Expanding the Role of Preambles to Support User-defined Functionality in MIMO-based WLANs

Zhengguang Zhang*, Hanif Rahbari†, and Marwan Krunz*
*Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ
†Department of Computing Security, Rochester Institute of Technology, Rochester, NY
Email: zhengguangzhang@email.arizona.edu, rahbari@mail.rit.edu, krunz@email.arizona.edu

***Abstract*—As the Wi-Fi technology goes through its sixth generation (Wi-Fi 6), there is a growing consensus on the need to support security and coordination functions at the Physical (PHY) layer, beyond traditional functions such as frame detection and rate adaptation. In contrast to the costly approach of extending the PHY-layer header to support new functions (e.g., Target Wake Time field in 802.11ax), we propose to turn a specific part of the frame preamble into a data field while maintaining its primary functions. Specifically, in this paper, we develop a scheme called *extensible preamble modulation* (*eP-Mod*) for the MIMO-based 802.11ac protocol. For each frame, *eP-Mod* can embed up to 20 bits into the 802.11ac preamble under 1×2 or 2×1 MIMO transmission modes to support the operations of a given PHY-layer function. The proposed scheme enables several promising PHY-layer services, such as PHY-layer encryption and channel/device authentication, PHY-layer signaling, etc. At the same time, it allows legacy (*eP-Mod*-unaware) devices to continue to process the received preamble as normal by guaranteeing that our proposed preamble waveforms satisfy the structural properties of a standardized preamble. Through numerical analysis, extensive simulations, and hardware experiments, we validate the practicality and reliability of *eP-Mod*.**

***Index Terms*—Preamble embedding, OFDM, MIMO, IEEE 802.11ac, USRP experiments.**

I. Introduction

Over the past two decades, the sole function of the Physical (PHY) layer in IEEE 802.11-based wireless local area networks (WLANs) has been to assist the receiver (Rx) in decoding frames. For example, the Rx uses PHY-layer fields to synchronize with the transmitter (Tx); estimate the Tx-Rx channel state information (CSI); learn frame duration, rate, and the number of spatial streams of a Multiple-Input-Multiple-Output (MIMO) transmission, etc. However, it is increasingly evident that an ideal PHY layer needs to support other functions besides these. For example, the Tx may need to adjust its spatial reuse factor [1] or adapt its full-duplex modes [2]. It may also need to obfuscate the transmission attributes of a communication to achieve higher secrecy [3]. The Rx may need to detect channel hijacking/spoofing attacks (e.g., [4]), identify the Tx in case of PHY-layer encryption [5], and so on. Unfortunately, the rather rigid structure of the 802.11 PHY-layer frame prevents its protocols from communicating information needed to support these new functions.

With regard to wireless security, we have seen a surge in PHY-layer-based attacks. For example, the eye-opening Key Reinstallation Attacks (KRACKs) [6] against WPA2 leverages a channel-based man-in-the-middle attack [4] at the PHY layer. KRACK, along with other attacks, underscores the insufficiency of existing security measures, and the need for devices to directly authenticate and coordinate with each other at the PHY layer. Accordingly, researchers have developed various PHY-layer security measures, including friendly jamming for confidentiality [7], RF fingerprinting for device authentication, etc. The effectiveness of friendly jamming as a security solution depends on the relative locations of eavesdropping devices or the availability of accurate CSI [8]. RF-based fingerprinting is sensitive to channel impairments and measurement errors [9], [10], making it prone to high false alarm and mis-detection rates. Thus, a more reliable and flexible identifier/signature/nonce exchange mechanism is needed for encryption and channel/device authentication at the PHY layer.

From an operational perspective, Wi-Fi systems can significantly benefit from a signaling mechanism at the PHY-layer. In fact, IEEE Task Group AX (TGax) is considering moving part of MAC signaling to the signal (SIG) field of PHY layer because it is always transmitted with the most robust modulation scheme and can be decoded before the payload is fully received [1]. The new features that can be supported with such a mechanism include, but are not limited to, frequency resource allocation for Multi-User MIMO (MU-MIMO), coloring of overlapping BSSs for adaptive collision avoidance in 802.11ax [1], Target Wake Time (TWT) signaling for power saving in IoT devices [11], operation mode advertisement for full-duplex devices (e.g., transmit/receive vs. transmit/sense), and so on. In fact, 802.11ah and 802.11ax support TWT scheduling and negotiation through a special trigger frame, aiming at significantly increasing the lifetime of an energy-constrained device by waking up only when communication is necessary [11]. One can reduce the overhead of transmitting such management frames if the same information can be embedded/encoded within the PHY-layer fields of a data frame; a philosophy that we advocate in this paper.

However, this approach of introducing a new SIG field for each new function is costly because of the rigid structure of the PHY-layer frame and the fact that SIG is transmitted at the lowest rate, so each new SIG field extends the frame duration by a nonnegligible amount. In this paper, we explore an alternative approach that allows devices to embed user-defined bits within specific parts of the preamble waveform. These

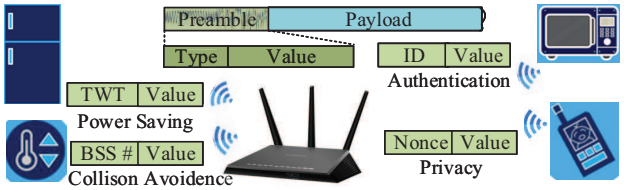


Fig. 1. Example of four applications of *eP-Mod*.

bits can be used to support new features/functions at the PHY layer. We focus on the latest MIMO-based 802.11 protocols and make use of a mandatory field in the frame preamble that is common across all MIMO-based Wi-Fi devices. The information embedded in the preamble can be timely decoded before decoding the payload, so it is not impacted by an encrypted or corrupted payload. By repurposing that specific preamble field into a generic data fields that can be used for a wide range of signalling purposes, we prevent the overhead of introducing new SIG fields.

Our proposed MIMO-based preamble embedding technique is called *extensible preamble modulation* (*eP-Mod*). At the Tx side, *eP-Mod* leverages multiple antennas to transmit several jointly designed variants of a preamble waveform under strict constraints required to support the preamble's primary functions and ensure backward compatibility. At the Rx side, *eP-Mod* treats specific parts of the preamble as a special data field and efficiently combines the multiple received waveforms to reconstruct the particular preamble waveform variant that carries the user-specified information. Our design provides more flexibility to support new services at the PHY-layer (see examples in Fig. 1) and offers extensibility to different MIMO schemes and channel widths. Using BPSK modulation for embedding user bits as the benchmark, we conclude that *eP-Mod* can embed up to 21 frame-specific bits in the preamble for a 80 MHz channel.

The main contributions of this paper are as follows:

1) We study the preamble design in MIMO-based 802.11n/ac/ax systems, and analyze its functions, backward-compatibility, and unique limitations when used for modulating user-defined bits under *eP-Mod*.
2) We consider 1×2 SIMO and 2×1 MISO scenarios separately, and study how *eP-Mod* can benefit from diversity gains. In the case of 1×2 SIMO, we use a combination of maximum-ratio combining (MRC) and equal-gain combining (EGC) to reliably extract the bits from the received waveforms. For the 2×1 MISO case, we use a variant of Alamouti code to encode the bits using two parts of the preamble. These MISO and SIMO special cases form the building blocks of a more general MIMO treatment, which is left for future work.
3) We simulate *eP-mod* for an 802.11ac MIMO system and further implement it on a USRP testbed. Our experiments over a 40 MHz channel show that *eP-mod* can communicate up to 20 and 18 bits per frame in the SIMO and MISO cases, respectively, while matching the bit-error rate (BER) performance of BPSK. Our implementation includes all the major Rx functions, such as coarse and fine timing/frame detection and frequency offset estimation, as well as low-complexity channel estimation and equalization.

II. Related Work

In many wireless systems (e.g., 802.11, 802.15.4, ...), the preamble is of great importance for the Rx to correctly decode a received frame. Accordingly, any (secondary) use of the preamble to communicate user-defined bits should not hinder its primary functions, and must also support backward compatibility and interoperability with legacy systems.

The preamble of non-OFDM (single carrier) 802.11b systems was considered in [5] for embedding a sequence of bits. This preamble has a different structure than the one in the OFDM-based Wi-Fi systems. It must also be a prior known to the Rx to be used for CSI estimation. A covert channel for OFDM-based Wi-Fi systems was proposed in [12], where the stegotext was camouflaged in the preamble by shifting its phase. However, the sensitivity of PSK to multipath fading and noise constrains the throughput of this covert channel to 4 bits at a moderate BER. Perhaps the closest work to ours is [13], in which the authors proposed embedding in the preamble of single-input-single-output (SISO) OFDM 802.11a systems by imposing phase and time shifts on a portion of the preamble for transmission over a 20 MHz channel. The design of *eP-mod* is challenging and different from [13] because in our case we must address the standard cyclic shift on different antennas, unintentional beamforming, subcarrier phase rotation on every 20 MHz channel, synchronization of multiple chains and MIMO gain techniques, etc. We address these challenges in a more general context, where we consider OFDM-based 802.11a/n/ac/ax preambles for embedding bits.

Several methods have been proposed for embedding bits in OFDM-based Wi-Fi frames by utilizing a redundant portion of the frame to constrain the embedding's negative impact. WiPad (Wireless Padding) [14] is one such method, where bits are embedded in the padding of frames (as opposed to conventional zero padding). However, the padding bits are at the end of a frame, where distortion is more severe than on its beginning. The Cyclic prefix (CP), another redundant field, is a concatenation of the last several samples of an OFDM symbol to its beginning. Szymon *et al.* suggested replacing conventional CP with information symbols [15]. However, their method is vulnerable to inter-symbol interference (ISI). In fact, it degrades the primary function of CP and may further impact data symbols. Frequency Offset Embedding for Authenticating Transmitters [16] is another embedding scheme in which the Rx must receive multiple frames to extract the embedded bits. In contrast, our scheme does not even require one full frame to extract these bits and achieves a higher per-frame embedding capacity than the $1 \sim 4$ bits in [16].

III. Frame Preamble – A Primer

In WLANs, the preamble is the first part of any PHY-layer frame. The preambles of MIMO-OFDM-based 802.11n/ac/ax systems start with a copy of the legacy 802.11a preamble for

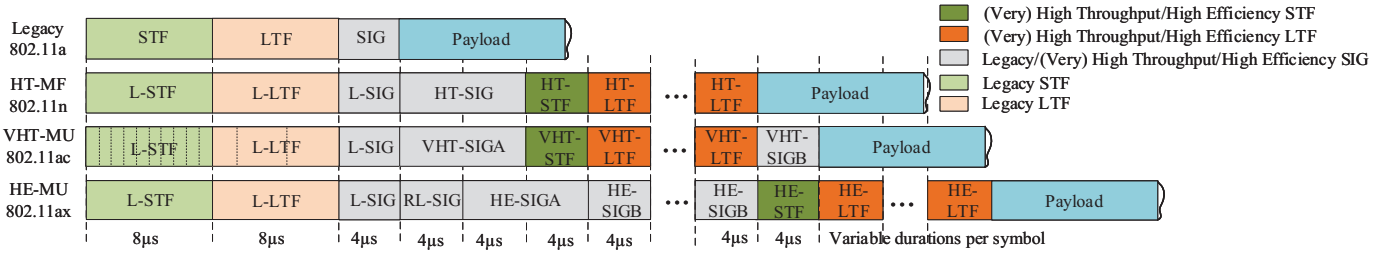


Fig. 2. Preambles in 802.11a/n/ac/ax standards.

backward compatibility, followed by additional short training fields (STFs), long training fields (LTFs), and SIG[1] fields, see Fig. 2. STFs and LTFs are essentially standardized *waveforms*. Bits of the SIG fields are always transmitted at the most-reliable modulation and coding scheme (BPSK with code rate $1/2$), irrespective of the channel conditions. As a result, the duration of the preamble is independent of the payload size and transmission rate, and can be up to $68\,\mu$s in 802.11ac [17]. In here, we take 802.11ac as the representative example of MIMO-OFDM-based 802.11 systems, and study its preamble structure, generation, and functions[2].

A. 802.11ac Preamble

The legacy part of the 802.11ac preamble consists of one STF (L-STF), one LTF (L-LTF), and one L-SIG field. The L-STF waveform is constructed by transmitting only on subcarriers that are four subcarrier-spacings apart from each other, resulting in a periodic OFDM waveform, named the short training signal (STS). Its period is a quarter of that of other OFDM symbols. In 802.11ac, the duration of a typical OFDM symbol without its guard interval is $3.2\,\mu$s. So within the $8\,\mu$s duration of the L-STF, there are $8/(0.25\times 3.2)=10$ repetitions of an STS. The L-LTF waveform, on the other hand, has the same period as typical OFDM symbols.

802.11ac supports MIMO operations as well as channels wider than 20 MHz. For MIMO operations, *Very High Throughput* (VHT) preambles are appended to the legacy preamble: one VHT-STF and multiple VHT-LTFs. The duration of each VHT-STF or VHT-LTF is $4\,\mu s$, half of their legacy counterparts. VHT-STF consists of five repetitions of the same legacy STS, while the VHT-LTF waveform is slightly different from L-LTF and is mapped to multiple VHT-LTFs by an orthogonal matrix. For different MIMO transmit chains, different cyclic shifts are applied to the legacy and VHT preambles to prevent unintentional beamforming [17]. As for channels wider than 20 MHz (40, 80, and 160 MHz), their preambles are essentially the replications of that of the base 20 MHz channel but with a subcarrier phase rotation on each additional 20 MHz channel. The rotation is necessary to reduce the peak-to-average power ratio (PAPR) of OFDM symbols [18], [19].

[1]Formerly known as PHY-layer header.

[2]In the 802.11ac standard, the preamble referrs to what comes before the PHY-layer payload, so by definition it includes the SIG fields. For the remaining of this paper and to simplify the exposition, we refer to the preamble as the part that comes before the SIG.

As an illustrating example, we consider an 802.11ac system with 40 MHz channel width. The L-STF occupies 24 out of 128 available subcarriers, indexed by $4k$, where $k\in\Lambda$, $\Lambda=\{-14,\cdots,-9,-7,\cdots,-2,2,\cdots,7,9,\cdots,14\}$. Let $\mathcal{S}=\{S_k\}_{k\in\Lambda}$ be the symbol sequence carried in these 24 subcarriers. The L-STF signal for the ith Tx antenna at time t, $0\le t<8\,\mu s$, is [17]:

$$s^{(i)}(t)=\sqrt{\frac{128}{24\,N_t}}\sum_{k\in\Lambda}\gamma_{4k}S_k\exp\left(j2\pi 4k\Delta_F(t-T^i_{lcs})\right) \quad (1)$$

where N_t is the number of Tx antennas, γ_{4k} represents the subcarrier phase rotation, $\Delta_F=312.5\,$kHz is the subcarrier spacing, and T^i_{lcs} is the legacy cyclic shift on the ith Tx antenna. Note that $\mathcal{S}$ for 40 MHz is a concatenation of two copies of its counterpart for the base 20 MHz channel, denoted by $\ddot{\mathcal{S}}$ and defined in [20]. That means, $\mathcal{S}=[\ddot{\mathcal{S}},\ddot{\mathcal{S}}]$.

B. Primary Preamble Functions in 802.11ac Systems

The preamble fields assist the Rx in performing the following functions:

1) Frame Detection and Time Synchronization: The repetitive structure of the L-STF (or the superposition of multiple L-STFs in the case of MIMO) is used by the Rx to detect the start of a frame and time-synchronize with the Tx. Because the channel coherence time in WLANs is larger than the preamble duration (as discussed in III-B3), the channel response does not change during the transmission of the preamble, meaning that the Rx can still detect the repetitive structure of the L-STF using auto-correlation methods. It is important to note that this method does not require knowledge of the transmitted L-STF for frame detection.

For fine-tuned time synchronization, however, the Rx must calculate the cross-correlation between the transmitted L-LTF and the received L-LTF. This method requires full knowledge of L-LTF signal, but is usually more accurate.

2) Frequency Synchronization: The inherent mismatch between the oscillators of the Tx and the Rx along with Doppler shift result in carrier frequency offset (CFO). CFO can cause significant performance deterioration to a MIMO-OFDM system [21]. Similar to time synchronization, CFO estimation can also be performed using periodic L-STF and L-LTF based on an autocorrelation method. Assuming perfect symbol timing and a stationary channel, a CFO of δ_f results in a phase difference of $2\pi t\delta_f$ between two repetitions of an STS that are transmitted t seconds apart. Thus, CFO can be estimated by measuring such phase differences averaged over a period

of time. Since the period of an L-STF is shorter than that of the L-LTF, the Rx can achieve higher accuracy by using the L-LTF to resist noise. Again, the Rx does not require knowledge of the transmitted L-STF for CFO estimation.

3) CSI Estimation: L-LTF is also used for SISO channel estimation, whereas VHT-LTFs are utilized for MIMO channel estimation and sounding. In the frequency domain, SISO channel estimation is done by simply dividing the subcarriers of L-LTF or VHT-LTF by the subcarriers of the corresponding received signals. However, CSI estimation in MIMO must leverage the orthogonal mapping matrix $\mathbf{P}$ [17, Eq.22-43] used in 802.11ac for VHT-LTF generation, and also account for the standard cyclic shifts on different Tx antennas.

More specifically, suppose that $N_t = 2$ and denote the channel matrix for the kth subcarrier of a 2×1 MIMO system by $\mathbf{h}_k = [h_{1,k}\ h_{2,k}]$. At the Tx, a vector of the VHT-LTF signals is pre-multiplied by the matrix $\mathbf{P}$ to generate the VHT-LTFs for each antenna. The rows of this matrix correspond to different Tx antennas and its columns correspond to different VHT-LTFs. The Rx can take advantage of the orthogonality of $\mathbf{P}$ and multiplying its Hermitian transpose by the received VHT-LTF signals to obtain the CSI estimate $[\hat{h}_{1,k}\ \hat{h}_{2,k}]$. This method can be generalized to all MIMO scenarios. However, because of mobility and Doppler spread, $\mathbf{h}_k$ may vary. To check the channel coherence time T_c, we use the following approximation:

$$T_c = \frac{1}{16\pi a_0 f_c / c} \tag{2}$$

where c is the speed of light, f_c is the operating frequency, and a_0 is the device speed. We note that the device mobility in 802.11ac WLANs almost never exceeds $a_0 = 108$ km/h$= 30$ m/s. The resulting coherence time at this speed is $83\,\mu s$ and $40\,\mu s$ for 2.4 GHz and 5 GHz bands, respectively. It means that the preamble is almost always within the coherence time and the same CSI estimate can be safely used throughout the preamble.

C. Preamble Design Criteria

Given the criticality of the aforementioned functions for frame decoding, any change in the waveform of the STFs should maintain the properties required to support these functions for compatibility and interoperability. Three main criteria restrict our design: (1) The repetitive structure and the fixed duration of the standard STFs with exact same period to facilitate reliable time and frequency synchronization; (2) The need for having different cyclic shifts at different antennas (to prevent unintentional beamforming); and (3) The small provisioned dynamic range (DR) in the standard (7.01 dB) for fast automatic gain control (AGC) locking and A/D conversion without overflow/underflow, and the low PAPR (2.24 dB) with respect to the nonlinearities of the existing power amplifiers [22]. Note that for embedding bits we can only redesign the STF waveforms, because knowledge of the transmitted STF is not necessary at the Rx. On the other hand, LTFs must be known for CSI estimation, and hence cannot be used for embedding user-defined bits.

i	8	9	10	11	12	13	14	15	16
$\theta_i^{(0)}$	π	0	0	0	$\pi/2$	π	π	π	0

TABLE I
A PART OF THE DEPENDENCY PATTERN $\Theta^{(\nu)}$ OF $\mathcal{S}$ WHEN $\nu = 0$.

IV. *eP-Mod* IN SIMO

In this section, we present the core idea of *eP-Mod* using, as an example, a simple 1×2 SIMO system (one transmit and two receive antennas), operating on a 40 MHz 802.11ac channel. First, we describe in details how to modulate an input bit sequence in an STF waveform.[3] As discussed above, the Rx does not need to know the exact STF waveform to perform the primary preamble functions as long as the waveform that carries the modulated bits satisfies its expected properties (see Section III-C). Next, we apply two typical combining techniques at the Rx, effectively leveraging the receiver diversity gain. Finally, we explain the process of demodulating this sequence.

A. Preamble Modulation Using Single Tx Antenna

We propose to use variants of the STF waveform with distinctive characteristics to modulate different bit sequences. Conventionally, a bit sequence is punctuated and modulated into a plurality of symbols. However, the strict requirements for STF restrict us to treat its entire waveform as one single modulation symbol. In addition, we need to keep the particularly low PAPR and DR of the STF and the most reliable way to do that is to maintain its amplitude. This can be realized by time and/or phase shift operations at the time domain of the entire STF waveform as a means to generate variants of this waveform and modulate input bit sequences (similar to the technique in [13]). Based on this idea, we design a modulation scheme that can also be readily applied with low complexity to any bandwidth in any OFDM-based 802.11 systems.

Starting with the time shift operation, assume we cyclically shift the STF waveform by t_{cs}. Plugging it into (1), this time shift translates to a linear phase shift $2\pi 4k\Delta_F t_{cs}$ along the subcarriers. Now let $\theta_i, i = 1, \ldots, 23$ be the (wrapped) phase differences of successive S_k's (for example, $\theta_1 = \measuredangle(S_{-13}) - \measuredangle(S_{-14})$) and define $\Theta = [\theta_1, \ldots, \theta_{23}]$ as the symbols *dependency pattern* for an STF waveform. Define the dependency pattern for standard STF as the *parent pattern* $\Theta^{(0)}$ (see Table I). Because of the linear phase shift, θ_i's all change by $\nu = 2\pi 4\Delta_F t_{cs}, \nu \in [-\pi, \pi]$ from $\Theta^{(0)}$. Thus, we can generate other compliant variants of STFs by generating *child patterns* $\Theta^{(\nu)}$, whose elements are determined by:

$$\theta_i^{(\nu)} = \begin{cases} \theta_i^{(0)} + 4\nu, i = 12 \\ \theta_i^{(0)} + 2\nu, i = 6, 18 \\ \theta_i^{(0)} + \nu, \text{otherwise} \end{cases} \tag{3}$$

The changes by a multiple of ν in (3) are due to null tones.

The concept of dependency pattern helps us to alternatively represent $\mathcal{S}$ using its first symbol S_{-14} and the associated

[3] VHT-STF and L-STF are both repetition of the same signal with different cyclic shifts, and embedding scheme is the same for them, so we refer to them as STF, unless mentioned otherwise.

$t_{cs}(\mu s)$	ν	b_2b_1
0	0	00
0.2	$\pi/2$	01
0.4	π	11
0.6	$-\pi/2$	10

TABLE II
DEPENDENCY PATTERNS WHEN $Q = 4$. THE IEEE STANDARD USES THE DEPENDENCY PATTERN $\Theta^{(0)}$ AND $\Delta\varphi = 0$ WHEN $S_{-14} = \sqrt{1/2 + j/2}$.

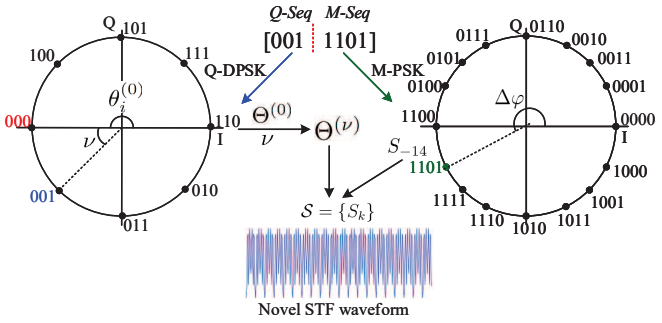


Fig. 3. Preamble modulation.

$\Theta^{(\nu)}$. Then the rest of the sequence $\mathcal{S}$ is derived recursively: $S_{-13} = S_{-14}\exp(j\theta_1^{(\nu)})$, $S_{-12} = S_{-13}\exp(j\theta_2^{(\nu)})$, and so on and so forth. In general, we can embed $\log_2 Q$ bits, namely *Q-Seq*, by $\nu = 2\pi q/Q, q \in \{0, 1, \ldots, Q-1\}$ to get Q time-shifted waveforms. An example of using four different ν's, corresponding to four time shifts, for modulating two bits is shown in Table II. The bits are Gray-coded based on ν.

In addition to time shift, we can rotate the constellation of each S_k by a common phase offset $\Delta\varphi$. To do this, we leverage the propagation of S_{-14}'s phase change, and first select a M-PSK-modulated S_{-14} with an amplitude of $\sqrt{2}$. Then, following one of the patterns $\Theta^{(\nu)}$ with the chosen S_{-14}, the phase shift $\Delta\varphi$ is propagated to the rest of the symbols in $\mathcal{S}$. If we make full use of all M symbols of the M-PSK scheme, $\log_2 M$ Gray-coded bits referred as *M-Seq*, can be modulated into the STF waveform. In turn, with the same $\Delta\varphi$, we can modulate $\log_2 Q$ bits (referred to as *Q-Seq*) using different dependency patterns. It is equivalent to a form of frequency-domain differential PSK (FD-DPSK), where the phase difference ν is encoded into $\theta_i^{(\nu)}, i = 1, \ldots, 23$. Thus, it is robust to channel phasor and CFO estimation errors. In contrast, $\Delta\varphi$ is encoded into the phase of all 24 symbols in $\mathcal{S}$ and sensitive to channel phasor, especially at high order. One can implement one or a combination of these two techniques. For example, we can set ν to 0 and only use $\Delta\varphi$ to modulate bits. However, in the general case as illustrated in Fig. 3, we can modulate $L = \log_2 M + \log_2 Q$ bits using the STF waveform, as shown below, where time shift and phase rotation are represented by Q-DPSK and M-PSK symbols, respectively.

$$\big[\underbrace{b_{\log MQ}, \ldots, b_{1+\log M}}_{\text{Q-Seq}}, \underbrace{b_{\log M}, \ldots, b_1}_{\text{M-Seq}}\big]. \tag{4}$$

Now that we have the frequency domain sequence for the STF, we can go ahead and generate the STF waveform using (1). However, instead of applying γ_{4k} for each S_k and then accounting for it at the Rx, we incorporate it into the parent pattern by modifying $\theta_{12}^{(0)}$ (as shown in Table I). This way, γ_{4k} can automatically impact new generated STFs through incorporated parent pattern without changing the relationship in (3), making it easier to detect $\Delta\varphi$.

The resulting STF waveform under *eP-Mod* maintains the periodicity, low DR and PAPR, and other general standardized features of the STF waveform such as cyclic shift and sub-carrier phase rotation. Therefore, it is backward compatible and could interoperate with devices with or without the implementation of *eP-Mod*. Our carefully-designed *eP-Mod* has little impact on normal preamble functions by complying to all the STF requirements stated above.

B. SIMO Diversity Gain under eP-Mod

Once the Rx synchronizes with the Tx in time and frequency and estimates the CSI on each Rx antenna, it applies the 32-point FFT (Fast Fourier Transform) on the 32 samples of each received STS (a total of 320 L-STF samples per antenna) to obtain the frequency-domain symbols. In the case that Rx has multiple antennas, it can first combine the symbols received on different antennas using the estimated CSI to obtain diversity gain before demodulating the bits, improving the effective SNR. In this paper, we study selection combining (SC), maximal ratio combining (MRC), and equal gain combing (EGC) schemes. Assuming an i.i.d. Rayleigh fading channel, the received symbol on the kth subcarrier, denoted by $\mathbf{y}_k \in \mathbb{C}^{2\times 1}$, is

$$\mathbf{y}_k = \mathbf{h}_k S_k + \mathbf{z}_k, \tag{5}$$

where $\mathbf{z}_k \sim \mathcal{CN}(0, 1)$ is zero mean circularly symmetric complex Gaussian noise vector. For simplicity, we omit the index k in the subsequent discussions, e.g., $\mathbf{y}_k$=**y**=$[y_1\ y_2]^T$. In SC, the Rx selects the strongest signal branch for demodulation. We theoretically and experimentally studied its performance compared to MRC and EGC. It turns out that SC has worse performance than the other two schemes, mainly because it does not take advantage of the potential gain from the other candidate signal, and so we do not report its results here.

In MRC and EGC, the symbol used for detection is a weighted sum of y_1 and y_2, as follows:

$$\acute{S} = \mathbf{w}^T\mathbf{y} = \sum_{n=1}^{2} w_n y_n \tag{6}$$

where w_n, $n = 1, 2$, is the combining weight and $\mathbf{w} = [w_1\ w_2]^T$. The weights for EGC and MRC are: $w_n^{EGC} = e^{-j\phi_n}$ and $w_n^{MRC} = h_n^*$, respectively, where $\phi_n = \measuredangle h_n$ is used to co-phase signals from each antenna. Hence, the combined signals of each technique are:

$$\acute{S}_{EGC} = \sum_{n=1}^{2} |h_n|\, S + z' \tag{7}$$

$$\acute{S}_{MRC} = \sum_{n=1}^{2} \|h_n\|^2 S + z'' \tag{8}$$

where $z' = \sum_{n=1}^{2} z_n e^{-j\phi_n}$ and $z'' = \mathbf{h}^H \mathbf{z}$. It has been proved that 1×2 MRC achieves higher effective SNR with array gain as 2, which is greater than in EGC where the array gain is $1 + \pi/4$ [23, Eq.1.33, 1.35].

C. Preamble Demodulation Using Multiple Rx Antennas

Before we compare the performance of MRC and EGC under *eP-Mod*, we first need to explain the demodulation process given a combined signal. The process is basically the inverse of modulation showed in Fig. 3. It starts by detecting the dependency pattern and deriving the reference symbols corresponding to that pattern. Thereafter, phase shift is optimally estimated based on the average phase difference between received symbols and their corresponding reference symbols. Finally, the embedded *Q-Seq* and *M-Seq* are decoded from estimated pattern and phase shift.

1) Pattern Detection: The dependency pattern can be identified by ν, so the Rx has to first find out the child pattern of received STF by estimating ν. Denotes $\tilde{\mathcal{S}}_l = [\tilde{S}_{l,-14}, \ldots, \tilde{S}_{l,-2}, \tilde{S}_{l,2}, \ldots, \tilde{S}_{l,14}], l \in \{1, \ldots, 9\}$ as the symbol sequence on the lth STS after receive combination in IV-B, and let $\tilde{\nu}$ be the estimate of ν based on all the nine[4] $\tilde{\mathcal{S}}_l$'s. Because the next step (phase shift detection) depends on the correct detection of the pattern, robust minimum mean-square error (MMSE) approach is used to estimate ν with respect to parent pattern $\Theta^{(0)}$. As the pattern is the effect of time shift, any timing error would add onto ν, so the estimation of ν requires accurate frame detection.

2) Phase Shift Detection: Next, a reference symbol sequence $\tilde{\mathcal{S}}$ is constructed based on $\Theta^{(\tilde{\nu})}$ for the sake of estimating $\Delta\varphi$, say $\Delta\tilde{\varphi}$. Then, the Rx calculates the phase shifts from the reference elements in $\tilde{\mathcal{S}}$ to the corresponding elements in $\tilde{\mathcal{S}}_l$, $l = 1, \ldots, 9$. Owing to the impact of noise and imperfect CSI and CFO estimation, the Rx sum the results of all $24l$ elements to get a more accurate $\Delta\tilde{\varphi}$. Finally, the bit sequence is fully demodulated based on $\tilde{\nu}$ and $\Delta\tilde{\varphi}$. The estimation accuracy of $\Delta\varphi$ relies on pattern detection, and also the CFO and CSI estimation accuracy because it is sensitive to any phasor error.

D. Capacity and Reliability Analysis

As we propose embedding bits by *eP-Mod* for various PHY-layer signaling and security functions initialization, It is important to study how many bits can be reliably communicated under *eP-Mod*. Because the number of bits determines Q and M, the orders of DPSK and PSK, respectively, one can observe that increasing the number of embedded bits will automatically decrease the demodulation performance. In this paper, we consider as our benchmark the BER performance of SIG fields, which always use BPSK for modulating the bits with highest reliability.

Compared to a BPSK symbol on one of the subcarriers in the SIG or payload, the Q-DPSK and M-PSK symbols in *eP-Mod* enjoy a higher energy-per-symbol to noise-power-spectral-density (E_s/N_0) under the same OFDM symbol signal-to-noise ratio (SNR) because of the way we detect the dependency pattern and phase rotation. This higher E_s/N_0 is due to the following factors:

1) The amplitude of each S_k in L-STF is $\sqrt{128/24}$ times larger than a BPSK symbol on a SIG/payload subcarrier, resulting in a gain of $128/24 = 16/3$ for both Q-DPSK and M-PSK symbols;
2) *eP-Mod* uses the patterns over 9 STSs and 23 mutually dependent differential phases among 24 symbols within each STS to average noise for estimating ν, where each STS lasts for a quarter of the duration of a typical subcarrier. That brings about an additional gain of $9/4 \times 23/2$ for Q-DPSK symbols;
3) Similarly, the M-PSK symbol is estimated using 9 STSs and 24 symbols S_k within each STS, which add up to an additional gain of $9/4 \times 24$.

Besides, both *eP-Mod* and BPSK symbols have the diversity gain of 2 and 1.79 in the case of MRC and EGC, respectively. The effective Es/N_0 gain for Q-DPSK and M-PSK symbols is summarized in Table III.

	MRC	EGC
Q-Seq	$\frac{16}{3} \times \frac{9}{4} \times \frac{23}{2} \times 2 = 276$	$\frac{16}{3} \times \frac{9}{4} \times \frac{23}{2} \times 1.79 = 247$
M-Seq	$\frac{16}{3} \times \frac{9}{4} \times 24 \times 2 = 576$	$\frac{16}{3} \times \frac{9}{4} \times 24 \times 1.79 = 514$

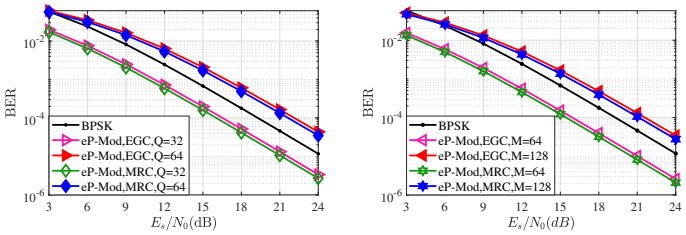
TABLE III
EFFECTIVE GAIN FOR Q-DPSK AND M-PSK SYMBOLS IN 1×2 SIMO UNDER *eP-Mod* FOR L-STF.

Because there is no closed-form expression of Q-DPSK and MPSK BER under fading channels, we use the MATLAB function *berfading* for approximating their BER and search sequentially to find the maximum M and Q that result in comparable BER as BPSK. In this section, we assume accurate time and frequency synchronization, and perfect CSI estimation to derive the maximum M and Q.

In Fig. 4(a), we depict the BER of Q-DPSK symbol in *eP-Mod* compared to BPSK for 1×2 SIMO system. It indicates that $Q = 32$ (5 bits) guarantees lower BER than BPSK, and MRC outperforms EGC. But for $Q = 64$, neither MRC nor EGC could help Q-DPSK symbol achieve the BER of BPSK. We also compare the performance when $M = 64$ and $M = 128$ (see Fig. 4(b)). In this case, $M = 64$ (6 bits) guarantees lower M-PSK symbol BER than BPSK, and MRC still outperforms EGC. But for $M = 128$, the BER is larger than BPSK either with MRC or EGC.

Thus, it is reliable enough to embed a total of $5 + 6 = 11$ bits in the L-STF of 1×2 SIMO systems. Additionally, we can embed a second sequence of $4 + 5 = 9$ bits in the VHT-STF with half of the effective gain in the L-STF because its duration is half of the L-STF. Therefore, we can embed a total of 20 bits in the preamble of 1×2 SIMO systems. However, in practical systems, Rx doesn't have the exact knowledge of CSI but instead uses estimated channel response $\tilde{\mathbf{h}}$ in (7) and (8). So this conclusion may not always hold in practice, which we will study in Section VII.

[4]The first STS $\tilde{\mathcal{S}}_1$ may be distorted by pulse shaping and other RF impairments and we discard it during detection.



(a) Q-DPSK (b) M-PSK

Fig. 4. BER of uncoded BPSK and *eP-Mod* for L-STF with different combining schemes vs. payload subcarrier E_s/N_0.

V. *eP-Mod* IN MISO

In the previous section, we assumed that the Tx has only one antenna and it modulates the input bits in the L-STF and VHT-STF independently. In contrast, in this section we assume the Tx has two antennas (a 2×1 MISO system), and explore how in the absence of CSI one can use space-time block codes (STBC) in the preamble to achieve Tx diversity gain. It would be another challenging problem to design beamforming precoders for the two L-STFs based on the knowledge of CSI, but we do not discuss it here as the CSI is not always available.

A. Challenges and Our Approach

The simplest form of STBCs is Alamouti code. It generates four orthogonal symbols for a two-transmit antenna system to be transmitted at two time-slots. However, as discussed before, the L-STF must be regarded as a single modulation symbol and cannot be divided into two time-slots for transmitting two distinct symbols. Otherwise, its DR, PAPR, and especially periodicity properties will not hold. At the same time, the transmitted STF waveforms from the two antennas should be designed in a way that they do not end up with the same cyclic shift because it creates unintentional beamforming, which would deteriorate the received signals.

Examining the 802.11ac preamble format (see Fig. 2) reveals that we can actually take advantage of two different STF fields, one the L-STF and the other VHT-STF, to create two time slots for the Alamouti code. We scanned the entire 802.11ac standard and verified that *the standard does not have any operational restriction on the two STF fields to be identical*. The L-STF is crucial for frame detection, CFO estimation and coarse AGC, whereas the VHT-STF is only used for fine AGC. Conjugation and negation operations in Alamouti keep the DR, PAPR and period of the waveform intact. Hence, the Alamouti-coded STFs are still functional.

Another assumption for Alamouti is that the channel does not change over the two time slots. Looking back into the preamble structure, L-STF and VHT-STF are separated by 20μs, rather than being consecutive as in general Alamouti code systems. In spite of that, we have derived a minimum coherence time of $40\,\mu s$ in III-B3. It's much shorter than a typical coherence time in Wi-Fi systems, so we can safely implement Alamouti code in these two fields assuming that they experience the same channel.

B. eP-Mod with Alamouti

Consider two Tx antennas Tx1 and Tx2 and two bit-sequences of length L to be modulated using the L-STFs and VHT-LTFs. At first, using the scheme elaborated in IV-A, these two sequences can be modulated independently by Tx1 and Tx2 to get frequency domain symbol sequences, say $\mathcal{S}_1$ and $\mathcal{S}_2$, for their own L-STFs. Then, these two sequences are exchanged between two antennas and used to generate VHT-STFs. Let $\mathcal{S}_1 = \{S_{1,k}\}$, and $\mathcal{S}_2 = \{S_{2,k}\}, k \in \Lambda$, we have the Alamouti code for kth subcarrier:

$$\hat{\mathbf{S}} = \begin{bmatrix} S_{1,k} & -S_{2,k}^* \\ S_{2,k} & S_{1,k}^* \end{bmatrix} \tag{9}$$

where $S_{1,k}$ is the symbol for Tx1's L-STF while $S_{2,k}$ is for Tx2's L-STF, which will be transmitted simultaneously during the L-STF period. When it comes to the VHT-STF period, Tx1 uses $-S_{2,k}^*$ to generate its VHT-STF waveform while Tx2 uses $S_{1,k}^*$ for its VHT-STF. Let $Y_{1,k}$ and $Y_{2,k}$ denote the received signals at times t and $t+T$, respectively. Considering the channel matrix $\mathbf{h}_k = [h_{1,k}\ h_{2,k}]$ of the kth subcarrier, then

$$Y_{1,k} = h_{1,k}S_{1,k} + h_{2,k}S_{2,k} + z_{1,k} \tag{10}$$

$$Y_{2,k} = -h_{1,k}S_{2,k}^* + h_{2,k}S_{1,k}^* + +z_{1,k} \tag{11}$$

where $z_{1,k}$ and $z_{2,k}$ are the additive noise at time t and $t+T$, respectively. We may further express (10) and (11) as

$$\begin{bmatrix} Y_{1,k} \\ Y_{2,k}^* \end{bmatrix} = \underbrace{\begin{bmatrix} h_{1,k} & h_{2,k} \\ h_{2,k}^* & -h_{1,k}^* \end{bmatrix}}_{\mathbf{H}_e} \begin{bmatrix} S_{1,k} \\ S_{2,k} \end{bmatrix} + \begin{bmatrix} z_{1,k} \\ z_{2,k}^* \end{bmatrix} \tag{12}$$

Now, $S_{1,k}$ and $S_{2,k}$ could be easily estimated by multiplying $\mathbf{H}_e^H$ to both sides as (13), and repeat it over all subcarriers to eventually reconstruct $\mathcal{S}_1$ and $\mathcal{S}_2$. Then, we could directly apply the demodulation procedure as in IV-C. As we can see in (13), Alamouti code could effectively eliminate the interference of two transmitted STFs. Thus, the demodulation performance of embedded sequence is improved. Meanwhile, this scheme maintains all the properties of STFs waveforms, hence it does not impact the accuracy of frame detection, CFO and CSI estimation, AGC.

$$\mathbf{H}_e^H \begin{bmatrix} Y_{1,k} \\ Y_{2,k}^* \end{bmatrix} = \left[|h_{1,k}|^2 + |h_{2,k}|^2\right] \mathbf{I} \begin{bmatrix} S_{1,k} \\ S_{2,k} \end{bmatrix} + \mathbf{H}_e^H \begin{bmatrix} z_{1,k} \\ z_{2,k}^* \end{bmatrix} \tag{13}$$

However, there are two aspects of limitations that constrain the capacity of this scheme. On the one hand, VHT-STF only contains 5 STSs while L-STF contains 10, so we have to repeat the received VHT-STF once to get 10 STSs and then perform Alamouti decoding with L-STF as described above. Indeed, the actual effective gain in VHT-STF is lower than L-STF, which restricts the total bits that can be modulated. On the other hand, to avoid unintentional beamforming, the time shift we modulated in the STFs of two Tx antennas should keep a minimum difference of 50ns as in 802.11ac standard. Since the STS period is $T_s = 800$ns, when Tx1 could embed $\log Q$ bits by a time shift of $t_{s1} \in [0, 800]$ns in its STFs, Tx2 should not cyclically shift its STFs by $t_{s2} \in [t_{s1} - 50, t_{s1} + 50]$ns.

This results in effective bits number of $\log \frac{7}{8}Q$, reducing the effective total bits in MISO to $(4+5)+(3.8+5)=17.8$.

VI. Extension to Higher Bandwidths

The schemes in the preceding sections are for special MIMO systems operating in 40 MHz channels. We now explain how our design can be extended to higher bandwidths. In OFDM-based 802.11 standards, for whatever bandwidth, the STFs are generated using the same sequence $\ddot{\mathcal{S}}$, defined for 20 MHz channel [20]. The corresponding frequency domain symbol sequence for higher bandwidth is given in [17, Eq. 22.29–32]. Basically, $\ddot{\mathcal{S}}$ is distributed with 4 subcarrier spacings and inserted with null tones, then duplicated on each 20 MHz channel with a subcarrier phase rotation, and finally the time domain STFs after inverse FFT (IFFT) are cyclically shifted on each Tx antenna. This way, the STF is customized for each antenna with bandwidth up to 160 MHz.

Denote the parent pattern of $\ddot{\mathcal{S}}$ as $\ddot{\Theta} = [\theta_1, \theta_2, \ldots, \theta_{11}]$. We can easily extend our proposed modulation scheme to any bandwidth by leveraging the replicative structure of the STFs and embed even more bits, as described in Algorithm 1.

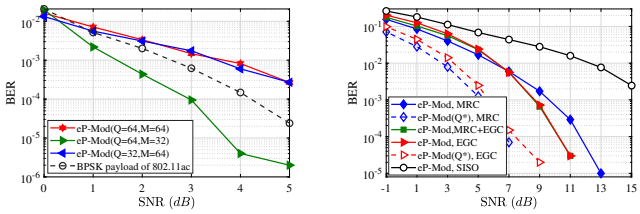
Algorithm 1 Extensible Preamble-Modulation (eP-Mod)

1: **procedure** EP-MOD(*Q-Seq*‖*M-Seq*)
2: Generate the parent pattern $\Theta^{(0)}$ by repeating $\ddot{\Theta}$ and applying the phase rotation for each 20 MHz block
3: $\nu = 2\pi q/Q$, where q is the Gray-coded *Q-Seq*'s index
4: Construct child pattern $\Theta^{(\nu)}$ from $\Theta^{(0)}$ and ν
5: Set S_{-N} as the M-PSK symbol of Gray-coded *M-Seq*
6: Derive subsequent STF symbol S_k with S_{-N} and $\Theta^{(\nu)}$
7: Normalize power, apply IFFT, and add CP
8: **end procedure**

Following this algorithm, each Tx antenna could embed different bit sequences in both its L-STF and VHT-STF. At the Rx side, all Rx antennas have to run time and frequency synchronization, then perform CSI estimation after FFT. Next, MRC and EGC are used to equalize the channel effect with diversity gain so that the embedded bits could be extracted by preamble demodulation as in IV-C. Through similar analysis as in IV-D, we conclude that up to 21 frame-specific bits could be embedded in a preamble for 80 MHz channel width.

VII. Performance Evaluation

To evaluate the performance of our proposed scheme in terms of BER as well as its impact on the the primary preamble functions, we conduct extensive LabVIEW simulations and indoor experiments using NI-USRP RIOs. For both simulations and experiments, we implemented the same 802.11ac PHY-layer system with our proposed *eP-Mod* schemes along with the standard 802.11ac PHY-layer system as our benchmark. We further implemented an uncoded BPSK payload in 20 OFDM symbols for both systems. In the SIMO scenarios, and for evaluation purposes, we apply *eP-Mod* to embed bits only in the L-STF, whereas in the MISO scenarios, we apply *eP-Mod* with and without Alamouti code where two Tx antennas jointly embed bits in their L-STFs and VHT-LTFs. Here, for simplicity, we don't impose the restriction with regard to unintentional beamforming at the Tx and let each antenna select its bit sequence independently. As a convention, "eP-Mod" refers to the scheme combining time shift and phase shift, while "eP-Mod(Q*)" only applies time shift.



(a) *eP-Mod* vs. BPSK payload, AWGN channel. (b) *eP-Mod* SISO vs. SIMO modes in Rayleigh channel ($Q = M = 32$).

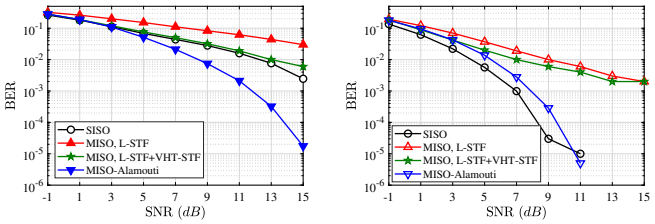
Fig. 5. BER of *eP-Mod* in SIMO modes under different channels.

A. Simulations

We study the performance of different *eP-Mod* schemes under different channel models through simulating the PHY-layer systems. First, we consider SIMO and $5 \sim 6$ bits for both *Q-Seq* and *M-Seq*, i.e. $Q = 32, 64$ and $M = 32, 64$. Fig. 5(a) compares the BER of *eP-Mod* and the BPSK payload against OFDM-symbol SNR in AWGN channel. It validates our conclusion from Fig. 4 that we can successfully embed 11 bits in the L-STF and achieve a better BER than BPSK, but only with 6 bits in *Q-Seq* and 5 bits in *M-Seq* (not the other way around). This implies the tradeoff between Q and M that slightly higher Q than M, i.e, $Q = 64, M = 32$, achieves a better BER because Q-DPSK is less sensitive to noise than M-PSK. As expected, when Q and M are both increased to 64, the overall BER of *eP-Mod* is worse than BPSK.

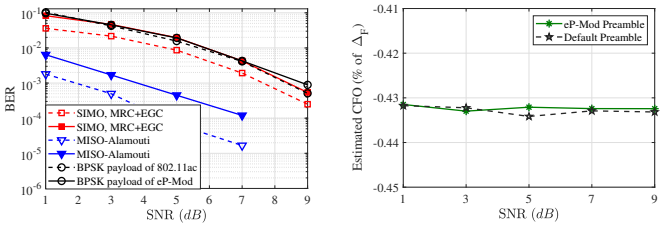
To compare the diversity combining techniques, we simulate *eP-Mod* under SIMO with MRC and/or EGC in a Rayleigh channel of 5 paths –see Fig. 5(b). MRC performs better than EGC at low SNRs, but falls behind EGC at high SNRs. Meanwhile, MRC always outperforms EGC for demodulating *Q-Seq* bits. This implies that for *M-Seq* bits, EGC often performs better than MRC. It is attributed to the fact that imperfect CSI estimation and uncompensated channel phasor would impact successive symbols alike, resulting in less perturbations in their phase differences $\theta_i^{(\nu)}$ (i.e., dependency pattern) than their absolute phase. Looking into (8), at low SNR, stronger signal branches are amplified by higher weights while weak signals are further weakened by smaller weights in MRC, allowing more reliable signal branches to dominate the phase of the combined signal. When it comes to high SNR, even weaker signal branches are reliable enough to contribute to the phase of combined signal. Therefore, we combine them together by using *(1) MRC for the detection of dependency pattern* and *(2) EGC for the phase-shift detection.*

As for MISO, we first study the performance without Alamouti code. Here, two Tx antennas have to embed the same sequence of 10 bits, i.e., $Q = 32$ and $M = 32$, so that the single Rx antenna can demodulate it. The BER of *eP-Mod* (especially the *Q-Seq*) in this naive MISO case is worse than SISO, as shown in Fig. 6(a) and (b). Even if we



(a) *eP-Mod*($Q = M = 32$). (b) *eP-Mod*(Q^*, $Q = 32$).

Fig. 6. BER of *eP-Mod* for MISO vs. SISO, Rayleigh channel (simulations).



(a) BER of *eP-Mod* vs BPSK payload. (b) Average of estimated CFO.

Fig. 9. BER and CFO in USRP experiments, *eP-Mod*($Q = 64, M = 16$).

additionally modulate the same bit sequence in VHT-STFs to obtain a higher effective gain, it is still worse than the SISO performance. It is because the naive MISO cannot decompose the two interfering signal branches. In contrast, when Alamouti code is used in *eP-Mod* to counter the interference, not only the BER is improved significantly, but also the number of embeded bits per frame is doubled.

Besides maximizing the number of bits *eP-Mod* can reliably transmit, maintaining the primary functions of our proposed preamble is crucial. Specifically, we compare the frame detection accuracy of *eP-Mod* in MISO schemes with default 802.11ac preamble under Rayleigh channel in Fig. 7. It shows that the accurate detection probability is not deteriorated by our methods. Moreover, the accuracy does not noticeably change as SNR decreases since we detect the frame by three steps: *Max Energy Detection*, L-STF-based autocorrelation, and L-LTF-based crosscorrelation, and L-LTF is not impacted by our design.

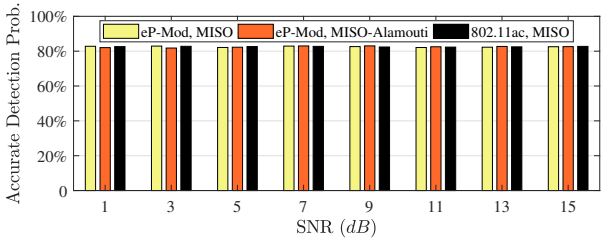


Fig. 7. Frame detection accuracy of *eP-Mod* vs. 802.11ac in MISO mode.

B. USRP Experiments

We further evaluate the practicality of *eP-Mod* on a testbed consisting of two NI-USRP 2942Rs. The indoor experiment setup is shown in Fig. 8, where the Tx and Rx are separated by $2\,m$ and each is equipped with $8\,$dBi antennas operating at $2.5\,$GHz frequency. Due to the processing limitations of the host's CPU, the bandwidth is downgraded from $40\,$MHz to $400\,$kHz. Since the environmental noise floor at the Rx is too low, a synthetic Gaussian noise is added at the Tx so as to lower the overall SNR. In the following, the SNR refers to the the synthetic SNR at the Tx (not the exact SNR at the Rx).

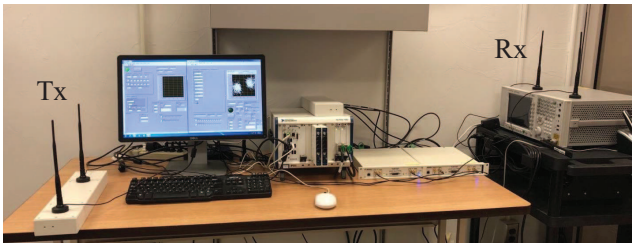


Fig. 8. Experimental setup with USRP 2942R and antennas.

Similar to the simulations, we have been able to reliably communicate 10 bits per antenna in both SIMO and MISO-Alamouti schemes with comparable or lower BER as BPSK, as shown in Fig. 9(a). However, different from the simulations, we need to set $Q = 64$ and $M = 16$ to get the best performance, which means the demodulation of *Q-Seq* is much more reliable in practice than detecting the phase shift for *M-Seq*. The BER performance of *eP-Mod* for SIMO and MISO-Alamouti schemes are compared in Fig. 9(a) too. Although diversity gain by Alamouti in MISO is comparable as MRC+EGC in SIMO, additional effective gain in VHT-STF guarantees lower BER in MISO-Alamouti scheme than SIMO scheme.

We also test the impact of our schemes with respect to frame detection and CFO estimation accuracy. First, we note in Fig. 9(a) that the BER of BPSK payload is not impacted by *eP-Mod*, an indication that the preamble functions have been successfully maintained. Specifically, as shown in Fig. 9(b), the estimated CFO under *eP-Mod* is very close to that of the default 802.11ac preamble. We also compared the frame detection accuracy of the SIMO and MISO modes of *eP-Mod*. It turns out that the accurate frame detection probability in SIMO is 91.8%, which is worse than 99.5% in MISO, because two Rx antennas detecting independently suffer from fading.

VIII. Conclusion

We presented the extensible design and implementation of a novel preamble in MIMO-OFDM based 802.11 systems, named *eP-Mod*, enabling the Tx operating in 80MHz to embed up to 21 frame-specific bits for anticipated applications. To do this, we encode time shift and phase shift of STF waveform into the characteristics of STF frequency domain symbols. Diversity gain techniques are customized and applied to *eP-Mod* to improve its throughput and reliability. Most importantly, our schemes take accounts of standard preamble properties, thus maintain all the functions of preamble. Our evaluation of its performance with BPSK payload as benchmark demonstrates that it could be utilized for PHY/MAC signaling and PHY-layer security.

Acknowledgment

This research was supported in part by NSF (grants CNS-1513649, CNS-1563655, CNS-1731164, CNS-1813401, and IIP-1822071) and by the Broadband Wireless Access Applications Center (BWAC). 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] E. Khorov, A. Kiryanov, A. Lyakhov, and G. Bianchi, "A tutorial on IEEE 802.11ax high efficiency WLANs," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 197–216, 2018.

[2] M. Hirzallah, W. Afifi, and M. Krunz, "Full-duplex-based rate/mode adaptation strategies for Wi-Fi/LTE-U coexistence: A POMDP approach," *IEEE Sel. Areas Commun.*, vol. 35, no. 1, pp. 20–29, 2016.

[3] 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.

[4] M. Vanhoef and F. Piessens, "Advanced Wi-Fi attacks using commodity hardware," in *Proc. 30th Ann. Computer Security Applications Conf. (ACSAC)*, New Orleans, Louisiana, USA, 2014, pp. 256–265.

[5] H. Rahbari and M. Krunz, "Full frame encryption and modulation obfuscation using channel-independent preamble identifier," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 12, pp. 2732–2747, Dec. 2016.

[6] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in wpa2," in *Proc. ACM SIGSAC Conf. Computer and Communications Security (CCS)*, Dallas, Texas, USA, 2017, pp. 1313–1328.

[7] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, 2008.

[8] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *IEEE Symp. Security and Privacy*, 2013, pp. 160–173.

[9] B. Danev, D. Zanetti, and S. Capkun, "On physical-layer identification of wireless devices," *ACM Comput. Surv.*, vol. 45, no. 1, pp. 6:1–6:29, Dec. 2012.

[10] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Proc. IEEE Int. Conf. Commun.*, June 2007, pp. 4646–4651.

[11] "IEEE Draft Std 802.11ax d4.0," *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment Enhancements for High Efficiency WLAN*, March 2019.

[12] J. Classen, M. Schulz, and M. Hollick, "Practical covert channels for wifi systems," in *2015 IEEE Conference on Communications and Network Security (CNS)*, Sep. 2015, pp. 209–217.

[13] H. Rahbari and M. Krunz, "Exploiting frame preamble waveforms to support new physical-layer functions in ofdm-based 802.11 systems," *IEEE Transactions on Wireless Communications*, vol. 16, no. 6, pp. 3775–3786, June 2017.

[14] K. Szczypiorski and W. Mazurczyk, "Hiding data in ofdm symbols of ieee 802.11 networks," in *2010 International Conference on Multimedia Information Networking and Security*, Nov 2010, pp. 835–840.

[15] S. Grabski and K. Szczypiorski, "Steganography in OFDM symbols of fast IEEE 802.11n networks," in *2013 IEEE Security and Privacy Workshops*, May 2013, pp. 158–164.

[16] V. Kumar, J.-M. Park, and K. Bian, "Blind transmitter authentication for spectrum security and enforcement," in *Proc. ACM Conf. Computer and Communications Security (CCS'14)*, Scottsdale, Arizona, USA, 2014, pp. 787–798.

[17] "IEEE Std 802.11ac-2013," *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications–Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz*, 2013.

[18] Y. N. Leonardo Lanante Jr., "Phase rotation for the 80 mhz 802.11ac mixed mode packet," Jul. 2010, doc.: IEEE 802.11-10/0791r0. [Online]. Available: https://bit.ly/2ZoTiXY

[19] E. Perahia and R. Stacey, *Next generation wireless LANs: 802.11 n and 802.11 ac*. Cambridge university press, 2013.

[20] "IEEE Std 802.11a-1999," *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHz Band*, 1999.

[21] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM wireless communications with MATLAB*. John Wiley & Sons, 2010.

[22] R. Boehnke and T. Doelle, "Alternative proposal for BRAN SYNCH preamble," Mar. 1999, doc.: IEEE 802.11-99/048. [Online]. Available: http://goo.gl/NIy6BM

[23] C. Oestges and B. Clerckx, *MIMO wireless communications: From real-world propagation to space-time code design*. Academic Press, 2010.