

Deep Learning-based Modulation Classification of Practical OFDM Signals for Spectrum Sensing

Byungjun Kim*, Christoph Mecklenbräuer[‡], Peter Gerstoft*[†]

*Dept. of ECE, University of California, San Diego, La Jolla, USA

[†]Marine Physical Laboratory, University of California, San Diego, La Jolla, USA

[‡]Institute of Telecommunications, TU Wien, Vienna, Austria

Abstract—In this study, the modulation of symbols on OFDM subcarriers is classified for transmissions following Wi-Fi 6 and 5G downlink specifications. First, our approach estimates the OFDM symbol duration and cyclic prefix length based on the cyclic autocorrelation function. We propose a feature extraction algorithm characterizing the modulation of OFDM signals, which includes removing the effects of a synchronization error. The obtained feature is converted into a 2D histogram of phase and amplitude and this histogram is taken as input to a convolutional neural network (CNN)-based classifier. The classifier does not require prior knowledge of protocol-specific information such as Wi-Fi preamble or resource allocation of 5G physical channels. The classifier’s performance, evaluated using synthetic and real-world measured over-the-air (OTA) datasets, achieves a minimum accuracy of 97% accuracy with OTA data when SNR is above the value required for data transmission.

Index Terms—Modulation classification, spectrum sensing, OFDM, Wi-Fi, 5G.

I. INTRODUCTION

The growth of wireless technologies in the scarce radio spectrum has strongly prioritized spectral efficiency: A challenge that is being addressed by, e.g., (massive) MIMO technology, joint radar communications, and cognitive radio [1]–[3]. Here, we focus on an essential component of cognitive radio, namely intelligent spectrum sensing, which allows for real-time characterization of radio spectrum usage and aids in online decision-making for spectrum allocation. Spectrum sensing encompasses signal detection [4], predicting available spectrum [5], and identifying modulation schemes. In this study, we focus on the classification of modulations of state-of-the-art wireless orthogonal frequency division multiplexing (OFDM) signals.

OFDM transmission has become foundational in current wireless communication systems, such as Wi-Fi 6 and 5G. In these systems, message bits are first encoded and subsequently mapped to digital symbols using quadrature amplitude modulation (QAM) on individual subcarriers. Many QAM symbols are modulated onto many subcarriers, so each time sample contains only a small fraction of the information carried by an OFDM symbol. As a result, the modulation classifiers designed for single-carrier signals [6], [7] are not directly applicable to OFDM signals. Therefore, an accurate modulation classifier for Wi-Fi 6 and 5G signals requires additional processing beyond using raw time-domain samples as inputs.

In contrast to a dedicated receiver (RX) as a node in a wireless network, a spectrum sensor must be able to handle OFDM signals with diverse subcarrier configurations without access to prior information about the transmission format. In Wi-Fi 6 and 5G systems, information about the user data transmission, including the modulation, is provided to the RX through a protocol-specific procedure. However, since a spectrum sensor does not have prior knowledge of the type of signals it detects, it cannot deploy the procedure to obtain user data transmission information. The parameters shaping OFDM signals, fast Fourier transform (FFT) size to generate inverse fast Fourier transform (IFFT) sequence, and cyclic prefix (CP) length, might be different even among OFDM signals with the same modulation scheme. The diverse parameter options complicate the Wi-Fi preamble structure and in the recent Wi-Fi 6 these become more diverse. This makes spectrum sensing harder only with Wi-Fi preamble to identify the modulation scheme, even though the preamble structure is known. Moreover, the carrier frequency configurations in 5G become increasingly diverse and data transmission might occupy only a part of channel bandwidth. As a result, estimation of these carrier frequency configurations is becoming increasingly difficult using transmission bandwidth and center frequency alone. Thus, a modulation classifier for spectrum sensing should estimate the modulation scheme using only the observed user data transmission without knowledge of the OFDM signal parameters including FFT size, CP length, and carrier frequency.

We propose and analyze a modulation classifier for Wi-Fi 6 [8] and 5G [9] for a spectrum sensing system. Without knowledge of the transmitter (TX) carrier frequency, Wi-Fi preamble, or 5G control information, the classifier exploits only the basic OFDM structure, IFFT sequence, and CP. This includes the estimation of OFDM parameters: CP length and subcarrier spacing (SCS), which is directly related to the FFT size of the IFFT sequence. We focus on identifying modulation schemes used in the payload of Wi-Fi 6 signals and the physical downlink shared channel (PDSCH) of 5G signals. Signals studied in this paper are single-input single-output (SISO). For 5G, they are in the frequency range 1 (FR1), whose frequency band is below 7.125 GHz.

For the SCS and CP length estimation, the cyclic autocorrelation function (CAF) is deployed. The capability of CAF to detect intervals of repeated sequences and repetition periods

enables the estimation of those parameters. We observe that symbol-level synchronization is not perfect if autocorrelation using CP is utilized only. Our preprocessing removes the effect of the synchronization error by using phase differences between phases of two adjacent OFDM symbols. The modulation classifier for Wi-Fi 6 and 5G signals should recognize high-order modulations such as 256QAM and 1024QAM since these state-of-the-art protocols include those schemes. We change the feature format to a histogram representing the distribution of the features so that the classifier can effectively capture high-order modulation characteristics.

Related work on modulation classification: Many papers address modulation classification for wireless communication signals [6], [7], [10]–[17]. The works in [10]–[15] study modulation classification of OFDM signals and achieve at least 78% accuracy at 20 dB SNR for an AWGN channel. It is assumed that the inputs start from the first sample of the OFDM symbol duration [10]–[12], [15], which requires detecting the timing of the Wi-Fi preamble or 5G synchronization signals. To apply this approach to a spectrum sensor, the sensor needs to follow protocol-specific procedures. Further, neither of these works is evaluated on real-world measured data.

Previous works on OFDM modulation classification without symbol-level synchronization [13], [14], [16], [17] and the algorithms [13], [14], [17] are evaluated with hardware-generated data. However, their algorithms [13], [14], [17] are not evaluated with high-order modulations such as 256QAM or 1024QAM, as used in Wi-Fi 6 and 5G. Moreover, since their classifier structures [13], [14] are designed to recognize only a fixed set of modulations, the overall structure needs to be re-designed to identify a new modulation scheme. The work [16] proposes the system to estimate SCS of OFDM signals and modulation of single-carrier signals jointly. Nonetheless, it does not estimate the modulation of OFDM signals. The neural network-based modulation classifiers [6], [7] study how environmental change affects classification performance for only the single-carrier signals, not OFDM signals.

Related work on sniffing OFDM signals: One approach to modulation identification for spectrum sensing uses sniffing of control information which notifies the RX about modulation and coding formats. The work [18]–[21] attempts to overhear Long Term Evolution (LTE) signals. LTEye [18] and OWL [19] decode PHY DL control channel (PDCCH) data for LTE network monitoring. LTESniffer [21] decodes sniffed both user and control data using the PDCCH decoder FALCON [20]. FALCON overcomes the limitation of LTEye and OWL, which require more than 97% decoding accuracy. In LTE, the starting symbol of the PDCCH is always the first symbol in a slot. This is different from 5G, where the PDCCH starting symbol can be any symbol in a slot and its information is notified by radio resource control (RRC) signaling. Accordingly, it is not straightforward to modify the LTE PDCCH sniffer for 5G. Eavesdropping PDCCH data of 5G signals [22] applies to 5G signals with diverse configurations. Still, it is vulnerable to configuration changes since it takes a few minutes to learn a new PDCCH configuration. The authors

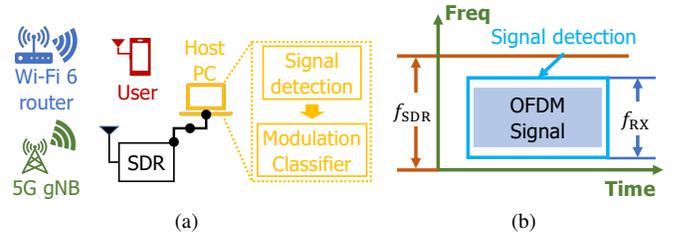


Fig. 1. (a) To capture DL Wi-Fi 6 and 5G signals and (b) Spectrum sensing scenario using USRP N310.

of [23] study sniffing Wi-Fi probe request packets, which is for mobile devices to broadcast the existence of themselves. They build a hardware model for a sniffer and test with real Wi-Fi probe request packets. However, the probe request packets are simpler in format than those for user data communication. Thus, it is not straightforward to deploy this approach to our setting.

To summarize, the main contributions of the paper are:

- **OFDM parameter estimation for up-to-date protocols:** We have applied the OFDM parameter estimation method with CAF [24] to Wi-Fi 6 and 5G signals to estimate SCS and CP length.
- **Feature extraction without symbol-level synchronization:** Only with estimated values of SCS and CP length, our system builds the features characterizing modulation of OFDM signals. The proposed feature extraction algorithm is designed to be resilient to symbol-level synchronization errors caused by using CP only.
- **Modulation classification without control information:** For spectrum sensing, control information might not be accessible. We show that the proposed classification system robustly works with diverse configurations with the evaluation of hardware-generated data without knowledge of the information.

II. SYSTEM OBJECTIVE

We aim to build a modulation classifier using IQ samples of SISO Wi-Fi 6 and FR1 5G DL signal for spectrum sensing. The system scenario is described in Fig. 1a. There is a Wi-Fi 6 or 5G TX transmitting its signal to an RX. SDR continuously senses the spectrum by generating IQ samples with sampling rate f_{SDR} and transfers those samples to the host PC. In the host PC, there is a signal detection algorithm and a modulation classifier. Using IQ samples generated from SDR, the signal detection algorithm detects the duration and frequency band where the OFDM signal is located and extracts IQ samples corresponding to the detected OFDM signal, described as the blue rectangle in Fig. 1b. We assume the accurate signal detection of Wi-Fi 6 or 5G signals and a single modulation scheme is used for data communication in one detected OFDM signal.

The IQ samples from SDR sampled with rate f_{SDR} are resampled to f_{RX} , 20 MHz. We only consider Wi-Fi 6 signals with 20 MHz channel bandwidth and 5G signals with a PDSCH bandwidth from 15 to 20 MHz. Thus, a 20 MHz

TABLE I
VARIABLE DEFINITIONS

Variable	Definition (unit)
f_{TX}	TX sampling rate (Hz)
f_{RX}	Sampling rate of a system input sequence (Hz)
Δf_{SCS}	Subcarrier spacing (Hz)
T_{IFFT}	IFFT sequence duration (s)
N_{FFT}	FFT size used to generate IFFT sequence
T_{CP}	CP duration (s)
N_{CP}	Number of time samples in CP for one OFDM symbol
$y[n]$	Received time-domain sequence after resampling to 20 MHz
$y'[n]$	5G time-domain sequence after resampling to 30.72 MHz
$y^s[n]$	Received time-domain IFFT sequence for the s th OFDM symbol
$Y^s[k]$	Received symbol in subcarrier k for the s th OFDM symbol
$(S \times S)$	Number of bins in a 2D histogram

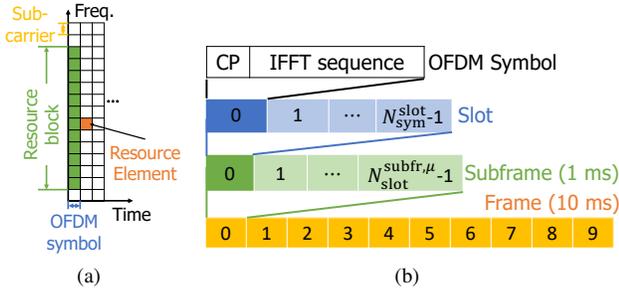


Fig. 2. 5G Resource structure: (a) Resource grid and (b) Frame structure.

sampling rate can let the resampled IQ sequence encompass the OFDM signal in our scenario. Extending the analysis to different transmission bandwidth ranges is straightforward. These resampled IQ samples, denoted by $y[n]$, are taken as inputs of the feature extraction algorithm, as elaborated in Sec. III in detail.

A. Wi-Fi 6 PHY layer

Wi-Fi 6 supports the high-efficiency (HE) transmission format as well as earlier formats, which are non-high throughput (non-HT), high throughput (HT), and very high throughput (VHT) formats. Table II summarizes the parameters that configure the payload of the Wi-Fi frame for each Wi-Fi format. In HE format, given channel bandwidth, the number of subcarriers is increased because the SCS (denoted as Δf_{SCS}) is one-fourth of that of the previous transmission formats. Over time, the Wi-Fi standard has evolved and several options for the CP duration are available.

B. 5G DL PHY layer

The 5G downlink (DL) resource structure and its associated terminology is illustrated in Fig. 2. A resource element (RE), illustrated in Fig. 2a, represents the smallest unit that carries data, encompassing a single OFDM symbol in the time domain and a single subcarrier in the frequency domain. A resource block (RB) is the smallest radio resource that can be allocated and refers to one OFDM symbol in the time domain and 12 subcarriers in the frequency domain.

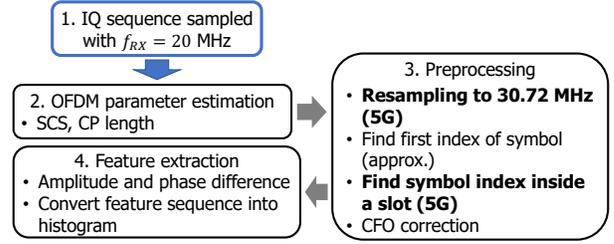


Fig. 3. Flow chart of proposed modulation classification algorithm.

Fig. 2b shows the 5G frame structure in the time domain. An OFDM symbol in 5G is comprised of both a CP and an IFFT sequence. The number of symbols within a single slot (N_{sym}^{slot}) varies following the CP length. There are normal and extended CP options in the transmission format. When a normal CP is used then $N_{sym}^{slot} = 14$, otherwise $N_{sym}^{slot} = 12$. The SCS, the distance between two adjacent subcarriers in OFDM systems, determines the number of slots within a single subframe, $N_{slot}^{subfr, \mu}$. μ represents an SCS option and corresponds to $\Delta f_{SCS} = 15 \times 2^\mu$ kHz. There are five SCS options in 5G, but we consider only three cases, namely 15, 30, and 60 kHz, which are available in FR1. The number of slots in a subframe for each SCS is computed as $N_{slot}^{subfr, \mu} = 2^\mu$. Finally, one frame of duration 10 ms consists of ten subframes.

The structural parameters that define the 5G frame are listed in Table III. The length of an IFFT sequence, T_{IFFT} , is:

$$T_{IFFT} = N_{FFT}/f_{TX} = 1/\Delta f_{SCS}. \quad (1)$$

There is a one-to-one correspondence between T_{IFFT} and Δf_{SCS} (1). Under the normal CP option, CP is longer than that in other symbols, every 0.5 ms, or equivalently, $7 \cdot 2^\mu$ OFDM symbols in OFDM symbol unit, called long CP. There is no long CP in the extended CP option, so T_{CP} is uniform. The transmission rate of 5G signals is a power of 2 times 15 kHz and 30.72 MHz is an example of a 5G transmission rate. N_{FFT} and N_{CP} values are arranged when f_{TX} is 30.72 MHz, the value used in our evaluation.

In addition to PDSCH, there exist other physical (PHY) channels that serve specific functions although not carrying user data. For instance, PDCCCH conveys downlink control information (DCI), which contains information required to decode PDSCH data such as modulation and coding scheme (MCS). Each of these channels utilizes predefined single-type modulation, see Table IV.

Compared to Wi-Fi, which has a predefined configuration of data, pilot, and null subcarriers, 5G resource configuration for PHY channels is flexible. Instead, the 5G system has a network dedicated to exchanging information on how data packets are forwarded, called the control plane, in addition to the network for data transmission, called the user plane. An example of data transferred over the control plane is RRC signals. Information on the starting OFDM symbol of PDCCCH and channel state information-reference signal (CSI-RS) is notified to an RX with RRC signals via control plane [9].

TABLE II
PARAMETERS FOR DIFFERENT FORMATS OF WI-FI

	Non-HT format	HT format	VHT format	HE format
T_{IFFT}	3.2 μs	3.2 μs	3.2 μs	12.8 μs
T_{CP}	0.8 μs	{0.4, 0.8} μs	{0.4, 0.8} μs	{0.8, 1.6, 3.2} μs
Modulations	BPSK, QPSK, 16QAM, 64QAM	BPSK, QPSK, 16QAM, 64QAM	BPSK, QPSK, 16QAM, 64QAM, 256QAM	BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM

TABLE III
5G FRAME STRUCTURE PARAMETERS

{SCS (kHz), CP option}	{60, Normal}	{60, Extended}	{30, Normal}	{15, Normal}
T_{IFFT}	16.17 μs	16.67 μs	33.33 μs	66.67 μs
{Short, long} T_{CP}	{1.17, 1.69} μs	{4.17, -} μs	{2.34, 2.86} μs	{4.69, 5.21} μs
N_{FFT} when $f_{\text{TX}} = 30.72$ MHz	512	512	1024	2048
{Short, long} N_{CP} when $f_{\text{TX}} = 30.72$ MHz	{36, 52}	128	{72, 88}	{144, 160}

TABLE IV
MODULATIONS USED FOR 5G PHYSICAL CHANNELS

Physical channel	PDSCH	PSS/SSS	PDCCH	CSI-RS	PBCH	PDSCH-PTRS	PDSCH-PTRS
Modulation	QPSK, 16QAM, 64QAM, 256QAM, 1024QAM	BPSK	QPSK	QPSK	QPSK	QPSK	QPSK

III. PROPOSED ALGORITHM

High-level procedures to build features characterizing the modulations of Wi-Fi 6 and 5G signals are illustrated in Fig. 3 and explained in Sec. III-A and III-B with additional processing for 5G signals in Sec. III-C. The 2D histogram is then taken as an input to the neural network model, described in Sec. III-D.

A. OFDM parameter estimation

Before building the features that characterize modulation, it is necessary to estimate two essential OFDM parameters of OFDM signals, SCS and CP length. To estimate these parameters, we use CAF, a Fourier-series coefficient of the autocorrelation function,

$$\mathcal{R}_{yy}(\alpha, \tau) = \sum_{n=-\infty}^{\infty} \mathcal{R}_{yy}(n, \tau) e^{-j2\pi\alpha n}. \quad (2)$$

CAF is used to extract a repeated pattern presented in wireless signals [24]–[26]. A variant of the CAF estimator presented in [24] is deployed here,

$$\hat{\mathcal{R}}_{yy}(\alpha, \ell) = \frac{1}{\mathcal{L} - l - \ell + 1} \sum_{n=0}^{\mathcal{L}-l-\ell} \left\{ \sum_{i=0}^{l-1} y[n+i] y^*[n+i+\ell] \right\} \times e^{-j2\pi\alpha n}, \quad (3)$$

where α is a cycle frequency and \mathcal{L} is the length of $y[n]$. One sample of our estimator is computed as the autocorrelation with delay ℓ . It differs from the estimator in [24], which corresponds to $l = 1$ in (3). The increase in the length of a sample sequence $y[n+i]$ aims to make peaks more distinct. We set $l = 8$ corresponding to the shortest CP length in our scenario.

CP in OFDM symbols causes a sequence to be repeated at both ends of each symbol. The distance between starting indices of the two repeated sequences at both ends of an

OFDM symbol is T_{IFFT} in time units or $N_{\text{FFT}}(f_{\text{RX}}/f_{\text{TX}}) = f_{\text{RX}}/\Delta f_{\text{SCS}}$ in time sample units. This repetition makes the CAF estimator at $\alpha = 0$ have a peak at $\ell = f_{\text{RX}}/\Delta f_{\text{SCS}} \cdot T_{\text{CP}}$. T_{CP} is also estimated with the CAF estimator, $\hat{\mathcal{R}}_{yy}(\alpha, f_{\text{RX}}/\Delta f_{\text{SCS}})$. Since $\sum_{i=0}^{l-1} y[n+i] y^*[n+i+\ell]$ in (3) has peaks at period of $f_{\text{RX}}(T_{\text{CP}} + 1/\Delta f_{\text{SCS}})$, it is expected of $\hat{\mathcal{R}}_{yy}(\alpha, f_{\text{RX}}/\Delta f_{\text{SCS}})$ to have a large amplitude at $\alpha = 1/\{f_{\text{RX}}(T_{\text{CP}} + 1/\Delta f_{\text{SCS}})\}$.

In our scenario, there are five candidates ℓ values, $\ell_C = \{64, 256, 333, 667, 1333\}$, each corresponding to an IFFT sequence length for a given SCS at $f_{\text{RX}} = 20$ MHz. IFFT sequence length is estimated as:

$$T_{\text{IFFT}} = \ell' / f_{\text{RX}} \quad \text{s.t.} \quad \ell' = \arg \max_{\ell \in \ell_C} |\hat{\mathcal{R}}_{yy}(0, \ell)| \quad (4)$$

When the estimated T_{IFFT} corresponds to that of Wi-Fi 6 or 60 kHz SCS NR, where multiple CP options are available, CP length is further estimated as:

$$T_{\text{CP}} = \frac{1}{f_{\text{RX}}} \left(\frac{1}{\alpha'} - \ell' \right) \quad \text{s.t.} \quad \alpha' = \arg \max_{\alpha \in \alpha_C'} |\hat{\mathcal{R}}_{yy}(\alpha, \ell')| \quad (5)$$

where α_C' denotes a set of possible values of $\alpha = 1/\{\ell' + (f_{\text{RX}} \cdot T_{\text{CP}})\}$, given ℓ' .

B. Feature extraction

The motivation behind our proposed feature extraction lies in the observation that when a sampled time-domain sequence is contained within a single OFDM symbol s , the FFT of that sequence yields the original symbols with a phase drift that scales linearly with subcarrier index k and synchronization error Δn , as shown in

$$\begin{aligned} Y_{\Delta n}^s[k] &\triangleq \mathcal{F}(y^s[n - \Delta n]) \\ &= \sum_{n=0}^{N_{\text{FFT}}-1} y^s[n - \Delta n] e^{-j2\pi nk / N_{\text{FFT}}} \\ &= Y^s[k] e^{-j2\pi \Delta n k / N_{\text{FFT}}}. \end{aligned} \quad (6)$$

To build a feature characterizing modulation based on this property, two objectives must be achieved: first, sampling a sequence fully contained in an OFDM symbol, and second, removing the phase drift caused by synchronization errors.

Utilizing the knowledge of N_{CP} and N_{FFT} , the CP position is determined through autocorrelation analysis,

$$R_{yy}(m, N_{\text{FFT}}) = \frac{1}{N_{\text{CP}}} \sum_{i=0}^{N_{\text{CP}}-1} y[m+i]y^*[m+i+N_{\text{FFT}}], \quad (7)$$

where m is the first index of original sequence of autocorrelation $R_{yy}(m, N_{\text{FFT}})$. The position of CP is indicated by the peaks in $|R_{yy}(m, N_{\text{FFT}})|$ since it is expected that $|R_{yy}(m, N_{\text{FFT}})|$ peaks when m is the first index of CP. To locate a peak, we search for a sample whose amplitude is larger than both of its neighboring samples while ensuring that the minimum distance between two adjacent peaks is 90% of the OFDM symbol duration (i.e., $(256 + 64) \times 0.9 = 288$ -time samples for HE format with $3.2 \mu\text{s}$ CP), to avoid selecting undesired local peaks. The indices of peaks are denoted as $\{p'_0, \dots, p'_{S-1}\}$ for S potential OFDM symbols. Using those peaks, the first index of the OFDM symbol is estimated:

$$p = \text{Median}_i \{ \text{mod}(p'_i, N_{\text{FFT}} + N_{\text{CP}}) \}, \quad (8)$$

where $i \in \{0, \dots, j-1\}$. Noise and varying amplitudes of time samples can introduce small errors in the estimated CP position. To reliably sample the sequences contained in a single OFDM symbol, we deploy the sequence $\{y[p + N_{\text{CP}}/2], y[p + N_{\text{CP}}/2 + 1], \dots, y[p + N_{\text{CP}}/2 + N - 1]\}$. This sequence is entirely within a single OFDM symbol for estimation error of p below $N_{\text{CP}}/2$.

We demonstrated (6) that $Y_{\Delta n}^s[k]$ exhibits a phase drift, $e^{-j2\pi\Delta nk/N}$, while maintaining amplitude $Y^s[k]$. We compute the phase differences between successive potential symbols s and $s+1$ in subcarrier k to build the feature invariant of this phase drift due to synchronization errors as:

$$\begin{aligned} \Delta \angle Y_{\Delta n}^s[k] &\triangleq \angle Y_{\Delta n}^{s+1}[k] - \angle Y_{\Delta n}^s[k] \\ &= \angle \left\{ Y^{s+1}[k] e^{-j2\pi\Delta nk/N} \right\} - \angle \left\{ Y^s[k] e^{-j2\pi\Delta nk/N} \right\} \quad (9) \\ &= \angle Y^{s+1}[k] - \angle Y^s[k]. \end{aligned}$$

Despite Δn unknown, sequences with constant Δn are obtained by adjusting the interval between the starting indices of two sampled sequences to be one OFDM symbol. The feature used to identify the modulation type is

$$Y_f^s[k] \triangleq |Y_{\Delta n}^s[k]| e^{j\Delta \angle Y_{\Delta n}^s[k]}. \quad (10)$$

For Wi-Fi 6, the null subcarrier symbols are eliminated by discarding symbols with the N_{null} smallest average amplitudes.

In protocol-compliant reception, the Wi-Fi preamble and 5G PDSCH-phase tracking reference signal (PDSCH-DMRS) are deployed for CFO estimation. However, since not accessible to a spectrum sensor, the CP in each OFDM symbol is used for CFO estimation Δf_c , i.e.,

$$\angle (y[p + N_{\text{FFT}} + i] \cdot y^*[p + i]) = 2\pi\Delta f_c / \Delta f_{\text{SCS}}, \quad (11)$$

where $y[p + i]$ is in CP. We use $i \in \{ \lfloor N_{\text{CP}}/4 \rfloor, \dots, \lceil 3N_{\text{CP}}/4 \rceil \}$ so that the sequence $y[p + i]$

are entirely within CP unless estimation error of p exceeds $N_{\text{CP}}/4$. We determine CFO as the average of Δf_c (11) evaluated over multiple OFDM symbols. If the absolute value of the CFO is larger than $\Delta f_{\text{SCS}}/2$, the CFO cannot be accurately estimated due to aliasing. It is discussed in Sec. III-C.

C. Additional procedures for 5G signal

To build a modulation feature for 5G, 5G characteristics distinct from those of Wi-Fi, including a different transmission rate, long CP, and flexible usage of subcarriers, should be considered. First, the transmission rate of 5G signals is not $f_{\text{RX}} = 20 \text{ MHz}$, but is a power of 2 times 15 kHz. Hence, for the signal classified as 5G, we resample the sequence to $f_{5\text{G}} = 30.72 \text{ MHz} = 2048 \cdot 15 \text{ kHz}$, the smallest sampling frequency above 20 MHz. N_{FFT} and N_{CP} with 30.72 MHz sampling rate for each Δf_{SCS} are arranged in the last two rows in Table III.

In the case of the normal CP option, there is a long CP every $T_{\text{LCP}} = 0.5 \text{ ms}$, which is slightly longer than that of other OFDM symbols. Long CP breaks the assumption of uniform OFDM symbol duration, which is required by the method to find the first indices of OFDM symbols and estimate CFO. Moreover, in building $Y_f^s[k]$, maintaining the fixed interval does not guarantee the constant Δn over multiple OFDM symbols. Therefore, long CP also should be located when finding the first index of the OFDM symbol.

Algorithm 1: Finding first index of long CP in 5G

Data: ($y'[n]$ of length (3 ms + 3 OFDM symbols)), μ
1 $M = 7 \cdot 2^\mu$, $N_{\text{FFT}} = 512 \cdot 2^{2-\mu}$, $N_{\text{CP}} = 18 \cdot 2^{2-\mu}$;
2 for $i = 0 : 5$ **do**
3 $\mathbf{y}'_i \triangleq \{y'[f_{5\text{G}}T_{\text{LCP}} \cdot i], \dots, y'[f_{5\text{G}}T_{\text{LCP}}(i + 1) + 2(N_{\text{FFT}} + N_{\text{CP}}) + N_{\text{CP}} - 1]\}$;
4 Find peaks $\{p'_{i0}, \dots, p'_{i(M-1)}\}$ with \mathbf{y}'_i using $|R_{\mathbf{y}'_i \mathbf{y}'_i}(m, N_{\text{FFT}})|$ and peak locating function in Sec. III-B;
5 $p_{ij} = \text{mod}(p'_{ij}, N_{\text{FFT}} + N_{\text{CP}})$;
6 end
7 $\Delta p_j = (\sum_{k=0}^5 \{p_{k(j+1)} - p_{k(j-1)}\})/6$ where $j \in \{1, 2, \dots, M\}$;
8 $\{\Delta p_{r_0}, \dots, \Delta p_{r_{M-1}}\} = \text{sortDescending}(\{\Delta p_j\})$;
9 $\text{symLongCP} = \arg \max_{r_q} \text{Var}(\{p_{0r_q}, \dots, p_{5r_q}\})$ where $q \in \{0, 1\}$;
10 $q_{ij} = \begin{cases} p_{ij} & \text{if } j \leq \text{symLongCP} \\ p_{ij} - 16 & \text{otherwise} \end{cases}$
 $q = \text{Median}_j(\sum_{k=0}^5 q_{kj}/6)$;
Result: $\text{IndexLongCP} = q + \text{symLongCP}(N_{\text{FFT}} + N_{\text{CP}})$

Algorithm 1 explains the detailed steps to estimate the first index of OFDM symbol with long CP. \mathbf{y}'_i in line 3 is a sequence cropped to be as long as (0.5 ms + 2 OFDM symbols + T_{CP}).

In line 4, we find $M + 2$ peaks from \mathbf{y}'_i using autocorrelation $|R_{\mathbf{y}'_i \mathbf{y}'_i}(m, N_{\text{FFT}})|$, where M denotes the number of OFDM symbols in T_{LCP} given μ and we also compute the

autocorrelation at the two symbols at each end. The M average differences between the remainders of two peaks separated by two OFDM symbols modulo OFDM symbol duration, Δp_j , are computed in line 7. We expect that Δp_j is the largest when p_j corresponds to long CP. For a more reliable estimation of a long CP, we add a criterion.

In line 10, we choose the two candidates k_0 and k_1 that give Δp_{k_i} the two largest values. We select k_q where the set $\{p_{0k_q}, \dots, p_{5k_q}\}$ has the larger variance between two candidates of k_q . This is because we expect that $\{p_{0j}, \dots, p_{5j}\}$ has the largest variance if p_{ij} corresponds to long CP since long CP makes $|R_{y'_i y'_i}(m, N_{\text{FFT}})|$ a plateau with some width. Using estimated **IndexLongCP**, we put an additional 16 samples delay at the OFDM symbol with long CP while extracting the feature $Y_f^s[k]$ to maintain uniform Δn . The number of 16 samples comes from the difference between long CP and non-long CP with a 30.72 MHz sampling rate.

In contrast to Wi-Fi 6 signals, some subcarriers might not be used for transmission amid transmission. If no transmission is made in $Y^s[k]$ or $Y^{s+1}[k]$, their phases are random, and $\Delta \angle Y_{\Delta n}^s[k]$ cannot be the phase difference between two constellation points. Therefore, we set the threshold for the amplitude, denoted as β , to check whether the RE is being used for transmission. Only when $|Y^s[k]|$ and $|Y^{s+1}[k]|$ are higher than β , $Y^s[k]$ is used.

The discrepancy between the center frequency of TX and that of received IQ samples of 5G signals might be much larger than for Wi-Fi. In contrast to Wi-Fi, which covers the entire channel bandwidth unless OFDMA is used, PDSCH in 5G might use only the part of channel bandwidth so the center frequency of PDSCH might be different from that used for transmission. Thus, the discrepancy is solely from hardware imperfection in Wi-Fi. For a Wi-Fi link operating at $f_c = 5$ GHz and a frequency tolerance of 1 ppm for commercial-off-the-shelf temperature-compensated crystal oscillators [27] on both sides of the Wi-Fi link, the worst-case CFO is $\Delta f_c = 2f_c \cdot 10^{-6} = 10$ kHz. However, in 5G, the CFO can escalate to an MHz scale if we consider the center frequency of transmission bandwidth to be carrier frequency. If the method presented earlier in this section is employed, the difference could result in an inaccurate estimation of CFO due to aliasing. Even in the absence of noise, it is only possible to measure Δf_c accurately up to $\Delta f_{\text{SCS}}/2$, since $\Delta f_c + z\Delta f_{\text{SCS}}$ cannot be distinguished from each other, where $z \in \mathbb{Z}$. The algorithm makes the corrected CFO a multiple of Δf_{SCS} , not a zero.

However, the CFO correction is still deployed for feature extraction. This is because even though this method cannot find the exact CFO, it can recover the orthogonality among subcarriers. The CFO effect in our feature is represented as:

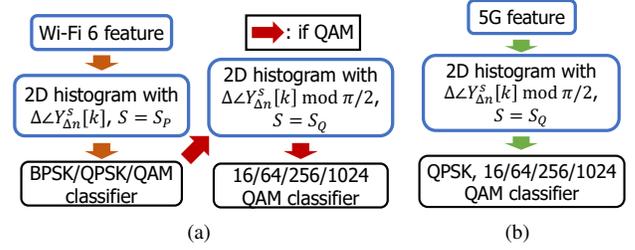


Fig. 4. Flow chart of proposed classifier system: (a) Wi-Fi 6 and (b) 5G.

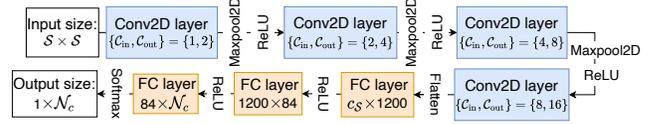


Fig. 5. CNN-based modulation classifier structure. N_c is the number of modulations a classifier aims to recognize.

$$\begin{aligned}
 Y_{\Delta n}^s[k] &= \sum_{n=0}^{N_{\text{FFT}}-1} y[n - \Delta n] e^{-j2\pi n(\Delta f_c/f_{\text{TX}} + k/N_{\text{FFT}})} \\
 &= Y^s[k + N_{\text{FFT}}\Delta f_c/f_{\text{TX}}] \times \\
 &\quad e^{-j2\pi\Delta n(k/N_{\text{FFT}} + \Delta f_c/f_{\text{TX}})} \\
 Y_{\Delta n}^{s+1}[k] &= Y^{s+1}[k + N_{\text{FFT}}\Delta f_c/f_{\text{TX}}] \times \\
 &\quad e^{-j2\pi(\Delta n k/N_{\text{FFT}} + (\Delta n + (N_{\text{FFT}} + N_{\text{CP}})\Delta f_c/f_{\text{TX}}))} \\
 \Rightarrow \Delta \angle Y_{\Delta n}^s[k] &= \angle Y^{s+1}[k + \Delta f_c/\Delta f_{\text{SCS}}] \\
 &\quad - \angle Y^s[k + \Delta f_c/\Delta f_{\text{SCS}}] \\
 &\quad - 2\pi\Delta f_c(1/\Delta f_{\text{SCS}} + T_{\text{CP}}).
 \end{aligned} \tag{12}$$

To maintain orthogonality of $\angle Y_{\Delta n}^s[k]$ across k , $\Delta f_c/\Delta f_{\text{SCS}}$ should be an integer. We have demonstrated that after the CFO correction using CP, the CFO is expressed as $z \cdot \Delta f_{\text{SCS}}$, which renders $\Delta f_c/\Delta f_{\text{SCS}}$ to be an integer. Consequently, the phase of our feature becomes the sum of a phase difference of originally transmitted symbols and a phase caused by the CFO. Since $\Delta \angle Y_{\Delta n}^s[k]$ in (12) contains T_{CP} term, the CFO effect on $\Delta \angle Y_{\Delta n}^s[k]$ is different when OFDM symbol $s+1$ is an OFDM symbol with long CP. To make the CFO effect uniform in the feature, $\Delta \angle Y_{\Delta n}^s[k]$ where OFDM symbol $s+1$ is an OFDM symbol with long CP is not used for building the feature.

The features may contain the effect of other PHY channels that use modulations other than those used by PDSCH. It is impossible to perfectly filter out the effect because information about which REs were used for which PHY channels is not accessible for spectrum sensors. However, since the modulations of other PHY channels are either BPSK or QPSK, the constellation diagram of the features is only affected by changes in PDSCH modulation. Thus, the distribution of phase differences is still an intrinsic characteristic of PDSCH modulation.

D. Neural network classifier

The obtained feature $Y_f^s[k]$ goes through two preprocessing steps to become input to the classifier:

1) instead of $\Delta \angle Y_{\Delta n}^s[k]$, $\Delta \angle Y_{\Delta n}^s[k]$ modulo $\pi/2$ is used as a phase of $Y_f^s[k]$. A constellation diagram of every target

TABLE V
DL MODEL PARAMETERS

Batch size	32	Learning rate	$5 \cdot 10^{-5}$
Epochs	200	Loss	Cross-entropy

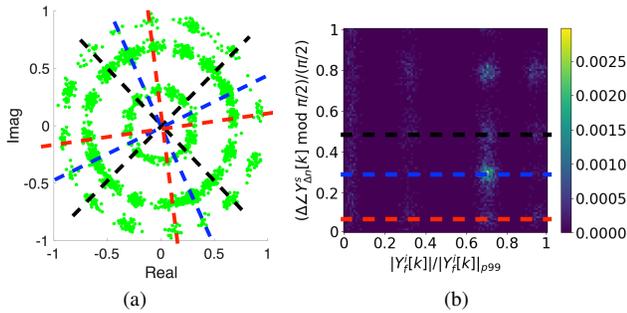


Fig. 6. Measured 16QAM features at SNR= 25 dB with 5G OTA data: (a) Scatterplot of $Y_f^s[k]$ and (b) Corresponding histogram of $|Y_f^s[k]|/|Y_f^s[k]|_{p99}$ and $(\Delta\angle Y_{\Delta n}^s[k] \bmod \pi/2)/(\pi/2)$.

modulation and corresponding features $Y_f^s[k]$ without noise are rotationally symmetric with $\pi/2$. Thus, $\Delta\angle Y_{\Delta n}^s[k]$ modulo $\pi/2$ is used as a phase of our feature to characterize a modulation. For Wi-Fi 6 signals, BPSK cannot be distinguished from QPSK if $\Delta\angle Y_{\Delta n}^s[k]$ modulo $\pi/2$ is used. Thus, an additional classifier with the original phase as an input is used to distinguish BPSK and QPSK from the high-order QAM modulations, see Fig. 4.

2) A 2D histogram of the normalized amplitude of the features $|Y_f^s[k]|/|Y_f^s[k]|_{p99}$, where $|Y_f^s[k]|_{p99}$ denotes 99th percentile of $|Y_f^s[k]|$ in a single data, and the phases $\angle Y_f^s[k]/2\pi$, as an input for the classifier. The histogram value of each bin is computed as:

$$Z(u, v) = \text{The number of } Y_f^s[k] \text{ s.t.} \\ u/S \leq |Y_f^s[k]|/|Y_f^s[k]|_{p99} \leq (u+1)/S \text{ and} \quad (13) \\ v/S \leq \Delta\angle Y_{\Delta n}^s[k]/\phi \leq (v+1)/S.$$

If $\Delta\angle Y_{\Delta n}^s[k]$ modulo $\pi/2$ is used, ϕ is $\pi/2$, otherwise 2π . We normalize histogram value to be classifier input:

$$Z'(u, v) = Z(u, v)/Z, \quad (14)$$

where Z denotes the number of valid $Y_f^s[k]$ in one data. To remove outliers, $Y_f^s[k]$ whose amplitude is larger than $|Y_f^s[k]|_{p99}$ was not included in the histogram.

The overall structure and the parameter of the classifier with the histogram input are summarized in Fig. 4 and Table V. The neural network structure used for each classifier is described in Fig. 5. C_{in} and C_{out} in Conv2D layers correspond to the number of input and output depth. A 2×2 size kernel is used in every Conv2D and Maxpool2D layer. N_c is the number of modulations that a classifier aims to recognize. For the classifier to identify BPSK and QPSK, the third Maxpool layer is not used, $S = S_P$, and $N_c = 3$. The classifier for 5G and for identifying the QAM types for Wi-Fi 6 use $N_c = 5, 4$, respectively.

For 5G 16QAM real-world measured over-the-air (OTA) data, Fig. 6a shows a scatterplot of the IQ data of $Y_f^s[k]$ and Fig. 6b the corresponding 2D histogram with $\Delta\angle Y_{\Delta n}^s[k]$

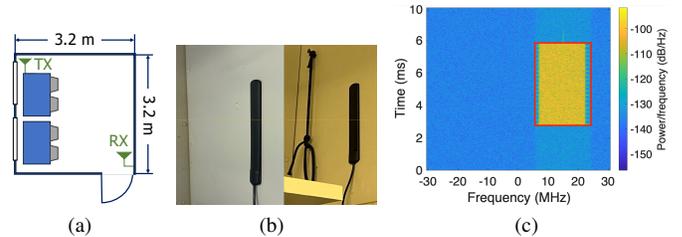


Fig. 7. OTA data propagation environment: (a) map with TX/RX locations, (b) vertically polarized antennas for TX (left) and RX (right), attached to the wall, and (c) Example spectrogram from data observed by USRP N310.

TABLE VI
DATA GENERATION PARAMETERS

SNR	AWGN data: [5, 40] dB in steps of 5 dB OTA data: [4, 32] dB in steps of 4 dB
Carrier frequency	2.4 GHz (Wi-Fi 6), 2.6 GHz (5G)
The number of {train, test} data	{800, 200} per each ($T_{IFFT}, T_{CP}, \text{modulation}$) case
{S_P, S_Q}	{15, 50}
Time duration of each data	400 μ s (Wi-Fi 6), 5 ms (5G)

modulo $\pi/2$. $\angle Y_f^s[k]$ on the red and black dashed lines are the sum of the noise-free phase differences between two 16QAM constellation points and the phase shift caused by CFO. Blue dashed lines are from the phase differences between BPSK or QPSK symbols of the PHY channel other than PDSCH and the shift by CFO. The red, blue, and black dashed lines in Fig. 6a correspond to the red, blue, and black dashed lines in Fig. 6b, respectively. Fig. 6a and Fig. 6b show that symbols are densely located at the points in the dashed lines, which is consistent with our expectations.

An advantage of using a histogram is that they are invariant to the length of $Y_f^s[k]$. This enables a neural network with a fixed structure to handle signals of any duration. This property is useful when dealing with 5G features where the number of samples of $Y_f^s[k]$ is unknown due to unused resources. Moreover, in a histogram input, the effect of CFO estimation error caused by aliasing (12) is a movement along the y-axis of the histogram as far as orthogonality of $\angle Y_{\Delta n}^s[k]$ across k holds. The neural network can be trained to identify histogram movements along the y-axis as a single class.

IV. EVALUATION

A. Data collection

The proposed classifier is evaluated with synthetic data generated from AWGN channel simulations and real-world measured OTA data with the details in Table VI. MATLAB R2023a WLAN and 5G toolbox [28] are deployed to generate the synthetic AWGN dataset. Wi-Fi HT [29] and HE format [8] are used to generate data with $T_{IFFT} = 3.2 \mu$ s and 12.8μ s in Wi-Fi 6. For 5G data, every SCS option in FR1, $\mu \in \{0, 1, 2\}$, is tested. All PHY channels listed in Table IV are included in every 5G data item.

To evaluate whether the performance of the proposed system remains invariant across varying 5G PHY channel configurations, the parameters for allocating REs to PHY channels are

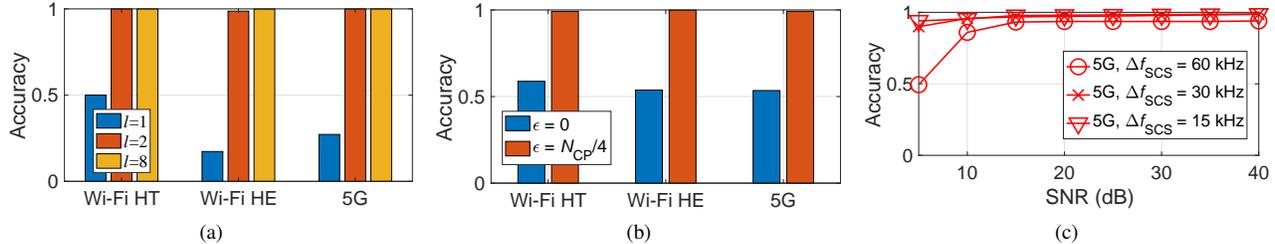


Fig. 8. Results with synthetic AWGN channel data: (a) Accuracy for estimating $T_{1\text{FFT}}$ and T_{CP} , (b) Accuracy for choosing the first index of CP with acceptable error ϵ , and (c) Accuracy for finding an OFDM symbol with long CP of 5G signals.

set for each data. For example in PDCCH, symbol duration, aggregation level, and starting symbol number are randomly selected. PHY broadcast channel (PBCH), primary synchronization signal (PSS), and secondary synchronization signal (SSS) are included only when $\mu \in \{0, 1\}$ since they are not available for $\mu = 2$. The other 5G PHY channel parameters are from FR1 test models in [30], [31].

Figure 7 documents the propagation environment where OTA data are measured. We deploy two networked software-defined radios, USRP N310 [32], for transmitting and receiving signals OTA. Both TX and RX are in the same room and the distance between TX and RX is 4.52 m, see Fig. 7a. TX and RX antenna are attached to the wall, see Fig. 7b. Fig. 7c shows a spectrogram with a 5G signal detected. Utilizing the assumed accurate signal detection, an IQ sequence corresponding to a detected signal (red box in Fig. 7c) is extracted. After resampling to 20 MHz ($y[n]$), the sequence is taken as an input of the OFDM parameter estimator.

B. Building classifier input

First, to avoid using the Wi-Fi preamble, we remove the first 2000 samples from each data. If the estimated $T_{1\text{FFT}}$ corresponds to those of Wi-Fi 6, an IQ sequence whose length corresponds to 40+2 or 10+2 OFDM symbols is deployed to build $Y_f^s[k]$, starting with a random sample. We need an additional OFDM symbol due to the unknown starting index of an OFDM symbol sequence, $p \in [0, N_{\text{FFT}} + N_{\text{CP}} - 1]$. One more symbol is required since phase differences between those of every OFDM symbol and the next one should be computed. N_{null} is set to 8 and 32 for Wi-Fi HT and HE, respectively. If the estimated $T_{1\text{FFT}}$ refers to 5G, $y'[n]$ of length (3 ms + 3 OFDM symbols) is used to estimate p and **IndexLongCP**.

For 5G, the sequence of 14 OFDM symbols is utilized for a classifier input. β is set to $|Y_f^s[k]|_{p99}/10$ in each input. We also evaluate $Y_f^s[k]$ values as an input to assess how much the histogram input contributes to the performance. In this case, one data input consists of 2240 samples for Wi-Fi 6 or 7900 samples for 5G, which is the average number of feature elements in a single 5G histogram data. We use fixed-duration data for a fair comparison, but the classifier can take the variable length data as input as the obtained feature is processed to a histogram using the algorithms in Sec. III-D. For both input formats, an input with both phases of $\angle Y_{\Delta n}^s[k]$ modulo $\pi/2$ and $\angle Y_{\Delta n}^s[k]$ are evaluated.

C. Evaluation results

TABLE VII
SNR REQUIRED FOR DATA COMMUNICATION WITH EACH MODULATION

Modulation	BPSK	QPSK	16QAM
SNR for Wi-Fi 6 (dB)	5	10	16
SNR for 5G (dB)	-	15	18
Modulation	64QAM	256QAM	1024QAM
SNR for Wi-Fi 6 (dB)	22	30	35
SNR for 5G (dB)	21	27	30

1) *AWGN channel data*: Results in Fig. 8 are obtained with synthetic AWGN channel data. Fig. 8a shows estimation accuracy of the OFDM parameters $\{T_{\text{CP}}, T_{1\text{FFT}}\}$ over different l , the length of $y[n+i]$ in CAF estimator (3). Using $l = 2, 4$ achieves 99% accuracy for both Wi-Fi 6 formats and 5G and outperforms $l = 1$ as used in [24]. In Fig. 8b, the estimation accuracy of *correctly finding* the starting index of an OFDM symbol is shown for the method in Sec. III-B. *Correctly finding* means that the starting index time is within ϵ samples tolerance of the true time. In Fig. 8b, we note that the estimation accuracy for identifying the starting index of an OFDM symbol falls below 60% for both Wi-Fi 6 formats and 5G. When the tolerance is relaxed to $N_{\text{CP}}/4$ time samples, the reported estimation accuracy increases to 99%.

The accuracy of estimating an OFDM symbol with long CP is shown in Fig. 8c. Aside from $\Delta f_{\text{SCS}} = 60$ kHz, the performance is over 90% even at low SNR of 5 dB. Accuracy at $\Delta f_{\text{SCS}} = 60$ kHz is low because the period of an OFDM symbol with long CP is larger than the others. The degraded peak detection performance due to the large number of symbols that the peak detection function needs to detect also negatively affects the estimation performance. At $\Delta f_{\text{SCS}} = 60$ kHz, 30 peaks should be identified in line 4 of Algorithm 1, which is considerably larger than the 9 or 16 peaks at $\Delta f_{\text{SCS}} = 15$ kHz and $\Delta f_{\text{SCS}} = 30$ kHz.

Figure 9 shows modulation classification accuracy with synthetic AWGN channel data. The proposed algorithm with a histogram input with the phases $\Delta \angle Y_{\Delta n}^s[k]$ modulo $\pi/2$ outperforms in all considered cases, except for Wi-Fi 6 at 5 dB SNR. The performance gap between using the histogram as classifier input as opposed to using the feature value input increases in Wi-Fi HE and even more so in 5G. This is because the histogram input helps the classifier to discriminate the detailed symbol constellation of high-order modulations.

2) *OTA data*: The modulation classification accuracy with measured OTA data is in Fig. 10. The achieved OTA accuracy

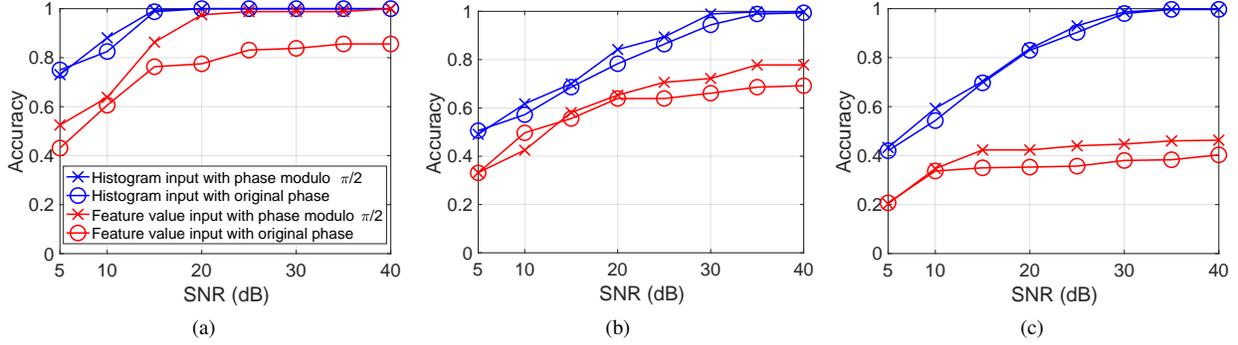


Fig. 9. Classification accuracy for modulations vs. SNR with synthetic AWGN channel data: (a) Wi-Fi HT, (b) Wi-Fi HE, (c) 5G.

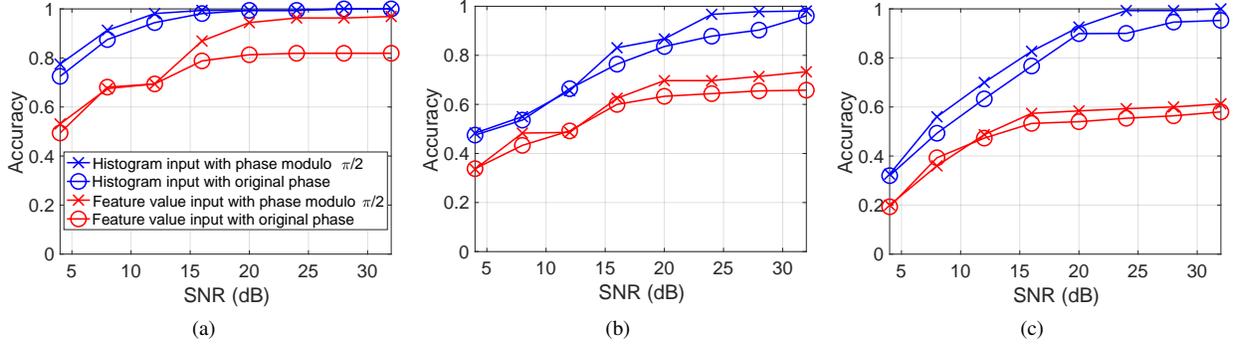


Fig. 10. Classification accuracy for modulations vs. SNR with OTA data. (a) Wi-Fi HT, (b) Wi-Fi HE, (c) 5G signals.

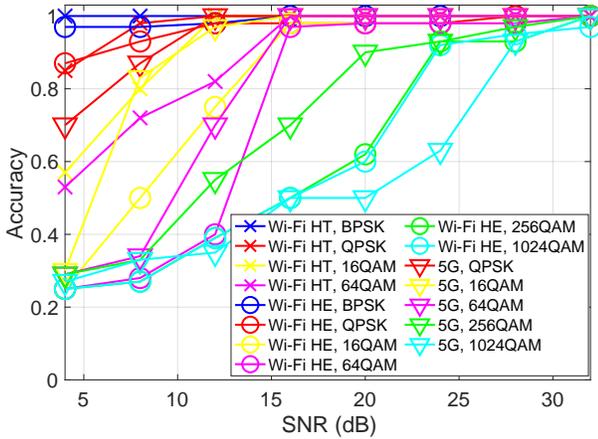


Fig. 11. Classification accuracy for modulation with OTA data for each modulation format separately.

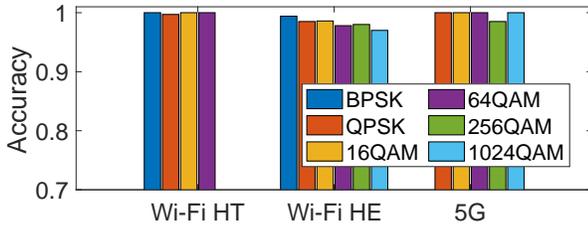


Fig. 12. Classifier accuracy with OTA data when SNR exceeds the minimum requirements required for standard-compliant data communication.

is similar to the synthetic AWGN channel data: a histogram input with the phases $\Delta Y_{\Delta n}^s[k]$ modulo $\pi/2$ achieves the highest classification accuracy, except for Wi-Fi 6 at 5 dB SNR and a larger performance gap for Wi-Fi HE and 5G.

The classification accuracy of all considered modulation for-

ats with OTA data is in Fig. 11. For a chosen accuracy, higher modulation orders require higher received SNR. E.g., Wi-Fi HE 16QAM signals have 90% accuracy if the SNR exceeds 16 dB, whereas Wi-Fi HE 256QAM requires 24 dB SNR. In Fig. 12, the accuracy of each modulation format is shown when the SNR satisfies the minimum requirement for standard-compliant data communication. We deploy error vector magnitude (EVM) levels required for data communication with each modulation for Wi-Fi 6 and 5G documentations [8], [31]. Required SNR values are calculated using the relation between EVM and SNR [33]. SNR required for the smallest coding rate are chosen for each modulation and chosen values are arranged in Table VII. For every modulation with both Wi-Fi 6 formats and 5G, accuracy is at least 97%.

V. CONCLUSION

Modulation classification of Wi-Fi 6 and 5G signals for spectrum sensing is studied. Simulations show that our classifier which uses SCS and CP length estimates based on the CAF achieves 99% accuracy. The classifier includes a preprocessing stage that is agnostic to control information, and extracts signal features characterizing modulation schemes insensitive to synchronization errors. For 5G signals, the preprocessing also estimates the symbol positions with a long CP. The features are converted to a more suitable form as inputs for the CNN-based classifier. This improves the classification of high-order modulation constellations. The modulation classifier identifies OFDM modulations with 97% accuracy when the SNR satisfies the requirements for standard-compliant data transmission for each modulation format with both synthetic AWGN channel data and measured OTA data.

REFERENCES

- [1] E. Björnson, E. G. Larsson, and M. Debbah, "Massive MIMO for maximal spectral efficiency: How many users and pilots should be allocated?" *IEEE Trans. on Wireless Commun.*, vol. 15, no. 2, pp. 1293–1308, 2016. doi: 10.1109/TWC.2015.2488634
- [2] K. V. Mishra, M. Bhavani Shankar, V. Koivunen, B. Ottersten, and S. A. Vorobyov, "Toward millimeter-wave joint radar communications: A signal processing perspective," *IEEE Signal Processing Mag.*, vol. 36, no. 5, pp. 100–114, 2019. doi: 10.1109/MSP.2019.2913173
- [3] N. Devroye, P. Mitran, and V. Tarokh, "Limits on communications in a cognitive radio channel," *IEEE Commun. Mag.*, vol. 44, no. 6, pp. 44–49, 2006. doi: 10.1109/MCOM.2006.1668418
- [4] J. Gao, X. Yi, C. Zhong, X. Chen, and Z. Zhang, "Deep learning for spectrum sensing," *IEEE Wirel. Commun. Letters*, vol. 8, no. 6, pp. 1727–1730, 2019. doi: 10.1109/LWC.2019.2939314
- [5] L. Yu, J. Chen, and G. Ding, "Spectrum prediction via long short term memory," in *Proc. IEEE ICC*, 2017, pp. 643–647.
- [6] V. Sathyanarayanan, P. Gerstoft, and A. El Gamal, "Rml22: Realistic dataset generation for wireless modulation classification," *IEEE Trans. on Wireless Commun.*, 2023. doi: 10.1109/TWC.2023.3254490
- [7] D. Liu, K. Ergun, and T. S. Rosing, "Towards a robust and efficient classifier for real world radio signal modulation classification," in *Proc. IEEE ICASSP*, 2023. doi: 10.1109/ICASSP49357.2023.10094907 pp. 1–5.
- [8] IEEE 802.11ax, "Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 1: enhancements for high-efficiency WLAN," May 2021.
- [9] 3GPP TR 38.331, "NR; Radio Resource Control (RRC); Protocol specification," Mar. 2023, ver 17.4.0.
- [10] S. Hong, Y. Zhang, Y. Wang, H. Gu, G. Gui, and H. Sari, "Deep learning-based signal modulation identification in OFDM systems," *IEEE Access*, vol. 7, pp. 114 631–114 638, Aug. 2019. doi: 10.1109/ACCESS.2021.3102223
- [11] D. H. Al-Nuaimi, N. A. M. Isa, M. F. Akbar, and I. S. Z. Abidin, "AMC2-pyramid: Intelligent pyramidal feature engineering and multi-distance decision making for automatic multi-carrier modulation classification," *IEEE Access*, vol. 9, pp. 137 560–137 583, Sept. 2021. doi: 10.1109/ACCESS.2021.3115888
- [12] Z. Zhang, H. Luo, C. Wang, C. Gan, and Y. Xiang, "Automatic modulation classification using cnn-lstm based dual-stream structure," *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 13 521–13 531, Nov. 2020.
- [13] R. Gupta, S. Kumar, and S. Majhi, "Blind modulation classification for asynchronous ofdm systems over unknown signal parameters and channel statistics," *IEEE Trans. Veh. Technol.*, vol. 69, no. 5, pp. 5281–5292, Mar. 2020. doi: 10.1109/TVT.2020.2981935
- [14] A. K. Pathy, A. Kumar, R. Gupta, S. Kumar, and S. Majhi, "Design and implementation of blind modulation classification for asynchronous mimo-ofdm system," *IEEE Trans. Instrum. Meas.*, vol. 70, pp. 1–11, Sept. 2021. doi: 10.1109/TIM.2021.3109737
- [15] S. Hong, Y. Wang, Y. Pan, H. Gu, M. Liu, J. Yang, and G. Gui, "Convolutional neural network aided signal modulation recognition in OFDM systems," in *Proc. IEEE VTC*, May 2020. doi: 10.1109/VTC2020-Spring48590.2020.9128455 pp. 1–5.
- [16] M. C. Park and D. S. Han, "Deep learning-based automatic modulation classification with blind OFDM parameter estimation," *IEEE Access*, vol. 9, pp. 108 305–108 317, 2021. doi: 10.1109/ACCESS.2021.3102223
- [17] A. Kumar, K. K. Srinivas, and S. Majhi, "Automatic modulation classification for adaptive OFDM systems using convolutional neural networks with residual learning," *IEEE Access*, vol. 11, pp. 61 013–61 024, Jun. 2023. doi: 10.1109/ACCESS.2023.3286939
- [18] S. Kumar, E. Hamed, D. Katabi, and L. Erran Li, "Lte radio analytics made easy and accessible," *Proc. ACM SIGCOMM*, vol. 44, no. 4, pp. 211–222, Aug. 2014. doi: 10.1145/2740070.2626320. [Online]. Available: <https://doi.org/10.1145/2740070.2626320>
- [19] N. Bui and J. Widmer, "Owl: A reliable online watcher for lte control channel measurements," in *Proc. 5th Workshop on All Things Cellular: Operations, Applications and Challenges*. New York (NY), USA: Association for Computing Machinery, 2016. doi: 10.1145/2980055.2980057. ISBN 9781450342490 pp. 25–30. [Online]. Available: <https://doi.org/10.1145/2980055.2980057>
- [20] R. Falkenberg and C. Wietfeld, "FALCON: An accurate real-time monitor for client-based mobile network data analytics," in *Proc. IEEE GLOBECOM*. Waikoloa (HI), USA: IEEE, 2019. doi: 10.1109/GLOBECOM38437.2019.9014096 pp. 1–7.
- [21] T. D. Hoang, C. Park, M. Son, T. Oh, S. Bae, J. Ahn, B. Oh, and Y. Kim, "Ltesniffer: An open-source lte downlink/uplink eavesdropper," in *Proc. 16th ACM Conf. on Security and Privacy in Wireless and Mobile Networks (WiSec)*, Guildford, UK, May 29–Jun. 1 2023. doi: 10.1145/3558482.3590196 pp. 43–48.
- [22] N. Ludant, P. Robyns, and G. Noubir, "From 5g sniffing to harvesting leakages of privacy-preserving messengers," in *2023 IEEE Symposium on Security and Privacy (SP)*. Los Alamitos, CA, USA: IEEE Computer Society, may 2023. doi: 10.1109/SP46215.2023.00110 pp. 1919–1934. [Online]. Available: <https://doi.ieeecomputersociety.org/10.1109/SP46215.2023.00110>
- [23] Y. Li, J. Barthelemy, S. Sun, P. Perez, and B. Moran, "A case study of wifi sniffing performance evaluation," *IEEE Access*, vol. 8, pp. 129 224–129 235, 2020. doi: 10.1109/ACCESS.2020.3008533
- [24] A. Punchihewa, V. K. Bhargava, and C. Despins, "Blind estimation of OFDM parameters in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, pp. 733–738, Mar. 2011. doi: 10.1109/TWC.2010.010411.100276
- [25] S. S. Hong and S. R. Katti, "Dof: A local wireless information plane," in *Proc. ACM SIGCOMM*, 2011. doi: 10.1145/2018436.2018463 pp. 230–241.
- [26] W. A. Gardner and C. M. Spooner, "The cumulant theory of cyclostationary time-series. I. Foundation," *IEEE Trans. Signal Process.*, vol. 42, no. 12, pp. 3387–3408, Dec. 1994. doi: 10.1109/78.340775
- [27] G. E. Ltd. (2023) GTXO-203T | 1.8V~3.6V SM TCXO | Gollodge. [Online]. Available: <https://www.gollodge.com/products/gtxo-203t-ultra-miniature-tight-stability-tcxo/c-26/p-287/>
- [28] MathWorks. (2023) MATLAB Products. [Online]. Available: <https://www.mathworks.com/products.html/>
- [29] IEEE 802.11n, "Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications amendment 5: enhancements for higher throughput," Oct. 2009.
- [30] 3GPP TR 38.521-4, "NR; User Equipment (UE) conformance specification; Radio transmission and reception; Part 4: Performance requirements," 2023, ver 17.2.1.
- [31] 3GPP TR 38.141-1, "NR; Radio Resource Control (RRC); Base Station (BS) conformance testing; Part 1: Conducted conformance testing," 2023, ver. 18.1.0.
- [32] Ettus Research, "USRP N300/N310," in *Knowledge Base*. Ettus Research, 2018–2022, last accessed 2023-07-01. [Online]. Available: <https://kb.ettus.com/N300/N310>
- [33] R. A. Shafik, M. S. Rahman, and A. H. M. R. Islam, "On the extended relationships among EVM, BER and SNR as performance metrics," in *Proc. IEEE ICECE*, 2006. doi: 10.1109/ICECE.2006.355657 pp. 408–411.