Adaptive Demodulation for Wireless Systems in the Presence of Frequency-Offset Estimation Errors

Hanif Rahbari∗, Peyman Siyari†, Marwan Krunz†, and Jerry Park‡

∗ Rochester Institute of Technology

†University of Arizona

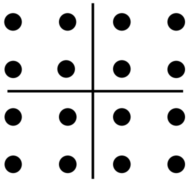
‡Virginia Tech

April 18, 2018

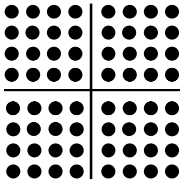
Honolulu, HI

INFOCOM 2018

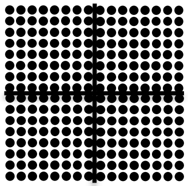
Increasing Applications of High-Order Modulations



16-QAM



64-QAM



256-QAM

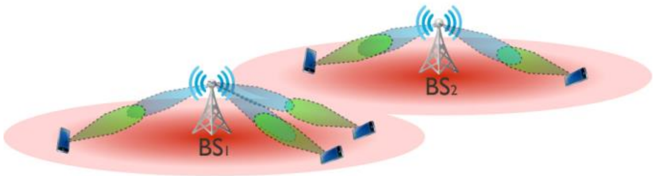
Increasing Applications of High-Order Modulations

Supporting higher data rates and better spectral efficiency

Increasing Applications of High-Order Modulations

Supporting higher data rates and better spectral efficiency

- mmWave systems: up to **64-QAM**



Source: [http://www.profheath.org/research/millimeter-wave-cellular-systems/]

Increasing Applications of High-Order Modulations

Supporting higher data rates and better spectral efficiency

- mmWave systems: up to **64-QAM**
- DVB-S2X satellite television: up to **256-APSK**

Increasing Applications of High-Order Modulations

Supporting higher data rates and better spectral efficiency

- mmWave systems: up to **64-QAM**
- DVB-S2X satellite television: up to **256-APSK**
- 5G New Radio: up to **1024-QAM**

Increasing Applications of High-Order Modulations

Supporting higher data rates and better spectral efficiency

- ❑ mmWave systems: up to **64-QAM**
- ❑ DVB-S2X satellite television: up to **256-APSK**
- ❑ 5G New Radio: up to **1024-QAM**
- ❑ IEEE 802.11ax: up to **1024-QAM**

Increasing Applications of High-Order Modulations

Supporting higher data rates and better spectral efficiency

- ❑ mmWave systems: up to **64-QAM**
- ❑ DVB-S2X satellite television: up to **256-APSK**
- ❑ 5G New Radio: up to **1024-QAM**
- ❑ IEEE 802.11ax: up to **1024-QAM**

Providing higher security by obfuscating payload's modulation scheme

Payload's modulation order leaks the payload size and data rate

Used to launch various attacks: user tracking, traffic analysis, selective jamming, etc.

Increasing Applications of High-Order Modulations

Supporting higher data rates and better spectral efficiency

- ❑ mmWave systems: up to **64-QAM**
- ❑ DVB-S2X satellite television: up to **256-APSK**
- ❑ 5G New Radio: up to **1024-QAM**
- ❑ IEEE 802.11ax: up to **1024-QAM**

Providing higher security by obfuscating payload's modulation scheme

Payload's modulation order leaks the payload size and data rate

Used to launch various attacks: user tracking, traffic analysis, selective jamming, etc.

Example (802.11a systems):

$1\ ms$ **QPSK**-modulated payload:

→ 250 OFDM symbols (symbol duration: $4\mu s$)

→ 24 Mbps data rate (2 bits/symbol, 48 subcarriers)

→ $3{,}000$ coded bytes

Review: Modulation Obfuscation [MobiHoc'15, TIFS'16]

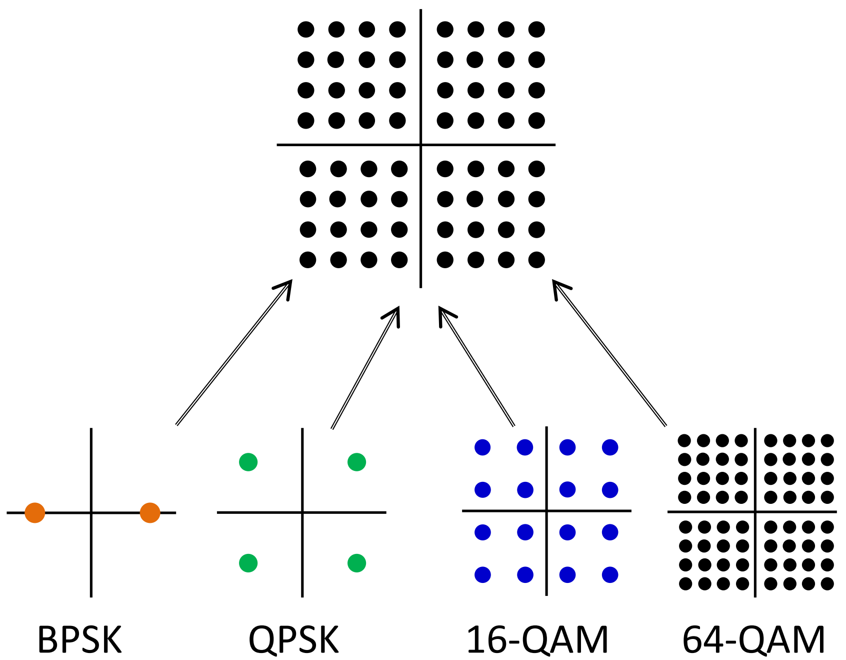
Hide (obfuscate) the payload's modulation scheme

Covertly "embed" modulated symbols of every payload into the dense constellation map of the highest-order modulation scheme

- Hide true modulation scheme without changing it

  → Same information rate (rate adaptation algorithm works as normal)

- Example:



Review: Modulation Obfuscation [MobiHoc'15, TIFS'16]

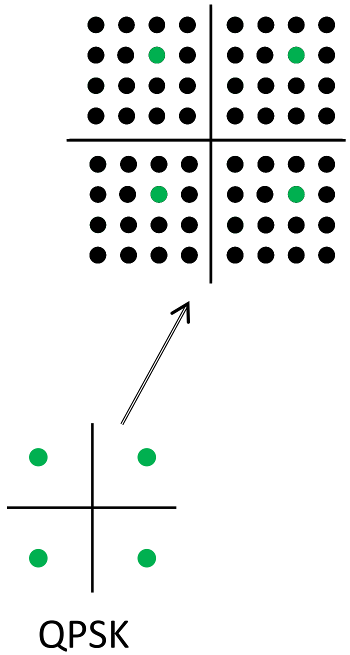
Hide (obfuscate) the payload's modulation scheme

Covertly "embed" modulated symbols of every payload into the dense constellation map of the highest-order modulation scheme

- Hide true modulation scheme without changing it

  → Same information rate (rate adaptation algorithm works as normal)

- Example:



Review: Modulation Obfuscation [MobiHoc'15, TIFS'16]

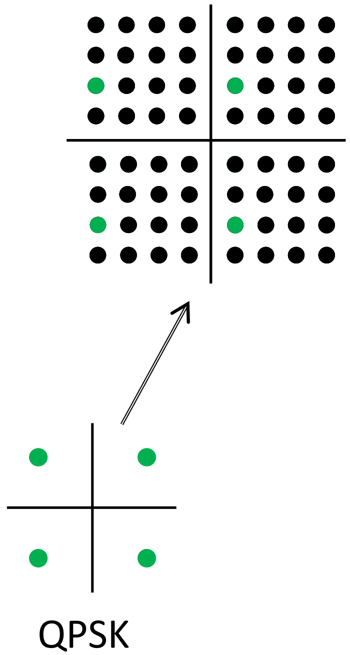
Hide (obfuscate) the payload's modulation scheme

Covertly "embed" modulated symbols of every payload into the dense constellation map of the highest-order modulation scheme

- Hide true modulation scheme without changing it

  → Same information rate (rate adaptation algorithm works as normal)

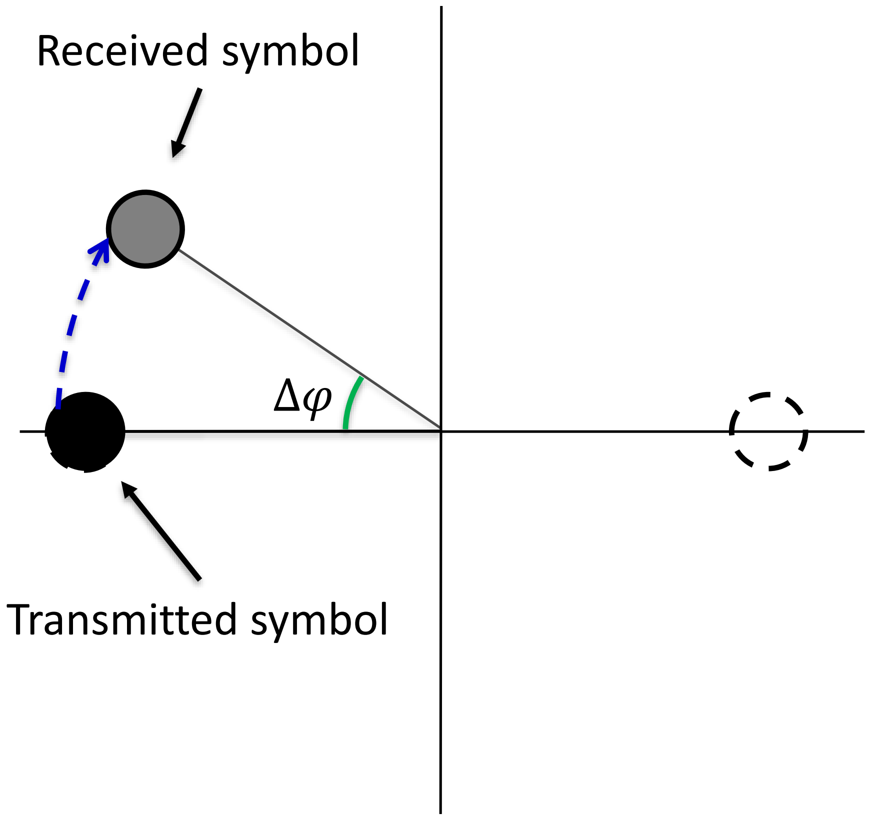
- Example:



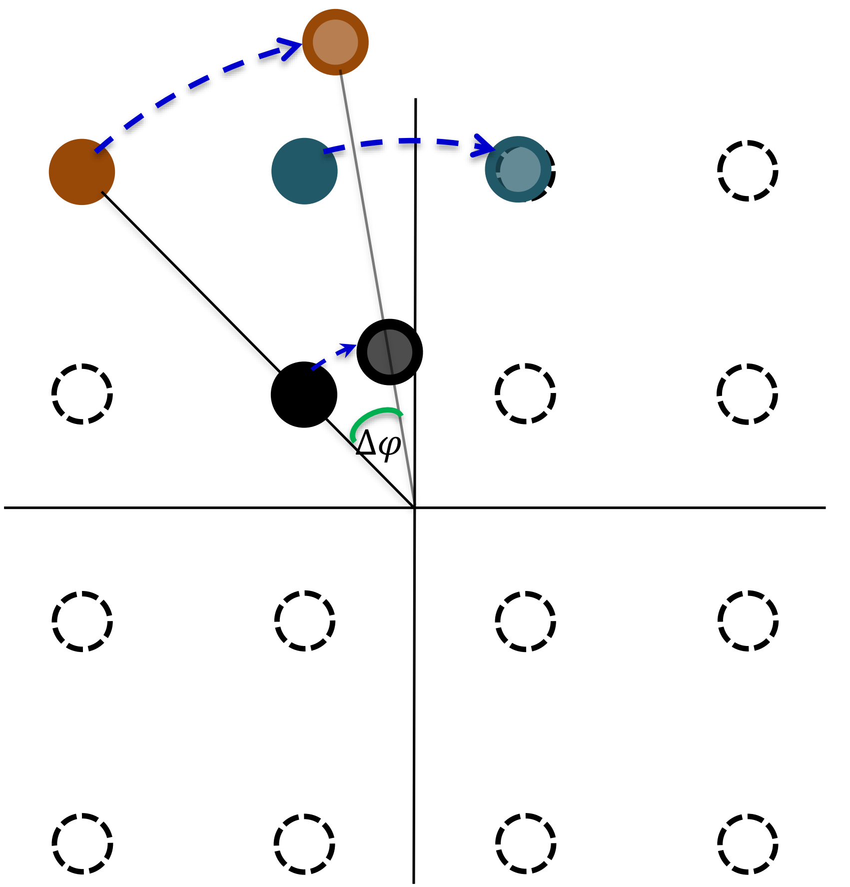
Challenge: High Sensitivity to Phase Offset

Denser constellation maps are more vulnerable to phase offset

Example: BPSK vs. 16-QAM at the receiver



BPSK
(no demodulation error)



16-QAM
(several demodulation errors)

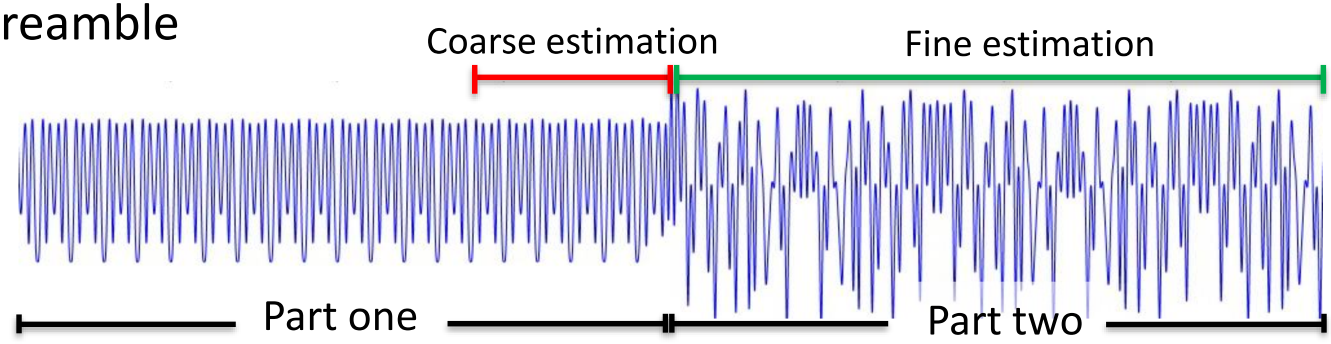
Residual Phase Offset

Common causes

- Imperfect channel estimation
- **Residual carrier frequency offset (CFO)**
  - CFO: Mismatch between operating freq. of two devices (+ Doppler shift)

Receiver uses frame preamble to estimate CFO

- Example: Wi-Fi preamble



In a noisy channel, CFO estimation can never be perfect

$$\Delta\varphi(t) = 2\pi \times \delta_f \times t$$

Time-varying phase offset

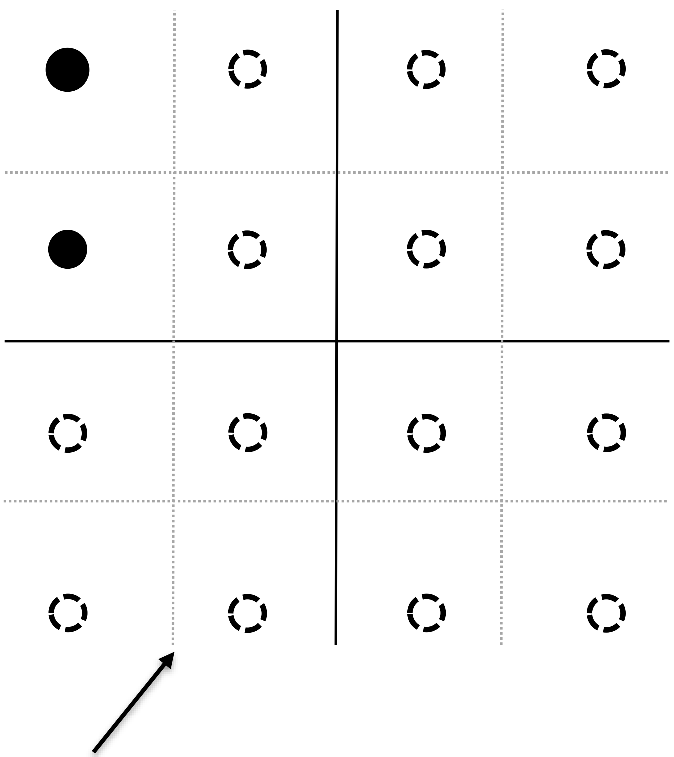
Residual CFO

time

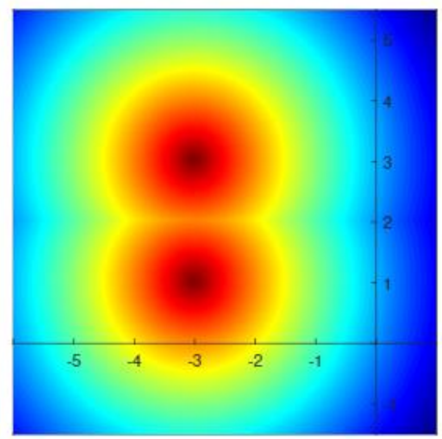
Symbol Distribution under CFO-induced Phase Offset

Symbols with **unequal** amplitudes have **unequal** sensitivity to $\Delta\varphi(t)$

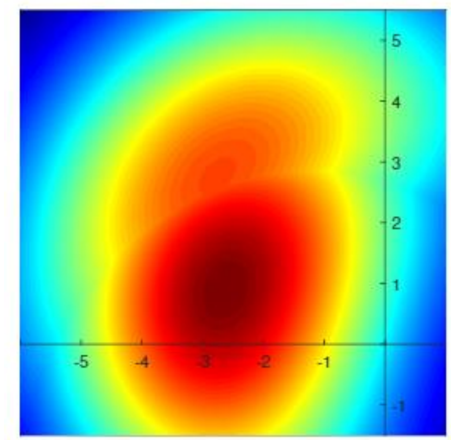
Example: Heatmap of the location of two received 16-QAM symbols under AWGN



Default demodulation boundaries



No residual CFO



With residual CFO

Main contribution: A probabilistic approach for adaptive (CFO-aware) demodulation

Theoretical Analysis (Wi-Fi Systems)

Probability density function of phase offset per symbol (under AWGN)

$$f_\Psi(\psi) \sim \frac{\sqrt{l\gamma}\cos^2\frac{\psi}{2}}{\sqrt{2\pi\cos\psi}} e^{-2l\gamma\, sin^2(\frac{\psi}{2})}$$

# of preamble samples

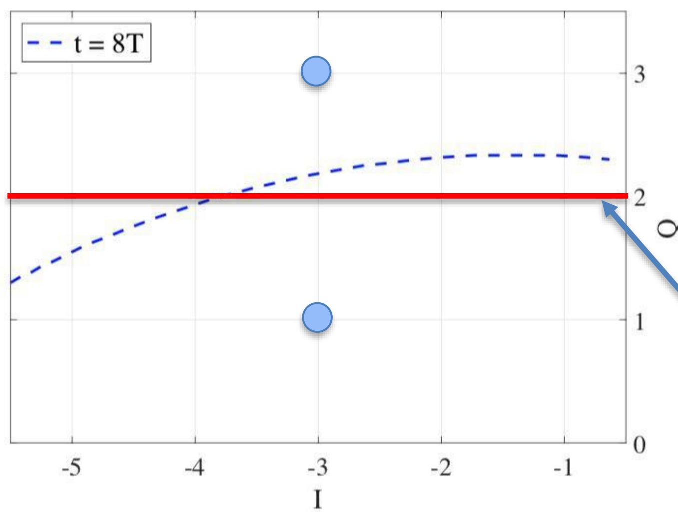
SNR

residual phase offset per symbol duration (T)

Decision rule:

$$S^* = \arg\max_S p(I, Q|S)$$

Transmitted symbols



Default boundary

CFO-aware demodulation boundaries for two points (-3,1) and (-3,3), $\gamma = 7\ dB$.

Theoretical Analysis (Wi-Fi Systems)

Probability density function of phase offset per symbol (under AWGN)

$$f_{\Psi}(\psi) \sim \frac{\sqrt{l\gamma}\cos^2\frac{\psi}{2}}{\sqrt{2\pi\cos\psi}} e^{-2l\gamma\, sin^2(\frac{\psi}{2})}$$

# of preamble samples

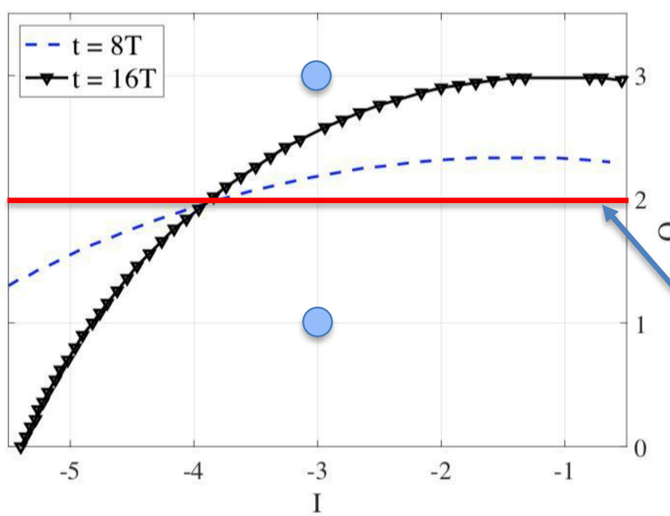
SNR

residual phase offset per symbol duration (T)

Decision rule:

$$S^* = \arg\max_S p(I, Q|S)$$

Transmitted symbols



Default boundary

CFO-aware demodulation boundaries for two points (-3,1) and (-3,3), $\gamma = 7\ dB$.

Theoretical Analysis (Wi-Fi Systems)

Probability density function of phase offset per symbol (under AWGN)

$$f_\Psi(\psi) \sim \frac{\sqrt{l\gamma}\cos^2\frac{\psi}{2}}{\sqrt{2\pi\cos\psi}} e^{-2l\gamma\, sin^2(\frac{\psi}{2})}$$

# of preamble samples

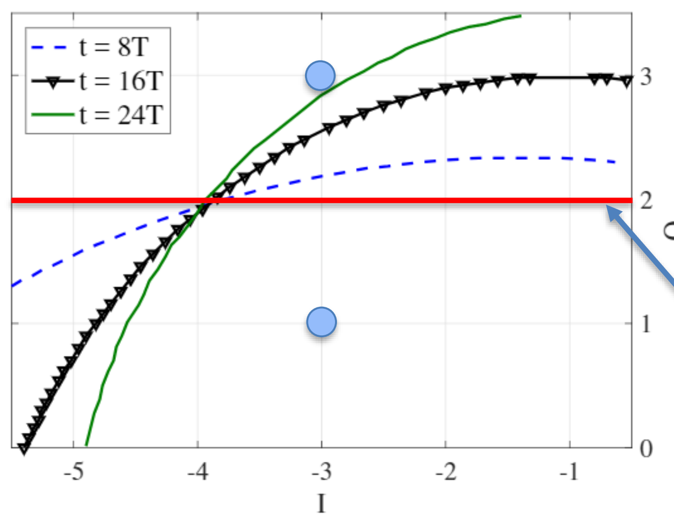
SNR

residual phase offset per symbol duration (T)

Decision rule:

$$S^* = \arg\max_S p(I, Q|S)$$

Transmitted symbols

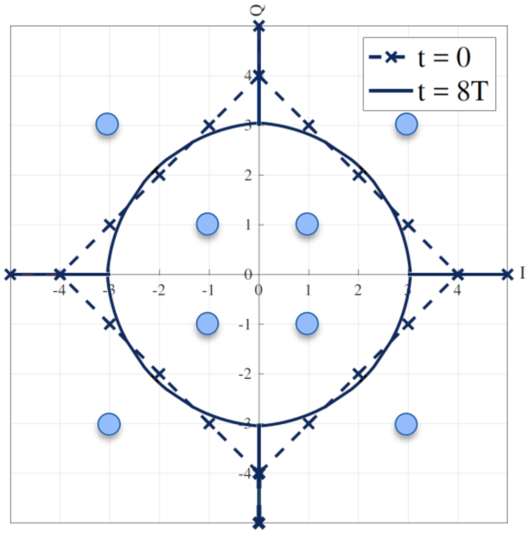


Default boundary

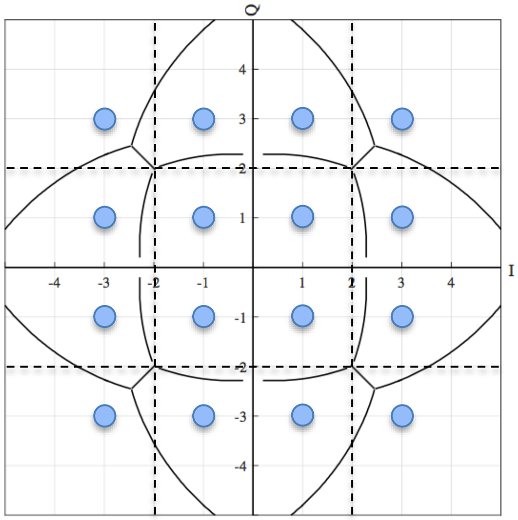
CFO-aware demodulation boundaries for two points (-3,1) and (-3,3), $\gamma = 7\ dB$.

CFO-Aware Demodulation Boundaries

Default boundaries vs. CFO-aware boundaries



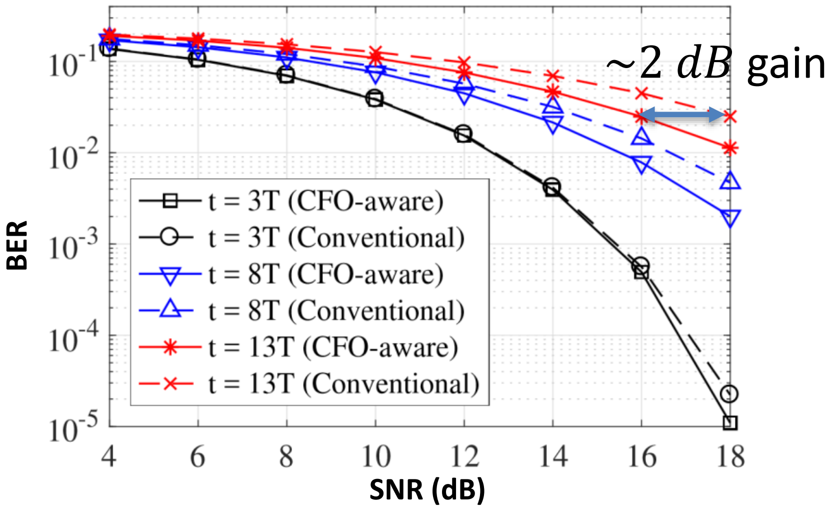
(4×2) 8-APSK



16-QAM

BER Performance gain

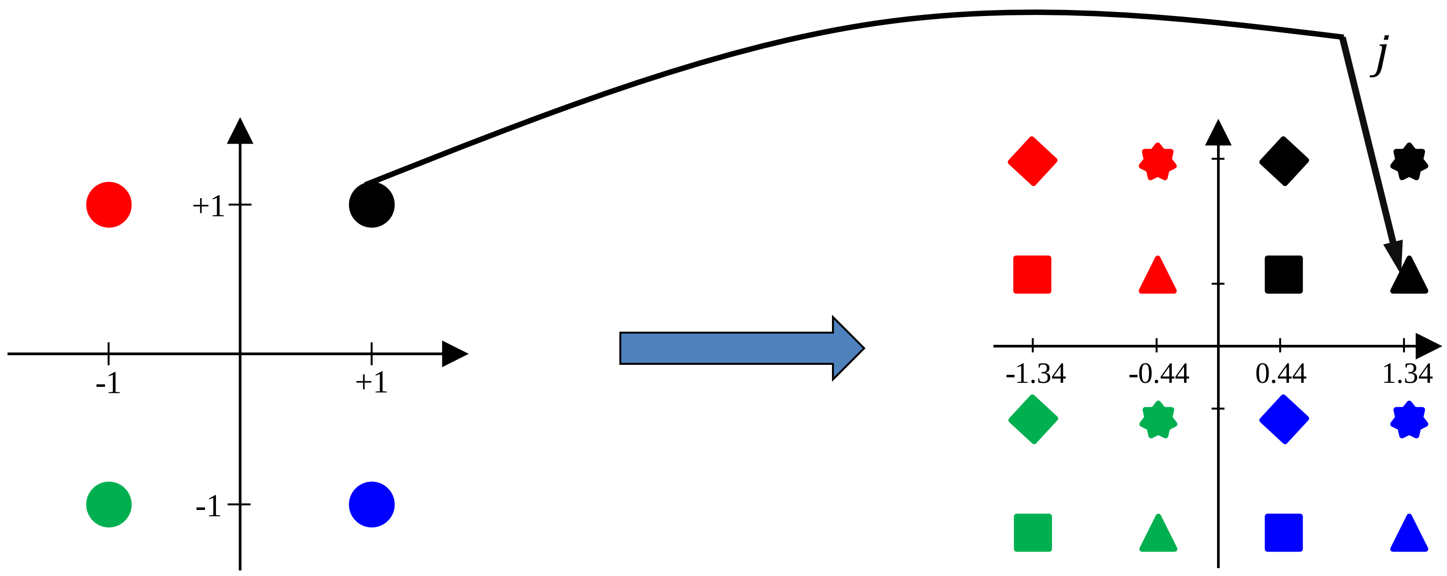
Example: 16-QAM



(Uncoded) Modulation Obfuscation

Map symbols of a mod. scheme to a subset of higher-order symbols

- Selection of an optimal sub-constellation is based on a secret *j*
- Example: QPSK → 16-QAM

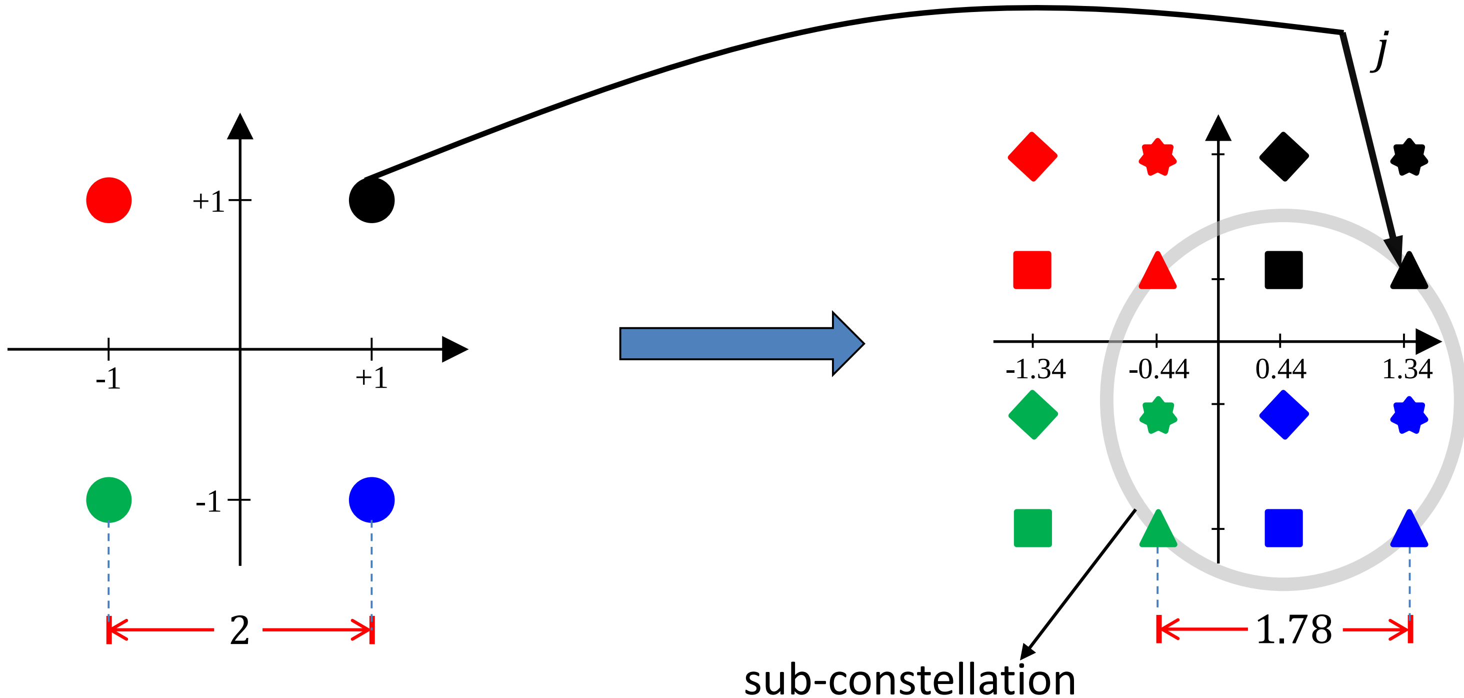


(Uncoded) Modulation Obfuscation

Map symbols of a mod. scheme to a subset of higher-order symbols

Selection of an optimal sub-constellation is based on a secret *j*

Example: QPSK → 16-QAM



BER performance degradation

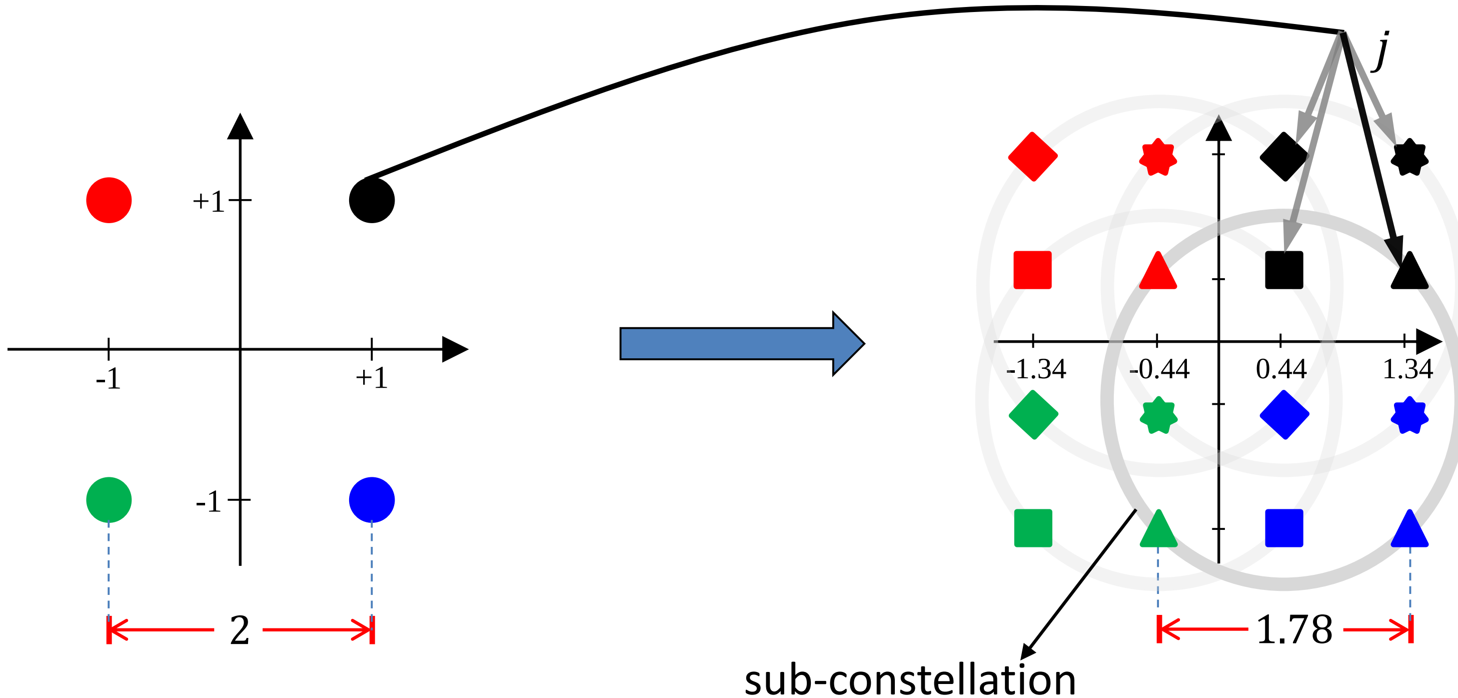
- Higher sensitivity of denser constellation maps to noise
- Higher sensitivity of denser constellation maps to phase offset

(Uncoded) Modulation Obfuscation

Map symbols of a mod. scheme to a subset of higher-order symbols

Selection of an optimal sub-constellation is based on a secret j

Example: QPSK → 16-QAM



BER performance degradation

- Higher sensitivity of denser constellation maps to noise
- Higher sensitivity of denser constellation maps to phase offset

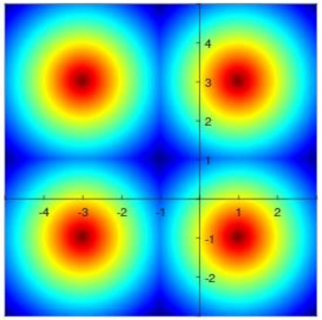
Modulation Obfuscation under Phase Offset

Denser constellation maps increase the vulnerability to phase offset

→ A low-order modulation scheme becomes more sensitive to CFO than usual

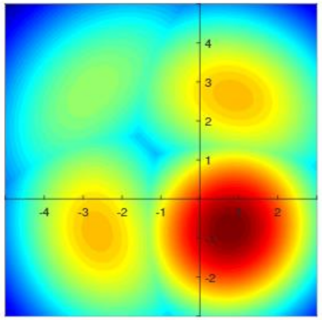
Example:

QPSK → 16-QAM

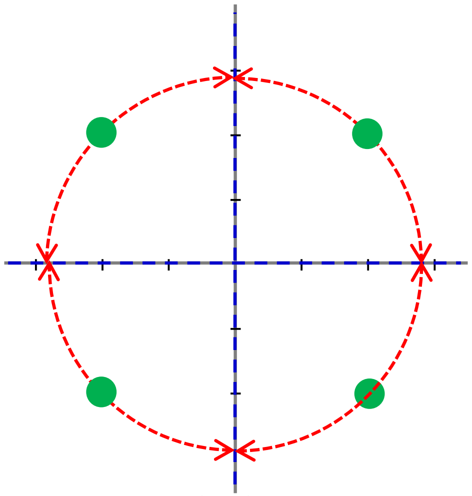


No residual CFO

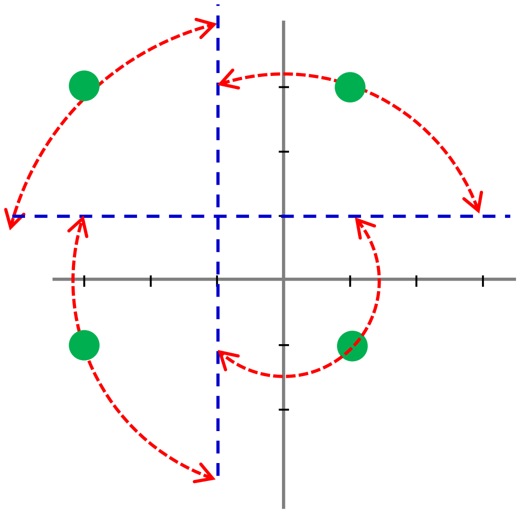
QPSK → 16-QAM



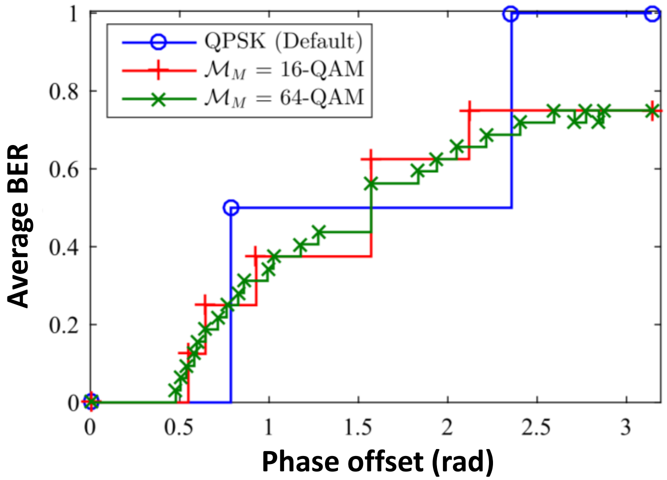
With residual CFO



QPSK



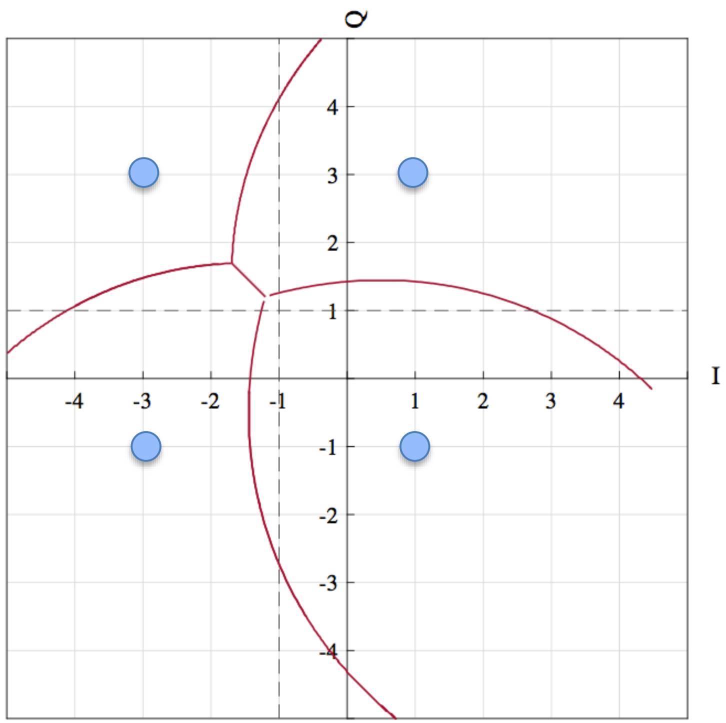
QPSK inside 16-QAM



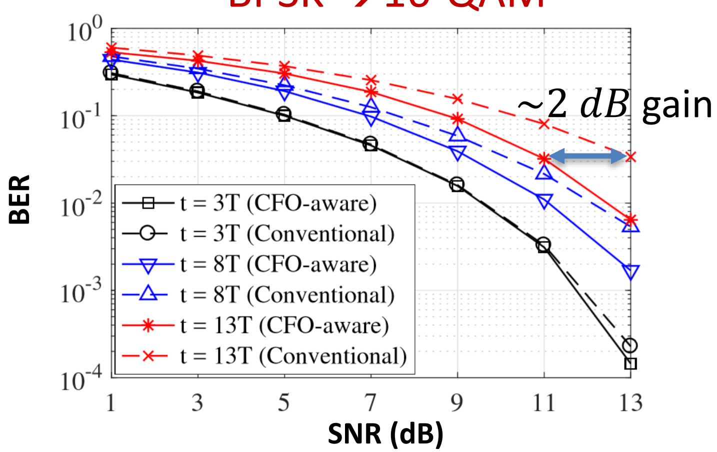
CFO-Aware Demodulation for Uncoded Obfuscation

- Default demodulataion boundaries may not be optimal
  - Example: mapping BPSK/QPSK symbols to (a subset of) 16-QAM symbols

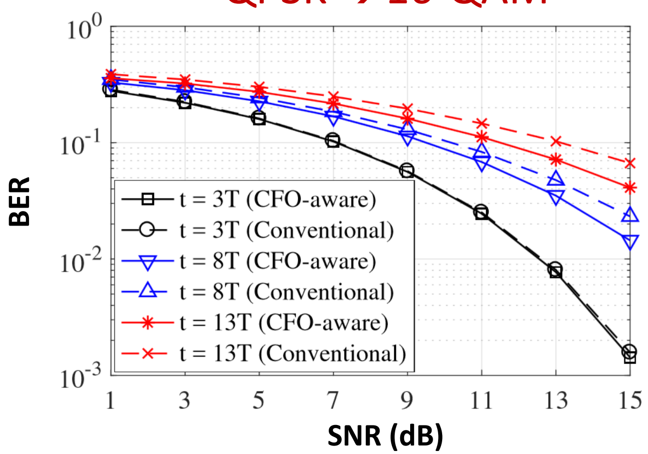
QPSK → 16-QAM



BPSK → 16-QAM



QPSK → 16-QAM



Coded Modulation Obfuscation [TIFS'16]

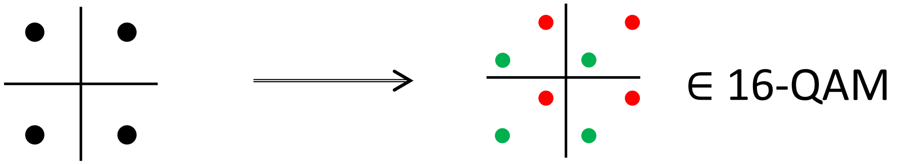
Use lightweight Trellis-Coded Modulation (TCM) to improve BER

Needs (at least) two optimal sub-constellations

Example:

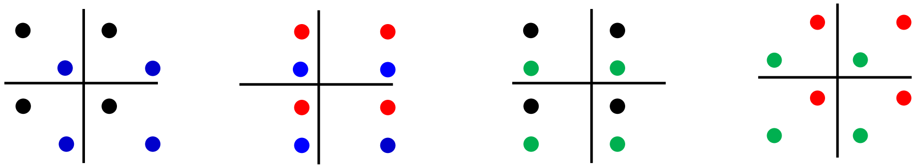
QPSK → 16-QAM using TCM

Needs two sub-constellations (2×4 16-QAM symbols) for the four QPSK symbols



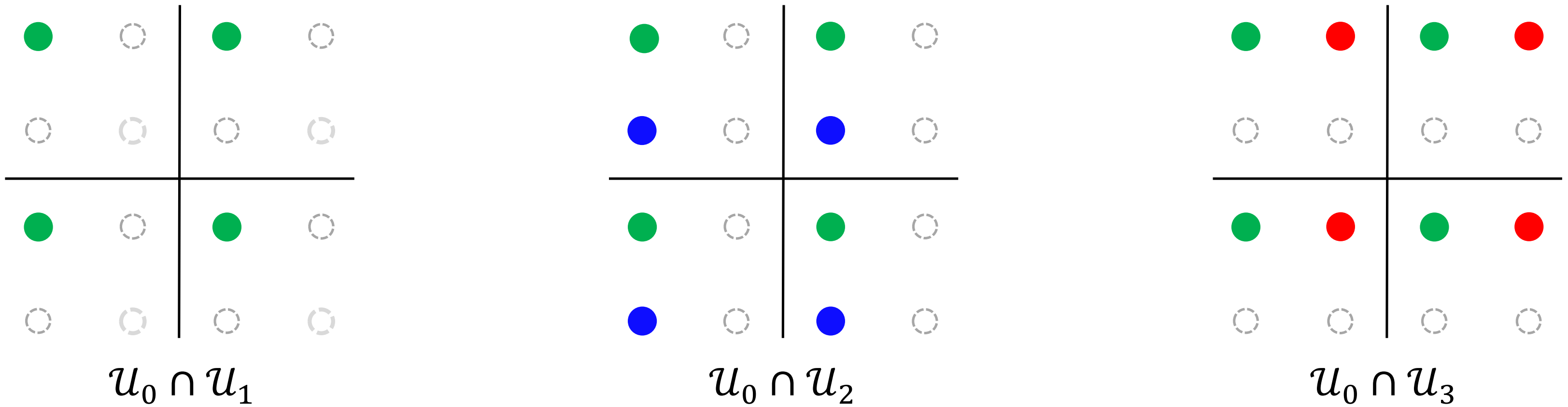
Similarly, two sub-constellation (2×2 16-QAM symbols) for the two BPSK symbols

Covertly vary the sub-constellations based on secret j to cover all possible symbols



Optimizing Coded Obfuscation w/ Phase Offset Consideration

1) Find optimal pairs of sub-constellations with maximum inter-sub-constellation distance



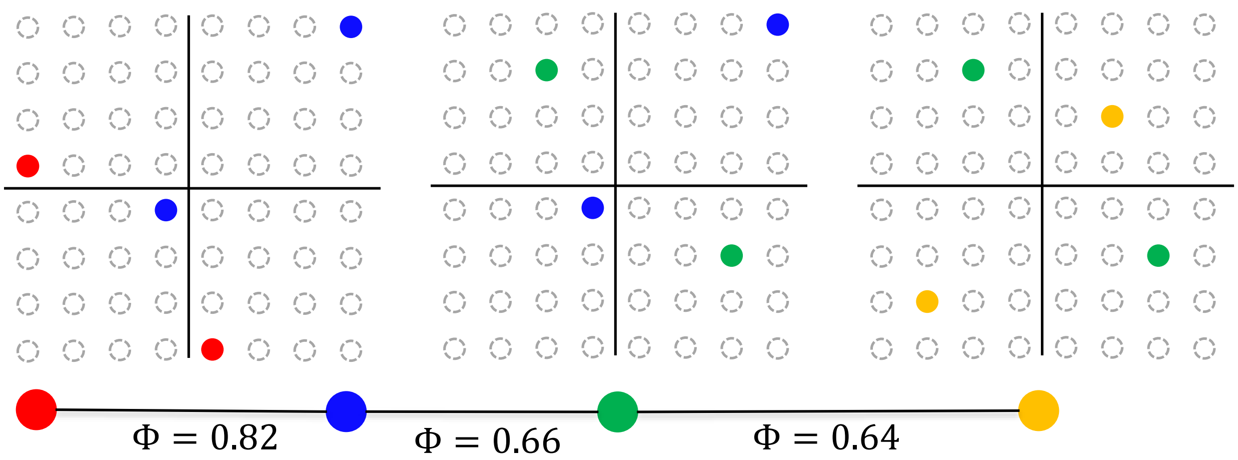
1) What if there are multiple optimal pairs?

Φ: max phase offset

Tie breaker: Φ

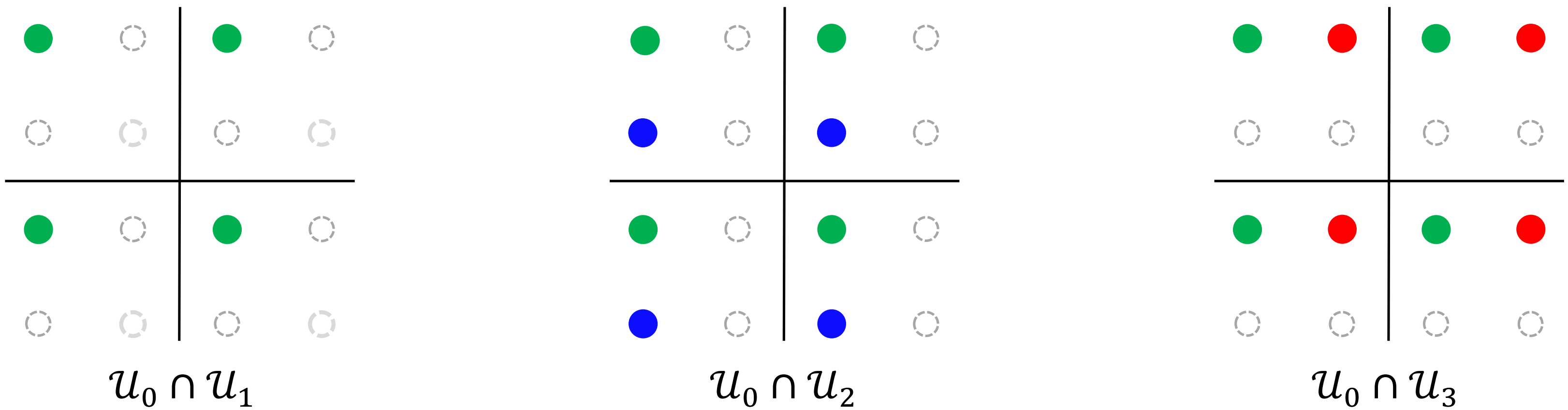
Vertex cover algorithm

Ex: BPSK → 64-QAM



Optimizing Coded Obfuscation w/ Phase Offset Consideration

1) Find optimal pairs of sub-constellations with maximum inter-sub-constellation distance



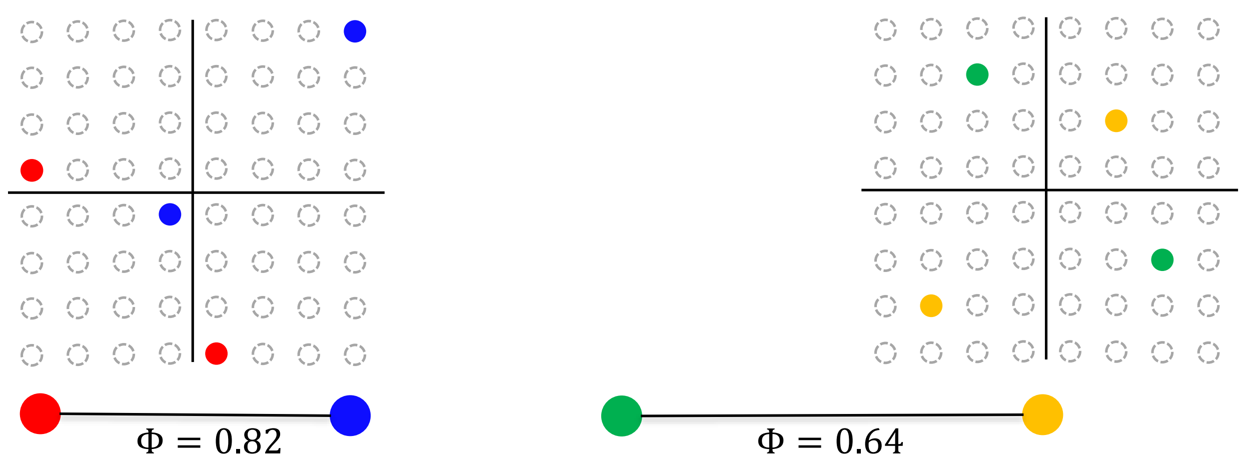
1) What if there are multiple optimal pairs?

Φ: max phase offset

Tie breaker: Φ

Vertex cover algorithm

Ex: BPSK → 64-QAM



Performance (Gain) Improvement

Least-complex TCM is sufficient to maintain the performance under AWGN

1) Mapping to 16-QAM

	Minimum-distance reduction after mapping to 16-QM	Gain (uncoded)	Gain (w/ 2-state TCM)	Enhanced Gain (w/ 2-state TCM)
BPSK	$2 \rightarrow 1.79$	-0.97 dB	-0.46 dB	0.79 dB
QPSK	$1.41 \rightarrow 1.26$	-0.97dB	0 dB	0.79 dB

2) Mapping to 64-QAM

	Minimum-distance reduction after mapping to 64-QM	Gain (uncoded)	Gain (w/ 2-state TCM)	Enhanced Gain (w/ 2-state TCM)
BPSK	$2 \rightarrow 1.75$	-1.18 dB	-1.05 dB	0 dB
QPSK	$1.41 \rightarrow 1.23$	-1.18 dB	-0.92 dB	0.58 dB
16-QAM	$0.63 \rightarrow 0.62$	-0.21 dB	0.76 dB	1.55 dB

Resulting Robustness to Phase Offset

What is the maximum phase offset (in Rad) that does not create error?

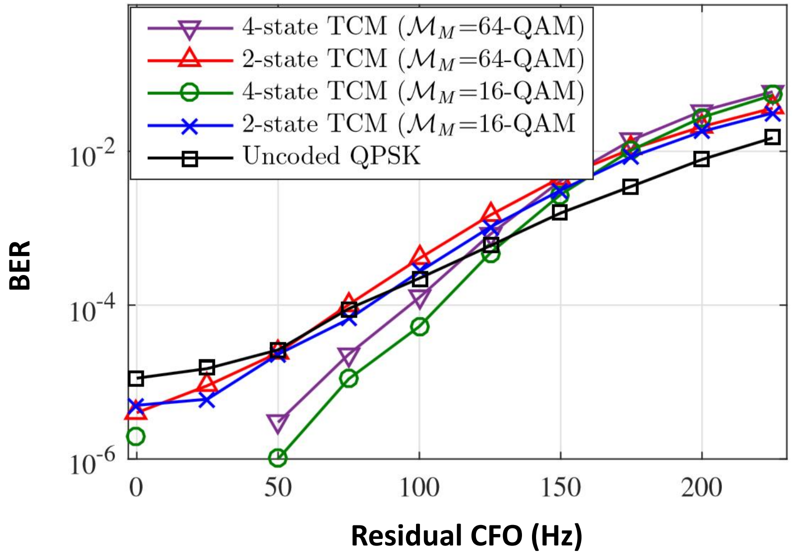
	Default	→ 16-QAM		→ 64-QAM	
		CBM scheme	Proposed	CBM scheme	Proposed
BPSK	$\pi/2 = 1.57$	0.295	0.545	0.135	0.51
QPSK	$\pi/4 = 0.78$	0.295	0.464	0.135	0.381
16-QAM	0.259	N/A	N/A	0.135	0.165

BER performance under phase offset

Example:

QPSK → 16-QAM

QPSK → 64-QAM



Conclusions

Sensitivity of higher-order modulation schemes to phase offset may hinder using (and securing) them in emerging wireless systems

Default demodulation boundaries are inept at high transmission rates (i.e., at dense constellation maps)

Adaptive (CFO-aware) demodulation boundaries can achieve up to $2\ dB$ gain for 16-QAM and 64-QAM modulation schemes

By redesigning the coding scheme for modulation obfuscation w.r.t. phase offset, one can achieve additional $2-3\ dB$ gain

➔ Up to $\mathbf{5\ dB}$ gain for modulation obfuscation over conventional demodulation schemes that are not obfuscated and are oblivious to residual CFO