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

Hanif Rahbari
Department of Computing Security
Rochester Institute of Technology, NY
Email: rahbari@mail.rit.edu

Peyman Siyari, Marwan Krunz
Dept. of Electrical & Computer Engr.
University of Arizona, Tucson, AZ
Email: {psiyari, krunz}@email.arizona.edu

Jung-Min (Jerry) Park
Dept. of Electrical & Computer Engr.
Virginia Tech, VA
Email: jungmin@vt.edu

***Abstract*—Carrier frequency offset (CFO) arises from the intrinsic mismatch between the operating frequencies of the transmitter and the receiver, as well as their relative speeds (i.e., Doppler effect). Despite advances in CFO estimation techniques, estimation errors are still present. Residual CFO creates time-varying phase error. Modern wireless systems, including WLANs, 5G cellular systems, and satellite communications, use high-order modulation schemes, which are characterized by dense constellation maps. Accounting for the phase error is critical for the demodulation performance of such schemes. In this paper, we analyze the post-estimation probability distribution of residual CFO and use it to develop a CFO-aware demodulation approach for a set of modulation schemes (e.g., QAM and APSK). For a given distribution of the residual CFO, symbols with larger amplitudes are less densely distributed on the constellation map. We explore one important application of our adaptive demodulation approach in the context of PHY-layer security, and more specifically modulation obfuscation (MO) mechanisms. In such mechanisms, the transmitter attempts to hide the modulation order of a frame's payload from eavesdroppers, which could otherwise exploit such information to breach user privacy or launch selective attacks. We go further and complement our CFO-aware demodulation scheme by optimizing the design of a low-complexity MO technique with respect to phase errors. Our results show that when combined, our CFO-aware demodulation and optimized MO techniques achieve up to 5 dB gain over conventional demodulation schemes that are not obfuscated and are oblivious to residual CFO.**

***Index Terms*—Frequency offset, demodulation, PHY-layer security, modulation obfuscation, WLAN.**

I. Introduction

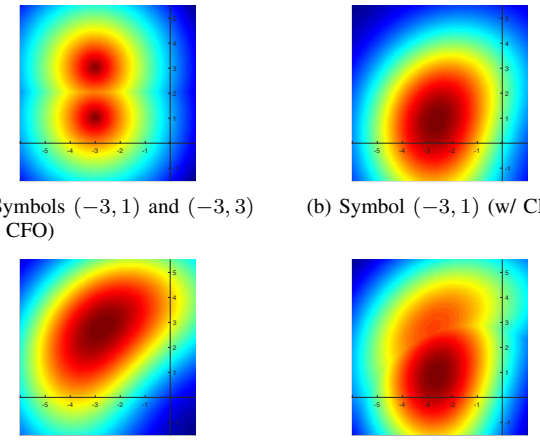
Emerging wireless systems increasingly rely on high-order modulation schemes to increase spectral efficiency. The first anticipated 5G New Radio (NR) as well as the IEEE 802.11ax amendment draft are expected to support quadrature-amplitude modulation (QAM) of orders as high as 1024-QAM [1]–[3]. It is also predicted that mmWave systems will employ 64-QAM schemes [4]. Similarly, DVB-S2X standard for satellite television predominantly uses asymmetric phase-shift keying (APSK) with orders up to 256 [5]. The constellation maps of such modulation schemes are dense, resulting in high sensitivity to phase errors. A phase error (offset) is usually caused by imperfect channel estimation or uncompensated carrier frequency offset (CFO). CFO results from the inherent mismatch between the operating frequencies of the transmit and receive oscillators. It may also be attributed to mobility and Doppler effect. When the phase offset is due to CFO, it increases linearly during a frame transmission. Phase-offset-induced demodulation errors degrade the bit-error-rate (BER) performance of the system and may propagate over multiple symbols if the symbols are correlated via coded-modulation schemes, e.g., trellis-coded modulation (TCM) [6]. Various CFO estimation methods (e.g., [7]–[9]) have been proposed over the past decades to mitigate the demodulation errors of high-order modulation schemes.

In principle, CFO estimation can *never* be perfect. Even a small post-estimation (residual) CFO can translate into a large phase offset during frame reception. This, in turn, unnecessarily prevents the transmitter (Tx) from using high-order modulation schemes. For example, residual CFO has been shown to be detrimental to some of the functionalities of 802.11ax (WiFi) systems, including high-efficiency uplink multiuser multiple-input multiple-output (UL MU-MIMO) [10]. Future 5G systems are also required to support high data rates in very high-speed vehicular environments (up to 500 km/h [11]). The resulting Doppler shift at the received signal can create CFO of up to 2 kHz at 4.2 GHz band (equivalent to 13% of the subcarrier spacing), which needs to be accurately estimated to maintain the target throughput. High-order modulation is also used in modulation obfuscation (MO) techniques (e.g., [9], [12]) to hide the transmission rate by randomly (and secretly) mapping the modulated symbols into an expanded constellation map. Otherwise, the leakage of the modulation order to an eavesdropper opens the door for traffic analysis and packet classification, subsequently enabling various types of privacy breaches and selective jamming attacks [13]–[15].

Although most wireless devices employ mechanisms to estimate CFO at the start or in the middle of a frame transmission (e.g., pilot subcarriers in IEEE 802.11a/ac/n systems), a typical demodulator overlooks the possibility of imperfect CFO estimation and does not adjust its demodulation regions over time. In fact, residual CFO has disproportional impacts on the spatial distribution of symbols (on the constellation map) if such symbols exhibit unequal amplitudes. The resulting asymmetry in the spatial distribution at the receiver (Rx) has not been previously accounted for in the demodulation process.

To illustrate, consider Fig. 1 which shows an example of the spatial distribution at the Rx for two transmitted 16-QAM values of unequal amplitudes under Gaussian noise. In

978-1-5386-4128-6/18/$31.00 ©2018 IEEE



(a) Symbols $(-3,1)$ and $(-3,3)$ (w/o CFO)

(b) Symbol $(-3,1)$ (w/ CFO)

(c) Symbol $(-3,3)$ (w/ CFO)

(d) Symbols $(-3,1)$ and $(-3,3)$ (w/ CFO)

Fig. 1. Heatmap of the spatial probability distribution of received symbols of two transmitted 16-QAM values simulated under white Gaussian noise. Warm colors (e.g., red) denote higher probability density while cold colors (e.g., blue) represent lower probability.

Fig. 1(a) the CFO estimation is assumed to be perfect and so the spatial distribution of received symbols is symmetric with respect to the nominal constellation points. Hence, a horizontal line at equal distance from the two nominal constellation points optimally splits the constellation map according to the maximum-likelihood (ML) criterion. However, with residual (uncompensated) CFO, the distribution of received symbols is no longer symmetric, as can be seen in parts (b) and (c) of the figure. Additionally, the amplitude of a transmitted symbol impacts the distribution of the received symbols. For example, received symbols that were transmitted as $(-3,3)$ are distributed over a wider region, compared to the lower-amplitude symbol $(-3,1)$. Hence, a horizontal line is no longer an optimal ML-based boundary for the demodulation regions (see Fig. 1(d)). Such contrast is accentuated as the difference in the amplitudes of the constellation points increases.

In this paper, we consider the impact of residual CFO on the decoding performance of QAM and APSK schemes, and propose an *adaptive* demodulation approach for such schemes. The proposed approach complements existing CFO estimation techniques by probabilistically accounting for the residual CFO that those techniques fail to remove.

The main idea behind our approach is to continuously adapt the demodulation regions during frame reception based on the probability distribution of the CFO-induced phase offset. While our main motivation is to achieve reliable demodulation for any modulation scheme whose constellation points exhibit different amplitudes (as in WiFi and satellite communications systems), our approach can also benefit MO techniques in PHY-layer security. As a use case, we consider asymmetric constellation maps used in [12] for a TCM-aided MO, and we improve the robustness of this MO technique to phase offset. The contributions of this paper can be summarized as follows:

- We analytically derive the probability distribution of received symbols under AWGN when CFO estimation is imperfect. Because no closed-form expression exists for the probability distribution, we consider one QAM and one APSK scheme as illustrative examples and numerically approximate their optimal CFO-aware demodulation boundaries.
- We study the BER performance when the Rx employs CFO-aware demodulation regions for 16-QAM, 64-QAM, regular (4×2) 8-APSK, and modulation obfuscation; and we show that the proposed scheme can achieve up to 2 dB gain.
- We enhance the MO schemes in [12] without increasing their complexity and show that a simple TCM is sufficient to account for any BER performance loss due to MO.
- We optimize the Ungerboeck TCM codes [16] (also used in [12]) w.r.t. robustness against phase errors by solving a graph vertex cover problem; we also propose a normalized distance metric to be used in the Viterbi decoder of TCM under our adaptive demodulation scheme.

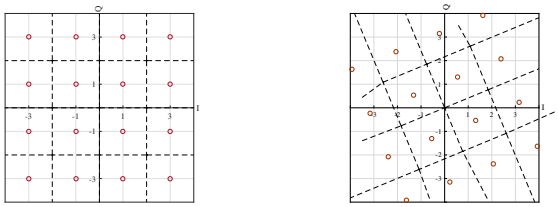
II. Preliminaries – CFO Estimation Errors

To better understand the impact of residual CFO on the demodulation process, we first explain how CFO is typically estimated at the Rx. Without loss of generality, we assume that the PHY header is part of the frame payload and that the Tx employs QAM or APSK as its modulation scheme to transmit the payload. Every payload is prepended by a preamble. The preamble structure can be different for different systems (or even from one IEEE 802.11 standard to another). For the analysis in this paper, we consider the preamble structure of OFDM-based 802.11 systems, which contains a periodic signal of period T seconds. This signal is comprised of two or more identical cycles of some standardized waveform, and is used by the Rx to estimate the channel and CFO, and perform other functions. The identical parts (cycles) remain so even under a multipath channel of certain coherence times (larger than $8\,\mu$s in OFDM-based 802.11 systems).

Let Δ_f denote the true CFO between the Tx and the Rx. CFO creates a time-varying phase offset $\varphi(t) \triangleq 2\pi t\,\Delta_f$, where t is the time since the start of the transmission. To estimate Δ_f, Rx considers two successive cycles of the preamble, estimates the phase difference between pairs of identical samples in these cycles, and compensates for the estimated CFO when decoding the rest of the frame. We explain Moose's ML estimator of the phase offset, which is used in OFDM-based 802.11 systems [7]. Let S_t^p and n_t be the transmitted preamble sample and the AWGN, respectively, at time t. We assume that n_t is random with a circularly symmetric complex normal distribution of zero mean and variance σ_n^2. To estimate $\varphi(T) = 2\pi T\,\Delta_f$, the Rx first multiplies the complex conjugate of a received preamble sample, say $S_t^p + n_t$, by the preamble sample that is received T seconds later ($S_{t+T}^p + n_{t+T} = S_t^p\, e^{j\varphi(T)} + n_{t+T}$):

$$\begin{aligned} d_t &\triangleq \left(S_t^p + n_t\right)^* \left(S_{t+T}^p + n_{t+T}\right) \\ &= |S_t^p|^2 e^{j2\pi T\Delta_f} + S_t^{p*} n_{t+T} + S_{t+T}^p n_t^* + n_t^* n_{t+T} \end{aligned} \tag{1}$$

where $|x|$ and x^* are the amplitude and conjugate of a complex number x, respectively. To estimate the CFO, the Rx then



(a) Default constellation ($\varphi(t) = 0$) (b) Rotated constellation ($\varphi(t) = \frac{\pi}{8}$)

Fig. 2. Optimal ML demodulation regions for 16-QAM under AWGN.

measures the phase of d_t and divides it by $2\pi T$. Because the duration of the preamble is less than the coherence time, the channel coefficient does not impact CFO estimation and so is not shown in (1). If the noise is nonnegligible, the phase of d_t will not be $2\pi T\Delta_f$. To improve the accuracy, the Rx takes l different sample pairs from the preamble and averages out the noise. More specifically, the estimated phase offset over l sample pairs, denoted by $\widetilde{\varphi_l(T)}$, is computed as follows:

$$\widetilde{\varphi_l(T)} \triangleq \measuredangle\Big(\sum_{i=0}^{l-1} d_{Ti/l}\Big) \tag{2}$$

where $\measuredangle(x)$ represents the phase of a complex number x, and

$$\begin{aligned}\sum_{i=0}^{l-1} d_{Ti/l} =& e^{j2\pi T\Delta_f} \sum_{i=0}^{l-1} |S^p_{Ti/l}|^2 \\ &+ \sum_{i=0}^{l-1} \Big(S^{p*}_{Ti/l} n_{t+T} + n_t^* S^p_{Ti/l+T} + n^*_{Ti/l} n_{Ti/l+T}\Big)\end{aligned} \tag{3}$$

Although the above summation improves the accuracy, noise often prevents perfect phase estimation. A residual CFO $\delta_f \triangleq \Delta_f - \widetilde{\varphi(T)}/2\pi T$ remains. (For the ease of explanation, we assume that l is constant and drop the subscript l from $\widetilde{\varphi_l(T)}$ in the rest of paper, unless indicated otherwise.)

If δ_f is known, the Rx can design an optimal demodulator. In the case of AWGN and equiprobable transmitted symbols, the optimal demodulation regions (boundaries) are specified by the Voronoi diagram whose cells (regions) are centered at the nominal constellation points. These boundaries can be alternatively drawn by rotating the default demodulation regions of the underlying modulation scheme by $2\pi\delta_f t$ radian(s) (see Fig. 2). The default regions are defined as the Voronoi cells computed when $\varphi(t) = 0$. However, the Rx in typical wireless systems uses only the most probable value of $\varphi(T)$, which is computed using the ML phase offset estimator [7], [8]. When this estimation is erroneous and $\delta_f \neq 0$, the Rx demodulates the symbols based on non-optimal regions. As we discuss below, the resulting BER in this case can be significant. One of the key points in this paper is to go beyond relying on the most likely value of $\varphi(T)$ (equivalently, the default regions) and improve the overall BER by accounting for other possible values of $\varphi(T)$ during demodulation.

III. CFO-Aware Adaptive Demodulation

Let $\psi \triangleq 2\pi T\delta_f$ and let S_t denote the noise-free received symbol t seconds after the end of the preamble transmission. The impact of residual CFO δ_f on the received payload symbol $S_t + n_t$ is reflected by multiplying it by $e^{j2\pi\delta_f t} = e^{j\frac{\psi}{T}t}$. Therefore, to study the distribution of received symbols after CFO estimation and correction, we first rewrite the received signal with residual CFO, as follows:

$$(S_t + n_t)e^{j\frac{\psi}{T}t} = S_t e^{j\frac{\psi}{T}t} + n_t e^{j\frac{\psi}{T}t}. \tag{4}$$

Note that $|n_t e^{j\frac{\psi}{T}t}| = |n_t|$. However, $\measuredangle(n_t e^{j\frac{\psi}{T}t})$ is the modulo-2π addition of $\measuredangle(n_t)$ and $\frac{\psi}{T}t$. While receiving S_t, n_t is independent of the noise that was added during the transmission of the preamble and that resulted in residual CFO δ_f. Thus, n_t and $\frac{\psi}{T}t$ are independent random variables. The probability density function (pdf) of the sum of two independent periodic random variables with period 2π is the modulo-2π circular convolution of their individual distributions. Hence, the pdf of the phase of $n_t e^{j\frac{\psi}{T}t}$ is the circular convolution of the pdf of $\measuredangle(n_t)$ and the pdf of the phase offset. The phase of the circularly symmetric white Gaussian n_t is drawn from uniform distribution.

Let $f_N(\theta)$ and $f_\Phi(\theta)$ represent the pdfs of $\measuredangle(n_t)$ and $\frac{\psi}{T}t$, respectively, where $\theta \in [0, 2\pi)$. The phase $\measuredangle(n_t e^{j\frac{\psi}{T}t})$ would take the same value for the unwrapped phases θ and $\theta \pm 2\pi$. So the circular convolution of $f_N(\theta)$ and $f_\Phi(\theta)$, denoted by $(f_N \star f_\Phi)(\theta)$, can be analytically expressed as [17]:

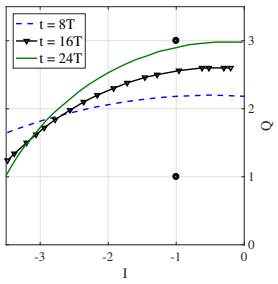
$$\begin{aligned}(f_N \star f_\Phi)(\theta) &= \int_{-\infty}^{\infty} f_N(\tau)\big[f_\Phi(\theta-\tau-2\pi) + f_\Phi(\theta-\tau) \\ &\qquad + f_\Phi(\theta-\tau+2\pi)\big]d\tau \\ &= \frac{1}{2\pi}\int_0^{2\pi} \big[f_\Phi(\theta-\tau-2\pi) + f_\Phi(\theta-\tau) \\ &\qquad + f_\Phi(\theta-\tau+2\pi)\big]d\tau = \frac{1}{2\pi} = f_N(\theta).\end{aligned} \tag{5}$$

In other words, the residual CFO does not change the pdf of $\measuredangle(n_t)$, i.e., n_t remains as white Gaussian noise. However, the phase error causes S_t to rotate on the constellation map. To calculate the pdf of the received symbol S_t given that S is the transmitted version of this symbol, we need the pdf of the phase offset $\frac{\psi}{T}t$, which depends on the pdf of ψ.

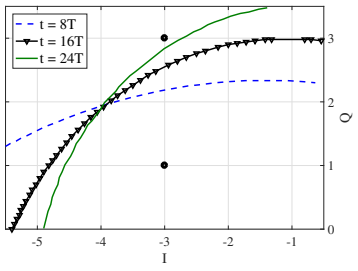
To derive the pdf of ψ, we use the distribution of the phase error provided in [18, eq. 5-119] for the case of two transmitted signals with the same amplitude but possibly different phases under uncorrelated AWGN. Accordingly, the pdf of the phase estimation error ψ when the Rx estimates the phase based on only a single pair of samples (see (1)) is

$$\begin{aligned}f_\Psi(\psi) = \frac{1}{2\pi}\int_0^{\pi/2} &\sin(\tau)\big[1+\gamma(1+\cos(\psi)\sin(\tau))\big] \\ &\times e^{-\gamma\left(1-\cos(\psi)\sin(\tau)\right)}d\tau\end{aligned} \tag{6}$$

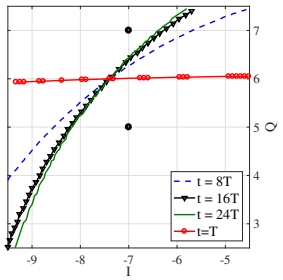
where $\gamma \triangleq \mathbb{E}[|S^p_t|^2]/\sigma_n^2$ is the SNR and $\mathbb{E}[|S^p_t|^2]$ is the average transmission power for the preamble. However, Moose's ML-based CFO estimation method for OFDM systems [7] uses l such preamble pairs and computes (2), whose distribution, to the best of our knowledge, has not previously been derived. Moreover, the expression in (3) cannot be easily converted



(a) $(x_{S_1}, y_{S_1}) = (-1, 1)$ and $(x_{S_2}, y_{S_2}) = (-1, 3)$ (16-QAM symbols).



(b) $(x_{S_1}, y_{S_1}) = (-3, 1)$ and $(x_{S_2}, y_{S_2}) = (-3, 3)$ (16-QAM symbols).



(c) $(x_{S_1}, y_{S_1}) = (-7, 5)$ and $(x_{S_2}, y_{S_2}) = (-7, 7)$ (64-QAM symbols).

Fig. 3. Optimal CFO-aware boundaries between two adjacent QAM symbols under imperfect CFO estimation ($\gamma = 7$ dB and $l = 64$).

to (1) by substituting $\sum_{i=0}^{l-1} S^p_{Ti/l}$ for S^p_t and adjusting the noise power (SNR), because the equivalent distribution of the sum-product of the noise terms in (3) is not known[1], although $S^p_{Ti/l}$'s and the pdf of n_t are known.

To address this issue and derive the pdf of ψ under (2), we adjust the SNR in (6) based on the variance of δ_f under Moose's method. For simplicity, assume that $\mathbb{E}[|S_t|^2]/\sigma_n^2 = \gamma$, i.e., preamble and payload symbols are transmitted at the same power. Schimdl and Cox derived the variance of $\widetilde{\varphi(T)}$ in [8] under Moose's method, which is given by $\sigma^2_\Psi = \frac{1}{\pi^2 l\gamma}$. Given that ψ has zero mean (see (6)), we have $\int f_\Psi(\psi)\psi^2 \partial\psi = \sigma^2_\Psi$. Hence, the equivalent SNR when l pairs are used is given by $l\gamma$, i.e., using l pairs of identical samples boosts the SNR by l. In OFDM-based 802.11 systems, l is usually 64 and T is the same as the symbol duration. Such an SNR boost is enough to ensure that the system operates in the high SNR regime. This allows us to use the following approximation for (6) [20]:

$$f_\Psi(\psi) \sim \frac{\sqrt{l\gamma}\cos^2\frac{\psi}{2}}{\sqrt{2\pi\cos\psi}} e^{-2l\gamma\sin^2(\psi/2)}, 0 \le |\psi| < \pi/2. \quad (7)$$

Note that ψ is defined based on T and f_Ψ is an even function which remains stationary after transmitting the preamble and compensating for the estimated CFO. So on average, after each symbol, the phase offset during the payload increases by $\mathbb{E}(|\psi|)$, the expected value of the phase offset after one OFDM symbol duration. As an example, when $\gamma = 20$ dB, the SNR at which 16-QAM achieves BER $=10^{-6}$, one can show using numerical methods that $\mathbb{E}(|\psi|) \approx \pi/462$ [2].

Next, we derive the pdf of the received symbol under AWGN channel, given that the Tx transmits symbol S. Suppose that S is located at (x_S, y_S) in the constellation map and that the phase offset ψ satisfies $0 \le |\psi| < \pi/2$. With this phase offset and with $n_t = 0$, the symbol rotates on the constellation map and moves to the point X^ψ_S. Hence, we denote the rotated version of S (i.e., $Se^{j2\pi\frac{\psi}{T}t}$) by $X^\psi_S \triangleq \{x_S\cos(\psi) - y_S\sin(\psi), x_S\sin(\psi) + y_S\cos(\psi)\}$. The probability of receiving a symbol at location (x, y) at time $t = T$ under AWGN given that S was transmitted is:

$$p(x, y|S) = \int_\Psi p(x, y|S, \psi) f_\Psi(\psi) d\psi \approx \quad (8)$$

$$\int_{-\pi/2}^{\pi/2} \frac{\sqrt{l\gamma^3}\cos^2(\psi/2)}{P_{avg}(2\pi)^{3/2}\sqrt{\cos(\psi)}} \times e^{-2l\gamma\sin^2(\psi/2) - \frac{||X - X^\psi_S||^2}{2\frac{\sqrt{P_{avg}}}{\gamma}}} \partial\psi$$

where P_{avg} is used to normalize the power of the underlying modulation scheme. For example, with equiprobable transmitted symbols, $P_{avg} = 10$ and 42 for 16-QAM and 64-QAM, respectively. When $t \neq T$, ψ in (8) is replaced by $\frac{\psi}{T}t$.

A. Demodulation Regions under Imperfect CFO Estimation

Using an ML-based demodulator, the Rx maps the received symbol to:

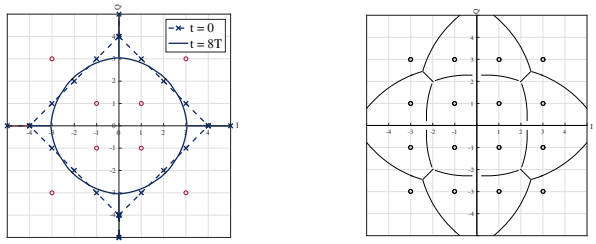
$$S^* = \arg\max_S p(x, y|S). \quad (9)$$

However, because the integral in (8) does not have a closed-form solution, it is difficult to solve (9) and precisely identify the *CFO-aware boundaries*, except when the transmitted symbols have the same amplitude, as in the case of QPSK. The CFO-aware boundaries in this case are the same as when $\delta_f = 0$. In general, the CFO-aware boundary between any two adjacent reference constellation points $S^{(1)}$ and $S^{(2)}$ of equal amplitude is the same as when $\delta_f = 0$ because $p(x, y|S^{(1)})$ and $p(x, y|S^{(2)})$ continue to be symmetric functions w.r.t. the perpendicular bisector of the line segment determined by the two points. However, when $|S^{(1)}| \neq |S^{(2)}|$, it is not possible to reliably predict the shape of such boundaries, and we need to numerically compute (8). Similar to the case when $\delta_f = 0$, we assume that the optimal CFO-aware boundary is located at the curve where $p(x, y|S^{(1)}) = p(x, y|S^{(2)})$.

Fig. 3 depicts an example of the CFO-aware demodulation boundary for three different pairs of symbols from the second quadrant of the QAM constellation map. Note that for a given δ_f, the phase offset $\frac{\psi}{T}t$, and hence $p(x, y|S)$, varies with time. Thus, in each figure, we plot the boundaries at different time instances. Observe that the boundary can differ significantly over time. At the beginning of the payload (e.g., $t = T$), the boundary is almost identical to the default case. However, as more symbols are received, in the absence of any robust CFO tracking mechanism, the boundary starts to look like a part

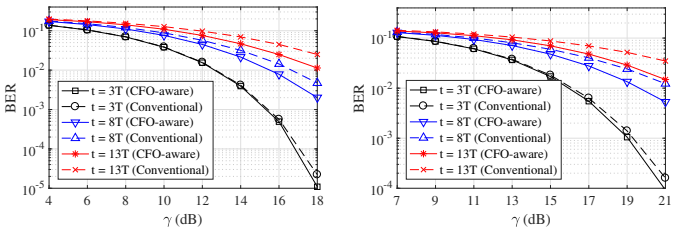
[1]There are approximations for the product of Gaussian random variables (e.g., [19]). However, these approximations often suggest zero variance when the mean values of the respective random variables are zero.

[2]For 16-QAM, once the phase offset exceeds 0.295, the Rx will experience nonzero BER even in the absence of noise [12]. So with $\gamma = 20$ dB, the Rx will experience nonzero BER as early as the 44th symbol.



(a) (4×2) 8-APSK ($t = 0$ and $8T$) (b) 16-QAM ($t = 8T$)

Fig. 4. Optimal demodulation regions for regular (4×2) 8-APSK and 16-QAM ($\gamma = 5$ dB).



(a) 16-QAM (b) 64-QAM

Fig. 5. BER performance vs. received SNR (γ).

of an ellipse where the outer side of the boundary (w.r.t. the origin) leans toward the lower-amplitude symbol and the inner side toward the other symbol. The accumulation of phase offset over time increases the likelihood of the higher-amplitude symbol to be received at the left side of the other symbol. At the same time, the lower-amplitude symbol pushes the boundary up towards its right side. By exploiting the symmetry in the constellation map, one can obtain the boundaries in other quadrants. Snapshots of the CFO-aware boundaries for regular (4×2) 8-APSK and 16-QAM modulations are shown in Fig. 4.

B. Performance Gain Using CFO-Aware Demodulation

In this section, we study the performance gain of our CFO-aware demodulation technique when is employed under 16-QAM and 64-QAM modulation schemes. The results for (4×2) 8-APSK show negligible gain due to its regular structure, and hence we do not show them here. However, as discussed below, the gain is nonnegligible in the case for QAM.

Fig. 5(a) shows the BER improvement versus SNR under conventional and CFO-aware demodulation boundaries. When the frame duration is short (or a short time has passed after the preamble and preamble-based CFO correction), the amount of improvement is not substantial. Such observation is inline with the intuition that when the amount of phase offset is small at the beginning of the payload transmission, the conventional demodulation boundaries have almost the same performance as the CFO-aware boundaries. However, as the frame duration increases, the reduction in BER achieved by using CFO-aware boundaries becomes more significant. In particular, our adaptive demodulation technique achieves 2 dB performance gain at time $t = 13\,T$ and $\gamma \geq 16$. Imperfect CFO estimation rotates the received symbols irrespective of the SNR value. Hence, even when noise is not high, the symbol rotation can jeopardize the correct decision at the Rx. Such a phenomenon was already seen in Fig. 1. Specifically, the contour (heatmap) of the received symbols in the presence of CFO estimation error expands more than when CFO estimation is perfect. Such expansion becomes more significant as SNR increases.

The same trend can be seen under 64-QAM but with a higher gain. Specifically, in Fig. 5(b) it can be seen that our adaptive demodulation technique achieves 3 dB performance gain at time $t = 13T$ and $\gamma \geq 18$.

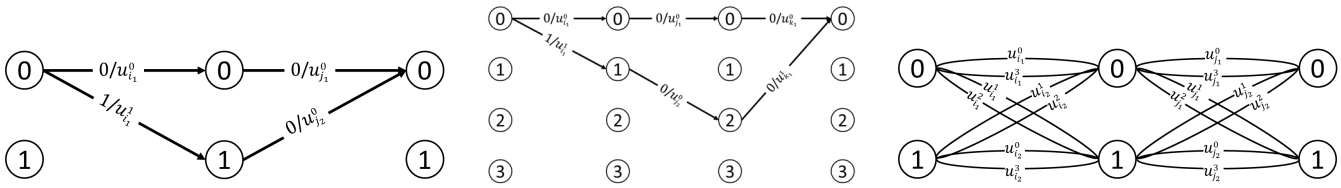
IV. CFO-aware Adaptive Demodulation for MO

In this section, we explore an important application of our CFO-aware adaptive demodulation in the context of modulation obfuscation (MO). MO is a PHY-layer security technique that aims at hiding the payload's modulation scheme (and hence, its transmission rate). In typical multi-rate wireless systems, the transmission rate of the frame payload is adjusted according to channel conditions and contention. Rate adjustment is done by varying the modulation scheme (or its order). By detecting the modulation scheme for one or more packets, a curious eavesdropper can perform traffic classification to breach user privacy or launch selective attacks [13]–[15]. MO techniques remedy such vulnerability by obfuscating the payload's true modulation scheme. This is done by secretly mapping the transmitted symbols under each supported modulation scheme to the constellation map associated with the highest-order modulation scheme available. For example, BPSK, QPSK, 16-QAM, and 64-QAM symbols would all be mapped to the 64-QAM constellation map. Because the mapping is done based on a time-varying shared secret, it is varied on a per-symbol basis (e.g., the projection of the four QPSK constellation points onto the 64-QAM map is varied from one QPSK symbol to the next).

We use the notation $\mathcal{M}_i, i = 1 \ldots, M$, to refer to the payload's modulation schemes, where $\mathcal{M}_1$ is the lowest-order and $\mathcal{M}_M$ is the highest-order modulation scheme. Recent MO techniques [9], [12] take advantage of TCM to perform the $\mathcal{M}_i \rightarrow \mathcal{M}_M$ mapping and at the same time, maintain the same BER performance of $\mathcal{M}_i$. However, because of the higher susceptibility of higher-order modulation schemes to CFO, these techniques need complex CFO estimation methods to successfully retrieve the original $\mathcal{M}_i$-modulated symbols from the constellation of $\mathcal{M}_M$. Otherwise, their BER performance deteriorates significantly.

One such obfuscation technique is called Conceal and Boost Modulation (CBM) scheme [9]. CBM potentially uses all the symbols of $\mathcal{M}_M$ to directly map an $\mathcal{M}_i$-modulated symbol. So, our proposed adaptive demodulation scheme for QAM can be readily used to enhance the performance of CBM under erroneous CFO estimation. Another MO technique, called Friendly CryptoJam (FCJ) [12], often uses a proper subset of the symbols of $\mathcal{M}_M$ for mapping and then secretly varies this set for different symbols so as to utilize all $\mathcal{M}_i$-modulated symbols. Without loss of generality, we discuss MO application of our CFO-aware demodulation based on FCJ.

Although the density of the set of $\mathcal{M}_M$ points used in FCJ may be less than actual $\mathcal{M}_M$, FCJ exhibits the same level of sensitivity as $\mathcal{M}_M$ to CFO because two symbols in the



(a) Two-state TCM, $\mathcal{M}_i$ = BPSK. (b) Four-state TCM, $\mathcal{M}_i$ = BPSK. (c) Two-state TCM, $\mathcal{M}_i$ = QPSK.

Fig. 6. Trellis of minimal TCM codes [16] for different $\mathcal{M}_i$'s.

selected subset of $\mathcal{M}_M$-modulated symbols can be as close to each other as the symbols in the constellation of $\mathcal{M}_M$. In this section, we take advantage of the sparsity of $\mathcal{M}_M$-modulated FCJ symbols to improve its robustness to CFO. Specifically, we first jointly optimize its TCM code design w.r.t phase offset and coding gain. We then customize our adaptive demodulation scheme in Section III for the particular modulation in FCJ to further enhance its performance.

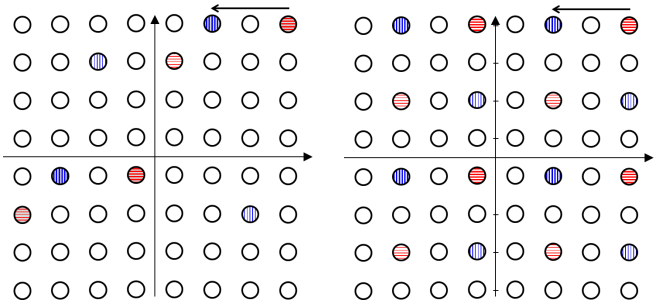
A. Optimizing TCM Codes w.r.t. Phase Offset

FCJ uses minimal two- and four-state TCM codes to obfuscate the payload's modulation scheme by defining several distinct subconstellations of $\mathcal{M}_M$, denoted by $\mathcal{U}_j = \{u_j^0, \ldots, u_j^{|\mathcal{M}_i|-1}\}$, where $|\mathcal{M}_i|$ is the order of $\mathcal{M}_i$ and $j = 0, \ldots, |\mathcal{M}_M|/|\mathcal{M}_i|$ ($|\mathcal{M}_i| = |\mathcal{U}_j|$). The rationale behind relying on minimal codes is that they have the lowest constraint lengths among all possible TCM codes, which means their encoder and Viterbi decoder have the least complexities. In addition, power consumption and decoding delay[3] at Rx are minimized with the use of minimal codes, a feature that can better justify incorporating these schemes in practical systems.

For each $\mathcal{M}_i$-modulated symbol at the Tx, two of these subconstellations (a total of $2|\mathcal{M}_i|$ symbols) are arbitrarily selected and used as the set of output symbols. The assignment of indices j to subconstellations is arbitrary. Even though the design of each individual subconstellation $\mathcal{U}_j$ in FCJ is optimal w.r.t. demodulation performance under AWGN, selection of a pair from $\binom{|\mathcal{M}_M|/|\mathcal{M}_i|}{2}$ possible pairs was not optimized there.

Before describing our optimal pair-selection scheme, we explain how coding gain for TCM codes is calculated. The free distance of a q-state TCM, d_{free}, is defined as the minimum Euclidean distance between all possible paths in the underlying trellis. Accordingly, the asymptotic coding gain $\gamma_i^{(q)}(M)$ used in the $\mathcal{M}_i \rightarrow \mathcal{M}_M$ mapping is defined as $\gamma_i^{(q)}(M) = \frac{d_{free}^2}{d_{min,i}^2}$, where $d_{min,i}$ is the minimum distance between the points on the constellation map of $\mathcal{M}_i$ [21]. In Fig. 6(a)-(b), a pair of paths with minimum free distance is shown for the minimal two- and four-state rate-$(\log_2|\mathcal{M}_i|/(1+\log_2|\mathcal{M}_i|))$ TCM codes [16] when $\mathcal{M}_i$ = BPSK. For higher-order QAM, parallel transitions will be introduced in the trellis (e.g., see Fig. 6(c)). In the latter case, the free distance will be the minimum of the distance between the symbols along parallel transitions and the free distance of the paths that span multiple states. These minimal codes need only a set of $2|\mathcal{M}_i|$ constellation points as output symbols. This design minimizes the coding complexity but at the expense of lower coding gain compared to CBM. The authors in [12] assign $\mathcal{U}_a \bigcup \mathcal{U}_b$ as the set of output symbols in each transition, where the pair $(a, b) \in j \times j$ is selected arbitrarily.

[3]The decoding delay is mainly specified by the path truncation depth of the Viterbi decoder, which is linearly proportional to the constraint length.



(a) $\mathcal{M}_i$ =BPSK (b) $\mathcal{M}_i$ =QPSK

Fig. 7. Examples of optimal pairs in 64-QAM and how a shift results in another optimal pair. The points with horizontal bars (red color) belong to pairs $(\mathcal{U}_{i_1}, \mathcal{U}_{i_2})$ while the points with vertical bars (blue color) belong to $(\mathcal{U}_{j_1}, \mathcal{U}_{j_2})$. Inside a pair, $\mathcal{U}_{i_1}$ and $\mathcal{U}_{j_1}$ are shown with thicker bars.

Now, consider the trellis of the two-state TCM in Fig. 6(a). The optimal subconstellation $\mathcal{U}_a$ in FCJ should maximize the Euclidean distance between any u_a^0 and $u_a^1 \in \mathcal{U}_a$. However, because of the arbitrary assignment of the indices to subconstellations, the distance between $u_a^0 \in \mathcal{U}_a$ and $u_b^0 \in \mathcal{U}_b$, which appear in the second transition, can be as small as the minimum distance in $\mathcal{M}_M$. We propose an optimal pairing of the subconstellations such that if $\mathcal{U}_a$ and $\mathcal{U}_b$ are to be used in the same transition, the minimum distance between the elements in $\mathcal{U}_a$ and $\mathcal{U}_b$ is also maximized. At the same time, this minimum distance is the same across different pairs. This way, the gain is also maximized, irrespective of the pair used in a given transition. A similar optimization can be applied to boost the gain of the four-state TCM.

1) Maximizing the Coding Gain: To find a set of optimal pairs, we first pick one of the sets $\mathcal{U}_j$ and then find a different set whose elements have the largest possible distance from the first set (for example, see the points with horizontal bars in Fig. 7). This is an attempt to find an upper bound on the maximum distance between the set of optimal pairs. Using the set partitioning results in [16], we can find such a pair, say $(\mathcal{U}_{i_1}, \mathcal{U}_{i_2})$. Next, we construct the rest of the optimal pairs by circularly shifting $\mathcal{U}_{i_1}$ and $\mathcal{U}_{i_2}$ horizontally and/or vertically on the constellation map of $\mathcal{M}_M$ (see the examples $(\mathcal{U}_{j_1}, \mathcal{U}_{j_2})$ in Fig. 7). This guarantees that all pairs have the same maximum Euclidean distance and so they are optimal. Note that this optimal solution is not necessarily unique.

TABLE I
CODING GAIN OF THE OPTIMAL MAPPING FROM BPSK AND QPSK TO 16-QAM.

i	$\mathcal{M}_i$	FCJ [12]		Enhanced (Optimal)	
		$\gamma_i^{(2)}(3)$	$\gamma_i^{(4)}(3)$	$\gamma_i^{(2)}(3)$	$\gamma_i^{(4)}(3)$
1	BPSK	-0.46 dB	2.3 dB	0.79 dB	3 dB
2	QPSK	0 dB	2.04 dB	0.79 dB	2.04 dB

TABLE II
CODING GAIN OF THE OPTIMAL MAPPING FROM LOW-ORDER QAM SCHEMES TO 64-QAM.

i	$\mathcal{M}_i$	FCJ [12]		Enhanced (Optimal)	
		$\gamma_i^{(2)}(3)$	$\gamma_i^{(4)}(3)$	$\gamma_i^{(2)}(3)$	$\gamma_i^{(4)}(3)$
1	BPSK	-1.05 dB	1.9 dB	0 dB	2.46 dB
2	QPSK	-0.92 dB	1.83 dB	0.58 dB	1.83 dB
3	16-QAM	0.76 dB	2.8 dB	1.55 dB	2.8 dB

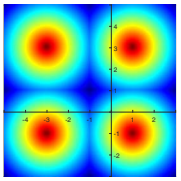
In Tables I and II we show the enhanced coding gains when the sets are optimally paired. While the gains are improved in all the cases of the two-state TCM, only the case of $\mathcal{M}_i =$ BPSK benefits from the optimal pairing in four-state TCM. For other $\mathcal{M}_i$ and $\mathcal{M}_M$ combinations, parallel transitions curb the gain. The enhanced (and nonnegative) gains of the two-state TCM suggest that using this code, which is the least-complex TCM code ever, would be sufficient for an MO scheme that needs to preserve the BER performance. In addition, the achieved gains are close to the ones achieved in [9] but with smaller constraint length (i.e., complexity) and/or more robustness to phase offset. For example, the least-complex code for upgrading BPSK to 16-QAM in [9] has a constraint length of 3 and gain of 3.42 dB, while here, we use a code with constraint length of 2 and the gain of 3 dB.

In contrast to FCJ, CBM does not vary the set of possible $\mathcal{M}_M$-modulated symbols for each transition. This implies that all $\mathcal{M}_M$ symbols must be considered in each transition to guarantee uniformly distributed constellation points (a requirement of the obfuscation). Although this gives a slight coding gain advantage over the codes in FCJ, it forces the Rx to check for all $|\mathcal{M}_M|$ symbols during decoding. Checking all symbols of a dense constellation makes the decoder more complex and more sensitive to phase offset whereas using $2|\mathcal{M}_i|$ symbols with maximum Euclidean distance automatically brings about more robustness to phase offset. Before we compare the sensitivity of these schemes to phase offset and apply our adaptive demodulation scheme, we further optimize the optimal pairs obtained above w.r.t phase offset. The optimal pairing w.r.t. coding gain may not be unique. We exploit this fact and search for those optimal pairs that have maximum robustness to phase offset.

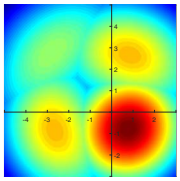
2) Maximizing robustness to CFO: Let each subconstellation $\mathcal{U}_j$ be a graph vertex with label j and assume that there is an edge between two vertices if the associated subconstellations have the maximum Euclidean distance, i.e., they can potentially be an optimal pair w.r.t. coding gain. Knowing the minimum distance between two optimal subconstellations, we first detect all such pairs by iterating over each subconstellation $\mathcal{U}_j$ and comparing the minimum distance to those that are cyclic shifts of $\mathcal{U}_j$. Second, for each potential pair, we measure the minimum phase offset ϕ_{min} that results in a demodulation error. This phase offset will be the weight of the edge between the two subconstellations in the graph. Third, we apply a *vertex cover* algorithm to find a set of optimal pairs that maximizes ϕ_{min} over all the pairs in the set. This set of pairs maximizes the phase offset that does not result in BER in the absence of noise.

TABLE III
OPTIMAL ϕ_{min} (IN RAD) COMPARED TO THE SCHEME IN [9]. DEFAULT REFERS TO THE ORIGINAL VERSION OF THAT SCHEME

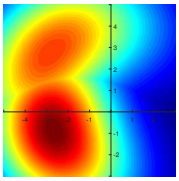
$\mathcal{M}_i$	Default	$\mathcal{M}_M = 16$-QAM		$\mathcal{M}_M = 64$-QAM	
		CBM [9]	Optimal	CBM [9]	Optimal
BPSK	$\pi/2 = 1.571$	0.295	0.5475	0.135	0.5055
QPSK	$\pi/4 = 0.783$	0.295	0.4636	0.135	0.3805
16-QAM	0.295	N/A	N/A	0.135	0.1651



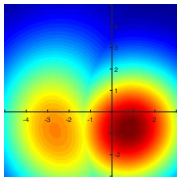
(a) Four symbols without CFO



(b) Four symbols with CFO



(c) Symbols $(-3,-1)$ and $(-3,3)$ with CFO



(d) Symbols $(-3,-1)$ and $(1,-1)$ with CFO

Fig. 8. Spatial distribution of received symbols for subconstellation $\{(-3,-1),(-3,3),(1,-1),(1,3)\}$ under simulated AWGN.

In Table III, we provide the maximum ϕ_{min} for the TCM codes derived above and compare it with uncoded $\mathcal{M}_i$ and with the scheme in [9] for different combinations of $\mathcal{M}_i$ and $\mathcal{M}_M$. The results show that ϕ_{min} under our optimal pairing scheme is almost four times larger than ϕ_{min} in CBM [9]. However, our enhanced TCM codes are still more sensitive to phase offset than the default scheme, which motivates employing our adaptive demodulation scheme.

B. Adaptive Demodulation for Modulation Obfuscation

We now customize our adaptive demodulation scheme for the enhanced TCM-coded MO method presented in Section III-A. The set of $2|\mathcal{M}_i|$ symbols in this method may consist of symbols with drastically different amplitudes. For example, for $\mathcal{M}_i =$ BPSK and $\mathcal{M}_M =$ 16-QAM, this method may produce "optimally" paired subconstellations $\mathcal{U}_a = \{(-3,3),(1,-1)\}$ and $\mathcal{U}_b = \{(-3,-1),(1,3)\}$. We illustrate the spatial distribution of these sets in Fig. 8. We observe in Fig. 8(b) that the distribution of the transmitted symbol $(1,-1)$ is very dense while the distribution of symbol $(-3,3)$ is stretched across a wider area. That will push the optimal demodulation boundaries towards the symbols that have higher amplitudes (see Fig. 9).

Similar to the approach used in Section III-A for QAM, here each demodulation region can be approximated using (8). However, to decode coded-modulated symbols in MO, the Rx needs to compute the sum of Euclidean distances for Viterbi

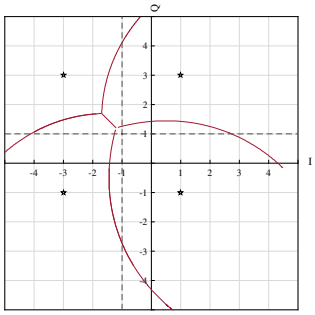


Fig. 9. Optimal demodulation regions for a quaternary subconstellation ($\gamma = 7$ dB and $t = 16T$). Dashed lines denote the default boundaries when $\delta_f = 0$.

algorithm rather than identifying the most probable region for each individual symbol. Under our adaptive demodulation, a received symbol may no longer belong to the region of the symbol that is closest to it. So the Rx cannot rely on distances for decoding, unless the distance is normalized w.r.t the underlying region boundaries. Hence, we propose the following distance normalization scheme for calculating the distance in the Viterbi algorithm:

For each received symbol, the Rx first identifies the region of a reference symbol, say S, that the received symbol belongs to. It then finds a line that passes through both the received symbol and S and finds the farthest point on that line which is inside the region. Finally, the distance from the received symbol to S is normalized w.r.t. the distance from the farthest point to S. This normalized distance can be used in the Viterbi algorithm to detect the most probable sequence of symbols.

V. Performance Evaluation

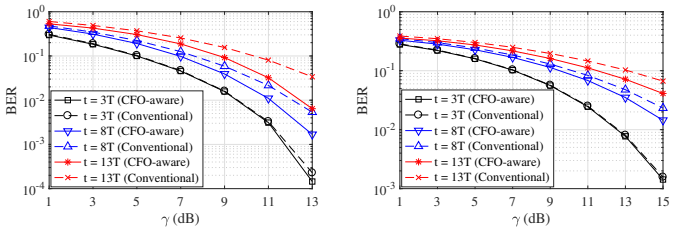
In this section, we evaluate the BER performance of our adaptive demodulation scheme when applied to uncoded MO. We vary the SNR γ and the residual CFO δ_f. The SNR values are selected from the range of SNRs at which the BER without CFO is expected to perform well for most of the applications, i.e., BER between 10^{-5} and 10^{-7}. We also verify the coding gain and the robustness to CFO of the enhanced TCM scheme to CFO. The scale of δ_f values in the simulations is determined by the magnitude of the phase offset when $l = 64$.

A. Gain of Adaptive Demodulation in Uncoded MO

Fig. 10 shows the BER improvement of our adaptive demodulation for BPSK $\rightarrow$ 16-QAM and QPSK $\rightarrow$ 16-QAM cases when TCM is not used (simply $\mathcal{M}_i \rightarrow \mathcal{U}_j$). By accounting for residual CFO, our scheme achieves the same BER of default boundaries for subconstellations $\mathcal{U}_j$ but at lower SNRs. Specifically, for the case $\mathcal{M}_i$ = BPSK, using CFO-aware boundaries alone achieves more than 2 dB gain when $t = 13T$ and $\gamma \geq 11$. When $\mathcal{M}_i$ = QPSK, our proposed scheme achieves the same 2 dB gain when $t = 13\,T$ and $\gamma \geq 13$.

B. Gain and Robustness of Optimal TCM Codes to CFO

In Fig. 11, we consider frames of 100 symbols each and study the impact of CFO (phase offset) on the performance of the enhanced TCM-aided MO scheme as well as the uncoded modulation $\mathcal{M}_i$. For each $\mathcal{M}_i$, we select the SNR that results



(a) $\mathcal{M}_i$ = BPSK (b) $\mathcal{M}_i$ = QPSK

Fig. 10. BER improvement in uncoded MO when CFO-aware demodulation boundaries are employed versus SNR at the intended Rx ($\mathcal{M}_M$ = 16-QAM).

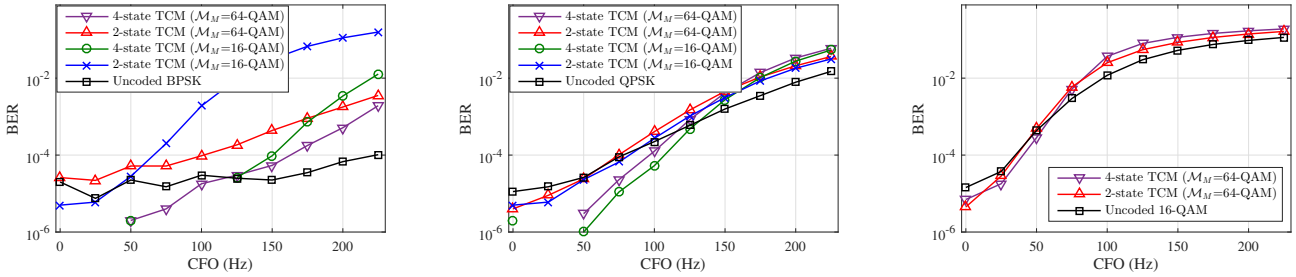
in 10^{-5} BER for the uncoded scheme. As expected (see Table III), mapping BPSK to higher modulation schemes is highly vulnerable to CFO. It can be seen in Fig. 11(a) that while employing TCM helps in accounting for the small residual CFO ($\delta_f < 75$ Hz), the sensitivity of high-order modulation schemes dominates the coding gain for larger δ_f and often results in high BER compared to uncoded BPSK. For QPSK and 16-QAM (Fig. 11(b) and Fig. 11(c), respectively), however, the extra coding gain and optimal pairing of subconstellations w.r.t. phase offset contribute to mitigating the sensitivity of higher-order modulation schemes to CFO. In QPSK, as long as $\delta_f \leq 125$ Hz, the four-state TCM-aided MO can maintain the BER performance of uncoded QPSK. This range for 16-QAM is $\delta_f \leq 50$ Hz.

Next, Fig. 12 and 13 show the BER of the enhanced TCM schemes for $\mathcal{M}_M$ = 64-QAM and 16-QAM, respectively. The results confirm our analysis in Section IV and also verify that using the least-complexity two-state TCM is sufficient to maintain the performance of the original $\mathcal{M}_i$. Altogether, assuming $\mathcal{M}_M$ = 16-QAM, our proposed techniques in Section IV can achieve up to 2.79–5 dB overall gain when $\mathcal{M}_i$ = BPSK and up to 2.79–4.04 dB gain when $\mathcal{M}_i$ = QPSK.

VI. Conclusions and Future Directions

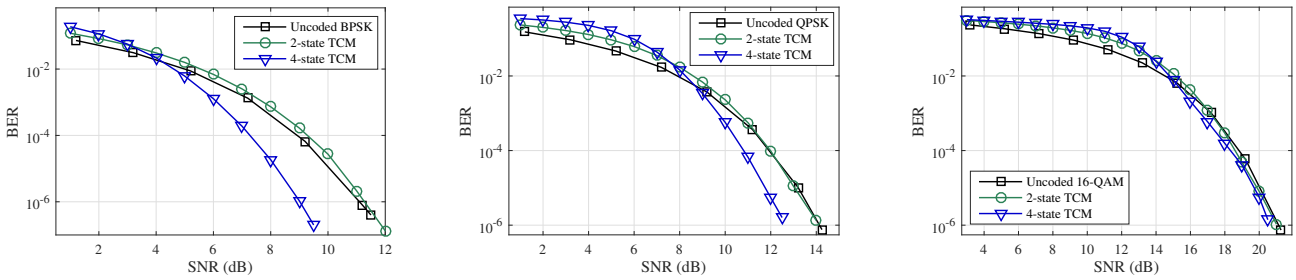
High-order modulation schemes are particularly sensitive to CFO estimation errors, which may hinder employing such modulation schemes in emerging systems and PHY-layer security techniques. Conventional demodulators are not adaptive to the time-varying phase offset induced by the residual CFO. In this paper, we derived the expression for the probability distribution of received symbols under imperfect CFO estimation and AWGN. For illustration purposes, we considered QAM and APSK, and numerically determined their optimal modulation boundaries. Using a similar analysis, we customized our adaptive demodulation technique for use in modulation obfuscation. We further boosted the gain and the reliability of modulation obfuscation by redesigning its coding scheme w.r.t. phase error. We then showed that the modified modulation obfuscation combined with the proposed adaptive demodulation can achieve up to 5 dB performance gain.

Deriving the exact expression for the CFO-aware demodulation boundaries is neither analytically possible nor practical because the Rx will need to solve a symbol detection problem with a set of *nonlinear* inequality constraints that define the



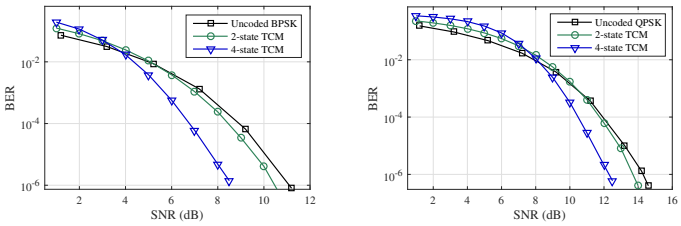
(a) $\mathcal{M}_i$ = BPSK, $\gamma = 10$ dB (b) $\mathcal{M}_i$ = QPSK, $\gamma = 13.2$ dB (c) $\mathcal{M}_i$ = 16-QAM, $\gamma = 20$ dB

Fig. 11. BER of different MO schemes versus residual CFO.



(a) $\mathcal{M}_i$ = BPSK (b) $\mathcal{M}_i$ = QPSK (c) $\mathcal{M}_i$ = 16-QAM

Fig. 12. BER after MO versus received SNR when $\mathcal{M}_M$ = 64-QAM.



(a) $\mathcal{M}_i$ = BPSK (b) $\mathcal{M}_i$ = QPSK

Fig. 13. BER after MO versus received SNR at the intended Rx when $\mathcal{M}_M$ = 16-QAM.

demodulation regions. However, it would be more practical to approximate these boundaries by a set of lines as functions of t and γ. This can be considered as a subject for future work.

Acknowledgment

This work was supported in part by NSF, the industry affiliates of Broadband Wireless Access & Applications Center (BWAC), and the Wireless@Virginia Tech group. Any opinions, findings, conclusions, or recommendations expressed in this paper are those of the author(s) and do not necessarily reflect the views of NSF.

References

[1] Qualcomm Technologies, Inc., "Making 5G NR a reality," Sep. 2016. [Online]. Available: https://goo.gl/gg6kbM
[2] The 3rd Generation Partnership Project (3GPP), "3GPP feature and study item list: Rel-16." [Online]. Available: https://goo.gl/xsY1eB
[3] IEEE P802.11 - TASK GROUP AX, "Status of project IEEE 802.11ax." [Online]. Available: https://goo.gl/iJCMbX
[4] K.-C. Huang and Z. Wang, *Millimeter Wave Communication Systems*. Hoboken, NJ, USA: Wiley/IEEE Press, 2011.
[5] DVB (Digital Video Broadcasting) Consortium, "Digital Video Broadcasting (DVB); second generation framing structure, channel coding and modulation systems for broadcasting, interactive services, news gathering and other broadband satellite applications," Mar. 2014. [Online]. Available: https://goo.gl/DNBXZe
[6] G. Ungerboeck, "Trellis-coded modulation with redundant signal sets part II: State of the art," *IEEE Commun. Mag.*, vol. 25, no. 2, pp. 12–21, 1987.
[7] P. H. Moose, "A technique for orthogonal frequency division multiplexing frequency offset correction," *IEEE Trans. Commun.*, vol. 42, no. 10, pp. 2908–2914, 1994.
[8] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Trans. Communications*, vol. 45, no. 12, pp. 1613–1621, 1997.
[9] T. D. Vo-Huu and G. Noubir, "Mitigating rate attacks through crypto-coded modulation," in *Proc. ACM MobiHoc Conf.*, Hangzhou, China, Jun. 2015, pp. 237–246.
[10] F. Jiang, R. Porat, and T. Nguyen, "On the impact of residual CFO in UL MU-MIMO," in *Proc. ICASSP Conf.*, Mar. 2016, pp. 3811–3815.
[11] International Telecommunication Union (ITU), "Minimum requirements related to technical performance for IMT-2020 radio interface(s)," Feb. 2017. [Online]. Available: https://www.itu.int/md/R15-SG05-C-0040/en
[12] H. Rahbari and M. Krunz, "Full frame encryption and modulation obfuscation using channel-independent preamble identifier," *IEEE Trans. Inf. Forensics Security*, 2016.
[13] J. S. Atkinson, J. E. Mitchell, M. Rio, and G. Matich, "Your WiFi is leaking: What do your mobile apps gossip about you?" *Future Generation Comput. Syst.*, 2016.
[14] H. Rahbari and M. Krunz, "Secrecy beyond encryption: obfuscating transmission signatures in wireless communications," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 54–60, 2015.
[15] G. Noubir, R. Rajaraman, B. Sheng, and B. Thapa, "On the robustness of IEEE 802.11 rate adaptation algorithms against smart jamming," in *Proc. 4th ACM WiSec Conf.*, Hamburg, Germany, Jun. 2011, pp. 97–108.
[16] G. Ungerboeck, "Channel coding with multilevel/phase signals," *IEEE Trans. Inf. Theory*, vol. 28, no. 1, pp. 55–67, 1982.
[17] R. Pawula, S. Rice, and J. Roberts, "Distribution of the phase angle between two vectors perturbed by gaussian noise," *IEEE Trans. Commun.*, vol. 30, no. 8, pp. 1828–1841, Aug. 1982.
[18] W. C. Lindsey and M. K. Simon, *Telecommunication systems engineering*. Courier Corporation, 1973.
[19] A. Seijas-Macías and A. Oliveira, "An approach to distribution of the product of two normal variables," *Discussiones Mathematicae Probability and Statistics*, vol. 32, no. 1-2, pp. 87–99, 2012.
[20] R. F. Pawula, "On the theory of error rates for narrow-band digital FM," *IEEE Trans. commun.*, vol. 29, no. 11, pp. 1634–1643, 1981.
[21] E. Biglieri, D. Divsalar, M. K. Simon, and P. J. McLane, *Introduction to Trellis-Coded Modulation with Applications*, 1st ed., J. Griffin, Ed. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1991.