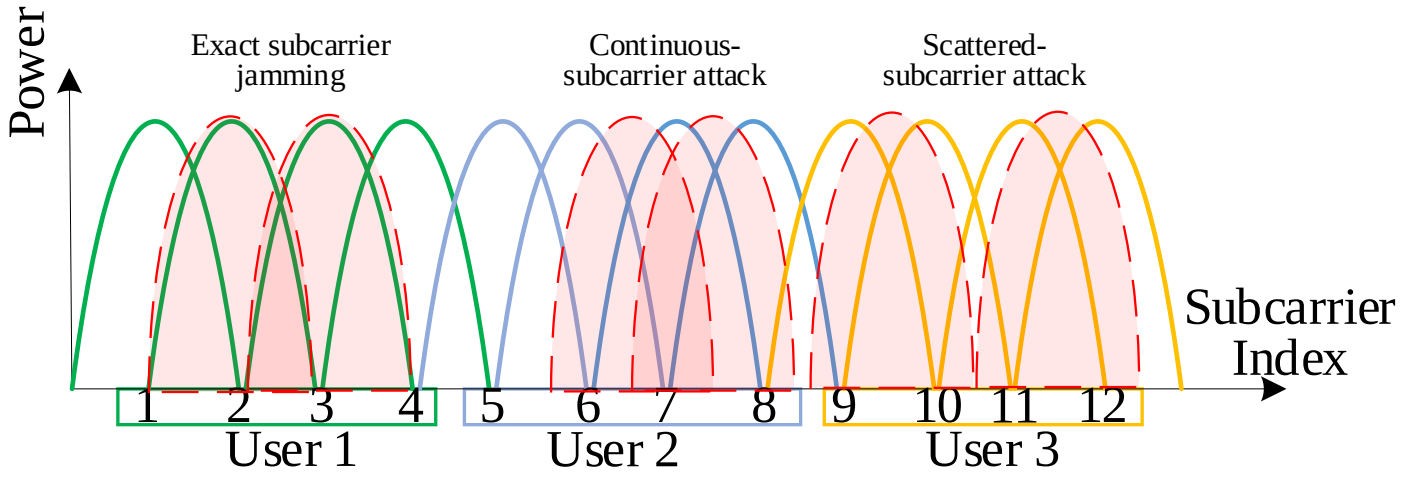
ATTACK

- Attack with *frequency offset*



ATTACK STRATEGIES

- Strategies
  - Exact subcarrier jamming ⟹ no offset
  - Continuous-subcarrier attack ⟹ same offset
  - Scattered subcarrier attack ⟹ different offsets



EXPERIMENTS

- Experimental setup

  --- USRP X300s with CBX daughterboards

  --- 8 USRPs are users, 1 USRP is AP, and 1 USRP is attacker

  --- Use Linksys EA8500 as the commercial AP (802.11ac)

- Parameters setting (802.11ax)

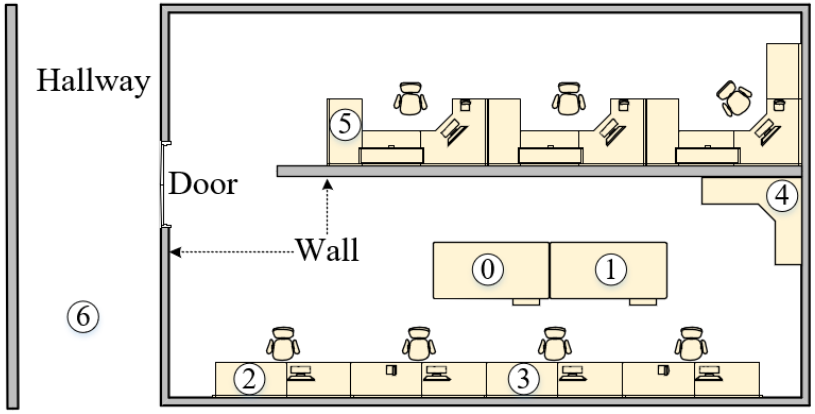
  --- 245 subcarriers

  --- attacker user 18 subcarriers

  --- each user occupies 26 subcarriers

EXPERIMENTS

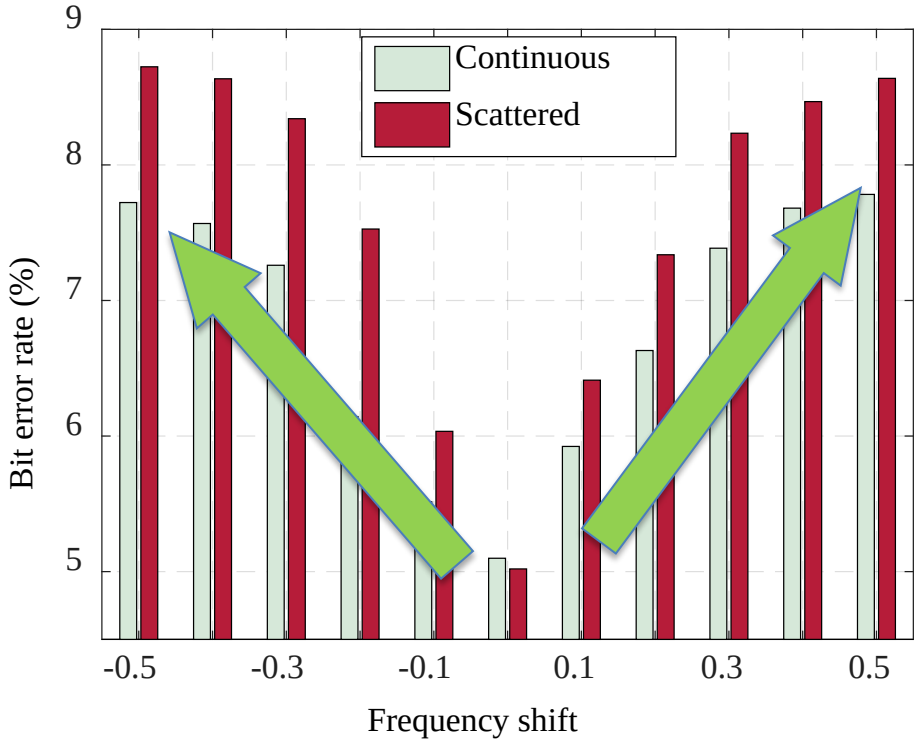
- Indoor environment



- Metrics
  - Bit error rate (BER)
  - Packet drop rate
  - Normalized throughput

802.11AX NETWORK

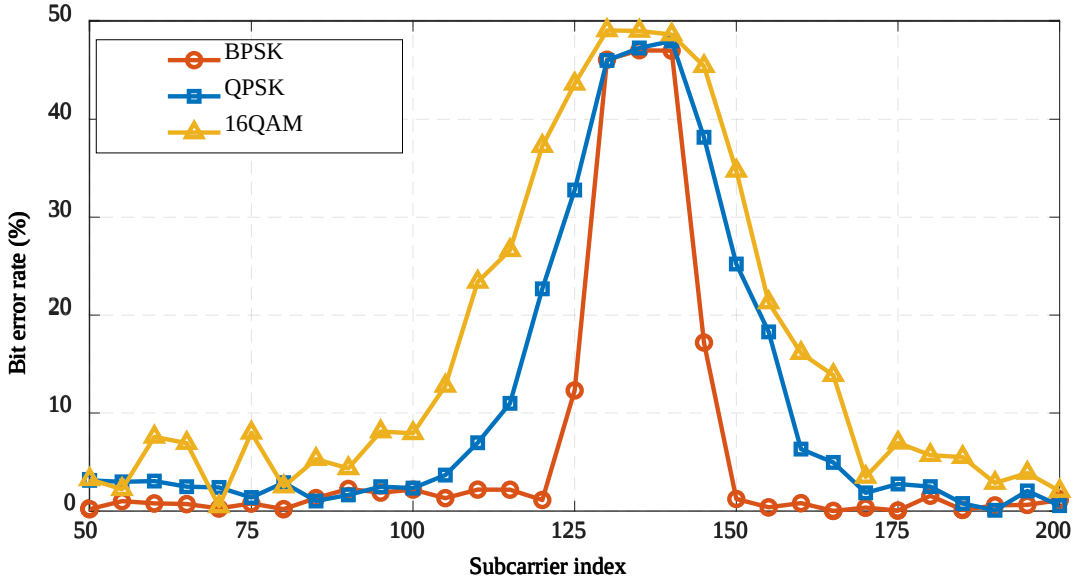
- Varying frequency offset



BER reaches the maximum at |0.5| bandwidth of subcarrier

802.11AX NETWORK

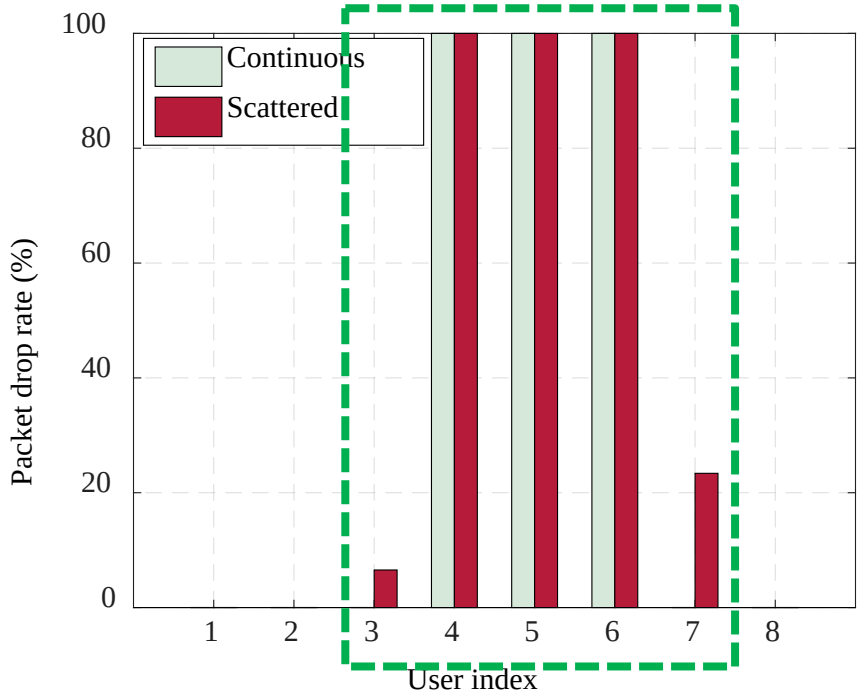
- Varying modulation scheme



Attack can disrupt the signal with up to a bandwidth 500% broader than its own bandwidth

802.11AX NETWORK

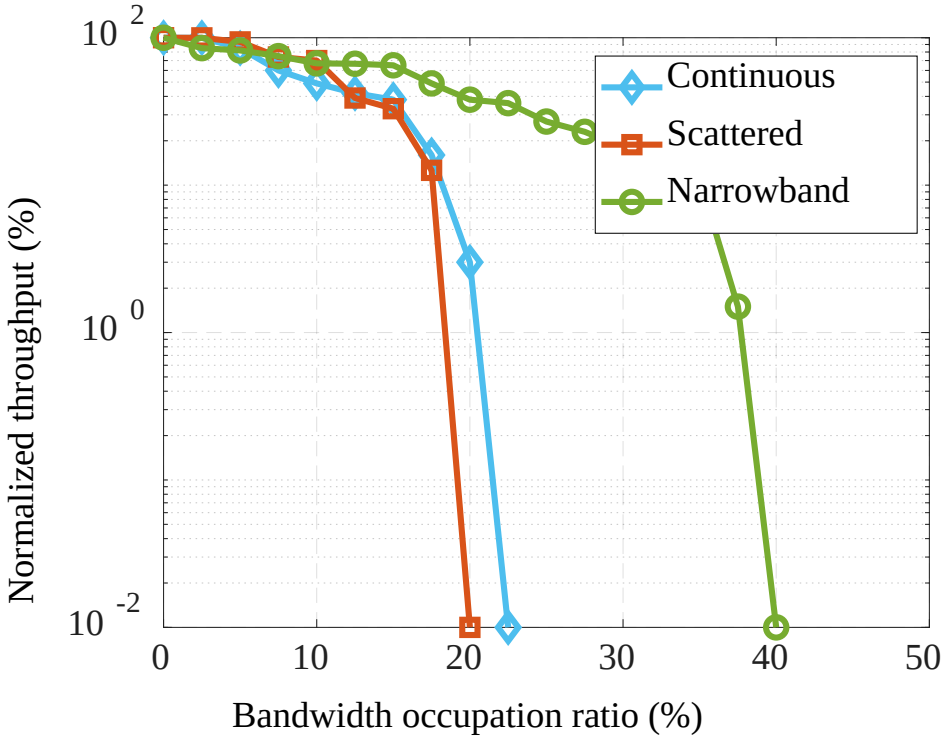
- Impact on users



Attack can affect up to 5 users using a single user's bandwidth

802.11AC NETWORK

- Impact on commercial AP (Linksys EA8500)



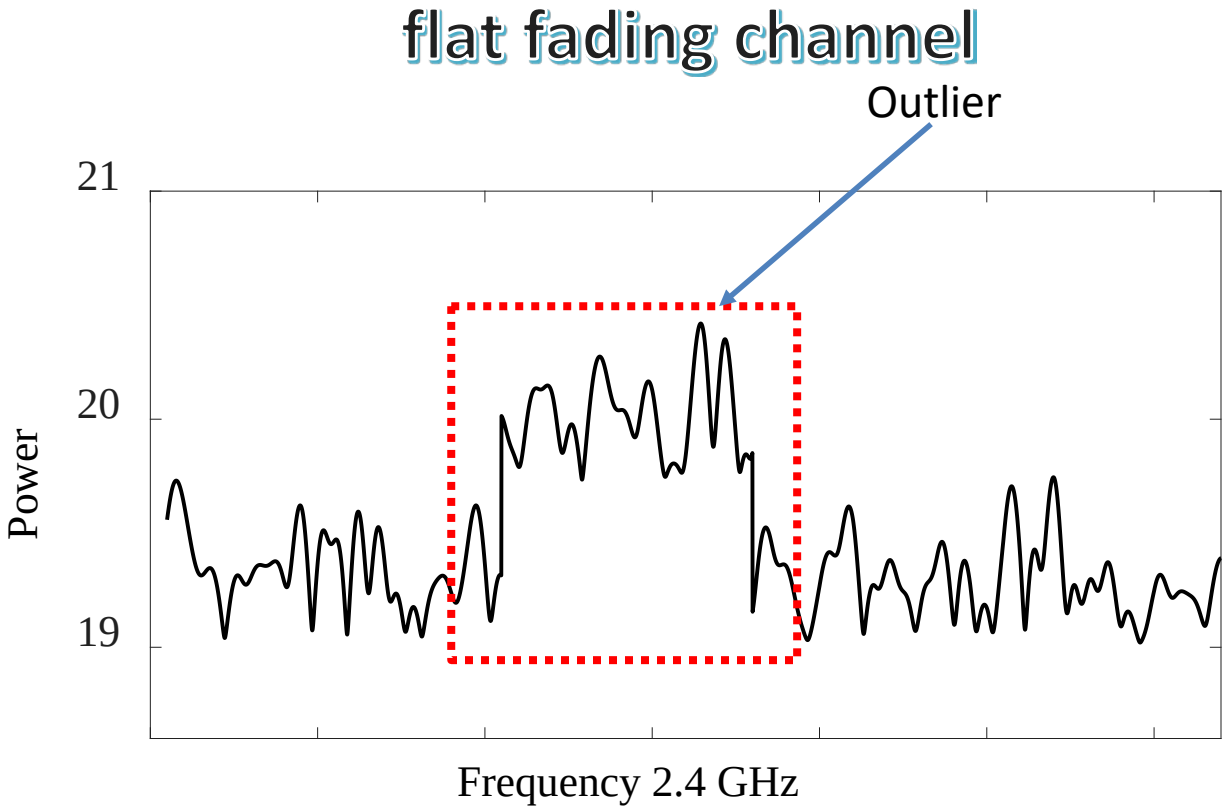
Orthogonality-Sabotaging Attacks are more efficient

IDENTIFICATION AND LOCALIZATION

How to identify and localize such attacks ?

IDENTIFICATION AND LOCALIZATION

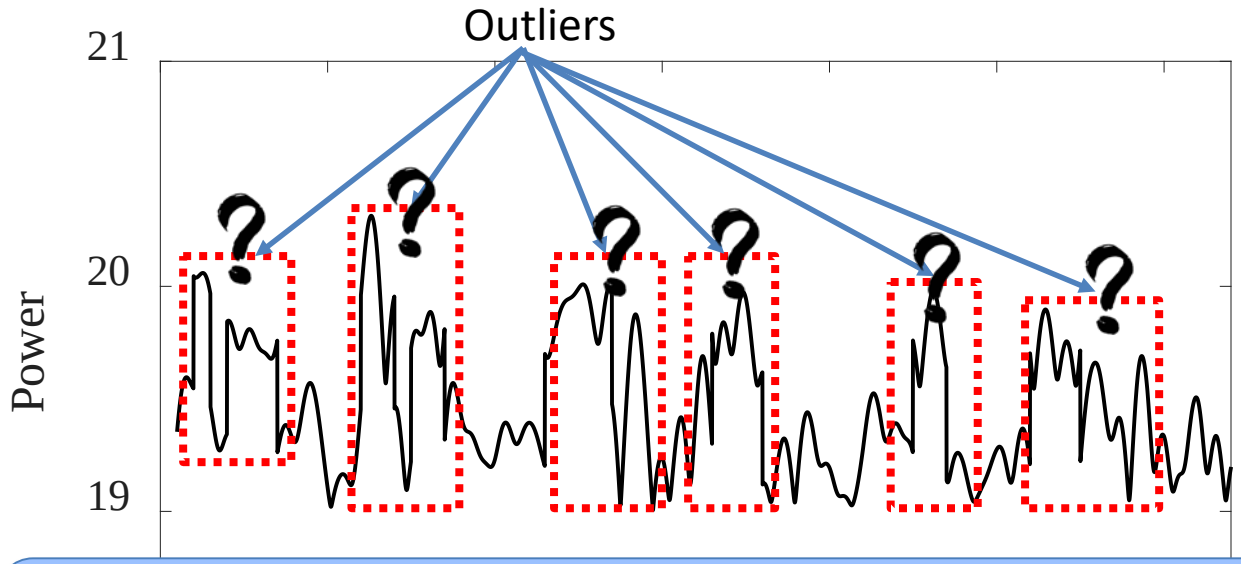
- Spectrum analysis



IDENTIFICATION AND LOCALIZATION

- Spectrum analysis

frequency-selective fading channel

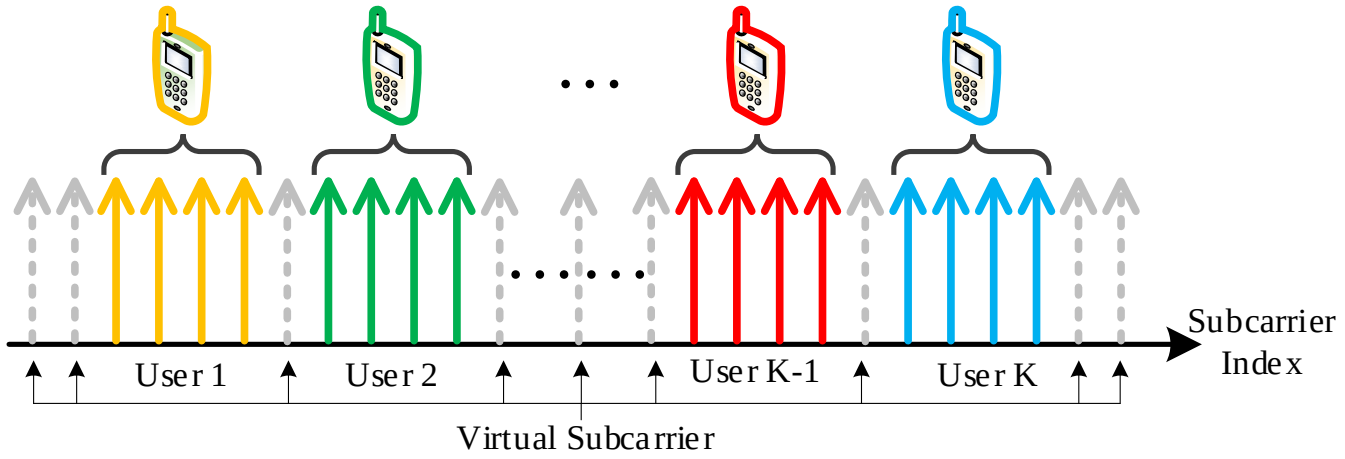


Hard to say which one is from attacks or random fading.

IDENTIFICATION AND LOCALIZATION

- virtual subcarriers

  --- serves as the guard zones to protect interferences between users

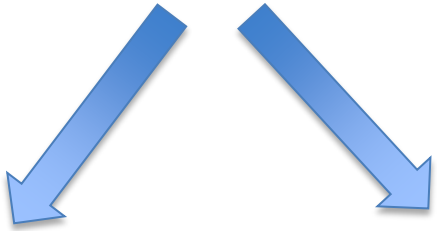


--- carry no information with 0 power, so …

A positive measurement of power can be only due to noise or jamming interference.

IDENTIFICATION AND LOCALIZATION

- Given measurements on virtual subcarriers, we can do …



Localization

Find the locations of subcarriers where attacker occupy

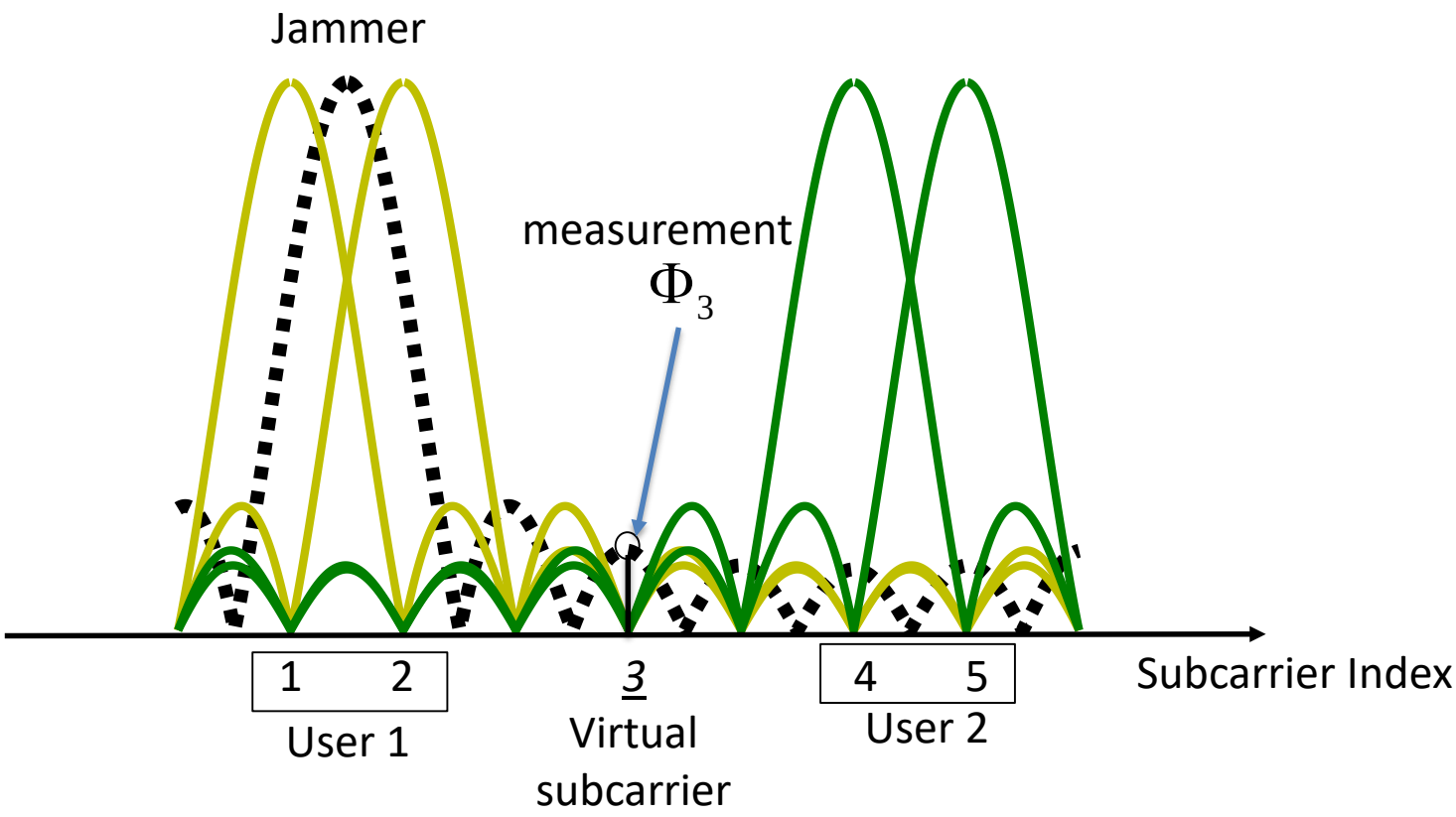
Identification

Identify the attack is:

- Broadband jamming
- Orthogonality sabotaging attack
- Exact subcarrier jamming

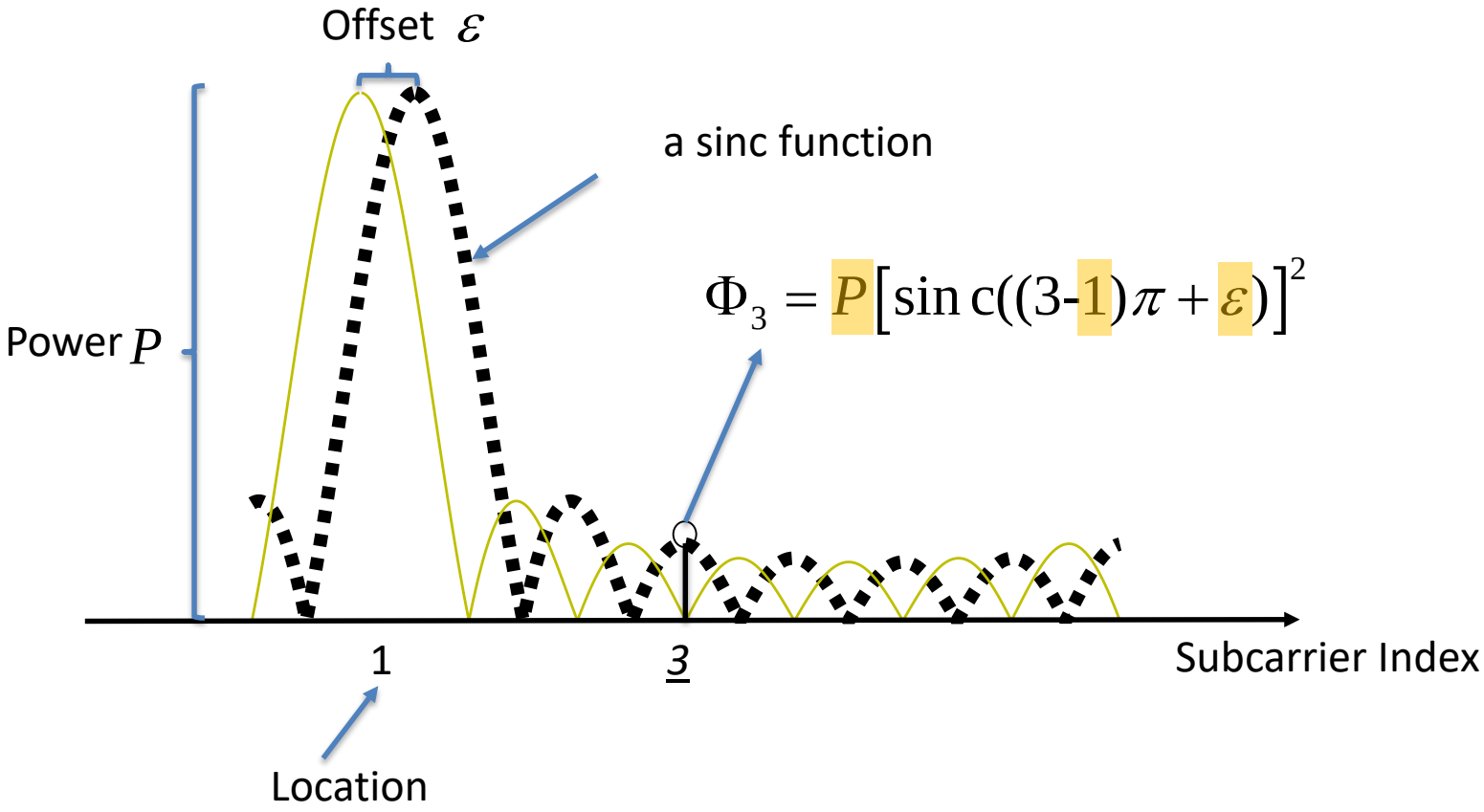
LOCALIZATION

- Localization



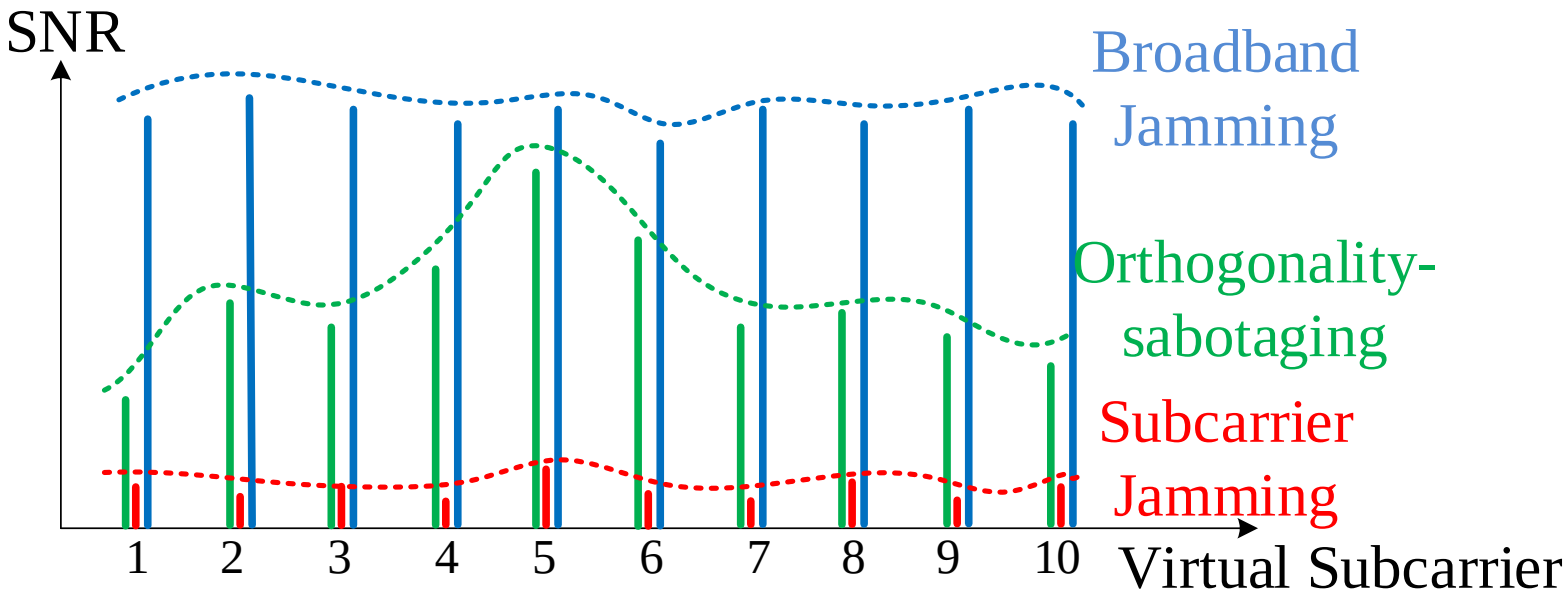
LOCALIZATION

- Localization



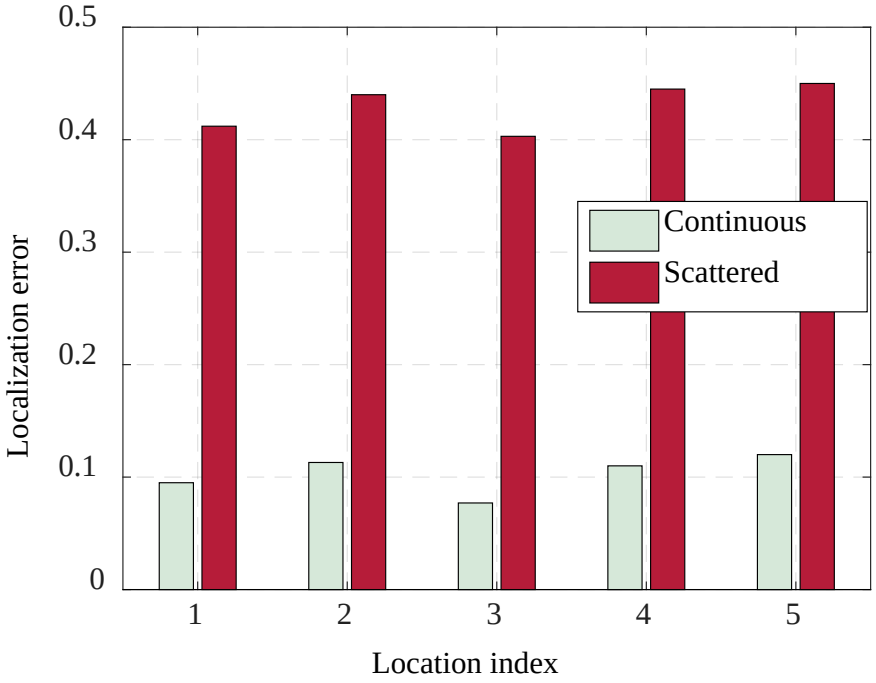
IDENTIFICATION

- Identification
  - Broadband-like jamming
  - Orthogonality sabotaging attack
  - Exact subcarrier jamming



ATTACK LOCALIZATION

- Localization error



Localization error is as low as 0.1–0.45 subcarrier spacing.

ATTACK IDENTIFICATION

- Identification accuracy

	Orth. - Sab	Broad. - like	Exact - sub.
Iden. as Orth. - Sab	92.99%	2.4%	0.2%
Iden. as Broad. - like	2.62%	98.6%	0.0%
Iden. as Exact - sub.	4.39%	0.0%	99.8%

The overall accuracy is no less than 92% under different attacks

SUMMARY

- Orthogonality-Sabotaging attacks are very efficient.
  - is orthogonal to recent smart jamming strategies (e.g., jamming preambles)

- The localization and identification methods achieve a high accuracy.

SUMMARY

Thank you !