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**

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
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:

```
BPSK  QPSK  16-QAM  64-QAM
```
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:

![Diagram of QPSK constellation]
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:

QPSK
Challenge: High Sensitivity to Phase Offset

Denser constellation maps are more vulnerable to phase offset

Example: BPSK vs. 16-QAM at the receiver

Transmitted symbol

Received symbol

Δφ

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

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)

\[
f_{\psi}(\psi) \sim \frac{\sqrt{l\gamma \cos^2 \frac{\psi}{2}}}{\sqrt{2\pi \cos \psi}} e^{-2l\gamma \sin^2 \left(\frac{\psi}{2}\right)}
\]

residual phase offset per symbol duration (T)

Decision rule:

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

Transmitted symbols

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)

\[ f_\Psi(\psi) \sim \frac{\sqrt{\gamma \cos^2 \frac{\psi}{2}}}{\sqrt{2\pi \cos \psi}} e^{-2\gamma \sin^2 \left(\frac{\psi}{2}\right)} \]

residual phase offset per symbol duration (T)

Decision rule:

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

CFO-aware demodulation boundaries for two points (-3,1) and (-3,3), \( \gamma = 7 \, \text{dB} \).
Theoretical Analysis (Wi-Fi Systems)

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

\[
f_{\Psi}(\psi) \sim \frac{\sqrt{l\gamma \cos^2 \frac{\psi}{2}}}{\sqrt{2\pi \cos \psi}} e^{-2l\gamma \sin^2 \left(\frac{\psi}{2}\right)}
\]

residual phase offset per symbol duration (T)

SNR

# of preamble samples

Decision rule:

\[
S^* = \operatorname{arg\,max}_S p(I, Q|S)
\]

Transmitted symbols

CFO-aware demodulation boundaries for two points (-3,1) and (-3,3), \(\gamma = 7 \text{ dB}\).
CFO-Aware Demodulation Boundaries

Default boundaries vs. CFO-aware boundaries

Example: 16-QAM

BER Performance gain

~2 dB gain
(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 $\rightarrow$ 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 $\rightarrow$ 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 \( \rightarrow \) 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

With residual CFO

- QPSK inside 16-QAM

Average BER vs. Phase offset (rad)
CFO-Aware Demodulation for Uncoded Obfuscation

Default demodulation boundaries may not be optimal

Example: mapping BPSK/QPSK symbols to (a subset of) 16-QAM symbols

QPSK $\rightarrow$ 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 $\rightarrow$ 16-QAM using TCM

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

Similarly, two sub-constellation ($2 \times 2$ 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

```
Φ: max phase offset
Tie breaker: Φ
Vertex cover algorithm
Ex: BPSK → 64-QAM
```

1) What if there are multiple optimal pairs?

Φ = 0.82  Φ = 0.66  Φ = 0.64
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

<table>
<thead>
<tr>
<th></th>
<th>Minimum-distance reduction after mapping to 16-QM</th>
<th>Gain (uncoded)</th>
<th>Gain (w/ 2-state TCM)</th>
<th>Enhanced Gain (w/ 2-state TCM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPSK</td>
<td>$2 \rightarrow 1.79$</td>
<td>$-0.97,\text{dB}$</td>
<td>$-0.46,\text{dB}$</td>
<td>$0.79,\text{dB}$</td>
</tr>
<tr>
<td>QPSK</td>
<td>$1.41 \rightarrow 1.26$</td>
<td>$-0.97,\text{dB}$</td>
<td>$0,\text{dB}$</td>
<td>$0.79,\text{dB}$</td>
</tr>
</tbody>
</table>

2) Mapping to 64-QAM

<table>
<thead>
<tr>
<th></th>
<th>Minimum-distance reduction after mapping to 64-QM</th>
<th>Gain (uncoded)</th>
<th>Gain (w/ 2-state TCM)</th>
<th>Enhanced Gain (w/ 2-state TCM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BPSK</td>
<td>$2 \rightarrow 1.75$</td>
<td>$-1.18,\text{dB}$</td>
<td>$-1.05,\text{dB}$</td>
<td>$0,\text{dB}$</td>
</tr>
<tr>
<td>QPSK</td>
<td>$1.41 \rightarrow 1.23$</td>
<td>$-1.18,\text{dB}$</td>
<td>$-0.92,\text{dB}$</td>
<td>$0.58,\text{dB}$</td>
</tr>
<tr>
<td>16-QAM</td>
<td>$0.63 \rightarrow 0.62$</td>
<td>$-0.21,\text{dB}$</td>
<td>$0.76,\text{dB}$</td>
<td>$1.55,\text{dB}$</td>
</tr>
<tr>
<td>16-QAM</td>
<td>$0.63 \rightarrow 0.62$</td>
<td>$-0.21,\text{dB}$</td>
<td>$0.76,\text{dB}$</td>
<td>$1.55,\text{dB}$</td>
</tr>
</tbody>
</table>
Resulting Robustness to Phase Offset

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

<table>
<thead>
<tr>
<th></th>
<th>Default</th>
<th>→ 16-QAM</th>
<th></th>
<th>→ 64-QAM</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>CBM scheme</td>
<td>Proposed</td>
<td>CBM scheme</td>
</tr>
<tr>
<td>BPSK</td>
<td>π/2 = 1.57</td>
<td>0.295</td>
<td>0.545</td>
<td>0.135</td>
</tr>
<tr>
<td>QPSK</td>
<td>π/4 = 0.78</td>
<td>0.295</td>
<td>0.464</td>
<td>0.135</td>
</tr>
<tr>
<td>16-QAM</td>
<td>0.259</td>
<td>N/A</td>
<td>N/A</td>
<td>0.135</td>
</tr>
</tbody>
</table>

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 5 $dB$ gain for modulation obfuscation over conventional demodulation schemes that are not obfuscated and are oblivious to residual CFO.