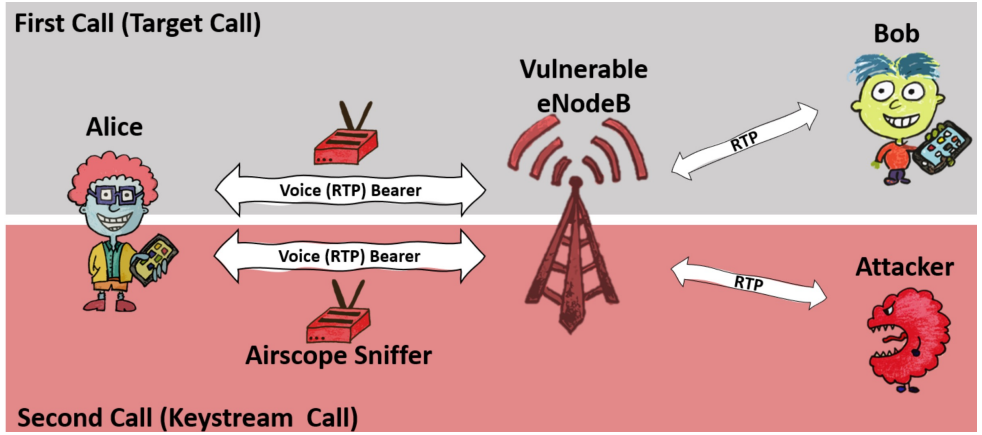
M3A: Multipath Multicarrier Misinformation to Adversaries

Zhecun Liu, Keerthi Priya Dasala, Di Mu, **Rahman Doost-Mohammady**, and Edward W. Knightly

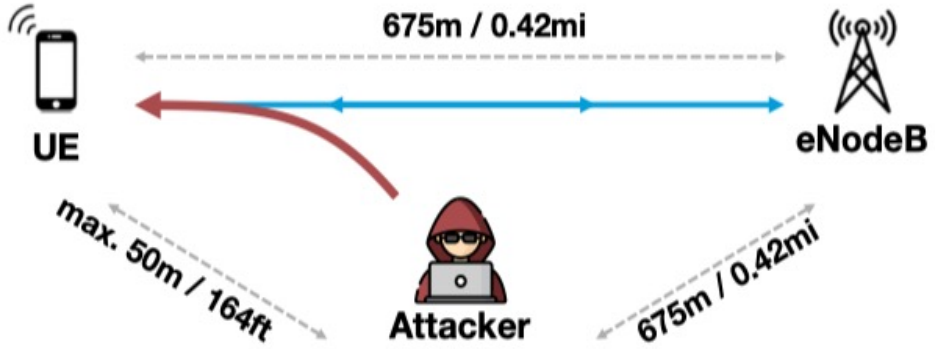
Broad Set of Attacks in Wireless Networks

Snoop Conversations on VoLTE [Rupprecht et al. '20]



Stealthy Tracking & Localization [Kotuliak et al. '22]

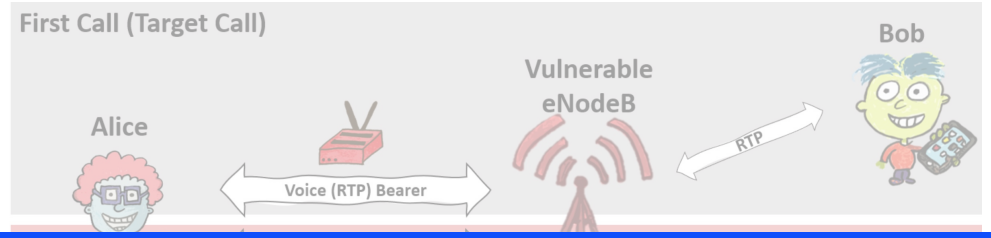
Man-In-The-Middle DoS [Erni et al. '22]



Replay Ciphertext on iMessage [Garman et al. '16]

Broad Set of Attacks in Wireless Networks

Snoop Conversations on VoLTE
[Rupprecht et al. '20]

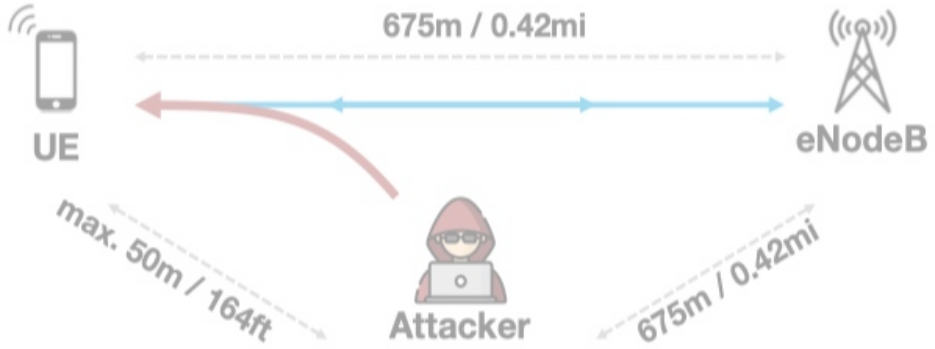


Stealthy Tracking & Localization
[Kotuliak et al. '22]

M3A Key Idea:

- **Wrong Symbols at Adversaries**

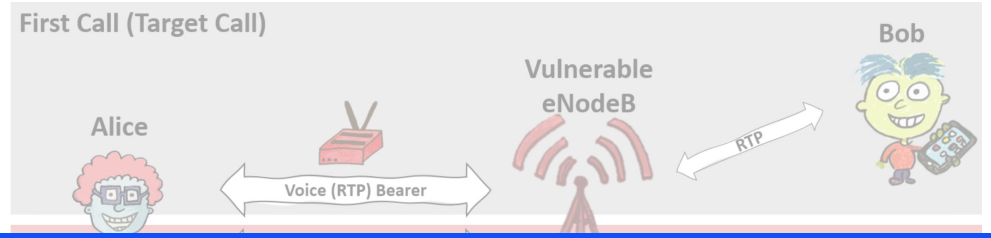
[Erni et al. '22]



[Garman et al. '16]

Broad Set of Attacks in Wireless Networks

Snoop Conversations on VoLTE
[Rupprecht et al. '20]

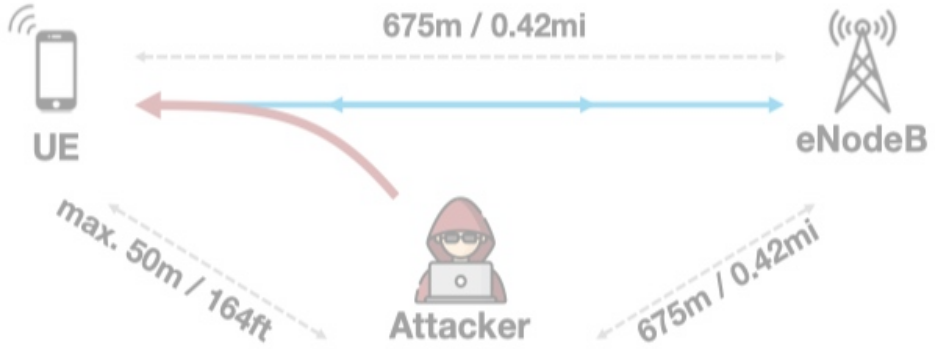


Stealthy Tracking & Localization
[Kotuliak et al. '22]

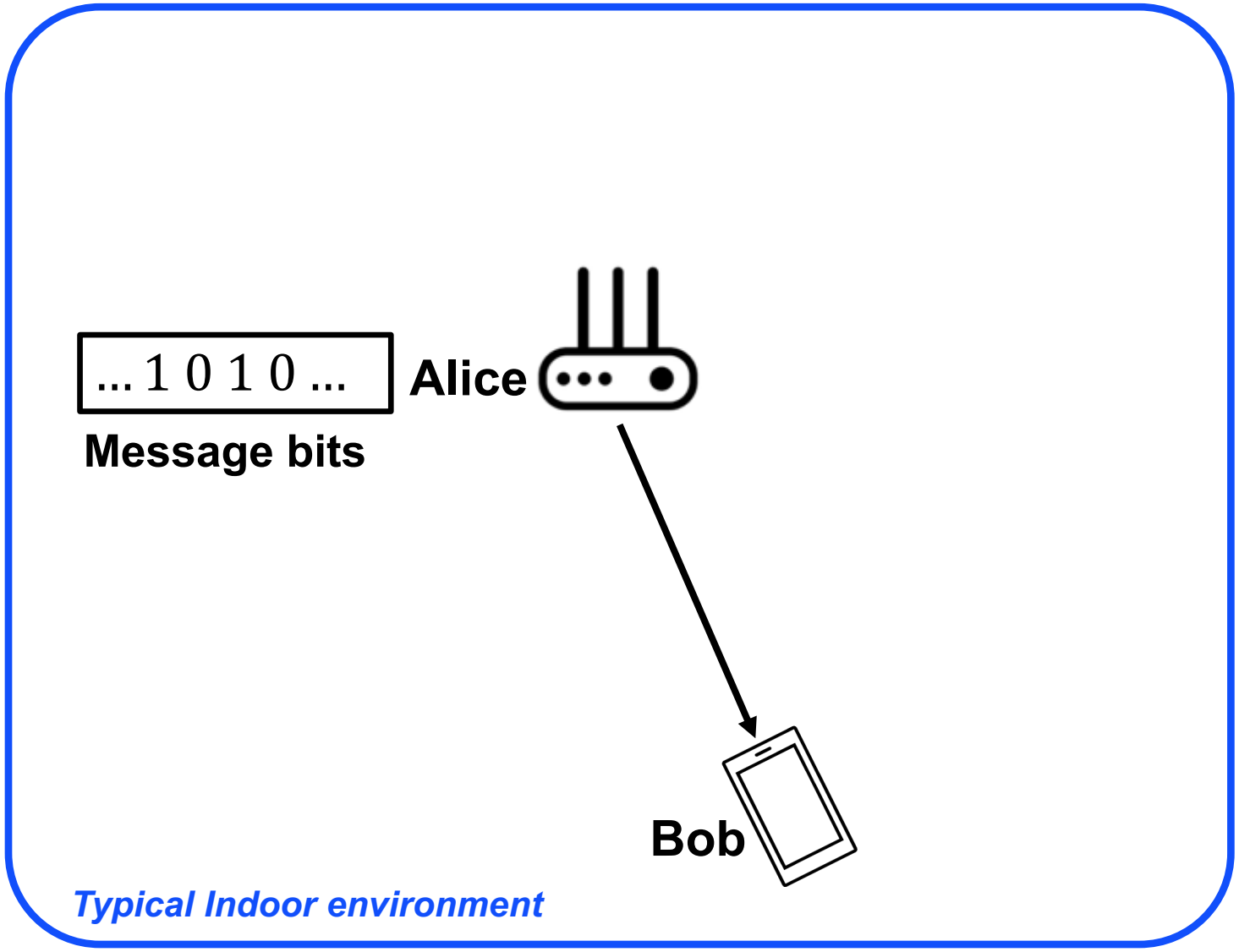
M3A Key Idea:

- **Wrong Symbols at Adversaries**
- **True Data Symbols at Intended Users**

[Erni et al. '22]

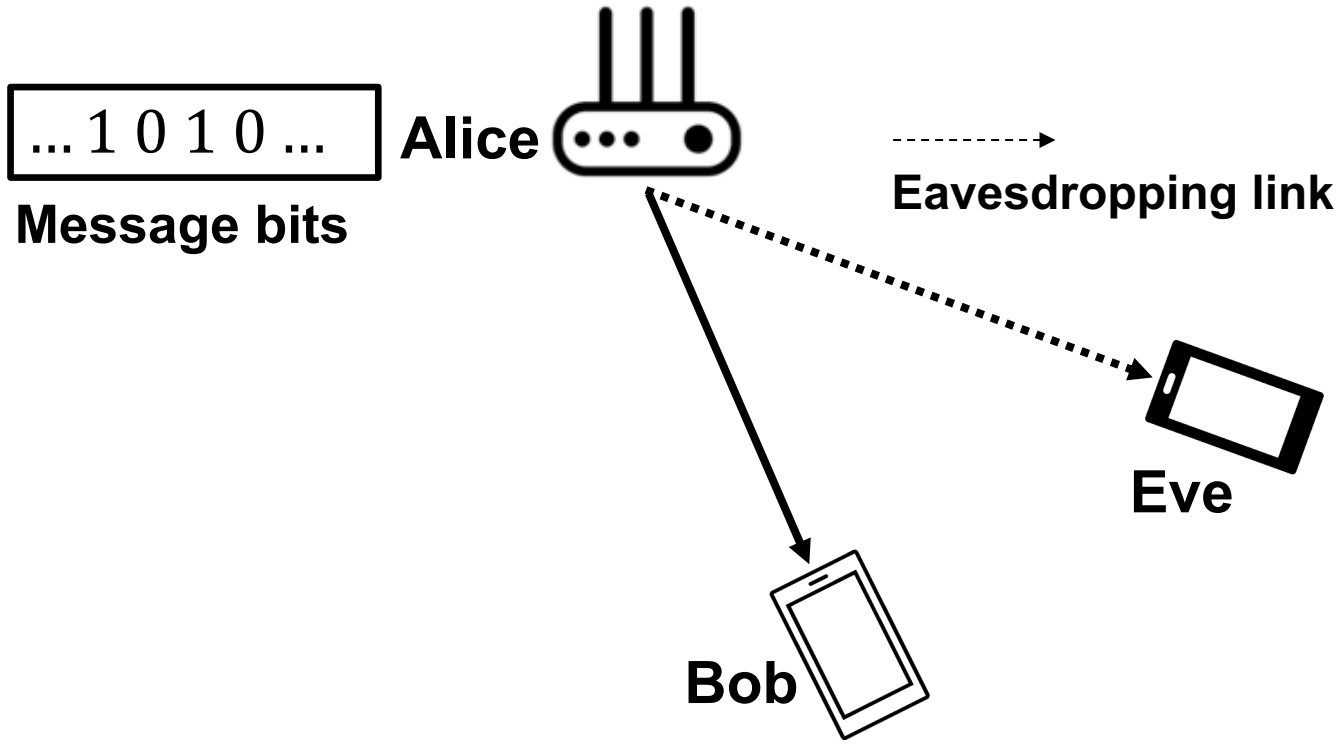


System & Modeling



System & Modeling

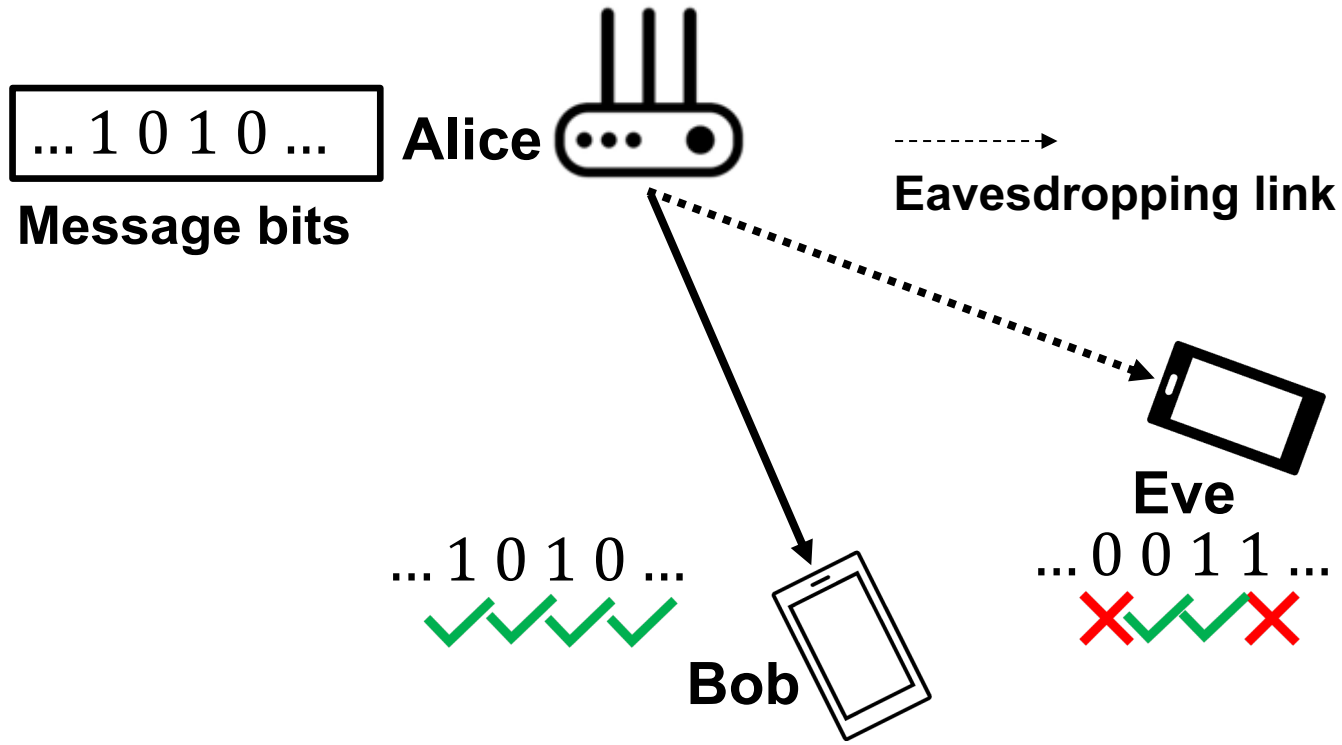
- **Randomly located in coverage range**
- **Eve can overhear messages through shared wireless medium**



Typical Indoor environment

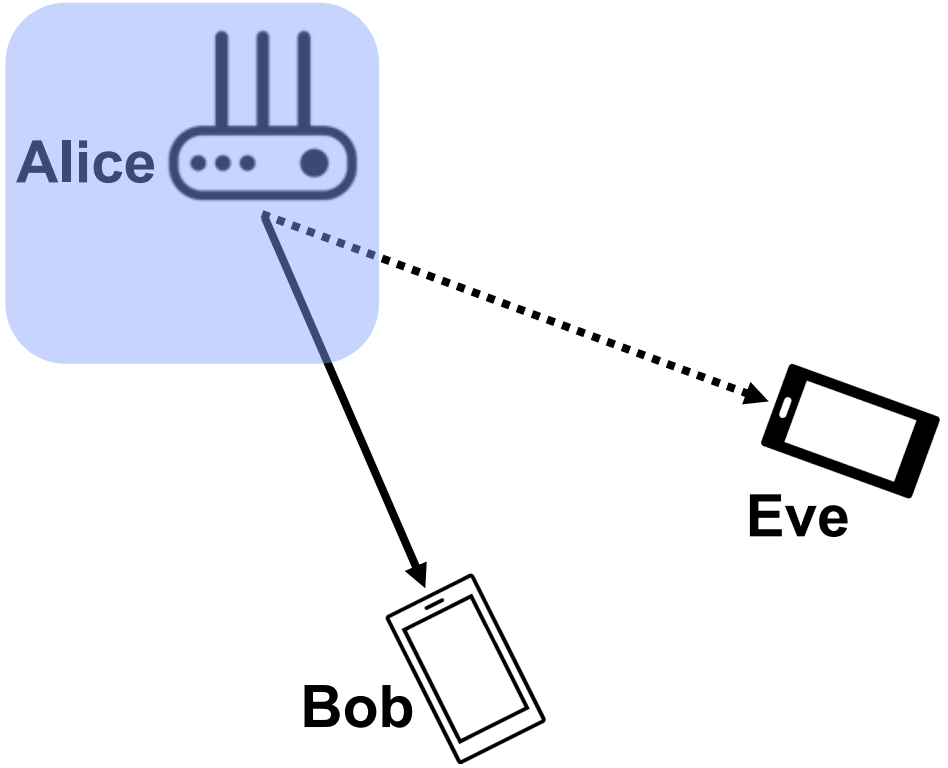
System & Modeling

- **Goal: Bob reliably decodes, and prevent Eve from decoding reliably**



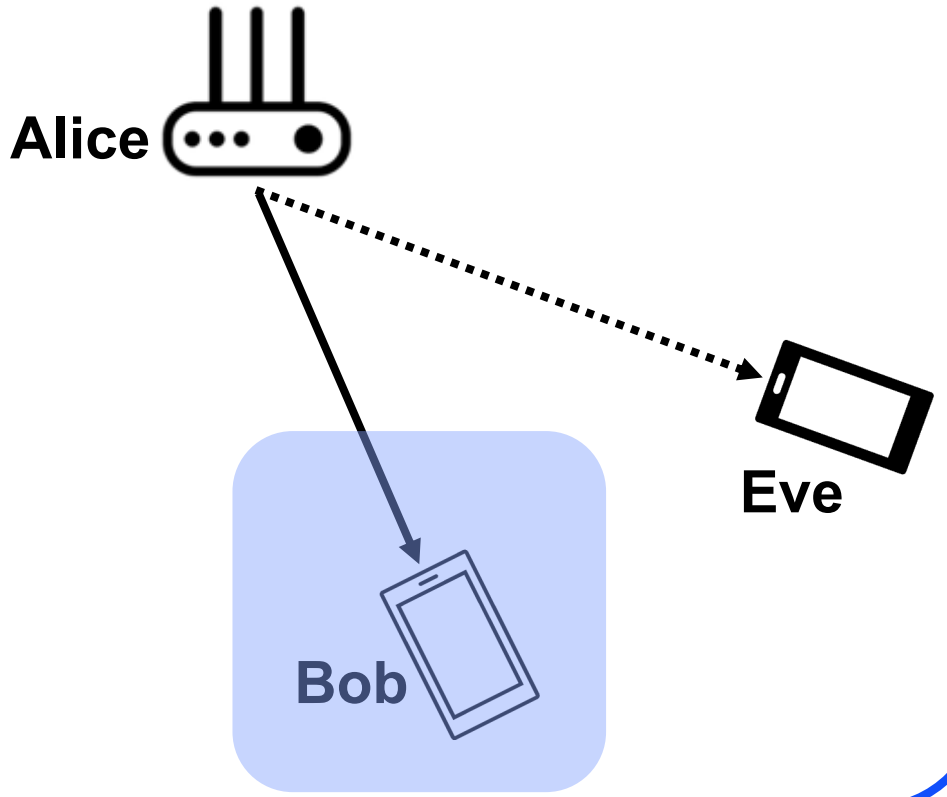
Threat Model

- An array of digital RF chains
- Can acquire Bob's Channel State Information (CSIT)



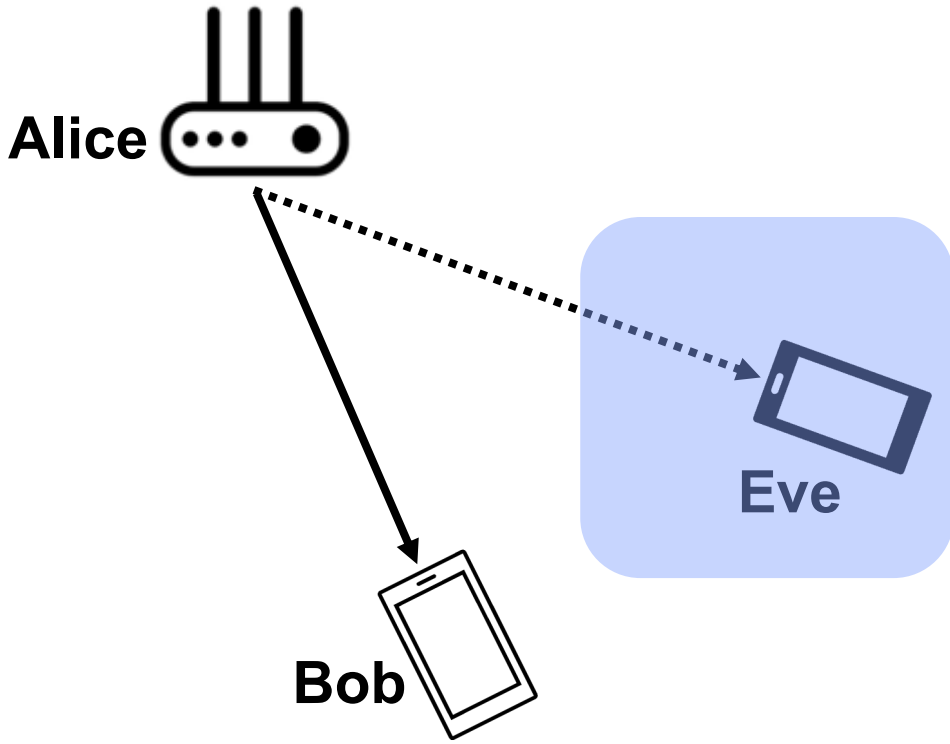
Threat Model

- **Bob has a single RF chain**
- **Can acquire his own Channel State Information (CSIR)**



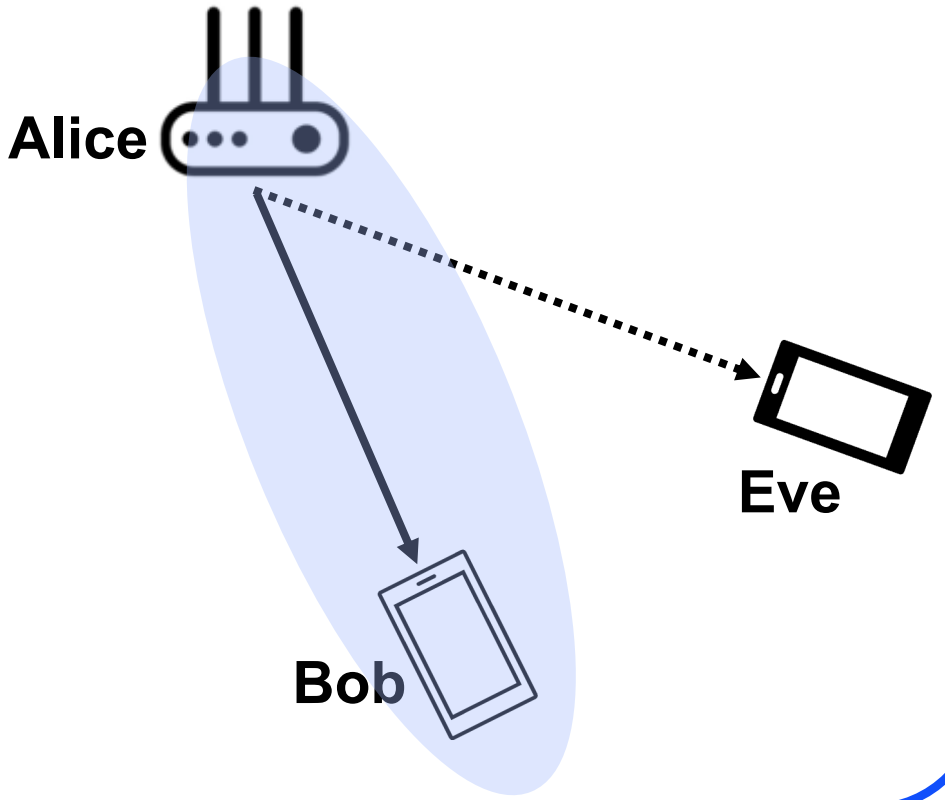
Threat Model

- **Eve has a single RF chain**
- **Can use her CSIR to decode signals**



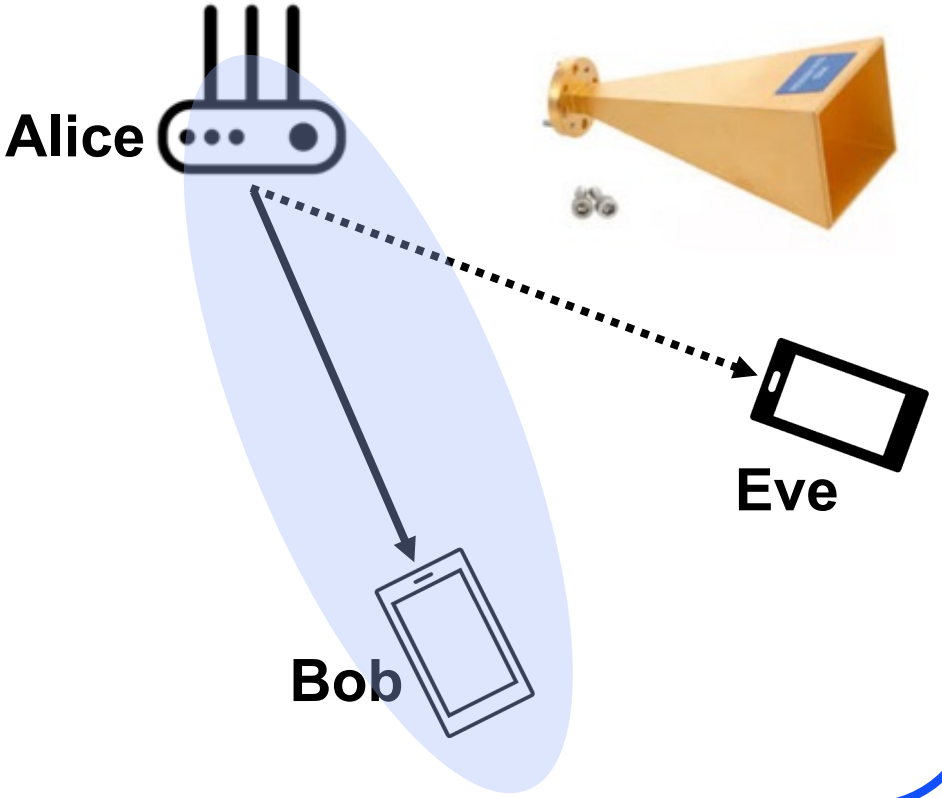
Conventional Beamforming

- **Keep signal power level low outside the main lobe**



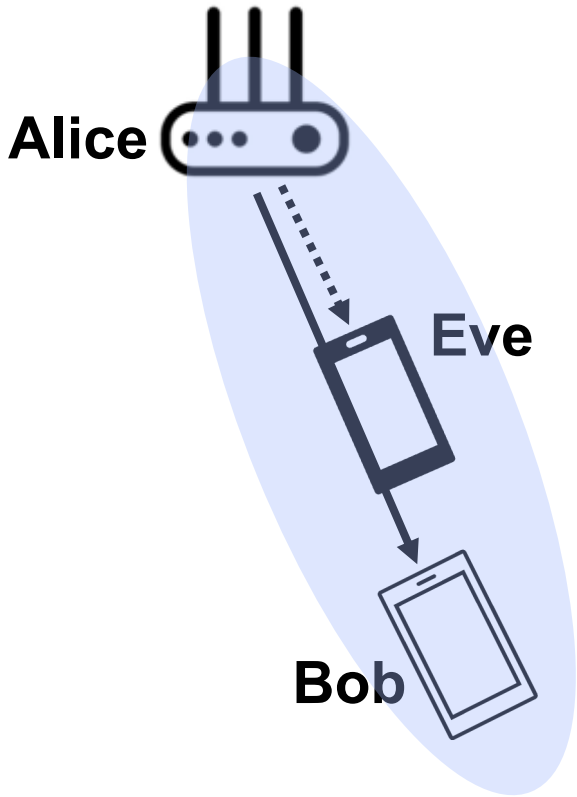
Eve's Countermeasure

- **Mount a high-gain antenna to increase Rx directivity**



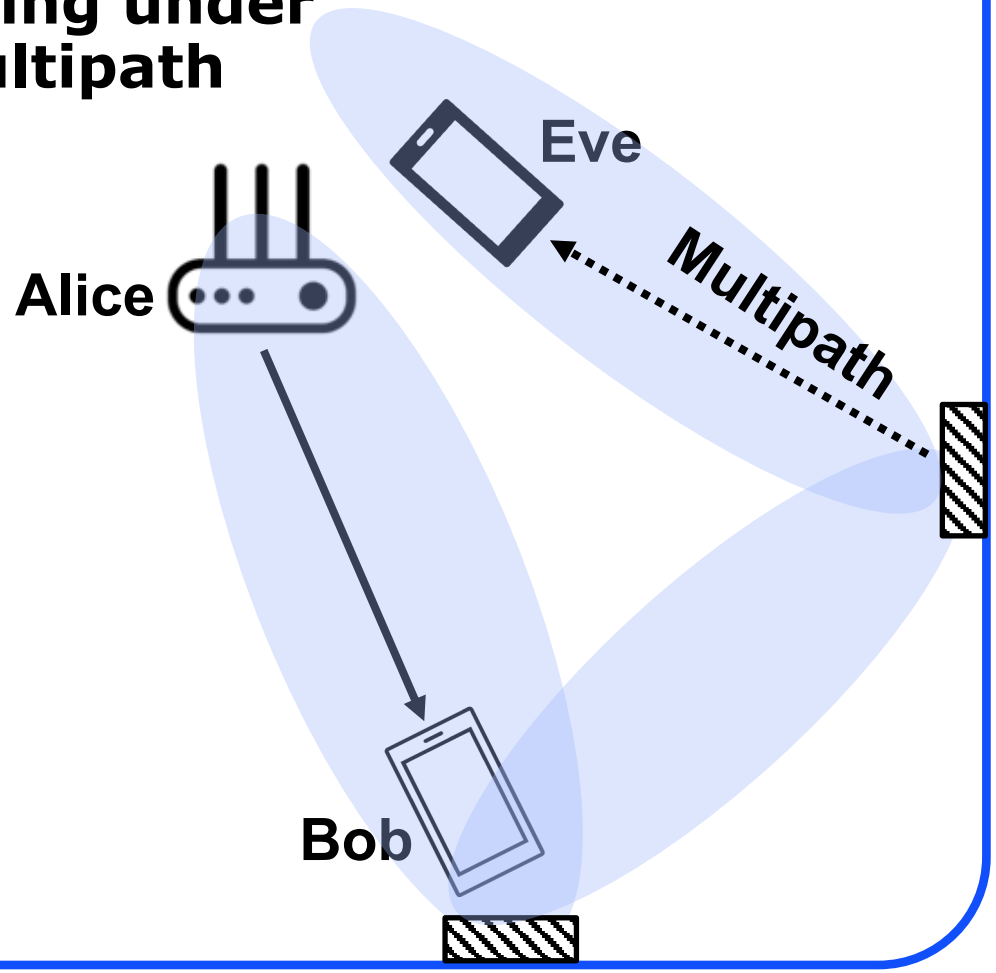
Eve's Countermeasure

- **Eve being nomadic**



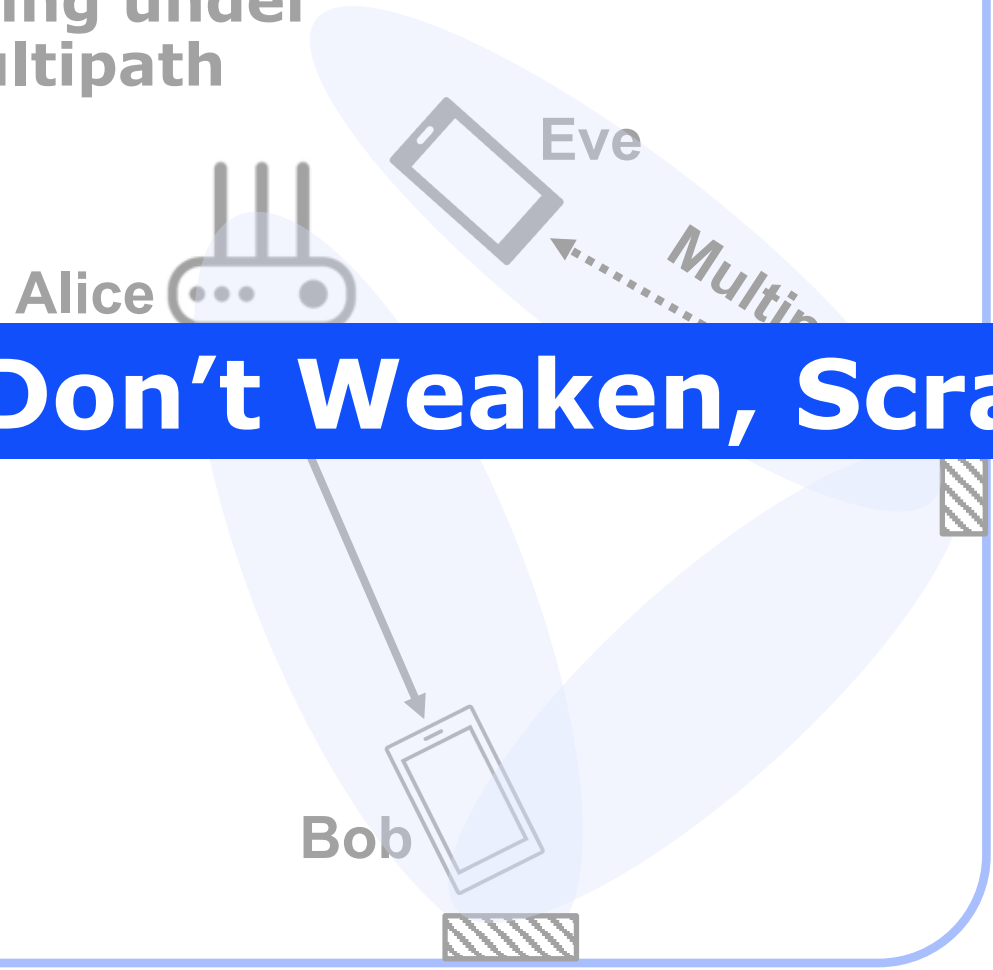
Eve's Countermeasure

- **Opportunistic eavesdropping under ambient multipath**



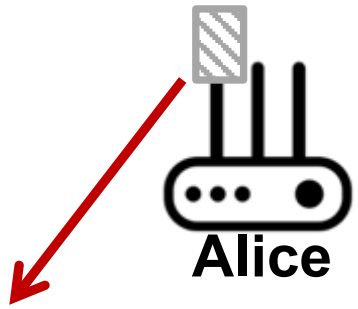
Eve's Countermeasure

- Opportunistic eavesdropping under ambient multipath



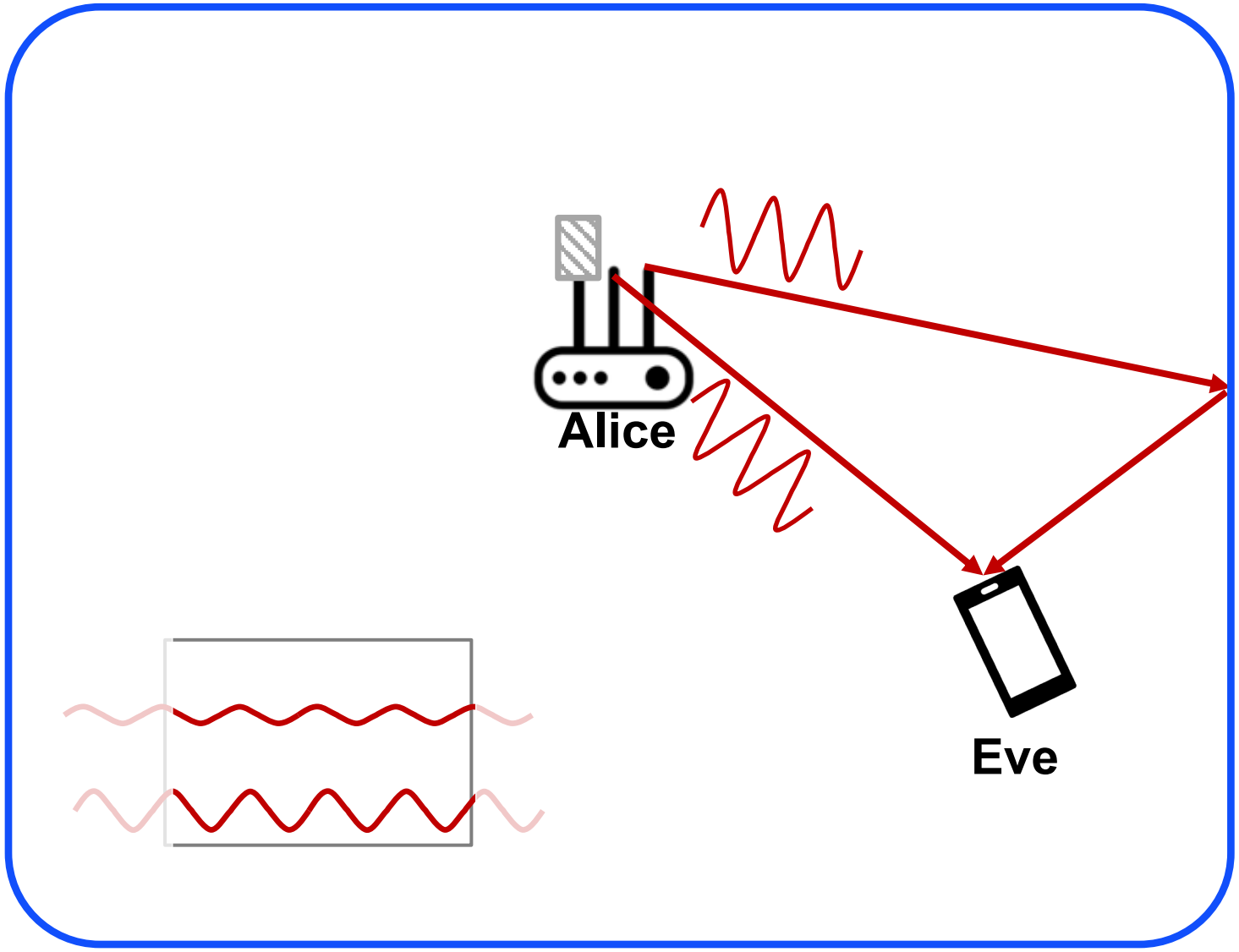
M3A Solution: Don't Weaken, Scramble!

Misinformation to Eve



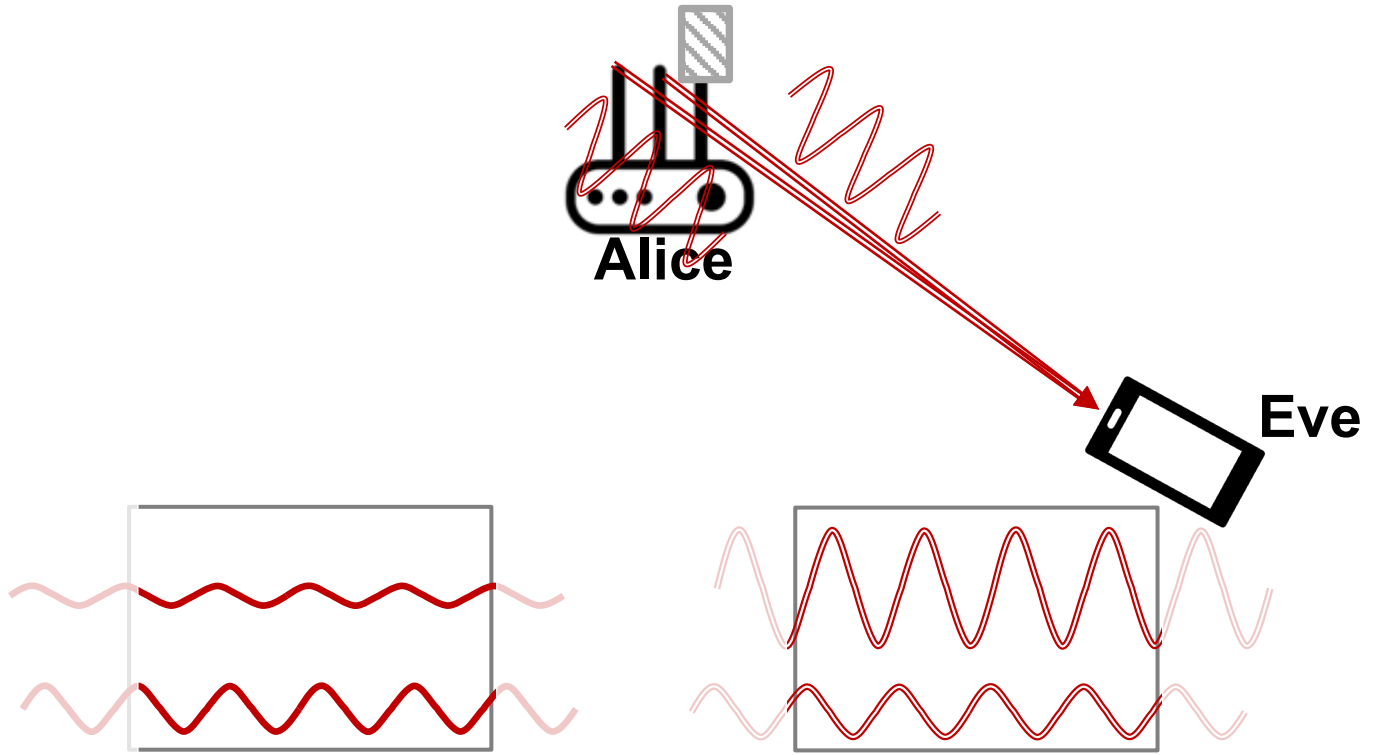
Leftmost antenna is OFF

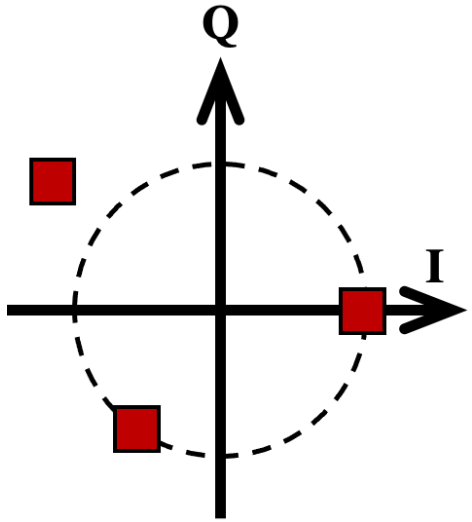
Misinformation to Eve



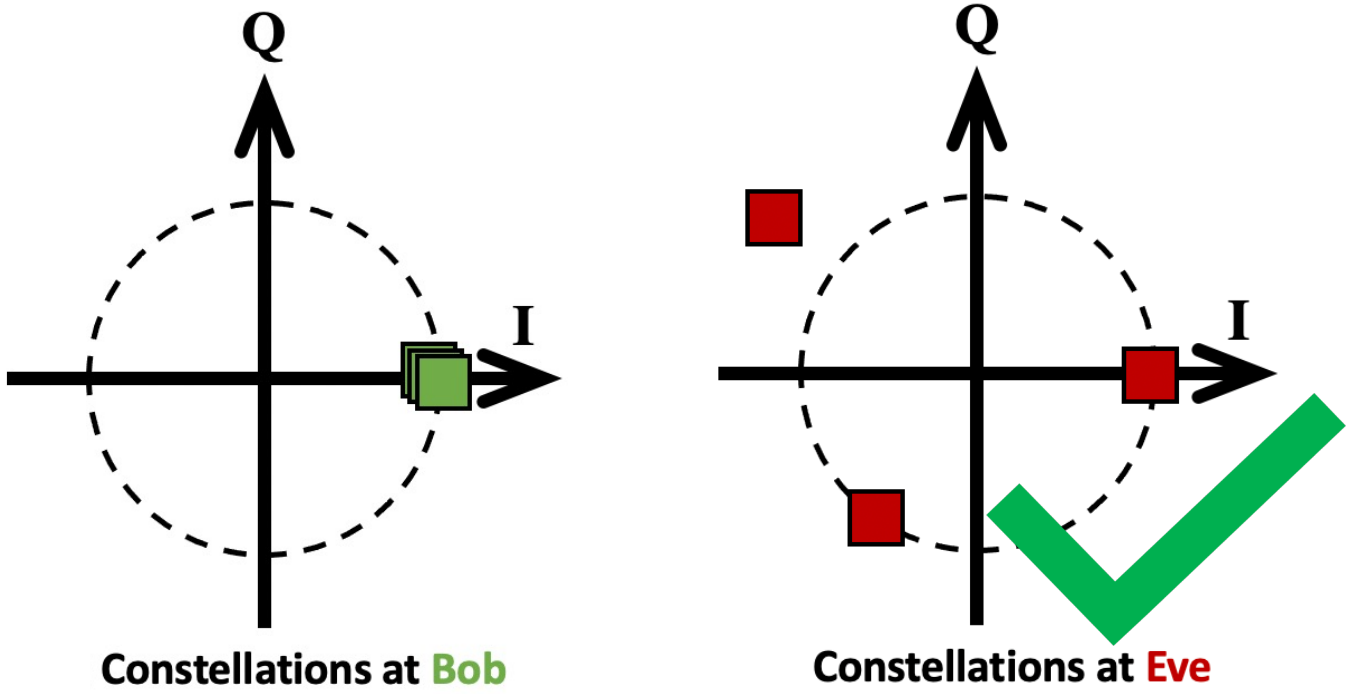
Misinformation to Eve

- Eve sees time-varying channel within a channel coherence block
- Scrambled constellations at Eve



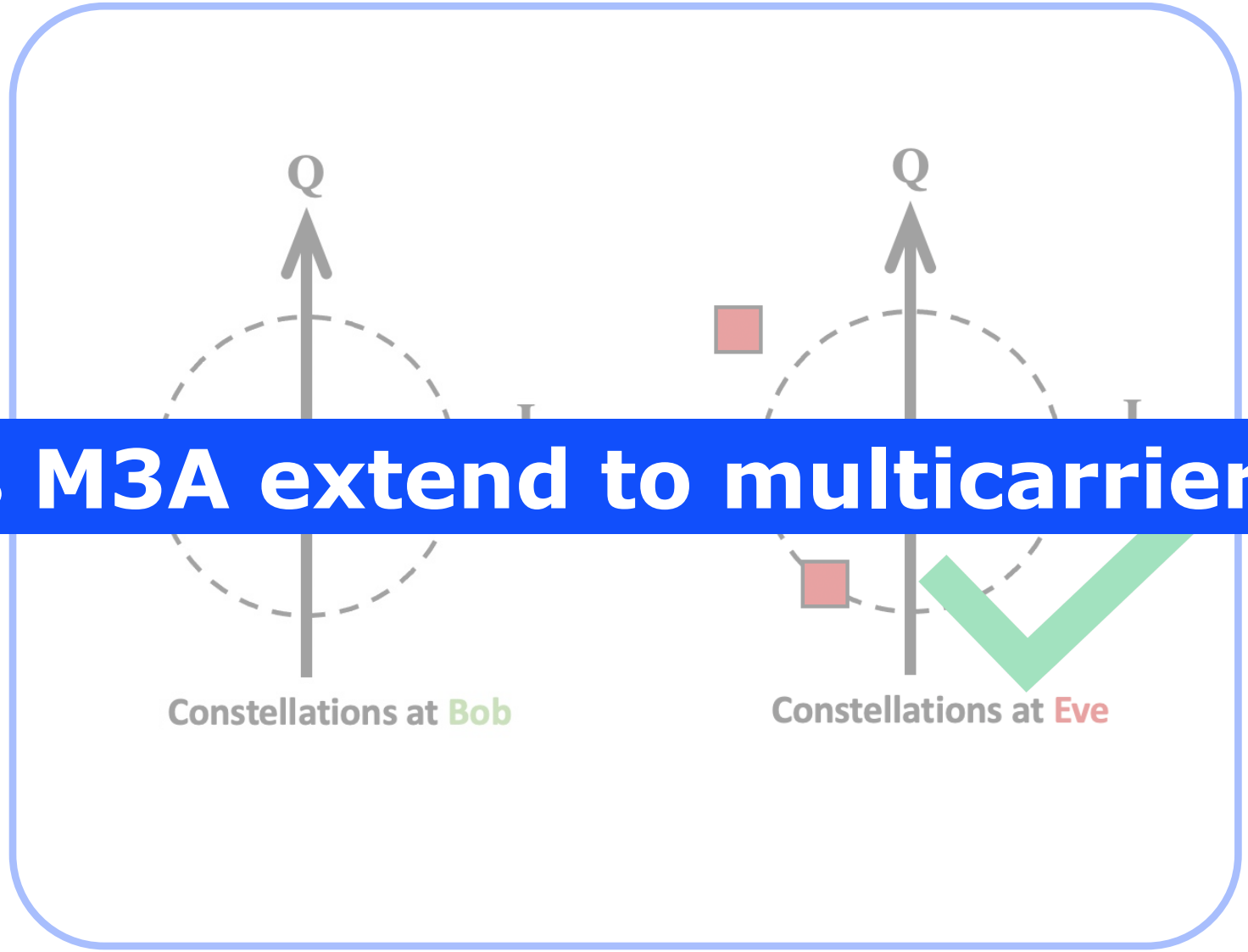


Our System: M3A



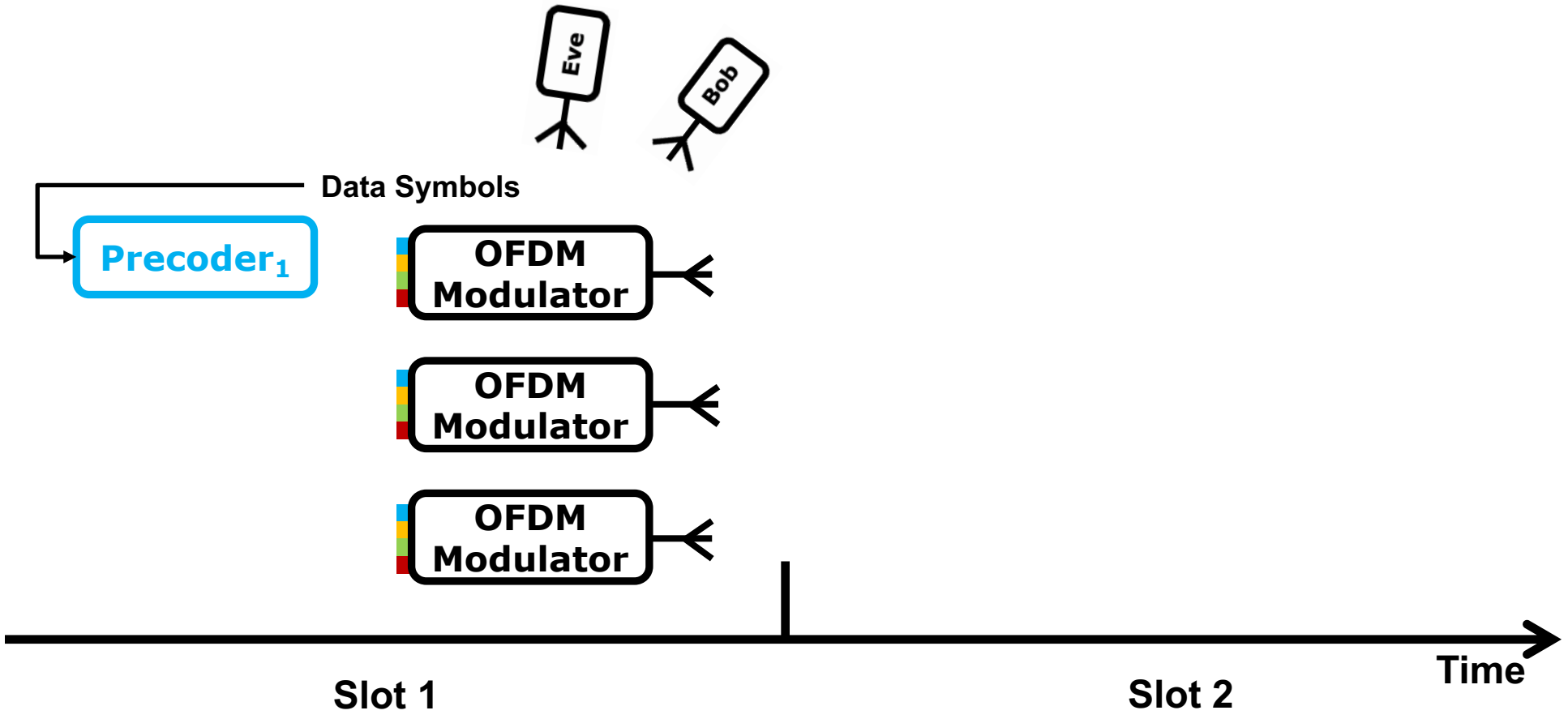
First-time realization of random antenna switching idea in digital beamforming

Our System: M3A

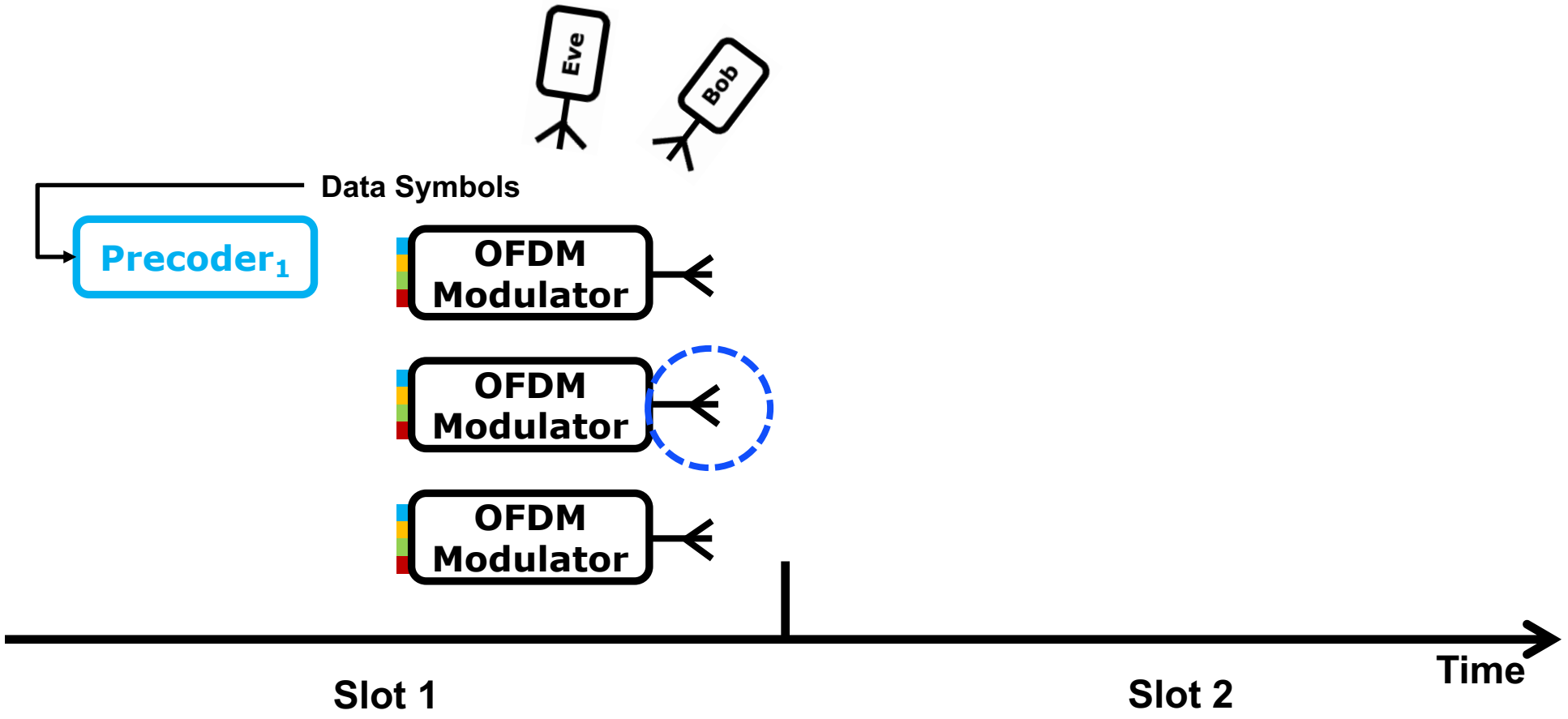


How does M3A extend to multicarrier scheme?

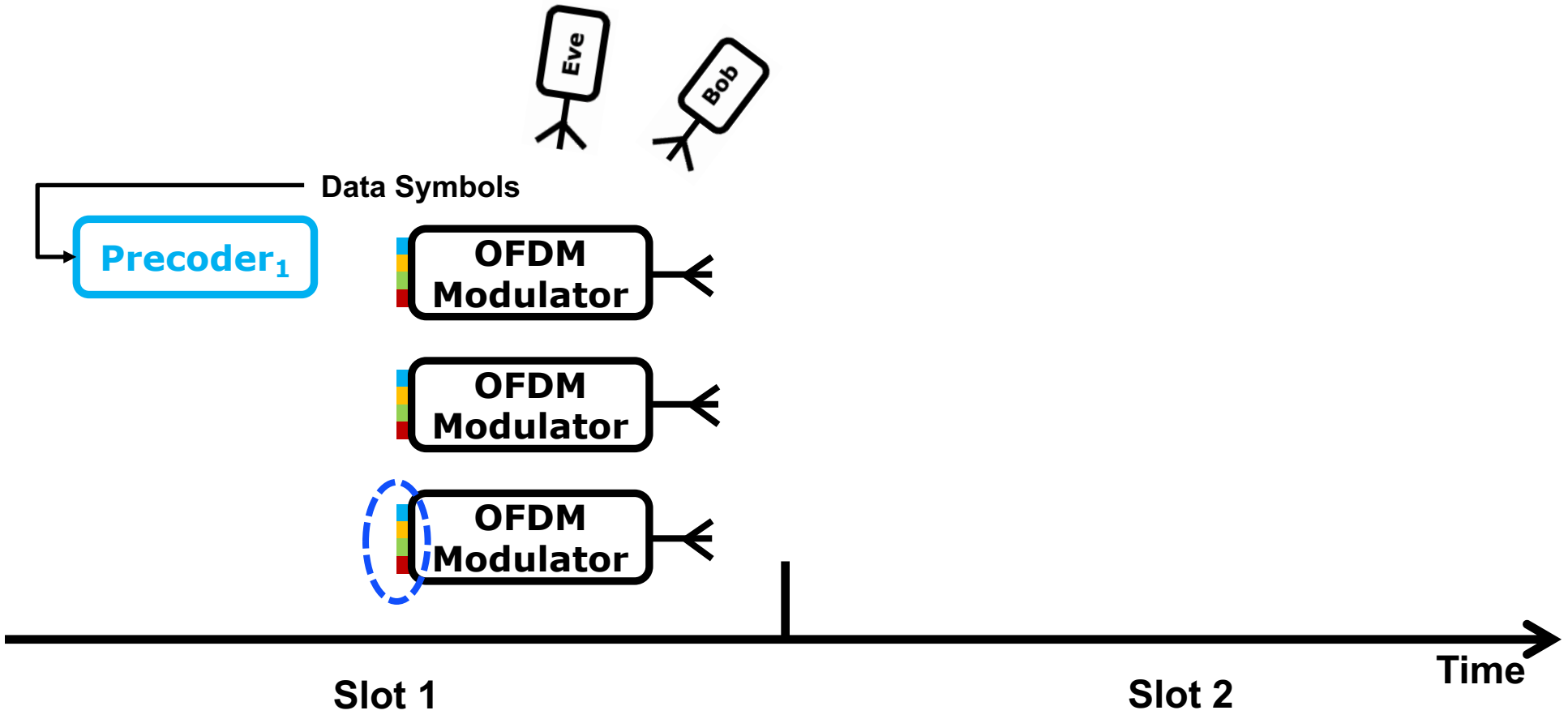
Multicarrier Virtual Antenna Selection



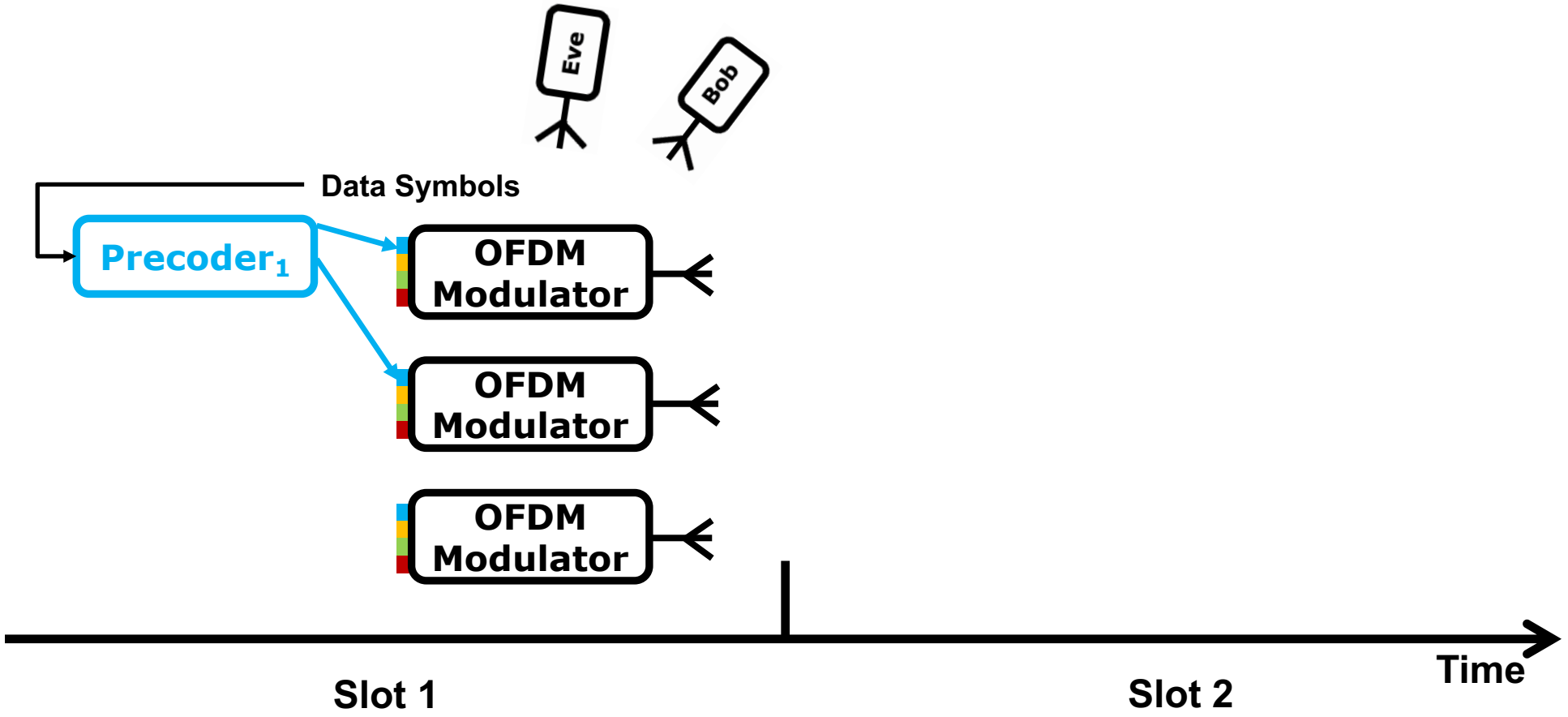
Multicarrier Virtual Antenna Selection



Multicarrier Virtual Antenna Selection

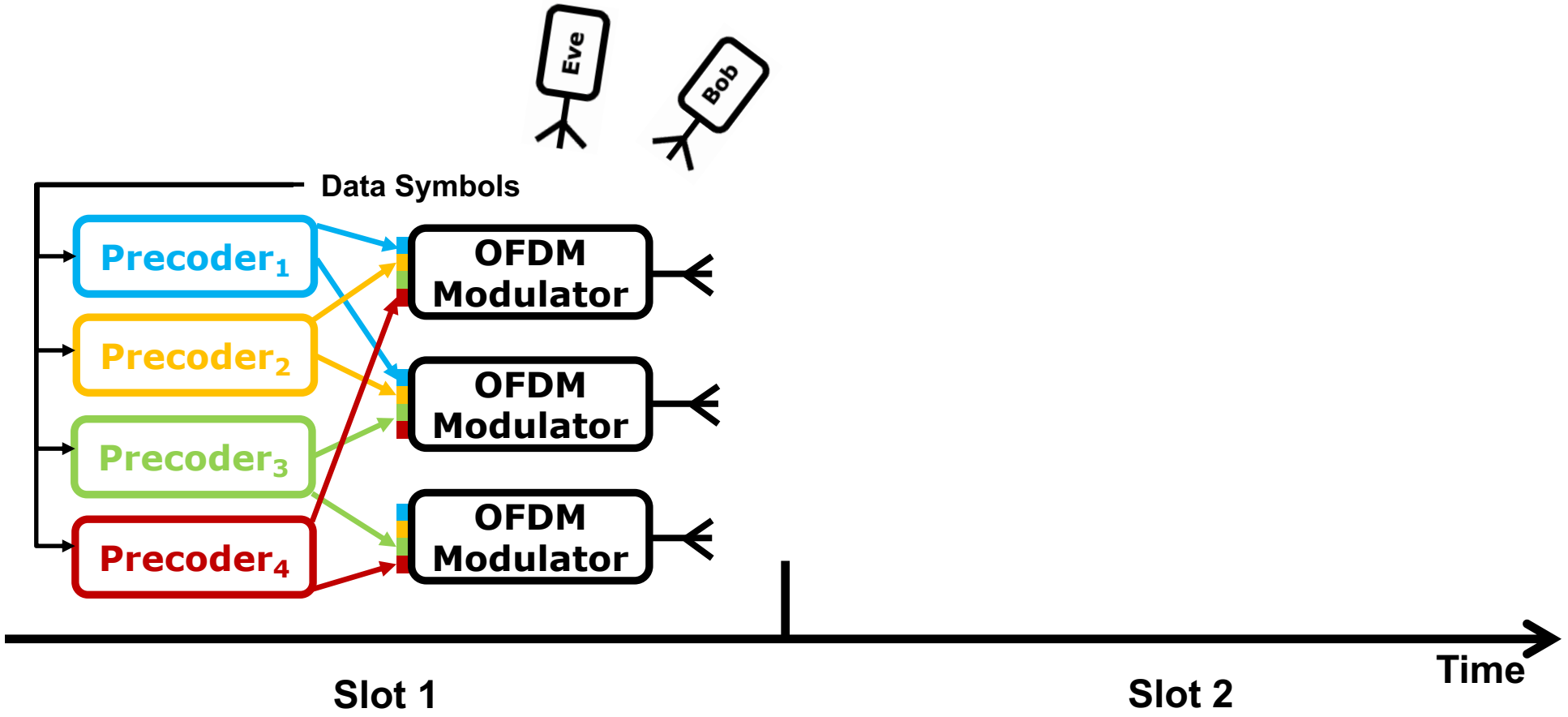


Multicarrier Virtual Antenna Selection



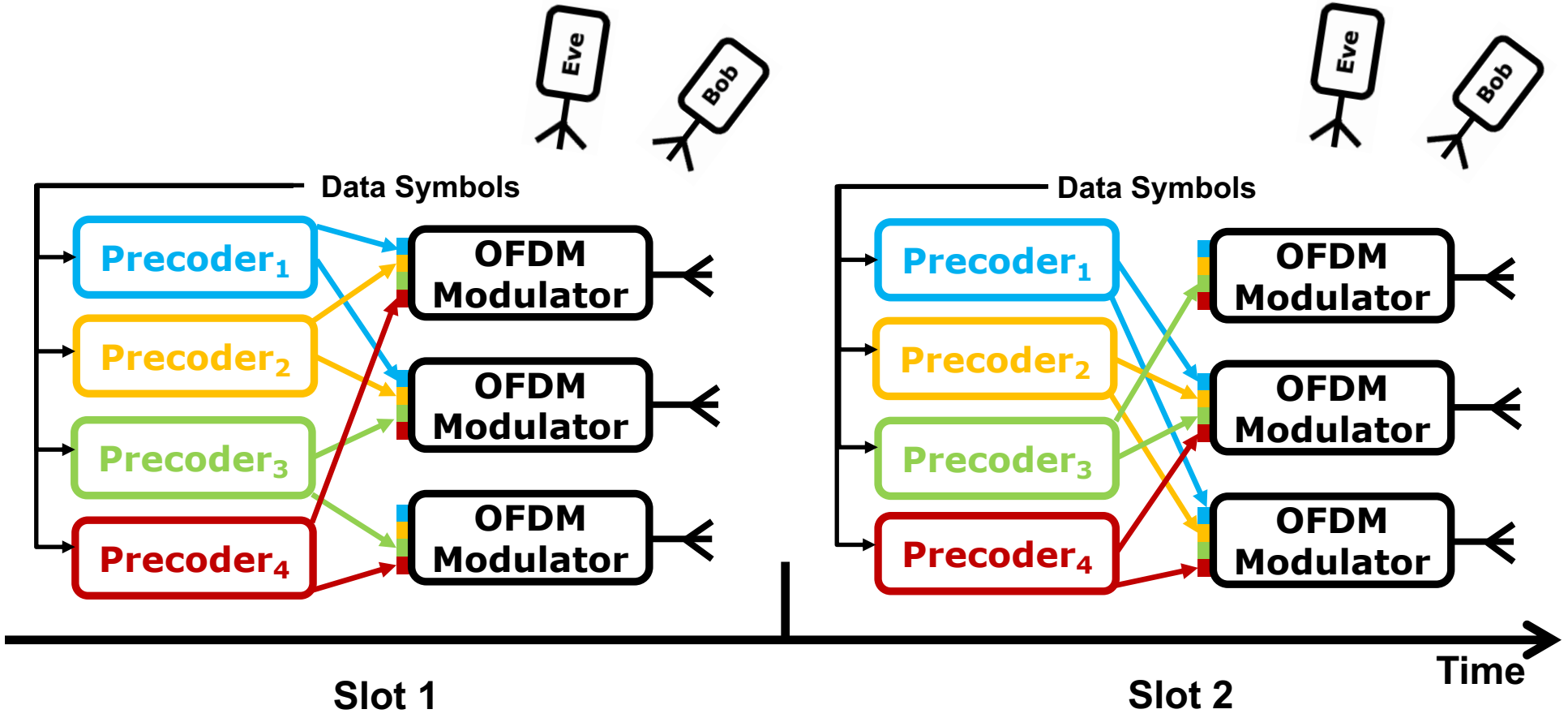
- **Each subcarrier's precoder sends precoded symbols to subset of OFDM modulators, which generate baseband waveforms**

Multicarrier Virtual Antenna Selection



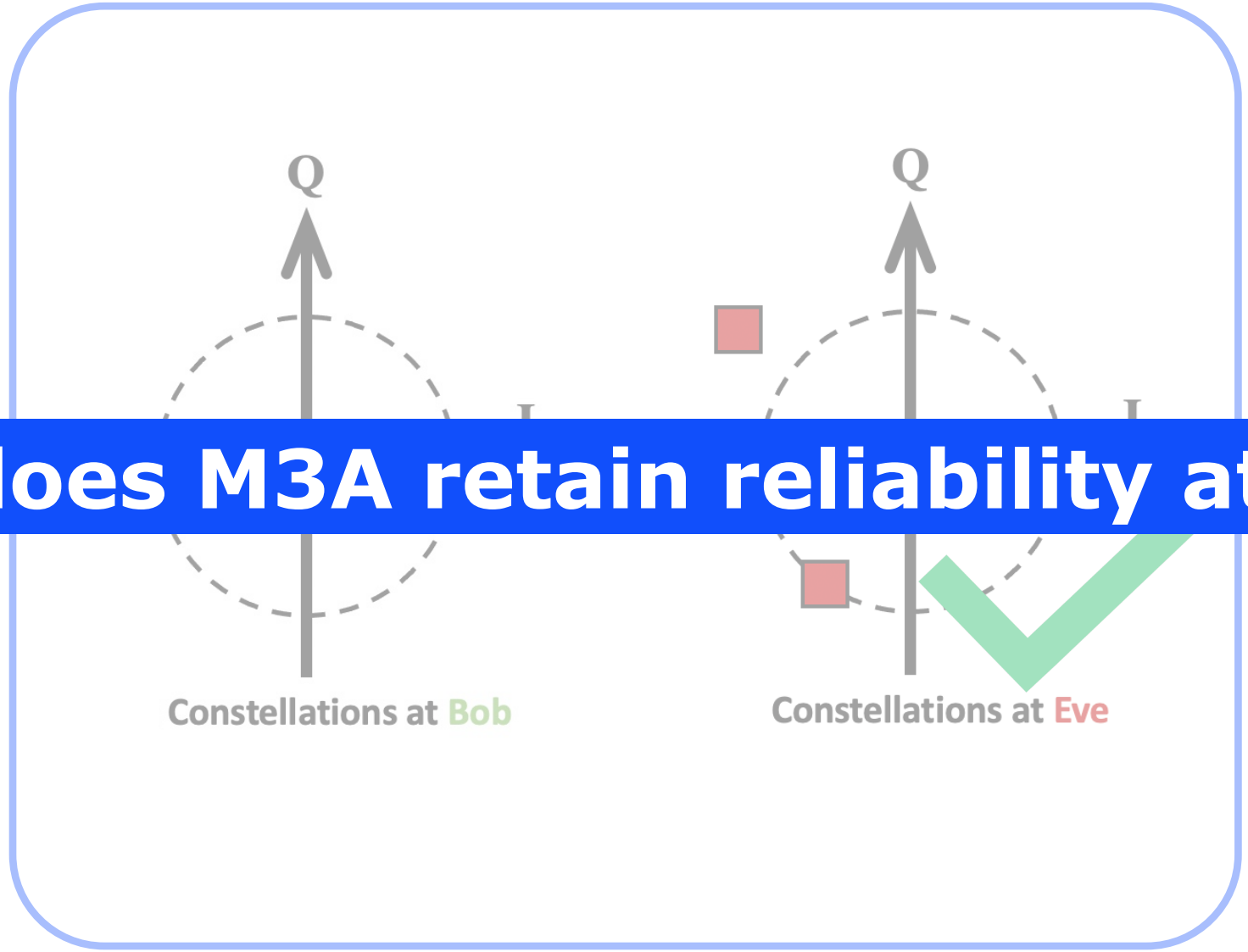
- **Each subcarrier virtually selects transmit antennas independently**

Multicarrier Virtual Antenna Selection



- **Alice scrambles constellations at Eve in both time and frequency.**

Our System: M3A

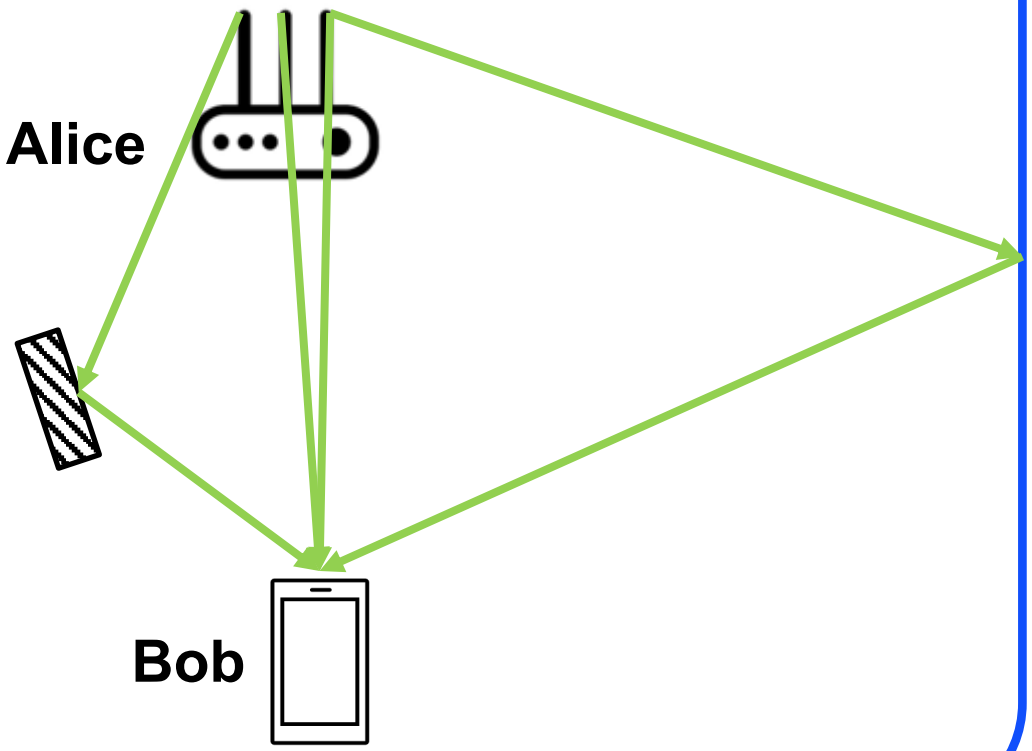


How does M3A retain reliability at Bob?

Effect of Antenna Switching at Bob

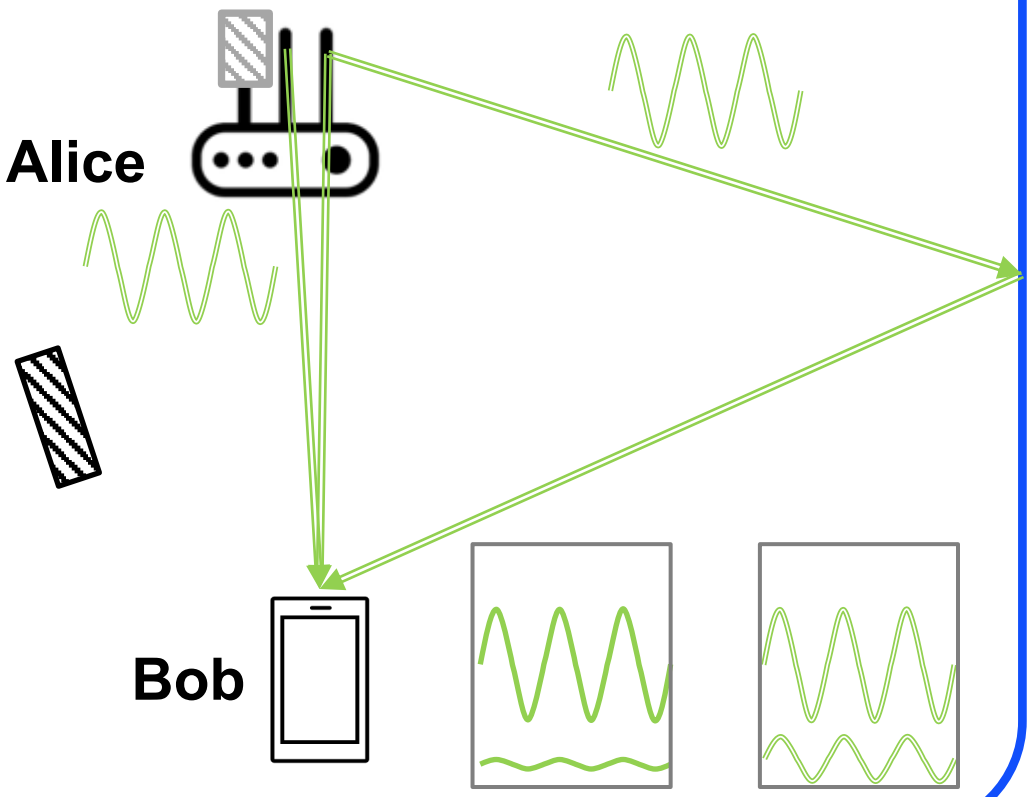
- ***Challenge: Indoor Multipath effect***

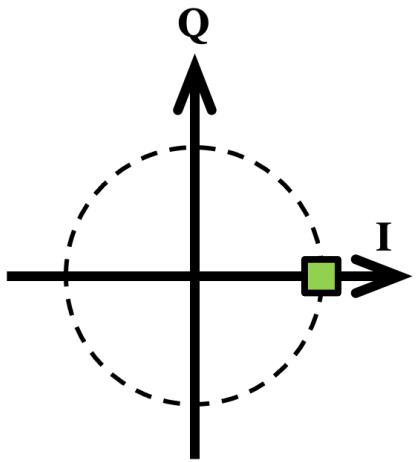
  signal arrives through multiple paths for each Tx-Rx antenna pair.



Effect of Antenna Switching at Bob

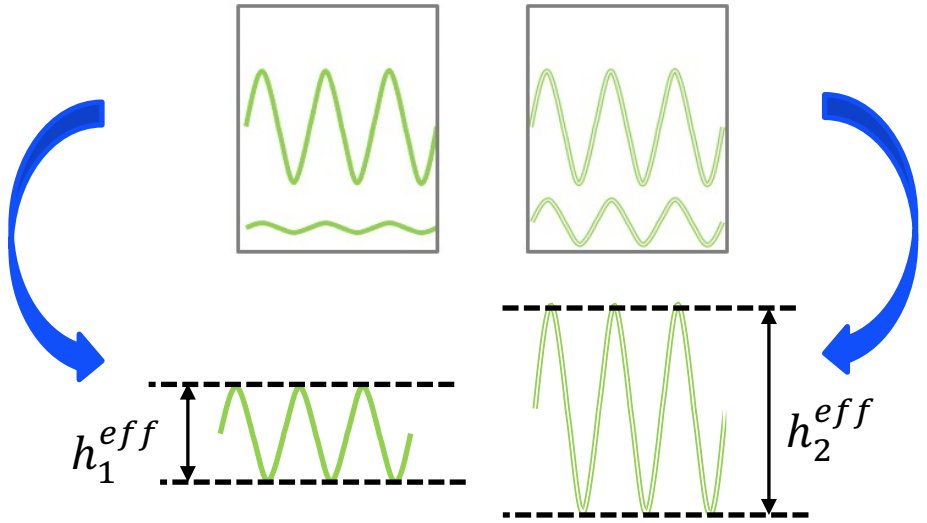
- **Even with perfect CSIT, amplitudes are still changing!**





Preserving Reliability at Bob

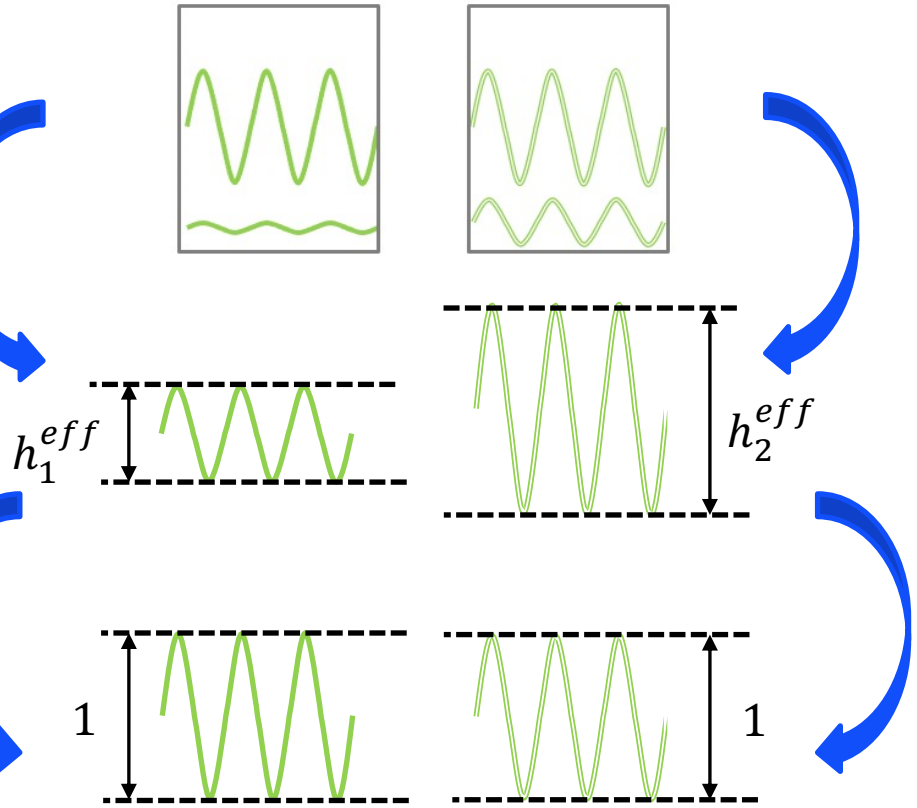
- **Idea: pre-cancel unwanted fading at Alice's precoder**



1. Alice finds effective channel gains

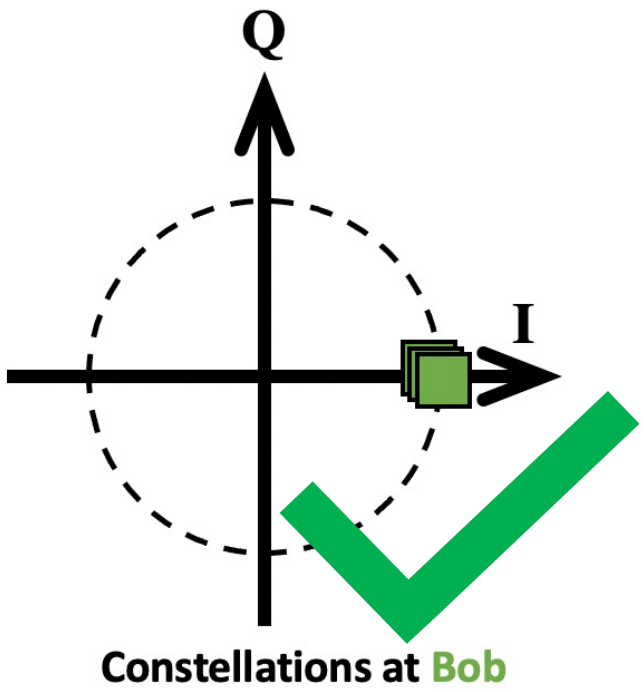
Preserving Reliability at Bob

- **Idea: pre-cancel unwanted fading at Alice's precoder**

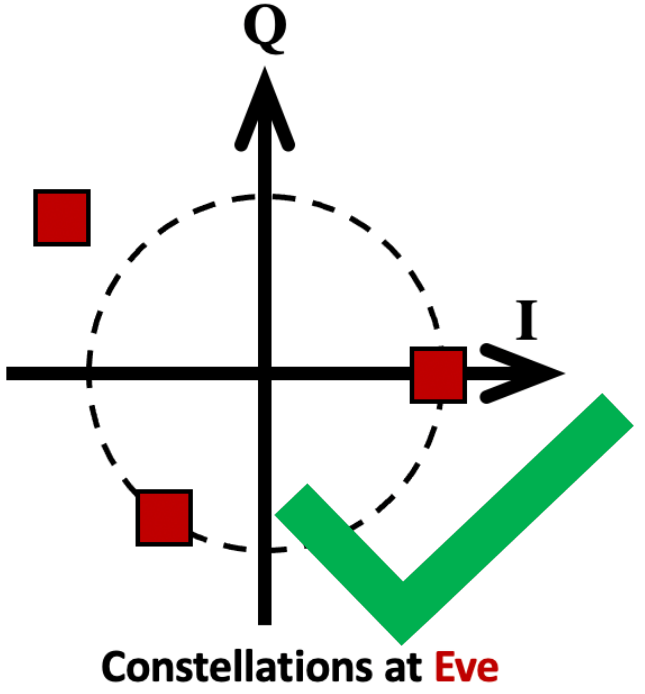


2. Normalize to unity amplitude

Our System: M3A

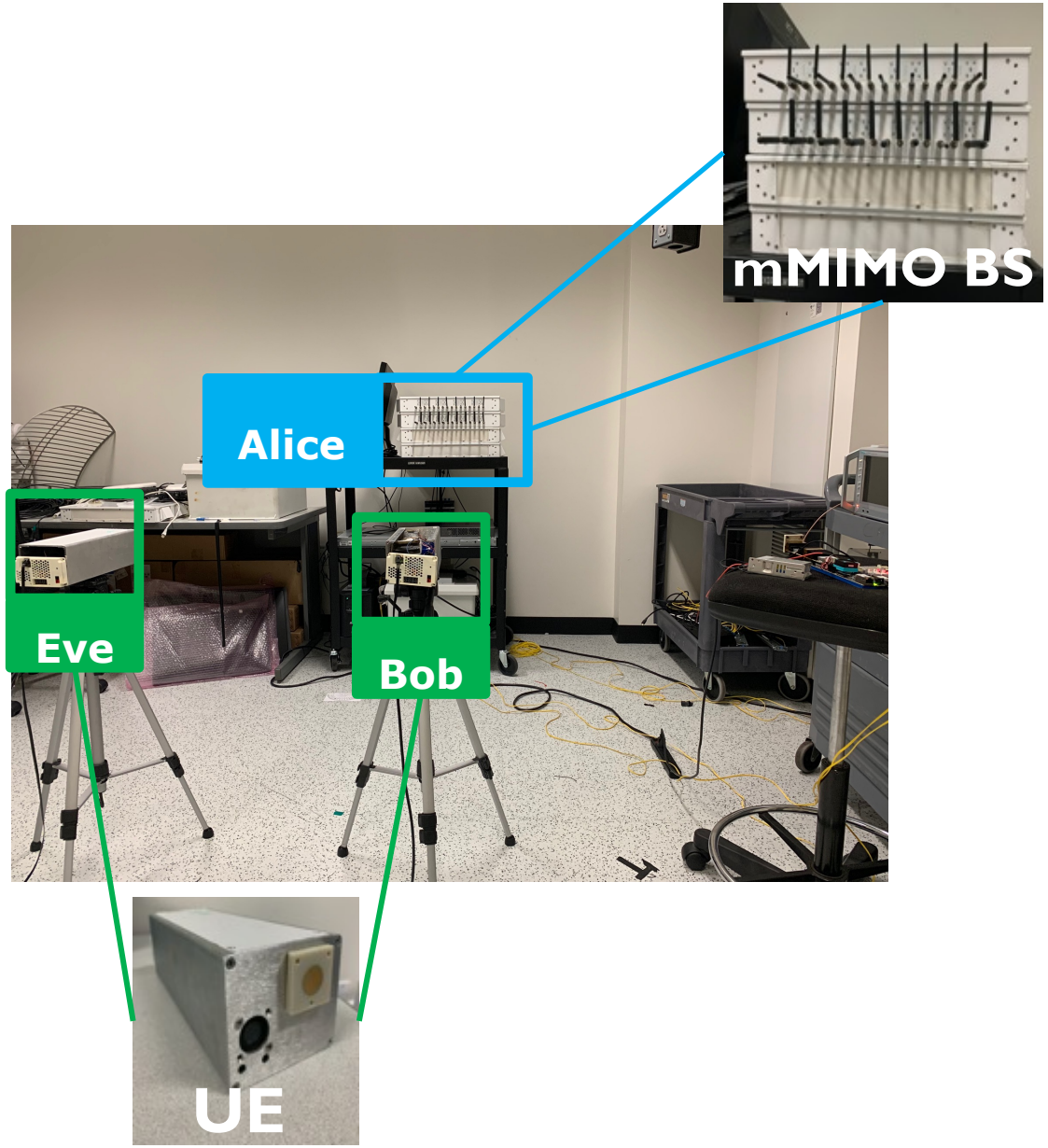


Constellations at Bob



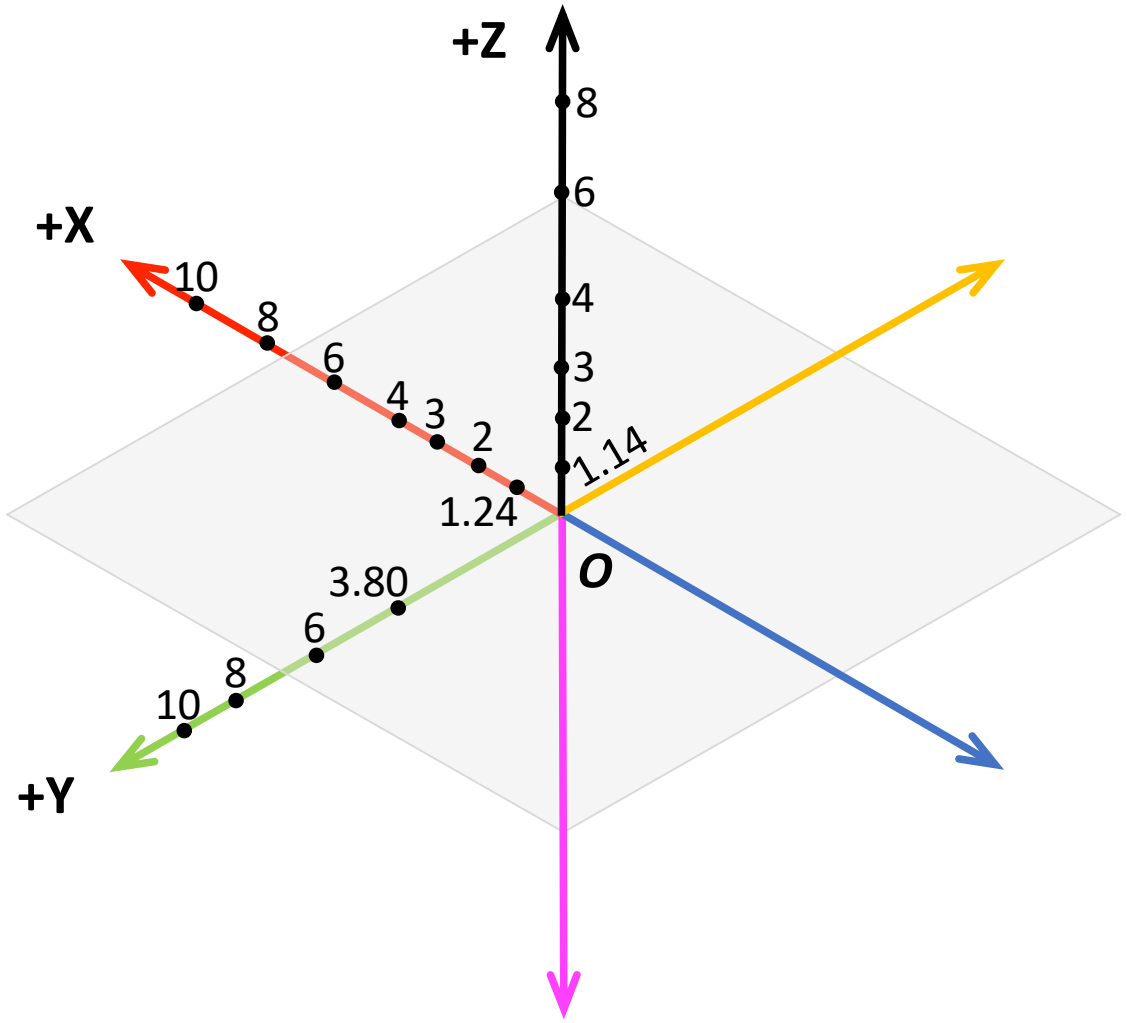
Constellations at Eve

Evaluation: *SDR Testbed*



- Testbed: **RENEW** Platform
- **Agora** mMIMO real-time baseband Software
- TDD OFDM transmission
- CBRS band (3.6 GHz)

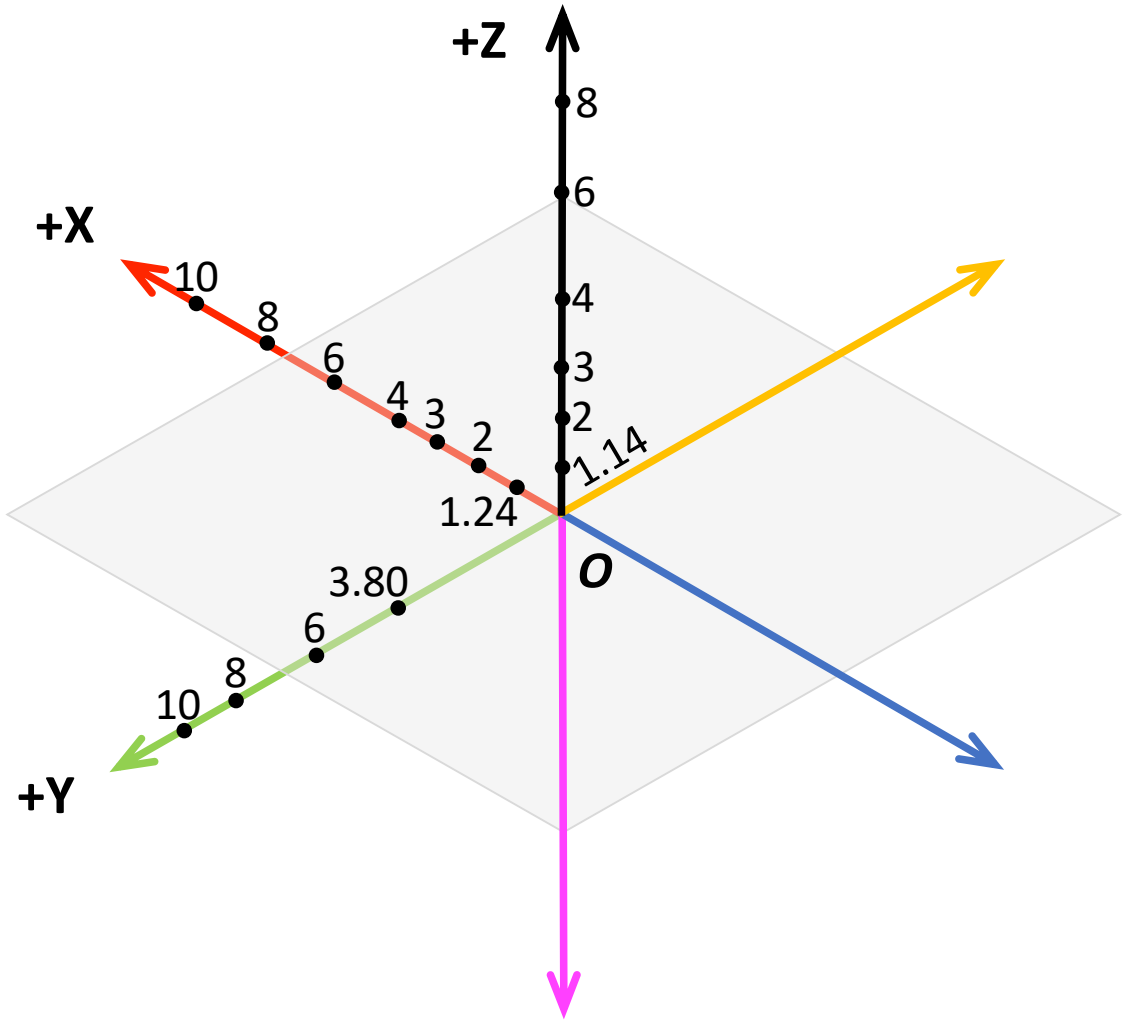
Evaluation: Security



- 6 different directions
- Distance normalized to the wavelength
- BER Gain $(x, s) =$

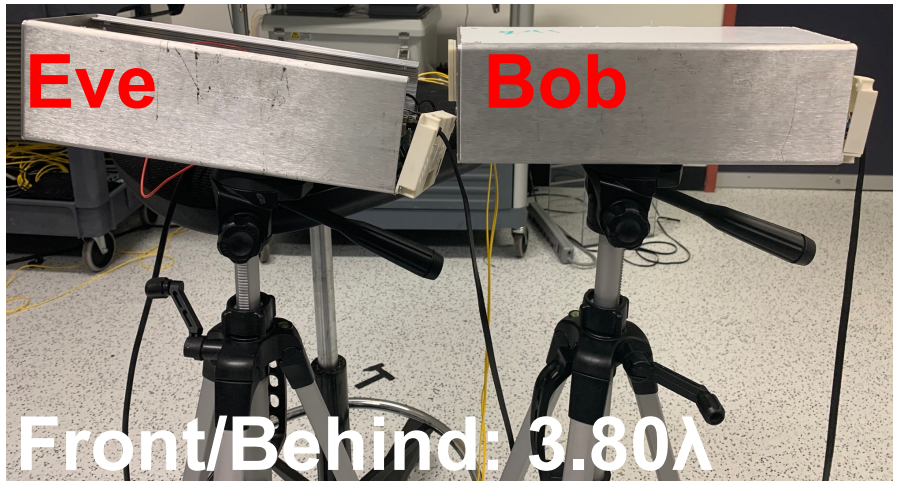
$$\frac{BER_{Eve}(x, s)}{BER_{Eve}(x, BF)}$$

Evaluation: Security



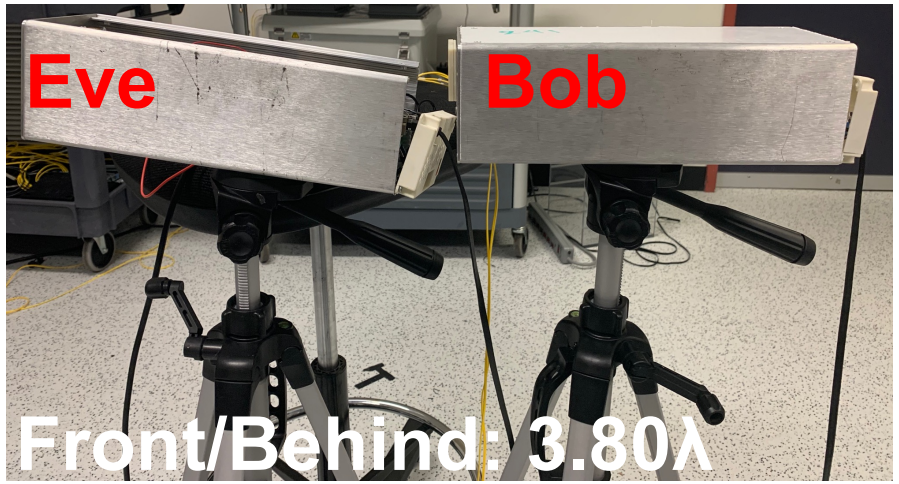
- Median BER Gain:
  - **115x** (horizontal)
  - **125x** (vertical)

Evaluation: Security



- M3A can scramble constellations even if Eve is between Alice and Bob
  - E.g., in front of Bob (with BER gain of 110x)

Evaluation: Security



- M3A can scramble constellations even if Eve is between Alice and Bob
  - E.g., in front of Bob (with BER gain of 110x)

- M3A achieves better security than BF even at wavelength-scale in 3D space
  - Rapid channel decorrelation in multipath environment

Evaluation: Reliability at Bob

- M3A maintains reliability at Bob under diverse channel conditions

- BER loss$(x, s) = \dfrac{BER_{Bob}(x, s)}{BER_{Bob}(x, BF)}$

Scheme	Median	95-th percentile
M3A	2.98	4.86
$M3A_{lc}$	4.09	66.2
FASM	22.6	93.3

Summary

- M3A can thwart passive eavesdroppers effectively even in wavelength-scale eavesdropping proximity.
- M3A retains reliability at Bob in practical indoor multipath environment.
- M3A has been implemented and extensively evaluated using an open-source real-time software-defined massive MIMO platform.
- M3A can be implemented in multi-antenna 5G and beyond base stations and does not require any modification in the UE.

Thank You!